Abstract

**Objectives:** For dynamic spectrum sharing and for spectrum scarcity problem solution, Cognitive radio is used. This paper provides Primary User Emulation Attack analysis on Cognitive radio. **Methods:** This paper presents simulation framework to evaluate the impact of Primary User Emulation Attack on Cognitive radio network. For evaluation of the capability analysis of Cognitive radio networks under Primary User Emulation Attack, a hypothesis test at secondary user based on measured Probability density function of power received has been conducted. Simulation is done with MATLAB 2012b. **Findings:** For Primary User Emulation Attack analysis on Cognitive radio, the simulation results based on probabilities of miss detection as well as false alarm have been shown. The conclusion is that with increased number of malicious users within the system, false alarm probability also increases. **Application:** These results are useful for Primary User Emulation Attack analysis on Cognitive radio and are also useful to telecom operators.

**Keywords:** Cognitive Radio (CR), Primary User Emulation Attack (PUEA), Probability Density Function (PDF), Probability of False Alarm

1. Introduction

FCC (Federal Communications Commission) has revisited the spectrum management issue to light on the spectrum need of evolving applications in Wireless Communication and to better exploit available spectrum. A conventional spectrum management technique allows only legitimate users to occupy the available spectrum for given interval of time, but the spectrum scarcity has led FCC (Federal Communications Commission) to allow opening of licensed bands for the unlicensed operators with non-interference policy. This new communication standard where unlicensed users opportunistically operate in spectrum band occupied by the licensed users without interfering their transmission is known as Opportunistic Spectrum Sharing. Cognitive radios are the permitting technology for opportunistic spectrum sharing. CRs (Cognitive Radios) are adaptive to their environment as they can sense and proactively change their parameters according to the environment. Cognitive Radio performs spectrum sensing to find spectrum holes, known as “white spaces”. When spectrum holes found, CRs artfully uses these spectrum holes to transmit their data without affecting primary user’s transmission. To ensure trustworthy operation cognitive radio must be able to differentiate into primary users signal and secondary users signal. Recognizing two signs is non-trifling, yet it turns out to be particularly troublesome when the CRs are working in unfriendly situations. In an intimidating situation, an assailant may adjust transmission characteristics of a CR to copy primary signal qualities, and hence resulting the secondary users to recognise as primary signal as that of attacker signal. This type of attack is called as PUEA.

The below part is structured as follows, 2nd section discusses PUE attack, 3rd section discuss system model to detect primary user emulation attack. Finally 4th section discusses simulation parameters followed by discussion of results and conclusion in Section 5.
2. The Primary User Emulation (PUE) Attack

Differentiating incumbent signals from secondary user signals is the major challenge faced by any spectrum sensing algorithm. A conventional algorithm such as Energy Detector\(^5\) follows a trust model to distinguish primary and secondary user’s signals. While using energy detection based spectrum sensing algorithm, it is assumed that a secondary user can recognize secondary user’s signal but not that of primary. In such situation, when there is a detection by secondary user which is recognizable, it is assumed that the detected signal belongs to secondary user otherwise it is considered to be primary user’s signal. Under this type of trust model, spectrum sensing process can be easily exploited by the attacker. For example, an attacker may pretend as primary transmitter while transmitting undistinguishable signals in order to prevent secondary user to use any spectrum band. Other techniques of sensing of spectrum like Match filter and cyclo-stationary detection\(^6\) uses inherent characteristics of primary users, causing secondary users to discriminate primary signals with other secondary signals. Yet, these algorithms are not strong enough to cope with Primary User Emulation attacks. An attacker may use same cyclic spectral characteristic as primary transmitter to make the transmissions indistinguishable by cyclo-stationary detection technique. Depending upon the inspiration at the back of attack, Classification of PUE attack is given below.

2.1 Selfish Primary User Emulation Attack

Selfish PUEA are intended to boost own usage of spectrum. When selfish attacker finds an unused spectrum band, it averts other secondary users from accessing that band by transmitting signals that have same characteristic that of primary users.

2.2 Malicious Primary User Emulation Attack

Malicious PUEA are intended to barricade the opportunistic spectrum sharing process at secondary users i.e., to stop genuine secondary users to detect and use variant spectrum.

3. System Model

For evaluation of the Primary user emulation attack, let us consider the system model given in Figure 1. Consider a circular area of radius \(R\) meters; all the malicious and secondary users are restricted to this region. The distance between Primary users and Secondary users is \(D_p\) meters. Energy detection based spectrum sensing algorithm is considered for primary user detection. The energy detection algorithm is based on comparing received signal power with some predetermined threshold value. If received signal contains more energy than threshold then it considered that the channel is occupied by primary user. To evaluate the performance of PUEA, the spectrum sensing algorithm is considered to have two threshold values \(T_L, T_H\). The reason behind this assumption is that if prediction is done on single threshold value, even a single malicious user can also alter the results by transmitting at higher powers\(^7,8\). The probability of deploying successful PUEA is calculated based on the absolute difference between the received powers from the primary and that from all the intruders below a specified threshold, \(\varepsilon\). The following assumptions have been made for our analysis.

- Number of malicious users and secondary users in the system are \(M, N\) respectively.
  - The location of Primary user is at a fixed point \((r_p, \theta_p)\) as far from all the users by distance \(D_p\) and transmission is done at \(P_t\) watts.
  - All the secondary users (both malicious and good) are uniformly distributed over a circular area of radius \(R\), and are statistically independent to each other. Moreover malicious users transmits at \(P_m\) watts, where \(P_m \ll P_t\).
- The signal propagation undergo Independent and Identically Distributed (i.i.d) lognormal shadowing and Rayleigh type fading. The exponent of path loss considered for primary user transmission is about 2 (free space propagation) and for malicious user transmission is about 4 (two-ray ground model).
- Each secondary user located at a fixed point \((r, \theta)\) has an exclusive region of radius \(R_o\) meters where no malicious user is present. The reason behind this assumption is that if malicious users are allowed in this vicinity, the received power from any malicious user will be much higher than the received power due to transmission from primary user. This will result in failed PUEA every time. Though malicious user can
adopt power control mechanisms to alter transmit power such that PUEA is successful all the time.

3.1 PUE Attack Investigation Model

The PUEA investigation model presented in this paper considers no cooperation between secondary users hence probability of primary user emulation attack is same on each user. Without the loss of generality, we can analyse the impact of PUE attack on any of the user. Let us consider the malicious users coordinates are transformed in a way that the secondary users of interest lies at \((0,0)\), accordingly the primary user is then shifted to co-ordinates \((d_p, \theta_p)\). Finally malicious users are allowed to reside within circular region with radius \(R_o\) and \(R\). The system model adopted is given in Figure 1. To analyse the impact of primary user emulation attack, PDF of received signal strength from primary and malicious users has been evaluated.

Received Signal Strength Calculation:

Let \(M\) malicious users with co-ordinates \((r_j, \theta_j)\) are uniformly distributed in a circular region between bounds \(R_j\) and \(R\) with \((r_j, \theta_j)\) being statistically independent of \(j\).

The PDF of \(r_j, p(r_j)\) is mentioned as:

\[
p(r_j) = \begin{cases} 
\frac{2r_j}{R^2-R_o^2} & r_j \in [R, R_o] \\
0 & \text{otherwise}
\end{cases}
\]

With \(\theta_j\) being distributed uniformly over \((-\pi, \pi)\) \(\forall j\).

Amount of power received at other secondary user as a result of transmission from primary user, \(P_j^{(p)}\) can be calculated as:

\[
P_j^{(p)} = P_t d_p^2 G_p^2
\]  

(2)

Where \(P_t\) being transmitter power, \(d_p\) is distance between primary and the term \(G_p^2 = 10^{50}\) where \(\xi_p \sim N(0, \sigma_p^2)\). As \(P_t, d_p\) are fixed, the PDF of \(P_j^{(p)}, p^{(p)}(\gamma)\) is log normally distributed and given below:

\[
p^{(p)}(\gamma) = \frac{1}{A\sigma_p\sqrt{2\pi}\gamma} \exp \left\{ \frac{-(10\log_{10} \gamma - \mu_p)^2}{2\sigma_p^2} \right\}
\]  

(3)

The amount of power received at secondary user as a result of transmissions from all different malicious users can be calculated as:

\[
P_j^{(m)} = \sum_{j=1}^{M} P_m d_j^2 G_j^2
\]  

(4)

Here \(d_m, G_m^2\) being distance and shadowing between secondary users and \(j\)th malicious user under observation, \(\Lambda = \frac{\ln^{10}}{10} \) and \(\mu_p = 10\log_{10} P_t - 20\log_{10} d_p\).

Conditioned on the positions of all the malicious users, each term in the summation in the right hand side of Eqn. (4) is a log normally distributed random variable of the form \(\omega_j N(\mu_j, \sigma_j^2)\), also \(\mu_j = 10\log_{10} P_m - 40\log_{10} r_j\).

Figure 1. System model.
Based on the measured values of received signal strength, we have considered two hypotheses: \( D_1 \)- that the identified signal belongs to primary user and \( D_2 \)-that the identified signal belongs to malicious user. Based upon the observations there may be two types of threats experienced by the secondary user:

- **Probability of False Alarm**: When the transmissions from malicious users are identified to be sent from primary users.
- **Miss**: When transmissions from primary users are identified to be sent from malicious users.

It must be noted that false alarm probability is the probability of successful PUEA. In our hypothesis, we have used two separate thresholds \( a_1, a_2 \) for probability of false alarm and probability of miss detection respectively. The decision is made by averaging the results of \( n \)-sequential tests and given by:

\[
\Lambda_n = \prod_{i=1}^{n} p^{(m)}(x_i) / p^{(p)}(x_i)
\]

Where \( x_i \) being measured power at \( i^{th} \) stage. The terms \( p^{(m)}(x_i) \) and \( p^{(p)}(x_i) \) in above equation are calculated in Equations (3), (4) respectively. The conclusion is done by following criteria:

\[
\begin{align*}
\Lambda_n &\leq T_1 \frac{a_1}{1-a_2} & D_1: \text{Primary Transmitter} \\
\Lambda_n &> T_2 \frac{a_1}{1-a_2} & D_2: \text{Malicious Transmitter} \\
\text{else} & & D_3: \text{Take Another observation}
\end{align*}
\]

The above equation 6 is for practical calculation of primary user emulation attack

### 4. Results

Figure 2 shows the curve of false alarm probability and miss detection probability for the number of malicious users \( M = 15 \), outer region radius \( R = 100m \), Primary exclusive region radius \( R_o = 30m \), transmitter power of primary signal \( P_t = 100Kw \), transmitter power of malicious signal \( P_m = 4w \), \( \sigma_m = 5.5dB \), \( \sigma p = 8dB \).

Figure 3 shows the plot for false alarm probability. With number of malicious users be \( M = 10 \), the outer region radius \( R = 100m \), Primary exclusive region radius \( R_o = 30m \), transmitter power of primary signal \( P_t = 100Kw \), transmitter power of malicious signal \( P_m = 4w \), \( \sigma m = 5.5dB \), \( \sigma p = 8dB \). Probability of False Alarm is calculated for 500 numbers of simulations. The threshold value chosen for above simulation is set as 2. Therefore, \( \lambda = 2 \).

![Figure 2](image.png)

**Figure 2.** Probabilities of miss detection and false alarm measured in this model.
Figure 4 is the plot for the miss detection probability. With the number of malicious users is \( M = 5 \), outer region radius \( R = 100m \), Primary exclusive region radius \( R_o = 30m \), transmitter power of primary signal \( P_t = 100Kw \), transmitter power of malicious signal \( P_m = 4w \), \( \sigma m = 5.5dB \), \( \sigma p = 8dB \). Probability of miss detection is calculated for 500 numbers of simulations. The threshold value chosen for above simulation is set as 2. Therefore, \( \lambda = 2 \).

![Figure 3. Probability of false alarm over simulation times.](image1)

![Figure 4. Probability of miss detection curve for PUEA Model.](image2)
5. Conclusion

This research work presents simulation framework to evaluate the effect of primary emulation attack on cognitive radio networks. Simulation environment contains of a primary users, N non-cooperative secondary users and M-malicious users. For evaluation of the performance of cognitive radio networks under the influence of PUE Attack, a hypothesis test based on measured PDF of received power at secondary user has been conducted. Simulation has been carried on MATLAB-2012b and simulation results based on probabilities of false alarm and miss detection have shown. The conclusion is that with increased number of malicious users within the system, false alarm probability also increases.

6. References

1. Ruiliang C, Park JM. Ensuring trustworthy spectrum sensing in cognitive radio networks. 1st IEEE Workshop Networking Technologies for Software Defined Radio Networks, SDR’06; USA. 2006 Sep 25-25. p. 110–9.
2. Nanthini SB, Hemalatha M, Manivannan D, Devasena L. Attacks in Cognitive Radio Networks (CRN) – a survey. Indian Journal of Science and Technology. 2014 Jan; 7(4). DOI: 10.17485/ijst/2014/v7i4/48646.
3. Ghasemi A, Sousa ES. Spectrum sensing in cognitive radio networks: Requirements, Challenges and Design Trade-offs. IEEE Communication Magazine. 2008 Apr; 46(4):32–9.
4. Simon H. Cognitive radio: Brain-empowered wireless communications. IEEE Journal on Selected Areas in Communications. 2005 Feb; 23(2):201–20. DOI: 10.1109/JSAC.2004.839380.
5. Olivieri MP, Barnett G, Lackpour A, Davis A, Ngo P. A scalable dynamic spectrum allocation system with interference mitigation for teams of spectrally agile software defined radios. IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks; USA. 2005 Nov. p. 170–9.
6. Cabric D, Mishra SM, Brodersen RW. Implementation issues in spectrum sensing for cognitive radios. IEEE 38th Asilomar Conference on Signals, Systems and Computers; Berkeley, CA, USA: Berkeley Wireless Research Center, California Univ. 2004 Nov 7-10. p. 772–6.
7. Akyildiz IF, Lee W, Vuran MC, Mohanty S. Next generation/dynamic spectrum access/cognitive radio: A survey. Elsevier Journal on Computer Networks. 2006 Sep 15; 50(13):2127–59.
8. Zituo J, Anand S, Subbalakshmi KP. Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. ACM SIGMOBILE Mobile Computing and Communications Review. 2009; 13(2):74–85.
9. Arulselvi S. Higher order statics based primary user emulation attack detection. Indian Journal of Science and Technology. 2015 Nov; 8(32). DOI: 10.17485/ijst/2015/v8i32/88844.
10. Avila J, Thenmozhi K. Upgraded spectrum sensing method in cognitive radio network. Indian Journal of science and Technology. 2015 Jul; 8(16). DOI: 10.17485/ijst/2015/v8i16/57499.
11. Melsa JL, Cohn DL. Decision and estimation theory. McGraw-Hill Inc; 1978.