TELKOMNIKA, Vol.15, No.3, September 2017, pp. 1096~1102
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v15i3.5794

Malicious User Attack in Cognitive Radio Networks

N. Armi*[1], S. Rizvi[2], W.Z. Khan[3], H. Zangoti[3], W. Gharibi[4], C. Wael[5]
[1,3,4,5]Jazan University, Department of Computer Engineering and Networks,
Jazan, Kingdom of Saudi Arabia
[1,6]Indonesian Institute of Sciences, Research Center for Electronics & Telecommunication,
Bandung, Indonesia
[2]Bahria University, Department of Computer Science, Karachi, Pakistan
*Corresponding author, e-mail: nasrullah.armi@gmail.com

Abstract

Signal detection in cognitive radio network (CRN) is influenced by several factors. One of them is malicious user that emulate primary user (PU) signal. Emulation of PU signal causes detection error. This paper investigates the impact of malicious user attack to PU signal detection. A number of malicious users are randomly deployed around secondary user (SU) at a certain distance. They attempt to attack primary signal detection that is transmitted from 100 km to SU receiver. Then, the received signal power at secondary receiver and the performance of probability of false alarm and probability of miss detection under two hypothesis of Neyman Pearson criterion are studied. The derived results show that a number of malicious users has a significant impact to the performance of received power at SU and detection error rate.

Keywords: *Cognitive Radio, Spectrum Sensing, Malicious user, Primary User Emulation Attack, Secondary User*

1. Introduction

Due to increasing demand of wireless users cause scarcity of spectrum. Therefore, spectrum must be efficiently used to accommodate users at one time. Researchers and engineers have been intensively investigating solution for efficiency of spectrum use since a few years ago. They propose new paradigm and regulation where replacing fix spectrum access into dynamic spectrum access (DSA) system. In DSA system, unlicensed users dynamically access available spectrum and hop to others spectrum when licensed user return to use.

Cognitive Radio (CR) was nominated as DSA system. This technique is possible to opportunistically access the license spectrum bands when it is available [1]. Unlicensed user continuously monitors license spectrum for possible accessible. An exhaustive sensing must be periodically performed to achieve sensing outcome properly.

Spectrum sensing is a first task for unlicensed user that continuously monitors available spectrum. It must be well performed prior to access channel spectrum. Unlicensed users must strictly confirm that channel is genuinely available to avoid collision with licensed user activity. A lots of research related spectrum sensing and its performance has been conducted such as presented in [2-4].

Interferences (i.e. fading, noise, hidden and exposed nodes, etc) are occurred in channel detection. These noises certainly influence sensing outcomes and cause detection errors, such as miss detection and false detection. Such errors make unlicensed user misses the opportunity to access spectrum or collision among licensed and unlicensed users.

Cognitive radio networks vulnerable to attack by malicious user. All functionalities of CR networks such as spectrum sensing, spectrum mobility, spectrum sharing, and spectrum management are potentially vulnerable to attack [5]. The presence of malicious users significantly affects the detection performance in cognitive radio network (CRN). A user acts as disturber due to selfish or malfunction sensor reasons. A malicious user can transmit fake signal as if signal transmission from licensed user. Then, unlicensed user refrains from channel access. Malicious user can also have a jamming attack to license user signal. Unlicensed user estimates the spectrum is available and starts to access and transmit a signal. Unfortunately, it

Received April 5, 2017; Revised June 28, 2017; Accepted July 13, 2017

causes collision amongst licensed and unlicensed users. Primary user emulation (PUE) attack is considered as a source of interference in CRN and causes signal detection errors.

Malicious users are capable to harm spectrum sensing process. As an attacker, they may transmit fake signal as primary signal in licensed band. Detection of fake signal causes SUs preventing from spectrum access [6]. In [7], Chen et al., studied the use of PU location to identify primary user emulation attack (PUEA). They used directional antennas to determine the angle of primary signal, the time arrival, and signal strength of received signal for location of primary transmitter detection. The first analytical model to achieve a lower bound on the probability of successful PUEA was discussed in [8]. The authors considered fading into analysis and derived expressions for the probability of successful PUEA and provide a lower bound on the probability of successful PUEA using Fenton's and Markov approximation, respectively. Moreover, authors in [9] applied Wald's sequential probability ratio test to detect the attack by malicious users. Authors in [10] investigated strategies to combat primary user attack caused by selfish and malicious user attacks. They used game theory-based to counter primary user attack in cognitive radio networks. Authors in [11] studied primary user emulation attack in dynamic spectrum access without location information of users. They presented miss detection as a function of network radius with different number of SU for both theoretical and experimental studies. However, they did not present false detection probability and how the performance of received power by SU with a certain number of transmitted power from PU was not studied.

This paper studies the performance of PU signal detection due to malicious user as attacker. We study the received signal at secondary user due to primary transmission and malicious users. Two hypothesis of Neyman Pearson decision criterion is used to study statistical signal detection error. The rest of the paper is organized as follows. Section II discusses system model and assumption used in simulation. Theoretical analysis and calculation is presented in section III. Section IV discusses numerical and simulation results. Finally, conclusion is briefly presented in Section V.

2. System Model

Security issue in cognitive radio networks pays more attention in recent year. Attacker to PU causes errors in signal detection. Errors in primary signal detection could be false and miss detection. Malicious user identifies vacant bands. Secondary user refrains to access those bands since malicious user transmits signal as if it comes from PU. In other case, malicious user prevents SU to detect PU signal, hence it is seen the bands are available for access. However, in fact, bands are used by PU.

Figure 1 describes a simple model of CRN. Assumption is made that malicious users (M) are actively available and ready to attack in the network system. These users are circularly distributed with radius R and independently transmit amongst each other's. Secondary user is placed at the center of the network and separated to primary user with a distance D. Coordinate of primary transmitter is fixed at (r_{pt}, θ_{pt}) and transmit power P$_t$. Secondary user is free of malicious users at the range of radius Ro which is known as the exclusive radius of SU.

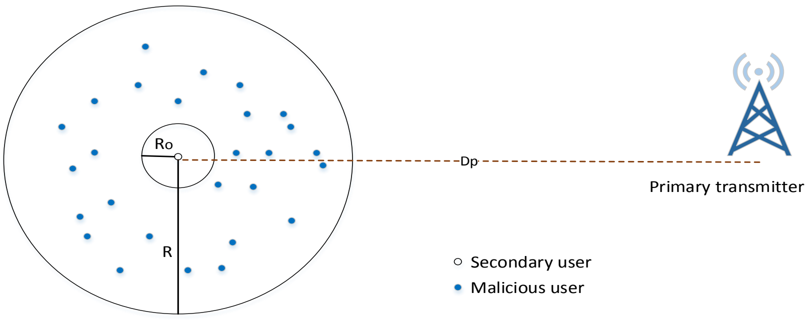

Figure 1. System model of cognitive radio networks with malicious users

3. Numerical Analysis

This section discusses numerical modeling for the assumption earlier. Let us consider M malicious users at (r_j, θ_j) where 1≤j≤M. Calculation of probability density function (PDF) of r_j as given in [11]:

$$p(r_j) = \frac{2r_j}{R^2 - Ro^2} \qquad Ro \le r \le R \tag{1}$$

Where θ_j is uniformly distributed in $(-\pi, \pi)$. The received power at secondary user from primary transmitted is given by the following formula:

$$Pr^{(p)} = P_t {d_p}^{-2} {G_p}^2 \tag{2}$$

Where $Gp^2 = 10^{\frac{\varepsilon p}{10}}, \varepsilon p \sim N(0, \sigma p^2)$. Since P_t and d_p are fixed, then the PDF of $pr^{(p)}$ follows a log normal distribution and can be written as the following calculation.

$$Pr^{(p)}(\gamma) = \frac{1}{\gamma A \sigma_p \sqrt{2\pi}} exp\left\{\frac{(10log_{10}\gamma - \mu_p)^2}{2{\sigma_p}^2}\right\} \tag{3}$$

Where $A = \frac{ln10}{10}$ and $\mu_p = 10log_{10}P_t - 20log_{10}d_p$.

The total received power at the secondary user from all malicious users can be given by:

$$Pr^{(m)} = \sum_{j=1}^{M} P_m {D_j}^{-4} {G_j}^2 \tag{4}$$

The values of D_j and ${G_j}^2$ are the distance and shadowing between j^{th} malicious user and secondary user, respectively.

${G_j}^2 = 10^{\frac{\varepsilon_j}{10}}$ where $\varepsilon_j \sim N(0, \sigma^2{}_m)$. The right side of the equation (4) is log normally distributed random variable of the form $10^{\frac{\omega_j}{10}}$ where $\omega_j \sim N(\mu_j, \sigma^2{}_m)$, where μ_j is given by:

$$\mu_j = 10log_{10}P_m - 40log_{10}D_j \tag{5}$$

The PDF of ${p_r}^m$ conditioned on the positions of all malicious users can be written as the following equation:

$$P_{x|r}{}^{(m)} = \frac{1}{xA\sigma_M\sqrt{2\pi}} exp\left\{\frac{(10log_{10}x - \mu_M)^2}{2{\sigma_M}^2}\right\} \tag{6}$$

r is the vector elements $r_1, r_2, \ldots, r_m$. The values of $\sigma^2{}_M$ and μ_M are given as the following equation:

$${\sigma_M}^2 = \frac{1}{A^2} ln\left[1 + \frac{\left(e^{A^2{\sigma_m}^2} - 1\right)\sum_{j=1}^{M} e^{2A\mu_j}}{\left(\sum_{j=1}^{M} e^{A\mu_j}\right)^2}\right] \tag{7}$$

$$\mu_M = \frac{1}{A} ln\left(\sum_{j=1}^{M} e^{A\mu_j}\right) - \frac{A}{2}({\sigma_M}^2 - {\sigma_m}^2) \tag{8}$$

The PDF of the received power from malicious users can be derived by:

$$P^m(x) = \int_{Ro}^{R} \prod_{j=1}^{M} P_{x|r}{}^{(m)}(x|r)p(r_j)dr_j \tag{9}$$

This equation is approximately calculated by a log normally distributed random variable with parameters μ_x and σ_x as:

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

Supposed that p_r^m is a log normally distributed random variable, then μ_x and σ_x can be derived by:

$$\sigma_x^2 = \frac{1}{A^2}\left(lnE\left[\left(p_r^{(m)}\right)^2\right] - 2lnE\left[p_r^{(m)}\right]\right) \tag{11}$$

$$\mu_x = \frac{1}{A}\left(2lnE\left[p_r^{(m)}\right]\right) - \frac{1}{2}lnE\left[\left(p_r^{(m)}\right)^2\right] \tag{12}$$

From equation (6) average probability of p_r^m and $E[p_r^m|r]$ simply is calculated by the following equation:

$$E\left[p_r^{(m)}|r\right] = Me^{A\mu_j} * e^{\frac{A^2\sigma_m^2}{2}} \tag{13}$$

Where,

$$\mu_j = 10log_{10}\left(P_m * D_j^{-4}\right) \tag{14}$$

$$e^{A\mu_j}=e^{A10log_{10}\left(P_m*D_j^{-4}\right)} = P_m * D_j^{-4} \tag{15}$$

Hence,

$$E\left[p_r^{(m)}|r\right] = MP_m * D_j^{-4} * e^{\frac{A^2\sigma_m^2}{2}} \tag{16}$$

By integrating equation over range of r_1, r_2,…, r_M, it becomes:

$$\begin{aligned} E\left[P_r^{(m)}\right] &= \int_{Ro}^{R} Mp\left(r_j\right)P_m * D_j^{-4} * e^{\frac{A^2\sigma_m^2}{2}}dr_j \\ &= \int_{Ro}^{R} MP_m e^{\frac{A^2\sigma_m^2}{2}} \int_{Ro}^{R} \frac{2r_j}{R^2-Ro^2} * D_j^{-4}dr_j \end{aligned} \tag{17}$$

If secondary user position at (0, 0), it means that $D_j = r_j$.

$$\begin{aligned} E\left[P_r^{(m)}\right] &= MP_m e^{\frac{A^2\sigma_m^2}{2}} \int_{Ro}^{R} \frac{2r_j}{R^2-Ro^2} * \frac{1}{{r_j}^4}dr_j \\ E\left[P_r^{(m)}\right] &= \frac{MP_m}{R^2Ro^2} e^{\frac{A^2\sigma_m^2}{2}} \end{aligned} \tag{18}$$

Then, let us consider two hypotheses in Neyman Pearson decision criterion, where M$_1$ is primary transmission in progress, and M$_2$ is emulation attack in progress. There are two types of detection error. Those are false alarm, where secondary user detects transmission, but it comes from malicious user, and miss detection means secondary user detects transmission from malicious user, but it comes from primary user.

Decision variable is calculated by using power of received signal as follows:

$$\Lambda = \frac{p^m(x)}{p^{(p_r)}(x)} \tag{19}$$

The derived value of Λ is then compared with the threshold for decision as bellows:

$\Lambda \leq \lambda\ D_1$: Primary transmission

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

Then, probability of errors depends on the decision rule as given bellows:

$P\{D_2|M_1\}$ = probability of missed detection, where decides D_2 when M_1 is true.

$P\{D_1|M_2\}$ = probability of false alarm, where decides D_1 when M_2 is true.

These two probability of errors can be expresses mathematically as follows:

$$P\{D_2|M_1\} = \int_{\Lambda\geq\lambda} p^{(p_r)}(x)dx = \alpha \quad (20)$$

$$P\{D_1|M_2\} = \int_{\Lambda\leq\lambda} p^{(m)}(x)dx \quad (21)$$

In this section, it is explained the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily [2], [5]. The discussion can be made in several sub-chapters.

4. Results and Discussion

This section discusses the performance of signal detection under PUEA in cognitive radio network. As illustrated in Figure 1, a simple model of cognitive radio network, secondary user is located in the center of circular network with R=1000m, Ro= 30m, $P_m = 4W$, $\sigma_p = 8dB$, $\sigma_m = 5.5dB$, primary transmitter power $P_t = 50kW$ with distance D_p = 100 km to secondary user. Probability of density function (pdf) for received power at secondary user is shown in Figure 2. We studied the derived theoretical and simulation results. This comparison has identical values and reach maximum at a certain point. Then, number of malicious users is reset to 15 users where the rest of setup remains the same values. The result is shown in Figure 3.

Furthermore, probability of error rate is investigated. Cumulative density function for error rate of primary signal detection is shown in Figure 3. Probability of false alarm and probability of miss detection is derived with threshold, $\lambda = 2$ and number of 25 malicious users interfere primary signal detection. Figure 4 shows probability of error rate with 10 number of malicious user, where the rest of setup remains the same values

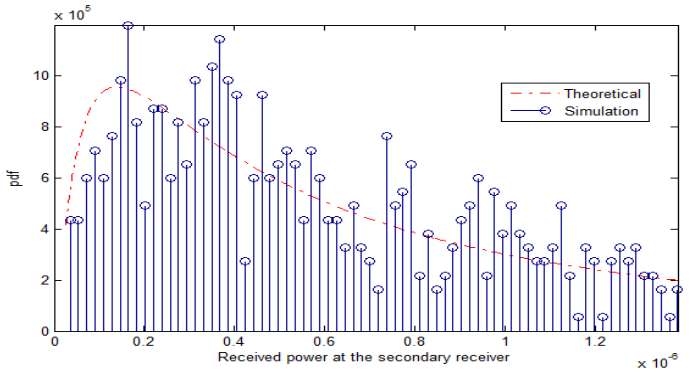

Figure 2. Probability of density function for received power at secondary user from primary transmitter $P_t = 50kW$, M = 30

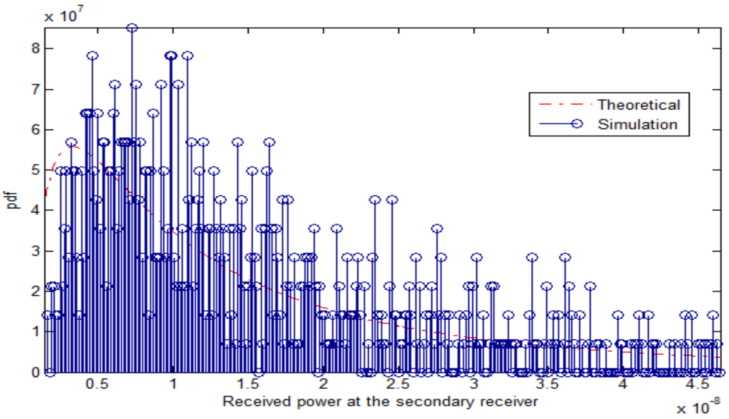

Figure 3. Probability of density function for received power at secondary user from primary transmitter $P_t = 50kW$, M = 15

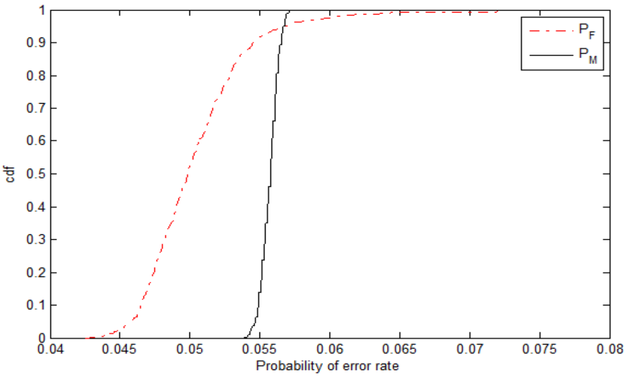

Figure 3. Cumulative density function with threshold $\lambda = 2, P_t = 100kW$, and M = 25

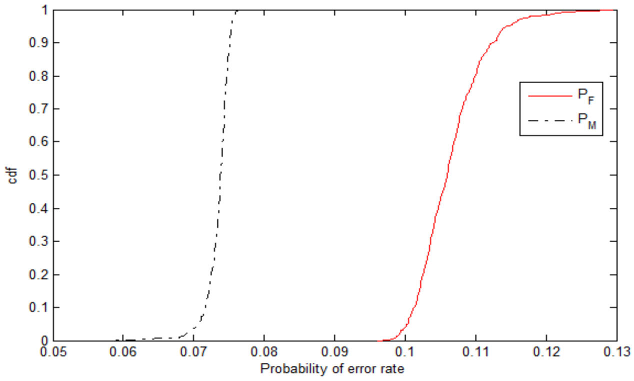

Figure 4. Cumulative density function with threshold $\lambda = 2, P_t = 100kW$, and M = 10

5. Conclusion

Interference of primary signal detection caused by a number of malicious user has been studied with Neyman Pearson criterion. The statistical characteristic of probability of false alarm and probability of missed detection is also demonstrated. The derived results show that primary user emulation attack due to malicious user decreases detection performance. Error rate increases due to miss detection and false alarm. It influences performance of signal detection and decreases fidelity of sensing outcomes. This study considered one primary transmitter located at a certain distance to SU. We will consider two or multiple primary base station at different distances to SU transmit signal continuously for further study. Evaluation the impact of power transmitter of malicious user and PU, then how far number of malicious user influences signal detection will be further investigated.

References

[1] J Mitola, GQ Maguire. Cognitive radio: Making software more personal. *IEEE Personal Communications.* 1999; 6: 13-18.

[2] Y Wang, P Wan, Q Deng, Y Fu. Application of Stochastic Resonance of the Single-mode Nonlinear Optical System in Spectrum Sensing of Cognitive Radio Networks. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2015; 13(2): 487-493.

[3] H Venkatesh Kumar, MN Giriprsad. A Novel Approach to Optimize Cognitive Radio Network Utilization using Cascading Technique. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2015; 14: 1233-1241.

[4] N Armi, BAW Chaeriah, Muhammad Arshad. *Spectrum Sensing Performance in Cognitive Radio System*. In Proc. of ICITACEE. 2015: 382-385.

[5] ST Zargar, et al. *Security in Dynamic Spectrum Access Systems: A Survey*. In Proc. of Telecommunication Policy research Conf. Arlington VA. 2009.

[6] R Chen, J Park. *Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks.* In proc., IEEE workshop on Networking Technol. for Software Defined Radio Networks (SDR). 2006: 110-119.

[7] R Chen, J Park, JH Reed. Defence Against Primary User Emulation Attacks in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications, Special Issue on Cognitive Radio Theory and Applications.* 2008; 26(1).

[8] S Anand, Z Jin, KP Subbalakshmi. *An analytical model for primary user emulation attacks in cognitive radio networks.* In Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN). 2008.

[9] Z Jin, S Anand, KP Subbalakshmi. Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. *ACM Mobile Computing and Communications Review,Special Issue on Cognitive Radio Technologies and Systems*. 2009; 13(2): 74-85.

[10] N Nguyen-Thanh, P Ciblat, AT Pham, VT Nguyen. Surveillance Strategies Against Primary User Emulation Attack in Cognitive Radio Networks. *IEEE Transactions on Wireless Communications*. 2015; 14(9): 4981-4993.

[11] Z Jin, S Anand, KP Subbalakshmi. *Detecting primary user emulation attacks in dynamic spectrum access networks.* In Proc. of IEEE International Conference on Communications (ICC'2009). 2009.