Attack and Defense Countermeasures of cognitive radio

JinFeng Li*, Bingcheng Sun, Hongfeng Cui
Academy of Information & Communication National University of Defense Technology, Wuhan, 430010, China

*Corresponding author e-mail: LiJinFeng@nudt.edu.cn

Abstract. With the development of cognitive radio theory and technology, its application in various fields will be more and more extensive. She's trying to bring AI technology to the Internet. In this paper, the attack and defense of cognitive radio will become more and more intense. The mobile communication process of cognitive radio is summarized, and the attack and Defense Countermeasures of cognitive radio are analyzed.

Key words: cognitive radio, attack and Defense Countermeasures.

1. Introduction
Cognitive radio finds the appropriate spectrum in the complex and changeable electromagnetic environment through the spectrum sensing of each unit, and establishes adaptive communication through cognitive reasoning, network standard and rule learning and real-time adjustment of transmission parameters. This paper focuses on the application trend of cognitive radio in various fields, summarizes its communication process, analyzes the weaknesses of the process, and deeply studies the attack and defense problems of cognitive radio, so as to be invincible in the future electronic technology competition.

2. Mobile communication process of cognitive radio
Cognitive radio is also called intelligent radio, which realizes the rational use of electromagnetic spectrum resources through automatic sensing of spectrum environment, intelligent learning and dynamic adjustment, so as to achieve the purpose of effective utilization of spectrum resources. The communication process of cognitive radio mainly includes spectrum sensing, analysis and decision-making, and spectrum access, as shown in Figure 1
2.1. **Spectrum sensing**
By analyzing the signals received in a specific frequency band, the spectrum resources that can be used in time domain, frequency domain and spatial domain are found out. At the same time, the presence of authorized users is detected in real time in the process of using spectrum to avoid interference to authorized users.

2.2. **Analysis and decision making**
Based on spectrum sensing, the main characteristic parameters of idle spectrum are analyzed. According to the current situation, combined with the quality of service requirements of users, real-time processing decision scheme is constructed to select the appropriate spectrum for the current users, and determine the data rate of information transmission, signal modulation mode, acceptable bit error rate, transmission delay limit and the best transmission power level and transmission time, so as to ensure the frequency compatibility of various communication equipment. At the same time, the priority can be determined according to the different types of requests, and the spectrum can be allocated to the high-level requests first.

2.3. **Spectrum access**
All kinds of communication equipment adjust the transmission parameters according to the decision-making scheme to ensure good electromagnetic compatibility between the equipment. At the same time, it can also determine the equipment and frequency according to the requirements, so as to achieve the highest efficiency of frequency use and frequency on-demand access. When the authorized user is detected to access and use the frequency band, or the quality of communication channel is seriously degraded at this time, the frequency band is vacated and its own configuration is adjusted again to seek access to another "idle spectrum" to continue communication, that is, spectrum moving.

3. **Countermeasures for cognitive radio**
Although cognitive radio has a strong ability to adapt to the environment and improves the spectrum utilization, it also introduces new security vulnerabilities, which makes it possible to implement targeted radio.
3.1. Seizing spectrum resources and improving interception jamming effect

The other party can adopt the possessive trap technology, that is, by using the multi carrier forming technology to occupy the limited spectrum, the "spectrum pool" of the cognitive wireless network signal will shrink, greatly reducing the spectrum space that the cognitive communication equipment can use, while the other party's detection equipment can control other limited idle spectrum that the cognitive signal may use and implement interference; in addition, the other party can also adopt the possessive trap technology Driven trap technology, that is, through multi carrier forming technology or interference signal scanning technology, dynamically changes the "spectrum pool" of cognitive wireless network signal, and "drives" cognitive wireless network signal to the frequency band of its device's interception and interference control, so as to improve the interference detection effect.

3.2. Release false signal and destroy spectrum sensing

The other side takes the cognitive user as the entrance, releases the false signal, improves the false alarm probability of the sensing system, and reduces the access opportunity of the cognitive wireless communication system. One is to imitate the signal mode of authorized users to send information, so that other cognitive users mistakenly think that authorized users occupy the frequency band and can not use the spectrum resources. Second, by eavesdropping on the data transmitted by the public control channel, we can obtain the frequency band used by the cognitive network, and simulate the transmission signal of authorized users in this frequency band, forcing cognitive users to change the frequency band, and interrupt the communication of cognitive users through repeated pairing. Third, it can launch "Mask" interference, so that cognitive users can not receive the existing information of authorized users, thus inducing cognitive users to send signals, resulting in conflicts with authorized users.

3.3. Tampering with spectrum sensing data affects analysis and decision-making

The other party reports the wrong sensing results to the data fusion center as a normal user, which induces the fusion center to get the wrong spectrum analysis results and reduces the chances of cognitive users using the authorized frequency band. The other party can always send a higher sensing state, which makes the cognitive user mistakenly think that the current channel is occupied; it can also always send a lower sensing state, which makes the cognitive user mistakenly think that the current channel is not used; even in order to enhance the deception, it can send high and low sensing states with random probability. When conditions permit, the other party can cooperate with each other, exchange information, reach a consensus, and report the wrong data to the fusion center. This kind of cooperation is more destructive to the behavior, and has strong maneuverability to the global decision of the fusion center.

3.4. Cross layer joint pair

In order to ensure the effectiveness of network control and management, cognitive radio uses common control channel to transmit network control and management information. The information transmitted in the common control channel is very important for spectrum sensing, analysis decision and spectrum access. The other party can make use of the information transmitted by the public channel which is intercepted and stolen to carry out targeted attack. It can even suppress or block the common channel, which makes the cognitive radio network unable to communicate normally. In addition, if the control frame lacks authentication, the other side is easy to interrupt communication or unfairly allocate network resources by forging MAC frame or inserting forged information into MAC control frame.

4. Cognitive radio defense strategy

4.1. Establish a trusted network to weaken the impact on spectrum sensing

People have "new spears", I can't use "old shields". In order to weaken the influence of the other party on the cognitive radio network, we must implement fine-grained control on the behavior and the state.
of the cognitive radio network, strengthen the network with fixed points, overcome the invasion of the enemy, and give the other party no opportunity from the source. Therefore, we need to build a trusted network access framework based on Trusted Computing and trusted access technology to verify the legitimacy and credibility of access users. If the user behaves badly, he will get a lower trust value, so that his spectrum sensing results will be assigned a lower weighting factor in the process of data fusion, or even refuse to use the data he sends, so as to reduce the impact of the other party on spectrum sensing. The frame structure is shown in Figure 2

![Figure 2](image)

**Figure 2. Trusted network access framework**

The access framework consists of access request point, network access control point and trusted access server. From top to bottom, there are evaluation layer, authentication layer and access layer. The evaluation layer realizes the quantitative verification of trusted state; the authentication layer realizes the two-way authentication of identity and trusted state information; the access layer realizes the bottom access. When the access request point enters the network, the initial state of the connected port is controlled. Only the specific initialization packet can be processed by the network access control point, and other packets are discarded. According to the authentication result and authorization policy of the server, the network access control point allows or denies the access request point to enter the network.

4.2. Mining signal features to improve the timeliness of recognition and judgment

One is based on power feature recognition. When the deployment range of cognitive radio communication equipment is certain, by predicting the deployment range of the other party, starting from the probability density function of the received power of the cognitive user, and using the variance of the received signal power of the cognitive user, the normal user and the other party are identified and judged, so as to analyze and judge whether the current segment is occupied. The second is based on channel feature recognition. The other party can simulate the transmission power, modulation method and cyclostationary characteristics of the authorized user, but it is difficult to simulate the characteristics of the communication channel. The transmission of signals from the other party and normal users usually needs to go through different channels, and the channel parameters of different channels are not the same. The existence of the pair can be detected by detecting the unique parameters of the channel. The third is based on voice feature recognition. In voice communication, because the voice waveform of the other party is different from that of the authorized user, the voice sensor can be used to detect the correlation of the voice information, so as to detect the authenticity of the user. The fourth is based on process feature recognition. In view of the fact that legitimate users need to maximize the use of channel resources, and the other party’s purpose is to maximize the number of channels, the interaction process between legitimate users and the other party can be abstractly modeled as a game process. Through the differential game process, the Nash equilibrium of the pair can be obtained, so as to find the pair behavior and maximize the channel utilization of the network in the presence of the other party.
4.3. **Strengthen the depth of data fusion and increase the accuracy of analysis and decision-making**

One is to realize cooperative spectrum sensing. The performance of single point sensing is limited, so it needs cooperation between different cognitive users in the same frequency band to improve the reliability of detection. By processing the sensing results of multiple cognitive users, cooperative detection can judge the spectrum usage more accurately. In this way, the influence of the tampering behavior of a single malicious node on the whole analysis decision is greatly reduced. Second, the fusion center participates in spectrum sensing. That is, the difference probability between the fusion center perception results and the reliable user reported data is taken as the benchmark, and the difference probability between the fusion center perception results and the detected user reported data is taken as the detection quantity. Experiments and data show that by setting a reasonable threshold, pairing behavior can be detected effectively. Even in the scene of large-scale malicious pairing, correct analysis and decision-making can still be made, and a good decision-making scheme can be obtained. Third, the realization of external cooperation awareness. That is to say, the fusion of the special sensing devices of other networks can improve the accuracy of analysis and judgment, and broadcast the sensing results to all legitimate users in the sensing network. In this way, all legitimate users in the sensing network will not need to participate in spectrum sensing frequently, nor need to report or interact with sensing information frequently, only need to communicate normally, so as to greatly save network bandwidth resources, shorten communication cycle, improve communication efficiency, and be able to identify each other from the behavior characteristics.

**References**

[1] Zhou Xianwei, cognitive radio [M], National Defense Industry Press, 2008.
[2] Feng Jingyu, review of cognitive radio security [J], Journal of Xian University of Posts and telecommunications, 2012.
[3] Liu Yujun, cognitive radio network [J], electronic industry press, 2018.
[4] Guo Caili, cognitive radio network technology and application [J], electronic industry press, 2010.
[5] He Xukai, overview of security threats and response technologies of cognitive radio networks [J], computer and information technology, 2016, (10).