Journal of information and
communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 13(2): 74-80, Jun. 2015 Regular paper

Mitigation of Adverse Effects of Malicious Users on Cooperative Spectrum Sensing by Using Hausdorff Distance in Cognitive Radio Networks

Muhammad Sajjad Khan and Insoo Koo[*], ***Member, KIICE***

School of Electrical Engineering, University of Ulsan, Ulsan 680-749, Korea

Abstract

In cognitive radios, spectrum sensing plays an important role in accurately detecting the presence or absence of a licensed user. However, the intervention of malicious users (MUs) degrades the performance of spectrum sensing. Such users manipulate the local results and send falsified data to the data fusion center; this process is called spectrum sensing data falsification (SSDF). Thus, MUs degrade the spectrum sensing performance and increase uncertainty issues. In this paper, we propose a method based on the Hausdorff distance and a similarity measure matrix to measure the difference between the normal user evidence and the malicious user evidence. In addition, we use the Dempster-Shafer theory to combine the sets of evidence from each normal user evidence. We compare the proposed method with the k-means and Jaccard distance methods for malicious user detection. Simulation results show that the proposed method is effective against an SSDF attack.

Index Terms: Cognitive radio, Dempster-Shafer evidence theory, Hausdorff distance, Spectrum sensing data falsification (SSDF)

I. INTRODUCTION

According to the Federal Communication Commission, most of radio spectrum is underutilized, which leads to inefficient usage of the allowed spectrum [1]. Cognitive radio (CR) technology has been studied as an approach to increase spectrum efficiency by allowing dynamic spectrum access. A major challenge in CR is spectrum sensing, which is used to detect whether a spectrum is occupied by a licensed user (LU). The sensing performance of a secondary user (SU) degrades because of the presence of channel effects such as fading, shadowing, and the hidden terminal problem. These problems are overcome by the use of cooperative spectrum sensing, which involves an exchange of local sensing results between multiple SUs by using a centralized or decentralized fusion center to arrive at the final decision regarding the presence or absence of an LU [2].

However, multiple SUs sending their local sensing result to the fusion center also increases the number of security risks. One of the security issues is the spectrum sensing data falsification (SSDF) attack, where a malicious user (MU) purposely reports false local sensing data to the SUs, thereby negatively influencing the overall decision. In [3], the authors discussed the security threats from passive and active points of view; the authors discussed the physical layer security for a passive attack; and MU detection is introduced for an active attack by using signal detection techniques to reduce the system interference. In [4], the authors used a weighted sequential probability test (WSPRT)

Received 02 February 2015, **Revised** 30 March 2015, **Accepted** 28 April 2015

***Corresponding Author** Insoo Koo (E-mail: iskoo@ulsan.ac.kr, Tel: +82-52-259-1249)
School of Electrical Engineering, University of Ulsan, 93 Daehak-ro, Nam-gu, Ulsan 680-749, Korea.

Open Access http://dx.doi.org/10.6109/jicce.2015.13.2.074 print ISSN: 2234-8255 online ISSN: 2234-8883

to identify MUs on the basis of their reputation, which is determined by the rating assigned to every user. In [5], the authors proposed a correlation of utilization and shadow fading to detect malicious users. In [6], the authors proposed a scheme where the maximization of the secondary secrecy rate is subject only to the maintenance of a certain level of quality of service for a primary user via the interference threshold. In [7], the authors considered cooperative spectrum sensing with the existence of an MU; the authors formulated the detailed detection performance to analyze the impact of incorrect information on the sensing. Further, an authentication mechanism is proposed to filter out the incorrect information from the system. In [8], the authors addressed the problem of cooperative spectrum sensing in a CR network: in the presence of misbehaving CRs, an iterative expectation maximization is formulated and solved for hypothesis verification and radio classification. Similarly, in [9], the authors proposed a cross-layered approach to provide SUs with the ability to differentiate between a primary user and an MU by using a hidden Markov model at the media access control (MAC) sublayer. In [10], the authors presented a decentralized scheme for detecting MUs in cooperative spectrum sensing.

The authors of [11] and [12] explored the Dempster-Shafer (D-S) evidence theory in cooperative spectrum sensing but have not taken into account the MU's activity. In [13], the authors proposed a reliable method based on clustering cooperating sensors; a cluster with no malicious user was found by using a fast sensor search algorithm. The authors' model is based on trusted sensors and uses only the results obtained by these sensors; thus, the information of malicious sensors is not considered in the spectrum decision process. In [14], the authors utilized both the advantages of the D-S evidence theory combined with an enhanced weighted stage and the capability of robust statistics used for the elimination of MUs. In [15], the authors proposed a robust cooperative spectrum sensing scheme based on the D-S theory and the calculation of the trustworthiness degree. In [16], the authors developed a trust-based data aggregation scheme to tackle an MU attack; the scheme combined first-hand and second-hand sensing evidence to guarantee performance and adopt a static game model to discourage MUs from fake reporting. In [17], the authors proposed a similarity degree that calculated the reliability of evidence and then combined reliable sets of evidence sent by honest users, but the authors did not consider the physical position of the users, and MUs were found on the basis of its cardinality, which was practically unreliable.

In this paper, we propose a method using the Hausdorff distance and a similarity measure matrix. First, the Hausdorff distance is used for measuring the difference between two sets of evidence, and then, the similarity measure matrix is used for calculating the similarity between each normal user's evidence and identifying MUs. The credibility (reliability) of MUs is less than that of normal users, and by using this value, we can remove the MUs. Finally, after removing the MUs, we use the D-S evidence theory to combine the normal users and estimate the performance of cooperative spectrum sensing.

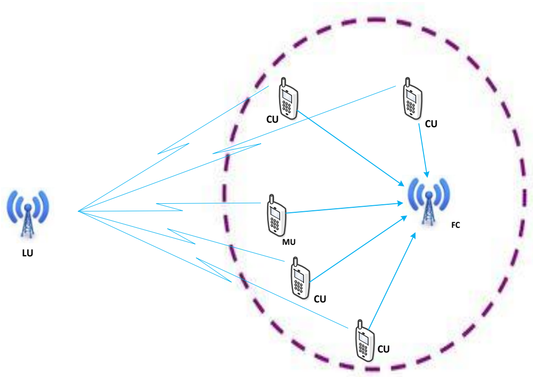

Fig. 1. System model of cognitive radio network. LU: licensed user, CU: cognitive user, MU: malicious user, FC: fusion center.

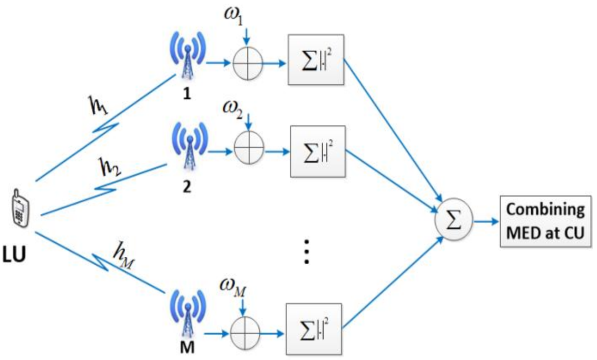

Fig. 2. Multiple energy detector (MED) of each cognitive user (CU). LU: licensed user.

The rest of this paper is organized as follows: In Section II, we describe the system model of the proposed system. In Section III, we describe the proposed cooperative spectrum sensing-based Hausdorff distance method and the D-S evidence theory. In Section IV, we discuss the simulation results. Finally, we conclude the paper in Section V.

II. SYSTEM MODEL

We consider a CR network, which consists of a LU, cognitive user (CU), MU, and fusion center (FC), as shown in Fig. 1. In the proposed system, we consider a multiple energy detector (MED), which has M energy detectors, each having a single antenna; the result of these antennas is combined at the CU by using the equal gain combining (EGC) method, as shown in Fig. 2.

In the first step, each CU performs local sensing by using MED. The local sensing at each CU (with a single energy detector) can be formulated as a binary hypothesis as follows:

$$X_i = \begin{cases} \mathrm{w}(n) : H_o \\ h_i(n)\mathrm{s}(\mathrm{n}) + w(n) : H_1 \end{cases}, \tag{1}$$

where H_o and H_1 denote the absence or presence of the LU, respectively.

In the case of MED, local sensing can be formulated as follows:

$$X_{i,j} = \begin{cases} \mathrm{w}_{\mathrm{i,j}}(n) : H_o \\ h_{i,j}(n)\mathrm{s}(\mathrm{n}) + w_{i,j}(n) : H_1 \end{cases}, \tag{2}$$

where $i = 1,2,3...N_c$ denotes the number of CUs, $j = 1,2,3...M$ represents the number of antennas, $n = 1,2,3...N$ indicates the number of samples, $s(n)$ refers to the LU signal, $h_{i,j}$ denotes the fading channel coefficient of the i^{th} CU at the j^{th} antenna, and $w_{i,j}(n)$ represents the additive white Gaussian noise.

The signal received at each antenna is multiplied by a weight ω. The energy received at each antenna is measured and is given as follows:

$$E_{i,j} = \sum_{n=1}^{N} \omega_{\mathrm{i,j}} \, |\, \mathrm{X}_{i,j}(\mathrm{n}) \,|^2 \; . \tag{3}$$

The energy of each CU received from M antennas is given as follows:

$$E_i = \sum_{j=1}^{M} E_{i,j} \; . \tag{4}$$

The energy calculated at each detector is combined using the EGC method, which is given as follows:

$$E = \sum_{i=1}^{N_c} E_i \; , \tag{5}$$

where $X_{i,j}(\mathrm{n})$ denotes the sample of the received signal and $N = 2TW$, where T represents the detection time and W indicates the bandwidth. When N is sufficiently large, E can be well approximated by the Gaussian random variable in the cases of both hypotheses H_0 and H_1, and can be expressed as follows [18]:

$$\begin{cases} H_0 : \; \mu_0 = MN, & \sigma_0^2 = 2MN \\ H_1 : \; \mu_1 = MN(\gamma_{i,j} + 1), & \sigma_1^2 = 2MN(2\gamma_{i,j} + 1) \end{cases}, \tag{6}$$

where μ_0 and μ_1 denote the mean of E, and σ_0^2 and σ_1^2 represent the variances of E in the cases of hypotheses H_0 and H_1, respectively, and $\gamma_{i,j}$ indicates the signal-to-noise ratio of the primary signal at the CU.

III. PROPOSED COOPERATIVE SPECTRUM SENSING BASED ON HAUSDORFF DISTANCE AND D-S THEORY OF COMBINATION

In this section, we provide a detailed description of the proposed method for the detection of an MU and the mitigation of its adverse effects. First, we measure all the users' evidence by using the basic probability assignment (BPA) method. Then, we calculate the differences among the sets of evidence by using the Hausdorff distance and formulate the similarity measure matrix. After forming the similarity measure matrix, we calculate the credibility of the sets of evidence and compare it with a fixed threshold value. If the credibility value is greater than the threshold value, the user is considered a normal user, and if it is less than the threshold value, the user is considered to be an MU. Finally, we combine the evidence of the normal users at the fusion center. The overall flow chart of the proposed system is shown in Fig. 3.

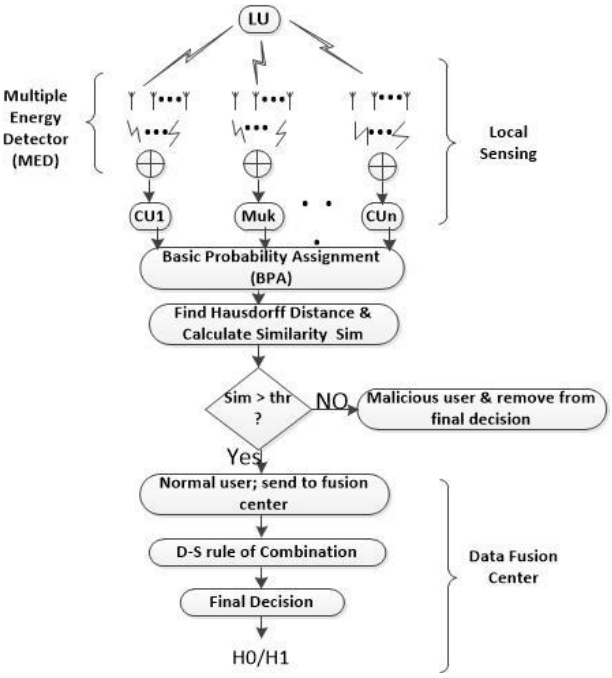
LU
Multiple Energy Detector (MED)
Local Sensing
CU1
Muk
CUn
Basic Probability Assignment (BPA)
Find Hausdorff Distance & Calculate Similarity Sim
Sim > thr ?
NO
Malicious user & remove from final decision
Yes
Normal user; send to fusion center
D-S rule of Combination
Final Decision
H0/H1
Data Fusion Center

Fig. 3. Proposed cooperative spectrum sensing based on Hausdorff distance and Dempster-Shafer (D-S) evidence theory. LU: licensed user, CU: cognitive user.

A. Basic Probability Assignment

The D-S evidence theory is one of the candidates for the decision-making to combine users' evidence, where the system faces an uncertainty problem. In the D-S evidence theory, the frame of discernment A can be defined as $\{H_1, H_0, \Omega\}$, where Ω denotes the ignorance hypothesis, which describes whether the hypothesis is true. After MED performs sensing, each CU collects the local information from MED by using the EGC method and then, measures the basic BPA $\mathrm{m}(H_0)$ and $\mathrm{m}(H_1)$ by using hypotheses H_0 and H_1, respectively. The BPA function is defined as a cumulative density function as follows [12]:

$$\mathrm{m_i}(H_0) = \int_{E_i}^{+\infty} \frac{1}{\sqrt{2\pi}\sigma_{0i}} \exp\left(-\frac{(x-\mu_{0i})^2}{2\sigma^2_{0i}}\right) dx \ , \qquad (7)$$

$$\mathrm{m_i}(H_1) = \int_{-\infty}^{E_i} \frac{1}{\sqrt{2\pi}\sigma_{1i}} \exp\left(-\frac{(x-\mu_{1i})^2}{2\sigma^2_{1i}}\right) dx \ , \qquad (8)$$

$$\mathrm{m_i}(\Omega) = 1 - m_i(H_0) - m_i(H_1) \ , \qquad (9)$$

where $\mathrm{m_i}(H_0)$, $\mathrm{m_i}(H_1)$, and $\mathrm{m_i}(\Omega)$ represent the BPA function of the i^{th} CU.

B. Detection of Malicious User and Mitigation of Its Adverse Effects Using Hausdorff Distance

An MU falsifies the local detection results, and thus, its evidence is different from that of a normal user to some extent. Several alternatives for quantifying a similarity between focal elements have been proposed [19]. In this paper, we propose a method using the Hausdorff distance to measure the difference between the evidence of two different sources, because the Hausdorff distance measures the degree of mismatch between two sets; we then form a similarity matrix to find the similarity between the sets of evidence. After the similarity matrix formation, malicious users and normal users are separated on the basis of their credibility values.

The Hausdorff distance provides a simple method for quantifying the distance between two sets of evidence m_i and m_j, and is one of the most widely used measures for quantifying such a distance. It can quantify the distance between two sets of evidence as follows:

$$\mathrm{H}(\mathrm{m}_i, \mathrm{m}_j) \ = \max\{\mathit{sup}_{m_i \in A_i} \inf_{m_j \in A_j} \mathrm{h}(\mathrm{m}_i, \mathrm{m}_j), \sup_{m_j \in A_j} \inf_{m_i \in A_i} \mathrm{h}(\mathrm{m}_j, \mathrm{m}_i)\}, \qquad (10)$$

where $\mathrm{h}(\mathrm{m}_i, \mathrm{m}_j)$ denotes the distance between two elements of the sets and can be defined as any valid distance in the measurement space [20].

The similarity measure $\mathrm{Sim}(\mathrm{m}_i, \mathrm{m}_j)$ between sets of evidence is defined as follows:

$$\mathrm{Sim}(\mathrm{m}_i, \mathrm{m}_j) \ = 1 - \mathrm{H}(\mathrm{m}_i, \mathrm{m}_j). \qquad (11)$$

Suppose that we have n sets of evidence; after obtaining the degree of similarity between the sets of evidence, we can construct the similarity measure matrix (SMM), which expresses the agreement between the sets of evidence as follows:

$$\mathrm{SMM} \ = \begin{bmatrix} 1 & \mathrm{Sim}(\mathrm{m_1},\mathrm{m_2}) & \cdots & & \mathrm{Sim}(\mathrm{m_1},\mathrm{m_n}) \\ \vdots & & & & \vdots \\ \mathrm{Sim}(\mathrm{m_2},\mathrm{m_1}) & 1 & \cdots & & \mathrm{Sim}(\mathrm{m_2},\mathrm{m_n}) \\ \vdots & & \ddots & & \vdots \\ \mathrm{Sim}(\mathrm{m_i},\mathrm{m_1}) & & 1 & & \mathrm{Sim}(\mathrm{m_i},\mathrm{m_n}) \\ \vdots & & & \ddots & \vdots \\ \mathrm{Sim}(\mathrm{m_n},\mathrm{m_1}) & \cdots & \cdots & & 1 \end{bmatrix} . \qquad (12)$$

The degree of support of the evidence of a CU with respect to the evidence of other CUs is given as follows:

$$\mathrm{Support}(\mathrm{m}_i) \ = \sum_{\substack{j=1 \\ i \neq j}}^{n} \mathrm{Sim}(\mathrm{m}_i, \mathrm{m}_j) \ . \qquad (13)$$

The credibility degree of evidence is given as follows:

$$\mathit{Credibility}(\mathrm{m_i}) \ = \frac{\mathrm{Support}(\mathrm{m}_i)}{\sum_{i=1}^{n} \mathrm{Support}(\mathrm{m}_i)} \ . \qquad (14)$$

After calculating the credibility of the evidence, we compare it with a fixed threshold value. If the credibility is greater than the threshold value, the user is authenticated as a normal user, and if the credibility is less than the threshold value, the user is considered to be an MU and is prevented from sending its evidence to the fusion center for the final decision.

C. Final Decision at Fusion Center

Once MUs are removed by using the proposed method using the Hausdorff distance, the sets of evidence of the normal users are sent to the fusion center. The fusion center combines these sets of evidence by using the D-S evidence theory. At the fusion center, BPAs are sequentially combined in the order of the arrival of normal evidence as follows:

$$m_{k,global}(H_j) = m_{k-1,global}(H_j) \oplus m_k(H_j) \ , \qquad (15)$$

where j = 0,1, $m_{k,global}(H_j)$ and $m_{k-1,global}(H_j)$ denote the k-th and (k-1)-th global BPA hypothesis H_j , respectively, and the combination operator $\oplus$ is defined on the basis of the evidence theory as follows:

$$m_a(H_j)\oplus \mathrm{m_b}(\mathrm{H_j})=\frac{m_a(H_j)m_b(\Omega)+m_a(H_j)\mathrm{m_b}(\mathrm{H_j})+m_a(\Omega)m_b(H_j)}{1-[(m_a(H_j)\mathrm{m_b}(\mathrm{H_{1-j}})+m_a(H_{1-j})\mathrm{m_b}(\mathrm{H_j})]}\ , \quad (16)$$

where $j = 0,1$ and a and b denote the two arbitrary combining sources.

The final decision f_d at the fusion center can be calculated as follows:

$$f_d=\begin{cases} H_1 & ;\ \dfrac{m(H1)}{m(H0)}>\lambda \\ H_0 & ;\ \dfrac{m(H1)}{m(H0)}\le\lambda \end{cases}, \quad (17)$$

where λ denotes the threshold for the hypotheses H_0 and H_1, respectively.

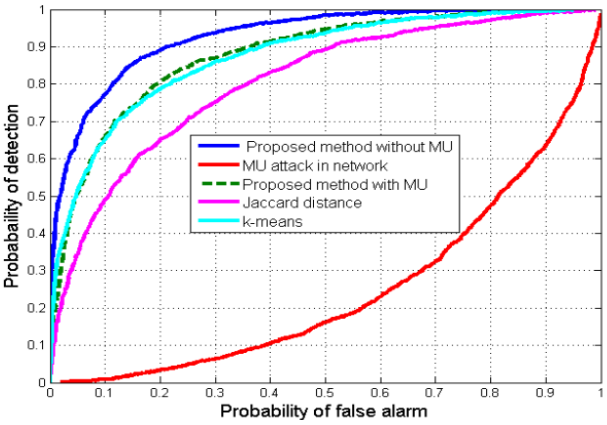

Fig. 4. ROC curve in always busy attack. MU: malicious user.

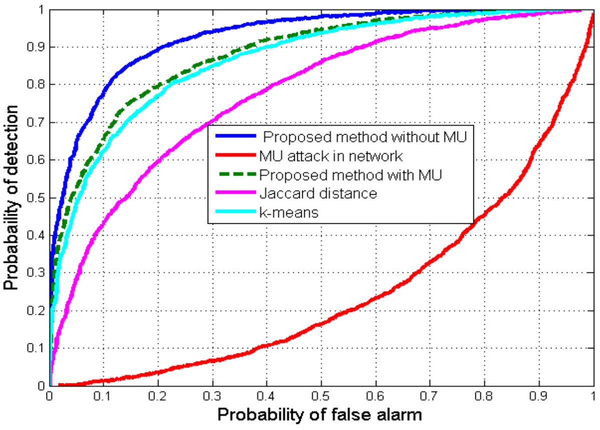

Fig. 5. ROC curve in always free attack. MU: malicious user.

IV. SIMULATION RESULTS AND ANALYSIS

This section presents the results of MATLAB simulations of the proposed method and compares the performance of the proposed method with that of the k-means and Jaccard distance methods. Simulations consider scenarios with and without MUs. According to the CR system, every CU should vacate the channel if an LU signal is detected. Thus, the existence of an MU will degrade the performance of cooperative spectrum sensing.

In scenarios with MUs, five CUs are randomly placed, among which one is an MU. The energy of each CU is measured using MED, and the information from MED is combined at each CU by using the EGC method; the number of MEDs = 2. The probability of the presence of an LU is set to 0.5, the bandwidth is set to 6 MHz, and the sensing time is set to 50 µs. The fusion center combines the sets of evidence of the normal users sequentially and forms a global decision.

We consider three types of SSDF attacks: always busy (AB), always free (AF), and random attack in the network. In an AB attack, the MU changes the evidence of $\mathrm{m_i}(H_1)$ in the absence of an LU, which increases the probability of a false alarm and decreases the probability of detection. In an AF attack, the malicious user changes the evidence of $\mathrm{m_i}(H_0)$ in the presence of an LU, which increases the probability of misdetection and decreases the probability of a false alarm, whereas in the case of a random attack, the MU carries out the AB and AF attacks randomly with probability p.

In Fig. 4, we have drawn the receiver operating characteristic (ROC) curve of the proposed method for an AB attack and compared its performance with the performance of the k-means and Jaccard distance methods. We have shown the performance of the proposed method with and without an MU attack in the network. It can be observed that when an AB attack occurs in the network, the probability of a false alarm increases and the probability of detection decreases; for example, when the probability of a false alarm equals 0.2, the probability of detection decreases from 0.9 to 0.1. The proposed method is able to detect and remove an MU from the network, resulting in better performance than the Jaccard distance and k-means methods.

In an AF attack, the probability of a false alarm decreases, while the probability of misdetection increases, which increases the interference in the network. In Fig. 5, we have plotted the ROC curve with and without an MU in the network. It can be observed that the proposed method detects an MU and mitigates its adverse effects more effectively than the Jaccard distance method. The k-means method matches the performance of the proposed method at some points because it randomly selects the starting point for differentiating between the MU evidence and the normal user evidence.

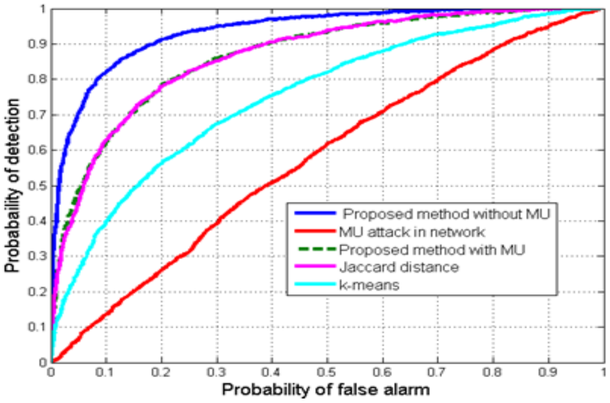

Fig. 6. ROC curve in random attack. MU: malicious user.

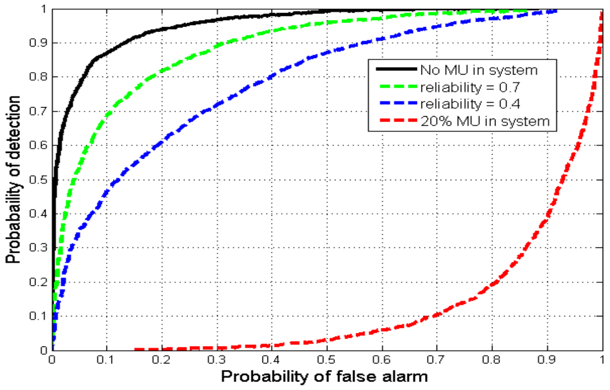

Fig. 7. ROC curve of proposed method for different reliability values. MU: malicious user.

The simulation results of a random attack by an MU are shown in Fig. 6. The performance of the proposed method is better than that of the k-means and Jaccard distance approaches. From the simulation results, we can conclude that in all cases, i.e., AB, AF, and random attacks, the proposed method is better than the Jaccard distance and k-means methods in detecting an MU and mitigating its adverse effects on cooperative spectrum sensing.

In Fig. 7, we have shown the ROC curve for scenarios with and without an MU and different values of reliability. As the reliability of the CU increases, it allows more sets of evidence to be sent to the FC and yields better results, which can be observed in Fig. 7, when the reliability increases from 0.4 to 0.7, because more sets of evidence reach the FC to help formulate a better decision.

V. CONCLUSION

In this paper, we proposed a method using the Hausdorff distance and a similarity measure matrix with the D-S evidence theory to detect an MU in a network and mitigate its adverse effects. The D-S evidence theory is one of the candidates to deal with the uncertainty of the evidence and improve the spectrum sensing performance. In this work, we considered three types of SSDF attacks, i.e., AB, AF, and random attacks. In our simulation, we compared the proposed method with the Jaccard distance method, which is also based on similarity, and with the k-means method. On the basis of the simulation results, we have shown that the proposed method is more effective than the other methods with respect to SSDF attacks.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) funded by the Korea government (MEST) (No. NRF-2012R1A1A2038831).

REFERENCES

[1] Federal Communications Commission, *Spectrum Policy Task Force* (ET Docket No. 02-135). Washington, DC: Federal Communications Commission, 2002.

[2] A. Ghasemi and E. S. Sousa, “Collaborative spectrum sensing for opportunistic access in fading environments,” in *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, Baltimore, MD, pp. 131-136, 2005.

[3] J. Li, Z. Feng, Z. Feng, and P. Zhang, “A survey of security issues in cognitive radio networks,” *China Communications*, vol. 12, no. 3, pp. 132-150, 2015.

[4] R. Chen, J. M. Park, and K. Bian, “Robust distributed spectrum sensing in cognitive radio networks,” in *Proceedings of the 27th Conference on Computer Communications (INFOCOM 2008)*, Phoenix, AZ, pp. 1876-1884, 2008.

[5] A. W. Min, K. G. Shin, and X. Hu, “Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation,” *IEEE transactions on Mobile Computing*, vol. 10, no. 10, pp. 1434-1447, 2011.

[6] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, “Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users,” *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 1058-1073, 2014.

[7] S. Liu and B. Hu, “Analysis of sensing efficiency for cooperative spectrum sensing with malicious users in cognitive radio networks,” *IEEE Communications Letters*, vol. 18, no. 9, pp. 1645-1648, 2014.

[8] E. Soltanmohammadi and M. Naraghi-Pour, “Fast detection of malicious behavior in cooperative spectrum sensing,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 377-386, 2014.

[9] A. U. Aisha, J. Qadir, and A. Baig, “Mitigating the effect of malicious users in cognitive networks,” in *Proceedings of 2013*

11th International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, pp. 7-12, 2013.

[10] C. Chen, M. Song, C. Xin, and M. Alam, "A robust malicious user detection scheme in cooperative spectrum sensing," in *Proceedings of 2012 IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, pp. 4856-4861, 2012.

[11] Q. Peng, K. Zeng, W. Jun, and S. Li, "A distributed spectrum sensing scheme based on credibility and evidence theory in cognitive radio context," in *Proceedings of IEEE 17th international symposium on Personal, Indoor and Mobile Radio Communications*, Helsinki, pp. 1-5, 2006.

[12] N. Nguyen-Thanh and I. Koo, "An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context," *IEEE Communications Letters*, vol. 13, no. 7, pp. 492-494, 2009.

[13] M. Ghaznavi and A. Jamshidi, "A reliable spectrum sensing method in the presence of malicious sensors in distributed cognitive radio network," *IEEE Sensors Journal*, vol. 15, no. 3, pp. 1810-1816, 2015.

[14] N. Nguyen-Thanh and I. Koo, "A robust secure cooperative spectrum sensing scheme based on evidence theory and robust statistics in cognitive radio," *IEICE Transactions on Communications*, vol. 92, no. 12, pp. 3644-3652, 2009.

[15] J. Wang, S. Feng, Q. Wu, X. Zheng, Y. Xu, and G. Ding, "A robust cooperative spectrum sensing scheme based on Dempster-Shafer theory and trustworthiness degree calculation in cognitive radio networks," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, 1-12, 2014.

[16] J. Wang and I. R. Chen, "Trust-based data fusion mechanism design in cognitive radio networks," in *Proceedings of 2014 IEEE Conference on Communications and Network Security (CNS),* San Francisco, CA, pp. 53-59, 2014.

[17] Y. Han, Q. Chen, and J. X. Wang, "An enhanced DS theory cooperative spectrum sensing algorithm against SSDF attack," in Proceedings of *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, Yokohama, Japan, pp. 1-5, 2012.

[18] M. S. Khan and I. Koo, "An enhanced cooperative spectrum sensing scheme based on new rule of combining evidences in cognitive radio," in *Ubiquitous Computing Application and Wireless Sensor: UCAWSN-14.* Heidelberg: Springer, pp. 77-87, 2015.

[19] J. Diaz, M. Rifqi, and B. Bouchon-Meunier, "A similarity measure between basic belief assignments," in *Proceedings of 2006 9th International Conference on Information Fusion*, Florence, Italy, pp. 1-6, 2006.

[20] F. Hausdorff, *Set Theory*, 1st ed. New York, NY: Chelsea Publishing, 1957.

Muhammad Sajjad Khan

received his B.Sc. in Computer Information Systems Engineering from University of Engineering & Technology, Peshawar, Pakistan, in 2004, and his M.E. degree from Mehran University of Engineering & Technology, Jamshoro, Pakistan, in 2007. He is currently pursuing his Ph.D. degree at the University of Ulsan, S. Korea. His research interests include wireless communication and cognitive radio networks with an emphasis on cooperative spectrum sensing.

Insoo Koo

received his B.E. degree from Konkuk University, Seoul, Korea, in 1996, and his M.S. and Ph.D. degrees from Gwangju Institute of Science and Technology (GIST), Gwangju, Korea, in 1998 and 2002, respectively. From 2002 to 2004, he worked with Ultrafast Fiber-Optic Networks (UFON) Research Center in GIST, as a research professor. For one year from September 2003, he was a visiting scholar at Royal Institute of Science and Technology, Sweden. In 2005, he joined University of Ulsan, where he is now a full professor. His research interests include next-generation wireless communication systems and wireless sensor networks.