Enhancement of Security in Cognitive Radio Network

Nouman Maqbool Rao[1], Rao Zeeshan Maqbool[2] and Rao Imran Maqbool[3]

[1]Higher Education Commission Islamabad Pakistan
[2]Oman Telecom, Muscat, Oman
[3]Dascon Engineering Lahore, Pakistan

Abstract – *Reference to the latest developments the spectrum shortage problems are because of the wireless communication. For the future networks the most practical, scientific and systematic challenges is the use of licensed or unlicensed wireless networks with opportunistic use of the spectrum with, without and limited rules. Since different wireless networks are using different frequency bands. So there is a need to use lessening bands when there is no activity on them. Cognitive radio is a new technology which leads to solve these problems through dynamically utilization of rules and spectrum. Several spectrum sharing schemes have been proposed. Now a day's security in cognitive radio network becomes a major and challenging issue, and chances are prearranged to the attackers in cognitive radio technology as compared to the wireless networks in a general form. In cognitive radio, mobile station equipment may switch to any available frequency band, as it makes a list of available free channel and make handoff decision accordingly. So whenever handoff is made whether soft or hard there will be a chance that malicious attacker may hack ongoing traffic or he may even interrupt established traffic by imitating any kind of passive or active attack like interception, spoofing denial of service etc. This paper explore the key challenges to provide security in cognitive radio networks, and discusses the current security carriage of emerging IEEE 802.22 cognitive radio typical and recognizes security threats and vulnerabilities along with the countermeasures and solutions.*

Key Words— *Cognitive Radio, IEEE 802.22, Security Threats, Sensing*

1. Introduction

Communication is growing changing and increasing subscriber base. The occurrence of high data throughput application continue to increase the fast growing request for broadband wireless service these have led to the expansion of several wireless technologies which continuously grow with ever-increasing competencies. Under licensed frequency band IEEE has offered multiple standards. While 802.16a/d/e and 802.20 have focused on providing the necessary infrastructure to create wireless metropolitan area networks (MAN) which has the radius of approximately 1km to 5 kms, 802.22 is pursuing to define a standard Capable of serving vast regions up to 100km in size [14]. Frequency band of unlicensed frequency is being utilized by using IEEE 802.22. A typical working group (WG) is working to finalize the standard of 802.22 after the Federal Communication Commission (FCC), which passed the resolution. 802.22 is also called wireless radio area network (WRAN) or cognitive radio network (CRN) by IEEE [13].

Most of the radio function as a software base that run on microprocessor and programmable electronic devices. These technology is referred to software define radio (SDR). Cognitive Radio (CR) is further enhance as compared to SDR by employing software for measurement of the vacant portion of the wireless spectrum which is already there and operate that spectrum in a way that bound the interfering with other devices [11]. In dynamic spectrum Access (DSA) licensed; user is stated to be as a primary / key user or occupants. The user who didn't have any licensed that got the permission for spectrum opportunistically are referred to as secondary user [4].

If we compared with the typical radio networks, Cognitive Radio (CR) is more flexible and exposed to wireless network. Therefore more threats and vulnerabilities found then traditional radio environment. For example CR first senses the spectrum which is scanning a certain range of the spectrum to identify unoccupied range / spectrum. During this methodology the secondary user can determine that which spectrum can be used either radio or not. When the result of spectrum sensing in altered maliciously network activities which are normal will be disabled, even whole traffic may be broken down. [3] [7] CR is the main technique which realizes DSA policy

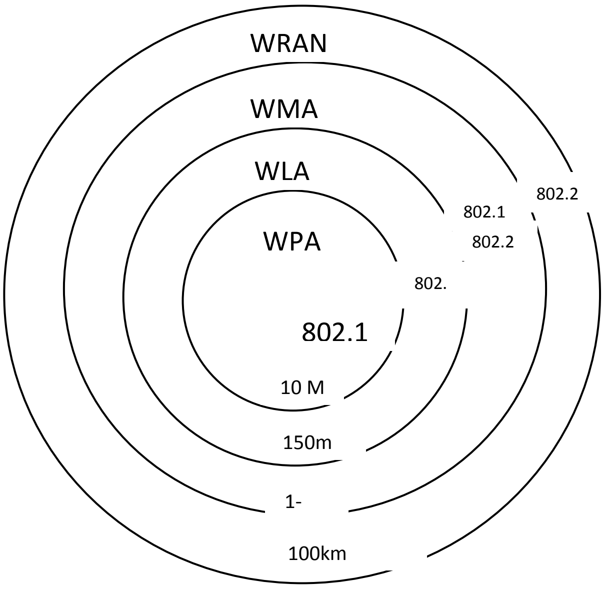

Fig. 1: Categorization of the various

The composition of this research paper is as follows. Under section II Cognitive Radio Architecture is reviewed. In III Security overview is presented. In section IV security threats and vulnerabilities are focused. In section V literature review will be discuss. In section VI countermeasures and solutions are describe. In section VII conclusion and future work is given.

2. Cognitive Radio Architectures

Basic component of the cognitive radio is shown in figure II. The operating system (OS) characterizes the higher-layer communication; Operating system can generate and receives the traffic information. The sensing component measures the parameter of the radio atmosphere and transforms the parameters to the cognitive engine. The cognitive engine than combine the information received from sensor and with policy information to make an appropriate decision about how and when it will transfer / communicate by using the radio transmitter and receiver. Some Cognitive Radios (CRs) also depend on information of transmitter location which is provided by a geo locater.

Cognitive Radios could be broadly categorized into one of three network architectures which is as shown in Fig. III. They could range with reference to architectures which include all the six components in one single non-cooperating device to networked architectures where none of the CR components may be co-located with each other. This architecture includes multiple examples of each module. Further to this there are many distributed CRs which may select to share the information such as measurements, location, or policy in order to make more knowledgeable and synchronized communication decisions. In the cognitive engine, the other CRs are effectively sensing, geo-location, or communication extensions. [3] [11].

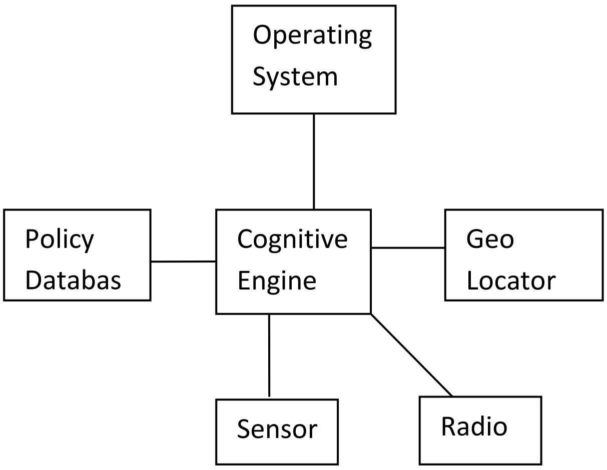

Fig. II: Cognitive Radio Component [11]

The security vulnerabilities will be occurred when any cognitive radio components are not synchronized with each other.

3. Security Overview

Cognitive Radio itself is a broader term with many potential senses. Whereas the security requirements may be different with application environment; usually there are some common requirements providing basic safety controls like cognitive radio networks. For which the security requirements are the same as in a general wireless networks because of the nature of operating on wireless media. These security requirements are outlined below. [9]

3.1. **Access Control:** The transmission of information from an object to a subject is called access. Control of access to a resource is one of the major objectives of security. Access control addresses more than just controlling which users can access which files or services. The relationships between subjects and objects are generally covered under the term of Access Control.

3.2. **Confidentiality:** Confidentiality is defined by the International Organization of Standardization (OSI). Confidentiality involves by make it sure that each part of a system is appropriately secured and Accessible only by subjects who need it.

3.3. **Authentication:** It is a process of verifying or testing that the demanded identity is valid. Authentication requires that the subject provide additional information that must exactly correspond to the identity mentioned. In this regard Password is the most common form of authentication.

3.4. **Integrity:** Integrity it offers a high level of assurance that the data, objects, and resources are unaltered from their original protected state. This includes alterations occurring while the object is in storage, in transit, or in process.

There is multiple consideration factors when the security is implemented in cognitive radio network due to the nature of CR communication, such as the flexible utilization of frequency range / spectrum and the appearances of different licensed user is unscheduled. So the additional special security issues need to be considered especially. For example it will be more difficult to authenticate the identity of the licensed user at present there are still not completed and the final solution to solve the security problems bought by CRN [3].

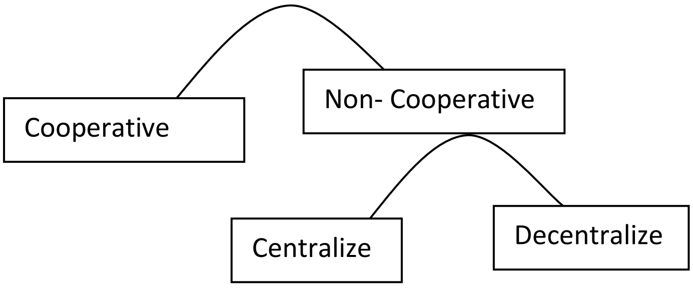

Fig. III: Cognitive Radio Network

4. Security Threats & Vulnerabilities

4.1 Rogue Base Station Attack

The attackers lie in the center of the Base Station Offer (BSO) and Base Station Renter (BSR). The attacker could take off himself as an occupant and can send back a resource return message to the offer. In the same way the attacker could pose as offer and request for resource allocation. Attacker can generate the BS-IDs and can forge the network. Attacker can get BS-IDs and negotiated channels between the offer and renter at the time of resource sharing. The attacker abuses this information and sends bogus messages [5]

4.2 Replay Attack

The attacker can capture the packet and resend these packets maliciously after passing some delay for mismanagement of the network characteristic & resources. Attacker can retransmit the packet after certain time to cause DoS [5] [8].

4.3 The Motivation of Attacks

The motivation of attack in cognitive radio network are classifies into four types [6] [9].

Selfish Attack: The attacker can access the spectrum with high priority. He occupies the spectrum resource as he wants.

Malicious Attack: The opponent slows down the unlicensed user from spectrum usage and caused denial of services (DoS).

Cheat Attack: The attacker increase his effectiveness function as well as at the same time decrease contestant's profit.

Misbehaving: CR didn't follow any general rule for sensing and managing of range of the spectrum.

4.4 Denial of Service (DoS)

During the period of sensing any attacker / hacker can flood the spectrum with inconsistent data to show off that the range is unavailable for the same because of this the sensing during is the most vulnerable to DoS. The major objective of DoS attack is to put the burden on the resources and to stop the utilization of the resources for the nodes which are also present in the network [7] [8].

4.5 Incumbent Emulation (IE) Attacks

Under the Incumbent Emulation the user tried to get the priority on the other secondaries by sending signals which could help to emulate the features of an incumbent. The impact of Incumbent Emulation attack is the genuine secondary's abilities for differentiate the signals of attacker with the actual incumbent signals during the sensing period [4] [8].

4.6 Spectrum Sensing Data Falsification (SSDF) Attacks

The hacker can spoof or mask primary user and transmit incorrect spectrum deduct sensing outcomes to a data collector, which is a major source of incorrect spectrum detection decision taken by the data collector [3] [4].

4.7 Policy Radio Threats

This is artificial intelligence (AI) threat comes by two aspect absence of any policy as well as the failure while a policy is being used. The attacker can block the policy or jam the radio which announces the policies or Attacker can modify policy or implement false policies which are in his favor [3] [10].

4.8 Learning Radio Threats

In this AI threat CR can be mature from the past experience as well as with the current situation to predict and assume the future environment and to identify the optimum processes. Attacker can change and alter the past statistics of a network for impact of the CR prediction efficiency. [3] [10].

4.9 Parameters Threats

By using different parameters Cognitive Radio has to control the operation and assess its performance. There is mixture of characteristics for these types of functions. Some parameters are used to estimate the performance of CR as well as the weigh. Attacker can alter these characteristics which can be a reason for sub-optimal for the CR along with wrong operation [3][10].

4.10 Spectrum Management Threats

The function of spectrum organization is categorized as analysis and decision. Threat here comes from the possibility of incorrect parameters which affects the result for spectrum decision and analysis. CR may select wrong spectrum as a result the communication performance within a network may be damage [3] [10].

4.11 Common Control Channel (CCC) Attacks

The successful jamming may stop or delay communication across a large frequency range in this regard the DoS attacks are the target for the Common Control Channels. [11].

4.12 Transmitter / Receiver Failures

The attacker could get the control on the transmitter and can restrict to practice of an attack that is possible with any radio network to send as well as restrict with the licensed users of the Radio Network. This is also open the probability for the Sybil attack whenever it transmits the radio by using multiple characteristics, out of those some behaves while some others are misbehave [11].

4.13 Spurious Transmissions in QPs

The attacker can post any threat by using 802.22 as a fake transmission which ultimately results as a congestion in quiet periods (QPs). The opposite party can be interfere by multiple co-occurrence approved during the Quiet Periods which relates to the controlled procedures and he cause hardware or software defects [8].

5. Literature Review

[1] Discuss the idea of cognitive radio network by J. Mitola from software define radio (SDR) which is originally considered to improve the spectrum utilization. CR is an intelligent communication system which is aware of the environment. CR completes two major objectives which are extremely trustworthy communication when and wherever needed and effective operation of the radio spectrum. Paper discuss major three type of network architecture in CR. 1-Infrastructure, 2- Add-hoc and 3- Mesh architectures.

The author use pictorial diagram which helps the reader to easily understand the topics the paper describes. Paper used vast referencing in his paper. This paper cannot complete the whole architecture of cognitive radio network. More work related to CRN is pending.

In [2] author of the paper said that network layer can use to integrate MAC's and PHY layer for better service. And it discusses the mathematical framework for routing trust in CRN. Network layer structure can provide better service in MAC and PHYs and it integrate transport and application layer. Paper discusses the location management handoff management, security attacks and misbehaviour and security services. Papers discuss the security service which is provided in CRN. For all those services of security deliver the security enable environment as compare to malicious threats and trouble sameness. In this paper author used best and updated referencing. Paper used mathematical preposition in trust CRN. Author cannot simulate to his mathematical propositions. And cannot propose any countermeasure against malicious attack and misbehaviours.

The security threats in CR/CRN as discussed in [3]. The attacks are artificial intelligence behavior threats and dynamic spectrum access threats. Author Use the best referencing in his short paper. Paper is categorized and arrange in the appropriate manner. Author of this paper use mathematical notation. Author cannot propose any model to prove his point of view. The countermeasure of the attacks cannot discus.

The author of the paper [4] defends Incumbent emulation attack and SSDF attack. Two technique are used one is DRT which is distance Ratio Test while the second is DDT which is Distance Different Test to eliminate the IE attacks. Author use two levels in the first all native spectrums deducting result should be validated by the data receiver. Whereas second layer of protection is placement of data synthesis schemes which are strongly against attack of SSDF. The author use simulation result to prove his result and to prove his simulation the author use diagrams. No mathematical formula is used to prove his simulation.

Paper [5] discuss the potential attacks these attack are rouge base station attack and replay attacks to eliminate these attacks author proposed three solutions . These solutions are Time Stamp, Nonce, and Digital Signature. Most of the issues are discussed in detail along with appropriate proposed solution. The major weakness which was figured out is its limited vision in context of defining solution analysing criteria.

Paper [6] author describe the access point(AP) attack and misbehaviour and to encounter these attack and misbehaviour he proposed Locdef technique verifies that given signal is incumbent transmitter which estimates its location and signal individuality. So trust relationship is proposed to avoid unauthorized nodes attack to CR. Paper is categorized in good referencing. Paper discusses misbehaviour and attacks in detail tabular format which is easy to understand. Paper cannot fulfill the countermeasure of the Access Point misbehaving and Access Point attacks.

To eliminate the DOS attack flow control can be introduced [7] at MAC layer to validate the genuine nodes of the network during the channel compromise phase. In this phase no major authority or reliable outsider party is involved. The paper proposed a result to identify malicious node. Updated referencing is used in this paper. No Verification with its examination is discussed in this paper. No simulation work is done .The author point of view is very rare.

Paper [8] describe the security threat and it present two solutions which is Key management Infrastructure and Distributed key Management. Graphical Simulation and pictorial diagram used. Author cannot complete the arguments of Possible DoS Threats in Cognitive Radio Network and their Countermeasure

Author of the paper [9] discuss two approaches which is protection based layer considering different protocol layers and 2nd is detection based layer considering different protocol layers. Paper discusses protection and detection on different layer on more detail. Pictorial diagram can be used. No main security threats is discuss in this paper Countermeasures are not full filling the whole security parameters.

In [10] author describe the threats to CR and dynamic spectrum access threats and proposed Three Mitigation technique robust Sensory, Mitigation in Individual Radios and Mitigation in Network. The paper provides well background knowledge about the CR architecture and pictorial representation to clarify the security issues. Security threats and solutions are well defined, respectively. We did not found any significant weakness in the paper except the proven theory may be more validated by simulation in NS-2 or MatLab.

Paper [11] paper discuss 7 remedies against the failures they are negotiated supportive CR, CCC attacks, occupancy failures by spectrum, policy, location, sensor and by transmitter as well as receiver. Paper discuss the main security threats and as well their countermeasure. Different security can be followed against the attack. Author cannot prove his countermeasure with any model through simulation. No pictorial diagram is used in this paper.

6. Countermeasures & solutions

The countermeasure of Rogue Base Station and the return attack. For succeed on those declared attacks, our research paper [5] proposed three constraints or strategies to secure the sharing of network; which are Digital Signature, Nonce and Timestamp.

Time stamp help to prevent the replay attack. The mixture of data along with the time of dispatcher is the Time Stamp if these packets are newly generated then it is receive otherwise it is discarded.

In nonce repeat packet is discarded so DoS and replay attacks can be eliminated. Digital Signatures are used to validate the dispatcher and for recognize the alternation of received packet. Applying DS built verification of the dispatcher is actual to escape the above mention attacks.

In [6] author has proposed that LocDef arrangement authenticates either a given signal is that of an incumbent transmitter with the approximating of its position as well as detecting the signal features. LocDef could be helpful to remove or moderate some of the above-mentioned drawback. This scheme can eliminate the motivation of attacks.

Malicious nodes could be thrown the undesirable packets on the channels to halt this undesirable packets [7] discuss the impression of flow control which could be initiated at MAC level with the inclusion of time limitation. Receiver describes the monitoring of Time Interval (TI) that is why the sender is unable to transmit the data regularly. If sender spreads the data on the high rate and receiver is receiving packet regularly its means that the mentioned TI and the receiver identify the misconduct by one point / node which spread the information about malicious node.

The key point is to protecting beside IE threats is to develop any new technique which could able to handle these situations and for validating the genuineness of the incumbent signal. Paper [4] discusses the solution of IE attacks. One approach is a signature which is embedding in the incumbent signal. One more process is to work and verification procedure with incumbent transmitter and an authenticator. Two techniques are being used the first is DRT which is Distance Radio Test this use RSS which is received signal strength quantities gained from the location verifier (LV). Other technique is known as DDT which is distance difference test. This procedure is being used whenever the signals are being transmitted by a signal point to LVs, the virtual phase variance could be identified whenever the signal influences the two LVs because of opposing locations from the sender.

Two prevent SSDF attack paper [4] proposed two level of defense. The first phase of all native spectrum deducting result must be validated from data collector. The main objective is to avoid the return attacks of untruthful data inoculation by the objects outside the networks. Second phase of protection is placement of data synthesis arrangement that is forceful with compare to attacks of SSDF.

In case of policy attack paper [11] suggests that in cooperative policy can be freely exchanged and in non-cooperative nodes policy updates and renewals can require infrequent. Effective rules could be replaced freely and with self-assurance and kept for long time. It is difficult that attacker stops a CR even presence of some rules and regulations. Paper [10] elaborates that without the knowledge of policy attacker can use different funny and obvious techniques to suppose about policy. This comes into picture that the radio rule and regulations should be carefully check and validated to defend against the threats.

To improvement against learning, parameters and spectrum management threats paper [10] present a solution robust sensory input and mitigation in Network. In vigorous sensory the data entry educating sensor, input can be considerably in helping in reduction of the acceptance of CR. In scattered situation the network of CR can fuses sensor data to increase throughput. All sensor contribution would consider noisy with or without the occurrence of attackers, statistic can sometimes incorrect.

Author of the paper [11] defends against the common control channel use a robust coding of different spread spectrum. The schemes of the media access would be vigorous which could provide the fair access of data on the network. This fairness had to be brought around by the multiple layers and the simple access arrangements which should have focus on the control channels for which the need is preferable.

In Key management infrastructure the security sub layer didn’t resolve the issues of inter-cell key management. Whereas the sub layer comprises with PKM protocol, this protocol can handle the intra-cell solutions which didn’t allow the rations to care the administration of inter-cell solutions. The workable method for planning of inter-cell solution is to operate the backhaul substructure which would be able to interconnect many WRANs. These are linked for ACR via backhaul stations. If a common backhaul infrastructure amongst cells is not available the scattered significant organization system is required over there. For these types of arrangements 802.22 BSs helpfully operate a disseminated algorithm for inter-cell managements. Key management scheme is in two types; one is contributory while the other is distributive. Contributory group is well-defined for incorporate scheme as an output of joint struggle of different points / nodes. The distributive group contains arrangements there all important invents by one nodes [8].

Paper [11] discusses related arrangements, not reliable third party who is accountable for the generation and circulation of the cryptographic keys. And in the scattered arrangements all the nodes produces a unique key and issues it to the others nodes of the network.

In [9] author has proposed that Physical layer attacks. Jamming of signals can be prevented by spread spectrum scheme. Scrambling is another Physical layer attack that can be a countermeasure for monitoring and deducting of system anomalies. Second and secure is MAC layer that uses X.509 certificate for authentication mechanism between Mobile Station (MS) and BS. X.509 certificate holds the Public Key (PK) of MS.

Another attack which has been identified is rogue BS. Its countermeasure is done by joint verification at user-network level. Mutual Authentication can be performed after scanning, achievement of channel explanation as well as reaching and competence concession which are built on EAP with specific authentication method as EAP-Transport Layer Security [9].

7. Conclusion and future work

Cognitive radio introduces a new level of sophistication to wireless communication technology. Still CR procedures and methods are at the initial ages. Security is an important part in CR. Under this research paper we discussed in detailed a comprehensive variety of security attacks for IEEE 802.22. These threats and attacks on IEEE 802.22 can be potentially carriage a danger to the performance and sustainability of CR network. Literature review based on references material proposes CR facing bunch of threats. The security in spectrum sensing threats may be proposed in future work.

8. References

[1] K.-C Chen, Y.-J Peng, N. Parasad, Y.-C Liang, S. Sun “Cognitive Radio Network Architecture: Part I – General Structure” ACM 2008

[2] K.-C Chen, Y.-J Peng, N. Parasad, Y.-C Liang, S. Sun “Cognitive Radio Network Architecture: Part I I – Trusted Network Layer Structure” ACM 2008

[3] Yuan Zhang Gaochao Xu Xiaozhong Geng ” Security Threats in Cognitive Radio Networks” High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference.

[4] Ruiliang Chen Jung-Min Park Hou, Y.T. Reed, “Toward secure distributed spectrum sensing in cognitive radio networks” Communications Magazine, IEEE Publication.

[5] Shaukat, R. Khan, S.A. Ahmed, A. “Threats Identification and their Solution in Inter-Basestation Dynamic Resource Sharing IEE-802.22” IEEE International Conference on Convergence and Hybrid Information Technology 2008.

[6] Arkoulis, S. Kazatzopoulos, L. Delakouridis, C. Marias “Cognitive Spectrum and Its Security Issues” This paper appears in: Next Generation Mobile Applications, Services and

Technologies, 2008. NGMAST '08. The Second IEEE International Conference.

[7] Shaukat, R. Khan, S.A. Ahmed, A. "Augmented Security in IEEE 802.22 MAC layer Protocol" Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th IEEE International Conference.

[8] Kaigui Bian and Jung-Min "Security Vulnerabilities In IEEE 802.22" ACM 4th Annual International Conference on Wireless Internet

[9] Xueying Zhang, Cheng Li "The security in cognitive radio networks: a survey" ACM 2009 International Conference on Communications and Mobile Computing.

[10] Clancy, T.C. Goergen, N. "Security in Cognitive Radio Networks: Threats and Mitigation" Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd IEEE International Conference.

[11] Timothy X Brown, Amita Sethi "Potential Cognitive Radio Denial of Service Attack and Remedies"

[12] Cordeiro, C.; Challapali, K.; Birru, D.; Sai Shankar, N. "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios "New Frontiers in Dynamic Spectrum Access Networks, 2005 First IEEE International Symposium

[13] Krenik, W. Batra, A. "Cognitive radio techniques for wide area networks "Design Automation IEEE Conference, 2005.

[14] Justin Thiel "Metropolitan and Regional Wireless Networking: 802.16, 802.20 and 802.22"