International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.193-204
http://dx.doi.org/10.14257/ijsia.2016.10.6.19

The Research of Network Security Based on Cognitive Radio

Ruihui Mu [1, a,*] and Junwei Li [2]

[1] *College of Computer and Information Engineering, Xinxiang University, Xinxiang, 453000, China*
[2] *Office of Academic Affairs, Xinxiang University, Xinxiang, 453000, China*
[a] *MURUIHUI@126.com*
** Corresponding Author: Ruihui Mu*

Abstract

Firstly, we are given the security problems faced by a detailed analysis of the cognitive radio networks, and introduces the related basic cognitive radio network problems. Then, based on the difference between the cognitive radio network and the existing wireless network, which analyzes security and artificial intelligence, dynamic spectrum access and discussion. It concluded for the safety of cross-layer design.

Keywords*: Network Security; Cross-Layer; Radio Network; Spectrum*

1. Introduction

Spectrum is a scarce resource, one of the current spectrum management framework. With the rapid development of wireless communications technology, the emergence of an increasingly prominent on how to effectively use spectrum resources. In many countries, most of the radio spectrum allocated to the business units. In this already authorized and unauthorized distribution of the band, as well as use of the spectrum there is an imbalance of resources: on the one hand, the band spectrum authorization has occupied a large part, but many authorization is in idle state (empty spectrum). Study by the Federal Communications Commission (FCC) revealed that the average frequency spectrum authorized for 15 percent, and between 85% most of the time and area. On the other hand, open use of unauthorized small portion of the spectrum band footprint. But the user is huge and traffic congestion, resulting in radio frequency band has tended to be saturated. Static spectrum allocation principle is to enable the low utilization rate of frequency bands, the use of appropriate frequencies contradiction to other users of the main reasons. If it can use the idle spectrum resources is temporary, tensions lack of spectrum resources will be eased, and has been greatly improved. Cognitive Radio (CR), proposed to effectively solve this problem. Its main function is to make the future of radio equipment to identify an independent spectrum holes, and efficient use of spectrum.

2. Concepts and Cognitive Radio Features

The concept of cognitive radio stems from Joseph Mitola of its basic core idea in 1999, in the CR with a learning and environment surrounding communicate to the perception of space, limiting the ability of the available spectrum and reduce conflict occurred . Since the emergence of the concept of cognitive radio, various organizations and scholars from different angles presented many definitions of cognitive radio [1]. The most representative definitions have been submitted to the US Federal Communications Commission (FCC) and the famous professor Xi Meng. Any adaptive spectrum awareness raised by the US Federal Communications Commission should be called

* Corresponding Author

ISSN: 1738-9976 IJSIA

cognitive radio, which is defined as: CR is a wireless, can its transmitter parameters dynamically according to changing operating environment. It has a function of environmental awareness and self-modified transmission parameters. But from the perspective of signal processing point of view, Xi Meng that CR is an intelligent wireless communication system. It can sense the external environment and knowledge through artificial intelligence techniques. By real-time changes of some of the operating parameters, it can adapt to changes in the statistical properties of the wireless signal. Accordingly, recognized, highly reliable communication can be implemented anywhere, at any time and effective use of spectrum resources.

Cognitive radio from conventional radio it has the ability to cognitive intelligence, to achieve real-time detection of different environments. Through research and decision-making adaptive changes in parameter settings, you can make full use of spectrum resources effectively. The premise of CR is an open spectrum, that is, the network should be divided into primary user (authorized users) and secondary users (illegal users). In the open spectrum on the basis of secondary users can find free spectrum rights detecting spectrum holes through which the main users do not use, and take advantage of access to the band without compromising the user's communication [2]. This requires a secondary user real-time detection capability for spectral holes, has the following three characteristics [3]:

1) Must be able to identify -CR sensing unused spectrum;

2) Flexibility -CR must be able to change the frequency of the signal, the frequency band to unused;

3) No interference CR may not result in harmful interference to the primary user.

3. Cognitive Radio Network Security

A significant impact on the shortage of spectrum in consciousness, FCC believes that unlicensed spectrum should open portion unauthorized user in the main user [4] without any precondition impacts. This is a test spectrum hole important things. To address how to detect these free bands and use them, it has been proposed for dynamic spectrum access technology. Free zone by spectrum sensing algorithm to secondary users can under the premise of the primary user of communications, without any influence, make full use of spectrum resources. Cognitive radio networks as a wireless communications technology, it is not only traditional security issues, but also introduced a number of new security risks. For example, in the spectrum access many of the steps in the process, such as spectrum sensing, spectrum management, spectrum and spectrum sharing migration [5]. Each process exits security issues. Cognitive radio can learn and adapt to intelligent external environment, so a lot of research is working with various states of reasoning and optimization algorithm. However, with the value of information continues to reflect information security design gaining more and more attention. Security of communication has become an important part of the system design, especially involving military, commercial secrets, has been widely used in these areas of cognitive radio, we must pay more attention to safety. In addition to traditional wireless security issues, cognitive radio is also faced with its unique risks [6].

3.1. Traditional Wireless Network Security

Because of electromagnetic waves used in wireless communications for the media, physical separation method is difficult to achieve. Compared to wired communications, wireless communications have more insecurity, mainly in the following aspects:

3.1.1. Traditional Wireless Network Security: In the process of wireless communication, all communication and information transmitted over the radio channel.

According to the cable channel, it's easier, if only attacker captured using the appropriate equipment. In the commercial wireless communication system, the information transmitted may include the user's identity, billing information, key information, such as location and signaling information leaked information to the user's economy and reputation damage, including leaking users' privacy.

Wireless eavesdropping program is widely leave a wireless network, and the solution in this is to send an encrypted message. The importance of various information transmission encryption is applied with different intensities. The method can effectively protect information transmitted. But with the rapid development of computer hardware technology, the possibility of violence, break with a key encryption transmission with. Therefore, it needs to improve the strength of encryption algorithms, in order to take measures to prevent major risks.

3.1.2. Forgery Attack: In wireless communications, the terminal and the base station do not have the physical cabling. Identity information exchange between the terminal and the base station via a radio channel to achieve. The identity information related network control, network services and network access. Because of the radio channel, the attacker can eavesdrop on a radio channel to obtain identification information. When the attacker obtain a valid user's identity, the identity information of illegal access to the network that he can use, and even allow network services or are engaged in cyber-attacks.

In different wireless communication systems, the purpose of the false attack is different. Forged identity information by intercepting the legitimate user, an attacker can take advantage of communication services without having to pay network service fees. By using the base station equipment, an attacker could deceive the end user, the user's identity in order to get more information.

3.1.3. Information Tampering: Information tampering means that the attacker faucet to relevant information, and passes it to the original information, including deletions, modifications before they replace and modify. Information tampering usually occurs in store and forward network. Information between two wireless terminals can be forwarded by other wireless terminals or hubs, which are "transit station" there is a possibility of tampering information. Information tampering would seriously threaten the integrity and effectiveness of network traffic, resulting in unnecessary losses user.

3.1.4. Service Repudiation: Deny recognition service point communication service or communication processing after the user rejects the connection to send data. It consists of two parts:

1) Deny communication services. In the commercial networks, users use the network denied, and thus he refused to pay the associated network costs.

2) Repudiation of communication content. Users about his refusal to transmit the contents of the transmission. For example, e-commerce and electronic payment in, the user deny the transaction has taken place and they refused to pay.

3) Service repudiation may affect the credit of the network, it will cause unnecessary losses and operators. Present mainly in the authentication and asymmetric encryption algorithms, in order to avoid such security risks approach.

3.1.5. Replay Attack: Replay attack is an attacker taps into useful information in a time interval, and then he offered to the receiver once. Its aim is to use information in a timely and effective change to win, in order to obtain the trust of more useful information recipient. For example, after obtaining the user's password, the attacker control of the network, license and access to network resources.

3.1.6. Denial of Service and Information Interference: An electromagnetic wave is the carrier of wireless communication. With the rapid development of hardware technology, the attacker can stop by the transmitter power of communication. In the normal communication by making noise in the signal spectrum, communication may be disturbed. Resources which will lead to the wireless base station equipment is not enough, the user's access will be denied. Information interference, it will have serious social impact. For example, when the interference occurred in 2001, a communication satellite VSAT terminal case because the offender is set by a high-power satellite service interruption.

3.2. Cognitive Radio Network Security

3.2.1. Threat of Dynamic Spectrum Access: The current spectrum policy with a fixed distribution, that is, at a fixed frequency spectrum allocated to authorized users fixed area for a very long time by the government. Spectrum is a limited resource. With the requirements of the wireless devices and communications increasingly spectrum allocation has been almost exhausted. However, given the significant existing fixed allocation of spectrum, cognitive radio can skillfully use secondary spectrum so as to achieve full use of resources. This requires cognitive user can in the case of every moment of perception channels and try to signal to access without interruption to the main user's premise. This solution requires the use of advanced technology; otherwise it will make some interference, even harm to major users. Dynamic spectrum access is a spectrum sensing, spectrum management and spectrum migration, where each stage exit unsafe. With traditional wireless networks, cognitive radio has its own specific security issues: Spectrum abuse and selfish act, by imitating the primary user, the common control channel blocking evolved cognitive node into malicious nodes attack [7] the following The part will be analyzed in cognitive radio systems existing security problems from the dynamic aspects of spectrum sensing.

The Main Users Simulated Attack

Primary user emulation (PUE) attack security issues, the physical layer to face, this one has a great perception of the threat spectrum. CR attacker sends a signal through imitation primary user signal characteristics. The case of this attack can be achieved under the CR for a highly flexible and software-based air interface. In the dynamic spectrum access (DSA) in the environment, the master user can authorize band freedoms of all times. When the licensed spectrum becomes idle state, the main user releases the resources, so the subprime users try to access [8]. A necessary condition is that the user must be able to sense the presence of a secondary free band. Therefore, it needs spectrum sensing algorithms for real-time spectrum is detected by the sensing device. In this case, the attacker creates indeed cause errors as the main user of spectrum, leading state secondary spectrum users to make mistakes entirely similar signals. This will allow the channel in the system, and to attack those who have access to such channels. This attack is known as the primary user of mock attacks [9].

The study found PUE attack could cause serious interference spectrum sensing process significantly reduces the user's perception of the available legal channel resources. Screening and matching capabilities rotation detection spectrum sensing technology can achieve. These nodes detection technology able to identify the essential characteristics of the main users, so they can distinguish between the primary and secondary signals between users. However, this is not enough to fight PUE attack. For the purposes of attack, PUE attack devices can be divided into two categories: selfish attacks and malicious attacks. For selfish act, the attacker's goal is to maximize their own interests. When the attack detection zone, he will simulate the primary user signals to prevent signal other secondary users to access [10]. When the attackers reached their goal, they

will exit channel. Attack is short. Once the attacker out of the channel, users will access the channel again detected perceived freedom. Malicious behavior, the attacker legitimate efforts to restrain the secondary user detects and uses authorized band, resulting in a denial of service attack. The difference is that malicious attacks without using a free license for themselves, they just launched a comprehensive multi-band PUE attack. Whether selfish or malicious attack, it caused great inconvenience to the network. For PUE attack, which is the difference between how a key signal to identify the primary users and malicious cognitive user signals. The base station can be verified by a certificate authorized user, but it is difficult to control, once the certificate is missing. Therefore, it should provide a soft authenticate with less computational complexity quickly authenticate users. In addition, upon detection of malicious behavior, it will immediately allow a malicious user will be punished appropriate measures. This may reduce their credibility on the network, and even forced him to leave the network.

The Main User Interference

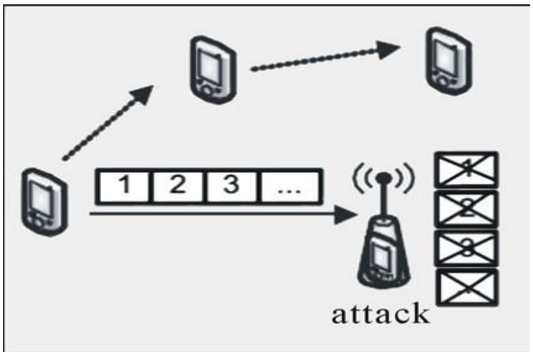
In DSA, which is the main user of high-frequency interference malicious users, which is a common form of attack. Because CR flexibility and adaptability, the introduction of secondary users will inevitably result in the user interference, or even a denial of service attack. Subprime users must use the spectrum in two ways: one is the use of authorized users whitish free "it demanded to know the exact model of the primary user activity Another is to allow users to take advantage of the secondary gray space at the same time the primary user. Obviously, the latter will be the primary user of a crucial impact in order to avoid the interference of users' cognitive needs not only accurate perception, but also need to know the main user of the message "appears. Therefore, an attacker can attack. And interference by preventing cognitive information received, this will cause the user interference. This will cause serious damage to the network performance. This may make the work of the main users of the noise, not even the band is available. It violates the purpose of the development of cognitive radio technology, it is to visit, without interfering with the normal use of the primary user. Therefore, it causes the switching frequency of the spectrum of cognitive users. Once the primary user signal found cognitive users should evacuate immediately by switching the band.

Spectrum Sensing Data Tampering Attacks

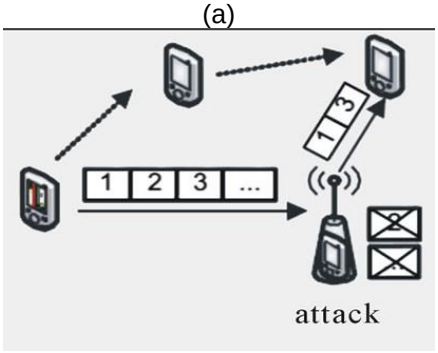
In a distributed spectrum sensing process, the attacker sends the wrong message spectrum sensing data collection center, which leads to bad decision making, data collection center, shown in Figure 1 [11] FIG. This is the most common perception of tampering with data. In order to improve cognitive efficiency, the literature [12, 13] proposed a cooperative spectrum sensing technology to effectively improve the efficiency of spectrum detection. But it gives people bring new problems, such as node deception and partnerships, create erroneous results. Whether or cooperative distribution network, spectrum sensing data, if there is a serious impact has been tampered with. Abnormal, S.Arkoulis divided into four sub-node The access point (AP) behavior: a misconduct AP, an AP selfish, cheating and malicious AP [14]. Malicious nodes can distort, deceive, flashflooding and gang influence cooperative spectrum sensing process. This allows data fusion center through with deceit, flashflooding, gangs cooperation process, tampering were given the wrong data and instructions. It can make the spectral data fusion center erroneous data and instructions. Channel allocation will be exploited by attackers. Once the input data tampering, cognitive radio system can not accurately adjusted according to the external environment itself. The best adaptive function will also be provided to the attacker. Therefore, spectrum sensing accuracy of the data is very important.

In addition, MAC layer also have serious security problems, including selfishness attacks and denial of service attacks. Selfish behavior attack is the use of a selfish way

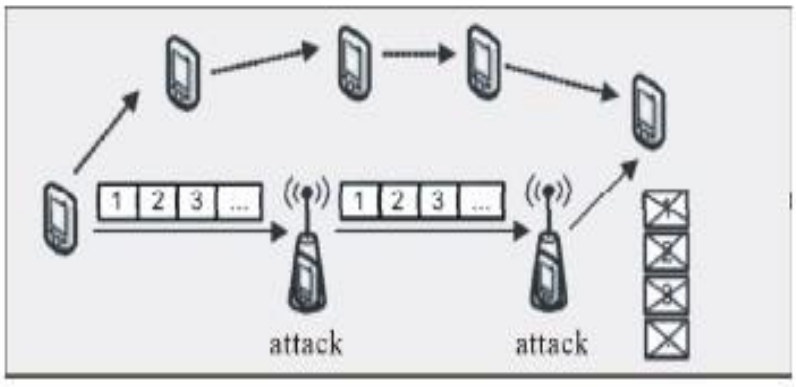
consultations CR packet node selfish behavior breaking process. Denial of service attacks are the attacker by weakening the saturation control channel common control, dynamic resource allocation and reduce the ability of the network. MAC layer Distributed Network Protocol CR has the following drawbacks: First, it is the lack of accreditation of the MAC layer. In one hop networks such as 802.22 WRAN, the presence of security sub-lay, to ensure confidentiality and provide security and authentication mechanisms MAC frame. Through the security layer, it can prevent DOS attacks modify genuine MAC frames. However, the agreement does not multi-hop network to use, because there is no reliable entity acting as a server to control the distribution of key materials. If there is no authentication mechanism, the attacker can fake MAC control frames denial of service attacks. Secondly, it is a saturated channel control problem. From a security point of view, it plays an important role in the control channel network availability. If an attacker can control the channel saturation, they can stop the negotiations and distribution channels, form DOS attacks. By multi-hop CR MAC protocol, an attacker could easily forge channel consultation launched DOS attacks. Using malicious MAC frame saturation control, legitimate users can not use a shared control channel negotiation and allocation data channel. Third, busy predictable sequence control channel. If the control frame exchange unencryption form, any cognitive user, comprising an attacker can easily obtain the channel list, for attack.



(a)



(b)



(c)

Figure 1. Spectrum Sensing Data Tampering Attacks.

With the Progress of cognitive radio, spectrum sensing win more and more attention. Because it is vulnerable to tampering perceived result nodes it has been proposed spectrum sensing and cooperation. It can avoid tampering single malicious node information behavior [15]. Determine the authenticity of the nature of electromagnetic SIG- understanding of the data. For cooperative spectrum security cheating gang problem, Wenkai Wang *et. al.*, Proposed a method that can distinguish between normal users and malicious users [16], in order to identify perceived authenticity of the data.

3.2.2. Artificial Intelligence Behavior Threats:

Learning Threats

CR has the ability to learn, it can be under the past experience and the current environment to predict the future, and select the best set of parameters [17]. CR can be seen as the human mind [18] extensions. Because the ability to learn, it can use a comprehensive analysis of memory and experience, for the new environment. However, in the learning phase, it is very vulnerable to attack. An attacker can modify the interference or change under the current conditions of the previous data, as shown in Figure 2 cognitive node without any criteria might make the wrong tampering with the data as the actual input. Through this learning and reasoning, it may affect predictions of CR. This influence tampering with CR input is long-term, the operation is called faith attack [19]. And the memory will remain in the memory, which will affect future decisions.

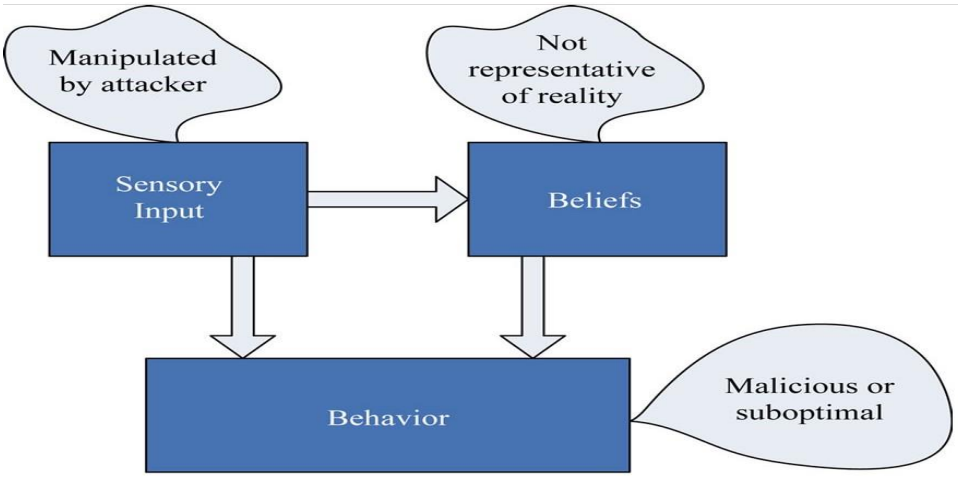


Figure 2. Relationship Sensor Inputs, Beliefs and Behaviors Cognitive Engine, shows a rival manipulating sensory input can change cognitive radio beliefs and behaviors.

The traditional password encryption, both to ensure the security of data transmission, and can not determine whether or not to send the data in line with the objective reality. This requires comparing the test results and a comprehensive analysis of data in order to find out whether the received user data has been tampered with. It should be regularly updated repository to avoid long-term memory errors influenced later decisions.

CR has great parameters to control and evaluate the performance. Regardless, CR parameter to control and estimate policy or learning network performance. These parameters are caused by many types of parameters, such as performance evaluation, policy conversion conditions such as changes in the parameters of risk are seen as a threat, but a typical example is the objective function of attack. In general, cognitive radio has three objectives: low power consumption, high speed and security. According to various circumstances, these three objectives have different degrees of importance. The following is the objective function expression:

$$F = \alpha_1 P + \alpha_2 R + \alpha_3 S \tag{1}$$

Wherein α_i, i = 1,2,3 are by weight P, R, S represents.

Because CR decisions by maximizing the objective function, the attacker do to suppress CR adjusted by varying the parameters of the target. This results in a CR can not achieve the desired effect. Threats parameters, which can be solved by PSO optimization algorithm, and compared with the value of the mathematical model appropriate for each child targets.

Cross-Layer Design Safety Issues

Cross layer of cognitive radio has been paid more attention to, and urgent problems facing security. Cross-Layer attention and research has also pressing security issues facing layer. Network problems, such as throughput, equality and delay issues to be addressed [19]. Figure 3 shows a physical layer security and cognitive radio link layer:

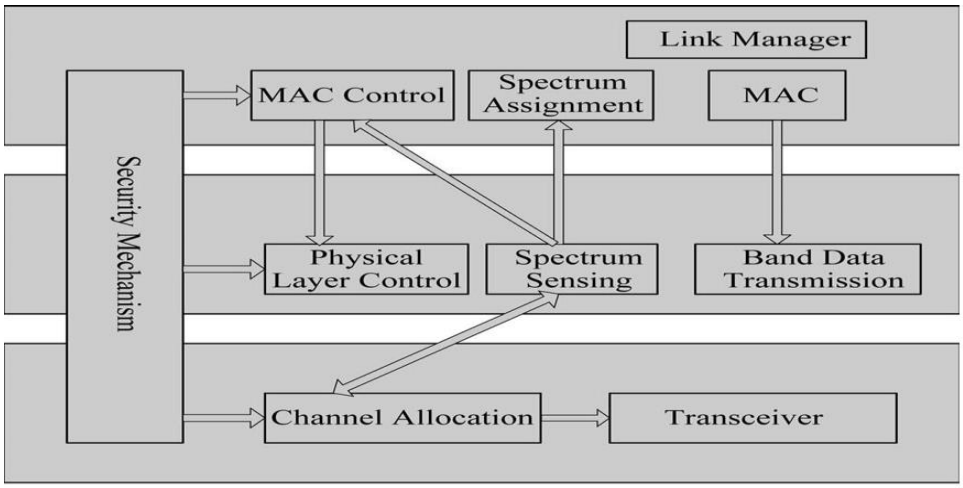


Figure 3. Cross-layer Security Issues.

The main purpose of cross-layer design is to optimize the exchange of information, but also brought a cross-layer attacks. Malicious actions layer may be other layers a dangerous. Cognitive radio has the following key points:

The channels: the rapid changes in the available spectrum and frequency. The main users are in the "a" or "disappeared" switch. The disturbance caused by natural, human disturbance

Equipment: it needs to be the main users of real-time spectrum monitoring and testing large consumption.

Global context: There is more cooperation and competition complex network topology changes and allocation of available spectrum and spectrum, and nodes.

In the cross-layer design of cognitive radio, many aspects to consider, including the physical layer transmission scheduling information spectrum sensing, the main users of signal detection, dynamic spectrum allocation, channel variations and power equipment in the link layer may be a Other layers sharing to improve the performance of network devices. The network layer is capable of converting link congestion and maintenance information in the transport layer as the optimization of data transmission to end-to-end. However, cooperation between each layer and shared cognitive radio network has also brought new problems, such as data transmission at different frequencies of the physical layer. It is with traditional wireless networks are very different. Data is transmitted from one frequency to another frequency band switching delay may be generated. This switching delay will lead to the physical layer of a malicious attack, such as deliberately blocked continuous channel interference. Therefore, it is worth studying the safety of cross-layer design.

We take it as a cognitive radio network the temptation to attack the problem. Security issues are designated as: In the routing phase, the first increase in malicious nodes false information available channels to request routing of packets received. After that, it lure other nodes to route around, and discard the packet forwarding. Security threats, seriously affecting the communication performance of the network. To solve this problem, the key is to find a method to detect malicious nodes, other nodes refused to establish a connection with a malicious node. Through in-depth study of cognitive radio networks, we found that many of the attackers were the same as Ad Hoc networks, such as on-demand routing stage attacks black hole discovered routing distributed network and security threats.

4. Conclusion

In recent years, cognitive radio technology, because of the shortage of radio spectrum resources rapidly. It is the basis of software-defined radio and adaptive changes in the environment on the development of an intelligent wireless communication system. Its core idea is that the wireless communication device having a spectral hole and use them to find a reasonable capacity. Cognitive radio technology, it opens up a new way, the conflict from growing demand for wireless communications and limited radio spectrum resources to solve problems. Currently, most researchers have focused on spectrum sensing. They made a lot of ways to improve the efficiency of cooperation views. However, the security study was not thorough. While some security mechanisms have been proposed, they do not fully meet the needs of CRN operations, it also requires further study in many ways. Key to the future research direction is to settle the issue of safety in the design of the network layer encountered.

References

[1] J. Mitola III, "Cognitive radio for flexible Mobile Multimedia Communications", Journal Mobile Networks and Applications, vol. 6, no. 5, **(2001)**, pp. 345-381.
[2] Q. Zhang, A. B. J. Kokkeler and G. J. M. Smit, "A Reconfigurable Radio Architecture for Cognitive Radio in Emergency Networks", The 9th European Conference on Wireless Technology, Manchester, England **(2006)** September, 10-12.
[3] H. y. Tang, "Some Physical Layer Issues of Wide-band Cognitive Radio Systems", First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Baltimore, USA, **(2005)** November, 8-11.
[4] R. Chen, J. M. Park and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," Journal on Selected Areas in Communications, vol. 26, no. 1, **(2008)** p. 25-37.
[5] Y. Zhang, G. c. Xu and X. z. Geng, "Security Threats in Cognitive Radio Networks", 10th IEEE International Conference on High Performance Computing and Communications, Dalian, CHINA, **(2008)**, September, 25-27.
[6] X. w. Zhou and X. y. Xin, "Key Technology Research on Cognitive Radio Security", Telecommunications Science, vol. 24, no. 2, **(2008)**, pp. 35-40.
[7] Q. H. Mahmoud, "Cognitive Networks", John Wiley & Sons Ltd., Chichester, **(2007)**.
[8] Q. Liu, Z. Zhou, C. Yang and Y. b. Ye, "The Coverage Analysis of Cognitive Radio Network", 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, CHINA, **(2008)** October, 12-14.
[9] K. g. Bian and J. Min, "Security Vulnerabilities in IEEE 802.22", Proceedings of the 4th Annual International Conference on Wireless Internet, Maui, USA, **(2008)**, November, 17-19.
[10] R. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Secure cooperative Sensing Techniques for Cognitive Radio Systems", IEEE International Conference on Communications, Beijing, CHINA, **(2008)**, May, 19-23.
[11] X. y. Zhang and C. Li, "Constructing secured cognitive Wireless Networks: Experiences and Challenges", Wireless Communications and Mobile Computing, vol. 10, no. 1, **(2010)**, pp. 50-69.
[12] M. K. Baek and J. Y. Kim, "Effective Signal Detection Using Cooperative Spectrum Sensing in Cognitive Radio Systems", 11th International Conference on Advanced Communication Technology, Phoenix Park, The Republic of Ireland, **(2009)** February, 15-18.
[13] R. s. Gong, Z. y. Hu and T. Shen, "Adaptive CRN spectrum Sensing Scheme with excellence in topology and Scan Scheduling", 3rd International Conference on Sensing Technology, Tainan, TAIWAN, **(2008)** December, 30.
[14] S. Arkoulis, L. Kazatzopoulos, C. Delakouridis and G. F. Marias, "Cognitive Spectrum and Its Security Issues", The Second International Conference on Next Generation Mobile Applications, Services and Technologies, Beijing,CHINA, **(2008)**, September, 16-19.
[15] A. O. Richard, K. Kim and A. Ahmad, "On Secure Spectrum Sensing in Cognitive Radio Networks using Emitters Electromagnetic Signature", Proceedings of 18th Internatonal Conference on Computer Communications and Networks, San Francisco, USA **(2009)**, August, 3-6.
[16] W. k. Wang and H. s. Lit, "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks", 43rd Annual Conference on Information Sciences and Systems, Baltimore, USA, **(2009)**, March, 18-20.

[17] K. Takeuchi, S. Kaneko and S. Nomoto, "Radio Environment Prediction for Cognitive Radio", 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Singapore **(2008)**, May, 15-17.
[18] D. Cabric, S. M. Mishra and R. W. Brodersen, "Implementation issues in Spectrum Sensing for Cognitive Radios", Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, Asilomar, USA, **(2004)**, November, 7-10.
[19] T. C. Clancy and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation", 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Singapore, **(2008)** May, 15-17.