A Survey on Primary User Emulation Detection Mechanisms in Cognitive Radio Networks

V. Jayasree MPhil Research Scholar[1], R. Suganya M.Sc, MPhil[2]

[1] *Research Scholar, Department of Computer Science, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore*

[2] *Assistant professor, Department of Computer Science, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore.*

Abstract— **Cognitive radio is one of the main technologies in the wireless communications. The cognitive radio networks are composed of cognitive, spectrum-agile devices which is able to modify their network configurations according to the spectral environment. This cognitive radio provides the chance reusing portions of the spectrum temporarily for the secondary users. But security is a main issue in the cognitive radio networks. Because in the cognitive radio networks, primary user emulation attack is a harmful attack which degrades the network performance. Primary user emulation (PUE) attack is one of the harmful attacks in which an attacker sends signals as same as the primary user signals during the period of spectrum sensing so that truthful secondary users provide their consequent channels so that it causes the crucial threat in the cognitive radio network. Because of the high sensitivity of spectrum sensing the PUE attack make the serious threat in the network which degrades the network performance. So, in this survey several primary user emulation detection mechanisms are suggested to improve the network performance. The major two methods are location authentication or hardware fingerprint authentication. But these methods are not effectual in which the problem is not completely solved. These methods provide the problems in the previous methods and give idea about to develop an efficient approach.**

Keywords— **Cognitive radio network, primary user emulation attack, primary user emulation detection.**

I. INTRODUCTION

Cognitive radio (CR) is the one of the opportunistic communication technologies which is designed to exploit the maximum available licensed bandwidth for the unlicensed users. There is tremendous growth in the wireless communication devices so that there is an excessive spectrum demand and it is necessary to maximize the spectrum utilization. In the conventional spectrum management system, most of the spectrum is allocated to licensed users. The cognitive radio technology is taken in two steps: Firstly, by using the spectrum-sensing technology, it finds the available spectrum for the secondary users. If the licensed primary user is not utilizing the spectrum, the available bands are allocated to the unlicensed secondary users. For the secondary user, the available channels will be assigned by dynamic signal admittance behavior. Suppose, the primary user present in the cognitive radio network, the secondary user will instantly provide the channel to the primary user.

The main intent of the CR is to recognize the available channels for the secondary users without interfering the primary user and also with the consciousness of the adjoining environment it can adjust its internal states with the corresponding alterations in certain operating parameters like transmit power, carrier frequency, modulation type etc. [1]. There are many challenges in the CR because of the unique features of the cognitive radio and unreliable nature of wireless communication channel. The unique features of the CR give the chance for the attackers to introduce a new threat to damage the normal activities of the network.

Security [2] is a significant deliberation in the cognitive radio networks. One of the harmful attacks in the cognitive radio is primary user emulation (PUE) attack originally projected in [3] [4] [5]. In this type of attack, the attacker sends the signals as same as the primary users during the spectrum sensing period and degrade the performance of the network. But the actual primary users are not present in the network. While a very weak signal, e.g. far below the noise level, can 'scare' away the honest secondary users because of the high sensitivity of spectrum sensing.

In the following survey several mitigating techniques are suggested for mitigating the primary user emulation attacks in the cognitive radio networks. The existing methods of the PUE attacks can be categorized into two types: one is detection approach and another one is defense approach. The approach for defense based schemes [6] is same as for the anti-jamming. The secondary user does not aware of the signal from the primary user or attacker. It basically senses the channels, and chooses an idle channel for communications by using some game theoretic methods which increase the opportunity to escape from the attackers. However, this approach is not effectual for PUE attacks launched by selfish SUs, which have the interior knowledge of a CRN. Also this method is not applicable for Sybil PUE attacks where one malicious user launches many attacks on different channels concurrently [7]. The detection based methods targets to authenticate if the transmitter of a PU signal is a PU or an attacker [8]–[9]. There are some detection approaches like location certification or hardware fingerprint authentication. While the existing studies on PUE detection are promising, the trouble is not entirely solved.

II. PRIMARY USER EMULATION DETECTION MECHANISMS

Husheng Li et.al [6] presented passive anti-PUE approach which is same as the random frequency hopping in the conventional anti-jamming schemes, is projected and called dogfight in spectrum. The main objective is to develop the theories of game and learning for the honest secondary users. The major dissimilarity between the approaches in this work and also the proactive methods is: the result of the spectrum sensing is avoided if the secondary users proactively discover that the signal is not from a primary user; in a sharp difference, the secondary users must obey the spectrum sensing results in the approaches studied in this work. As a result, the proactive approach is applied in the single channel systems whereas the method works in only multiple channel systems. Meanwhile, the proactive approach necessitates the ability of discriminating primary and secondary users, which is complicated to accomplish in signal processing.

Yi Tan et.al [7] investigated a new category of the denial-of-service attack on dynamic spectrum access networks – Sybil enabled attack. In this type of attack, the attacker not only creates the primary user emulation (PUE) and also penetrates multiple Sybil identities to concession the decision making process of the secondary network through Byzantine attacks. This attack is implemented in the cognitive radio test to show the possibility and attack impact. Furthermore, analyze the optimal attack strategy from the perspective of the malicious attacker, i.e., the most favorable allotment of Sybil interfaces for dissimilar attacks, to exploit the impact on the secondary network. Under the two different scenarios the attack models are analyzed: with and without a reputation system in the network fusion center. But the drawback is this method is not effectual for Sybil PUE attacks where one malicious user launches many attacks on dissimilar channels concurrently.

Nam Tuan Nguyen et.al [10] suggested a passive, nonparametric classification technique for deciding the number of transmitting devices in the PU spectrum. This method is named as DECLOAK, is passive while the sensing device take note and captures signals without introducing any signal to the wireless environment. It is nonparametric due to the number of active devices desires not to be known as a priori. Channel independent features are chosen forming fingerprints for devices, which cannot be changed postproduction. For categorizing the extracted fingerprints, the infinite Gaussian mixture model (IGMM) is adopted and a modified collapsed Gibbs sampling method is presented. Because of the unsupervised nature, there is no necessitate to gather legitimate PU fingerprints. The integration with the received power and device MAC address, the simulation is shown in which the presented method can effectually discover the PUE attack.

Ruiliang Chen et.al [9] suggested localization based Defense method for mitigating primary user emulation (PUE) attack. For authenticating the primary signal transmitters, this method utilizes both signal distinctiveness and position of the signal transmitter. To detect the PUE attacks and pinpoint attackers, a robust non-interactive localization method is used. This localization method utilizes a primary wireless sensor network to gather snapshots of received signal strength (RSS) dimensions in the CR network. By smoothing the gathered RSS measurements and finding the RSS peaks, one can compute the transmitter locations. But the disadvantage is some difficulties in the spectrum access and software protection.

Shaxun Chen et.al [11] presented a new method for discovering wireless microphone emulation attacks. In the cognitive radio networks, an attacker transmits signals whose distinctiveness emulates those of primary users, in order to avoid secondary users from transmitting. This type of attack is named as primary user emulation (PUE) attacks. In the white space there are two main categories of primary users: one is TV towers and another one wireless microphones. So, in this method to distinguish the attacks every secondary user outfitted with an acoustic sensor. The correlations between energy level of RF signal and acoustic information received by the sensor are demoralized to validate the faithfulness of wireless microphones.

Bin Zhao et.al [12] presented a method called entirely unsupervised dynamic sparse coding method for discovering unusual events in videos. This method identifies the unusual events according to the online sparse reconstructibility of query signals from an atomically learned event dictionary, which structure sparse coding bases. According to the intuition that usual events in a video are more probable to be reconstructible from an event dictionary, while unusual events are not, this algorithm utilizes a principled convex optimization formulation which facilitates both a sparse reconstruction code, and an online dictionary to be jointly inferred and updated. This method is entirely unsupervised, making no preceding postulations of what unusual events may look like and the settings of the cameras. The bases dictionary is updated in an online fashion. This algorithm examines more data, evades any concerns with concept drift.

Zhou Yuan et.al [13] suggested a method called received signal strength (RSS)-based defense system for detecting the PUE attacks in the cognitive radio network. By evaluating the allocation of the received signal power from the suspect and that from the primary user, every secondary user can have an approximate belief about the probability that whether there is the PUE attacker or not, while the secondary user has no acquaintance about the transmission output power of the attacker, and also the distance from the attacker to the secondary user. A defense method based on belief propagation is suggested for precisely identify [13] the attacker. In the CR, if the primary user is inactive the PUE attacker will transmit the primary user emulation signals for degrading the

cognitive radio network. Whenever the secondary user receives this signal, the local clarifications are executed after that use the belief propagation for exchanging the information for discovering whether the signal is from a PUE attacker to not. The local estimation of the suspect is calculated and computes the compatibility functions for modeling the relations between neighboring users and update and exchange messages with the neighboring users in an iterative way using BP. The PUE attacker can be identified based on the mean of the entire beliefs. The mean of the final belief values is lower than threshold the suspect can be identified as an attacker. Else, the suspect is seen as an honest secondary user. Finally, all the secondary users in the network will be informed in a broadcast way about the PUE attacker's distinctiveness, and disregard the PUE attacker's primary emulation signal in the future.

Shaxun Chen et.al [14] suggested a new method for identifying the emulation attack of wireless microphones. Because in the cognitive radio networks, an attacker broadcasts the signals impersonating the distinctiveness of primary signals, in order to avoid secondary users from transmitting. This category of attack is named primary user emulation (PUE) attack. There are two categories of the primary users: TV towers and wireless microphones. The previous work only concentrated on the first category. The primary users are mobile and their transmission power is low. So, these unique properties posses main disputes on PUE detection and existing methods are not pertinent. In this method, every secondary user is outfitted with an acoustic sensor. To authenticate the wireless microphones, the association between the energy level of the RF signals and the acoustic information received by the sensor are demoralized.

Alexandros G. Fragkiadakis et.al [15] suggested Security threats and detection techniques in the cognitive radio networks. Due to the tremendous growth in the wireless technologies, the spectrum demand is a major problem. So, to reduce the spectrum demand the opportunistic idea is used which reuses the spectrum band which is called cognitive radios and cognitive radio networks. Cognitive radios have enabled the prospect to transmit in numerous licensed bands without causing destructive interference to licensed users. But the problem is security threats in the cognitive radio network. There are two main distinctiveness of cognitive radios in the security threats: cognitive capability, and reconfigurability. A threat associated to the cognitive capability contains attacks launched by attackers that reduce the primary transmissions and transmits the false observations associated to the spectrum sensing. Reconfiguration can be demoralized by attackers through the utilization of malicious code established in cognitive radios. Additionally, due to the wireless nature of the cognitive radio there are many security challenges.

Jianchao Yang et.al [16] presented a mixture sparse coding method which produce high-dimensional sparse demonstrations very proficiently. In addition to the computational advantage, this model efficiently encourages data that are analogous to each other to like similar sparse depictions. This method can be observed as estimation to the newly proposed local coordinate coding (LCC). The computation mentions that the sparse coding generally learns the nonlinear manifold of the sensory data in a locally linear manner. Consequently, by utilizing the mixture sparse coding method the feature is learned with the linear classifiers.

ANALYSIS OF PRIMARY USER EMULATION DETECTION MECHANISMS

S.NO	TITLE	AUTHOR	METHOD	ADVANTAGES	DISADVANTAGES
1.	Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics	Husheng Li and Zhu Han	Passive anti-PUE approach	Applicable for both the single defender, multiple defender.	Not effective for PUE attacks launched by selfish SUs.
2.	Using Sybil Identities for	Yi Tan, Kai Hong,	New Sybil-enabled DoS	Highly secure.	Complexity is high.

	Primary User Emulation and Byzantine Attacks in DSA Networks	Shamik Sengupta, K.P. Subbalakshmi	attack		
3.	On Identifying Primary User Emulation Attacks in Cognitive Radio Systems Using Nonparametric Bayesian Classification	Nam Tuan Nguyen, Rong Zheng, and Zhu Han	Passive, nonparametric classification method	High performance is achieved.	Does not consider other security applications.
4.	Defense against Primary User Emulation Attacks in Cognitive Radio Networks	Ruiliang Chen, Jung-Min Park, and Jeffrey H. Reed	Localization based defense method	Highly effective in identifying PUE attacks under certain conditions.	Spectrum access and software protection is not addressed.
5.	Hearing is Believing: Detecting Mobile Primary User Emulation Attack in White Space	Shaxun Chen, Kai Zeng, Prasant Mohapatra	Novel method to detect the PUE attack	Achieves both false positive rate and false negative rate lower than 0.1.	Does not consider the correct detection time.
6.	Online Detection of Unusual Events in Videos via Dynamic Sparse Coding	Bin Zhao, Li Fei-Fei, Eric P. Xing	Fully unsupervised dynamic sparse coding approach	High efficiency.	Less secure.
7.	Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks	Zhou Yuan, Dusit Niyato, Husheng Li, Ju Bin Song, and Zhu Han	Defense strategy	High effective to detect the PUE attacker.	Not effective for Sybil PUE attacks.
8.	Hearing Is Believing: Detecting Wireless Microphone Emulation Attacks in White Space	Shaxun Chen, Kai Zeng, and Prasant Mohapatra	Novel method to detect the emulation attack	Achieves both false positive rate and false negative rate lower than 0.1 even in a noisy environment	High computation cost.
9.	A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks	Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis	Detection Techniques	Detect the PUE attacks.	Not efficient.

10.	E_cient Highly Over-Complete Sparse Coding using a Mixture Model	Jianchao Yang, Kai Yu, and Thomas Huang	Mixture sparse coding model	Improves the performance.	Descriptor mixture modeling and the sparse codes pooling are not considered.

III. CONCLUSION

There is tremendous growth in the wireless technologies so that there is high spectrum demand. So, spectrum scarcity is a main problem in the wireless networks. So, cognitive radio technology is a used which facilitates the opportunistic use of the frequency bands which is called cognitive radios. But the security is an important consideration. Specifically, the unlicensed secondary users get the channels whenever the channel is not utilized by the primary users. Sometimes the attackers act as a primary user and get the channels from the secondary users. This is called as primary user emulation (PUE) attacks. So, in this survey various detection methods are presented for the primary user emulation attacks. There are some disadvantages of these methods like computation complexity and less secure. At the end of this survey conclude that efficient mechanism is proposed to detect the primary user emulation attacks.

REFERENCES

[1] [1] 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.

[2] [2] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," in *Proc. IEEE Int. Workshop Mobile Multimedia Communications*, pp. 3–10, 1999.

[3] [3] K. Bian and J.-M. Park, "Security vulnerabilities in IEEE 802.22," in *Proc. Fourth International Wireless Internet Conference (WICON)*, Nov. 2008.

[4] [4] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE Conference on Computer Communications (Infocom)*, 2008.

[5] [5] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, Jan. 2008.

[6] [6] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part II: Unknown channel statistics," *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 274–283, Jan. 2011.

[7] [7] Y. Tan, K. Hong, S. Sengupta, and K. Subbalakshmi, "Using Sybil identities for primary user emulation and byzantine attacks in dsa networks," in *Proc. IEEE GLOBECOM*, Houston, TX, USA, 2011.

[8] [8] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in *Proc. IEEE WCNC*, Cancun, Mexico, 2011.

[9] [9] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[10] [10] N. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems use nonparametric Bayesian classification," *IEEE Trans. Signal Process.* vol. 60, no. 3, pp. 1432–1445, Mar. 2012.

[11] [11] S. Chen, K. Zeng, and P. Mohapatra, "Hearing is believing: Detecting mobile primary user emulation attack in white space," in *Proc. IEEE INFOCOM*, 2011.

[12] [12] Bin Zhao, Li Fei-Fei, Eric P. Xing," Online Detection of Unusual Events in Videos via Dynamic Sparse Coding," Proceedings of the 2011 IEEE Conference on Computer Vision and Pattern Recognition, pp. 3313-3320, 2011.

[13] [13] Zhou Yuan, Dusit Niyato, Husheng Li, Ju Bin Song, and Zhu Han," Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks," IEEE journal on selected areas in communications, vol. 30, no. 10, November 2012.

[14] [14] Shaxun Chen, Kai Zeng, and Prasant Mohapatra," Hearing Is Believing: Detecting Wireless Microphone Emulation Attacks in White Space," IEEE Transactions On Mobile Computing, Vol. 12, No. 3, March 2013.

[15] [15] 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, Vol. 15, No. 1, First Quarter 2013.

[16] [16] J. Yang, K. Yu, and T. Huang, "Efficient highly over-complete sparse coding using a mixture model," in *Proc. 11th ECCV*, Heraklion, Greece, 2010, pp. 113–126.