COGNITIVE SENSOR NETWORKS

LIMITED SPECTRUM CHALLENGES

The limited spectrum resource can not meet the growing demand of wireless application.

In addition, due to the existing fixed spectrum allocation strategy, most frequency bands are specified for the licensed user (LU) where the other communication device is not allowed to utilize it in spite of the unoccupied band.

For example, the frequency range between 512 MHz and 608 MHz is assigned as TV channel 21−36, which means that only TV user can use it, but the others can not occupy it at any time.

A mass of allocated frequency bands cause that the available spectrum is so little.

Even more unfortunately, the spectrum utilization rate of LU are unexpectedly under 30% [1], as shown in Figure 1.1. The fixed mobile frequency band 1850−1990 MHz and the air traffic control frequency band 108−138 MHz are even used at 5%

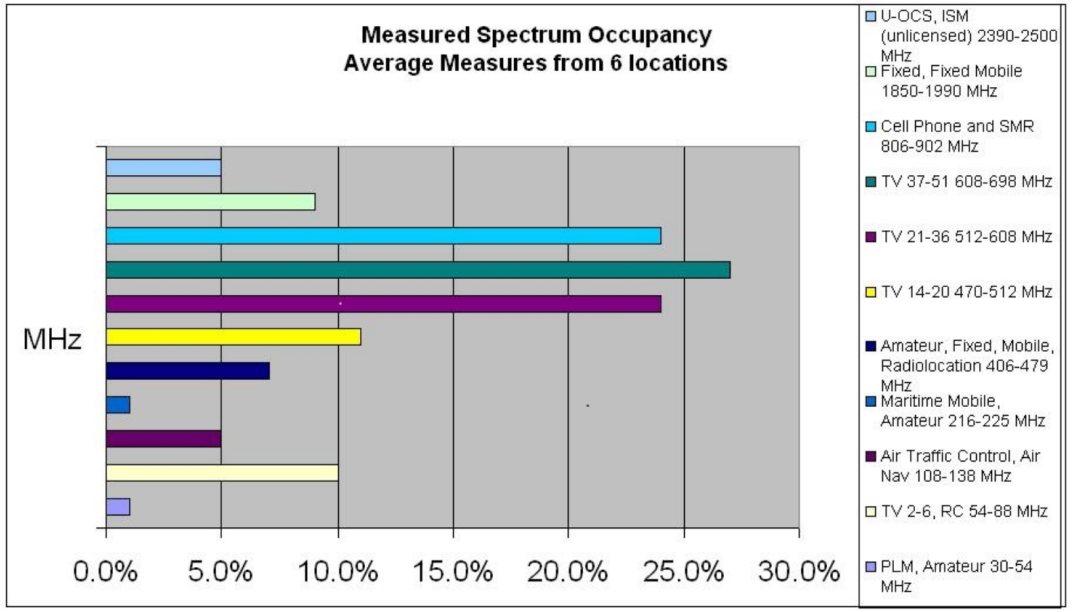


Figure 1.1 – A snapshot of spectrum utilization where each band averaged over 6 locations [1].

In order to solve the scarcity of spectrum resource and the low spectrum utilization, dynamic spectrum allocation (DSA) which is a flexible and intelligent spectrum management mode has been proposed. In DSA, according to the actual requirements of wireless communication system, spectrum resource is dynamically allocated to those wireless systems.

SPECTRUM MULTIUSER APPROACH

Wireless sensor network (WSN) includes a massive number of sensor nodes which performs sensing, processing and observing physical parameters in a distributed manner.

The sensor nodes gather fixed data like temperature, acoustics, pressure, gas level, movement, and so to observe the environment for daily activities as well as military purposes.

The available frequency spectrum for wireless communication is exhausting and almost the complete spectrum is used at some space–time point. And as such, it is becoming rather difficult to deploy SN in large scale deployments.

This has triggered the development of dynamic spectrum access schemes.

The key enabling technology providing dynamic, i.e., opportunistic, spectrum access is the cognitive radio (CR).
Cognitive radio has the capability to sense the spectrum and determine the vacant bands. By dynamically changing its operating parameters, cognitive radio can make use of these available bands in an opportunistic manner surpassing the traditional fixed spectrum assignment approach in terms of overall spectrum utilization.

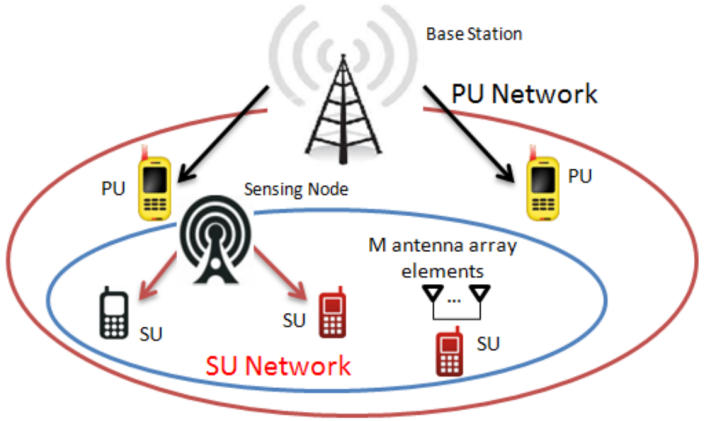
COGNITIVE-RADIO ENABLED SENSORS

With these capabilities, cognitive radios can operate in licensed bands as well as in unlicensed bands. In licensed bands, wireless users with a specific license to communicate over the allocated band, i.e., the primary user (PU), has the priority to access the channel.

Cognitive radio enabled sensors, called secondary users (SU), can access the channel as long as they do not cause interference to the PU.

Upon the natural habitants of a specific frequency band, i.e., PU, start communication; the cognitive radio enabled sensors must detect the potentially vacant bands, i.e., spectrum sensing.

Then, they decide on which channels to move, i.e., spectrum decision. Finally, they adapt their transceiver so that the active communications are continued.



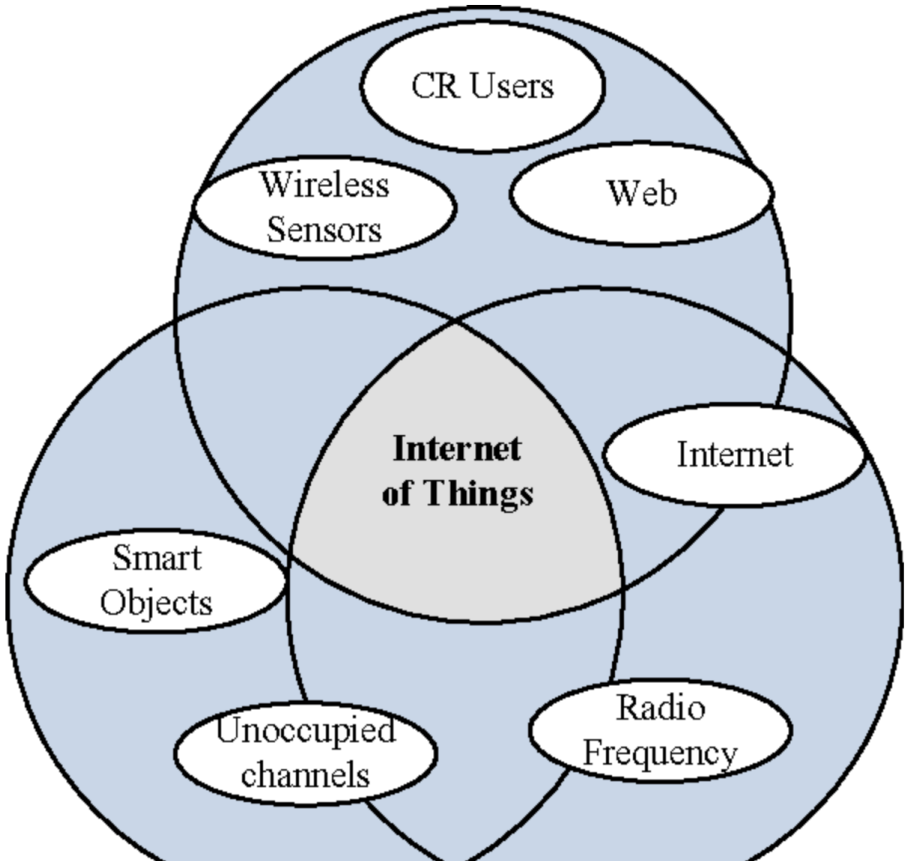
COGNITIVE NETWORKS

The word ‘cognitive’ has recently been used in several different contexts related to computing, communications and networking technologies, including cognitive radio and discussed later, and cognitive networks. Several definitions of cognitive networks have been proposed.

For example, one view presents a vision for cognitive networks in which networks should be self-aware in the sense that they can make configuration decisions in the context of a mission and a specific environment.

Networks that manage themselves require a new kind of technology known as cognitive technology. They should understand what the application is trying to accomplish, and an application should be able to understand what the network is capable of doing at any given moment.

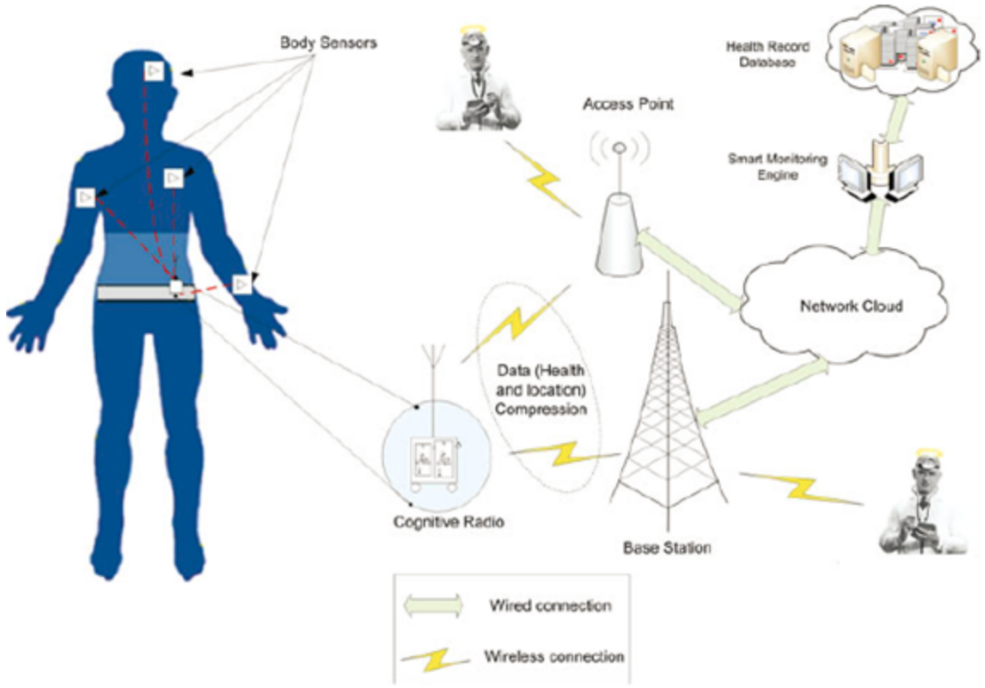
This would allow a network to make use of new capabilities by learning application requirements and dynamically choosing the network protocol that will meet these requirements. Domain-specific languages that could enable users and operators to describe their goals and requirements, and the statements in such languages would be used by the cognitive network to determine the proper balance of resources.



COGNITIVE NETWORKS

Another view defines the term ‘cognitive’ when applied to networks to refer to the intended capability of the network to adapt itself in response to conditions or events, based on reasoning and the prior knowledge it has acquired.
Adding a cognitive layer on top of an active network, however, doesn’t make that network a cognitive network. It needs to provide an end-to-end performance, security, quality of service and resource management, and satisfy other network goals.

Another view defines a cognitive network as a network that can dynamically alter its topology and/or operational parameters to respond to the needs of a particular user while enforcing operating and regulatory policies and optimizing overall network performance. As such, cognitive networks would use self-configuration capability to respond and dynamically adapt to the operational and context change, and feature a distributed management functionality that can be implemented in accordance with the autonomic computing paradigm.



PRINCIPLES OF BIOLOGICALLY INSPIRED NETWORKING

There are several key factors which can be observed in biological systems. Especially, features such as self–organization and robustness are of great importance when biological methods are applied to computer networks. However, there is also a trade–off to make when it comes to considering self–organized, distributed systems over those which are centrally controlled.

Although scalability is improved, the approach towards fully distributed topologies comes at a cost of performance. Since there is no global view of the entire network, global optimization of network parameters is no longer feasible. Methods searching for local ad hoc solutions may yield only inferior results, so a trade–off must be found which balances scalability with controllability and performance. The figure illustrates such a trade–off relationship.

As illustrated in the figure, The distinction is made between systems with centralized control and those that are fully self–organized. Distributed systems could be considered as intermediate, hybrid networks which allow the management of large numbers of nodes in a scalable way while preserving the benefits from a centralized control.

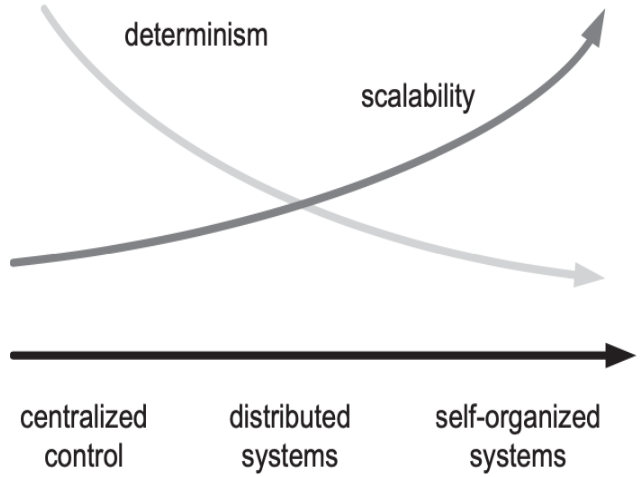


Figure 1.1 Trade-off between controllability and scalability in system control

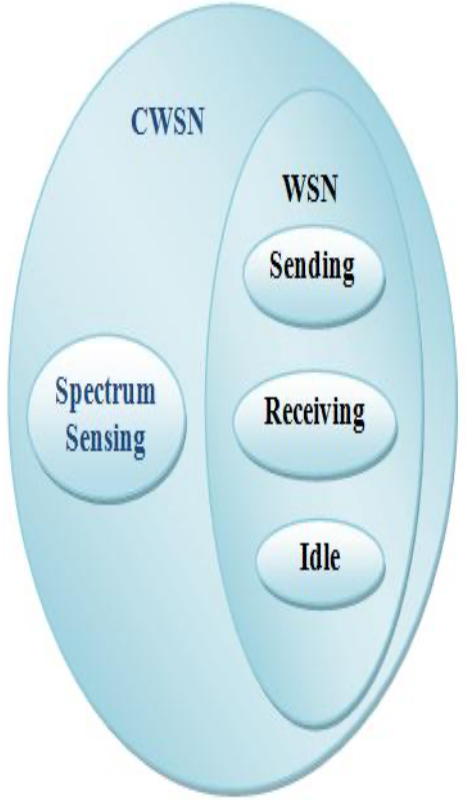
WSN VS CWSN

In CWSN, secondary users (SUs) sense the medium to identify the presence of unused frequency bands by licensed users called primary users (PU).

Next, SU make use of the available frequency bands for transmitting as well as receiving data. Hence, the identification of the available frequency band in the nearby area of SU is the main idea and purpose in CR, indicating spectrum sensing (SS).

SS take place in a centralized as well as distributed way. In a centralized way, every SU sense the frequencies and make a decision among them. In a distributed way, many SUs share the local sensing data to attain reliability and enhanced sensing performance. Presently, CR is mainly assumed as a major portion in the next generation networks.

The difference between WSN and CWSN is shown in Fig. 1. From the figure, it is clearly exhibited that the CWSN has an additional SS operation in which the WSN has no SS operations.



THE ADVANTAGES IN WSNS

- **Efficient spectrum utilization:** Current WSNs are deployed over unlicensed frequency band, such as industrial, scientific and medical (ISM) radio bands, which faces an increased level of interference from various wireless system. ISM bands are overcrowded which limits the development of new technologies. Dynamic spectrum access in CR is able to make SU cooperate efficiently with other types of users.
- **Multiple channels utilization:** In traditional WSNs referring to the detection of an event, several sensor nodes generate bursty traffic. Especially, when in densely deployed WSNs, a large number of sensor nodes attempt to access the same channel at the same time. It increases the probability of collisions and packet losses, which decreases the communication reliability with excessive power consumption. CWSNs access multiple channels opportunistically to alleviate these potential challenges.
- **Energy efficiency:** CWSNs may be able to change their operating parameters according to the surrounding channel conditions in order to avoid the power waste for packet retransmission due to packet losses in traditional WSNs.
- **Global operability:** Due to different spectrum regulations, a certain band in one

specific region or country may be available, while it is not available in another places. However, the sensor nodes with cognitive capability in CWSNs may overcome this potential problem.

CWSNs is defined as distributed networks of wireless cognitive radio sensor nodes, which sense event signals and collaboratively communicate their readings dynamically over available spectrum bands in a multihop manner to ultimately satisfy the application−specific requirements, which can be constructed by incorporating CR technology into the traditional wireless sensor networks (WSNs). Therefore, the sensor nodes in WSNs are equipped with cognitive ability, which may benefit the WSNs.

CR utilizes a mechanism called cognition cycle as shown in Figure 1.2 for sensing the spectrum (spectrum sensing, SS), determining the vacant bands (spectrum decision) and making use of these available bands in an opportunistic manner (spectrum mobility and spectrum sharing).

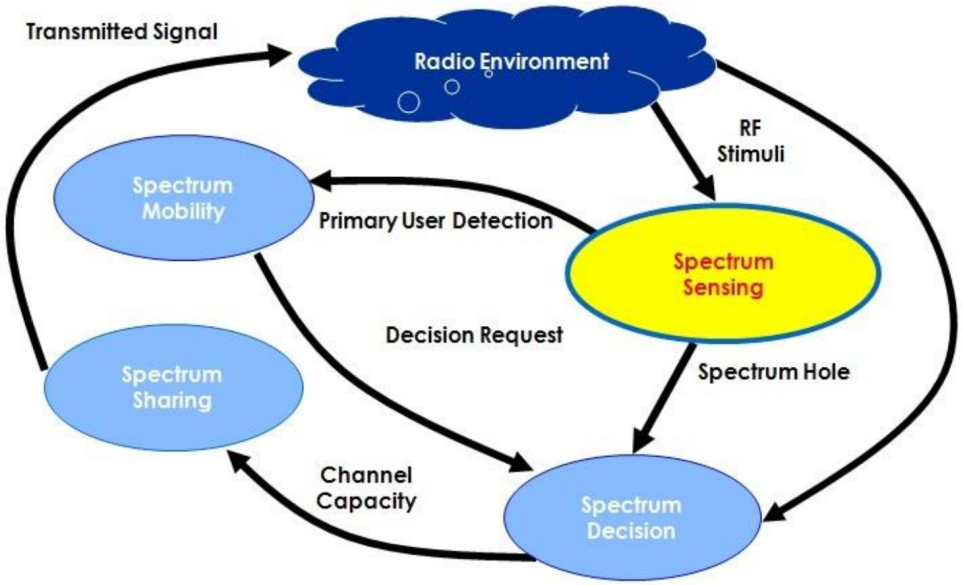


Figure 1.2 – Cognition cycle.

As the first step of cognition cycle, spectrum sensing plays an essential and central role in CR. The key of SS is that the cognitive user (as the secondary user, SU) needs to detect quickly and reliably that the licensed user (as the primary user, PU) is present or not in a considered frequency band.

There are various method of spectrum sensing for CR in the literature [9, 10], but a very few of them seem to be really suitable in the context of cognitive wireless sensor networks (CWSNs).

SPECTRUM SENSING

Spectrum sensing is the process of periodically monitoring a specific frequency band, aiming to identify presence or absence of primary users.

Spectrum sensing is a critical step in cognitive radio to learn the radio environment.

The basic idea of a cognitive radio is to support spectrum reuse or spectrum sharing, which allows the secondary networks/users to communicate over the spectrum allocated/licensed to the primary users (PUs) when they are not fully utilizing it.

To do so, the secondary users (SUs) are required to frequently perform spectrum sensing, i.e., detecting the presence of the PUs. Whenever the PUs become active, the SUs have to detect the presence of them with a high probability, and vacate the channel or reduce transmit power within certain amount of time.

Two types: Local Spectrum Sensing
Cooperative Spectrum Sensing

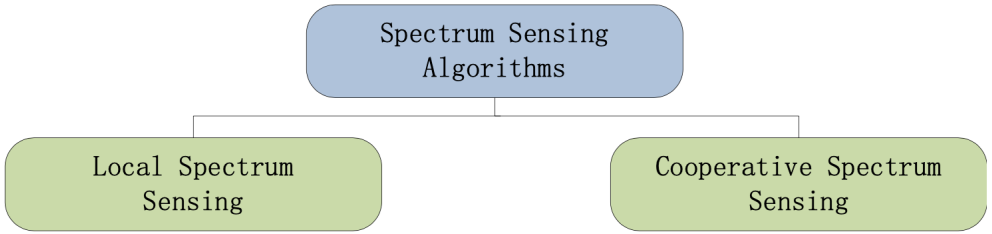


Figure 2.1 – The classification of spectrum sensing techniques.

SPECTRUM SENSING: THE PU/SU HYPOTHESIS

$$\begin{aligned} \mathcal{H}_0 &: y[n] = w[n] && n = 1, 2, \cdots, N_s \\ \mathcal{H}_1 &: y[n] = \overbrace{h[n] \otimes s[n]}^{x[n]} + w[n], && n = 1, 2, \cdots, N_s \end{aligned} \tag{2.1}$$

where $\mathcal{H}_0$ is the hypothesis of the absence (vacant channel) whereas the hypothesis $\mathcal{H}_1$ denotes the presence (occupied channel) of the PU's signal, $y[n]$ represents the received data at the SU with $s[n]$ and $w[n]$ denoting the signal transmitted from the PU and the additive white Gaussian noise (AWGN) with variance σ_w^2, respectively. Moreover, $h[n]$ denotes the channel impulse response from the PU to the SU, and $x[n]$ is the received PU signal with channel effects. N_s is the number of samples. Note that, for purpose of guaranteeing that the received data $\mathbf{y}$ ($\mathbf{y} = \left[y[1]y[2]\cdots y[N_s]\right]^T$) does not include SU's own signal, we assume that the SU executes alternatively spectrum sensing and data transmission.

SPECTRUM SENSING

$\mathcal{H}_0$

In general, spectrum sensing needs to be able to reliably detect the presence of PU and leave PU's frequency band as quickly as possible in order to avoid interference to PU. On the other hand, it needs to provide spectrum access opportunities as many as possible to SU. In order to specifically show the performance of spectrum sensing, some indicators are defined as follows [26]:

- **Probability of detection** (P_d)
  It denotes the probability that we decide $\mathcal{H}_1$ when $\mathcal{H}_1$ is true.

$$P_d = P(\mathcal{T}(\mathbf{y}) > \zeta | \mathcal{H}_1) \tag{2.3}$$

- **Probability of miss** (P_m)
  It denotes the probability that we decide $\mathcal{H}_0$ but $\mathcal{H}_1$ is true.

$$P_m = 1 - P_d = P(\mathcal{T}(\mathbf{y}) < \zeta | \mathcal{H}_1) \tag{2.4}$$

- **Probability of false alarm** (P_{fa})
  It denotes the probability that we decide $\mathcal{H}_1$ but $\mathcal{H}_0$ is true.

$$P_{fa} = P(\mathcal{T}(\mathbf{y}) > \zeta | \mathcal{H}_0) \tag{2.5}$$

SPECTRUM SENSING

The high probability of detection indicates that the SU provides reliable protection for PU and the high probability of false alarm indicates that the SU loses spectrum access opportunities.

For an outstanding spectrum sensing algorithm, both high probability of detection and low probability of false alarm need to be accomplished as fully as possible.

In order to preferably show the performance of spectrum sensing, the receiver operating characteristic (ROC) curve is presented in Figure 2.2, which gives the probability of detection as a function of the probability of false alarm.

As shown in Figure 2.2, the ROC curve is a concave function. The better spectrum sensing algorithm is, the deeper the concave of the ROC is. In that case, both a low probability of false alarm and a high probability of detection are obtained. Therefore, the ROC curve is a key indicator to evaluate the performance of spectrum sensing techniques.

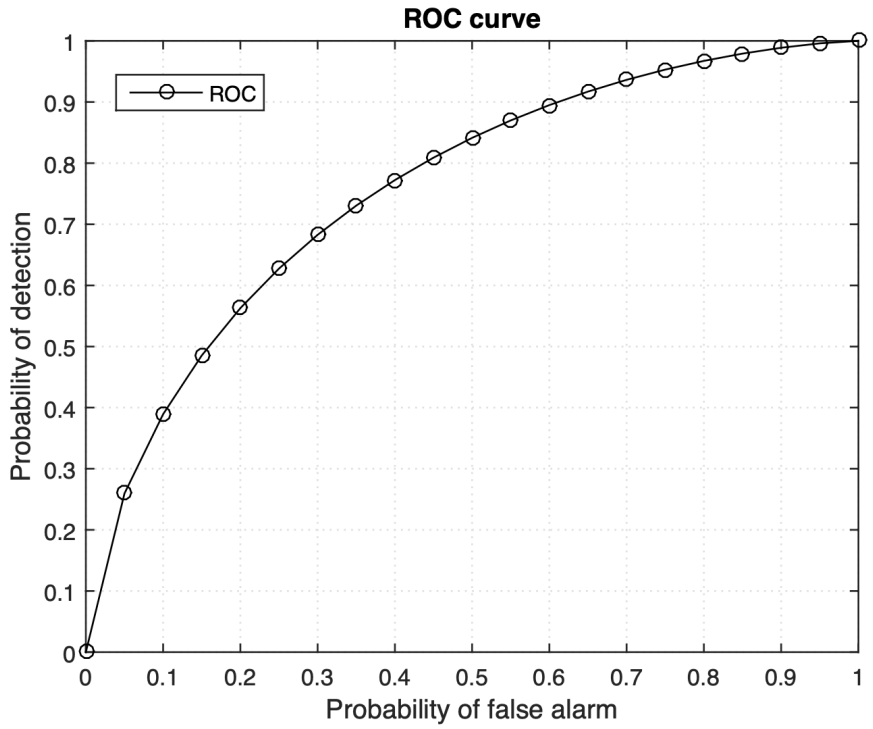


Figure 2.2 – Illustration of the ROC curve in [19].

LOCAL SPECTRUM SENSING

Local spectrum sensing is substantially a detection process conducted by each SU.

- It is based on local SU's observation and aims to sense whether the PU signal is present or not in a specific frequency band.
- Several local spectrum sensing techniques have been studied in the literature.
- Matched filter detection (MFD) is the optimal method when the PU signal is known.
- Cyclostationary feature de-tection (CFD) which requires a prior knowledge of the PU signal characteristics, is robust against noise uncertainty. However, it needs a long observation time and complex computation in order to get a good detection performance.
- Energy detection (ED) is popular due to its low implementation complexity, but it suffers from the noise uncertainty and requires a large number of samples for achieving a high probability of detection.

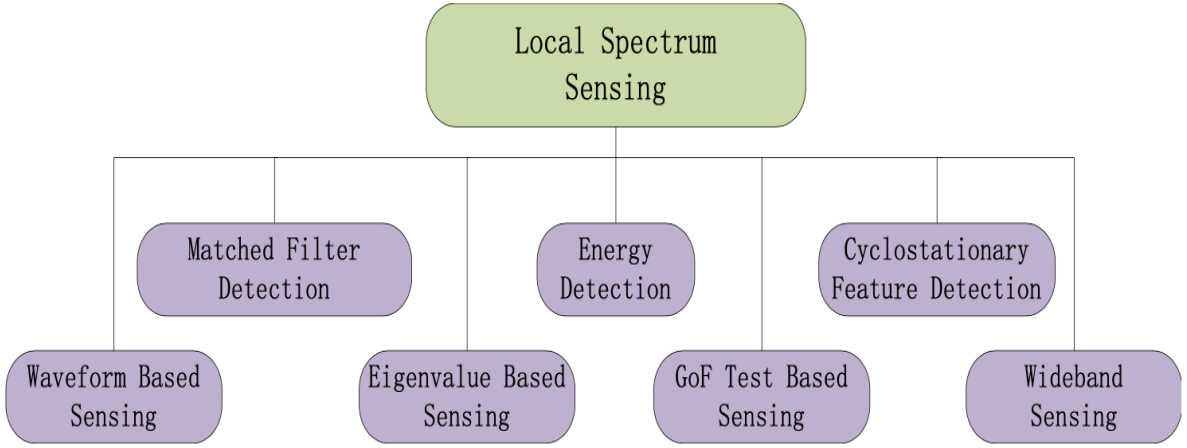


Figure 2.3 – Local spectrum sensing techniques.

- Waveform based sensing (WBS) as a simplified version of the MFD is also robust to the noise uncertainty, but it also needs a prior knowledge of the PU signal.
- Eigenvalue based sensing (EBS) is not only robust to noise uncertainty, but also requires no prior information of the PU signal [43, 44, 45, 46, 47, 48, 49, 50]. Unfortunately, it suffers from the long sensing time and the high computational complexity.
- Goodness of fit (GoF) test based sensing presents an advantage under a small number of samples, which utilizes the distribution characteristics of the background noise and is able to obtain a high detection performance. In addition, wideband sensing has also attracted a lot of interests.

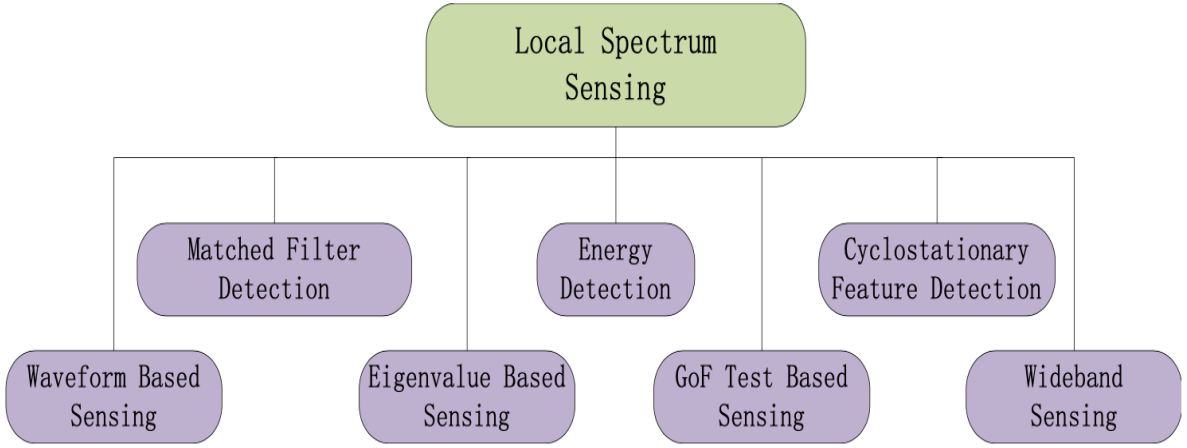


Figure 2.3 – Local spectrum sensing techniques.

COOPERATIVE SPECTRUM SENSING

Local spectrum sensing has a number of limitations.

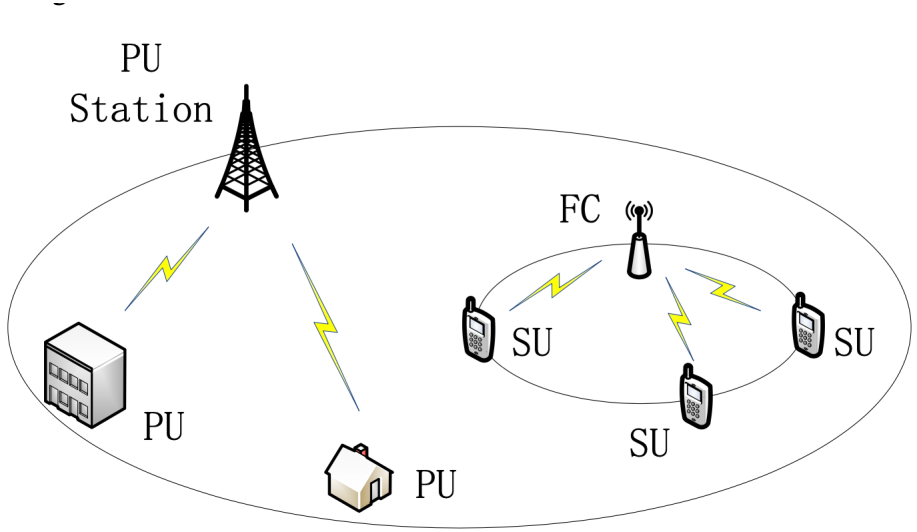
- First of all, the detection sensitivity of a single detector can not meet the requirement of PU signal because of the limits of processing and energy. Furthermore, local spectrum sensing can miss the detection of PU who experiences a deep fading.

- Moreover, the SU who is shadowed might not detect the PU signal, and then may try to utilize the frequency band of PU when in the presence of PU. That is known as the hidden terminal problem. In order to effectively improve the detection sensitivity of SS and make it more robust against depth attenuation, multipath shadows and the hidden terminal, cooperative spectrum sensing is considered.

- Cooperative spectrum sensing generally utilizes more than one detectors and com− bines their results to make a more reliable decision. According to the different collaboration model, cooperative spectrum sensing technology is classified into two categories: centralized cooperative spectrum sensing and distributed cooperative spectrum sensing.

CENTRALIZED COOPERATIVE SPECTRUM SENSING

In centralized cooperative spectrum sensing techniques, multiple sensor nodes (SUs) distributed in different locations firstly independently sense the local environment, and then transmit the sensing information to a central unity called fusion center (FC), finally the FC makes the decision whether PU is present or not on basis of the received information and diffuses the decision back to each SU. The diagram of the centralized cooperative spectrum sensing is shown in the figure.



DISTRIBUTED COOPERATIVE SPECTRUM SENSING

In distributed cooperative spectrum sensing, due to lack of a central cooperator, it works in a distributed manner. The SUs share their information among themselves and update periodically on the spectrum information table in order o reach an unanimous collaborative decision, which thus occupies more storage and consumes more energy than those nodes in the centralized CSS. The diagram of the distributed cooperative spectrum sensing is shown in the figure.

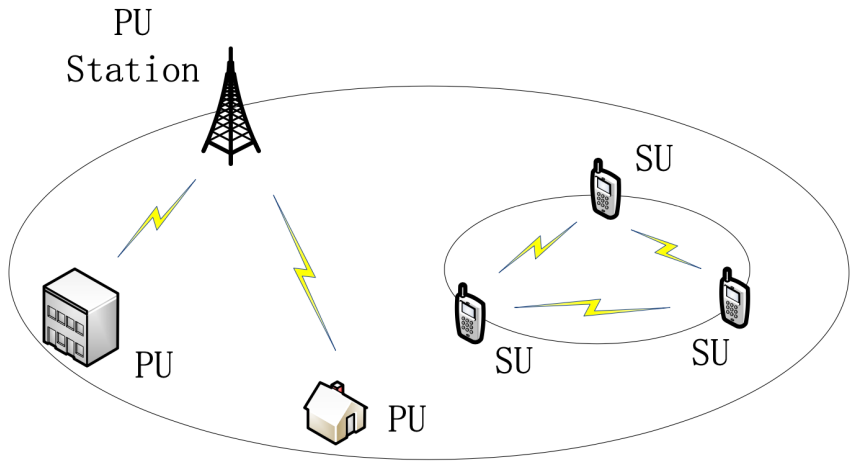


Figure 2.11 – The diagram of distributed cooperative spectrum sensing.

PRACTICAL DIFFICULTIES IN CWSN

CWSN vary from traditional WSN in various dimensions. Due to the process of safeguarding the rights of PUs in CWSN, many practical difficulties arose in traditional WSN.

Detection, False Alarm, and Miss-Detection Probability

The detection probability is a measure employed to detect correctly with respect to the non-existence of PU in the channel. The miss-detection probability is a measure detects the existence of primary signal on the channel, and the false- alarm probability is a measure fails to identify the sensor node which fails to identify the non-existence of the primary signal.

A false alarm leads to non-usage of available spectrum efficiently and the miss detection leads to interference with the PUs. Additionally, the false alarm and miss detection leads to high delay, often switching between frequencies and low throughput. This problem has to be studied well to satisfy the needs of CWSN.

PRACTICAL DIFFICULTIES IN CWSN

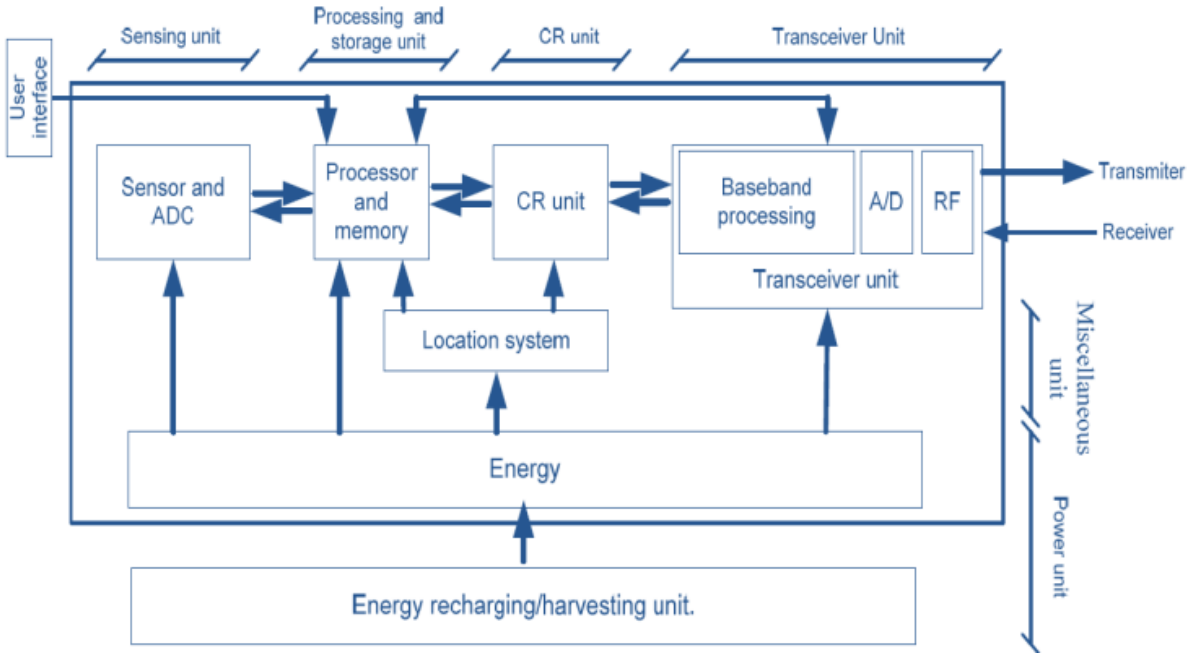
Hardware

The sensor nodes in CWSN have limited resources interms of processing, memory and power supply. Opposite to traditional wireless sensor nodes, it has the ability to sense the channels, investigate and decide. The sensor nodes have the capability to modify the parameter or transmitter with respect to the interaction with the physical world.

The architecture of a sensor node in CWSN has 6 main components as shown in Fig. 4: sensing unit, processing and storage unit, CR unit, communication unit, power supply and miscellaneous unit. The sensing unit has actual sensors and analog to digital converter (ADC).

The analog signals captured by the sensor are transformed to digital data and is process by the processing unit. The CR unit has the cognitive ability and it requires adapting with the transmission variables like carrier frequency, transmission power, and modulation.

The CR unit requires choosing the optimum channel, handling the movement of spectrum and so on. The communication unit has the responsibility of transmitting and receiving data. The design of intelligent hardware in CWSN is a difficult process. Several artificial intelligence methods have been presented to satisfy the fundamental concept of CR.



PRACTICAL DIFFICULTIES IN CWSN

Topology modifications

Topology straightly influences the network lifetime in CWSN. Based on the application nature, sensor nodes undergo deployment in a static or dynamic manner. In most of the cases, the node failure in CWSN exists because of hardware failure of energy exhaustion. The topologies of the CWSN and WSN are same. An adaptable self−configuration topology is essential for CWSN to obtain scalable, reduced energy utilization and achieve better results. The dynamic self−configuration topology offers static topology, even though it is a demanding problem to design and implement. This field needs to be explored more.

Fault Tolerant

The CWSN should have autonomous, self configure and self−healing capabilities. It can be stated as, when the link failure occurs, a substitute path will be derived that eliminates the presence of fault nodes. There are various ways to make the node faults like hardware or software not working, or natural calamity, and so on. The nodes in CWSN should deal with these scenarios. Various types of faults exist namely node fault, network fault, and sink fault, etc. [12] defined the fault tolerance or reliability $R_k(t)$ of a node by the use of Poisson distribution in the time interval $(0,t)$ as follows:

$$R_k(t) = \exp(-\lambda_k t) \quad (1)$$

where λ_k is the failure rate of wireless sensor node k and t

is the time period. The fault tolerance is a main issue in CWSN and techniques need to be developed should be fault tolerant.

PRACTICAL DIFFICULTIES IN CWSN

Installation Cost

In general, many sensor nodes are deployed in the CWSN to cover the intended region. So, the installation cost should be low. Contrasting to traditional WSN, it needs low storage space and processing abilities. For minimizing the hardware cost, the techniques developing for CWSN should operate with minimum storage and processing abilities. In addition, the use of intelligent radio, application specific positioning systems (e.g., GPS), energy harvesting unit and so on enhances the installation cost.

Channel Selection

In CWSN, as there exists no devoted channel to transmit data, with the neighbors, the sensors require to settle and choose a channel for data communication. As there exists no collaboration among SU and PU, this is difficult problem. At any time, PU might arise at channels. The SU tends to leave out of the channel at that time when PU claims for the channel. Assuming the PU behavior over the channel and employing few AI methods, data channels should be chosen wisely.

Scalability

In larger counts, the CR wireless sensors should be place for few applications. For spectrum data sharing, CR wireless sensors need collaborations over nodes unlike traditional WSN nodes. For CR wireless sensor with heterogeneous environment, it is very complex to coordinate. Because of the increasing network size, protocols and method built for CWSN must be able to resolve the problems.

PRACTICAL DIFFICULTIES IN CWSN

Power Consumption

With a constrained energy source, CR wireless sensors are energy limited devices. Power required for reception and transmission of data packets, data processing, spectrum sensing, route discovery, back off, channel negotiation, in addition to all of the above, CR wireless sensors need power for frequent spectrum handoff. A CR wireless sensor requires to intellect PU action over the channel. To PU action monitoring, numerous applications need numerous antennas, therefore high power is utilized. For energy retrieval, there exist many researches, and these methods comprise its own disadvantages. Replacing the energy resources or energy retrieval is not probable in few applications. Power utilization is not a significant consideration in ad hoc CRNs, however it is an significant design factor. But, it is one among the major performance measure in CWSN which straightly affects network lifespan.

Quality of Service (QoS)

The QoS is commonly divided through four attributes in traditional WSNs: jitter, bandwidth, reliability and delay. WSN requires managing a sufficient QoS level in order to prevent risky consequences in significant applications. In WSN, memory, power resources and processing power are the resource limitations which the QoS support is a difficult problem. It also suffers from other problem like preserve the PU rights to acquire incumbent spectra. With SU, PU communication shall be interference free. This is highly difficult that it is complex to PU arrival prediction over the channel. False alarm and primary signal miss-detection can add extra difficulty.

PRACTICAL DIFFICULTIES IN CWSN

Security

In an unattended environment, the wireless sensors are generally placed and are highly probable to have the problems like privacy and security.

Physically, the CR wireless sensors can be attacked in addition the data might get stolen. When compared to traditional WSN, CWSN are prone to security threats, as there exist no collaboration among SU and PU communication.

Through unauthorized entities, the data gathered through CR wireless sensors can be destroyed, modified or sniffed.

Through SU via spectrum sensing data falsification (SSDF), attacker can hinder with PUs transmission or avoid the channel implications. Over the possible attacks and threats, CWSN might comprise few allowed security robustness level. Additional difficulties exist in CWSN, with the traditional WSN security problems.