A survey on Attacks and Detection Strategies for Primary User Emulator in Cognitive Radio Networks

Shilpa Biradar[1], Giriraj Patil[2], Gurusiddaraj Konded[3]
Gndec Bidar.

Abstract: A Cognitive Radio (CR) can be programmed and configured dynamically to use the best wireless channels in its vicinity. Such a radio automatically detects available channels in wireless spectrum, then accordingly changes its transmission or reception parameters to allow more communication in a given spectrum band. As CR technology is being used to provide a method of using the spectrum more efficiently, spectrum sensing is key to this application. During Spectrum Sensing there are possibilities of having so many attacks, one of these attack is Primary User Emulation Attack (PUEA). In this a malicious user pretends to be like a Primary User. Many detection and mitigation techniques have been proposed but still there are so many issues regarding the security of Cognitive Radio Network (CRN).In this paper we present a study on various attack and defense strategies to enhance the security of Primary User Emulator (PUE) in CRN.

Keywords: CRN, Primary User Emulator Attack, PUEA detection.

1. Introduction

The increase in the wireless users has led to the spectrum shortage problem. Federal Communication Commission (FCC) showed that licensed spectrum bands are underutilized, specially TV bands. The IEEE 802.22 standard was proposed to exploit these white spaces in the (TV) frequency spectrum. Cognitive Radio allows unlicensed users to use licensed bands while safeguarding the priority of licensed users. Cognitive Radio is composed of two types of users, licensed users also known as Primary Users(PUs) and unlicensed users also known as Secondary Users(SUs).SUs use the resources when spectrum allocated to PU is vacant, as soon as PU become active, the SU has to leave the channel for PU. Hence the opportunistic access is provided by CR to SUs whenever the channel is vacant. Cognitive Users sense the spectrum continuously and share this sensing information to other SUs, during this spectrum sensing, the network is vulnerable to so many attacks. One of these attacks is Primary User Emulation Attack (PUEA), in which the malicious secondary users can mimic the characteristics of primary users thereby causing legitimate SUs to erroneously identify the attacker as a primary user, and to gain access to wireless channels. PUEA is of two types: Selfish and Malicious attacker. A selfish attacker aims in stealing Bandwidth form legitimate SUs for its own transmissions while malicious attacker mimic the characteristics of PU.

2. Layered Approach in CRN

There are four layers in CRN, the bottom most layer
is the Physical layer, next is link layer, the third layer is the network layer and the uppermost layer is the transport layer[5].

2.1 Attacks on Physical layer: Physical layer provides an interface to transmission medium. Following are the attacks on Physical layer.

i) **PUE attack**: In PUEA, an attacker emulates the primary user’s signal characteristics causing other secondary users to falsely determine that the frequency is in use by the primary user, and so vacate the frequency or selfishly attacker aims in stealing bandwidth from legitimate SUs for its transmission.

ii) **Objective function attack:** To increase the data rate, the cognitive users sense the environment and adapt to changes of environment by calculating some parameters such as bandwidth, power, modulation, coding rate, frequency, frame size, encryption type, and channel access protocol. An attacker may manipulate these parameters to give false results.

iii) **Jamming attack:** In this attack, the malicious user purposely transmits on licensed band, making unavailable to primary users or other secondary users.

2.2. Attacks on link layer: In Link layer, multiple users can share the medium within the same network. A Common Control Channel (CCC) can be used for an exchange of control messages to coordinate the users.

i) **Byzantine Attack:** Byzantine attack is also named as Spectrum Sensing Data Falsification (SSDF).SSDF attack occurs when an attacker sends false local spectrum sensing results to its neighbor or a fusion centre to make them to take a wrong spectrum sensing decision.

ii) **Control Channel Saturation Attack:** In control channel saturation attack, when a channel is saturated by large numbers of contending cognitive radios and if cognitive radio is unable to complete its negotiation within the limited time, then radio defers from its transmission during next data phase. In this, an attacker intention is to saturate the control channel by broadcasting a large number of packets.

iii**) Control Channel Jamming Attack:** In common control jamming, when a strong signal is injected in to control channel, the receivers are stopped from receiving valid control messages.

2.3. Attacks on Network Layer: In network layer, the packets are routed from a source node on one network to destination node on another network, while maintaining quality of service.

i) **Sinkhole Attack:** In sinkhole attack, an attacker take the advantage of multi-hop routing by publicizing itself as best route to specific destination and allows the neighboring nodes to use it to forward the packets.

ii) **Wormhole Attack:** In wormhole attack, the received messages are tunneled by the attacker in one part of the network and these messages are replayed in another part of the network.

2.4. Attacks on Transport layer: Transport layer is responsible for flow control, congestion control and end-to- end error recovery.

***LION attack*:** In this, attacker use PUEA to interrupt transmission of data through TCP protocol. When PUE attack occurs, the SUs has to leave the channel for PUs, but still TCP transmits packets continuously and these packets are intercepted by the attacker.

3. PUE Attack Detection Techniques.

3.1.Distance Ratio Test(DRT) and Distance Difference Test(DDT): The DRT uses the Received Signal Strength(RSS) based method, where the two dedicated cognitive nodes measures RSS of the signal source and calculate the ratio of these two RSS to check whether it coincides with their distances to the true PU[6]. Using DDT, the arrival time of transmitted signal from the source is measured by the two cognitive nodes. The product of time difference and light speed is then compared to distance difference from the true PU to the two dedicated nodes in order to identify the source.

3.2.Maximum and Minimum Eigen Value: The maximum and minimum value was calculated based on the covariance matrix of received signal. The ratio of Maximum to Minimum Eigen was found to find the presence of signal. Then the value was quantized to some threshold value in order to find the false alarm probability[7].

3.3 Localization Scheme: One of the localization scheme, Time Difference of Arrival(TDOA) is suitable in CRN since it utilizes the difference between arrival times of pulse transmitted by an emitter without knowledge of pulse transmitted times. It does not require Base Station(BS) to equip with extra omni directional antennas. BS updates SUs which require such information as soon as the signal source is localized. The requirement of TDOA was, all the BSs have to be time synchronized for accurately detecting the time difference when a same signal pulse was received[8].

3.4 Robust Spectrum Decision Protocol: In[9], a centralized controller collects individual sensing results from SUs and makes the final spectrum decision for the entire network. In this authors used a flexible log-normal sum approximation to characterize the received power at good secondary user, then they proposed an individual detection mechanisms for SUs to achieve individual sensing results. The probability of successful PUEA at each good user is then derived to analyze the effect of PUEA on the whole network, in terms of the number of good users successfully attacked by the malicious users.

3.5 Belief Propagation: In [10], each user calculate some belief value of neighboring nodes and shares in the network. Then the mean value was calculated from these values for each node, if this value was less than the threshold then it was assumed to be an attacker.

3.6.Physical Network Layer Coding: In[11], when two signal sequences interfere at the receiver, the starting point of the collision was determined by the distances among the receiver and the sender. Using this interference result at the multiple receiver and the position of reference sender, the position of claimed PU can be found. This localized result is compared with the known position of the PU to detect PUEA.

3.7Advanced Encryption Standard: In[12], proposed a solid AES-helped DTV plot, in which an AES-scrambled reference signal is produced at the TV transmitter and utilized as the match up bits of the DTV information outlines. By permitting a mutual mystery between the transmitter and the collector, the reference signal can be recovered at the collector and used to accomplish precise distinguishing proof of the approved essential clients. Moreover, when joined with the investigation on the autocorrelation of the got reference signal, the nearness of the malicious user can be identified precisely regardless of whether the PU is available or not.

3.8 SPARS(Signal Activity Pattern Acquisition and Reconstruction): In[13], Signal Activity Pattern(SAP) was defined as a series of ON and OFF periods of transmission along the time. The ON period refers to busy period ,that the transmitter is transmitting and SUs are refrained from communications. An OFF period refers to idle period between two ON periods. In this SAP of transmitter is acquired through spectrum sensing and compared with SAPs of PUs through reconstruction model. If the observed SAP is not “like” the SAPs of PUs, which was measured by reconstruction error, then the transmitter was assumed to be an attacker.

3.9.Data Fusion Technique: The Spectrum Sensing Data Falsification or Byzantine attack happen when an attacker sends false local spectrum sensing results to its neighbor or a fusion centre to make them to take a wrong spectrum sensing decision. Data fusion technique was proposed to detect byzantine attack which was based on the idea of summing up the number of sensing terminals reporting “busy” and if the sum was greater than a fixed threshold, then the channel was considered to be occupied[14].

3.10. Data Assisted Approach: In this[15] each SU was integrated with local database and cognitive BS was build up with global database. Local database stores historical spectrum sensing data and local detection decision of each SU. The global database collects and records all the SUs spectrum sensing data and the local detection decisions. By this, the global database in cognitive BS can provide interface to incumbent database for information query, e.g. the geo-location of a primary BS and the list of available channels.

4. Conclusion

In this paper we discussed layered approach of Cognitive Radio Network and types of attacks on various layers. Further we discussed detection techniques for Primary User Emulation Attack. The techniques which were proposed were not much effective in detecting PUEA. So, future we can use some hybrid model to detect PUEA.

REFERENCES

[1] S. T. Zargar, M. B. H. Weiss, C. E. Caicedo, and J. B. D. Joshi,“Security in Dynamic Spectrum Access Systems: A Survey,” in *Proc*.Telecommunications Policy Research Conference, Arlington VA, 2009.

[2] Bhagavathy S. Nanthini,, M. Hemalatha, D. Manivannan, & L. Devasena ,“Attacks in cognitive radio networks (CRN) ” A survey. Indian Journal of Science and Technology, 2014, 7(4), 530–536.

[3] D. Das ,“ Primary User Emulation Attack in Cognitive Radio Networks ” A Survey. International Journal of Computer Networks and Wireless Communications,2013, 3(3), 312–318.

[4] C. Kiruthika, A.C. Sumathi, “ A Study on Primary User Emulation Attack in Cognitive Radio Networks”, International Journal of Computer Science Engineering and Technology(IJCSET), 2014,4(10), 260–262

[5] Deanna Hlavacek, J. Morris Chang,” A layered approach to cognitive radio network security, elesvier,2014.

[6] R. Chen , J.M. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks”. IEEE workshop on Networking Technologies for Software Defined Radio (SDR) Networks,2006, 110–119.

[7] Y. Zeng, & Y.C. Liang,,“Maximum-Minimum Eigen-value Detection for Cognitive Radio”. IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications, 2007, pp1-5.

[8] R. Chen , J.-M. Park & J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks". IEEE Journal on Selected Area in Communications,2008,26(1),pp 25-37.

[9] Z. Jin, S. Anand, & K.P. Subbalakshmi, " Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks". Global Telecommunications Conference (GLOBECOM) IEEE,2010,pp1-5.

[10] Z. Yuan, D. Niyato, H. Li, J.B. Song & Z. Han," Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks". Selected Areas in Communications, IEEE Journal,2012, 30 (10), pp1850-1860 .

[11] X. Xie, & W. Wang, " Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding"Proceeding of Computer Science, 2013, 21, pp430–435.

[12] A. Alahmadi, M. Abdelhakim, J. Ren, & T. Li, " Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard". Global Communications Conference (GLOBECOM), IEEE, 2013, pp3229–3234.

[13] C. Xin, S. Member, M. Song, & S. Member," Detection of PUE Attacks in Cognitive Radio Networks Based on Signal Activity Pattern", IEEE transactions on mobile computing , 2014,13(5), pp1022–1034.

[14] Linyuan Zhang, Guoru Ding, Qihui Wu, Yulong Zou," Byzantine Attack and Defense in Cognitive Radio Networks" DOI 10.1109/COMST.2015.2422735, IEEE Communications Surveys & Tutorials.

[15] R. Yu, Y. Zhang, Y. Liu, , S. Gjessin, & M. Guizani, "Securing cognitive radio networks against primary user emulation attacks". IEEE Networks, 2015, 29(4),pp 68–74.