Indian Journal of Science and Technology, *Vol 7(4), 530–536, April 2014*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Attacks in Cognitive Radio Networks (CRN) — A Survey

S. Bhagavathy Nanthini[1] *, M. Hemalatha[1], D. Manivannan[1] and L. Devasena [2]

[1]School of Computing, SASTRA University, Thanjavur, Tamil Nadu-613401, India; nanthubha@gmail.com, hemalatha@it.sastra.edu, dmv@cse.sastra.edu
[2]School of EEE, SASTRA University, Thanjavur, Tamil Nadu-613401, India; devasena@eie.sastra.edu

Abstract

As the wireless communication greatly depends on spectrum utilization, the increase in demand for new wireless services and their application leads to the spectrum scarcity. In order to utilize the available spectrum efficiently, "cognitive radio"- The demanding technology is introduced. It is a dynamic technology that can sense the medium, utilizes the available white spaces, for transmission by detecting its neighboring devices. The cognitive radio targets to increase the efficiency of the spectrum changes without causing any intervention to the licensed users. Since cognitive radio works in the open network space, it increases the chance of the attacker to show intervene on the spectral medium. So, the security becomes the key factor. This leads to the realization of various security threats in the cognitive radio. There are various papers covering the security issues over the threats in cognitive radio, but this paper provides an advanced survey over attacks and common threats and the possibility of securing the available spectrum from the attackers. In addition to that future scope and challenges are also addressed. This survey will help the researchers to identify the space left out and the problems to be attached related to security issues on cognitive radio.

Keywords: Attacks, Digital Signatures, Cognitive-radio, Security, Spread Spectrum Modulation

1. Introduction

For the past decade wireless technology shows a drastic improvement in its technological and its application aspects. This increases the number of available wireless users. These wireless users greatly rely on the available radio spectrum, which leads to a scarcity in the available spectrum. The Federal Communications Commission (FCC) insists that certain portions of the RF spectrum are made available for public use, which is vacant[1]. These vacant spaces termed as White space devices comprised with technologies to prevent interference, Technologies constitutes spectrum sensing and geo-location capabilities. Based on this a new promising technology called cognitive radio is implemented. Mitola developed the design of cognitive radio[2] at the defense advanced project research agency in U.S.A.

Cognitive radio is defined as a software defined radio[3,4] in wireless communication, that sense the environment and detect the free space amongst the crowded channel, and utilize the vacant space efficiently. It can also work on the available channel as a secondary user paving way for both the user without any interference[6]. It is also defined as a transceiver which has the ability to find the available communication channel in the wireless spectrum and perform transmission and reception characteristics according to the available channel. While two users rely on the particular channel there is a possibility of causing interferences and also there occurs a wide chance for the attackers to interfere the particular channel. In order to avoid those possibilities, we are securing cognitive radio in different methods[7,8].

This paper focuses on the analysis of security issues in various perspectives on the cognitive radio networks.

*Author for correspondence

First view says the various methods of securing cognitive radios relying over each layer, which is named as layered attacks. This layered attack can be classified based on the various layers in the ISO / OSI model. Attacks falling under physical layer is said to be a physical layer attack, which rely on link layer is said to be MAC layer attacks, and over the network layer is said to be network layer attacks, and on transport layer is said to be transport layer attacks. Based on the attacks, threats are detected and the security measures are taken. Second view conveys the method of securing the spectrum channel by combining the cognitive radio with the spread spectrum modulations[9]. By using this method the unique characteristics of the cognitive radio provide a protected and consistent communication over the given medium. Here, the spread spectrum modulations are combined with the encryption technique so that it is possible to secure as well as it can have the potential to switch over to the various frequency bands. According to the third view, the CRN is secured by means of Digital signature[9]. Here, efficient Primary User Identification (PUI) from public key cryptography is used to secure the communication made through the channel. Using this method, the interruption caused by the other unauthorized users can be avoided. The digital signature method which uses the public key cryptography is an effective method and is easily implementable since its light weighted one and key management is simple.

Attackers launch their attack on each layer, but most commonly they target on the lower level layer i.e. physical layer. When comparing the physical layer to the other corresponding layers the security over the higher layers is done through various higher layer authentication and encryption methods. Here, they focus on securing cognitive radio from the lowest layer i.e., physical layer, since the CR relies heavily on PHY layer spectrum sensing leaving the system vulnerable to physical layer attacks[10,11]. This physical layer is secured by means of location specific information's by locating the finger prints. By promoting PUE attack the extraction of transmitter fingerprints is made multipath fading propagation environment. Wavelett transformations detect the transmitter finger prints and analyze them.

Another way of securing the cognitive radio is by means of generating a random number with the help of various algorithms. Here, all the algorithms that are used to generate random number is compared and the one superior algorithm is detected for securing the CR, One such focused algorithm is ULSI.

In this paper Section 1 covers the methods of securing layered attacks in cognitive radio. Section2 deals with securing cognitive radio by the spread spectrum modulation techniques. Section3 points on the specific layer and the process of securing it. Section 4 discuss about securing by means of digital signature method.

2. Cognitive Radio Networks

Now a day, on the whole communication process totally depends on the wireless medium. Technological improvement reaches the peak level, and their user's gets increase in the higher rate. The wireless technology greatly depends on the radio frequency spectrum, whereas the available spectrum is low when compared to their utilization. Thus the effective utilization of these spectra becomes a necessity, and so the cognitive radio becomes the promising technology. The cognitive radio is termed as the software defined radio technology that avails the license to the unlicensed users without any inference.

It also considered as a model for wireless technology which takes an intelligent decision by changing its transmission or reception parameters based on the neighboring networks without providing any interference to other users. The cognitive radio network architecture can be broadly divided into two clusters: primary network also named as licensed users in the existing networks. The other is cognitive radio networks otherwise called as unlicensed users.

Figure 1 shows the architecture of the cognitive radio, where the lower most layer is the physical layer. Next to that there is link layer, network layer and transport layer. Each layer performs different functions which are explained in detail.

Physical layer performs three functions they are, Spectrum sensing, Channel estimation and Data transmission. Spectrum sensing becomes the much needed task when compared to other two functions. As the name implies, the task of spectrum sensing is to sense the available free medium for an effective transmission, also to avoid the occurrence of any interference to potential primary users in their vicinity. Then comes the channel estimation, before setting up the link, the quality of the sub channels is estimated based on their transmission parameters such as transmit power, bit rate and coding. In data transmission, after assigning the spectrum by means of spectrum sensing and channel estimation, the transmission of data takes place. It should have the capability

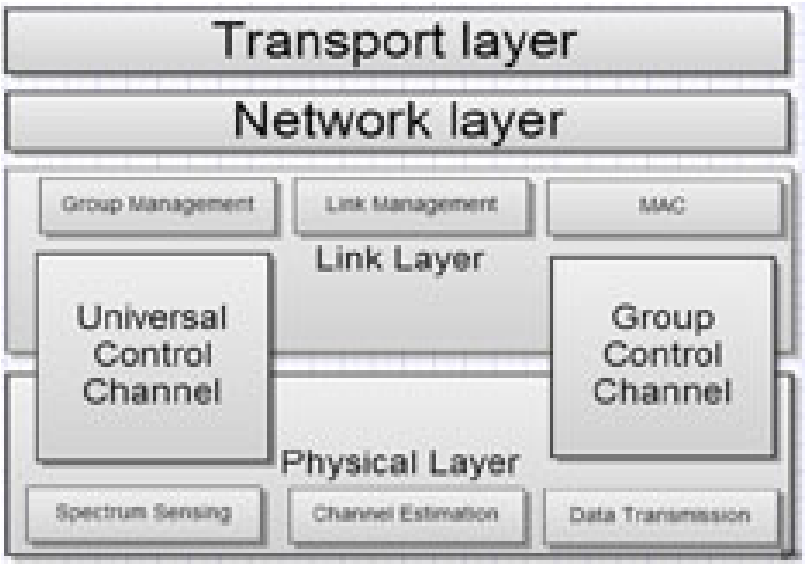

Figure 1. Architecture of cognitive Radio

to operate at variable symbol rates, different channel coding schemes, power levels, and capable of using multiple antennas to nullify the interference.

The functions of the link layers are group management, link management, and medium access control. In group management, there will be number of secondary user groups, where the arriving user can join any of the existing groups or form a new one through a universal control channel. Link management covers the set up on the link to enable the communication between any two secondary users and also maintain the link until the duration of the communication. Medium access control controls the sub channels. If any of the sub channels is used by the particular secondary users, then the particular channel cannot be used by any other secondary users. Whereas the network layers and transport layers known as the higher layer is used for the transferring of the data allocating the particular network.

The characteristics over the cognitive radio are Cognitive capability, Re-configurability. Cognitive capability makes the device to sense the environment and to choose the best available spectrum for transmission. This becomes possible through the spectrum management process. Re configurability enables the device to make it adapt to its environment by modifying its parameters such as frequency, modulation etc. There are three different mechanisms in cognitive cycle to analyze the best spectrum in the available environment. They are given by Spectrum sensing in which is used to sense the available spectrum and chooses the best possible one, Spectrum analysis is based on the information over the available spectrum holes and analyzes the network and channel characteristics for each spectrum hole, Spectrum decision decides the appropriate spectrum hole for transmission.

3. Need for Security in CRN

Cognitive radio has the capability of adapting to the environment and make changes based on their communication capabilities for the secure communication. Comparing the wired network and the wireless network, the security is susceptible in case of wireless network. When the data are sent via a wireless network, then there is a possibility of eavesdropped, or can be altered, jamming may take place. The cognitive radio networks have a unique characteristic that security becomes essential over it. This paper has summarized various possibilities of attacks over it, and the security issues to be taken to overcome those attacks in CRN.

4. Attacks Over the Layers and its Detection

The best capability of the cognitive radio network is to take advantage over the available vacant spaces in a spectrum. A study done at Berkeley Wireless Research Center (BWRC) says the frequency ranging from 1GHz to 10 GHz is underutilized. These nodes can sense the

environment and utilize the free spectrum. The challenges over the Cognitive radio are transparency to primary users and non-interference. So there occurs an increase in the possibility for the attackers. The attacks over each layer are analyzed by four major classes based on the layer where the attack falls: Physical layer attack, Data Link layer attack, Network layer attack and Transport layer attack.

In physical layer the possible attacks are Primary User Emulation (PUE), objective function attack and jamming[13]. First we confer about the PUE attack. The primary user emulation attack is carried out by a malicious secondary user emulating a primary user or masquerading as a primary user to obtain the resource of a given channel[14]. Based on their motivations they are classified into two categories. These are SELFISH PUE: 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: In malicious PUE, attackers try to prevent the legitimate secondary users from using the holes found in the spectrum. The PUE attack can target both the types of cognitive radio such as learning radios and policy radios[15]. When dealing with the policy radios, the effect of the attack vanishes when the attackers leave the channel. Then the secondary users claim the channel thinking that the channel is idle. On the other hand in learning radios, information about the primary users current and the past behaviors are gathered in order to know when the channel gets idle. The attackers perform this attack when the channel gets idle. There are various remedies to solve this PUE attack one such therapy, and to focus on the cross layer pattern recognition technique. This technique exploits the radio signatures of each cognitive radio device. To overcome this attack, waveform recognition is used to detect the malevolent devices. The process involved in this proposal are the enrollment in collecting data's and testing in order to determine the user This approach is a cross layer security, which is capable of highlighting the peculiarity among cognitive radio devices. It is also defined as one of the perfect method to shield the PUE attack.

The second type of attack in the physical layer is Objective function attack. In this attack Radio parameters are considered such as bandwidth, center frequency, modulation type, power, encryption type, protocol,coding rate, frame size, and channel access,. The cognitive engine calculates these parameters to find the radio parameters that can maximize the data rate and minimize the power. When cognitive engine is running to calculate these parameters, the attackers launch their hit. By means of this hit, the particular attacker takes over the control make results biased and tailored to his interest. Whenever the cognitive engine tries to use the higher security level the attackers commence the jamming attack on the radio reducing the overall objective function. Then the cognitive engine will refrain from increasing the security level in order not to decrease the objective function. This attack is affective only on on-line learning radios and has no effect on off-line learning radios. There is no good solution to safe guard cognitive radio from this attack; rather a simple suggestion is made to define threshold values for each radio parameters. If the parameters are not up to the threshold level the communication stops. The third type of attack over physical layer is jamming[16,17]. In jamming the attackers or jammer sends the packet continuously to hamper the legitimate participants in a communication session. This makes the legitimate user to never sense the medium as idle, or the attacker sends the packets to the legitimate user and forces them to receive the junk packets. It also disrupts the communication by blasting a radio transmission resulting in the corruption of packets received by legal users. There exist four types of jammers they are 1. Constant, 2. Deceptive, 3. Random, 4. Reactive.

Two strategies are used to defend against jamming. The first strategy is to escape the denial of service is channel surfing, or frequency hopping. The second strategy is spatial retreat where legitimate user changes their location to escape their interference range imposed by the attacker. In this approach essential point is to leave the region where the attacker is present and the users must stay within the range of each other to continue communication.

The attacks on LINK LAYER are Spectrum Sensing Data Falsification (SSDF), Control Channel Saturation Dos attack (CCSD), Selfish Channel Negotiation (SCN)[18]. In SSDF the attack occurs when an attacker sends false local spectrum sensing results to its neighbors or to the fusion center, causes the receiver to make a wrong spectrum-sensing decision[19]. 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. If the sum is above or approx equal to the

threshold value then the sensed effect says the medium is full by saying that the incumbent signal is present, otherwise the band is said to be free, i.e., it says the incumbent signal is absent. Here, there is a possibility of miss detection. This can be overcome by increasing the threshold value. Next attack we find in link layer is Selfish channel negotiation. In multi hop cognitive radio network, a cognitive radio can refuse to forward any data for other host. This cause the conservation of energy and increase in throughput. 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[21,22].

The attacks found in the network layers are sinkhole attack and HELLO flood attacks[20]. In the Sinkhole attack shows itself as a best route to a specific destination, luring neighboring nodes to use it to forward their packets. An attacker can use this way to perform another attack called selective forwarding, where he can modify or discard the packets from any node in the network. 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. This attack is overcome by Geographic routing protocols[24]. Geographic protocols try to construct a topology on demand using only local communication than relying on the base station. 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 HELLO flood attack, the attack gets accomplished when an attacker sends broadcast messages to all nodes in a network with a enough power to convince them that it is their neighbor. When this attack is detected there occurs a possibility of packet loss, absence of neighbors to forward the packets. This attack is defended by introducing a key called a symmetric key to share it with the trusted base station. The Kerberos algorithm in cryptography is used to facilitate the establishment of session keys between the different parties in the network. To prevent an attacker from creating the session key is by limiting the shared keys. The symmetric key is suggested because they are faster and lower overhead on system resources.

In transport layer the possible attack is LION attacks[23]. 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.

5. Cognitive Radio along with Spread Spectrum Modulation

Here, cognitive radio is secured by means of the spread spectrum modulation. Cognitive utilizes the licensed spectrum for transmission where, the security for such spectrum is essential. Such, a secure communication is made by the combinations of spread spectrum modulation and encryption algorithms with the cognitive radio technology. Cognitive radio is said to be an advancement of SDR making the sensing and adaptation parameters dynamic. Cognitive radio can be viewed as a collaborative form of an application constitutes SDR and intelligent signal processing also comprises the functional elements of radio flexibility, spectral awareness and intelligent decision making. Various encryption techniques are also applied to secure the cognitive radios, the commonly used techniques are symmetric encryption technique recognized as private key encryption algorithm. Commonly used techniques are RSA, elliptic, SHA etc.

6. Securing Spectrum Sensing in Multi-Channel

In this paper, the cornered attack is the byzantine attacks. Byzantine attack includes coalition head and CR as their attackers. These attackers targets on reducing the channels available and sense the multichannel cooperative spectrum sensing. The probability of these attacks is derived and a new selection formula is formulated for the coalition head. The probability of the change in local decision for each cognitive radio becomes the Byzantine attacker by which the probability of attack is derived. When the Byzantine attackers continue their attack, contribution of their related coalitions in the system decreases and they get blocked out of the coalition. In considering the distributed cooperative multichannel spectrum sensing, attacks such as coalition head and multichannel byzantine attacks are introduced. The simulation is being carried out to overcome the block attackers; the results have concluded that the various counter attacks can be used to mask the attackers from the coalition head. It also

increases the number of the channels available when the attackers are present.

7. Protocols for the Dynamic Cognitive Radio Networks

The Spectrum Sensing, resource allocation and management is the issues largely focused by cognitive radio networks. There are many existing protocols are introduced as a challenge to the process of the CRN. The lack of centralized authority makes the selfish node incline towards the self-centered behavior to maximize their supports. Here, a cross-layer is proposed for avoiding the selfish performance in the routing protocols for the dynamic cognitive radio network in preference to selfish nodes. Simulation results proposed that SAR provides better performance, by means of higher throughput, lower delay, and better delivery ratio. So, it can be said as the cross layer selfishness avoiding routing protocol.

8. Secure Communication based on Digital Signature

Cognitive radio is a challenging concept to improve the consumption of limited electromagnetic spectrum resources for upcoming wireless communications. It is essential to secure the cognitive radios to avoid interference. There may be various members join the CRN or vacate the network any time. So there occurs a compulsion to secure the network. This is done through the digital signature. Here, there are two users utilizing the cognitive radio. They are primary user and secondary user. Primary is of licensed user and secondary is of unlicensed user who can use the medium cognitively without causing injurious to the primary user. Here the primary user identification technique is used to secure the cognitive. Various encryption techniques are used to safeguard the cognitive networks.

9. 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.

10. References

1. El-Hajj W, Safa H, Guizani M. Survey of security issues in cognitive radio networks. J Internet Tech. 2011; 12(2).
2. Mitola J III. Software radios – survey, critical evaluation and future directions. IEEE Aero Electron Syst Mag. 1993 Apr; 8(4):25–36.
3. Tuttlebee W. Software defined radio: enabling technologies. Chichester: Wiley; 2002.
4. Ulversøy T. Software defined radio: challenges and opportunities. IEEE Communications Surveys & Tutorials. 2010; 12(4):531–50.
5. Hsu C-S, Chen Y-S, He C-E. An efficient dynamic adjusting MAC protocol for multichannel cognitive wireless networks. 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS); 2010 Jun 25–27; Beijing, China. IEEE. p. 556–60.
6. Liu Y, Zhao Z, Tang H. Radio resource management between two user classes in cognitive radio communication. 2010 Second International Conference on Networks Security. Wireless Communications and Trusted Computing. 2010 Apr 24–25; Wuhan, Hubei . IEEE. p. 215–18.
7. Tang L, Wu J. Research and analysis on cognitive radio network security. Computer Science & Communications. 2012 Apr; 4(4):120–26.
8. Zhang Y, Xu GC, Geng XZ. Security threats in cognitive radio networks. 10th IEEE International Conference on High Performance Computing and Communications. HPCC '08. 2008 Sep 25–27; Dalian. IEEE. p. 1–7.
9. Parvin S, Hussain FK. Digital signature-based secure communication in cognitive radio networks. 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA). Barcelona. IEEE. p. 9–12.
10. Zhao C, Xie L, Jiang X, Huang L, YaoA Y. PHY-layer authentication approach for transmitter identification in cognitive radio networks. 2010 International Conference on Communications and Mobile Computing (CMC). 2010 Ap 12–14; Shenzhen. IEEE. p. 154–58.
11. Wang H, Lightfoot L, Li T. On PHY-layer security of cognitive radio:collaborative sensing under malicious attacks. 44th Annual Conference on Information Sciences and Systems (CISS); 2010 Mar 217–19; Princeton, NJ. IEEE. p. 66–73.
12. Sampath A, Dai H, Zheng H, Zhao BY. Multichannel jamming attacks using cognitive radios. Proceedings of 16th International Conference on Computer Communications

and Networks. ICCCN 2007; 2007 Aug 13–16; Honolulu, HI. IEEE. p. 352–57.
13. Chen R, Park J-M. Ensuring trustworthy spectrum sensing in cognitive radio networks. SDR '06.1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks; 2006 Sep 25; Reston, VA, USA. IEEE. p. 110–19.
14. Anand S, Jin Z, Subbalakshmi K. An Analytical model for primary user emulation attacks in cognitive radio networks. 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks. DySPAN; 2008 Oct; Chicago, IL. IEEE. p. 3905–14.
15. Pei Y, Liang Y-C, Zhang L, The KC, Li KH. Secure communication over MISO cognitive radio channels. IEEE Trans Wireless Comm. 2010; 9:1494–502.
16. Xu W, Trappe W, Zhang Y, Wood T. The feasibility of launching and detecting jamming attacks in wireless networks. MobiHoc '05 Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing; 2005 May; Urbana, IL. p. 46–57.
17. Sampath A, Dai H, Zheng H, Zhao BY. Multi-channel jamming attacks using cognitive radios, Proceedings of 16th International Conference on Computer Communications and Networks (ICCCN 2007). 2007 Aug 13–16; Honolulu, HI. IEEE. p. 352–57.
18. Kaligineedi P, Khabbazian M, Bhargava VK. Secure cooperative sensing techniques for cognitive radio systems. IEEE International Conference on Communications (ICC '08). 2008 May. Beijing, China. IEEE. p. 3406–10.
19. Wang W, Li H, Sun Y, Han Z. Attack-proof collaborative spectrum sensing in cognitive radio networks. 43rd Annual Conference on Information Sciences and Systems (CISS 2009). 2009 Mar; Baltimore, MD. IEEE. p. 130–34.
20. Wang W, Sun Y, Li H, Han Z. Cross-layer attack and defense in cognitive radio networks. 2010 Dec 6–10. Miami, FL. IEEE. p. 1–6.
21. Zhu L, Zhou H. Two types of attacks against cognitive radio network MAC protocols. International Conference on Computer Science and Software Engineering; 2008 Dec; Wuhan, China. IEEE. p.1110–13.
22. Bian K, Park J-M. MAC-layer misbehaviors in multi-hop cognitive radio networks. US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006); 2006 Aug.
23. Hernandez-Serrano J, León O, Soriano M. Modeling the Lion Attack in Cognitive Radio Networks. EURASIP Journal on Wireless Communications and Networking. 2011; 10:242–304.
24. Hu Y-C, Johnson DB, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02); 2002 Jun; Callicoon, NY.