IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol-6, Special Issue-3, Apr 2018 E-ISSN: 2347-2693

Analysis of the various Security Attacks and Countermeasures in Cognitive Radio Network

Jagsir Singh[1*], Jaswinder Singh[2]

[1]Dept. Of Computer Engineering, Punjabi University, Patiala, India
[2]Dept. Of Computer Engineering, Punjabi University, Patiala, India

[*]*Corresponding Author: erjagsirsingh18@gmail.com*

Available online at: www.ijcseonline.org

Abstract— The cognitive radio technology is one of the best candidates to handle the problem of the scarcity of the radio spectrum. The basic principle of cognitive radio is that it allows to secondary users to use the free (idle) primary channels. The cognitive radio networks do not only face the traditional security attacks, but also new security attacks due to the new characteristics of the cognitive radio technology. A number of the major news attacks in the Cognitive Radio Networks (CRNs) are the primary user emulation, spectrum sensing data forgery, and jamming attacks. In wireless networks, security is a challenging aspect. In the CRN, it is much more difficult because Cognitive Radios (CR) performs the various functions such as sensing the radio spectrum, managing the spectrum, spectrum mobility and sharing the spectrum. To perform all these functions efficiently without any attack, security mechanisms are required to implement. In this paper, major security attacks in the cognitive radio networks are discussed. Also, the various countermeasures to these security attacks in CRN are described.

Keywords— Cognitive Radio (CR); Cognitive Radio Networks (CRNs); Primary Users (PUs); Spectrum Sensing Data forgery (SSDF) Secondary Users (SUs).

I. INTRODUCTION

The numbers of wireless devices are increasing with emerging wireless technologies. The radio spectrum is becoming gradually more overcrowded. Every wireless device needs a radio channel to communicate over the wireless network. As the wireless technologies are developing, the numbers of wireless devices are increasing such as cellular phones, smart phones, Bluetooth, data cards, Personal Digital Assistants (PDA) and laptops. According to the report of International Telecommunication Union (ITU), the numbers of mobile phone subscriptions are estimated from 738 million in 2000 to more than 7 billion mobile phone subscription by the end of 2015 which is large than the world population. Similarly, mobile internet users are increasing at the high rate as well. In 2000, there were only 400 million users because the internet facility was not accessible all over the world. Now the internet users have been increased up to 3.2 billion by the end of 2015. Therefore, it is a big challenge to fulfill the requirement of radio spectrum to the wireless devices.

According to the report of FCC, the primary channels(licensed channel) are underutilized and secondary channel are bands are over utilized [1]. Therefore to utilize the primary radio channel the CR technology was developed. In an intelligent way, the idle primary channels can provide the opportunity to cognitive users to transmit the data. Thus, when the licensed channels are free then these free channels are accessed by secondary users[2]. The cognitive user vacates the primary channel for the primary user when the primary user returns back on that licensed channel and moves onto another free available licensed channel. The cognitive user is very much aware of the environment and its changes [3]. It adapts transmission parameters accordingly to avoid the disturbance between primary users and secondary users. The cognitive user continuously senses the radio frequency spectrum and find out the available free licensed channels over which transmission can take place. Then it moves on the best channel from available free channels of having good QoS for communication.

In CR networks, security is the main concern for proper utilization of free licensed channel. In order to prevent security attacks at the different layers in cognitive radio, numbers of security mechanism are required to implement. Cognitive radio network does not only face the traditional security attacks, but also new security attacks due to the new characteristics of cognitive radio technology. The major news attacks in CR network are primary user emulation, spectrum sensing data deception, jamming attacks etc. The purpose of these attacks can be to produce the interference between the licensed user and unlicensed user, make the secondary user unavailable to primary channels even though primary channels are free or occupy the primary channel for a long time by not giving an opportunity to the secondary user to use the primary channel. It produces the adversary effects in the cognitive radio networks. Therefore, it is necessary to take action against security attacks in order to prevent the cognitive radio network from these malicious actions. In this paper, we investigate several security attacks and countermeasures to defend against these security attacks

This paper is partitioned into two major sections. The various security attacks in CR network are presented In section-II. Section-III describes the security mechanisms in CR systems. At last, this technical paper is concluded.

II. SECURITY ATTACKS IN CR NETWORK

The fundamental principle of CR is that it allows to secondary users to use the primary channel when are free. Secondary users must switch to other licensed channels when the primary user comes back on that channel. In this survey paper, the traditional attacks on cognitive radio networks are not covered. Because of unique characteristics of cognitive radio networks than other wireless technologies, it experiences new kinds of security attacks. In this section, we have discussed major security attacks in CR networks.

A. Primary Emulation Attack

Primary User Emulation Attack (PUEA) is the major security problem of CRNs [4,5]. When a secondary user (cognitive user) pretends as the primary user, is known as primary user emulation attack. It is done by the malicious unlicensed user to take advantage of licensed channels and not giving an opportunity to the other secondary users for using the free licensed channels. The chances of PUEA are reasonable due to the dynamic behaviour of Cognitive Radio [6]. The main technical challenge in sensing from the perspective of security is to stop the PUE attack. PUE attack is a physical layer [7]] attack which jeopardizes the throughput of the CRNs.

The purpose of PUE attack is classified into two categories: the first one is malicious primary emulation attack and the second one is Selfish primary emulation attack. When the attacker prevents the secondary users to use the licensed channel that attack is called the malicious primary emulation attack. And in the Selfish attack, the attacker does not leave the primary channel to other secondary users. Basically, in this attack, a malicious user pretends as primary user and does not give the opportunity to legitimate secondary users. In [8], a new kind of primary user emulation attack was discussed which attacks the cognitive radio network during its “quiet periods”. The quiet periods in cognitive networks are those time intervals in which secondary users switch from transmitting the data mode to sensing the spectrum mode in order to find out the free primary channels. In this time, a user whose received signal power greater than the certain limit (threshold) is considered as the primary user. During the quiet periods, an attacker sends the high power signals and convinces the secondary users that a primary user is present. Another primary-user emulation assault is performed during the hand-off process. It is Denial-of-service kind of assault which degrades the throughput of the CR network.

B. Spectrum Sensing Data Forgery Attack

Spectrum Sensing Data Forgery (SSDF) assault is executed at data link layer of the cognitive radio network. This attack is also known as the Byzantine attack. In distributed CR networks, the local secondary users share the sensing information for taking the decision about the availability of primary channels. In this case, a malicious secondary user sends the wrong spectrum sensing outcomes to the local legitimate secondary users that lead the wrong spectrum sensing decision [9]. This attack not only targets the distributed cognitive radio network but also target the centralized CRNs. A centralized node collects the sensed information from the local secondary user, this node is called fusion center. After collecting the sensed data, it is confirmed which primary channels are occupied or free. If the spectrum sensing decision taken by an individual secondary user or fusion center is false then there will two problems: either the legitimate secondary user will not access the primary channel even though channel is available or secondary users will use those primary channels which are already occupied by PUs. It will produce the obstruction between the primary users and secondary users. In SSDF attacks, wrong information about the spectrum sensing is delivered to the local secondary users or fusion center to create the collision between the primary users and secondary users.

C. Jamming Attacks

Jamming attacks target at the physical later [10] of the CR network. These are denial-of-services attacks, which has the main purpose to deny the legitimate secondary users to use the free primary channels. In this attack, an attacker continuously sends data packets and make the legitimate user as there are all the channel are busy. In literature, four types of jammers which affect the CRN in different ways [11]. The first jammer is the constant jammer, it continuously sends the data packet on the channel without waiting when the channel will free. The second jammer is deceptive jammer; it compels the other user to switch into receiving state and making that user stay in that state. It means the legitimate user continuously receives the junk data packets from the attacker and remains busy in receiving state. The third jammer is random jammer; this jammer is different than previous jamming attacks. It takes the break. During sending the junk data packet, it behaves like either the constant jammer of the deceptive jammer. The last one is the reactive jammer; it is intelligent jammer because it senses the channels constantly. Whenever any legitimate secondary user sends the data on that channel then it starts sending the junk data packet to disturb the communication between the intended users or to produce the interference between the communicating users.

D. *Black & Gray Hole Attacks*

The Black and Gray Hole both are denial-of-service attacks. An attacker tries to mislead the legitimate user by defining the optimum path itself to the destination node in black hole attack [12]. Hence, all the data packets of the secondary user will be passed through the malicious node. Then, the attacker can discard all the data packets or stop them to reach the end node. The sender user transmits the RREQ packet to receive the acknowledgment from the legitimate destination. The attacker (black hole node) replies to the RREQ packet to the source by inserting the information (hop count) of the shortest path. Here, sources node is deceived and believes that the attacker node as an intermediate node which is providing the short path or the destination node. Once the path is established through a black hole node then it is up to the black hole node how the data packets are discarded. The effect of this attack depends on the location of black hole node. If the node is located at the corner of the cognitive radio networks then only the data packet of few nodes will be discarded whose route through that node. In the second case, if the attacker located near the base station then it may break off the all networks traffic.

Gray Hole attack is a variant of Black Hole attack. Unlike the Black Hole attack, in the Gray Hole attack selecting forwarding approach is used [12]. The attacker only discards the selective data packet and passes the rest of data packet. By doing this it influences the sending user that it is an optimal shortest path. Once the sending user has been influenced then it starts sending the entire data packet through this malicious route and packet can be discarded by Gray Hole node in a selective manner. That’s why it more difficult to detect than black hole attack. Because both the source and destination do not experience any malicious activity during transmitting the data packet in CRN.

E. *Saturation of Common Control Channels*

In the CR network, a control channel is required to make the link between source node and destination node. MAC control frames are negotiated between the CR users to reserve the frequency band (licensed channel). The malicious user generates a false MAC frame to saturate the common control channels [13]. It decreases the network performance drastically. This attack is only possible in multi-hop cognitive radio network because unlike centralized CRN, all MAC frames are not stamped and authenticated by the base station. This attack decreases the throughput of CRN near to zero.

In next section, several security countermeasures in CR networks are explained.

III. VARIOUS SECURITY MECHANISMS IN COGNITIVE RADIO NETWORK

Various security countermeasures corresponding explained security attacks in CR networks are:

A. Countermeasures for the PUE Attack

To stop the PUE attacks, a strong transmitter authentication approach has to design with the purpose of discrimination between the genuine PUs and the malicious unlicensed user. A public key encryption phenomenon was used to handle this attack, in which the primary user encrypts own identity by its private key [14]. The secondary users receive the signature then decrypts with the public key and verify that signature to know it is valid primary user or not. It prevents the unauthorized user to create a valid signature. However, this approach is not according to FCC regulations which disallow changing the primary user system. Other security mechanisms are proposed by various researchers which are based on the location of the users. If the position of the transmitting node matches with the position of the PU then that source node is considered a PU or else, that node is considered a malicious node.

In [4], two location-based techniques have been proposed to find out the location of the source node: Distance Difference Test (DDT) and Distance Ratio Test (DRT). Both techniques depend on the source verification procedure. This procedure carries the location confirmation method which discriminates between the legitimate the PUs and the attackers (pretending as the PUs). These approaches totally depend on the Location Verifiers (LVs).The main problem with these approaches is that tight synchronization is needed among the LVs. Another location-based approach was suggested in [15]. In this technique, two methods are applied. Firstly, Time Difference of Arrival method is applied then Frequency Difference of Arrival to find out the locations of the source node. The drawback of this technique is that it is much more relies on assumptions that make it very restrictive. Therefore, it is not appropriate to the common cognitive radio network.

A different technique in [16], fingerprinting was proposed to authenticate the source node. This technique uses the Electromagnetic Signatures (EMS) for each cognitive user to construct a security system in CRNs for protecting the CRN from the PUE attack. The electromagnetic signature is used to authenticate the identity of the primary user. It is the best approach out of proposed countermeasures. But it needs extra storage than other suggested techniques.

B. *Countermeasures for the SSDF Attack*

In literature, various techniques have been proposed to protect the CRN from the SSDF attack. In [17], a Decision fusion approach was suggested. In which spectrum sensing data from the local nodes are collected and then summed up to take the decision. A threshold value is set. The value of threshold must be between 1 and number of sensing nodes. If the sum of all local sensing results is greater than the threshold then it is determined that PU is there. Otherwise, the radio channel is free. Therefore, it protects the legitimate user to have false knowledge about the primary channels. However, this technique is not optimal in the case of many attackers in the CRN.

In [18], a data fusion strategy was proposed is known as Weighted Sequential Ratio Test (WSRT). The WRST consists of two phases. In the first phase, reputation value is maintained. At first, the reputation value of each node is set to zero. The value of each node is increased by one upon receiving the right spectrum-sensing results from local nodes. In the second phase, Sequential Probability Test is performed to check the status of the channels. Also, another weight based technique was suggested in [19], it uses pre-filtering and trust techniques which show the good performance.

A new SSDF detection algorithm was proposed in [10], it is based on the trust value of the cognitive user. This trust value is updated according to the behavior of the secondary user. This algorithm calculates the distrustful level of the users. Based on this suspicious level the malicious users are eliminated. If a cognitive user turned into an attacker then its trust level decreases. When the trust value of the users crosses the certain limit then those users are declared as the malicious users. It is good malicious user detection algorithm for protecting the CRN from SSDF assault however the major weakness of this algorithm is it can’t perform well in multiple malicious user environments, not in multiple malicious user environments.

C. *Handling Jamming Attacks*

The jamming (Dos) attack [21] is performed by an attacker at the physical layer and data link layer. Numbers of approaches have been proposed to handle the jamming attack in CRN. The best technique to defend against the jamming attack in CRN network is the frequency hopping approach. It is a traditional phenomenon in wireless communication to transmit the data over different frequency band by switching in a random fashion for escaping from the attacker. Similarly, in CRN it is used to handle the jamming attack. One more technique can be used to handle the jamming attack, that approach is called special retreat. In this approach, the user changes their position to run away from the interference range. Although, the problem with this technique is that the user must be in the range of the communicating user.

In [11], two parameters are calculated: Packet Delivery Ratio (PDR) and signal strength. If the value of PDR is low and the signal strength is high then the legitimate secondary user believe it is being blocked (jam) until a neighbor has both high PDR and signal strength.

D. Defending Black & Gray Hole Attack

It is a very tedious job to detect the both Black and Gray Hole assault in CR networks because they exploit the architecture of network and routing protocols. Though, Geographical Routing Protocols (GRP) can oppose the Black and Gray Hole assault in CRNs [22]. On-demand, topology is constructed by the geographical routing algorithm using local communication. Consequently, all the data packets are routed through the secured path. Thus, it becomes difficult for an attacker to create the false path to interrupt the network traffic in CRN.

E. *Countermeasures for Saturation of Common Control Channels Attack*

Trusted architecture is used to mitigate the saturation of common control channel attack in CRNs. In the trusted system, neighbors monitor and evaluate the cognitive radio networks and find out the suspicious user if that is present there. Then, a Sequential Probability Ratio Test is executed by a neighbor to conclude a final result whether it is a malicious user or not.

IV. CONCLUSION

In this survey paper, various recent attacks on cognitive radio networks are discussed. Also, the corresponding countermeasures to these attacks are described in detail. Cognitive Radio is a new wireless technology which was invented to utilize the free licensed radio channels in an intelligent manner to solve the crisis of radio spectrum shortage. However, it suffers from the security threats which create the adversary effect in the cognitive radio network. We have investigated various countermeasures to defend the security attacks in CRNs. By implementing these security mechanisms properly, the cognitive radio network can be protected from attackers

REFERENCES

[1] Akyildiz, I.F., Yeol, L.W., Vuran, M.C., Shantidev, M., "Next generation /dynamic spectrum access/cognitive radio wireless networks a survey", Elsevier Computer Network, vol:50, pp no. 2127-2159, 2006.

[2] Salem, T.M., Abd El-kader S.M., Ramadan, S.M., Abdel-Mageed, M.Z., "Opportunistic Spectrum Access in Cognitive Radio Ad Hoc Networks" IJCSI International Journal of Computer Science Issues, vol. 11(1), pp no-41-50, 2014.

[3] Rawat, D. B., Song,M., Shetty,S., " Dynamic Spectrum Access for Wireless Networks". Springer, 2015.

[4] Chen, R., Park, J.M., "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks", IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR), Reston, pp no.110-119, 2006.

[5] Alahmadi, A., Abdelhakim, M., Ren, J., Li, T., "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," Information Forensics and Security, IEEE Transactions on, vol: 9(5), pp no. 772-781, 2014.

[6] Haykin, S., "Cognitive radio: Brain-Empowered wireless communication," IEEE journal on selected areas in communication, vol: 25, pp no. 201-220, 2005.

[7] Zou, Y., Wang. X., Shen, Z., "Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks," IEEE Transactions on Communications, vol:61(12), pp no.5103-5113, 2013.

[8] Tafazzoli, S., Berangi, R., "Cognitive Radio Handover in Cellular Networks", IJCSI International Journal of Computer Science Issues, vol:11(2),no 1, pp no 1694-0784, 2014.

[9] Mathur, C., Subbalakshmi, K., "Security Issues in Cognitive Radio Networks, Cognitive Networks: Towards Self-Aware Networks", Wiley, pp no. 284-293, 2007.

[10] Zhihui Shu; Yi Qian; Song Ci, "On physical layer security for cognitive radio networks," Network, IEEE, vol:27, no.3, pp no.28-33,2013.

[11] Xu, W., Trappe, W., Zhang, Y., Wood, T., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", ACM MobiHoc, pp no.46-57, 2005.

[12] Babu, B.R., Tripathi, M., Gaur,M.S., Gopalani, D., Jat,D.S., "Cognitive Radio Ad-Hoc Networks: Attacks and Its Impact" IEEE conference on Emerging Trends in Networks and Computer Communications (ETNCC), pp no. 125-130,2015.

[13] Zhu, L., Zhou, H., "Two Types of Attacks against Cognitive Radio Network MAC Protocols", International Conference on Computer Science and Software Engineering, vol:4, pp no.1110-111, 2008,.

[14] Mathur, C.N., Subbalakshmi, K.P.,"Digital signatures for centralized DSA network," in First IEEE workshop on cognitive radio networks, 2007.

[15] Huang, L., Xie, L., Yu, H., Wang, W., Yao, Y. "Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio Networks", International Conference on Communications and Mobile Computing (CMC), vol: l, no. 2, pp no. 169-17, 2010.

[16] Zhao, C., Wang, W., Huang, L., Yao, Y., "Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio", International Conference on Wireless Communications, Networking and Mobile Computing, pp no. 1-5, 2009.

[17] Pandharipande, A., , Kim, J.M., Mazzarese, D., Ji, B., "IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22", IEEE WG on WRANs, 2005.

[18] Chen, R., Park, J.M., Hou, Y.T., Reed, J.H., "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks", IEEE Communications Magazine, vol.46, no.4, pp no. 50-55, 2008.

[19] Kaligineedi, P., Khabbazian, M., Bhargava, V.K., "Secure Cooperative Sensing Techniques for Cognitive Radio Systems", IEEE International Conference on Communications, pp no.3406-3410, 2008.

[20] Wang, W., Li, H., Sun, Y., Han, Z., "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks", Conference on Information Sciences and Systems, 2009.

[21] Sodagari, S., Attar, A., Leung, V., Bilen, S., "Denial of service attacks in Cognitive radio networks through channel eviction triggering", IEEE Global Telecommunication, pp no. 610, 2010.

[22] Karlof, C., Wagner, D., "Secure Routing in Wireless Networks: Attacks and Countermeasures", Ad Hoc Networks, vol:1, pp no.293-315, 2009.

Authors Profile

Jagsir Singh is currently a Ph.D. Research Scholar in the department of Computer Engineering at the Punjabi University Patiala. He received his B.Tech degree from Punjabi University, Patiala in 2014. He got his Master of Engineering degree from Panjab University, Chandigarh in 2016. His research interests are in information and system security, Cognitive Radio, Wireless Networking, Machine Learning.

Dr. Jaswinder Singh is presently working as Assistant Professor, Department of Computer Engineering, Punjabi University, Patiala. He did Ph.D in Computer Engineering. He has more than 14 years experience in field of Computer Science & Engineering. His area of interest include: Computer and Network Security, Malware Analysis, Mobile Ad-Hoc Networks, Internet of Things, Machine Learning.