Indian Journal of Science and Technology, *Vol 10(1), DOI: 10.17485/ijst/2017/v10i1/110287, January 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Primary user Emulation Attack Defense in Filter Bank based Cognitive Radio

Sabiq P.V.* and D. Saraswady

Department of ECE, Pondicherry Engineering College, Puducherry, India; sabiqpv@pec.edu, dsaraswady@pec.edu

Abstract

Background/Objectives: The spectrum scarcity problem arising due to reckless development in wireless communication can be addressed using cognitive radio technology. An important step in cognitive radio technology is spectrum sensing and associated with that is an attack called primary user emulation attack. **Methods/Statistical Analysis**: A two channel Quadrature Mirror Filter (QMF) bank is employed for a single user spectrum sensing. The energy detection method is used as reference for comparing the performance of the filter bank method in the presence of attackers. Existing approaches like Neyman-Pearson Criterion, Improved Detection Scheme with Double threshold and Location Verification Method for detecting PUE attacks were examined. A new method which combines improved detection scheme and location verification method is proposed for detecting PUE attacks. **Findings**: The simulation result shows that the filter bank method shows better performance than the energy detection method in the presence of attackers. The probability of detection of PUE attacks using improved detection scheme and location verification method for the filter bank method and energy detection method was analyzed and found out that the filter bank based spectrum sensing method outperforms energy detection method. By incorporating AND rule logic, OR rule logic and Alternate logic approach into the filter bank spectrum sensing technique, the probability of detection of PUE attack was investigated and it is seen that the probability of detection has increased to 0.98 in FB method at SNR = 1 dB when employing an alternate approach. **Application/Improvements:** The feasibility of deploying the filter bank method integrated with the alternate logic is to be tested using Universal Software Radio Peripheral (USRP) module.

Keywords: Double Threshold, Filter Bank, Fusion Logic, Primary User Emulation Attack, Spectrum Sensing

1. Introduction

The whole world is now moving towards wireless. Almost everything we touch, every aspect of our lives nowadays, has a wireless component to it. This wireless technology has become the most stimulating areas of telecommunications and networking. As a result, there arises the problem of spectrum scarcity. In order to tackle this issue, CR network was proposed as a technology to access the spectrum in an effective and adaptable manner so as to increase spectral efficiency. A CR network consists of PU's and SU's, where SU's are allowed to access the frequency bands allotted to PU's without upsetting them in an opportunistic manner[1]. There are four main functions in CR – spectrum sensing, spectrum management, spectrum mobility and spectrum sharing. Among the four functions, spectrum sensing is the foremost step taken to identify the white spaces. CR nodes opportunistically engage these white spaces by operating across them without interfering with the PU's. The SU's has to vacate the occupied band when the PU begins to transmit across this frequency band. All SU's has equal right to access unoccupied band when there is no active PU communication.

The SU will act as MU by modifying the air interface, thereby mimic the PU's characteristic and gets the same privilege as the PU. Therefore, the SU's has to vacate the occupied band for the MU trusting that it is a PU. Hence, the MU gets unequaled access to the PU's band. This kind of attack against CR networks is called as PUE attacks. PUE attacks are unique to CR networks in which

**Author for correspondence*

the intimidating user takes the advantage of the integral decorum in CR networks so that the authentic SU has to evacuate the spectrum band. The presence of PUE attack may severely affect the performance of CR networks. The consequence of PUE attacks is band width waste, QoS degradation, connection unreliability, denial of service and interference with the primary user. A PUE attack can happen while the spectrum sensing is performed by using cyclostationary, energy, matched filter or FB detection method. In this work, a FB based detection method is employed as it is considered as an optimum waveform for the 5G system[2]. An Improved Energy Detection Scheme based on Channel Estimation and implementation of energy detection scheme was discussed[3,4]. Similarly Filter Bank Multicarrier (FBMC) can be used as an integrated tool for data communication as well as channel sensing. An illustration of the launching of a PUE attack on CR network is shown in Figure 1.

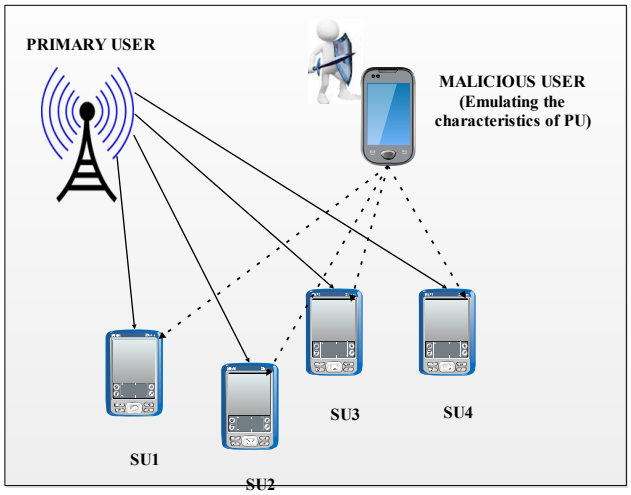

Figure 1. Illustration of PUE attack launching scenario.

In[5], the author have incorporated authentication scheme to combat a PUE attack against CR users. A hybrid machine learning method for malicious activity or policy violations in a network was proposed[6]. The author proposes a new mechanism based on physical layer network coding to detect the emulators[7]. In[8], a PUE attack on ED method using Neyman –Pearson composite hypothesis test was discussed. A survey on security aspects in software defined radio and CR Networks was elaborated[9,10]. In[11], the author proposes an approach that estimates the attack strength and innovatively applies in a Neyman-Pearson or likelihood ratio test to improve collaborative sensing performance. In[12], authors has focused on Cooperative Spectrum Sensing (CSS) for double threshold improved energy detector. The vulnerabilities present in CR, attack classifications and their effect on the working of cognitive radio network are discussed[13]. A threat detection technique based on localization of primary signal was proposed[14]. The inclusion of fusion logic into cooperative spectrum sensing was discussed[15].

The paper is organized as follows. In section 2, the basics of the FB based detection method are presented. The system model for PUE attack to frame the problem is discussed in section 3. The section 4 gives the existing approaches for PUE attacks. In section 5, a new approach for defending PUE attack in CR network is proposed. In section 6, the simulation results and discussion are provided, while section 7 concludes the paper.

2. Filter Bank based Detection Method

The basic building blocks for Multirate signal processing are decimation and interpolation[16]. The process of reducing the sampling rate by an integer factor M is called decimation. The process of increasing the sampling rate by an integer factor L is called interpolation. The down sampling process and up sampling process is shown in Figure 2(a) and 2(b). The filter bank is set of band pass filters with either a common input or a summed output. The decomposition and reconstruction process is called the analysis filter bank and synthesis filter bank. Three basic operations are used in filter banks: linear filter, down sampling and upsampling. The function of spectrum sensing can be performed using an analysis filter bank. A M-band analysis filter bank is shown in Figure 2(c). The analysis filter bank is used to decompose the input signal into a set of subband signal, where each subband occupies a portion of the original frequency band. A two channel Quadrature Mirror Filter (QMF) bank is adequate for a single user spectrum sensing. A block diagram of spectrum sensing based on the analysis filter bank under single user scenario is shown in figure 3.The signal received from the PU is divided into two subbands and filtered using low pass and high pass filter with equal pass band respectively, and are down sampled to reduce the sample rate by an integer M. The total energy of the down sampled subband signals is added and compared with the predefined threshold to find whether PU is present or not.

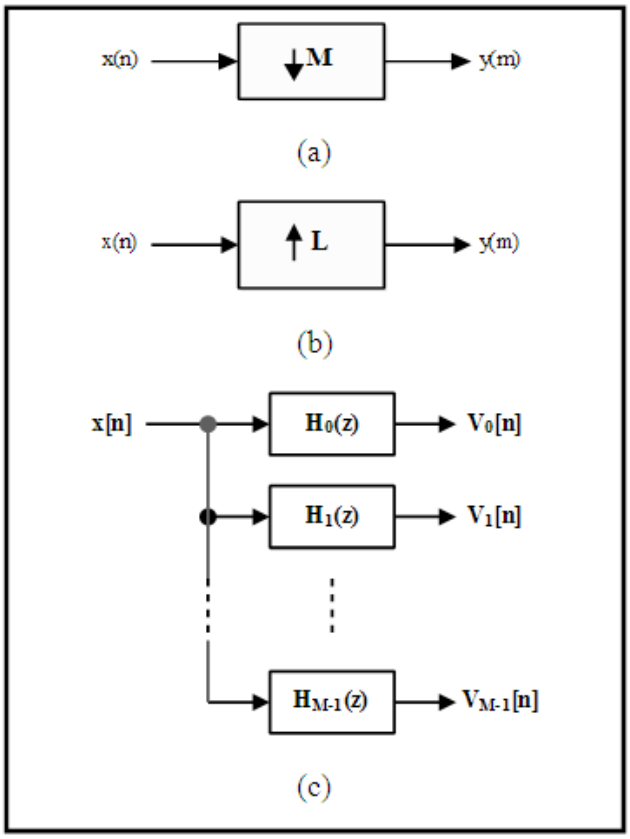

Figure 2. (a) Down sampling Process (b) Up sampling Process (c) M-band analysis filter bank.

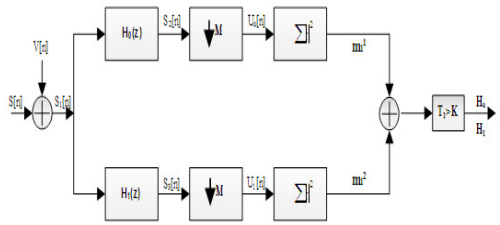

Figure 3. Analysis filter bank based spectrum sensing for a single user.

The entire process involved in FB based spectrum sensing is summed in equation (1)

$$m_1^1 = \sum_{n=1}^{N/2} |U_0[n]|^2$$

$$m_1^2 = \sum_{N/2}^{N} |U_1[n]|^2 \quad (1)$$

$$T_1 = m_1^1 + m_1^2$$

$$k = (Q^{-1}(P_f)/\sqrt{L}) + 1$$

3. System Model For PUE Attack Detection

A system model for analyzing the PUE attacks is as shown in Figure 4 (a). The malicious and SU's is confined to a circular area of radius R. The PU's and SU's are separated by a distance of atleast d_p. For PU detection, the method deployed for spectrum sensing is a FB based detection method. In the FB based detection method, the total energy of the down sampled subband signals is calculated and matched with the predefined threshold to find whether PU is present or not. The coordinates of the entire MU are transformed in such a way that the SU of interest lies at the origin as shown in Figure 4 (b).

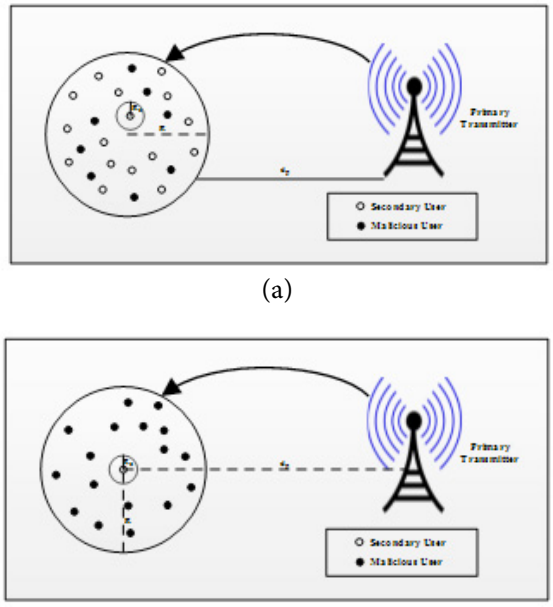

Figure 4. (a) A CRN with SU's and MU's in a circular grid of radius R (b) Coordinates of SU and MU are transformed.

This is because the probability of PUE attack on to any user in the network is the same as there is no support between SU's. Hence, here the Probability Density Function (PDF) of the signal received from one SU only is analyzed. The primary transmitter coordinates are transformed as (d_p, θ_p). The MU's are present uniformly in an annular Region (R_0, R).The amount of power received due to the transmission from PU at the SU, $P_r^{(p)}$ can be obtained as:

$$P_r^{(p)} = P_t d_p^{-2} G_p^2 \quad (2)$$

$G_p^2 = 10^{\frac{\varepsilon_p}{10}}$, is taken as shadowing from the transmitter at the SU with a mean of 0 and variance σ_p^2 and $\varepsilon_p \sim N(0,\sigma_p^2)$.

The PDF of the received power is calculated as

$$P^{(\ )}(\ ) = \frac{}{\sigma\sqrt{\pi\gamma}} \exp\left\{-\frac{(10\log_{10}\gamma \quad \mu)}{}\right\} \tag{3}$$

Where

γ is the random variable,

$$A = \frac{\ln 10}{10} \text{ and}$$

$$\mu_p = 10\log_{10} P_t - 20\log_{10} d_p$$

The amount of power received at the secondary node due to the transmissions from all m MU's is calculated as

$$P_r^{(m)} = \sum_{j=1}^{M} p_m d_j^{-4} G_j^2 \tag{4}$$

Where d_j - the distance between SU and j^{th} MU.

G_j^2 - the shadowing between SU and j^{th} MU,

$G_j^2 = 10^{\frac{\varepsilon_j}{10}}$ where $\varepsilon_j \sim N(0,\sigma_m^2)$.

The PDF of received power is calculated as

$$P^{(m)}(x) = \frac{1}{Ax\sigma_x\sqrt{2\pi}} \exp\left\{-\frac{(10\log_{10} x - \mu_x)^2}{2\sigma_x^2}\right\} \tag{5}$$

Where $\acute{o}_x^2 = \frac{1}{A^2}\left(\ln E\left[(p_r^{(m)})^2\right] - 2\ln E\left[(p_r^{(m)})\right]\right)$

$$\mu_x = \frac{1}{A}\left(2\ln E\left[p_r^{(m)}\right] - \frac{1}{2}\ln E\left[(p_r^{(m)})^2\right]\right)$$

4. Existing Approaches for PUE Attack

In CR network, prevention of PUE attack is vital. Hence the detection techniques have to verify the truthfulness of PU signal. The approach to detect PUE attack depends on individual or combined Received Signal Strength (RSS) measurements. The following defense techniques exist for PUE Attack mitigation.

4.1 Neyman-Pearson Criterion

To analyze the impact of the PUE attacks on CR network, Neyman Pearson composite hypothesis testing mathematical model are used. In this method, the PDF of the received signal due to transmission by the primary and the MU at the SU is calculated. In order to calculate the decision variable, the power of the signal received from the source is measured and is given by the ratio term, ∧

$$\Lambda = \frac{P^{(m)}(x)}{P_t^{(m)}(\gamma)} \tag{6}$$

Where, $P^{(m)}(x)$ is the received power from the MU calculated using (5) and $P_r^{(p)}(\gamma)$ is the received power from the primary transmitter calculated using (3).

The ratio term is then compared with predefined threshold and from that the SU decides the following

$\Lambda \le \lambda$: D_1: Primary user transmission is taking place

$\Lambda \ge \lambda$: D_2: PUE Attack is in progress

There can be two possibilities

- The SU may take the decision D_2 when M_1 is true.
- The SU may take the decision D_1 when M_2 is true.

The errors associated with this probability are termed as

Missed Probability: $P\{D_2|M_1\}$ = Probability of taking decision as D2 when the hypothesis M_1 is true.

False Alarm Probability: $P\{D_1|M_2\}$ = Probability of taking decision as D_1 when the hypothesis M_2 is true.

4.2 Improved Detection Scheme with Double Threshold

By using a conventional FB method which uses single threshold value, it is difficult to differentiate between PU signal and PUE attacker. The power level of the signal received at the SU receiver is measured. Then it is compared with that from the true PUs in order for a CR network to decide whether the signal originates from an attacker or not. The test statistics in the case of FB method is calculated as

$$Y = \sum_{n=1}^{N} |x(n)|^2 \tag{7}$$

However, a FB detector is not dynamic enough to challenge an advanced PUE attack. Hence, by using a double threshold value called improved detection scheme is employed. The conditions which are used to differentiate between PU and PUE attacker is given as follows.

Test statistics < Threshold1, only noise

Threshold1< Test statistics < Threshold2, Primary user

Test statistics > Threshold2 PUE Attacks

In order to distinguish a PUE attacker from a real PU, an improved detection scheme with two energy thresholds, denoted by λ_1 and λ_2 are used. Here, $\lambda 1 < \lambda_2$ and λ_1 is the earlier threshold in a conventional FB method. When the received signal energy, $E < \lambda_1$, then it is said that there is no PU or PUE attacker. If the signal energy is between the two threshold λ_1 and λ_2, then there is presence of PU. When the signal energy is above λ_2, then it indicates PUE attack.

4.3 Location Verification Method

Location verification is another defense technique which is used to distinguish PU and PUE attacker based on the distance. There are two location verification schemes - Distance Ratio Test and Distance Difference Test. To perform the analysis some assumptions are considered. The assumptions are,

- All users should broadcast information regarding their location.
- All the users have a predefined transmit power level and are known to each other. A ground reflection model is used for calculating the power level of the received signal. The received power level is given by equation (8).

$$P_r = P_t G_t G_r \frac{h_t^2 h_r^2}{d_2^4 L} \quad (8)$$

Where,

P_t =Transmit power level,

h_t = Height of a transmitter

h_r = Height of a receiver

G_t = Transmitter antenna gain

G_r = Receiver antenna gain

L = System loss factor

d = Distance between transmitter and receiver

Here, the distance between a SU and other users is calculated based on the coordinates location and received power level. The user is a truthful user, when the distance calculated from both these technique matches. Otherwise, it is a malicious user.

4.3.1 Distance Estimate based on Location Coordinates

The distance between the users can be calculated based on the location coordinates. Let us assume (x, y) is x and y coordinates of a SU and (x1,y1) is x and y coordinates of an existing primary transmitter. The distance between them d, is given as

$$d_1 = \sqrt{(x - x_1)^2 + (y - y_1)^2} \quad (9)$$

The simulation is performed based on the assumption that the location coordinates of all users are broadcasted. Hence, using eq (9) it is possible to calculate the distance between any users.

4.3.2 Distance Estimate based on Received Power Level

In Received Signal Strength (RSS) approach, the parameter on which the received power level is depended is the transmitting power and distance on the path between two devices. Knowing the transmit power level; it is possible to calculate the distance between users from the measured received power level. Equation (10) gives the received power level, P_r, for a specific transmit power level P_t. Assume h_t, h_r, G_t, G_r and L are constant and equal to one. Therefore, the received power level can be expressed as a function of transmit power level and distance.

$$P_r = \frac{P_t}{d^4} \quad (10)$$

The distance between the user can be approximated based on the received power level and known transmit power level as

$$d = \sqrt[4]{\frac{P_t}{P_r}} \quad (11)$$

If d_1, the distance estimated from location coordinates and d_2, the distance estimated from the received signal power is approximately equal, then it is decided that the signal is from the legitimate PU. Otherwise, a malicious user is in attack. The accuracy of distance calculation will depend on the presence of noise level in the signal received. However, statistically, the distance d_1 and d_2 calculated should come close.

5. Proposed Approach for PUE Attack Detection

The performance of existing method which employs double threshold for FB based spectrum sensing technique to detect the presence of the PU is pitiable at low signal to noise ratio. At the same time the location verification method also gives poor performance at low SNR. In order to detect PU's in the presence of PUE attack, a new method is suggested which combines improved detection scheme and location verification method. This approach is called fusion approach. Hence the probability of detecting the presence of PU can be increased. The malicious user cannot mimic the PUs location coordinates and transmit power level. Therefore, the authenticity of PU signal can be confirmed based on the distance measurement taken out from location coordinates and the signal power level received. Three different combinations are possible by using improved detection method and location verification method. They are discussed below.

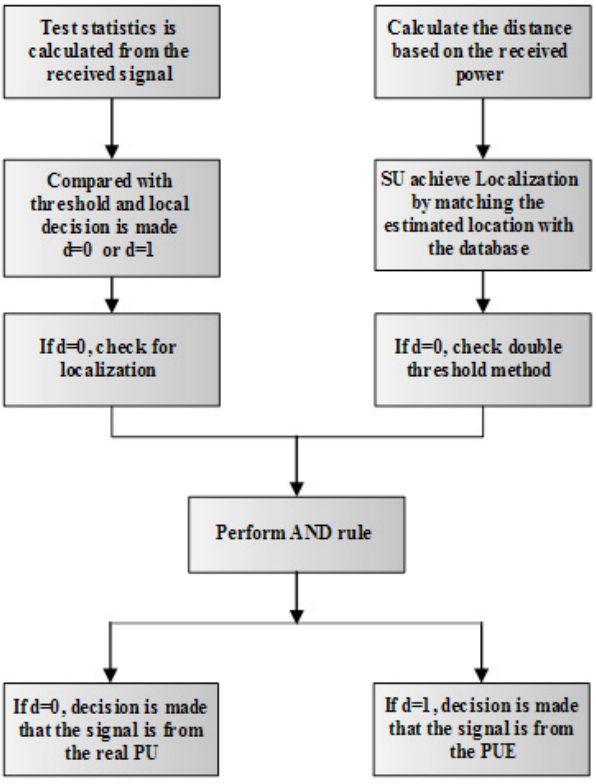

Figure 5. AND rule logic for fusion approach.

5.1 AND Rule Logic

The logic is to perform both improved detection scheme and location verification method simultaneously. If both the method says that the signal is from the attacker then the final decision is made that, it is from the attacker. The flow chart for AND rule logic is as shown in Figure 5.

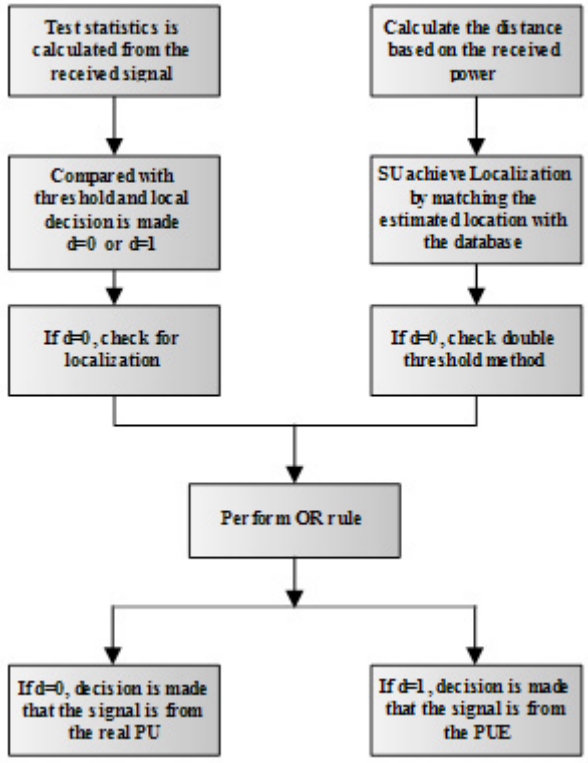

Figure 6. OR rule logic for fusion approach OR Rule Logic.

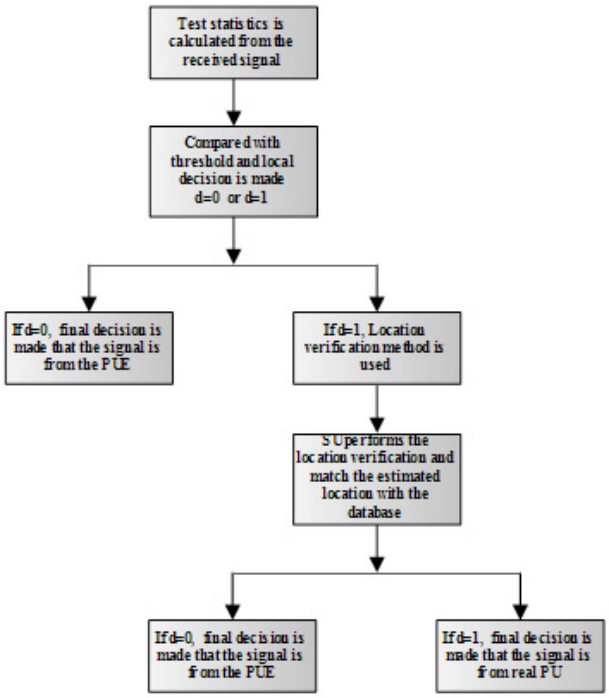

Figure 7. Alternate logic for fusion approach.

5.2 OR Rule Logic

The flowchart for OR rule logic is as shown in Figure 6. Here, both improved detection scheme and location verification method are carried out simultaneously. If any one of the method say that the signal is from the attacker, the final decision is made that the signal is from the attacker.

5.3 Alternate Logic

The improved detection scheme is performed initially and local decision (d) is made. If d = 0, the final decision is made that the signal is from the PUE attacker. Otherwise, it will perform location verification and match the estimated location with the content in the database. Here if d = 0, the final decision is made that the signal is from the PUE attacker. Else the final decision is made that the signal if from real PU. The flow chart for the alternate logic is as shown in Figure 7.

6. Result and Discussions

The proposed method was simulated in Matlab. In order to simulate FB based spectrum sensing method, the values for the system parameters considered are listed in Table 1.

Table 1. Parameters and its value used for simulation

Parameter	Type/Value
Modulation	BPSK
Order of filter	99
Pass band edge for LPF	0.45
Pass band edge for HPF	0.55

The values of system parameters considered for simulating PUE attacks in CR network is listed in Table 2.

Table 2. Parameters and its values used for simulating PUE attacks

Message signal	Analog: Sin(pi*t/2)
	Digital: 1 1 0 1 1 0 0 1 1 0
Channel	AWGN
Number of samples	10
SNR	-5:1:5
Threshold1	15.98
Threshold2	50
R_o	300meter
R	1000meter
P_t	100KW
P_m	400W
d_p	10Km
σ_p	8dB
σ_m	5.5dB
Testing times	10000
No. of MU	10

It is difficult to differentiate between PU signal and PUE attacker when a conventional FB method with single threshold value is used. Therefore, an improved detection scheme which uses a double threshold value is employed in order to detect PUE attackers.

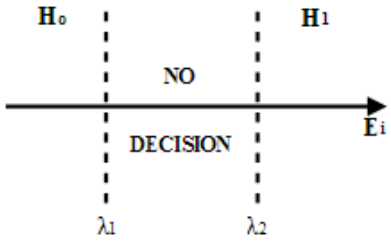

Figure 8. Double threshold detection.

Two threshold values are used instead of a single threshold to make local decision in the double threshold FB method. Double threshold FB offers a benefit over conventional FB with respect to bandwidth. The threshold1 value is calculated using equation (1) and threshold 2 is decided such that the difference between thresholds is minimum or no decision region shown in Figure 8 should be less.

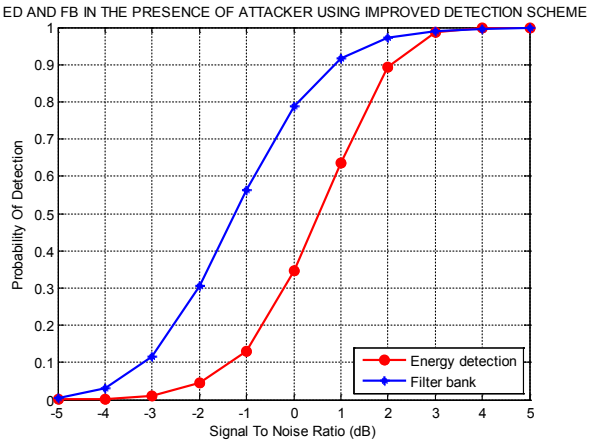

Figure 9. Comparison of ED and FB method using improved

detection scheme.

For the reference purpose, ED method is used in order to compare the performance of the FB method in the presence of attackers. Figure 9 shows the comparison between ED method and FB method in the presence of a PUE attacker using improved detection scheme. The FB method shows better performance than the ED method. The probability of correctly detecting the presence of the attacker using the location verification method is shown Figure 10. This method works only, when the distance coordinates and the transmit power of the primary transmitter is known to all the users.

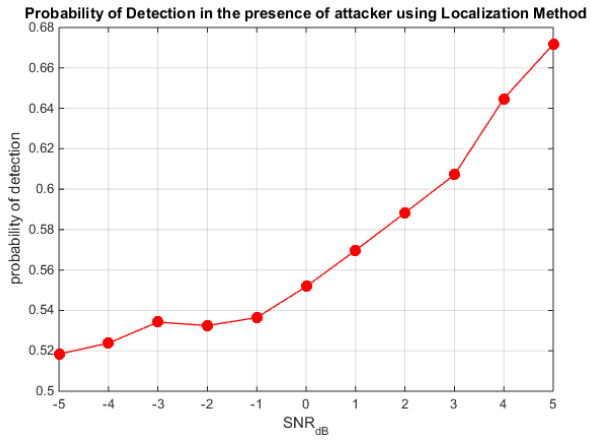

Figure 10. Probability of detection in the presence of an attacker using location verification method.

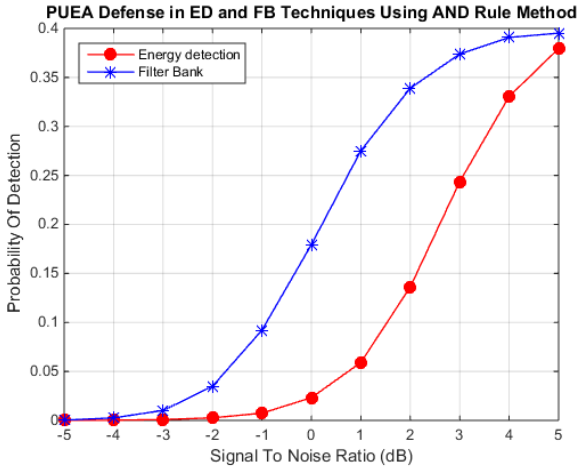

Figure 11. PUEA defense in ED and FB techniques using AND rule logic.

The performance of the improved detection scheme and location verification method is poor in low signal to noise ratio values. So by combining the improved detection scheme with the location verification method the probability of detecting the presence of the PU in the presence of the attacker can be increased. There exist three different combinations when we fuse these two methods. The probability of detection versus SNR using ED method and FB method in the presence of attackers incorporating AND rule logic is plotted in figure 11. It basically illustrates how well the AND logic rule, introduce a better defense technique towards PUE attacks. Also, it explains that the FB technique along with AND rule logic works jointly to demolish PUE attacks better than ED technique.

The final decision of PUE attack is made when any one of the method says that the signal is from PUE attacker and this is called OR rule logic. OR rule logic was performed for both ED and FB method and it was found that again FB method has a better probability of detection in the presence of attackers. Figure 12 shows the PUE attack defense in the ED and FB techniques using OR Rule Logic. Comparing Figure 11 and Figure 12, it is shown that the employment of OR Rule logic introduce better probability of detection at respective SNR. For example, at SNR = 1 dB, the probability of detection of FB method is 0.28 when incorporating AND rule logic and it is 0.5 when incorporating OR rule logic. The percentage increase in probability of detection of a PU signal in the presence of PUE attacks is 78.6.

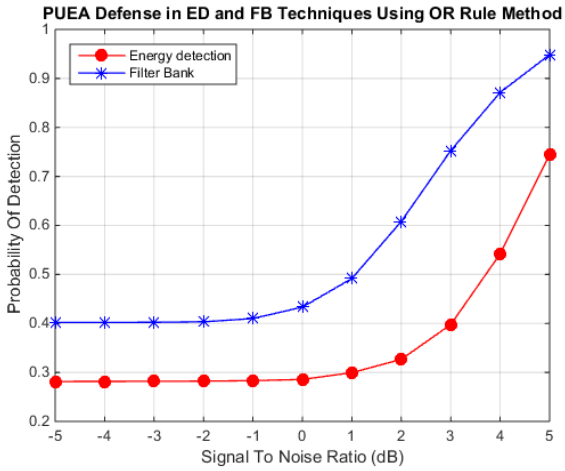

Figure 12. PUEA defense in ED and FB techniques using OR rule logic.

As stated earlier, an alternate approach for defending PUE attack is to perform improved detection scheme at first and decide the presence of attacker based on the out-

come. If unable to decide the presence of the attacker, then go for location verification method and make the final decision on the presence of PUE attacks. Using alternate logic the performance of ED method and FB method in the presence attackers is shown in Figure 13. Again the FB method is having better performance than ED method. The probability of detection has increased to 0.98 in FB method at SNR = 1dB.

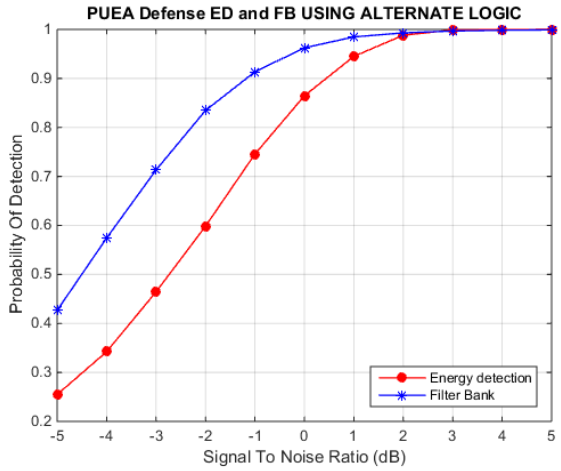

Figure 13. PUEA Defense in ED and FB method using alternate logic.

A comparison of different defense techniques discussed in this paper is examined for FB method alone and a graph between probability of detection versus SNR is plotted as shown in figure 14. By employing alternate logic there is a better probability of detection in the presence of attackers. Hence, by integrating alternate logic with FB method we can shield PUE attacks in a CR network.

A numerical comparison between ED method and FB method when integrating different defense techniques is enumerated in Table 3. The table highlights the probability of detection versus SNR for different defense techniques. From the table it shows that FB method integrated with alternate logic will yield better probability of detection when compared to other combination. For example, at SNR = 1 dB, the increase in probability of detection when integrating FB method with improved detection and alternate logic is 0.75. Similarly, at SNR = 5 dB, the increase in probability of detection is 0.1.

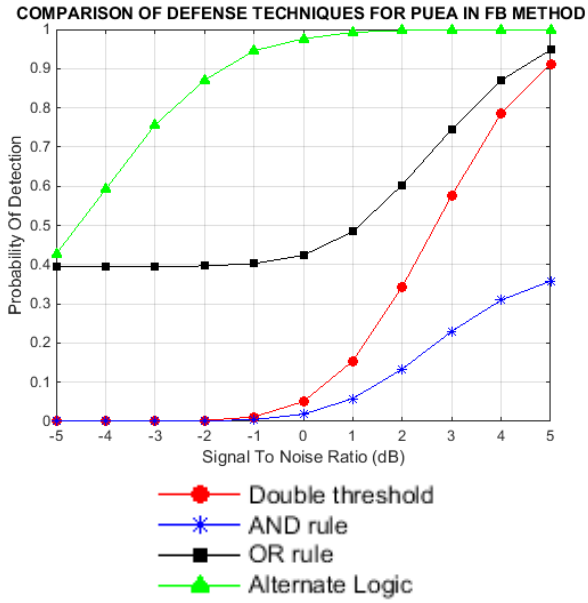

Figure 14. Comparison of different defense techniques for PUEA in FB method.

It also states that the FB method produces a better probability of detection at low SNR when compared to ED method. Hence FB method integrated with the alternate logic can be deployed in CR network for shielding PUE attacks.

7. Conclusions and Future Work

In this work, PUE attacks on a CR network are studied. The spectrum sensing techniques employed here is ED method and FB method. Firstly, a double threshold scheme was integrated with each spectrum sensing

Table 3. Comparison of ED method and FB method by integrating different defense techniques

Method	ED Method				FB Method			
	P_d				P_d			
SNR	-5 dB	-1 dB	1 dB	5 dB	-5 dB	-1 dB	1 dB	5 dB
Improved Detection	0	0.01	0.1	0.8	0	0.04	0.2	0.9
AND Rule Logic	0	0.01	0.06	0.37	0	0.1	0.27	0.4
OR Rule Logic	0.39	0.4	0.42	0.76	0.38	0.4	0.5	0.95
Alternate Logic	0.3	0.75	0.9	0.97	0.42	0.9	0.98	1

method to defend the presence of PUE attacks. Later a new approach of fusing both location verification method and double threshold scheme were introduced to protect the CRN system from PUE attack. This scheme shows a tremendous improvement in probability of detection in the presence of attackers. Therefore, FB method integrated with the alternate logic can be utilized in CR network for preventing PUE attacks. The future work includes setting up a hardware module using Universal Software Radio Peripheral (USRP) to test the feasibility of the proposed method to defense PUE attack.

Nomenclature

ED	Energy Detection
FB	Filter Bank
PU	Primary User
SU	Secondary User
CR	Cognitive Radio
PUE	Primary User Emulation
MU	Malicious User
P_t	PU transmitting Power
P_m	MU transmitting Power
d_p	Distance between the primary user& other users
R	Circular grid radius
σ_p^2, σ_m^2	Variance of Primary & MU's

8. References

1. Haykin S. Cognitive radio: Brain-empowered wireless communications. IEEE Journal on Selected Areas in Communication. 2005; 23(2):201-20.
2. Farhang-Boroujeny B. Filter bank multicarrier modulation: A waveform candidate for 5G and beyond. Advances in Electrical Engineering. 2014; 482805:1-25.
3. Divyapraba V, Kishore Kumar K, Pratheepa R, Elamaran V. Spectrum sensing based on energy detection using MATLAB_Simulink. Indian Journal of Science and Technology. 2015 Nov; 8(29):1-5.
4. Amanpreet K, Dishant K. An improved energy detection scheme based on channel estimation. Indian Journal of Science and Technology. 2016 Oct; 9(37):1-6.
5. Avila J, Thenmozhi K. Authentication scheme to combat primary user emulation attack against cognitive radio users. Security Communication Networks. 2015; 8(18):4242–53.
6. Hemati HR, Ghasemzadeh M. Meinel C. A hybrid machine learning method for intrusion detection. IJE Transactions C: Aspects. 2016 Sept; 29(9):1242-6.
7. Xie X, Wang W. Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding. Journal of Ubiquitous Systems and Pervasive Networks. 2015; 5(1):01-8.
8. Orumwense E, Oyerinde O, Mneney SH. Impact of primary user emulation attacks on cognitive radio networks. International Journal on Communications Antenna and Propagation. 2014 Feb; 4(1):19-26.
9. Marinho J, Granjal J, Monteiro E. A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. EURASIP Journal on Information Security. 2015 Dec; (4):1-14.
10. Baldini G, Sturman T, Biswas AR, Leschhorn R, Godor G, Street M. Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead. IEEE Communications Surveys and Tutorials. 2012; 14(2):355-79.
11. Sharifi AA, Sharifi M, Niya MJM. Collaborative spectrum sensing under primary user emulation attack in cognitive radio networks. IETE Journal of Research. 2015 Sept; 62(2):205-11.
12. Sanket S. Kalamkar, Adrish Banerjee. Improved double threshold energy detection for cooperative spectrum sensing in cognitive radio. Defense Science Journal. 2013 Jan; 63(1):34-40.
13. Leon O, Hernandez-Serrano J, Soriano M. Securing cognitive radio networks. International Journal of Communication System. 2010 Feb; 23(5):633–52.
14. Ammar M, Riley N, Mehdawi M, Fanan A, Zolfaghari M. Detection threats and mitigation techniques in cognitive radio based on localization of signal source and trust worthiness. Proceedings of 4th ICAESAM; Malaysia. 2015. p. 77-83.
15. Hossain E, Bhargava V. Wireless Communications Networks. Springer Publication; 2007.
16. Vaidyanathan PP. Multirate systems and filter banks. Pearson Education; 1993.