ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 3, March 2018

Efficient Channel Allocation Using Cognitive Radio and Avoiding Malicious Attacks

[1] Tanusshri Sivakumar, [2] Swathi Rajeev, [3] Mrs. Caroline Jebakumari S
[1][2] B.E Electronics & Communication, Easwari Engineering College
[3] Assistant Professor, ECE department, Easwari Engineering College

Abstract: **In cognitive radio networks (CRNs), Cooperative spectrum sensing (CSS) is generally adopted for improving spectrum sensing accuracy to increase spectrum utilization and avoid interference with primary users. Along with CRs, new types of security threats have evolved, for instance; Primary User Emulation Attack (PUEA) and Spectrum Sensing Data Falsification (SSDF) attack. The results show that the already proposed techniques fail when malicious secondary users outnumber the genuine secondary users, which is a possible threat scenario in Cognitive Radio(CR) networks. The proposed technique is independent of the number of malicious SUs in the network. A simple yet efficient technique to counter the SSDF attack has been proposed. It makes use of primary user's received signal strength of a SU to localize its position and compare this with that of the calculated value using RSS of SU transmissions from DFCs. Simulation results are provided to show that the proposed system works better than its predecessors.**

Keywords— Cognitive radio network, PUEA, SSDF, Data Fusion Centres (DFCs), Cooperative Spectrum Sensing

INTRODUCTION

To enhance the spectrum utilization and meet the demands of the various communication services, cognitive radio has emerged as an intelligent technology in the future wireless communication systems. In the cognitive radio networks (CRNs), vacant licensed spectrum of primary users (PUs) can be employed by the secondary users (SUs) through the concept of spectrum sensing (SS). Relative to individual spectrum sensing, cooperative spectrum sensing (CSS) can improve the accuracy of spectrum sensing in addition to the already existent methods. Along with CRs, new types of security threats have evolved, for instance; Primary User Emulation Attack (PUEA) and Spectrum Sensing Data Falsification (SSDF) attack. In Cognitive Radio Networks, the primary goal of the secondary users is to detect the presence of primary users. The situation becomes cumbersome in the case of presence of malicious users especially primary user emulator. In an SSDF attack, some malicious users intentionally report incorrect local sensing results to the fusion center (FC) and disrupt the global decision-making process. The results show that the already proposed techniques fail when malicious secondary users outnumber the genuine secondary users, which is a possible threat scenario in CR networks. The proposed technique is independent of the number of malicious SUs in the network.

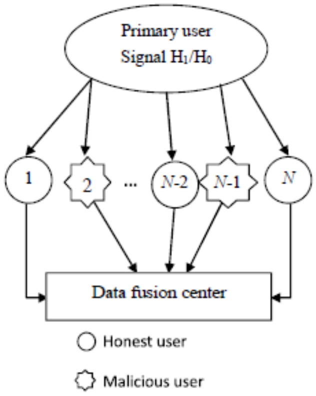

Fig 1. CR networks system model in the presence of SSDF attack

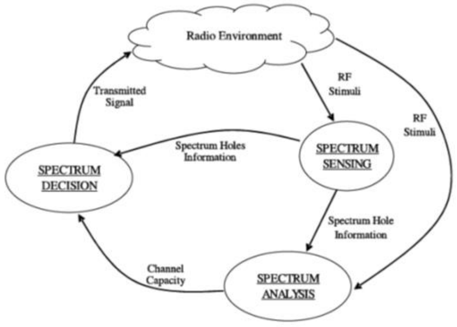

Fig 2. Cognitive Cycle

Some of the major disadvantages of systems already in existence include the use of software defined radio, increased arrival time and presence of hard handover. The proposed system eliminates these disadvantages by increased security, reliability, accuracy localization and reduced false alarm rate. Instead of using non-cooperative spectrum sensing that would lead to many complex situations, cooperative spectrum sensing is employed. The use of cognitive radio cooperative spectrum sensing provides many advantages, but to provide this ability there are a number of requirements that need to be provided. While these may be seen as an overhead and in some instances a disadvantage, the advantages often outweigh the disadvantages.

- ***Control channel:*** In order for the different elements within the cognitive radio cooperative spectrum sensing network to communicate, a control channel is required. This will take up a proportion of the overall system bandwidth.
- ***System synchronisation:*** It is normally necessary to provide synchronisation between all the nodes within the cognitive radio cooperative spectrum sensing network. This is to keep the channel free from transmissions from the cognitive network while sensing is under way. In some instances, adaptive scheduling of the sense period may prove beneficial. In this way the dead time arising from sense periods can be minimised within the need to ensuring the sensing is undertaken sufficiently well. Accurate spectrum sensing requires a longer period of time than a rough sense to see if a strong signal has returned. By adapting the sense periods, channel throughput can be maximised, although there is a greater need to maintain synchronisation under these circumstances.
- ***Suitable geographical spread of cooperating nodes:*** In order to gain the optimum sensing from the cooperating nodes within the cognitive network, it is necessary to obtain the best geographical spread. In this way the hidden node syndrome can be minimised, and the most accurate spectrum sensing can be gained.

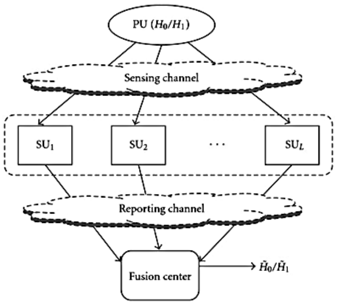

Fig 3. Cooperative detection model

The rest of this paper is organized as follows: proposed system model is discussed in Section II. Section III evaluates the three modules which are part of the spectrum analyses. Numerical results and simulation observations are then demonstrated in Section IV, and the paper is concluded in Section V.

II. PROPOSED TECHNIQUE

This is 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. It provides the Localization of Mobile users. The system also entails a Tracking Prediction facility of Mobile user.
There are basically 3 modules included,
1.Cooperative spectrum sensing in the presence of PUEA
2.Optimal Combining Scheme for Cooperative Spectrum Sensing in the Presence of PUEA
3.Cooperative Spectrum Sensing Data Falsification Attack
These modules will be explained in detail in the following section.

III. PROJECT MODULES

1. Cooperative spectrum sensing in the presence of PUEA

Cognitive radio cooperative spectrum sensing occurs when a group or network of cognitive radios share the sense information they gain. This provides a better picture of the spectrum usage over the area where the cognitive radios are located.

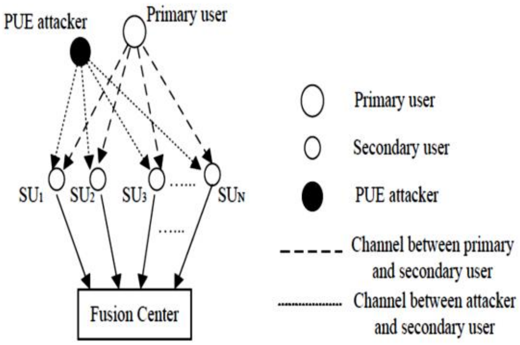

Fig 4. Cooperative spectrum sensing in the presence of PUEA

$$y_i(k) = \alpha\sqrt{P_p}h_{pi}(k)x_p(k) + \beta\sqrt{P_m}h_{mi}(k)x_m(k) + n_i(k), \quad i = 1,2,\dots,N$$

Where,
$x_p(k)$ - primary user transmitted signal

$x_m(k)$- attacker Transmitted signal

$h_{pi}(k)$ – channel response b/w primary user and secondary user

$h_{mi}(k)$-channel response b/w attacker and secondary user

Y(k)-received signal
Alpha -primary user coefficient
Beta -attacker coefficient
The above equation gives the received signal which is a combination of primary user signal, attacker signal and some amount of noise.

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

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

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

Where,
T - detection threshold
P_f- false alarm probability
P_d- detection probability
Ho- noise
H1-original received signal + noise
When the probability of false alarm turns true ,indicates that channel is unoccupied.
When the probability of detection turns true ,indicates that channel is occupied.

3.Cooperative Spectrum Sensing Data Falsification Attack

A. Algorithm
B. Attack Detection

A. Algorithm of SSDFA

The steps are given as follows:
Step I: Secondary User Senses Primary User signal
Step II : Secondary User Transmits RSS Vector
Step II: DFCs Calculate Declared SU Position
Step IV: DFCs Calculate Actual SU Position
Step V : DFCs Compare Pdec and Pact

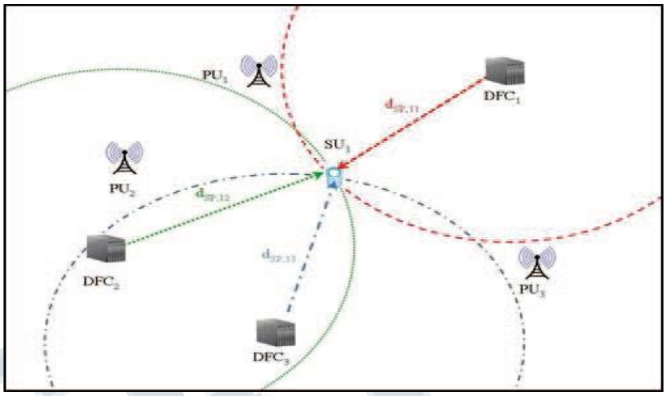

Fig 5. Calculation of Actual SU Position using DFCs

B. Attack Detection

There are 3 cases involved in detection of attack and they are:-
Case I - Increase in actual received signal strength
Case II -Decrease in actual received signal strength
Case III - Intelligent Attack
Case I/II : Increase/Decrease in actual received signal strength

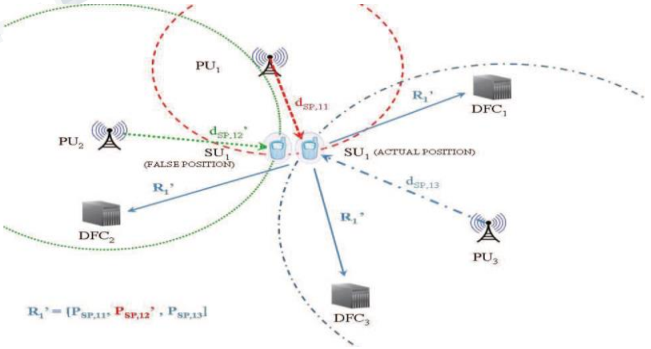

Fig 6. Increase/Decrease in actual received signal strength

Case III: Intelligent Attack

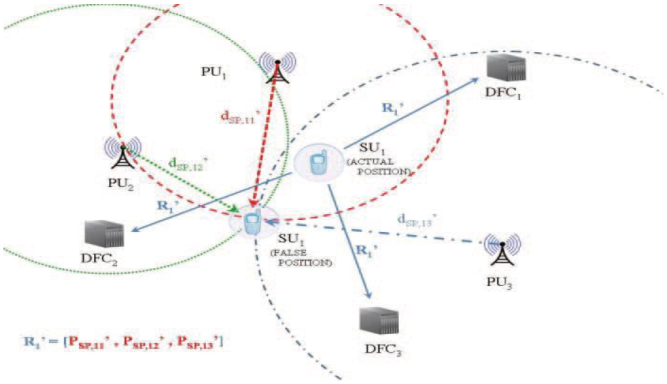

Fig 7. Intelligent Attack

IV. SIMULATION OBSERVATIONS

In this section, all observations are recorded from which various parameters are calculated. Fig 8 and Fig 9 shows the power spectral density using the concept of spectrum sensing when secondary users are 3 or 4 in number. The resulting signal when the primary user is absent is showcased in Fig 10.

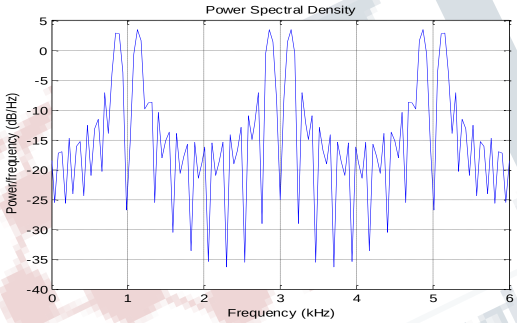

Fig 8. Spectrum sensing of 3 secondary users

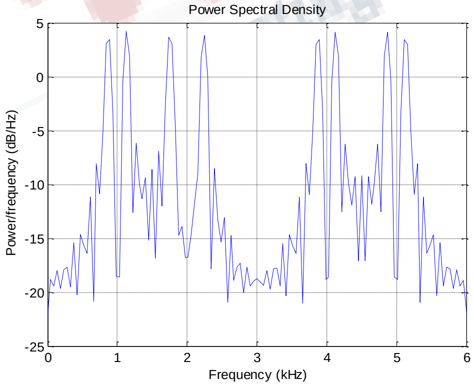

Fig 9. Spectrum sensing of 4 secondary users

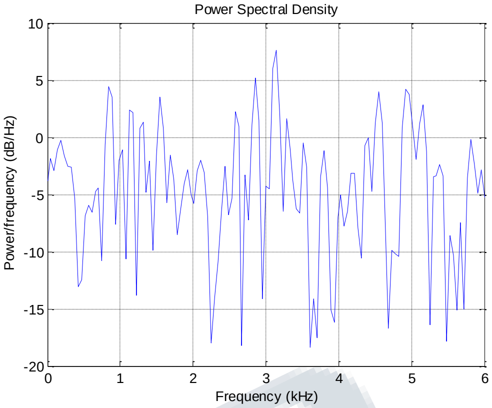

Fig 10. Output signal if the primary user is absent

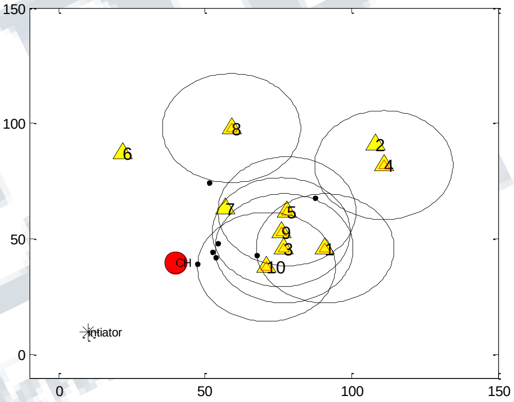

Fig 11. Frequency allocation of secondary user by primary user

V. CONCLUSION

A simple yet efficient technique to counter the SSDF attack has been proposed in this paper. It makes use of primary user's received signal strength (RSS) of a Secondary User (SU) to localize its position and compare this with that of the calculated value using RSS of SU transmissions from DFCs. The analysis and simulation results establish 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.

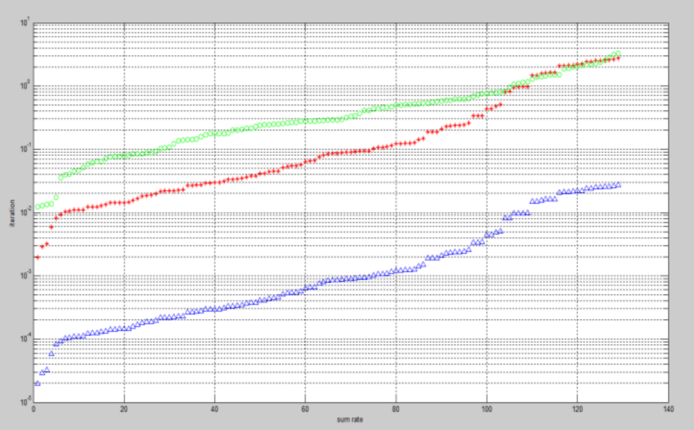

Fig 12. Comparison of conventional radio, software defined radio and cognitive radio

Figure 12 illustrates the comparison between convention radio, Software defined radio and cognitive radio. The graph clearly shows that the green linear line that represents the cognitive radio technology has a much bigger impact than its counterparts.

REFERENCES

[1]. J. Mitola, III, G. Q. "Maguire, Cognitive radio: making software radiosmore personal," IEEE Personal Communication, vol. 6, no. 4, pp. 13-18,1999.

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

[3] A. Goldsmith, S. A. Jafar, I. Maric, S. Srinivasa, "Breaking spectrumgridlock with cognitive radios: an information theoretic perspective,"
IEEE Signal Processing Magazine, vol. 24, no. 3, pp. 79-89, 2007.

[4] T. Yucek, H. Arslan, "A survey of spectrum sensing algorithms forcognitive radio applications," IEEE Communications Surveys & Tutorials,
vol. 11, no. 1, pp. 116-130, 2009.

[5] Y. Zeng, Y.-C. Liang, A.T. Hoang, R. Zhang, "A review on spectrumsensing for cognitive radio: challenges and solutions," EURASIP Journalon Advances in Signal Processing, vol. 2010, no. 1, pp. 1-15, 2010.

[6] A.S. Cacciapuoti, I.F. Akyildiz, L. Paura, "Correlation-aware userselection for cooperative spectrum sensing in cognitive radio Ad Hoc
networks," IEEE Journal on Selected Areas in Communications, vol. 30,no. 2, pp. 297-306, 2012.

[7] W. Yue, B. Zheng, Q. Meng, J. Cui, P. Xie, "Robust cooperative spectrumsensing schemes for fading channels in cognitive radio networks,"
Science China Information Sciences, vol. 54, no. 2, pp. 348-359, 2011.

[8] W. Xia, W. Yuan, W. Chen, W. Liu, S. Wang, J. Xu, "Optimization ofcooperative spectrum sensing in Ad-Hoc cognitive radio networks," in
Proc. GLOBECOM, 2010, pp. 1-5.

[9] X. Kang, Y.-C. Liang, H.K. Garg, L. Zhang, "Sensing-based spectrumsharing in cognitive radio networks," IEEE Transactions on Vehicular
Technology, vol. 58, no. 8, pp. 4649-4654, 2009.

[10] X. Zhou, G. Y. Li, D. Li, D. Wang, A.C.K. Soong, "Probabilistic resourceallocation for opportunistic spectrum access," IEEE Transactions onWireless Communications, vol. 9, no. 9, p. 2870-2879, 2010.