SECURITY THREATS AND DETECTION TECHNIQUE IN COGNITIVE RADIO NETWORK WITH SENSING STRATEGIES

Sandeep Thakre[1], Shruti Dixit[2]

[1] Student, [2]Prof., EC, SIRT, Bhopal, MP, India,

Abstract

Communication world is growing day by day In wireless communication system introduces a new technology which I known as cognitive radio network its name as CRN. In CRN Un-authorized user can used empty channel from the spectrum band of authorized user this help to improve the spectrum efficiency as well generate a problem like some malicious or fake users can used the channel and hamper the communication. So in this paper we discuss on security threats and technique to find them with sensing strategies

Keywords: *Cognitive radio network, Pus, SUs, Spectrum sensing, spectrum holes*

----------***----------

1. INTRODUCTION

Communication is a process of transmitting information from one place to another through the medium information sends in the form of electromagnetic waves through the medium air. Here we see the advances in wireless communication. Cognitive radio network is advancement in wireless communication cognitive means sharing, in Cognitive radio network Un-authorized user can used empty channel from the spectrum band of authorized user. Cognitive Radio Networks (CRNs) is an intelligent network that adapt to changes in their network to make a better use of the spectrum. CRNs solve the spectrum shortage problem by allowing unlicensed users to use spectrum band of licensed user without interference, generally authorized or licensed users known as primary users and un-authorized or un-licensed users known as secondary users. When data or information send by authorized or primary user here primary user not used total band some of them are free these empty channels are allowed to used by un-authorized or secondary users .Secondary users always observe the activities of primary user, and when secondary user detect the empty channel and occupy the channel without disturbing the primary user. When the primary users are sending information or it is active, the secondary user should either avoid using the channel. An Empty channel also known as spectrum holes. A spectrum hole is a band of frequencies assigned to a primary user, but at a particular time and specific geographic location, the band is not being utilized by that user. [2].Figure-1 shows the basic structure of cognitive radio network. In this secondary user occupy the space called white space of primary user band which is under-utilized. Normally primary user has own communication area, in which secondary user utilized the empty channel without any interference

1.1Basic Cognitive Radio Network

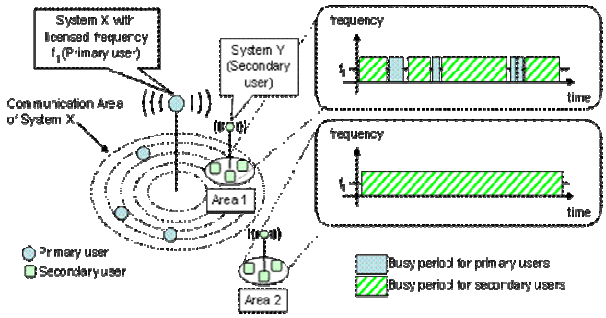


Fig.1 Basic cognitive radio network

Figure-1 shows the architecture of cognitive radio cycle. When a primary user (PU) transmits data signal from a licensed spectrum band, it may be possible that it use only few channels of spectrum other channels are empty. These empty channels are sensed by secondary user (SU) which has no license for using this spectrum. Firstly secondary users sensed the spectrum andsend the information of spectrum holes to the SU's. SU analyses the spectrum that PU ever uses these channels or not, because sometime PU use the empty channels which they not use before operation. After spectrum analysis SU's decide how many channels they required to send their data signal

1.2 Spectrum Sensing Technique

It is very important in Cognitive radio network that secondary user properly sense the empty spectrum band. In this paper we use energy sensing technique. But first look into the original bit sequences of primary and secondary

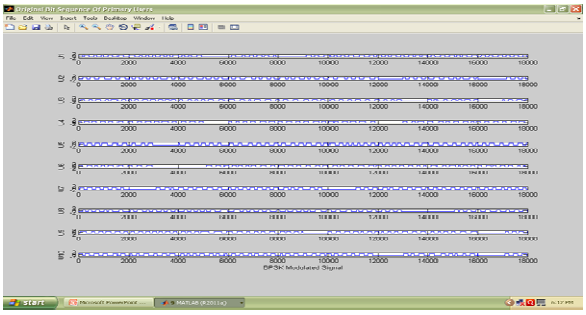


Fig2: Original bit sequence of primary user.

Figure23 shows bit sequence of primary user , whose data is send in the form of bits, but there is some holes as shown in figure as a gap in between two BPSK modulated signals. This signal gaps is nothing but an empty channels or spectrum holes.

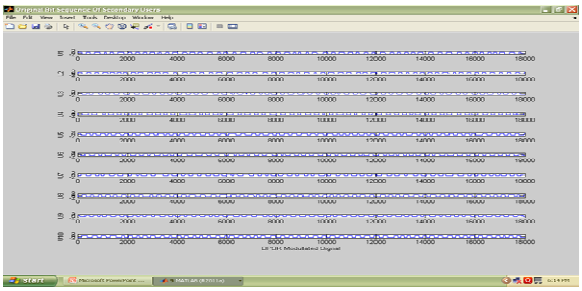


Fig 3 Original bit sequence of Secondary User

In figure 3 shows bit sequence of secondary user, we use Energy spectrum technique and find the spectrum holes or empty channel without interfering or disturbing the licensed user or primary user. In this Energy Spectrum Sensing techniques, secondary user or un-licensed user analyze the channel whether the channel have some data packets or not, if its energy level is zero then they decided that the spectrum is empty, and SU's easily send their data to the desired receiver.

2. THREATS OF COGNITIVE RADIO NETWORK

PUEs or Primary User Emulsion Attack:

Primary user emulsion attack means when primary user send data secondary user continuously monitor the channel. When primary sends data it means channel busy, secondary knows this by using energy spectrum sensing technique but primary not send continuously When it is ideal or not busystate secondary sense channel and send data but when primary requires channel then sold the control. But if somewhere else malicious or fake secondary user work as primary and wants control of channel and secondary send data at same time malicious user behaves as primary so secondary sold control and not send data such attack referred as primary user emulsion attack.Additional fake or malicious secondary users, may use a primary user emulation attacks to take advantage of the secondary user's ability to avoid primary users and cause excessive and unexpected disruptions to communications.[10] A fundamental characteristic of a CR is its ability for spectrum sensing, as it shall use the spectrum in an opportunistic manner. This means that the CR has to vacate a currently used spectrum band if an incumbent signal is detected. In this case, CR's perform spectrum hand-off seeking for different spectrum holes for transmissions. Performing spectrum hand-off very often results in degradation of the CR performance since more time for sensing of the spectrum is required, and this decreases the available time for accessing the spectrum.[3]

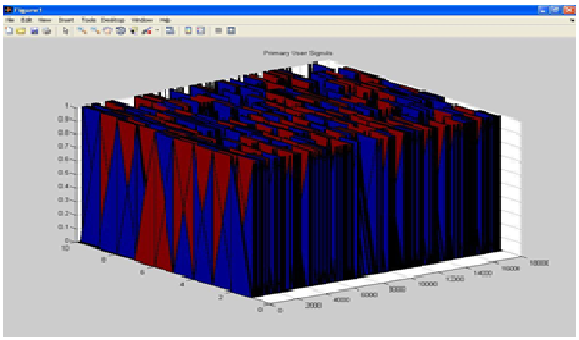


Fig4

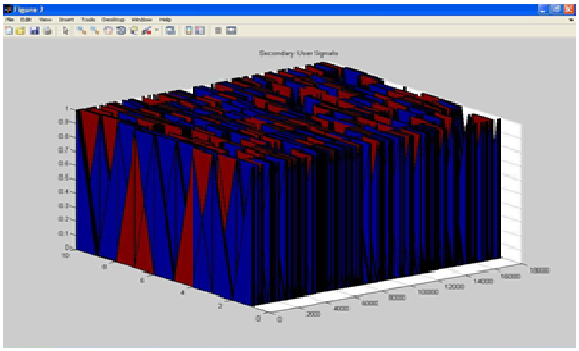
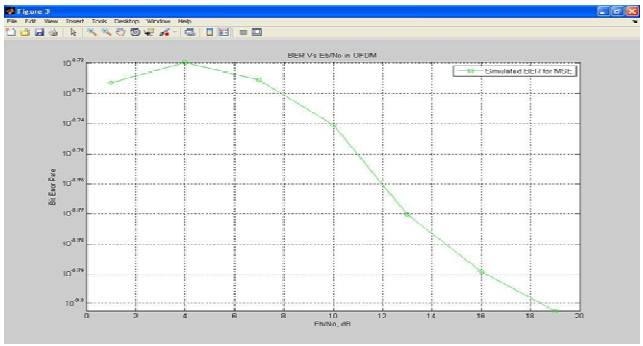


Fig5

Figure 4&5 shows Primary User Signals and Secondary User Signals for Primary User Emulsion Attack in Cognitive Radio Network. This figure shows 18000 samples for the simulation with 2 BPSK.



5 N R	1	4	7	10	13	16	19
B E R	0.18 77	0.19 07	0.18 81	0.181 7	0.16 97	0.16 24	0.1 57 6

This figure 6 shows the Bit error rate reduced continuously when Primary User Emulsion Attack occurred in network.

3. CONCLUSION

Through this paper, we practically find the threats from the wireless communication environment and sense the empty spectrum band through Energy sensing technique. Because of the practical approach of a secondary user which sense an empty channel and send their data packets without disturbing the authorized user. In this we work on two types of threats like primary user emulation attack and jamming attack .These two are the major threats of cognitive radio network wireless communication environment. Jamming is the common attack of wireless communication. It is similar to Denial of Service (DoS) attack. In future we willimprove the work on cognitive radio network and try to practically work on the security of threats.

REFERENCES

[1]F. Akyildiz, W. Lee, M. C. Vuran, S. Mohanty, “A survey on spectrum Management in Cognitive Radio Networks,” IEEE Communications Magazine, April 2008.

[2] Chetan N. Mathur, K.P. Subhalakshami, “Security issues in cognitive radio netwroks,” Cognitive network: Towards Self-Aware Networks, 2007.

[3] X. Zhang, C. Li, “Constructing secure cognitive wireless networks experiences and challenges,” Wireless Communications and Mobile Computing, vol. 10, pp. 55-69. 2009.

[4]R. Chen and J. Park “Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks,” Proc., IEEE workshop on Networking Technol. For Software Defined Radio Networks (SDR) 2006, pp. 110-119, Sep. 2006.

[5] S. Haykin, \Cognitive radio: Brain-empowered wireless communications," IEEEJ. Selected. Areas of Communications, vol.23, no.2, pp. 201-220, Feb 2005.

[6] S. Anand, Z. Jin, K. P. Subbalakshmi, “An analytical model for primary user emulation attacksin cognitive radio networks,” To appear in Proc., IEEE symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) , Oct.2008.

[7] Author-Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis “A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks” IEEE Communications Surveys & Tutorials, Accepted For Publication July-2012

[8]T. Aysal, S. Kandeepan, and R. Piesewicz, “Cooperative Spectrum Sensing with Noisy Hard Decision Transmissions,” in Proc. ICC, 2009, pp. 1–5.

[9] Y. Chen, “Collaborative spectrum sensing in the presence of secondary user interferences for lognormal shadowing,” Wireless Communications and Mobile Computing, 2010.

[10] Z. Jin, S. Anand, K. P. Subbalakshmi, “Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing,” Mobile Computing and Communications Review, vol. 13, no. 2, 200

Sandeep Bhaurao Thakre have completed diploma from Nagpur poly. Nagpur in Electronics & Communication at 2004, BE from Government college Nanded i.e. Shri Guru GobindSinghaji College of Engineering & Technology Nanded in Electronics & Telecommunication at 2007, now persuingM.Tech from Sagar Institute of Research & Technology Bhopal