A Survey on Security Issues and Primary User Emulation Attack Detection Techniques in Cognitive Radio Network

Nikita Thalia
Assistant Professor
Viva Institute of Technology, shirgaon, Virar (E)

Archana Ingle
Associate professor
Viva Institute of Technology, shirgaon, Virar (E)

Karishma Raut
Associate professor
Viva Institute of Technology, shirgaon, Virar (E)

Madhura Tilak
Assistant Professor
Viva Institute of Technology, shirgaon, Virar (E)

ABSTRACT
With the improvement in wireless technology and services, unlicensed, Industrial, Medical and Scientific (ISM) band is getting overloaded, which leads to spectrum shortage problem. On the other hand, several part of fixed allocated spectrum is underutilized. Cognitive Radio is new and intriguing technology that enables a more flexible and efficacious usage of the radio spectrum. Basically, this technology allows unlicensed users to use licensed spectrum, without interfering with the incumbent transmission. As Cognitive radio networks are wireless in nature, they suffer from all the classic threats present in traditional wireless networks. This paper focuses on an attack that poses a threat to spectrum sensing function of CR, known as Primary User Emulation Attack (PUEA). In this attack is a malicious secondary user mimics signal characteristics of a primary user to acquire channel resources without sharing with other secondary users, thus reducing spectrum usage probability and efficiency. The objective of this paper is to highlight various security issues related to dynamic spectrum access then discuss the PUEA with the existing countermeasures to mitigate it. In addition, future security challenges are addressed.

General Terms
Cognitive Radio Network, Primary User Emulation Attack, spectrum sensing, Primary User (PU), Secondary User (SU)

Keywords
Radio spectrum, defense techniques, security issues, dynamic spectrum access

1. INTRODUCTION
RADIO spectrum is the heart of wireless technology and its efficacious usage is of uttermost significance. The distribution of this valuable and limited radio frequency resource, as decided by the Federal Communication Commission (FCC), is based on conventional fixed spectrum allocation policy. This conventional policy for spectrum assignment divides the spectrum into licensed and unlicensed band [1]. In Licensed spectrum, exclusive right is provided to a selected user or wireless services and other users are not permitted to access this band, even though it is free at a particular time and location. It has been observed by the Spectrum Policy Task Force. (SPTF) that several portion of licensed spectrum is highly utilized whereas some portions are very less or partially occupied at particular location and time [1]. Measurement were taken by Shared Spectrum Company (SSC) between Jan 2004 and Aug 2005 which shows that on the average only 5.2% of the spectrum between 30MHz and 3GHz is accessed at six different locations in the U.S.A. The highest value of accessed portion was 13% at New York City and lowest was 1% at the (NRAO) National Radio Astronomy Observatory. From all the measurements, it was concluded that large portion of licensed spectrum band remains underutilized. Due to this fixed nature of traditional spectrum allocation policy, unlicensed users are prohibited from accessing the spectrum band. This low frequency spectrum utilization as shown in Fig.1.

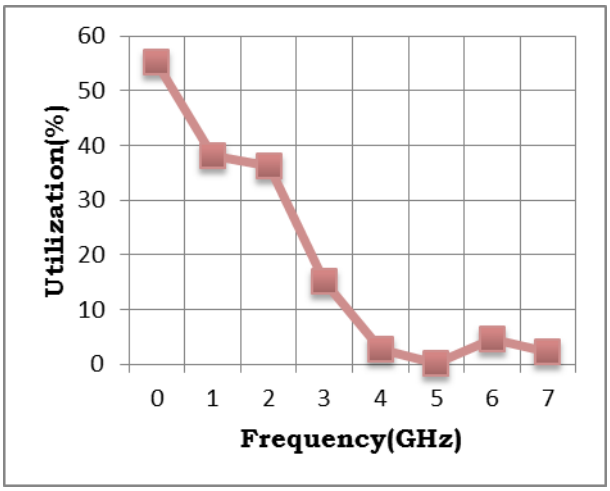

Fig 1: Spectrum underutilization [1]

Unlicensed frequency spectrums are those portions of spectrum which is kept aside for users to access free of cost. The most widely used unlicensed bands are the 2.4 GHz Industrial, Scientific and Medical (ISM) band, used by IEEE 802.11b/g/n and Bluetooth devices and the 5GHz band Unlicensed National Information Infrastructure (UNII) are used by IEEE 802.11a and European HIPERLAN standard [1],[3].

On the other hand, due to new wireless services and technology like internet, smartphones, social networking sites, these unlicensed bands are getting overcrowded which leads to a problem called spectrum scarcity. The problem is not the spectrum shortage; it is lack of the technology which can effectively access the spectrum.

This ineffective consumption of licensed spectrum and spectrum scarcity problem in unlicensed band forced Federal Communication Commission (FCC) to make modification in the existing conventional fixed spectrum allocation scheme. FCC decided to make the spectrum flexible by assigning permission unlicensed user to access licensed spectrum band

when it is idle, without causing any interference to the licensed user transmission [2].

In comparison with traditional wireless networks, there are more chances open to attackers in cognitive radio technology. As a result, security in cognitive radio networks has become a challenging task. Many general techniques proposed in the past cannot satisfy such special network needs, since the spectrum is used dynamically in cognitive radio.

The rest of the paper is organized is as follows: In section 2, spectrum sensing in Cognitive Radio significance is explained. In section 3 security issues related with dynamic spectrum access is described. Section 4 explains the effect of primary user Emulation attack on smooth operation of spectrum sensing. In section 5 different defense techniques for PUEA detection and mitigation is discussed and explained with advantage and disadvantage of existing solutions in tabular form. Finally section 6 concludes the paper by mentioning future challenges in existing techniques

2. SPECTRUM SENSING

Spectrum sensing is basic function of cognitive radio technology. In spectrum sensing operation, secondary users monitor the spectrum continuously, to identify arrival of primary users. The spaces in licensed spectrum which are not occupied by primary users are called spectrum holes or white spaces [3]. The most effective way to identify spectrum holes or white spaces is to detect the primary users that are receiving data within the communication range of a secondary user. Fig 2 shows spectrum holes or white space. Three techniques are used for spectrum sensing operation: Energy detection, matched filter detection and Cyclo-stationary detection.

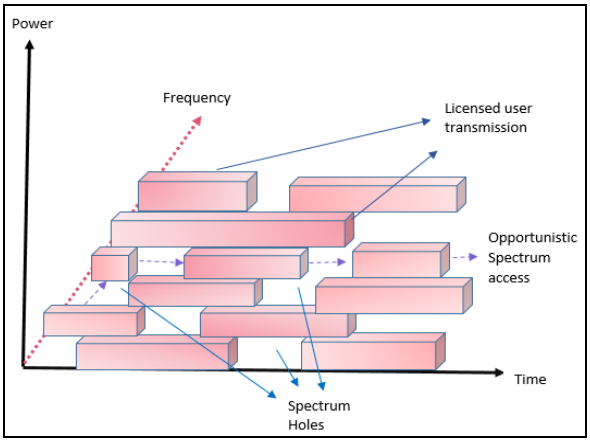

Fig 2: Spectrum Holes [1]

3. SECURITY ISSUES

To date, security issues of cognitive radio networks have become a hotspot of research activities [4]. Some work has engaged in this area which forecasts the potential susceptibilities on the structure, function and strategy of CR network that could be employed by the malicious or selfish users. Particularly, a selfish or malicious secondary user may obstruct a idle frequency band by imitating the primary user characteristics and thus prevents other secondary users from using that band

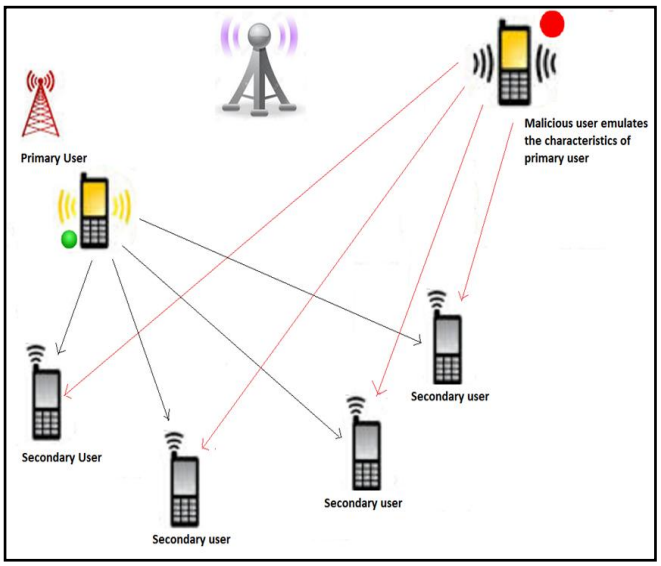

Fig 3: Primary User Emulation attack

4. PRIMARY USER EMULATION

Primary User Emulation (PUE) attack Fig.3 [11] [12 [13] is carried out by a malicious secondary user who mimics a primary user signal characteristics or behaving as a primary user to obtain the channel resources without having to share them with other cognitive users. As a result, the attacker is able to obtain full bands of a spectrum. This primary user emulation attack can be into two categories: Selfish Primary user emulation attack and Malicious Primary User Emulation attack. In the Selfish PUE attack, the attacker's objective is to increase its spectrum space from the available resources. In addition, this attack can be conducted by two attackers simultaneously to create a dedicated link between them. In the Malicious Primary User Emulation attack, the attacker's aim is to avoid genuine secondary users from using the holes found in a frequency spectrum band [5].

The task of differentiating genuine signals from secondary user signals becomes more difficult to implement when one considers the rule made by Federal Communication Commission (FCC) which states that no alteration to the primary user and its transmission system should be required to lodge opportunistic use of the frequency spectrum by secondary users. For this reason, conventional methods, such as implanting a signature in a primary user's signal or engaging in an interactive protocol between an incumbent signal transmitter and a verifier, cannot be used [17].

Physical layer is the lowermost and important layer of the OSI model and provides a transmission medium to the communication system. The CR is considered to be an intelligent radio which can adapts the surrounding environment and accesses the spectrum in dynamic fashion, which makes the operation more challenging. PUEA is one of the stern physical layer problem and a great threat to spectrum sensing [5]. So, in the next section, the PUEA with its influence on wireless communication technology users are deliberated and a detailed summary of PUEA defense techniques is specified along with its almost all existing techniques for mitigation, and some proposed solutions are highlighted[16].[17], [18], [19], [20].

5. DETECTION SCHEMES

To defend against Primary User Emulation attack, transmitting source identity needs to be verified. The regular and best way of knowing the user identity is to apply cryptographic authentication mechanisms, such as digital signatures. But such an approach cannot be adapted because of the FCC policy that forbid modifying primary user transmission systems. With this restriction and knowing that primary users' locations are known ahead of time, researchers started finding effective ways of pin pointing the transmitting source location [18], [19], [20]. If primary user location is matching with the source location, the source is treated to be a primary user. Otherwise it is considered to be an attacker trying to mimic a primary user.

Table 1. Existing defense techniques

Sr.no.	Contribution	Methodology	Advantages	Disadvantage
1.	R. Chen and J. Park[5]	Distance ratio and difference test-cryptographic authentication mechanisms	They have identified the PUE attack problem and demonstrated its disruptive effects in CR networks.	DDT requires tight synchronization among the LVs that may be expensive to implement. Both DRT and DDT can be deceived if the attacker is transmitting from the vicinity of the TV tower.
2.	R. Chen, J. Park, and J. Reed[6]	Based on localization of the primary user	Signal Energy Level is considered. Simple approach. A separate sensor network is used for attack detection so secondary users are not loaded with detection responsibilities.	Does not work as it requires modification in the primary user transmission system which does not follow FCC regulations. (i) the separate sensor network increases the distribution and maintenance costs (ii) Received signal strength is used that is very erratic (iii) Transmission power of attacker is assumed to fixed, which is not valid for practical implementation
3.	Olga León, Juan Hernández-Serrano [7]	Localization strategy that applies TDOA then FDOA	This approach is does not violate FCC rule.	Major drawback of these methods is that it depends on many assumptions that make them very restrictive and not applicable to practical cognitive technology.
6.	Z. Jin and K. Subbalakshmi [8]	Wald's sequential probability ratio test	Use of analytical models for the received power for attack detection.	(i) WSPRT is used that can lead to limitless sampling and long sensing times, and its performance degrades under dynamic environment (ii) It is assumed that there is Uniform distribution between genuine users and malicious users (iii) Major drawback of this method is that it assumes that the transmission power of the attacker is immobile
7.	Z. Jin, S. Anand, and K. Subbalakshmi [9]	Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing,	(i) The fading characteristics of the wireless environment are taken into account, (ii) multiple malicious users are considered.	(i) It is assumed that there is Uniform distribution between genuine users and malicious users (ii) it assumes that the transmission power of the attacker is immobile

9.	Y. Liu, P. Ning, and H. Dai [10]	Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures,	(i) Use of a novel physical layer authentication technique, Simulations and real implementation (ii) use of a light weight authentication protocol.	An extra node (helper node) is required for every primary transmitter.
10.	Z. Chen, T. Cooklev, C. Chen [11]	"Modeling primary user emulation attacks and defenses in cognitive radio networks,"	(i) Attackers with a changing transmission power are also considered, (ii) the detection method proposed does not depend on sensing	(i) There is a need to know attacker position in advance. (ii) The distances between the Primary Users, the Secondary Users and the attacker have to be known in advance.
11.	C. Mathur and P. Subbalakshmi [12]	Digital signatures for centralized DSA networks,"	A simple public key cryptography mechanism between Primary Users and Secondary Users.	i) Does not work as it requires modification of the primary user system which breaks FCC regulations (ii) a certification authority is needed, (iii) the proposed mechanism for encryption/decryption has several weaknesses that can lead to severe Denial of Service attacks.
12.	Shaxun Chen; Kai Zeng [13]	Hearing is believing: This is the first work dealing with PUEA with mobile FM wireless microphone as PU.	Simulation as well as Real world experiment. First work on detection of primary mobile users. Then the same method is realized in noisy environment	Here, SUs must be equipped with extra sound sensors. This is a real world experiment.
13.	Zhou Yuan; Niyato, D.; Husheng Li; Zhu Han[14], [15]	Belief propagation: To identify the attacker, a defense strategy based on belief propagation (BP).	To make this detection process more accurate, the author proposes BP framework based on Markov random field	The transmission power and transmission range of the attacker are assumed to be within a certain limit. The location of the primary user must be known to all SUs. The mean of final belief is more when the distance between PU and PUE attacker is less.
14.	Zhou, Xiao; Xiao, Yang; Li, Yuanyuan [15]	Encryption and displacement method: Encryption	Encryption algorithm is useful for defending PUEA, but if the attacker can know the information by air interception, then displacement algorithm is useful.	Workflow of entire method is verified by NS2 software. The result shows that too many users lead to packet loss.

15.	Chandrashekar, S.; Lazos [17]	PU authentication: Primary user authentication system relies on the deployment of stationary helper nodes, which authenticate PU by link signature	More number of SUs can be accommodated without the need for repeated training, and can defend the attack successfully.	The system requires extra deployment of fixed helper nodes, which must be initialized with public key and certificate from a trusted authority.

In [5], two Methods are suggested to figure out the location of the transmitting source: Distance Ratio Test (DRT) which

is depends on received signal strength measurements and Distance Difference Test (DDT) which is based on signal phase difference . Both techniques are rely on a transmitter verification procedure.

The procedure uses a location verification method to differentiate between primary and secondary signals impersonating as primary signals. Some assumptions are specified to create the environment where the attack is likely to occur. The primary users are TV broadcast towers with fixed locations, and there are several secondary user nodes within the transmission range of the towers' signals. There are trusted location verifiers (LVs) to execute DRT and DDT technique, and there are two types of LVs: master and slave LVs. A master Location Verifiers has a database record with the coordinates of the TV towers. LVs know their location using a secure GPS system. Location Verifiers analyze the

distances between them and the transmitters as they receive their signals. The received signal can be from the towers or an attacker behaving as a tower. Then the Location verifier task is to compare them to their database of towers' locations. If the result of verification fails, the signal's is considered to be an attacker [6]. For these techniques to work, the information exchanged between the verifiers must be encrypted and strictly authenticated to abstain eavesdropping, alteration or replay attacks implemented by the attacker. Different defense techniques, their advantages and disadvantages are explained in tabular form in Table 1. Below

6. CONCLUSION & FUTURE WORK

The awareness, consistency and flexibility nature of CR networks make it more precious to be organized successfully in nearby future. Along with this understanding, it has also unlocked the door for lots of threats, especially in security because of the presence of malicious nodes, who want to destroy the entire communication networks. A brief summary on safety threats, including physical, link, network and transport layer attacks is presented Finally issues in cognitive Radio which needs further development are emphasized. The most important challenge till now is need of a technique which can evade interference to stationary as well as mobile primary users. Although, some of the defense mechanisms have been proposed, they can't completely fulfill the need of CR networks operation. This leads us to our future research work which will give the ultimate solution to PUEA by considering channel approximation error into the mechanisms for detecting PUE attacker, which can support both stationary and a wireless microphone as the primary user.

7. REFERENCES

[1] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran and Shantidev Mohanty, Next Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey, Elsevier Computer Networks, Vol.50, 2006, pp.2127-2159.

[2] Mitola, J.; Maguire, G.Q., Jr., "Cognitive radio: making software radios more personal," Personal Communications, IEEE , vol.6, no.4, pp.13,18, Aug 1999.

[3] Haykin, S., "Cognitive radio: brain-empowered wireless communications," Selected Areas in Communications, IEEE Journal on , Vol. 23, no. 2, pp. 201,220, Feb. 2005.

[4] Wassim El-Hajj; Haider Safa; Mohsen Guizani, "Survey of Security issues in Cognitive Radio Network," journal of internet technology, volume 12 2011

[5] Ruiliang Chen and Jung-Min Park, Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks, First IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR), Reston, VA, September, 2006, pp.110-119.

[6] Ruiliang Chen; Jung-Min Park; Reed, J.H., "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," Selected Areas in Communications, IEEE Journal on , vol.26, no.1, pp.25,37, Jan. 2008.

[7] Olga León, Juan Hernández-Serrano, Miguel Soriano, Cooperative detection of primary user emulation attacks in CRNs, Computer Networks, Volume 56, Issue 14, 28 September 2012.

[8] Z. Jin and K. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," in Proc. ICC, 2009, pp. 1–5

[9] Z. Jin, S. Anand, and K. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," in Proc. ACM SigMobile Computing and Communication Review, 2009, pp. 74–85.

[10] Y. Liu, P. Ning, and H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," in Proc. 2010 IEEE Symposium on Security and Privacy, 2010, pp. 286–301.

[11] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in Proc. of IPCCC, 2009, pp. 208–215.

[12] C. Mathur and P. Subbalakshmi, "Digital signatures for centralized DSA networks," in Proc. 1st IEEE Workshop on Cognitive Radio Networks, 2007, pp. 1037–1041.

[13] Shaxun Chen; Kai Zeng; Mohapatra, P., "Hearing is believing: Detecting mobile primary user emulation attack in white space," *INFOCOM, 2011 Proceedings IEEE*, vol., no., pp.36, 40, 10-15 April 2011.

[14] Zhou Yuan; Niyato, D.; Husheng Li; Zhu Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," Wireless Communications and Networking *Conference (WCNC), 2011 IEEE* , vol., no., pp.599,604, 28-31 March 2011.

[15] Zhou Yuan; Niyato, D.; Husheng Li; Ju Bin Song; Zhu Han, "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks," Selected Areas in Communications, IEEE Journal on , vol.30, no.10, pp.1850,1860, November 2012.

[16] Zhou, Xiao; Xiao, Yang; Li, Yuanyuan, "Encryption and displacement based scheme of defense against Primary User Emulation Attack," Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference on , vol., no., pp.44,49, 27-30 Nov. 2011..

[17] Chandrashekar, S.; Lazos, L., "A Primary User authentication system for mobile cognitive radio networks," Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on, vol., no., pp.1, 5, 7-10 Nov. 2010.

[18] Jin, Z.; Anand, S.; Subbalakshmi, K.P., "Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks," Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE , vol., no., pp.1,5, 6-10 Dec. 2010.Y

[19] T. Charles Clancy and Nathan Goergen, Security in Cognitive Radio Networks: Threats and Mitigation, International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), Singapore, May, 2008, pp.1-8.

[20] Anand, S.; Jin, Z.; Subbalakshmi, K. P., "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks," New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on, vol., no., pp.1, 6, 14-17 Oct. 2008.