Wireless Sensor Network, **2012, 4, 120-126**
http://dx.doi.org/10.4236/wsn.2012.44017 Published Online April 2012 (http://www.SciRP.org/journal/wsn)

Research and Analysis on Cognitive Radio Network Security

Long Tang[1], Juebo Wu[2]
[1]State Key Laboratory of Software Engineering, Wuhan University, Wuhan, China
[2]Shenzhen Angelshine Co. Ltd., Shenzhen, China
Email: tlnoriko@163.com, wujuebo@gmail.com

Received January 7, 2012; revised February 17, 2012; accepted March 19, 2012

ABSTRACT

This paper firstly gives a detail analysis on the security problems faced in cognitive radio network, and introduces the basic issues about cognitive radio network. Then, according to the differences between cognitive radio network and existing wireless network, it analyses and discusses the dynamic spectrum access security and artificial intelligence. Finally, it draws a conclusion to security problems of cross layer design.

Keywords: Spectrum Access; Cognitive Radio Network; Artificial Intelligence; Network Security

1. Introduction

Spectrum is a one of scarce resources in the present spectrum management framework. With the rapid development of wireless communication technology, it appears increasingly prominent how to use the spectrum resources effectively. In many countries, most of the spectrum is assigned to radio business department. In the distribution of this already authorized and unauthorized frequency band, there exists imbalance in using spectrum resources as follows: On one hand, the authorized frequency band spectrum resources have occupied a large part, but many authorized is in the idle state (spectrum empty). The research by federal communications commission (FCC) shows that the average frequency of authorized spectrum is between 15% and 85% in most time and area. On the other hand, the open use of unauthorized frequency spectrum resources occupies small portion of the band. But the user is huge and the volume of business is crowded, causing the radio frequency band has tendency to be saturated. Static spectrum allocation principle is the main reason that causes the low utilization ratio of frequency band and the contradiction for other users' using the corresponding frequency. If it can use the idle spectrum resource temporarily, the tension of lack of spectrum resources will be eased and get a great improvement. Cognitive Radio (CR) is put forward to solve this problem effectively. Its main function is to make the future of radio equipment with independent to find out spectrum hole, and utilize the spectrum effectively.

2. Concepts and Characteristics of Cognitive Radio

The concept of cognitive radio is originated from Joseph Mitola's fundamental work in 1999. Its core idea is that the CR has the ability to learn and communicate with the surrounding environment so as to perceive the available spectrum in the space, limit and reduce the occurrence of conflicts. Since the concept of cognitive radio appeared, various organizations and scholars from different angle gave many definitions for cognitive radio [1]. The most representative definitions were presented by the U.S. federal communications commission (FCC) and a famous professor Simon Haykin. The FCC suggested any adaptive spectrum with consciousness should be called cognitive radio, which defined as: CR is one kind of radio which can change its transmitter parameters dynamically based on operating environment. It has the function of self modification by environmental awareness and transfer parameters. From the point of view of signal processing, Simon Haykin thought CR is an intelligent wireless communication system. It can perceive the external environment and learn knowledge by the artificial intelligence technology. Through the real-time change for some operating parameters, it can adapt to the statistical properties change of the wireless signal. Thus, it realizes that high reliable communications can achieve in any time and any place with using spectrum resources effective.

Cognitive radio is different from the traditional radio that it owns the ability of cognitive intelligence and realizes the real-time detection of environment. Through adaptive change parameter settings for the study and decision-making, it can make full use of spectrum resources effective. The prerequisite for CR is the openness of the spectrum, that is, the network should be divided into Primary users (authorized users) and subprime users (unauthorized users). On the basis of the spectrum openness, subprime users can find out the idle spectrum by detecting spectrum hole which the Primary users don't use right now, and make full use to access frequency band without impact on the premise of the user communication [2]. This requires subprime users with the ability of the real-time detection for spectrum hole, having the following three characteristics [3]:

1) Perception-CR must be able to identify unused spectrum;

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

3) No interference-CR must not cause harmful interference to Primary users.

3. Cognitive Radio Network Security

In consciousness to the major effect of the spectrum shortage, FCC considers that it should open parts of authorized spectrum for unauthorized users on the premise of no impact on Primary users [4]. It's vital thing for testing spectrum hole. In order to solve how to detect these free bands and use them, people put forward the dynamic spectrum access technology. Through the Spectrum Sensing to free band algorithm, subprime users can make full use of spectrum resources by no impact on the premise of Primary users' communications. Cognitive radio network as a wireless communication technology, it's not only the traditional security problems, but also has introduced some new hidden security. For example, there are many steps in the process of spectrum access, such as Spectrum Sensing, spectrum management, spectrum migration and spectrum sharing [5]. Each process exits security issues. Cognitive radio can learn and adapt to the external environment intelligently, so lots of research are making efforts into reasoning and optimization learning algorithm in various state. However, as the information value continuously reflecting, the concept of information security in the design gains more and more attention. The communication security has become an important part of the system design, especially involving military, commercial secrets, etc. Cognitive radio in these areas has been widely applied, so it must pay more attention to the safety. In addition to the traditional wireless security problems, cognitive radio is also facing its peculiar hidden trouble [6].

3.1. Traditional Wireless Network Security

Because wireless communication uses the electromagnetic wave as medium, the method of physical isolation is difficult to realize. Compared with cable communication, wireless communication has more unsafe factors, mainly shown in the following aspects:

3.1.1. Traditional Wireless Network Security

In wireless communication process, all of the communication and information are transmitted by wireless channel. In accordance to cable channel, it is intercepted more easily if only the attackers use the corresponding equipments. In the commercial wireless communication system, the information transmitted may include user identity, billing information, key information, position and signaling information, etc. The leaking information to users will bring economic and honorary loss, also including leaking user's privacy.

Wireless wiretapping program is widely exiting in the wireless network, and the solution at present is to transmit information by encryption. Different strength of encryption is applied in the variety of the importance of information transmission. The method can protect transmit information effectively. But along with the rapid development of computer hardware technology, using a single key encryption transmission has the possibility of violence break. Therefore, it needs to improve the encryption algorithm strength, in order to take measures to guard against the key risk.

3.1.2. Fake Attack

In wireless communication, the terminal and the base station do not have physical cable connection. The identity information exchange between terminal and base station is achieved by the radio channel. The identity information is related to the network control, network services and network access, etc. Due to the existence of a radio channel, attacker may get identity information through the wiretapping on a radio channel. When the attacker gets a legitimate user's identity, he can use the identity information to access network illegally, even getting network service or being engaged in network attack.

In different wireless communication system, the purpose of the fake attack is different. Through faking legitimate users by intercepting the identity information, attackers can use communication services without paying network service charge. By using base station equipments, attackers may deceive the end user, to gain more users' identity information.

3.1.3. Information Tampering

Information tampering means the attacker taps into the relevant information and revises them before passing them to the original information, including information delete, replace and modify. Information tampering usually occurs in storage-forward network. Information between two wireless terminals may forward through the other wireless terminal or network center, and these "transfer station" has the possibility to tamper information. Information tampering will make a serious threat to the integrity of the network communication and effectiveness, causing needless loss to user.

3.1.4. Service Repudiation

Service repudiation points that the user refuses to admit the transmission data of communication service or communication process after connection. It includes two parts:

1) Repudiation of communication service. In the commercial networks, the user has denied using the network, thus he refuses to pay relevant network cost.

2) Repudiation of communication content. The user deny to his content on the launching of the transmission. For instance, in e-commerce or electronic payment, users denied that they had occurred transactions and refused to pay.

3) Service repudiation will influence the credit of the network, and it will cause needless losses to operators and merchants. The present stage mainly takes the identity authentication and the way of using the asymmetric encryption algorithm to avoid such safe hidden trouble.

3.1.5. Replay Attack

Replay attack is the attacker taps into the effective information over a period of time interval, and then he delivers to the receiver again. Its purpose is to use effective information in time change to win the trust of the receiver in order to obtain more useful information. For example, after obtaining the user password, the attacker would control network license and the access network resources.

3.1.6. Denial of Service and Information Interference

The electromagnetic wave is the carrier of wireless communication. With the rapid development of hardware technology, the attacker can block normal communication through the power of the transmitters. Through making noise spectrum in normal communication signals, the communication may be interfered. This would cause the resources of wireless base station equipment are not enough, and users' access would be refused. Information interference will have serious social influence. For example, the event of Xin's communication satellite interference happened in 2001 is because the lawbreaker set up VSAT terminal through the high power to interrupt satellite service.

3.2. Cognitive Radio Network Security

3.2.1. Threat of Dynamic Spectrum Access

The current spectrum policy employs fixing allocation, that is, the fixed spectrum is assigned to the authorized user of fixed region by government department for a long time. Spectrum is a kind of limited resource. Along with the increasing demands of wireless equipment and communication, spectrum allocation is almost exhausted. However, in view of the existing fixed allocation of significant spectrum, cognitive radio can use of secondary spectrum cleverly so as to achieve the purpose of full use of resources. This needs the cognitive user can perceive the channel situation at every moment, and try to access the signal on the premise of no interrupt to Primary users. This kind of solution requires using advanced technologies; otherwise it will make certain interference even harm to Primary users. Dynamic spectrum access is composed of Spectrum Sensing, spectrum management and spectrum migration, where there exits unsafety in each phase. Different from the traditional wireless network, cognitive radio has its special safety problems: spectrum abuse and selfish behavior, to attack by imitating Primary users, public control channel obstruction, cognitive nodes evolution into malicious nodes [7], etc. The following section will analyze the existing safety problems in cognitive radio system from the aspects of dynamic Spectrum Sensing.

3.2.1.1. Primary User Emulation Attack

Primary User Emulation (PUE) attack is one of security problems that physical layer needs facing, which has great threat to Spectrum Sensing. The attacker sends CR signal by imitating the primary user's signal characteristic. This kind of attack method can realize a highly flexible and software based air interface under the circumstance of CR. In the environment of Dynamic Spectrum Access (DSA), the primary user can utilize the authorized frequency band free of all times. The authorized frequency band turns into idle state when the primary user releases the resources, so the subprime users can attempt to access [8]. One necessary condition is the subprime users must be able to perceive the existence of free frequency band. Hence, it needs Spectrum Sensing algorithm to carry out real-time perception for spectrum state by detection devices. At this time the attacker creates fully similar signal as the primary user does to cause an error frequency spectrum, which lead subprime users to make mistakes for the spectrum state. This will let the channel free in the system, and give attackers have the opportunity to access such channels. This kind of attack is referred to as Primary User Emulation attack [9].

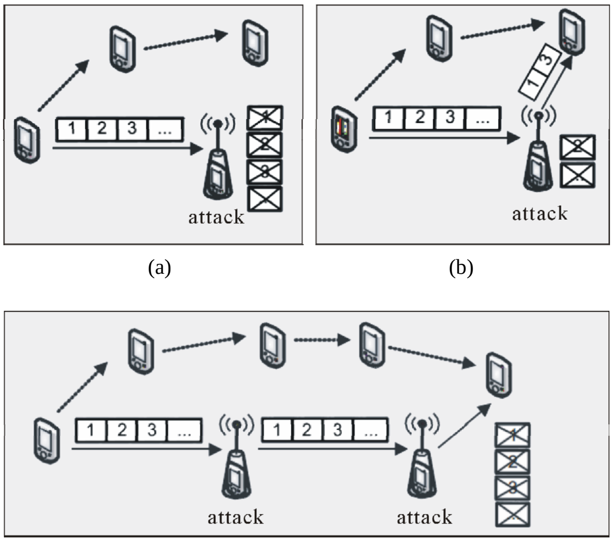
Research found that PUE attack can produce serious interference to the process of Spectrum Sensing, and significantly reduce the available channel resources of legitimate perception users'. Filter matching and feature rotating detection technology can achieve Spectrum Sensing. The nodes with these detection techniques are able to identify the primary users' essential characteristics, so they can distinguish the signal between primary and subprime users. But this is not enough to fight PUE attack. From attack purposes and means the PUE attack can be divided into two classes: selfish attack and malicious attack. For selfish behavior, the attacker's goal is to maximize their interests. When the attacker detected a band, he would emulate the primary user's signal to prevent other subprime user's signal to access [10]. When the attackers achieve their purpose, they will exit channel. Attack is short. Once the attacker exits channel, the user will access the channel again after detecting the perception free. For malicious behavior, the attacker make endeavor to restraint legitimate subprime user to detect and use authorized frequency band, causing denial of service attack. The difference is malicious attacks don't use the free license for themselves, and they just launch PUE attack in many frequency band on round way. Whether selfish or malicious attack, it will bring greatly inconvenience to the network. For PUE attack, it is the key how to identify the difference between primary users' signal and malicious cognitive users' signal. Base station can verify the authorized user by certificate, but it is difficult to control once the certificate is lost. So it should provide a soft authentication which verifies user quickly with less computational complexity. In addition, once detecting malicious attack behavior, it immediately makes corresponding measures for malicious users to impose punishment. This could reduce its credibility in the network even force him out its network.

3.2.1.2. Primary User Interference

In DSA, it is high frequency that malicious users disturb primary users, which also is a kind of common attack form. Because of CR's flexibility and adaptability, the introduction of subprime users will inevitably cause interference to the user, even denial of service attack. Subprime users have two ways to use spectrum: One is the use of the band white free of authorized users'. It demands to know the accurate model of primary users' activities. The other is to allow subprime users to utilize the gray space of primary users' at the same time. Obviously the latter will be essential to impact the primary users. In order to avoid the interference of the users', cognitive needs not only accurate perception, but also needs to know the news of the primary users' appearing. The attacker thus can launch attacks. Through preventing and interfering received cognitive information, this leads to the user's interference. This will cause serious damage to the performance of the network. This may make primary user work in the noise, even no frequency band available. It violates the purpose of the cognitive radio technology development, that is, to access without interfering the primary user's normal use. Therefore, it leads switch frequency spectrum for cognitive user. Once discovering the emergence of primary user's signal, cognitive users should evacuate immediately by switching frequency band.

3.2.1.3. Data Tamper Attack of Spectrum Sensing

In the process of distributed Spectrum Sensing, the attacker sends the wrong Spectrum Sensing information to data collection center, which caused make the wrong decision by data collection center, shown in **Figure 1** [11]. This is the most common perception tamper with the data. In order to improve the efficiency of perception, the literature [12,13] put forward the cooperation type Spectrum Sensing, effectively improved the efficiency of the Spectrum Sensing. But it gave rise to new problems, such as nodes cheat with partnership and creating wrong results. No matter distributed or cooperative network, Spectrum Sensing data have serious effects if being tampered. According to access abnormal behavior of point (AP), S. Arkoulis divided nodes into four categories: a misbehaving AP, a selfish AP, a cheat AP and a malicious AP [14]. Malicious node can influence the process of Spectrum Sensing by tampering, cheating, flashflooding and gang cooperation. This let data fusion center obtain the wrong data and instructions respectively through the tamper with, deception, flashflooding, gang cooperation way process. It could make spectrum data fusion center for the wrong data and instructions. Channel allocation will be utilized by the attacker. Once the input data tampered, cognitive radio system can't truthfully regulate according to outside environment by itself. The best adaptive function will also be provided for the attacker. Thus, the correctness of the Spectrum Sensing data is very important.



(a)

(b)

(c)

Figure 1. Data tamper attack of spectrum sensing.

In addition, the MAC layer also has serious security problems, mainly including selfish behavior attack and denial of service attack. Selfish behavior attack is packet breaking process of selfish behavior by selfish CR node using channel consultation. Denial of service attack is the attacker weakens public control channel by saturation control channel, and then lower the ability of network dynamic resource allocation. MAC layer protocol of distributed CR network has the following weaknesses: First of all, it lacks the MAC layer of authentication. In one hop network such as 802.22 WRAN, there is a security sub-lay to ensure the safety of the MAC frame with providing confidentiality and authentication mechanism. Through the security layer, it could prevent DoS attack made by modification and fake of MAC frame. But the protocol is not used in multiple hops network, because there is no reliable entity as a server to control key materials distribution. Without authentication mechanism, the attackers can launch the DoS by forging MAC control frame. Secondly, it is the saturation problem of channel control. From a security point of view, the control channel plays an important role in network availability. If the attackers can make control channel saturated, they can block negotiations and the distribution channel and form DoS attack. By MAC protocols in multi-hop CR, the attackers can easily forge channel negotiation to initiate DoS attack. Using the malicious MAC frame to saturation control, the legitimate users can't use the shared control channel consultation and distribution data channel. Thirdly, it is the predictable control channel of busy sequence. If the control frame is exchanged in the form of unencryption, any cognitive user including attackers can easily obtain the channel list so as to carry out attacks.

Along with the progress of the studies on cognitive radio, Spectrum Sensing wins more and more attentions. Because it's easy to tamper the perception results for nodes, people put forward Spectrum Sensing with cooperation. It can avoid the behavior of tampered information with single malicious node. Literature [15] judged the perception data authenticity by electromagnetic signature. For problems of co-operative spectrum security gang cheating, Wenkai Wang et al. put forward a kind of method which can distinguish between normal users and malicious users [16] so as to identify the perception data authenticity.

3.2.2. Artificial Intelligence Behavior Threats

3.2.2.1. Learning Threats

CR has the ability to learn, and it can predict the future through the past experience and the current environment and choose the best parameters Settings [17]. CR can be seen as the extension of the human mind [18]. Because of the ability to learn, it can use memory and experience to carry out comprehensive analysis for the new environment. But in learning stage it is very vulnerable to attack. The attacker can interfere through the modification of the previous data or to change the current conditions, as shown in **Figure 2**. Cognitive node in the absence of any judgment standard may make mistake to the tampered data as actual input. By such learning and reasoning, it may affect the prediction result of CR. This kind of input of tampering with the CR influence is long-term, referred to as Belief manipulation attacks [19]. And the memory will remain in memories, which will impact the future decision.

The traditional password encryption measures only guarantee the security of data transmission, and it cannot judge whether the transmission data is accord with the objective reality or not. This needs to compare each of the test results with comprehensive analysis data, in order find out if the user receives data have been tampered. And it should regularly update memory bank to avoid later decisions influenced by the mistakes of long-term memory.

3.2.2.2. Parameters Threats

CR has a great deal of parameters to control and assess performance. No matter in policy or learning, CR uses parameters to control and estimate network performance. These parameters are many types such as the performance measurement, policy conversion condition etc. The hidden danger caused by parameter change is regarded as parameters threats, and the typical example is objective function attack. Generally speaking, cognitive radio has three goals: low power, high speed and safety. Based on all kinds of different situations, these three goals have different important degree. The following is the objective

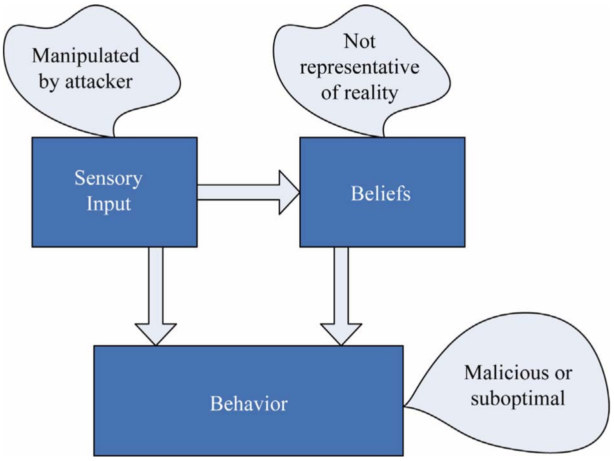


Figure 2. Relationship between sensor input, beliefs, and behavior in a cognitive engine, showing how an adversary manipulating sensory input can change the beliefs and behavior of a cognitive radio.

function expression:

$$F = \alpha_1 P + \alpha_2 R + \alpha_3 S \qquad (1)$$

where α_i, i = 1, 2, 3 and P, R, S stand for the weight.

Since CR makes decisions by maximizing the objective function, the attacker achieves the goal through the parameters change to restrain CR adjustment. It would lead the CR can't achieve the desired results. For parameters threats, it can be solved through PSO optimal algorithm and comparing each sub-goal with moderate value using mathematical model.

3.2.2.3. Security Problems of Cross-Layer Design

Cross-layer research of cognitive radio has been paid more attentions to, and the facing security problems are also pressing. Cross-layer research has attention span, and the security problems facing layer is also pressing. Network problems such as throughput, equality and delay need to be resolved [19]. **Figure 3** shows the security problems of the physical layer and the link layer for cognitive radio:

The main purpose of the cross-layer design is to optimize the information exchange, but it also brings a cross layer attack. A layer against malicious operation can be a danger to other layers. Cognitive radio has the following key points:

Channel aspects: Available spectrum changes quickly and frequency. The primary user is in the switching of "appeared" or "disappear". The interference is caused by nature, human interference, etc.

Equipment aspects: It needs to carry out real-time spectrum surveillance and primary user testing with large spending.

Global aspects: The network topology is changing with the available spectrum and spectrum allocation, and nodes exist more complex cooperation and competition.

In the cross-layer design of cognitive radio, many aspects need to be considered, including physical layer spectrum sensing, primary user signal detecting, dynamic spectrum allocation, channel change and power equipment, etc. The transmission scheduling strategy information in link layer can be shared with other layers, in order to improve the performance of the network equipment. The network layer is able to convert link congestion and maintenance information in transport layer as optimized data to end-to-end transmission. However, the collaboration between each layer and sharing for cognitive radio network also brings new problems, such as the physical layer in different frequency data transmission. It is very different with the traditional wireless network. Data transmission from a frequency switch to another frequency band can produce delay. This switching delay can cause malicious attacks in physical layer, such as deliberately continuous jam channel interference etc. So, it is worth studying cross-layer design security.

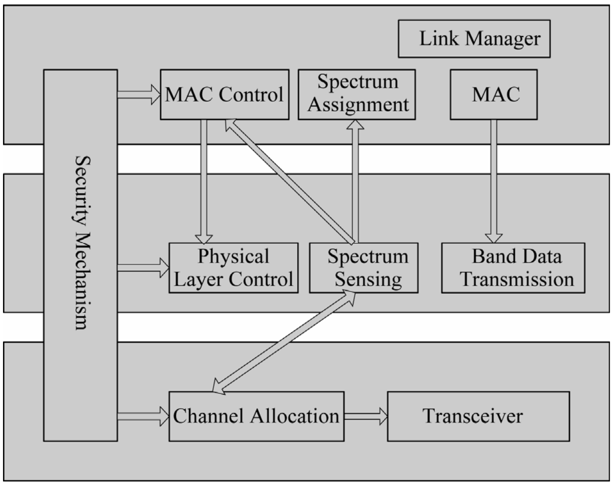


Figure 3. Cross-layer security problems.

We call it as Lure attack problem of cognitive radio network. The security problem is specified as: In the stage of routing found, malicious node firstly adds false available channel information to the request packet of receiving routing. After that, it lures other nodes into the routing lap, and discards the forward packets. The security threat seriously affects the communication performance of the network. To solve the problem, the key lies in finding detection method for a malicious node, making other nodes refused to establish connection with malicious nodes. Through depth study on cognitive radio network, we found that many attackers were the same as the black hole attack in Ad Hoc networks, such as on-demand routing way in the distributed network and security threats found in the routing stage.

4. Conclusion

In recent years, cognitive radio technology has developed quickly because of the shortage of wireless spectrum resources. It is an intelligent wireless communication system developed from the basis of software radio and self-adaptive to environmental changes. It is the core idea that the wireless communication equipment has the ability to find spectrum hole and utilize them reasonable. By cognitive radio technology, it opens up a new way to solve the problem from the growing wireless communication demands and the limited wireless spectrum resource conflicts. At present, most of the researchers are focused on spectrum perception. They put forward many methods to improve cooperation perception efficiency. However, the studies on security have not gone in-depth. Although some security mechanism has been proposed, they cannot be completely meeting the needs of CRN operation, which need further research in many ways. The key research direction in future is to settle the questions encountered in the design of safety across the network layer.

5. Acknowledgements

This paper is supported by Key Projects in the National Science & Technology Pillar Program (2011BAH20B03).

REFERENCES

[1] J. Mitola III, "Cognitive Radio for Flexible Mobile Multimedia Communications," *Journal Mobile Networks and Applications*, 2001, Vol. 6, No. 5, pp. 435-441. doi:10.1023/A:1011426600077

[2] Q. Zhang, A. B. J. Kokkeler and G. J. M. Smit, "A Reconfigurable Radio Architecture for Cognitive Radio in Emergency Networks," *The* 9*th European Conference on Wireless Technology*, Manchester,10-12 September 2006, pp. 35-38. doi:10.1109/ECWT.2006.280428

[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, 8-11 November 2005, pp. 151-159. doi:10.1109/DYSPAN.2005.1542630

[4] R. Chen, J. M. Park and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, Vol. 26, No. 1, 2008, pp. 25-37. doi:10.1109/JSAC.2008.080104

[5] Y. Zhang, G. C. Xu and X. Z. Geng, "Security Threats in Cognitive Radio Networks," 10*th IEEE International Conference on High Performance Computing and Communications*, Dalian, 25-27 September 2008, pp. 1036-1041. doi:10.1109/HPCC.2008.21

[6] X. W. Zhou and X. Y. Xin, "Key Technology Research on Cognitive Radio Security," *Telecommunications Science*, Vol. 24, No. 2, 2008.

[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," 4*th International Conference on Wireless Communications*, *Networking and Mobile Computing*, Dalian, 12-14 October 2008, pp. 1-4. doi:10.1109/WiCom.2008.306

[9] K. G. Bian and J. Min, "Security Vulnerabilities in IEEE 802.22," *Proceedings of the* 4*th Annual International Conference on Wireless Internet*, Maui, 17-19 November 2008, pp. 1-9.

[10] R. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," *IEEE International Conference on Communications*, Beijing, 19-23 May 2008, pp. 3406-3410. doi:10.1109/ICC.2008.640

[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," 11*th International Conference on Advanced Communication Technology*, Phoenix Park, 15-18 February 2009, pp. 1746-1750.

[13] R. S. Gong, Z. Y. Hu and T. Shen, "Adaptive CRN Spectrum Sensing Scheme with Excellence in Topology and Scan Scheduling," 3*rd International Conference on Sensing Technology*, Tainan, 30 November-3 December 2008, pp. 384-391. doi:10.1109/ICSENST.2008.4757133

[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*, 16-19 September 2008, pp. 565-570. doi:10.1109/NGMAST.2008.102

[15] A. O. Richard, K. Kim and A. Ahmad, "On Secure Spectrum Sensing in Cognitive Radio Networks Using Emitters Electromagnetic Signature," *Proceedings of* 18*th Internatonal Conference on Computer Communications and Networks*, San Francisco, 3-6 August 2009, pp. 1-5. doi:10.1109/ICCCN.2009.5235288

[16] W. K. Wang and H. S. Lit, "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks," 43*rd Annual Conference on Information Sciences and Systems*, Baltimore, 18-20 March 2009, pp. 130-134. doi:10.1109/CISS.2009.5054704

[17] K. Takeuchi, S. Kaneko and S. Nomoto, "Radio Environment Prediction for Cognitive Radio," 3*rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Singapore, 15-17 May 2008, pp. 1-6. doi:10.1109/CROWNCOM.2008.4562502

[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, 7-10 November 2004, pp. 772-776. doi:10.1109/ACSSC.2004.1399240

[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, 15-17 May 2008, pp. 1-8. doi:10.1109/CROWNCOM.2008.4562534