International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-3, Issue - 2, March- 2015

Higher Order Statics Based Primary User Emulation Attack Detection

S. Arul Selvi Dr.T.V.U.Kiran Kumar

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 user emulation attack is the major drawback in energy detector based spectrum sensing. 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 the 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, 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 so that 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.**

Keyword - **Primary User Emulation Attack, Received Signal Strength Indication, Nagagammi, Rayleigh Channel.**

1. INTRODUCTION

Recent studies [2, 3] reports proves that the wireless spectrum suffers from over utilization in some bands and underutilization in others. This happens because of the fixed spectrum 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 act 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 proactive security protocols, the DSA networks are vulnerable to various threats.

There are several attacks targeting the physical or medium access (MAC) layers in cognitive radio network. A common control channel (CCC) attack is the 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 attack targeting the physical layer is RF jamming that can severely disrupt Network's operation. Another physical layer attack that present in collaborative spectrum sensing is called spectrum sensing data falsification (SSDF) attack where a malicious CR can provide false observations on purpose.

Primary user emulation (PUE) attacks are 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 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 proposed a 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 of successful PUEA based on the energy detection is

Manuscript received March 25, 2015

S. Arul Selvi, Electronics and Communication Department, Bharath University,Chennai, Tamilnadu, 600073, India.
Dr. T.V.U. Kiran Kumar, Electronics and Communication Department, Bharath University,Chennai, Tamilnadu, 600073, India.

presented [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 an efficient method for the primary user emulation attack [6] in which a cooperative secondary user model was proposed for primary user detection in the presence of PUEA.

Traditional cryptography system can also be used to detect the PUEA .A public key cryptography mechanism is proposed [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 variable transmission power is proposed s[9].But in this the position of the attacker has to be known in advance and the distances between the 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 perform well 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 in 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.

II. SYSTEM MODEL

Primary user emulation attack scenario can be modelled by taking a primary network region and the secondary network region as shown in the fig.1.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 fig.1 is used to simulate the PUEA and detection process.

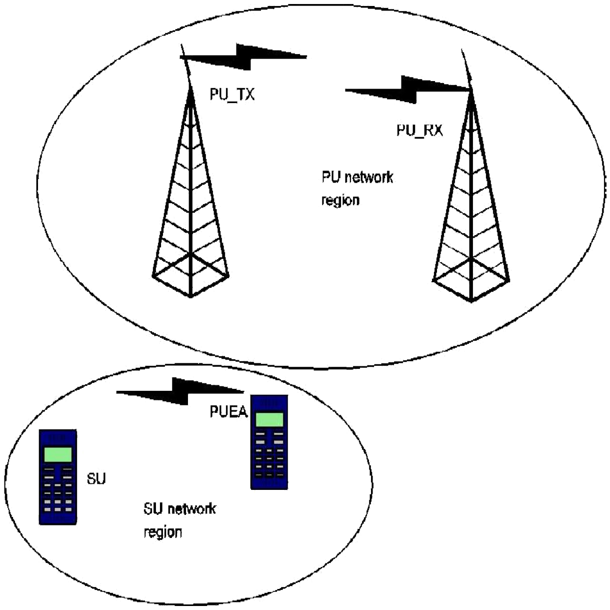

Fig.1 system model of primary user emulation attack

The PUEA detection process at the secondary user terminal is presented in the fig.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.

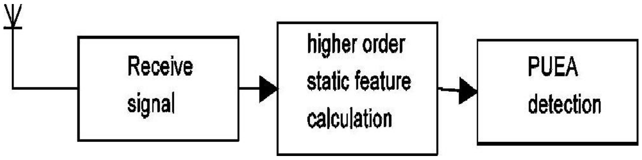

Fig.2 block diagram of higher order static based PUEA detection

The received signal by the secondary user will be

$$y_s(n) = h(n) * x(n) + n(n) \qquad (1)$$

Where the x(n) is the primary transmitted signal; h(n) is the channel co efficient 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 M_{20}=[$y^2(n)$] (2)

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

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

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

$$M_{21}=\sum_{n=1}^{N} |\,\mathrm{y(n)}|^{2} \qquad (5)$$

The fourth order moments and the cumulants for the received signal at the secondary user with sample values is

$$M_{4\ 0}=\frac{1}{N}\sum_{n=1}^{N} y^{4}(\mathrm{n}) - 3\,M_{20}{}^{2} \qquad (6)$$

$$M_{4\ 1}=\frac{1}{N}\sum_{n=1}^{N} y^{3}(\mathrm{n})\ y^{*}(\mathrm{n}) - 3M_{20}M_{21} \qquad (7)$$

$$M_{4\ 2}=\sum_{n=1}^{N} |\,\mathrm{y(n)}|^{4} - |M_{20}|^{2} - 2\,M_{21}{}^{2} \qquad (8)$$

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.

III. RESULT AND DISCUSSION

The system model as shown in the fig.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 cunulants 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, one PUEA node is introduced as shown in fig.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.

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

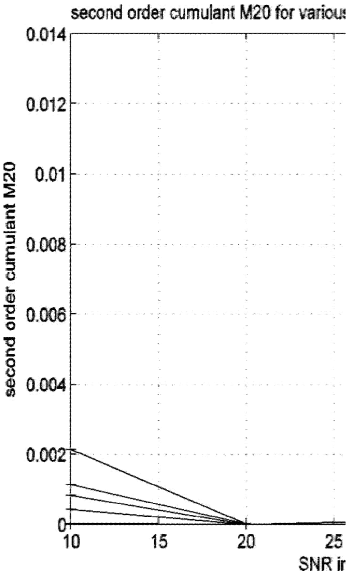

Fig.3 variation of second order cumulant $M_{20}$for various SNR and repeated random channels of Rayleigh.

Table.I 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}	$M_{4\ 0}$	$M_{4\ 1}$	$M_{4\ 2}$
10	9.05800055122081	9.06819043845575	7923520.50501201	23271249.2064019	10916518.0244008
20	0.00647585382085053	0.0076885462477 4843	1.830341535673	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	1.796944183344763e-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

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 values by 10 to compensate the small variation in the cumulant value due to fading channel.

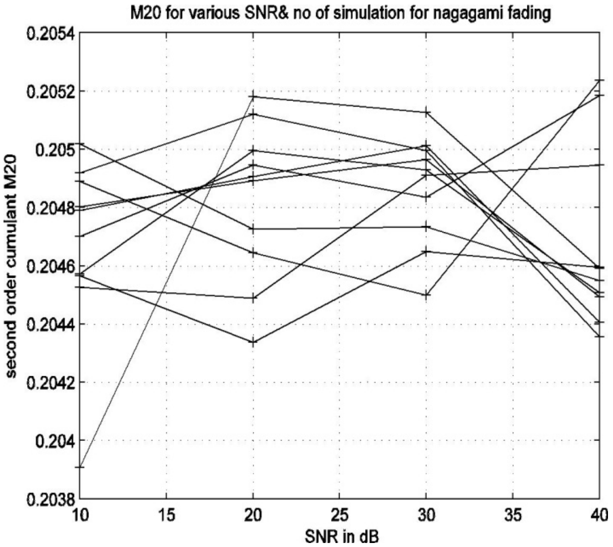

Fig.4 variation of second order cumulant M20 for various SNR and repeated random channels of nagagami

Table.II cumulant values for various SNR for nagagami channel

Primary user cumulant values for 10 unit distant between primary and secondary					
SNR (dB)	M_{20}	M_{21}	$M_{4\ 0}$	$M_{4\ 1}$	$M_{4\ 2}$
10	0.204668621649130	0.204678616437697	0.0831193304713818	0.0425548012838168	0.0425568454749695
20	0.204823779068742	0.204824789066937	0.0832476235851434	0.042611537077904	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

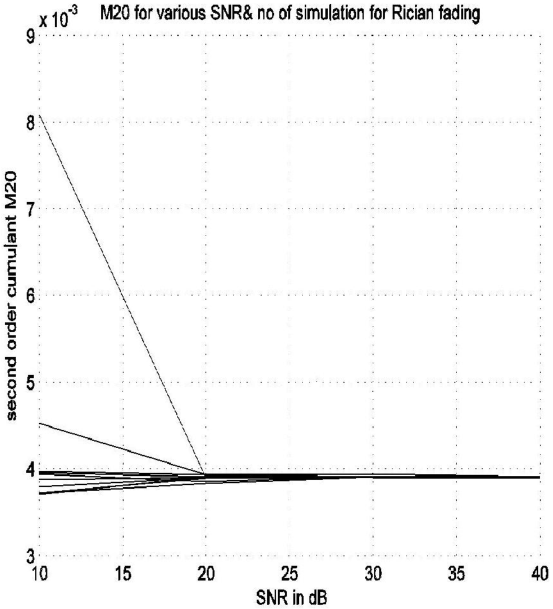

Fig.5 variation of second order cumulant M20 for various SNR and repeated random channels of Rician

Similarly the variation in cumulant value due to rician and nagagammi fading channels are captured by random no of channel relialization and plotted in fig.5 and fig.6 again this plot shows the cumulant value vary with little bit amount. From table II we can detect the PUEA unit in nagagammi 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.III cumulant values for various SNR for Rician channel

Primary user cumulant values for 4 unit distant between primary and secondary					
SNR (dB)	$_2M_{20}$	M_{21}	$M_{4\ 0}$	$M_{4\ 1}$	$M_{4\ 2}$
10	8.53376890105158e-05	0.00021874135 3098133	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	1.000475594469 62	1.0032910 2972669	2.001336525302 19	1.010026551996 71	1.013448581059 53

Similarly the rician channel case PUEA can be detected

If m40_cal/10 > m40_tab and 41_cal/10> m41_tab and m42_cal/10>m42_tab and m20_cal/10>m20_tab and m21_cal/10>m21_tab

IV. CONCLUSION

Primary user emulation attack detection is one of the important security issue in spectrum sensing of cognitive radio which will block the dynamic spectrum sharing .Even through 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 suffers 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.

REFERENCES

1. Nam Tuan Nguyen, Rong Zheng Zhu Han," On Identifying Primary User Emulation Attacks in Cognitive Radio Systems Using Nonparametric Bayesian Classification", IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 60, NO. 3, MARCH 2012

2. F.C.C.: 'Spectrum policy task force'. Rep. ET Docket no. 02-135, November 2002

3. 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

4. R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE J. Sel. Areas Commun. (Special Issue on Cognitive Radio Theory and Applications), vol. 26, no. 1, pp. 25–37, Jan. 2008

5. S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in Proc. 3rd IEEE Symp. New Frontiers Dyn. Spectrum Access Netw., Oct. 2008, pp. 1–6.

6. C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2135–2141,Jul. 2011

7. C. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in Proc. 4th IEEE CCNC, Jan. 2007, pp. 1037–1041.

8. Ananthram Swami and Brian M. Sadler, Hierarchical Digital Modulation Classification Using Cumulants, IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 48, NO. 3, MARCH 2000

9. Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in Proc. of IPCCC, 2009, pp. 208–215.

10. Z. Quan, S. Cui, and A. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," IEEE J. Sel. Topics Signal Process., vol. 2, 2008.

11. F. Digham, M. Alouini, and M. Sinon, "On the energy detection of unknown signals over fading channels," IEEE Trans. Commun., vol. 55, pp. 21–24, 2007.

12. H. Kim and K. Shin, "In-band Spectrum Sensing in Cognitive Radio Networks: Energy Detection or Feature Detection?" in Proc. MobiCom, 2008, pp. 14–19.

13. S. Gong, W. Liu, W. Yuan, W. Cheng, and S. Wang, "Threshold- Learning in Local Spectrum Sensing of Cognitive Radio," in Proc. VTC, 2009, pp. 1–6.

Ms.S.Arulselvi working as an Assistant professor in the department of Electronics and Communication Engineering, Bharath University, Chennai, India. I did my Master of Engineering in Computer and Communication Engineering in 2007. My research interests are in the area of Networking.

.

Dr. T.V.U. Kiran Kumar is a professor and Head of the department of Electronics and Communication Engineering, Bharath University, Chennai, India. He received his Doctorate in Electronics and Communication Engineering in 2010.He received his Master of Engineering in Computer and Communication Engineering in 2002. His research interests include Networking and Image Processing.