An Overview of Security Threats of Cognitive Radio Networks

Pooja.V
MTech IV sem, Department of CSE, SJBIT, Bangalore
pooja.v.88@gmail.com

Dr. K C Gouda
CSIR Centre for mathematial Modelling and Computer Simulation, Wind Tunnel Road, Bangalore-37

Abstract **-Recently wireless communication is gaining increasing demand. Cognitive Radio(CR) is a promising technology, which can be used to alleviate the spectrum shortage problem or the barriers to communication interoperability in various application domains.**

The successful deployment of CR technology will depend on the design and implementation of essential security mechanisms to ensure the robustness of networks and terminals against security threats.CR introduces entirely new classes of security threats and challenges including down-load of malicious software, licensed user emulation and selfish misbehaviours. An attacker could disrupt the basic functions of a CR network, cause interference to licensed users or deny communication to other CR nodes.

In recent years, the security issues of cognitive radio networks have drawn a lot of research attentions. This paper surveys the security related issues of cognitive radio networks. The fundamentals, Spectrum sensing and analysis techniques are first discussed. Later we discuss in detail the security issues and few solutions to these issues.

Keywords: Cognitive radio (CR), Primary user (PU), Secondary user (SU), Spectrum sensing, wireless communication

I.INTRODUCTION

Cognitive capability means the ability to sense and gather information from the surrounding environment, such as information about transmission frequency, bandwidth, power and modulation.

Fig.1. Cognitive Radio Networks.

With this capability, secondary users can identify the best available spectrum [1].Here we have two main users – Primary users (PU) and secondary users (SU). PU has exclusive rights to access the spectrum. SU utilizes the spectrum when it is not being accessed by the primary user. A typical duty cycle of CR, as illustrated in Fig. 2, includes detecting spectrum space (white space), choosing the best frequency bands, coordinating spectrum access with other users and vacating the frequency when a primary user appears. Such a cognitive cycle is supported by the following functions:

- Spectrum sensing and analysis;
- Spectrum management and handoff;
- Spectrum allocation and sharing.

Through spectrum sensing and analysis, CR can detect the spectrum white space i.e., a portion of frequency band that is not being used by the primary users i.e licensed user, and utilize the spectrum. Also, when primary users start using the licensed spectrum again, through sensing CR can detect their activity, so that no harmful interference is generated due to secondary users' transmission. After recognizing the spectrum white space by sensing, spectrum management and handoff function of CR enables secondary users to choose the best frequency band and hop among multiple bands according to the time varying channel characteristics to meet various Quality of Service (QoS) requirements.

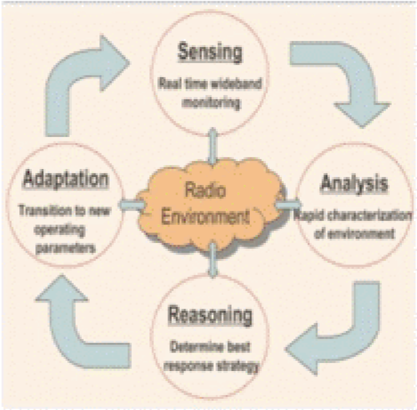
Sensing
Real time wideband monitoring
Analysis
Rapid characterization of environment
Reasoning
Determine best response strategy
Adaptation
Transition to new operating parameters
Radio Environment

Fig.2. Cognitive Cycle

For instance, when a primary user reclaims his/her frequency band, the secondary user that is using the licensed band can direct his/her transmission to other available frequencies, according to the channel capacity determined by the noise and interference levels, path loss, channel error rate, holding time, and etc. using the licensed spectrum again, CR detect their activity through sensing,

so that no harmful interference is generated.

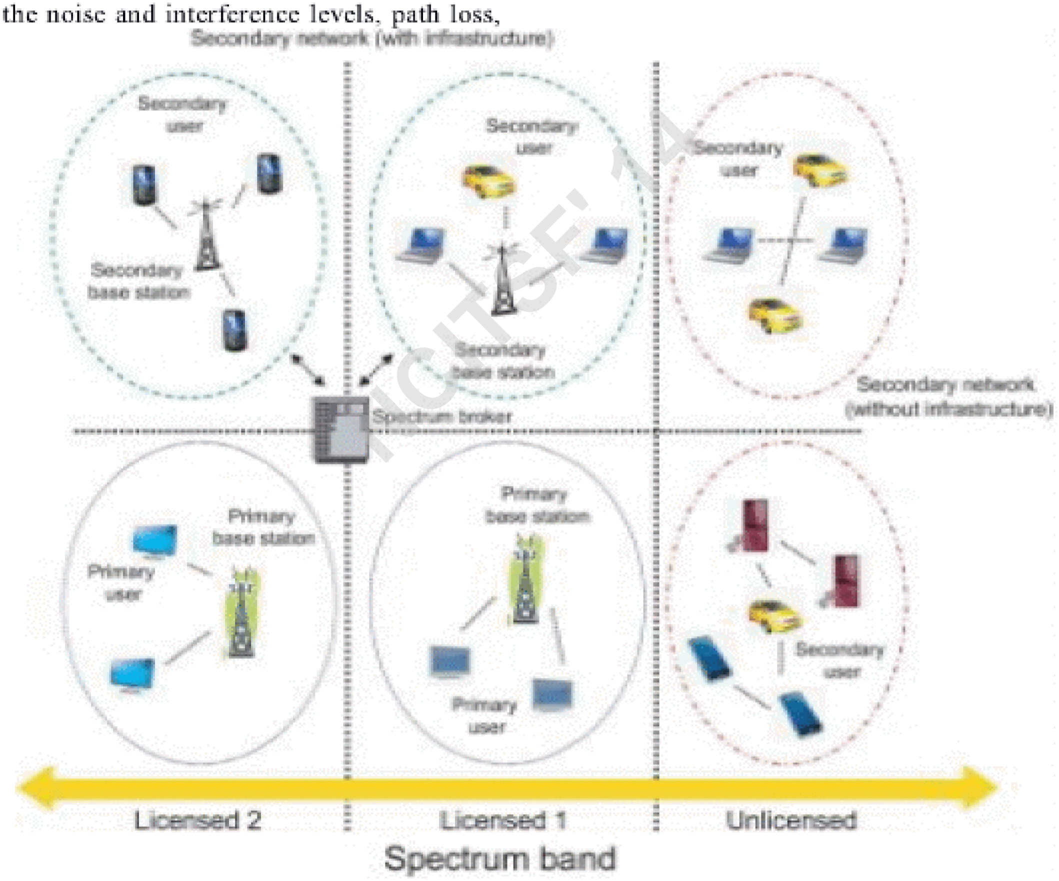

Fig.3. Network architecture of dynamic spectrum sharing.

II FUNDAMENTALS

Cognitive radio (CR) is one critical enabling technology for future communications and networking that can utilize the limited network resources in a more efficient and flexible way. In this section we discuss the network architecture, applications and spectrum sensing techniques

A. Network Architecture and Applications

With the development of CR technologies, secondary users who are not authorized with spectrum usage rights can utilize the temporally unused licensed bands owned by the primary users. Therefore, in CR network architecture, the components include both a secondary network and a primary network, as shown in Fig. 3. A secondary network refers to a network composed of a set of secondary users with/without a secondary base station. Secondary users can only access the licensed spectrum when it is not occupied by a primary user. The opportunistic spectrum access of secondary users is usually coordinated by a secondary base station, which is a fixed infrastructure component serving as a hub of the secondary network. Both secondary users and secondary base stations are equipped with CR functions. If several secondary networks share one common spectrum band, their spectrum usage may be coordinated by a central network entity, called a *spectrum broker*. The spectrum broker collects operation information from every secondary network, and allocates the network resources to achieve fair and efficient spectrum sharing. A primary network is composed of a set of primary users and one or more primary base stations. Primary users are authorized to use certain licensed spectrum bands under the coordination of primary base stations. Their transmission should not be interfered by applications, where a large amount of spectrum is idle. CR using dynamic spectrum access can alleviate the spectrum congestion through efficient allocation of bandwidth and flexible spectrum access. Therefore, CR can provide military with adaptive, seamless, and secure communications. Moreover, a CR network can also be implemented to enhance public safety and homeland security. A natural disaster or terrorist attack can destroy existing communication infrastructure, so an emergency network becomes indispensable to aid the search and rescue. As a CR can recognize spectrum availability and reconfigure itself for much more efficient communication, this provides public safety personnel with dynamic spectrum selectivity and reliable broadband communication to minimize information delay. Moreover, CR can facilitate interoperability between various communication systems. Through adapting to the requirements and conditions of another network, the CR devices can support multiple service types, such as voice, data, video, and etc.

Another very promising application of CR is in the commercial markets for wireless technologies. Since CR can intelligently determine which communication channels are in use and automatically switches to an unoccupied channel, it provides additional bandwidth and versatility for rapidly growing data applications. Moreover, the adaptive and dynamic channel switching can help avoid spectrum conflict and expensive redeployment. As CR can utilize a wide range of frequencies, some of which has excellent propagation characteristics, CR devices are less susceptible to fading related to growing foliage, buildings, terrain and weather. When frequency changes are needed due to conflict or interference, the CR frequency

secondary networks. Primary users and primary base stations are in general not equipped with CR functions.

Therefore, if a secondary network shares a licensed spectrum band with a primary network, besides detecting the spectrum white space and utilizing the best spectrum band, the secondary network is required to immediately detect the presence of a primary user and direct the secondary transmission to another available band so as to avoid interfering with primary transmission. Because CRs are able to detect, sense, and monitor the surrounding RF environment such as access availability and interference , and reconfigure their own operating characteristics to best match outside situations, cognitive communications can increase spectrum efficiency and support higher bandwidth service. Also, the capability of real-time autonomous decisions for efficient spectrum sharing also reduces the burdens of centralized spectrum management. As a result, CRs can be employed in many applications.

B. Cognitive radio applications.

First, the capacity of military communications is limited by radio spectrum scarcity because static frequency assignments freeze bandwidth into unproductive

management software will change the operating frequency automatically even without human intervention. Additionally, the radio software can change the service bandwidth remotely to accommodate new applications. Thus, CR is viewed as the key enabling technology for future mobile wireless services anytime, anywhere and with any device.

C. Spectrum sensing techniques. Cognitive radio generally includes four basic elements: spectrum sensing, spectrum management, spectrum sharing and spectrum mobility. Among them, Spectrum sensing is a fundamental functionality where the secondary users monitor the frequency spectrum and detect vacant channels to use. The spectrum sensing can basically be classified as non cooperative sensing, interference based sensing and cooperative sensing.

Through spectrum sensing, CR can obtain necessary observations about its surrounding radio environment, such as the presence of primary users and appearance of spectrum holes [2]. Only with this information can CR adapt its transmitting and receiving parameters, like transmission power, frequency, modulation schemes, and etc., in order to achieve efficient spectrum utilization. Therefore, spectrum sensing and analysis is the first critical step towards dynamic spectrum management. Spectrum sensing techniques can be categorized in the following types.

1) *Energy Detector:* Energy detection is easy to implement and requires no prior knowledge about the primary signal and hence it is the most common type of spectrum sensing.

2) *Feature Detector:* There are specific features

associated with the information transmission of a primary user. For instance, the statistics of the transmitted signals in many communication paradigms are periodic because of the inherent periodicities such as the modulation rate, carrier frequency, etc. Such features are usually viewed as the cyclostationary features, based on which a detector can distinguish cyclostationary signals from stationary noise [2].

3) *Matched Filtering and Coherent Detection:* If secondary users know information about a primary user' signal *a priori*, then the optimal detection method is the matched filtering, since a matched filter can correlate the already known primary signal with the received signal to detect the presence of the primary user and thus maximize the SNR in the presence of additive stochastic noise. The merit of matched filtering is the short time it requires to achieve a certain detection performance such as a low probability of missed detection and false alarm [1].

4) *Other Techniques:* There are several other spectrum sensing techniques proposed in recent literature, and some of them are variations inspired by the above-mentioned sensing techniques.

III SECURITY THREATS

The security issues of the cognitive radio (CR) networks have drawn a lot of research attentions in recent years. Conventional communication systems can only change their transmission parameters and use the radio frequency (RF) spectrum bands in the limits that have been defined by predefined standards and spectrum regulations. These limits are implemented in their hardware and firmware architecture, and hence they cannot be changed at runtime [3]. A CR may instead communicate in a wide range of spectrum bands and may have the capability to change its transmission parameters at runtime in response to changes in the sensed radio spectrum environment, information received from other CR nodes, or networks. This capability can be used to implement innovative approaches to spectrum management, where the allocation of spectrum bands to communication services can change in space or time.

In literature, a majority of the distributed or centralized approaches assume that the participating nodes are altruistic and make logical decisions to optimize the spectrum resources [4]. Such approaches make the CR network vulnerable to security threats, where malicious CR nodes implement selfish behaviour or would like to disrupt the protocols and algorithms defined to converge to optimal spectrum utilization. It is of crucial importance to identify the various types of security attacks and the related protection measures. Masquerading is a threat frequently cited in research literature. In this threat, a malicious CR node provides false information for the CR functions (e.g., spectrum sensing or spectrum sharing). The malicious CR node can inject false information on the spectrum environment into the other CR nodes with the objective of gaining an unfair advantage or just disrupting the CR network. This type of threat can affect both centralized and distributed CR networks. The distribution of incorrect or incomplete information on the spectrum environment can also be unintentional. In the case of the hidden node problem, two CR devices may have a different perception of the spectrum because they are located in two different locations and they detect different radio spectrum information. The hidden node problem is also called the hidden incumbent problem [5]. An obvious DoS threat is jamming. Jamming can be used to

a) Hamper or obstruct all the communications in a specific spectrum band or

b) Disrupt the management channels of the CR networks, which are used to distribute the cognitive messages among the CR nodes.

As described before, we identify the following CR functions, which can be impacted by a security threat: spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility.

A pictorial description of the main CR threats is presented in Figure 4.

The description of the threats is as follows:

1) *Jamming of the channel used to distribute cognitive messages*. This threat identifies the jamming of a cognitive control channel (CCC) used to distribute cognitive messages in the CR network. Jamming can be executed against an out-of-band CCC or an in-band CCC if the frequency of the channel is known.

2) *Malicious alteration of cognitive messages*. This threat identifies the alteration of cognitive messages exchanged in the CR network.

3) *Masquerading of a primary user*. This threat 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 an incumbent and they avoid using that frequency band. This can be a selfish attack, because the attackers may then use the frequency bands or just a DoS attack to deny spectrum resources to other secondary CR users.

4) *Malicious alteration of a cognitive radio node*. This threat identifies the alteration of the behaviour 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].

5) *Internal failure of cognitive radio node*. This threat identifies the failure of a CR node, which can have different causes: memory fault, physical failure, or others. This threat may have various impacts, depending on the type of failure. For example, the CR node can transmit in the wrong frequency band or not participate in the CR functions with other CR nodes.

6) *Masquerading of a cognitive radio node*. This threat identifies the masquerading of a CR node while collaborating with other CR nodes for CR functions: spectrum sensing, spectrum sharing, spectrum management, and spectrum mobility. For example, a malicious device can send wrong spectrum sensing information to other CR nodes.

7) *Hidden node problem*. This threat identifies the case in which a CR node is in the protection region of an incumbent node (i.e., the coverage area of a digital TV broadcaster) but fails to detect the existence of the incumbent. An example of the hidden node problem is shown in Figure 5. A CR terminal does not sense the presence of a Primary User BS because of an obstacle (e.g., a mountain). 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 [6].

8) *Unauthorized use of spectrum bands for selfish use*. This threat identifies the case where a malicious node or CR network uses spectrum bands for which is it not authorized, to gain more traffic capacity or bandwidth [4].

9) *Unauthorized use of spectrum bands for DoS to primary users*. This threat identifies the case where a malicious node or CR network emits power in unauthorized spectrum bands to cause DoS to primary users [7].

10) *Saturation of the cognitive control channel*. This threat 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. Note that specific designs of the CCC may prevent this type of attack.

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

12) *Disruption to the MAC, network layer, or cognitive engine of the cognitive radio network*. This threat includes attacks against the higher functions of the CR network, including the MAC, network layer, and cognitive engine.

IV COGNITIVE RADIO PROTECTION TECHNIQUES

Masquerading attacks and the distribution of false information in cooperative CR networks in relation to CR functions (i.e., spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility) are perceived by the research community as the most significant threats to CR [6]. In the current collaborative sensing schemes, secondary users are usually assumed to be trustworthy. Such schemes may fail in the presence of a masquerading threat.

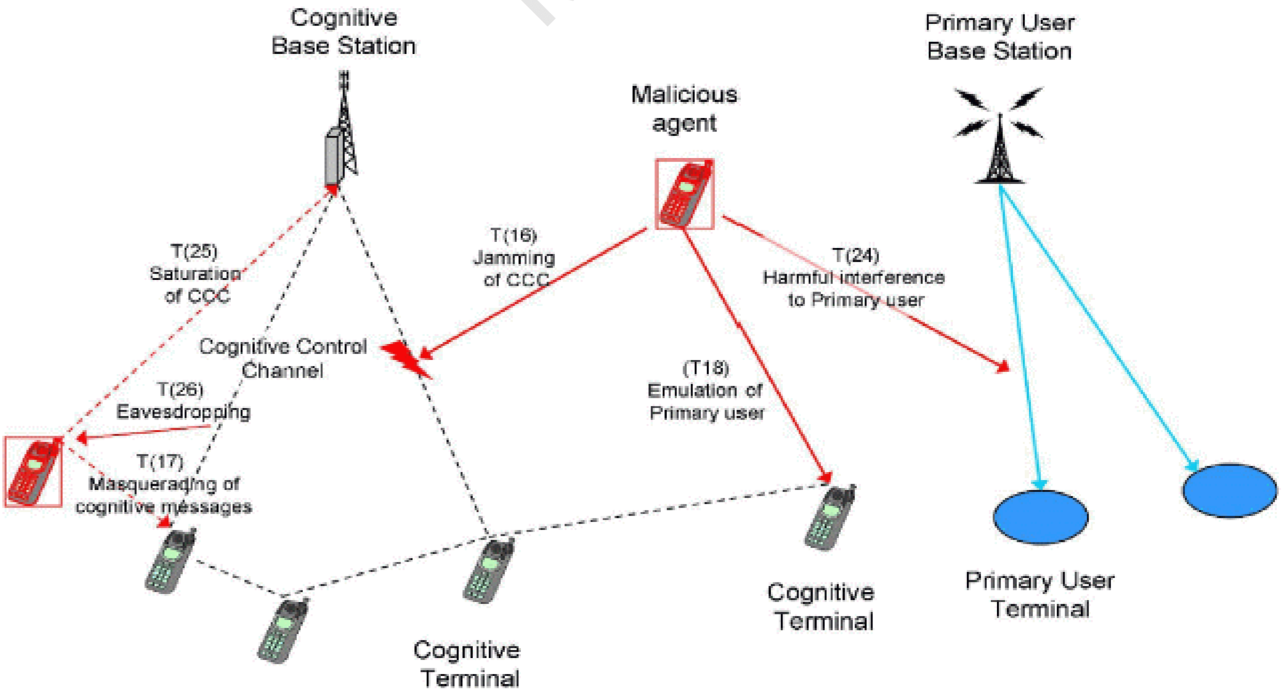
Cognitive Base Station
Primary User Base Station
Malicious agent
T(25) Saturation of CCC
T(16) Jamming of CCC
T(24) Harmful interference to Primary user
Cognitive Control Channel
T(26) Eavesdropping
(T18) Emulation of Primary user
T(17) Masquerading of cognitive messages
Cognitive Terminal
Cognitive Terminal
Primary User Terminal

Fig 4. Cognitive Radio Threats

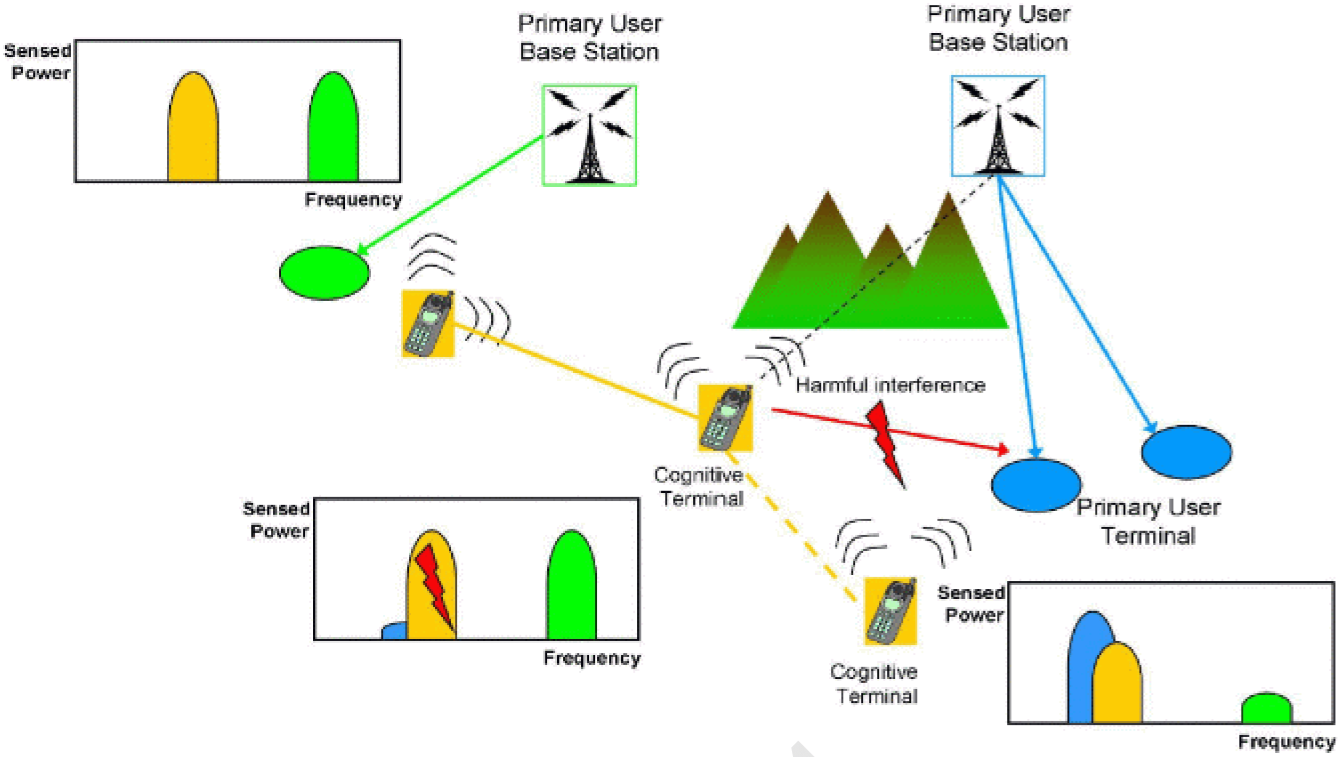

Fig 5. Hidden Node Problem

A number of protection techniques have been proposed by various authors to address such threats and improve the robustness of collaborative sensing algorithms.

We can classify the protection techniques against these types of threats in the following categories:

1) Protection techniques based on reputation and trust of the CR nodes.

2) Identification of the masquerading threat though signals analysis.

3) Authentication of the CR node through cryptographic techniques.

4) Geolocation database of primary users.

1) Protection techniques based on reputation and trust of the CR nodes

A number of protection techniques are based on the concepts of reputation or trust of the CR nodes (BS or terminals). For example, in the spectrum sensing function, a CR node can be classified at different levels of reputation or trust on the basis of spectrum sensing information, which they provide to the other nodes in the CR network. If the information is not correct after a number of iterations, then the contribution of that specific CR node is considered not valid, that may hint to a security threat by a malicious CR node.

2) Identification of the masquerading threat through signal analysis

This protection technique is based on signal analysis to distinguish a malicious attacker from a licensed user. This technique is mainly used to address threat here a malicious attacker can "masquerade" as an incumbent transmitter by transmitting unrecognizable signals in one of the licensed bands, thus preventing other secondary users from accessing that band.

3) Authentication of the CR node through cryptographic techniques

A number of papers have proposed authentication of CR nodes based on similar mechanisms already defined for other types of wireless networks like ad hoc networks. The challenge of this approach is that SDR/CR should be able to interface with a variety of communication systems and satisfy different security requirements. The authentication procedures defined for a specific communication network (e.g., UMTS) may not be apt for SDR/CR networks. The authentication mechanism should be extendible to all the communication systems with which the CR nodes have to interface.

4) Geolocation database of primary users

In the geolocation database approach, the CR network provider maintains a database with the position and transmission features (e.g., power) of all the primary users in the area. The CR geo-locates itself though the GNSS (e.g., GPS) and compares the data received from the spectrum sensing functionality with the known position of the primary users. A mismatch may indicate a malicious attacker. The database of the primary users can be downloaded periodically from a server. The position of the primary users' emitters does not change very frequently (e.g., in the order of months), so the database updates and related CR node synchronization will not have an impact on the performance of the system [7]. In comparison to other protection techniques, this approach are relatively simple to implement as the spectrum sensing functions in the CR node do not have to be very sophisticated.

V ACKNOWLEDGEMENT

Cognitive radio is a revolutionary solution towards even more efficient usage of the radio spectrum in a very intelligent way. By several spectrum detection and analysis techniques this can be achieved. Cognitive radio technology provides future wireless devices with additional bandwidth, reliable broadband communications, and versatility for rapidly growing data applications [1].

In this survey, the cognitive radio basics, network architecture and applications are presented, and then spectrum sensing and security issues of cognitive radio networks are discussed. More cryptographic solutions to CR are very much required to overcome the increasing security threats caused due to the distributed nature of CR networks. We show the promising future of cognitive radio in high speed seamless wireless communication with low implementation cost. New solutions with higher spectrum efficiency and also pipeline model of collaborative spectrum sensing are effective topics for future research work.

REFERENCES

[1] Beibei Wang and K. J. Ray Liu" Advances in Cognitive Radio Networks: A Survey" IEEE journal of selected topics in signal processing, vol. 5, no. 1, February 2011

[2] K-L. Du, Wai Ho Mow"Affordable Cyclostationarity – Based spectrum sensing for CR with smart antennas" IEEE transactions on vehicular technology, vol. 59, no. 4, May 2010

[3] Chao chen, Hongbing cheng, Yu-Dong Yao,"Cooperative Spectrum sensing in CR in presence of Primary User Emulation Attack" IEEE transactions on Wireless communications, vol. 10, no. 7, July 2011.

[4] Lingjie Duan, Alexander W.Min "Attack prevention for Collaborative spectrum sensing in CR" in IEEE journal on selected areas in communications, vol. 30, no. 9, October 2012.

[5] Z. Han and K. J. R. Liu, Resource Allocation for Wireless Networks:Basics, Techniques, and Applications. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[6] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," IEEE Commun. Surveys Tutorials, vol. 11, no. 1, pp. 116–130, First Quarter,2009.

[7] Gianmarco Baldini, Member,IEEE,Taj Sturman,Member,IEEE, Abdur rahim Biswas, Member, IEEE, Ruediger Leschhorn,Member,IEEE,"Security aspects of Software defined radio and Cognitive Radio Networks – A survey and a way ahead",IEEE communications surveys and tutorials,No.2,Vol.14,second quarter 2014.