International Journal of Scientific and Technical Advancements
IJSTA
ISSN: 2454-1532

Potential Security Threats to CRN: A Survey

Harsh Magotra, Sameru Sharma, Harinder Dhingra
Department of Electronics and Communication Engineering, Govt. College of Engineering and Technology, Jammu, India
Email address: harshmagotra09@hmail.com, sameru33@rediffmail.com, dhingra_h@yahoo.com

***Abstract*—** Cognitive Radio (CR) is an emerging technology, which can be used to remove the spectrum shortage problem or the barriers to communication interoperability in various application domains. The successful realization of CR will depend on the design and implementation of essential security features to ensure the network is robust against security attacks. CR may introduce various challenges including malicious user behaviors. An attacker could disrupt the basic functions of a CR network, cause harmful interference to licensed users or deny communication to other CR nodes.

***Keywords*—** Malicious users, false alarm, missed detection.

I. INTRODUCTION

With the expansion of wireless applications and services, there arises the huge demand for spectrum resources. As most of the spectrum has been already assigned by the governing authorities like FCC, so it becomes very tedious job to meet the requirements of ever expanding applications and services. If we scan the spectrum at some instance of time, we will find that most of the spectrum remains unoccupied for most of the time, which leads to the partial usage of the spectrum. Moreover spectrum scarcity issues are getting worse due to emergence of new wireless services and limited resources. Fortunately, the worries about spectrum scarcity are being shattered by a recent survey made by Spectrum Policy Task Force (SPTF) within FCC. It indicates that the actual licensed spectrum is largely under-utilized in vast temporal and geographic dimensions [1]. So, after considering all the facts and requirements, Cognitive radio comes into existence. It comes as a remedy to overcome the issues related to the spectrum scarcity.

Cognitive radio is the innovative technology that focuses on improving the spectrum utilization by allowing the secondary users to use the unused spectrum from licensed users. Cognitive radio emerges as an intelligent wireless communication system. Cognitive radio is aware of the radio frequency environment, selects the communication parameters to optimize the spectrum usage and adapts its transmission and reception accordingly. By sensing and adapting to the environment, a cognitive radio is able to able to fill in the spectrum holes and serve its users without causing harmful interference to the licensed user. To do so, the cognitive radio must continuously sense the spectrum it is using in order to detect the re-appearance of the primary user [2].

According to Akyildiz et.al [3], the four basic functions of the cognitive radios for enabling DSA are as follows:

• Sensing of Spectrum: Cognitive radio need to sense unused spectrum for secondary usage without interfering primary user.

• Management of Spectrum: Cognitive radio need to find the best available spectrum for optimizing the communication requirements.

• Mobility of Spectrum: Cognitive radio need to seamlessly transition the spectrum used for communication, when needed to leave the currently used spectrum

• Sharing of Spectrum: Cognitive radio need to fairly share the available spectrum among the coexisting secondary users.

II. SECURITY REQUIREMENTS

It is well known fact that important element of Wireless Communication is “Security”. As general rule, CRN, must follow the communication security requirements like:

- Data Confidentiality
- Privacy
- Availability
- Authentication
- Authorization

These are the result of general compliance to the standard and regulations defined for wireless communication systems, Security measures are not limited to the protection of data transmitted over the network but also to guarantee the requirements .Security threat is the probable violation of the security. Security threats can be intentional or non intentional [4].

As described in [10], the definition of the security requirements may be derived considering the concepts of stakeholders, asset, threat and risk.

The stakeholders can be users of the communications systems, public and government authorities or the network providers. *Assets* include the components of the network, the information stored or transmitted and the services provided by the network.

A security threat is defined as a potential violation of security. Examples of security threats are loss or disclosure of information or modification/destruction of assets. A security threat can be intentional like a deliberate attack or unintentional due to an internal failure or malfunctions.

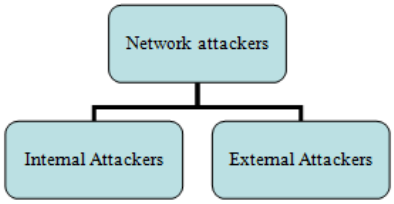
The security risk measures the impact of the realization of a security threat. Security countermeasures (protection techniques) strive to eliminate or reduce the security risks.

In this paper, an extension of the network security requirements defined by the International Telecommunications Union (ITU) in [11] is presented:

Harsh Magotra, Sameru Sharma, and Harinder Dhingra, “Potential security threats to CRN: A survey,” *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 155-158, 2016.

The following security requirements are defined:
1) Controlled access to resources
2) Robustness
3) Ensuring confidentiality
4) Maintaining system integrity
5) Maintaining data integrity
6) Adherence to regulatory framework
7) Accountability
8) Vigil on identities

Communication systems based on CR should be incorporated with the capability to address security threats. Attackers can be of following types:



Internal attackers can falsify regarding position and distance information

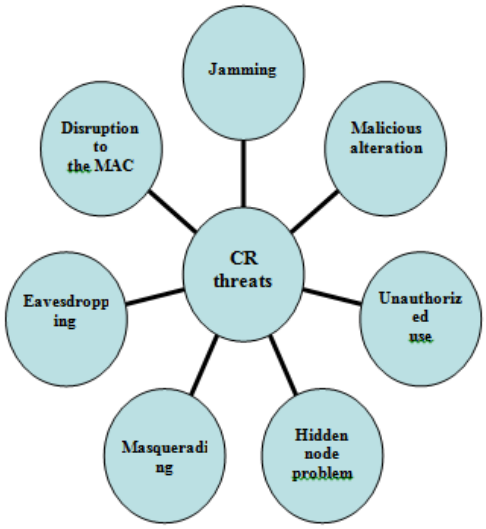
External attackers can spoof regarding the measured positions and distances of wireless nodes.

III. COGNITIVE RADIO THREATS

Conventional communication systems can only change their transmission parameters and use the radio frequency (RF) spectrum bands in the limits, which have been defined by predefined standards and spectrum regulations. A CR may instead communicate in a wide range of spectrum bands and have the capability to change its transmission parameters in response to changes in the sensed radio spectrum environment, information received from other CR nodes, or networks.CR functions, which can be impacted by a security threat are

I. Spectrum sensing
II. Spectrum management
III. Spectrum sharing
IV. Spectrum mobility.

Representation of the main CR threats is as follows:



The description of the threats is as follows:

1) *Jamming:*
This threat identifies the jamming of a cognitive control channel used to distribute cognitive Messages

2) *Malicious alteration*. It identifies the manipulation of cognitive messages exchanged in the CR network.
radio This threat identifies the alteration of the behavior of a CR node, which can be used to support other threats like harmful wireless interference to primary or secondary users or disruption of the CR network

3) *Masquerading*: It identifies the malicious masquerading of a primary user like a digital TV broadcaster. The malicious attacker may mimic the primary user characteristics in a specific frequency band (e.g., white space band), so that the legitimate secondary users erroneously identify the attacker as genuine user and they avoid using that frequency band, leading to false alarm and missed detection errors.

4) *Hidden node problem.* This threat identifies the case
in which a CR node is in the protection region of a primary node (i.e., the coverage area of a digital
TV broadcaster) but fails to detect the existence
As a consequence, it transmits in the same frequency bands of the primary user, causing harmful interference. Depending on their position, other CR terminals sense a different spectrum environment, and they can provide additional information to mitigate the threat.

5) *Unauthorized use of spectrum bands:* This threat identifies the case where a malicious node or CR network uses spectrum bands for which is it not authorized or licensed, to gain more traffic capacity or bandwidth.

6) Saturation: It identifies a DoS attack against the cognitive control channel (CCC) by saturation: a large number of cognitive messages are sent to the CCC to deny its service
to the CR network.

7) *Eavesdropping:* It identifies the eavesdropping of cognitive messages by a malicious attacker, who can then use this information for subsequent attacks.

8) *Disruption to the MAC:*It includes attacks against the higher functions of the CR network, including the MAC, network layer, and cognitive engine.

IV. CONCLUSIONS AND FUTURE WORK

The paper has provided an overview of the security threats for CRN. Since this is relatively recent research area still many contributions have already been proposed and a number of protection techniques are identified. The lack of available spectrum and the simultaneous increase in number of applications, notably the bandwidth hungry one, such as real-time video, is a driving force to explore spectrum sharing as an essential element of future wireless systems. As the discussed in this paper, major concern is to identify a range of threats, vulnerabilities which can create hindrance in proper deployment of CRN. This effort requires, as indicated in this paper, further integration between the various spheres of activities involved in spectrum regulation, security, certification with a view to create a balance Future work will

Harsh Magotra, Sameru Sharma, and Harinder Dhingra, "Potential security threats to CRN: A survey," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 155-158, 2016.

ISSN: 2454-1532

investigate the protection techniques to mitigate threats discussed here.

REFERENCES

[1] J.Mitola, "Cognitive radio an integrated agent architecture for software defined," Ph.D. dissertation, KTH Royal Institute of Technology, Stockholm, Sweden, 2000.

[2] Haykin, "Cognitive radio: brain-empowered wireless communications," IEEE J, Select. Areas in Commun, vol. 23, no. 2, pp. 201–220, February 2005.

[3] FCC, "Spectrum policy task force," Technology Advisory Council(TAC),Briefing, Tech. Rep., 2002

[4] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," Information Hiding Workshop,pp. 239–252, May 2004,

[5] J. L. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," in CROWNCOM'2008, pp. 1-7, Singapore, 2008

[6] Peter Steenkiste, Douglas Sicker, Gary Minden, Dipankar Raychaudhuri, Future Directions in Cognitive Radio Network Research,report of NSF workshop, March 9-10, 2009

[7] Chen, R., Park, J.-M., & Reed, J. H., (2008). Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications Special Issue on Cognitive Radio Theory and Applications, Vol. 26, No. 1.pp.25-37

[8] Ian F. Akyildiz, Brandon F. Lo, Ravikumar Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey", Physical Communication vol.4 (2011) pp.40–62

[9] NSA's IA Definition, Web-site: http://www.nsa.gov/ia/. Last accessed 4 December 2010).

[10] International Telecommunication Union. Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunication

[11] ITU-T E.408. Telecommunication networks security requirements.

Harsh Magotra, Sameru Sharma, and Harinder Dhingra, "Potential security threats to CRN: A survey," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 155-158, 2016.

ISSN: 2454-1532

Harsh Magotra, Sameru Sharma, and Harinder Dhingra, "Potential security threats to CRN: A survey," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 155-158, 2016.