The Security in Cognitive Radio Networks: A Survey

Xueying Zhang
Faculty of Engineering and Applied Science,
Memorial University of Newfoundland
St. John's, NL, A1B 3X5, Canada
xueying.zhang@mun.ca

Cheng Li
Faculty of Engineering and Applied Science,
Memorial University of Newfoundland
St. John's, NL, A1B 3X5, Canada
licheng@mun.ca

ABSTRACT
Recent developments of wireless communication lead to the problem of growing spectrum shortage. Cognitive radio, as a novel technology, tends to solve this problem by dynamically utilizing the spectrum. Security in cognitive radio network becomes a challenging issue, since more chances are given to attackers by cognitive radio technology compared to general wireless network. These weaknesses are introduced by the nature of cognitive radio, and they may cause serious impact to the network quality of service. However, at present there are no specific secure protocols for cognitive radio networks. Motivated by this, the current state of art in security of cognitive radio network is reviewed in this paper. We focus on analyzing the security system at the macroscopic level, where both protection and detection are significant parts for ensuring security of the whole network. Special characteristics of cognitive radio network in different protocol layers are also investigated, such as physical layer, link layer, network layer, transport layer and application layer.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – Security and Protection

General Terms
Security

Keywords
Cognitive Radio, Intrusion Detection, Protection, Protocol Layer, Security

1. INTRODUCTION
Cognitive radio technology presents a promising solution for the spectrum shortage in wireless networks [1][2]. It enables the efficient utilization of limited available spectrum by defining two kinds of user in wireless networks: licensed user and unlicensed user [3]. In cognitive radio networks, the unlicensed user can use the spectrum which is not temporarily used by licensed users. When the licensed user appears to use the spectrum, unlicensed user should return it back and search for other spectrum to use. Since in cognitive radio networks the spectrum is being used dynamically, general schemes cannot satisfy the special network requirements. Specific protocols need to be designed in order to manage the dynamic frequency spectrum and to ensure the quality of service (QoS).

Security guarantee becomes urgently needed in cognitive radio networks [4]. First of all, cognitive radio network operates on wireless media. Compared to wired network, the nature of wireless network makes the security vulnerability unavoidable. In wireless network, signal has to be transmitted through an open media without real connection. That is to say, the data might be eavesdropped and altered without notice; and the channel might be jammed and overused by adversary. These will obviously disturb the normal communication and impact the quality of service. More important, cognitive radio technology introduces more chances to attackers due to their intrinsic nature. For example, spectrum sensing is a key characteristic used in cognitive radio networks, which functions as scanning a certain range of the spectrum to detect unoccupied spectrum [5], [6], [7]. Through this process, unlicensed user can determine whether the radio spectrum can be used. However, if the spectrum sensing result is modified maliciously, normal network activities will be disabled, even the whole network traffic may be broken down.

In this paper, we analyze the security system of cognitive radio network based on protection and detection. The special characteristics of cognitive radio network are investigated in different protocol layers, such as physical layer, link layer, network layer, transport layer and application layer. We maintain that security system should be capable of both defending and detecting at the same time and operating on all protocol layers.

The organization of this paper is as follows: In Section 2, security background of cognitive radio network is reviewed, including security requirements, special challenge and attacking motivations. In Section 3, the architecture of two-layer security system is presented, where the first layer functions as defending attackers from outside and the second layer functions as detecting the intrusion inside the network. In Section 4, distinguishing features of different protocol layers are analyzed and discussed. Conclusion is given in Section 5.

2. BACKGROUND
2.1 Security requirements
Although security requirements may vary in different application environment, usually there are some common requirements providing basic safety controls. Like cognitive radio network, it

IWCMC'09, June 21–24, 2009, Leipzig, Germany.

has the same security requirements with those in general wireless networks due to the nature of operating on wireless media [8]. These security requirements are outlined below:

(1) Access control: Access control is a security requirement for physical layer. Users must be guaranteed to have access to the network, and they must obey their organization's policy.

(2) Confidentiality: Confidentiality is defined by the International Organization for Standardization (OSI). It is used to ensure that information can only be read by authorized users. That is to say, eavesdropping should be prevented.

(3) Authentication: Authentication is a mechanism being used to ensure the identity for both sides of communication parties. That is to say, communication should be established among parties with valid identity. Authentication is used to prevent attackers from forging data and masquerading identity.

(4) Integrity: Integrity means the data should be transmitted without changing. The communicating information should be protected in the whole wireless network, including both user's private data and control information during transmission.

2.2 Special considerations

There are multiple consideration factors when security is applied in cognitive radio network due to the nature of cognitive radio communications, such as the flexible utilization of frequency spectrum and unscheduled appearances of different licensed users. Hence, additional special security issues need to be considered especially. For example, it will be more complicated to authenticate the identity of the licensed user. At present, there are still not completed and final solutions to solve the security problems brought by cognitive radio networks.

2.3 The motivation of attack

The motivations of attack in cognitive radio network are discussed in [9], which classifies the motivation into two types: selfish attack and malicious attack.

(1) Selfish attack: Selfish attack happens in the situation that the attacker wants to have access to spectrum with higher priority. It can be achieved by misleading other unlicensed users to believe there is a licensed user. As a result, the adversary user can occupy the spectrum resource as long as he or she wants. Since this selfish behavior does not obey the spectrum sharing scheme [5], this attack is called selfish attack.

(2) Malicious attack: Malicious attack means that the adversary inhibits other unlicensed users from using the spectrum and causes the denial of service (DoS). As a serious result, malicious attack will extremely decrease the available bandwidth and break down the whole traffic.

3. TWO-LAYER SECURITY SYSTEM

3.1 Overview

Generally, security mechanisms can be divided into two categories: protection based and detection based [8], [10], [11]. Protection based technology can be viewed as the first line of the security system, using cryptography to prevent malicious attackers outside the networks from both passive and active attacks. At the same time, detection based technology is the second line of security system. It is used to detect the intrusion attack inside the network, preventing the situation when cryptographic system has been broken through. We maintain that security system in cognitive radio network should be constructed based on both protection and detection, and each protocol layer should be considered due to the specific characteristic. Figure 1 shows how the security system works.

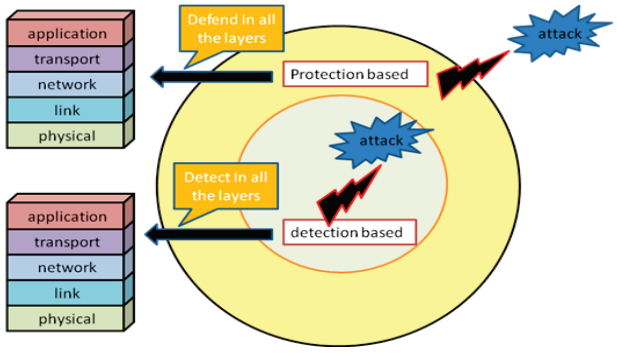

Figure 1. Two layer security system.

3.2 Protection based layer

As shown in Figure 1, the first layer of the security system is protection based layer. This layer functions as protecting the whole network from being attacked. Cryptography is implemented in this layer, satisfying multiple security requirements in cognitive radio networks. Although there are multiple cryptographic algorithms and protocols, in this paper we focus on interviewing macroscopic security system and leave cryptography as an open issue for future works.

3.2.1 Cryptographic algorithm

In cryptography, cipher is used to execute encryption and decryption, which enables the secure communication over an insecure channel. Cipher can be divided into two categories: symmetric key algorithm and asymmetric key algorithm; and for symmetric key algorithm, it can also be categorized into two types: block cipher and stream cipher.

3.2.2 Cryptographic protocols

Cryptographic protocols deal with the detailed process by applying cryptographic algorithms. These protocols include multiple purposes, such as key distribution through an insecure communication channel, identity authentication for the message transmitter, and methods for key agreement [12] and non-repudiation. Usually a third party, believed as a trust center, is involved in these protocols for key establishment; message authentication code (MAC) and digital signatures are also used to ensure authentication and integrity during communication.

3.2.3 Detection based layer

Figure 1 also shows the intrusion detection layer, which is the second layer of the security system. Intrusion detection can be applied either manually or automatically [11]. Manual detection includes examining the log files, detecting the signs of being attacked, and monitoring the network traffics. In comparison to manual detection, automatic detection needs an intrusion detection system to accomplish these tasks. Automatic detection system can be divided into two parts: host based and network

based. These two parts are integrated together to construct the whole intrusion detection system: Host based detection functions as monitoring the system report files; while network based detection takes charge of monitoring the flow of network packets.

(1) Intrusion detection system

The architecture of intrusion detection system is shown in Figure 2. Event data records the activity of the network. Database is used to record historical activities. There are two steps of detection included in the intrusion detection system: misuse detection and anomaly detection. Misuse detection is based on the intrusion detected previously, comparing the activity with the database. If there is nothing matched, anomaly detection will be implemented. Anomaly detection focuses on the abnormal behavior of the network and detecting the intrusion no matter it has been detected previously or not [13].

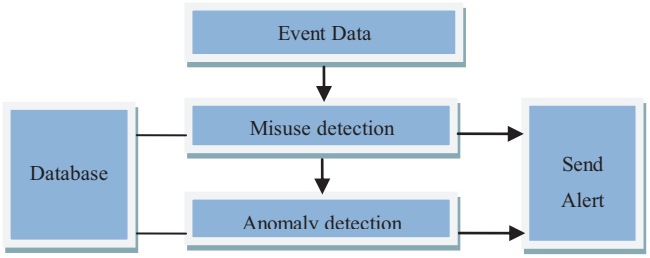

Figure 2. Architecture of intrusion detection system [13].

(2) Detection type

Misuse detection: Misuse detection depends on the experience accumulated. The known attacker activities are collected to build the database for checking the future misuse behavior. So if a malicious user wants to intrude the system with already known attacks, it will be caught due to its attack activity matching some records in the database.

Anomaly detection: Anomaly detection focuses on the abnormality of the network activity, which depends on the definition of what kind of activity can be regarded as normal. In the following section, activity according to different layer protocols will be discussed. These activities can be used to judge whether the activity is normal or abnormal. In the next section, different network activities are discussed at physical layer, link layer, network layer, transport layer and application layer respectively.

4. CHARACTERISTICS OF DIFFERENT PROTOCOL LAYERS

4.1 Different protocol layers

In this section, differences will be analyzed between cognitive radio network and conventional wireless network at each protocol layers [10]. As a special characteristic of cognitive radio network, reconfiguration influences every protocol layer due to accessing the spectrum dynamically [5].

4.1.1 Physical layer in cognitive radio networks

Physical layer operates on the data transmission directly through the physical medium. The component of spectrum sensing is the most obvious difference of the physical layer between cognitive radio networks and other conventional networks. Spectrum sensing is an important part in cognitive radio networks, functioning as detecting the spectrum hole for transmission. The sensing information is used to make the spectrum decision. Reconfiguration may occur if the licensed user appears, and the operation parameter (such as frequency, power and modulation) must be changed to adapt to the new operating spectrum.

4.1.2 Link layer in cognitive radio networks

Link layer frames the data and regulate the access to physical resources. There are multiple differences of link layer between the conventional wireless network and cognitive radio network. First, the characteristic of communication channels are different. In conventional networks, the users have fixed channels to use according to their protocols. On the contrary, in cognitive radio networks the channels are not fixed and may exist anywhere in the whole spectrum due to accessing spectrum dynamically. Another difference is that cognitive radio users always utilize multiple channels to transmit data simultaneously in order to increase the throughput. Therefore, the complexity of management is introduced to the link as the same time, when much bandwidth is offered to the data transmission. MAC (media access control) scheduling becomes an important issue to maintain the channel's utilization and avoid the data collision. Scheduling models are usually designed to facilitate analyzing the network performance. For example, in [14], a scheduling model is proposed, which introduce hybrid priority dynamic policy for cognitive radio networks.

4.1.3 Network layer in cognitive radio networks

The Network layer takes charge of routing, and cognitive radio network makes the routing scheme more complicated. In conventional networks, the paths are designed directly by the router. The data is transmitted from the source and delivered to the destination along the designed path in the network. However, it is different in cognitive radio networks. Since the spectrum can be accessed openly, reconfiguration information greatly influences the routing scheme. In cognitive radio networks, the availability of the spectrum directly affects the performance of the communication. Existing solutions for the routing problem are presented in [3], where a cross layer solution is proposed to make the transmission more efficient. It suggests that, instead of router's direct decision, the routing algorithm and spectrum management should be considered together to make decisions for the channel scheduling.

4.1.4 Transport layer in cognitive radio networks

The transport layer is mainly responsible for flow control, error control, and congestion control. UDP (User Datagram protocol) and TCP (Transport Control Protocol) are two main protocols at the transport layer. However, the current transport layer protocol needs changing to adapt to cognitive radio networks. There are two important factors involved in transport layer control: the round trip time and packet loss probability. Similarly, these factors are influenced by the characteristics in cognitive radio networks, such as spectrum accessing technology, operating frequency, interference level and available bandwidth. For example, it may take some time for certain transmission changing from one channel to another, since reconfiguration happens in cognitive radio network. Conventional protocol for transmission of fixed channel may be not appropriate for certain application conditions

in cognitive radio networks. Hence, new transport protocols still need to be designed to adapt to these changing.

4.2 Protection based layer considering different protocol layers

Table 1. Jamming attacks at physical layer

Type	description
Intentional jamming	Malicious user keeps using licensed bands by transmitting high power signals.
Overlapping unlicensed user	Malicious transmission in one network will impact on other coexisting networks.
Asynchronous sensing	The selfish user does not obey the rule of synchronous spectrum sensing.

The following section analyzes how to defend the security system in different protocol layers according to cognitive radio characteristics [8], [10], [11], [15].

4.2.1 Defending in physical layer

As we know, physical layer is in charge of how to send and receive the signal through the radio interface. The physical layer in cognitive radio networks is more complex than a general one because it can transmit on various frequencies across a wide frequency spectrum [11].

Jamming message attack often occurs in this protocol layer, which disrupts the wireless communication by transmitting arbitrary messages maliciously. There are some attacks which especially target on physical layer of cognitive radio networks [11], which are outlined in Table 1. The critical point for preventing jamming attacks is to get the location information of the signal's transmitter, because the location information may be helpful to determine whether there appears a licensed user. This will be especially useful in the certain cases that the licensed user has a fixed location such as a TV tower [9]. At present, there are two schemes for this situation: distance ratio test (DRT) and distance difference test (DDT) [9].

4.2.2 Defending in link layer

Link layer functions as transferring packet from one node to the other. It provides services of error correction, framing data, and modulation. Some attacks may happen in link layer of cognitive radio networks [11], which are described in Table 2.

4.2.3 Defending in network layer

Routing table is made at the network layer, offering the path through which a message can achieve to its receiver. It is vulnerable for routing table since there is a long distance between source and destination. Any attacker can pretend to be the next hop node for the message if it can access to the routing table and change its contents. As a result, other nodes transmit their packets to the masquerade node by following the routing table's indication.

The masquerade node is called a hole. "Black hole" is used to denote the attacker who received the packets and drop all of them; "Gray hole" is used to denote the attacker who drops parts of the packets avoiding being detected; "worm hole" attacks the network by two nodes working together. "Worm hole" is the most dangerous one since two nodes keep private connection each other, luring other nodes to believe there is a real path. It is difficult to detect these attacks in multiple-hop networks. Cryptography is currently used to encrypt the routing information and use authentication to ensure the data's integrity and the node's identity.

Table 2. Attacks at link layer

Type	description
Biased Utility Attack	Selfish user changes utility function parameters to get more bandwidths, so the bandwidths of other unlicensed users are decreased.
False Feedback Attack	Malicious user hides the truth about the occurrence of licensed users, and other nodes cannot sense the information due to signal fading or long distance.

4.2.4 Defending in transport layer

At the transport layer, key depletion attack may be the main attack. Malicious users utilize the probability of session key repetitions to break the cipher system. Since reconfiguration happens frequently in cognitive radio network, considerable number of sessions will initiate higher number cryptographic keys for each session compared to conventional wireless network. Vast quantities of session keys needed in cognitive radio networks are vulnerable to the key depletion attack.

4.2.5 Defending in application layer

Application layer is the highest layer in cognitive radio networks. It serves for users by many applications. Any attacks in lower layers (physical layer, link layer, network layer and transport layer) will directly impact the quality of applications. Hence, defending in application layer is also necessary in cognitive radio networks.

4.3 Detection based layer considering different protocol layers

In the following section, intrusion detection is analyzed in different protocol layers according to the characteristic of cognitive radio networks [8], [10], [11], [15].

4.3.1 Intrusion detection in physical layer

The signal strength is an important factor since the value has relationship with the distance in wireless medium. Since RSSI (Received signal strength indicator) value has strong relationship with the location of the emitter [16], it may be used in the intrusion detection system. If the value is in a different range, the data packet with this value will be noticed; also the sender is monitored. If it is detected as an intrusion, alert messages will be sent out to the system.

4.3.2 Intrusion detection in link layer

At the link layer, MAC (Media Access Control) address is monitored during the data transmission. Each channel has its own schedule, such as what kind of the time slot it can transmit. If a user does not follow the schedule, further observation on its activity should be given. Also, the average packet rate is another factor to monitor, because that attacks at the link layer is often out of the intention of using the bandwidth more than others. If the packet rate of some user is obviously higher than others and keeping for long period, there might be some abnormality.

4.3.3 *Intrusion detection in network layer*

At the network layer, certain factors may be monitored, such as identity of the neighbor and whether the neighbor has passed the exact packet through the path. In [17], an idea of watch dog is used to monitor the data packet passing through the routing path.

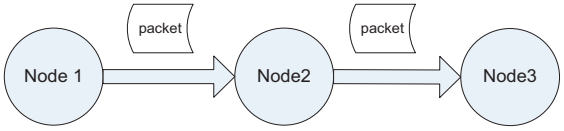

Figure 3. Normal activity at network layer.

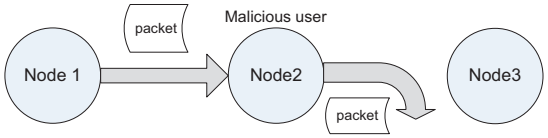

Figure 4. Abnormal activity at network layer.

Although this scheme is proposed in wireless sensor network, it might be applicable in cognitive radio networks. As shown in Figure 3 and 4, node 1, 2 and 3 are in the path. The packet is passed from node 1 to node 2, and then to node 3. If the node 2 is an attacker, it will drop or change the packet after receiving it from node 1. Then the node 3 will never get the packet or get a altered packet. The watch dog is used to buffer the packet from node 1 and compare it with the packet received by node 3. If there is difference or the node 3 did not receive the packet, it is believed as an abnormal activity, and alert messages will be sent.

4.3.4 *Intrusion detection in transport layer*

In transport layer, retransmission times and round trip time are two important factors to be monitored [11]. If retransmissions happen frequently more than usual or the round trip time often beyond an average range, more attention should be paid. Although there are many factors capable of affecting the performance of the transmission, security factor may be excluded at first time.

4.3.5 *Intrusion detection in application layer*

Intrusion detection in application layer is more flexible. It can be carried out by monitoring multiple protocol layers, since every protocol layer can influence each other.

5. CONCLUSION AND FUTURE WORK

The paper presents a survey on security in cognitive radio networks. Differences between cognitive radio networks and conventional wireless networks are analyzed in terms of each protocol layers. Challenging problems are outlined due to the characteristic of accessing spectrum dynamically in cognitive radio networks. We focus on analyzing the security system based on protection and detection at the macroscopic level. First, general security problems are analyzed in wireless networks because wireless media is the common characteristic in cognitive radio networks. Then, security problems, especially relative to cognitive radio network, are discussed. We investigate both attack defense and intrusion detection in cognitive radio networks in different protocol layers. Based on these, further study can be focused on specific security protocols, and on intrusion detection schemes in cognitive radio networks.

6. REFERENCES

[1] G. Staple and K. Werbach, “The End of Spectrum Scarcity,” IEEE Spectrum, vol. 41, no. 3, Mar. 2004, pp.48–52.

[2] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 23, NO. 2, FEBRUARY 2005.

[3] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohantly, ”Next generation/ dynamic spectrum access/cognitivw radio wireless network: a survey,” Elsevier Computer Networks, vol. 50, pp. 2127-2159, Sept.2006.

[4] J. L. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," CrownCom 2008. 3rd international Conference on , vol., no., pp.1-7, 15-17 May.

[5] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "A Survey on Spectrum Management in Cognitive Radio Networks," IEEE Communications Magazine, vol. 46, pp. 40-80, April 2008.

[6] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," 2008, Communications. ICC '08. IEEE International Conference.

[7] A. Naveed and S. S. Kanhere, “Security Vulnerabilities in Channel Assignment of Multi-Radio Multi-Channel Wireless Mesh Networks,” 2006, IEEE GLOBECOM 2006.

[8] L. Buttyan, J.Hubaus, Security and Cooperation in wireless Networks, Cambridge University Press, 2008.

[9] R. Chen, J. Park, Y. Hou, and J. H. Reed, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE Communications Magazine, vol. 46, pp. 50-55, April 2008.

[10] R. K. Nichols, P. C. Lekkas, Wireless security: models, threats, and solutions, McGraw-Hill Professional, 2001.

[11] Q. H. Mahmoud, Cognitive Networks, Wiley-Interscience, 2007.

[12] P. E. ABI-CHAR, A. MHAMED, and B. EL-HASSAN, "A Secure Authenticated Key Agreement Protocol for Wireless Security," Third International Symposium on Information Assurance and Security, 2007.

[13] P. Techateerawat, A. Jennings, “Adaptive Intrusion Detection in Wireless Sensor Networks”, 2007 International Conference on Intelligent Pervasive Computing.

[14] P.Zhu, J.Li and X.Wang, "Scheduling Model for Cognitive Radio," CrownCom 2008. 3rd International Conference.

[15] Q. H. Mahmoud, Cognitive Networks: Towards Self-Aware Networks, 2007, Wiley.

[16] Nekovee, M. B. Res, Suffolk, "Impact of Cognitive Radio on Future Management of Spectrum", CrownCom, 2008.

[17] R. Roman, J. Zhou and J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks", CCNC 2006. 3rd IEEE.