Physical layer attacks on cognitive radio networks

Sura Khalid Tawfeeq
Department of Computer Technology Engineering
Technical Engineering Collage /Mosul Northern Technical University Mosul ,Iraq
sura.khaled@ntu.edu.iq

Dr.Emad Ahmed Mohammed
Department of Computer Technology Engineering
Technical Engineering Collage /Mosul Northern Technical University Mosul ,Iraq
e.a.mohammed@ntu.edu.iq

Dr. Razan Abdulhamed
Department of Cybersecurity and Cloud Computing Techniques Engineering
Technical Engineering Collage /Mosul Northern Technical University Mosul ,Iraq
rabdulhammed@ntu.edu.iq

ABSTRACT

Due to the fact that wireless communication heavily relies on spectrum utilization, the growing demand for new wireless services and how they are used is causing a shortage of spectrum.The challenging technology known as "cognitive radio" is introduced in order to effectively use the spectrum that is currently available. It is an adaptive technology that can transmission by identifying its nearby devices. With no interference to the licensed users.cognitive radio aims to increase the effectiveness of the spectrum changes. The fact that cognitive radio operates in an open network environment increases the likelihood that an attacker will attempt to interfere with the spectral medium. Security then becomes a crucial factor.In this research we examine the physical layer security concerns for cognitive radio networks. We provide a summary of a number of current physical layer security attacks in cognitive radio networks.

Keywords: Cognitive Radio Network, Physical Layer ,Attacks

I. Introduction

In the past few years, many academics have conducted research in the emerging topic of cognitive radio [1]–[2], which is a new area of study for wireless communication.

In 2005 Haykins proposed a definition of cognitive radio, holding that it is an intelligent wireless communication system that is aware of its surrounding environment and uses the understanding-by-building methodology to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters in real time, with two main goals in mind: highly reliable communication and low-power consumption[3].

According to Chen et al. in 2008, cognitive radios could effectively assist valuable services and applications by taking

advantage of the chance to make communication with the spectrum holes [4].The demand for more spectrum for wireless users will be met with the advancement of cognitive radio, reaching the level of the network. The cognitive radio network will be able to utilize idle licensed

multiple types of physical layer attacks in CRNs have been garnering steadily increasing attention. And in order to defend against attacks made by hostile attackers, security measures are required. We then discuss these physical layer attacks on CRNs and assess relevant defenses, highlighting both their benefits and drawbacks.

II. LITERATURE REVIEW

In[5],The author summarizes the security assaults on the physical layer for cognitive radio networks and examines security challenges pertaining to the physical layer in those networks. To tested the network's capacity for secrecy, they also provided a cognitive radio network model. An upper bound on the amount of secure information that may be conveyed in cognitive radio networks can be established using the performance results that helped to characterize the secrecy capacity and outage probability between a node and its neighbors.

In[6],The author examined the dangers present in cognitive radio networks, which are thought to be one of the most effective ways to utilize the available spectrum. The limited spectrum and growing number of wireless applications made cognitive radio a flexible approach in the demanding wireless technology.

In[7],The principal secrecy assaults on the physical layer of the cognitive radio network are summarized in this article, along with some of the strategies used to defend against them. A case study to spur more research into the difficulties of security for cognitive radio networks is also included, along with open issues and future research areas in the field of physical layer security for cognitive radio networks.

airwaves and therefore improve the utilization of spectrum resources. Due to the physical characteristics of CRNs, where different unidentified wireless devices are permitted to opportunistically access the licensed spectrum

III. PHYSICAL LAYER SECURE THREATS IN CRNS

The physical channel used to connect two or more devices—such as network cards, cables, or the environment for wireless networks—is known as the basic platform layer of the TCP/IP model. Traditional wireless networks employ fixed frequency bands, whereas cognitive radio networks use dynamic Opportunistic Spectrum Access. This is how cognitive radio networks vary from traditional wireless networks. When using spectrum sensing to access unallocated spectrum bands and open air medium as the physical layer channel in CRNs, there are numerous security flaws that can be exploited by an attacker [8].

Primary User Emulation (PUE) Attack, Objective Function Attack (OFA), Jamming Attack, Eavesdropping, Primary Users' Location Attack, and Learning Attack (LA) are a few of the most frequent attacks against CRNs channel and block access to the physical layer of the cognitive radio network [9].

primary user emulation (PUE)

When attempting to occupy a certain channel in CRNs, a secondary user must determine whether the principal user is active or not. Additionally, he is permitted to utilize the particular band while a principal user is not using it. The secondary user should promptly change channels to an empty channel once a primary user is spotted [10]_[11].

Spectrum sharing techniques should be employed to achieve spectrum equity if the secondary user notices that the same band is already being used by another secondary user.

By emitting unique signals in the authorized band, a primary user emulation (PUE) attacker can pose as a primary user, tricking other secondary users into thinking

there are primary users present. The secondary users who consider the attackers to be the band's primary users must stop using it. The attack would therefore be successful in stopping secondary users from using this channel. PUE assaults come in a variety of forms as of right now [12], including selfish PUE attacks, malicious PUE attacks, and some more intricate PUE attacks. A selfish PUE attack involves two attackers concurrently establishing an appropriative link in order to enhance their part of the spectrum resources.

In a malicious PUE attack, the attacker's objective is to block secondary users from transmitting by using the open channel. Additionally,in some more sophisticated PUE attacks, the malicious node is only able to attack the network when the main user is not present in order to conserve energy for more potent attacks Fig.1.

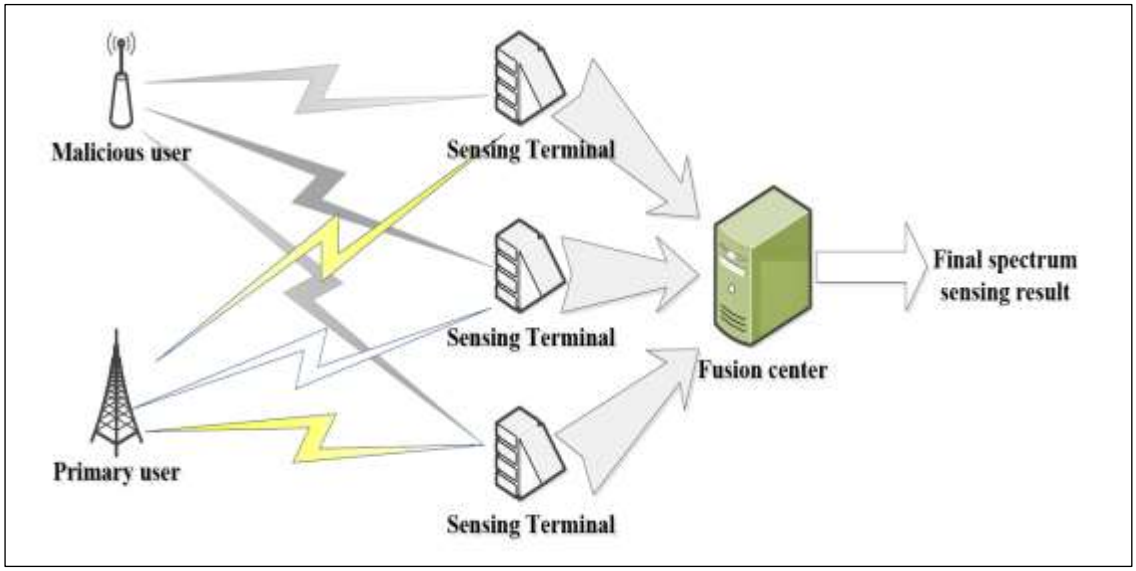

Fig.1 illustrates the main user emulation attack in network-centric cognitive radio

Learning Attack

In a learning attack (LA) [13], the adversary gives the learning radio in cognitive radios erroneous sensory input. When a learning radio picks up incorrect information regarding transmission schemes, it will use that information until it can pick up the right information.

A learning assault is typically paired with other attack kinds. When a cognitive radio tries to employ the best transmission method, for instance, an attacker may launch a PUE attack or an OFA attack. As a result, the learning radio may decide that the best transmission scheme is not the ideal one and instead choose sub-optimal transmission schemes, which results in less performance.A number of strategies have been put forth to counter learning attacks [13]. The learning outcomes must first always be periodically reevaluated. For instance, in a cognitive radio network, the activities of the primary users should be continually recalculated in order to discard any previously learned statistical process of their activities that may be inaccurate.

Second, the learning phases should take place in a truly controlled environment, meaning there shouldn't be any harmful signals present. Third, the learned action shouldn't be used if it violates certain fundamental theoretic conclusions. Fourth, group learning can be used with cognitive radios instead of solo learning.

A group of secondary users can come together to learn the environment, making it more difficult for an attacker to launch a learning attack.

Objective Function Attack[OFA]

Flexible, cognitive radio can sense the outside environment, learning from the past, and make wise decisions to adjust to the

environment's changing conditions [14], The cognitive engine of the adaptive cognitive radio has the capacity to tune a variety of radio characteristics to satisfy particular needs such high transmission data rate, low delay, high security level, and low power consumption. These radio parameters include frame size, bandwidth, power, modulation type, coding rate, MAC protocol, routing protocols, and encryption techniques [15]. These parameters are determined by solving one or more objective functions, albeit some of these functions have a direct connection to the channel's users' inputs.The attacker can modify and skew the findings when a cognitive engine is running to determine the radio parameters appropriate for the present environment. The method is depicted in Fig.2 and the attack is known as the objective function attack (OFA) [15].

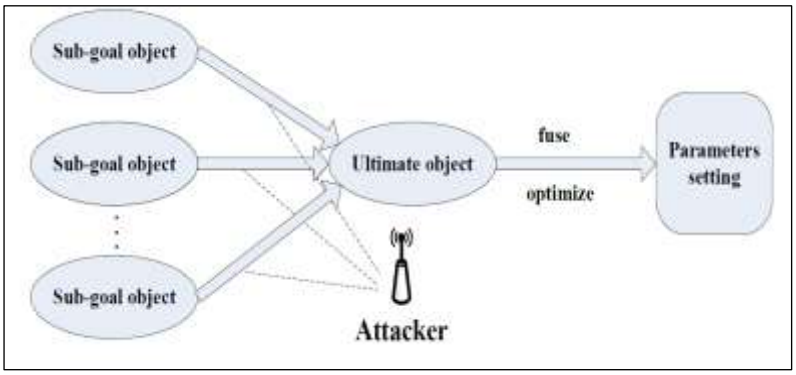

Fig.2 Objective function attack[15]

Jamming

The jamming attack, which can be categorized as a single-channel or multi-channel attack [16], is another assault against cognitive radio networks. The rogue node continuously sends out high-power signals on one channel during a single-channel jamming assault. Therefore, this channel will be jammed for all broadcasts. This kind of jamming is less effective, though, because the malicious node must communicate continuously, which uses a lot of energy Additionally, the strong interfering signal may be quickly found. A different, more effective method of channel jamming is to jam numerous channels at once.

The conventional method is to simultaneously emit interfering signals on all channels. However, even with a huge number of channels, this still uses too much energy. Using cognitive radio technology is a better method since it allows the attacker to change channels in response to what the principal users are doing. Attackers can more successfully jam the channel in this way because cognitive radios can considerably reduce the delay associated with channel switching.Secondary users must first recognize that a jamming attack is actually taking place in order to defend against it. Building a statistical model using adequate data about network noise can help you spot jamming attacks [17]. As a result, the secondary user may be able to distinguish between an attacker's interference and background noise when the attacker attempts to jam it with high power interference. In order to defend against a jamming attack, there are primarily two methods [18]. Use of frequency hopping is one option.

The secondary users will use their high switching abilities to switch to other channels once they discover a jamming

attack and will do so immediately. Spatial retreat is another option. The secondary users may relocate to a place without a jammer in order to leave the jamming area. Therefore, the secondary users won't be able to receive the interference signals that the jammer is sending out. The drawback of this approach is that spatial retreat could result in the secondary user losing contact with the users it is currently speaking with.

Primary Users' Location Attack

We include a new type of assault that can locate primary users and perform a direct physical attack on the equipment in addition to the security threats previously mentioned.

In CRNs, since every user can detect the signal the primary user emits, an attacker can estimate the distance between the primary user and itself based on the signal's strength. As demonstrated in Method A in Fig.3, when many attackers use this method to estimate the location of the primary user, they can obtain a crossover region to pinpoint the precise location of the primary user. While this is happening, the attackers can focus their attack even more due to their mobility and eventually locate the main user as indicated in Method B in Fig.3The attacker can locate the primary user and perform a direct physical attack on it based on its position, rendering the primary user disabled[9].

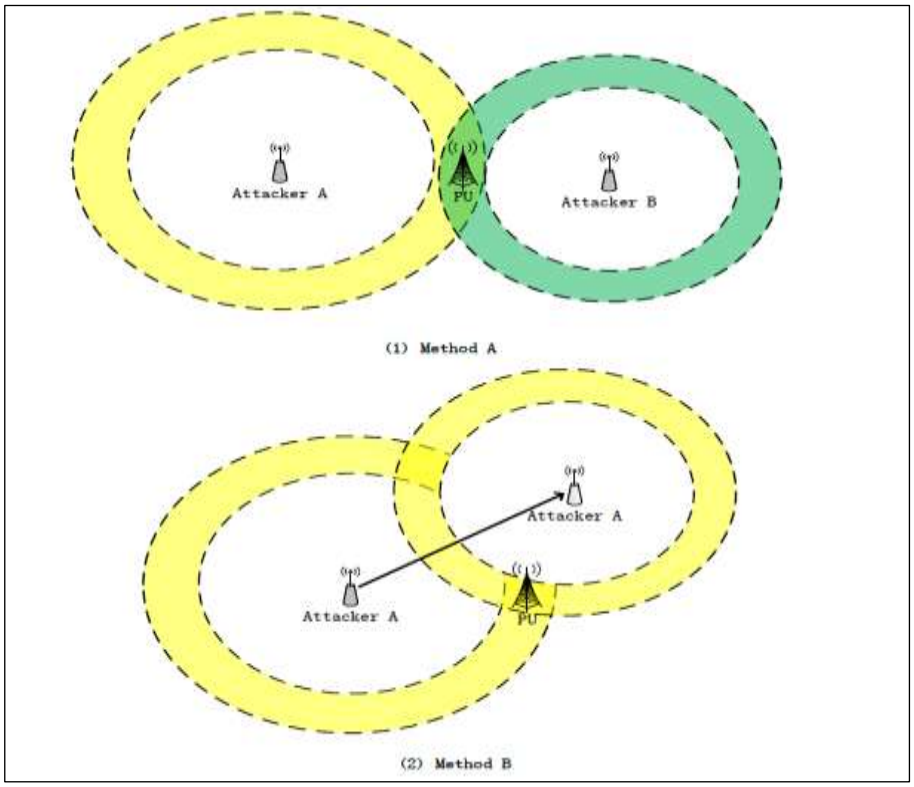

Fig.3 Primary users' location attack[9].

Eavesdropping

We discuss here is eavesdropping, in which a hostile node would listen in on normal users' communications. The authors of [19] investigated a network model in which the principal users utilize a single antenna, the eavesdroppers can use either a single antenna or multiple antennas, and the secondary users employ multiple input multiple output (MIMO) transmission. To increase secrecy capacity without interfering with primary users, the authors analyzed the possible rates of the MIMO secrecy rate between secondary users and created a non-convex max-min problem. When using Gaussian input, it is possible to maximize the secrecy rate by optimizing the transmit covariance matrix. For the case of single-antenna eavesdroppers, algorithms were proposed to calculate the highest attainable secrecy rate, and bounds on the secrecy rate were found for generic scenarios with multi-antenna secrecy and eavesdropper receivers. Here, it is clear that the main concept of [19] is to use power control algorithms to raise the rate between legal users while lowering the rate to eavesdroppers. Thus, the rate of concealment can be raised

Spectrum Sensing Data Falsification

Discusses Spectrum Sensing Data Falsification (SSDF)[18]. It is a common attack in cognitive radio networks and is also referred to as the Byzantine Attack. The receiver receives incorrect sensing data and decides on the improper spectrum access since the attacker sent bogus local spectrum sensing findings to its neighbors or the fusion center. The fusion center or one secondary user may be the target of this attack.

If it attacks the secondary user and provides incorrect sensing information to just one secondary user, the secondary user might not be able to distinguish between accurate and inaccurate sensing data, leading to incorrect decisions.

Although the fusion center is the target of the assault, many other users, including malevolent and legitimate secondary users, can provide the fusion center with sensing data. The fusion center will have a high probability of choosing correctly to identify which information would be authentic if the majority of the sensing information comes from reliable users.

In Cognitive Radio Networks[5] On the physical layer of cognitive radio networks, there have been a number of significant threats and attacks in recent years, which we highlight in Table1.

Table 1 lists the physical layer security attacks and their defenses in cognitive radio network[5]

attacks	Countermeasures	Characteristics
primary user emulation (PUE) [20]	LocDef [21] based on the primary user's location	the process of determining whether a signal is coming from an active transmitter by determining its position and analyzing its signal properties.
learning attack (LA)[13]	Effective and long-term learning [13]	The learning outcomes must constantly be updated across time.
objective function attack OFA [13]	Define threshold values whenever the radio parameters need to be updated [20]	User can use a good intrusion detection system.
Jamming [16]	Frequency hopping or	For cognitive radio,

	spatial retreat [17]_[18]	frequency hopping is advantageous.
Primary Users' Location Attack[9]	Changing the intensity of signals irregularly [9]	Location information can be shielded
Eavesdroppi[19]	Power control or beamforming [19]	Theoretical findings to establish a general bound.
Spectrum Sensing data falsification SSDF [18]	Powerful schemes at data fusion center [22]	reputation-based schemes or Sequential Probability Ratio Test

IV. COCLUSION

In this paper , we determined some of the dangerous attacks on physical layer in cognitive radio networks and describe the Characteristics of each one of them.
and discusses the many security flaws that can be exploited by an attacker against physical layer in Cognitive radio network

REFRENCE

1. S. S. Ivrigh, S. Siavash, and S. M. S. Sadough, "Spectrum sensing for cognitive radio networks based on blind source separation," KSII Transactions on Internet & Information Systems, vol. 4, pp. 613–631, 2013.
2. S. Chang, K. Nagothu, B. Kelley, et al., A Beamforming Approach to Smart Grid Systems Based on Cloud Cognitive Radio, 2014.
3. S. Haykin, "Cognitive radio: Brain-empowered wireless communications," Selected Areas in Communications, vol. 2, pp. 201-220, 2005.
4. K. C. Chen, Y. J. Peng, and N. Prasad, et al., "Cognitive radio network architecture: Part I--general structure," in Proc. 2nd International Conference on Ubiquitous Information Management and Communication, 2008, pp. 114-119.
5. SHU, Zhihui; QIAN, Yi; CI, Song. On physical layer security for cognitive radio networks. IEEE Network, 2013, 27.3: 28-33.
6. Nanthini, S. Bhagavathy, et al. "Attacks in cognitive radio networks (CRN)-A survey." Indian Journal of science and Technology 7.4 (2014): 530.
7. Tashman, Deemah H., and Walaa Hamouda. "An overview and future directions on physical-layer security for cognitive radio networks." IEEE Network 35.3 (2020): 205-211.
8. M. Khasawneh, A. Agarwal " A Survey on Security in Cognitive Radio Networks," Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada in 2014 6th International Conference on CSIT.
9. Yi. Yu, L. Hu, H. Li, Y. Zhang, F. Wu, and J. Chu "The Security of Physical Layer in Cognitive Radio Networks," Jilin University, Chang Chun 130012, China in Journal of Communications Vol. 9, No. 12, December 2014.
10. Q. Liu, Z. Zhou, C. Yang, et al., "The coverage analysis of cognitive radio network," in Proc. 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008, pp. 1-4.
11. A.N. Mody, R. Reddy, T. Kiernan, et al., "Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard," in Proc. Military Communications Conference, IEEE, 2009, pp. 1-7.
12. W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive

radio networks," Journal of Internet Technology, vol. 2, pp. 181-198, 2011.
13. T. C. Clancy, and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," IEEE Crowncom, May. 2008, pp. 1–8.
14. Q. Mahmoud, "Cognitive networks: Towards self-aware networks," Wiley E-Book, New York, 2007.
15. T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in Proc. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, IEEE, 2008.
16. A. Sampath, H. Dai, H. Zheng, and B. Y. Zhao, "Multi-channel Jamming Attacks using Cognitive Radios," IEEE ICCCN, Aug. 2007, pp.352–57.
17. W. Xu et al., "Channel Surfng and Spatial Retreats: Defenses Against Wireless Denial of Service," Proc. 3rd ACM Wksp. Wireless Security,Philadelphia, PA, Jan. 2004, pp. 80–89.
18. W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," J. Internet Tech., vol. 12, no. 2, 2011, pp.25–37.
19. L. Zhang et al., "On the Relationship Between the Multi-Antenna Secrecy Communications and Cognitive Radio Communications," IEEE Trans. Commun., vol. 58, issue 6, June 2010, pp. 1877–86.
20. O. Leon, J. H. Serrano and M. Soriano, "Securing Cognitive Radio Networks," Int'l. J. Commun. Systems, vol. 23, 2010, pp. 633–52.
21. R. Chen, J. M. Park, and J. H. Reed, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks," IEEE JSAC, vol. 26,issue 1, 2008, pp. 25–37.
22. R. Chen et al., "Toward Secure Distributed Spectrum Sensing in CognitiveRadio Networks," IEEE Commun. Mag., vol. 46, no. 4, 2008, pp. 50–55.