Security Threats in Cognitive Radio Networks

Yuan Zhang, Gaochao Xu*, Xiaozhong Geng
Department of Computer Science & Technology
Jilin University, Changchun, China
zhangyuan2u@gmail.com

Abstract

The research for Dynamic Spectrum Access (DSA) and cognitive radio network (CRN) becomes one of the focuses in wireless network currently. However, as many other new techniques, in the initialization period, the security factors in CRN are out of focus. This paper describes the special characteristics of cognitive radio (CR) and CRN, and analysis the current and potential security threats that due to their characteristics. Besides some countermeasures and keys need to attention are mentioned. The goal of this paper is to assist CR designers and the CR application engineers to consider the security factors in the initial development period of CR techniques.

1. Introduction

With rapid increasing of mobile devices and their requirements for the spectrum, the limit available spectrum becomes a constrained resource. However, according to Federal Communications Commission (FCC) Spectrum Policy Task Force [1][2]: at any given time and location, much of the prized spectrum lies idle. Therefore, the current static spectrum assignment policy needs to be improved to meet the requirements. As a result, Dynamic Spectrum Access (DSA) is proposed to solve these spectrum inefficiency problems. Recently, many researchers focus their works on DSA and cognitive radio (CR) searching for efficient solutions to the problems. For example, the Defense Advanced Research Projects Agency (DARPA) Next Generation (XG) project [3][4] in the United States and the End-to-End Reconfigurability (E2R) program in Europe are working towards devising techniques for realizing different aspects of cognitive radio devices [9]. In the view of FCC, there is no other advance "holds greater potential for literally transforming the use of spectrum in the years to come than the development of software-defined radio and cognitive radios or 'smart' radios" [5].

According to FFC, CR can be formally defined as follows [6][7]:

A "Cognitive Radio" is a radio that can change its transmitter parameters based on interaction with the environment in which it operates.

CR technique is the key technique of realizing DSA policy. However, as many other new techniques, in the initialization period, the security factors in CR are out of focus. Compared with traditional radio, CR are more flexible and exposed to the wireless network, as a result, there are more security threats than in the traditional radio environment. There is no comprehensive analysis for security threats caused specially by CR technique and special characteristics of CR. T. Clancy et al. in paper [8] considered security threats in CR from the intelligent behavior aspect. Paper [9] provided us the potential Denial-of-Service vulnerabilities and protection countermeasures in CR and CRN. None of them considered the security threats caused by CR characteristics from a whole comprehensive aspect.

This paper describes the special characteristics of CR and CRN, and analysis the current and potential security threats that due to their characteristics in detail. The goal of this paper is to assist CR designers and the CR application engineers to consider the security factors in the initial development period of CR techniques. In Section 2, we describe the characteristics of cognitive radio and cognitive radio network (CRN). We summarize two main characteristics of CR, which are the Dynamic Spectrum Access (DSA) characteristic and the Artificial Intelligence (AI) characteristic. And then, we describe three aspects of current classifications for CRN. In Section 3, the security threats due to each characteristic are discussed in detail, besides some

[*] Corresponding author: Gaochao Xu, Phn: 86-431-85159421, email: xugc@jlu.edu.cn

978-0-7695-3352-0/08 $25.00 © 2008 IEEE
DOI 10.1109/HPCC.2008.21

countermeasures and keys need to attention are mentioned. Finally, we conclude the paper in Section 4.

2. Characteristics of CR/CRN

2.1. Characteristics of cognitive radio

The terms software-defined radio and cognitive radio were promoted by Mitola in 1991 and 1998, respectively. Software-defined radio(SDR), sometimes shortened to software radio, is generally a multiband radio that supports multiple air interfaces and protocols, and is reconfigurable through software run on DSP or general-purpose microprocessors [1][10]. CR, built on a software radio platform, is a context-aware intelligent radio potentially capable of autonomous reconfiguration by learning from and adapting to the communication environment [11]. And cognitive radio represents a much broader paradigm where many aspects of communication systems can be improved via cognition [1]. Compared with traditional radio, CR has its special characteristics, such as artificial intelligence functionality and dynamic spectrum access application, which will be described as follows. Figure 1 show the characteristics of CR.

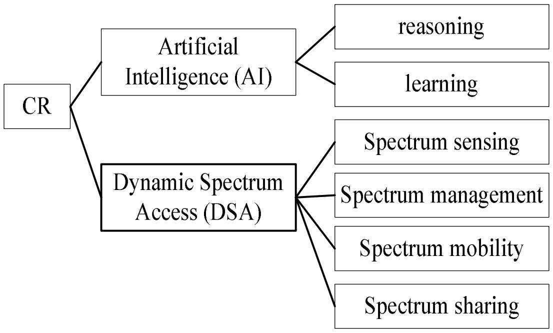

Figure 1. **Characteristics of CR**

2.1.1. Artificial intelligence cognitive radio. Cognitive radio offers the capabilities of learning from and adapting to their environment through its artificial intelligence (AI) characteristics including reasoning and learning.

In paper [12], Dietterich describes a standard agent model consisting of four primary components: observations, actions, an inference engine, and a knowledge base. In this agent model, reasoning and learning are a result of the combined operation of the inference engine and the knowledge base. Many researches are directing into learning and reasoning algorithms currently, assisting CRs to performance optimally in various situations.

A CR requires policies for reasoning to deal with different environments or react to different conditions. In another word, policies are the basis of reasoning. A reasoning engine is a set of logical inference rules [8]. It provides policies including a set of actions, under what conditions the actions should be execute, and how those actions affect the state of knowledge base. However, the shortage of reasoning engine is that it cannot adapt to new situations, and it needs preprogrammed policies, while the learning engine can make up this shortage.

A CR with learning functionalities can learn the experience from past statistics and present situation in order to predict future environment and select optimal operations. Learning is the process that the inference engine evaluates relationships, such as between past actions and current observations or between different concurrent observations, and converts this to knowledge to be stored in the knowledge base [8]. Learning engine can adapt to new situations and it start with no preprogrammed policies.

These AI features provide the advanced and flexible functionalities to CR, however, with the flexibility and the advanced performance, the security threats has also been exposed to the attackers, and it will be mentioned in section 3.1.

2.1.2. Dynamic spectrum access characteristics. Current regulation to spectrum is a kind of fixed (or static) spectrum assignment policy. The spectrum is regulated by governmental agencies and is assigned to license users on a long term basis for large geographical regions [6]. The spectrum is a constrained resource. With dramatic increase of wireless devices and communication demands, radio spectrum is running out of usable. However, according to Federal Communications Commission (FCC) [11], temporal and geographical variations in the utilization of the assigned spectrum range from 15% to 85%. Thus, increasing the efficiency of spectrum utilization is a way to deal with the problem. The FFC is considering on using DSA to opening up the licensed bands to unlicensed users on the basis of non-interference. DSA is an important application of CR, which provides the capability to use or share the spectrum in an opportunistic manner. Specifically, in order to realize DSA, CR provides functions as follows [6]:

- Spectrum sensing: detecting spectrum holes and sharing the spectrum without interfering with other users.
- Spectrum management: selecting the best available channels.
- Spectrum mobility: maintaining seamless communication during the transition to better spectrum.
- Spectrum sharing: coexisting with other users in one channel.

The implementation of these functionalities exposes severe security threats. We will propose the threats specifically in Section 3.

2.2. Characteristics of cognitive radio network

A cognitive radio network (CRN) is a network composed of CR nodes that, through learning and reasoning, dynamically adapt to varying network conditions in order to optimize end-to-end performance [6]. Mitola first makes brief mention of how his CRs could interact within the system-level scope of a cognitive network [14]. Spectrum sharing is right for solve the problems when the CR nodes interact with each other and share the constraint resources such as spectrum. There are three types of classification (as shown in Figure 2) about existing solutions for the CRN or spectrum sharing as follows [6].

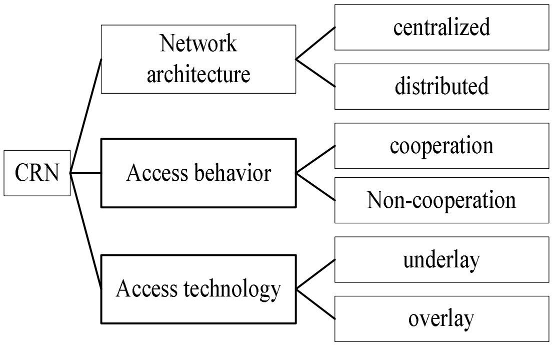

Figure 2. **Classifications of CRN based network architecture, access behavior, and access technology**

The first classification is based on the network architecture, which can be described as centralized network architecture and distributed network architecture. In the centralized network architecture, a centralized entity controls the spectrum allocation and access procedures [15], and each sub-centralized entity is proposed to forward its' measurement and information to the centralized entity. While in the distributed network architecture, each node is responsible for the spectrum allocation and access is based on local policies.

Second, based on the access behavior, there are cooperation and non-cooperation way. Cooperation solutions consider the effect of the node's communication on other nodes [16]. All the centralized solutions can be regarded as cooperative, and there are also distributed cooperative solutions. In the contrary, non-cooperative solutions consider only the node at hand [17].

Finally, considering the access technology, spectrum sharing can be classified into spectrum overlay and spectrum underlay [1]. A CR node using spectrum overlay approach accesses the spectrum which has not been used by licensed users. So, interference to primary users is minimized. Spectrum underlay exploits the spread spectrum techniques developed for cellular networks [18]. A CR using spectrum underlay approach operate below the noise floor of primary users, in another word, its transmit power at a certain portion of the spectrum is regard as noise by the primary user.

These solutions in CRN have their own characteristics and security threats, and we will describe the threats in section 3.3.

3. Security threats in CR/CRN

3.1. Artificial intelligence behavior threats

3.1.1. Policy threats. In order to communicate more effectively in an intelligence way, a CR needs policies for reasoning in different environment or from different conditions. Policy threats come from two aspects: lack of policy and failure when using policy.

If there is a lack of policy, a CR cannot make appropriate operations according policy in some certain conditions which are regulated by the lacked policy. Even, if a CR cannot receive any policy, it will not communicate. Policies are introduced at time of device manufacture, and the policies can be updated and extended during using. A CR can remote policy database for policies, and transfer policies from other CR. A CR also can receive announced local policies from radio beacon. In addition, policies can be distributed in the form of certifications with a period of validity. [8] The ways for a CR to receive policies are so variety. Thus, it is difficult for a CR to prevent from receiving any policies. However, reduce the chance of receiving policies, or decline required policies could affect the communication quality. For example, an attacker can decline the effective of communication by blocking accesses of policies. Or, an attacker can jam the radio beacon which announced policies.

Failure when using policy can also cause security problems. There are three types of threats when using policies: modification to policies, using false policies, and false input caused threat. First, policies may be modified by attackers. An attacker can get control of a CR, or get the administration of policy database to modify the policies inside. Second, using false policies also leads to security threats. An attacker can try to inject false policies into the CR policy database. If a CR operates according to the false policy, it may cause interference. Attackers can inject or modify policies when the CR is updating through radio beacons, from CRs transferring policies, and policy database. It is vulnerable these times. In addition, if an attacker spoof or mask sensor information, which is the input of policies, it will cause sub-optimal or false selection for communication. As mentioned in [8], by understanding how a radio's statistics are calculated, an attacker can manipulate them. Since these statistics operate on raw RF energy, there is no cryptographic means of securing them, as is frequently done to prevent typical communications threats. Through manipulating to the statistics, an attacker can provide a false sensor information, and leads to sub-optimal performance or false of communication.

Therefore, robust the policy management mechanism is an important task to CR's security.

3.1.2. Learning threats. Some CRs are designed with the capability of learning. These CRs can learn from the past experiences or current situations to predict future environment and select optimal operations, and they are vulnerable because of the learning capability. Attackers can modify past statistics or spoof current conditions to impact the CR predicting accurately. Based on the inaccurate prediction, the CR will operate sub-optimal or lead to a failure in communication. These attacks can have long-term effects on CRs, and are difficult to find out.

For example, both of [1] and [20] proposed a learning method through Marcov chain to predict the whether the channel is idle. They considered that a spectrum is composed of N channels. These N channels are allocated to a network of primary users. The traffic statistics of the primary system are such that the occupancy of these N channels follows a Marcov process with 2N states, where the state is defined as the availability (idle or busy) of each channel. If the input of the Marcov learning process is modified by an attacker, the result may be different, and secondary users may wait for idle channel when the channel in fact is idle; meanwhile, secondary users may consider the channel is idle when in fact it's busy, and may lead to interference to primary users.

3.1.3. Parameters threats. In this section, we discuss on the threats of altering parameters. A CR control a large number of radio parameters. Both in policies and learning process, CR use parameters to control operations and estimate its performance. The functionalities of these parameters are variety. For example, some of these parameters are used to weigh and estimate the performance of CR; some of them are the conditions or the switching bases of policies. Altering these parameters can cause sub-optimal or wrong operations for a CR.

Paper [8] shows us an example about the parameter threats. The paper proposed that a radio might have three goals: high-power, high-rate, and secure communication. Depending on the application, each of the three goals has a different weight. Accordingly, they use an objective function (as Formula. 1) to express the performance of a CR, and adjust operations according to the objective function result.

$$f = \omega_1 P + \omega_2 R + \omega_3 S \qquad (1)$$

Here, ω_i are the weights and P, R, and S represent the three goals of power, rate, and security. If an attacker wishes to force a radio to use some security level s_1 rather than the more secure version s_2, where $s_1 < s_2$. When the CR try to use s_2, the attacker can jam the channel, artificially decreasing R form r_2 to r_1 with $r_1 < r_2$. The consequence of such an attack is that whenever a higher security level is attempted, the CR's objective function f decreases, and that higher security level is never used.

In addition, an attacker can also manipulate a CR to behave malicious, and teach the CR to alter the parameters to impact the CR to operate sub-optimal.

3.2. Dynamic spectrum access threats

3.2.1. Spectrum sensing threats. In DSA environment, primary users have the license to use the certain frequency band whenever they want. When the primary uses don't use their spectrum, the spectrum is idle, and secondary users could use the available spectrum opportunistically. Such secondary users need sensing algorithms to detect spectrum holes for communication, and CRs have the capability of detecting the spectrum holes. In addition, a CR has to vacate the channel when the primary user uses it.

One of the threats comes from attackers who want to spoof or mask primary user. The attackers provide a feint of the channel will be used by a primary user, so the secondary within range will believe a primary user is active, and vacate the channel. This kind of attack is called Primary User Emulation (PUE), which was introduced in [19], and [21]. As a result, this attack provides the attacker accessing to the spectrum. However, this attack effects transient, because when the attackers vacate the channel, or stop to spoof a primary user, the secondary user could detect the idle channel and use it.

There is also another kind of threat, which prevents CR from receiving sensor information or provides the CR false information. The CR cannot receive information about spectrum holes or active primary user, or it receive the false information, so it cannot do right communication decisions. In some CR, sensor information was transmitted through a common control channel. It is easy for the attackers to jam or control the unique channel. Thus, designers of CR who want a common control channel should take consideration of this problem. Also, paper [8] showed us the leveraged jamming example: in some CR, the sensor and the radio share the same front end. Even when they are separate, the sensor sensitivity can be impaired by a nearby transmitter. So sensing and transmission cannot occur at the same time. The radio can only operate for some fraction of the time, f, with the remaining time being used for sensing. In this case, any jamming becomes leveraged by a factor 1/f， For instance, because of sensing, the radio can only operate for f=70% of the time. Then jamming 35% of the time will reduce the time for communication by 35%/f=50%. Jamming the sensing time can impact the communication time seriously. The key to avoid leveraged jamming is to make the fraction of time devoted to transmission, f, as close to one as possible. Thus, we need good sensing strategies.

3.2.2. Spectrum management threats. Through spectrum sensing, CR detected the idle spectrum bands for communication. These spectrum bands show different characteristics according to time-varying radio environment, operating frequency, bandwidth, and so on. Spectrum management should have the capacity of selecting the most appropriate bands from these bands for users. It should decide on the best spectrum band to meet the QoS requirement over all available spectrum bands [6]. In [6], the functions of spectrum management are classified as spectrum analysis and spectrum decision. Spectrum analysis enables the characterization of different spectrum bands; while spectrum decision select the appropriate spectrum band for the current transmission considering the QoS requirements and the spectrum characteristics.

The threats here come from the possibility of false or fake spectrum characteristic parameters. The false or fake parameters impact the results of spectrum analysis, and then impact the results of spectrum decision. So a CR may select the wrong band or the sub-optimal band, and the performance of communication may be impaired. For example, in spectrum analysis, spectrum characterization is focused on the capacity estimation recently. Paper [6] proposed a spectrum capacity estimation method considering the bandwidth and the permissible transmission power. Accordingly, the spectrum capacity, C, can be estimated as Formula 2:

$$C = B\log(1+\frac{S}{N+I}) \qquad (2)$$

Here B is the bandwidth, S is the received signal power from user, N is the receiver noise power, and I is the interference power received at the receiver due to the primary transmitter. If attackers change one of the parameters in Formula 2, C will vary. The result of spectrum analysis will less accurate or even wrong, and the spectrum decision will deviate from the optimal result.

3.2.3. Spectrum mobility threats. The function of spectrum mobility is to make sure seamless connection when a CR vacates a channel and moves to a better channel. In a CR, the available spectrum bands depend on the factors such as time and place. One should vacate the current band if the band is not available for the reasons like: a primary user is active, or the one moves from one place to another .etc. In order to maintain the communication smoothly as soon as possible, the CR needs to select a new appropriate spectrum band, and moves to the band immediately. The process from a CR vacating the current spectrum band to the CR moving to a new available spectrum band is called spectrum handoff [6].

During spectrum handoff, the security threats are seriously. Because a failed handoff may need a long time to resume the communication. An attacker can induce a failed spectrum handoff through ways of: compelling the CR vacating the current band by masking primary user; jamming to slower the process of selecting for a new available band or to cause a communication failure .exc.

For example, some CRs use common control channel. Attacker can gain control of the common control channel, to change the characteristic parameters of available band, or to interfere with primary users. And then prevent smoothly transmission functionality of spectrum mobility. Thus, robust and simple algorithms for seamless connection of spectrum mobility are needed.

3.3. Threats in cognitive radio network

In this section, we discuss about the security threats specially aiming at CRN. We have detailedly described the characteristics of CRN through three types of classifications in section 2.2, and here we will point out the security threats accordingly.

Comparing the centralized and distributed architectures and the cooperation and non-cooperation connecting approaches, obviously, the centralized architecture and cooperation approach are more vulnerable to attacks. The most severe attack to these two solutions is Denial of service (DoS) attack. In centralized architecture network, if an attacker can manipulate the central entity or prevent the central entity from communication, the whole network is under control of the attacker. In cooperation CRN, if an attacker controls one of the nodes, he can transmit fake information to other nodes, or terminate transmitting information to others. This kind of attack is valid the most in ad hoc network. Especially, common control channel is a target for DoS attacks since successful jamming of this one channel may prevent or hinder all communication [6][16]. In distributed architecture or non-cooperation network, an attack against one CR will not affect others, because other devices operate independently.

In addition, in spectrum overlay environment, a node accesses the network using a portion of the spectrum that has not been used by licensed users [6]. Thus, an attacker can use the method mentioned in section 3.2.1, spoofing or masking primary users to prevent the normal node from using the spectrum, and the worst-case is that the normal node cannot sense any available spectrum, and it would consider there is no spectrum to be used. Spectrum underlay environment requires sophisticated spread spectrum techniques and increased bandwidth [6]. Thus, it is comparatively easy for an attacker manipulating a CR node, and jamming to interference primary users.

4. Conclusion

CR techniques are still in the early age of its development. It is significant to consider security factors into the design and application techniques for CR. In this paper, the special characteristics of CR and CRN are described as the AI characteristic, DSA characteristic, and three aspects of classifications for CRN. Furthermore, the security threats due to these special characteristics are mentioned in detail, besides some countermeasures and keys need to attention are mentioned. In order to follow the flexible and cognition characteristics of CR, new and robust architectures and techniques are required. In addition, corresponding countermeasures against these security threats are also required.

5. References

[1] Qing Zhao, Brian M. Sadler, “A survey of dynamic spectrum access”, IEEE SIGNAL PROCESS MAGZINE, MAY 2007, pp. 79-89.

[2] FCC Spectrum Policy Task Force, “Report of the spectrum efficiency working group,” Nov. 2002. [Online]. Available: http://www.fcc.gov/sptf/reports.html.

[3] DARPA XG Working Group, “The XG vision”, Request for Comments, version 1.0, Prepared by BBN Technologies, Cambridge, Mass., USA. July, 2003.

[4] DARPA XG Working Group, “The XG architecturl framework”, Request for Comments, version 1.0, Prepared by BBN Technologies, Cambridge, Mass., USA. July, 2003.

[5] FCC ET Docket No. 03-108, “Faciliating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies”, FCC Report and Order adopted on March 10, 2005. [Online]. Available: http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pfd&id_document=6517509341.

[6] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, Shantidev Mohanty, “NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey”, Computer Networks, p2127-2159, (50)2006.

[7] FCC, ET Docket No 03-222 Notice of proposed rule making and order, December 2003.

[8] T. Clancy, N. Goergen, “Security in Cognitive Radio Networks: Threats and Mitigation”, Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), May 2008.

[9] Timothy X Brown, Amita Sethi, “Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: A Multi-dimensional Analysis and Assessment”, [Online].Available: http://www.its.bldrdoc.gov/isart/art07/slides07/bro_t/bro_t_slides-07.pdf

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

[11] J. Mitola, “Cognitive Radio: An integrated agent architecture for software defined radio”. PhD thesis, Royal Institute of Technology (KTH), 2000.

[12] T. Dietterich, P. Langley, “Machine learning for cognitive networks: Technologyassessment and research challenges”, tech. rep., Oregon State University, 2003.3

[13] FCC, ET Docket No 03-222 Notice of proposed rule making and order, December 2003.

[14] Captain Ryan W. Thomas, “Cognitive networks”, PHD thesis, Computer Engineering og Blacksburg, Virginia, 2007.

[15] Brik, E. Rozner, S. Banarjee, P. Bahl, DSAP: a protocol for coordinated spectrum access, in: Proc. IEEE DySPAN 2005, November 2005, pp. 611–614.

[16] J. Zhao, H. Zheng, G.-H. Yang, “Distributed coordination in dynamic spectrum allocation networks”, in: Proc. IEEE DySPAN 2005, November 2005, pp. 259–268.

[17] Q. Zhao, L. Tong, A. Swami, “Decentralized cognitive MAC for dynamic spectrum access”, in: Proc. IEEE DySPAN 2005, November 2005, pp. 224–232.

[18] J. Huang, R.A. Berry, M.L. Honig, “Spectrum sharing with distributed interference compensation”, in: Proc. IEEE DySPAN 2005, November 2005, pp. 88–93.

[19] R. Chen and J. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks,” IEEE Workshop on Networking Technologies for SDR 2006.

[20] Yiping Xing, R. Chandramouli, Stefan Mangold, Sai Shankar N, “Dynamic spectrum access in open spectrum wireless networks”, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 3, March, 2006.

[21] R. Chen, J. Park, and J. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” IEEE Journal on Selected Areas in Communications, 2007.