Cognitive Radio Network Security- A Survey

Roshan Singh Thakur
ABHA GAIKWAD-PATIL
College of Engineering,Nagpur

Prof. Parul Bhanarkar
ABHA GAIKWAD-PATIL
College of Engineering,Nagpur

Prof. Girish Agarwal
ABHA GAIKWAD-PATIL
College of Engineering,Nagpur

Abstract

In this paper we analysis the state of the art in CR system and determine its key functions, such as spectrum sensing, resource allocation, CR MAC protocol, spectrum-aware routing, CR transport protocol, QoS awareness, spectrum trading, and security. We also study the various schemes suggested for each of these functions and discuss the suitability, advantages, and limitations of their usage in the future. This paper also gives a detail analysis on the security problems faced in cognitive radio network, and introduces the basic issues about cognitive radio network. We also discuss about the differences between cognitive radio network and existing wireless network.

Keywords: Spectrum Access; Cognitive Radio Network; Network Security: state of art

1 INTRODUCTION

Cognitive radio (CR) is a new approach of sensing and utilizing wireless spectrum resources. CR is a reconfigurable radio that can adapt its operating parameters to the surrounding environment, which has been made possible by recent advances such as software-defined radio (SDR) and smart antennas. Using such CR devices enables flexible and quick access to the wireless spectrum, which can, in turn, improve efficiency in spectrum utilization.

Spectrum is a one of limited resources in the present spectrum management. It seems effectively use of spectrum resource in wireless communication technology. In different countries, different spectrum is assigned to radio. The distribution of this spectrum is already authorized. The authorized frequency band spectrum resources have employed a large part, but many authorized spectrum is empty. The research by federal communications commission (FCC) [6] proposed that the average frequency of authorized spectrum is between 15% and 85% in different time and area. On the other hand, the open use of unauthorized frequency spectrum resources employed small portion of the band. Static spectrum allocation is the main reason that causes the less utilization of frequency band. If we can use the empty spectrum resource temporarily, the problem of lack of spectrum resources will be arising. Cognitive Radio (CR) is use to solve this problem efficiently.

2. OVERVIEW ON COGNITIVE RADIO

The concept of cognitive radio is exposed by Joseph Mitola's in 1999. Its idea is that the CR has capability to communicate with the surrounding environment so as to recognize the available spectrum in the space, limit and reduce the problematic incidents. The most representative definitions were presented by the U.S. federal communications commission (FCC) [7] and a famous prof. 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. In signal processing, Simon Haykin thought CR is an intelligent wireless communication system. It can recognize 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 [3].

3. STATE OF ART OF CR'S

The essential for CR is the acceptance of the spectrum, that is, the network should be divided into Primary users (authorized users) and secondary users (un-authorized users). On the basis of the spectrum openness, secondary users can find out the idle spectrum by detecting spectrum channel which the Primary users don't use right now, and make full use to access frequency band without impact on the primary user communication. This requires secondary users with the ability of the real-time detection for spectrum channel, having the following three characteristics:

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.

Through the continuing efforts of spectrum regulators (e.g., the FCC in the United States and the Office of Communications [Ofcom] in the United Kingdom) and the research community, CR will soon be applied to the TV white spaces (TVWS) through which it is expected to moderate the spectrum shortage problem[4].

3.1. ARCHITECTURE OF CR

The CR architecture can be explore in the framework of the standard open systems interconnection (OSI) model, as shown in Fig. 1. In the physical (PHY) and link layers, *spectrum sensing* plays an important role in discovering spectrum WS as well as protecting PU's where PHY sensing employs various signal detection methods, such as energy and feature detection, and medium access control (MAC) sensing improves the primary signal detection performance by:

• Occupying multiple sensors (i.e., cooperative sensing), to exploit location multiplicity of sensors.

• To perform sensing multiple times (i.e., sensing scheduling), to exploit temporal multiplicity in received primary signal strengths.

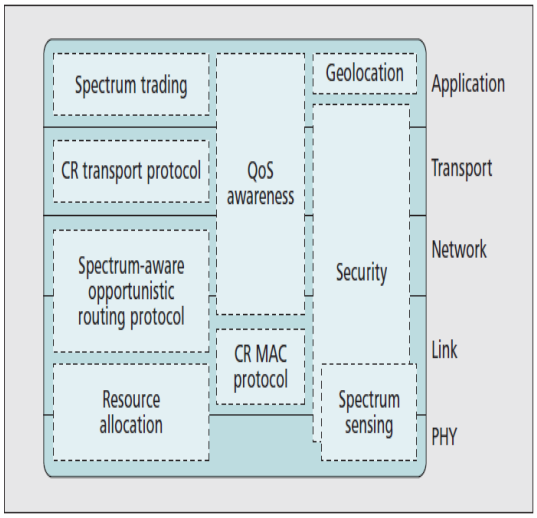

Fig1. *The architecture of CR in the layered model.[3]*

3.2. RESOURCE ALLOCATION AND CR MAC PROTOCOL

A DSA network should be aware and adapt to fluctuating spectrum, and be able to manage such time-varying spectrum resources .A dynamic channel selection and switching in CR devices require strong coupling between the PHY and link layers.

In the link and network layers, *spectrum aware opportunistic routing* manages CR-based routing in a multihop environment via cross layer interactions of link and network layers such that the best route can be examined by considering the hop-by-hop spectrum availability. In the transport layer, the *CR transport protocol* is designed to improve traditional transport protocols such as TCP/IP so that the impact of spectrum availability can be assumed for. This can be either by designing completely new transport protocols or through new management techniques of existing transport protocols. In the application layer, *spectrum trading* is concerned with the transfer of dynamic spectrum usage between PU's and SU's. Finally, *quality of service (QoS) awareness* and *security* are also inherent CR functions that span over multiple layers, where the former provides solutions to spectrum-aware QoS provisioning, and the latter protects PUs and SUs from various various threats that can disrupt efficient operation of core CR functions, such as spectrum sensing.

3.3. IEEE 802.22

The IEEE 802.22 WRAN is an infrastructure cellular network where the BS covers an area of radius 30 km (typical) to 100 km. The WRAN end user is referred to as CPE whose transceivers are installed. An IEEE 802.22 is provided in Fig.2. The WRAN is designed to provide throughput of 1.5 Mb/s in the downstream and 384 kb/s in the upstream, and its PHY utilizes OFDM modulation to overcome possibly excessive delays in a wide coverage area. In addition, it provides PU protection such as spectrum sensing and a geolocation database for PU-SU coexistence, and also supports self-coexistence between WRANs via the Coexistence Beacon Protocol (CBP). IEEE 802.22 is the first international CR standard, so it can become a touchstone for the potential of CR technology.

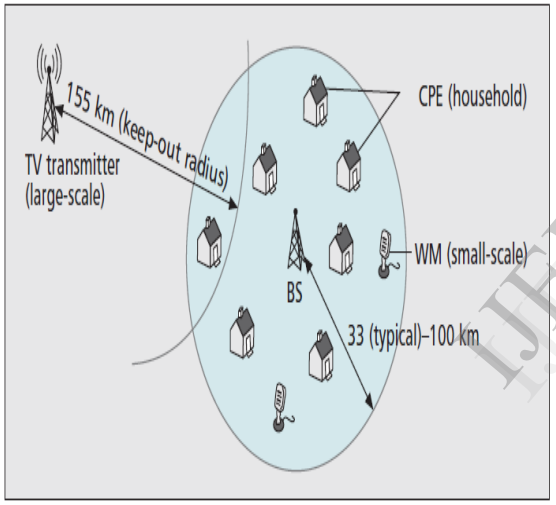

Fig 3. *An illustration of the IEEE 802.22 network.[3]*

3.4. STANDARDS OF CR'S

We categorize them into *SU-SU coexistence* and *PU-SU cooperation*. To deal with such a situation, there are two standards: IEEE 802.19 and IEEE SCC 41. IEEE 802.19 deals with coexistence between unlicensed wireless networks, such as 802.11, 802.15, 802.16, and 802.22. On the other hand, IEEE SCC 41, previously known as IEEE 1900, defines higher-layer standards for DSA networks in the layers higher than MAC and PHY. To development of the secondary wireless network, the traditional network may provide some fraction of their spectrum on a payment basis for DSA.

4. COGNITIVE RADIO NETWORK SECURITIES

In order to solve how to detect free bands and use them, people use dynamic spectrum access technology. Through the Spectrum Sensing to free band algorithm, secondary users can make full use of spectrum resources by no impact on the Primary users' communications. Cognitive radio network is a wireless communication technology; it has not only the traditional security problems, but also some new hidden security. Like there're many steps in the process of spectrum access, such as Spectrum Sensing, spectrum management, spectrum migration and spectrum sharing. Each process exits security problem.

4.1 TRADITIONAL WIRELESS NETWORK SECURITY

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

In wireless communication, all of the information is transmitted by wireless channel. In cable channel, it is 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 breaking information to users will bring economic and honorary loss, also including leaking user's privacy.

Wireless wiretapping is widely exiting in the wireless network, and the solution at present is to transmit information by encryption. An encryption is applied in the variety of the information transmission. The protection method can transmit information efficiently, but along with the rapid development of computer hardware technology, using a single key encryption transmission has the possibility of violence breaking. Therefore, it needs to improve the encryption algorithm strength, in order to take measures to security against the key risk.

4.2 FAKE ATTACK

In wireless communication, the terminal and the base station does not have physical cable connection. The authorized information exchange between terminal and base station is achieved by the radio channel. The authorized information is

related to the network control, network services and network access, etc. Due to this radio channel, attacker may get authorized information through the wiretapping on a radio channel. When the attacker gets an authentic user's identity, we can use the authorized 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 authentic users by intercepting the authorize information, attackers can use communication services without paying network service charge. By using base station devise, attackers may mislead the end user, to gain more users' identity information.

4.3 INFORMATION TAMPERING

Information tampering means the attacker taps into the appropriate information and revises them before passing them to the original information, including information delete, replace and modify. Information tampering usually occur 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 unnecessary loss to user.

4.4 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 relevant 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.

4.5 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 jam 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 ex-ample, 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.

4.6 THREAT OF DYNAMIC SPECTRUM ACCESS

Dynamic spectrum access is a Spectrum Sensing, spectrum management and spectrum migration, where there exits unsafely 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, etc. The following section will analyze the existing safety problems in cognitive radio system from the aspects of dynamic Spectrum Sensing.

[a]. PRIMARY USER EMULATION ATTACK

Primary User Emulation (PUE) attack is one of security problems that physical layer facing, which has great threat to Spectrum Sensing. The attacker sends CR signal by reflecting the primary user's signal characteristic. In the Dynamic Spectrum Access (DSA), the primary user can utilize the authorized frequency band free, the authorized frequency band turns into idle state when the primary user releases the resources, so the secondary users can attempt to access. One necessary condition is the secondary users must be able to distinguish the existence of free frequency band. Hence, it demands Spectrum Sensing algorithm to carry out real-time attention for spectrum state by detection devices. At this time the attacker creates similar signal as the primary user does to cause an error frequency spectrum, which lead secondary users to make misleads 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.

[b]. DATA TAMPER ATTACK OF SPECTRUM SENSING

In the 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 **Fig 3**[3]. In order to improve the efficiency of

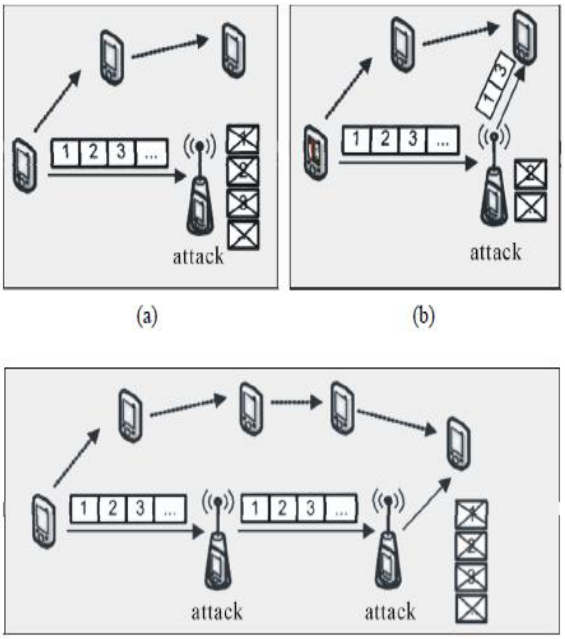

Fig3 . Data tamper attack of spectrum sensing. [3]

perception, the literature used the Spectrum Sensing, effectively improved the efficiency of the Spectrum Sensing. [3]

5. CONCLUSION

In present, cognitive radio technology has developed 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. It is the core idea that the wireless communication devise has the ability to find spectrum channel and utilize them. By cognitive radio technology, it invents a new way to solve the problem from the growing demands of wireless communication and the limited wireless spectrum resource problem. There is a use of many methods to improve perception efficiency. Some security mechanism has been introduced in further research. The key research direction in future is to settle the questions encountered in the design of safety across the network layer and physical layer

References

[1] M. McHenry, "NSF Spectrum Occupancy Measurements Project Summary," Shared Spectrum Company Report, *Aug. 2005*; http://www.sharedspectrum.com/measurements.

[2] M. McHenry *et al.*, "Chicago Spectrum Occupancy Measurements & Analysis and A Long-Term Studies Proposal," *Proc. ACM TAPAS*, Aug. 2006.

[3] Research and Analysis on Cognitive Radio Network Security Long Tang1, Juebo Wu2 1State Key Laboratory of Software Engineering, Wuhan University, Wuhan, China ***Wireless Sensor Network*, 2012, 4, 120-126** doi:10.4236/wsn.2012.44017 Published Online April 2012 (http://www.SciRP.org/journal/wsn)

[4] Cognitive Radios For Dynamic Spectrum Access: From Concept To Reality Kang G. Shin, Hyoil Kim, Alexander W. Min, And Ashwini Kumar,University Of Michigan**,** *1536-1284/10/$25.00 © 2010 IEEE IEEE Wireless Communications • December 2010*

[5] J. Mitola and G. Q. Maguire, "Cognitive Radio: MakingSoftware Radios More Personal," *IEEE Pers. Commun.*,vol. 6, no. 4, Aug. 1999, pp. 13–18.

[6] FCC, "Notice of Proposed Rulemaking," *ET Docket No.00-402, Nov. 2000.*

[7] FCC, "Notice of Proposed Rulemaking," *ET Docket No.04-113, May 2004.*

[8] IEEE 802.22 Working Group on Wireless Regional Area Networks; http://www.ieee802.org/22/.

[9] J. Wang *et al.*, "First Cognitive Radio Networking Standard for Personal/Portable Devices in TV White Spaces," *Proc. IEEE DySPAN*, Apr. 2010.

[10] "Standard ECMA-392: MAC and PHY for Operation in TV White Space," Dec. 2009; http://www.ecmainternational.org/publications/standards/Ecma-392.htm.

[11] R. Kennedy and P. Ecclesine, "IEEE P802.11af Tutorial,"IEEE 802.11-10/0742r0, July 2010; https://mentor.ieee.org/802.11/dcn/10/11-10-0742-00-0000-p802-11af-tutorial.ppt.

[12] Y. Zeng and Y.-C. Liang, "Covariance Based SignalDetections for Cognitive Radio," *Proc. IEEE DySPAN*,Apr. 2007.