ISSN : 2231-0711

A Study on Primary User Emulation Attack in Cognitive Radio Networks

C.Kiruthika
P.G. Scholar
Department of Computer Science and Engineering
SNS College of Engineering, Sathy main road,
Coimbatore-641035,Tamil Nadu, India.
kiruthikarc91@gmail.com

A.C.Sumathi
Associate Professor
Department of Computer Science and Engineering
SNS College of Engineering, Sathy main road,
Coimbatore-641035,Tamil Nadu, India.
Sumathi.ac@gmail.com

Abstract - **CR is an emerging technology in wireless communications. Based on their operating environment CRNs can dynamically reconfigure their characteristcics. So that many security issues has been an alarming fact to CRNs. One such attack is the Primary User Emulation Attack (PUEA). There are many techniques available to mitigate this attack. This paper presents a study about various defense techniques of PUEA and provide better solutions to defend against PUEA.**

Keywords – Cognitive Raio Networks(CRN), Primary User Emulation Attack (PUEA), PUEA defense.

I. INTRODUCTION

The Federal Communication Commission (FCC) defined Cognitive radio (CR) as the radio that can change its transmission parameters based on interaction with the environment in which it operates [1].

The Wireless communication has been increased and requirement of high data rate has also been increased. The licensed spectrum space remains idle at most of the times [1] due to inefficient allocation of frequencies and the cellular bands are overloaded. To meet the spectrum demands and to utilize the spectrum, FCC revisited the problem of spectrum management [2]. This inventiveness focused on Cognitive Radio (CR). The IEEE 802.22 is the standard for cognitive wireless regional area networks (WRANs). The main goal of CR is to identify the unused licensed spectrum for secondary users without causing interference to the Primary User (PU). As the Cognitive Radio can dynamically adapt to its operating environment they face many security issues [3].

Due to Dynamic Spectrum Access (DSA) CR network gives opportunity to the attacker to damage the routine activities of the communication networks. CR are capable of sensing the unused spectrum—i.e., spectrum “whitespaces” [4]. The key problem is to distinguish the primary user signal from the secondary user in an efficient way. On the other hand, the detection of Primary User Emulation (PUE) attack is important. The secondary users must sense and identify the emulation attacker.

Organization of this paper is as follows: section II describes the overview of security issues in CRNs. In section III gives details of PUEA in CRNs. In section IV the existing defense techniques. In section V some solutions for better performance are given. Finally, section VI concludes with the future work.

II. OVERVIEW OF SECURITY ISSUES

The dynamic spectrum allocation facilitates the secondary usage of licensed band. The spectrum must be carefully used by the secondary user (SU) in order to avoid interference with the primary user (PU) [5]. Based on the behavior of the protocol stack various attacks are categorized [5] as follows.

A. Physical Layer

In cognitive radio network, secondary users (without license) are allowed to access the licensed spectrum if primary users (having license) are not present. To protect the priority of primary users, secondary users must quit the spectrum when primary users emerge. Therefore, secondary users need to carry out spectrum sensing to detect the existence of primary users.The primary user emulation attack (PUEA) is performed in the physical layer, in which the PU signal characteristics are impersonated by the malicious user (MU) therefore the SUs may think the MU as the PU [6]. Jamming may be possible in this layer when the jammer sends the data packets continuously to the channel. Thus causes the SU unable to sense the idle channel [6]. The CR cannot adapt to the changing environment when the utility resource parameters are modified, thus causes the objective function attack (OFA) [6]. The spectrum sensing information to the attacker and the transmission can be interrupted by preventing the channels from sharing information leads to the common control data attack (CCDA) [5]. If the parameters are not up to the threshold level the communication stops.

B. Link Layer

The data transfer takes place from one node to another in the link layer and three types of attacks suck as spectrum sensing data falsification (SSDF) or the byzantine attack where the fusion centers decision is falsified because of the wrong spectrum sensing results [5]. This attack targets both centralized and distributed CRNs. In a centralized CRN, a fusion center is responsible for collecting all the sensed data and then making a decision on which frequency bands are occupied and which are set free. Fooling the fusion center may lose some legitimate users. This type of attack is defensive by calculating the threshold value. It is calculated by finding the sum of the collected spectrum that is sensed. The malicious user can change the route information of the node by providing wrong information about the node called the selfish channel negotiation (SCN) [5]. The control channel is reserved by the attackers and is saturated such attack is called the Control channel saturation Denial-of-service (DoS) [5]. This attack degrades the end to end throughput of the whole cognitive radio network. The sequential probability ratio test can be used for this purpose in order to prove its efficiency in terms of detection time.

C. Network Layer

The attacks in network layer are sink hole attack and hello flood attack. In sink hole attack the attacker mocks itself as the best route and pulls the neighbors to use this route to forward the packets and to discards those packets. This attack is effective in infrastructure and in a mesh architecture as all the traffic moves through the base station allows the attacker to falsely claim as a best router for packet forwarding. Thus the traffic will be routed to the physical location of the base station and it is difficult to go elsewhere to create a sinkhole. In the hello flood attack the attackers uses enough power and sends broadcasting signals to all the nodes in the network to convince them that it is the closest neighbor. When this attack is detected there occurs a possibility of packet loss, absence of neighbors to forward the packets.

D. Transport Layer

In transport layer the possible attack is LION attacks. In LION attack, it uses the primary user emulation attack to disrupt transmission control protocol (TCP) connection. It's said to be a cross layer attack pointed at the transport layer where imitating a licensed transmission will force a CRN to achieve a frequency handoffs and thus degrading TCP performance. The attacker intercepts the messages, and it predicts to be in hand off when the frequency band is tested and by claiming it using the PUE results in a total network starvation.

E. Application Layer

Since each layer is interconnected to each layer the attacks performed in other layers may cause adverse effect on the application layer.

III. Primary User Emulation Attack (PUEA)

PUEA is performed in the physical layer. The CR environment allows dynamic spectrum access, the authorized spectrum band is used by the PU and the SU can make use of this spectrum band when the PU is not using it. In PUEA, the attacker is capable of generating the similar signal as the PU, in order to confuse the SU. The incumbent SU identifies the attacker as the PU and vacates the channel immediately. This kind of attack is known as PUEA. The PUEA can cause intervention to the spectrum sensing and reduces the availability of channel to the incumbent SU. This attack is of two types [9].

They are malicious PUEA and selfish PUEA.

- Selfish PUEA: The attacker's objective is to maximize its own spectrum usage. Here, the goal of the attacker is to increase its share of spectrum resources. This attack is carried out between two attackers and establishes a dedicated link between the malicious PUE.
- Malicious PUEA: The attacker's objective is to obstruct secondary user's access to the spectrum. In malicious PUE, attackers try to prevent the legitimate secondary users from using the holes found in the spectrum.

IV. PUEA Defense Techniques

Despite of all the attacks in CRN the PUEA causes adverse effects so the prevention of PUEA is important in CRNs. The methods discussed here focus on the mitigation of PUEA and some assumptions are made to produce better results. Here the PU is TV transmitters. AT first mobile FM wireless microphone is considered as PU and PUEA is defined by Shaxun Chen et al in [7].

A. PU authentication

The stationary helper nodes are used to authenticate PU using link signature and the broadcast spectrum availability information to the SU [8]. The extra helper nodes which are fixed must be authenticated by the trusted authority with the help of public key and certificate. The helper resolution (HR) algorithm is used for the mobile users and the analysis has been done on different attacks. Without repeated training more SU can be served and the successful defense against the attack can be provided.

B. Location based method

Based on the location of PU there are three types of defense techniques. In the wavelet transform scheme the fingerprint is extracted using the multi-resolution time frequency property which can be used to distinguish the PUE attacker and the incumbent PU signal. The Time Difference of Arrival (TDOA) scheme is used to detect the PUE attack and to find the position of the emitter. The quadratic error can be minimized by the Weighted Least Square (WLS) method. In order to find the PUEA, tier hierarchical CRN and M-ary hypothesis is done in the two-tier scheme [10].

C. Fingerprint verification method

The phase noise is extracted from the received signal in the ANN based scheme. The ANN can identify the transmitter by using the wavelet analysis [11]. Fingerprint is considered as the unique characteristics in [11]. To get the false alarm rate the channel based hypothesis testing can be done. The OFDM uses this technique. Hence the detection probability can be increased by increasing the SNR.

D. Transmitter verification scheme

In this scheme three defense techniques are used. In the Distance Ratio Test (DRT), using the pair of verifiers the distance ratio of received signal strength can be obtained. To identify the transmitter location the phase difference of the received signal is obtained using the Distance Difference Test (DDT). In this method the location of all the users is assumed to be fixed and the verifiers must have tight synchronization. When the attacker is close to the SU performance of the system will be degraded. The peak of the RSS signal can be used to locate the transmitter by using the Location-based Defense (LocDef) [12].

E. Sybil attack

Sybil attack is similar to the Byzantine attack in which the Sybil identities are created to modify the decision of SU and launches PUEA. Spider radio, the CR test-bed is used to prove the feasibility [13]. With the decrease in the number of good nodes the cost increases adversely. The fusion center helps to estimate the expected cost.

F. Belief Propagation

Belief propagation of the location information can be calculated. Here the location and compatibility function, the message computation, message exchange between neighboring users and until its coverage calculation of belief is done. The PUE attacker can be found when the calculated mean of belief is less than the threshold [14]. Markov random process can be used to achieve better results. The attacker's transmission power and range is limited. All the SUs must be aware of the location information of the PU. When the distance between the PU and the attacker is less, then the calculated belief mean will be more.

G. Signal Activity Pattern

In this paper, the signal activity pattern acquisition and reconstruction system (SPARS) is used. In SAP through spectrum sensing the ON/OFF period of the transmitter can be observed. Here, the SU will not have prior knowledge about the PU. In the reconstruction system of SAP the Bayesian method and sparse model are used. Prior knowledge about the PU is not provided. By calculating the reconstruction error the attacker can be found [15].

H. Fast probe

Fast probe facilitates in band and out band sensing and for better accuracy cooperative sensing can be performed. Fast probe an active transmission system can be used to solve SSDF problem. The assumption can be done as that all the neighboring CR nodes have same readings. In fast probe the compute scheduling and test transmitter algorithm can be used for testing the CR node. If the transmission power is less than the threshold then the transmitter is the malicious user. Thus using this method we can proactively detect the malicious user and detect the malicious SU that don't perform in band sensing [16].

V. PROPOSED SOLUTION

In the practical wireless environment, the channel varies with the motion of SUs and the attacker. So, always the single threshold based detection method does not hold good for detecting malicious attacker, because the threshold is set primarily, and the probability of detection is achieved by comparing the received power with the threshold. The detection performance can be improved by adopting a technique to optimize the threshold according to the channel variation. Most of the techniques assume that the position of all the users are fixed and known to each other. So for motional users, the channel estimation can be applied to estimate the exact location of users, so as to identify the malicious users successfully.

VI. CONCLUSION

This paper discusses about the threats found in the cognitive radio networks, it is considered as one of the efficient methods to make use of the available spectrum. The lack of available spectrum, and increase in the applications on wireless systems made the cognitive radio an adaptable method in the demanding wireless technology. The discussion provided here gives a reliable measure to make it as an analysis paper relating the possible threats and their remedial methods.

REFERNCES

[1] Deepa Das, Susmita Das, "Primary User Emulation Attack in Cognitive Radio Networks: A Survey", IRACST, Vol.3, No3, June 2013.

[2] Carl R. Stevenson, Gerald Chouinard, "IEEE 802.22: The First Cognitive Radio Wireless Regional Area Network Standard", IEEE Communications Magazine, January 2009.

[3] M. T. Mushtaq, M. S. Khan, M. R. Naqvi, R. D. Khan, M. A. Khan, Prof. Dr. Otto F. Koudelka," Cognitive Radios and Cognitive Networks: A short Introduction", J. Basic. Appl. Sci. Res., 3(8)56-65, 2013.

[4] Abhilasha Singh, Anita Sharma," A Survey of Various Defense Techniques to Detect Primary User Emulation Attacks", International Journal of Current Engineering and Technology, Vol.4, No.2 ,April 2014.

[5] Shaxun Chen, Kai Ceng, 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.

[6] Elena Romero, Alexandre Mouradian," Simulation Framework for Security Threats in Cognitive Radio Networks", vol., no., pp. 1--7, 15--17 May 2009.

[7] Ruiliang Chen; Jung-Min Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on , vol., no., pp.110,119, 25-25 Sept. 2006.

[8] Caidan Zhao; Wumei Wang; Lianfen Huang; Yan Yao, "Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio," Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on , vol., no., pp.1,5, 24- 26 Sept. 2009.

[9] Caidan Zhao; Liang Xie; Xueyuan Jiang; Lianfen Huang; Yan Yao, "A PHY-layer Authentication Approach for Transmitter Identification in Cognitive Radio Networks," Communications and Mobile Computing (CMC), 2010 International Conference on , vol.2, no., pp.154,158, 12- 14 April 2010.

[10] 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.

[11] Yi Tan; Kai Hong; Sengupta, S.; Subbalakshmi, K. P., "Using Sybil Identities for Primary User Emulation and Byzantine Attacks in DSA Networks," Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE , vol., no., pp.1,5, 5-9 Dec. 2011.

[12] 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.

[13] 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.

[14] Zhou, Xiao; Xiao, Yang; Li, Yuan yuan, "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.

[15] Chun Sheng Xin, Min Song,""Detection of PUE Attacks in Cognitive Radio Networks Based on Signal Activity Pattern", IEEE Transactions On Mobile Computing, Vol. 13, No. 5, May 2014.

[16] Tarun Bansal, Bo Chen and Prasun Sinha," FastProbe: Malicious User Detection in Cognitive Radio Networks Through Active Transmissions", INFOCOM, May 2014.