Wireless Sensor Network, **2011, 3, 83-91**
doi:10.4236/wsn.2011.33009 Published Online March 2011 (http://www.SciRP.org/journal/wsn)

A Fault-Tolerant Cooperative Spectrum Sensing Algorithm over Cognitive Radio Network Based on Wireless Sensor Network

Mohammad Akbari, Abolfazl Falahati
Department of Electrical Engineering (*School of Secure Communication*), *Iran University of Science and Technology, Narmak, Tehran*
E-mail: *m_akbari@elec.iust.ac.ir, afalahati@iust.ac.ir*
Received January 25, 2011; *revised February* 15, 2011; *accepted March* 8, 2011

Abstract

A serious threat to cognitive radio networks that sense the spectrum in a cooperative manner is the transmission of false spectrum sensing data by malicious sensor nodes. SNR fluctuations due to wireless channel effects complicate handling such attackers even further. This enforces the system to acquire authentication. Actually, the decision maker needs to determine the reliability or trustworthiness of the shared data. In this paper, the evaluation process is considered as an estimation dilemma on a set of evidences obtained through sensor nodes that are coordinated in an underlying wireless sensor network. Then, a likelihood-based computational trust evaluation algorithm is proposed to determine the trustworthiness of each sensor node's data. The proposed procedure just uses the information which is obtained from the sensor nodes without any presumptions about node's reliability. Numerical results confirm the effectiveness of the algorithm in eliminating malicious nodes or faulty nodes which are not necessarily conscious attackers.

Keywords: Cognitive Radio Network (CRN), Cooperative Spectrum Sensing, Wireless Sensor Network (WSN), Trust Evaluation, Maximum Likelihood Estimation (MLE)

1. Introduction

One of the main limitations in developing next generation networks and new services for the existing networks is bandwidth scarcity. Cognitive radio network is a novel idea that will overcome the spectrum scarcity problem with providing the capability of sharing the wireless channel between unlicensed users (secondary users (SU)) and licensed users (primary users (PU)) in an opportunistic manner. The PUs take precedence of the SUs in spectrum access; a cognitive radio should not communicate on a channel that is being used by a licensed user [1-2]. This point makes the spectrum sensing process an essential, a process for discovering the spectrum holes or discovering the presence of an active PU in the desired band.

The spectrum sensing procedure can be accomplished individually or in a cooperative manner. Cooperative spectrum sensing itself might be accomplished via either *decision fusion* or *data fusion* [3]. In a data fusion scheme, SUs share their primary collected data from RF stimuli in a Fusion Center (FC) which decides the presence or the absence of the PUs in the desired band using the shared information. However, in a decision fusion approach the CR nodes send their decision (that are made individually) to FC for final decision. Match filtering; cyclo-stationary feature detection and energy detection are three well-known methods which are used to sense the CR spectrum [4]. The proposed method in this paper is based on energy detection

A. Taherpour *et al.* [5] proposed an energy-detection based data fusion method and show that in fading channels Equal Gain Combining (EGC) data fusion has near-optimal performance without the requirement of channel gains estimation. According to their method if the measured energies average that is reported by coordinated nodes becomes larger than a specific threshold value the presence of the PU can be assumed to be true, otherwise the absence of the PU becomes true. They have shown that when the SNRs of the SUs are large enough the detector approaches the optimum detector. However, Signal to Noise Ratio (SNR) fluctuations due

to multipath effects can complicate the spectrum sensing operation. We will show that by employing this method in a wireless channel condition, a poor performance is observed when the SNR at the SU's receivers are not necessarily high. Under such conditions, an accurate knowledge of the sensing statistics is required for collaborated spectrum sensing to form adequate decision statistics [6]. Estimation and deployment of these statistics in a hypothesis test approach are the main focus of this paper. To this end, we consider data fusion scheme as the final rule for incumbent detection.

The requirement to collect the information about energy distribution in the coverage area of the network naturally leads us to resort to an underlying wireless sensor network. The idea of deploying an underlying WSN to facilitate the spectrum sensing operation is utilized in several works such as [7-8]. S. Shankar *et al.* [7] propose a spectrum-aware sensor network architecture that can be used in collecting information about the spectrum opportunities throughout a CR network. But they do not propose any data fusion method or decision approach that is based on the collected data. [8] employs the WSN capability in measuring Revived Signal Strength (RSS) to solve the PU transmitter localization problem and developing a method for defense against Primary User Emulator Attackers (PUEA).

Wireless sensor network is one of the most compelling technologies comprising a large number of sensor nodes cooperatively monitor environment or perform surveillance tasks [9,10]. The architecture we utilized here to address the spectrum sensing issue is based on a sensor networks which is deployed for the spectrum sensing purpose. The network composed of many distributed nodes each of which measure the energy level of the desired band and communicate the measured value to the FC (sink node) for final decision about the occupancy of the desired frequency band. The sensor network can be either a dedicated WSN that is fully employed for spectrum sensing goal or cognitive sensor nodes that opportunistically make use of the spectrum as well as spectrum sensing. In the later case, each CR nodes must be equipped with a sensor module. Regardless of which architecture is deployed we use the term *sensor node* to refer to the node witch sense the spectrum. **Figure 1** depicts a typical network with the model of just mentioned cognitive WSN network architecture.

Beside the wireless channel effect, another source of ambiguity that is of concern in this paper is false spectrum sensing data that might be reported by some malicious nodes. Although so far several methods have been proposed for cooperative sensing and their performance have been studied extensively [3,11,12], most of previous works assume that the sensing nodes are completely reliable, but, what does happen if some of the coordinated nodes report false data intentionally? A serious threat to cognitive radio networks which sense the spectrum in a cooperative manner is the transmission of false spectrum sensing data by malicious secondary nodes. In this case, attacker (attackers) through false data injection in CRN database try to fool CRN and stimulate the CR nodes to use channels occupied by PUs or prevents the SUs from using the empty channels. In the literature, the term *spectrum sensing data falsification attack* (*SSDFA*) is used to refer to such an attack [13-15].

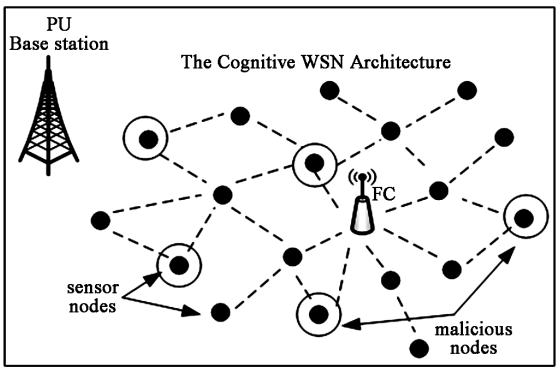

Figure 1. A typical distributed cognitive wireless sensor network that senses the spectrum in a cooperative scheme.

Due to cooperation and statistical data valuation, the proposed cooperative method is inherently resistant against misinformation but when the number of malicious nodes increases the false reports can degrade the performance. The other source of data falsification is when the sensors do not function properly. Therefore, the data fusion method to be employed in coordinated nodes must be robust against fraudulent local spectrum-sensing output that would be reported by either malicious nodes or faulty nodes. Our proposed method acquires this robustness by developing a soft trust management process among the sensor nodes. To this end, the likelihood of the reported observations are deployed to assign a trust factor to each report; the trust factor of a particular report determine the portion of that reported value on the final decision making in FC. This paper extends *our previous work* [16] on cooperative spectrum sensing by taking into account the effect of small scale multipath fading on the PU signal which is received at the sensor nodes as well as the effect of presence some SSDF attackers.

The rest of the paper is organized as follows. In section 2, the system model will be described. The proposed trust evaluation algorithm is introduced in section 3, and the numerical results are depicted in section 4. Section 5 concludes the remarks.

2. Basic Assumptions and System Model

A cooperative spectrum sensing scheme employing energy detection under fading channel condition is considered as illustrated in **Figure 1**. It is assumed that a total number of N sensor node in an underlying WSN are coordinated to detect the spectrum holes of a frequency band which is licensed for primary users of a primary network. The sensor nodes send their collected data to the fusion center for final decision for the absence or the presence of primary users in the desired frequency band [13,14,16].

The channel model between primary base station and sensor nodes is assumed to be Nakagami multipath fading [17-21]. The observation time interval T is small enough to presume that all received signal at energy detectors (CR nodes) experience the same fading condition during the observation. Besides uncertainty of reported energy that is measured by sensor devices due to multipath fading phenomena and/or their malfunctioning behaviour, it must be considered that a group of malicious nodes may try to misinform the FC. This issue is shown in **Figure 1** where the attacker nodes with a circle drawn around them are determined. **Figure 2** depicts the fusion center block diagram with the following variables:

$\boldsymbol{E}$ [1]: A $1\times N$ vector, represents reported energy of desired channel measured by N sensor nodes.

$\overline{\boldsymbol{E}}$: Prefiltering output, a $1\times M$ vector.

TF_i : Trust factor assigned to i^{th} sensor node

The actual model performance is obtained by performing three procedures namely pre-filtering, trust evaluation and data fusion. The sensor nodes use an energy detector for sensing the spectrum. if $r(t)$ represents the PU signal at the energy detector input of the sensor nodes under two hypotheses H_0 or H_1, *i.e.* absence or presence of a legitimate signal respectively, then:

$$r(t)=\begin{cases} n(t) & H_0 \\ s(t)+n(t) & H_1 \end{cases} \tag{1}$$

where, $n(t)$ is an Additive White Gaussian Noise (AWGN) with zero mean and variance of $N_0/2$; $s(t)$ represents the primary user signal which is influenced by the wireless channel. It is assumed that the sensor nodes sense the spectrum synchronously; thanks to the underlying WSN, the FC will be able to obtain a snapshot of the current state of signal energy distribution in its coverage area through the WSN network. This Synchronization can be obtained easily by a beacon transmission through central node or other well-known methods such as GPS [22].

[1]Hereinafter, we indicate the vectors with bold-face capital letters, random processes with capital letters indexed by time variable (e.g. X(t)), random variables with capital letters and others with minuscule letters.

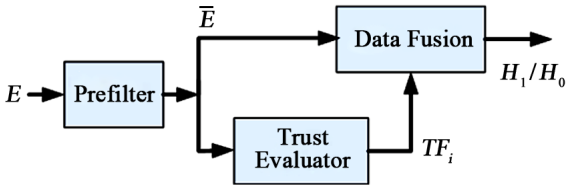

Figure 2. Fusion center block diagram representation.

3. Cooperative Spectrum Sensing Algorithm Based on Statistical Data Assessment

In the following, each one of the three components of the proposed method will be described in detail.

3.1. Prefiltering

In order to determine the trustworthiness of the sensor node's reports, a trust management process is developed throughout the sensor network. The trust evaluation algorithm is formulated as an estimation problem on a set of evidences $\boldsymbol{E}[k]=\{e_i[k], 1\le i\le N\}$ obtained from distributed sensor nodes in k^{th} sensing time. Very large or very small malicious node's reported values, depending upon the channel state, can extremely affect the estimated parameters and the trust evaluation. After receiving the reported $e_i[k]$s, pre-filter rejects these outliers that do not match the other reports. The chosen method for the outlier detection is a simple but efficient algorithm that is suitable to identify outliers with extreme different values in comparison with the others in a set [23]. Based on this algorithm, any particular value of the set of reported energy $e_i[k]$s should be tested to be in $[e_l, e_u]$ interval, otherwise, that value will be known as outlier. The upper bound e_u, and lower bound e_l, for values $e_i[k]$ s can be determined as [23]:

$$\begin{aligned} e_u &= \mu+3\sigma \\ e_l &= \mu-3\sigma \end{aligned} \tag{2}$$

where, μ and σ are mean and standard deviation of the set of $e_i[k]$s respectively.

3.2. Statistical Assessment and Trust Assignment to the Observations

1) *Trust Inference* (*Statistical Assessment*) *of The Observation over AWGN Channel:* It is well-known that under the AWGN channel condition assumption, in the absence of any deterministic signal, the reported random

variable $e_i[k]$ (which is normalized by two sided noise power spectral density $N_0/2$) will have a central Chi-square distribution. However, if a deterministic signal with energy E_s is present at the energy detector input, the reported value of $e_i[k]$ will have a noncentral Chi-square distribution [24] as:

$$E_i \sim \begin{cases} \chi^2_{2TW} & H_0 \\ \chi^2_{2TW}\left(2E_s/N_0\right) & H_1 \end{cases} \tag{3}$$

T, *W* and E_s are the observation time, channel band width and signal energy average $\left(E_s = \int_0^T s(t)^2 \,\mathrm{d}t\right)$ respectively. After prefiltering, we will have a vector of *M* values $e_i[k](i=1,\cdots,M)$ which are samples of *M* random processes E_i with known distribution (central Chi-square or noncentral Chi-square) but unknown parameters value.

The principle of maximum likelihood (ML) assumes that the sample data set $\overline{E}$ represents the $f_{\overline{E}}\left(e_1,\cdots,e_M;\overline{\theta}\right)$ population and it chooses those values for $\overline{\theta}$ that most likely cause the observed data to occur [25]. So, given $E_i = e_i[k]$ $(i=1,\cdots,M)$, the ML estimate for $\overline{\theta}$ can be determined from the likelihood equation as [25]:

$$\hat{\theta}_i = \max_{\theta_i} f_{\overline{E}}\left(e_1,\cdots,e_M;\overline{\theta}_i\right) \tag{4}$$

hence,

$$\left.\frac{\partial \log f_{\overline{E}_i}\left(e_1,\cdots,e_M;\overline{\theta}_i\right)}{\partial \overline{\theta}_i}\right|\hat{\theta}_i = 0 \tag{5}$$

It is supposed that the sensor nodes are distributed in a large geographical area, so it can be said that the received signal at each sensor experiences identical independent channel condition (i.i.d.) [5], thus:

$$f_{\overline{E}_i}\left(e_1,\cdots,e_M;\overline{\theta}_i\right) = \prod_{i=1}^{M} f_{E_i}\left(e_i,\overline{\theta}_i\right) \tag{6}$$

Now, using ML estimator (MLE), we will be able to estimate the probability distribution $f_{E_i}\left(e_i,\overline{\theta}_i\right)$. But what is the pdf type of the observation? Central Chi-square or noncentral Chi-square? In order to give a precise estimation on the parameters, we should know the pdf type of the process which is sampled by sensor nodes. This means, we should know the presence or absence of the PU in the under investigation band. To break the tie, we use an approximation model known as *Torrieri model* [26] that approximates a chi-square (central or noncentral) as a Gaussian distribution:

$$E_i \sim \begin{cases} N\left(\mu_0,\sigma_0^2\right) & H_0 \\ N\left(\mu_1,\sigma_1^2\right) & H_1 \end{cases} \tag{7}$$

where μ_0 and σ_0^2 are the mean and variance of the energy detector output when H_0 is correct (*i.e.* no signal present), and μ_1 and σ_1^2 are the mean and variance of the energy detector output when H_1 is correct. If $TW \gg 1$ is satisfied the given model provide an adequate accuracy [26]. Substitution of (7) into (6) and employment of (5), the e_i s distribution parameters can be estimated in a straight forward manner. For a normal distribution, as indicated in (8), it can be shown easily that *MLE* gives a simple closed form equation to estimate $\left(\mu_i,\sigma_i^2\right)$ parameters that will be suitable for a frequently used evaluation algorithm:

$$\begin{aligned} \mu_r &= \frac{1}{M}\sum_{i=0}^{M} e_i \qquad r=0,1 \\ \sigma_r^2 &= \frac{1}{M}\sum_{i=0}^{M}\left(e_i-\mu_r\right)^2 \quad r=0,1 \end{aligned} \tag{8}$$

Utilizing (8), we will be able to estimate the unknown parameters introduced in (7). In fact, (7) determines the probability distribution function for received power over the channel and also provides valuable information for FC to determine the expectancy of reported data. This expectancy helps FC to obtain the reliability of the node's reports that can be used to eliminate the malicious users influence on the primary user detection. The proposed algorithm steps for trust factor evaluation are summarized as follows:

1) Given detected energies $e_i[k](i=1,\cdots,M)$, first estimate the mean and variance of $e_i[k]$ probability distribution function through (8),

2) Assign unnormalized trust factor $TF_i^{'}$, to i^{th} detected energy,

$$TF_i^{'} = f_{E_i}\left(E_i = e_i[k]\right) \tag{9}$$

3) Normalized trust factor $TF_i^{'}$ for i^{th} CR user in k^{th} iteration will be as:

$$TF_i = \frac{TF_i^{'}}{\sum_{i=1}^{M} TF_i^{'}} \tag{10}$$

It is worth noting that the normalized-computed trust factor in (10) just determines the portion of corresponding nodes in final spectrum decision. One should consider that the trust factor of a node in comparison with trust factor of the other nodes would be a meaningful value. To include the pre-determined TF_i s values, the calculation of TF_i in previous subsection is modified as:

$$TF_i[k] = \sum_{p=1}^{H} \alpha_p TF_i[k-p] + \alpha_0 TF_i \tag{11}$$

This means, the trust factor $TF_i[k]$ in k^{th} iteration is

the weighting average of the current evaluated trust factor TF_i which is assigned to $e_i[k]$ and *H-1* previously determined trust factors $TF_i[k-p]$ $(p=1,\cdots,H-1)$. $0<\alpha_p<1$ determines the portion of $(k-p)^{th}$ assigned trust factor in the k^{th} iteration and is defined as:

$$\alpha_p=\frac{(1-p/H)^{\beta}}{\sum_{p=0}^{H-1}(1-p/H)^{\beta}} \tag{12}$$

$\beta\geq 1$ and H are the actual design parameters. $\beta=1$ corresponds to a linear decrease in participation of older judgments. Whatever a larger value to be selected for β, the older judgment participation decreases much faster.

2) *Trust Inference (Statistical Assessment) of The Observation over Nakagami fading channel:* When the received signal experiences the multipath fading condition, (3) is true for H_0 hypothesis only. Because, in the absence of the legitimate signal the energy detector just measures the noise energy level of the channel thus its distribution depends on the noise model only.

To solve this problem, we rewrite $P(e_i[k]|H_1)$ as

$$P(e_i[k])=P(e_i[k]|H_0)P(H_0)+P(e_i[k]|H_1)P(H_1)\cdot P(e_i[k]|H_0)$$

follows a central chi-square distribution but $P(e_i[k]|H_1)$ is generally unknown. In the following, we determine the conditional probability of $P(e_i[k]|H_1)$ if the PU's signal experiences a Nakagami multipath fading channel with parameter m. In this case, probability density function of instant received power p at energy detector is [17]:

$$f_p(p\,|\,H_1)=\left(\frac{m}{P_r}\right)^m\frac{p^{m-1}}{\Gamma(m)}\mathrm{e}^{\frac{-mp}{P_r}} \tag{13}$$

From (13), the probability density function of $P(E_i=e_i[k]|H_1,p)$ is a noncentral Chi-square distribution $\chi^2_{2TW}(2pT/N_0)$ with two parameters $2TW$ and $2pT/N_0$ which determine the degree of freedom and the noncentrality respectively [24]. Therefore:

$$P(E_i=e_i[k]|H_1)=\int_0^{\infty}P(E_i=e_i[k]|H_1,p)f_p(p|H_1)\mathrm{d}p \tag{14}$$

where P_r is the average received power. Furthermore, $P(e_i[k]|H_1)$ can be rewritten as:

$$\begin{aligned}&P(E_i=e_i[k]|H_1,p)\\&=\frac{1}{2}e^{-\frac{e_i[k]+\frac{2pT}{N_0}}{2}}\times\left(\frac{e_i[k]N_0}{2pT}\right)^{\frac{1}{2}(TW-1)}\\&\times I_{k/2-1}\left(\sqrt{e_i[k]2pT/N_0}\right)\end{aligned} \tag{15}$$

where $I_x(\cdot)$ is a modified Bessel function of the first kind. Substitution of (15) and (13) in (14) produce a complex expression for $P(E_i=e_i[k]|H_1)$ which can be solved numerically. Thus, in order to obtain an analytical closed form expression, an approximate solution is desired. To achieve this goal, we use an approximation model known as Torrieri model [26] that approximates a noncentral chi-square $\chi^2_{2TW}(2pT/N_0)$ as a Gaussian distribution with mean and variance of N_0TW+pT and $N_0^2TW+N_0pT$ respectively. If $TW\gg 1$ is satisfied, the given model provides an adequate accuracy [26,27]. Utilizing (13) and applying the normal approximation, (14) can be rewritten as:

$$\begin{aligned}&P(E_i=e_i[k]|H_1)\\&=\int_0^{\infty}\frac{1}{\sqrt{2\pi(N_0^2TW+N_0pT)}}\\&\times\mathrm{e}^{-\frac{(e_i[k]-N_0TW-pT)^2}{2N_0^2TW}}\left(\frac{m}{P_r[k]}\right)\frac{p^{m-1}}{\Gamma(m)}\mathrm{e}^{\frac{-mp}{P_r[k]}}\mathrm{d}p\\&=\int_0^{\infty}\frac{\left(\frac{m}{P_r}\right)^m}{\Gamma(m)T^{m-1}\sqrt{2\pi\left(N_0^2TW+N_0pT\right)}}\\&\times p^{m-1}\mathrm{e}^{-\frac{(e_i[k]-N_0TW-pT)^2}{2N_0^2TW}-\frac{mp}{TP_r[k]}}\mathrm{d}p\end{aligned} \tag{16}$$

In low power detection schemes, *i.e.* when the SNR at energy detector is small, the signal of $s(t)$ has a little effect on the variance of the test statistics [26]. So, we can ignore N_0pT and assume that the variance of the PU signal is $N_0{}^2TW$ in either decision cases. Considering these assumptions and performing some mathematical manipulation, (16) will be simplified as:

$$P(E_i=e_i[k]|H_1)=C_1\int_0^{\infty}\frac{p^{m-1}}{\sqrt{2\pi N_0^2TW}}e^{-\frac{(p-C_2)^2}{2N_0^2TW}}\mathrm{d}p \tag{17}$$

where, C_1 and C_2 are given by:

$$\begin{aligned}C_1&=\frac{\left(\frac{m}{P_r}\right)^m}{\Gamma(m)T^m}\mathrm{e}^{\frac{-2mN_0^2WP_r[k]^{-1}(e_i[k]-N_0TW)+m^2N_0^4P_r[k]^{-2}W^2}{2N_0^2TW}}\\C_2&=e_i[k]-N_0TW-mP_r[k]^{-1}N_0^2W\end{aligned} \tag{18}$$

Finally, using the well-known properties of the Gaussian function can be easily shown that:

$$\begin{aligned}&P(E_i=e_i[k]|H_1)\\&=C_1\int_0^{\infty}\frac{p^{m-1}}{\sqrt{2\pi N_0^2TW}}e^{-\frac{(p-C_2)^2}{2N_0^2TW}}\mathrm{d}p\end{aligned}$$

$$= C_1 \lim_{s\to 0} \frac{\partial^m}{\partial s^m} \left(\int_0^\infty \mathrm{e}^{sp} \frac{1}{\sqrt{2\pi N_0^2 TW}} \mathrm{e}^{-\frac{(p-C_2)^2}{2N_0^2 TW}} \mathrm{d}p \right)$$

$$= C_1 \lim_{s\to 0} \frac{\partial^{m-1}}{\partial s^{m-1}} \left(\mathrm{e}^{sC_2 + \frac{s^2 N_0^2 TW}{2}} Q\left(\frac{-\left(C_2 + sN_0^2 TW\right)}{\sqrt{N_0^2 TW}} \right) \right) \quad (19)$$

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \mathrm{e}^{-x^2/2} \mathrm{d}x$$

where, is the Gaussian Q-function. Equation (19) provides a closed-form relationship for computing $P\left(E_i = e_i[k] \middle| H_1\right)$. Finally, our proposed relationship for determining the conditional probabilities $P\left(E_i = e_i[k] \middle| H_1\right)$ and $P\left(E_i = e_i[k] \middle| H_0\right)$ will be as follows:

For a channel model with specific value of the parameter *m*, (20) should be calculated as a function of $e_i[k]$ only once and to be used repeatedly. In order to determine (20) for channel models with different values of parameter *m*, higher order derivatives of the *Q* function is necessary. It can be easily shown that:

$$Q^{(n)}(x) = \frac{a_n(x)}{\sqrt{2\pi}} e^{-x^2/2}$$
$$a_{n+1}(x) = a_n'(x) - x a_n(x),\ a_1(x) = -1 \quad (21)$$

Now, substituting (20) into

$$P\left(e_i[k]\right) = P\left(e_i[k] \mid H_0\right) P(H_0) + P\left(e_i[k] \middle| H_1\right) P(H_1)$$

we will be able to determine the likelihood of each prefiltered report $e_i[k]$ and determine the trust factor following the steps of trust evaluation algorithm that is presented in part 1.

3.3. Data Fusion Algorithm

Final decision for the presence or the absence of primary user in desired frequency band is devolved to data fusion block. This block deals with a group of reported energies with their known trust factors that are computed from (11). Generally speaking, every existing data fusion approach which is modified to include the reliability of each component can be deployed. The simplest one is weighting average combination scheme:

$$\sum_{i=1}^{K} \lambda_{i,k} e_i[k] = E \quad (22)$$

where $\lambda_{i,k}$ is weighting factor for particular $e_i[k]$ component and for our model is considered as its evaluated trust factor $\lambda_{i,k} = TF_i[k]$.

Final decision for hypothesis H_0 or H_1 is based on the calculated weighting average *E*, *i.e.* if $E > e_T$ is correct the channel is occupied, otherwise, the channel is empty. Where, e_T is a function of false alarm probability P_{fa}, and should be evaluated numerically. P_{fa} determines the probability that a free channel (spectrum hole) is imagined occupied wrongly.

4. Performance Evaluation

Using computer simulation, the performance of the proposed spectrum sensing method is evaluated and is compared with the reference model (EGC) as bearing the following steps:

4.1. Simulation Setup

Assume a group of *N* sensor nodes that are coordinated to sense the spectrum with the model as shown in **Figure 1**. The channel model between the CR nodes and the PU's base station is assumed to be Nakagami with $m = 1$, *i.e.* a Rayleigh fading channel. Mean received SNR at the CR users considered to be –10 *d*B*m*. Observation interval *T* and channel bandwidth *W* are chosen such that *TW* = 100. *H* and β both are chosen to be 3. e_T is determined numerically such that $P_{fa} = 0.01$ when no malicious node is present. The conditional probability of (20) for $m = 1$ will be as:

$$P\left(E_i = e_i[k] \middle| H_i\right) = \begin{cases} \dfrac{e_i[k]^{(TW-1)} \mathrm{e}^{-e_i[k]/2}}{2^{TW}\Gamma(TW)} & H_i = H_0 \\ \dfrac{1}{P_r[k]T} \mathrm{e}^{\frac{-2WP_r[k]^{-1}\left(e_i[k] - N_0 TW\right) + N_0^2 P_r[k]^{-2} W^2}{2TW}} \times Q\left(\dfrac{-e_j^f[k] + N_0 TW + P_r[k]^{-1} N_0^2 W}{\sqrt{N_0^2 TW}} \right) & H_i = H_1 \end{cases}$$

$$P\left(E_i = e_i[k] \mid H_i\right) = \begin{cases} \dfrac{e_i[k]^{(TW-1)} \mathrm{e}^{-e_i[k]/2}}{2^{TW}\Gamma(TW)} & H_i = H_0 \\ C_1 \lim\limits_{s\to 0} \dfrac{\partial^{m-1}}{\partial s^{m-1}} \left(\mathrm{e}^{sC_2 + \frac{s^2 N_0^2 TW}{2}} Q\left(\dfrac{-\left(C_2 + sN_0^2 TW\right)}{\sqrt{N_0^2 TW}} \right) \right) & H_i = H_1 \end{cases} \quad (20)$$

Although this relationship may at first seem complicated; in fact, considerable parts of this relationship are fixed values that need to be calculated only once. To evaluate

$$P\left(e_i[k]\right) = P\left(e_i[k]\middle|H_0\right)P\left(H_0\right) + P\left(e_i[k]\middle|H_1\right)P\left(H_1\right)$$

and make the final decision for hypothesis H_0 or H_1 for the fading channel case, the priority probabilities of $P\left(H_0\right)$ and $P\left(H_1\right)$ must be determined. Several methods are proposed for estimating these parameters, one of which is the method that is proposed by H. Kim in [28]. Without loss of generality, for simplicity in the simulation we assumed that $P\left(H_0\right) = P\left(H_1\right) = 0.5$.

To evaluate the performance of the given method, two prevalent parameters P_{fa} (false alarm probability) and P_d (detection probability) are considered. P_{fa} determines the ability strength of the applied method for detecting the spectrum holes and has impact on the spectral efficiency of the CRN; but, P_d determines the ability strength of the employed method in detecting and avoiding interference with the PUs. If H_i shows the decision about channel occupancy at the FC, false alarm and detection probability are defined as:

$$\begin{aligned} P_{fa} &= P\left(H_i = H_1\middle|H_0\right) \\ P_d &= P\left(H_i = H_1\middle|H_1\right) \end{aligned} \tag{23}$$

4.2. Simulation Results

To test the power of the proposed method in eliminating the effect of malicious sensor nodes or faulty nodes in the process of decision making about channel occupancy, worst condition is assumed; *i.e.*, when the channel is occupied, malicious nodes report the smallest possible value which can be passed from the pre-filter block, but when the channel is free, malicious nodes report largest possible value which can be passed from the pre-filter.

The false alarm probability of the proposed method for N = 50, N = 100, N = 200, N = 200 and N = 300 are depicted in **Figure 3** and is compared with EGC method [5]. As can be seen from **Figure 3**, the proposed trust algorithm works quite well in the presence of noticeable percentage of malicious nodes. The effect of malicious nodes, up to 18% of total nodes, is eliminated completely; Whereas, in similar conditions and for the same malicious nodes number, false alarm probability corresponding to EGC method is bigger than 0.97.

Figure 4 shows the detection probability of the proposed method in comparison with EGC. When the malicious node percent increase to 22%, the performance of simple averaging and our trust algorithm becomes similar. However, the performance of simple averaging decreases drastically for higher percentages of malicious nodes. When 30% of cooperating nodes are malicious, the detection probability of simple averaging is decreased to 0.5, whereas, the detection probability of proposed trust algorithm is bigger than 0.97.

However, the performance of simple averaging decreases drastically for higher percentages of malicious nodes. When 30% of cooperating nodes are malicious, the detection probability of simple averaging is decreased to 0.5, whereas, the detection probability of pro posed trust algorithm is bigger than 0.97.

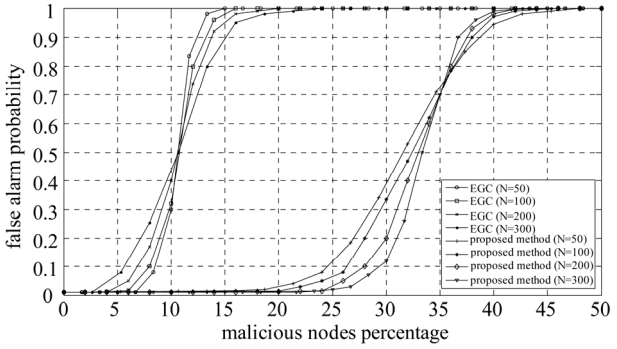

Figure 3. False alarm probability P_{fa} of the proposed method and EGC vs. malicious nodes percentage.

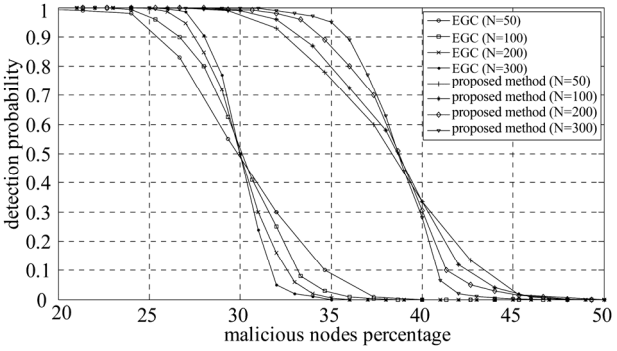

Figure 4. Detection probability P_d of the proposed method and EGC vs. malicious nodes percentage.

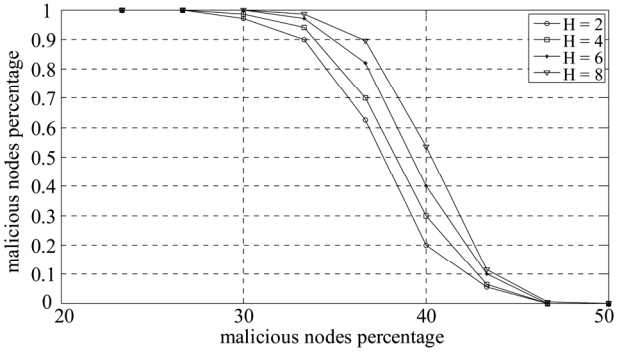

Figure 5. The effect of H on P_d.

The effect of H and β parameters, defined in section 3.2, on P_d are illustrated in **Figure 5** and **Figure 6** respectively. These parameters determine the portion of the previous judgments on current evaluation. Simulation results show that, this inclusion can improve the elimination of malicious nodes effect, and whatever the inclusion of the pre-determined values increase, the performance increases too. Also, the effect of H and β parameters on P_{fa} are depicted in **Figure 7** and **Figure 8** respectively. The total number of sensor nodes, N, are assumed to be 300.

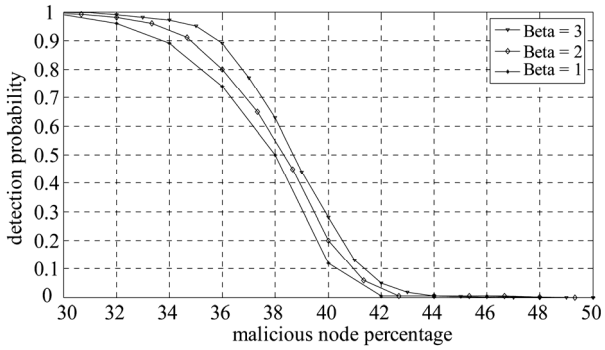

Figure 6. The effect of β on P_d.

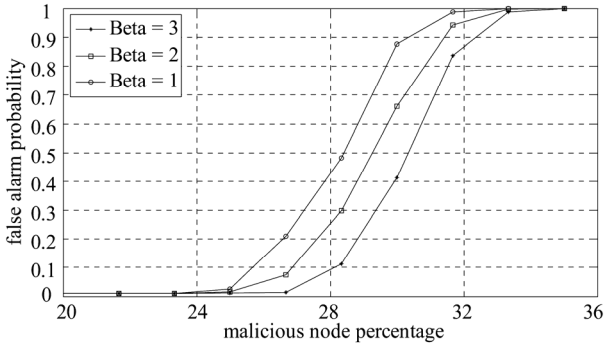

Figure 7. The effect of β on P_{fa}.

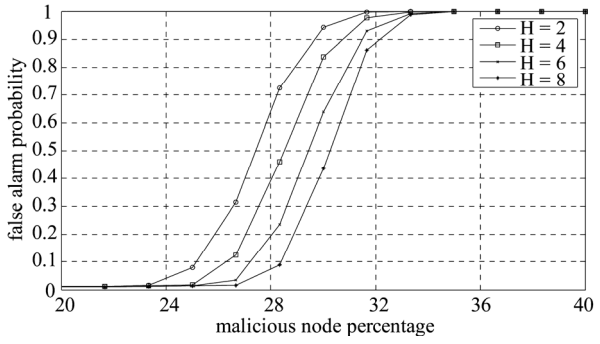

Figure 8. The effect of H on P_{fa}.

5. Conclusion

A computational trust evaluation algorithm was proposed to overcome malicious nodes trying to misinform CRN or the false data that might be reported by faulty nodes in a cooperative spectrum sensing process. The evaluation process is considered as an estimation dilemma on a set of evidences obtained from an underlying wireless sensor network. The network composed of many distributed nodes each of which measure the energy level of the desired band and communicate the measured value to the sink node for final decision about the occupancy of the desired frequency band. The sensor network can be either a dedicated WSN that is fully employed for spectrum sensing goal or cognitive sensor nodes that opportunistically make use of the spectrum as well as spectrum sensing. Utilizing the collected data and deploying the well-known characteristic of signals in wireless environment, a mechanism for secure spectrum sensing was developed. The sink node (fusion center) is laid out in a centralized manner and employs a likelihood-based trust evaluating algorithm to determine the reliability of all measured data. Utilizing the assigned trust factors, a simple combination scheme is employed to make a final decision for the presence or the absence of primary user in desired frequency band. Simulation results, in the worst condition, confirm the effectiveness of the algorithm in eliminating malicious or malfunctioning nodes effects.

6. References

[1] Federal Communications Commission (FCC), "Spectrum Policy Task Force," Report ET Docket, No. 02-135, November 2002.

[2] J. Mitola, "Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio," Ph.D. Thesis, KTH-Royal Institute of Technology, Stockholm, 2000.

[3] Y. C. Liang, Y. Zeng, E. C. Y. Peh and A. T. Hoang, "Sensing-Throughput Tradeoff for Cognitive Radio Networks," *IEEE Transactions on Wireless Communication*, Vol. 7, No. 4, April 2008, pp. 1326-1337. doi:10.1109/TWC.2008.060869

[4] T. Yucek and H. Arslan, "A Survey of Spectrum Sensing Algorithm for Cognitive Radio Applications," *IEEE Communication Survey & Tutorials*, Vol. 11, No. 1, Spring 2009, pp. 116-130.

[5] A. Taherpour, Y. Norouzi, M. Nasiri-Kenari, A. Jamshidi and Z. Zeinalpour-Yazdi, "Asymptotically Optimum Detection of Primary User in Cognitive Radio Networks," *IET Communications*, Vol. 1, No. 6, December 2007, pp. 1138-1145. doi:10.1049/iet-com:20060645

[6] S. Tseng, H. Chiang and J. Lehnert, "Parametric density estimation using EM algorithm for collaborative spectrum sensing," 3*rd International Conference on Cognitive Radio Oriented Wireless Network and Communications* (*CrownCom*), Singapore, 15-17 May 2008, pp. 1-6.

[7] S. Shankar, C. Cordeiro and K. Challapali, "Spectrum Agile Radios: Utilization and Sensing Architectures," *Pro-*

ceedings of IEEE DySPAN, 8-11 November 2005, pp. 160-169.

[8] A. W. Min, K. G. Shin and X. Hu, "Attack-Tolerant Distributed Sensing for Dynamic Spectrum Access Networks," 17*th IEEE International Conference on Network Protocols*, Princeton, 13-16 October 2009, pp. 294-303. doi:10.1109/ICNP.2009.5339675

[9] H. Chen, H. Wu, X. Zhou and C. Gao, "Agent-Based Trust Model in Wireless Sensor Networks," 8*th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, Qingdao, July-August 2007, pp. 119-124. doi:10.1109/SNPD.2007.122

[10] G. Vijay, E. Bdira and M. Ibnkahla, "Cognitive Approaches in Wireless Sensor Networks: A Survey," 25*th Biennial Symposium on Communications*, Kingston, 12-14 May 2010, pp. 177-180. doi:10.1109/BSC.2010.5472978

[11] A. Ghasemi and E. S. Sousa, "Asymptotic Performance of Collaborative Spectrum Sensing under Correlated Log-Normal Shadowing," *IEEE Communication Letters*, Vol. 11, No. 1, January 2007, pp. 34-36.

[12] T. Shu and M. Krunz, "Throughput-Efficient Sequential Channel Sensing and Probing in Cognitive Radio Networks under Sensing Errors," *Proceedings of ACM MobiCom'*09, September 2009.

[13] R. Chen, J. M. Park, Y. T. Hou and J. H. Reed, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," *IEEE Communication Magazine*, Vol. 46, No. 4, April 2008, pp. 50-55.

[14] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," *IEEE International Conference on Communications* (*ICC*), Beijing, 19-23 May 2008, pp. 3406- 3410.

[15] S. Xu, Y. Shang and H. Wang, "Double Thresholds based Cooperative Spectrum Sensing against Untrusted Secondary Users in Cognitive Radio Networks," 69*th IEEE conference on Vehicular Technology*, Barcelona, 26-29 April 2009, pp. 1-5. doi:10.1109/VETECS.2009.5073511

[16] M. Akbari and A. Falahati, "SSDF Protection in Cooperative Spectrum Sensing Employing a Computational Trust Evaluation Algorithm," 5*th International Symposium on Telecommunication*, December 2010.

[17] A. GoldSmith, "Wireless Communication," Cambridge University Press, Cambridge, 2005.

[18] Q. Wang, D. W. Yue and Y. Wang, "Performance Analysis of Spectrum Sensing Using Diversity Technique," 5*th International Conference on Wireless Communication, Networking and Mobile Computing*, Beijing, 24-26 September 2009, pp. 1-5. doi:10.1109/WICOM.2009.5301177

[19] W. Zhang, J. Yang, Q. Yan and L. Xiao, "Performance Analysis of Cooperative Sensing with Equal Gain Combining over Nakagami Channels in Cognitive Radio Networks," 6*th International Conference on Wireless Communication and Mobile Computing*, September 2010.

[20] H. G. Kang, I. Song, Y. H. Kim, T. An and D. Kim, "Spectrum Sensing Based on Nonlinear Combining for Cognitive Radio with Receive Diversity," 44*th Annual Conference on Information Sciences and Systems* (*CISS*), Princeton, 17-19 March 2010, pp. 1-6. doi:10.1109/CISS.2010.5464977

[21] C. Yu and K. Chen, "Multiple Systems Sensing for Cognitive Radio Networks over Rayleigh Fading Channel," *Vehicular Technology Conference* (*VTC*), Singapore, 11-14 May 2008, pp. 1574-1578.

[22] E. D. Kaplan and C. J. Hegarty, "Understanding GPS: Principles and Applications," 2nd Edition, Artech House Inc., London, 2006.

[23] R. K. Pearson, "Outliers in Process Modeling and Identification," *IEEE Transactions on Control System Technology*, Vol. 10, No. 1, January 2002, pp. 55-63. doi:10.1109/PROC.1967.5573

[24] H. Urkowitz, "Energy Detection of Unknown Deterministic Signals," *Proceedings of IEEE*, Vol. 55, No. 4, 1967, pp. 523-531. doi:10.1109/PROC.1967.5573

[25] A. Papoulis and S. U. Pillai, "Probability, Random Variables and Stochastic Processes," 4th Edition, McGraw-Hill, New York, 2002.

[26] R. F. Mills and G. E. Prescon, "A Comparison of Various Radiometer Detection models," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 32, No. 1, January 1996, pp. 467-473. doi:10.1109/7.481289

[27] C. Cordeiro, K. Challapali, D. Birru and S. Shankar, "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radio," *Journal of Communications*, Vol. 1, No. 1, April 2006, pp. 38-47.

[28] H. Kim and K. G. Shin, "Efficient Discovery of Spectrum Opportunities with MAC-Layer Sensing in Cognitive Radio Networks," *IEEE Transactions on Mobile Computing*, Vol. 7, No. 5, May 2008, pp. 533-545.

