International Journal of Science and Engineering Applications
Volume 4 Issue 5,2015, ISSN 2319-7560 (Online)

# Detection of PUE Attack by SPARS Model using WSPRT

S.Karthik Sairam
Department of ECE
Vardhaman College of Engineering
Telangana, India

T. Ramakrishnaiah
Department of ECE
Vardhaman College of Engineering
Telangana, India

**Abstract**: Cognitive radio is a system which improves the utilization of the spectrum by sensing the white spaces in its vicinity. This sensed information will be utilized by the Secondary User (SU) to transmit the data. But some of the malicious users attacks the system by generating the signal same as that of the primary transmitter. The attack caused by generating the signal same as that of the primary transmitter is called as Primary User Emulation Attack (PUEA). In this paper the Signal Activity Pattern Acquisition and Reconstruction System (SPARS) is used to detect the attack. But this system suffers from low True Positive Rate. To increase the True positive rate or sensitivity a new technique was proposed called as Weighted Sequential Probability Ratio Test (WSPRT). By improving the true positive rate or sensitivity, the detection capability of the system will be improved.

**Keywords**: Primary User Emulation Attack; Secondary User; Signal Activity Pattern; Signal Activity Pattern Acquisition and Reconstruction System; True Positive Rate; Weighted Sequential Probability Ratio Test; White Space.

## 1. INTRODUCTION

Cognitive radio is a dynamic spectrum management system which continuously senses the available channels in the wireless spectrum. The sensing process is continuously performed to detect the white spaces. The white spaces are the unused frequency bands of the primary user. The secondary user transmits the information by using the white spaces. But when the primary user comes, the secondary user has to vacate that frequency band. There are several spectral sensing algorithms [1] to detect the white spaces. As the information about the white spaces is continuously updated, the secondary user can jump from one frequency band or white space to another frequency band and continues its transmission.

But some of the secondary users act as selfish or malicious users. The selfish user attacks the unoccupied frequency band. It attacks the unoccupied frequency band for its own transmission. But the malicious user attacks both unoccupied frequency band and the band used by the legitimate secondary user for disturbing the transmission. They disturb the transmission by generating signal same as that of secondary user. The attack caused by generating the signal same as that of primary user is called Primary User Emulation Attack (PUEA) [2].

Primary user emulation attack has severe impact on the cognitive radio network. The impact includes Quality of Service degradation, wastage of bandwidth, connection unreliability and Denial of Service given by [3]. There are several detection schemes to detect Primary User Emulation Attack (PUEA) like Location Based Method, Hearing is believing [4], Dogfight [5], Belief Propagation [6] etc.

In this paper, a new detection technique called Signal Activity Pattern Acquisition and Reconstruction System (SPARS) technique [7] is used to detect the Primary User Emulation Attack. The advantages of the SPARS technique includes

1. SPARS technique doesn't require prior knowledge of Primary Users like location of primary user.
2. It has no limitation on static primary users or primary users with extractable identities.
3. This technique directly targets the objective of the attacker, which the attacker cannot hide.
4. Utilizes a "tolerance interval" technique to test the normality of the reconstruction error.

The SPARS system uses the Bayesian method [8] for data fusion to train SPARS and for Signal Activity Pattern (SAP) reconstruction. The sparse modeling has been widely used in the literature to solve various problems in science and engineering fields [9]-[11]. SPARS system suffers from byzantine failure problem. The Byzantine failure problem can be caused by malfunctioning sensing terminals or Spectrum Sensing Data Falsification (SSDF) attacks. The Spectrum Sensing Data Falsification (SSDF) attack was shown in Figure.1. A malfunctioning sensing terminal is unable to conduct reliable local spectrum sensing and may send incorrect sensing reports to the data collector. In an SSDF attack, a malicious secondary intentionally sends falsified local spectrum sensing reports to the data collector in an attempt to cause the data collector to make incorrect spectrum sensing decisions. Either case could potentially cause interference to legitimate secondary users and result in under-utilization of fallow licensed spectrum. We consider the Byzantine failure problem [12] from the perspective of data fusion techniques. This problem causes the decrease in True Positive Ratio.

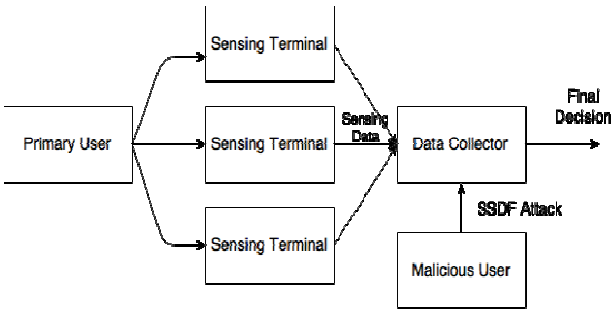


Figure.1 Spectrum Sensing Data Falsification Attack

True positive rate or Sensitivity measures the proportion of positives that are correctly detected as Primary User Emulation Attack. To improve the true positive ratio, a new technique was proposed called as Weighted Sequential Probability Ratio Test (WSPRT) [12] to improve robustness against Byzantine failures.

Rest of the paper organized as follows, Section II explains the WSPRT Technique, Section III explains the System Model, Section IV explains Simulation Results and Section V concludes the paper.

## 2. WSPRT TECHNIQUE

To improve true positive rate, WSPRT technique is used. WSPRT is composed of two parts.

1. A credit maintenance/ reputation maintenance/ weight allocation module and
2. A sequential hypothesis test module

In the credit/reputation/weight module, a terminal's credit is allocated based on the accuracy of its sensing. If it's local sensing report is consistent with the global decision, its credit receives one point bonus, otherwise one point penalty. The weight is defined as the normalized credit, and is applied as the index of probability ratio in the test.

Let $r_i$ is the each user's reputation, its weight is $w_i$ and $H_0$, $H_1$ are Hypothesis then decision variable

$$W_n = \prod_{i=0}^{n} \left(\frac{P[u_i / H_1]}{P[u_i / H_0]}\right)^{w_i} \quad (1)$$

Decision rule is as follows

If $W_n \geq \lambda_1 \rightarrow Accept\ H_1$

If $W_n \leq \lambda_0 \rightarrow Accept\ H_0$

If $\lambda_0 < W_n < \lambda_1 \rightarrow Take\ another\ Observation$

Decision threshold $\lambda_0$ and $\lambda_1$ is identified by false alarm probability $Q_f$ and Miss Detection probability $Q_m$.

$$\lambda_0 = Q_m / (1 - Q_f) \quad (2)$$

$$\lambda_1 = (1 - Q_m) / Q_f \quad (3)$$

Assuming, the reputation of a single cognitive radio user is expressed as $r_i$, each users local decision is $u_i$ and it is compared with the fusion center final decision u then update the reputation according to the rule

$$r_i = r_i + (-1)^{u_i + u} \quad (4)$$

The weight of each user can be adjusted as

$$w_i = f(r_i) = 0, r_i \leq g \quad (5)$$

$$w_i = f(r_i) = r_i + g / \max(r_i) + g, r_i > g \quad (6)$$

Where

$w_i = 0$ judges the user to the malicious user

In order to obtain a hypothesis test using Weighted Sequential Probability Ratio Test (WSPRT), it is essential to obtain the probability density function pdf of the received signal at the secondary user due to transmission by the primary and the malicious users.

## 3. SYSTEM MODEL

We consider a scenario where all secondary and malicious users are distributed in a circular grid. A primary user is located at some distance from all the users. The Secondary users sense the spectrum to detect the presence of the primary transmission. The secondary users 1 measure the received power on a spectrum band. If the received power is below a specified threshold then the spectrum band is considered to be vacant (white space). If the received power is above the specified threshold then based on the measured power, they decide whether the received signal is from a primary transmitter or by a set of malicious users. We design a WSPRT to obtain a criterion for making the decision mentioned above.

We make the following assumptions to perform the analysis.

1) Take M malicious users in the system.
2) Take the minimum distance between primary transmitter and the users is $d_p$.
3) Consider the power transmitted by the primary transmitter is $P_t$ and by the malicious user is $P_m$.
4) Take the circular grid of radius R and assume that the positions of secondary and malicious users are uniformly distributed and statistically independent.
5) Consider the position of the primary transmitter is fixed at a point $(r_p, \theta_p)$ and this position is known to all the users in the grid.
6) The Rayleigh fading of RF signal generated by the primary transmitter and malicious secondary users can be ignored..
7) The loss due to shadowing at any secondary user is normally distributed with mean 0 and variance $\sigma_p^2$ and $\sigma_m^2$, respectively.
8) The path loss exponent for the propagation from the primary transmitter to any secondary users is 2 and that between any malicious user and any secondary user is 4.
9) For any secondary user fixed at co-ordinates $(r, \theta)$, no malicious users are present within a circle of radius R0 centered at $(r, \theta)^3$.
10) There is no communication or co-operation between the secondary users. The impact of Primary User Emulation Attack (PUEA) on each secondary user is analyzed independently.

Since there is no co-operation between the secondary users, the probability of successful PUEA on any user is same as that on any other user. Hence, without loss of generality, we analyze the probability density function pdf of the received signal at any one secondary user. We transform the co-ordinates of all malicious users such that the secondary user of interest lies at the origin (i.e., at (0, 0)).

Then the primary transmitter is at a co-ordinate $(d_p, \theta_p)$[4].

All malicious nodes are uniformly distributed in the annular region with radii R0 and R by assumption 4. This scenario is shown in Figure.2. In order to obtain a hypothesis test using Weighted Sequential Probability Ratio Test (WSPRT), it is essential to obtain the probability density function pdf of the received signal at the secondary user due to transmission by the primary and the malicious users.

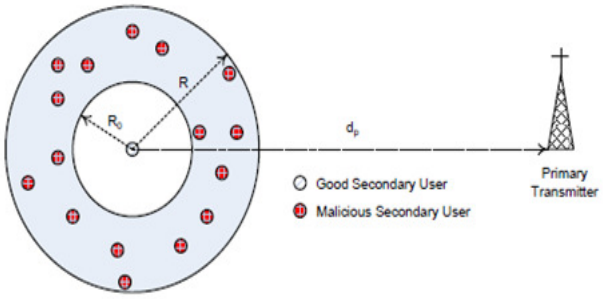


Figure. 2 Cognitive Radio Network in a circular grid with Secondary and Malicious Users

No malicious users can be closer than $R_0$ to the secondary user because if this restriction is not posted, then the power received due to transmission from any subset of malicious users present within this grid will be much larger than that due to a transmission from a primary transmitter thus resulting in failed PUEA all the time.

## 4. SIMULATION RESULTS

In this section we present simulation results of the proposed method. In our simulation, we take range = [-5 5 -5 5], M best=4, n=20, Max Generation=100.

The receiver operating characteristic (ROC) curve of SPARS is a plot of the true positive rate, i.e., 1- miss-detection probability versus the false positive rate, i.e., the false alarm probability.

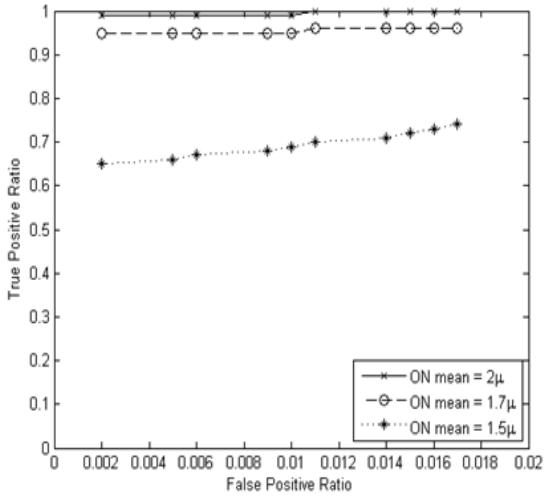


Figure. 3 ROC curves of SPARS for detecting smart attackers

Figure.3 shows the ROC curves of SPARS for detecting smart attackers. A smart attacker can manipulate its ON/OFF periods so that the mean ON/OFF period is more close to the one of PUs. Specifically, a smart attacker randomly generates a small fraction of very short ON periods.

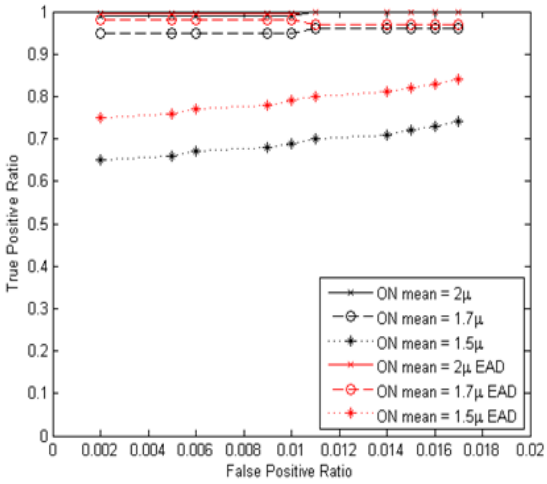


Figure. 4 ROC curves of SPARS for detecting smart attackers using WSPRT

Figure.4 shows the improvement of true positive rate in proposed method compared to the existing method which is achieved by using Weighted Sequential Probability Ratio Test (WSPRT) technique.

## 5. CONCLUSION

The SPARS model is an efficient detection technique which is used to detect the PUE attack based on the Signal Activity Pattern (SAP). This system suffers from low True Positive Ratio due to the impact of byzantine failure problem. In this paper, we proposed a technique called Weighted Sequential Probability Ratio Test. The performance of the SPARS model can be increased by increasing the sensitivity or True Positive Ratio of the system, which will be achieved by using the WSPRT technique.

## 6. REFERENCES

[1] Tevfik Yucek and Huseyin Arslan.2009, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications," *IEEE Communication Surveys and Tutorials*, Vol. 11, No. 1, pp. 116-130.

[2] Z. Jin, S. Anand, and K P. Subbalakshmi.2009, "Detecting primary user emulation attacks in dynamic spectrum access networks," IEEE IntI. Conf. on Commun. (ICC).

[3] Abhilasha Singh and Anita Sharma.2000, "A Survey of Various Defense Techniques to Detect Primary User Emulation Attacks," *International Journal of Current Engineering and Technology*, Vol. 4, No. 2.

[4] S. Chen, K. Zeng, and P. Mohapatra.2011, "Hearing is believing: Detecting mobile primary user emulation attack in white space," *Proc. IEEE INFOCOM*.

[5] H. Li and Z. Han.2011, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part II: Unknown channel statistics," *IEEE Trans. Wireless Commun*, Vol. 10, pp.274-283.

[6] Z. Yuan, D. Niyato, H. Li, and Z. Han.2011, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," *Proc. IEEE WCNC*.

[7] ChunSheng Xin and Min Song.2014, "Detection of PUE attack in cognitive radio system based on signal activity pattern," *IEEE Transactions on mobile computing*, Vol.13, No. 5.

[8] P. K. Varshney.1997, "Distributed Detection and Data Fusion," *Springer-Verlag*.

[9] R. Rubinstein, M. Zibulevsky, and M. Elad.2010, "Double sparsity: Learning sparse dictionaries for sparse signal approximation," *IEEE Trans. Signal Process*, vol. 58, no. 3, pp. 1553-1564.

[10] D. L. Donoho.2006, "For most large underdetermined systems of equations, the minimal l1-norm near-solution approximates the sparsest near-solution," *Wiley Commun. Pure Appl. Math*, vol. 59, no. 7, pp. 907-934.

[11] J. Wright, A. Yang, A. Ganesh, S. Sastry, and Y. Mal.2009, "Robust face recognition via sparse representation," *IEEE Trans. Pattern Anal. Mach. Intell*, vol. 31, no. 2, pp. 210-227.

[12] Ruiliang Chen, Jung-Min Park and Kaigui Bian.2008, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," *Lab for ARIAS*, DOI: 10.1109/INFOCOM.2008.251.