COGNITIVE RADIO

Fernando Mc'kelligan

Date of submission: February 12, 2011

Index

Summary ...3
1. Cognitive radio communications ...3
1.1 Dynamic Spectrum Access ...3
1.2 Spectrum Management ...4
1.3 Characteristics of Cognitive Networks ...4
1.3.1 Cognitive capability ...4
1.3.2 Reconfigurable Capability ...5
1.3.3 Self-Organized Capability ...5
2. Cognitive radio networks ...6
2.1 Configurability and Adaptability on SDR ...7
2.2 Cognitive Radio Networks Architecture ...7
2.3 Terminal Architecture of CRN ...8
2.3.1 Transceiver Module ...9
2.3.2 Mode Switching Control ...10
2.3.3 Spectrum Sensing ...10
3. Opportunistic Spectrum Access in OFDMA Systems ...11
3.1 Transmitter detection ...12
3.2 Implementation of cognitive techniques in OFDMA ...12
3.2.1 Detection Method ...12
3.2.2 Prediction Method ...13
3.2.3 Hybrid of Detection and Prediction Method (HDPM) ...14
4. Security in cognitive radio. Analysis for the IEEE 802.22 standard ...14
4.1.1 Ranking for potential vulnerabilities in WRAN ...14
4.2.1 Non cognitive security mechanism ...15
4.2.2 Cognitive security mechanism ...16
References ...18

Summary

Nowadays and due to the faster increase on services available to be delivered to the end user, different wireless technologies such as GSM/GPRS, IEEE 802.11, Bluetooth, UWB, Zigbee, 3G (CDMA series), HSPA, 3G LTE, IEEE 802.16, etc. are playing a key role for supporting all these applications.

Traditionally each technology has been defined to operate in a specific band of frequency, it make possible among other things to reduce the interference between wireless systems. However, the trend for the incoming years introduces the challenge to support 'up to 1 trillion wireless devices by 2020' [1] with a relative limited electromagnetic spectrum.

Recently studies show discrepancies in the usage of the radio frequency spectrum. It is means that the channels which allocate resources are not used completely all the time, that is the especially case of 'frequency bands below 3GHz' [1] that most of the time are used to provide services which does not require line of sight as the mobile communications with the subscribers.

1. Cognitive radio communications

The Cognitive Radio (CR) features appear as a solution to deal with the low usage of the available resources going deep in the use of the spectrum in an opportunistic mode. CR makes possible share radio frequency channels in band of frequencies that in the traditional scheme of operability are restricted for others users or applications. Then, the goal of CRs techniques is improve the use of the radio frequency spectrum to provide high performance with Quality of Service for the end user, indistinctly to the network architecture which can be providing wireless services to them.

1.1 Dynamic Spectrum Access

Several dynamic spectrum access techniques integrates the cognitive radio concept, users in CR applications must apply different features [1], it is in order to share radio spectrum and be available to support the requirements regarding the quality of service proper of each wireless standard. The set of features can be described as follow:

- Spectrum sensing. This feature makes possible to know the available spectrum.
- Spectrum decision. It allows selecting the best available channel.
- Spectrum sharing. It is makes possible to perform the synchrony with others users using the channel.

- Spectrum mobility. This feature provides priority to some users over others, and it makes that the opportunist user leave the channel when other user with the right privileges require using the complete channel.

1.2 Spectrum Management

The spectrum management is the core of the cognitive radio set of features and it is the responsible to fulfill the necessities of user authorized to operate in the band being used as well as the CR's users.

In the other hand, the spectrum management not only involves the techniques for has access and sharing to the medium, also it is related with the price and operative costs. It is due to the use of electromagnetic spectrum shows different levels of occupancy on a common day, in other words at busy hour the cost for the use the electromagnetic spectrum can be significantly increased than in other scenarios [1].

1.3 Characteristics of Cognitive Networks

The Cognitive Radio Networks (CRN) is characterized by three different capabilities that involves the techniques of operability, then a CRN capabilities are:

- Cognitive capability. It makes possible to sense the wireless medium present for connectivity. As well, this capability provides a wide range of options for connections making the network highly reliable [1].
- Self-organized capability. This capability represents the way that the network analyses and learns from the information sensed. The capability to learn of the RF conditions make possible to reconfigure different parameters such as carrier frequency, transmit power, modulation, etc. which have a direct impact in the performance [1].
- Reconfigurable capabilities. Finally the last capability is the way in which the network will be adapted to the wireless medium present based on the information sensed and which was previously analyzed [1].

1.3.1 Cognitive capability

The cognitive capability is characterized by the procedures which are executed in order to ensure the quality on the connection with the wireless medium without produce negative effects in devices sharing the radio frequency spectrum. The set of procedures for this capability are listed as follow:

- Location identification. This feature make possible to know the current location on the system as well as the other wireless devices sharing the medium. It is with help of this capability that the system can perform smart settings of frequency and power to be accessible [1].

- Network system discovery. This feature is used for discover the best network available for a cognitive terminal. It can be used to find a reachable network using a direct path or with help of hopes that could be in a different network or working in a different wireless standard [1].
- Service discovery. It is related with the procedures which are executed by the network system discovery. Services available on the network are providing across this capability. The cognitive terminal must find the appropriate set of services that can support the applications for what it is looking for [1].

1.3.2 Reconfigurable Capability

In order to reconfigure the set of parameters and hardware that provides the access on the wireless medium, cognitive radio networks require to implement a system called Software-Defined Radio (SDR) as well as to implement other features that working with it make possible the reconfiguration of cognitive equipments, then the following features play the most important role inside of this category:

- Frequency agility: This feature is used in order to make enable the cognitive device to chance dynamically the operative frequency [1].
- Dynamic frequency selection: This feature is in charge to the selection of available frequencies (logical and physical channels) in order to avoid co-channel operations with other systems that could be using the same radio resource [1].
- Adaptive modulation/coding (AMC): The aim of this feature is to enable the cognitive device to be adapted to different modulations techniques and in consequence make the system available to work with other wireless standards which can be working in a different modulation scheme, at the same time the shift of modulation technique can be implemented to improve the quality on the wireless link in presence of noisy or fading effects [1].
- Transmit power control (TPC): This feature is implemented to perform the smart power control. It is, TPC reduces or increases the transmission power according to the necessities of the system [1].
- Dynamic system/network access: The propose of this feature is providing to cognitive devices with the ability of changing its set of parameters dynamically, it is in order to be able to support different wireless systems which could be operative in different standards of communication [1].

1.3.3 Self-Organized Capability

Self Organized Capability is a set of features that represent the understanding by the cognitive device of sensing and re-configurability capabilities, then it is the way that the devices is going to organize its protocols to support the applications. The set of features are the following:

- Spectrum/radio resource management: This feature represents the way that radio resources are going to be used to produce high efficiency with QoS [1].
- Mobility and connection management: The aim of this feature is to make the cognitive device available to discover wireless networks in which it can be attached as well as support the mobility for execute vertical handoffs [1].
- Trust/security management: This feature provides to cognitive networks of security protocols to be used in heterogeneous applications and wireless standards [1].

2. Cognitive radio networks

Cognitive radio systems are networks based on the functionality of software defined radio (SDR), which goal is the use of spectrum “under-utilization” [2] for multiples applications and in heterogeneous environments.

SDR can be characterized by two key set of parameters: configurability and adaptability. These features represent the core of SDR and the architecture of cognitive radio networks is based on its functionality.

In a different way, the implementation of SDR in handy devices represents the path that will lead to growing of “rapidly deployable heterogeneous wireless networks (RDWN)” [2].

Figure 2.1 illustrate a Rapidly Heterogeneous Wireless Network (RWDN) which some of the most important components. In the picture can be appreciate multiples user working with different modulation schemes, as well as the Differential Binary Phase Shift Keying (DBPSK) technique been used for two cognitive radios.

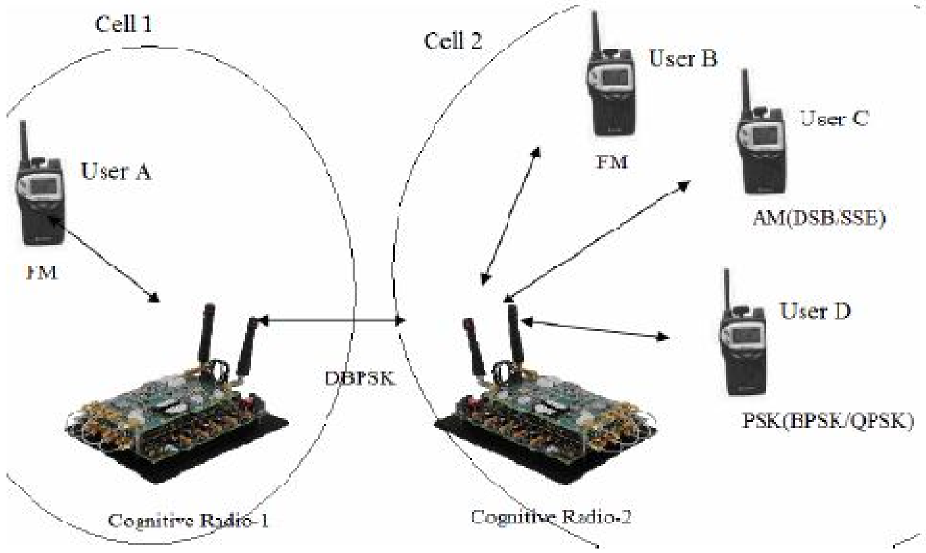

Figure 2.1: Heterogeneous Wireless Network (RWDN) [2].

2.1 Configurability and Adaptability on SDR

The configurability on SDR makes possible the interoperability among different communications standards, this feature represents the set of parameters required by operate the radio resources such as modulation techniques, frequency allocation and transmission power [2]. The entity responsible to execute the configurability inside of the cognitive device is digital transceiver which is located as a part of the communication management subsystem.

The adaptability represents the ability to select the correct operation model based on the sensed data such as bit error rate (BER), power consumption, signal to noise (SNR) and other interference levels presents on the wireless medium [2].

2.2 Cognitive Radio Networks Architecture

The cognitive radio networks based on SDR permit practically for every wireless device supporting the software applications be part of the RDWN.

The characteristics of SDR nowadays are managed by multiples architectures, e.g. Software Communication Architecture (SCA) and not only it makes possible work in a scheme based on modules, it can represent a represent a big challenge by constrains coming from the hardware [2].

In order to deal with this constraint the cognitive architecture has been classified as follow:

- Configurable digital transceiver
- Channel monitoring and spectrum sensing module
- Communication management and control

The Channel communication management and control subsystem is in charge of performing the tune the set of parameters related to the radio frequency activities and executed by the digital transceiver.

This module use the information which previously was analyzed on the monitoring and spectrum sensing module, based on it, the communication management module adjust the input parameters such as amplifier gain, operation frequency, channel filtering and bandwidth. The operation of this module is based on a block structure and it is characterized by its own physical layer specifications which at the same time are associated with the wireless standard properly of the device where the communication and control subsystem reside [2].

The most important functions that are executed on the Channel communication management and control subsystem are [2]:

- To take decisions based on the network performance
- Switching between different features
- Control of scanning in the wireless medium

2.3 Terminal Architecture of CRN

The platform for cognitive radio terminal can vary from providers, however in most of the cases the architecture can be represented by the modules as is showed in figure 2.3.1.

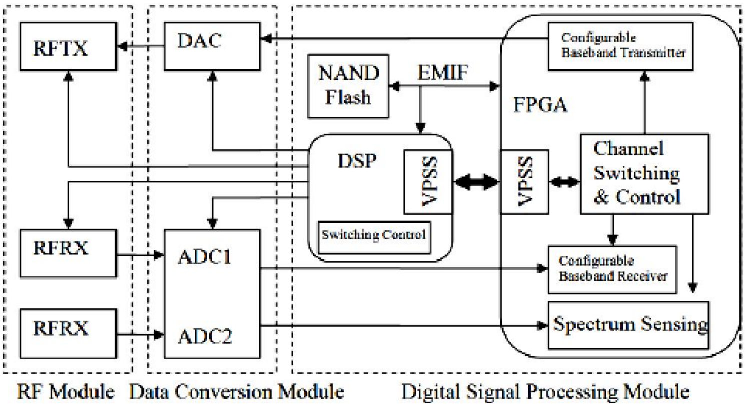

Figure 2.3.1: Block diagram of the cognitive radio system using SDR platform [2]

2.3.1 Transceiver Module

There are many limitations regarding the hybrid transceiver that must be taken in account when the device is being developed.
Cognitive devices includes two special modules which characteristics are strongly related with the connectivity in the network, they are configurable transceiver-interface and fixed Differential Binary Phase Shift Keying (DBPSK), both modules work as just one entity [2].
The configurable transceiver is design taking account different parameters such as in the case of sampling rate where the frequency IF is selected to be the same on the transmitter as in the receiver, it eliminated the necessity to use different clocks for synchrony between this entities. The common chosen frequency for the sampling rate is 125 MHz; in a different way the estimated channel coherence time provides a sample error rate estimation each 80 samples in the output [2].
DBPSK module inserts a logical channel into voice stream for a communication link between two cognitive devices. The aim of this application is perform a survey on the wireless medium, in order to reach up to four available channels with sample rate estimation [2].
It is important take in account that modulation and sampling rate conversion are responsible to improve the way as resources are managed

The modulation and sampling rate are two key factors to be taken in account in order to support different modulations techniques which could be present due to multiples wireless communications standards sharing the medium, as well to improve the constrains coming from the way that hardware resources are been used [2]. Then and based on these considerations, the following criteria receive a special importance at the moment to design a cognitive transceiver:

- Transmitted signal characteristics (Bandwidth)
- Sample rate conversion ratio
- Resolution (bit size)

Other modules present in the transceiver are signal generator and display, up/down conversion module, Digital to Analog Converter (DAC), Analog to Digital Converter (ADC) and RF Board. Not only all the modules has special functions, the two more relevant are the up/down conversion module and the DAC subsystem, the reason come from the direct relation that they keep with the constrains in the hardware resources [2].

The up/down conversion module includes the sampling and mixing subsystems where the sampling ratio is required for all communications channels; the sampling rate usually is set to 8 stages of conversion, the reason is due to it require the minimum quantity of hardware resources when different conversions configurations are implemented [2].

In a different way, the Digital Signal Processing (DSP) working with the FPGA module is responsible to execute the digital operations inside of the transceiver. The DSP module will be in charge to the execution regarding framing, modulation/demodulation and partial sampling conversion operations. On the other hand, the FPGA will execute the sampling and digital up/down conversions [2].

At the same time, the DSP will be responsible to perform switching operations with the digital signal and the FPGA will manage circular buffers to maintain the data integrity.

2.3.2 Mode Switching Control

The aim of the switching control mechanism is protecting the information from loss or data corruption in the time that the switched is being executed. In order to reach it objective, the switching control mechanism store the data information in a temporal buffer during the time when the switching functions are executed [2].
The size of the buffer keeps a direct relation with the number of samples creates during the interval of transmission between the transmitter and the receiver [2].
The cognitive radio scheme presents two different switching modes:

- Modulation Switching mode
- Radio Channel Switching mode

The mode switching control is implemented applying a known interference on the communication channel, as well as bit error rate and switching time are tested. However, when the presence of noisy is detected the cognitive radio must change to the closer channel available; the cognitive radio has a list of available channels regarding the spectrum sensing module [2]. At the same time, a good indicator of the presence of interference or noise is the BER, when it reach the value of 0.2 the communication must be switched and after this procedure the BER will be reset.
Finally other factor to be taken in account for the interference detection delay, that is the time between when the system detect the interference and when the system has finish to execute the switching; this time can vary based on the BER measurements [2].

2.3.3 Spectrum Sensing

The spectrum sensing is a technique which bases its functionality on the average energy that can be detected with the use of Fast Fourier Transform Algorithm (FFT) regarding the output amplitude for different cycles.
The cognitive software scans the spectrum with a mechanism that implement a sweep of frequency that comes from 200 to 930 MHz, first the entire spectrum is split in multiple channels, after that each channel is analyzed by the software sweep mechanism until the complete spectrum is scanned [2].

The Spectrum Sensing subsystem is an entity located inside of the FPGA module, but the entity responsible to execute the control of sweeping mechanism is the DSP.
On the other hand, in order to provides the enough capabilities to sweep the complete electromagnetic spectrum, the use of two radio frequency receivers is required; the first of them must be connected to one channel in the ADC dual module and it will be responsible to spectrum sensing, the second one must be connected to the other available channel present in the ADC module and it will be part of the configurable transceiver and in consequence responsible to execute the tasks given by this module [2].
Other of the responsibilities of this module is to deliver a list of available channels to the spectrum sensing module.

3. Opportunistic Spectrum Access in OFDMA Systems

Orthogonal Frequency Division Multiple Access (OFDMA) is a technique been used for sharing the electromagnetic spectrum with a scheme of multicarrier, this technique makes possible reduce the common issues present in wireless communication such as the Frequency Selective Fading (FSF) which produce Inter-symbol interference (ISI) [3]. At the same time, OFDMA has been designed to work with M-QAM modulation techniques and it is in consequence available to support high data rate.

However, the efficiency in the use of the RF spectrum in OFDMA can be enhanced with the use of cognitive radio systems, which are being deployed in order to give a better use to the radio resources that most of the time are being wasted [3].

Also it is important recognize the difference among OFDM and OFDMA. In OFDM “all sub-carriers are allocated to one user while in OFDMA the sub-carriers are partitioned into different groups named sub-channel”, sub-channels not necessary need to be adjacent [3].

As was mentioned previously, cognitive radio can be visualized as a smart radio with the capabilities to interact with the radio spectrum changing its set of parameters (operating frequency, modulation, transmission power and protocols properties of the communication standard) to operate in the white spectrum which is being wasted for other systems [3].

The cognitive cycle involves the following task (which previously were described) spectrum sensing, spectrum management, spectrum mobility and spectrum sharing. Due to the core of the OFDMA is a the technique to have the access to the medium, the approach of this analysis will be performed based on the spectrum sensing capability and in particular in the transmitter detection to find free sub-channels in the downlink for OFDMA systems.

3.1 Transmitter detection

The approach for the transmitter detection feature is to determine if there are present any signal from a licensed user (primary transmitter) or not in a specific frequency, it is to identify if the spectrum is free to be used for a cognitive device [3].

At the same way, the transmitter detection can be classified according to two different criteria used for perform the sensing:

- Matched filter detection. For this classification the cognitive terminal is synchronized with primary transmitter, and the CR has previous knowledge regarding the type of modulation, shape of pulse, packet format among others being used by the licensed user. So, the CR terminal use this information to run different tasks which generate a mirror signal which will be compared with any signal present in the channel in order to determine if it has an hole or not [3].
- Energy Detection. This technique is implemented when the CR does not have enough information regarding primary users. CR terminal using this technique can not differentiate between types of signals; the analysis is just based in the presence or absence of energy in the channel [3].

3.2 Implementation of cognitive techniques in OFDMA

Three different systems make possible the implementation of cognitive radio techniques in OFDMA, the aim of this techniques is to determine if exist a vacancy on one channel in order to allocate a cognitive device there. Different criteria also needs be consider, it is due to it is possible reach a empty channel but at the same time other phenomena could be presents, such as noise or interference, then regarding these external factors the relation between carrier to noise as a criteria to perform the switching is introduced. The methods that can be implemented for the implementation of cognitive radio techniques in systems based on OFDMA are described as follow.

3.2.1 Detection Method

Detection Method. This method is a hybrid between matched filter detection and energy detection techniques. Then, detection method is a set of two techniques that are available to determine if the channel is empty or nor based on subcarrier based opportunistic detection method and sub-channel based energy detection [3].

The goal of the detection method is making possible that both techniques can operate as a functional unit, then the detection of subcarrier by itself not represent a reliable method to estimate the availability of the channel, the reason is because it can be deliver false alarms and misdetections. On the other hand, when the subcarriers are well known, the energy detection method can improve significantly the performance due to its performance use the average energy of all samples (where each sample represent on single subcarrier inside of the sub-channel), then the result is compared with a threshold that make possible to determine if it is empty or is been used. Both methods working together represent a robust feature which can enhance the performance [3].

3.2.2 Prediction Method

The goal of this method is to be available to determine the future status of the channel, based on the previous information sensed. The fundaments of this method comes from the string of zeros and ones that are present in all digital communications, then regarding the sequence of this binary digits two periods are defined T_{on} and T_{off}, where T_{on} represent a sequence of consecutives 1s and T_{off} a sequence of consecutive 0s, the difference of two consecutives sub-channel states is also known as Δt. So the sensing of a single sub-channel is a sampling period of Δt seconds [3].

Prediction Method creates a classification for the trends on the channel status regarding the sub-channel history, it is illustrated as follow:

1. Periodic traffic with fixed ON + OFF time.
2. Fixed PL with random ON – OFF time.
3. Fixed OFF time, random ON time.
4. Fixed ON time, random OFF time.
5. PL, ON – OFF are random.

The trends which are depending of the samples are after used for the algorithm known as Traffic Classification Algorithm (TCA). This algorithm is the responsible to execute the smart switch to an available channel. Also this method improve the efficiency of the spectrum due to "it reduces the channel switching up to 55%" reducing the delay and increasing the throughput [3].

On the other hand, this method has the constraint to be dependent of periodic traffic [3].

3.2.3 Hybrid of Detection and Prediction Method (HDPM)

Finally, this technique represent the mix of the two first methods, and as well as the Prediction Method, the TCA algorithm will be used in order to determine what technique must be used (Detection or Prediction Method) regarding the traffic conditions; the reason is because one method work better than the other under traffic conditions and vice versa, it is in other words, Detection Method not require an estimation based on periodic traffic but Prediction Method can improve the efficiency of the spectrum, so the decision will be executed based on the random or fixed periods T_{on} and T_{off}, and then implemented by the TCA algorithm [3].

4. Security in cognitive radio. Analysis for the IEEE 802.22 standard

The aim of this section is provide a short overview regarding the most important characteristics to be considered regarding security implementation on the IEEE 802.22 standard.

4.1 Summary of IEEE 802.22 Standards

The IEEE 802.22 also knows as Wireless Regional Area Network (WRAN) will be the first entire international standard with a cognitive nature. WRAN is being developed with considerable improvements on the physical layer (PHY), medium access control (MAC) and with the applications proper of the cognitive radio such as spectrum sensing functions (SSF), spectrum management (SM) and the co-existence versus security [4].

Other technical aspects that WRAN involves are OFDMA as the multiple access technique, communication point to multipoint (PMP) with architecture consistent of a central base station (BS) and surrounding users called customer premises equipment (CPE) [4].

The capacity of WRAN typically makes possible to allocate up to 255 users per channel on a single cell and provides a reliable data rates (per users in absence of undesired interference) for downlink 1.5 Mbps and Uplink 384 kbps [4]. Also WRAN introduces the self co-existence window (SCW) after of the time division duplexer (TDD).

4.1.1 Ranking for potential vulnerabilities in WRAN

WRAN ranks different vulnerabilities according to the level of damage that they can produce to the network. The classification for the risk goes from 1 to 9 and at the same time it can be classified according to probability and impact in three different categories that are in the range of 1 (lowest) to 3 (highest). The table 4.1.1.1 shows the risk evaluation created by the risk evaluation [4].

		Rationale		
Criteria	Cases	Difficulty	Motivation	Rank
Likelihood	Unlikely	Strong	Low	1
	Possible	Solvable	Reasonable	2
	Likely	None	High	3
		User	System	
Impact	Low	Annoyance	Very limited outages	1
	Medium	Loss of service	Limited outages	2
	High	Long time loss of service	Long time outages	3
Risk	Minor	No need for countermeasures		1, 2
	Major	Threat need to be handled		3, 4
	Critical	High priority		6, 9

Table 4.1.1.1: Risk evaluation for WRAN

The action to be implemented is totally dependent on the level of risk, e.g. a minor risk can be ignored since it can produce a minimum impact on the performance of the network, but major or critical risks must be managed carefully due to they can produce severe degradation on the system [4].

4.2 Security Mechanism

Cognitive radio networks can operate in multiples wireless standards, band of frequencies and support multiples applications, in other words a cognitive radio network perform more functions and processes than traditional schemes of wireless communications and it is traduced on more security challenging. The security mechanism in CRN can be split in different modules for protecting the non cognitive functions as well as the proper of the cognitive nature [4].

4.2.1 Non cognitive security mechanism

Traditional security mechanism must ensure the availability, authentication, authorization, identification, data integrity, confidentiality, and privacy.

WRAN has contributed to improve the privacy key management version 1 (PKMv1) and 2 (PKMv2) "in order to introduce a more robust and advanced ciphering model that at the same time introduces a counter with cipher block chaining based on encryption and authentication scheme" [4]. Under this scheme BS and CPE have two keys authorization and two traffic encryption keys to be used in the network.

Finally the scheme for non cognitive applications inside of WRAN eliminates the HASH message for authentication (HMAC) and the cipher message authentication code (CMAC) [4].

4.2.2 Cognitive security mechanism

The nature cognitive of WRAN requires the introduction of a new block of applications regarding the security, also known as Security Sub-layer 2 and it is located in the cognitive plane.

Some of the mechanism implemented regarding the security at this layer also can have a direct impact in other cognitive modules such as SSF or Geo-location, e.g. signal classification, correlation, etc.

The most important security functions performed by security sub-layer 2 are classified as follow:

A. Availability. It represents the set of procedures performed by the CRN in order to sense the available spectrum, and for making it reachable to the CPEs. This function is responsible to ensure the availability of radio resources for licensed users and secondary cognitive terminals. Other of its functions it to minimize the Denial of Service (DoS) attacks against BS, CPEs or other device interacting with the cognitive radio [4].
   Mutual spectrum sensing and signal classification is used in order to have a better perspective regarding the use of the spectrum. Not only most of the algorithms used to determine the availability on the RF spectrum are based on energy detection, they represent some gaps in terms of security, then in order to minimize the DoS attacks algorithms based of detection methods represent a more robust feature in terms of authentication.
   The correlation between the sensed information and which is stored by the network in the internal data base is used to ensure the availability of the electromagnetic spectrum for the primary users [4].

B. Authentication. This feature is implemented in cognitive networks to determine between primary and secondary users. The main functions executed by this application are [4]:
   - Signal Validation for primary and secondary users.
   - Detect and counter attacks which are trying to use the available spectrum as well as the called man-in-the-middle.
   - Detect and count attacks the kind of spoofing and others similar.
   - Validate geolocation information

- Authenticate information for neighboring networks.
- Detect and inform regarding information which can be fake form different entities CPE.

C. Authorization. This feature represents the set of procedures required to allow access to resources on the network. The main functions performed for this feature are [4]:
  - To provide rights to users or entities inside of the network over the parameters that can be configured for the spectrum management capabilities.
  - To configure information that must be ciphered and authenticated.
  - To provide rights to BS in order to be available to eliminate secondary CPEs when they represent an issue for the performance of the primary users.

D. Identification. This feature is the complement for the authentication application; it helps to ensure that primary and secondary users can be identified. The mechanism involved on this application are [4]:
  - To identify CPEs and BS transmitting or receiving.
  - To ensure that the identification methods cannot be susceptible for incoming attacks.

E. Integrity. It is responsible to ensure that the information which is being transmitted will arrive to its destiny without distortion or that it can be corrupted. Integrity is in charge to execute the following functions [4]:
  - To provide protection versus false CBP signals
  - To protect versus attacks which can use valid information transmitted previously.

F. Confidentiality/Privacy. This application is implemented for encrypt information at the data link and upper layers. It provides [4]:
  - Robust ciphering and encryption methods.
  - To execute different mechanism in order to protect the available spectrum from espionage for unauthorized users or hackers.

G. Collaborative sensing, correlation with geolocation, information fusion and decision making. Collaborative sensing is a technique which involves more than one RF sensor to verify the availability on the electromagnetic spectrum. The information sensed after that is correlated with the info which is stored in the database of the system in order to validate that the user information is correct. Based on this criteria, the BS will determine if can provide or not the right to use in an opportunistic way the RF spectrum [4].

References

[1] Kwang Cheng Chen & Ramjee Prasad (2009), "Cognitive Radio Networks". John Wiley & Sons Ltd. ISBN: 978-0-470-69689-7, 2009.

[2] Tachwali, Y.; Basma, F.; Reafi, H.H; "Cognitive Radio Architecture for Rapidly Deployable Heterogeneous Wireless Networks". Consumer Electronics, IEEE Transactions, Vol. 56, No. 3, August 2010. ISSN: 0098-3063. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5606279 [Accessed 2011-02-06]

[3] Ahmad, S.; Shahid, A.; Ahmad, R.M.; Akram, A; Nasim, M.A;. "Opportunistic Spectrum Access in OFDMA Systems". Second International Conference on Computer and Network Technology (ICCNT), 2010. Print ISBN 978-0-7695-4042-9, Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5474504 [Accessed 2011-02-09].

[4] Mody, A.N.; Reddy, R.; Kiernan, T.; Brown, T.X.; " Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard". Military Communications Conference, 2009. MILCOM 2009, IEEE. Print ISBN: 978-1-4244-5238-5. Available from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5380058 [Accessed 2011-02-09]