E-ISSN 2250-0944
ISSN 2250-1150
DOI: 10.31838/ijprt/11.02.05

Research Article

Mitigation Techniques for PUEA In Cognitive Radio Networks Using Hypothesis Testing

PRADEEP P[1], PRAVEEN KUMAR M[2], PREM KUMAR S[3], DR.K.J. PRASANA VENKATESHAN M.E., PH.D.[4],
[1]Department of Electronics and Communication Engineering, National Engineering College, Tamil Nadu - 628503, India
[2]Department of Electronics and Communication Engineering, National Engineering College, Tamil Nadu - 628503, India
[3]Department of Electronics and Communication Engineering, National Engineering College, Tamil Nadu - 628503, India
[4]Assistant Professor (S/G) Department of Electronics and Communication Engineering, National Engineering College, Tamil Nadu - 628503, India
Email:171008@nec.edu.in[1],171068@nec.edu.in[2],2017-18ece24@nec.edu.in[3],prasanna@nec.edu.in[4]
Corresponding Author Email: necpraveenkumar@gmail.com
Received: 28.02.21, Revised: 22.03.21, Accepted: 05.04.21

ABSTRACT
This paper detects primary user emulation attacks in cognitive radio networks using Neyman-Pearson composite hypothesis test and Wald's sequential probability ratio test. Most approaches in the literature on Primary user emulation attacks assume the presence of underlying sensor networks for localization of the malicious nodes. There are no analytical studies available in the literature to study Primary user emulation attacks in the presence of multiple malicious users in fading wireless environments. An NPCHT and WSPRT based analysis to detect Primary user emulation attack in fading wireless channels in the presence of multiple randomly located malicious users. It shows there is a range of network radii in which PUEA is most successful. The results also show that for the same desired threshold on the probability of missing the primary, WSPRT can achieve a successful probability PUEA 50% less than that obtained by NPCHT.

Keywords: Primary user, Secondary user, Malicious nodes, Dynamic spectrum access, Cognitive radio network, Primary User Emulation Attack, NPCHT, WSPRT.

INTRODUCTION

Traditionally, radio spectrum bands have been assigned to license holders or services on a long term basis for large geographical regions. This fixed spectrum assignment policy has led to under-utilization of the available spectrum. The inefficiency in spectrum usage and the limited availability of spectrum have given rise to cognitive radio enabled dynamic spectrum access (DSA) as a new communication paradigm. "Secondary" nodes in a DSA network can use the licensed spectrum bands when it is idle, they vacate it according to the condition upon the return of the "primary" licensed users (incumbent, primary users). This paper uses the term primary to refer to the licensed, high priority user and the term secondary to denote the unlicensed users. One of the examples of cognitive radio networks is the usage of unused spectrum in the TV band. The TV transmitter and receivers are primary users who are licensed to access these bands. Based on ad-hoc Other users who can access these white spaces in the TV band on an ad-hoc basis are termed, secondary users. The IEEE 802.22 working group on wireless regional area networks provides the physical layer and medium access control specifications.

The FCC's mandated spectrum policy reform has resulted in a lot of research activities on various aspects of CRN including spectrum sensing and management, network architectures, capacity, codes, transmission techniques, spectrum etiquette, and evacuation protocols as well as test-bed development. Standardization efforts for DSA networks include the IEEE Standards Coordinating Committee 41 (IEEE SCC41)'s sponsored projects as well as IEEE 802.22. cations for the usage of the TV white spaces.

Spectrum sensing in DSA is essential both for the identification of empty spectral bands (white spaces) as well as for prompt evacuation upon the return of the incumbent. Protocols for sensing primary transmission and spectrum evacuation can be found in. Primary transmitter detection techniques include energy detection, cyclostationary feature detection, and matched

filter detection. Among these, energy-based detection is generally more popular due to ease of implementation.

Despite the body of work on other aspects of CRN, research on security issues is still in its nascence. In the particular case of Directory system agent networks, it can be argued that to stage a denial-of-service attack at the sensing level, During the sensing phase it is necessary to affect the decision on primary activity. This can be done in one of the following ways: (a) some malicious nodes can transmit spurious signals that emulate the primary user - primary user emulation attacks; (b) the spectrum sensing nodes can lie about the spectrum data (Byzantine attack) (c) by making use of the weaknesses of existing protocols for evacuation or (d) by modifying messages passed between the sensing nodes and the centralized decision-maker. In this paper, we study Denial-of-service attacks via primary user emulation. In this type of attack, a set of "malicious" secondary users could forge the essential characteristics of the primary signal transmission to make other "good" secondary users believe that the primary user is present or not. The secondary users following the normal spectrum evacuation process will vacate the spectrum unnecessarily, resulting in what is known as the primary user emulation attacks (PUEA). PUEA become easier when energy detection-based mechanisms are used for the identification of primary activity since the detector only checks received energy against a threshold rather than look for particular signal characteristics.

This paper, to study Denial-of-Service attacks via primary user emulation. In this type of attack, a set of "malicious users" could forge the essential characteristics of the primary signal transmission to make other "good" secondary users believe that the primary user is present or not. The secondary users following the normal spectrum evacuation process will vacate the spectrum unnecessarily, resulting in what is known as the primary user emulation attacks. PUEA becomes easier when energy detection-based mechanisms are used for identification of primary activity since the detector only checks received Chen et al propose two mechanisms to detect PUEA: distance ratio test and distance difference test based on the correlation between the length of the wireless link and the received signal strength. They consider a single malicious user in a non-fading wireless environment and detect a Primary user emulation attack using the ratio and the difference, respectively, of the distances from the primary transmitter and the malicious user, to the secondary users equipped with a global positioning system (GPS). In, Chen et al discuss defense against PUEA by localization of the suspect transmission via an underlying sensor network and comparing it with the known location of the primary transmitter. A mitigation technique for DoS attacks arising from fraudulent reporting of sensing results by malicious nodes is studied. The Primary user emulation attack methods described thus far do not take into account, the fading characteristics of the wireless environment and require estimation of the location of the malicious users via either a dedicated sensor network or via significant enhancement of the secondary nodes themselves. Energy against a threshold rather than look for particular signal characteristics.

The first analytical expression for the probability of successful PUEA based on energy detection was derived in, where to modeled the received power at a secondary user as a log-normally distributed random variable and used Fenton's approximation to determine the mean and the variance of this distribution. This was then used to determine, a lower bound on the probability of a successful Primary user emulation attack using Markov inequality. In this paper, we propose a Neyman Pearson composite hypothesis test and a Wald's sequential probability ratio test to detect PUEA in fading wireless environments, without assuming additional features to the secondary nodes or the presence of model of sensor nodes to assist in gathering information about the direction of the received signal. Fenton's approximation is used to model the received power at the secondary user from the transmission of the malicious users. Simulations confirm the theoretical result that NPCHT allows the secondary user to keep the probability of missing the primary around the desired threshold while trying to minimize the probability of successful PUEA. Since the Neymon-pearson hypothesis test cannot simultaneously provide a cap on the probability of missing the primary as well as the probability of a successful PUEA, we develop the WSPRT, which will allow us this flexibility in return for some added time complexity, in terms of several observations needed to arrive at a decision. We show that with a modest increase in computation, it is possible to mitigate PUEA significantly even when using only the energy-based detection.

Proposed Model

In this model, all secondary and malicious users are distributed in a circular grid of radius R as shown in Fig. 3.1. A primary user is located at a distance of at least dp from all other users. We consider energy-based mechanisms to detect the

presence of the primary. Typical energy-based detection methods assume that the primary is present if the received signal strength is -93dBm. Such a sensing technique will cause serious security issues if malicious users exist in the network. As described earlier, this detection method is susceptible to Primary user emulation attacks. To mitigate this threat, to devise two hypothesis based testing mechanisms to decide if the primary is transmitting or if an attack is in progress. The mathematical terminologies needed to derive the hypothesis tests are listed below.

- There is no communication between the secondary users. The Primary user emulation attack on each secondary user can be analyzed independent of each other.
- There are M malicious users in the system. M is a geometrically distributed random variable with the mean E[M] known to the secondary users.
- The primary transmitter is at a minimum distance of primary user from all the users.
- The positions of the secondary and the malicious users are uniformly distributed in the circular gird of radius R, and their positions are statistically independent of each other.
- For the secondary user fixed at polar co-ordinates (r0, θ0), no malicious users are present within a circle of radius R0 centered at (r0, θ0). To call R0 the "exclusive distance from the secondary user". Without this restriction, 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.
- The co-ordinates of the primary transmitter are known to all the users in the system

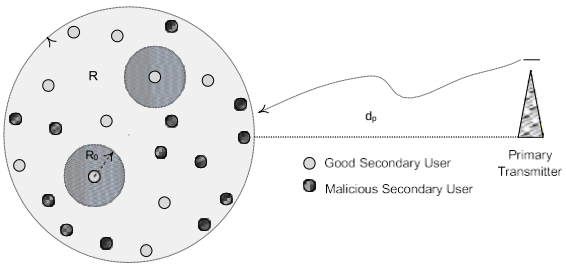


Fig.3.1: A typical cognitive radio network in a circular grid of radius R consisting of good secondary users and malicious secondary users. No malicious users are present within a radius R0 about each good secondary user. A primary transmitter is located at a distance of at least dp from all other users.

- The primary transmits at a power Pt and the malicious at a power Pm. Malicious nodes do not use power control.
- The RF signals from the primary transmitter and the malicious users undergo path loss and log-normal shadowing. The Rayleigh fading is assumed to be averaged out and can be ignored. This is because, the probabilities scale linearly with the mean of the Rayleigh fading, Δ, (as shown in [16]) and Δ = 1 in most cases.
- The shadowing loss (expressed in dB) at any secondary user both from the primary transmitter and from any malicious user is normally distributed with mean 0 and variance σ 2 p and σ 2 m, respectively.
- A free-space propagation model for the signal from the primary transmitter and a two-ray ground model for the signal from the malicious users thus resulting in a path loss exponent of 2 for the propagation from the primary transmitter of the system and a path loss exponent of 4 for the propagation from the malicious users. This is because the primary transmitter is so far away from the secondary user and malicious users that the signal due to multi-path can be neglected. However, the distances from malicious users are not large than to ignore the effects of multi-path.

Neyman-Pearson Composite Hypothesis Test to detect PUEA

The Neyman-Pearson composite hypothesis test can be used to distinguish between two hypotheses, given some constraints on the miss probability. In our case, the two hypotheses are:

H1 : Primary transmission in progress

H2 : Emulation attack in progress.

The observation space is the sample space of received power measured at the secondary user. It is observed that there are two kinds of risks

incurred by a secondary user in this hypothesis test.

False Alarm:

When the actual transmission is made by malicious users but the secondary user decides that the transmission is due to the primary. In this case, this is also the probability of a successful Primary user emulation attack.

Miss Alarm:

When the actual transmission is made by the primary transmitter but the secondary user decides that the transmission is due to the malicious users. This is a serious concern if the good secondary users do not wish to violate the spectrum etiquette.

The Neyman-Pearson criterion allows the secondary to minimize the probability of successful PUEA while fixing the probability of missing the primary user at a desired threshold, α. The decision variable, Λ, is given by

where x is the measured power of the received signal. In the above, p(Pr)(x) and $p^{(m)}(x)$ are given by Eqns.

$$\Lambda = \frac{p^{(m)}(x)}{p^{(Pr)}(x)}, \qquad (3.1)$$

The decision is then made based on the following criterion:

$\Lambda \leq \lambda$ D : Primary transmission

$\Lambda \geq \lambda$ D_2: PUEA in progress,

where λ satisfies the constraint that miss probability,

$Pr\{D_2|H_1\}$, is fixed at α, i.e.,

$$Pr\{D_2|H_1\} = \int_{\Lambda \geq \lambda} p^{(Pr)}(x)dx = \alpha. \qquad (3.2)$$

The probability of successful PUEA can be written as

$$Pr\{D_1|H_2\} = \int_{\Lambda \leq \lambda} p^{(m)}(x)dx. \qquad (3.3)$$

We can also represent the above detection statistic in shorthand notation as

$$\Lambda \underset{D_1}{\overset{D_2}{\gtrless}} \lambda. \qquad (3.4)$$

Let the received power in dB be denoted by y and let

$$\begin{aligned} a &= \frac{1}{2\sigma_p^2} - \frac{1}{2\sigma_\chi^2} \\ b &= \frac{\mu_\chi}{\sigma_\chi^2} - \frac{\mu_p}{\sigma_p^2} \\ c &= \frac{\mu_p^2}{2\sigma_p^2} - \frac{\mu_\chi^2}{2\sigma_\chi^2} + \ln \sigma_p - \ln \sigma_\chi - \ln \lambda, \end{aligned} \qquad (3.5)$$

by substituting $p^{(Pr)}(x)$ and $p^{(m)}(x)$, we obtain the decision statistic as:

$$ay^2 + by + c \underset{D_1}{\overset{D_2}{\gtrless}} 0. \qquad (3.6)$$

Without loss of generality, we assume a $=_f$ 0. Let

$\Delta = b^2 - 4ac$, two conditions are of interest:

- Case 1: $a > 0, \Delta > 0$
  The constraint of $Pr\{D \mid H\} = \alpha$ can be written as

$$\Phi\left(\frac{-b-\sqrt{\Delta}-2a\mu_p}{2a\sigma_p}\right)+\Phi\left(\frac{b-\sqrt{\Delta}+2a\mu_p}{2a\sigma_p}\right)=\alpha, \tag{3.7}$$

where $\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{t^2}{2}}dt,$ and $Pr\{D_1|H_2\}$ can be derived as

$$Pr\{D_1|H_2\}=\Phi\left(\frac{-b+\sqrt{\Delta}-2a\mu_\chi}{2a\sigma_\chi}\right)-\Phi\left(\frac{-b-\sqrt{\Delta}-2a\mu_\chi}{2a\sigma_\chi}\right). \tag{3.8}$$

- Case 2: $a < 0, \Delta > 0$
  The constraint of $Pr\{D \mid H\} = \alpha$ can be written as

$$\Phi\left(\frac{-b-\sqrt{\Delta}-2a\mu_p}{2a\sigma_p}\right)-\Phi\left(\frac{-b+\sqrt{\Delta}-2a\mu_p}{2a\sigma_p}\right)=\alpha, \tag{3.9}$$

and $Pr\{D_1|H_2\}$ can be derived as

$$Pr\{D_1|H_2\}=\Phi\left(\frac{-b+\sqrt{\Delta}-2a\mu_\chi}{2a\sigma_\chi}\right)+\Phi\left(\frac{b+\sqrt{\Delta}+2a\mu_\chi}{2a\sigma_\chi}\right). \tag{3.10}$$

As is expected, the Neyman-Pearson test only allows us to place a cap on one of the quantities: the miss probability or the false alarm probability. In our experimental results we found that under certain circumstances, the probability of false alarm (successful PUEA) is very high for the desired probability of miss. So, we now develop Wald's sequential probability ratio test which allows the user to set thresholds for both false alarm and miss probabilities. This is possible since Wald's test is set up to take more than one sample observation if necessary, to arrive at a decision.

Wald's Sequential Probability Ratio Test to detect PUEA

The WSPRT allows us to specify desired thresholds (α1 and α2 respectively) for both the false alarm and miss probabilities. The decision variable after n sequential tests, An, is given by

$$\Lambda_n = \prod_{i=1}^{n} \frac{p^{(m)}(x_i)}{p^{(Pr)}(x_i)}, \tag{3.11}$$

where x_i is the measured power at the i^{th} stage. In the above equation, $p^{(Pr)}(x_i)$ and $p^{(m)}(x_i)$. The decision is then made based on the following criterion:

$$\begin{array}{ll} \Lambda_n \le T_1 = \frac{\alpha_1}{1-\alpha_2} & D_1\text{: Primary transmission} \\ \Lambda_n \ge T_2 = \frac{1-\alpha_1}{\alpha_2} & D_2\text{: PUEA in progress} \\ \text{Otherwise} & D_3\text{: Take another observation .} \end{array} \tag{3.12}$$

The average number of observations required to arrive at a decision is given by

$$E[n|H_k] = \begin{cases} \frac{(1-\alpha_2)\ln T_1 + \alpha_2 \ln T_2}{E[f(x_1)|H_1]} & k = 1 \\ \frac{\alpha_1 \ln T_1 + (1-\alpha_1)\ln T_2}{E[f(x_1)|H_2]} & k = 2, \end{cases} \quad (3.13)$$

where the function f (x_1) = ln Λ.we can derive the expression for E[f (x_1)|H_1] and E[f (x_1)|H_2] as follows

$$E[f(x_1)|H_1] = \ln\left(\frac{\sigma_p}{\sigma_\chi}\right) + \frac{\sigma_\chi^2\mu_p^2 - \sigma_p^2\mu_\chi^2}{2\sigma_p^2\sigma_\chi^2} + \frac{2\mu_p(\sigma_p^2\mu_\chi - \sigma_\chi^2\mu_p)}{2\sigma_p^2\sigma_\chi^2} + \frac{(\sigma_\chi^2 - \sigma_p^2)(\sigma_p^2 + \mu_p^2)}{2\sigma_p^2\sigma_\chi^2}, \quad (3.14)$$

and

$$E[f(x_1)|H_2] = \ln\left(\frac{\sigma_p}{\sigma_\chi}\right) + \frac{\sigma_\chi^2\mu_p^2 - \sigma_p^2\mu_\chi^2}{2\sigma_p^2\sigma_\chi^2} + \frac{2\mu_\chi(\sigma_p^2\mu_\chi - \sigma_\chi^2\mu_p)}{2\sigma_p^2\sigma_\chi^2} + \frac{\sigma_\chi^2 - \sigma_p^2}{2\sigma_p^2\sigma_\chi^2}(\sigma_\chi^2 + \mu_\chi^2). \quad (3.15)$$

Substituting E [f (x_1)|H_1] and E [f (x_1)|H_2] in Eqn. (3.15), we evaluate E [n|H_1] and E [n|H_2].

RESULT AND DISSCUSSION

Neyman-Pearson Composite Hypothesis Test Results:

Test Results The results of NPCHT with a theoretical probability of missing the primary user set to α=0.2 are shown in Fig. 4.2. It is observed from Fig. 4.1(a) that the probability of false alarm rises and then falls with increasing value of R. This is because, for a given R0, if R is small, i.e., malicious users are closer to the secondary user, the total received power from all malicious users is likely to be larger than that received from the primary transmitter, thus decreasing the probability of successful PUEA. Similarly, for large R, the total received power from the malicious users may not be enough to successfully launch a PUEA. Fig. 4.1(b) shows that the experimental probability of missing the primary user is always close to the required value (within ±0.04 of the desired value).

As we lower α from 0.2 to 0.1, the maximum error between the experimental curve and the theoretical one falls from 0.133, shown in Fig. 4.2(a), to 0.083, shown in Fig. 4.2(a). These discrepancies exist because we needed to make approximations while deriving the expressions for the received power. However, since the experimental and theoretical values are not far apart, our approximations are fairly good. From Fig. 4.1(a) and Fig. 4.2(a) we note that as α is decreased, the probability of successful PUEA increases. This is expected since NPCHT only allows a threshold to be set on one of these parameters.

Wald's Sequential Probability Ratio Test Results

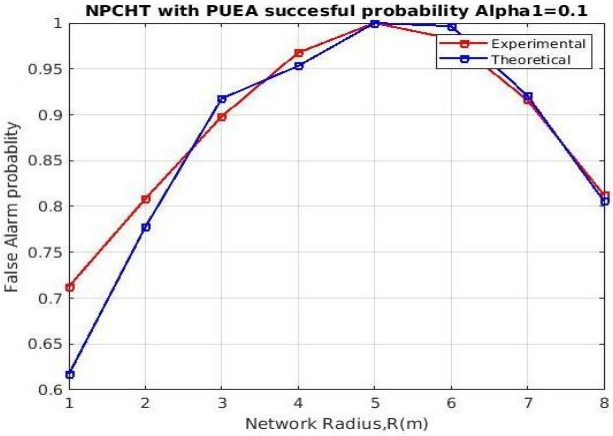
Fig. 4.3 shows the results of WSPRT with thresholds for the probability of successful PUEA, probability of missing primary user set to 0.2 each. Although the experimental curve in Fig. 4.3(a) goes above the theoretical one, we achieve much lower probabilities of successful PUEA compared to Fig. 4.1(a). The maximum probability of successful PUEA in the NP test can go as high as 0.778 whereas in Wald's test we can limit this to 0.407. The lower probabilities of successful PUEA are achieved at the cost of more observations as shown in Fig. 4.3(c) and Fig. 4.3(d). It is observed that a number of observations behaves likes the probability curves. This is because, more observations are always taken if a decision cannot be made easily, where decision error probabilities also tend to be relatively high. Note that the gap between the experimental and theoretical curves is typical of WSPRT because the expression for the expected number of observations is an approximation rather than an exact expression.

Fig. 4.4 shows the results obtained when the threshold for PUEA is set to Comparing this with Fig. 4.3(a) we see that for any α2, it is not possible to achieve arbitrary lower probabilities of

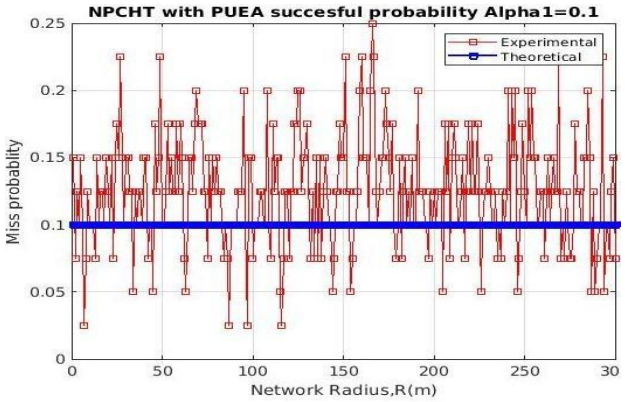
successful PUEA. Note, however, that it is always possible to make sure that the probability of missing primary user stays strictly below the required threshold, which can be seen from Fig. 4.3(b), Fig. 4.4(b) and Fig. 4.5(b) This is particularly important in CRN to ensure that the secondaries still obey the spectrum sharing etiquette.

As both α1 and α2 are lowered to 0.1, only the experimental curve of miss probability in Fig. 4.5(b) decreases accordingly. This indicates that it is not possible to always keep both the false alarm as well as the miss probability below arbitrarily desired thresholds.

From the curves showing the number of observations required to make a decision, it can be noticed that more observations are required as the α1 and α2 are decreased. This is because as α1 and α2 decrease, the threshold T1 decreases, and the threshold T2 increases which effectively reduces the range of values of the test statistic for which a decision is taken. Thus, it is more likely that the secondary user takes decision D3. Therefore, there is a trade-off between reliable decisions and time to detect.

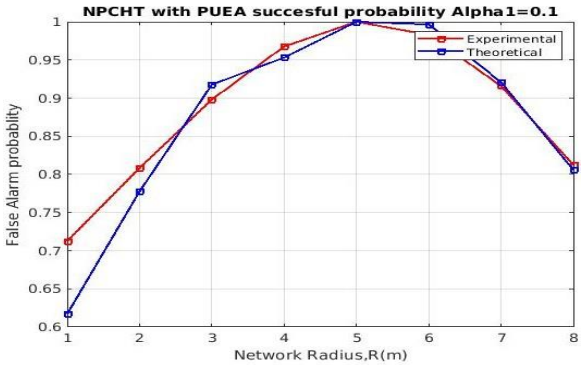


a) Probability of successful PUEA using the NPCHT. The average number of malicious users is fixed

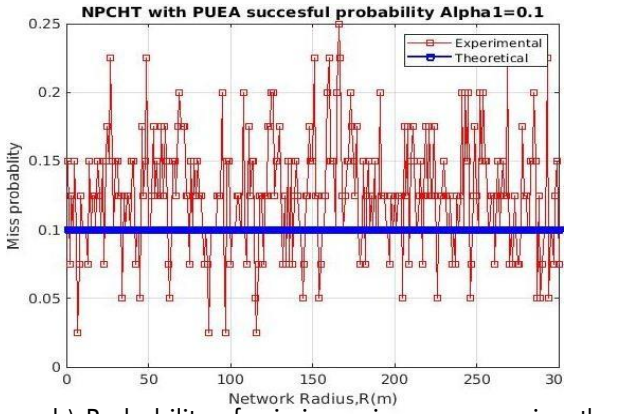


b) Probability of missing primary user using the NPCHT. Note that the experimental values are not too far from the desired threshold.

Fig.4.1: NPCHT with theoretical probability of missing primary user α=0.2

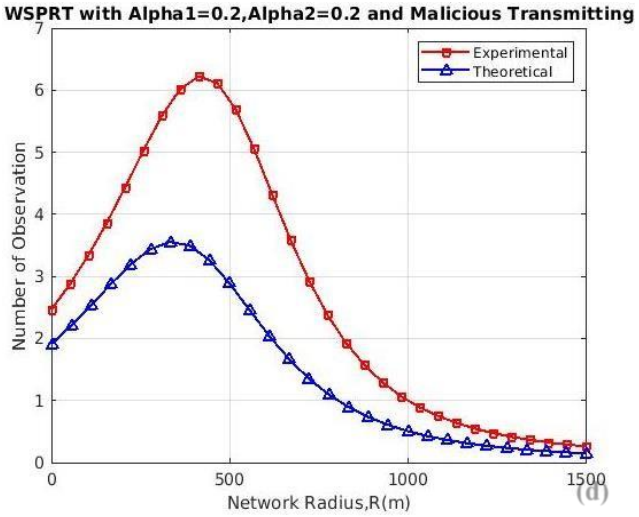


a) Probability of successful PUEA using the NPCHT. The average number of malicious users is fixed at 25.

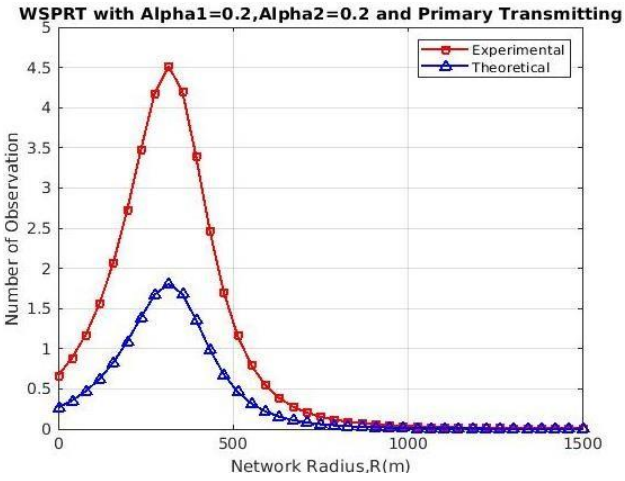


b) Probability of missing primary user using the NPCHT. Note that the experimental values are not too far from the desired threshold.

Fig.4.2: NPCHT with theoretical probability of missing primary user α=0.1.

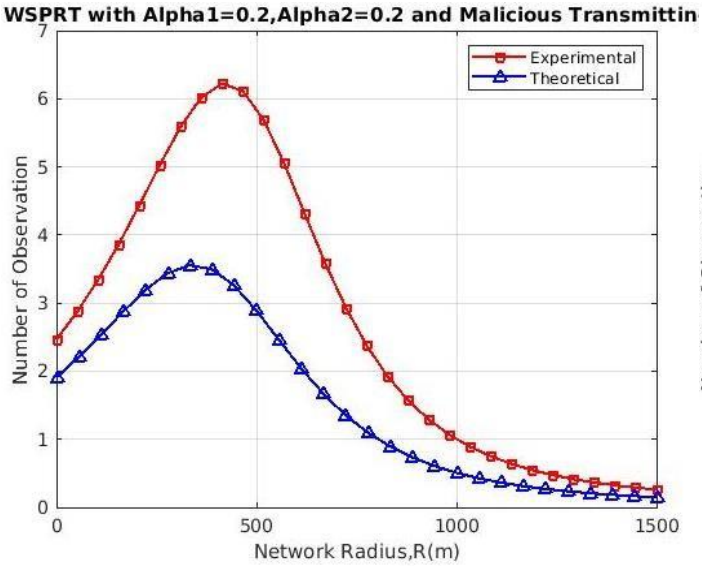


a) Probability of successful PUEA

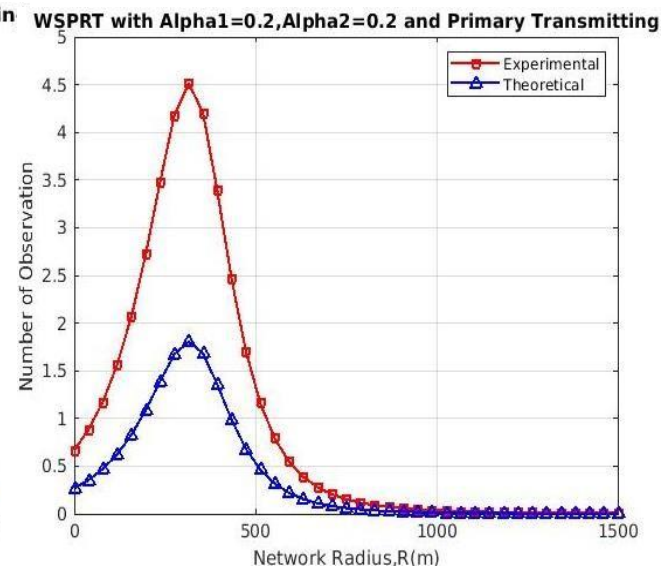


b) Probability of missing primary user

Fig.4.3: WSPRT with theoretical probability of successful PUEA α1 = 0.2 and theoretical probability of missing primary user α2 = 0.2.

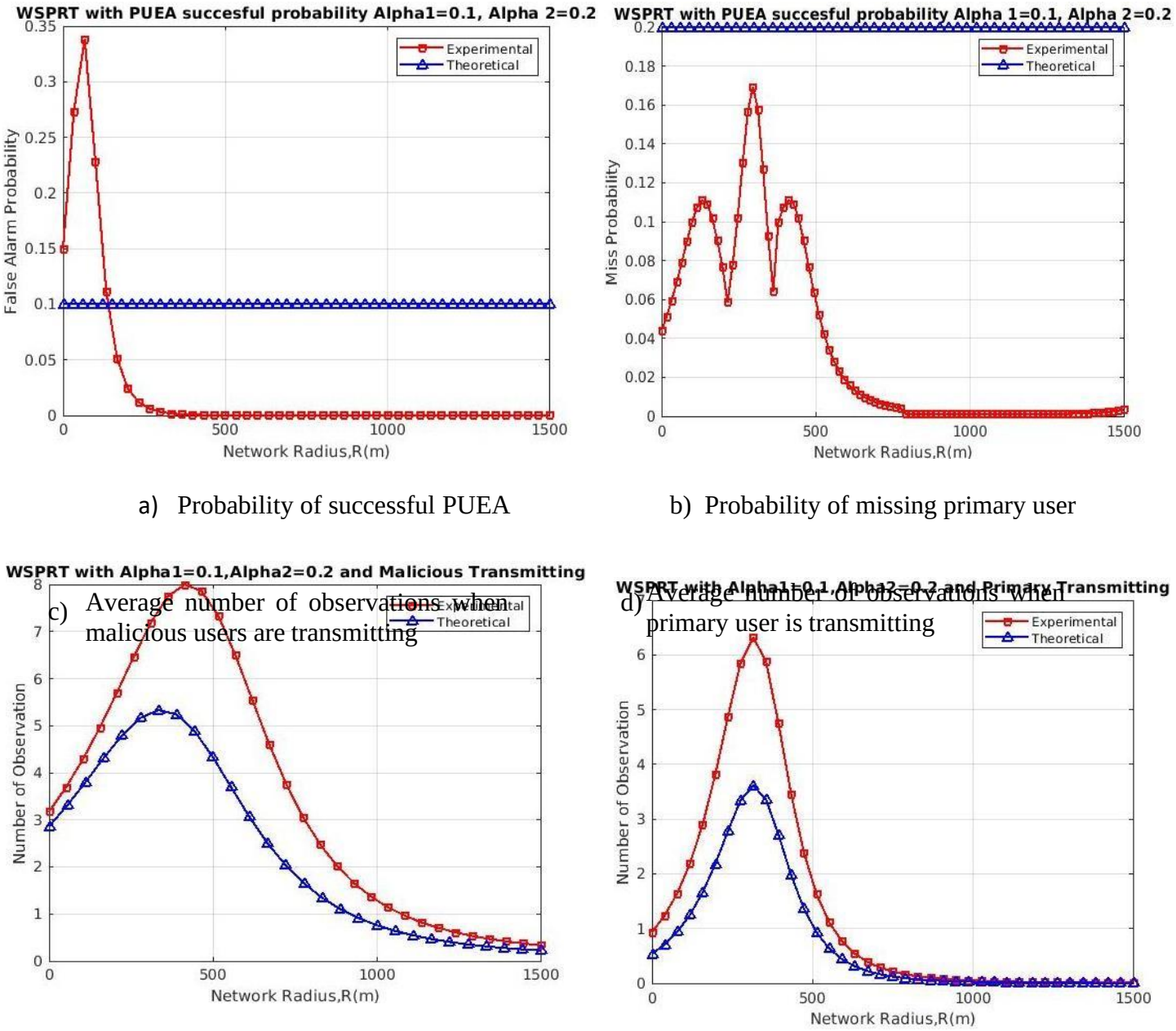


c) Average number of observations when malicious users are transmitting



d) Average number of observations when malicious users are transmitting

Fig.4.4: WSPRT with theoretical probability of successful PUEA α1 = 0.1 and theoretical probability of missing primary user α2 = 0.2



a) Probability of successful PUEA

b) Probability of missing primary user

c) Average number of observations when malicious users are transmitting

d) Average number of observations when primary user is transmitting

Fig.4.5: WSPRT with theoretical probability of successful PUEA α1 = 0.1 and theoretical probability of missing primary user α2 = 0.1.

CONCLUSION

Primary user emulation attacks in CR networks using a Neyman-Pearson composite hypothesis test and a Wald's sequential probability ratio test are computed. Both Wald's Sequential Probability Ratio Test and Neyman Pearson Composite Hypothesis Test resulted in a range of radii in which Primary user emulation attacks were most successful. For the desired threshold on the probability of missing the primary, WSPRT was found to achieve a 50% reduction in the probability of successful PUEA compared to NPCHT. To investigating the extension of our analysis for other distributions of the number of malicious users, M, and the determination of the best fit for the distribution of M. The extension of the analysis to include power control at the attackers is a topic for further investigation.

REFERENCES

1. M. Karimi and S. M. S. Sadough, "Efficient Transmission Strategy for Cognitive Radio Systems Under Primary User Emulation Attack," IEEE Syst. J., 2017.

2. M. Ghaznavi and A. Jamshidi, "Defence against Primary User Emulation Attack Using Statistical Properties of the Cognitive Radio Received Power," IET Commun., 2017.
3. E. M. Yousef, H. Y. Soliman, and A. M. Ghuniem, "SensingThroughput tradeoff with primary user traffic and cooperative sensing in cognitive radio," in 2017 2nd International Conference on Computer and Communication Systems (ICCCS), 2017, pp. 121–127.
4. Y. Li, C. Han, M. Wang, H. Chen, and L. Xie, "A primary user emulation attack detection scheme in cognitive radio network with mobile secondary user," in 2016 2nd IEEE International Conference on Computer and Communications (ICCC), 2016, pp. 1076–1081.
5. K. Yadav, S. D. Roy, and S. Kundu, "Enhanced Throughput Performance under Primary User Emulation Attack in Cognitive Radio Networks by Optimal Threshold Selection Approach," in 2018 2nd International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), 2018, pp. 1–6.
6. Yongcheng Li, Manxi Wang, Changdong Han, Lei Xie, "A Primary User Emulation Attack Detection Scheme in Cognitive Radio Network with Mobile Secondary User", 2nd IEEE International Conference on Computer and Communications,2016.
7. Dikita Salam, Amar Taggu, NingrinlaMarchang, "An Effective EmitterSource Localization-based PUEA Detection Mechanism in Cognitive Radio Networks"International Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016.
8. A. Abrardo, M. Barni, K. Kallas, and B. Tondi, "A game-theoretic framework for optimum decision fusion in the presence of byzantines," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1333–1345, June 2016.
9. T. Duc-Tuyen, N. Nguyen-Thanh, P. Maille, P. Ciblat, and V. T. Nguyen, "Mitigating selfish primary user emulation attacks in multi-channel cognitive radio networks: A surveillance game," in Proc. of IEEE Globecom, December 2016.
10. M. Dabaghchian and et al, "Online learning-based optimal primary user emulation attacks in cognitive radio networks," Proc. of IEEE Communications and Network Security (CNS), 2016.