Security Issues and Threats in Cognitive Radio Networks

Yenumula B. Reddy
Department of Computer Science, Grambling State University
Grambling, Louisiana, USA
ybreddy@gram.edu

Abstract—**Cognitive radio technology is the vision of pervasive wireless communications that improves the spectrum utilization and offers many social and individual benefits. The objective of the cognitive radio network technology is to utilize the unutilized spectrum by primary users and fulfill the secondary users' demands irrespective of time and location (any time and any place). Due to their flexibility, the cognitive radio networks are vulnerable for numerous threats and security problems that will affect the performance of the network. Little attention was given to security aspects in cognitive radio networks that include spectrum sensing (sensing primary user), attacks that threaten the network at various layers and adversary effects on performance due to the security threats. In this survey, we discuss the cognitive radio networks, problems involved in sensing and management, attacks on cognitive radio networks, attacks on various network layers, threats on cognitive radio networks, and the current security and privacy solutions available. Further, we illustrate the need of careful engineering with security checks while designing the cognitive radio networks.**

Keywords: Cognitive Networks; security; threats; frequency sensing; spectrum mobility; spectrum holes.

I. Introduction

The novel approach of cognitive radio (CR) in wireless communications was coined by Joseph Mitola III in 1998, in a seminar at Royal Institute of Technology, Stockholm. The work was later published by Mitola and Maguire [1] in IEEE personal communications. The aim was to provide appropriate intelligence (an intelligent agent) to portable devices (for example – personal digital assistants) so that they fulfill the common user communication needs [2]. The intelligent agent in the device detects available channels in the wireless spectrum band and automatically changes its parameters (transmission or reception) to meet user needs. The process of detecting unused or available channels from the wireless spectrum band at any place is called dynamic spectrum access (DSA). The DSA and DSM (dynamic spectrum management) concepts are derived from the principles of artificial intelligence, machine learning, and cross-layer optimization. The game theory applications are examples of DSM that improves the performance of cognitive radio networks (CRN).

The main functions of cognitive radios are spectrum sensing, spectrum management, spectrum mobility and spectrum sharing. The main goal of the cognitive radio is to detect the white spaces (unused spectrum or spectrum holes) in the primary spectrum and efficient use of that detected unused spectrum without harming the primary user. Detection of a transmitted signal can be done by using one or more of techniques including matched filter, energy detection, cyclostationary feature detection, cooperative detection (sensing spectrum with the cooperative effort of multiple cognitive radios), and interference based detection method. The spectrum management (analysis and decision) includes the selection of the best spectrum suitable to the cognitive users. Spectrum mobility is the process of allocating the best possible spectrum during mobility of cognitive user. Finally, the spectrum sharing is a fair scheduling method in spectrum usage.

Today more than 5 billion devices are in use, expected to increase 10 billion by 2017 and approximately 100 billion by 2025. This number includes high-end handsets, tablets, and laptops on mobile networks. These devices generate serious traffic on the communications. The anticipated demand in communications forces to incorporate compact devices, new features, and more battery life. Future cognitive radios offer the new technology with nanotechnology featured compact devices. Building flexible cognitive radio technology with large-scale deployment of cognitive radio networks is a complex task. The features include smart antennas, new hardware (Nano components incorporated) with software defined radio, spectrum sensing, spectrum measurement, medium access control, routing, self-organizing, adaptive control mechanisms, learning, policy definition and monitoring. Developing and introducing new technology requires appropriate security measurements and policies. Therefore, security at each step of cognitive wireless networks is a challenging job.

Berkeley wireless research center [3] shows that 2GHz to 10GHz spectrum is underutilized. To utilize the underutilized spectrum, the cognitive radio must detect the presence of primary signal (PS), and use that spectrum without interfering with primary signal. Security involves in misdetection and false detection of the primary user. False detection is that the primary signal presence is recorded when the signal was absent (falsely detecting the primary user). Further, false detection includes that a malicious user pretends as the primary user (PU) by sending a strong signal to other cognitive users. Misdetection is the presence of the primary user which is not detected by the cognitive user through matched filter, energy detection, and cyclostationary feature detection. To eliminate such false detection and misdetection of the primary user, a spectrum sensing mechanism must be created to enhance the trust worthiness of the primary signal detection.

In wireless networks, hacking and malicious attacks are inevitable. Further, security threats are unavoidable, and incorporating security facilities are challenging in cognitive radio networks due to its nature of openness. Therefore, more care and research need to be done to provide security mechanisms in cognitive radio networks. Better security mechanisms ensure the trustworthiness of the spectrum sensing. The detection problems arise when operating in a hostile environment. In a hostile environment, it is possible to mimic the incumbent signal characteristics and pretend (emulate the primary user characteristics) as the primary user. In such cases, integrating legitimate transmitters for primary and secondary users in spectrum sensing will improve the trustworthiness of the detection process. Further, embedded signature in PU or interactive protocol between an incumbent transmitter and verifier cannot be used due to FCC's document requirements [4].

In conventional radio technology, signals emitted by wireless devices were predictable (approved by FCC). Since the creation of a wide range of authorized and unauthorized signals are possible using low-cost consumer devices, it is relatively easy to create denial-of-service (DoS) attacks that can affect the critical applications such as traffic control or health care. Therefore, future FCC regulations need to be aware of these DoS attacks [6]. The issues to be considered in cognitive radios are:

- Type of security attacks
- Security implication in implementing software defined radio
- Trusted cognitive radio design with security concerns
- Requirement of authentication protocols in cognitive radio networks
- Ensuring the functionality of security mechanisms and
- Requirement in encryption mechanisms

This survey report focused on the above six problems. Further, the survey identifies and presents the new capabilities to defend against intrusions and denial of service attacks. More work is needed to develop better security models in spectrum sensing, emulation of denial of service, physical layer security enhancements, geo-location for improved wireless network security, and cooperative methods for isolating the intruders. Since the CRN is in a developmental stage, it is an opportunity to incorporate these security capabilities as part of the implementation.

The remaining part of the paper discusses the related work in Section II, cognitive radio network environment in Section II and threats and attacks in section IV. Section 5 provides the type of attacks on a network layer and counter measures. Section VI concludes the work and future requirements in CRN security

II. Related work

Most of the survey papers in cognitive radio networks (CRN) discussed the security problems in specific aspects of the network. The surveys on CRN show the state of the art research in specific or few general aspects. Fragkiadakis et al [7] discussed the security threats and detection techniques in CRN. The paper includes the challenges that cognitive radios and cognitive radio networks along with the current state-of-the-art to detect the corresponding attacks.

Wassim et al [3] discussed the security attacks along with the mitigation techniques in CRN. This paper provides the category of attacks at MAC layer, data-link layer, and transport layer. Further, they discussed the jamming attack, false detection of PU, and objective function attack which are common in most of the surveys. Their evaluation shows that the combination of the counter measures will produce better security.

The survey paper by Parvin et al [8] addresses the CRN architecture and security issues. The spectrum mobility threats, jamming counter measures, spectrum sensing challenges, and attacks on protocol layers are outlined in this survey. Further, attacks on protocol layer are listed in this survey paper. Leon et al discussed the attacks on cognitive radios including PU emulation attacks, objective function attacks, common control data attack, lion attack, false feedback attack, jamming countermeasures, and vulnerabilities inherent to those systems [9]. They further discussed mitigation of lion attack based on periodic PS emulation attacks. The document is the over view of some of the attacks on cognitive networks. Clancy et al [10] discussed the threats and mitigation of security in cognitive radio Networks. They outlined the policy radio threats, learning radio threats, and self-propagating behavior. Various classes of attacks including dynamic spectrum access (DSA) attacks, objective function attacks, and malicious attacks are part of this document. The authors felt that the earning the trust in cognitive radio networks is extremely important.

Newman and Clancy [11] discussed the security threats in signal classifiers. They discussed the signal classifier model, threat analysis, and threats on feature extractions. They claimed that signal classification algorithm opens a new area of security research related dynamic spectrum access and signal classification. They used the signal classification algorithm to distinguish the primary user (PU) and secondary user signals. Chen et al [12] designed a defense scheme to identify the malicious users by estimating location information and observing the signal strength. Spectrum sensing is also discussed by Chen et al in [13, 14]. In [13], the authors discussed the primary user emulation problem and demonstrated the disruptive effects in cognitive radio networks. They discussed the transmitter position for detecting the attacks. Further, they demonstrated the effect of the location verification with respect to the attacks. Chen et al [14] discussed the distributed spectrum sensing and incumbent emulation attacks. The sensing and management attacks are:

- Defending against incumbent emulation attacks
- Spectrum sensing data falsification attacks
- Defending against spectrum sensing data falsification (SSDF) attacks

Primary user emulation attack is one of the common security threats in CRN. Chen et al [15] proposed a transmitter verification scheme called LocDef (localization based defense) that verifies the received signal based on location and characteristics. They concluded that the signal disruptive process will be eliminated by incorporating the LocDef process into spectrum sensing processes. They showed through simulations that LocDef scheme is an effective program and can be employed in a hostile environment.

Common control channel security is vital in cognitive radio networks. Safdar and O'Neill [16] discussed the common control channel security for cooperatively communicating cognitive radio nodes. The authors presented an algorithm and demonstrated that low cost hash or message authentication code algorithm achieves information integrity.

The key challenges and evaluation approaches in CRN were presented in [17]. The paper discusses the current security posture of emerging IEEE 802.22 cognitive radio standard and identifies the potential vulnerabilities along with potential mitigation approaches. The features of cognitive radio from the perspective of an attacker were briefly presented. The author identifies that the CR must incorporate the ability to authenticate the local observations in perceived environments, strong collaboration of CR elements related to security, validity of observations between CR elements, and have self-analysis behavior. He further noted that security in CRN is a multi-disciplinary problem.

Implementation issues of spectrum sensing in cognitive radios were discussed by Cabric et al in 2004 [18]. The authors identified cyclostationary feature detection has more advantage among matched filtering and energy detection due to its ability in differentiate modulated signals, interference, and low signal noise ratio. The energy detection technique to detect the primary signal became the central issue of security threats and work on security was concentrated at later years in primary signal emulation analysis. Chen et al [12-15] used various techniques including LocDef for primary signal emulation to eliminate the false detection and misdetection.

III. COGNITIVE RADIO NETWORK ENVIRONMENT AND SECURITY

The increase in communication requirements, difficulties to meet the emergency communication connections and more effective communication services lead the idea of introduction of software defined radio. Cognitive radio is the improvement of software defined radio coined by Mitola [1, 2]. If the demand for spectrum increases continuously, additional radio resources are required to meet customer requirements. Further, we need an agent component that is intelligent enough to adjust transmission parameters with respect to location, environment, and serve the customer needs. This intelligent resource called cognitive radio that operates effectively and use the unused bands (spectrum holes) without disturbing the licensed user. The definitions from National Telecommunications and Intelligent Agency (NTIA), the position statement of IEEE-USA Board of Directors in 2003, and Scientific American conclude that 'cognitive radio is a smart radio that has the ability to sense external environment, learn from history, adjust its parameters to the current state and take intelligent decisions' [19-22]. The statements conclude that CR adapts to the current environment, reasons, learns, collaborates with other radios, and support future decisions. Further, the CRN nodes sense the current radio frequency spectrum environment, contains policy and configuration databases, have self-configuration, mission-oriented configuration, adaptive nature, distributed collaboration and security (authenticate, authorize and protect) of customers.

Due to the nature of CRN, security became a problem at every step (Spectrum Sensing, Spectrum sharing, Location Identification, etc.) of its functionality. The security problems will occur in different ways. For example:

- False detection (sensing) and misdetection of primary signal may happen due to denial of service or malicious user pretends as the primary signal.
- Environment could be controlled by a malicious user.
- An attacker could prevent the cognitive user from using available spectrum (primary signal sensing mechanism).
- An attacker could access the data unauthorized way or modify/inject the false data (integrity of data is required).

Therefore, we need to find the potential threats, potential attacks, likelihood of these threats and attacks, and potential consequences of these attacks. After finding these security risks, we will specify the basic security services such as confidentiality, privacy, and authentication similar to wireless networks. Little attention was given to location privacy threats which are a unique challenge in CRNs. Further, the encryption and mutual authentication techniques will help the data confidentiality.

Figure 1 shows the general architecture of cognitive radio. The security problems are in location identification, the cognitive radios contesting for free spectrum, spectrum sensing, spectrum analysis, and spectrum management. The external threats include hacking the information, incorporating the malicious nodes, corrupting the information at any level shown in the figure 1. Further, the security at the protocol level that interact various layers of the network is an essential issue to discuss in the study of securing cognitive networks.

Once the spectrum holes are detected, the available spectrum will be allocated as soon as possible. Therefore, cognitive radios are competent among themselves at each node to gain spectrum access. Due to these reasons, the design of CRs requires security and threat procedures. Further, the CRs are vulnerable to the threats and attacks while detecting the primary signal due to their localization and adaptive nature. The malicious attackers are common in wireless networks as well as CRs. The general requirements of security in CRs are discussed in [7-20].

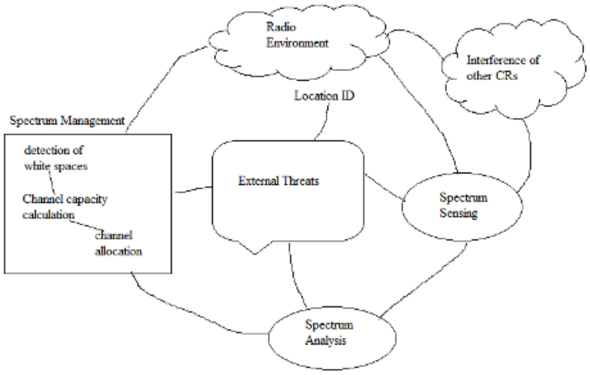

Figure 1. General architecture of cognitive radio

The security requirements in CRNs vary from location to location. Along with security requirements, we will discuss the current state of algorithms for protection in cognitive radio networks and security provisions through IEEE 802.22. The basic security requirements in CRN are confidentiality, integrity and availability. The other security issues include:

- Sensing and emulation of primary signal (detecting and verifying the signal).
- Spectrum management (detecting, verifying channel capacity, and allocating appropriate channel to cognitive user).
- Checking interference level, signal strength, and energy detection.
- Secure communication.

The motivations vary depending upon the attacker. The selfish nature of a cognitive user projects he/she as the primary user to use the spectrum with higher priority. They modify the spectrum sensing parameters for selfish advantage. The selfish user can prevent other users from using the spectrum by jamming or with DoS. The DoS can be created using various authorized and unauthorized waveforms with a low-cost consumer device. The selfish users can be controlled through access permissions and authentication. Further, by using channel sensing algorithms we can control the cognitive users from interference. We will discuss various threats, attacks and the counter measures in Section 4.

To minimize these selfish attacks it is necessary to identify the type of DoS attacks on CRN and possible hardware improvements, improve the weaknesses of Internet to implement software-based radio, trusted CR to address the security issues, and develop the algorithms and mechanisms to address the cooperative methods to detect and isolate intruders.

IV. Threats and Attacks in Cognitive Radio Networks

Threat is a constant danger through persons, objects, or any resources where as an attack is an act of or event that exploits the vulnerability. The policies, learning mechanisms, and self-propagation in cognitive radio architecture prevents the threats (cannot escape the threats). In CR, a threat can happen while sensing of information (due to involvement of a malicious user). This information will then feed for learning and decision making. The results produced will lead to inappropriate decisions (unacceptable decisions) due to a malicious user injected the faults. The threat analysis in unsupervised learning and signal sensing was discussed by Clancy et al [10, 11].

Attacks on spectrum management were briefly explained by Parvin et al [8] and Mathur and Subbalakshmi [23, 24]. They suggested strong encryption mechanism is required at physical and MAC layer level. The attacks were classified depending upon the protocol layers. The Table 1 provides the attack types, network layers involved, and reason for attacks.

TABLE 1. ATTACK TYPES, LAYER INVOLVED AND REASON FOR ATTACKS

Attack type	Network Layer	Reason	Countermeasures
Primary and secondary user Jamming	Physical	Lack of knowledge about location and unclear access rights to cognitive user	• Location Consistency Checks • Compare signal strength and noise level
Primary signal sensing	Phycal	Low level primary signal will be missed	• Energy-based sensing • Waveform-based sensing • Cooperative detection of PU
Overlapping secondary users	Physical	Location based. Hard to prevent	• Use game models and Nash equilibrium techniques to detect transmission power of SUs
SUs unauthorized gain in bandwidth by pretends as primary user or False feedback	MAC	Malicious SU tweaks with higher power bandwidth, and feed false information to gain signal	• Trust management on secondary users for resource hungry and collaborative trust • Management of systems objective function by controlling the radio parameters
Increase interference by malicious node	Network	Compromising with malicious node	• Appropriate local spectrum sensing controller • Eliminating internal hidden parasite nodes
Ripple effect	Network	False information about spectrum assignment	• Continuous trust management process on SUs

Key duplication	Transport	Breaks the cypher system	• Reinvestigate the protocol activity in the context of sessions • Use secure protocols with robust distribution of key management
Jelly fish	Transport	Effect on throughput	• Trust of node by verifying the packet loss

Cross-layer attacks are possible in CRN. There is a need to be given individual attention for such attacks. Jamming on routing information happens due to lack of common control channels. Traffic analysis attack on data privacy and location privacy will be avoided by authentication and controlling the access rights of cognitive user.

The defense mechanisms were discussed in [10-20]. The other attacks include false feedback of information from one group of cognitive users to mislead the different group of cognitive users. This consequence ends to mislead the detection of primary signal. Network Endo-Parasite (NEP) attack avoids the selection of the right channel by the other cognitive users. The NEP attack is played by a different group of cognitive users. The objective function attack controls a large number of radio parameters. According to Clancy and Georgen [10] secure communication with low or high power has provided the weights. The channel gain depends upon the weight rate. The dishonest users will mislead the other users to gain access. Further, they mislead the honest user to misdetection of the primary signal with the introduction of extra noise.

V. CHALLENGES AND DEFENDING MALICIOUS ATTACKS

Spectrum sensing, Spectrum management, spectrum sharing, and spectrum mobility are some of the challenges in CRN security. Ensuring trust worthy spectrum sensing is one of the essential mechanisms in CRs. The primary signal analysis is suggested in the current survey. Trust on spectrum sensing happens if the primary signal is emulated and recognized correctly. For example, a malicious user or hacker can interpret the primary user signal and occupy the spectrum for selfish use. The attack can be detected through transmitter verification procedures and location verification procedures. Further, a cognitive user simulates the primary user for personal gains. That means, a cognitive user crosses its user access limits. These activities can be controlled using the various privacy procedures and access limits. This problem can be fixed using a honey pot database to mislead the malicious user.

The primary signal cannot be detected because of interferences at location devices. Primary user signal detection gets difficult if it uses the spread spectrum signaling or altering the parameters by a malicious user. These problems can be eliminated using the cloud application. Further, the cloud application to eliminate the hidden terminal problem was discussed in [25, 26]. The solution for interference problem was proposed in [27] and spectrum sensing can be detected efficiently through multiple users in a cooperative manner. Once the free spectrum is detected, the best available band will be detected using local observations and statistical information.

The common control problem involves the exchange of security keys between the nodes. The authentication among the nodes provides confidentiality and integrity of the transactions. This technique provides the security and the hidden terminal problem still remain. The jamming problem, hidden terminal problem, exchange of keys between the nodes and malicious user acts can be eliminated by using the cloud application. The security to cloud still remains an open problem.

Malicious activity can be from outside or among the cognitive users. Detecting the malicious activity among the cognitive users can be done using the intruder detection procedures and incorporating honey pot database. Further, cross-layer technique with appropriate defense mechanism in communication protocol will help the attacks on upper layers. Incorporating the cryptographic techniques or digital signature based primary signal identification may help in distinguishing the malicious users. More work is required in this direction.

Spectrum mobility involves common control channel, operating frequency range, and location information. It requires the current location of the primary user and operating range so that the secondary user can vacate the occupied spectrum as soon as PU enters. Spectrum mobility depends upon the primary user entry and secondary user relocation. The cloud application will solve many attacks and hidden terminal problems in cognitive networks similar to problems like sudden entry of the primary user [26].

VI. CONCLUSIONS AND FUTURE WORK

The literature shows that the spectrum management sachems are lack of formal security models. The conventional authentication models for wireless security need to be modified to CRNs. The cooperative sensing models improves the sensing capability with overhead of jamming. In multi-user environment, the attackers have opportunities for malicious activities. Intrusion detection models are required in such situations. Cryptographic techniques are useful with the additional burden of computing time. The trust models are more appropriate than to cryptographic techniques due to their simplicity and computational efficiency. Cloud application helps to eliminate hidden terminal problem. But, cloud security is another open problem in CRNs.

The overview of the CRN shows that security is an essential at all levels (sensing, location, and management). Security mechanisms through protocols at different layers were discussed in this paper. The study shows that implementation at the protocol level is very important at each network layer (Physical, MAC, Network, and transport). Few authors stressed the need of security models at cross-layer design. The current research shows that future security on cross-layer design will get special attention.

Finally, we conclude that threat proof mechanism is difficult and impossible. The threat detection mechanisms can be developed for cognitive radio networks in the same lines of intrusion detection mechanisms. The threat detection and protection of information are serious issues in wireless networks as well as cognitive radio networks. It is recommended that threat detection mechanisms must be developed and incorporated as part of the design as and when need arises.

ACKNOWLEDGEMENTS

The research work was supported by the Minority Leaders Program through contract number GRAM 11-S567-0017-02-C2. The author wishes to express appreciation to Dr. Connie Walton, Provost and Vice President, Academic Affairs, Grambling State University for her continuous support.

REFERENCES

[1] J. Mitola and G. Q. Maguire, “Cognitive Radio: Making software radios more personal”, IEEE personal Communications, 1989, vol. 6, no. 4, pp. 13-18.

[2] J. Mitola, "Cognitive Radio – An Integrated Agent Architecture for Software Defined Radio", Ph.D. Dissertation, Royal Institute of Technology, Kista, Sweden, May 8, 2000, ISSN: 14035286, 313 pages..

[3] E. Wassim, S. Haidar and G. Mohsen, “Survey of Security Issues in Cognitive Radio Networks”, Journal of Internet Technology, 2011, vol. 12 No. 2, pp. 181-198.

[4] FCC, “Notice for Proposed Rulemaking (NPRM 03-322): Facilitating Opportunities for flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies,” ET Docket, No. 03-108, 2003.

[5] D. Sicker and R. Dhillon “Security of Cognitive Radio Networks (Synthesis Lectures on Communications)”, Morgan & Claypool Publishers (January 30, 2013), ISBN-13: 978-1608451005.

[6] Federal Communication Commission, “Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz in the 3GHz band,” ET Docket, No. 04-186, May 2004.

[7] A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, “A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks”, IEEE Communications Surveys & Tutorials, 2013, vol. 15 , issue: 1 , pp. 428 -445.

[8] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, “Cognitive radio network security: A survey”, Journal of Network and Computer Applications, 2012, vol. 35, pp. 1691–1708.

[9] O. León, J. Hernández-Serrano, and M. Soriano, “Securing cognitive radio networks”, Int. Jr. of Communication Systems, 2010, vol. 23, Issue 5, pp. 633-652.

[10] T. C. Clancy and N. Goergen, “Security in Cognitive Radio Networks: Threats and Mitigation”, CrownCom 2008, 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008, pp. 1 – 8.

[11] T. R. Newman and T. C. Clancy, “Security threats to cognitive radio signal classifiers”, Proceedings of the Virginia tech wireless personal communications symposium, 2009, pp. 1-9.

[12] K. C. Chen, Y. J. Peng, N. Prasad, N., Liang, Y. C. and S. Sun “Cognitive radio network architecture: part I. general structure”, 2nd international conference on ubiquitous information management and communication, 2008, CRs. pp.114–119.

[13] R. Chen and J. Park, “Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks”, 1st IEEE workshop on Networking Technologies for Software Defined Radio Networks,(SDR '06), 2006, pp. 110 – 119.

[14] R. Chen, J. Park, Y. T. Hou and J. Reed, “ Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks”, IEEE Communications Magazine, 2008,vol. 46, issue. 4, pp. 50-55.

[15] R. Chen, J. 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.

[16] G. A. Safdar and M. O’Neill, “Common Control Channel Security Framework for Cognitive Radio Networks”, 69th IEEE Vehicular Technology Conference, 2009, pp. 1-5.

[17] J. L. Burbank, “Security in Cognitive Radio Networks: The Required Evoluation in Approaches to Wireless Network Security”, CrownCom 2008, pp. 1-7.

[18] D. Cabric, S. M. Mishra and R. W. Brodersen, “Implementation Issues in Spectrum Sensing for Cognitive Radios”, 38th Asilomar Conference on Signals, Systems and Computers, 2004, pp. 772-776.

[19] “IEEE 802 Tutorial: Cognitive Radio”, Scott Seidel, Raytheon, presented at IEEE 802 Plenary, 18 July 2005.

[20] T. R. Shields, "SDR Update," Global Standards Collaboration, Sophia Antipolis, France, Powerpoint Presentation GSC10_grsc3 (05)20, 2005.

[21] R. W. Thomas, L. A. DaSilva and A. B. MacKenzie, "Cognitive networks," IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, November, 2005, pp. 352-360.

[22] FDR Forum, Cognitive Radio Definitions and Nomenclature, Approved Document SDRF-06-P-0009-V1.0.0, 10 September 2008.

[23] C. N. Mathur and K. P. Subbalakshmi, “Security issues in cognitive radio networks”, Cognitive networks: towards self-aware networks. John Wiley and Sons, Ltd; 2007.

[24] C. N. Mathur and K. P. Subbalakshmi, “Digital signatures for centralized DSA networks”, 4th IEEE conf. on consumer comm. and networking, 2007, pp. 1037–1041.

[25] Y. B. Reddy, “Solving Hidden Terminal Problem in Cognitive Networks Using Cloud Application”, SENSORCOMM 2012, pp. 235-240.

[26] Y. B. Reddy and S. Ellis, “Modeling Cognitive Radio Networks for Efficient Data Transfer Using Cloud Link”, ITNG 2013, April 2013, Las Vegas, USA.

[27] M. Shahid and J. Kamruzzama, “Agile spectrum evacuation in cognitive radio networks”, IEEE international conference on communications (ICC), 2010, pp. 1–6.