Indian Journal of Science and Technology, Vol 8(32), DOI: 10.17485/ijst/2015/v8i32/88884, November 2015 ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Higher Order Statics based Primary user Emulation Attack Detection

S. Arulselvi*

Department of ECE, BharathUniversity, Chennai - 600073. Tamil Nadu, India

Abstract

Cognitive radio is one of the promising technique for dynamic spectrum sharing to solve the spectrum scarcity problem. Spectrum sensing is the key process in cognitive radio for the dynamic spectrum usage. But security in sensing is still in research issues .there are many security threads in cognitive radio but the primary user emulation attack is the predominant one which will not allow the dynamic spectrum sharing in effect. This primary emulation attack is the major drawbacks in energy detector based spectrumsensing. There are various methods to detect the emulation attack like RSSI based, location based etc. But the accuracy of detection is not good because of the uncertainty in the received power due to the random behavior of the channel condition. Most of those methods assume that primary users are stationary and channel variations are not significant. But in real time this assumption is not valid one. Here in this paper we propose higher order statics based primary user attack detection is proposed which can model the features of the primary user and primary user emulator attackers very well and we are able to detect the primary user emulation attack accurately. Here various fading channel scenarios like Rayleigh, rician and nagagammi is considered between the primary user and the attackers on that the performance of the detection of primary user emulation is analyzed.

Keywords:

1. Introduction

Recent studies[2,3] reports provesthat the wireless spectrum suffers from over utilization in some bands and underutilization in others. This happens because of the fixedspectrum assignment policies. To overcome this, the new spectrum allocation policy called dynamic spectrum sharing is going to be used. This new policy would allow unused licensed spectrum bands called as white spaces to be used by unlicensed user called as Secondary Users (SUs). The success of this policy depends on the accuracy of the spectrum sensing that is used by the SUs to detect the spectrum hole. The Cognitive Radio technology acts as the enabling technology for this dynamic spectrum sharing. Cognitive Radio (CR) enabled Dynamic Spectrum Access (DSA) networks are designed to detect and opportunistically utilize the unused or under-utilized spectrum bands. But due to the open paradigm of CR networks and lack of proactivesecurity protocols, the DSA networks are vulnerable to various threats[13].

There are several attacks targeting the physical or Medium Access (MAC) layers in Cognitive Radio network.Common Control Channel (CCC) attacks ithe Medium Access layer attack targeting CCC through MAC spoofing, congestion attacks, jamming attacks. Beacon Falsification (BF) attack is another Medium Access attack that disrupt the synchronization between IEEE 802.22 WRANs.

The physical layer attacks are given more attendance in recent days. Such a physical layer attacks targeting the physical layerare RF jammingthat can severely disruptNetwork's operation. Another physical layer attack that present in collaborative spectrum sensing iscalled Spectrum Sensing Data Falsification (SSDF) attack where a malicious CR can provide false observations on purpose[14].

Primary User Emulation (PUE) attacks is another main physical layer attack, where attackers mimic the signals of Primary Users (PUs), can cause significant performance degradation in Cognitive Radio (CR) systems. Detection

* *Author for correspondence*

of the presence of PUE attackers is thus an important problem[1].There are many PUE attack detection mechanism in literature in[4]the authors proposeda location based authentication scheme for the TV white spaces spectrum in which the location based RSSI database is formulated and the real time measured RSSI values are compared with this data base to detect the primary user emulation attack. An analytical model for the probability ofsuccessful PUEA based on the energy detection is presented in[5] in which the received signal power is modeled as a log-normally distributed random variable.Cooperative spectrum sensing based on energy detector is proposed as a efficient method for the Primary User emulation attack. In[6] in which a cooperative Secondary User model was proposed for PrimaryUser detection in the presence of PUEA.

Traditional cryptography system can also be used to detect the PUEA. A public key cryptography mechanism is proposed in[7] between Primary Users and Secondary Users. This enables the identification of Primary User by using a public key.

For any sensing algorithm with consideration of with a variable transmission power is proposed in[9]. But in this the position of the attacker has to be known in advance and the distances betweenthe PUs, the SUs and the attacker have to be known in advance.

Energy detection based PUEA detection methods is the most widely method used because of its simplicity and low computational overhead[10–13]. But it does not performwell in low SNR environments.

Our method proposed in this paper is based on second order and fourth order moments and their cumulants is less complex and accurate method that can be used fading environment where the fluctuations of received signal strength is rapid and the traditional RSSI based method can't give the better detection of the PUEA[15].

2. System Model

Primary User emulation attack scenario can be modeled by taking a primary network region and the secondary network region as shown in the Figure1. From the figure it is clear the Secondary User who is trying to detect the spectrum hole of Primary User spectrum is out of the primary network region In absence of the PUEA it has to detect the spectrum hole,but due to the one of the Secondary User involve in PUEA it will not detect the hole .the scenario shown in the Figure 1 is used to simulate the PUEA and detection process.

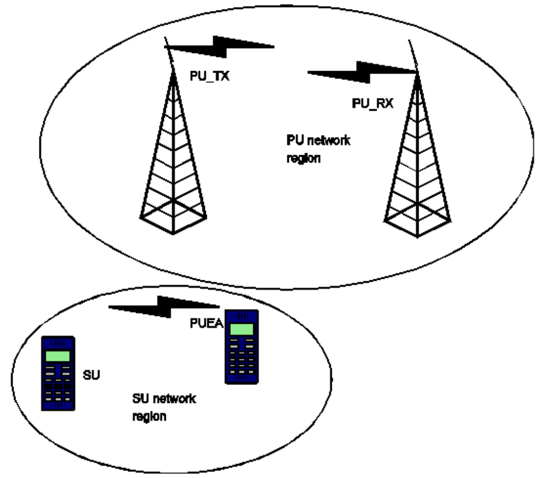

Figure 1. System model of Primary user Emulation Attack.

The PUEA detection process at the Secondary User terminal is presented in the Figure 2. Each secondary receiver which tries to sense the spectrum hole will receive the signal and computes the higher order statics. This computed static values are compared with the template data base if that matches then secondary will ensure the received signal is from the valid primary user else it will assume that the received signal is from the attacker[16].

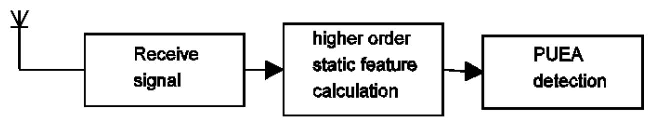

Figure 2. Block diagram of higher order static based PUEA detection.

The received signal by the secondary user will be:

$$y_s(n) = h(n) * x(n) + n(n) \tag{1}$$

Where the x (n) is the primary transmitted signal;h(n) is the channel coefficient between primary transmitter and secondary receiver; $y_s(n)$ is a complex valued stationary random process because of the additive noise.

The second order moments for the above random process are:

$$M_{20} = E[y^2(n)] \tag{2}$$

$$M_{21} = E[|y(n)|^2] \tag{3}$$

If we compute the moments from the samples collected at the secondary receiver, the second order moments can be defined as below[8].

$$M_{20} = \frac{1}{N}\sum_{n=1}^{N} y^2(n) \quad (4)$$

$$M_{21} = \frac{1}{N}\sum_{n=1}^{N} | y(n) |^2 \quad (5)$$

The fourth order moments and the cumulants for the received signal at the Secondary User with sample values is:

$$M_{40} = \frac{1}{N}\sum_{n=1}^{N} y^4(n) - 3M_{20}{}^2 \quad (6)$$

$$M_{41} = \frac{1}{N}\sum_{n=1}^{N} y^3(n) y^*(n) - 3M_{20}M_{21} \quad (7)$$

$$M_{42} = \frac{1}{N}\sum_{n=1}^{N} [| y(n) |^4 - |[M_{20} |]^2 - 2M_{21}{}^2] \quad (8)$$

The above higher order statics are calculated for the Primary User signal on the various scenarios and tabulated as data base for the comparison purpose.

3. Result and Discussion

The system model as shown in the Figure 1 is taken for the simulation with one primary transmitter and one primary receiver. The primary signal is generated with QAM modulation with the random input bits. The simulation consists of two phases;the first phase will be training phase where the Secondary User will create the data base of the cumulants values of the Primary User. On the second phase the secondary receiver is used to calculate the cumulants value of the received signal and compares the calculated cumulant with the database values. To test the system functionality, the one PUEA node is introduced as shown in Figure 1 and for the attack signal the cumulants values are compared with the data base value and the mismatch is used to detect the PUEA[17].

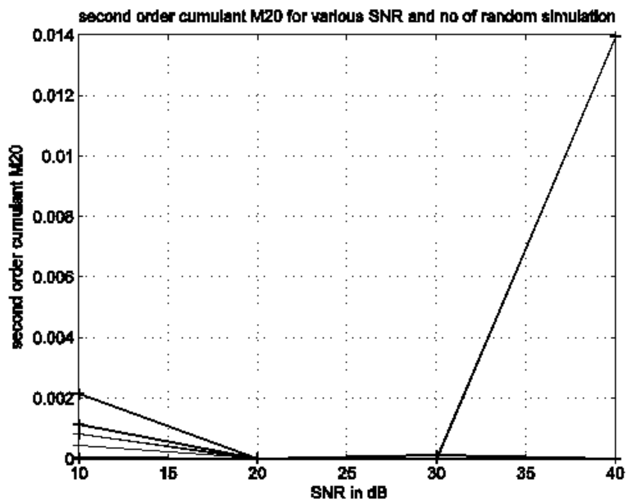

Figure 3. Variation of second order cumulant M20 for various SNR and repeated random channels.

In order to check the variation of the cumulant values due to variation of the fading channel coefficient,a no. of random realization of fading channels are done and the values are plotted. Figure 3 shows the M20 value variation for a no. of different Rayleigh fading realization with different SNR values. Figure 3 shows that there is only little negligible level of variation on the M20 value so it can be used as parameter to detect PUEA detection with

Table 1. Cumulant values for various SNR for the Rayleigh channel fading

Primary User cumulant values for 10 unit distant between primary and secondary					
SNR (dB)	M_{20}	M_{21}	M_{40}	M_{41}	M_{42}
10	9.05800055122081	9.06819043845575	7923520.50501201	23271249.2064019	10916518.0244008
20	0.00647585382085053	0.00768854624774843	1.83034153567300	1.90513928439763	1.94425271250936
30	0.00860979814604354	0.0147377155431392	7.00838353398962	5.23478669721672	7.01649416325310
40	9.02263550745943e-05	0.000134384977993286	1.77852189403686e-05	1.78115728303474e-05	1.79694418334763e-05
PUEA cumulant values for 4 unit distant between PUEA unit and Secondary User					
10	0	0	0	0	0
20	0	0	0	0	0
30	0	0	0	0	0
40	0.000777222485577366	0.000777222485577366	1.17995223950962e-08	1.82402389865617e-06	1.82402389865617e-06

some threshold value. The computed cumulants values for different SNR values for the Rayleigh fading channel is tabulated in Table 1.

For low SNR case from 10Db to 30 Db PUEA can be easily detected by zero value of all the cumulant whereas for Primary User it is some non-zero value for 40db SNR. The PUEA can be detected by comparing the Primary User tabulated value and the computed value.

If m20_cal*10 < m20_tab and m21_cal*10<m21_tab.

We can conclude that the PUEA is present. Here we divide the value by 10 to compensate the small variation in the cumulant value due to fading channel.

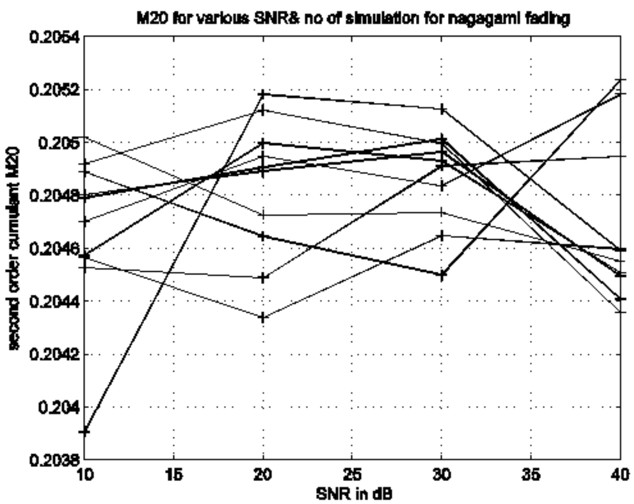

Figure 4. Variation of second order cumulant M20 for various SNR and repeated random channels of Nagagami.

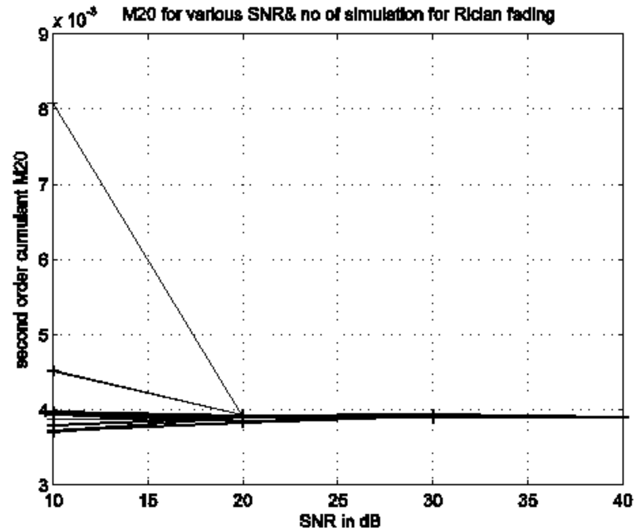

Figure 5. Variation of second order cumulant M20 for various SNR and repeated random channels of Rician.

Similarly the variation in cumulant value due to Rician and Nagagami fading channels are captured by random. No. of channel realization and plotted are in Figure 5 and Figure 6.Again this plot shows the cumulant value vary with little bit amount. From Table2,we can detect the PUEA unit in Nagagami channel by comparing the table value of the primary unit. For upto 30db we can see for the PUEA the cumulant values are zero but for the Primary User it is non zero. For 40 db and above the cumulant value of primary is high so we can detect the PUEA.

If m40_cal*10 < m40_tab and m41_cal*10<m41_tab and m42_cal*10<m42_tab

Table 2. Cumulant values for various SNR forNagagami channel

Primary User cumulant values for 10 unit distant between primary and secondary					
SNR (dB)	M_{20}	M_{21}	M_{40}	M_{41}	M_{42}
10	0.204668621649133	0.204678616437697	0.0831193304713818	0.0425548012838168	0.0425568454749695
20	0.204823779068742	0.204824789066937	0.0832476235851434	0.0426115370779045	0.0426117439706750
30	0.204865570340756	0.204865670287870	0.0832816301697525	0.0426282334448204	0.0426282539339674
40	0.204686911509702	0.204686921530717	0.0831388467433977	0.0425516276594248	0.0425516297100674
PUEA cumulant values for 4 unit distant between PUEA unit and secondary user					
10	0	0	0	0	0
20	0	0	0	0	0
30	0	0	0	0	0
40	0.0312646102056927	0.0312646102056927	-0.00193998596535421	0.000992441588557946	0.000992441588557948

Table 3. Cumulant values for various SNR for Rician channel

Primary user cumulant values for 4 unit distant between primary and secondary					
SNR (dB)	M_{20}	M_{21}	M_{40}	M_{41}	M_{42}
10	8.53376890105158e-05	0.000218741353098133	2.00701113709494e-05	1.84936342967248e-05	2.29225651592912e-05
20	0.000105506682335319	0.000116895141517537	3.63132249847814e-06	3.62417708891230e-06	3.64668844880943e-06
30	9.98095987112898e-05	0.000101515365927155	2.50595160432354e-08	1.77357782248088e-08	2.08679515544991e-08
40	0.000100023403619584	0.000100148983532966	2.00004178123070e-08	1.00249402621626e-08	1.00697990245198e-08
PUEA cumulant values for 2 unit distant between PUEA unit and Secondary User					
10	0	0	0	0	0
20	0	0	0	0	0
30	0	0	0	0	0
40	1.00047559446962	1.00329102972669	2.00133652530219	1.01002655199671	1.01344858105953

Similarly the Rician channel case PUEA can be detected if:

If m40_cal/10 > m40_tab and m41_cal/10>m41_tab and m42_cal/10>m42_tab and m20_cal/10>m20_tab and m21_cal/10>m21_tab

4. Conclusion

Primary User emulation attack detection is one of the important security issues in spectrum sensing of Cognitive Radio which will block the dynamic spectrum sharing. Even though there are many methods to detect the PUEA in CR network using the received signal strength indication based which is very simple low complexity one but they suppers due to the variation of RSSI values especially in the fading environment. So in this paper we have proposed higher order statics based PUEA detection scheme which is simple as RSSI based but more accurate than RSSI based since the cumulant values not varying much due the fading effect. From the simulation result we can conclude that the PUEA detection can be done with the help of calculated cumulant and primary used cumulant data base.

5. References

1. Nguyen NT, Zheng R,Han Z. On identifying Primary User Emulation Attacks in Cognitive Radio systems using non-parametric Bayesian classification. IEEE Transactions on Signal Processing. 2012 Mar; 60(3):1432–45.
2. Lydia Caroline M, Vasudevan S. Growth and characterization of pure and doped Bis thiourea zinc acetate: Semi-organic nonlinear optical single crystals. Current Applied Physics. 2009 Sep; 9(5):1054–61. ISSN : 1567-1739.
3. F.C.C.: Spectrum policy task force. Rep. ET Docket no. 02-135; 2002 Nov.
4. Lydia Caroline M, Kandasamy A, Mohan R, Vasudevan S. Growth and characterization of dichlorobis l-proline Zn(II): A semiorganic nonlinear optical single crystal. Journal of Crystal Growth. 2009 Feb; 311(4):1161–5. ISSN: 0022-0248.
5. F. C. C: In the matter of unlicensed operation in the TV broadcast bands. Second Report and Order and Memorandum Opinion and Order no. FCC-08-260A1; 2008.
6. Nagarajan C, Madheswaran M. Experimental study and steady state stability analysis of CLL-T series parallel resonant converter with fuzzy controller using state space analysis. Iranian Journal of Electrical and Electronic Engineering. 2012 Sep; 8(3):259–67. ISSN: 1735-2827.
7. Chen R, Park JM, Reed JH. Defense against Primary User Emulation Attacks in Cognitive Radio networks. IEEE J Sel Areas Commun. (Special Issue on Cognitive Radio Theory and Applications). 2008 Jan; 26(1):25–37.
8. Parthasarathy R, Ilavarasan R, Karrunakaran CM. Antidiabetic activity of Thespesia Populnea bark and leaf extract against streptozotocin induced diabetic rats. International Journal of PharmTech Research.2009 Oct-Dec; 1(4):1069–72. ISSN: 0974-4290.
9. Anand S, Jin Z, Subbalakshmi KP. An analytical model for Primary User Emulation Attacks in Cognitive Radio networks. Proc 3rd IEEE Symp New Frontiers Dyn Spectrum Access Netw; Chicago, IL. 2008 Oct 14-17. p. 1–6.
10. Poongothai S, Ilavarasan R, Karrunakaran CM. Simultaneous and accurate determination of vitamins B_1, B_6, B_{12} and alpha-lipoic acid in multivitamin capsule by reverse-phase high performance liquid chromatographic method. International Journal of Pharmacy and Pharmaceutical Sciences. 2010 Oct; 2(S4):133–9. ISSN: 0975–1491.
11. Chen C, Cheng H, Yao YD. Cooperative spectrum sensing in Cognitive Radio networks in the presence of the Primary User Emulation Attack. IEEE Trans Wireless Commun. 2011 Jul; 10(7):2135–41.

12. Mathur C, Subbalakshmi KP. Digital signatures for centralized DSA networks. Proc 4th IEEE CCNC; Las Vegas, NV, USA. 2007 Jan. p. 1037–41.
13. Swami A, Sadler BM. Hierarchical digital modulation classification using cumulants. IEEE Transactions on Communications. 2000 Mar; 48(3):416–29.
14. Chen Z, Cooklev T, Chen C, Pomalaza-Raez C. Modeling Primary User Emulation Attacks and defenses in Cognitive Radio networks. Proc of IPCCC; Scottsdale, AZ. 2009 Dec 14-16. p. 208–15.
15. Quan Z, Cui S, Sayed A. Optimal linear cooperation for spectrum sensing in Cognitive Radio networks. IEEE J Sel Topics Signal Process. 2008 Feb; 2(1):28–40.
16. Digham F, Alouini M, Sinon M. On the energy detection of unknown signals over fading channels. IEEE Trans Commun. 2007 Jan; 55(1):21–4.
17. Kim H, Shin K. In-band spectrum sensing in Cognitive Radio networks: Energy detection or feature detection? Proc Mobi Com; 2008. p. 14–25.
18. Gong S, Liu W, Yuan W, Cheng W, Wang S. Threshold-learning in local spectrum sensing of Cognitive Radio. Proc VTC; Barcelona. 2009 Apr 26-29. p. 1–6.
19. Kimio T, Natarajan G, Hideki A, Taichi K, Nanao K. Higher involvement of subtelomere regions for chromosome rearrangements in leukemia and lymphoma and in irradiated leukemic cell line.Indian Journal of Science and Technology. 2012 Apr; 5(1):1801–11.
20. Cunningham CH. A laboratory guide in virology. 6th ed. Minnesota: Burgess Publication Company; 1973.
21. Sathishkumar E, Varatharajan M. Microbiology of Indian desert. Ecology and vegetation of Indian desert.D.N.Sen editor, India: Agro Botanical Publ; 1990, p. 83–105.
22. Varatharajan M,Rao BS, Anjaria KB, Unny VKP, Thyagarajan S. Radiotoxicity of sulfur-35. India; Proceedings of 10th NSRP; 1993. p. 257–8.
23. Elango P, Balaguru S. Welding Parameters for Inconel 625 Overlay on carbon steel using GMAW. 2015. Available from: http://www.indjst.org/index.php/vision