Abstract - The frequency spectrum bandwidth used in modern wireless systems is limited while the number of wireless systems is rapidly increasing. In order to reduce the spectrum scarcity, secondary systems can opportunistically access the temporarily unused licensed bands of primary systems which are known as spectrum holes or white spaces, by altering their transmitting parameters so that the interference is minimum to primary user. Cognitive radio is the exciting technologies that offer new approaches to the spectrum usage. Cognitive Radio provides a tempting solution to spectral crowding problem by introducing the opportunistic usage of frequency bands that are not heavily occupied by their licensed users. This paper survey intoduce fundamental of cognitive radio technology, architecture of a cognitive radio network and its applications are first introduced.

Keywords: Cognitive radio, Cognitive radio Network, Primary User, Secondary User, Spectrum Sensing

I. INTRODUCTION

The concept of CR was first proposed by Dr. Joseph Mitola in 1999. Cognitive radio technology is the key technology that enables a network to use spectrum in a dynamic manner. The term, cognitive radio, can be formally defined as follows: A Cognitive Radio is a radio that can change its transmitter “parameters based on interaction with the environment in which it operates” [1].

Since a cognitive radio operates as a secondary user which does not have primary rights to any pre-assigned frequency bands, it is necessary for it to dynamically detect the presence of primary users. From this definition, two main characteristics of the cognitive radio are defined as follows [2], [3]:

- Cognitive capability: Cognitive capability refers to the ability of the radio technology to capture or sense the information from its radio environment. Through this capability, the portions of the spectrum that are unused at a specific time or location can be identified. Consequently, the best spectrum and appropriate operating parameters can be selected.
- Re-configurability: The cognitive capability provides spectrum awareness whereas re-configurability enables the radio to be dynamically programmed according to the radio environment. More specifically, cognitive radios can be programmed to transmit and receive over a broad range of frequencies and to use different transmission access technologies supported by their hardware.

The cognitive radio enables the usage of temporarily unused spectrum (figure 1), which is referred to as spectrum hole or white space. Spectrum holes are frequency bands left unused by a primary used for a certain amount of time. In order to exploit the spectrum holes, the cognitive radio can adjust its transmission parameters.

II. COGNITIVE RADIO CYCLE

The main functions of cognitive radio are Spectrum Sensing, Spectrum mobility, Spectrum management and Spectrum Sharing. The cognitive radio technology will enable the users (a) to determine which portions of the spectrum is available and detect the presence of licensed users when a user operates in a licensed band (spectrum sensing), (b) to select the best available channel (spectrum management), (c) to coordinate access to this channel with other users (spectrum sharing), and (d) to vacate the channel when a licensed user is detected (spectrum mobility)[1]. Figure shows a Cognitive radio cycle [4].

- Spectrum Sensing: As the first and most important function of a cognitive radio, it is the process of detecting unused portions of spectrum in order to use them opportunistically.
- Spectrum management: Once the spectrum holes are detected, the cognitive radio must then have the ability to choose the channel that suits its communication requirements.
- Spectrum mobility: Since the cognitive radios are given lower priority, they should be able to suspend their communication in case a licensed user comes back and seamlessly move onto another vacant channel.
- Spectrum sharing: In a network there must a scheduling algorithm involved to ensure that all the cognitive radios get a fair chance to use the spectrum [1].
Since the cognitive (unlicensed) users utilize the licensed band, they must detect the presence of licensed (primary) users in a very short time and must vacate the band for the primary users.

III. COGNITIVE RADIO NETWORK

The components of the cognitive radio network architecture, as shown in Figure 3 can be classified in two groups as the primary network and the cognitive network. Primary network is referred to as the legacy network that has an exclusive right to a certain spectrum band. While, cognitive network does not have a license to operate in the desired band.

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 spectrum broker [5].

The spectrum broker collects operation information from each secondary network, and allocates the network resources to achieve efficient and fair spectrum sharing.

IV. SPECTRUM SENSING

Spectrum sensing technique can be categorized into two types. They are: Direct and Indirect Techniques. Direct Technique is also called as frequency domain out in which estimation is carried out directly from signal approach. Where as in Indirect Technique (also called as time domain approach), in this technique estimation is performed using autocorrelation of the signal. Another way of classification depends on the need of spectrum sensing as stated below.
A. Spectrum Sensing for Spectrum opportunities
1) Primary transmitter detection: Based on the received signal at CR users the detection of primary users is performed. This approach includes matched filter (MF) based detection, energy based detection, covariance based detection, waveform based detection, cyclostationary based detection, Primary Transmitter Detection etc.
2) Cooperative and collaborative detection: The primary signals for spectrum opportunities are detected reliably by interacting or cooperating with other users, and the method can be implemented as either centralized access to spectrum coordinated by a spectrum server or distributed approach implied by the spectrum load smoothing algorithm or external detection.

B. Spectrum Sensing for Interference Detection
1) Interference temperature detection: In this approach, CR system works as in the ultra wide band (UWB) technology where the secondary users coexist with primary users and are allowed to transmit with low power and are restricted by the interference temperature level so as not to cause harmful interference to primary users.
2) Primary receiver detection: In this method, the interference and/or spectrum opportunities are detected based on primary receiver’s local oscillator leakage power

A. Primary Transmitter Detection: In this we are going to discuss about few primary transmitter detection techniques. They are:
1) Energy Detection: In this technique there is no need of prior knowledge of Primary signal energy

Where $H_0 = \text{Absence of User}$.

Where $H_1 = \text{Presence of User}$.

The block diagram for the energy detection technique is shown in the Figure 4. In this method, signal is passed through band pass filter of the bandwidth $W$ and is integrated over time interval. The output from the integrator block is then compared to a predefined threshold. This comparison is used to discover the existence of absence of the primary user. The threshold value can set to be fixed or variable based on the channel conditions.

$$y(k) = n(k) \text{…………… } H_0$$
$$y(k) = h * s(k) + n(k) \text{…… } H_1$$

Where $y(k)$ is the sample to be analyzed at each instant $k$ and $n(k)$ is the noise of variance $\sigma^2$. Let $y(k)$ be a sequence of received samples $k \in \{1, 2, \ldots, N\}$ at the signal detector, then a decision rule can be stated as,

$$H_0 \ldots \text{ if } \varepsilon > v$$
$$H_1 \ldots \text{ if } \varepsilon < v$$

Where $\varepsilon = \mathbb{E}[y(k)]$ the estimated energy of the received signal and $v$ is chosen to be the noise variance $\sigma^2$.

2) Matched Filter:

Where $H_0 = \text{Absence of User}$.

Where $H_1 = \text{Presence of User}$.

A matched filter (MF) is a linear filter designed to maximize the output signal to noise ratio for a given input signal. When secondary user has a priori knowledge of primary user signal, matched filter detection is applied. Matched filter operation is equivalent to correlation in which the unknown signal is convolved with the filter whose impulse response is the mirror and time shifted version of a reference signal. The operation of matched filter detection is expressed as:

$$Y[n] = \sum h[n-k] x[k]$$

Where ‘x’ is the unknown signal (vector) and is convolved with the ‘h’, the impulse response of matched filter that is matched to the reference signal for maximizing the SNR. Detection by using matched filter is useful only in cases where the information from the primary users is known to the cognitive users.

B. Cooperative Techniques
1) Decentralized Uncoordinated Techniques: In uncoordinated techniques Cognitive Radio will independently detects the channel and will vacate the channel when it finds a primary user without informing the other users. So these are not advantageous when compared to coordinated techniques.
2) Centralized Coordinated Techniques: Here in this...
technique we have Cognitive Radio controller. When one
Cognitive Radio detects the presence of primary user then it
intimates the Cognitive Radio controller about it. Then that
controller informs all the Cognitive radio users by broadcast
method.
3) Decentralized Coordinated Techniques: This type of
coordination implies building up a network of cognitive radios
without having the need of a controller. Various algorithms
have been proposed for the decentralized techniques among
which are the gossiping algorithms or clustering schemes,
where cognitive users gather to clusters, auto coordinating
themselves. The cooperative spectrum sensing raises the need
cost sensor node close to a primary user's receiver in order to
detect the local oscillator (LO) leakage power emitted by the
RF

<table>
<thead>
<tr>
<th>Spectrum Sensing Technique</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matched Filtering</td>
<td>Optimum performance</td>
<td>Requires full primary signal knowledge, high power consumption and implementation complexity</td>
</tr>
<tr>
<td>Energy Detection</td>
<td>Low complexity, no primary knowledge required</td>
<td>Vulnerable to noise uncertainty</td>
</tr>
<tr>
<td>Cyclo Feature Detection</td>
<td>Robust to interference and noise uncertainty</td>
<td>High computational complexity, vulnerable to sampling clock offsets and model uncertainties, long observation time</td>
</tr>
</tbody>
</table>

Table 1: Summary of main spectrum sensing Technique

front end of the primary user's receiver which are within the
communication range of CR system users. The local sensor
then reports the sensed information to the CR users so that
they can identify the spectrum occupancy status. We note that
this method can also be used to identify the spectrum
opportunities to operate CR users in spectrum overlay.
2) Interference Temperature Management: The basic idea
behind the interference temperature management is to set up
an upper interference limit for given frequency band in
specific geographic location such that the CR users are not
allowed to cause harmful interference while using the specific
band in specific area. Typically, CR user transmitters control
their interference by regulating their transmission power (their
in CRNs. There is an inherent requirement to distinguish
between PUs and CRUs. Therefore, authentication can be
considered as one of the basic requirements for CRNs. In the
infrastructure based CRNs, where the primary and secondary
BSs are connected to a wired backbone network, it may be
for a control channel, which can be implemented as a
dedicated frequency channel or as an underlay UWB channel

C. Interference Based Detection: In this section, we present
interference based detection so that the CR users would
operate in spectrum underlay (UWB like) approach.
1) Primary Receiver Detection: Primary receiver emits
the local oscillator (LO) leakage power from its RF front end
while receiving the data from primary transmitter. It has been
suggested as a method to detect primary user by mounting a
low
out of band emissions) based on their locations with respect
to primary users. This method basically concentrates on
measuring interference at the receiver. The operating principle
of this method is like an UWB technology where the CR users
are allowed to coexist and transmit simultaneously with
primary users using low transmit power that is restricted by
the interference temperature level so as not to cause harmful
interference to primary users[7].

V. SECURITY CHALLENGES IN COGNITIVE RADIO NETWORKS

Security and privacy have been essential problems since the
arrival of the information era. Security is essential in any
network and has been relatively well studied. There is a well-
defined security architecture, which consists of security
attacks, security mechanisms, and security services/requirements, to define, study, and evaluate security
needs in a systematic way. In the context of CRNs, the main
security goals include the following:
• Confidentiality: It prevents unauthorized disclosure of
transmitted information from passive attacks, such as
eavesdropping. This is achieved by employing ciphers and
encrypting the data to be transmitted with a secret key which is
shared only with the recipients. The encrypted data are then
transmitted and only the recipients with a valid key can
decrypt and read the data. This issue is even more pronounced
in CRNs, where the CRU access to the network is
opportunistic and spectrum availability is not guaranteed.
• Integrity: It ensures that the transmitted information is not
illegally modified. Modification includes changing, deleting,
creating, delaying, or replaying transmitted messages.
Integrity is extremely important in wireless networks because,
unlike their wired counterparts, the wireless medium is easily
accessible to intruders. A message integrity check (MIC),
which is used to verify the integrity of the message by the
recipient, can also be employed in CRNs.
• Authentication: The primary objective of an authentication is
to prevent unauthorized users from gaining access to protected
systems. It is a necessary procedure for verifying both an
entity’s identity and authority. Several aspects of
authentication issues should be considered when securing
collaborative
works
easier to have the certificate authority (CA) or TTP connected
to the wired backbone. However, in the infrastructure less
CRNs with a number of CRUs dispersed over a large
dis geographical area, providing the functionalities of a CA can be
quite a challenge.
The usage of frequency spectrum is increasing, it is becoming more valuable. So we need to access the frequency spectrum wisely. For this purpose we are using Cognitive Radio. In our paper we discussed about the cognitive radio concept including cognitive radio cycle, Network Architecture, Spectrum sensing techniques and security challenges of cognitive radio.

VI. REFERENCES


