A Method to Detection And Prevent PUK Attack in CRN

[1]Sundar Srinivasan, [2]Dr. K.B Shiva Kumar

[1]Research Scholar, Dept of E&C, Mewar University, Chittorgarh, Rajasthan,

[2]Professor & HOD, Dept of Telecommunication Engineering, Sri Siddhartha Institute of Technology ,Tumkur

***Abstract*—**Cognitive Radio is an adaptive, intelligent radio & network technology can detect available wireless channel automatically & improve radio operating behavior by changing transmission parameter dynamically in turn enabling more channel communications. A PUE attack is one where a secondary user with partial information of the modulation and the underneath spectrum scheme pretends to be a primary user and injects its signal into the primary spectrum. Even though the spectrum reallocation is an immensely powerful mechanism to ensure better spectrum utilization, it also leads to primary user emulation (PUE) attack. This invariably results in denial of service attack on the primary user. Several authors in the past have proposed robust mechanism for PUE attack detection and prevention. Various blind detection techniques are more popular in this area. A blind spectrum sensing technique [8] is one where base station has no prior knowledge of the transmission cycle & are not controlled in synchronous ways. Such techniques fail to detect and prevent PUE attack as the attacker signal often is integrated in the base band. To detect such attacks efficiently & prevent this paper helps with a unique Empirical Mode Decomposition based model technique with double modulation.

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

I. INTRODUCTION

In order to offer a defense against not-so secured CR network, various schemes can be adopted which includes encryption, authorization and so on. However, such mechanisms lead to protection of data leakage rather than protecting the network against spectrum level attacks such as PUE attack. 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.

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. This is done through spectrum sensing. Once the free spectrum is detected, it can be requested to be allocated to the cognitive user through its nearby requesting cognitive base station.

The Concept of CR address issue of spectrum efficiency [12] & capability to optimally adapt operating parameters according to surrounding radio environment. The recent development [10] in wireless communication has led to the problem of growing spectrum scarcity. A significant amount of allocated radio frequency spectrum is used sporadically, causing underutilization of spectrum. Cognitive radio technology provides a promising solution [9] for the spectrum scarcity issues in wireless networks and allows efficient use of the finite usable radio frequency spectrum. In cognitive radio terminology, existence of cognitive networks is justified by the fact [11] 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.

Current paper proposes a novel technique for EMD to offer a defense 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. In order to effectively simulate this fundamental, we present a simple model of cognitive network running on BPSK modulation & FDM.

First layer of modulation with acts like the signature for the primary user and the second modulation shifts the signal baseband transmission signal, exposing only the outer carrier envelope to the attacker. At the base station, a signal is decomposed to its intrinsic mode function (IMF) which results in extraction of the signature modulation as well as the main baseband carrier. By evaluating the encoder envelop a base station can easily detect an emulated attack. On the other hand, intermediate signal spreading enhances the used bandwidth which leaves little or no bandwidth for the attack. We compare our results with FFT based technique. Results shows that 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.

II. RELATED WORK

K Shim et al., [6] explained the effect of imperfect channel state information which is importance issue in underlay CR. Huichao Jiang et al., [7] proposed method to identify threat (PUK) & to deal advanced encryption standards scheme was experimented which helps in mitigating PUE attacks. Reshma Rajan et al., [4] stated crucial features of Cognitive radio Networks namely awareness, reliability & adaptability & and preventing the network from threats and malicious intent is equally important and a challenging task. The physical layer is significant in terms of detection of this malicious node. PUEA is one of the security issues in the physical layer of the protocol stack & defensive system has been proposed.

K Shim et al., [2] security problems arising from PUE attacks in CR networks & explained a comprehensive introduction to PUE attacks, from the attacking rationale & its impact, to detection and defense approaches.

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, deriving model of coalition formation game with nontransferable utility, proposing algorithm for merge & split.

Priya Goyal et al., [1] Proposed AES-assisted system for robust and reliable primary & secondary system operations. In the proposed system, the primary user generates a pseudo-random AES-encrypted reference signal that is used as the segment sync bits.

G. V Pradeep Kumar et al., [3] solved the spectrum scarcity problem by allocating the spectrum dynamically to unlicensed users using free spectrum bands which are not being used by licensed users without causing interference to the incumbent transmission.

III. PROPOSED MODEL

The figure 1 describes the system level block of base station for proposed model that perform a spectrum analysis of the received signal & energy wise spectrum band marking, forming 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.

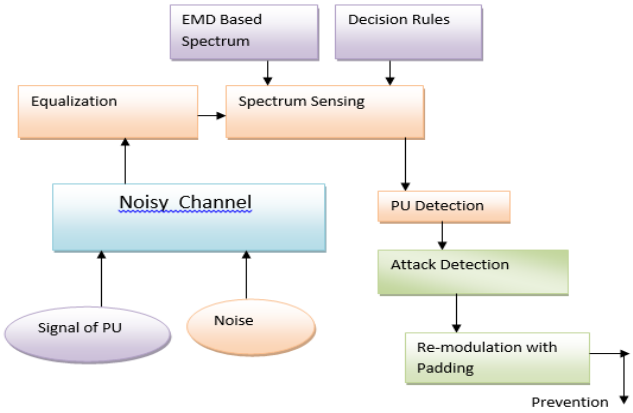


Figure 1 System Design Overview of Base Station

A. *Analysis (Base Station)*

In figure 2 we see the process 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.

The threshold 30% of the average energy of the spectrum. Threshold is determined based on observations.

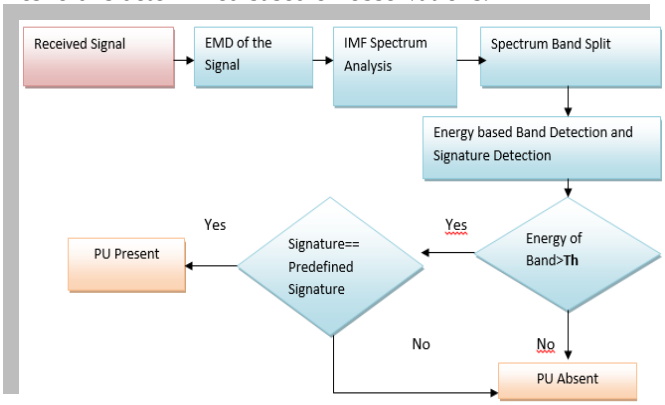


Figure 2 : Model of PU Detection

The above figure shows the detailed blocks of our PUE detection system, part of spectrum sensing block of a typical CR base station.

B. *Detection Approaches (PUE Attacks)*

Model can be divided in to A) Transmission Model: We assume that the 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).

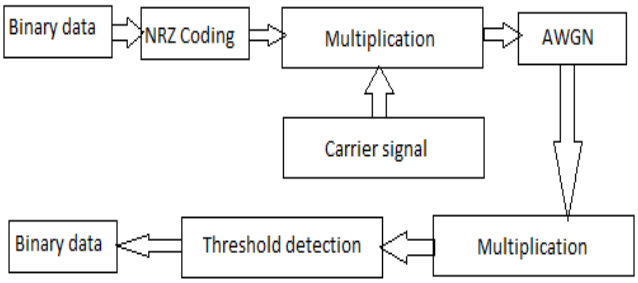


Figure 3 Transmitter Receiver System

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.

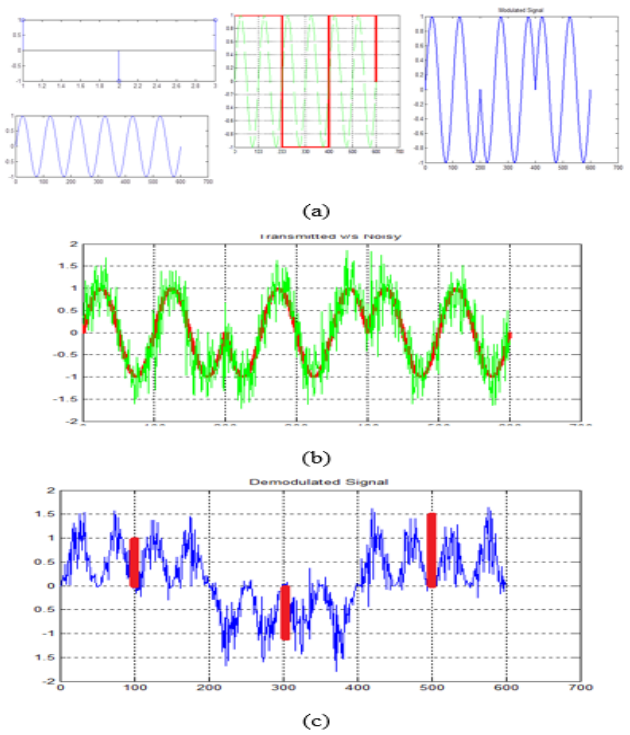


Figure 4 Transmitter Receiver Signal Transmission
(a) TX (b) Responsive Channel (C) RX

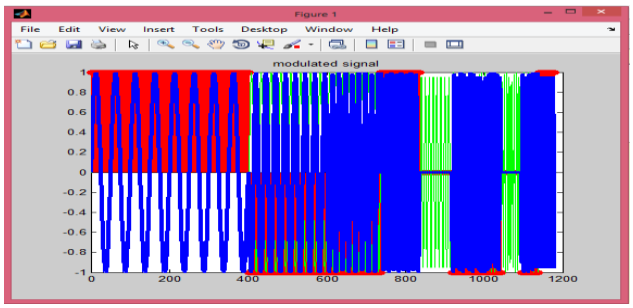


Figure 5 User Modulated signal for CR

The figure 5 is N user's modulated data. One can also see that there is a void for user 7 and 9 who are not transmitting any signal. The figure 6 is Gaussian noise effected received signal which now needs to be demodulated by the receiver. The above plot is for 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. Compare Figure 6 & figure 4C which is low SNR. Hence signal distortions are more).

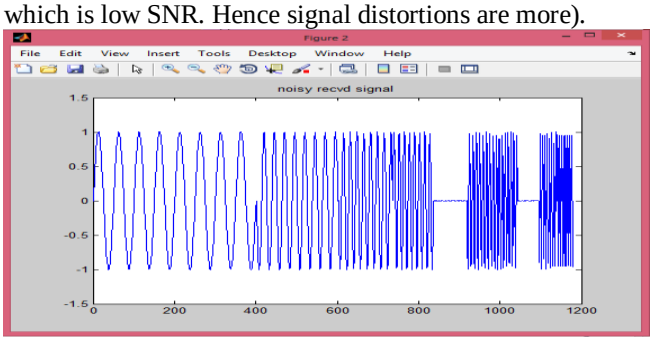


Figure 6 AWGN affected signal at the Receiver

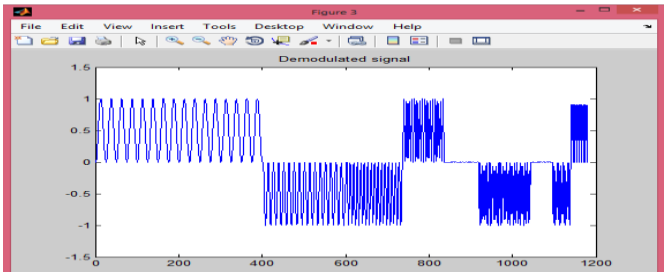


Figure 7 Time domain visualization of demodulated data

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 N users with a time series carrier sequence of 10 frequencies.

C. EMD Model

Empirical Mode Decomposition (EMD) has been introduced by Huang et al. [20] to nonlinear & 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 model signal decomposition is presented in fig 8

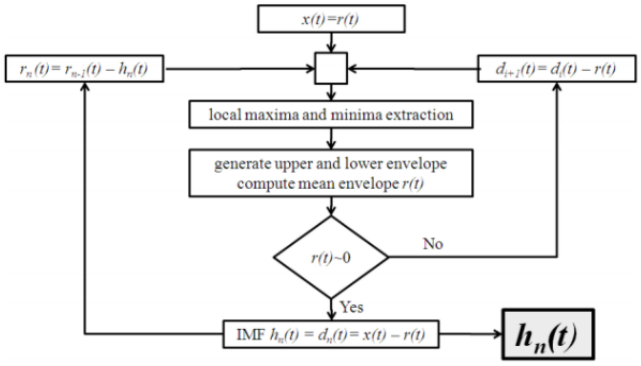


Figure 8 EMD Signal decomposition model

The 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.

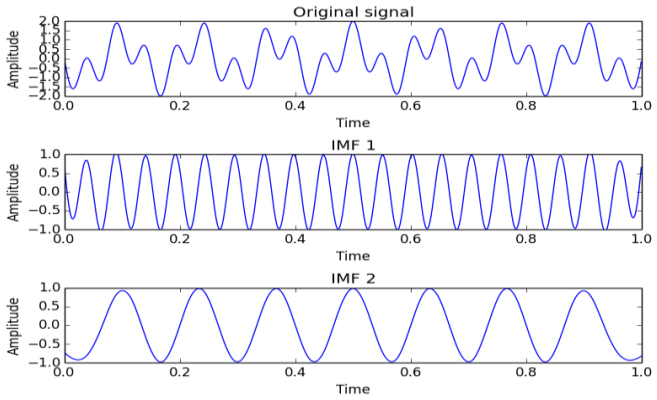


Figure 9 Decomposition of Signals in to 2 IMF Signals

Figure 10 indicates the combined IMF function spectral analysis & plots 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 is obtained which is marked as the primary user's data. The plot in figure 16 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.

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.

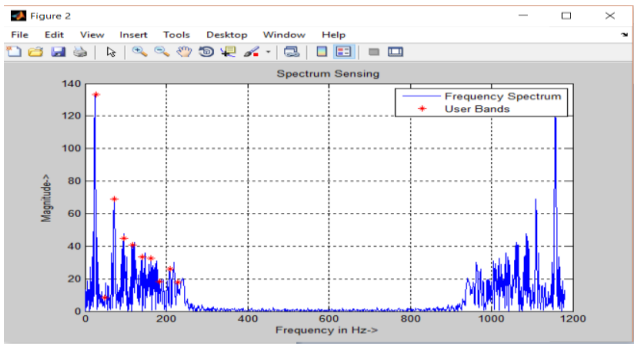


Figure 10 Spectrum Analysis of the IMF function of the transmitted signal at the Base Station

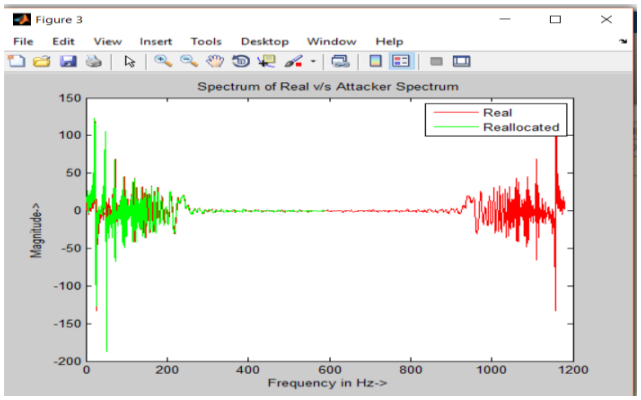


Figure 11 Result signal of Attacker attacking first free band

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 the 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
5. High M Value will Succeed in Emulation
6. Assume that attacker has prior knowledge of Fs
7. Attacker creates carrier as attacker can append only one bit, he will modulate it
8. Now the attacker actually has to mix this signal with actual transmitted signal
9. Way to do it is:
    a) Decompose Modulated Signal to IMF Functions
    b) Take FFT of his IMF signals and combined them in a single spectrum XaF
    c) Take FFT of rec Signal xrXrf
    d) Result Attack Signal xra= ifft(Xaf+Xrf)
10. Now the Emulated signal crosses through channel and is received Defense Appr. against PUE Attacks

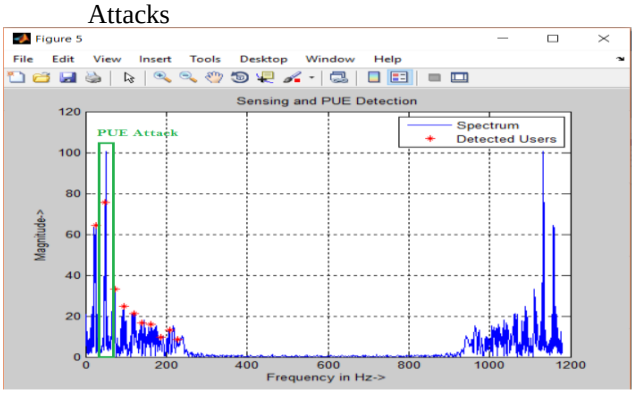


Figure 12 Spectral Analysis at Cognitive Radio Base Station

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. Performance EVALUATION

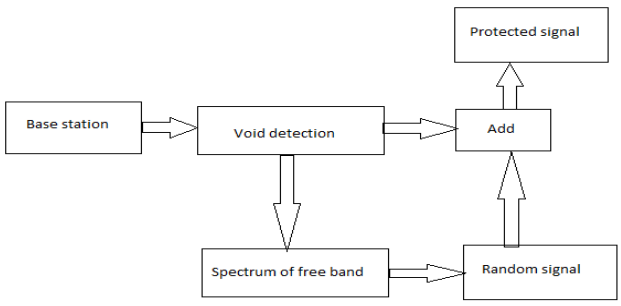
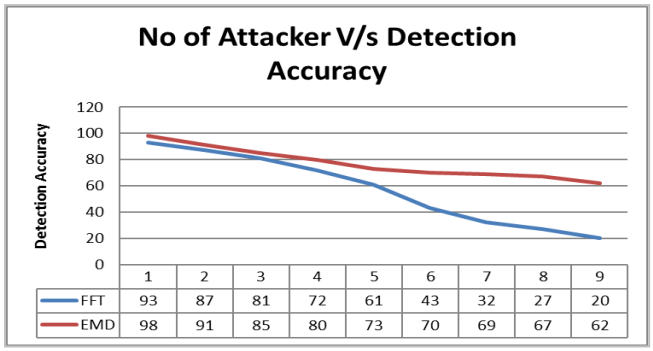


Figure 13 Block diagram of defence against PUE attack

We consider a cognitive radio network with 15 PU's & only 2 users as active PU user. We vary the number of attackers where each of the attackers pretends to be a particular primary user & comparisons as shown in Fig 14 Detection Accuracy. IMF are weighted function. Hence the attacker signals become much more prominent than in FFT analysis.

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 function. Therefore, the attacker signals become much more prominent than in FFT analysis. Performance of Proposed technique described in Fig 15 indicating preventive measure, Signature matching technique introduced, the detection accuracy improves significantly in proposed model.

Figure 14 Technique of FFT verses proposed based Performance Comparison



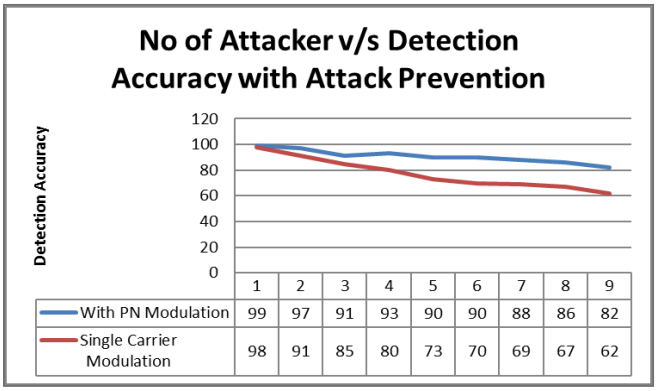


Figure 15 Evaluation of System with & without proposed technique Performance Comparison

IV. CONCLUSION

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. In this paper, one can have proposed a unique PUE attack detection and prevention mechanism by combining EMD method with spectral analysis.

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 11.3 (2016): 609-620.

[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] 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, 2009, 13(2), 74-85

[8] 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, 2013, 3229–3234

[9] Chen R, Park JM, Reed J "Defense against primary user emulation attacks in cognitive radio networks". Selected Areas Commun., IEEE J 2008, 26: 25-37

[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 BlesaEmail author, Elena Romero, Alba Rozas and Alvaro Araujo "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