An Enhanced D-S Theory Cooperative Spectrum Sensing Algorithm against SSDF Attack

Yong Han
School of Electronic Science and Engineering
National University of Defense Technology
Changsha, China
e-mail: han_yong@163.com

Qiang Chen, Jian-Xin Wang
Institute of China Electronic System Engineering Corporation
Beijing, China

Abstract—**The current D-S theory cooperative spectrum sensing algorithms think all cognitive users are honest and don't consider malicious user existing. When a malicious user falsifies its local sensing result and sends error data to the data fusion center, it will damage the cooperative spectrum sensing performance badly, which is called spectrum sensing data falsification (SSDF) attack. Due to the difference between the malicious user's evidence and other cognitive users', we use the similarity degree to calculate the reliability of evidence and propose a detection method against SSDF attack. The data fusion center removes the evidence with lower reliability and combines reliable evidences which is considered to been sent by honest cognitive users. As simulation results shown, the proposed method defends against the SSDF attack effectively and enhances the robustness of the D-S theory cooperative spectrum sensing algorithm.**

Keywords-Cooperative spectrum sensing; D-S theory; SSDF attack

I. INTRODUCTION

Recently, cognitive radio is proposed to solve the conflicts between spectrum scarcity and spectrum under-utilization [1]. It can improve the spectrum utilization by allowing cognitive user (CU) to borrow unused radio spectrum from the licensed user (LU) or to share the spectrum with the licensed user. Spectrum sensing by far is the most important component for the establishment of cognitive radio, which is the task of obtaining awareness about the spectrum usage and existence of LU in a geographical area [2]. However, due to the hidden-terminal problem which is caused by multipath fading, shadow effect and obstacles, single cognitive user can't distinguish between vacant band and deep fading band. In order to solve the uncertainty of local spectrum sensing, cooperative spectrum sensing with a distributed sensing model has been considered [3~8]. Through combining two or more cognitive user's local sensing result and makes the final decision, it can improve the performance of spectrum sensing remarkably. In [5], an optimal data fusion rule combining with a counting rule is proposed. In [6], the half-voting rule is the optimal fusion rule under identical threshold for all CUs. In [7] and [8], Dempster Shafer theory of evidence (D-S theory) is applied into cooperative spectrum sensing. Every cognitive user is assigned proper credibility according to its local sensing result. Combining all cognitive users' credibility by D-S theory, it can get a better performance than the traditional "And" and "Or" logic fusion rule.

But these schemes assume all cognitive users are honest and treat all cognitive users' local sensing result undiscriminating. When a malicious user (MU) falsifies its local sensing result and sends error data to the data fusion center, existing cooperative spectrum sensing schemes are typically vulnerable to attacks, which is called spectrum sensing data falsification (SSDF) attack [10]. In order to avoid the damage from SSDF attack, [11] uses a weighted sequential probability ratio test scheme to lessen the malicious user's influence. In [12], a reputation-based mechanism is introduced to identify misbehaviors and mitigate their harmful effect on sensing performance. In [13], it applies an outlier detection method to detect such malicious users. Pre-filtering of the sensing data is essential in identifying and removing the malicious nodes which significantly affect the final decision at the data fusion center by giving extreme false decision. D-S theory is an available uncertainty reasoning method which behaves well in cooperative spectrum sensing. However, above methods can't be used into the D-S theory cooperative spectrum sensing algorithm against SSDF attack. Reference [7] and [8] just study how to apply D-S theory in the cooperative spectrum sensing, but they don't take into account the malicious user existing. In SSDF attack, a malicious user falsifies its local sensing result. There is a difference between the malicious user's evidence and other cognitive user's, which can be used to detect the SSDF attack.

The rest of the paper is organized as follows. In Section II, the system model and D-S theory are introduced. We present an available detection method against SSDF attack in Section III, which uses the similarity degree among evidences to scale evidence reliability and only allow evidences with enough high reliability to participate the final fusion. Simulation results are given in Section IV followed by conclusions in Section V.

II. SYSTEM DESCRIPTION

In the cooperative spectrum sensing based on D-S theory, the data fusion center receives evidence from each cognitive user. Then it combines all evidences and makes the final decision as shown in Fig. 1.

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

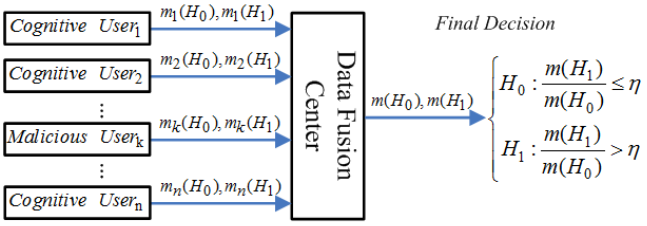

Figure 1. Cooperative spectrum sensing based on D-S theory

A. D-S Theory

Due to stochastic characteristics of wireless channels, there is uncertainty in local detection results at CU. D-S theory uses credibility not using probability so it can deal with uncertainty. As an available way to process uncertainty, D-S theory is just one good choice for decision making in CR system [9].

Define 2.1: U is a finite set of mutually exclusive and exhaustive hypotheses, called the frame of discernment. There is a mapping function $m : 2^U \rightarrow [0,1]$ satisfying

$$m(\phi) = 0 \text{ , and } \sum_{A \subset U} m(A) = 1 . \qquad (1)$$

$m(A)$ is called basic probability assignment (BPA) of A. For any $A \subseteq U$, $m(A)$ represents the belief that one is willing to commit exactly to A, given a certain piece of evidence. The subsets A of U such that $m(A) > 0$ are called the focal elements of U.

In D-S theory, evidences can be combined by the so-called D-S rule of combination which provides the way to combine evidences. The combination rule is the foundation of uncertainty reasoning. Dempster rule is the most basic combination rule, as shown in (2). Suppose m_1 and m_2 are two independent basic probability assignments. Their element are A_{11} ,…, A_{1n} and A_{21} ,…, A_{2n} respectively. Through Dempster rule, we can get a new BPA $m = m_1 \oplus m_2$.

$$m(A) = \frac{1}{1-k} \sum_{A_{1i} \cap A_{2j} = A} m_1(A_{1i}) m_2(A_{2j}) \qquad (2)$$

and $k = \sum_{A_{1i} \cap A_{2j} = \phi} m_1(A_{1i}) m_2(A_{2j})$

B. Cooperative Spectrum Sensing

Local spectrum sensing is essentially a binary hypotheses testing problem, with the null hypothesis H_0 corresponding to LU signal absent and the alternative hypothesis H_1 corresponding to LU signal present, that is

$$\begin{cases} H_0 : x(t) = n(t) \\ H_1 : x(t) = h(t)\, s(t) + n(t) \end{cases} \qquad (3)$$

In (3), $x(t)$ represents received signal at CU, $h(t)$ is the channel gain, $s(t)$ is the transmitting signal from LU and $n(t)$ is the additive white Gaussian noise. All CUs and LU are considered in the same region where they share common spectrum allocation schemes.

The power of received signal samples is measured at CU [14]. The sensing statistic is equivalent to an estimation of received signal power which is given at each CU by

$$x_{E_i} = \sum_{j=1}^{N} \left| x_j \right|^2 , N = 2TW \qquad (4)$$

where x_j is the j-th sample of received signal and TW represents the detection time and signal bandwidth product. When N >250, x_{E_i} can be well approximated as a Gaussian random variable under both hypotheses H_0 and H_1, with mean μ_0 , μ_1 and variance σ_0^2 , σ_1^2 respectively [8].

$$\begin{cases} \mu_0 = N, \sigma_0{}^2 = 2N \\ \mu_1 = N(\gamma+1), \sigma_1{}^2 = 2N(2\gamma+1) \end{cases} \qquad (5)$$

where γ is the signal to noise ratio (SNR) of the LU transmitting signal at the CU.

$$\begin{aligned} H_0 : m_i(x_{E_i} \mid H_0) &= \frac{1}{\sqrt{2\pi}\sigma_0} \exp(-\frac{(x_{E_i} - \mu_0)^2}{\sigma_0^2}) \\ H_1 : m_i(x_{E_i} \mid H_1) &= \frac{1}{\sqrt{2\pi}\sigma_1} \exp(-\frac{(x_{E_i} - \mu_1)^2}{\sigma_1^2}) \end{aligned} \qquad (6)$$

In cooperative spectrum sensing based on D-S theory, every CU must estimates the BPA according to its local sensing result under the framework of discernment $U = \{H_0, H_1\}$. Equation (6) is the BPA according to the cumulated power x_{E_i} of received signal for energy detection [7]. Once receiving $m_i(H_0)$ and $m_i(H_1)$ from CU_i, the data fusion center uses Dempster rule to combine the evidence. It makes the final decision when all cognitive users' evidences have been received and combined.

III. DETECTION METHOD AGAINST SSDF ATTACK

As shown in Fig. 1, there is a malicious user which disturbs the cooperative spectrum sensing and wants to acquire more chance to use spectrum band. It falsifies its local sensing result and sends error data to the fusion center. In the data fusion center these error data conflict with other CU's, which worsen the performance of cooperative spectrum sensing.

A. Max-Min Similarity Degree

Because a malicious user falsifies its local sensing result, its evidence is different from other CU's in some degree. If one CU's evidence is similar to others, its evidence has a higher reliability, namely it is supported by others. If one CU's evidence isn't similar to others, its evidence has a lower reliability. When the reliability of evidence is lower than a fixed threshold, the cognitive user can be considered as a malicious user which sends falsified local sensing result.

Define 3.1: U is the frame of discernment. H_0 and H_1 are two mutually exclusive and exhaustive hypotheses ($N=2$). m_i and m_j is two basic probability assignment on U , the similarity degree between m_i and m_j can be described:

$$sim(m_i,m_j)=\frac{\sum_{k=1}^{2^N}\min(m_i(A_k),m_j(A_k))}{\sum_{k=1}^{2^N}\max(m_i(A_k),m_j(A_k))} \qquad (7)$$

where $A_k \in P(U)$, $P(U)=\{\phi,H_0,H_1,\Theta\}$ is set of all result of discernment. $\Theta=\{H_0,H_1\}$ represents uncertain information that maybe H_0 or H_1 is true and ϕ is empty set [15].

For n cognitive users, the similarity degree matrix Sim can be attained:

$$Sim=\begin{bmatrix} 1 & ... & sim(m_1,m_j) & ... & sim(m_1,m_n) \\ \vdots & 1 & \vdots & \vdots & \vdots \\ sim(m_i,m_1) & ... & 1 & ... & sim(m_i,m_n) \\ \vdots & \vdots & \vdots & 1 & \vdots \\ sim(m_n,m_1) & ... & sim(m_n,m_j) & ... & 1 \end{bmatrix} \qquad (8)$$

So the support to CU_i from other n-1 cognitive users can be defined.

$$Sup(m_i)=\sum_{j=1}^{n} sim(m_i,m_j) \qquad j\neq i \qquad i,j=1...n \qquad (9)$$

Then the reliability of evidence m_i can be acquired by normalization.

$$Rel(m_i)=\frac{Sup(m_i)}{\max\limits_{i=1...n}(Sup(m_i))} \qquad (10)$$

B. Detection Method

The malicious user aims to disturb the final decision so its evidence can't bring any help for the cooperative spectrum sensing. The reliability of evidence can be used to detect the malicious user. If $Rel(m_i)$ of evidence m_i is lower than the threshold r , the evidence is considered to be sent by malicious user, which can't be used for the combination in the data fusion center. When $Rel(m_i)$ is higher than the threshold r , the evidence can be used for the final decision. Detailed step is as follows:

(1) Cognitive user CU_i calculates $m_i(H_0)$ and $m_i(H_1)$ according to its local sensing result by (6);

(2) The data fusion center collects all evidences and calculates the evidence reliability $Rel(m_i)$ of CU_i ;

(3) If $Rel(m_i)\leq r$, the evidence m_i is removed. r is the fixed reliability threshold;

(4) If $Rel(m_i)>r$, the evidence m_i is reliable, and can be combined in the data fusion center;

(5) Using Dempster rule to combine all reliable evidence $m_i(H_0)$ and $m_i(H_1)$.

C. Final Decision

After getting the final combination result $m(H_0)$ and $m(H_1)$, the data fusion center compares $\frac{m(H_1)}{m(H_0)}$ with the decision threshold η . If $\frac{m(H_1)}{m(H_0)}\leq\eta$, the final decision is H_0 ; if $\frac{m(H_1)}{m(H_0)}>\eta$, the final decision is H_1 . With η changing, the corresponding false alarm probability P_f and detection probability P_d can be acquired, which is used to draw the receiver operating characteristics curves (ROC).

IV. Simulation and Analysis

In our simulation, we set up a scene in which there is a wireless LAN within DTV television signal transmitting area. DTV signal is LU signal. The probability of LU appearing is 0.5. The band is 6 MHz. The WLAN is composed of ten cognitive nodes. Ten cognitive nodes lie around arbitrarily, which use energy detection as local spectrum sensing algorithm. The sensing time is 50 μs . As the data fusion center, the access point (AP) combines evidences from each cognitive user and makes the final decision. AWGN channel is considered between LU and CU. The channel between CU and AP is perfect. Three typical SSDF attacks are considered: Always Busy, Always Free and Random attack. In Always Busy SSDF attack a malicious user changes $m_i(H_1)$ to $m_i(H_1)+\Delta$ when LU signal is absent, which probably make the fusion center think LU is present. Always Free SSDF attack changes $m_i(H_0)$ to $m_i(H_0)+\Delta$ when LU signal is present. And in Random SSDF attack a malicious user starts Always Busy attack and Always Free attack randomly by probability p .

Assume there is a malicious user in WLAN, namely 10% malicious user existing. When LU signal is absent, the malicious user starts Always Busy attack. As shown in Fig. 2, P_d descends from 0.6 to almost equal to zero at P_f =0.2. When using the proposed detection method to remove the evidence of malicious user, cooperative spectrum sensing performance improves obviously. When $r=0.7$ or $r=0.9$, the performance is very close to the performance without malicious user. Because of the statistic characteristics of x_{E_i} , the evidence of malicious user maybe have a higher reliability than the threshold $r=0.5$ so the performance improves just a little better. In Fig. 3 malicious user starts Always Free attack when LU is present. At P_f =0.2, P_d descends from 0.6 to almost zero. When using the proposed detection method, the performance also improves obviously.

As shown in Fig. 4, it depicts the performance improved when there is Random attack. The malicious user starts attack by $p = 0.5$. When LU is absent, the malicious user starts Always Busy attack. When LU is present, the malicious user starts Always Free attack. It proves that the proposed detection method can defend against the SSDF attack effectively. In Fig. 5, it depicts the curves between P_f and P_d with different attack probability p . Here, the final decision threshold η is 1. With the attack probability p increasing, the Random attack from malicious user makes P_d decrease from 0.6 to zero and P_f increase from 0.3 to 1. When using SSDF attack detection method, the evidence of malicious user is excluded from the combination in the fusion center. As show in Fig. 5 the ROC curve keeps steady with the attack strength increasing.

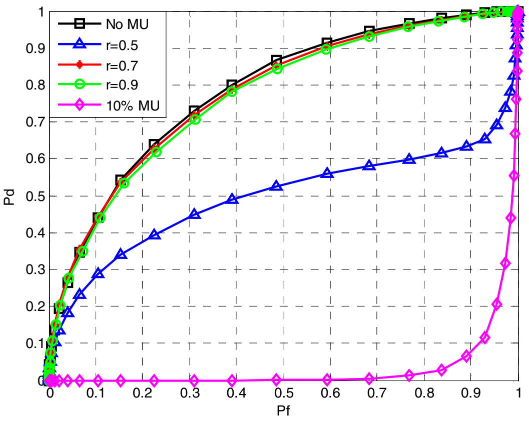

Figure 2. Spectrum sensing performance in Always Busy attack

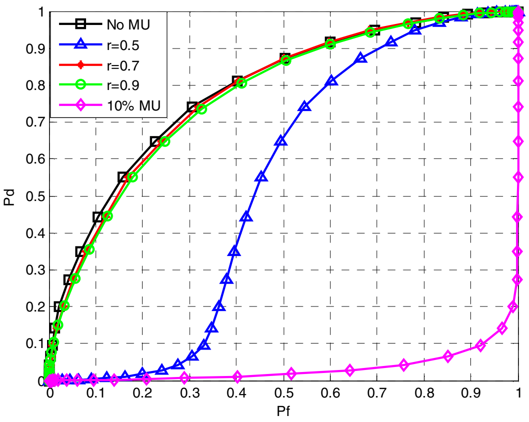

Figure 3. Spectrum sensing performance in Always Free attack

V. Conclusion

D-S theory is an available uncertainty reasoning method which has behaved well performance in the cooperative spectrum sensing. Because of the malicious user existing, SSDF attack can damage the cooperative spectrum sensing performance badly. In order to improve the robustness of the cooperative spectrum sensing based on D-S theory, we use similarity degree to measure the evidence reliability and propose an available SSDF attack detection method. Through the reliability of evidence, we think the evidence with very low reliability is sent by malicious user and is excluded from the combination in the fusion center. By simulation verification, the proposed method can defend against the SSDF attack effectively and enhances the robustness of the D-S theory cooperative spectrum sensing algorithm.

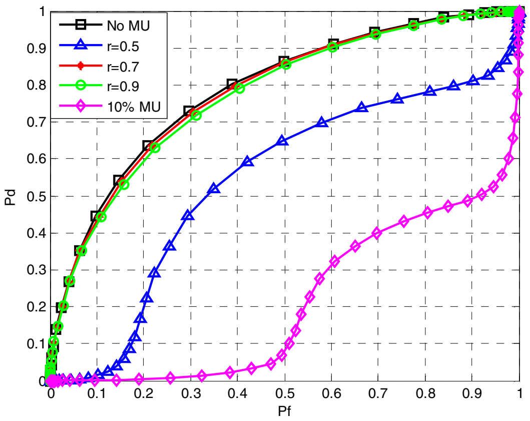

Figure 4. Spectrum sensing performance in Random attack (*p*=0.5)

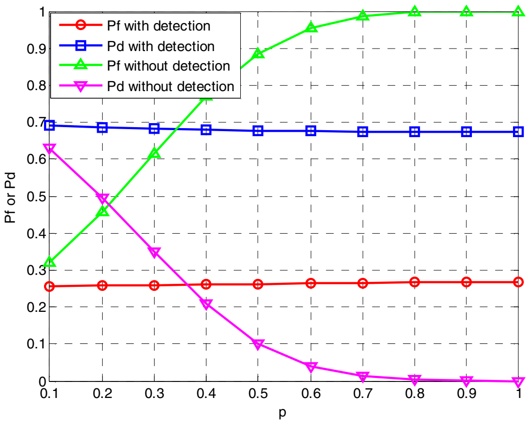

Figure 5. *Pf, Pd* at different attack probability *p*

References

[1] S.Haykin, "Cognitive radio: brain-empowered wireless communications," IEEE Journal on Selected Areas in Communications, vol. 23, no.2, pp.201-220, Feb. 2005.

[2] T.Yucek, and H.Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," IEEE Communications Surveys & Tutorials, vol.11, no.1,pp. 116-130, First Quarter 2009.

[3] A.Ghasemi, and E.S.Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," IEEE 1st International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005, pp.131-136.

[4] B.Shen, T.P.Cui and K.Kwak,et al, "An Optimal Soft Fusion Scheme for Cooperative Spectrum Sensing in Cognitive Radio Network," IEEE

Wireless Communications and Networking Conference,April 2009, pp.1-5.

[5] L.Chen, J.Wang, and S.Li, "An adaptive cooperative spectrum sensing scheme based on the optimal data fusion rule," in Proc.4th Int.Symposium on Wireless Communication Systems, Oct. 2007,pp.582-586.

[6] Z.Wei, R.K.Mallik, and K.Ben Letaief,"Cooperative spectrum sensing optimization in cognitive radio networks," IEEE International Conference on Communications, May 2008,pp.3411-3415.

[7] Q.H.Peng, Z.Kun and J.Wang, et al, "A Distributed Spectrum Sensing Scheme Based On Credibility and Evidence Theory in Cognitive Radio Context," IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications,Sept. 2006, pp. 1-5.

[8] Nhan Nguyen-Thanh and Insoo 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,July 2009, pp.492-493.

[9] G.Shafer, A Mathematical Theory of Evidence, Princeton, NJ: Princeton Univ.Press,1976.

[10] R.L.Chen, J.M.Park and Y.T.Hou, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE Communications Magazine, vol.46,no.4, April 2008,pp.50-55.

[11] R.L.Chen, J.M.Park and K.G.Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE 27th Conference on Computer Communications, April 2008,pp.1876-1884.

[12] K.Zeng, P.Pawelczak and D.Cabric, "Reputation-Based Cooperative Spectrum Sensing with Trusted Nodes Assistance," IEEE Commun. Letters, vol.14,no.3,March 2010,pp.226-228.

[13] P.Kaligineedi, M.Khabbazian and V.K.Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," IEEE International Conference on Communications, May 2008,pp.3406- 3410.

[14] F. F. Digham, M. S. Alouini and M. K. Simon, "On the Energy Detection of Unknown Signals Over Fading channels," IEEE Transactions on Communications, vol. 55,no.1, Jan. 2007,pp.21-24.

[15] L.F. Hu, X Guan, and Y.He, "Evidence Fusion Method Based on Reliability," Signal Processing, vol.26,no.1, Jan. 2010,pp:17-22.