Emulation Attack in Cognitive Radio Networks: A study

Ms. Shikha Jain
Department of Computer Science,
BR Ambedkar College, Delhi University, India

Ms. Anshu Dhawan, Dr. C.K Jha
Computer Science & Engg. Banasthali Vidyapith
AIM & ACT, Banasthali University, Rajasthan, India

A latest communication technology named "Cognitive Radio Network" is a network in which an un-licensed user can use a freed channel in a spectrum band of licensed user. One of the spectrum management functions is spectrum sensing which the most critical function in the entire communication. If there will be any discrepancy in its functioning then the entire network will be disturbed which would make the network prone to attacks. One such attack is primary User Emulation Attack (PUEA) which dwindle the spectrum access likelihood of proper functioning. The objective of this paper is to give a variety of security requirements for cognitive radio networks and then discusses the PUEA with the preventive procedures to mitigate it.

Keyword: Cognitive Radio Networks (CRNs), Primary User Emulation Attack (PUEA), Primary users (PUs), Secondary users(SUs).

I. INTRODUCTION

Spectrum scarcity necessitates an important aspect of wireless communication systems that is spectrum sharing. Maguire and Mitola coined the term cognitive radio for the first time in 1999[1]. Cognitive radios are the devices having the capability to share spectrum among them. Cognitive radio nodes form an intelligent and self operating network called Cognitive Radio Network (CRN) which can adapt to spectrum changes in the network for betterment of the spectrum usage problem. There are 2 types of users in a cognitive radio network. One are licensed users, also known as primary users (PUs) which are the license holders of some spectrum bands and can use these bands whenever required. Other ones are unlicensed users which are also known as secondary users (SUs) who do not have the spectrum license but can use these spectrum bands whenever available i.e. when PUs are not using them. PUs while communicating among them uses some of the frequency channels in their licensed bands leaving rest of them as empty. These empty channels are called as spectrum holes in [2]. These spectrum holes are then used by the SUs for their communication purposes. But SUs continuously observe the activities of PUs and occupy only the left vacant bands of them without interfering with their communication process. One such practical example of cognitive radio network in [3] is the utilization of white spaces which are spectrum holes in television band. In this network scenario, TV transmitter device acts as PU transmitter and TV subscribers act as PU receivers. Other wireless devices who want to use the available white spaces in between this communication become the SUs of the network. After identification of the spectrum holes, SUs can utilize these holes in 3 ways: (a) opportunistically, (b) periodically and (c) probabilistically depending upon the properties of the mechanism used. Meanwhile if a SU detects any PU signal in its currently used band it should vacate this band for PUs and senses another vacant band in its environment and switches to new sensed hole. Essential security mechanisms should be used for successful deployment of cognitive radio networks (CRNs) to prevent misuse of valuable spectrum bandwidth.

II. ARCHITECTURE OF CRNS

[4] Describes 3 kinds of basic components for any cognitive radio network architecture. These are (a) Mobile Station (MS), (b) Base Station (BS) / Access point (AP) and (c) Backbone / Core network. These components can be used to propose following network architectures:

- Infrastructure Based: In infrastructure based architecture a MS can access a BS in a one hop manner. Therefore MSs under the transmission of same BS will communicate with each other through BS.
- Ad hoc Architecture : This is an infrastructure-less architecture in which MSs communicate with each

other using existing communication protocols like Bluetooth and Wi-Fi etc using spectrum holes.

- Mesh Architecture: Mesh architecture is a combination of both above defined architectures i.e. infrastructure based architecture and ad hoc architecture.

III. Security Requirements in CRN

Due to fast advancement in wireless communication along with need for high data rate has augmented the need of spectrum resource. Because of unreliable nature of wireless communication, CRNs faces many research challenges. The security is one of the major concerns amongst all. This gives various opportunities to malicious users to initiate a new suite of threats targeting to damage the communication networks. Various security requirements of cognitive networks like authentication, integrity, identification, authorization, availability confidentiality and non- repudiation need to be handled in order to analyze and enhance security aspects. CRNs have high sensitivity towards weak primary signals and unknown primary receiver location. Each of these vulnerabilities can be utilized by malicious users to perform attacks at various layers of the protocol stack.

The concept behind CRNs is to have intrinsic intelligence potential to detect and avert intrusions and attacks on the communication network. Even then they are vulnerable to attacks. The fundamental idea behind CRNs is that it offers flexible methods which would keep the intruders out of the network. In order to make communication network more robust and resilient to attacks, the defense mechanism should be implemented at various layers of the stack

IV. Primary User Emulation Attack in CRN

The key technology which facilitated this tedious task of spectrum sharing is dynamic spectrum access (DSA) [5], [6]. DSA technology requires the SUs to sense their spectrum environment correctly and avoid interference with PUs. This distinguishing requirement of spectrum access in CRNs can be exploited by the attackers and raises new security implications. Cooperative spectrum sensing which is described as a tool in [7], [8], [9], [10] to significantly improve the accuracy of spectrum sensing, also invites new security threats to the system. Primary user emulation (PUE) attack is one such physical layer threat on spectrum sensing mechanism [11], [12], [13]. PUE attack is an outsider attack, targeting both collaborative and non collaborative spectrum sensing. Another type of attack is insider attack that targets collaborative spectrum sensing.

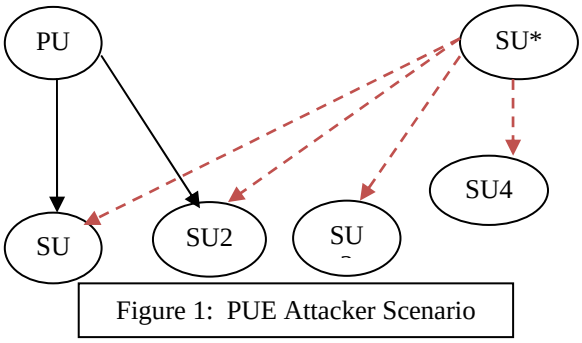

Figure 1: PUE Attacker Scenario

In collaborative sensing schemes, SUs are often assumed to report their sensing information honestly. The malicious nodes affect the nodes in the scenario and can send counterfeit sensing information to deceive the entire network. In PUE attack, a malicious SU emulates as licensed PUs to fully occupy the given channel without sharing with other genuine SUs. This can be made possible by highly flexible software-based air interface of SUs. PUE attack results in denial-of-service (DoS) on SUs in the network. For example a number of SUs can forge the PU's signal properties and generate enough power at genuine SUs locations to confuse them with PU transmission. As result the genuine SUs will vacate the spectrum which leads to poor spectrum usage by authorized users and an unfair advantage for PUE attackers. Hence PUE attacker node does not aim to cause interference to PUs transmission but to pre-empt the spectrum resources from other SUs. The motivation behind the PUE attack classifies this attack in 2 categories [13]:

1) Selfish PUEA: In this attack, a selfish node attempts to exploit maximum spectrum usage. When a node senses an unutilized spectrum band, they start imitating the signal similar to that of PU and stop other SUs from competing for that band by transmitting signals.
2) Malicious PUEA: In this attack DSA process of legal SUs is blocked. It avoids genuine SUs from detecting and using unutilized licensed spectrum bands. It grounds for denial of service. As oppose to selfish attacker, a malicious attacker may or may not use bare spectrum band for its own communiqué.

Fig [1] illustrates PUEA attack. In this network scenario there are 4 SUs (SU1, SU2, SU3, and SU4), 1 PU and 1 PUE attacker (SU*). The attacker emulates the characteristics of PU signal and starts communication in the network. Other SUs by considering it as PU vacates spectrum band resulting in performance and quality degradation of the network.

In [11] PUE attack, malicious node behaves in the similar fashion as that of PU. It pretends to be like PU to fool SUs so that they leave the channel straight away causing interruption

in the entire communication. PUE attack causes disturbance in the spectrum sensing process and considerably decreases available bandwidth resource for genuine SUs. There can be two possibilities in such attacks. Generally, almost all the channels are negatively influenced by both malicious users and greedy users [14]. This attack is commenced and communication is interrupted or hold-up when there is no free channel left for SU. A delayed communication is not reliable and also degrades the quality of service [15].

V. DEFENCE TECHNIQUES AGAINST PUE ATTACK

In [11] authors have proposed two dimensional methods to prevent PUE attack. One of the methods is Distance Ratio Test (DRT) and other is Distance Difference Test (DDT). DRT is based on the measurements of the signal received where as DDT is based on phase difference of the malicious user and PU transmitter from the SU to sense the invader node. In [12] authors have proposed that defence mechanism is based on primary transmitter localization. Directional antennas were proposed to determine the angle of arrival of the primary signal. The time of arrival and the received signal strength is calculated for SUs to agree on the location of the primary transmitter.

Authors have discussed [13] a threat which is not directly related to PUEA. It considers a scenario in which spectrum sensing is made by using a hypothesis testing. It is used for detection purpose. Due to deceitful report of spectrum sensing, a byzantine failure model and a weighted sequential ratio test was projected to prevail over this kind of security hit. They proposed a transmitter verification scheme for spectrum sensing which is suitable for unfriendly surrounding area.

Authors aim on the problem of primary signal transmitter (PST) localization problem. A transmitter verification scheme, which works in three stages, verification of signal characteristics, measurement of received signal energy level, and localization of the signal source is called LocDef. It validates if a given signal is that of a present transmitter by doing approximation of location and monitoring its signal characteristics. For estimation, LocDef utilizes a non-interactive localization scheme. In order to collect the snapshot of received signal strength (RSS) across the CR network, the localization scheme utilizes its underlying wireless sensor network (WSN). It then makes out and approximates the transmitter locations. Therefore, LocDef can be incorporated into current spectrum sensing schemes to improve the sensing decisions. An invader node tries to attempt the location-based detection approach by transmitting its signals in the environs of one of the TV towers. In order to sense PUEA, the signal's energy level together with the signal source's location is used. Once an occurrence of a PUEA is sensed, the estimated signal location can be then used to locate the invader node.

In [3] authors have claimed a logical and analytic method which is based on Fenton's approximation and Markov inequality. This is being done by keeping in view few assumptions [16] like losses due to decrease in signal strength, diminishing and variation of the energy detection mechanism. It has acquired a minimal possibility of a definite attack on a SU. A group of collaborative malicious users initiates this attack. The likelihood of success is greatly enhanced and is dependent on the distance between transmitter and SU.

The receiving end of the power equation at SU level is distributed unevenly and Fenton's approximation is applied to achieve the mean and variance of the receiving power. By using Markov inequality along with these derived values they determined a minimal probability value of a successful attacker. Each SU calculates the received power from any other user and compares it with its two thresholds values. If the measured signal power lies in above range, then the primary transmission is detected and SUs try to cease themselves from using the spectrum space. Otherwise, the SUs have concluded that there exists a white space. When there is difference between the received powers from the primary transmitter and the malicious users and also it is below a particular threshold bound, then it concludes that an attack has occurred i.e. there is some malicious node in the network scenario. It shows that their set bounds facilitate in obtaining possible ranges of limited area in which an attack is expected to occur.

[17] Proposed a reliable AES-encrypted DTV scheme, in which an AES-encrypted reference signals, is produced. It is used as the sync bytes of each DTV data frame. With the help of this a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver. It can then be used to accomplish precise detection of authorized PUs. This proposal necessitates no modification in hardware or system structure except of a plug-in AES chip. It can also be applied to today's DTV system directly to diminish PUEA, and achieve efficient spectrum sharing. In the DTV system, the generated AES-encrypted reference signal is also used for synchronization purposes at the authorized receivers. The proposed representation diminishes PUEA, enabling robust system operation, and guarantees resourceful spectrum sharing. The efficiency of the proposed approach is verified through both mathematical derivations. The PU generates a pseudo-random AES-encrypted reference signal thereby highlighting that synchronization is definite in the proposed model.

VI. Conclusion

There are few of the crucial features of CRNs like awareness, reliability and adaptability need to be deployed successfully for better communication. At the same time preventing the network from threats and malicious intent is equally important and a challenging task. The physical layer is significant in terms of detection of this malicious node. PUEA is one of the security issues in the physical layer of the protocol stack. The modus operandi of this paper is the mitigation methods for PUEA. The defensive system have been proposed, but still advancement is required to achieve

the definitive solutions to PUEA by taking into consideration channel evaluation technique into the detection scheme which is supportive in both static and dynamic environments.

References

[1] Mitola III J, Maguire Jr G. Cognitive radio: making software radios more personal. *Personal Communications, IEEE* [*see also IEEE Wireless Communications*] 1999; 6(4):13–18. DOI: 10.1109/98.788210.

[2] C. Xin, B. Xie, and C. Shen, "A novel layered graph model for topology formation and routing in dynamic spectrum access networks," in Proc. of IEEE DySPAN, 2005.

[3] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for PUEA in cognitive radio networks," in Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2008, Oct. 2008.

[4] T.Lakshmibai, B.Chandrasekaran " PRIMARY USER AUTHENTICATION IN COGNITIVE RADIO NETWORKS: A SURVEY", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2014

[5] P. Leaves, K. Moessner, R. Tafazoli, D. Grandblaise, D. Bourse, R. Tonjes, M. Breveglieri, Dynamic spectrum allocation in composite reconfigurable wireless networks, IEEE Comm. Magazine, vol. 42, May 2004, pp. 72–81.

[6] S. Haykin "Cognitive radio: brain-empowered wireless communications", IEEE J. Select. Areas Commun., vol. 23, no. 2, pp.201 -220 2005.

[7] G. Ganesan and Y. Li "Cooperative spectrum sensing in cognitive radio networks", *Proc. IEEE DySPAN*, pp.137 -143 2005.

[8] S. M. Mishra , A. Sahai and R. Brodersen *Cooperative sensing among cognitive radios*, 2006.

[9] S. Shankar, C. Cordeiro and K. Challapali "Spectrum agile radios: utilization and sensing architectures", Proc. *IEEE DySPAN*, pp.160 -169 2005.

[10] J. S. Simonoff Smoothing *Methods in Statistics*, 1996: Springer-Verlag.

[11] R. Chen and J. M. 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.

[12] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," Proc., IEEE Conference on Computer Communications (INFOCOM) 2008 mini-conference, Apr. 2008.

[13] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Jl. on Sel. Areas in Commun.: Spl. Issue on Cognitive Radio Theory and Applications, vol. 26, no. 1, pp. 25-37, Jan. 2008.

[14] Jin, Z. Anand, S., "Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks," Communications, IEEE Transactions, vol.60, no.9, pp.2635, 2643, September 2012.

[15] Jin, Z.; Anand, S.; Subbalakshmi, K. P., "Performance Analysis of Dynamic Spectrum Access Networks under Primary User Emulation Attacks," Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, vol., no., pp.1, 5, 6-10 Dec. 2010.

[16] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio: A survey," Elsevier Journal on Computer Networks, vol. 50, pp. 2127-2158, May 2006.

[17] Ahmed Alahmadi Mai Abdelhakim, "Mitigating Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption standard, Globecom- Signal Processing for Communications Symposium, 2013

Author's Profile

Ms. Shikha Jain is an Assistant Professor in the Department of Computer Science, BR Ambedkar College of the Delhi University,India. Shikha Jain received her B.Sc. degree (First class Hons.) in Physics from Delhi University, India in 2008 and the M.Sc. degree from the Institute of Informatics and Communication, University of Delhi South Campus, India in 2010. Her research interests include cognitive radio, delay tolerant networks, security in wireless networking, and Ad-hoc networks.

Ms. Anshu Dhawan worked as Assistant Professor in the department of Computer Science in various colleges affiliated to G.G.S I.P University. She holds eight years of teaching experience. She graduated in B.Sc (Hons.) with distinction from Miranda House, North Campus, Delhi University, India in 2002. She received her MCA degree with distinction from Banasthali Vidyapith, Rajasthan, in 2005. She has strong interest in research and currently pursing Ph.D. in computer Science from Banasthali Vidyapith. Her research interests lie in wireless networks particularly in Cognitive Radio Ad-hoc Networks.

Dr. C. K Jha is an Associate Professor in the *Computer Science & Engg. AIM & ACT Banasthali Vidyapith.* .His research interests lie in Advanced Networks, DBMS, Web Enabled Services, Localization, Performance Analysis, Wireless networks.