Efficient Channel Allocation Using Cognitive Radio And Avoid Malicious Attacks

K.ABIRAMI[1], M.DHIVYA[2], K.DIVYA[3], S.T.SANTHANALAKSHMI[4]
[1] k.abirami96@gmail.com, [2]dhivyameyyappan@gmail.com, [3]divyaarumugam68@gmail.com,
[4]anandh.shantha@gmail.com
[1,2,3] STUDENT, FINAL YEAR, PANIMALAR ENGINEERING COLLEGE, DEPARTMENT OF CSE, CHENNAI-600123
[4] ASSISTANT PROFESSOR, PANIMALAR ENGINEERING COLLEGE, DEPARTMENT OF CSE, CHENNAI-600123

ABSTRACT: Concept of Cognitive Radio (CR) has been proposed to overcome this issue of spectrum scarcity by making use of opportunistic spectrum access. Along with CRs, new types of security threats is being evolved e.g. Primary User Emulation Attack (PUEA) and Spectrum Sensing Data Falsification (SSDF) attack. .. The results show that the proposed techniques fail when malicious secondary users exceeds the genuine secondary users, which is a possible threat scenario in CR networks. We propose a technique that is independent of the number of malicious SUs in the network. It uses primary user's Received Signal Strength (RSS) at an SU to localize its position and compare this with that calculated received signal strength of SU transmissions at data fusion center.

Keywords—Cognitive Radio; Opportunistic Spectrum Access;Spectrum Sensing; PUEA; SSDF; RSS.

I.INTRODUCTION

Currently, the frequency bands are statically allocated for various wireless services. However, with emergence of numerous wireless applications in recent years, it has become evident that the current system cannot cater to ever increasing demand of usable frequencies. CR is a promising concept to alleviate this scarcity of usable frequencies. Federal Communications Commission (FCC) defines CR as: "A system that senses its operational electromagnetic environment ,can dynamically and autonomously adjust its operating parameters to modify system operation, such as maximize throughput, reduces interference, ease interoperability and access secondary markets. Cognitive radio (CR) technology, proposed by Mitola, allows unlicensed (secondary) users to access the licensed (primary) frequency bands without interfering with the licensed users in order to realize more effective and reliable communication. Spectrum sensing, as a fundamental functionality of cognitive radio, enables the secondary users to monitor the frequency spectrum and detect vacant channels to use. Among the various sensing schemes for CR networks, cooperative spectrum sensing method stands out due to its high detection performance of spectrum holes. Meanwhile, the security issues of cognitive radio have received more and more attentions recently since the intrinsic properties of CR networks would pose new challenges to wireless communications.

Primary user emulation attack (PUEA), as a popular attack against spectrum sensing which is proposed by Chen and Park, identifies one potential vulnerability of spectrum sensing in CR networks where an attacker occupies the unused channels by emitting a signal with similar form as the primary user's so as to deter the access of the vacant channels from other secondary users . To date, several detection approaches of PUEA have been presented, however, the detection performance of white spaces in the presence of PUEA is not yet well understood. In this dissertation, we will investigate the detection performance of vacant channels in CR network in the presence of PUEA, attempting to mitigate the impact of PUEA on the detection performance of white spaces in CR networks.

II. RELATED WORK

To counter SSDF attacks, cooperative sensing techniques perform anomaly detection depending on sensing reports and on that basis try to distinguish malicious SUs from genuine SUs. These malicious SU reports are excluded from decision making process, ensuring correctness of the final decision. Weighted Sequential Probability Ratio Test [4] is a reputation metric based scheme, wherein weights are applied to each sensing report of SU based on its previous reporting history. Weights are increased when the individual report of SU matches with final fusion decision and it is decreased if report doesn't match final decision. In this manner contribution of malicious SUs in final decision is reduced. In [5] authors proposed a scheme to detect outliers among the sensing reports by various SUs and filtering these reports before making final decision. Trust value of each SU is calculated based on how close is its report to the mean value of all reports calculated at DFC. A mechanism in which consensus is arrived at in distributed way is proposed in [6]. Every SU iteratively selects neighbours for sharing sensing reports. For selecting a neighbour for cooperation, received reports are compared against local mean value and the reports which deviate maximum from the mean value are discarded and thus doesn't contribute in final result. The results in [4][5][6] show that the proposed techniques fail when malicious SUs outnumber the genuine SUs which is a possible threat scenario in CR. We propose a technique that is independent of the number of malicious SUs in the network. Our proposed technique anticipates that in CR, the sensing targeted attacks can be executed by an assailant with ease. Hence, it is evident that, simple yet efficient techniques to counter the SSDF attack are a genuine need for the robust functioning of CRs.

III.PROPOSED SYSTEM

In this paper, we propose a novel mechanism which makes use of the SU location information to establish its reliability. This technique establishes the reliability of the individual SU and hence, works well in scenarios where number of malicious SUs outnumbers the genuine SUs. This scheme works even when there are only single/few SUs. the proposed work with respect to RSS based ranging, network model and attack model. We consider a centralized cooperative spectrum sensing scenario in this paper. Herein, a SU uses energy detection technique for spectrum sensing to detect PU signals. Sensed received signal strength reports are sent by SUs to DFCs . Further, based on received signal strength of SU transmissions, DFCs calculate the reliability of each report and make final decision about whether to include a secondary user's report in final decision or not.

***COOPERATIVE SPECTRUM SENSING*:**

Since it is usually impossible for secondary users to detect the location of primary receiver, the interference cannot be avoided. Moreover, an CR transmitter may not be able to detect the primary transmitter due to the channel fading or shadowing. Consequently, the sensing information from other users is required for more accurate detection and cooperative spectrum sensing arises.

A. *MODULE DESCRIPTION:*

Module 1: Co-operative Spectrum Sensing in the presence of PUEA

This module is implemented mainly to identify the spectrum holes. The spectrum holes are identified using the Cognitive radio algorithm. The secondary users are to be allocated vacant channels found in the frequency spectrum even in the presence of PUEA attack .i.e., the SU's receive signals from both PU's and attackers.Then the signals are sent to the Data Fusion Center(DFC).The DFC's then identifies the PU since it has the details of all SU and PU.Once when the PU's are detected then the algorithm senses the wholes in the frequency spectrum in a dynamic manner. Thus the channles are allocated in a co-operative manner to make use of the available frequency spectrum.

Module 2: Optimal Combining Scheme for Cooperative Spectrum Sensing in the Presence of PUEA

The vital role played by this module is to find the direction from which usually a propagating waves arrives at in conjunction with RSS(Received Signal Strength).The algorithms used to implement this module is angle of arrival and RSS.The genuine SU's are to allocated channels in an optimal manner i.e.,the channel allocation should be done as soon as possible and at a the same time the routing path should be done in an optimal way by using an optimal routing algorithm. During the spectrum sensing of CRN,false alarm probability *Pf* and detection probability *Pd* over a detection interval are defined as

$$P_f = P_r(Y \geq T|\mathcal{H}_0)$$

$$P_d = P_r(Y \geq T|\mathcal{H}_1)$$

T- Detection Threshold

P_f - false alarm probability

P_d - detection probability

The below given derivation obtains,the optimal weights Wopt so that the detection probability Pd is maximized under the constraint of a false alarm

$$\mathbf{w_{opt}} = arg\max_{\mathbf{w}}\{P_d|P_f = \zeta\}$$

Module 3: Co-operative Spectrum Sensing Data Falsification Attack

This module is implemented using singular value decomposition algorithm. It consists of two steps :

1.Techniques

2. Attack Detection

Step I: Secondary User Senses Primary User Signals
Ri = [PSP,i1, PSP,i2, …., PSP,in]---(1)
Step II: Secondary User Transmits RSS Vector
Di = [dSP,i1, dSP,i2, ..., dSP,in]---------(2)
(dSP,ij)2 = (xj – x0)2 + (yj – y0)2------(3)
Step III: DFCs Calculate Declared SU Position
Step IV: DFCs Calculate Actual SU Position
Step V: DFCs Compare Pdec and Pact
Step VI: Attack Detection
PSP`= PSP +δ------------------(4)
Ri ' = [PSP,i1' , PSP,i2' , …., PSP, in']---(5)

$$DFC\ Decision = \begin{cases} 0 & SU\ is\ genuine\ if\ P_{dec} = P_{act} \\ 1 & SU\ is\ malicious\ if\ P_{dec} \neq P_{act} \end{cases}$$

IV.EXPERIMENTAL RESULT ANALYSIS

In this section, we will implement the simulations of the cooperative sensing scheme with the existence of PUEA. The channels are assumed to be identically and independently distributed block Rayleigh fading. In our simulation, the number of samples during a detection interval is $M = 3$. Notice that when we consider complex signal for $yi(k)$, the samples is equivalent to $M = 6$ .In simulation, all channel information are assumed to be known to the secondary users. The average SNR is set as 0 dB and the emitting power of the primary user and the attacker is set as same, i.e., Pp = Pm = 1

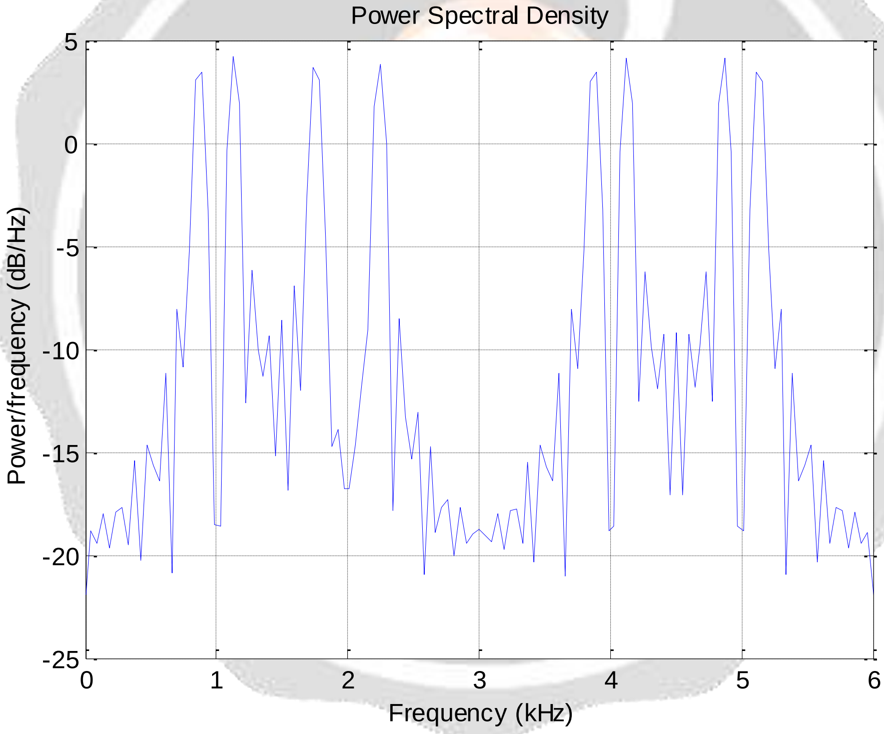

Figure 1 Spectrum Sensing Of Number Secondary User Su=4

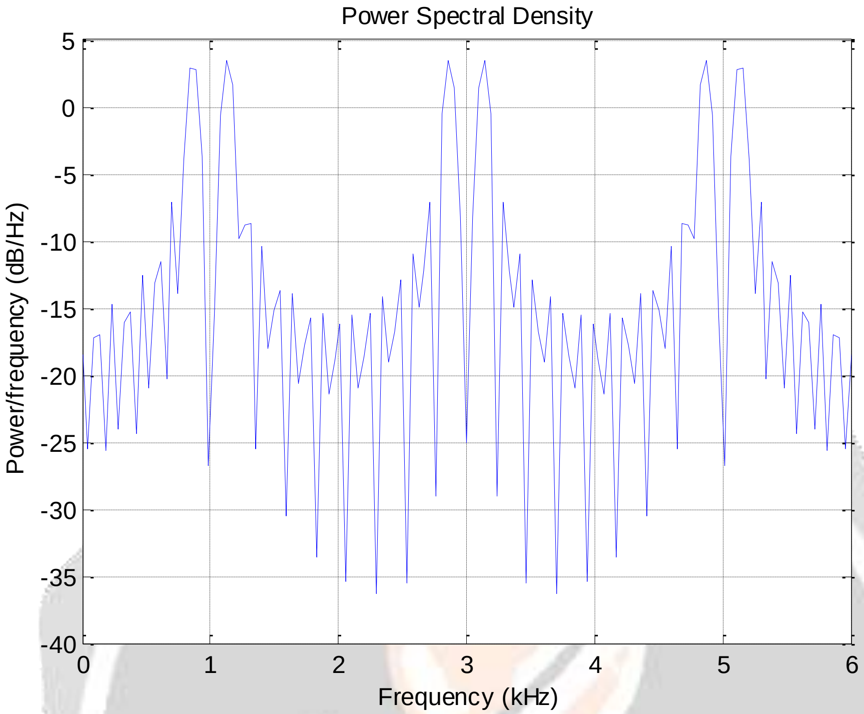

Figure 2 Spectrum Sensing Of Number Secondary User Su=3

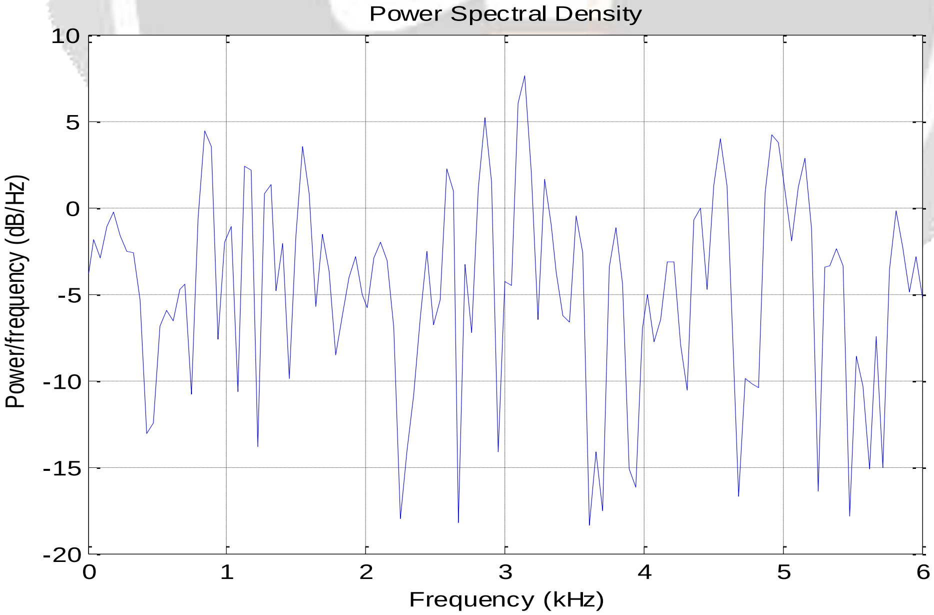

Figure 3 Noise when primary user absent

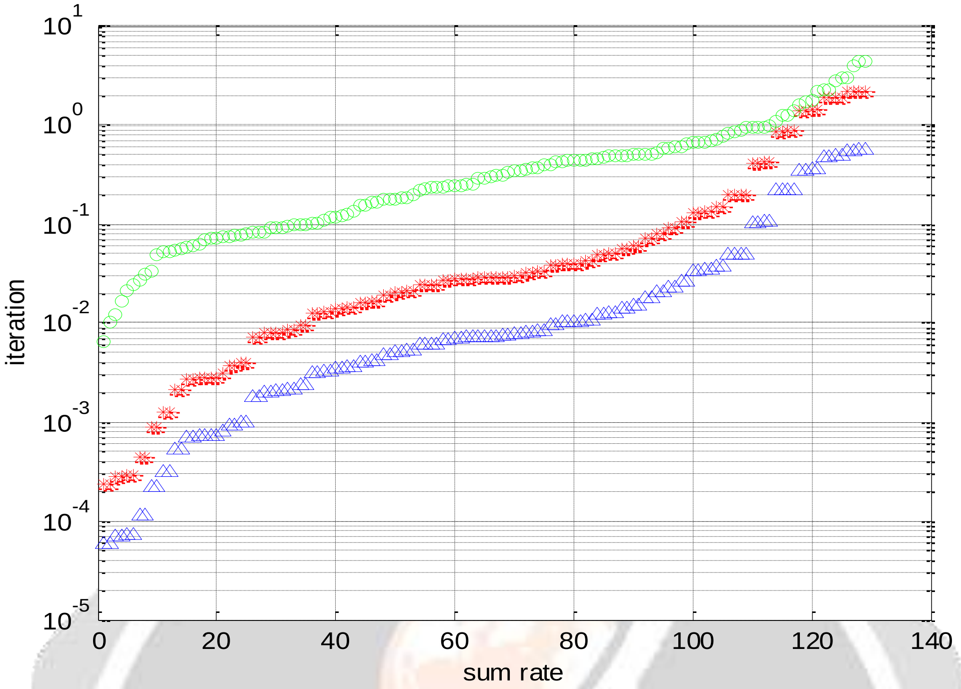

Figure 4 Cooperative spectrum sensing

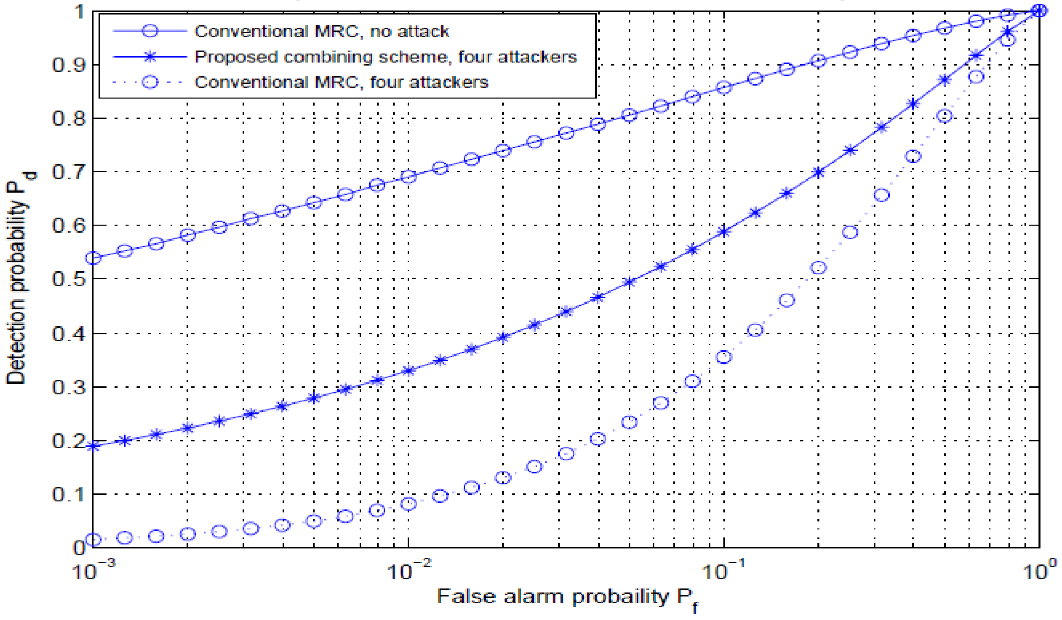

Figure 5 Cooperative spectrum sensing PUEA

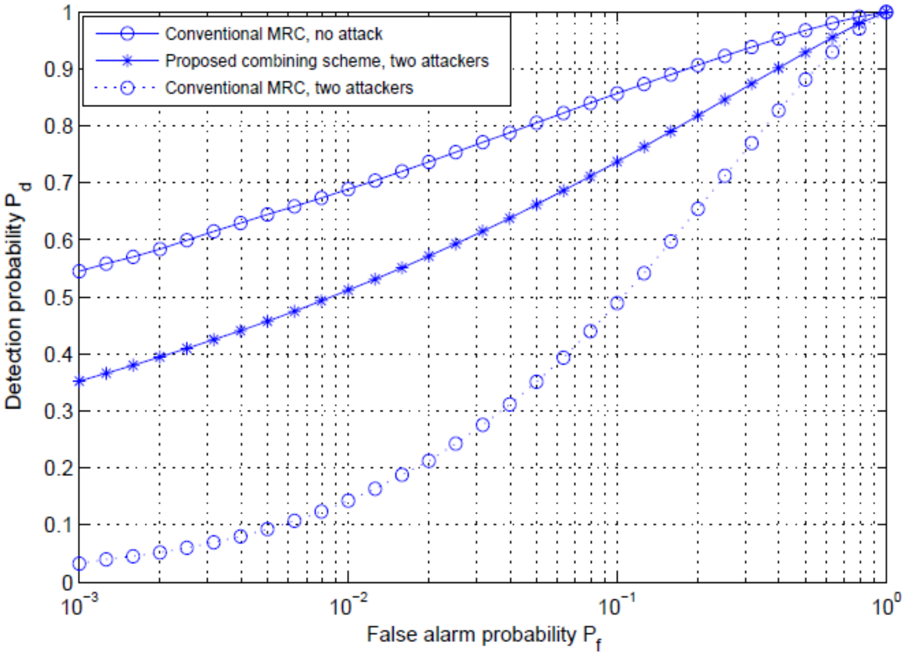

Figure 6 Spectrum Sensing Falsification Attacks

V.CONCLUSION

In this paper we introduce a simple yet efficient technique to counter the SSDF attack. Though a number of techniques have been proposed to counter SSDF attack they fail when malicious SUs outnumber the genuine SUs. Our proposed technique is independent of the number of malicious SUs in the network. It uses primary user's received signal strength at an SU to localize its position and compare this with that calculated using RSS of SU transmissions at DFCs. Experimental results gives performance spectrum sensing cognitive radio while present secondary user.

REFERENCES

[1]. Federal Communications Commission, “Notice of proposed rulemaking and order: Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies,” ET Docket No. 03-108, Feb. 2005.

[2]. N. Patwari, A. Hero III, and M. Perkins, “Relative location estimation in wireless sensor networks,” IEEE Trans. Signal Process, vol.51, no. 8, pp. 2137–2148, August 2003.

[3]. Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis,“A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks” IEEE Communications Surveys & Tutorials, 2012.

[4]. R. Chen, J.-M. Park, K. Bian, “Robust distributed spectrum sensing in cognitive radio networks”, in: Proc. of IEEE INFOCOM 2008, 2008, pp. 1876–1884.

[5]. P. Kaligineedi, M. Khabbazian, V. Bhargava, “Secure cooperative sensing techniques for cognitive radio systems”, in: IEEE International Conference on Communications, ICC, 2008, pp. 3406–3410.

[6]. F. Yu, H. Tang, M. Huang, Z. Li, P. Mason, “Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios, in: Proc. of IEEE MILCOM 2009, 2009, pp. 1–7.