Cognitive Radio Networks Security Threats and Attacks: A Review

Suchismita Bhattacharjee
North Eastern Regional Institute of Science and Technology Nirjuli-791109,
Arunachal Pradesh,INDIA

Roshni Rajkumari
North Eastern Regional Institute of Science and Technology Nirjuli-791109,
Arunachal Pradesh,INDIA

Ningrinla Marchang
North Eastern Regional Institute of Science and Technology Nirjuli-791109,
Arunachal Pradesh,INDIA

ABSTRACT
Cognitive Radio (CR) is a technology that promises to solve the spectrum shortage problem by allowing secondary users to coexist with primary user without causing any interference to the communication. It aims to improve the utilization of the radio spectrum. Although the operational aspects of CR are being explored widely, its security aspects have gained little attention. In this survey, we present a comprehensive list of major known security threats and attacks within a Cognitive Radio Network (CRN). Our objective in this paper is to analyze the security issues of the main recent developments (which includes attacks and mitigations) of Cognitive Radio Networks. We hope that this survey paper can provide the insight and the roadmap for future research efforts in the emerging field of CRN security and utility.

Keywords
Cognitive Radio, Cognitive Radio Network, security

1. INTRODUCTION
The current wireless network is characterised by a fixed static spectrum policy, i.e., the governmental policy provides spectrum access to those users who are licensed [1]. But, due to tremendous demand of the spectrum by different users, the governmental policy is fading. Despite the shortage of spectrum bands, it has been found out that the existing spectrum bands are also not utilized properly. To tackle the problem of inefficient use of spectrum, a new technology called as Cognitive Radio Network emerged, which is based on the technique called Dynamic Spectrum Access technique [2]. A cognitive radio (CR) is capable of sensing its surrounding environment and adapting the communication parameters accordingly. A CR continuously senses and collects different types of information regarding the wireless environment. It also has the ability to find other frequency band if interference is detected on the frequencies being used instantly. In order to address these challenges, each CR user in the CR network must be able to determine the available spectrum, select the best available channel, coordinate the free channel access with other users and vacate the channel when a licensed user is detected [2].

A major concern with CRN is the security issue. To ensure a smooth operation of CRNs, the establishment of a secure communication is needed.

This paper describes the special characteristics of CRN and analyses the current and potential security threats which can arise as attacks. In section II, the main characteristic of CRs, which is Dynamic Spectrum Access (DSA) is described. In section III, we present the various threats and attacks on CRN. Their mitigations or countermeasures are described in section IV. Finally in section V, conclusions are presented.

2. CHARACTERISTIC OF A CRN
The terms SDR (Software Defined Radio) and CR (Cognitive Radio) were promoted by Mitola in 1991 and 1998 respectively [3]. Software Defined Radio (SDR), also known as Software Radio, is a multiband radio that supports multiple air interferences and is reconfigurable through software which runs on Digital Signal Processor (DSP) or general purpose microprocessors [4]. It is a highly configurable wireless communication device, where it is capable of synthesizing a large number of communication waveforms, by combining and composing the processing graphs of different radio components. CR is built on a Software radio platform, which is a context aware intelligent radio, potentially capable of autonomous reconfiguration by learning from and adapting to the communication environment [3].

2.1 Dynamic Spectrum Access
Current regulation on spectrum is a kind of static spectrum assignment policy. The spectrum is assigned to licensed users on a long term basis for large geographical regions [2]. With the increase in wireless devices, the demand of communication is rising. The spectrum demand is so high that the Federal Communication Commission (FCC) of the U.S.A. is considering on using Dynamic Spectrum Access (DSA) to open up the licensed bands to unlicensed users on the basis of non-interference [2].

A CR has four functions, viz., spectrum sensing, spectrum management, spectrum mobility and spectrum sharing. The implementation of these functionalities exposes severe security threats. Spectrum sensing is defined as detecting spectrum holes and sharing the spectrum without interfering with other users. In DSA, the primary users have the license to use the certain frequency band and when they are not in use, it is left idle. Thus, their available spectrum could be used by the secondary users. Such secondary user requires sensing algorithm to detect the spectrum holes for communication.

Spectrum Management is the process of selecting the best available channel. It is capable of selecting the most appropriate bands from among the available bands according to the QoS requirements of the application [2]. Spectrum sharing prevents multiple users colliding the overlapping portion of the spectrum. There is another concept called spectrum mobility which refers to the maintenance of seamless communication during the transition to better spectrum. The process of a CR, vacating the current spectrum band and moving to a new available spectrum band is called spectrum hand- off [2]. During spectrum handoff, the security threats are serious. These attacks and the mitigations for the threats and attacks will be discussed in next two sections.

3. SECURITY ATTACKS IN CRN

In the phase of design and analysis of secure distribution system, trust is an important feature [5]. Trust and security in Cognitive Radio Networks are always interlinked. They are complementive and mutually inclusive to each other. To discuss the attacks on CRN, we classify them based on the layers in which the attack can occur. Table I summarizes various attacks in different layers.

At the Physical layer, Primary User Emulation attack (PUE), Objective Function Attacks, Jamming, etc. are discussed. Attacks at the Link layer include Spectrum Sensing Data Falsification (SSDF), Control Channel Saturation DOS Attack (CCSD), etc. At the Network layer, Hello Flood Attack and Sinkhole Attack are discussed. At the Transport layer, Lion attack is well known. Some of these attacks might work on different layers too, such as, jamming, which can be launched at physical or MAC layers.

3.1 Primary User Emulation Attack (PUEA)

One of the major technical challenges associated with spectrum sensing is the problem of exactly distinguishing primary user signals from secondary user signals. In CR network, primary users possess the priority to access the channel. If a primary user be- gins to transmit across a frequency band occupied by a secondary user, it is required to leave that particular specific spectrum band immediately. Conversely, when there is no primary user activity present within a frequency range, all the secondary users possess equal rights to the unoccupied frequency channel. Based on these paradigms, there exists the potential for malicious secondary users to mimic the spectral characteristics of the primary users in order to gain priority access to the wireless channels occupied by other secondary users. This scenario is referred as Primary User Emulation [6][7], which is carried out by a malicious secondary user emulating a primary user or masquerading itself as a primary user. As a result the attacker is able to have the bands of a spectrum. In the presence of energy detection, a secondary user can recognize the signal of other secondary users but cannot recognize the signal of primary users. When a signal is recognized, which is detected when a secondary user is on, it is assumed that the signal is that of a secondary user only; otherwise it concludes that the signal is of a primary user.

Depending on the motivation of the attacker, PUE attack can be a selfish PUE attack or a malicious PUE attack. A selfish PUE attach tries to maximize its own spectrum usage. When a selfish PUE attacker detects a free spectrum band, they prevent other secondary users from using that band by emulating the signal characteristics of the primary user. Malicious PUE attack is similar to denial of service attack. It prevents the legitimate secondary users from detecting and using the free spectrum bands.

3.2 Objective Function Attack (OFA)

Objective function attacks are those in which attackers prevents CR from adapting changes by tampering data [8]. A CR has a cognitive engine, which includes many radio parameters that are under its control. The cognitive engine calculates these parameters by solving one or more objective functions, for instance finding the radio parameters that maximize data rate and minimize power.

In[8], a scenario is presented where the radios (in learning phase) try different combinations of input parameters as center frequency, bandwidth, power, modulation type, coding rate, channel access protocol etc and measures the observed statistics such as bit error rate. Then the cognitive engine will refrain the whole process by evaluating the objective function to observe which input will give the best result for their application. Here, an adversary can manipulate the optimized objective function by affecting the channel. In this way, the attacker forces the radio to use a low security level that can be hacked easily.

3.3 Jamming Attack

The objective of jamming attack in the communication network is to deny service by eating up high percentage of bandwidth. In jamming attack, the attacker (or the jammer) maliciously sends out packets continuously to obstruct the legitimate participants in a communication session from sending or receiving data; simultaneously it creates a denial of service situation. The jammer can also disrupt communication by blasting a radio transmission resulting in the corruption of packets received by legitimate users. A more dangerous attack that a jammer can perform is jamming the dedicated channel that is being used to exchange sensing information between CRs [5]. Thus, jamming is an attack that is known to both physical and MAC layers.

Four types of jammers have been identified in [9] viz., Constant Jammer, Deception Jammer, Random Jammer and Reactive Jammer. Constant/Static jammer emits signal continuously on a particular channel. Deception jammer is similar to constant jammer. But, in this case, the pulses are similar to the regular data packets from a legitimate user. Reactive jammer transmits jamming pulses only when it finds the channel to be busy, so as to cause collision to an on-going transmission. Random jammer alternates between jamming and sleeping mode [11].

3.4 Cross- layer Attack

A smart attacker can launch several attacks in different layers co-ordinately. This is referred to as the cross-layer attack [12]. This coordination of attack activities can reduce the attacker's probability of being detected, lowers the cost to conduct the attack and helps to achieve the attacker's goal which may not be possible in a single layer. To make this attack a success, all attackers should have a clearly defined goal. It can also reduce channel utilization both in PHY layer and MAC layer. Cross-layer attack can be defined as, a collection of attack activities that are conducted co-ordinately in multiple network layers in order to achieve specific attack goals.

3.5 Spectrum Sensing Data Falsification Attack (SSDF)

This attack is the transmission of false spectrum sensing data by malicious secondary users. SSDF are referred to such attacks where an attacker may send false local spectrum sensing results to a data collector, causing the data collector to make a wrong spectrum sensing decision. This attack is also known as the Byzantine Attack. It takes place when an attacker sends false local spectrum sensing data to its neighbours or to the fusion center [13][14]. In a centralized CRN, a fusion center collects all the sensed data and then uses them to take a decision on which frequency bands are occupied and which are free. Cheating and fooling the fusion center will either deny some legitimate users from using a free band or al- low users to use a band that is already occupied. Similar problems are found with distributed CRN at the time of spectrum sensing decision. Thus, it is being considered that SSDF attack could be more harmful in a distributed CRN because the false information can propagate quickly with no means to control them. While in the centerlized CRNs, the fusion center can control and lessen the effect of false information by comparing the data received from all CRs.

3.6 Control Channel Saturation DoS Attack (CCSD)

This attack leaves the CRN with near-zero throughputs. In a multi-hop CRN, CRs communicate with each other performing a channel negotiation process. MAC control frames are exchanged to reserve channel during the negotiation phase. The common control channel has limited capacity for supporting concurrent data channels. When many CRs communicate at the same time, the channel becomes a bottleneck. The attackers take advantage of this situation and generate forged MAC control frames for saturating the channel, thus decreasing the network performance.

3.7 Sinkhole Attack

The two most relevant attacks at the Network layer are Sinkhole and Hello flood attack. In a Sinkhole Attack, an attacker advertises itself as having the best route to a specific destination. The neighbouring node uses it to forward their packets [15]. Then it can modify or drop the packets that pass through it. Another attack can be performed by an attacker known as selective forwarding, where an attacker can modify or discard packets from any node in the network. The Sinkhole attack is very effective in infrastructure and mesh architecture as all traffic goes through a base station.

3.8 Hello Flood Attack

In Hello-flood attack, the attacker sends broadcast message to all the nodes in a network with enough power to convince them it is their neighbour. For instance, an attacker sending a packet to a specific destination can encourage even far away nodes to use this route, convincing them he is their neighbour. As a result, the packet is lost and it will have no neighbour to forward its packet.

3.9 Lion Attack

Lion attack is defined as a jamming targeted to reduce the through- put of Transmission Control Protocol (TCP) by forcing frequency handoffs [16]. The lion attack, together with the PUE attack, can effectively reduce the throughput of TCP. The attacker can even perform a Denial of Service (DoS) by emulating a primary transmission at specific instant of time, if he knows some of the connection parameter.

4. SECURING COGNITIVE RADIO NETWORKS

In this section, some general countermeasures for attacks from each layer are discussed.

For alleviating jamming attacks in CRN, Spread Spectrum approach is being used. The available spectrum band is divided into a number of non-overlapping channels. From among this channel, only a small portion of the channel is used for transmission at a time. The attacker can even jam a channel, but with negligible jamming effect or the channel may not be used by the Cognitive Radio. Forward Error Correction (FEC) schemes can be used to construct the lost data due to jamming attack in CRN. Intrusion Detection System (IDS) also serve as valuable tool for detecting jamming attack.

For securing against PUE attack, the transmitting source needs to be identified, i.e., whether the transmitting source is a primary user or a malicious user. For this, cryptographic authentication mechanism can be applied for identifying the user. As the FCC regulation does not allow altering primary user system, researchers opted to find the exact location of a primary user. If the transmitting source matches the location of the primary user, the source is considered to be primary user. Otherwise, it is considered to be an attacker. To determine the location of the transmitting source, two approaches are considered, Distance Ratio Test (DRT) and Distance Difference Test (DDT), which is based on signal phase difference [11]. Objective Function attack modifies the parameter of the wireless media by jamming at a specific time and frequency in respect to the parameters defined in the policy. A simple solution to this attack is to define a threshold value for every updatable radio parameter [17]. This will prevent any communication when one or more parameters do not fulfil its predefined threshold. Intrusion Detection System (IDS) can also be used to mitigate Objective Function attack.

For securing against Spectrum Sensing Data Falsification (SSDF) attack, a data fusion technique called Weighted Sequential Ratio Test (WSRT) is used [18]. WSRT has two steps: Reputation maintenance and Sequential Probability Ratio Test (SPRT). In reputation maintenance step, every node has initial reputation value equal to zero. Upon each correct local spectrum report, the reputation value will be increased by 1. Another approach for identifying the Byzantine attack is by counting the mismatches between local decisions and global decisions at the fusion center over a time window [19].

CCSD attack can be controlled by adapting a trusted architecture. Here, any suspicious CR host will be monitored and evaluated by its neighbours. A neighbour can perform a sequential analysis based on the observation data and draw a final decision. The Sequential Probability Ratio Test (SPRT) can also be used [16].

For defending against Hello Flood attack, symmetric key algorithms are suggested [13]. A symmetric key is shared with a trusted base station. The base station serves as a Third Party, which facilitates the establishment of session keys between the parties in the network.

Sinkhole attack is very difficult to detect, as it exploits the routing protocol design and network architecture [13].

Lion attack aims to reduce the throughput of TCP. To mitigate this attack, the TCP protocol must be aware of what is happening in the physical layer and modify its behaviour according to the network condition, thus improving its performance [20]. To secure the control data from eavesdropping during transmission, a group key management (GKM) can be used to allow CRN members to encrypt, decrypt and authenticate themselves. Then, cross-layer IDS can be used to detect the attack. Another technique for mitigating lion attack is particle swarm optimization (PSO) [8]. Here, each cognitive radio acts as a particle which has idea about the best behaviour in a particular situation.

5. CONCLUSION

In this paper, a background on CRNs security and common threats/ attacks on protocol layers are analyzed and addressed with their countermeasures. CRNs are built on the basis of existing technologies and the approaches to provide effective security for these networks are not enough. Due to the particular characteristics of CRNs, new attacks arise and some of the previous ones increase in its complexity. Moreover, as CRN technology continues to grow and becomes more common, further expectation of security will be required. Similarly, new security proposals are needed to be effective against specific attacks, particularly in the physical layer to the upper layers (till transport layer). In addition, there is still needs for comprehensive mechanism to prevent or counter act the attacks at all protocol layers.

In order to address these challenges, each CR users in the CR network must have the following features:

—Determine the available spectrum.
—Select the best available channel.
—Coordinate the free channel access with other users.
—Vacate the channel when a licensed user is detected.[1]

Througho ut the paper, we have identified the threats to the different layers and within each we have sub classified the major topics. In particular, signal authentication and mechanisms to detect malicious insiders will overcome most of the specific attacks to CRN, but they are not trivial and require future in-depth research.

6. REFERENCES

[1] I.F. Alyildiz et al., A survey on Spectrum Management in Cognitive Radio Networks, IEEE Communication Magazine, pp. 40-48, April 2008.

[2] I.F. Akyildiz et al., NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey, Elsevier Jl. on Comp. Networks, vol-50, pp. 2127-2159, September 2006.

[3] Q. Zhao and M.Brian Sadler, A survey of dynamic spectrum Access, IEEE Signal Processing Magazine, vol.24, pp. 79- 89, May 2007.

[4] J. Mitola, Software Radios: Wireless Architecture for the 21st century, New York Wiley, 2000.

[5] Y. Zhang, G. Xa and X. Creng, Security threats in Cognitive Radio Networks, In10th IEEE International Conference on High Performance Computing and Processing(HPCC 2008) Dalian, China, Sept.2008, pp.1036-1041.

[6] R. Chen, Y. Thomas and J. Park, Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks, First IEEE workshop on Networking Technologies for Software defined Radio Network(SDR), Reston, VA, Sept. 2006, pp.1-11.

[7] R. Chen, Enhancing Attack Resilience in Cognitive Radio Network, Dissertion, Virginia Poly technique Institute and State University, Blocksburg, VA, 2008.

[8] T.Charles Clancy and N. Goergen, Security in Cognitive Radio Networks: Threats and Mitigation, 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Singapore, May 2008, pp.1-8.

[9] S. Haykin, Cognitive Radio: Brain-Empowered Wireless Communications, IEEE Jl. on Sel. Areas in Communication, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[10] J.L. Burbank, Security in Cognitive Radio Networks: The required Evolution in approaches to wireless Network Security, Johns Hopkins University, MD, 2012.

[11] K. Pelechrinis, M. Iliofotou and S.V. Krishnamurthy, Denial of Service Attacks in Wireless Networks: The Case of Jam- mer, In IEEE Communication Surveys and Tutorials, vol.13, pp.245-257, April 2011.

[12] A.C. Toleda and X. Wang, Robust detection of Selfish misbehavior in Wireless networks, IEEE Journal on Selected Areas in Communication, vol.25, pp.1124-1134, August 2007.

[13] C. Karlof and D. Wagner, Securing Routing in Wireless Sensor Networks: Attacks and Countermeasures, in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Berkeley, CA, May-2003, pp.113-127.

[14] N. Chetan Mathur and K.P. Subbalakshmi, Security Issues in Cognitive Radio Networks, Stevens Institute of Technology, NJ, USA, 2007.

[15] W. Wang, Denial of Service attacks in cognitive radio networks, in International Conference on Environmental Science and Information Application Technology(ESIAT), 2010, pp. 530-533.

[16] K. Bian and J. Park, MAC-layer Misbehaviors in Multi-hop Cognitive Radio Networks, in Proceedings of US- Korea Con- ference on Science, Technology and Enterpreneurship (UKC 2006), August 2006, pp.1-8.

[17] O. Leon, J. Hernandez-Serrano and M.Soriano, Securing Cognitive Radio Networks, International Journal of Communication Systems. vol.23, pp.116-130.

[18] R. Chen, J. Park, Y. Thomas and H. Jeffrey, Towards Secure Distributed Spectrum Sensing in Cognitive radio Networks, IEEE Communication Magazine, vol. 46, pp.50-55, 2008.

[19] A. Rawat, P. Anand, H. Chen and P. Varshney, Countering Byzantine Attack in Cognitive Radio Network, IEEE International Conference on Acoustic Speech and Signal Processing(ICASSP), Dallas, TX, Mar.2010, pp.3098-3101.

[20] J. Hernandez-Serrano, O. Leon and M. Soriano, Modeling the Lion Attack in Cognitive Radio Networks, Journal on Wireless Communications and Networking, pp.1-10, 2011. [21] T. Yucek and H. Arslam, A survey of Spectrum Sensing Algorithms for cognitive radio applications, IEEE Communi- cations surveys and tutorials, vol.11, No.1, pp.116-130, First Quarter 2009.

[22] K. Pramod Varshney, Distributed Detection and data fusion, Springer, verlag, New York, 1997.

[23] S. Marti, T. Giuli, K. Lai and M. Baker, Mitigating routing misbehaviour in mobile ad hoc networks, in 6th ACM Inter- national Conference on Mobile Computing and Networking, Aug 2000, pp.255- 265.

[24] S.Farahmand, G. Giannaris and X.Wang, Max-Min Strategies for power-limited games in the presence of correlated jam- ming, in 41st IEEE Conference Information Science and Sys- tems, 2007, pp.300-305.

[25] X. Wenyuan, W. Trappe, Y. Zhang and T. Wood, The Feasibil- ity of launching and Detecting Jamming Attacks in Wire- less Networks, in Proceedings of 6th ACM International Sympo- sium on Mobile Ad hoc Networking and Computing, Urbana, IL, May 2005, pp.46-57.

[26] L. Zhu and H. Zhou, Two types of attacks against Cognitive Radio Network MAC Protocols, in International Confer- ence on Computer Science and Software Engineering, vol.4, Wuhan,China,Decembe.2008, pp.1110-1113.

[27] O.Uretan, N.Serinken, Wireless Security through RF finger- printing, Canadian Journal of Winter Electrical and Computer Engineering, 2007, vol.32, pp.27-33.