www.ioirp.com

International Journal of Innovative Research in Technology, Science & Engineering (IJIRTSE)
ISSN: 2395-5619, Volume – 1, Issue – 10. December 2015

A Robust Spectrum Sensing in Cognitive Radio Networks in the Presence of Malicious Attack

Dr.R.Suresh Babu M.E.,M.B.A.,Ph.D.,
Head of the Department, ECE
Kamaraj College of Engineering and
Virudhunagar

A. Maria Lavanya
PG Scholar, Department of ECE
Kamaraj College of Engineering and
Virudhunagar
14pcnw10@kamarajengg.edu.in

***Abstract*— In this paper to propose an approach for detecting the presence of malicious attack which is commonly known as primary user emulation attack (PUEA), this type of attack act as the primary signal and delude the secondary user and occupy the whole frequency spectrum. The PUE attack sends fake signal similar to the primary signal in which it aware of whole spectrum. Then the cooperative spectrum sensing (CSS) OR rule is applied in cognitive radio network and spectrum sensing is based on energy detection scheme. The proposed method is well suitable for AWGN environment which minimize the error.**

Keywords*— cooperative spectrum sensing, cognitive radio, primary user emulation attack, malicious attak.

I. INTRODUCTION (*HEADING 1*)

Cognitive radio [1] is mainly used for improving the radio Spectrum . Spectrum sensing in cognitive radio is to gather information about the spectrum status . Cognitive radio consists of two users they are primary users are said to be licensed users and has license to operate the desired frequency band which is controlled by the primary base station. secondary users are said to be unlicensed users or cognitive radio users (CR) in Cooperative Spectrum Sensing (CSS) [2] environment and has no license spectrum. The secondary network is controlled by the xG base station. The CR users can utilize the frequency bands of primary users when the primary users are not present. Therefore the secondary users sense the band of primary user whether it is occupied or not. In case the primary user occurs then the secondary user should handoff the Spectrum to the primary user.

In cognitive radio the spectrum holes gives information about the available unused spectrum and this spectrum holes depends on three phases in cognitive cycle as spectrum detection, sensing and mobility. The cognitive radio analyse the data rate, the transmission mode, and the bandwidth of the transmission. Depending upon these parameter the appropriate spectrum is chosen according to the user requirements. The ultimate objective of the cognitive radio is to obtain the best available spectrum through cognitive capability and reconfigurability as described before. Since most of the spectrum is already assigned, the most important challenge is to share the licensed spectrum without interfering with the transmission of other licensed users as illustrated in Figure 1.The cognitive radio enables the usage of temporally unused spectrum, which is referred to as spectrum hole or white space. If this band is further used by a licensed user, the cognitive radio moves to another spectrum hole or stays in the same band, altering its transmission power level or modulation scheme to avoid interference. Here the technique used is cooperative spectrum sensing in which it deals with finding accurate detection of primary signal by multiple CR.

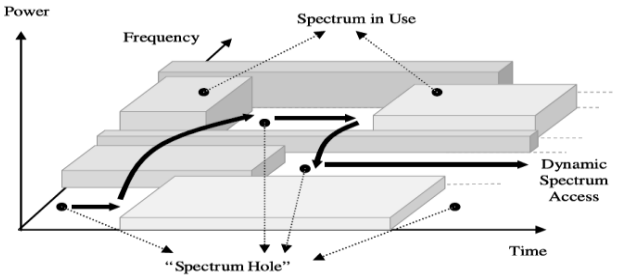

Fig. 1. Spectrum hole concepts.

. There are some attacks present in the cognitive radio [3] network which leads to degrades in system performance and one of the attack is Primary User Emulation Attack (PUEA) and the system model of PUE attack is shown in the Fig.2 . This PUEA attack acts like a primary user and keep on sensing the spectrum of primary user and does not allow the CR user to occupy the spectrum of PU .

The PUEA attack sends the fake signals to the secondary user to vacate the band of PU [3,4]. There are several technique have been used to defeat the PUEA attack. The PUEA attack is represented as 'always present attack' [8] and the action of this attack is to keep on sensing the spectrum like CR and able to differentiate the occupied and unoccupied spectrum band. And there by using the CSS rules in CR networks known as logical data function rules of OR rule in the presence of attack. The local spectrum sensing method is used by the CR networks and hard decision of PU activity is taken by the CR. The hard decision is send to fusion center (FC).The FC takes the decision based OR rule depends on the present and absent of the primary user.

This paper explain the effect of PUEA attack, the fake signal in the presence of primary user is assumed to be zero [9] and it occupies the frequency band when the primary user was absent. Therefore the PUEA attacker perform a kind of spectrum sensing. We derived the rules and new result and conclusions [9] are obtained for various channel the rest of the paper deals with spectrum sensing in CR by energy detection technique by OR fusion rule, energy detection technique in the present of PUEA attack.

.

II. SYSTEM MODEL

The system model consists of CR networks with N number of CR users. The attacker sends the fake signal to PU and deceives the secondary user in cognitive radio network. Let $\sqrt{P_P}S_P^k$ be the signal transmitted by PU, where $\sqrt{P_P}$ is power coefficient and S_p is assumed to be independently and identically distributed (i.i.d) complex Gaussian random variable with zero mean and a constant known variance σ_p^2. Then the primary user emulation attack also sends the fake signal $\sqrt{P_E}S_E^k$ where $\sqrt{P_E}$ is the power coefficient of attacker and S_E is assumed to (i.i.d) Gaussian random variable with zero mean and variance σ_E^2.

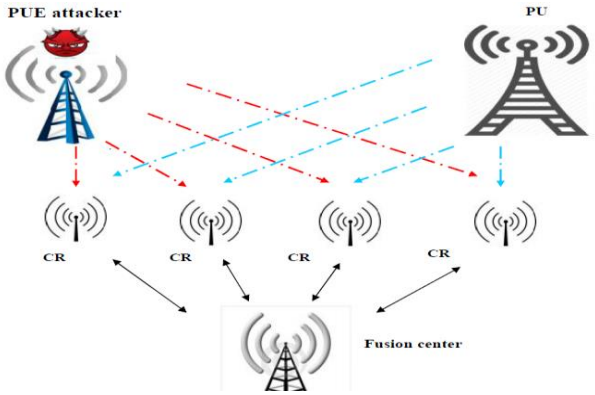

Fig. 2. System model for PUE attack

Then the output signal received at the i^{th} CR user in k^{th} time instant. The presence and absence of the primary signal is indicated by H_1 and H_0 respectively and also the presence and absence of the attacker signal is represented by E_0 and E_1. Depending on the presence and absence of the PU and PUEA in our method, there would be four possible cases to express the received signal at the i^{th} CR users as:{ E_1, H_1 },{ E_0, H_1 },{ $E_1., H_0$ },{ E_0, H_0 }.

$$y_i^k = \begin{cases} \sqrt{P_P} S_P^k h_{P,i}^k + \sqrt{P_E} S_E^k h_{E,i}^k + n_i^k, & under(E_1, H_1) \\ \sqrt{P_P} S_P^k h_{P,i}^k + n_i^k, & under(E_0, H_1) \\ \sqrt{P_E} S_E^k h_{E,i}^k + n_i^k, & under(E_1, H_0) \\ n_i^k, & under(E_0, H_0) \end{cases} \quad (1)$$

where n_i^k is the additive white Gaussian noise at the i^{th} CR user with zero mean and variance $\sigma_{n,i}^2$ and $h_{p,i}^2$ is channel gain between PU and i^{th} CR user at the k^{th} time instant, the channel coefficients are assumed constant in every detection cycle.

A. Spectrum sensing using decision rule in presence of PUEA

In this section, the spectrum sensing includes the presence of PUEA attack and sends the fake signals to the primary user and deceives the secondary users. The number of secondary users made local decision of presence of primary user in cooperative spectrum sensing environment. The fusion center made the global decision based on the decision rule. In the OR decision rule, the FC gives decision 1(primary user present) if any one of the decisions from the cognitive radios is 1. By using this rule, the probability of false alarm increases, meanwhile the probability of detection is reduced. Probability of detection is represented by P_{det}^i and the probability of false alarm is represented by P_{fal}^i for OR rules of i^{th} CR users.

The P_{det}^i and P_{fal}^i in spectrum sensing in the presence and absence of PUEA attack along with the primary signal be defined by

$$P_d^i = p(D_1^i \mid E_0, H_1)p(E_0 \mid H_1) + p(D_1^i \mid E_1, H_1)p(E_1 \mid H_1) \quad (2)$$

$$P_f^i = p(D_1^i \mid E_0, H_0)p(E_0 \mid H_0) + p(D_1^i \mid E_1, H_0)p(E_1 \mid H_0) \quad (3)$$

Note that $p(E_0|H_1)$, $p(E_1|H_1)$, $p(E_1|H_0)$ and $p(E_0|H_0)$ are conditional probabilities regarding to the presence and absence of PUEA and PU signals and this condition probabilities have constant known values and defined by

$$p(E_1 \mid H_1) = \alpha \quad (4)$$

$$p(E_0 \mid H_1) = 1 - p(E_1 \mid H_1) = 1 - \alpha \quad (5)$$

$$p(E_1 \mid H_0) = \beta \quad (6)$$

$$p(E_0 \mid H_0) = 1 - p(E_1 \mid H_0) = 1 - \beta \quad (7)$$

Therefore the equation (1) and (2) can be rewrite as

$$P_{\text{det}}^i = p(D_1^i / E_1, H_1)\alpha + p(D_1^i / E_0, H_1)(1-\alpha) \quad (8)$$

$$P_{fal}^i = p(D_1^i / E_1, H_0)\beta + p(D_1^i / E_0, H_0)(1-\beta) \quad (9)$$

International Journal of Innovative Research in Technology, Science & Engineering (IJIRTSE)
ISSN: 2395-5619, Volume – 1, Issue – 10. December 2015

In OR fusion center rule, the global detection probability (P_d^{OR}), global false alarm probability (P_f^{OR}) and missed detection probability (P_{mis}^{OR}) [10] can be expressed as

$$P_{\text{det}}^{OR} = 1 - \prod_{i=1}^{N} (1 - p_{\text{det}}^{i}) \tag{10}$$

$$P_{fal}^{OR} = 1 - \prod_{i=1}^{N} (1 - p_{fal}^{i}) \tag{11}$$

$$P_{mis}^{OR} = \prod_{i=1}^{N} (1 - p_{\text{det}}^{i}) \tag{12}$$

B. Energy detection technique based on PUEA attack

Based on the energy detection technique spectrum sensing at CR users in M samples of energy y_i^k are summed during one detection interval.

$$Y_i = \sum_{k=1}^{M} \left| y_i^k \right|^2 \tag{13}$$

Then by comparing the Y_i to a threshold the secondary user decides the presence and absence of the primary signal. The threshold is calculated by the Neyman Pearson criterion [14] and it is given by

$$\lambda_i = \sigma_{k,i}^2 \left(Q^{-1}(P_{FA}) \sqrt{2N} + N \right) \tag{14}$$

Where λ_i is the threshold of i^{th} CR user. Here $\sigma_{k,i}{}^2$ represents the variance of signal of CR i^{th} users at k^{th} time instant, $P_{fal}{}^i$ represents the Probability of false alarm and N represents the number of Cognitive users.

To calculate $P_{fal}{}^i$ in terms of energy detector parameters we needs values of $p(D_1{}^i|E_1,H_1)$, $p(D_1{}^i|E_1,H_0)$, $p(D_1{}^i|E_0,H_1)$ and $p(D_1{}^i|E_0,H_0)$

$$p\left(D_1^i \mid E_1, H_0\right) = \frac{\Gamma\left(M, \left(\lambda_i / \sigma_{3,i}^2\right)\right)}{\Gamma(M)} \tag{15}$$

$$p\left(D_1^i \mid E_0, H_0\right) = \frac{\Gamma\left(M, \left(\lambda_i / \sigma_{4,i}^2\right)\right)}{\Gamma(M)} \tag{16}$$

$$p\left(D_1^i \mid E_1, H_1\right) = \frac{\Gamma\left(M, \left(\lambda_i / \sigma_{1,i}^2\right)\right)}{\Gamma(M)} \tag{17}$$

$$p\left(D_1^i \mid E_0, H_1\right) = \frac{\Gamma\left(M, \left(\lambda_i / \sigma_{2,i}^2\right)\right)}{\Gamma(M)} \tag{18}$$

Where $\Gamma(.)$ and $\Gamma(.,.)$ are gamma function [13] and upper incomplete gamma function respectively. From equation (2) and (3) the $P_{det}{}^i$ and $P_{fal}{}^i$ are expressed as

$$P_{\text{det}}^{i} = \frac{\Gamma\left(M, \left(T_i / \sigma_{1,i}^2\right)\right)}{\Gamma(M)} \alpha + \frac{\Gamma\left(M, \left(T_i / \sigma_{2,i}^2\right)\right)}{\Gamma(M)} (1 - \alpha) \tag{19}$$

$$P_{fal}^{i} = \frac{\Gamma\left(M, \left(T_i / \sigma_{3,i}^2\right)\right)}{\Gamma(M)}\beta + \frac{\Gamma\left(M, \left(T_i / \sigma_{4,i}^2\right)\right)}{\Gamma(M)}(1-\beta) \qquad (20)$$

Note that in Neyman pearson criterion, it is proved that the given probability of false alarm, the optimal threshold increases the probability of detection when the given probability of false alarm is equal to actual P_{fal}^{i} . Therefore the threshold is taken based on the presence of PUEA attack and the secondary users does not consider the fake signal and it consider only the threshold. The probability of error can be defined as the probability of making a wrong decision in spectrum sensing.

The probability of error for OR rules is given by

$$P_e^{OR} = P(H_0)P_f^{OR} + P(H_1)P_m^{OR} \qquad (21)$$

III. SIMULATION RESULTS

In this section, we analyze the numerical simulation based on PUEA attack in CSS environment. The threshold [14] is obtained from the equation (14). The simulation is performed for AWGN, Rayleigh fading channel and Rican channel and its coefficients are assumed identically and independently distributed. In addition, the channel state information is assumed to be known to the CR network. It is assumed that there are 4 CR users in the CR network. The number of samples within a detection interval (M) is equal to 3. A priori probabilities $p(H_0)$ and $p(H_1)$ are assumed to be known and equal to 0.8 and 0.2, respectively.

The curve clearly shows the presence and absence of attack in AWGN. For α=0.1,β=0.6 the Probability of false alarm at 10^{-3} and 10^{-1}, the Probability of error for With Attack is 0.2767 and 0.5445 and for Without Attack is 0.2679 and 0.5412 in AWGN.

For α=0.6,β=0.8 the Probability of false alarm at 10^{-3}, then the Probability of error for With Attack is 0.2792 and 0.5460 and for Without Attack is 0.2694 and 0.5420 in AWGN.

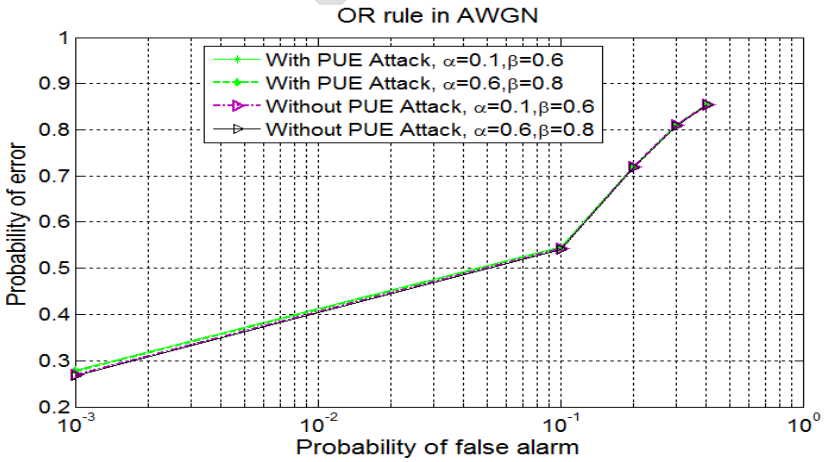

Fig. 3. Probability of false alarm versus Probability of error on OR FC rule in both with and without attack with α=0.1,β=0.6 and α=0.6,β=0.8 in AWGN.

Figure 4 explains about the ROC curve between the probability of false alarm and probability of missed detection for N number of cognitive radio users. The number of cognitive user is referred to be 4.

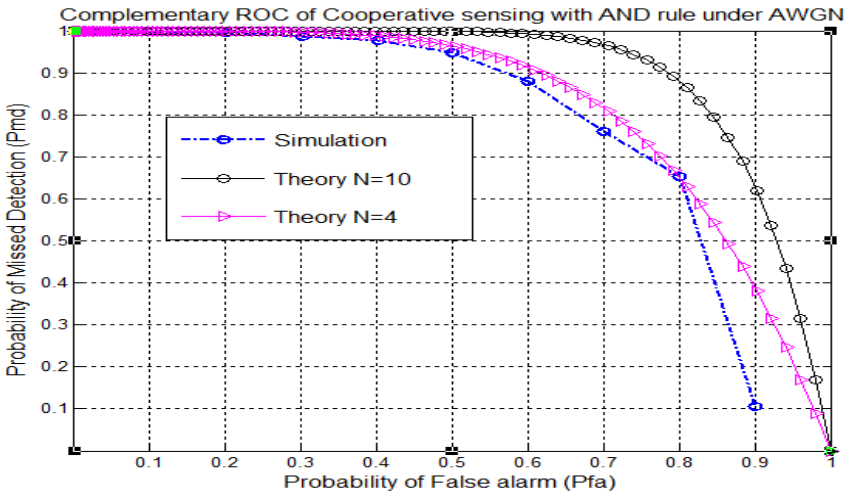

Fig. 4. Probability of false alarm versus Probability of missed detection of ROC with Theoretical value N=10 and N=4 and practical simulation for N=4 for cognitive users.

IV. CONCLUSION

The Performance of cooperative spectrum sensing over AWGN are presented. It has been found that probability of error is decreased for AWGN . Even though in the presence of attacker the system works well and false alarm is minimized in AWGN channel and also the ROC for number of CR users has been observed. Therefore performance has effectively improved.

References

[1] Haykin S. Cognitive radio: brain-empowered wireless communications. IEEE Journal on Selected Areas in Communications 2005;23(2):201–220.
[2] Ben Letaief K, Zhang W. Cooperative communications for cognitive radio networks. Proceedings of the IEEE 2009;97(5):878–893.
[3] Chen R, Park J-M. Ensuring trustworthy spectrum sensing in cognitive radio networks. In:1st IEEE workshop on networking technologies for software defined radio networks.2006.p.110–119.
[4] Chen Z, Cooklev T, Chen C, Pomalaza-Raez C. Modeling primary user emulation attacks and defenses in cognitive radio networks. In: IEEE 28th International Performance Computing and Communications Conference (IPCCC). 2009. p.208–215.
[5] Chen R, Park JM, Reed JH. Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications 2008;26(1):25–37.
[6] Anand S, Jin Z, Subbalakshmi K. An analytical model for primary user emu- lation attacks in cognitive radio networks. In: IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN). 2008. p. 1–6.
[7] Yuan Z, Niyato D, Li H, Han Z. Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks. In: IEEE Wireless Communications and Networking Conference (WCNC).2011 .p.599–604.
[8] Chen C, Cheng H, Yao Y-D. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack. IEEE Transactions on Wireless Communications 2011;10(7):2135–2141.
[9] Haghighat M, sadough SMS. Cooperative spectrum sensing in cognitive radio networks under primary user emulation attacks. In: 2012 Sixth International Symposium on Telecommunications (IST2012). 2012.
[10] Peh E, Liang Y-C. Optimization for cooperative sensing in cognitive radio networks. In: IEEE Wireless Communications and Networking Conference (WCNC). 2007. p. 27–32,
[11] Kay SM. Fundamentals of statistical signal processing: detection theory, Vol. II.Englewood Cliffs, NJ: Prentice-Hall; 1998. p. 595.
[12] Digham FF, Alouini M-S, Simon MK. On the energy detection of unknown signals over fading channels. IEEE Transactions on Communications 2007;55(1):21–4.
[13] Gradshteyn I, Ryzhik I. Table of integrals, series, and products. 5th ed. San Diego, CA: Academic Press; 1994.
[14] Daniela Mercedes Martínez Plataa, Ángel Gabriel Andrade Reátiga, "Evaluation of energy detection for spectrum sensing based on the dynamic selection of detection-threshold", Procedia Engineering, Vol 35,Pages 135-143,2012.