Effect of malevolent interferences on Cooperative Spectrum Sensing

[1]Mahak Kalra[0000-0001-9341-9836],[2]Anil Vohra[0000-0003-1377-3451],[3]Nikhil Marriwala[0000-0002-1093-630X]

[1]Department of Electronic Science, Kurukshetra, India
[2]Electronic Science Department, Kurukshetra University Kurukshetra, India
[3]UIET, Kurukshetra University Kurukshetra, India

ABSTRACT The existence of malevolent interferences and intrusions in the Cognitive Radio networks will dramatically deteriorate the efficiency of spectrum sensing. Throughout this paper, the changes in the cooperative spectrum sensing network model have been proposed .In this paper we have modified the cooperative spectrum sensing model to analyse malevolent interferences, where a fusion centre is transmitted the local signal to noise and disruption power ratios for making appropriate decisions. Performance analysis has been done in terms of various variables i.e. false alarm and detection chance. Simulation findings are given to validate the theoretical analysis.

Keywords*:* - Cognitive Radio, Cooperative Spectrum Sensing, Malevolent interferences, False alarm probability, Detection probability.

INTRODUCTION

Cognitive Radio, **a wireless networking network** is based on a software that describes a radio technology which offers a forum for modular radio network, multiservice, multi-standard, multiband, reconfigurable and reprogrammable device as evolving technology. It utilizes environmental sensing and modelling methods and adapts in real time to statistical variations. The nodes present in the wireless network change their parameters of transmission of the signal or its reception to communicate effectively anywhere and at any time , avoiding interference with licensed or unlicensed users for the effective use of the radio spectrum Shadowing, faulty sensors or shadowing attenuates the performance of the single detector, so we use cooperative spectrum sensing to get better performance. It increases the detector 's efficiency and merges with the one and several other SUs to feel the frequency and locate the gaps in the range. This provides the specifics of the spectrum usage of the different locations where cerebral radios are best placed. Typically the detectors we use have previous information but in some of the detectors we don't require the previous awareness. Another version of CSS detector can be employed in which estimation of local signal to interference and noise (SINRs) is done in Sus and sent to the fusion centre for decision making[1]. Malicious User (MU) degrades the detection performance of cooperative spectrum sensing. A MU is an unauthorized and undesired user who fakes the identity as an authorized user and manipulates the status of the primary signal. In order to nullify the negative impact caused by malicious users, many CSS detectors have been considered. Initially the detector that was proposed required some previous knowledge to be known like statistical characteristics of channel from primary users to secondary users, signal to noise power ratios (SNR) at secondary users and noise power. But sometimes the previous knowledge is not available to secondary users hence in order to solve this dilemma a new detector that doesn’t require previous knowledge was proposed and could also deal with malicious interference. In this paper there is a new approach given to tackle with the malicious interferences where the SINRs are approximated at secondary users and later sent to the fusion center for making decisions .

In this paper, we propose modifications in [1] and studied the variations in different factors like number of malevolent users, number of segments etc. to observe the corresponding changes in the false alarm probability, detection probability and the ROC curve.

I. SYSTEM MODEL

Let us imagine a cerebral radio network scenario in which, along with certain harmful applications, there are a variety of secondary users in the service region of a PU. Such secondary users operate together to detect the spectrum that is not being utilized by the PU and the malevolent users pose barriers and deteriorate the efficiency of spectrum sensing.
Let K denote the number of SUs,P denote the total number of malevolent users who trigger interferences, and let L denote the number of samples who the device gets in one sensing time.

A. Proposed Detector

Because of our low number complexity, we can divide the L samples of each UC into successive J segments for each N-sample segment with a limited number of SINRs. As a result, we divide each SU into N-samples segments. JN = L. J. It is rational to take the view that the SUs will use the communication protocol in the PU network to estimate the SINRs by several methods, such as second-order frequency domain estimators[2]. The SUs have the primary signal characteristics of the PU. Inspired by work[3], a new CSS detector is used in the fusion center to make decisions using local SINRs at SUs.
In this scenario, the malevolent interferences are taken into account and therefore the normalization factor is considered to be the background interference and noise.

B. Performance Analysis

We define the approximate distribution of Tproposed to obtain the likelihood of a false alarm and the detection for the following detector proposed:-

$$T_{\text{Proposed}}|\mathcal{H}_0 \sim \text{Gamma}\left(\frac{K-1}{2}, \frac{2(K-1)}{KJ}\sigma_0^2\right).$$

$$T_{\text{Proposed}}|\mathcal{H}_1 \sim \text{Gamma}\left(\frac{K-1}{2}, \frac{2(K-1)}{KJ}\sigma_1^2\right).$$

Where H0 and H1 are the null and alternative hypotheses describing the lack of main signs and their existence respectively.
Consequently, the false alarm and the detection probability of a decision threshold can be respectively given by:-

$$P_f(\lambda) = \int_{\lambda}^{+\infty} f\left(u; \frac{K-1}{2}, \frac{2(K-1)}{KJ}\sigma_0^2\right) du$$

$$P_d(\lambda) = \int_{\lambda}^{+\infty} f\left(u; \frac{K-1}{2}, \frac{2(K-1)}{KJ}\sigma_1^2\right) du$$

Where

$$f(u; \alpha, \beta) = \frac{1}{\Gamma(\alpha)\beta^{\alpha}} u^{\alpha-1} e^{-\frac{u}{\beta}}.$$

Hence the SINR is calculated as

$$\text{SINR} = \frac{\frac{1}{K}\sum_{k=1}^{K} g_k^0 |h_k^0|^2 \sigma_s^2}{\frac{1}{K}\sum_{k=1}^{K}\sum_{p=1}^{P} g_k^p |h_k^p|^2 \sigma_i^2 + \sigma_n^2}.$$

$$\sigma_0^2 = \frac{2n_2^2(n_1+n_2-2)}{n_1(n_2-2)^2(n_2-4)}$$

$$\sigma_1^2 = (1+\mathrm{SINR})^2\frac{2n_2^2(n_1+n_2-2)}{n_1(n_2-2)^2(n_2-4)}.$$

And SINR=1/[(1/SIR)+(1/SNR)].

Where

n1 and n2 are DOF given as n1 = 2(N −|Sns|) and n2 = 2|Sns|

where the set of null subcarriers are denoted by Sns and its cardinality is denoted by |Sns|.

II. SIMULATION RESULTS

Numerical evidence is given in this section to verify the theoretical findings and to test the output of the detector being proposed.

Illustration. 1 Shows variances between the P=2, 4, 6, 8, 10 identification likelihood and the judgment threshold.

Illustration. 2 Shows the difference between a false warning likelihood and a judgment threshold holding P stable and increasing J from 5 to 20 at an interval of 5 each.

Illustration. 3 Shows the ROC curve varying from 5 to 25 at 10 intervals each where the graph is plotted between the likelihood of missed detection and the likelihood of false alarm.

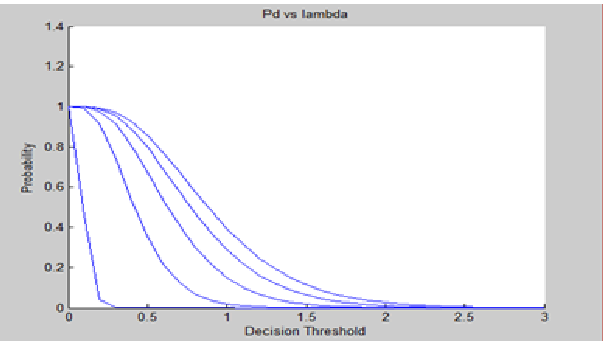

Fig. 1

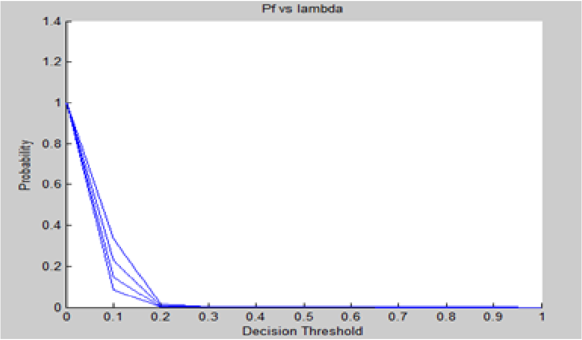

Fig. 2

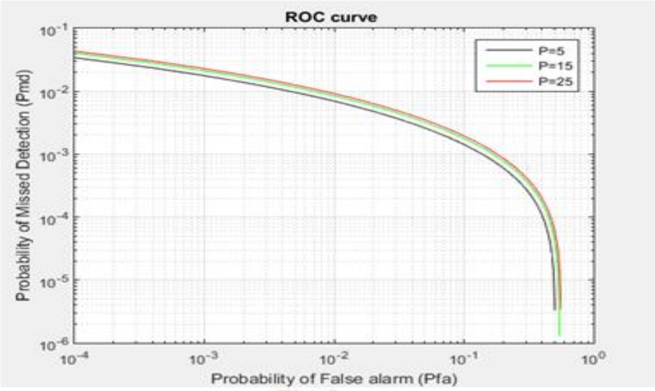

Fig. 3

In comparison with previous detectors, detector performance proposed in the approach taken above is quite good, the detection probability is high, and the likelihood of false alarm is low for an efficient detector as required.

The different factors that influence the results vary, and the shifts in the curves concerned are respectively observed.

In likelihood of detection vs decision threshold curve, as the number of malicious users is raised, we get identification chance as zero at a higher decision threshold value.

From the curve it can be verified that the probability rate of detection decreases as the curve slope decreases with a higher value of the number of malicious users.

In the likelihood of false alarm vs decision threshold curve, as the value of J increases, the decision threshold remains the same but the rate of fall of false alarm probability decreases.

Hence it can be said that if the samples include more segments then the detector 's performance becomes more efficient.

The increase in the amount of malicious users does not modify the risk of false alarm versus decision threshold. In the ROC graph, the probability of missing identification and the risk of false warning decreases with the amount of malicious users(P) producing intervention for the same lambda decision threshold.

III. CONCLUSION

A mutual spectrum sensing device was suggested and introduced in this paper to examine the efficacy of detection in terms of false warning and likelihood of identification to cope with malevolent interferences. Numerical models are tested for checking the efficacy of detectors or the theoretical words. Various impact parameters were found.

IV. REFERENCES

[1] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (EUTRA); Physical Layer Procedures (Release 14), document TS36.213 V14.1.0, 3GPP, Dec. 2016.

[2] J. Pérez-Romero, O. Sallent, H. Ahmadi, and I. Macaluso, “On modeling channel selection in LTE-U as a repeated game,” in Proc. IEEE Wireless Commun. Network. Conf., Doha, Qatar, Apr. 2016, pp. 1–6.

[3] J. So and W. Sung, “Group-based multibit cooperative spectrum sensing for cognitive radio networks,” IEEE Trans. Veh. Technol., vol. 65, no. 12, pp. 10193–10198, Dec. 2016.

[4] A. Ali and W. Hamouda, “Advances on spectrum sensing for cognitive radio networks: Theory and applications,” IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 1277–1304, 2nd Quart., 2017.

[5] S. A. Alvi, M. S. Younis, M. Imran, F.-E. Amin, and M. Guizani, “A near-optimal LLR based cooperative spectrum sensing scheme for CRAHNs,” IEEE Trans. Wireless Commun., vol. 14, no. 7, pp. 3877–3887, Jul. 2015.

[6] H. Sadeghi and P. Azmi, “Performance analysis of linear cooperative cyclostationary spectrum sensing over Nakagami-m fading channels,” IEEE Trans. Veh. Technol., vol. 63, no. 9, pp. 4748–4756, Nov. 2014.

[7] M. Jin, Q. Guo, Y. Li, J. Xi, G. Wang, and D. Huang, “Blind cooperative parametric spectrum sensing with distributed sensors using local average power passing,” IEEE Trans. Veh. Technol., vol. 65, no. 12, pp. 9703–9714, Dec. 2016.

[8] E. Soltanmohammadi and M. Naraghi-Pour, “Fast detection of malicious behavior in cooperative spectrum sensing,” IEEE J. Sel. Areas Commun., vol. 32, no. 3, pp. 377–386, Mar. 2014.

[9] S.-Q. Liu and B.-J. Hu, “Analysis of sensing efficiency for cooperative spectrum sensing with malicious users in cognitive radio networks,” IEEE Commun. Lett., vol. 18, no. 9, pp. 1645–1648, Sep. 2014.

[10] M. J. Saber and S. M. S. Sadough, “Multiband cooperative spectrum sensing for cognitive radio in the presence of malicious users,” IEEE Commun. Lett., vol. 20, no. 2, pp. 404–407, Feb. 2016.

[11] Y. Li, “Blind SNR estimation of OFDM signals,” in Proc. Int. Conf. Microw. Millim. Wave Technol., Chengdu, China, May 2010,