ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Novel System Modeling for Investigating Security Challenges in Cognitive Radio Networks

Vani Macharla[*1], R.Evans Mephisto[2]

[*1] PG Scholar, [2]Assistant Professor, [3]Professor, Department of Electronics and Communication Engineering, DMI College of Engineering, Chennai-600123, India

vani473@gmail.com

Abstract

As wireless communication increases day by day the available spectrum becomes scarcer as the demand for spectrum usage increasing day by day for all wireless applications. The major cause is significant amount of the spectrum leads to underutilization. To mitigate this problem effective utilization of spectrum is must. For this Cognitive Radio (CR) was introduced. Cognitive Radio enables secondary users to sense which portions of the spectrum are available, select best available channel, coordinate spectrum access with other users and vacate the channel when a primary user reappears for spectrum usage rights. If the spectrum is utilizing by malicious user instead of secondary user it is primary user emulsion attack (PUEA). So that the problem of spectrum misuse arises. We proposed a novel system with maximum likelihood criterion to mitigate the problem of spectrum misuse. Maximum Likelihood based analysis to detect PUEA in fading wireless channels in the presence of multiple randomly located malicious users. We show that the proposed model can achieve a probability of successful PUEA less than that obtained by existing model with Neyman-Pearson criterion.

Keywords: PUE, PUEA, CR, PDF

Introduction

The spectrum is assigned to license holders that is in CR terminology called primary users and secondary users are unlicensed users can use the spectrum when not being used by the primary user. During this allocation of vacant bands to secondary users attacks may happen by a set of “malicious” secondary users could forge the essential characteristics of the primary signal transmission. Other “good” secondary users believe that the primary user is present when it is not. So the secondary users are in wait state. In other case when vacant band used by the secondary user, the malicious user makes the secondary user to believe that the primary user reappears. So that the secondary user stops its transmission resulting in primary user emulation attacks (PUEA).

Cognitive Radio

“A radio frequency transceiver designed to intelligently detect whether a particular segment of radio spectrum is in use and to jump into and out of temporarily unused spectrum very rapidly without interfering with the transmission of other authorized users. Cognitive radio enables secondary user to sense which portions of spectrum are available, select best available channel, coordinate spectrum access with other users and vacate the channel when a primary user reclaims the spectrum usage rights"

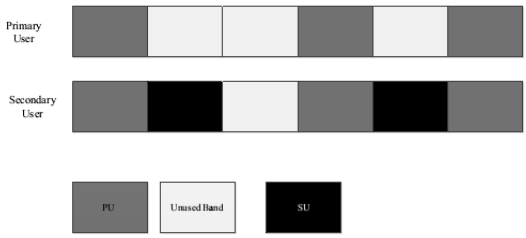

Figure 1: Cognitive radio scenario

The functions of Cognitive Radio are as follows

A. Spectrum Sensing: Spectrum sensing allows the CR users to detect spectrum holes without causing interference to the primary network. One of the primary requirements of a cognitive radio is that, it should scan the radio frequency spectrum and identify “white spaces.

B. Spectrum Decision: Cognitive radio user should decide which frequency spectrum is the best

ISSN: 2277-9655
Impact Factor: 1.852

among the available bands according to the Qos requirements for the applications.

C. Spectrum Sharing: Since there may be multiple cognitive radio users trying to access the spectrum, network access should be coordinated to prevent multiple users colliding in overlapping portions of the spectrum.

D. Spectrum Mobility: It should vacate the licensed band when the primary transmitter reappears and should search for another vacant frequency band in order to carry out its transmission. Thus spectrum mobility is defined as the ability of CR user to switch between spectrum bands when the channel condition becomes worse or the primary user reappears.

Security Challenges in Cognitive Radio Networks

Cognitive Radio network similar to wireless network as the medium for transmission is air. So the transmitted data in these networks is more prone to attacks compared to wired networks. The transmitted data in these wireless or cognitive radio networks may eavesdropped, altered and can also used by eaves for their purpose that is misuse. Primary User Emulsion Attack is one of the severe threats in Cognitive Radio Networks.

A.Primary User Emulsion Attack

A malicious user can imitate the primary user, other secondary user in the network believes that the primary user reappears and they terminate their communication and release the frequency band. Primary user emulation (PUE) attack is considered to be one of the severe threats to cognitive radio systems. It poses a great threat to spectrum sensing. In this attack, a malicious node transmits signals whose characteristics emulate those of incumbent signals. There are two types of behavior associated with the primary user emulation attack, which are

A. Selfish PUE Attack: The main objective is to maximize attacker's bandwidth. For an instance, when malicious node identifies vacant band, it will prevent other secondary users from using that band by transmitting signals that resembles the incumbent (Primary) signals.

B. Malicious PUE Attack: The main objective is to obstruct the secondary users from identifying and using vacant spectrum bands. Malicious attacker does not necessarily use vacant bands for its own communication purposes. It is important to note that in PUE attacks, malicious nodes only transmit in vacant bands.

System Model With Maximum Likelihood Criterion

Following assumptions are made for the new system model.

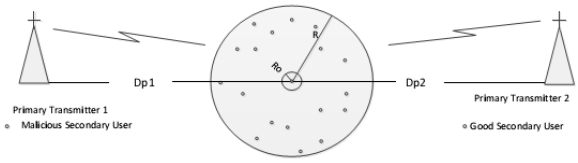

Figure 2: System model

There are M malicious users in the system which transmits at power 'P_m'. The primary transmitter P_{t1} is at distance D_{p1} and the primary transmitter P_{t2} is at distance D_{p2} from all the users and transmits at power 'P_t'. The positions of secondary and malicious users are uniformly distributed in circular region of radius R and are statistically independent of each other. Position of primary transmitter is known to all the users and is fixed at (r_p,θ_p). The RF signals from primary transmitter and malicious users undergo path loss and log normal shadowing. The path loss exponent for transmission from primary transmitter is 2 and that from malicious user is 4. For any secondary user fixed at co-ordinates(r,θ) no malicious users are present within a circle of radius R_o which is called the exclusive radius from secondary user. There is no co-operation between the secondary users.

The received power at the secondary user from the primary transmitter1 is given by,

$$p_r^{(p1)} = P_{t1} d_{p1}^{-2} {G_{p1}}^2 \quad (1)$$

The received power at the secondary user from the primary transmitter1 is given by,

$$p_r^{(p2)} = P_{t2} d_{p2}^{-2} {G_{p2}}^2 \quad (2)$$

The total power at receiver is then given by, $p_r^{(p)} = p_r^{(p1)} + p_r^{(p2)}$ due to their independence. (3)

The total received power at the secondary user from all the malicious users is given by,

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

PDF of $p_r^{(p)}$ follows a log normal distribution and can be written as

$$p^{(Pr)}(\gamma) = \frac{1}{\gamma A \sigma_p \sqrt{2\pi}} \exp\{-\frac{(10\log_{10}\gamma - \mu_p)^2}{2\sigma_p^2}\} \quad (5)$$

PDF of $p_r^{(m)}$ follows a log normal distribution and can be written as

$$p^m(x) = \frac{1}{xA\sigma_x\sqrt{2\pi}} \exp\{-\frac{(10\log_{10} x - \mu_x)^2}{2\sigma_x^2}\} \quad (6)$$

ISSN: 2277-9655
Impact Factor: 1.852

Simulations

The probability of false alarm and miss detection in existing Neyman-Pearson method over network radius of 500m is about 0.25 and probability of miss detection is about 0.46. Using Maximum Likelihood method it is observed that in figures 3 probability of false alarm does not change too much over the distance 50Km to 100Km. But it reduced to minimum value. And the probability of miss detection decreases with the distance and is 0.27 and reduced as the distance increased from primary transmitter1 to secondary user. The number of malicious users considered as 10. The radius of outer region R=500m, Radius of primary exclusive region $R0$=30m, primary transmitter power $Pt1$=100kw, primary transmitter power $Pt2$= 100kw, Malicious transmitter power Pm=4w, $\sigma p1$=8dB, $\sigma p2$=10dB, σm=5.5dB. In Maximum Likelihood method it is noted that the probability curves show symmetric around 75Km in figure 4 because we set up two transmitters equally.

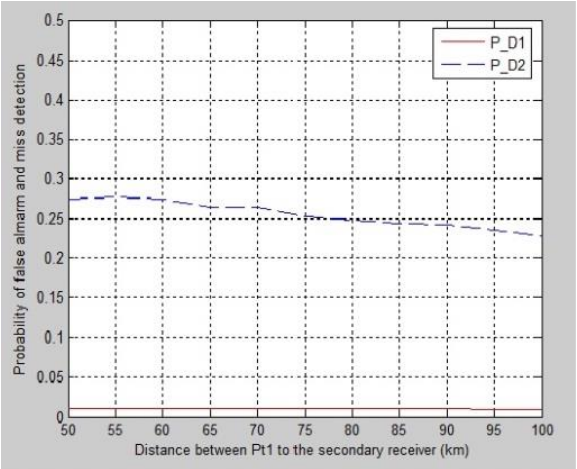

Figure 3: Probability of false alarm and miss detection

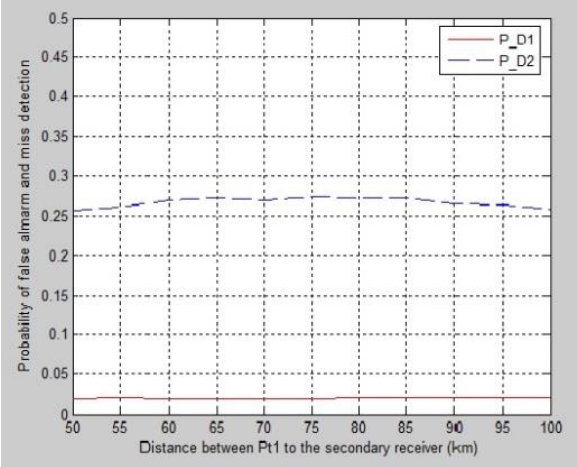

Figure 4: Probability of false alarm and miss detection

Conclusion

The probability of false alarm and miss detection in this system model with maximum likelihood criterion reduced as compared with Neyman-Pearson criterion. So the proposed system model with Maximum Likelihood criterion achieved probability of successful PUEA less than that of system model with Neyman-Pearson criterion.

Future Work

The probability of false alarm and miss detection has to reduce to zero for accurate detection of primary user transmission, to mitigate the problem of spectrum misuse by malicious secondary users.

References

[1] G. Jakimoski and K. P. Subbalakshmi, "Towards secure spectrum decision,"To appear, IEEE Intl. Conf. on Commun. (ICC'2009), Jun. 2009.

[2] Y. Wu, B. Wang, K. J. Ray Liu. "Optimal Defense against Jamming Attacks in Cognitive Radio Networks using the Markov Decision Process Approach". IEEE Globecom 2010 proceedings.

[3] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitiga-tion,"Proc., Intl. Conf. on Cognitive Radio Ori-entedWireless Networks and Commum. (Crown-Com'2008), May 2008.

[4] G. Jakimoski and K. Subbalakshmi, "Denial-of-service attacks on dynamic spectrum access networks,"IEEE CogNets Workshop, IEEE Intl. Conf. on Commun. (ICC'2008), pp. 524–528, May 2008.

[5] I. F. Akyildiz, W.-Y. Lee, K. R. Chowdhury: "CRAHNs: Cognitive Radio Ad Hoc Networks", Ad Hoc Networks, Elsevier, vol. 7, no. 5, pp. 810-836, July 2009.

[6] M. Vu, N. Devroye, V. Tarokh, "On the Primary Exclusive Region of Cognitive Networks", IEEE Transactions On Wireless Communications, vol. 8, no. 7, July 2009.

[7] R. Chen, J. M. Park, and K. Bian, "Robust dis-tributed spectrum sensing in cognitive radio net-works,"Proc., IEEE Conf. on Comp. and Com-mun. (INFOCOM'2008), pp. 1876–1884, Apr.2008

[8] Z. Chen, T. Cooklev, C. Chen and C. Pomalaza-R´aez "Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks" IEEE 28th International Performance Computing and

Communications Conference (IPCCC), 2009.

[9] Z. Jin, S. Anand, and K. P. Subbalakshmi, "NEAT: A Neighbor Assisted Spectrum Decision Protocol for Resilience against Primary User Emulation Attacks," Technical Report, Dec. 2009

[10] S. Anand, R. Chandramouli "On the Secrecy Capacity of Fading Cognitive Wireless Networks" Proc., IEEE Cognitive Radio Oriented Wireless Networks and Communications May 2008.

[11] X. Liu and Z. Ding, "ESCAPE: A Channel Evacuation Protocol for Spectrum-Agile Networks", IEEE DySPAN 2007, pp. 292-303, 2007.

[12] P. A. Frangoudis, S. Arkoulis, G. F. Marias, and G. C. Polyzos, "Incentives and Security Considerations in Distributed Spectrum Sensing", Proc. 1st Euro-NF Socioeconomics Workshop, Athens, Greece, October 2008.

[13] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar, "Ieee 802.22: The first worldwide wireless standard based on cognitive radios," Proc., IEEESymposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2005, pp. 328–337, Nov. 2005.

[14] M. Vu, N. Devroye, and V. Tarokh, "Primary exclusive region in cogni-tive networks," Proc., IEEE Consumer Communcations and Networking Conference, January 2008.

[15] R. W. Thomas, L.A. DaSilva, and A. B. Machenzie. Cognitive networks. In the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DYSPAN), 2005.

[16] Timo Weiss and Friedrich Jondral. Spectrum pooling: An innovativestrategy for the enhancement of spectrum efficiency. IEEE Communi-cations Magazine, 42(4), 2004.

[17] Xiangpeng Jing and D. Raychaudhuri. A spectrum etiquette protocol for efficient coordination of radio devices in unlicensed bands. In Proceedings of PIMRC 2003, Beijing, China, 2003.