An Efficient Spectrum Sensing Framework and Attack Detection in Cognitive Radio Networks using Empherical Mode Decomposition for CRN

Sundar Srinivasan,Research Scholar, Dept of E&C, Mewar University, Chittorgarh, Rajasthan, India. sundars23@hotmail.com

Dr. K.B Shiva Kumar, Professor & HOD, Department of Telecommunication Engineering , Sri Siddhartha Institute of Technology, Tumkur, India. kbsssit@gmail.com

Abstract—**Cognitive Radio offers software controlled spectrum reallocation which enables unutilized spectrum to be distributed amongst non-licensed secondary user and reallocate back to the primary licensed user when demand surges. Several authors in the past have proposed robust mechanism for PUE attack detection and prevention, but not very efficient. In order to detect such attacks efficiently and prevent we propose a unique EMD (Empirical Mode Decomposition) based technique with Double Modulation (First modulation layer acts like a signature for PU and Second modulation shifts signal baseband transmission signal, exposing only the outer carrier envelope to attackers). At the base station, a signal is decomposed to its intrinsic mode function (IMF) which results in extraction of the signature modulation and main baseband carrier. By evaluating the encoder envelop a base station can easily detect an emulated attack. The proposed EMD based technique performs much better over FFT based counterpart in terms of accuracy of attack detection and minimizing the probability of the attack.**

Keywords – Intrinsic mode function (IMF);Primary User(PU); SecondaryUser,Emulation Attack(PUEA);Cognitive Radio(CR);EMD (Empirical Mode Decomposition;

I. Introduction

The Spectrum Sensing is key link for Cognitive Radio. The recent development in wireless communication has led to the problem of growing spectrum scarcity [10]. Due to increasing spectrum demand for new wireless applications the available radio frequency spectrum has become scarcer. A significant amount of allocated radio frequency spectrum is used sporadically, causing underutilization of spectrum. Cognitive radio (CR) technology provides a promising solution for the spectrum scarcity issues in wireless networks [9]. It allows the efficient use of the finite usable radio frequency spectrum. Licensed or Primary users are users who have right to use the spectrum band whereas unlicensed or Secondary users who can use the spectrum which is temporarily not used by licensed users[8], without causing interference. The existence of cognitive networks is justified by the fact that many spectra are not fully used by their dedicated users, and therefore allowing secondary user access will give the opportunity to fully use the bandwidths and provide more spectrums to users [12].

When a node moves from one network to another cognitive network, it gets connected with nearby unlicensed cognitive base station. If this node with unlicensed spectrum needs more bandwidth for its application, then it requests for paid bandwidth to nearby licensed base station through the cognitive base station. Cognitive Base station forwards the request only if it sense that the licensed network has sufficient bandwidth which is done through spectrum sensing. Once the free spectrum is detected, requested to allocated send to the cognitive user through its nearby requesting cognitive base station.

In order to offer a defense against not-so secured CR network, various schemes can be adopted which includes encryption, authorization and soon. However, such mechanisms lead to protection of data leakage rather than protecting the network against spectrum level attacks such as PUE attack [14]. In order to detect and present such attacks more intelligent system is needed at the link layer and the physical layer that can offer the security without any significant changes over the existing protocol stack and without significantly adding receiver complexity [15].

This paper proposes a unique EMD based technique to provide a defense mechanism against PUK attacks as well as efficient detection of the same. Efficient detection of the emulating node may even be handled by network layer by various policy based protection like black listing [16] etc. In order to effectively simulate this fundamental, we present a simple cognitive network running on BPSK modulation and FDM.

DOI : 10.18231/2454-9150.2018.0394

The current paper is structured as follows: Section II Literature Survey, Section III Proposed Methodology & Implementation details, Section IV describes performance comparison & Section V Conclusion of findings

II. RELATED WORK

Priya Goyal et al., [1] Proposed AES-assisted system for robust and reliable primary & secondary system operations where primary user generates a pseudo-random AES-encrypted reference signal that is used as the segment sync bits. The sync bits in the field sync segments remain unchanged for the channel estimation purposes. At the receiving end, the reference signal is regenerated for the detection of the primary user and malicious user.

K Shim et al., [2] the security problems arising from Primary User Emulation (PUE) attacks in CR networks, introducing comprehensive study to PUE attacks, from the attacking rationale and its impact on CR networks, to detection and defense approaches.

G. V Pradeep Kumar et al., [3] solved the spectrum scarcity problem by allocating spectrum dynamically to unlicensed users using free spectrum bands which are not being used by licensed users without causing interference to incumbent transmission. PUEA is one of the major threats in spectrum sensing discussing various security issues in CRN. Proposed new Approach for detecting PUE attach on SWSN based on anomaly detection & cognitive features such as sensing, learning, & collaboration proposed [16].

Reshma Rajan et al., [4] stated crucial features of CRNs are awareness, reliability & adaptability for better communication and preventing the network from threats. PUEA is one of the security issues in the physical layer of the protocol stack & defensive system has been proposed.

Hang Zhang et al., [5] experimented using the SUs' interference to improve the PU's secrecy capacity & providing the SUs the opportunity to access the spectrum as a reward. Tradeoff between the SUs' channel capacity & the PU's secrecy capacity decided by which SUs can share the spectrum with the PU, hence model derived a coalition formation game model with nontransferable utility, proposing a merge & split algorithm.

K Shim et al., [6] explained the effect of imperfect channel state information (CSI) which is of importance issue in underlay CR. Huichao Jiang et al., [7] proposed method to identify the threat & to deal a advanced encryption standards scheme was experimented which helps in mitigating PUE attacks in certain situations.

III. PROPOSED METHODOLOGY

The figure 1 describes the overall block diagram of the proposed research work. A base station will perform a spectrum analysis of the received signal followed by an energy wise spectrum band marking. It would then form a decision rule based on adaptive threshold to detect independent spectrum present in the received signal which are decomposed using EMD techniques. As the received signal will be often affected by noise, prior to any spectrum sensing decision, it needs to filter the signal using equalization process. Equalization can be performed using matched filter. Once all the primary spectrums are detected, each of these spectrums will be analyzed in comparisons to all others to detect anomaly. The anomaly marks an attack PU. That spectrum band will then be padded up with controlled noise to prevent the void being detected by any attacker.

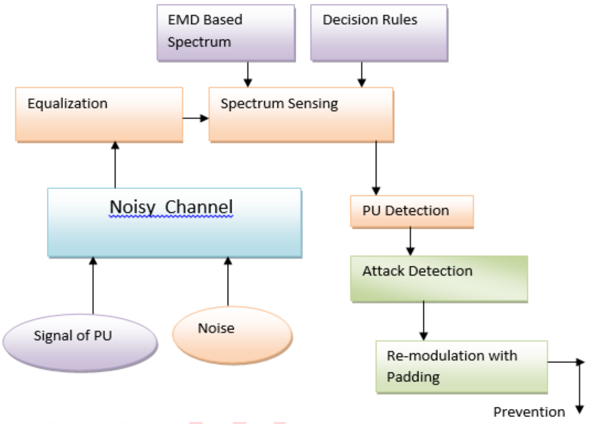


Figure 1 Base Station Block Diagram (System Design)

A. EMD Based Attack detection

In figure 2 represents Primary User Detection Process flow detection followed by the base station to detect the presence or absence of a primary user and detection of unused spectrum. The technique includes a FFT of the received signal followed by Energy envelope thresholding. We use an adaptive thresholding to obtain the optimum and average energy in normal spectrums and detect the absence of it by searching for low energy area in the spectrum.

It is clearly mentioned in implementation section that threshold is 30% of the average energy of the spectrum. Threshold is determined based on experimental observations.

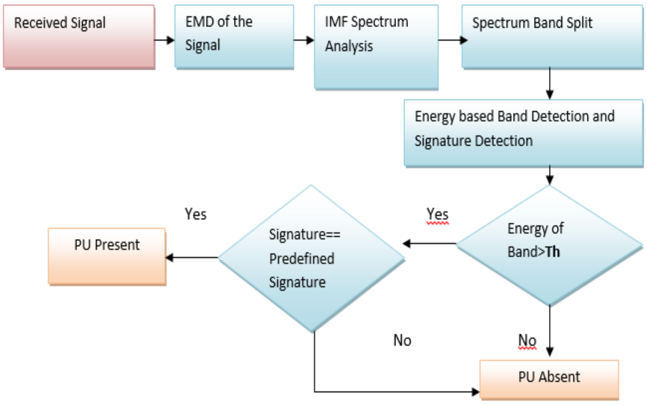


Figure 2 : Flow Diagram of Primary User Detection

DOI : 10.18231/2454-9150.2018.0394

The *Figure 2* shows the detailed blocks of proposed PUE detection system which is a part of spectrum sensing block of a typical CR base station. The void spectrum detection is followed by misuse detection.

B. Detection Approaches for PUE Attacks

In Proposed Transmission Model, we assume that network supports NRZ coding. Each signal is converted into 1 and -1 and modulated with carrier sequence. The signal is transmitted through an AWGN channel. At receiver, we use a matched filter to detect signal (fig 3).

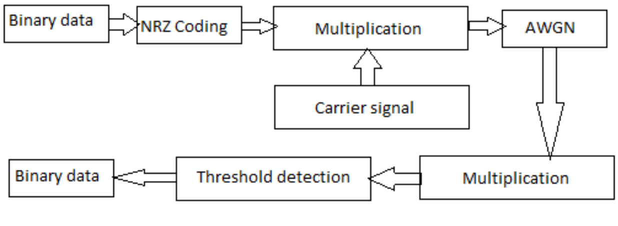


Figure 3: Basic Transmitter Receiver System

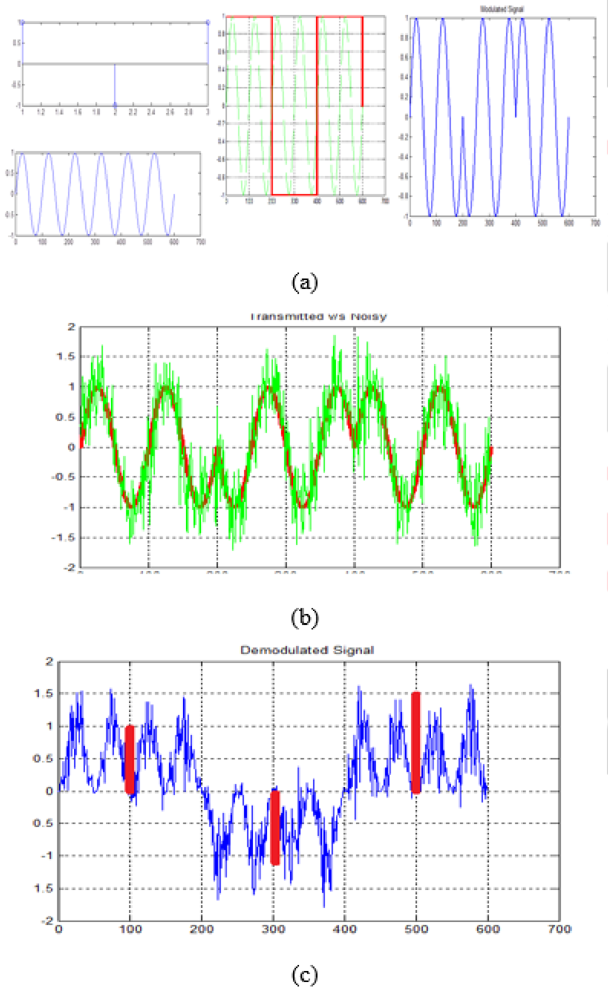


Figure 4 : Result of the transmitter receiver stage (a) Transmitter (b) Channel Response (C) Receiver

In figure 4(a) shows that a message 101 is converted to NRZ coding and becomes 1-11. This is multiplied by a sinusoidal carrier to obtain a modulated BPSK signal. We used a modulation index M=2, which results in transmission of two cycles of carrier against each message bits. Whenever there is a change from 1 to -1 or vice versa, there is a phase change.

Figure 4(b) shows the received signal at the receiver. One can clearly see the effect of noise (green color) over the actual signal. This is due to effect of additive white Gaussian noise.

Figure 4(c) is the matched filter response at the receiver. The matched filter response clearly offers 1 and -1 levels (marked with red) which is then used for decoding the message to [1 0 1] using threshold detector.

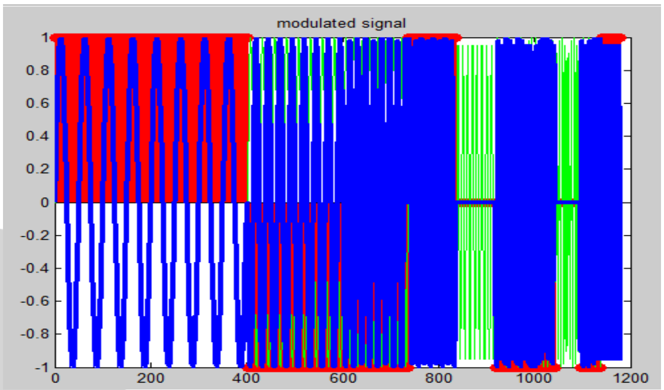


Figure 5 : Ten user modulated signal for CR

The figure 5 refers 10 user's modulated data where each user is transmitting a bit and their spectrums are 100Hz, 200Hz...1000Hz respectively. One can also see that there is a void for user 7 and 9 who are not transmitting any signal.

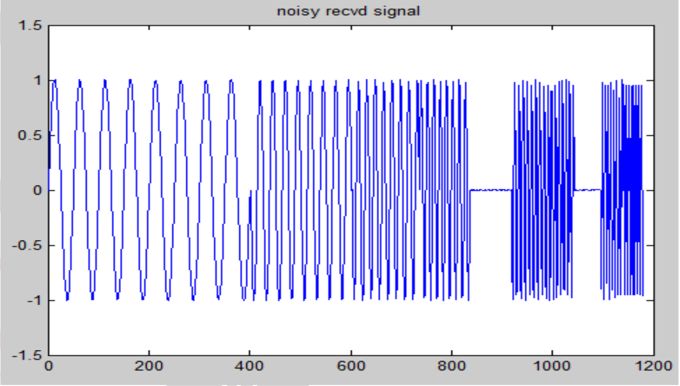


Figure 6 : AWGN affected signal at Receiver

The figure 6 is Gaussian noise effected received signal which now needs to be demodulated by the receiver & indicates relatively high SNR of 20 dB (If the SNR is more like >10 dB, distortion is minimum. Less distorted signal is the mark of high SNR.

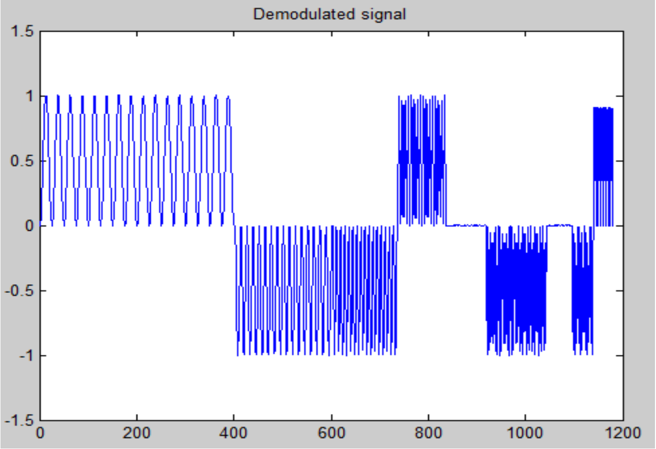


Figure 7 : Time domain visualization of demodulated data

In figure 7, graph is the result of demodulation at the receiver. The signal is obtained by multiplying the received signal containing modulated data from 10 users with a time series carrier sequence of 10 frequencies. My multiplying the carrier with the received signal one can clearly see Sequence of positive and negative signals. We then use a threshold detector for extracting 1's and -1's from this signal and finally decode them as 1's and 0's.

C. EMD Model

Empirical Mode Decomposition (EMD) has been introduced by Huang et al. [20] to nonlinear and non-stationary time series. Like Wavelet Analysis, EMD attempts to decompose a time series into individual components (intrinsic oscillations) by exploiting both local temporal and structural characteristics of the data.

The typical signal decomposition model is represented in fig 8

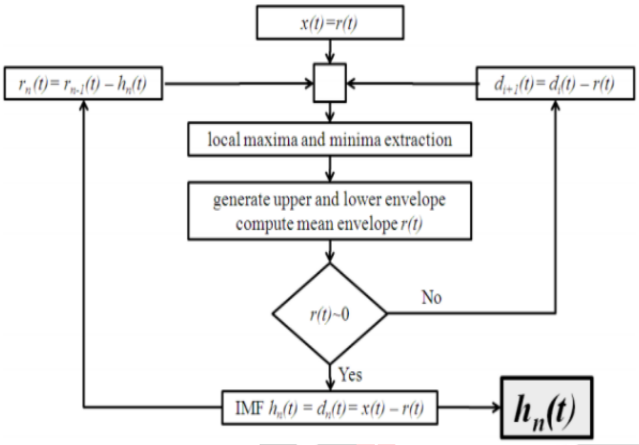

$x(t)=r(t)$
$r_n(t)=r_{n-1}(t)-h_n(t)$
$d_{i+1}(t)=d_i(t)-r(t)$
local maxima and minima extraction
generate upper and lower envelope
compute mean envelope $r(t)$
$r(t)\sim 0$
No
Yes
IMF $h_n(t)=d_n(t)=x(t)-r(t)$
$h_n(t)$

Figure 8 : EMD Signal decomposition model

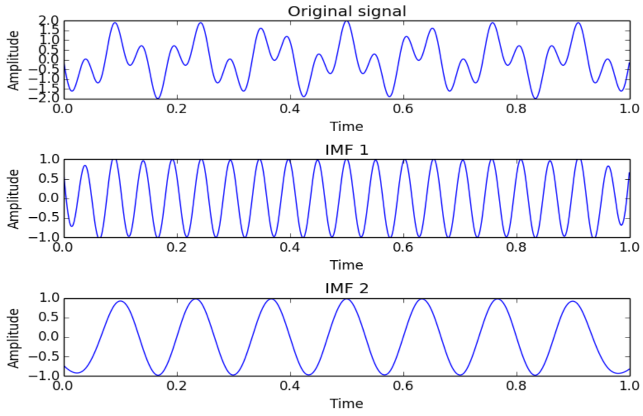


Figure 9 : Decomposition of Signals in to 2 IMF Signals

The above figure 9 shows the decomposition of a signal into two IMF signals. It can also be clear that EMD decomposes a complex signal with multiple frequency bands. EMD typically decomposes a signal into decreasing band of frequency.

If we take the power spectral density of the IMF and organize them in same spectral band we get the independent spectral maxima of each signal over entire transmission range. The spectral analysis of the combined IMF functions is as shown below in figure 10

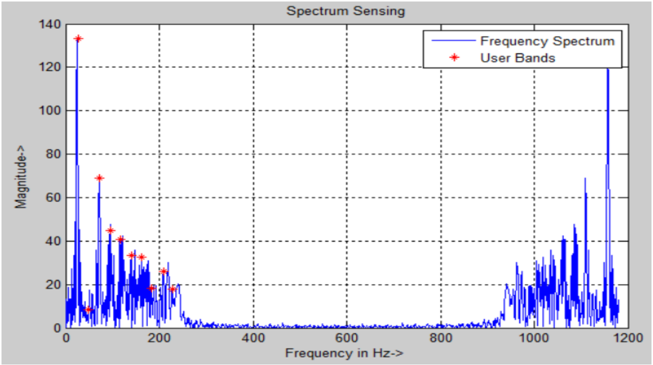


Figure 10 : Spectrum Analysis of the IMF function of the transmitted signal at Base Station

The figure 10 shows the spectrum analysis plotting the signal analysis graph in base station and when user’s data reaches base station, it analyses the spectrum. Base station performs a FFT on the received signal as elaborated by the block diagram in figure 8. Once the spectrum magnitude is obtained, the spectrum is divided into spaces of 100 HZ and then maxima in each band are obtained which is marked as the primary user's data. The plot in Figure 11 is for signal [1 0 -1 1 -1 -1 -1 -1 1 1] where once can clearly see the second user's spectrum is minimum. This proves that frequency domain analysis can conclusively produce void spectrum and well as used spectrum. The Spectrum once the signal is attacked by the attacker is plotted in below figure 11.

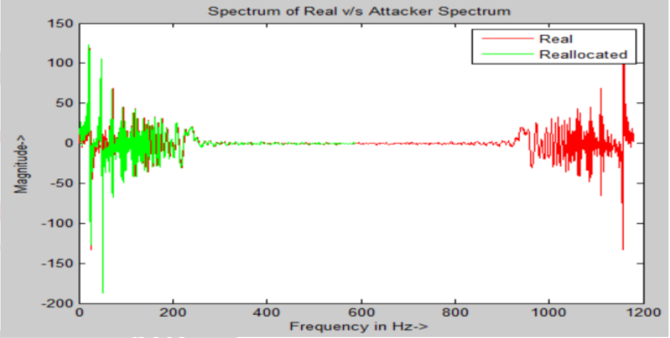


Figure 11 : Result of Attacker attacking first free band

The Spectrum of the second user was minimum as referred in figure 11. But once attacker attacks the second band which is free, there is a significant increase in the spectrum of the second user.

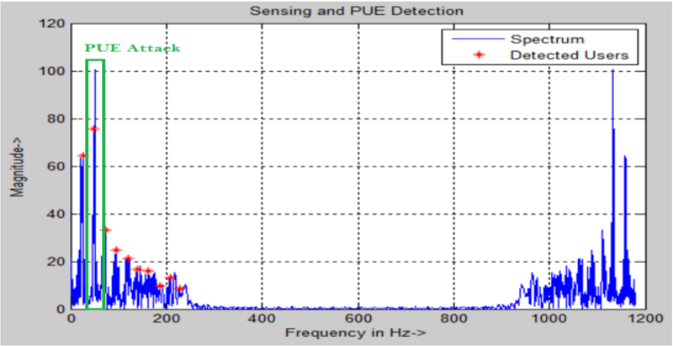


Figure 12 : Spectral Analysis at Cognitive Radio Base Station

DOI : 10.18231/2454-9150.2018.0394

The figure 12 shows the spectral analysis of CR base station. Note that there is an attack at the second spectrum and the attacker has emulated the free spectrum of the second user. Still the CR base station is able to detect our presence of PUE attack using our technique.

Malicious user predicts the average spacing between the frequency and attack the free band. The objective of the sensing model is to detect these missing bands and hence absent user through frequency domain analysis.

Attacker can see the transmitted multi user signal. We assume that attacker has prior knowledge to the sampling frequency of the network but has no prior knowledge about the primary user frequency. It tries to find the void user in the technique specified above. As the attacker does not have access to primary frequency, he tries to locate two highest maxima which are obviously first two user's data. He predicts the guard band based on the difference between the samples of these two frequencies. Now taking guard band as basis the attacker will try to locate the free frequency band and emulate that user first through frequency domain and then followed by inverse transform. The steps are as given bellow.

1. Now Attacker will Assume the Primary Frequencies
2. Attacker will see the difference between subsequent frequencies and predict
3. Now Attacker will try to send a signal through emulated frequency
4. Attacker can't know Modulation depth. So, predicts M
   High M Value will succeed in Emulation
5. Assume that attacker has prior knowledge of Fs, Attacker creates carrier as attacker can append only one bit, he will modulate it
6. Now the attacker actually has to mix this signal with actual transmitted signal. Way to do it is:
   a) Decompose Modulated Signal to IMF Functions
   b) Take FFT of IMF signals & combined them in to Single spectrum XaF
   c) Take FFT of rec Signal xrXrf, Result Attack Signal xra= ifft (Xaf+Xrf)
7. Now Emulated signal crosses through channel & Rx

D. *Defence Approaches against PUE Attacks*

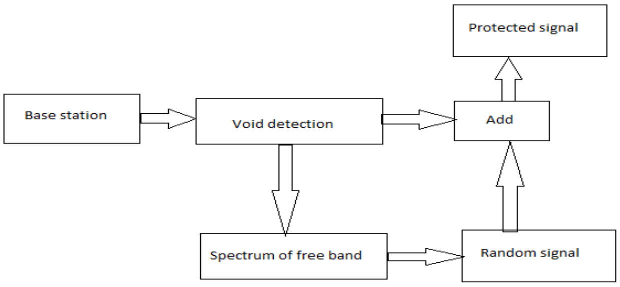


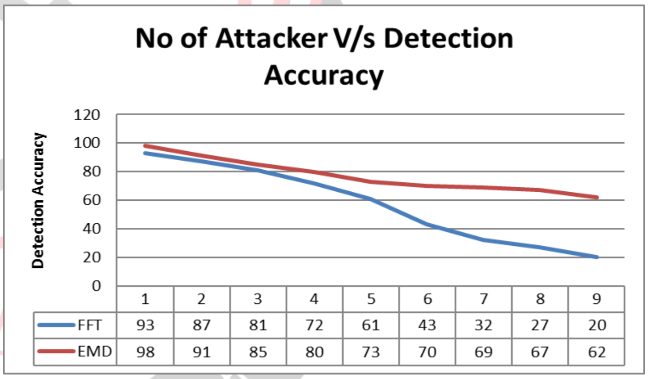
Figure 13 : Block diagram of defence against PUE attack

The Block diagram of defence against PUE attack showed in Figure 13. The defence can be predicted by ensuring the free spectrum is not visible to intruders. This can be done by either adding intentional noises in the spectrum by adding time domain sequence. In both the domains this can be achieved by reserving a signal band for void users and transmitting pseudo random data in this band, only a base station will have prior knowledge about the particular spectrum being linked to void users. An attacker will see this as another user's data. Therefore, due to lack of void in the spectrum the simulation attack becomes impossible.

IV. Performance Evaluation

We consider a cognitive radio network with ten primary users and only two users as active PU user. We vary the number of attackers where each of the attackers pretends to be a particular primary user. Performance is evaluated in MATLAB Tool and comparisons as shown in Fig 14 indicating the Detection Accuracy. Even though EMD based technique also relies on the spectral analysis of the IMF function of the transmitted signal, it is eliminating the analysis of the frequencies outside the band of interest. Also unlike FFT which assumes IMF are weighted functions. Therefore, the attacker signals become much more prominent than in FFT analysis.

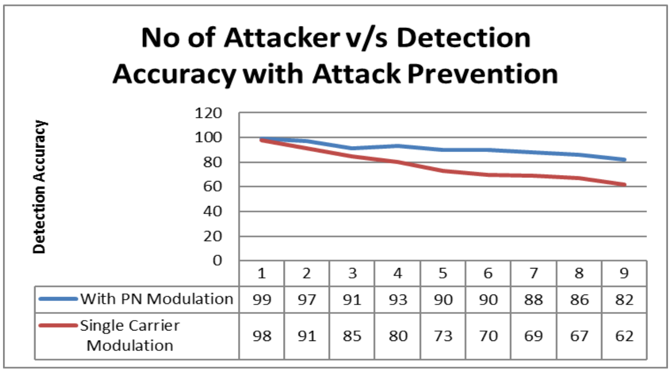
Figure 14 : Performance comparisons FFT verses Proposed based



	1	2	3	4	5	6	7	8	9
FFT	93	87	81	72	61	43	32	27	20
EMD	98	91	85	80	73	70	69	67	62

technique

Even though EMD based technique also relies on the spectral analysis of the IMF function of the transmitted signal, it is eliminating the analysis of the frequencies outside the band of interest. Also unlike FFT which assumes IMF are weighted functions. Therefore, the attacker signals become much more prominent than in FFT analysis



	1	2	3	4	5	6	7	8	9
With PN Modulation	99	97	91	93	90	90	88	86	82
Single Carrier Modulation	98	91	85	80	73	70	69	67	62

Figure 15 : System Performance Comparison with Proposed Technique

DOI : 10.18231/2454-9150.2018.0394

In Figure 15, Performance of Proposed technique indicating preventive measure where the signal is modulated by an intermediate known PN sequence before modulating and transmitting with the common carrier. By introducing a signature matching technique, the detection accuracy improves significantly, justifying use of proposed prevention technique.

V. CONCLUSION

A novel spectrum based sensing approach is proposed in this paper involving mechanisms for PUK attack and detection using EMD technique with spectral analysis experimented in Matlab. With the increasing popularity of the cognitive radio network, the threat prospect of such network is also increasing. With more and more PUE attacks, new techniques are needed to defend CR from PUE and other selfish or DDOS attacks. By decomposing the signal into its IMFs, one can clearly find the anomalies introduced by emulated attacker signal. Further by incorporating an intermediate modulation of the signal with signature PN sequence, the detection accuracy increases significantly which indirectly is an indication of the PUE attack risk minimization.

REFERENCES

[1] Priya Goyal, Avtar Singh Buttar, and Mohit Goyal. "An efficient spectrum hole utilization for transmission in Cognitive Radio Networks." Signal Processing and Integrated Networks (SPIN), 2016 3rd International Conference on. IEEE, 2016.

[2] Shim, Kyusung, Nhu Tri Do, Beongku An, Sang-Yep Nam "Outage performance of physical layer security for multi-hop underlay cognitive radio networks with imperfect channel state information." Electronics, Information, and Communications (ICEIC), 2016 International Conference on. IEEE, 2016.

[3] G. V. Pradeep Kumar & D. Krishna Reddyy. "Frequency domain techniques for void spectrum detection in cognitive radio network for emulation attack prevention." Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on. IEEE, 2016.

[4] Hang Zhang , Tianyu Wang, Lingyang Song & Zhu Han "Interference Improves PHY Security for Cognitive Radio Networks." IEEE Transactions on Information Forensics and Security, 609-620, 2016.

[5] K Shim, NT Do, B An, SY Nam. "Outage performance of physical layer security for multi-hop underlay cognitive radio networks with imperfect channel state information." Electronics, Information, and Communications (ICEIC), 2016 International Conference on. IEEE, 2016.

[6] Huichao Jiang, Xiao Jing, Songlin Sun & Dongmei Cheng "Mitigating Primary User Emulation attacks in Cognitive Radio networks using advanced encryption standard.":Proceedings of the 1st International Congress on Signal and Information Processing, Networking and Computers (ICSINC 2015), October 17-18, 2015 Beijing, China. CRC Press, 2016.

[7] Alahmadi, M. Abdelhakim, J. Ren, & T. Li, “Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard”. Global Communications Conference (GLOBECOM), IEEE, 3229–3234, 2013

[8] Chen R, Park JM, Reed J “Defense against primary user emulation attacks in cognitive radio networks”. Selected Areas Commun.of IEEE Journal, P25-37, 2008

[9] Zhou Yuan,Dusit Niyato,Husheng Li,Ju Bin Song,and Zhu Han,“Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks,” IEEE J. Sel. Areas Communications, vol. 30, no.10, November 2012

[10] Hao D, Sakurai K “A differential game approach to mitigating primary user emulation attacks in cognitive radio networks”. In IEEE 26th International Conference on Advanced Information Networking and Applications, 2012. Fukuoka-shi; 26–29 March 2012:495-502.

[11] Javier Blesa and Elena Romero et al “PUE attack detection in CWSNs using anomaly detection techniques”. EURASIP Journal on Wireless Communications and Networking,2013

[12] Wang and K. J. R. Liu, “Advances in cognitive radio networks: A survey,” IEEE Journal of Selected Topics in Signal Processing, vol. 5, no. 1, pp. 5 –23, Feb 2011

[13] Mahdi Al-Badrawi and Nicholas J. Kirsch, “An EMD-Based Spectrum Sensing Technique for Cognitive Radio Networks,” 81st IEEE Vehicular Technology Conference (VTC Spring) , DOI:10.1109, May 2015

[14] Mahdi Al-Badrawi and Bessam Al-Jewad et all, “An adaptive energy detection scheme using EMD for spectrum sensing,” 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), DOI: 10.1109/CCNC.2017.7983072, Jan 2017

[15] R. Chen, J. Park, and J. H. Reed, “Defense against primary user emulation. attacks in. cognitive radio networks,” IEEE Journal Selected Areas J Communication, vol. 26, no. 1,. pp. 25–37, Jan. 2008

[16] Z. Jin, S. Anand, & K. P. Subbalakshmi, “Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing”. ACM Mobile Computing and Communications Review (MC2R): Special Issue on Cognitive Radio Networks,74-85, 2009.

About Authors

Sundar Srinivasan is Research Scholar in area of Machine Learning Cognitive Radio Networks & Security. He Completed MTech from M.S.Ramaiah Institute of technology, B.E from Sri Siddhartha Institute of technology, Diploma from M.N.Technical Institute in Electronics and Communication Engineering. He has got over 17years of SW experience in Mobile and Embedded technologies. His Area of research includes Mobile Technology, Machine to Machine Communication, Internet of things (IoT), Artificial Intelligence, Cognitive Radio Wireless networks, Multimedia and DSP Technologies.

Dr. K.B. Shiva Kumar received the BE degree in Electronics & Communication Engineering during 1983, ME degree in Electronics during1989, MBA degree during 1998 from Bangalore University, Bangalore and M Phil Degree during 2009 from Dravidian University Kuppam. He obtained Ph.D. during 2012 in Information and Communication Technology from Fakir Mohan University, Balasore, Orissa. He has got 33 years of teaching experience and has over 60 research publications in National and International Conferences and Journals. Currently he is working as Professor, Dept. of TC Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka. His research interests include Signal processing, Image processing, Steganography and Multirate Systems and Filter Banks.