Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 752507, 6 pages
http://dx.doi.org/10.1155/2014/752507

Research Article

Goodness-of-Fit Based Secure Cooperative Spectrum Sensing for Cognitive Radio Network

Hiep Vu-Van and Insoo Koo

The School of Electrical Engineering, University of Ulsan, San 29, Muger 2-dong, Ulsan 680-749, Republic of Korea

Correspondence should be addressed to Insoo Koo; iskoo@ulsan.ac.kr

Received 7 March 2014; Accepted 25 April 2014; Published 18 May 2014

Academic Editor: Yuxin Mao

Cognitive radio (CR) is a promising technology for improving usage of frequency band. Cognitive radio users (CUs) are allowed to use the bands without interference in operation of licensed users. Reliable sensing information about status of licensed band is a prerequirement for CR network. Cooperative spectrum sensing (CSS) is able to offer an improved sensing reliability compared to individual sensing. However, the sensing performance of CSS can be destroyed due to the appearance of some malicious users. In this paper, we propose a goodness-of-fit (GOF) based cooperative spectrum sensing scheme to detect the dissimilarity between sensing information of normal CUs and that of malicious users, and reject their harmful effect to CSS. The empirical CDF will be used in GOF test to determine the measured distance between distributions of observation sample set according to each hypothesis of licensed user signal. Further, the DS theory is used to combine results of multi-GOF tests. The simulation results demonstrate that the proposed scheme can protect the sensing process against the attack from malicious users.

1. Introduction

Nowadays, more bandwidth and higher bit-rates have been required to meet usage demands due to an explosion in wireless communication technology. According to the Federal Communications Commission's spectrum policy task force report [1], the actual utilization of the licensed spectrum varies from 15% to 80%. In some cases, the utilization is only a small percentage of the total capacity. Cognitive radio (CR) technology [2] has been proposed to solve the problem of ineffective utilization of spectrum bands. Both unlicensed and licensed users, termed the cognitive radio user (CU) and primary user (PU), respectively, operate in CR networks. In CR network, CUs are allowed to access the frequency assigned to PU when it is free. But CU must vacate the occupied frequency when the presence of PU is detected. Therefore, reliable detection of the PU's signal is a requirement of CR networks.

In order to ascertain the presence of a PU, CUs can use one of several common detection methods, such as matched filter, feature, and energy detection [2, 3]. Energy detection is the optimal sensing method if the CU has limited information about PU's signal (e.g., only the local noise power is known) [3]. In energy detection, frequency energy in the sensing channel is received in a fixed bandwidth W over an observation time window T to compare with the energy threshold and determine whether or not the channel is utilized. However, the received signal power may fluctuate severely due to multipath fading and shadowing effects. Therefore, it is difficult to obtain reliable detection with only one CU. Better sensing performance can be obtained by allowing some CUs to perform cooperative spectrum sensing [4–6].

CSS can use some combination methods such as equal gain combination (EGC) and maximum gain combination (MGC) [7] to combine sensing information of all CUs in the network and make a global decision about status of PU signal. Since EGC gives the same weight for all CUs in the network, it is easy to execute but with limited performance. MGC is known as the optimal combination rule. However, it requires information about the SNRs of the sensing channel, which is difficult to obtain in practice. In addition, MGC is sensitive to attack by malicious users who send false sensing data to the fusion center (FC) [8]. The research presented in [8, 9] determined that the presence of a few malicious users can severely reduce the performance of a CSS scheme. Algorithms used to identify the malicious users have been proposed in the studies of [8, 9]. In previous research, a simple technique (i.e., outlier-detection) is used to detect less damage malicious CUs such as *always No* or *always Yes* CU. In addition, the technique is unable to protect the CSS in the event of a large number of malicious users in the network.

In this paper, we utilize multi-goodness-of-fit (GOF) tests to design a robust CSS, in which the event detection technique [10, 11] will be used to provide the combination of different evidence of each type of GOF test which are supported by a particular hypothesis of PU signal. The proposed scheme considers two types of GOF tests, Kolmogorov-Smirnov (KS) and Cramer-von Mises (CM) tests. The proposed scheme can distinguish the sensing information of normal CUs and that of malicious users and reject the harmful effect of malicious user to sensing combination process. Three common types of malicious users including *always Yes*, *always No,* and *opposite* are considered in this paper.

2. Background

2.1. Goodness-of-Fit Test. The GOF test summarizes the discrepancy between the observed samples with theoretical distributions or empirical distributions and the reference distribution. For the n independent and identical distributed observation, the sample is first arranged in ascending order such that $s_1 \le s_2 \le \cdots \le s_n$. The GOF test is used to determine whether or not the samples set was drawn from the same distribution with a cumulative distribution function (CDF) F_0. The testing hypothesis can be formulated as follows:

$$\begin{gathered} F(s) = F_0(s) : H_o, \\ F(s) \neq F_0(s) : H_1, \end{gathered} \tag{1}$$

where $F(s)$ is the empirical CDF of the sample. It can be calculated as follows:

$$F(s) = \frac{1}{n}\sum_{i=1}^{n} I\{s_i \le s\}, \tag{2}$$

where $I\{\cdot\}$ is the indicator of event $\{\cdot\}$.

There are many types of GOF tests, for instance, Cramer-von Mises (CM), Kolmogorov-Smirnov (KS), AndersonDarling (AD), and Hosmer-Lemeshow (HL) tests. In this paper, we consider two types of GOF tests, CM and KS tests, which can run well with a low number of samples.

(1) Kolmogorov-Smirnov (KS) test: the KS test, which is based on the empirical CDF of the samples set and the reference CDF, can be calculated according to the largest difference of two distributions as follows:

$$D_{\text{KS}} = \sup\{|F(s_i) - F_0(s_i)| : i = 1, \ldots, n\}, \tag{3}$$

where $\sup\{\cdot\}$ is supremum function, which indicates the greatest element of the set. If the sample comes from distribution $F_0(x)$, then D_{KS} will converge to 0.

(2) Cramer-von Mises (CM) test: CM test is used for judging the goodness-of-fit of the sample set's CDF $F(s)$ and reference distribution's CDF $F_0(s)$. The test statistic is given by

$$D_{\text{CM}} = n\int_{-\infty}^{+\infty} [F(s) - F_0(s)]^2 dF_0(s) \tag{4}$$

and can be approximated as

$$D_{\text{CM}} = \frac{1}{12n} + \sum_{i=1}^{n}\left[\frac{2i-1}{2n} - F_0(s_i)\right]^2. \tag{5}$$

If this value, D_{CM}, is larger than the threshold, the hypothesis that the sample data come from the reference distribution F_0 can be rejected.

2.2. Combination of Evidence in Dempster-Shafer Theory. Dempster-Shafer (DS) theory was first introduced by Demperster and was later extended by Shafer. This is a potentially valuable tool for the evaluation of risk and reliability in engineering applications when it is not possible to obtain a precise measurement from experiments or when knowledge is obtained from expert elicitation. An important aspect of this theory is the combination of evidence obtained from multiple sources and the modeling of conflict between them.

In DS theory [12], a representation of ignorance is provided by assigning a nonzero mass function to hypothesis m, also called the basic probability assignment (BPA), and is defined for every hypothesis A such that the mass value $m(A)$ belongs to the interval $[0, 1]$ and satisfies the following conditions:

$$\begin{gathered} m(\phi) = 0, \\ \sum m(A) = 1, \quad A \subseteq \Omega, \end{gathered} \tag{6}$$

where Ω is the frame of discernment, which is a fixed set of q mutually exclusive and exhaustive elements.

By assigning a nonzero mass in a compound hypothesis, $A \cup B$ means that there exists the option to not make a decision between A and B but to leave the formulation in the $A \cap B$ class. In DS theory, two functions, belief (Bel) and plausibility (Pls), are defined to characterize the uncertainty and support of certain hypotheses. Bel measures the minimum or necessary support, whereas Pls reflects the maximum or potential support for that hypothesis [13]. These two measures, derived from mass values, are defined as a map from a set of hypotheses to interval $[0, 1]$ as follows:

$$\begin{gathered} \text{Bel}(A) = \sum_{B \subseteq A} m(B), \\ \text{Pls}(A) = \sum_{A \cap B \neq 0} m(B). \end{gathered} \tag{7}$$

The sum of mass functions from different information source, m_j $(j = 1, 2, \ldots M)$, combined with the DS rule is known as the orthogonal sum, which is commutative and

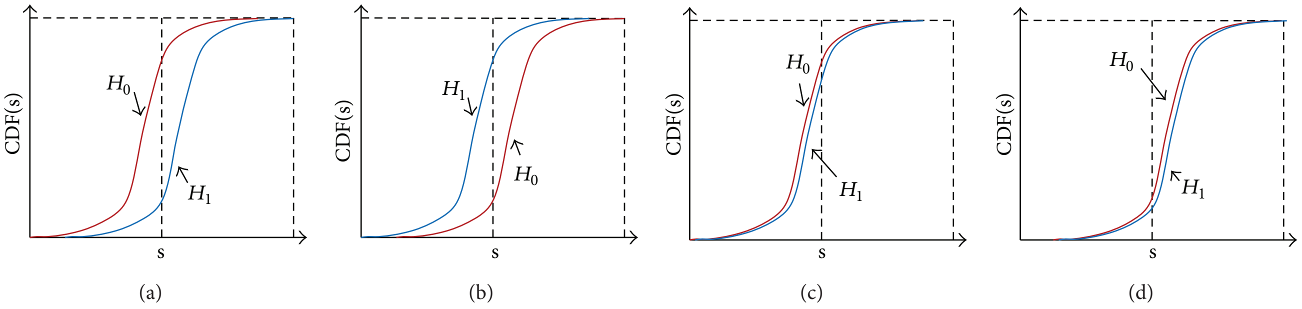

Figure 1: The CDF of received signal energy at CU under absence and presence hypothesis of PU signal for (a) normal CU, (b) *opposite* malicious CU, (c) *always Yes* malicious CU, and (d) *always No* malicious CU.

associative. The result is a new mass function, $m(A_k) = (m_1 \oplus m_2 \oplus \cdots m_d)(A_k)$, which incorporates the joints information provided by the sources as follows:

$$m(A_k) = \frac{1}{1-K}\sum_{A_1\cap A_2\cdots A_d=A_k}\left(\prod_{1\le j\le M} m_j(A_j)\right),$$
$$K = \sum_{A_1\cap A_2\cdots A_d=\phi}\left(\prod_{1\le j\le M} m_j(A_j)\right), \qquad (8)$$

where K is the measure of conflict between the different sources and is introduced as a normalization factor.

3. The Proposed Secure Cooperative Spectrum Sensing Based on GOF Test

There is a definite difference between the CDF of received signal energy of normal CU and that of the malicious users as shown in Figure 1. The CDF of the received signal energy of normal CU corresponding to the presence of the PU is always "*under*" that one corresponding to the absence of the PU. On the contrary, the *opposite malicious* CU has the CDF corresponding to the presence of PU to be "*above*" the CDF corresponding to the absence of PU. The *always Yes* and *always No* malicious CUs have a similar CDF corresponding to presence and absence of PU. Due to the difference between CDF of normal and malicious CUs, we utilize GOF test to detect the appearance of malicious users in the network, so that their harmful effect can be rejected out of CSS process. Multi-GOF tests including KS and CM tests will be applied for adaptive robust CSS. The DS theory will be used to combine results of multi-GOF tests.

In this paper, we consider a CR network including N CUs who cooperate to sense the signal from a PU. There are $p < N$ malicious CUs appearing in the network which can be classified as three common types: *always Yes*, *always No,* and *opposite* malicious CUs. All CUs use energy detectors to perform spectrum sensing and send their sensing data to the FC through a control channel. Based on the sensing data obtained from the CUs, the FC makes a global decision concerning the presence or absence of the PU signal by using the proposed data fusion scheme. The proposed scheme has 3 steps as follows.

Step 1. All CUs perform spectrum sensing by using energy detection method to determine received signal energy $E_j = \{e_{1,j}, e_{2,j}, \ldots, e_{M,j}\}$, where M is the number of sensing samples that the jth CU takes in the sensing interval.

Step 2. At the FC, GOF test statistics of each CU will be computed according to hypothesis of the PU as given in (11). After that, BPA and final BPA for current sensing data will be estimated based on the "*reputation level*" of each CU, which is updated from previous sensing interval. Based on final BPA, a global decision rule will be proposed to make global decision about status of PU signal.

Step 3. Update "*reputation level*" of each CU according to the global decision.

The detailed description of each step will be given in the following subsections.

3.1. Energy Detection. At the sensing interval for the jth CU, the local spectrum sensing is to decide between the two following hypotheses:

$$H_0 : s_j(k) = n_j(k),$$
$$H_1 : s_j(k) = h_j p(k) + n_j(k), \qquad (9)$$

where H_0 and H_1 correspond to the hypothesis of the absence and presence of the PU signal, respectively, h_j denotes the amplitude gain of the channel, $s(k)$ is the signal transmitted from the PU, $n_j(k)$ is the additive white Gaussian noise, and k is index of sensing sample at each sensing interval.

A received signal energy of a sensing sample, $e_{k,j}$, is given as

$$e_{k,j} = \begin{cases} \left|n_j(k)\right|^2, & H_0 \\ \left|h_j s(k) + n_j(k)\right|^2, & H_1. \end{cases} \qquad (10)$$

3.2. BPA Estimation. The GOF test statistics of the current sensing data $e_{k,j}$ $(k = 1, \ldots, M)$ of the jth CU will be

Table 1: Reputation ranges according to each type of CUs.

Status of PU	Normal CU	*Always Yes* CU	*Always No* CU	*Opposite* CU
H_1	$D^t_{0,j} \gg D^t_{1,j}$	$D^t_{0,j} \gg D^t_{1,j}$	$D^t_{0,j} \ll D^t_{1,j}$	$D^t_{0,j} \ll D^t_{1,j}$
	$D^t_{1,j} \approx 0$	$D^t_{1,j} \approx 0$	$D^t_{0,j} \approx 0$	$D^t_{0,j} \approx 0$
	$r^t_{0,j}(i) \gg 0$	$r^t_{0,j}(i) \gg 0$	$r^t_{0,j}(i) \ll 0$	$r^t_{0,j}(i) \ll 0$
H_0	$D^t_{0,j} \ll D^t_{1,j}$	$D^t_{0,j} \gg D^t_{1,j}$	$D^t_{0,j} \ll D^t_{1,j}$	$D^t_{0,j} \gg D^t_{1,j}$
	$D^t_{0,j} \approx 0$	$D^t_{1,j} \approx 0$	$D^t_{0,j} \approx 0$	$D^t_{1,j} \approx 0$
	$r^t_{1,j}(i) \gg 0$	$r^t_{1,j}(i) \ll 0$	$r^t_{1,j}(i) \gg 0$	$r^t_{1,j}(i) \ll 0$

calculated according to each hypothesis of PU signal based on (3) and (5) as follows, respectively:

$$D^{\mathrm{KS}}_{h,j} = \sup\left\{\left|F\left(e_{k,j}\right) - F_h\left(e_{k,j}\right)\right| : k = 1, 2, \ldots, M\right\},$$
$$D^{\mathrm{CM}}_{h,j} = \frac{1}{12M} + \sum_{i=1}^{M}\left[\frac{2i-1}{2M} - F_h\left(e_{k,j}\right)\right]^2, \qquad (11)$$

where $h = \{0, 1\}$ is index of hypothesis H_h of PU signal, $e_{k,j}$ is the received signal energy of kth sensing sample of the jth CU, $F(\cdot)$ and $F_h(\cdot)$ are empirical CDF of observed sensing sample and CDF of H_h hypothesis of PU, and M is the number of samples for each sensing interval.

It is noteworthy that normal CU and malicious CU have different characteristics of $D^t_{1,j}$ and $D^t_{0,j}$ as shown in Table 1, where t indexes types of GOF tests: KS and CM.

Based on the values of $D^t_{1,j}$ and $D^t_{0,j}$, we will estimate BPA of current sensing data of each CU and their "*reputation level*" for robust CSS as follows:

$$\Delta^t_{1,j} = \frac{D^t_{0,j}}{D^t_{1,j} + D^t_{0,j}} R^t_{0,j},$$
$$\Delta^t_{0,j} = \frac{D^t_{1,j}}{D^t_{1,j} + D^t_{0,j}} R^t_{1,j}, \qquad (12)$$

where $R^t_{h,j}$ is "*reputation level*" of the jth CU according to hypothesis h, and it can be determined based on history observation of the jth CU as follows:

$$R^t_{h,j}(i) = \frac{r^t_{h,j}(i-1)}{\sum_j r^t_{h,j}(i-1)}, \qquad (13)$$

where i is the index of current sensing interval and $r^t_{1,j}(i-1)$ and $r^t_{0,j}(i-1)$ are updated from the previous sensing interval according to global decision:

$$r^t_{1,j}(i-1) = r^t_{1,j}(i-2) + \left(D^t_{1,j}(i-1) - D^t_{0,j}(i-1)\right), \qquad (14)$$

$$r^t_{0,j}(i-1) = r^t_{0,j}(i-2) + \left(D^t_{0,j}(i-1) - D^t_{1,j}(i-1)\right). \qquad (15)$$

By using $r^t_{1,j}$ and $r^t_{0,j}$, types of CUs will be easily distinguished. The normal CU has positive value of both $r^t_{1,j}$ and $r^t_{0,j}$ that will be increased after updating step. $r^t_{1,j}$ of *always Yes* and $r^t_{0,j}$ of *always No* malicious CUs are almost negative and tend to decrease after updating step. On the other hand, both values of opposite CU are negative and have a tendency to decrease. We define "*malicious threshold*" as ρ to reject the attack of malicious CR in CSS, so that the CU, which has either $r^t_{1,j} < 0$ or $r^t_{0,j} < 0$, will be determined as malicious CU. The sensing data of malicious CUs will not be considered to make global decision by giving them $r^t_{1,j} = 0$ and $r^t_{0,j} = 0$.

The BPA of all CUs will be combined with their reputation levels as

$$\Delta^t_1 = \frac{1}{n_\Omega}\sum_{j\in\Omega}\frac{D^t_{0,j}}{D^t_{1,j} + D^t_{0,j}} R^t_{0,j},$$
$$\Delta^t_0 = \frac{1}{n_\Omega}\sum_{j\in\Omega}\frac{D^t_{1,j}}{D^t_{1,j} + D^t_{0,j}} R^t_{1,j}, \qquad (16)$$

where Ω and n_Ω are set of normal CUs and number of members of the set, respectively.

Because the error in estimating Δ^t_0 and Δ^t_1, $\Delta^t_0 + \Delta^t_1$ can be bigger than 1, we need to normalize those values as

$$\Delta^{t*}_0 = \frac{\Delta^t_0}{\Delta^t_0 + \Delta^t_1},$$
$$\Delta^{t*}_1 = \frac{\Delta^t_1}{\Delta^t_0 + \Delta^t_1}. \qquad (17)$$

3.3. DS Theory Combination. The DS theory will be used to combine the BPA of both GOF tests according to each hypothesis as follows:

$$\Delta_1 = \Delta^{\mathrm{KS}*}_1 \oplus \Delta^{\mathrm{CM}*}_1 = \frac{\Delta^{\mathrm{KS}*}_1 \Delta^{\mathrm{CM}*}_1}{1 - \left(\Delta^{\mathrm{KS}*}_1 \Delta^{\mathrm{CM}*}_0 + \Delta^{\mathrm{KS}*}_0 \Delta^{\mathrm{CM}*}_1\right)},$$
$$\Delta_0 = \Delta^{\mathrm{KS}*}_0 \oplus \Delta^{\mathrm{CM}*}_0 = \frac{\Delta^{\mathrm{KS}*}_0 \Delta^{\mathrm{CM}*}_0}{1 - \left(\Delta^{\mathrm{KS}*}_1 \Delta^{\mathrm{CM}*}_0 + \Delta^{\mathrm{KS}*}_0 \Delta^{\mathrm{CM}*}_1\right)}. \qquad (18)$$

Finally, the global decision will be made as follows:

$$G = H_1, \quad \text{if } \frac{\Delta_1}{\Delta_0} \geq \eta,$$
$$G = H_0, \quad \text{otherwise}, \qquad (19)$$

where η is the threshold for global decision.

According to the global decision, $r^t_{1,j}$ or $r^t_{0,j}$ will be updated for the next sensing interval as follows, respectively.

(i) If the global decision is $G(i) = 0$, we update $r^t_{1,j}(i)$ by using (14).

(ii) Otherwise, we update $r^t_{0,j}(i)$ by using (15).

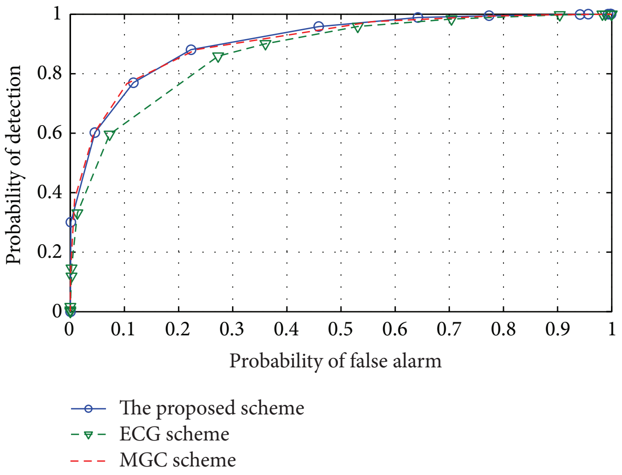

Figure 2: ROC of the proposed scheme and reference schemes when no malicious CU is considered.

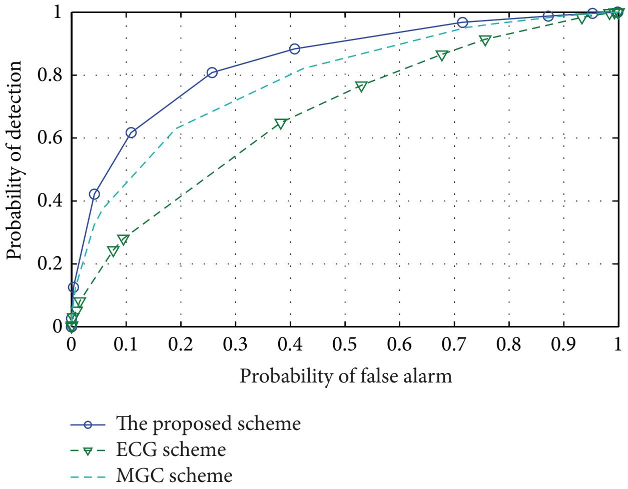

Figure 3: ROC of the proposed scheme and reference schemes when 4 *always No* malicious CUs are considered.

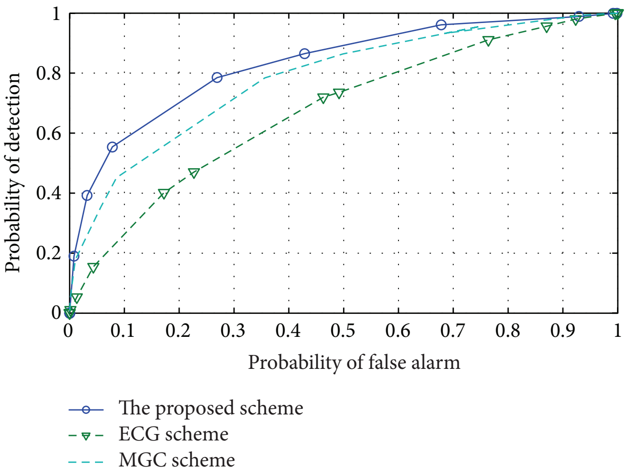

Figure 4: ROC of the proposed scheme and reference schemes when 4 *always Yes* malicious CUs are considered.

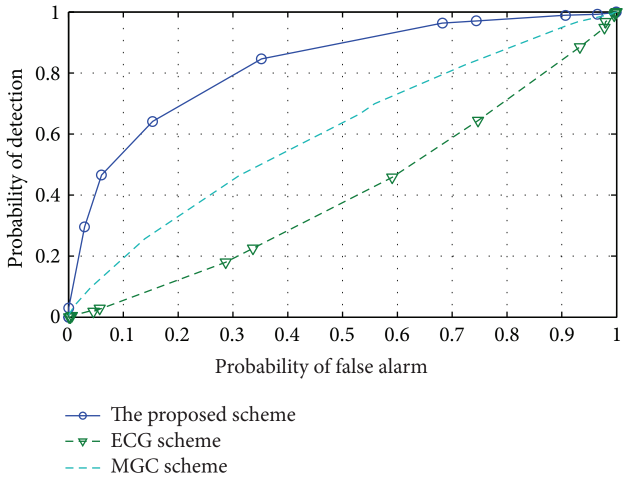

Figure 5: ROC of the proposed scheme and reference schemes when 4 *opposite* malicious CUs are considered.

4. Simulation Results

In this section, simulation results of the proposed scheme and other soft combination schemes such as maximum gain combination (MGC) and equal gain combination (EGC) are provided. The network is considered in which 5 CUs exist and some of them can be malicious CUs.

In order to verify the reliability of the proposed combination scheme, we perform a simulation without considering malicious CU. The sensing results in Figure 2 show that the proposed scheme can obtain better sensing performance in comparison with EGC scheme and obtain a similar sensing performance to that of the MGC scheme when no malicious CU is considered.

The robustness of the proposed scheme will be investigated in the network with the appearance of *always No*, *always Yes*, and *opposite* malicious CUs in the network. Figures 3 and 4 show performance of the proposed scheme when 4 CUs are *always No* or *always Yes* malicious CUs among 5 CUs in the network. The results show that the proposed scheme with all CUs can achieve much better sensing performance than that one of the MGC and EGC schemes. This means that, by applying GOF test to CSS, the proposed scheme can detect the presence of those types of malicious CUs and reject their harmful effects to sensing process.

Opposite malicious CU causes the most damage to sensing performance. However, the proposed scheme is expected to protect CSS against this type of malicious CU. Figure 5 shows the sensing performance of the network when 4 CUs are *opposite* malicious among 5 CUs. MGC and EGC with all CUs provide very low performance due to the attack of *opposite* malicious CU. However, the proposed scheme can defend their attacks and achieve high sensing performance.

5. Conclusion

In this paper, multi-GOF tests are proposed to measure the difference between sensing data of normal CU and that of malicious CU. Further, the DS theory is used to combine results of multi-GOF tests. The proposed scheme considers the appearance of the most common types of malicious CU: *always Yes*, *always No,* and *opposite* types. The simulation results prove that the proposed scheme can reject almost harmful effect from those malicious CUs to protect CSS.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the KRF funded by the MEST (NRF-2012R1A1A2038831).

References

[1] Federal Communications Commission, "Spectrum policy task force," Tech. Rep. 02-135, ET Docket, 2002.

[2] Y. Hur, J. Park, W. Woo et al., "A wideband analog Multi-Resolution Spectrum Sensing (MRSS) technique for cognitive radio (CR) systems," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '06)*, pp. 4090–4093, Island of Kos, Greece, May 2006.

[3] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits on cognitive radio," in *Proceedings of the Allerton Conference on Communications, Control, and Computing*, Monticello, Va, USA, 2004.

[4] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," in *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05)*, pp. 137–143, Baltimore, Md, USA, November 2005.

[5] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proceedings of the IEEE International Conference on Communications (ICC '06)*, vol. 5, pp. 1658–1663, July 2006.

[6] 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, pp. 716–725, 2012.

[7] J. Ma and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," in *Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07)*, pp. 3139–3143, November 2007.

[8] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proceedings of the IEEE International Conference on Communications (ICC '08)*, pp. 3406–3410, May 2008.

[9] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2488–2497, 2010.

[10] J. Li, J. Liu, and K. Long, "Reliable cooperative spectrum sensing algorithm based on Dempster-Shafer theory," in *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM '10)*, pp. 1–5, December 2010.

[11] X. Zheng, J. Wang, Q. Wu, and J. Chen, "Cooperative spectrum sensing algorithm based on Dempster-Shafer theory," in *Proceedings of the 11th IEEE Singapore International Conference on Communication Systems (ICCS '08)*, pp. 218–221, November 2008.

[12] N. Nguyen-Thanh and I. Koo, "Empirical distribution-based event detection in wireless sensor networks: an approach based on evidence theory," *IEEE Sensors Journal*, vol. 12, no. 6, pp. 2222–2228, 2012.

[13] K. Sentz and S. Ferson, "Combination of evidence in Dempster-Shafer theory," Sandia Report SAND2002-0835, Sandia National Laboratories, Albuquerque, NM, USA, 2002.

Journal of Engineering
The Scientific World Journal
International Journal of Rotating Machinery
Journal of Sensors
International Journal of Distributed Sensor Networks
Advances in Civil Engineering
Journal of Control Science and Engineering
Journal of Robotics
Journal of Electrical and Computer Engineering
Advances in OptoElectronics
VLSI Design
International Journal of Navigation and Observation
Modelling & Simulation in Engineering
International Journal of Aerospace Engineering
International Journal of Chemical Engineering
International Journal of Antennas and Propagation
Active and Passive Electronic Components
Shock and Vibration
Advances in Acoustics and Vibration