Secure Cooperative Spectrum Sensing Based on the Distance between Bodies of Evidence

Yi Wang¹, Yanjun Hu¹, Xiwen Tang¹, Yingguan Wang²

¹Key Laboratory of Intelligent Computing and Signal Processing, Ministry of Education, Anhui University, Hefei, China
²Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai, China

Email: ricky198324@yahoo.com.cn

Received September 21, 2011; revised November 6, 2011; accepted November 29, 2011

ABSTRACT

In cognitive radio (CR) networks, unlicensed secondary users need to conduct spectrum sensing to gain access to a licensed spectrum band. And cooperation among CR users will solve the problems caused by multipath fading and shadowing. In this paper, we propose a multi-threshold method at local nodes to cope with noises of great uncertainty. Functions of distance between bodies of evidence are used at fusion centre to make synthetic judgment. To guarantee security which is an essential component for basic network functions, we will take selfish nodes into account which try to occupy channels exclusively. The proposed technique has shown better performance than conventional algorithms without increase the system overhead.

Keywords: Cognitive Radio; Spectrum Sensing; Multiple Thresholds; Energy Detection; Evidence Theory

1. Introduction

Cognitive radio is able to fix concurrent problems of scarce spectrum resources and low utilization rate. As an indispensable part of cognitive radio, spectrum sensing can be applied to search for spectrum “space holes” and determine whether to make use of the frequency range, making itself the mostly studied section at present.

Spectrum sensing technologies can be sorted into single user and cooperative spectrum sensing [1]. When the primary user’s information is unknown, utilizing cooperative sensing technologies of multi-CR users exceeds single node algorithm [2] in terms of energy consumption and accuracy. Based on different ways of fusing sensing knowledge, regular fusion algorithms are usually divided into two methods consisting of hard information-combining (HIC) [3] and soft information-combining (SIC) [4]. HIC has relatively smaller communication flow. SIC has relatively smaller communication flow. SIC includes methods based on likelihood ratio detection and linearity. Besides, there are two other special fusion algorithms, one of which relies on relaying protocol and is suited to distributed systems, while the other of which relies on cluster tree[5], which actually is classified as hybrid fusion algorithm. MAC layer detection algorithm focuses on multi-channels and detection time [6]. The spectrum security with regards to malicious nodes gradually becomes the centre of attention [7].

With low SNR and interfering energy of relatively great uncertainty [8], most of the sensing methods cannot lead to correct results. Once every sensing node is in a disparate noise environment, the performance of HIC will be unstable and the capabilities of SIC will also be sharply decreased. The Dempster-Shafer theory [9] of evidence has been proposed for decision making [10] [11]. However, the existing conflict between various CR users is not managed properly by the conventional combination rules [12]. Considering the relevance between CR users, the article will propose an adaptive multi-threshold sensing method based on the distance between bodies of evidence on condition that flow load and algorithm complexity are not excessively augmented. The proposed sensing method achieves better performance in terms of such indexes as probability of false alarm and probability of misdetection.

2. System Description

Assuming there is a sensing network consisting of a fusion centre and N sensing nodes in the complex electromagnetic environment, as is shown in Figure 1.

Sensing nodes receive the noises, interferences and information from primary user simultaneously. Each one reflects as to its own surroundings, and then sends results to fusion centre which makes the final decision after receiving judgment results from all sensing nodes: primary user exists \((H_1)\) or primary user does not exist \((H_0)\):

\[
\begin{align*}
H_0 : y(t) &= n(t) \\
H_1 : y(t) &= x(t) + n(t)
\end{align*}
\]  

(1)
where $y(t)$ denotes mixed signal, $x(t)$ represents received signal from primary user, and $n(t)$ represents received noise.

For local nodes, energy detection is a simple and efficient method. It accumulates energy in a certain range of frequency. When the energy exceeds a certain threshold, it can be concluded that signal from primary user exists. After Nyquist sampling, received signal energy can be expressed as:

$$V = \sum_{i=1}^{N} |y_i|^2$$

(2)

The signal with duration of $T$ and bandwidth of $W$ can be represented by $N$ sampling points, while $N = 2TW$ is two times product of duration and band width.

If output sampling points are approximately regarded as independent gaussian variables, output energy meets chi square distribution. On the condition of $H_0$ and $H_1$, output statistics are subject to central and non-central chi square distribution with freedom degree of $N$ respectively. When $N$ stands at a certain large value, detection statistics can approximately be regarded in accordance with gaussian distribution [13]:

$$H_0 : \quad V \sim N\left(N\sigma_n^2, 2N\sigma_n^2\right)$$

$$H_1 : \quad V \sim N\left(N\left(\sigma_n^2 + \sigma_s^2\right), 2N\left(\sigma_n^2 + \sigma_s^2\right)^2\right)$$

(3)

where $\sigma_n^2$ represents noise variance, $\sigma_s^2$ represents signal average power.

### 3.1. New Spectrum Sensing Methods

#### 3.1. Multi-Threshold Detection Methods of Local Nodes

Noise uncertainty will lead to energy fluctuation. When the fluctuation goes up to a certain level, just a threshold value would not be enough to judge primary users accurately, since regular fluctuation can also lead to excessive uncertainty around the threshold. The article will adopt an adaptive multi-threshold detection method at local nodes to adjust to different SNR.

When the SNR is relatively small, if the noise fluctuation during a detection time appears to be large, it will raise probability of false-alarm or probability of missde-

tection:

$$V = \sigma_s^2 > V_r \quad \text{or} \quad V = \sigma_n^2 + \sigma_s^2 < V_r$$

(4)

Thus, this algorithm enables every CR user to utilize energy detection methods of two thresholds (TH2) or four thresholds (TH4) that corresponds to relatively large or small SNR respectively. The two thresholds of the former one are named as $T_1$ and $T_2$ and the detected energy is divided into three ranges, while the four thresholds of the later one are named as $T_{h1}, T_{h2}, T_{n1}$ and $T_i$ and the detected energy is divided into five ranges. The eight ranges are just demonstrated by three bits value, as is shown in Figure 2.

In four-threshold detection method of low SNR, the credibility of energy range 001 and 011 is relatively higher than that of the other three. 001 tends to represent that primary users do not exist while 011 represents the existence of primary users. When the SNR is high, two threshold detection methods should be used. In this situation, 101 and 111 have higher credibility than 110.

Before putting nodes into service, they need to go through an establishing stage when to get familiar with noises in the surroundings based on which the SNR can be determined, and then the threshold mode would be chosen to use. During the working process, the threshold mode can be switched if the SNR changes or sensing performance turns to be undesirable.

CR users are allowed to measure the noise energy received in the establishing stage when primary user does not send signals. The total measuring time is set as $nT$ which can be divided into $n$ stages, with the time for each stage set as $T$. Thus, peaks and valley values for $n$ stages can be obtained. Average these $n$ groups of data and multiply the average number by necessary coefficients so that $T_1$ and $T_2$ can be approximately obtained. Through multiplying all the measured values by their corresponding coefficients, such as 0.9 and 1.1, we can get $T_{n1}, T_2$ and $T_{n2}, T_i$.

After the fusion centre receives $N$ groups of binary number $r_i$ from CR users, the following evidence theory will be used to decide: $R_1$ primary user exists, $R_0$ it does not exist.

#### 3.2. Evidence Theory Determination of Fusion Centre

The information delivered from different CR users might
be diverse but undoubtedly related. The article will adopt the
functions of distance between two bodies of evidence [14] in evidence
type, and use parameters like the similarity of information transferred among nodes to
judge synthetically.

In view of basic belief assignment \( m \in [0, 1] \), \( m(A) \) represents the credibility level evidences have in event \( A \).
A few basic belief assignments are organized into a be-

\( m_i(A) \), \( m_i(B) \) and \( m_i(C) \) represent the credibility the

\( m_i \) represents the basic belief assignment of the

\( m_i \) represents the basic belief assignment of the \( i \)th user, and

\( A, B, C \) represent three focal elements respectively; therefore,

\( m_i(A), m_i(B) \) and \( m_i(C) \) represent the credibility the

\( m_i(A) \) and \( m_i(B) \) are supported to the existence of primary user, non-exis-
tence of primary user and uncertainty. Each of the eight
conditions for energy detection corresponds to one prob-

\( m_i(B) \) is a matrix of \( 3 \times 3 \), \( D_g = \begin{bmatrix} A_i \cap A_j \end{bmatrix} \). Thus,

the specific computing method of the distance between
two bodies of evidence is as follows:

\[ d(m_i, m_j) = \frac{1}{\sqrt{2}} \left( \| m_i \|_2^2 + \| m_j \|_2^2 - 2\langle m_i, m_j \rangle \right) \]  

(7)

where \( \| m_i \|_2 \) is the inner product

of \( m_i \) and \( m_j \).

Then, the similarity between two nodes can be ac-

\[ s_{ij} = 1 - d(m_i, m_j) \]

(8)

\( s_{ij} \in [0, 1] \) and \( s_{ij} = 1 \) can be easily drawn. All \( s_{ij} \) can be

indicated in one matrix to obtain the support of wholly

sensing network to node \( CR_i \)

\[ \text{Sup}(m_i) = \sum_{j=1, j \neq i}^{N} s_{ij} \]  

(9)

The bigger the value of \( \text{Sup}(m_i) \), the more supported
the node \( CR_i \), and the more the fusion centre relying on it. All \( \text{Sup}(m_i) \)s need to be normalized to get the weight of

nodes when combining:

\[ Rl(m_i) = \frac{\text{Sup}(m_i)}{\sum_{j=1}^{N} \text{Sup}(m_j)} \]  

(10)

The probability distribution after combination can be

achieved through Equation (5) and (10):

\[ \begin{bmatrix} m(A) \\ m(B) \\ m(C) \end{bmatrix} = \begin{bmatrix} m_1(A) & \cdots & m_N(A) \\ \vdots & \ddots & \vdots \\ m_1(C) & \cdots & m_N(C) \end{bmatrix} \begin{bmatrix} Rl(m_1) \\ \vdots \\ Rl(m_N) \end{bmatrix} \]  

(11)

When \( m(A)/m(B) > 1 \), the probability of primary user’s
existence is relatively higher; Or according to the objective
probability of false alarm and probability of misdete-
tection, a certain proportion value \( p \) should be set up, and

then when \( m(A)/m(B) > p \), primary user exists.

\( CR_i \) in Figure 1 might be a selfish node to occupy

channels exclusively to claim the existence of primary

user. In this algorithm, selfish nodes would try to send

the message of “011” or “111”. Thus, common work of

primary user would be dramatically influenced, and the

sensing abilities of other nodes would be seriously

weakened. The safety coefficient \( sc_i \) will be used to avoid

such a phenomenon as follows:

\[ \text{if } (R_g \& r_i = 011) \& (R_e \& r_i = 111), \quad sc_{i+1} = sc_i + 1 \]

\[ \text{else if } (R_g \& r_i = 011) \& (R_e \& r_i = 111) \& (sc_i \neq 1), \quad sc_{i+1} = sc_i - 1 \]

\[ sc_i = \frac{1}{1 + sc_i} \]  

(12)

New weight is drawn through Formula (10):

\[ Rlnew(m_i) = sc_i \times Rl(m_i) \quad i = 1, 2 \cdots, N \]  

(13)

This enables the whole system to identify selfish nodes
to lower adverse influences to the greatest extent. A cer-
tain test result can also be set up, so when the safety co-
efficient is less, fusion centre would ditch the informa-
tion of the relevant node.

4. Simulation Results

This section will test the performance of the algorithm
(SCS) through simulation. To make the experimental results more universal, relatively small product of duration and bandwidth $TW = 5$ is chosen. Primary user sends BPSK modulating signal the existence probability of which is 50%, assuming channel noises are gaussian white noise.

Comparison algorithms select the classical algorithms of “OR” and “AND” that all belong to HIC methods. In the algorithm of “OR”, as long as one of the sensing nodes detects primary user, it would be regarded as exists. In the algorithm of “AND”, only if all sensing nodes detect primary user, can it be regarded as exists.

As in Figures 3 and 4, the SNR is set up as 1dB and there are 3 and 6 sensing users respectively, two technical indexes including probability of false alarm and probability of misdetection are utilized. From the comparison with two classical algorithms, the algorithm in the article is with better performance and from two pictures lower probability of misdetections can all be gained under the same probability of false-alarm. When the number of CR users raises from 3 to 6, the three algorithms’ curves all move downwards but the capabilities of this algorithm increase more obviously.

Taken the complex physical background into consideration, every CR user might be in an environment with distinct SNR. In Figure 5, assuming there are five nodes, the SNR are –3, –1, 0, 1 and 3 dB respectively. It is easily seen that due to the existence of nodes with high SNR, the algorithm of “OR” is better than “AND”, but in comparison, the algorithm in the article is still able to achieve better performance.

Figure 6 plays the role to investigate safety coefficient, in which ten users are involved and comparisons are made with 0 ~ 5 selfish nodes. The same local thresholds are used and the probability of misdetection turns to be less than 10%. The results demonstrate that when the number of selfish nodes surpasses two, the safety coefficient still guarantees the probability of false alarm to

![Figure 3. Complementary ROC curves (CR = 3, SNR = 1 dB).](image3)

![Figure 4. Complementary ROC curves (CR = 6, SNR = 1 dB).](image4)
remain at the quite low level.

5. Conclusion

We have proposed a secure spectrum sensing method based on functions of distance between two bodies of evidence. The simulation results have shown that the proposed sensing technique achieves good performance on condition that no excessive communication flow is added. With the growth of CR users, the probability of detection will also be enhanced. When all CR users are with disparate SNR, primary user can still be precisely detected. The proposition of safety coefficient also gives the system the capability to deal with the assault of several selfish nodes to improve the reliability. However, the study also indicates that when there are not so many nodes and SNR is relatively low, probability of false alarm will not be very high. We will discuss this issue in the future.

6. Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61071168) and the 211 Project of Anhui University.

REFERENCES


Copyright © 2012 SciRes.