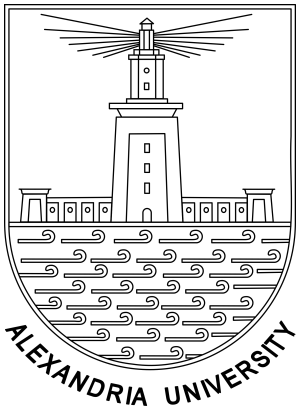
Wireless Regional Area Network (WRAN) Using Cognitive Radio



Graduation Project 2018

Department of Electrical Engineering
Communications Section
Alexandria University

Supervised by: Prof. Dr. Hassan El-Kamchouchi

Faculty of Engineering July 2018

Such is the Bounty of Allah, which He bestows on whom He will: and Allah is the Lord of the highest bounty [Quran: 62-4]

Acknowledgements

All praise and thanks are due to the Almighty Allah who always guides us to the right path and has helped us to complete this work.

Then, we would like to express our special thanks to our supervisor, Prof. Hassan El-Kamchouchi, for his academic advices, constant encouragement, guidance, and support during our graduation project at Alexandria University. We also would like to take this opportunity to express gratitude to all members of the Department of Electrical Engineering for their help and support.

To our parents, Words do not exist to describe your importance in our life.

Abstract

To satisfy future bandwidth demands, existing Cognitive Radio with Wireless Communication must be upgraded to make the best use of the bandwidth. Wireless Communication is data transfer between two or more points that are not physically connected. The most common wireless technologies use electromagnetic wireless telecommunications, such as radio. With radio-waves, distances can be short; a few meters for television or far as thousands of kilometers for deep-space radio communications.

In this thesis we discuss the IEEE 802.22 WRAN standard which uses the wireless solution to deliver Internet to the rural areas. Since cables underground in deserts are prohibitively expensive and arduous to be constructed, besides we cannot use high frequencies to send through due to the free space path losses. Also according to the radio propagation theory, transmitting in higher frequencies lead to a weak signal.

The solution for this problem is to use the cognitive radio technology to reuse the licensed bands such as the TV which are bands of low frequency from 50 MHz to 850 MHz, and this is because TV and radio broadcasting are over large areas that one TV tower can cover the whole city. Cognitive radio technology gives the ability to use these licensed bands by means of spectrum sensing techniques and another techniques.

In the later chapters we also provide an introduction to the advanced measurements instrumentation for nuclear power plants. In addition, we introduce shield effectiveness theory for electromagnetic waves. Electromagnetic shielding is frequently used to reduce emissions or completely avoid radiation from different sources to penetrate the outer surface to secure humans and the surrounding environment. Radiation protection is the science and practice of protecting people and the environment from the harmful effects of ionizing radiation. It is a important not only in nuclear reactor stations, but also in other industries such as medical centers.

Finally, we give a numerical example on calculating shield effectiveness for various materials that can be used to protect nuclear power plants from harmful radiations.

Table of contents

List of figures

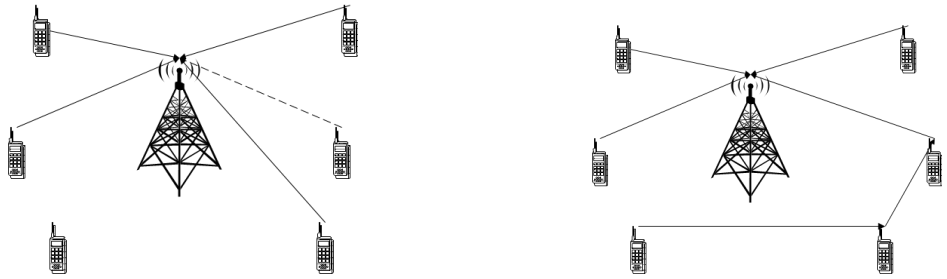
Chapter 1

Introduction to WRAN Using Cognitive Radio

1.1 Motivation

In the prosperous world we are living right now, communications enter our daily lives in manifold ways that it is easy to overlook the multitude of its facets. Mobile phones, radio broadcasting, TV towers, satellite antennas, and PCs with the access of the Internet seem to rule the communications world. Data communication networks are a crucial system to any modern city that is because they are used extensively in numerous applications such as financial transactions, social interaction, education, national security, and other more. Although passive optical networks (PONs) may be the best solution for a complex network that requires a high speed data communications, but the design of the system suffers from high costs and other fiber problems, thus wireless communications solve these troubles. However, there are some problems in wireless communications such as, frequency dependent, relatively low bandwidth, and tightly licensed by the government.

Mobile devices are only allowed to certain frequencies which are getting crowded. With cognitive radio technology, we can use all available frequencies even though those dedicated to TV or satellites. The intelligent devices negotiate in order to use the whole radio spectrum in the most efficient way, this way we can multiply the current networks needs. By the word radio we mean any kind of wireless communications, at the moment radios can communicate only with other radios of the same kinds. Cognitive radio can understand the language of any radio, this combined with new single radios embedded in any object, would allow any interaction any physical objects, this can also provide solutions for communications between people at different languages and cultures. In any big events with tens of thousands of people,



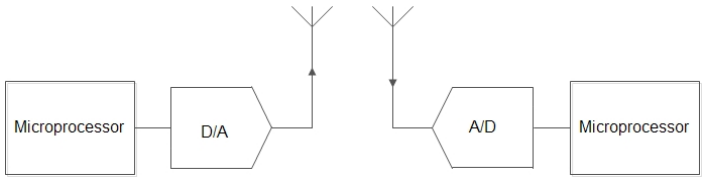
(a) Before Cognitive Radio (b) After Cognitive Radio

Fig. 1.1 Radio communications systems before and after cognitive radio

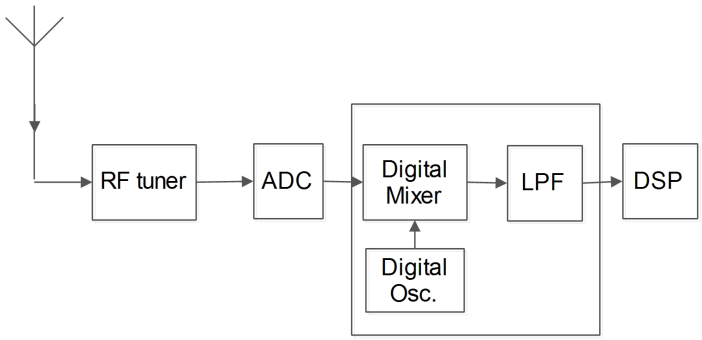
the local network may get overloaded,with current spectrum usage limitations the provided capacity just is not enough for the users. Cognitive radio can use all available frequencies and connectivity methods, it can quickly adapt to unusual situation and ensure the proper operations of the networks. The devices connect not only to through the network cells but also by forming spontaneous networks, this way real time video streams can be transmitted by many more users. Fig.1.1 illustrates the difference between radio communications systems before and after cognitive radio. Before cognitive radio, radio devices sometimes cannot reach the radio tower, it can be seen as dotted line, but after cognitive radio, radio devices are able to connect with each other until it reaches the radio tower.

1.2 Software Defined Radio (SDR)

Software Defined Radio is a radio communication system where components that have been traditionally implemented in hardware are instead implemented by means of software and perform the baseband processing as modulation/demodulation, error correction coding and compression. We can define it in another way, a (SDR) is a radio in which some or all of the physical layer functions are software defined The ideal (SDR) is shown in Fig. 1.2.a The user data is mapped to the desired waveform in the microprocessor. The digital samples are then converted directly into an RF signal and sent to the antenna. The transmitted signal enters the receiver at the antenna, is sampled and digitized, and finally processed in real time by a general purpose processor. Generally, its physical components were only an antenna and an Analog Digital Converter (ADC) on the receiver side. Likewise, the transmitter would have a Digital Analog Converter (DAC) and at transmitting antenna.[1] Fig. 1.2.b shows non-ideal (SDR) Receiver. At first, the RF tuner converts the analog signal to IF, next, the IF signal is passed to the ADC converter in charge of changing the signal's domain, offering digital samples. The samples are feed to the following stage's input which is a Digital Down



(a) Ideal SDR



(b) Non-Ideal SDR Receiver

Fig. 1.2 Ideal SDR system versus Non-Ideal SDR Receiver

Converter (DDC). The (DDC) is commonly a monolithic chip and it stands as the key part of the (SDR) system. It consists of three main components: (a digital mixer - a digital local oscillator - low-pass filter output). The digital mixer and the local oscillator shift the IF digital samples to baseband, while the low-pass filter limits the bandwidth of the final signal. For the implementation of each of its parts, the (DDC) includes a high number of multipliers, adders and shift registers. Finally, the baseband samples are passed to the Digital Signal Processing (DSP) block, where task such as demodulating and decoding are performed, among others.

1.3 The Evolution of SDR

SDR is currently used to build radios that support multiple interface technologies (e.g., CDMA, GSM) with a single modem by reconfiguring it in software. However, SDR modems are expensive, since they typically entail programmable devices like Field-programmable gate array (FPGAs), as opposed to the mass-produced, single-produce Application-specific integrated circuit (ASICs) used in most consumer devices today. Even today's multi-mode devices tend to just have multiple ASICs or multiple cores on a single ASIC.

1.4 Overview on Cognitive Radio and IEEE 802.22

In the next chapter we are going to dig deeper in cognitive radio and IEEE 802.22 standard, but first we would like to give an overview on each of them. Cognitive radio is a particular extension of software radio that employs model-based reasoning about users, multimedia content, and communications context. [2]

In the last decade, there has been a significant amount of research work focusing on the different aspects of cognitive radios such as spectrum sensing and signal classification techniques, transmission power control, and adaptive channel access protocols at the link layer, and much more. The current and future trends in CR including the applications (e.g., smart grid, machine-to-machine communications, and cloud computing) The first cognitive radio wireless regional area network (WRAN) standard, IEEE 802.22, was developed by IEEE 802 LAN/MAN Standard Committee (LMSC) and published in 2011. This standard uses geolocation and spectrum sensing for spectral awareness. Geolocation combines with a database of licensed transmitters in the area to identify available channels for use by the cognitive radio network. Spectrum sensing observes the spectrum and identifies occupied channels. IEEE 802.22 was designed to utilize the unused frequencies or fragments of time in a location. This white space is unused television channels in the geolocated areas. However, cognitive radio cannot occupy the same unused space all the time. As spectrum availability changes, the network adapts to prevent interference with licensed transmissions. [3]

The development of the IEEE 802.22 WRAN standard is aimed at using cognitive radio techniques to allow sharing of geographically unused spectrum allocated to the television broadcast service, on a non-interfering basis, to bring broadband access to hard-to-reach, low population density areas, typical of rural environments, and is therefore timely and has the potential for a wide applicability worldwide. It is the first worldwide effort to define a standardized air interface based on CR techniques for the opportunistic use of TV bands on a non-interfering basis. The ability of the cognitive radios to monitor the Radio Frequency (RF) in the environment and their ability to adapt to the changes in the environment by changing their configurations run time make them suitable for many useful applications.

In the next chapters we will discuss cognitive radio and IEEE 802.22 in more details.

Chapter 2

Cognitive Radio Networking Preliminaries

2.1 Cognitive Radio Technology

A cognitive radio is the key technology that allows a cognitive wireless terminal to dynamically access the available spectral opportunities. For cognitive radio, an SDR can take advantage of underutilized spectrum. If the owner of the spectrum is not using it, an SDR can 'borrow' the spectrum until the owner comes back. This technique has the potential to dramatically increase the amount of available spectrum.

The definition of cognitive radio by Mitola that we discussed in chapter 1 for was generalized by the Federal Communications Commission (FCC) to be "a radio or system that sense its electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, access secondary markets". Another definition by Haykin: cognitive radio is a radio which capable of being aware of its surroundings, learning, and adaptively changing its operating parameters in real time with the objective of providing reliable anytime, anywhere, and spectrally efficient communication.

Despite the differences in the last definitions, a cognitive radio has two key features that distinguish it from a traditional radio: *the cognition capability* (intelligent adaptive behavior) and *the reconfigurability.*

Figure 2.1 illustrates how these unique features of a cognitive radio conceptually interact with the radio environment. This illustration is referred to as the cognition cycle that is continually run by the cognitive radio to observe spectral opportunities, create plans to adapt itself, decide, and act to explore the best opportunities. [4]

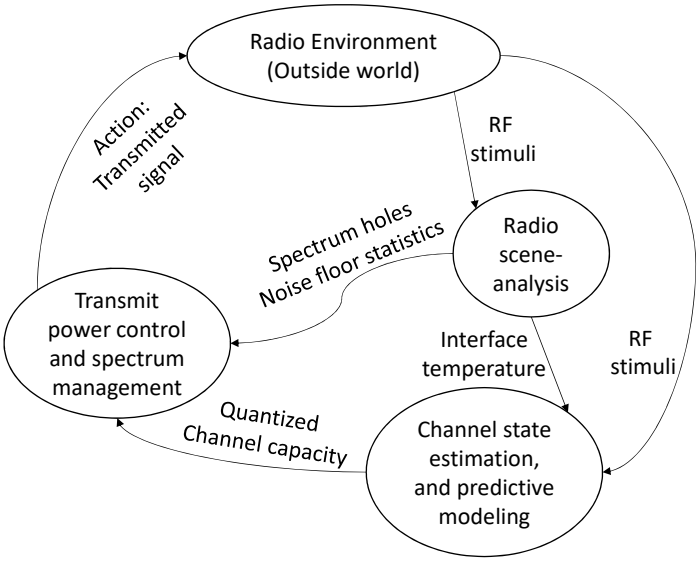


Fig. 2.1 Basic cognitive radio cycle

2.2 Cognitive Radio Network Applications

As discussed, CRs are highly agile wireless platforms capable of autonomously choosing operating parameters based on both prevailing radio and network conditions [5],[3]. Consequently, CRs have the potential to revolutionize how devices perform wireless networking. For instance, CRs allow radios operating on different protocols and standards to communicate with each other. This is known as interoperability [6], [7]. Furthermore, CRs are capable of transmitting in unoccupied wireless spectrum while minimizing interference with other signals in the spectral vicinity; that is, Dynamic spectrum access (DSA) [8].

2.2.1 Interoperability

Due to its ability to rapidly assume any available radio configuration, CR platforms can reconfigure themselves to a legacy communications standard in order to communicate with any communication system deployed in the field or facilitate communications between two non-CR platforms employing different standards. Furthermore, with its onboard artificial intelligence, CR can automatically distinguish between different communication standards in the absence of any centralized control.

Fig. 2.2 illustrates how public safety and emergency teams within the same geographical area can work at the same time, where members of (police) employ a communications standard operating on a carrier frequency that is different from the communication equipment employed by both (firefighter) and (military). Thus, unless these teams are coordinated with

respect to operating parameters and communication standards, effective communications between them would be nearly impossible.

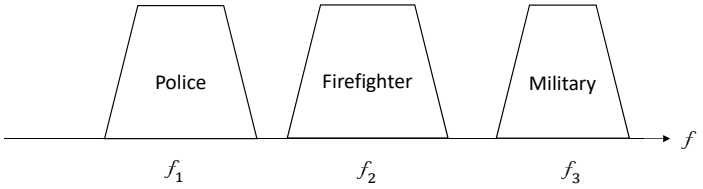


Fig. 2.2 Example of public safety and emergency responder teams within the same geographical area operating on different center frequencies and potentially using different communication standards.

2.2.2 Dynamic Spectrum Access

With the increasing demand for additional bandwidth to support existing and new services, both spectrum policy makers and communication technologists are seeking solutions for this apparent spectrum scarcity. Meanwhile, measurement studies have shown that much of the licensed spectrum is relatively unused across time and frequency[9]. Nevertheless, current regulatory requirements prohibit unlicensed transmissions in these bands, constraining them instead to several heavily populated, interference-prone frequency bands. To provide the necessary bandwidth required by current and future wireless services and applications, the FCC has commenced work on the concept of unlicensed users “borrowing" spectrum from spectrum licensees [10]. This approach to spectral usage is known as dynamic spectrum access. With recent developments in CR technology, it is now possible for these systems to simultaneously respect the rights of incumbent license holders while providing additional flexibility and access to spectrum.

To achieve higher spectral efficiency, multiple access techniques can be employed such that multiple secondary users can transmit data within the same frequency range. Several techniques have been proposed to achieve multiple secondary user access, including those based on code division multiple access (CDMA) [11], spatial multiplexing [12], and orthogonal frequency division multiplexing (OFDM) [13]. With respect to OFDM-based techniques, the spectrum pooling concept can be effectively employed, where data are transmitted across unoccupied portions of frequency using a subset of active subcarriers [14].

2.2.3 Cognitive Mesh Networks

Multi-hop wireless mesh networks have recently gained significant popularity as a cost-effective solution for last-mile Internet access. Traditional wireless mesh network are chal-

lenged by the scarcity of the wireless bandwidth needed to meet the high-speed requirements of existing wireless applications. Opportunistic Spectrum Access can be used to alleviate the bandwidth scarcity problem of mesh networks by allowing the mesh nodes to dynamically explore any available spectral opportunities. Such cognitive mesh networks are meant be used to provide broadband access to rural, tribal, and other under-resourced regions [15].

2.2.4 Public Safety Networks

Public safety networks are another type of networks that can exploit Cognitive Radio Networking. Public safety networks are used for communications among police officers and fire and paramedic personnel. Such networks are also challenged by the limited amount of allocated spectrum. Even with the recent extensions of the allocated public safety spectrum bands, the public safety personnel do not have the technology to dynamically operate across the different spectrum segments. Recall that public safety licensees have a wide variety of bands available (VHF-Low, VHFHi, 220 MHz, UHF below 800, UHF-800, etc.). The cognitive radio technology can offer public safety networks more bandwidth through Opportunistic Spectrum Access. Furthermore, a public safety CRN can provide a substantial communication improvement by allowing the interpretability across different public safety services while smartly adapting to the high peak-to-average nature of the traffic carried out by such networks [16].

2.2.5 Disaster Relief and Emergency Networks

Natural disasters such as hurricanes, earthquakes, wild fires, or other unpredictable phenomena usually cause the communications infrastructure to collapse. For example, some base stations of cellular networks can fall, the connectivity between sensor nodes and the sink node in static wireless sensor networks can be lost, existing Wireless Local Area Networks (WLANs) can be damaged, etc. This results in a set of partially or fully damaged coexistent networks that were previously deployed and then became disconnected. Meanwhile, there is an urgent need for a means of communications to help the rescue teams to facilitate organized help, rehabilitation efforts, and to locate the disaster survivors. CRNs can be used for such emergency networks (e.g., see [17] and references therein). The use of Opportunistic Spectrum Access in disaster relief networks can provide a significant amount of bandwidth that can handle the expected huge amount of voice, video, and other critical and time-sensitive traffic. It is worth mentioning that WLANs were used in the relief of the Haiti earthquake. However, the communication over such a network was unreliable and suffered significant delays [18].

2.2.6 Battlefield Military Networks

Unfortunately, the recent advances in wireless technologies made the job of communication jamming and/or hacking much easier. Consequently, achieving reliable and secure communications in modern battlefields has become a more challenging task. Recall that a battlefield communication network provides the only means of communications between soldiers, armed vehicles, and other units in the battlefield amongst themselves as well as with the headquarters. This implies that such networks do not only require significant amount of bandwidth, but also mandate secure and reliable communications to carry vital information. The cognitive radio is the key enabling technology for realizing such densely deployed networks which use distributed Opportunistic Spectrum Access strategies to fulfill the bandwidth and reliability needs. Note that, the dynamic nature of OSA makes the ability to track and jam a communication more difficult. Thus motivated, DARPA initiated the Wireless Network after Next (WNaN) program aiming at creating a flexible architecture for military communications. The main goal of the WNaN program is to develop a low-cost handheld cognitive radio terminal that is capable of selecting its own frequencies and forming a dense network within a large battlefield area.

2.2.7 Leased Networks

All of the aforementioned CRN applications have the secondary users exploiting the resources of the primary networks without being beneficial to the primary networks in any way. However, a primary network can benefit from leasing a fraction of its licensed spectrum to secondary operators adopting cognitive radio technology to opportunistically access the spectrum. The entrance of the secondary operator to the market of the incumbent primary network can increase the revenue of the primary licensed operator [19].

2.3 Reconfigurability of a Cognitive Radio

The second key feature that distinguishes a cognitive radio from a traditional one, and completes the cognition cycle depicted in Fig. 2.1, is its ability to re-tune its transceiver parameters on the fly based on its assessment of the surrounding radio environment. While today's radios have considerable flexibility in terms of their ability to reconfigure some transmission parameters such as the transmission rate and power, they are typically designed to operate over certain frequency band(s) according to a certain communication protocol. A cognitive radio transceiver should be more flexible than just this in order to be able to exploit emerging spectral opportunities over a wider spectrum range. For instance, a

cognitive radio must be able to configure the transmission bandwidth to adapt to spectral opportunities of different sizes. Furthermore, a cognitive radio cannot be constrained to a certain communication protocol. Instead, a cognitive radio must determine the appropriate communication protocol to be used over different spectral opportunities based its recognition of the radio environment.

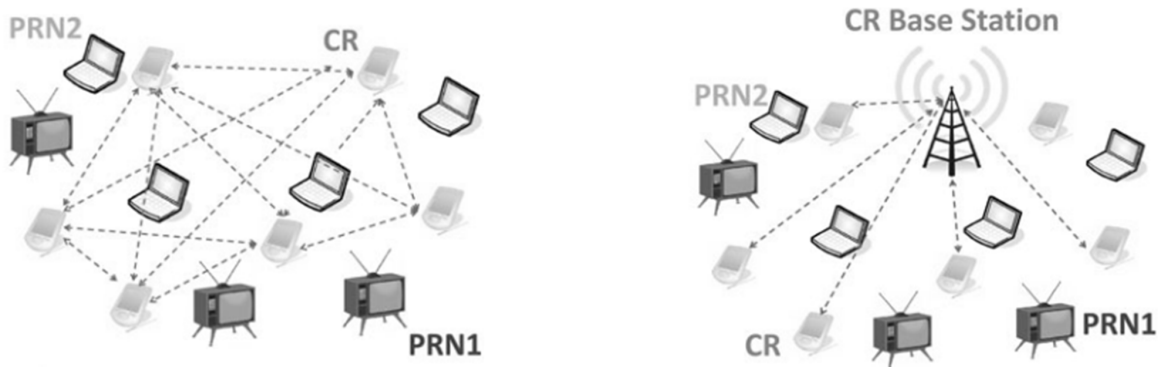
2.3.1 Spectrum Mobility

The reconfigurability of a cognitive radio transceiver reflects the spectrum mobility function introduced by Mitola in his definition of the cognitive radio [2]. Spectrum mobility refers to the process in which a cognitive radio terminal changes its frequency of operation. In order to maintain seamless wireless connectivity, a cognitive radio terminal should be able to switch to a new frequency band upon either the appearance of the primary licensed user(s) of the current band or the deterioration of the channel quality of the currently used channel. In other words, spectrum mobility is the cognitive radio functionality that actually allows the cognitive radio to dynamically explore the available spectral opportunities. Thus, spectrum mobility is associated with a handoff mechanism that guarantees the transition to the new frequency band without breaking (or significantly degrading the quality of) the communication between communicating cognitive radio terminals. While the cognition functions of the cognitive radio mainly affect the lower layers of the cognitive radio network (CRN), namely the physical and medium access layers, spectrum mobility and handoff also affect higher layers. Hence, spectrum mobility schemes should ensure smooth and fast frequency transition and protocol/paramter adjustment in order to minimize the latency that could harm the performance of higher layer protocols. Even though mobility-based handoff mechanisms have been investigated in the context of cellular networks and can be used to lay the foundation for spectrum mobility, CRN spectrum mobility poses several new challenges.

2.4 Cognitive Radio Network Architectures

A typical CRN environment consists of a number of Primary Radio Networks (PRNs) that coexist within the same geographical area of a single CRN (also referred to as the secondary network). A primary network is an existing network that is licensed to operate in a certain spectrum band. Hence, a primary network is also referred to as a licensed network. Primary networks can either be based on a centralized infrastructure or distributed ad-hoc (formed) in nature. The users of a primary network can only access the spectrum licensed to this particular network. Primary users have priority with respect to spectrum access and operate as they

are the sole users of their licensed spectrum. Hence, primary users do not provide any type of cooperation with the secondary network. PRNs are non-intrusive and the transmissions of the primary users should not be affected by the secondary users. Therefore, the primary networks define upper bounds on the CRN activities in their licensed bands, typically in terms of maximum power levels, to guarantee the promised performance level to their legitimate users. On the other hand, the CRN is not licensed to operate in a predefined band. Spectrum access for the CRN is achieved in an opportunistic manner that allows the secondary users to opportunistically access the entire spectrum available to all of the geographically-collocated PRNs. Recall that the cognitive users can also exploit the unlicensed spectrum. This is referred to as spectrum heterogeneity of CRNs [8]. When operating in a licensed band, the CRN transmissions must adhere to the constraints imposed by its primary owner. A CRN can either be centralized infrastructure-based network or a distributed ad-hoc network as shown in 2.3.



B- Distributed ad-hoc CRN. A-Centralized infrastructure based CRN.

Fig. 2.3 Centralized infrastructure based CRN and Distributed ad-hoc CRN.

2.4.1 Centralized Cognitive Radio Networks

Centralized CRNs are infrastructure-based networks in which cognitive radio base stations control and coordinate the transmission activities of the secondary cognitive radio users as shown in Fig. 2.3 A. The cognitive radio base stations control the secondary transmissions over both the licensed and unlicensed bands by collecting all the spectrum-related information from the cognitive radio users. Based on the collected information, the base stations take global spectrum access decisions for all nodes. An example centralized infrastructure-based CRN is the IEEE 802.22 network model. The IEEE 802.22 standard defines the specifications of a point-to-multi-point communication scheme over the unused television (TV) bands in

which a base station manages cognitive radio users within 33 km radius using a centralized spectrum database.

Other examples include the European Dynamic Radio for IP services in Vehicular Environment (DRiVE) [20] and Spectrum Efficient Uniand Multi-cast Services Over Dynamic Radio Network in Vehicular Environments (OverDRiVE) [21] projects. These projects have a centralized entity that coordinates the dynamic utilization of the temporal and spatial spectral opportunities. Centralized infrastructure-based CRNs are beyond the scope of this book.

2.4.2 Distributed Cognitive Radio Networks

Alternatively, CRNs can also have the cognitive nodes communicating with each other via ad-hoc point-to-point connections over either the licensed or the unlicensed bands as shown in Fig. 2.3 B. While alleviating the infrastructure cost, such infrastructureless CRNs have increased networking complexity. In the absence of a controlling centralized entity, cognitive radio nodes in a distributed CRN jointly coordinate their spectrum access decisions to share the available spectral opportunities. Thus, global mechanisms such as network-wide synchronization might be needed for spectrum access coordination. In addition, distributed cooperative detection and communication techniques are used to improve the overall network performance. This book targets Opportunistic Spectrum Access in distributed CRNs. Our goal is to alleviate the network-wide coordination overhead by omitting inter-flow communications in such a network model.

2.5 Guidelines of Cognitive Radio Networking

The coexistence of the primary networks within the CRN environment distinguishes CRNs from other traditional networks. The CRN transmissions should not disturb the transmissions within the primary networks. This constraint does not exist in legacy wireless networks. Therefore, Medium Access Control (MAC) protocols developed for such networks (more specifically, those developed for multi-channel and/or multi-radio networks) are not well suited to the unique characteristics of CRNs. The existence of the primary users makes the Opportunistic Spectrum Access problem fundamentally different from the medium access problem in multi-channel networks since the latter problem is simply a resource sharing problem for users within a given network. In order to realize an Opportunistic Spectrum Access network, the following design guidelines are mandated [8]:

1. An Opportunistic Spectrum Access network should be transparent to the users of the primary networks. Hence, no coordination is required between the primary and the secondary users.

2. An Opportunistic Spectrum Access network should provide guarantees to the performance of the primary licensed networks.

3. Cognitive radio nodes should make efficient and accurate spectrum sensing and spectrum access decisions while exploring either the unutilized or the utilized bands. These decisions should account for the dynamics of the time-varying activities of the primary users.

4. The CRN should define a coordination mechanism (either explicit or implicit) to maximize the spectrum utilization efficiency and allow cognitive radio users to fairly share the available spectral opportunities.

Chapter 3

Spectrum Sensing and Identification

3.1 Introduction

Multiple measurement campaigns reveal that much of the licensed spectrum remains unused both in time and in frequency: traffic in wireless networks tends to be bursty. Hence, efficient exploitation of the spectrum requires the ability to exploit instantaneous opportunities at a rather fine time scale [22]. For cognitive networks to operate efficiently, secondary users should be able to exploit radio spectrum that is unused by the primary network. A critical component of cognitive networking is thus spectrum sensing. The secondary user (SU) should sense the spectrum efficiently, quickly seize opportunities to transmit, and vacate the spectrum should a primary user (PU) reoccupy the spectrum. As noted in [23], a critical component of opportunistic spectrum allocation is the design of the spectrum sensor for opportunity detection.

3.1.1 Primary signal detection

In this section, we discuss the detection of primary signals, which, while not equivalent to the detection of spectrum opportunities, constitutes a basic step in spectrum opportunity detection as shown in Section 4.3. In later sections, we discuss how primary signal detection can be translated to the problem of spectrum opportunity detection.

The spectrum sensor essentially performs a binary hypothesis test on whether or not there are primary signals in a particular channel.1 The channel is idle under the null hypothesis and busy under the alternate:

$$H_0(idle) \quad \text{vs.} \quad H_1(busy) \tag{3.1}$$

Under the idle scenario, the received signal is essentially the ambient noise in the radio frequency (RF) environment, and under the busy scenario, the received signal would consist of the PU's signal and the ambient noise; thus,

$$H_0: \quad y(k) = w(k) \qquad H_0: \quad y(k) = s(k) + w(k) \tag{3.2}$$

for k= 1, ...,n, where n is the number of received samples, $w(k)$ represents ambient noise, and $s(k)$ represents the PU signal. It seems natural that the received signal will have more energy when the channel is busy than when it is idle; this is the underlying concept in the energy detector.

3.2 From Detection Primary Signals to Detecting Spectrum Opportunities

In this section, we highlight the differences between detecting primary signals and detecting spectrum opportunities. We show that, besides noise and fading, the geographic distribution and traffic pattern of primary users have significant impact on the performance of spectrum opportunity detection.

3.2.1 Definition and Implications of Spectrum Opportunity

A rigorous study of cognitive radio systems must start from a clear definition of spectrum opportunity and interference constraint. An initial attempt in defining these two central concepts can be found in [24]. To protect primary users, an interference constraint should specify at least two parameters ρ, ζ . The first parameter ρ is the maximum allowable interference power perceived by an active primary receiver; it specifies the noise floor and is inherent to the definition of spectrum opportunity as shown later. The second parameter ζ is the maximum outage probability that the interference at an active primary receiver exceeds the noise floor. Allowing a positive outage probability ζ is necessary due to opportunity detection errors. This parameter is crucial to secondary users in making transmission decisions based on imperfect spectrum sensing [25].

Spectrum opportunity is a local concept defined with respect to a particular secondary transmitter and its receiver. Intuitively, a channel is an opportunity to a pair of secondary users if they can communicate successfully without violating the interference constraint imposed by the primary network. In other words, the existence of a spectrum opportunity is determined by two logical (binary value) conditions: the reception at the secondary receiver

being successful and the transmission from the secondary transmitter being "harmless." Deceptively simple, this definition has significant complications in cognitive radio networks where primary and secondary users are geographically distributed and wireless transmissions are subject to path loss and fading.

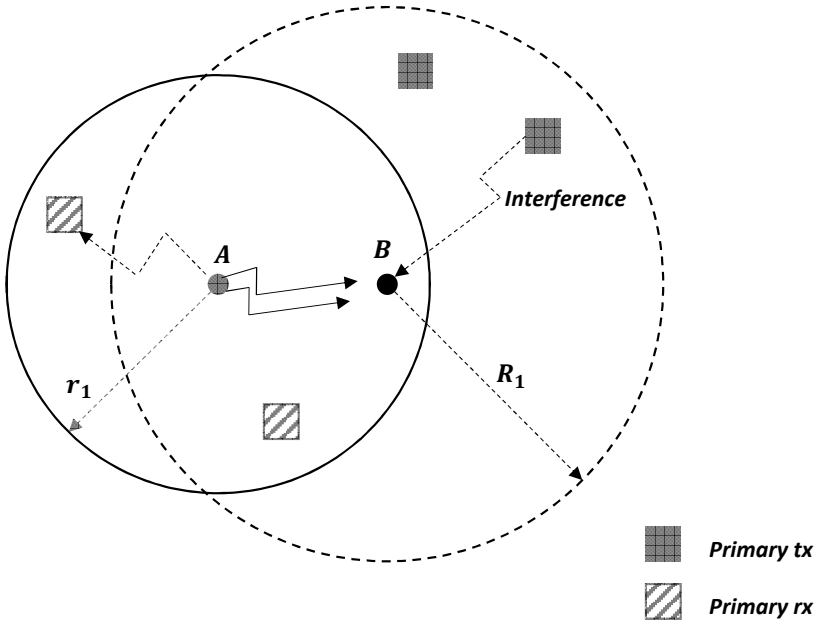


Fig. 3.1 The spectrum opportunity

For a simple illustration, consider a pair of secondary users (A and B) seeking to communicate in the presence of primary users as shown in Figure 3.1. A channel is an opportunity to A and B if the transmission from A does not interfere with nearby *primary receivers* in the solid circle, and the reception at B is not affected by nearby *primary transmitters* in the dashed circle. The radius r_I of the solid circle at A depends on the transmission power of A and the parameter ρ of the interference constraint, whereas the radius R_I of the dashed circle depends on the transmission power of primary users and the interference tolerance of B.

The use of a circle to illustrate the interference region is simplistic and immaterial. This definition applies to a general signal propagation and interference model by replacing the solid and dashed circles with, respectively, the subset of primary receivers that are potential victims of A's transmission and the subset of primary transmitters that can cause interference with the reception at B. The key message is that spectrum opportunities must be defined jointly at the transmitter and the receiver. It is a function of:

1. The transmission powers of both primary and secondary nodes.
2. The geographical locations of these nodes.
3. The interference constraint.

From this definition, we arrive at the following properties of spectrum opportunity.

Property 1 Spectrum Opportunity

P1.1 Spectrum opportunity depends on both transmitting and receiving activities of primary users.

P1.2 Spectrum opportunity is, in general, asymmetric: A channel that is an opportunity when A is the transmitter and B the receiver may not be an opportunity when B is the transmitter and A the receiver.

P1.1 shows clearly the difference between detecting primary signals (i.e., the presence of primary transmitters) and detecting spectrum opportunities. P1.2 leads to a complex relationship between opportunity detection performance at the physical layer and the link throughput and interference constraint at the MAC layer.

3.2.2 Spectrum Opportunity Detection

Spectrum opportunity detection can be considered a binary hypothesis test. We adopt here the disk signal propagation and interference model as illustrated in Figure 3.1. The basic concepts presented here, however, apply to a general model.

Let $II(A,d,\mathrm{rx})$ denote the logical condition that there exist primary receivers within distance d to the secondary user A. Let $\overline{II(A,d,\mathrm{rx})}$ denote the complement of $II(A,d,\mathrm{rx})$. The two hypotheses for opportunity detection are then given by:

$$H_0 : \text{opportunity exists; that is,} \overline{II(A,r_1,\mathrm{rx})} \cap \overline{II(B,R_1,\mathrm{tx})}$$

$$H_1 : \text{no opportunity; that is,} II(A,r_1,\mathrm{rx}) \cup II(B,R_1,\mathrm{tx})$$

where $II(B,R_1,\mathrm{tx})$ and $\overline{II(B,R_1,\mathrm{tx})}$ are similarly defined, and R_1 and r_1 are, respectively, the interference range of primary and secondary users under the disk model. Notice that $\overline{II(A,d,\mathrm{rx})}$ corresponds to the logical condition on the transmission from A being "harmless" and $\overline{II(B,R_1,\mathrm{tx})}$ the logical condition on the reception at B being successful. Also notice the difference in the definition of the hypotheses for spectrum opportunity detection as compared to those for primary signal detection given in Equation (3.1).

Detection performance at the physical layer is measured by the probabilities of false alarm P_{FA} and miss detection P_{MD}. $P_{FA} = \Pr\{\text{decides}H_1 \mid H_0\}$, $P_{MD} = \Pr\{\text{decides}H_0 \mid H_1\}$. The trade-off between false alarm and miss detection is captured by the receiver operating characteristic, which gives $P_D = 1 - P_{MD}$ (probability of detection or detection power) as a function of P_{FA} (see Figure 3.3,later for illustration). In general, reducing P_{FA} comes at the price of increasing P_{MD} and vice versa. Since false alarms lead to overlooked spectrum

opportunities and miss detections are likely to result in collisions with primary users, the trade-off between false alarm and miss detection is crucial in the design of cognitive radio systems [25].

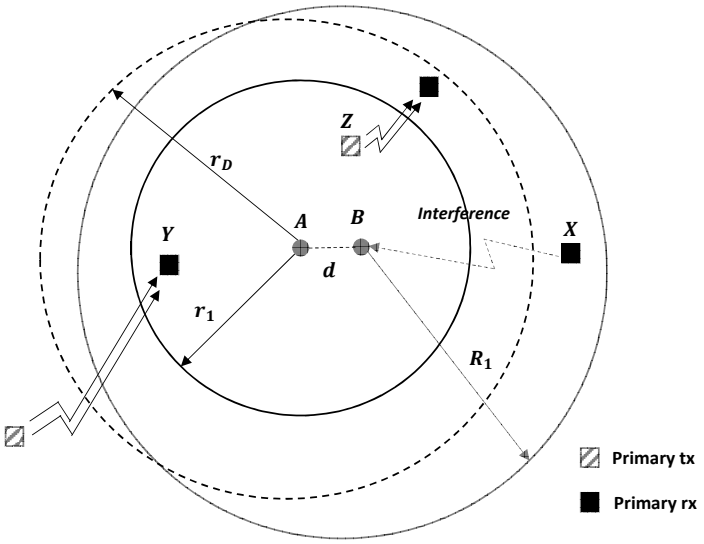


Fig. 3.2 The spectrum opportunity detection

Without assuming cooperation from primary users, the observations available to the secondary user for opportunity detection are the signals emitted from primary transmitters. This basic approach to opportunity detection is commonly referred to as listen before talk (LBT); that is, detecting spectrum opportunities by detecting primary signals. As shown in Figure 3.2, A infers the existence of spectrum opportunity from the absence of primary transmitters within its detection range r_D, where r_D can be adjusted by changing, for example, the threshold of an energy detector. The probabilities of false alarm P_{FA} and miss detection P_{MD} for LBT are thus given by:

$$P_{FA} = \Pr\{II(A, r_D, \text{tx}) \mid H_0\}, \quad P_{MD} = \Pr\{\overline{II(A, r_D, \text{tx})} \mid H_1\}. \tag{3.3}$$

Uncertainties, however, are inherent to such a scheme, even if A listens to primary signals with perfect ears (i.e., perfect detection of primary transmitters within its detection range r_D). Even in the absence of noise and fading, the geographic distribution and traffic pattern of primary users have significant impact on the performance of LBT. Specifically, there are three possible sources of detection errors: hidden transmitters, hidden receivers, and exposed transmitters. A *hidden transmitter* is a primary transmitter located within distance R_I to B but outside the detection range of A (node X in Figure 3.2). A *hidden receiver* is a primary receiver located within the interference range r_I of A but its corresponding primary

transmitter is outside the detection range of A (node Y in Figure 3.2). An *exposed transmitter* is a primary transmitter located within the detection range of A but transmits to a primary receiver outside the interference range of A (node Z in Figure 3.2). For the scenarios shown in Figure 3.2, even if A can perfectly detect the presence of signals from any primary transmitter located within its detection range r_D, the transmission from the exposed transmitter Y is a source of false alarms, whereas the transmission from the hidden transmitter X and the reception at the hidden receiver Z are sources of miss detections. As illustrated in Figure 3.3, adjusting the detection range r_D leads to different points on the ROC. It is obvious from Equation (3.3) that P_{FA} increases but P_{MD} decreases as r_D increases.

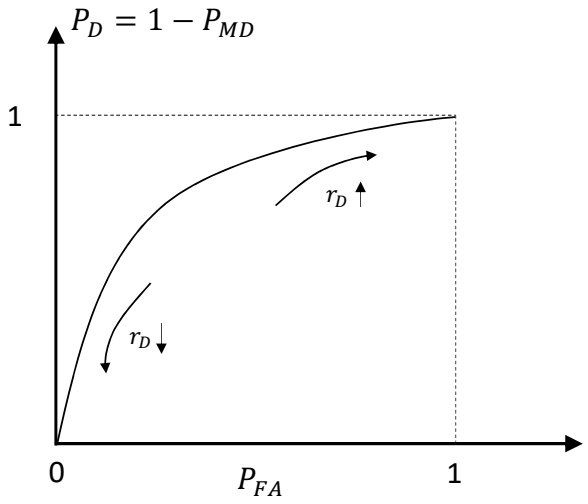


Fig. 3.3 ROC of spectrum opportunity detection (the ROC is obtained by varying the detection range r_D

3.3 Fundamental Trade-Offs: Performance vs. Constraint

A fundamental question in designing the spectrum opportunity detector is how to choose the detector operating point (P^*_{FA}, P^*_{MD}) to achieve the optimal trade-off between false alarms and miss detection. Such a trade-off, however, should be addressed in terms of Medium Access Control (MAC) layer performance: the throughput of the secondary user and the probability of colliding with primary users. A translation from the physical layer performance in terms of $\{P_{FA}, P_{MD}\}$ to the MAC layer performance in terms of throughput and interference constraint is therefore crucial in choosing the optimal operating point of the spectrum opportunity detector. The issue is addressed in this section, where we consider separately the so-called global and local interference models introduced in [26].

3.3.1 MAC Layer Performance Measures

The MAC layer performance is measured by the throughput of the secondary user and the interference to the primary users. The design objective is to maximize the throughput under a constraint on the maximum outage probability ζ that the interference at an active primary receiver exceeds the noise floor ρ. We refer to such events as *collisions with primary users*. The figures of merit at the MAC layer are given by the probability P_S of successful data transmission and the probability P_C of colliding with primary users. The objective and constraint at the MAC layer is thus given by:

$$\max \quad P_S \quad \text{subject to} \quad P_C \leq \zeta$$

We first consider P_S, which is application dependent. For applications requiring guaranteed delivery, an acknowledgment (ACK) signal from B to the secondary transmitter A is required to complete a data transmission. Specifically, in a successful data transmission, the following three events should occur in sequence: A detects the opportunity $\overline{II(A, r_D, \text{tx})}$ and transmits data to B; B receives data successfully $\overline{II(B, R_1, \text{tx})}$ and replies to A with an ACK; A receives the ACK $\overline{II(A, R_1, \text{tx})}$, which completes the transmission. We thus have

$$\begin{aligned} P_S &= \Pr\{\overline{II(A, r_D, \text{tx})} \cap \overline{II(B, R_1, \text{tx})} \cap \overline{II(A, R_1, \text{tx})}\} \\ &= \Pr\{\overline{II(A, r_E, \text{tx})} \cap \overline{II(B, R_1, \text{tx})}\}, \end{aligned} \tag{3.4}$$

where $r_E = \max\{r_D, R_1\}$. For best-effort delivery applications [27], acknowledgments are not required to confirm the completion of data transmissions. In this case, we have

$$P_S = \Pr\{\overline{II(A, r_D, \text{tx})} \cap \overline{II(B, R_1, \text{tx})}\}. \tag{3.5}$$

The probability of collision is defined as (In obtaining the definition of P_C, we have assumed that the interference caused by the ACK signal is negligible due to its short duration):

$$P_C = \Pr\{A \text{ transmits data} \mid II(A, r_1, \text{rx})\}. \tag{3.6}$$

Note that P_C is conditioned on $II(A, r_1, \text{rx})$ instead of H_1. Clearly, $\Pr[II(A, r_1, rx)] \leq \Pr[H_1]$.

Since the secondary transmitter A transmits data if and only if A detects no nearby primary transmitters, we have

$$P_C = \Pr\{\overline{II(A, r_D, \text{tx})} \mid II(A, r_1, \text{rx})\}. \tag{3.7}$$

3.3.2 Global Interference Model

Consider first a global interference model where the transmission from every primary user of interest affects the reception at B and the transmission from A affects the reception at every primary user. Under this condition, an opportunity occurs if and only if no primary users are transmitting. Spectrum opportunities are thus symmetric, and detecting primary signals is equivalent to detecting spectrum opportunities. Furthermore, we have the following properties, assuming that A transmits in a slot if and only if the channel is detected as an opportunity at the beginning of this slot.

Property 2 PHY-MAC Translation under the Global Interference Model

P2.1 Successful transmissions from A to B can result only from opportunities (i.e., H_0).

P2.2 Every correctly identified opportunity leads to a successful transmission.

P2.3 Every miss detection results in a collision with primary users.

These properties lead to the following simple relationship between $\{P_{FA}, P_{MD}\}$ and $\{P_S, P_C\}$.

$$P_S = (1 - P_F)\Pr[H_0], \quad P_C = P_{MD}. \tag{3.8}$$

With this relationship, to maximize P_S under the constraint of $P_C \leq \zeta$, we can obtain the optimal operating point (P^*_{FA}, P^*_{MD}) for the spectrum sensor. The joint design of the spectrum sensor at the physical layer and the tracking and access decisions at the MAC layer are addressed in [25], which shows that the optimal detector operating characteristic is given by $P^*_{MD} = \zeta$ and the optimal access policy at the MAC layer is to simply trust the spectrum detector: Transmit if and only if the channel is detected as an opportunity.

3.3.3 Local Interference Model

When the transmissions from primary and secondary users have local effect, the statements and the relationship between $\{P_{FA}, P_{MD}\}$ and $\{P_S, P_C\}$ given in Equation (3.8) no longer hold. The relationship between PHY and MAC has complex dependency on the applications and the use of MAC handshaking.

Impact of Application

We illustrate here the impact of applications on the relationship between PHY and MAC. Specifically, we compare applications requiring guaranteed delivery with those relying on best effort (for example, media streaming and network gaming). For the former, we assume immediate acknowledgment is required at the end of each slot to complete a successful data transmission. For the latter, acknowledgments are not necessary. Due to the asymmetry of spectrum opportunities and the local effect of transmissions, we have the following relationship between $\{P_{FA}, P_{MD}\}$ and $\{P_S, P_C\}$.

Property 3 PHY-MAC Translation under the Local Interference Model

P3.1 For both types of applications, $P_C \neq P_{MD}$.

P3.2 For applications with guaranteed delivery, correctly detected opportunities may lead to failed data transmission, and miss detections may lead to successful data transmission; that is,

$$\Pr[success \mid H_0] \leq 1 - P_{FA}, \quad 0 < \Pr[success \mid H_1] \leq P_{MD}$$

P3.3 For best-effort delivery, correctly detected opportunities always result in successful data transmission, and miss detections may also lead to successful data transmission; that is,

$$\Pr[success \mid H_0] = 1 - P_{FA}, \quad 0 < \Pr[success \mid H_1] \leq P_{MD}$$

Impact of MAC Handshaking

The fundamental deficiency of detecting spectrum opportunities from detecting primary signals resembles the hidden and exposed terminal problem in the conventional ad hoc networks of peer users. It is therefore natural to consider the use of a (Request To Send/ Clear To Send) RTS/CTS handshaking to enhance the detection performance of LBT. We show here that, although RTS/CTS signaling can improve the performance of opportunity detection at the physical layer, it may lead to decreased throughput at the MAC layer for best-effort delivery applications.

For RTS/CTS-enhanced LBT, spectrum opportunity detection is done jointly by A and B through the exchange of RTS/CTS signals. Specifically, the transmitter A first detects a chosen set of primary transmitters. If there are no signals from this set, it transmits an RTS to B. Upon receiving the RTS (which automatically indicates the absence of interfering primary transmitters), B replies with a CTS. A successful exchange of RTS/CTS indicates an opportunity, and A starts to transmit data to B. For this RTS/CTS-enhanced LBT, we have the following relationship between $\{P_{FA}, P_{MD}\}$ and $\{P_S, P_C\}$.

Property 4 PHY-MAC Translation with RTS/CTS Signaling

P4.1 $P_C = \frac{Pr[H_1]}{Pr[II(A,rx)]} P_{MD} \geq P_{MD}$

P4.2 Correctly detected opportunities always result in successful data transmission, as well as miss detections; that is,

$$P_S = (1 - P_{FA}) \Pr[H_0] + P_{MD} \Pr[H_1]$$

The PHY and MAC performance of RTS/CTA-enhanced LBT in a Poisson primary network with uniform traffic can be similarly analyzed [28]. An example ROC curve is shown in Figure 3.4. Note that (0, 0) does not belong to the ROC curve of RTS/CTS-enhanced LBT.

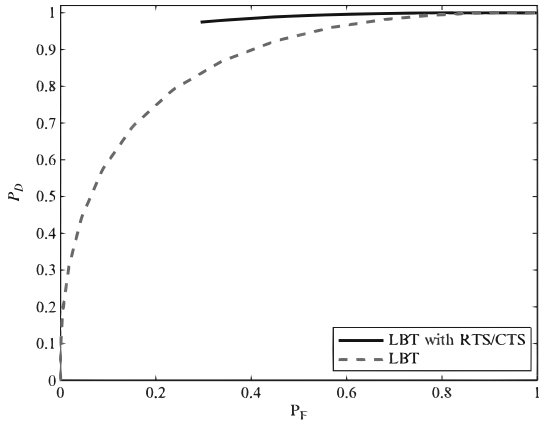


Fig. 3.4 ROC performance comparison.

This is because the effective detection range is bounded above RI, since to receive the CTS signal successfully, no primary transmitters can be within R_1 of A. In other words, a detection range $r_D \leq R_1$ leads to the same (P_{FA}, P_{MD}) as $r_D = R_1$. It can be shown that the ROC performance of RTS/CTS-enhanced LBT is always better than or equal to that of LBT when $r_D \geq R_1$. However, at the MAC layer, RTS/CTS-enhanced LBT may lead to lower throughput when the collision constraint is less restrictive and the application requires only best-effort delivery, as shown in Figure 3.5. Note that, using RTS/CTS-enhanced LBT, the throughput is the same for guaranteed delivery and best-effort delivery. This suggests that whether to adopt handshaking at the MAC layer depends on the applications and the interference constraint ζ.

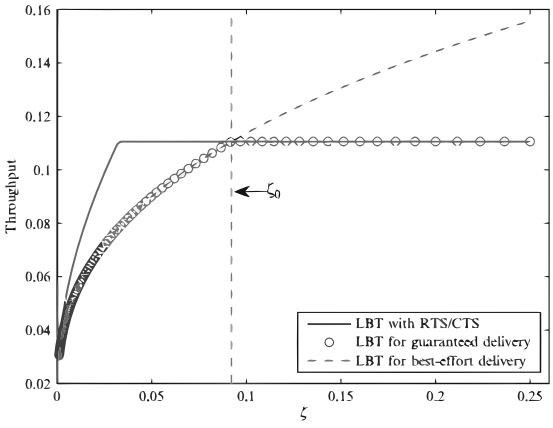


Fig. 3.5 Throughput comparison.

Chapter 4

Spectrum Access and Sharing

4.1 Introduction

This chapter deals with methods of accessing and sharing radio spectrum in wireless communications. Wireless communication is achieved by transmission and reception of electromagnetic waves utilizing swaths of radio spectrum ranging from (in some exceptional cases) as low as the extremely low-frequency (ELF) band (3–30 Hz) to as high as the extremely high-frequency (EHF) band (30–300 GHz). Due to the physical characteristics of different frequency bands, such as wavelength, information capacity, and propagation, the 30–3000 MHz portion of the radio spectrum is the most sought-after resource for various mobile and wireless applications. Given that multiple users, or ultimately multiple entities, need to access

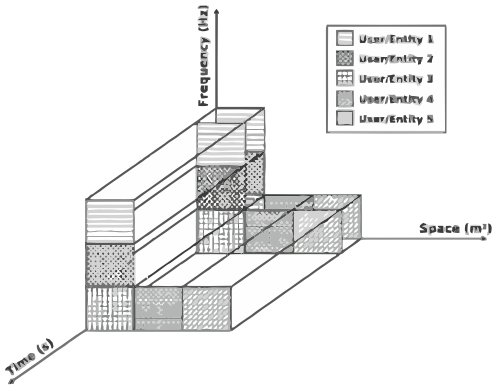


Fig. 4.1 Dimensions of spectrum access and sharing.

the radio spectrum for a variety of purposes, mechanisms should exist to allow the sharing of this resource, facilitating maximum utilization of every frequency band. A number of spectrum sharing scenarios can be envisaged, whereby the physical dimensions upon which

spectrum sharing can be realized include time, frequency, and space, as shown in Figure 4.1. The propagation characteristics of electromagnetic waves do not, however, generally allow precise decomposition of the radio spectrum into orthogonal components as depicted in Figure 4.1; for instance, it is generally not possible to confine the propagation of radio waves to a specific location, such as an urban or rural area. The raw principles of spectrum sharing do, however, normally assume the possibility of such decomposition. Frequency-domain spectrum sharing is widely used in the form of frequency division multiple access (FDMA) and orthogonal FDMA (OFDMA)–based systems.

A different way of looking at spectrum sharing classifications is from the spectrum access rights point of view. In this context, the first possibility is sharing the *licensed spectrum* resource, for instance, within a radio access network (RAN) among all users. To this end, depending on the radio access technology (RAT) used, multiple access control (MAC) techniques, such as time division multiple access (TDMA), frequency division multiple access (FDMA), or code division multiple access (CDMA), can be utilized. In either network-to-user communications, referred to as *downlink* (DL) communications in many cellular contexts, or user-to-network communications, referred to as *uplink* (UL) in many contexts, a unique set of spectrum resources, such as time slots, subchannels, codes, or a combination of these, are allocated to each user.

Another spectrum sharing possibility from the spectrum access rights point of view is the coexistence of several radio access technologies or service providers in the same licensed frequency band. Since all participating systems have equal rights in accessing the spectrum, such an approach is one manifestation of *horizontal spectrum sharing*. One example realization of this concept is "lite-licensing," recently introduced by the FCC [29].

Finally, a *vertical spectrum sharing* technique in a licensed band can be envisioned as a primary system, which is generally the license holder of that specific band, having the highest priority in accessing the resource, coexisting with a lower-priority secondary system that can access the spectrum only by complying with the primary's stringent requirements. Such requirements might include interference avoidance rules or maximum allowable transmission power, among other constraints.

Definition: Spectrum sharing is the simultaneous usage of a specific radio frequency band in a specific geographical area by a number of independent entities, leveraged through mechanisms other than traditional multiple- and random-access techniques.

4.2 Unlicensed Spectrum Sharing

Unlicensed frequency bands are chunks of spectrum set aside to be used by devices that wish to operate in a way that is not constricted by licenses and the associated complicated transmission/ownership rules and are therefore prone to interference. The most commonly used unlicensed bands are the 2.4 GHz ISM band, used by IEEE 802.11 b/g/n and Bluetooth devices, and the 5 GHz UNII band, as used by IEEE 802.11a and the European HyperLAN standards. As mentioned previously, as they are unlicensed, none of these bands is solely reserved for specific wireless communications technologies; for instance, most microwave ovens also operate in the 2.4 GHz ISM band, thereby creating additional interference.

There are actually a number of reasons as to why the usage of such unprotected bands is so popular. First, there is the ease of developing innovative technologies to operate in unlicensed bands, since a cumbersome approval process similar to licensed technologies is not involved; second, there is no cost to the consumer of using such bands. The successful deployment and rapid growth of WLAN technologies, such as the IEEE 802.11 family, is one of the fruits of the creation of unlicensed bands.

4.3 licensed Spectrum Sharing

licensed bands are frequency bands assigned exclusively to a licensee, for instance, a specific mobile operator. Traditionally, such a license award also stipulates a specific technology to be used in the band, for example, GSM or UMTS.

4.4 Secondary Spectrum Access

A promising approach to tackle the problem of spectrum underutilization is the secondary spectrum analysis (SSA) paradigm. The two categories of SSA solutions are real-time and non-real-time SSA, elaborated on in the following sections. A viable enabling technology to harness the potential of SSA is cognitive radio (CR).

There are two classes of SSA solutions, based on the method of coexistence of the primary and secondary systems. In the overlay approach, the secondary is allowed to access bands only where and when no primary communication is available. The second possibility is the underlay approach, where the primary accepts the possibility of interference up to a predefined (and agreed) threshold. In the former case, the main challenge is the accurate and timely sensing of the shared channel to identify the existence of the primary transmissions. After reliable detection of spectrum opportunities is achieved, adaptive transmission schemes

should be employed to efficiently "aggregate" the randomly distributed spectrum holes into a wideband, high-data-rate communication channel. Multicarrier modulation schemes are invaluable enabling mechanisms to this end.

In section 4.6.3 we introduce a multicarrier CDMA transceiver capable of cognitive communication. In the latter case of primary–secondary coexistence—that is, the underlay approach—the interfering effect of the secondary's transmissions on the available primary receivers should be determined. This in turn mandates acquiring channel state information (CSI) to every primary receiver within the transmission range of the secondary transmitter. We investigate the underlay transmission principle through an OFDM-based underlay scheme in Section 4.6.4.

Secondary spectrum access, as leveraged through the deployment of cognitive radio technology, provides a vertical spectrum sharing solution in the sense that the secondary user of the spectrum is allowed to access the licensed band of the primary user only in adherence to strict access rules and the requirements of the primary system. The main requirement here is that of interference avoidance, so as not to degrade the primary system's quality of service.

4.5 Non-Real-Time SSA

In some situations, the license owner of a specific band might be willing to allow a temporary secondary system to access that band for a specific time period and in a specific location. This spectrum sharing paradigm, which is referred to as *non-real-time SSA*, can be interpreted as the temporary suballocation of the rights to transmit in a band, at a certain time and space, to a system other than the license holder of the band. Consider, for instance, a local council/school/university/church, which has received a license to broadcast its public service programs, such as training courses/public information, in a particular band. Such services are generally arranged for a limited duration of time, such as the opening time of the council. If the regulations concerning the award of the band's license allow, the license owner could rent the unutilized spectrum in a specific time (and location) when (and where) it is not being used to raise additional capital. This approach to sharing the medium has been used extensively in wired broadcasting services, such as cable TV, whereby a number of content providers share a specific cable channel to broadcast their content. Therefore, spectrum regulations are, perhaps, the most pertinent obstacle to this spectrum sharing approach, rather than specific technical solutions.

4.6 Real Time SSA

The rest of this chapter focuses on technical solutions regarding the application of real-time SSA. In general, it is possible to classify such technical solutions into *negotiated* or *opportunistic* access approaches.

4.6.1 Negotiated Access

Whenever a medium for interaction between the primary and secondary systems exists, negotiated SSA is a possibility, depending on the negotiating terms. One interesting possibility assisting negotiated access is the availability of a universal signaling channel for cognitive purposes. One task of such a signaling channel could be to facilitate overlay SSA by indicating the availability of spectrum opportunities in a licensed band. To this end, the primary system might broadcast information (including access constraints, such as the permitted transmission power level and usage time interval) about an idle resource on the cognitive pilot channel (CPC), for potential secondary users to seize the chance to transmit on the offered resource [30],[31]. Alternatively, under a different access paradigm, which puts the onus for protecting the spectrum on the primary system, the primary system might broadcast information about busy resources, so as to ban the secondary transmitter from interfering in those bands at specific times or locations. Note that identification of an idle band, such as through broadcasts on the CPC, does not guarantee optimum prevention of interference to the primary receivers (or indeed optimum secondary use of resources), due to the "hidden node" problem, for example (see Figure 4.2). Conversely, an essential consideration for secondary

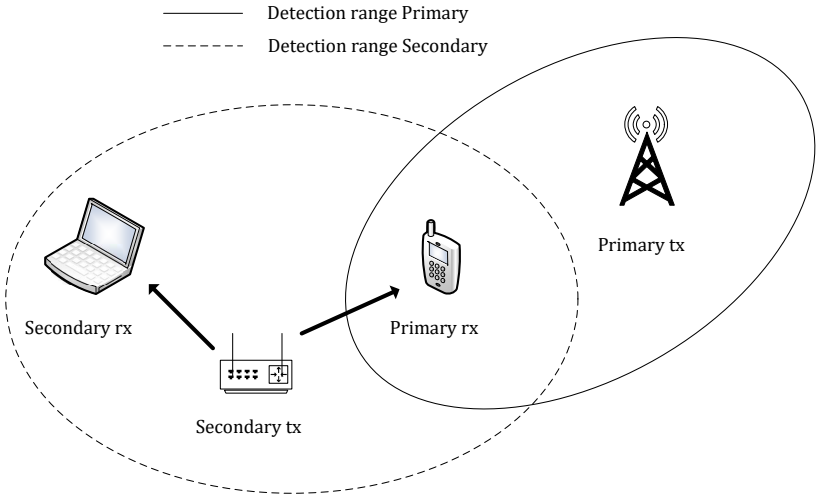


Fig. 4.2 Hidden node problem, pertinent to primary–secondary spectrum access with the transmitter-centric interference detection approach.

transmitters in an underlay SSA regime is the determination of the interference effects of their transmissions on the primary receivers. This calls for a receiver-centric approach to interference mitigation, as opposed to the current transmitter-centric approach. To this end, instead of identifying an idle spectrum band for secondary access, the CR needs to determine which transmission power should be used in a specific channel in order to mitigate interfering with the primary receivers.

4.6.2 Opportunistic Access

In many real-time SSA scenarios, the possibility of interaction between primary and secondary systems does not exist. This might be due to the lack of a signaling channel such as the CPC, or simply might be a result of the nature of the primary system, for instance, the primary system being a TV channel or a radar system. Under such circumstances, the secondary system might instead "opportunistically" identify and utilize idle resources, as appropriate.

Spectrum opportunities in opportunistic SSA contexts arise in two forms: overlay access, also known as spectrum holes or white spaces, where a portion of the band is left completely idle by the primary users, and *underlay access*, also known as *gray spaces*, where although the primary system is active on a specific band, it can be determined by the secondary system that its transmissions will not impose an inadmissible level of interference to the primary system [5]. To identify transmission opportunities within either the spectrum hole or the underlay approach, reliable spectrum sensing techniques can be exploited. The reliability of such sensing techniques is most challenging when uncertain elements exist in the channel due to shadowing and fading or in the receiver due to thermal noise [32],[33].

4.6.3 Overlay Approach

A CR should ideally sense a large swath of spectrum, to identify sufficient secondary access opportunities. There is a high probability that, at any given timeand location, a CR will identify several smaller and randomly located idle bands, rather than a single large chunk of idle bandwidth that it can opportunistically access. It is therefore necessary to "aggregate" smaller noncontiguously located spectrum opportunities to create a higher data rate transmission for cognitive communication. To this end, multicarrier modulations schemes are appropriate tools for opportunistic spectrum access. We discuss some such schemes later.

Currently, many wireless communication standards are being develop based on orthogonal division frequency multiplexing (OFDM). The capability of OFDM modulation for spectrum

sharing has been known for some time [14]. In [14], using an allocation vector—that is, a vector of zeros and ones for the bins of the inverse fast Fourier transform (IFFT) block at the OFDM transmitter—the use of portions of the band can be banned to mitigate interference. Furthermore, [34] proposes an OFDM-based design for cognitive operations, namely, discontiguous OFDM. The proposed technique in [34] also follows the methodology of deactivating fixed-bandwidth subbands overlapping with the primary system, to mitigate interference. However, even taking into account this subband deactivation at the secondary transmitter, there is still the possibility of interference in the nullified subbands, due to the side lobes of adjacent OFDM subbands. These side lobes do not impose any interference on the secondary OFDM-based receiver, as they are zero at the sampling instants (i.e., the orthogonality of OFDM subbands). However, given that the primary receiver is not synchronized with the secondary transmitter, they do cause interference to the primary receiver. One solution to eliminate these interfering side lobes is to use a filter after the IFFT process in the secondary transmitter; however, this causes performance degradation due to the loss of orthogonality of the OFDM subbands [34]. Alternatively, not only the overlapped subchannels, but also adjacent OFDM subchannels to the primary's signal should be deactivated in a bid to create a "guard band" between the primary and secondary systems. This approach, however, is not spectrally efficient, and spectral efficiency is the very issue that primary–secondary spectrum sharing is trying to solve.

Another multicarrier modulation approach is to use the principles of direct sequence CDMA (DS-CDMA) to create multicarrier CDMA (MC-CDMA) [35]. In single-carrier DS-CDMA, data symbols are spread using a unique, very long spreading code per user, which results in distribution of signal power over a large bandwidth. MC-CDMA uses shorter spreading codes, spreading data symbols over a series of disjoint carrier frequencies. Use of such multicarrier modulations is desirable due to the achieved frequency diversity and effective mitigation of frequency selective fading.

Let us now focus on the problem of aggregating a number of spectrum holes without creating uncontrolled interference to the primary receivers. Interference to primary receivers when transmitting using a MC-CDMA system can be avoided through using the subband deactivation technique, similarly to the OFDM case. A comparison of noncontiguous OFDM (NC-OFDM) and noncontiguous MC-CDMA (NC-MC-CDMA) has been investigated in [36]. It is shown that, as the number of deactivated subbands increases, the bit error rate (BER) performance degradation of NC-MC-CDMA becomes more than for the NC-OFDM approach. Instead of deactivating fixed-bandwidth subbands, we proposed a cognitive MC-CDMA that can adaptively change its transmission parameters, such as bandwidth and power of subbands, according to the interference pattern in the shared channel [37],[38]. This

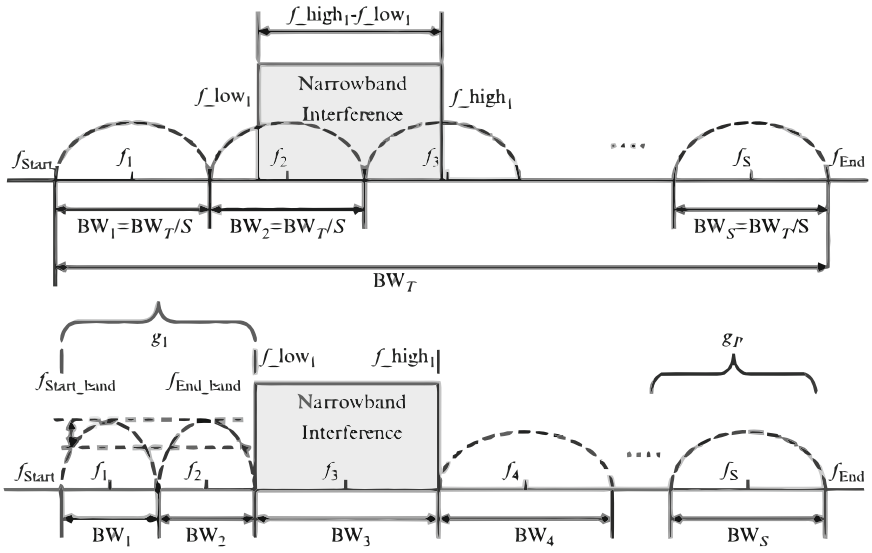


Fig. 4.3 Comparison of spectrum partitioning for legacy and adaptive MC-CDMA in the presence of a narrowband interfering signal; that is, the primary signal in the channel.

approach is shown in Figure 4.3. Compared to the subband deactivation method, our method increases spectrum usage efficiency considerably, because it excludes only the portion of the band affected by the interference. Also, the proposed method avoids the OFDM interference leakage problem [34]. The bottleneck for cognitive MC-CDMA, however, is the availability of sharp adjustable filters and appropriate spreading codes. It is worth noting that due to the spread-spectrum nature of this approach, the imperfect implementation of filters results in only minimal interference on legacy systems.

4.6.4 Underlay Approach

While identifying and using spectrum holes provides higher insurance in interference mitigation toward primary users, far more spectrum capacity can be leveraged through the secondary system transmitting in portions of band that are being actively used by the primary system. This, of course, must be done such that the operation of the secondary system does not cause performance degradation on the primary system through imposing an unacceptable level of interference to it[1].

A deterministic solution for such an underlay scheme is ultra-wideband (UWB) transmission. By deterministic, we are referring to the fact that transmission power and the occupied

[1] In an overlay cognitive transmission scheme, as discussed previously in this chapter, the secondary cognitive transmitter identifies the absence of the primary transmission in the band before starting its own transmission. In such scenarios there is a nonzero probability that the secondary transmitter erroneously decides a band is free to use while primary signal is still transmitting in the band

bandwidth of UWB systems is independent of any primary system and fixed through regulations. The stringent transmission power mask defined by spectrum regulatory bodies for UWB transmission, together with the relatively high operating frequency of UWB, ensures a very localized interference pattern toward any nearby primary receiver.

Another interesting solution for opportunistic underlay SSA can be envisioned in cases where the secondary transmitter can receive and "decode" the primary transmitter's message before the primary receiver. In such situations, powerful coding techniques, such as dirty paper coding [39], can be utilized to allow the secondary link to share the band with infinitesimal interaction with the primary system [40]. In this context, the knowledge of the channel as well as transmitted data are effectively utilized to undo the received interference at the primary receiver, given a known channel condition.

Further opportunities for underlay access can be identified through random variations of the shared channel. More specifically, if the signal power of the secondary transmissions is considerably attenuated before reaching the primary receiver, through channel propagation phenomena such as path loss, shadowing, or fading, coexistence of primary and secondary systems is indeed possible. Such desirable channel conditions, however, follow random patterns, usually characterized by their statistical characteristics. Consider Figure 4.4 depicting an interference channel where $tx_1 - rx_1$ are the primary and $tx_2 - rx_2$ are the secondary users of a band. There are N subchannels in a total channel bandwidth B, all with the same bandwidth ω. Each subchannel is narrow enough for flat fading to be a realistic assumption, and channel gains follow an independent and identical distribution with unit mean.

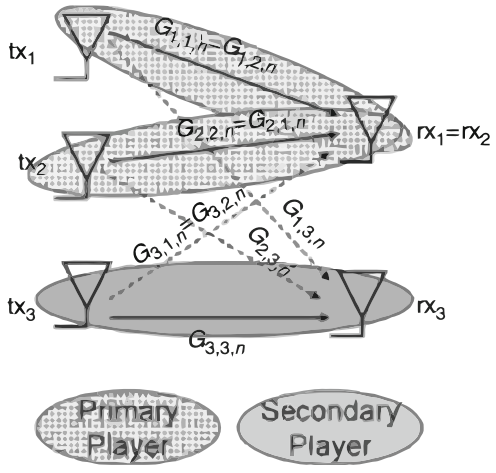


Fig. 4.4 Two-link interference channel setup, pertinent to many spectrum sharing scenarios.

Chapter 5

Agile Transmission Techniques

5.1 Introduction

The physical layer (PHY) is the first layer of the open system interconnection model (OSIM). The physical layer deals with bit-level transmission between different devices and supports electrical or mechanical interface connecting to the physical medium for synchronized communication.

This layer plays with most of the network's physical connections - wireless transmission, cabling, cabling standards and types, connectors and types, network interface cards, and more - as per network requirements. However, the physical layer does not deal with the actual physical medium (like copper, fiber). The physical layer is aimed at consolidating the hardware requirements of a network to enable the successful transmission of data. Network engineers can define different bit-transmission mechanisms for the physical layer level, including the shapes and types of connectors, cables, and frequencies for each physical medium. The physical layer sometimes plays an important role in the effective sharing of available communication resources, and helps avoid contention among multiple users. It also handles the transmission rate to improve the flow of data between a sender and receiver. The physical layer provides the following services:

- Modulates the process of converting a signal from one form to another so that it can be physically transmitted over a communication channel.
- Bit-by-bit delivery.
- Line coding, which allows data to be sent by hardware devices that are optimized for digital communications that may have discreet timing on the transmission link.
- Bit synchronization for synchronous serial communications.

- Start-stop signaling and flow control in asynchronous serial communication.
- Circuit switching and multiplexing hardware control of multiplexed digital signals. Carrier sensing and collision detection, whereby the physical layer detects carrier availability and avoids the congestion problems caused by undeliverable packets.
- Signal equalization to ensure reliable connections and facilitate multiplexing.
- Forward error correction/channel coding such as error correction code.
- Bit interleaving to improve error correction.
- Auto-negotiation.
- Transmission mode control.

The physical (PHY) layer fundamentals concerning the use of orthogonal frequency division multiplexing (OFDM). Several underlying principles and the resulting advantages confirm the efficiency with which OFDM enables high-speed wireless communications.

The choice of a physical layer transmission technique is a very important design decision when implementing a cognitive radio. In particular, the technique must be sufficiently agile to enable unlicensed users to transmit in a licensed band while not interfering with the incumbent users. Moreover, to support throughput-intensive applications, the technique should be capable of handling high data rates. One technique that meets both these requirements is a variant of orthogonal frequency division multiplexing called *noncontiguous OFDM* (NC-OFDM) [36].

Compared to other techniques, NC-OFDM is capable of deactivating subcarriers across its transmission bandwidth that could potentially interfere with the transmission of other users. Moreover, NC-OFDM can support a high aggregate data rate with the remaining subcarriers and simultaneously maintain an acceptable level of error robustness. Despite the advantages of NC-OFDM, two critical design issues are associated with this technique. First, the detection of the white spaces in the licensed bands for secondary-user transmissions. Radio parameter adaptation and hardware reconfiguration are another crucial requirement.

5.2 Wireless Transmission for Dynamic Spectrum Access

Figure 5.1 shows a dynamic spectral access (DSA) scenario that is viewed as a solution to the problem of the artificial spectral scarcity. As shown in this figure, at any time instant, several noncontiguous spectral regions are left unused. These unused portions can be used by secondary users for high-speed wireless communications while simultaneously ensuring

that the primary user's rights are not violated. This idea of using multiple noncontiguous portions of spectrum is referred to as *spectrum pooling* [30].

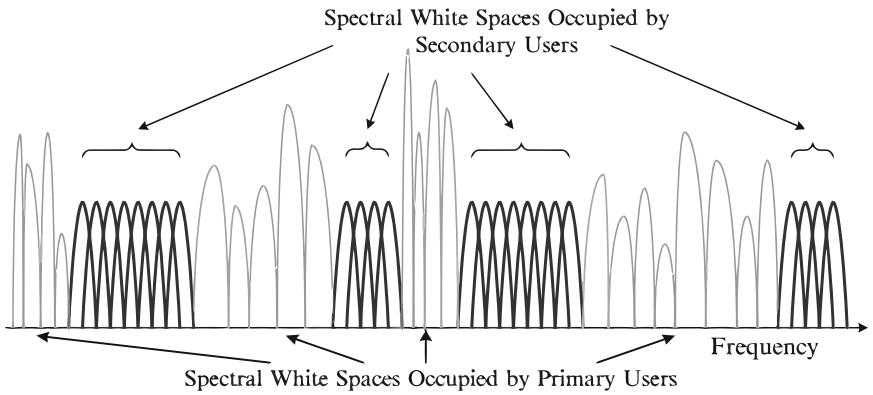


Fig. 5.1 The utilization of noncontiguous regions of spectrum for wireless transmission.

5.2.1 Underlay and Overlay Transmission

Spectrum sharing techniques can be classified into *underlay* and *overlay* spectrum sharing based on the spectrum access techniques. Underlay systems use ultrawideband (UWB) [41] or spread-spectrum techniques, such as code division multiple access (CDMA) [42], to transmit the signal below the noise floor of the spectrum [43].

An example of the time- and frequency-domain information of an underlay spectrum sharing system is shown in Figure 5.2(a). In this figure, we see that the underlay systems use wideband low-power signals for transmissions. However, this technique can increase the overall noise temperature and thereby worsen error robustness of the primary users as compared to the case without underlay systems. To avoid any interference to the primary users, the underlay system can use interference avoidance techniques, such as *notching* [44] and *waveform adaptation* [45].

The spectrum holes[1] filled in by secondary transmissions in an overlay system are shown in Figure 5.2(b). When interference among the users is high, it has been shown that frequency division multiplexing is an optimal technique [46].

As shown in this figure, the overlay systems use the unoccupied portions of the spectrum with guard intervals for secondary transmissions, keeping the interference to the primary users to a minimum. Since the licensed system has privileged access to the spectrum, it must not be disturbed by any secondary transmissions. This results in two main design goals for an overlay system [47]:

[1] A spectrum hole is an unused portion of the licensed spectrum.

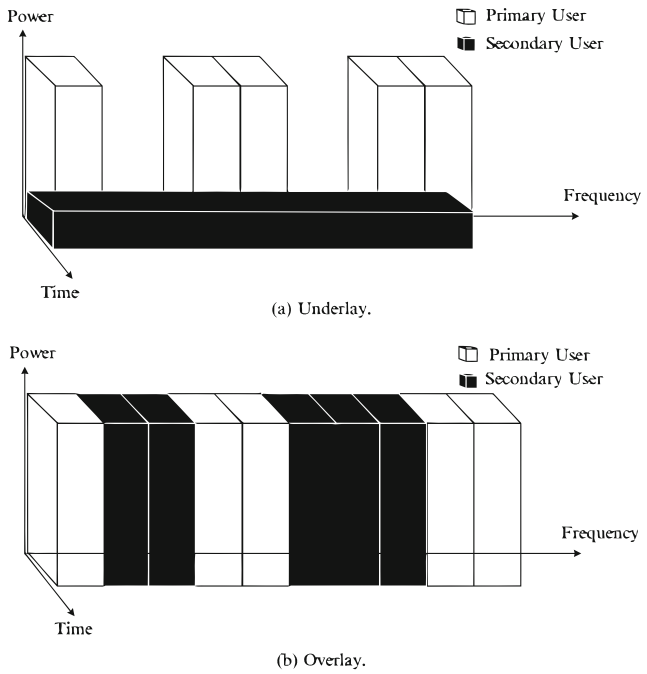


Fig. 5.2 Overlay and underlay spectrum sharing.

- Minimum interference to licensed transmissions.
- Maximum exploitation of the gaps in the time–frequency domain.

To achieve these goals, the overlay system needs information about the spectrum allocation of the licensed systems.

5.3 Noncontiguous Orthogonal Frequency Division Multiplexing

A general schematic of an NC-OFDM transceiver is shown in Figure 6.4. Without loss of generality, a high-speed data stream, $x(n)$, is modulated using $M-ary$ phase shift keying (MPSK). Then, the modulated data stream is split into N slower data streams using a serial-to-parallel (S/P) converter. Note that the subcarriers in the NC-OFDM transceiver do not need to be all active as in conventional OFDM. Moreover, active subcarriers are located in the unoccupied spectrum bands, which are determined by dynamic spectrum sensing techniques. The inverse fast Fourier transform (IFFT) is then applied to these modulated subcarrier signals. Prior to transmission, a guard interval with a length greater than the channel delay spread is added to each NC-OFDM symbol using the cyclic prefix (CP) block

to mitigate the effects of intersymbol interference (ISI). Following the parallel-to-serial (P/S) conversion, the baseband NC-OFDM signal, $s(n)$, is passed through the transmitter radio frequency chain, which amplifies the signal and up-converts it to the desired center frequency.

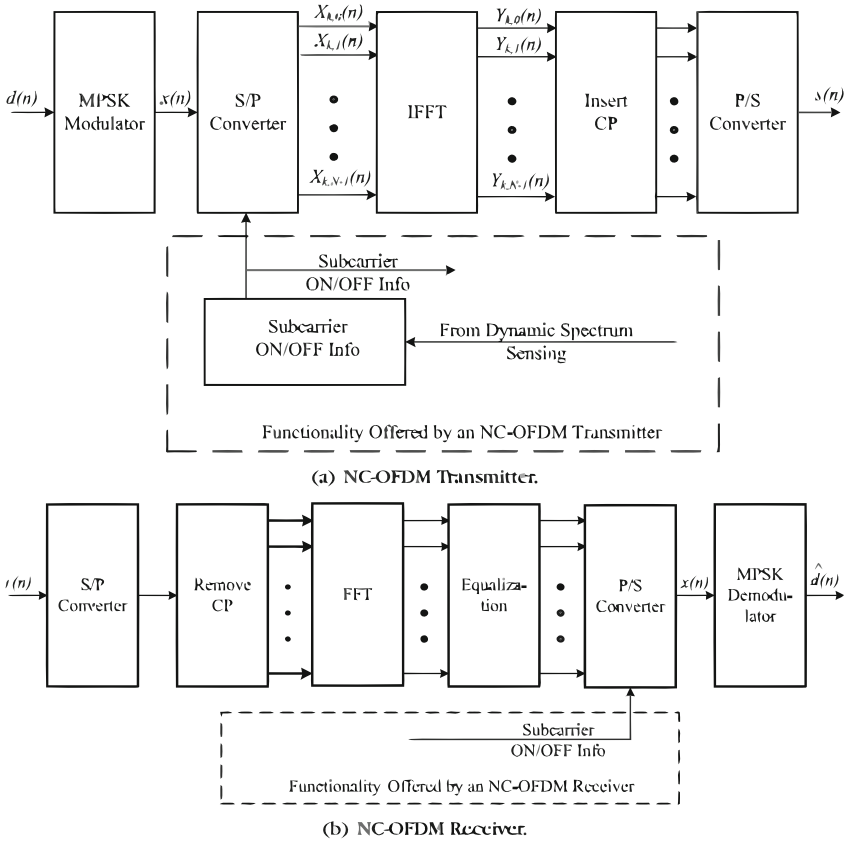


Fig. 5.3 An NC-OFDM transceiver.

The receiver performs the reverse operation of the transmitter, mixing the RF signal to the baseband for processing, yielding the signal $r(n)$. Then, the signal is converted into parallel streams using the S/P converter, the CP is discarded, and the FFT is applied to transform the time domain data into the frequency domain. After compensating distortion introduced by the channel using equalization, the data in the active subcarriers are multiplexed using a P/S converter, and demodulated into a reconstructed version of the original high-speed input, $\hat{x}(n)$.

From this system overview, we observe that the spectrum sensing, spectrum shaping, peak-to-average power ratio, radio parameter adaption, and efficient radio implementation are critical issues associated with an OFDM-based cognitive radio.

Chapter 6

CR for Broadband Wireless Access in TV Bands: The IEEE 802.22 Standards

6.1 Introduction and Defining CR

We mentioned earlier some definitions of CR. Presented here is a figurative glossary of definitions—and some of them paraphrased from different sources and put together for easy comparison.

Mitola [30]: Wireless personal digital assistants and the related networks that are sufficiently computationally intelligent about radio resources, and related computer-to-computer communications, to detect user needs as a function of use context and to provide radio resources and wireless services most appropriate to those needs.

Wikipedia: Cognitive radio is a paradigm for wireless communication in which either a network or a wireless node changes its transmission or reception parameters to communicate efficiently, avoiding interference with licensed or unlicensed users. This alteration of parameters is based on the active monitoring of several factors in the external and internal radio environment, such as radio frequency spectrum, user behavior, and network state.

IEEE 1900.1 [48]: (a) A type of radio in which communication systems are aware of their environment and internal state and can make decisions about their radio operating behavior based on that information and predefined objectives; (b) cognitive radio [as defined in item a] that uses software-defined radio, adaptive radio, and other technologies to adjust automatically its behavior or operations to achieve desired objectives.

Haykin[5]: Cognitive radio is an intelligent wireless communication system that is aware of its environment and uses the methodology of understanding by building to learn from the

environment and adapt to statistical variations in the input stimuli to achieve high reliability and efficient utilization of the radio spectrum.

Scientific American: Cognitive radio is an emerging smart wireless communications technology that will be able to find and connect with any nearby open radio frequency to best serve the user. Therefore, a cognitive radio should be able to switch from a band of the radio spectrum that is blocked by interference to a free one to complete a transmission link, a capability that is particularly important in an emergency.

Rondeau and Bostian [49]: Cognitive radio is a system that has a cognitive engine performing modeling, learning, and optimizing the processes to reconfigure the communication system including the radio layer by taking the information from users, radio, and the context.

To conclude, here we define the CR—in layman's terms—as the concept with which the wireless nodes adapt their properties, including radio, to achieve overall efficient spectrum usage, in time and space, based on the factors such as radio, radio environment, policies, and higher-layer requirements with an inherent and constant learning to improve the spectrum usage.

6.2 Concepts Related to Spectrum Management

We can consider three essential models: *exclusive spectrum management* (ESM), the *spectrum commons* (SC) sharing model, and *hierarchical spectrum management* (HSM). The ESM model still gives exclusive channel usage to each user or service provider but differs from a static assignment in the sense that the channels are allocated dynamically among possible licensees. The process of exclusive channel access is usually governed by radio regulation bodies. The differences between ESM approaches, specified in Figure 6.1, depend on the economic model, which varies from country to country. In the SC model, different users compete for the assigned frequencies on equal terms. The HSM model gives *primary (licensed)* users (PUs) more rights to use the spectrum than other *secondary (unlicensed)* users (SUs). We can distinguish two HSM approaches. In *overlay* HSM, only one user/system can use a frequency band at a particular space and time, and the SUs have to back off when a PU is present. However, when no PU is present, the SU can opportunistically use the frequency band, so this technique is also referred to as *opportunistic spectrum access*. In *underlay* HSM, an SU can transmit on an already occupied band if this transmission does not increase the interference to the PU above a given threshold.

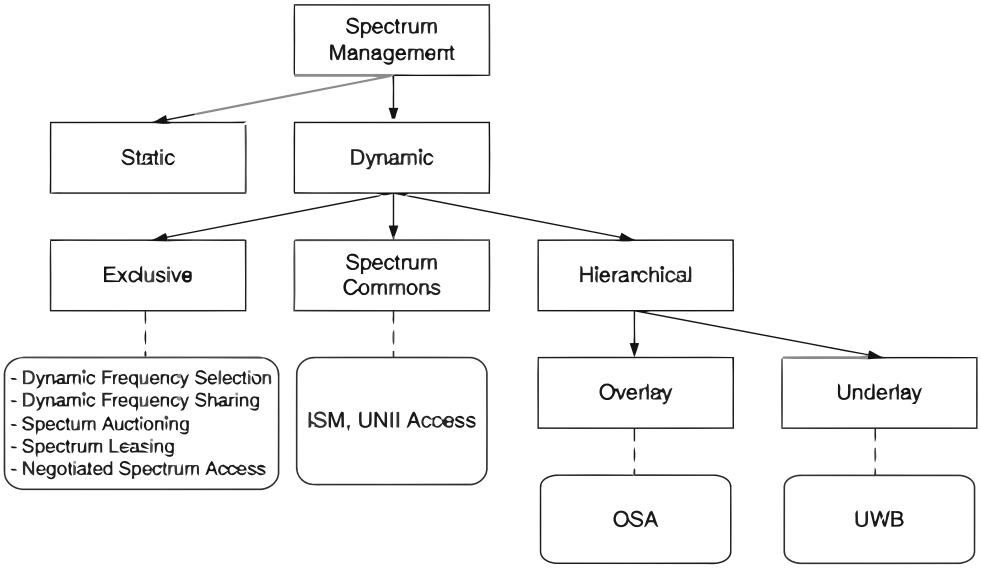


Fig. 6.1 Modern spectrum management: classification with the application examples.

6.3 Regulatory Scenario for TV White Space

The IEEE 802.22 standard was formed in light of the TV band NPRM released by the FCC [50], which proposes to open the spectrum allocated to the TV service for unlicensed operation based on CRs. In the United States, TV stations operate from channels 2 to 69 in the VHF and UHF portions of the radio spectrum. All these channels are 6 MHz wide and span from 54–72 MHz, 76–88 MHz, 174–216 MHz, and 470–806 MHz. In addition to the TV service, also called *primary service*, other services such as wireless microphones are also allowed by the FCC to operate on vacant TV channels on a non-interfering basis, and so are private land and commercial mobile radio services (PLMRS/CMRS) including public safety.

6.4 Dynamic Spectrum Access Models

The two models with which spectrum access can be done are spectrum property rights and the spectrum commons approach. The *spectrum property* rights approach suggests that the spectrum can be treated like land, and private ownership of the spectrum is viable. This approach entails the holder of spectrum to have exclusive use of the spectrum portion it possesses, without the potential of harmful interference from other parties. Owners would be able to trade their spectrum in a secondary market. The use of the spectrum would be flexible, in that the authorized party could use the spectrum portion for any purpose. The

FCC has chosen a partial implementation of this approach by employing spectrum auctions as a means of licensing. But this approach has efficiency issues, as seen in TV bands.

The spectrum commons approach allows the bands to be open to technologies as long as they follow the rules of access in the specific band; as smart technologies evolve, communicating devices will become able to avoid interference through mutual cooperation and coexistence and the spectrum will become unscarce. This phenomenon has been seen in the 2.4 GHz industrial, scientific, and medical (ISM) band as well as the 5 GHz UNII band. The emergence of cognitive and software defined radio concepts, multiple-antenna and multicarrier techniques, as well as ultra-wide-band (UWB) technologies and mesh network topologies provide a technology panacea that proponents of this approach use to support their arguments.

The approach for IEEE 802.22 WRAN is slightly different in the sense that the operation of WRAN causes no interference to the incumbents on the TV bands and there are mechanisms in the entire system design to build an efficient radio.

6.5 Overview of IEEE 802.22 Standard

The wireless regional networks for which this standard is developed are expected to operate in lower population density areas and provide broadband access to data networks using vacant TV channels in the VHF and UHF bands in the range of frequencies between 54 MHz and 862 MHz, while avoiding interference to the broadcast incumbents on these bands. A typical application will be the coverage of the rural area around a village, as illustrated in Figure 6.2, within a radius of 17–30 km, depending on the effective isotropic radiated power (EIRP) of the base station using adaptive modulation, although the MAC could accommodate user terminals located as far as 100 km when exceptional radio frequency (RF) signal propagation conditions prevail.

As indicated in the 802.22 functional requirement document, the capacity at the user terminal is expected to be of 1.5 Mb/s in the downstream and 384 kb/s in the upstream. The service availability due to radio frequency propagation is assumed to be at 50% of locations to allow the service provider to reach subscribers in fringe areas, and 99.9% of the time to provide a reliable connection where it is possible. The average spectrum efficiency over the coverage area is expected to be around 2 bps/Hz, given the adaptive modulation parameters and the operating constraints described later; and assuming a 6 MHz TV channel bandwidth and a 40:1 over-subscription ratio resulting from the stochastic nature of the data network usage, this translates into a total of 255 user terminals that can be served by the base station per TV channel.

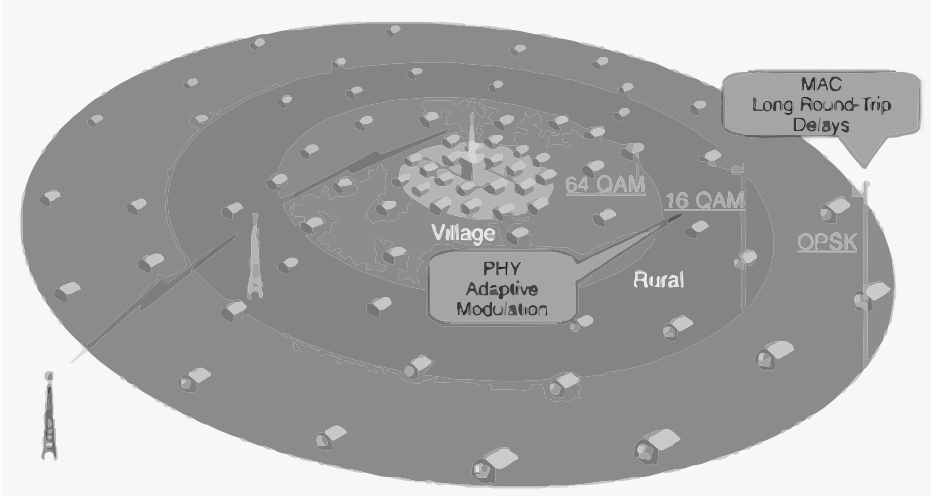


Fig. 6.2 Typical application of the 802.22 WRAN standard.

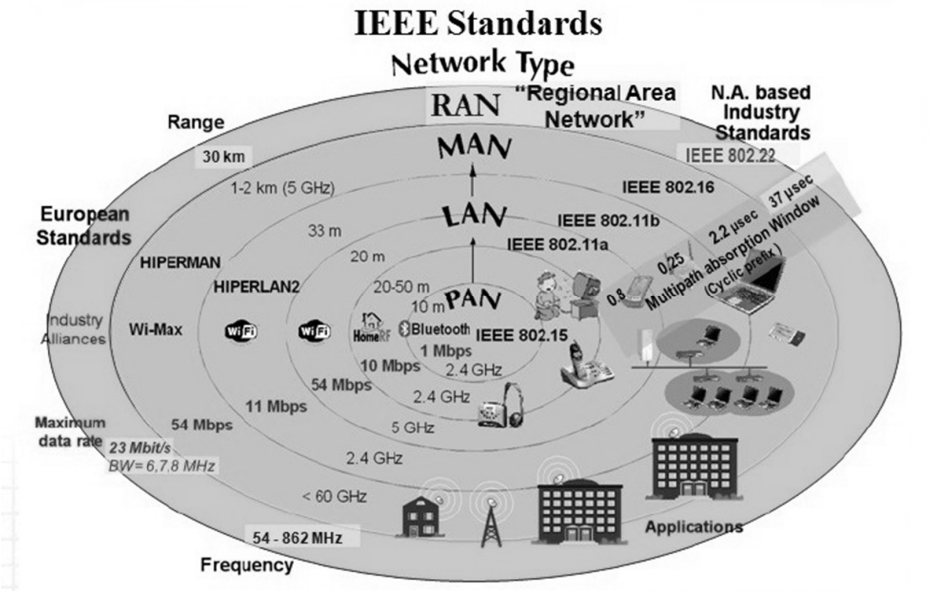


Fig. 6.3 Characteristics of the WRAN standard relative to other wireless network standards.

Figure 6.3 illustrates the main characteristics of the 802.22 WRAN standard relative to the other existing wireless network standards.

6.5.1 Applications

The most prominent target application of 802.22 WRANs is wireless broadband access in rural and remote areas with performance comparable to those of existing fixed broadband–access technologies (e.g., DSL and cable modems) serving urban and suburban areas [51]. While the availability of broadband access may not be so critical in urban and perhaps suburban areas, the costs of which remain high, this certainly is not the case in rural and remote areas where about half of the United States and most of the developing nations (other countries located in South America, Africa, and Asia) populations are concentrated. Therefore, this has triggered the FCC to stimulate the development of new technologies (e.g., based on CRs) that increase the availability of broadband access in these underserved markets.

6.5.2 Reference Architecture

The 802.22 system specifies a fixed point-to-multipoint (PMP) wireless air interface whereby a base station (BS) manages its own cell and all associated consumer premise equipment (CPEs), as depicted in Figure 14.3.

The BS (a professionally installed entity) controls the medium access in its cell and transmits in the downstream direction to the various CPEs, which respond back to the BS in the upstream direction. To ensure the protection of incumbent services, the 802.22 system follows a strict masters/slave relationship, wherein the BS performs the role of the master and the CPEs are the slaves. No CPE is allowed to transmit before receiving proper authorization from a BS, which also controls all the RF characteristics (e.g., modulation, coding, and frequencies of operation) used by the CPEs. In addition to the traditional role of a BS, which is to regulate data transmission in a cell, an 802.22 BS manages a unique feature of distributed sensing. This is needed to ensure proper incumbent protection and is managed by the BS, which instructs the various CPEs to perform distributed measurement activities.

6.6 IEEE 802.22 Physical Layer

The 802.22 PHY layer is specifically designed to support a system that uses vacant TV channels to provide wireless communication access over distances of up to 100 km. The PHY specification is based on orthogonal frequency division multiple access (OFDMA) for

both upstream (US) and downstream (DS) access, and its key parameters are summarized in Table 6.4. The PHY modes for a reference 6 MHz TV channel are given in Table 6.5.

Parameter	**Specifications**	**Remark**
Frequency Range	54-862 MHz	
Bandwidth	6 MHz, 7 MHz, 8 MHz	To accommodate TV band channelization of different regulatory domains
Payload modulation	QPSK, 16-QAM, 64-QAM	BPSK used for preambles, pilots and CDMA codes
Transmit effective isotropic radiated power	Default 4 W for CPEs	Currently 4 W for BS in the United States but may vary in other regulatory domains
Multiple access	OFDMA	
FFT size	2048	
Cyclic prefix modes	1/4, 1/8, 1/16, 1/32	
Duplexing	TDD	

Fig. 6.4 IEEE 802.22 System Parameters

PHY Mode	Modulation	Coding Rate	Data Rate Mbps	Spectral Efficiency 6 MHz Channel
1	BPSK	Uncoded	4.54	0.76
2	QPSK	1/2	1.51	0.25
3	QPSK	1/2	4.54	0.76
4	QPSK	2/3	6.05	1.01
5	QPSK	3/4	6.81	1.13
6	QPSK	5/6	7.56	1.26
7	16-QAM	1/2	9.08	1.51
8	16-QAM	2/3	12.10	2.02
9	16-QAM	3/4	13.16	2.27
10	16-QAM	5/6	15.13	2.52
11	64-QAM	1/2	13.61	2.27
12	64-QAM	2/3	18.15	3.03
13	64-QAM	3/4	20.42	3.40
14	64-QAM	5/6	22.69	3.78

Fig. 6.5 PHY Modes the Data Rates Are Calculated Based on a CP to FTT Ratio of 1/16

6.6.1 Preamble, Control Header, and MAP Definition

Preamble Definition Two types of frequency domain sequences are defined to facilitate burst detection, synchronization, and channel estimation at a 802.22 receiver:

1. **Short training sequence (STS)** This sequence is formed by inserting a nonzero binary value on every fourth subcarrier. In the time domain, this results in four repetitions of a 512-sample sequence in each OFDM symbol.

2. **Long training sequence (LTS)** This sequence is formed by inserting a nonzero binary value on every second subcarrier. In the time domain, this results in two repetitions of a 1024-sample sequence in each OFDM symbol.

Control Header and MAP Definition In this subsection we define the structure of the two control headers (superframe control header (SCH) and frame control header (FCH)) and the MAPs (DS-MAP, US-MAP, DCD, and UCD). The SCH is transmitted using the PHY mode 1 (see Table 6.5) and TCP = 1/4 TFFT. It is transmitted over all data subcarriers, encoded by a rate-1/2 convolutional coder, and after interleaving, is mapped using QPSK constellation resulting in 336 QPSK symbols. To improve the robustness and make better utilization of the available subcarriers, spreading by a factor of 4 is applied to the output of the mapper, resulting in a maximum length of 42 bytes.

The FCH is transmitted as part of the DS protocol data unit (PDU) in the DS subframe and uses the basic data rate mode. The length of FCH is 4 bytes and it carries, among other things, the length (in bytes) information for the DS-MAP if it exists or the length of the US-MAP. The FCH is sent in the first two subchannels of the symbol immediately following the preamble symbol. To increase the robustness of the FCH, the encoded and mapped FCH data may be retransmitted, which is indicated through the SCH. The receiver can combine corresponding symbols from the two or three OFDM slots and decode the FCH data to determine the lengths of the following fields in the frame.

6.6.2 Channel Coding and Modulation Schemes

Figure 14.6 describes the channel coding process used in 802.22. Channel coding includes data scrambling, convolutional coding or advanced coding, puncturing, bit interleaving, and constellation mapping.

The frame payload data are first processed by the data scrambler using a pseudorandom binary sequence generator with the generator polynomial $1 + X^{14} + X^{15}$. The preamble and the control header fields of the frame are not scrambled. The forward error correction (FEC) scheme follows the data scrambler. The mandatory coding scheme in 802.22 is convolutional

coding. The data burst is encoded using a rate-1/2 binary convolutional encoder. Duo-binary convolutional turbo code, lowdensity parity check (LDPC) codes, and shortened block turbo codes (SBTCs) are optional advanced coding schemes. For the interleaving stage, the same interleaver used for subcarrier interleaving is employed to interleave encoded bits at the output of the encoder. The interleaving algorithm used in 802.22 is described by the block size K and three integer parameters (p,q,j). The global equation of the algorithm depends on the interleaving pattern of the previous iteration $(j-1)$, the position index of samples (k), and two integer parameters (p,q). The parameter P gives the interleaving partition size multiple of the interleaving block size K.

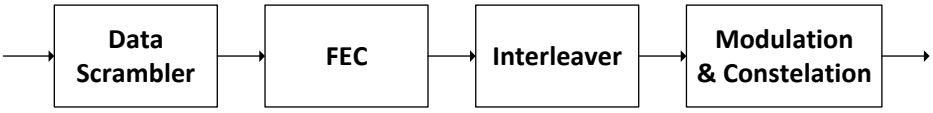


Fig. 6.6 Channel coding in 802.22.

Finally, the output of the bit interleaver is entered serially into the modulation and constellation mapper. The input data to the mapper are first divided into groups of N_{cbpc} (two for quadrature phase-shift keying (QPSK), four for 16-QAM, and six for 64-QAM) bits and converted into complex numbers representing QPSK, 16-QAM or 64-QAM, constellation points. The mapping for QPSK, 16-QAM, and 64-QAM is performed according to gray-coding constellation mapping. The pilot subcarriers are modulated according to the BPSK modulation using a modulation-dependent normalization factor equal to 1.

6.6.3 Transmit Power Control

Transmit power control (TPC) is an important feature in 802.22, since it requires that only the minimum transmit power necessary to keep a link be used while maintaining the link quality, which further enhances incumbent protection in addition to spectrum sensing, incumbent databases, geolocation, and so on. Each regulatory domain has its own transmit power constraints, and 802.22 is defined to comply with different regulatory requirements. The BS and CPE support monotonic power-level control with accuracy of ±0.5 dB, over a range of at least 60 dB, with a resolution (step size) of 1 dB. The EIRP of each CPE device is limited to the cap obtained from the BS, which, in turn, can obtain the power limits from an incumbent database or locally at the BS.

6.7 IEEE 802.22 Medium-Access Control Layer

In this section we provide an up-to-date overview of the 802.22 MAC layer with emphasis on the CR features key to support-required incumbent protection, self-coexistence among WRANs, and quality of service (QoS).

6.7.1 Superframe and Frame Structures

The 802.22 MAC uses a synchronous timing structure, where frames are grouped into a superframe structure, which was introduced to allow for better incumbent protection and self-coexistence. The superframe structure, depicted in Figure 6.7, consists of 16 frames with a fixed duration of 10 ms each. The BS starts the first frame within the superframe with the superframe preamble followed by the frame preamble and the superframe control header. The superframe preamble is used for time synchronization, while the frame preamble is used for channel estimation, allowing robust decoding of the SCH and following messages. The SCH carries the BS MAC address along with the schedule of quiet periods for sensing, as well as other information about the cell [52]. The SCH is transmitted at a very robust rate to allow for successful decoding over long distances, which is important to ensure neighboring WRANs to discover each other and avoid harmful interference. After the SCH, the BS transmits the frame control header (FCH), which is followed by the messages within the first frame. The remaining 15 frames within the super-frame start with the frame preamble followed by the FCH and subsequent data messages.

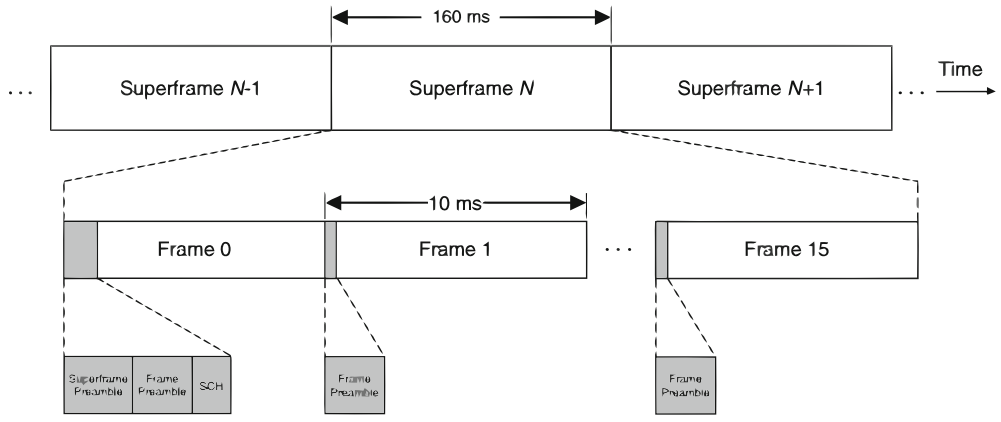


Fig. 6.7 MAC superframe structure.

The time-domain structure for a typical MAC frame is depicted in Figure 6.8. The frame is divided into DS and US subframes and the self-coexistence window (SCW), which can be scheduled by the BS at the end of the frame. The first downstream burst after the FCH

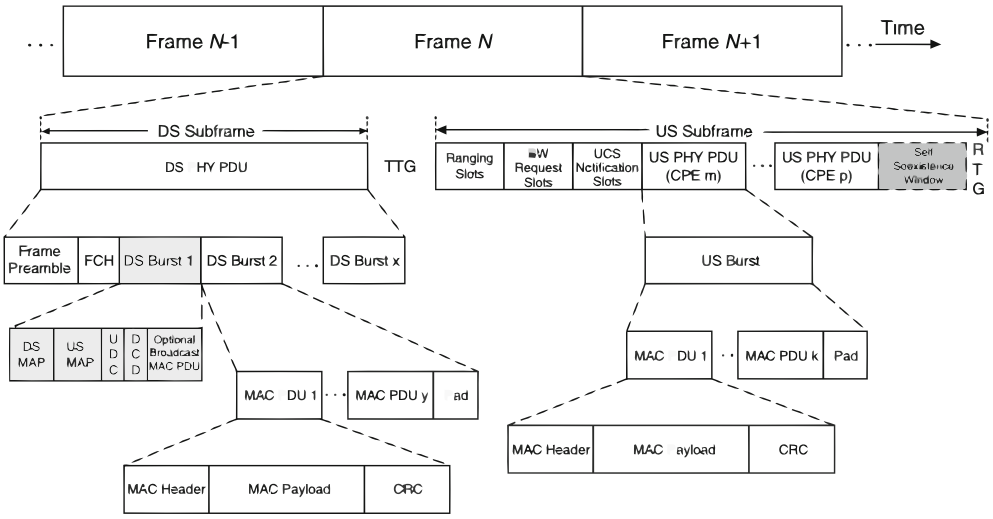


Fig. 6.8 MAC frame structure.

is used to transmit the DS/US MAPs, the DS/US channel descriptor messages (DCD and UCD), and other MAC broadcast messages. The DS/US MAPs are broadcast messages that specify the resource allocation in the DS and US subframes, respectively. The DCD and UCD are usually transmitted by the BS at periodic intervals to define the characteristics of the DS and US physical channels, respectively. After the initial control signaling, the BS can schedule the DS bursts for data transmission using different modulation/coding schemes for each burst [52]. In the US subframe, the BS can allocate resources for contentionbased access before the data bursts, which can be used for ranging, bandwidth (BW) request, and urgent coexistence situation (UCS) notification. The UCS window is another new feature in the 802.22 MAC, which can be used by CPEs to transmit an indication that an incumbent has been detected on the channel. Furthermore, the BS may also reserve up to five symbols at the end of the frame for the self-coexistence window. The SCW is used for execution of the coexistence beacon protocol (CBP), which involves transmission of coexistence beacons (or CBP packets) carrying information about the cell and specific coexistence mechanisms. The SCW and CBP packets are new cognitive radio features that allow for over-the-air coordination among neighboring 802.22 cells to facilitate incumbent protection and spectrum sharing mechanisms. They are described in more detail in the following sections.

6.7.2 Incumbent Detection and Notification Support

In this section we describe how the 802.22 MAC layer supports incumbent detection and notification, which may trigger events for frequency agility operations.

Two important capabilities were introduced in the MAC layer to support reliable incumbent detection:

1. **Network quiet periods.** To avoid interference with spectrum sensing, which has to meet very low incumbent detection thresholds (IDTs) (e.g., -116 dBm for DTV), the BS can schedule networkwide quiet periods (QPs), during which all transmissions are suspended, and hence sensing can be performed more reliably. Without QPs for sensing, the WRAN may face a high false alarm rate, especially in areas where multiple WRANs coverage areas overlap. Two types of QPs can be scheduled: intraframe and interframe QPs (see Figure 6.9). Intraframe QPs, as the name suggests, are short-duration QPs (less than a frame) and are useful for regular sensing of in-band channels [1] without affecting the QoS for WRAN users. However, the BS can also schedule longer interframe QPs across multiple frames, in case more time is needed for sensing. Interframe QPs should be used on an on-demand basis, since it affects the QoS of the users. Overall, the BS can limit the number and duration of QPs to the minimum necessary to meet the sensing requirements in terms of probability of detection and probability of false alarm. The BS can schedule QPs by using the QP scheduling fields in the SCH or it can use a specific management message, called *channel quiet request* (CHQ-REQ), to stop traffic at anytime within its cell.

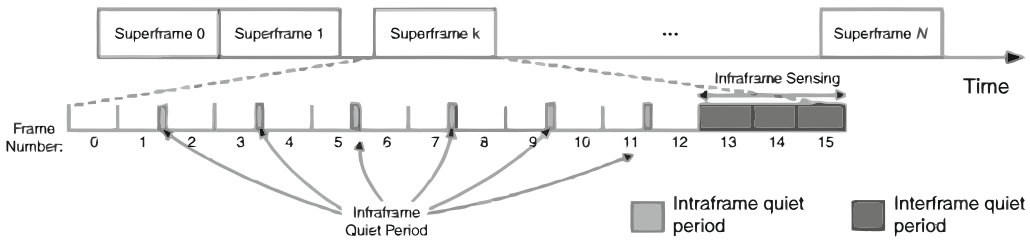


Fig. 6.9 Intraframe and interframe quiet periods.

2. **Channel measurement management.** In case an incumbent is detected by the BS, the BS can take the appropriate action to avoid interference, but when a CPE detects an incumbent, it has to report it to the BS. For that, the MAC layer includes channel measurement request and report messages, which allow the BS to take full control of the incumbent detection and notification process within its cell. The BS can also use management frames to request CPEs to perform other type of measurements, such as detection of other WRAN and other performance-related measurements. The

[1] In-band channels are the operating channel (N) and its first adjacent channels ($N-1$ *and* $N+1$).

BS is also responsible for allocating US resources for the CPEs to transmit their measurement reports after the sensing is completed. In case a CPE has detected the presence of incumbents but has not been allocated sufficient US bandwidth to transmit its measurements back to the BS, the CPE can use the UCS notification slots in the US subframe to inform the BS of the situation. The CPE uses a contention-based mechanism to transmit a UCS notification message to indicate an incumbent has been detected on the channel.

6.7.3 Multichannel Operation

To maintain connectivity for 802.22 users with QoS support in an incumbent detection situation. The 802.22 group tackled this issue using the concept of backup channels. During normal operation, the BS proactively maintains a list of backup channels. In case an incumbent is detected on in-band channels, the BS is responsible for triggering a switch to a backup channel within the CMT, which should occur seamlessly to maintain QoS guarantees for the 802.22 users. Obviously, the backup channel must also be clear of incumbents in order to be used right away. Therefore, incumbent detection must also be done in outof-band channels; that is, channels that may be used as backup. However, sensing backup channels may be done during the CPE's idle time and not require QPs in the operating channel. But, if the backup channel to be sensed is occupied by another WRAN, the CPEs should use the QPs scheduled in the corresponding channel to avoid interference from the other WRAN.

6.7.4 Synchronization

Synchronization is a key factor for successful operation of 802.22 systems, and it is needed not only for communication purposes between BS and CPEs but also for incumbent protection. The BS and CPEs in a cell must be synchronized to ensure no transmissions occur during the QP for sensing. Also, neighboring WRANs sharing the same channel (N) or operating on first and second adjacent channels $(N-2, N-1, N+1, N+2)$ must synchronize their QPs to avoid interference with incumbent sensing and reduce the false alarms rate. Although in-band channels include only up to first adjacent channels $(N, N+1 and N-1)$, synchronization of QPs up to second adjacent channels $(N+2 and N-2)$ is needed to avoid interference when sensing the first adjacent channels.

To facilitate synchronization of QPs, all the 802.22 BSs are required to be equipped with a satellite-based positioning system (e.g., GPS), which is used to derive the timing information for the superframes. Therefore, by specifying a common reference time, the standard ensures

all the superframes are synchronized. Once the superframes are synchronized, the next step is to synchronize the intraframe and interframe QPs.

To ensure QoS, the interframe QPs should be used only when strictly needed, and hence, they are scheduled on demand. Once other neighboring BSs receive information about a new interframe QP scheduled, they perform an algorithm to decide whether they should change their own QP schedule to align with the received schedule. The mechanism is based on the following rule to reduce the ping-pong effect [52]: "A BS 1 shall only modify its inter-frame sensing quiet period schedule to synchronize with the inter-frame sensing quiet period of another nearby BS 2 if the remaining time to BS 1's next inter-frame sensing quiet period is larger than the remaining time to BS 2's next inter-frame sensing quiet period."

6.7.5 Self-Coexistence

Self-coexistence also plays a key role in protecting the incumbents, due to the required coordination for reliable spectrum sensing; that is, synchronization of QPs. The self-coexistence problem is approached in 802.22 with the following key elements:

1. **Neighboring network discovery and coordination.** Network discovery is part of the initialization procedures for both BSs and CPEs, but it is also continuously done during the normal network operation as well. WRANs can be discovered through the SCH transmitted by the BSs or by CBP packets, which are transmitted during the SCW window by CPEs or BSs. CPEs that discover other neighboring WRANs send this information back to their BS in the format of measurement report messages. Upon discovery of new neighboring WRANs, the BS must consider whether QP synchronization is required.

2. **Coexistence beacon protocol.** The CBP protocol plays a key role in enabling efficient discovery and coordination of neighboring networks. BSs and CPEs can discover other WRANs by detecting CBP packets transmitted during the SCW window. The CBP packets carry information about the cell (e.g., BS MAC address, schedule of QPs, backup channels). During normal operation, the CPE should listen to its BS's SCH to identify any changes relevant to its cell, and since superframes are synchronized across cells, CPEs may not be able to detect neighboring BSs'SCH transmissions. The CBP packets provide additional support for network discovery, since they are transmitted during the SCWs, and the BS can explicitly request CPEs to listen to the channel during the SCW to detect CBP packets from other neighboring cells. The CBP packets may also carry information required for executing several resource sharing mechanisms, which requires information exchange between cells. In other words, the

CBP serves as an underlying protocol for inter-WRAN communication. The CBP protocol is useful in many scenarios, and a possible situation is illustrated in Figure **??**. In this example, the BSs A and B are outside of the communication range of each other, but CPEs A and B in the overlap area can relay information between the two cells via CBP packets.

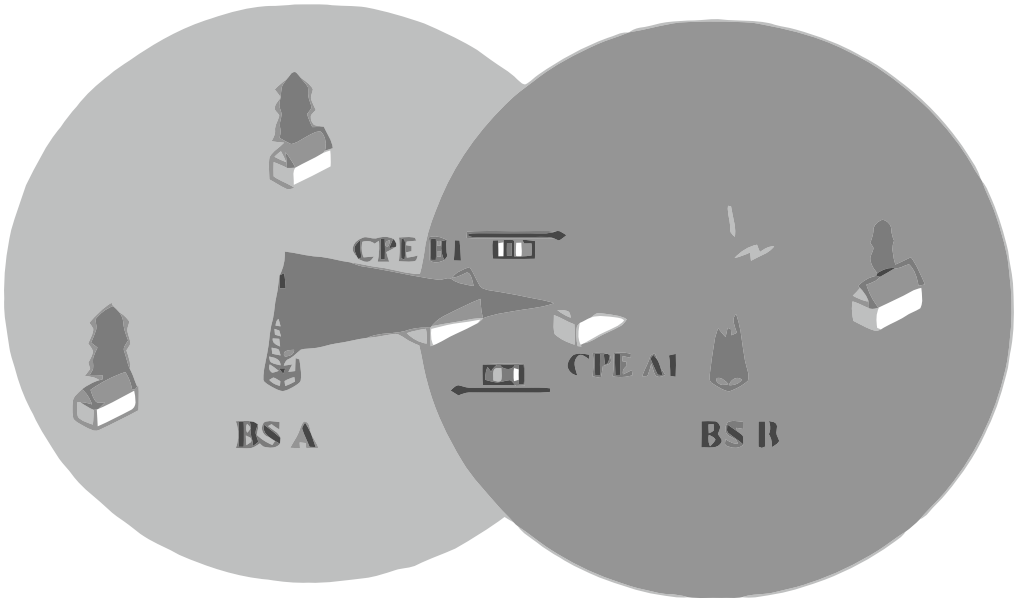


Fig. 6.10 Example scenario of inter-WRAN communication with CBP.

3. **Resource sharing mechanisms.** After network discovery, neighboring WRANs may have to consider how to share the available spectrum. Consider the example scenario in Figure 6.10 and suppose BS A and CPE A1 operate on a given channel N. When a new BS B and CPE B1 start operation, they first scan the available channels and CPE B1 eventually detects BS A's SCH or CBP packet transmitted by A1. At this point, BS B must execute the first coexistence mechanism, called *spectrum etiquette*. The main idea behind spectrum etiquette is to avoid operating cochannels with other existing WRANs. Therefore, BS B first searches for an available channel that is not used by BS A. However, if no other channel is available, BS B can share the same channel with BS A. Although not a desirable situation, this might happen in areas with only a few channels available, and the standard provides the required support for coexistence in such cases. BSs may engage in a negotiation process to share the channel on a frame-by-frame basis. Such negotiation may be based on spectrum contention mechanisms [52]. The negotiation between BSs is carried out through CBP packet exchanges. In the example in Figure 6.10, the CPEs are used to exchange CBP

packets, but in a scenario where BSs are within each other's communication range, they can transmit and receive the CBP packets themselves. It should be noted that such negotiation process between BSs may become a bottleneck as the number of neighboring BSs on the same channels increase.

Another problem that should be considered in coexistence scenarios where multiple BSs share the same channel is the potential collision of SCH transmissions from neighboring cells. Synchronization of the superframes across cells results in simultaneous transmissions of SCHs by all BSs in the beginning of every superframe, which may lead to collisions at CPEs in the overlapping areas. Due to the robust transmission mode, a CPE may be able to decode the SCH from its BS, even in presence of other SCH transmissions. However, depending on the distance between interfering BSs, SCH collisions might occur, which could prevent operation at some specific locations. This is still an open issue for the standard, but its impact might be minimal, depending on the availability of incumbent-free channels. Neighboring BSs will always try to find empty channels, and cochannel operation with other BSs is pursued only as the last resort to maintain connectivity. Nevertheless, several proposals are being considered to address this problem. In one possible approach, called *single-frequency network* (SFN), all overlapping BSs transmit a self-coexistence mode SCH, which is the same across all BSs and carries the frame allocations for different cells, while another option is to multiplex the SCH transmissions in the time domain.

6.7.6 Quality-of-Service Support

The adopted QoS service model is based on the IEEE 802.16d standard [53], which includes the following basic concepts:

1. **Service flow QoS scheduling.** The primary purpose of the QoS support at the MAC layer is to define the transmission ordering and scheduling onthe-air interface. That is achieved by associating packets traversing the MAC layer to a service flow, which is identified by a SFID (service flow identifier). A service flow is a unidirectional flow of packets provided a particular QoS support level, which is specified by a set of QoS parameters such as latency, jitter, and throughput guarantees. Four basic scheduling services are supported: unsolicited grant service (UGS), real-time polling service (rtPS), non-real-time polling service (nrtPS), and best effort (BE). The UGS service is designed to support real-time data streams consisting of fixed-size data packets sent at periodic intervals. The rtPS is designed to support real-time data streams consisting of variablesized data packets issued at periodic intervals, such as MPEG video. The nrtPS is designed to support delay-tolerant data streams consisting of variable-sized

data packets for which a minimum data rate is required, such as FTP. The BE service is designed to support data streams for which no minimum service level is required. More details about the QoS parameter sets for these services are described in the standard [52].

2. **Activation model.** Service flows can be classified as provisioned, admitted, or active. Provisioned service flows require a negotiation between CPE and BS to be activated. During this negotiation, the CPE sends the SFID and the associated QoS parameter sets to the BS, which may authorize the flow if resources are available. To activate a service flow, the BS maps the service flows to a CID (connection identifier), which identifies a connection between the CPE and BS across which the data are delivered. Service flows can also be in a transient admitted state, where the resources are not yet completely activated. In this two-phase model, the service flows are first admitted (passing admission control, where availability of the requested resources is verified), and the service can be activated later after the final end-to-end negotiations are finalized. This model saves network resources and is useful for applications in which a long-term reservation of resources is necessary or desirable. For instance, resources used by a voice call put on hold could be temporarily allocated to other services, but such resources should be available for resuming the call when needed.

3. **Dynamic service establishment.** The MAC layer provides a series of management messages and procedures to create (DSA), change (DSC), or delete (DSD) service flows. The DSA messages create a new service flow. The DSC messages change an existing service flow. The DSD messages delete an existing service flow. These procedures can be initiated by CPEs or BSs. Changing a service flow modifies the QoS parameters associated with the flow. The set of DSx messages provide full flexibility for the BS and CPEs to adapt the air interface resource allocation to their traffic requirements.

6.7.7 Spectrum Management Model

The 802.22 standard has adopted a spectrum management model, where each WRAN BS has a central entity, called a spectrum manager (SM). The SM is shown in Figure 6.11 as part the 802.22 protocol reference architecture [54]. The architecture shown in Figure **??** includes a new cognitive plane and security features and it replaces the previously adapted system architecture in Draft 1.0 [52]. The data and management planes are separated from the cognitive plane, which was introduced to support the new features for spectrum sensing and management and geolocation capabilities. As can be noted, security features are included

as sublayers in the three planes (data, management, and cognitive). These sublayers provide functions to verify spectrum and service availability, as well as various forms of device, data, and signal authentication; authorization; data; control and management message integrity; confidentiality; nonrepudiation; and so forth.

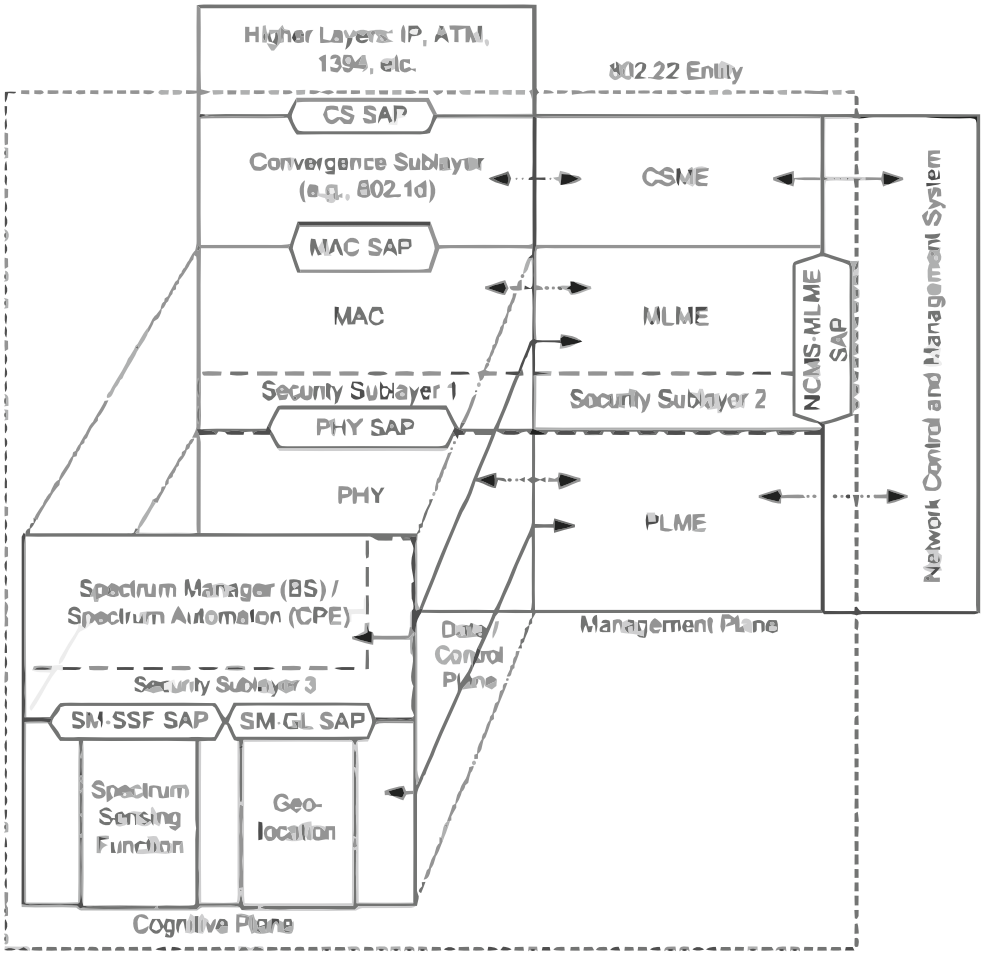


Fig. 6.11 Protocol reference architecture for an 802.22 BS or CPE.

6.7.8 Spectrum Manager

The SM collocated with the BS can be seen as the central intelligence of the system and it is part of the cognitive plane. On the other hand, the CPEs implement a corresponding entity called spectrum automaton (SA), which is basically a "slave" of the SM running at the BS. The CPE SA controls the local CPE's spectrum sensing function (SSF) when it is not under the control of a BS, for example, during initialization and scanning procedures. The

CPE SA can also use the SSF to perform sensing autonomously during the CPE's idle time. During normal operation the CPE SA responds to requests from the BS's SM, for instance, to perform spectrum sensing and report the results.

Within a WRAN cell, the SM centralizes all the decisions with respect to spectrum management, which includes the following:

1. Maintain up-to-date spectrum availability information.
2. Classify, set priorities, and select channels for operation and backup.
3. Maintain association control.
4. Trigger frequency agility-related actions (i.e., channel switch).
5. Manage mechanisms for self-coexistence (interference-free scheduling, renting/offering, and spectrum contention).

6.7.9 Incumbent Database Support

Incumbent databases may reduce the overhead on the system due to spectrum sensing, especially for DTV signals. For instance, if a channel is occupied in a given area by a TV station and this information is accessible through a database, the 802.22 BS may decide to reduce the frequency in which the channel is sensed by its associated CPEs or it may even decide to perform no sensing at all on that channel. there are other issues related to incumbent databases, such as accuracy of the database information and maintenance costs. Also, incumbent databases may not be efficient for more dynamic incumbents, such as wireless microphone; and the cost of maintaining a database for a large number of low-power devices (i.e., wireless microphones) may be prohibitive.

6.8 Limitation of Spectrum Sensing

Spectrum sensing is an important component of cognitive radio and the IEEE 802.22 standard, and this sections first derives the keep-out radius and the sensing radius to which the incumbents have to abide.

6.8.1 Incumbent Protection Radius

Table 6.12 states the incumbent protection parameters as outlined in IEEE 802.22 standard [52]. Assume that a DTV broadcasting station, is transmitting at 1 MW (90 dBm) effective radiated power (ERP) with an antenna height of 500 m. This DTV operates at 615 MHz in

the UHF band. Next, consider a WRAN sensor with a 0 dBi receive antenna gain, operating at some distance from the TV transmitter. The receive power for such a sensor is plotted in Figure 6.13 as a function of distance from the DTV transmitter, assuming a signal propagation model is conforming to ITU-R P1546 [2] [55].

Parameter	Wireless Microphones	TV Services
Incumbent detection threshold (IDT)	−107 dBm (over 200 kHz)	−116 dBm (over 6 MHz)
Probability of detection (PD)	90%	90%
Probability of false alarm (PFA)	10%	10%
Channel detection time (CDT)	≤2 sec	≤2 sec
Channel move time (CMT)	2 sec	2 sec
Channel closing transmission time (CCTT)	100 ms	100 ms

Fig. 6.12 IEEE 802.22 Incumbent Protection Parameters.

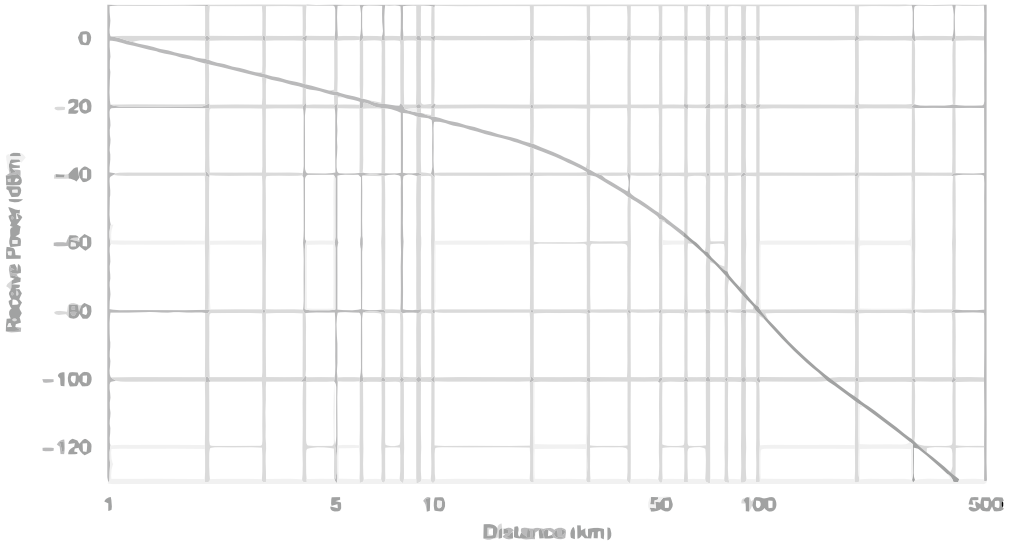


Fig. 6.13 DTV receive power versus distance for a 0 dBi rx antenna.

[2]This paper uses the propagation models specified in the ITU-R document P.1546-1, as is used in the IEEE 802.22 working group

Let P_{rx} be the instantaneous receive power (in dBm) and the average receive power be represented by $\bar{P}_{rx}$ (in dBm). The spatial mean receive power is given by the ITU-R recommended practice [55] as the sum of the average power and the shadow fading, which is a zero-mean normal random variable with a standard deviation of 5.5 dB. This is represented by

$$P_{rx} = \bar{P}_{rx} + F_S \quad [dBm]. \tag{6.1}$$

Having constructed the propagation model, we now describe how to calculate the "keep-out region" as outlined in IEEE 802.22 WRAN system. The keep-out region is a region around the primary user (e.g., DTV transmitter) where the WRAN system is not permitted to transmit, since it may cause harmful interference to the primary user. These calculations are based on [56], [57].

Calculating the Base Station Keep-out Region

The DTV protection contour, also referred to as the *noise-limited contour*, is located at a distance where the field strength is 41 $dB\mu$ using the $F(50,90)$ [3] propagation curve. All TV receivers within the protection contour must be free of harmful interference. In this scenario, this contour occurs at 134.2 km from the DTV transmitter. According to the FCC NPRM for DTV the desired to undesired (D/U) [4] ratio is 23 dB assuming that the interferer (i.e., the undesired signal) is another DTV transmitter. For the purpose of our study, we assume this D/U ratio also applies when the interferer is a WRAN signal.

Next, calculate the maximum undesired field strength at the edge of the noise limited contour. From that field strength, it is possible to determine how far away the WRAN transmitter must be located to cause no harmful interference to the DTV receiver. The undesired signal's allowable field strength is given by the following formula:

$$FS_U = FS_D - D/U + F/B \tag{6.2}$$

Here FS_U, FS_D, and F/B represent the undesired signal field strength at the noise limited contour, the desired field strength, and the antenna front-to-back ratio, respectively. The desired $F(50,90)$ field strength at this point is 41 dBu, which is the signal that needs to be protected. Hence, the D/U ratio must exceed 23 dB. Using a front-to-back ratio of 14 dB for the DTV receive antenna [57], the following limit on the undesired field strength at the DTV receiver is derived:

$$FS_U \leq 41 - 23 + 14 = 32 dBu. \tag{6.3}$$

[3] F(X, Y) represents the spatial and temporal relationship of the TV signal propagation as specified in P1546. It represents the field strength that would exceed a certain threshold at X% of locations for Y% of time [57].

[4] This is also referred to as the *signal-to-interference ratio* in wireless communications.

We assume a base station antenna height of 75 m. The distance at which the field strength of the undesired signal reaches 32 dBu is approximately 16.1 km, as can be seen in Figure 6.14. Adding 16.1 km to the DTV protection contour of 134.2 km, we obtain a keep-out region of 150.3 km from the DTV transmitter.

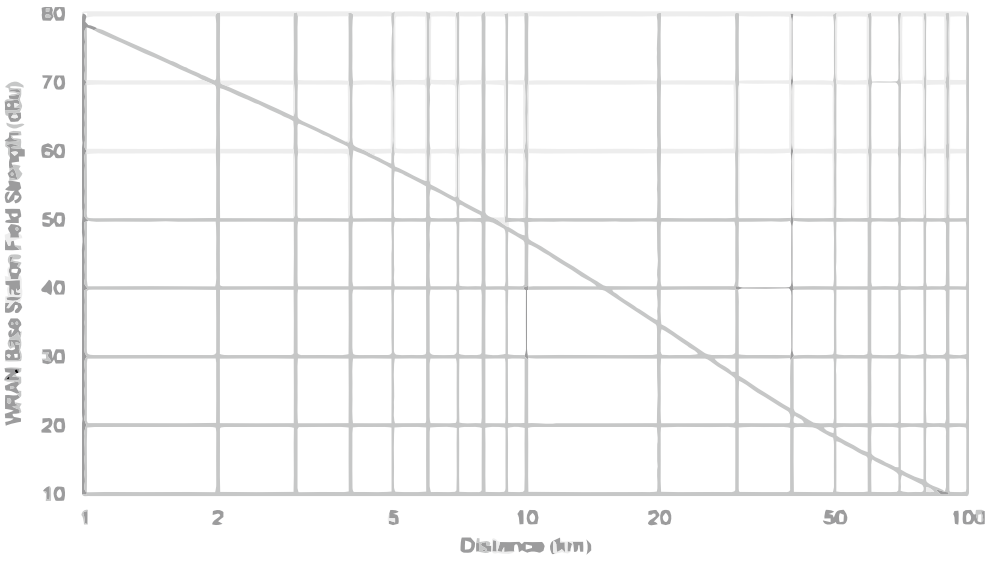


Fig. 6.14 WRAN base station field strength.

Calculating the CPE Keep-out Region

This analysis is similar to what was done for the base station keep-out region. The primary differences are the antenna height and antenna directionality. For residential use, antenna heights are typically 10 m, and antennas are assumed to be directional with a front-to-back ratio of 14 dB.

Assuming the CPE antenna height of 10 m and using the F(50, 10) propagation curve, we can calculate the required separation between the CPE and the noise protection contour. The distance at which the field strength of the undesired signal reaches 32 dBu is approximately 3.45 km, as seen in Figure 6.15. Adding 3.45 km to the DTV protection contour of 134.2 km gives a keep-out region of 137.6 km around the DTV transmitter. Now consider a CPE on the opposite side of the WRAN cell to the TV protection contour; it has higher EIRP in the direction of the DTV receiver and hence it is worth calculating the distance the CPE must be placed from the DTV receiver. Its EIRP is fixed at 36 dBm, which corresponds to a distance of 6.9 km from the DTV receiver. So the CPE on the "opposite" side of the base station that is more than 3.5 km away from the protection contour causes approximately the same interference. Typically the WRAN cell diameter is larger than 10 km and CPEs that are not at the edge of the cell use transmit power control, so even though they are somewhat closer

they transmit at a lower power. Hence, it is required to place the CPE at least 3.45 km from the DTV receiver so that it does not cause harmful interference.

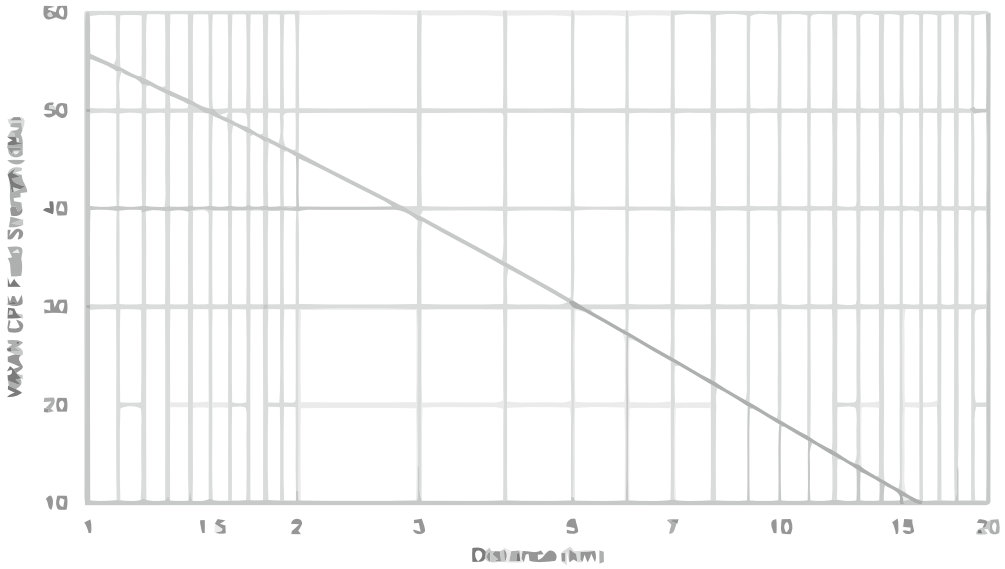


Fig. 6.15 WRAN CPE field strength.

Chapter 7

Cognitive Radio Network Security

7.1 Introduction

The IEEE 802.22 is an emerging standard for CR-based wireless regional area networks (WRANs). The IEEE 802.22 standard aims at using dynamic spectrum access (DSA) to allow the unused, licensed TV frequency spectrum to be used by unlicensed users on a non-interfering basis [58]. To protect the primary incumbent services, IEEE 802.22 devices (e.g., base station and consumer premise equipment) are required to perform periodic spectrum sensing and evacuate promptly upon the return of the licensed users [59].

Even though the primary user protection mechanisms have been proactively specified, neither the secondary-secondary interaction mechanisms nor the protection of secondary devices/networks have been specifically defined or addressed in IEEE 802.22 standard [60]. Hence, the IEEE 802.22 networks are vulnerable to denial-of-service (DOS) attacks, by which the attacker will prevent the secondary networks from using the spectrum band effectively or at all. Spectrum sharing, or coexistence, is an important attribute of CR networks. CR networks support two types of coexistence: *incumbent coexistence* (i.e., coexistence between primary and secondary networks) and *self-coexistence* (i.e., coexistence between secondary networks).

Threats against 802.22's incumbent–coexistence mechanisms:

Primary-User Emulation (PUE): [61] A CR's ability to distinguish between primary-user signals and secondary-user signals , but it becomes especially difficult when the CRs operate in hostile environments. In a hostile environment, an attacker may modify the air interface of its own CR to mimic a primary-user signal's characteristics, thereby causing legitimate secondary users to erroneously identify the attacker as a primary user. We coin the term PUE attack to refer to this attack.

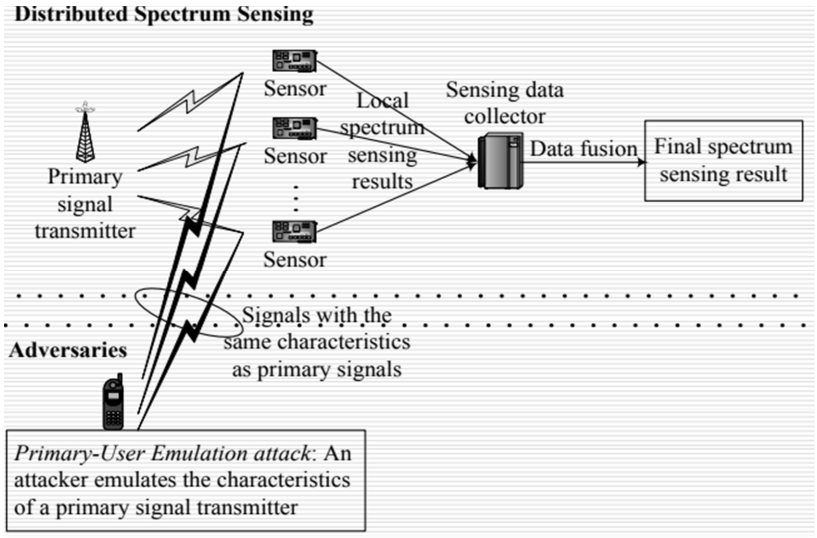


Fig. 7.1 Primary user emulation attack

There are alternative techniques for spectrum sensing, such as matched filter, Energy detector and Cyclostationary feature detection, but this techniques has problem that If a malicious secondary user transmits signals that emulate the characteristics of primary user signals, it will be identified as a primary user by the other secondary users so such detection techniques are still not robust enough to counter PUE attacks.

Classification of PUE Attacks

Selfish PUE attacks: In this attack, an attacker's objective is to maximize its own spectrum usage. When selfish PUE attackers detect a fallow spectrum band, they prevent other secondary users from competing for that band by transmitting signals that emulate the signal characteristics of primary-user signals.

Malicious PUE attacks: The objective of this attack is to obstruct the DSA process of legitimate secondary users; that is, prevent legitimate secondary users from detecting and using fallow licensed spectrum bands, causing denial of service. Unlike a selfish attacker, a malicious attacker does not necessarily use fallow spectrum bands for its own communication purposes. It is quite possible for an attacker to obstruct the DSA process. An attacker can effectively limit the legitimate secondary users from identifying and using fallow spectrum bands. We use a transmitter verification scheme for detecting PUE attacks.

Transmitter verification scheme Transmitter verification for spectrum sensing is composed of three processes:

1. Verification of signal characteristics.

2. Measurement of received signal energy level.

3. Localization of the signal source.

If the location of the source matches the location of a primary user, the source is considered to be a primary user. Otherwise it is considered to be an attacker trying to emulate a primary User.

Two approaches have been suggested to determine the location of the transmitting source: Distance Ratio Test (DRT) which is based on received signal strength measurements and Distance Difference Test (DDT) which is based on signal phase difference. Both DRT and DDT can be fooled if the attacker is transmitting from the Vicinity (near area) of the TV tower (location of primary user). A solution to this problem is presented by combining localization of transmitters with signal energy level detection.

We state some of the assumptions that form the foundation of the scheme: *The primary user* is network composed of TV signal transmitters (i.e., TV broadcast towers) and receivers. *The secondary users* is equipped with a hand-held CR device, form a mobile ad hoc network, Each CR is assumed to have self-localization capability and a maximum transmission output power that is within the range from a few hundred milliwatts to a few watts—this typically corresponds to a transmission range of a few hundred meters. An attacker, equipped with a CR, is capable of changing its modulation mode, frequency, and transmission output power. The primary signal transmitters are TV broadcast towers placed at fixed locations. Hence, if a signal source's estimated location deviates from the known location of the TV towers and the signal characteristics resemble those of primary-user signals, then it is likely that the signal source is launching a PUE attack.

An attacker, however, can attempt to circumvent this location-based detection approach by transmitting in the vicinity of one of the TV towers. In this case, the signal's energy level in combination with the signal source's location is used to detect PUE attacks. It would be infeasible for an attacker to mimic both the primary-user signal's transmission location and energy level since the transmission power of the attacker's CR is several orders of magnitude smaller than that of a typical TV tower. Once an instance of a PUE attack has been detected, the estimated signal location can be further used 0to pinpoint the attacker.

Existing Localization Techniques According to Fig. 7.2, the primary signal transmitter localization problem (which is referred to as the PST localization problem. The conventional localization approaches are based on one or several of the following techniques: time of arrival (TOA), time difference of arrival (TDOA), angle of arrival (AOA), and resolved signal strength (RSS).

TDOA is a passive localization technique that utilizes the difference between the arrival times of pulses transmitted by a transmitter but does not rely on any knowledge of the pulse

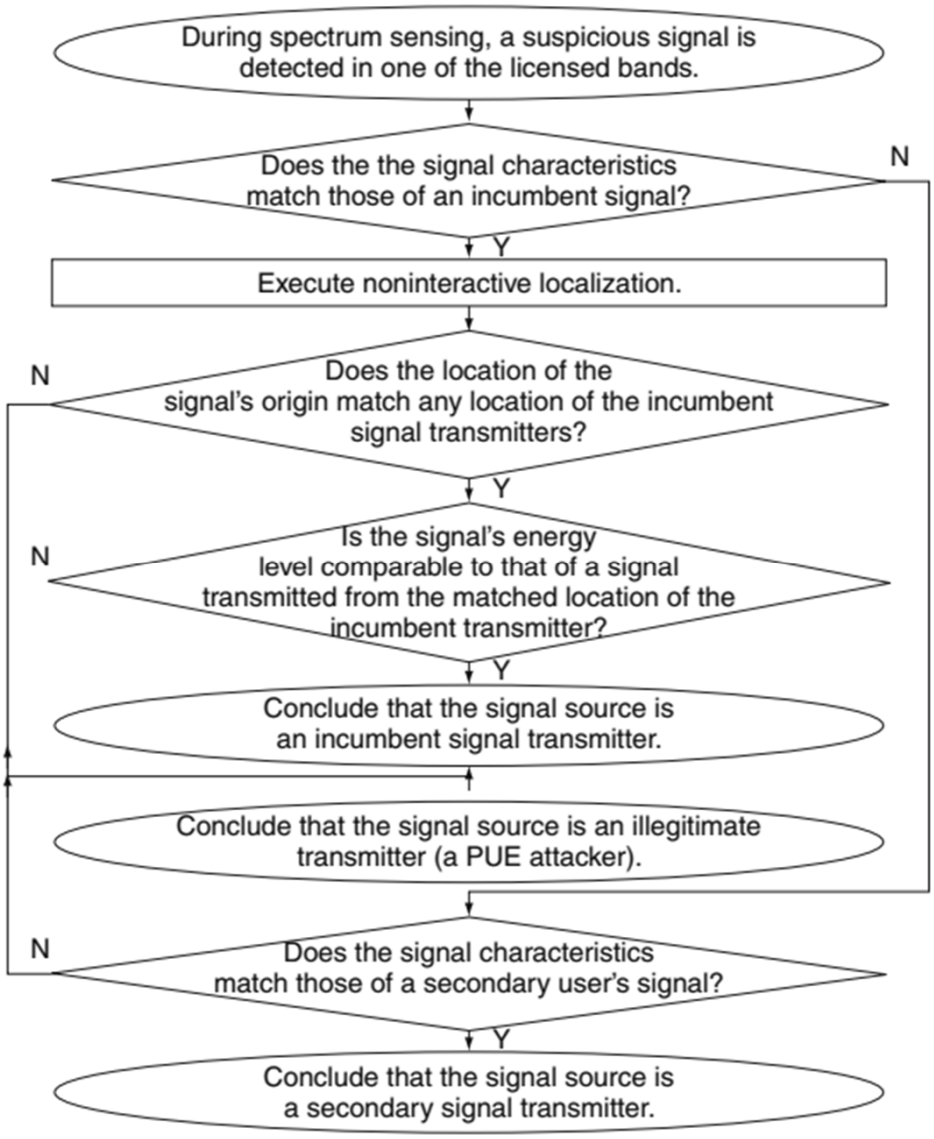


Fig. 7.2 A flowchart of the transmitter verification scheme.

transmission time. The technique measures the time differences at multiple receivers with known locations and subsequently computes a location estimate [62].

AOA technique a receiver measures the angel of arrival from two or more transmitters. If the locations of the transmitters are known, the receiver can calculate its own location using triangulation [63] Using the same principle, angle of arrival information to multiple receivers can be used to determine the transmitter's location.

RSS-based localization techniques arise from the strong correlation between the distance of a wireless link and RSS [64]. Specifically, given a transmitter receiver pair, RSS can be modeled as a function of transmitted power and transmitter-receiver distance. Therefore, if a correct model is used and multiple observers take RSS measurements from a transmitter, then the transmitter location can be estimated using the model. For example, one of the techniques for radio location in Wireless E911 [65] is to use "location signatures". The location signature scheme stores and matches multipath patterns (fingerprints) that mobile phone signals are known to exhibit at different locations in each cell.

Byzantine failure problem Due to Byzantine failures, such as device malfunction or

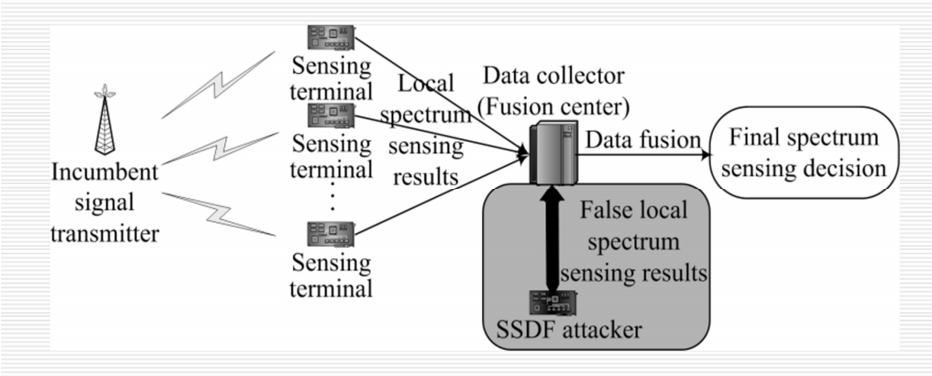


Fig. 7.3 Byzantine failures.

attacks, a neighboring secondary user may send wrong sensing information. This might severely obstruct correct spectrum sensing. In an SSDF attack, a malicious secondary user intentionally sends falsified local spectrum sensing reports to the data collector in an attempt to cause the data collector to make incorrect spectrum sensing decisions. Either case could cause interference to incumbents and result in underutilization of fallow licensed spectrum.

Signal fading can result in the "hidden node problem." The hidden node problem in the context of CR networks can be described as an instance in which a secondary user in a CR network is within the protection region 3 (the area in which secondaries cannot operate while the incumbent is transmitting so that no interference to the incumbent introduced) of an operating incumbent but fails to detect the existence of the incumbent. It is also possible

for a secondary user to falsely detect an incumbent because of noise or interference in the wireless environment.

Solution:

Distributed Spectrum Sensing (DSS) Each secondary acts as a sensing terminal that conducts local spectrum sensing. The local results are reported to a data collector (or "fusion center") that executes data fusion and determines the final spectrum sensing result. The application of DSS requires that the distance between any two sensing terminals is small relative to their respective distances from an incumbent transmitter.

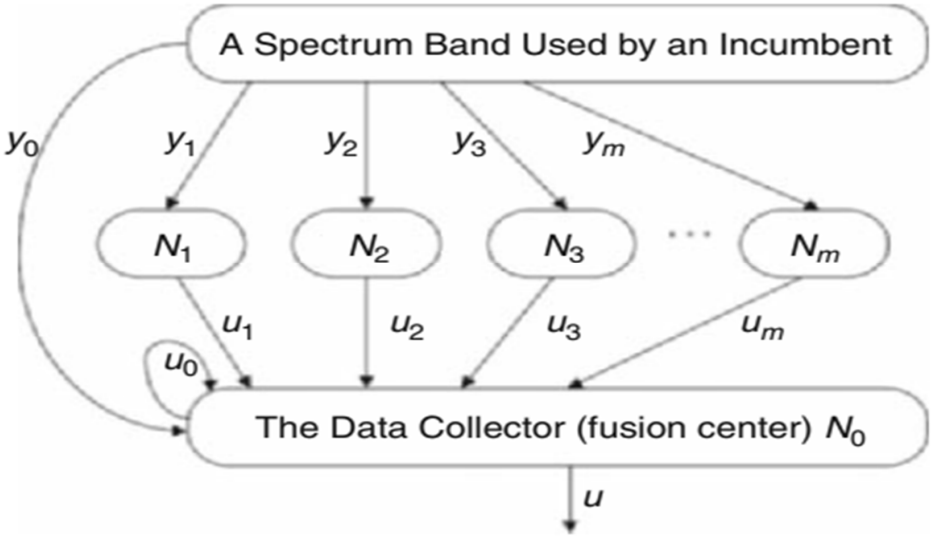


Fig. 7.4 Modeling DSS into a parallel fusion network.

In figure **??**, N_0 is a data collector, N_i is N_0's neighboring sensing Terminal, and u is the final sensing decision, which is a binary variable—1 denotes the presence of an incumbent signal, and 0 denotes its absence.

Decision fusion Requires the data collector to sum up all the values of u_i . A threshold value that is no less than 1 and no greater than $m+1$. (m is the number of neighbor sensing terminals). If the sum of u_i values is greater than or equal to the threshold then the final sensing decision is "occupied"; that is, $u = 1$ and H_1 is accepted; otherwise , the band is determined to be "fallow"; that is, $u = 0$ and H_0 is accepted.

Bayesian detection Requires the knowledge of a priori probabilities of the ui values when u is 0 or 1; that is, $P(u_i \mid H_0)$ and $P(u_i \mid H_1)$. It also requires the knowledge of a priori probabilities of u; that is, $P_0 = P[u = 0]$ and $P_1 = P[u = 1]$, respectively. There are four possible cases. In two cases the sensing decisions are correct, while in the other two cases the decisions are incorrect. The two incorrect decisions are referred to as misdetection ($u = 0$ when the band is occupied) and false alarm ($u = 1$ when the band is fallow), respectively.

The two correct decisions (i.e., $u = 0$ when the band is fallow and $u = 1$ when the band is occupied).

The DSS approach is vulnerable to a number of security threats. In particular, Byzantine failure is a major threat to the data fusion process. Results in one or more sensing terminals sending false local spectrum sensing reports to a data collector, causing the data collector to make a wrong spectrum sensing decision.

7.2 Security Vulnerabilities in IEEE 802.22

IEEE 802.22 [59] is the first wireless access standard based on cognitive radio technology. An 802.22 cell is a single-hop, pointto-multipoint wireless network composed of a base station and several consumer premise equipment. The BS manages the CPE within its cell and controls medium access via cognitive multiple-access control (CMAC).

The IEEE 802.22 standard mandates that CPE performs distributed spectrum sensing under the control of the BS. In this cooperative spectrum sensing approach, each CPE executes spectrum sensing on its own and sends its "local" spectrum sensing report to the BS, which then makes a final spectrum sensing decision. The presence of Part 74 devices is much more difficult to detect than TV broadcast transmitters, due to their low transmission power. To protect Part 74 communications, 802.22 prescribes two classes of solutions: class A and class B. Information gathered from regular CPE and class B CPE is used by the BS to identify fallow spectrum bands that are free of incumbent signals.

In IEEE 802.22, self-coexistence is an important problem and the standard prescribes several mechanisms for addressing it. There are two main technical challenges in self-coexistence: (1) minimizing the self-interference between overlapping cells and (2) satisfying the quality of service of the cells' admitted service workloads in a dynamic spectrum access environment. The 802.22 CMAC addresses self-coexistence using the inter-BS dynamic resource sharing mechanisms.

7.2.1 The 802.22 Air Interface

Various aspects of 802.22's air interface relevant to coexistence:

PHY Layer Support for Incumbent Coexistence

The 802.22 entities perform spectrum sensing to identify fallow licensed bands free from incumbent signals. The standard describes a twostage spectrum sensing approach: fast sensing and fine sensing. The fast sensing stage is executed before the fine sensing stage, and it typically uses a quick and simple detection technique such as energy detection. The

measurements from the fast sensing stage are used to determine the need and the duration of the subsequent fine sensing stage. The accuracy of a sensing technique is dependent on various environmental factors, such as the signal-to-interference ratio (SIR). Using the local spectrum sensing results, the BS determines and adjusts various PHY layer parameters such as channel bandwidth and modulation/encoding rate.

Cognitive Medium-Access Control Layer

The MAC protocol data unit (MPDU) is the smallest unit of transmission/reception in the CMAC. It comprises the MAC header, the MAC payloads, and the CRC (cyclic redundancy checking) field. There are two types of MPDUs, distinguished by their respective MAC headers:

- **General MAC header.** This header is used for intracell general MPDUs. It is used in general MPDUs that contain either higher-layer data traffic or management messages in their payload.
- **Beacon MAC header.** This header is used for intercell beacons. An intercell beacon only carries beacon information elements (IEs) in its payload.

In IEEE 802.22, BSs and CPEs exchange intercell control messages using intercell beacons. Intercell beacons play a vital role in incumbent coexistence and self-coexistence mechanisms. Two types of intercell beacons are defined in the standard:

- **BS beacons.** These beacons are used to provide information about the BS's traffic schedule, the current operation channel of the cell, and the like.
- **CPE beacons.** These beacons are used to provide information about a CPE's current cell of attachment as well as information on the traffic flows between the CPE and its BS.

Intercell Synchronization To facilitate incumbent signal detection, a BS periodically schedules a quiet period (QP). IEEE 802.22 recommends that neighboring BSs, if possible, synchronize their QPs to improve the reliability of incumbent signal detection. During these QPs, all network traffic is suspended, and 802.22 entities sense the channel for incumbent signals.

Suppose two overlapping cells, with two base stations, BS_1 and BS_2, need to synchronize their transmissions. For every intercell beacon received from BS_1, BS_2 records the frame offset that indicates when it was received. Accuracy of this reception offset [1] is critical for

[1] The reception offset indicates the offset (in units of slot duration) relative to the start of the first slot of the frame where the beacon was received.

successful synchronization. The transmission offset[2] is indicated in the beacon sent by BS_1. Figure **??** depicts the relationship between the transmission offset and the reception offset. After receiving BS_1's beacon, BS_2 attempts to synchronize with BS_1 by sliding its frames using the following *convergence rule*:

- If (FDC - O_{tx} + $O_{rx} \leq$ [FDC/2]), slide frames right by (FDC - O_{tx} + O_{rx});
- Otherwise, slide frames left by (O_{tx} - O_{rx}),

where O_{tx} is the transmission offset, O_{rx} is the reception offset, and FDC is the frame duration code (i.e., time duration of a frame).

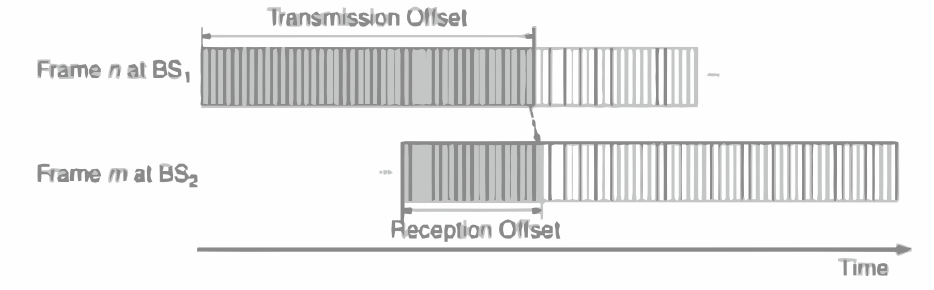


Fig. 7.5 Synchronization of overlapping BSs.

Inter-BS Dynamic Resource Sharing

When the current channel condition is insufficient to support the required QoS of its workload, a BS in need of spectrum initiates an inter-BS dynamic resource sharing process, so that better channels or more channels can be acquired from neighboring cells. The 802.22 prescribes two types of inter-BS dynamic resource sharing mechanisms: *nonexclusive* spectrum sharing and *exclusive* spectrum sharing.

After selecting a *target channel*, the BS in need of spectrum has to determine whether nonexclusive sharing of the selected channel is feasible using the following criterion: nonexclusive spectrum sharing is feasible as long as the maximum achievable SIR on the selected channel is higher than the required SIR threshold of the network's supported services. If nonexclusive sharing is feasible, the BS schedules data transmissions on the selected channel with appropriate transmission power control settings. Transmission power control is needed to minimize interference to cochannel neighboring 802.22 systems.

Protection of Part 74 Devices

Part 74 devices are much harder to detect than TV broadcast transmitters due to their

[2]The transmission offset indicates the offset (in units of slots) relative to the start of the first slot of the frame where the beacon is transmitted.

significantly lower transmission power. The current 802.22.1 task group is considering options for the protection of Part 74 devices. Two classes of solutions, class A and class B, have been identified. In class A, a separate beacon device is deployed to transmit short wireless microphone beacon (WMB) messages to notify collocated 802.22 systems about the presence of cochannel wireless microphone operations. In class B, the 802.22 system supports a special type of CPE that has specific capabilities to inform collocated 802.22 systems about wireless microphone operations. The 802.22 draft standard states that a single approach is not the best solution.

7.2.2 An Overview of the IEEE 802.22 Security Sublayer

The security sublayer has two components: an encapsulation protocol and a privacy key management (PKM) protocol. The encapsulation protocol defines a set of supported cryptographic suites (i.e., pairings of data encryption and authentication algorithms) and the rules for applying those algorithms to an MPDU payload. The PKM protocol ensures the secure distribution of keying material from the BS to the CPE. The security sublayer protects only intracell CMAC management messages and not intercell beacons. Figure 7.7 illustrates the 802.22 air interface's functionalities and the ones protected by the security sublayer.

In an opportunistic spectrum sharing environment, it is necessary to ensure the availability of spectrum for the incumbent users as well as the secondary (WRAN) users. In the context of opportunistic spectrum sharing, a denial-of-service (DoS) attack involves the insertion of forged management messages by rogue terminals to create havoc for the spectrum sensing or spectrum allocation processes. The 802.22 security sublayer provides protection against this type of attack in two ways: (1) PKMv2 is used to provide mutual authentication between a BS and a CPE, thus preventing a rogue terminal from masquerading as a legitimate terminal, and (2) message authentication codes are used to protect the authenticity and integrity of critical management messages exchanged within an 802.22 cell.

In an incumbent replay attack [66], an adversary captures and replaysthe local sensing reports (which is one of many types of intracell management messages defined in 802.22) sent by CPE to their BS. This may cause the BS to make incorrect spectrum sensing decisions.

7.2.3 Security Vulnerabilities in Coexistence Mechanisms

We describe two attacks—one disrupts the intercell spectrum contention process and the other impedes intercell synchronization. In both attacks, the adversary forges intercell beacons to achieve its attack objective. We coin the term *beacon falsification* attack to refer to such an attack. **Exploiting Intercell Spectrum Contention**

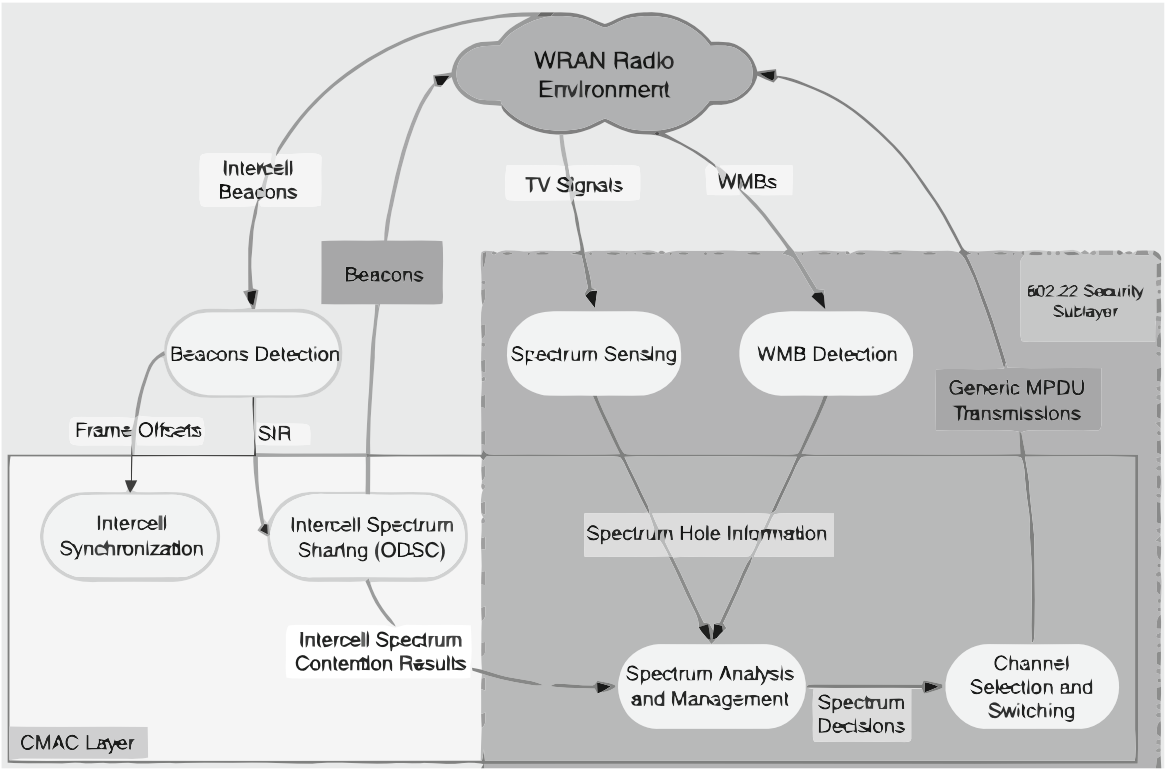


Fig. 7.6 The 802.22 air interface's functionalities and the ones protected by the security sublayer.

A terminal under the control of an adversary first selects the operation channel of a WRAN cell (i.e., "victim cell") as the target channel by eavesdropping on the BS beacons transmitted by the victim cell's BS. Then the attacker's terminal sends spurious contention requests via forged intercell beacons to the victim cell. This triggers the victim cell to participate in an intercell spectrum contention process via the ODSC protocol. To increase the probability of winning the target channel, the malicious terminal may arbitrarily select a very large CCN value. If the victim cell loses the contention, then it vacates the current operation channel (i.e., target channel) and switches to another channel.

7.3 Security Threats to the Radio Software

The programmability of SDR and CR devices is made possible by the signal processing capabilities of the radio software. However, the programmability of such devices raises serious security concerns. Without proper security measures to protect the radio software, the trustworthiness of an entire CR network can be compromised by the insecurity of the software.

Radio software for a CR has unique properties that distinguish it from conventional software. Because of the intrinsic operating characteristics of CRs, software running on them is likely to have the following attributes:

- **Software Portability and Generic Datapath.** The design methodology of existing software-defined radio architectures (e.g., GNU Radio) suggest that software portability will likely be a primary requirement that drives the hardware and software architectures of most SDR/CR systems. A design approach that aims to maximize software portability leans toward the use of a generic datapath rather than a specialized one customized for a specific application. Many in the SDR industry predict that the importance of portability will lead to the adoption of generic datapaths in most software radios. The importance of portability suggests that security schemes that require support from specific hardware, operating system, or other parts of the computing system may have limited utility.

- **Modular Software Architecture.** Such an architecture naturally promotes the use of modular software. The modular architecture of radio software needs to be considered when designing a security scheme to protect such software.

- **Real-Time Requirements.** Radio systems have very stringent real-time requirements. One way of satisfying these requirements is to tightly control the timing of software execution. However, this approach limits the radio software to platforms that have very

predictable execution rates, and consequently this requirement reduces software portability. To overcome this problem, some existing SDR systems relax the requirement of a predictable execution rate by significantly increasing the buffering carried out at the system input and output. In such an approach, real-time requirements are satisfied as long as the processor is fast enough for the signal processing code's average processing rate to be faster than the input/output rate. Satisfying real-time requirements while maintaining portability and platform flexibility is a challenging task.

Without proper software protection mechanisms in place, CRs are vulnerable to a host of security threats targeting the radio software.

- Execution of malicious code: illegal modification of radio software components, resulting in unauthorized changes in signal or protocol parameters.
- Removal of software-based authentication or access control functions.
- Disruption of radio software reconfiguration or obstruction of software management and version control.
- Reverse engineering or pirating of downloaded software components, resulting in intellectual property loss.

Most of these threats can be attributed to one of the following security problems: security vulnerabilities in the software download process, lack of protection against Internet protocol (IP) theft and software pirating, and vulnerability to unauthorized software tampering. The threat posed by the third problem is especially serious because adversaries may attempt to manipulate radio software to gain operational advantages (e.g., transmit at power higher than the authorized limit) or launch attacks against primary-user networks. The prospect of malicious users making unauthorized changes to a CR's operating characteristics is a major concern for regulators and developers.

Chapter 8

Public Safety and Cognitive Radio

8.1 Introduction

At a first glance, it may seem that an emergency situation is not something in which one wants to experiment with such a new technology as cognitive radio. There are, however, a number of arguments that justify the application of cognitive radio in this field. One of the reasons behind this is that it is not sensible from an economic perspective to permanently reserve the large bandwidths required for such applications. One of the most difficult aspects of cognitive radio, in general, is that it is not allowed to cause interference to any primary user. This problem also applies to the public safety field but to a lesser extent. When a large-scale emergency occurs, the importance of the situation makes the rescue workers, at least in principle, primary users of the spectrum.

8.1.1 Requirements

The next-generation communication system for public safety will have very extensive requirements. These requirements are studied and specified by commissions such as SAFECOM in the United States and Project MESA [67] in Europe. Most of these requirements deal with the higher layers in the network protocol stack. In this chapter we restrict ourselves to the physical layer.

Communication Structure

A public safety wireless network consists of a backbone network, base stations, and handsets. The backbone network is used for inter–base station communication. In case the entire public safety network is down, emergency workers should still have the option for direct communication. In a rescue situation, the network consists of different types of network nodes, such as emergency workers, vehicles, helicopters, airplanes, and robots.

In a critical situation, rescue workers lack the time to dial a number before they can communicate. A typical system will set up a call within 350 ms.

Reliability

Robustness is the ability of a system to avoid total failure despite unforeseen conditions or partial damage. A public safety communication system should always be available, especially during large disasters. The network should have guaranteed coverage in the whole service area, including special coverage locations like tunnels. All base stations have power supply backup batteries, so that the system remains operational for about 4 to 5 h during a power failure.

Coverage in this area can be obtained by mobile base stations (on a truck) and by overdesigning the network, so other neighboring base stations can handle the communication needs. In Section 8.2.1 we describe that cellular networks are interference limited. A third solution is that handsets should be able to communicate directly with other handsets (without a base station). Robustness can be obtained by having at least two independent backbone connections to each base station. Security is the ability of a system to withstand malicious attacks. The communication should be secure against eavesdropping, spoofing, and jamming. It should also be able to block lost or stolen handsets from using the network. In addition, handsets should not contain information that can help unauthorized users access the network.

Broadband

Although voice will always be the primary mode of communication during an emergency, there is a huge demand for multimedia. The next-generation public safety communication equipment will provide advanced features, like sensors for biomedical and environmental signals.

Paging

In paging communication short, predetermined text messages are sent to mobile devices that are very important for public safety applications. The advantage of such predefined messages is that they convey a lot of meaning in very few data bits.

8.1.2 Commercial Wireless Communication Networks

If a disaster occurs, these networks have two important drawbacks. First, the network gets overloaded, as each person in the vicinity tries to communicate with his or her friends and family. As a result the communication network may collapse. The second reason is that, when a disaster occurs, a part of the infrastructure may be damaged. For instance, the power may be unavailable in the area of the disaster. For economic reasons, commercial networks have no backup for the power supply and hence the affected network is down. In addition, commercial networks lack coverage in rural areas where there are very few

customers. Moreover, they also lack coverage in special coverage locations like tunnels and metro stations.

Spectral Efficiency

With cognitive radio one of the goals is to use the spectrum more efficiently. To get insight in the economics of spectrum usage, a good starting point is the ShannonHartley theorem for the capacity of an additive white Gaussian noise (AWGN) channel,

$$C = B.\log_2(1+SNR) \quad [b/s] \tag{8.1}$$

in which C is the channel capacity in bits per second, B the channel bandwidth in hertz,

$$SNR = \frac{P_{rx}}{N_0 B} \tag{8.2}$$

is the signal-to-noise ratio, with P_{rx} the received signal power in watts, and N_0 is the power spectral density of the white noise in watts per hertz. The noise in a radio link is caused by various sources. The most fundamental source of noise is thermal noise, which originates from all warm matter with a power of

$$S(f) = N_0 = kT \quad [W/Hz], \tag{8.3}$$

in which $k \approx 1.3806504 \times 10^{-23} J/K$ is the Boltzmann constant. For a temperature of $15.2^o C$ this gives a noise floor of about $-174 dBm/Hz$.

Based on this Shannon limit, we can identify two "regimes" of operation of a communication link (see Figure 8.1). First, if the SNR is good ($\approx 10dB$ and more), we have

$$C \approx B.log_2(SNR) \approx B.\frac{1}{3}SNR(dB). \tag{8.4}$$

In this regime the capacity depends linearly on the bandwidth but only logarithmically on the transmit power. Therefore, this regime is called bandwidth limited or spectrally efficient, since most capacity improvement can be gained by increasing the bandwidth. If we choose to divide the bandwidth by a factor N and maintain capacity by increasing the transmit power, we see that the required power grows exponentially with N.

8.1.3 Benefits of Cognitive Radio

The general meaning of a cognitive radio is a smart device that does all kinds of useful things for its owner, based on sensory input and machine learning. In a more specific meaning, it is a radio that can opportunistically use white space in licensed bands without causing

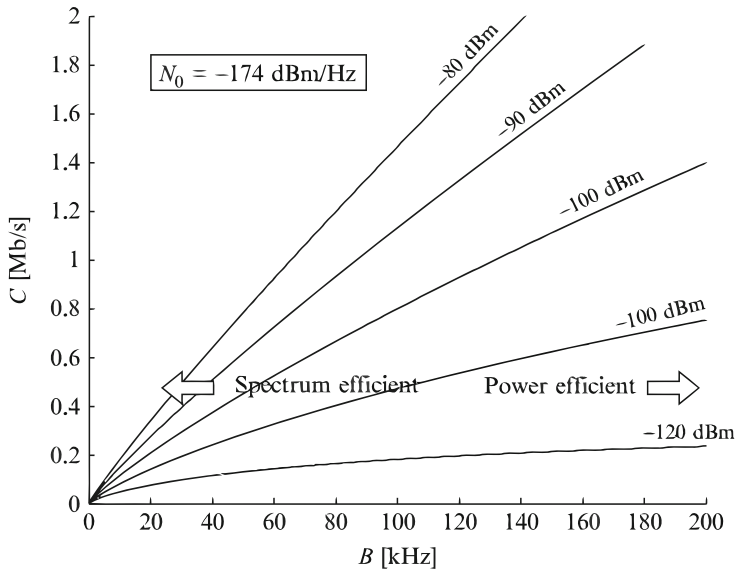


Fig. 8.1 Channel capacity as function of channel bandwidth for various received signal power levels.

interference. Due to the special requirements of public safety networks, there are several benefits of cognitive radio technology.

Improved Communication Structure

- **Communication with other networks** A cognitive radio with support for military standards and other public safety standards would solve this problem.
- **Backwards compatibility** Cognitive radio allows an upgrade of the existing equipment to this new release without replacing the hardware.
- **Introduction of new services** New services could be enabled more easily by cognitive radio, as it can adjust its parameters according to the requirements of the new service. It does not have limitations set by existing standards.

Improved Reliability

A cognitive radio always tries to minimize interference to other networks by changing its frequency if other signals are present. This feature automatically makes a cognitive radio more resilient to jamming.

Enabling Broadband

In case of an emergency, public safety networks are heavily used, and there is demand for more capacity. Implementing this capacity beforehand in the whole network would be very costly. A different approach would be to use cognitive radio to sense for empty frequency bands (white space) and use it as a secondary user to set up an auxiliary communication

network. The relatively large bandwidths required for broadband communication could be provided by secondary spectrum usage.

8.2 Standards for Public Safety Communication

Several communication standards have been developed for public safety applications. The first generation of standards was based on analog modulation (FM/AM) and used an optional speech scrambler to prevent eavesdropping. By the end of the last century, second-generation standards emerged based on digital modulation and trunking. These are now used in most countries. There are three second-generation public safety communication standards: P25 (APCO Project 25), TETRAPOL, and TETRA. APCO Project 25 systems are used by the federal, state/province, and local public safety agencies in North America. This means that P25 handsets have support for an analog and digital communication mode. More information about P25 can be found in [68]. TETRAPOL [69] was one of the first digital public safety standards, developed in France. By 1988 it was used by the French Gendarmerie Nationale. The terrestrial trunked mobile radio (TETRA) [70] communication network was developed almost ten years later and is now used in most European and other countries.

8.2.1 TETRA

TETRA was formerly known as trans-European trunked radio and standardized by ETSI in 1995. TETRA was specifically designed for use by government agencies, emergency services (police forces, fire departments, ambulance), rail transportation staff, transport services, and the military.

Handhelds can communicate in direct mode operation (DMO), in which they work similar to a walkie-talkie, or in trunked radio mode operation (TMO), in which the TETRA base station infrastructure is used. The DMO allows direct communications in situations where network coverage has been lost. In addition to voice services, the TETRA system supports several types of data communication: status messages, short data services, packet data, and circuit-switched data communication. TETRA uses time division multiple access (TDMA) with four user channels on one radio carrier and 25 kHz spacing between carriers. Both point-to-point and point-to-multipoint transfer can be used. Digital data transmission is also included in the standard though at a low data rate. All voice and data traffic is protected by encryption, so that it is practically impossible to eavesdrop or spoof the communication. Figure 8.2 summarizes the air interface parameters.

Parameter	Value
Frequency Range	150 to 900 MHz
Channel Bandwidth	25 KHz
Modulation	$\pi/4$ QPSK
Bits per symbol	2
Transmit filter	Root Nyquist with 0.35 roll-off
Symbol rate	18,000 symbol/s
Raw data rate	36 kb/s
Spectral efficiency	1.44 b/s/Hz
Time slot duration	85/6 = 14.167 ms
TDMA frame	4 time slots = 56.656 ms
Bit rate per channel	36 kb/s per 4 slots = 9 kb/s
Voice codec	ACELP
Handheld rx sensitivity	-104 dBm
Vehicle rx sensitivity	-107 dBm
Mobile tx power classes	1 W, 3 W, 10 W, 30 W

Fig. 8.2 Air Interface Parameters of TETRA.

Trunking

For no call to be lost on a communication system even in a worst-case scenario requires an enormous amount of capacity. Moreover, most of this capacity remains unused most of the time. Because such an approach is highly uneconomical, it is almost never used anymore. Instead, practical systems are designed for an average load with some margin for peak loads. The average load, or traffic intensity, of a system is defined by

$$A = \frac{\lambda}{\mu} \quad \text{[Erlang]}, \tag{8.5}$$

in which λ calls/sec is the average arrival rate of calls, usually measured during a busy period, and μ calls/sec is the average service rate. The unit of average load is named after A. K. Erlang, the originator of traffic engineering and queueing theory.

In a trunking system, all channels are kept in a pool, from which they are dynamically assigned to users. A user can request a channel via a control channel. After the call is finished the channel is placed back in the pool. On average, enough free channels are available in the pool to handle all incoming requests. However, since the tail of the Poisson distribution extends to infinity, there is always a chance that a large numbers of calls are made simultaneously, so that the pool is exhausted. When that happens there are a number of scenarios. The simplest of them is that the call is just dropped and lost forever. The chance

that this happens is given by the Erlang-B equation:

$$\Pr\{\text{blocking}\} = B(A,N) = \frac{A^N/N!}{(\sum_{n=0}^{N} A^n/n!)} \tag{8.6}$$

Spatial Reuse Modern mobile radio communication networks are usually based on a cellular architecture. In a cellular system a large geographical area is partitioned into cells. Each cell has its own base station that works with a specific set of frequency channels.

Conceptually it is convenient to model the cell shape as a hexagon because of its nice geometrical properties. If R is the radius of a hexagon then its width is $W = \sqrt{3}R$ and its area is $A = 1.5\sqrt{3}R^2$. Cells are grouped in clusters of size K, and each cell in the cluster is given a different set of frequencies in such a way that neighboring cells have different frequencies. From the geometrical properties of the hexagonal cell shape, it is straightforward to derive that the number of cells in a cluster must be a number $K \in \{1,3,4,7,9,12,13,...\}$ for which $K = i2 + j2 + ij$ holds with i and j positive integers including 0. Furthermore, the distance between two clusters can be shown to be $D = \sqrt{3K}R$.

In a cellular system, the dominant noise contribution in the downlink is not from thermal noise but from interference from neighboring cells that use the same frequency. This interference is called cochannel interference (CCI). The system is called interference limited rather than noise limited. The worst-case CCI occurs if the mobile user is in a corner of a cell, because then it is at the largest distance from its base station. The mobile will receive most of its interference from the six nearest surrounding cells that work on the same frequency. The interference from these first-tier cells gives

$$SNR = \frac{P_{tx}.(R)^{-\gamma}}{\sum_{n=1}^{6} P_{tx}.(d_n^{-\gamma})} = [\sum_{n=1}^{6} (\frac{R}{d_n})^{\gamma}]^{-1} \tag{8.7}$$

in which γ is the path loss exponent and dn the exact distance from the corner of a cell to the nth interfering base station. If we approximate d_n by D this simplifies to

$$SNR \approx \frac{1}{6}(3K)^{\gamma/2} \tag{8.8}$$

From this we get the somewhat counterintuitive result that the SNR, and thus the capacity, is independent of the transmitted power and cell size, and it becomes better with a higher path loss. Furthermore, increasing the number of cells in a cluster increases the SNR but decreases the total system capacity. This is because each cell needs a unique channel, which cannot be used by the other cells in the cluster.

8.2.2 C2000

The public safety communication network in The Netherlands is called C2000. It consists of three components:

T2000

A TETRA-based network for voice and low-rate data communication. It uses the frequency band 380–385 MHz for uplink and 390–395 MHz for downlink communication. It uses both direct mode and trucked radio mode. For special coverage locations, like tunnels and stadiums.

P2000

Paging is a very important communication application in public safety, where short predetermined texts are transmitted and displayed on pager devices. For instance, they are used to alarm firefighters. C2000 uses a different network for paging. This network, P2000, is based on the FLEX[1] protocol in the 169.650 MHz band. TETRA has also support for paging, but the current outdoor coverage is too low for this application.

M2000

M2000 is a software system used in the public safety answering point (PSAP). A PSAP is a call center responsible for answering calls to an emergency telephone number for police, firefighting, and ambulance services. It facilitates the communication among the different PSAPs. PSAP is to act as an info/help desk in talk groups. The M2000 system facilitates these tasks. Finally, it is also used for network management and network planning. Once a network has been built, it is not finished. New residential areas are developed, new high-rise buildings are constructed that block the radio signal, and so forth. So, every year, several base stations have to be moved or added to the network. The C2000 network fulfills all important public safety requirements but lacks support for multimedia/broadband Internet communication. In the frequency band in which C2000 operates, the inflexible and fragmented licensing scheme made it difficult to find more static allocated spectrum. On the other hand, a huge amount of this spectrum always is temporarily unused. But traditional radio equipment lacks the technology to find this free spectrum, and there is not yet a legal system that allows ad hoc secondary usage.

[1] FLEX (Flexible Wide Area Paging Protocol) is Motorola's high speed one-way paging protocol FLEX can transmit tone, numeric, alphanumeric, and binary data

8.3 Another Applications for CR

8.3.1 The Firework Disaster in The Netherlands

On May 13, 2000, a large disaster took place in the city of Enschede, The Netherlands. On a nice warm Saturday afternoon, a crowd gathered to witness a small fire in their neighborhood, at what they thought was a paper recycling depot. Only the firemen and police knew that actually a fireworks storage was burning. What they did not know was that the safety regulations were violated, and much more and much heavier fireworks were stored than was allowed. After about 20 min the first big explosion occurred, followed shortly by a detonation that ruined the whole area. The result was that an area of 1 km^2 was destroyed (400 houses), 23 people were killed, and about 950 injured [71].

Even before the explosions, the central control post and PSAP were flooded with calls. Soon after the final explosion all communication systems collapsed because everyone started calling. Most of the calls over the GSM network involved people notifying their friends and family. Many calls over the public safety network were made by police officers who offered their help after they heard the explosion. However, the first responders that survived the explosion could not reach the control center, because the network was overloaded. Even hours after the explosion, communication remained difficult. For example, much time was wasted because experts could not get reliable information about the risks of explosion of an ammonia cylinder in the refrigeration system of the nearby Grolsch brewery, which also caught fire.

From May 13 until May 25 in total 141 ambulances and 15 helicopters (680 rescue workers), 7980 police officers, and 1675 firefighters were active [71] in the area of the disaster. From these numbers, we estimate that around 2500 rescue workers were active during May 13 in an area of several square kilometers. For normal tasks like house fires or surveillance, only up to 25 rescue workers would be working in this area. So, a large disaster increases the regional/local demand for a public safety communication network by a factor of approximately 100.

8.3.2 Bandwidth Requirements

In this section, we derive the spectral requirements in the case that a cognitive radio system would have been used during this disaster. In the previous section, we estimated that at maximum 2500 rescue workers were present at the disaster location. The primary disaster region was 1 km^2, but rescue workers are of course active in a larger area, so the extended disaster region would be 10 km^2. In this area, we estimate that 25 video streams of 256 kb/s

each (MPEG-4 streams) should be uploaded to the central command. Moreover, 25 photos of 1 Mb each are taken per second and should also be uploaded. In total, this results in a gross 31.4 Mb/s stream to the central command.

The cognitive radio network consists of vehicles and rescue workers. We assume that the vehicles can act as relay stations for the rescue workers to communicate with the central command. So, this is similar to normal 2G and 3G networks: The vehicles are base stations and the rescue workers are modeled as mobile terminals. Between the vehicles is a high-bandwidth backbone network for which cognitive radio also may be used.

The noise-limited communication occurs from rescue worker to vehicle and is therefore the most challenging task. For this type of communication, a frequency band has to be selected that has both good propagation conditions and small antennas suited to be mounted on handheld terminals. Frequency bands from 400 MHz to 1 GHz are appropriate bands. On the other hand, communication from the vehicle to central command is not limited by power and therefore higher-frequency bands can be selected, which are less optimal.

So, for rescue worker–to-vehicle communication, we have to derive how much spectrum is required. We assume that the average distance between the rescue worker and the vehicle is 100 m, a spectral efficiency of 1.3 b/s/Hz and an overhead of 50% (encryption, protocol overhead, etc.). Finally, we assume that 70% of the rescue workers can communicate directly with the vehicle and 30% require another rescue worker as relay. The core of the fireworks disaster is the 1 km^2 area, and in the other 9 km^2 surroundings, fewer rescue workers are active. So, the frequency demands are highest in the core of the disaster. If 50% of the 2500 workers are in this area, a total of $31.40.51.51.3 = 30.6MHz$ is needed. If the network can distinguish between primary users and its own network[2], frequencies can be reused more efficiently. A cluster radius D, which determines the number of times a frequency can be used in a square kilometer. In our case the cluster[3] area is 0.165 km2. So, frequencies can be reused six times in a square kilometer. This makes our spectral requirement in the core of the disaster 5 MHz. So, for this scenario a cognitive radio network has to find 5 MHz of empty space.

[2]This is possible as each vehicle knows which frequencies are used and the backbone network between vehicles can be used to distribute this information.

[3]We assume in our example that the number of cells in a clusters is seven, which is also used by GSM networks

8.3.3 Spectrum Organization

The C2000 system uses frequencies around 400 MHz. For easy integration of the cognitive radio add-on, it is beneficial to use frequencies near 400 MHz. In this section we review frequencies from 100 to 800 MHz.

Between the FM radio and the UHF television broadcasting band lies a region of the spectrum that is ideal for digital land mobile communication. Below the FM band, it becomes difficult to find a reasonable amount of bandwidth, and above the TV band, indoor coverage becomes difficult unless a lot of base stations are used. The FM band lies worldwide between 88 and 108 MHz, and the television band lies in Europe between 470 and 846 MHz. In the United States, the actual UHF television band starts at 512 MHz, but the numbering of the channels also starts at 470 MHz. Figure 8.3 shows a simplified overview of the band plan

Fig. 8.3 A simplified spectrum band plan of The Netherlands between the FM and TV broadcasting bands.

(allocation chart) in The Netherlands between the FM and TV band. Directly above the FM band one finds the aviation band, which in utilization measurements appears much quieter than the FM band. However, since the signals in this band are used to guide airplanes, the risk of interference is much too large, so that it is unsuitable for cognitive radio and every other type of spectrum sharing.

The band between 137 and 174 MHz is typically used by private mobile radio (PMR) networks used by private security personnel, public transportation, taxies, and the like. Typical equipment in use in this band are analog FM radios that use a 12.5 kHz raster without trunking. Because of this old-fashioned technology, there is a lot of white space in this band, which could be harvested by a cognitive radio.

The band between 174 and 240 MHz was traditionally used for television (VHF band III) but is now used for various purposes and for digital audio broadcasting (DAB). Directly after VHF band III, a large international NATO military band follows. The upper part of this band is shared with the C2000 system.

Between 400 and 470 MHz we find a second band for various applications. Typical usage is for public access mobile radio (PAMR). A PAMR network is a trunked radio system

operated by a telecom service provider that licenses capacity to its, usually professional, customers. Digital PAMR systems often use TETRA, and older networks often use the analog MPT1327 standard. Because PAMR is deployed only in the area of its customers, a lot of white space exists in this band, which could be harvested by a cognitive radio.

Above 470 MHz (up to 862 MHz), we find television band IV (UHF). The frequencies in this band are internationally coordinated. This means, in each area, a part of this spectrum is used by terrestrial TV. Neighboring areas use different frequencies to avoid interference.

At this moment there is a transition from analog terrestrial TV to digital terrestrial TV. Digital terrestrial TV uses lower transmission power and allows the use of multiple transmitters at the same frequency (single-frequency networks). Basically this means that the spectrum is used more efficiently. In this band a cognitive radio could also harvest a lot of spectrum. The reason for this is that outside the service area is a large surrounding area where this frequency cannot be used by another terrestrial TV transmission due to interference. So, cognitive radio can use these frequencies for local communication, and because this frequency band is used for broadcasting, its transmitters are fixed. So, a cognitive radio would only require its own GPS coordinates and a database of TV transmitters. Spectrum sensing is then only necessary for detecting wireless microphones.

8.3.4 Propagation Conditions

The propagation conditions determine how far a radio wave propagates. It seems beneficial to have good propagation conditions; that is, low path loss. However, for spatial reuse, it is beneficial to have a large path loss. A high path loss allows more spectrum reuse, and this means that the spectrum usage increases. Also, for cognitive radio, a high path loss is better, because it reduces the area in which interference can be caused. At UHF frequencies, ionospheric reflections play only a small role in the propagation of radio waves. Therefore, we can assume that the range of a signal is in principle limited to the horizon. The distance to the horizon is approximately given by

$$d \approx \sqrt{2krh} \tag{8.9}$$

in which k is a factor that corrects for the bending of radio frequency waves around the Earth, which is about 4/3, r is the radius of the Earth, which is about 6371 km, and h the sum of the heights of the transmit and receive antennas. So the signal of a 30 m–high base station cannot be detected beyond about 23 km, and the signal from a handheld cognitive radio cannot cause interference to another handheld radio much farther than 5 km.

8.3.5 White Space Assessment

To get permission from spectrum regulators to apply cognitive radio in a certain band, one has to convince them the spectrum in this band is structurally underutilized. This can be done with a spectrum survey. Figure 8.4 shows an overview spectrogram over a full day of a large portion of the UHF spectrum.

At first sight, there appears to be quite some white space in this spectrogram, especially between the TV channels. However, we must be careful not to draw premature conclusions. For example, TV channel 38 (channel 37 in the U.S. channel numbering), just above 600 MHz, is always empty because it is assigned worldwide to radio astronomy. Also the region around 900 MHz seems far less busy than the region around 950 MHz. However, both regions belong to the GSM system, and the uplink frequencies on 900 MHz are in fact paired with the downlink frequencies 45 MHz higher. The uplink channels appear much weaker because a cell phone uses its transmit power much more sparingly than a base station. But because of the symmetry in typical phone conversations, the occupancy in the uplink and downlink must be about equal. Figure 8.5(a) shows a close-up of Figure 16.4 in the 400 to

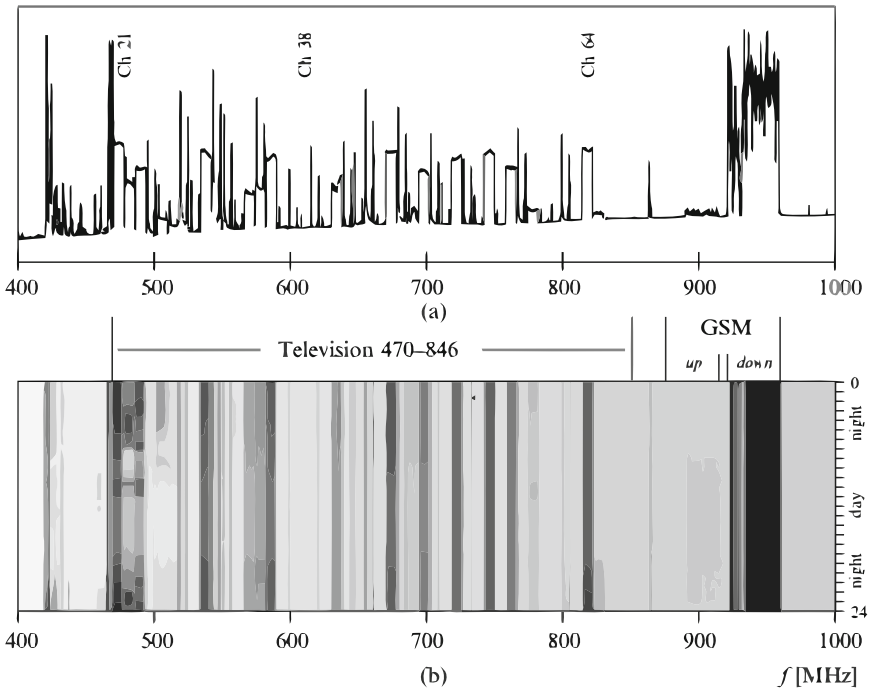


Fig. 8.4 Overview of the UHF spectrum in The Netherlands: (a) spectrum averaged over 24 h; (b) spectrogram over 24 h.

470 MHz band. Again, we see a remarkable amount of white space. Figure 16.5(b) shows the average over a full day, and Figures 8.5(c) and (d) show the maximum and minimum,

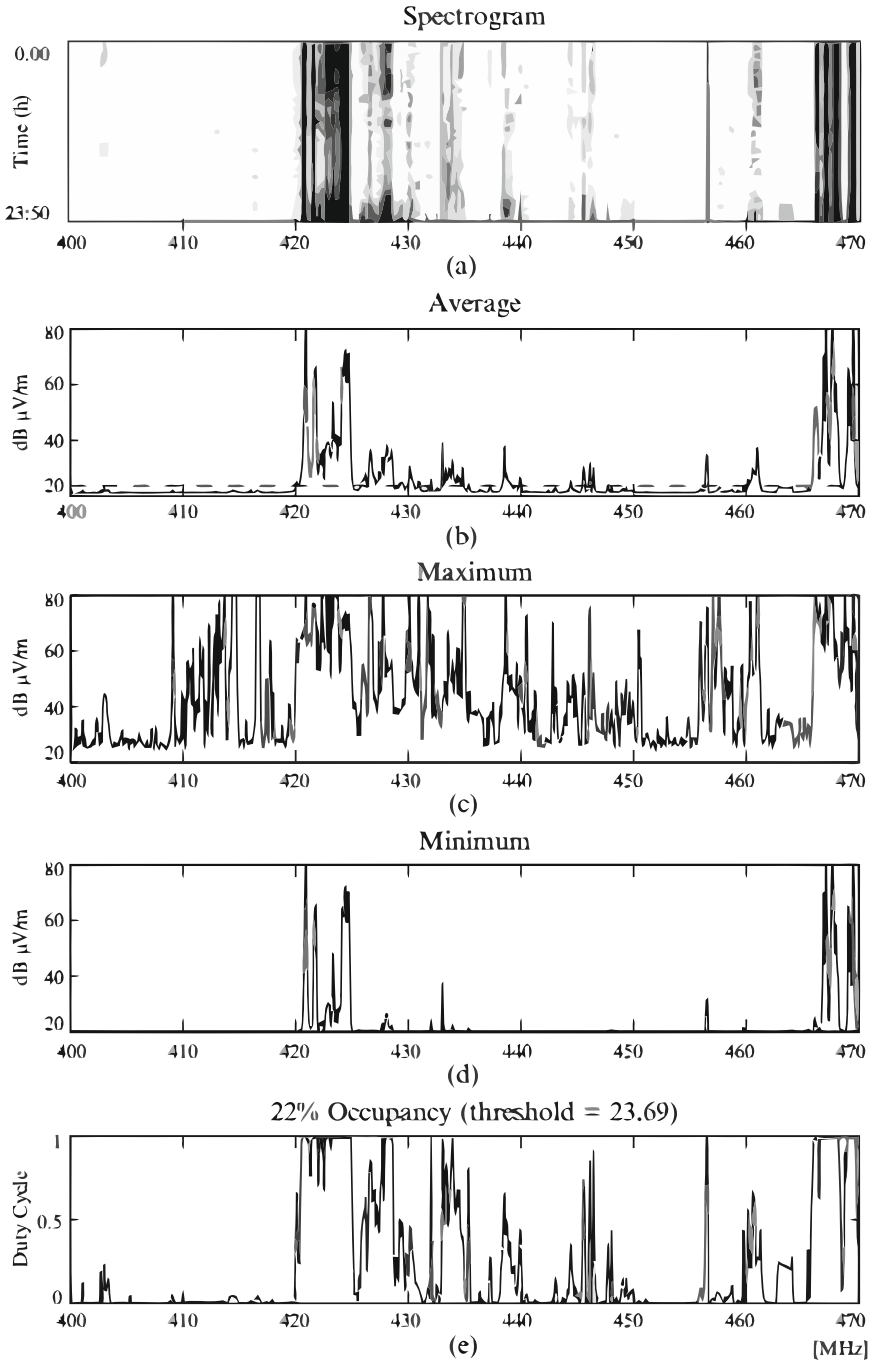


Fig. 8.5 Overview of the UHF spectrum in The Netherlands: close-up of the 400 to 470 MHz band.

respectively. The dashed line in Figure 8.5(b) indicates a threshold level, which was set 2 dB above the median power level. Figure 8.5(e) shows the duty cycle obtained by using this threshold. As we can see, a bandwidth of 5 MHz can be found as a contiguous block of spectrum. If our cognitive radio can use noncontiguous spectrum, much more bandwidth can be found.

Why Is the 400 MHz to 1 GHz Band Optimal for Mobile Communication?
Below the 240 MHz, the antenna is too large for mobile communication (i.e., larger than 30 cm). One well-known trick to make an antenna shorter is to roll it up, but this makes it too selective for only one narrow-frequency band. Frequencies from 240 to about 400 MHz are used by military communication and the frequency range from 1 to 1.4 GHz is in use by aeronautical radio navigation and radio astronomy. Therefore, these bands also are not suitable for cognitive radio.

8.3.6 System Spectral Efficiency

A wireless communication system should use the spectrum in an efficient manner. The system spectral efficiency can be defined as

$$\eta \approx \frac{R/B}{K} \quad [b/s/Hz/site], \tag{8.10}$$

in which R is the bit rate, B is the bandwidth, and K is the cluster size. Increasing K also decreases the system spectral efficiency. o, it is up to the system designer to choose these parameters in an optimal way. For example, the GSM system has a system efficiency of 0.17, and for the WiMAX (IEEE 802.16) system this value increased to 1.2, which makes the system spectral efficiency seven times higher compared to GSM.

8.3.7 Antijamming

An important requirement of public safety networks is resistance to jamming. Jamming is the intentional use of a strong radio signal, for instance by terrorists, in an attempt to disrupt communication.

In a spread-spectrum signal, the signal energy is spread over a much wider bandwidth than the original signal. Since jammers usually have narrowband signals, they disturb only a relatively small part of the signal. There are two well-known spreading techniques: direct-sequence spread spectrum (DSSS) and frequency hopping (FH). In DSSS the signal is multiplied with a pseudorandom spreading code, which is also known at the receiver. To make a signal practically unjammable, the signal bandwidth should be at least several tens of

megahertz. This means that, in our example, DSSS would be infeasible due to the limited amount of white space below the 1 GHz. In a frequency-hopping system, the transmitter hops after each packet to another frequency. The hopping sequence is known to both the transmitter and receiver. In a cognitive radio, we have an accurate map of available white space, so we could hop from white space to white space.

On the other hand, a cognitive radio network may be extra vulnerable to a "smart" jammer that follows its target signal. If such a smart jammer is used against a cognitive radio network, the network is required to continuously change its frequency. However, each frequency change must be coordinated with other nodes over a control channel and must be preceded by spectrum sensing. Therefore, the jamming of a single network node affects the whole network.

However, a truly cognitive radio may outsmart even such a smart jammer, because it understands the situation it is in. When a public safety network is clearly under attack, different policies may apply, and the primary-user avoidance scheme can be replaced by a jamming avoidance scheme. In such a jamming avoidance scheme, spread-spectrum techniques are very useful.

8.4 Chapter Summary

For the next-generation system of public safety communication, there is a huge demand for broadband applications. One reason for this is that pictures and video are very efficient in describing a situation. Another reason is that modern cell phones have broadband Internet access, and public safety personnel may start to rely on it. But during a large emergency, cell phones are likely to fail. Therefore, broadband Internet access is a requirement for the next-generation public safety communication system.

Chapter 9

Simulations of Cognitive Radio System by Using MATLAB and LabVIEW

9.1 Introduction

The basics of cognitive radio technology will allow us to create awareness among Electrical & Electronic Engineers regarding the scope and applications of this tremendous new technology. There are very few experimental simulation techniques present regarding cognitive radios, thus we intend to come out with a simpler and efficient simulating technique MATLAB.

9.2 MATLAB

9.2.1 Problem Finding: Spectrum Holes

In some locations or at some times of the day, 70 percent of the allocated spectrum may be sitting idle. The Federal Communications Commission of the United States Government (FCC) has recently recommended that significantly greater spectral efficiency could be realized by deploying wireless devices that can coexist with the licensed users.

9.2.2 Assigning Primary User to the Frequency Spectrum

We have designed our system to have 5 different frequency channels and each User is assigned a particular frequency band. Once we run our program it will ask to add a User and assign it a particular band in ascending order. Here in Fig. 9.3 we have not entered User 2, 3 & 5, thus their respective bands are still un-allocated. We can see them below in the power spectral density graph of our carrier signal.

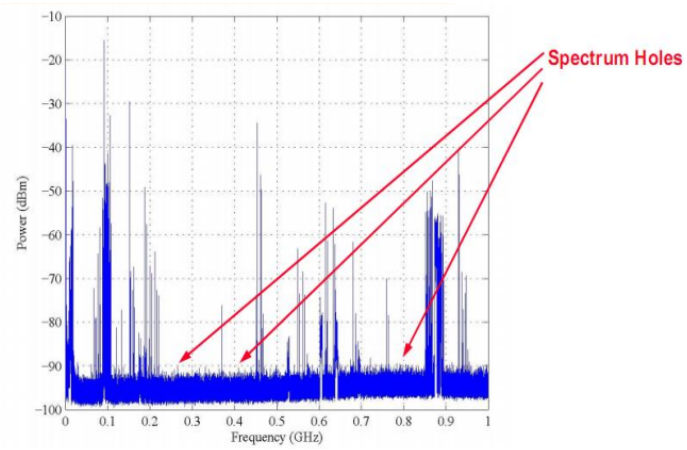


Fig. 9.1 Spectrum measurement across the 900 KHz - 1 GHz band.

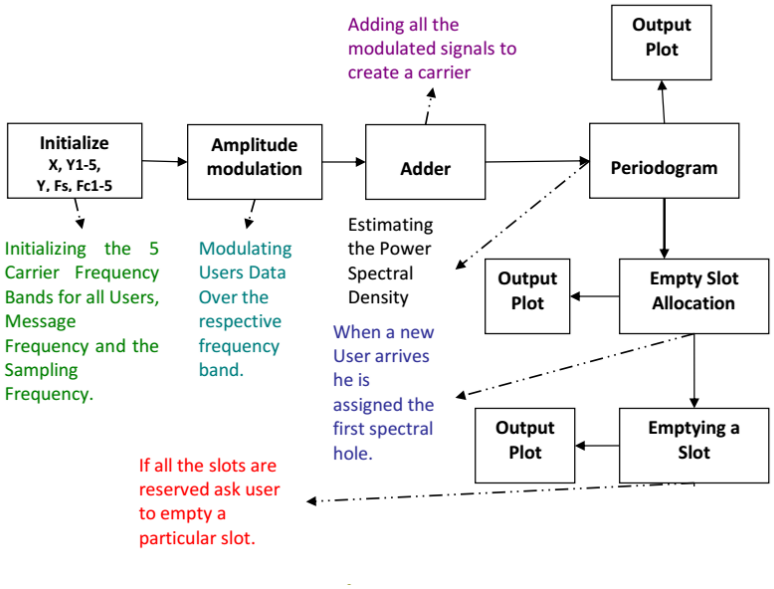


Fig. 9.2 Block diagram of simulation test-bed.

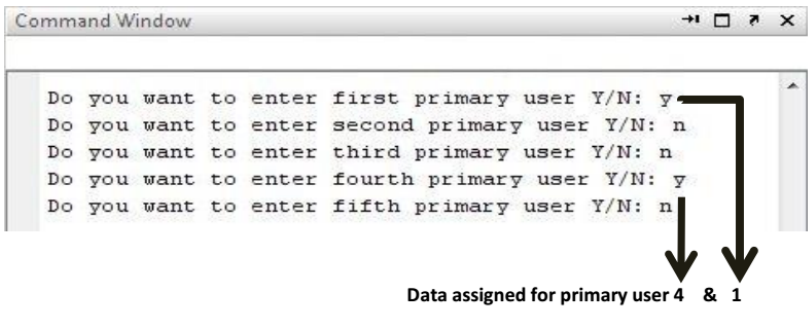


Fig. 9.3 Addition of primary user in the frequency spectrum in Command Window.

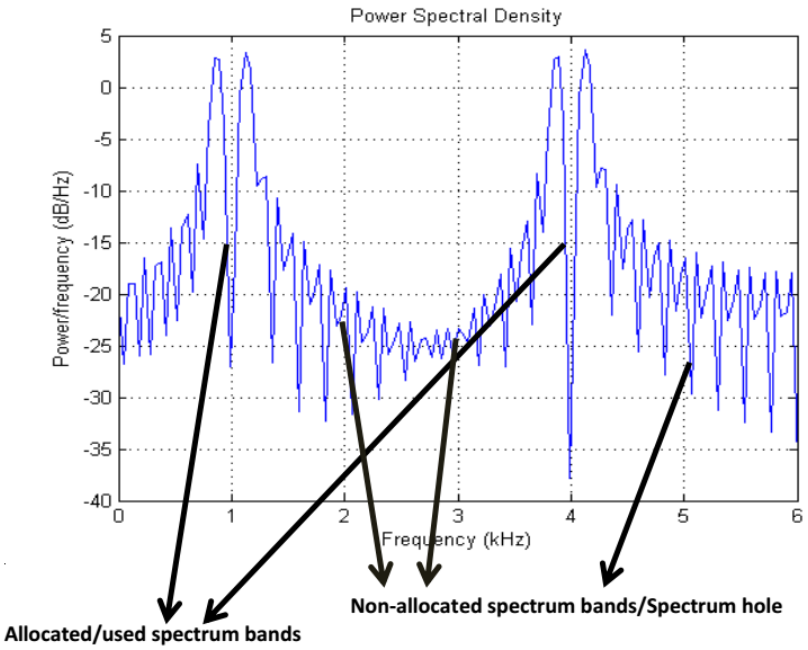


Fig. 9.4 Power spectral density curve.

9.2.3 Assigning new user to the Spectrum Holes

Now we are adding another User, the system will search the first available gap in the spectrum and automatically assign it to the new user. As the first available gap was after User-1 as User-2 was not sending any data so the band reserved for User-2 at start is now assigned to this new User.

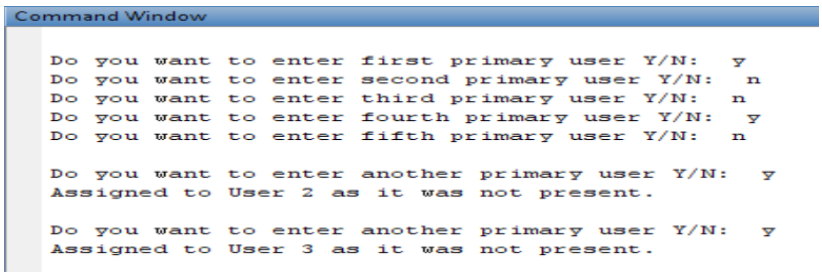


Fig. 9.5 Assigning new user to the Spectrum Holes in Command window.

Here we can see that the first spectral gap has been filled by assigning the new incoming User's data. The first spectral gap belonged was that of User-2.

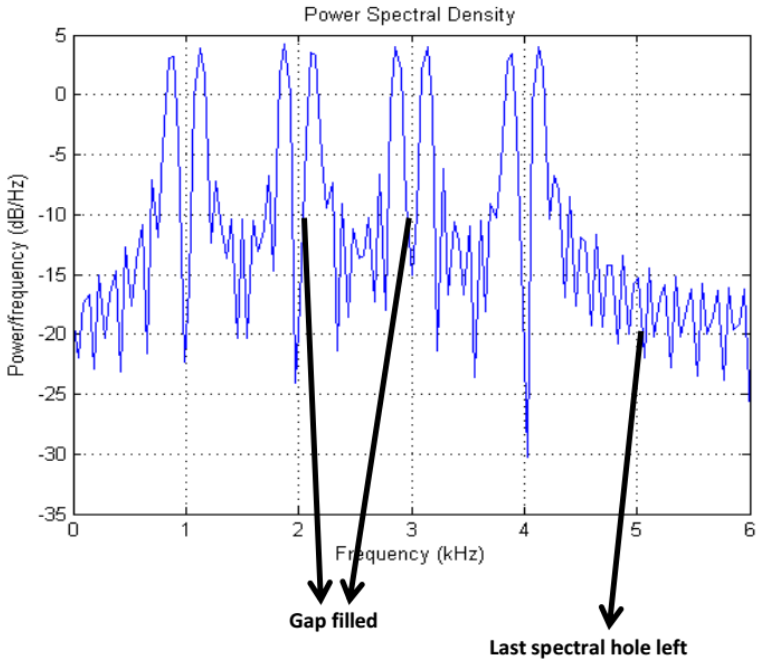


Fig. 9.6 Power spectral density curve: one slot remaining in the frequency spectrum.

9.2.4 Efficient frequency Band width

Now we have just one empty slot left which will get filled by addition of another Primary User. The power spectral density curve of the signal shows us that all of the frequency bands are efficiently in use after the addition of the last incoming user.

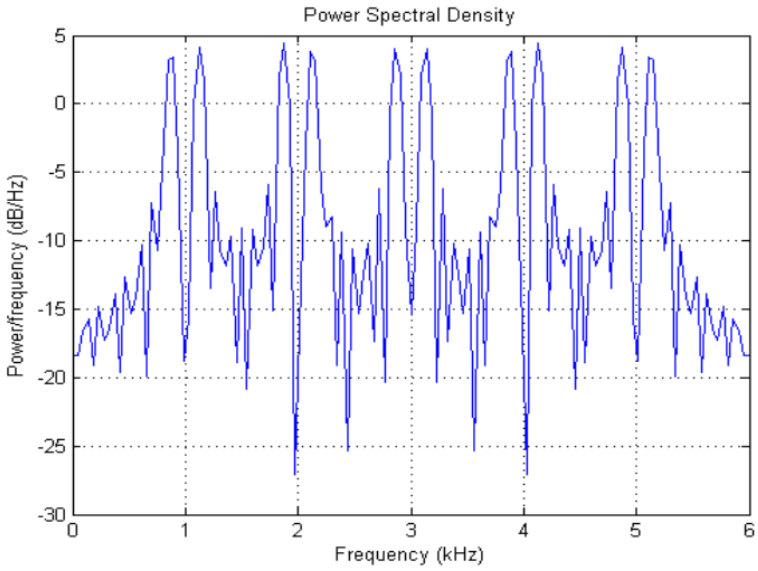


Fig. 9.7 Power spectral density curve: All of the frequency bands are efficiently in use.

9.2.5 Elimination of a Slot

Once all the slots are being assigned, our system will entertain no other User and will be able to free up the slots one by one as shown below. If we ask it to empty a slot, it will remove the data of that slot and make it ready for the next assignment.

```
Do you want to empty a slot: y
Which slot do you want to empty for your entry: 3
slot3 is fired
```

Fig. 9.8 Elimination of a slot in Command Window.

Following graph is shown in 9.9.

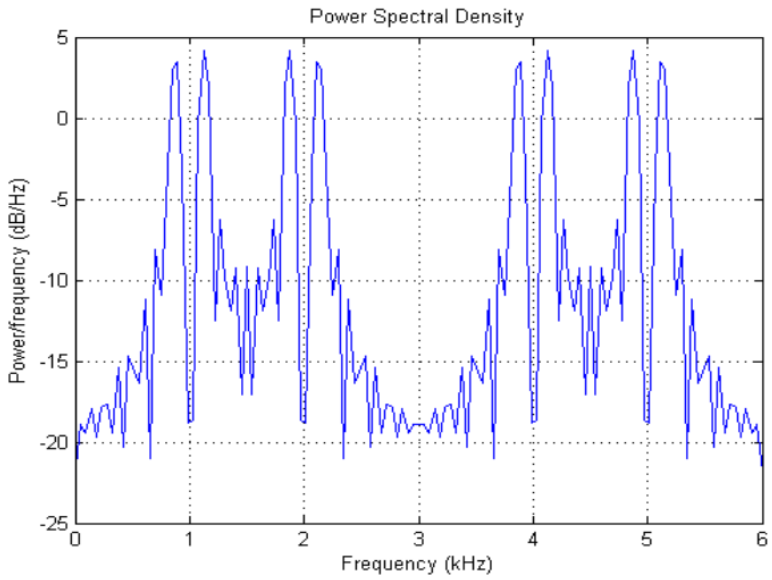


Fig. 9.9 Power spectral density curve: From the frequency spectrum 3rd slot has been eliminated.

9.3 LabVIEW

LABORATORY VIRTUAL ENGINEERING WORKBENCH is a system-design platform for a visual programming language from National Instruments. “G" is its graphical language. Usage of LabVIEW is increased nowadays. It is mainly used for Instrument control, Data acquisition and Industrial automation. It can be worked on various operating systems like Microsoft windows, Unix, Linux, macOS. The programming language used,“G", is a dataflow programming language. In LabVIEW the execution is done with the help of graphical block

diagram on which the programmer connects various function nodes. It is made by drawing wires which propagate variables and as soon as all input data becomes available, any node can execute the program.

9.3.1 USRP NI 2920

Term USRP stands for Universal Software Radio peripherals, USRP 2020 is a software programmable radio transceiver which is designed for teaching and research. It is helpful in the implementation of in the Industry's based wireless operation prototypes. Hardware of USRP is a device to utilize RF platform, it has the ability to transmit and receive signals for a wide frequency range and it also provide MIMO support. It enhances the platform, which are used for graphical programming such as labVIEW.

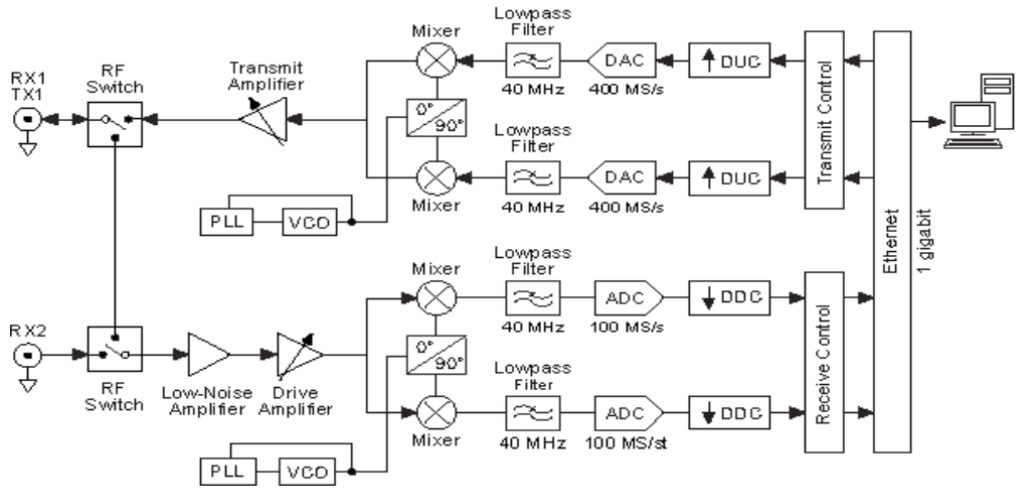


Fig. 9.10 Hardware architecture of NI-USRP.

For Transmission, The USRP hardware interpolates the incoming signal to a higher sampling rate using a digital up conversion (DUC) and then converts the signal to analog with a digital-to- analog convertor (DAC). The resulting analog signal is mixed with a carrier frequency. The phaselocked-loop is used to control Voltage-Control-Oscillator (VCO). Transmit Amplifier amplify the signal and then transmitted with the help of antenna. For Receiver, Low noise amplifies and drive amplifier amplifies the signal and mixer converts the signal into Baseband in-phase and Quadrature phase signal, then ADC convert the signal into digital form and Digital down converter (DDC) is used to provide user specified rate.

9.3.2 Block diagram of transmitter and receiver

We are working on Amplitude Modulation (AM) module, Fig. 9.11.

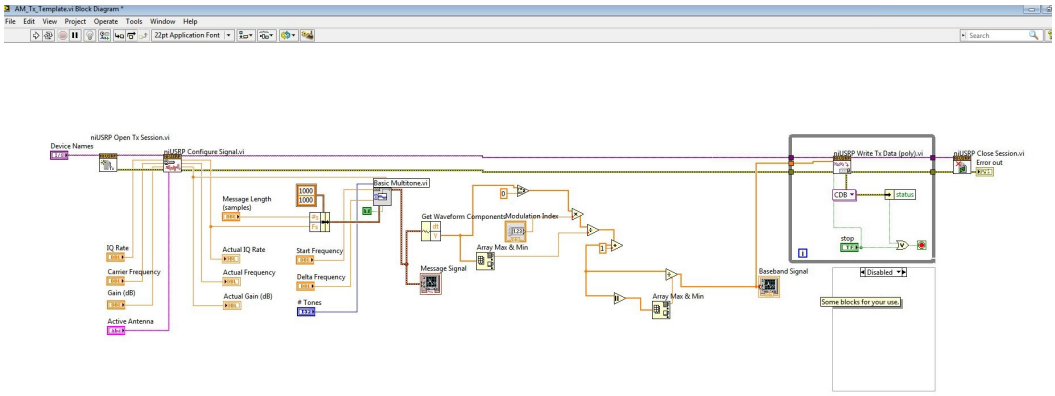


Fig. 9.11 AM Transmitter Block Diagram.

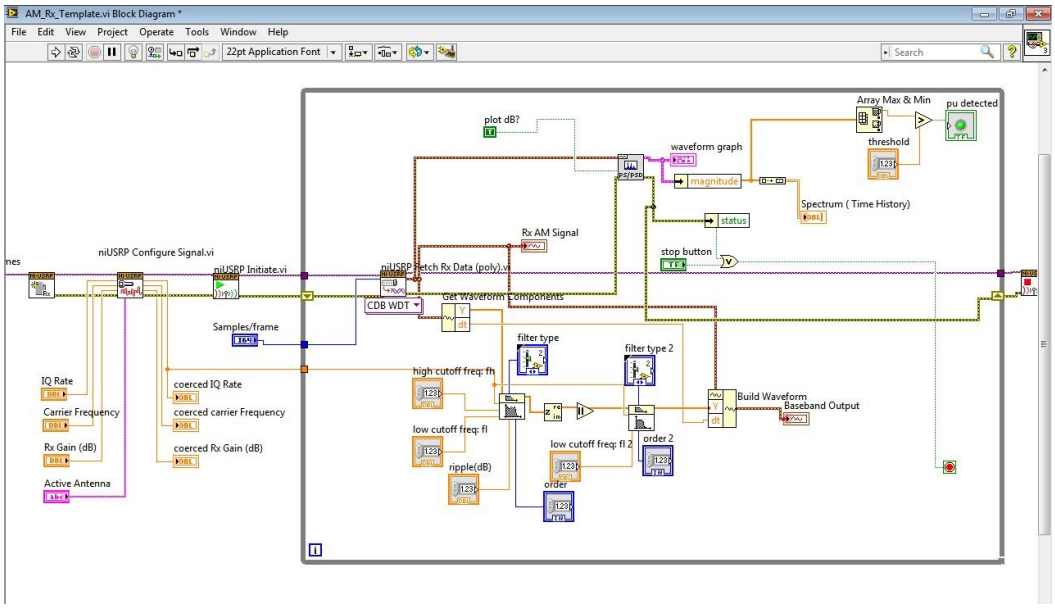


Fig. 9.12 AM Receiver Block Diagram.

9.3.3 While there is no primary user

In the absence of primary user the magnitude of PSD will be less than the threshold value. In this case only noise signal is present. As we can see in this figure there is no frequency response and the amplitude is very low.

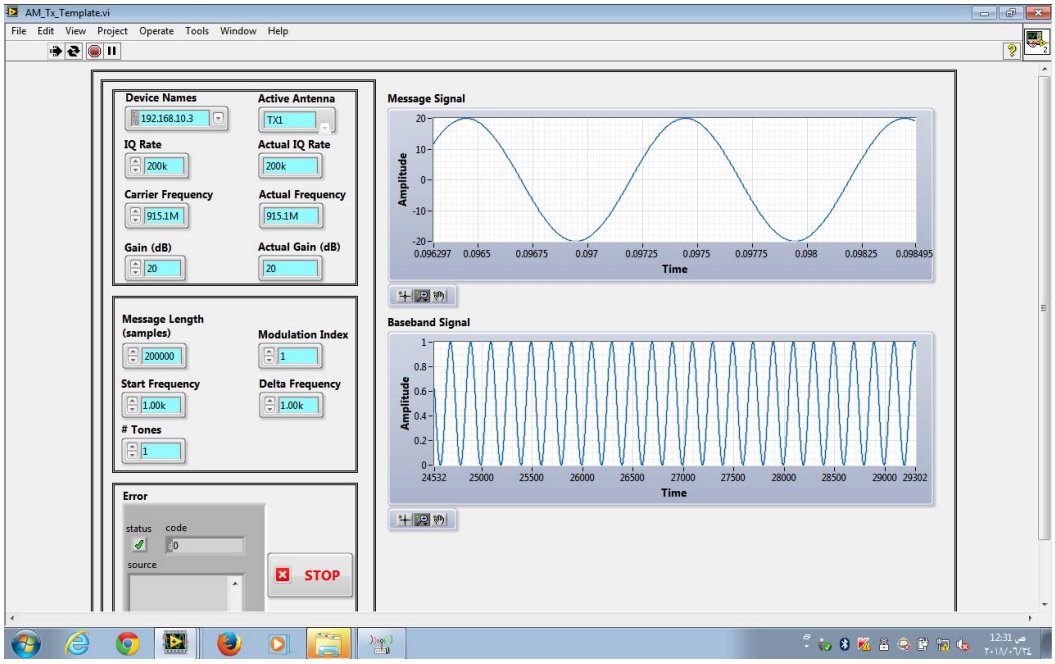


Fig. 9.13 AM Transmitted Signal.

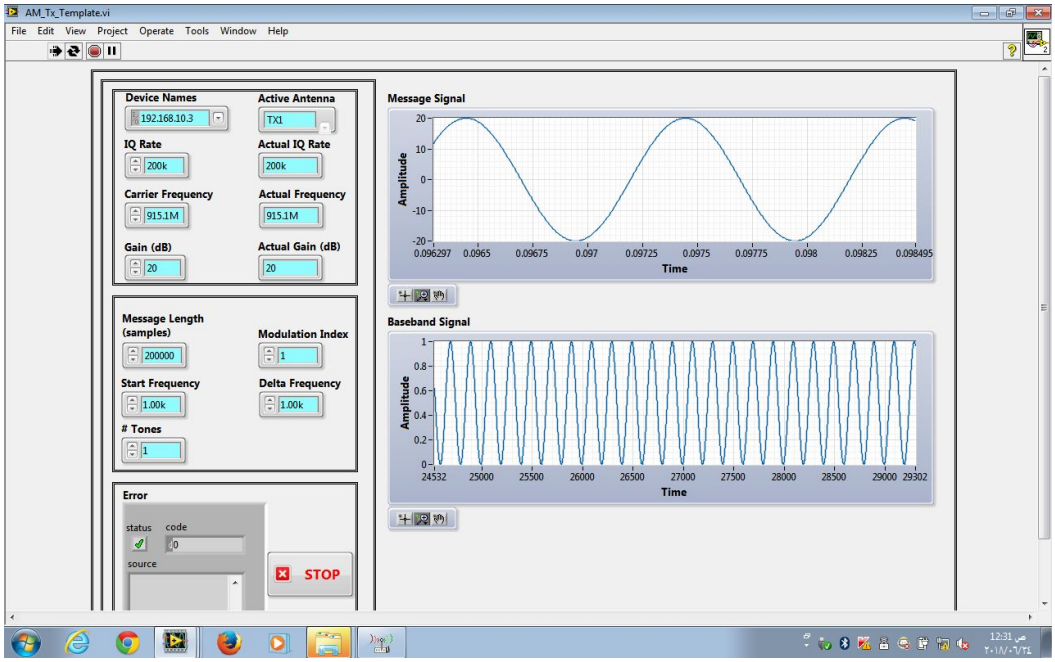


Fig. 9.14 AM Transmitted Signal.

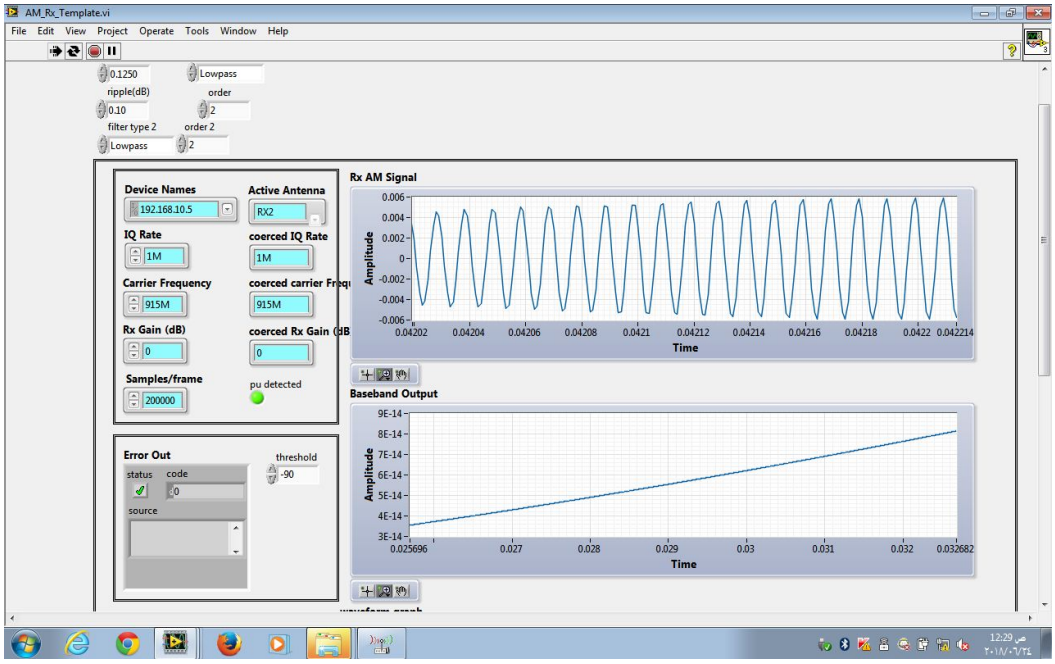


Fig. 9.15 AM Received Signal in case of present of primary user.

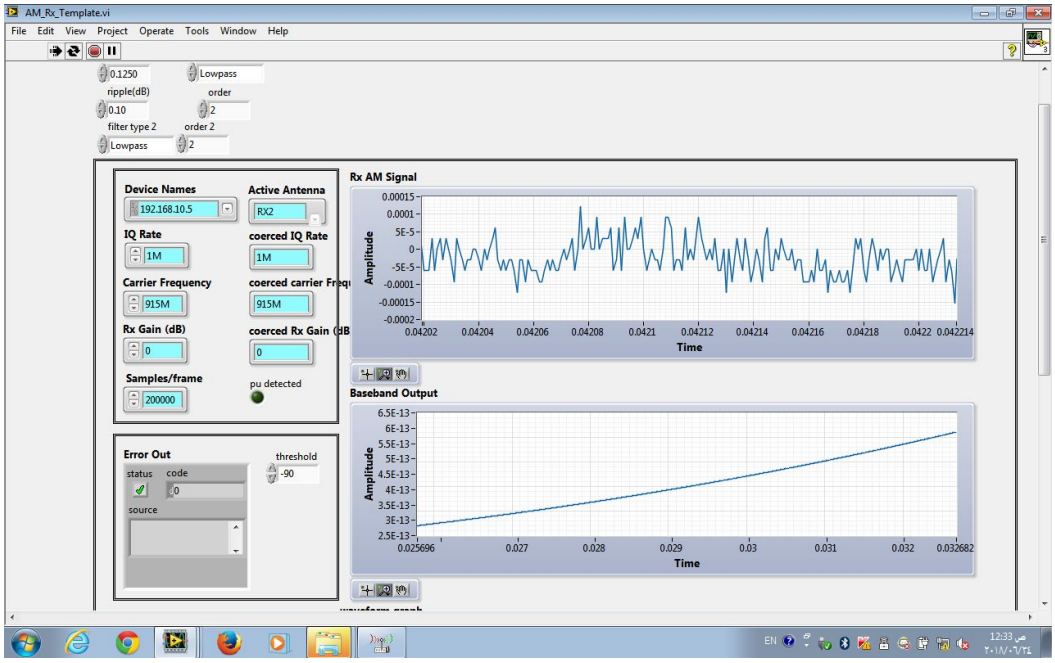


Fig. 9.16 AM Received Signal in case of absence of primary user.

9.3.4 When primary user is present

In this case we will receive a frequency response of received signal. After performing the PSD operation of this signal we can see that the amplitude is higher in this case and this is greater than the threshold value. Therefore, after comparing these two values (Amplitude of PSD and Threshold), LED will glow because of the lower value of threshold and this will alert that the primary user is present.

9.3.5 Conclusion

In this section we have sensed the presence of primary user. We have used energy detection technique to detect the spectrum. We have used LabVIEW platform and NI-USRP 2920 tool kit and designed the required model. We have placed two USRP NI 2920 kits on different distances and as we know that threshold value are affected due to different factors such as Geographical Conditions, Transmission Lines and some others. In this we have used hit and try values of Threshold. In Cognitive Radio's operation spectrum sensing plays an important role. New interpretation of spectrum space will provide different opportunities in this area. As technology is changing day by day and there is no doubt that we will experience various technologies which will create more opportunities in this field and in coming years Cognitive Radio will be the key of future wireless communication/ telecom world.

Chapter 10

Advanced Measuring (Instrumentation) Methods for Nuclear Installations

10.1 Introduction

The nuclear technology has been widely used in the world. The research of measurement in nuclear installations involves many aspects, such as nuclear reactors, nuclear fuel cycle, safety and security, nuclear accident, after action, analysis, and environmental applications. In last decades, many advanced measuring devices and techniques have been widely applied in nuclear installations. In this chapter we introduce the development of the measuring (instrumentation) methods for nuclear installations and the applications of these instruments and methods.

In last decade, nuclear technology has developed rapidly and became more important to human society with the development of science and technology. Nuclear technology has many advantages, such as zero carbon emissions, energy independence, and safety. At present, nuclear installations are more prevalent than ever before. Therefore, with the rapid development and wide applications of nuclear technology, many new technologies have been emerging to guarantee its reliability and safety, where measuring devices and techniques that can exactly measure and monitor the nuclear installations show particular importance.

This chapter is a review of advances in measuring (instrumentation) technology focus areas that have applications in nuclear installations. The instruments used in nuclear installations mainly include multifarious detectors, sensors, and meters.

10.2 Nuclear Power Reactors

10.2.1 Nuclear Power Reactors Instrumentations

In this section, instrumentations to measuring the neutron fission, the neutron dose, the flux, the reactor fission rate, and temperature are discussed.

A new set-up at the Conseil Europeen pour la Recherche Nucleaire (CERN) n_TOF facility has been built and tested by Guerrero et al. which allowed measuring simultaneously neutron, induced fission and capture reactions by combining a 4π Total Absorption Calorimeter (TAC) with several Micro-Me-gas (MMGAS) detectors [72]. The sketch is shown in Fig. 10.1. Bolshakova discussed the issues of creating the instrumentation for measured the semiconductor magnetic field sensors during their irradiation with neutrons in nuclear reactors up to fluences similar to neutron fluences in steady-state sensor locations in international thermonuclear experimental reactor [73].

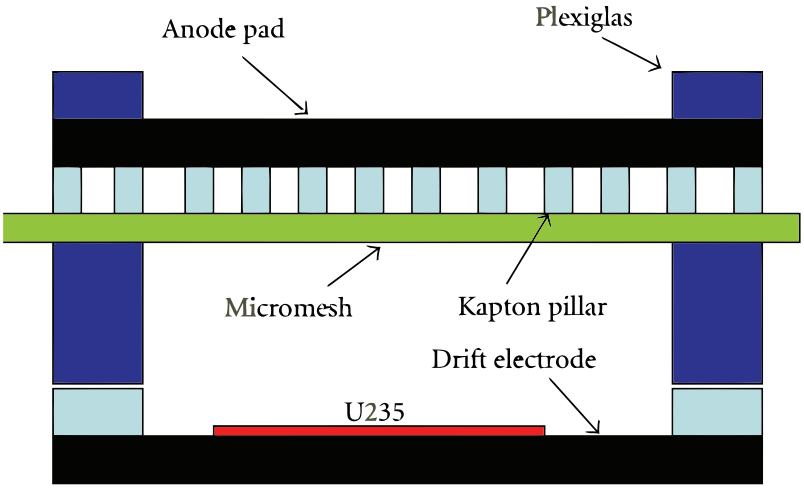


Fig. 10.1 Detail of the MMGAS detectors.

They used the tissue equivalent proportional counter to measure the neutron dose and dose equivalent rates, and the multi-sphere spectrometers were used in measurement of energy distributions [74]. Fourmentel et al. did a lot of work to measure more accurately photon flux, nuclear heating, and neutron flux in the reactor [75]. The devices measure the photon flux by two different sensors (Ionization chamber and Self-Powered Gamma Detector), the nuclear heating by two different ones (Differential calorimeter and Gamma Thermometer), and the neutron flux by three different kinds of sensors (Uranium Fission chamber, Plutonium Fission chamber and Self Powered Neutron Detector).

The devices measure the photon flux by two different sensors (Ionization chamber and Self-Powered Gamma Detector), the nuclear heating by two different ones (Differential calorimeter and Gamma Thermometer), and the neutron flux by three different kinds of sensors (Uranium Fission chamber, Plutonium Fission chamber and Self Powered Neutron Detector).

A key technique in nuclear installations is monitoring of temperature. Brixy used the noise thermometer to measure the temperature in nuclear reactors [76]. The noise thermometer rooted in the Nyquist theorem which is used to determine absolute temperatures. Both of the two resistors have noise voltages, one at the unknown temperature, the other at room temperature. Compared with the ratio of the resistances, when the noise voltages from the two resistors are matching, the ratio of their absolute temperatures is determined. Bily and Sklenka designed a new instrumentation for measurement of thermal effects on the training reactor which called VR-1 [77]. Rempe et al. contrasted the types of sensors available to support in-pile irradiations measurement and those sensors available to Advanced Test Reactor (ATR) currently [78]. Accomplishments from new sensor technology deployment efforts are remarkable by describing new thermal and temperature conductivity sensors available to ATR users now. The sketch is shown in Fig. 10.2.

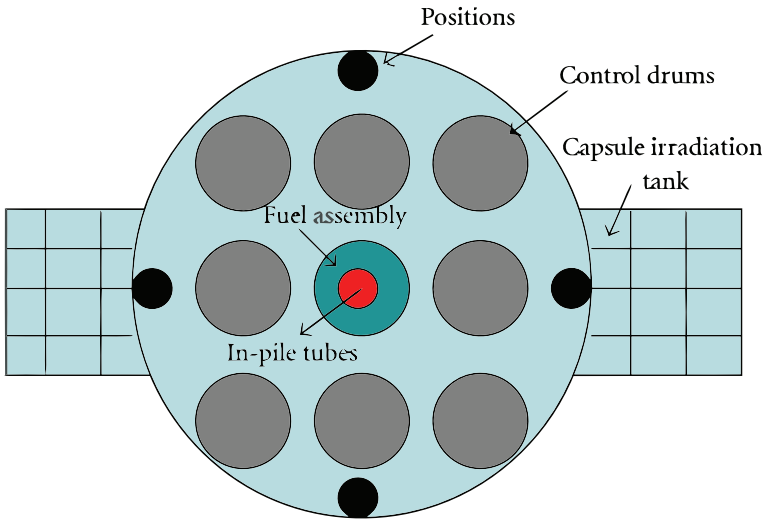


Fig. 10.2 The irradiation locations of ATR core cross-section.

The major superiority obtained over the last decade in the understanding of fundamental neutrino physics allowed us to put into use the detection of reactor anti-neutrino signals to automatic and non-intrusive nuclear power plant investigates. Porta et al. presented the NUCIFER experiment, which used a 1-ton Gd-doped liquid scintillator detector to be installed a few 10 m from a reactor core for measurements of its Plutonium content

and thermal power [79]. The design of such a small bulk detector has been focused on good background rejection and high detection efficiency. The advanced qualification of innovative high-temperature thermocouples specifically for in-pile applications was designed by Villard et al. [80]. This new kind of thermocouple was based on niobium thermoelements and molybdenum, which persisted nearly unchanged by thermal neutron flux even though under harsh nuclear environments, whereas Type *C* or Type *S* as typical high-temperature thermocouples is changed by significant drifts caused by material deformations under the same conditions.

The other key issue for advanced irradiation programs in nuclear research reactors is in situ measurement, especially in Material Testing Reactors (MTR). With the prospective, Optical Fiber Sensors (OFSs) is a good choice. OFS can provide unique feature substantial properties that bring intrinsic advantages over conventional sensing approaches. An initial condition for the development of OFS ensures that the Radiation-Induced Absorption (RIA) of the light in the fiber does not exceed a predefined threshold. Cheymol et al. reported the results of a long-lasting irradiation investigation, which carried out various fibers, including Single Mode (SM) fibers and Multimode (MM) and hollow core Photonic Band Gap (PBG) fibers [81].

10.3 Radiation Monitoring Instruments

Radiation exposure to humans can be broadly classified as internal and external exposure. Sealed sources, which are unlikely to cause internal exposure, are used almost exclusively in radiotherapy. This chapter deals with the monitoring of external exposures.

External exposure monitoring refers to measuring:

- Radiation levels in and around work areas;
- Radiation levels around radiotherapy equipment or source containers;
- Equivalent doses received by individuals working with radiation.

Radiation monitoring is carried out:

- To assess workplace conditions and individual exposures;
- To ensure acceptably safe and satisfactory radiological conditions in the workplace;
- To keep records of monitoring, over a long period of time, for the purposes of regulation or good practice.

Radiation monitoring instruments are used both for area monitoring and for individual monitoring. The instruments used for measuring radiation levels are referred to as area survey meters (or area monitors) and the instruments used for recording the equivalent doses received by individuals working with radiation are referred to as personal dosimeters (or individual dosimeters). All instruments must be calibrated in terms of the appropriate quantities used in radiation protection.

10.4 Area Survey Meter

Radiation instruments used as survey monitors are either gas filled detectors or solid state detectors (e.g. scintillator or semiconductor detectors). A gas filled detector is usually cylindrical in shape, with an outer wall and a central electrode well insulated from each other. The wall is usually made of tissue equivalent material for ionization chamber detectors and of brass or copper for other types of detector.

Depending upon the design of the gas filled detector and the voltage applied between the two electrodes, the detector can operate in one of three regions, shown in Fig. 10.3 (i.e. the ionization region B, proportional region C or Geiger–Müller (GM) region E). Regions of recombination and of limited proportionality in the 'signal versus applied voltage' plot (regions A and D, respectively, in Fig. 10.3) are not used for survey meters.

Survey meters come in different shapes and sizes, depending upon the specific application (see Fig. 10.4).

The gas is usually a non-electronegative gas in order to avoid negative ion formation by electron attachment, which would increase the collection time in the detector, thus limiting the dose rate that can be monitored. The increase in charge collection time results from the relatively slow mobility of ions, which is about three orders of magnitude smaller than that of electrons. Noble gases are generally used in these detectors.

β-γ survey meters have a thin end window to register weakly penetrating radiation. The γ efficiency of these detectors is only a few per cent (as determined by the wall absorption), while the b response is near 100% for β particles entering the detector.

Owing to their high sensitivity, the tubes of GM based γ monitors are smaller in size than ionization chamber type detectors.

Depending upon the electronics used, detectors can operate in a 'pulse' mode or in the 'mean level' or current mode. Proportional and GM counters are normally operated in the pulse mode.

Owing to the finite resolving time (the time required by the detector to regain its normal state after registering a pulse), these detectors will saturate at high intensity radiation fields.

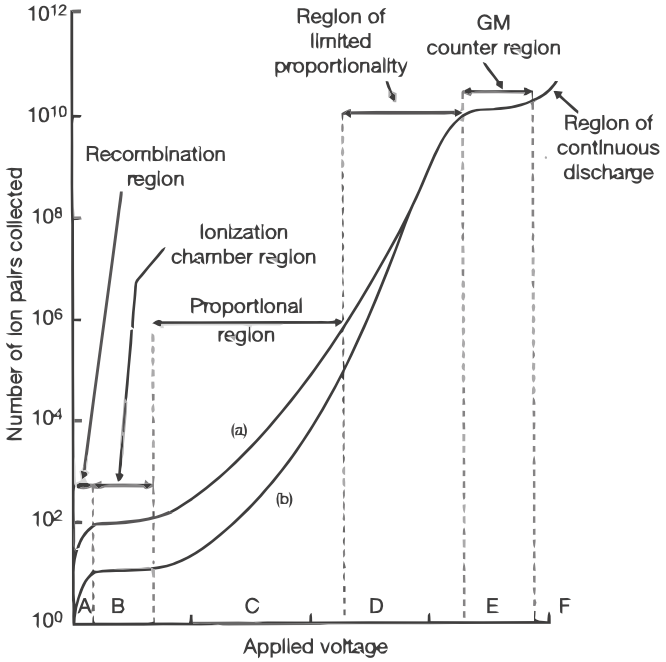


Fig. 10.3 Various regions of operation of a gas filled detector. Region A represents the recombination region, region B the ionization region, region C the proportionality region, region D the region of limited proportionality and region E the GM region. Curve (a) is for 1 MeV b particles, curve (b) for 100 keV b particles.

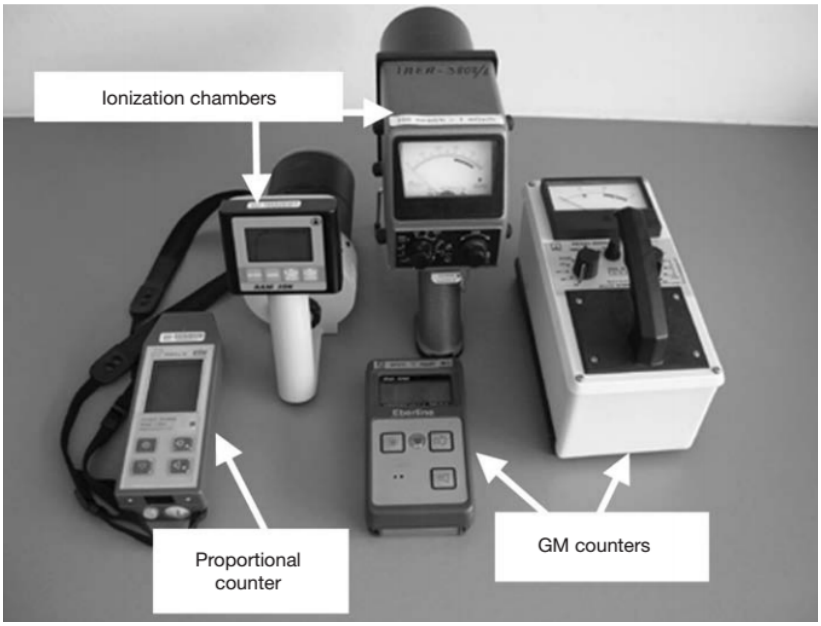


Fig. 10.4 Area survey meters commonly used for radiation protection level measurements: ionization chambers, a proportional counter and GM counters

Ionization chambers operating in the current mode are more suitable for higher dose rate measurements.

10.4.1 Ionization chambers

In the ionization region the number of primary ions of either sign collected is proportional to the energy deposited by the charged particle tracks in the detector volume. Owing to the linear energy transfer (LET) differences, the particle discrimination function can be used (see Fig. 10.3). Buildup caps are required to improve detection efficiency when measuring high energy photon radiation, but they should be removed when measuring lower energy photons (10-100 keV) and β particles.

10.4.2 Proportional counters

In the proportional region there is an amplification of the primary ion signal due to ionization by collision between ions and gas molecules (charge multiplication). This occurs when, between successive collisions, the primary ions gain sufficient energy in the neighbourhood of the thin central electrode to cause further ionization in the detector. The amplification is about $10^3 - 10^4$-fold.

Proportional counters are more sensitive than ionization chambers and are suitable for measurements in low intensity radiation fields. The amount of charge collected from each interaction is proportional to the amount of energy deposited in the gas of the counter by the interaction.

10.4.3 Neutron area survey meters

Neutron area survey meters operate in the proportional region so that the photon background can be easily discriminated against.

Thermal neutron detectors usually have a coating of a boron compound on the inside of the wall, or the counter is filled with BF_3 gas.

A thermal neutron interacts with a ^{10}B nucleus causing an (n,a) reaction, and the a particles can easily be detected by their ionizing interactions.

To detect fast neutrons the same counter is surrounded by a moderator made of hydrogenous material (Fig.10.5); the whole assembly is then a fast neutron counter. The fast neutrons interacting with the moderator are thermalized and are subsequently detected by a BF_3 counter placed inside the moderator.

Fig. 10.5 Neutron dose equivalent rate meter with a thermalizing polyethylene sphere with a diameter of 20 cm.

10.4.4 Geiger–Müller counters

The discharge spreads in the GM region throughout the volume of the detector and the pulse height becomes independent of the primary ionization or the energy of the interacting particles. In a GM counter detector the gas multiplication spreads along the entire length of the anode. Gas filled detectors cannot be operated at voltages beyond the GM region because they continuously discharge.

Owing to the large charge amplification (nine to ten orders of magnitude), GM survey meters are widely used at very low radiation levels (e.g. in areas of public occupancy around radiotherapy treatment rooms). They are particularly applicable for leak testing and detection of radioactive contamination.

GM counters exhibit strong energy dependence at low photon energies and are not suitable for use in pulsed radiation fields. They are considered indicators of radiation, whereas ionization chambers are used for more precise measurements.

GM detectors suffer from very long dead times, ranging from tens to hundreds of milliseconds. For this reason, GM counters are not used when accurate measurements are required of count rates of more than a few hundred counts per second. A portable GM survey meter may become paralysed in a very high radiation field and yield a zero reading. Ionization chambers should therefore be used in areas where radiation rates are high.

10.4.5 Scintillator detectors

Detectors based on scintillation (light emission) are known as scintillation detectors and belong to the class of solid state detectors. Certain organic and inorganic crystals contain activator atoms, emit scintillations upon absorption of radiation and are referred to as phosphors. High atomic number phosphors are mostly used for the measurement of γ rays, while plastic scintillators are mostly used with β particles.

10.4.6 Semiconductor detectors

Bulk conductivity detectors are formed from intrinsic semiconductors of very high bulk resistivity (e.g. CdS or CdSe). They act like solid state ionization chambers on exposure to radiation and, like scintillation detectors, belong to the class of solid state detectors. Extrinsic (i.e. doped with trace quantities of impurities such as phosphorus or lithium) semiconductors such as silicon or germanium are used to form junction detectors. They too act as solid state ionization chambers on application of a reverse bias to the detectors and on exposure to radiation. The sensitivity of solid state detectors is about 104 times higher than that of gas filled detectors, owing to the lower average energy required to produce an ion pair in solid detector materials compared with air (typically one order of magnitude lower) and the higher density of the solid detector materials compared with air (typically three orders of magnitude higher). These properties facilitate the miniaturization of solid state radiation monitoring instruments.

Chapter 11

Electromagnetic Interference (EMI) and Shielding Effectiveness

11.1 Introduction

Electromagnetic interference (EMI) is an undesirable and uncontrolled off-shoot of explosive growth of electronics and widespread use of transient power sources. Conducting polymers nanocomposites represent a novel class of materials that possess unique combination of electrical, thermal, dielectric, magnetic and/or mechanical properties which are useful for suppression of electromagnetic noises. Now it is possible to incorporate various dielectric or magnetic fillers within conducting polymer matrices to form multifunctional nanocomposites. In the next section we give a brief overview of fundamentals of EMI shielding and microwave absorption, theoretical aspects of shielding, governing equations, various techniques for measurement of shielding effectiveness and different strategies for controlling EMI.

Electromagnetic shielding is frequently used to reduce emissions or completely avoid radiation from different sources to penetrate the outer surface to secure humans and the surrounding environment. Radiation protection is the science and practice of protecting people and the environment from the harmful effects of ionizing radiation. It is a important not only in nuclear reactor stations, but also in other industries such as medical centers. Radiation shielding usually consist of barriers of lead (Pb), concrete or water [82]. There are many many materials, which can be used for radiation shielding, but there are manifold situations in radiation protection. It highly depends on the type of radiation to be shielded, its energy and many other parameters. For example, even depleted Uranium can be used as a good protection from gamma radiation, but on the other hand uranium is absolutely inappropriate shielding of neutron radiation. Most commonly used neutron shielding in

many sectors of the nuclear science and engineering is shield of concrete. Concrete is a hydrogen-containing material, but unlike water concrete have higher density (suitable for secondary gamma shielding) and does not need any maintenance. Because concrete is a mixture of several different materials its composition is not constant. Generally concrete are divided to “ordinary" concrete and “heavy" concrete. Heavy concrete uses heavy natural aggregates such as barites (barium sulfate) or magnetite or manufactured aggregates such as iron, steel balls, steel punch or other additives. As a result of these additives, heavy concrete have higher density than ordinary concrete (2300 kg/m3). Very heavy concrete can achieve density up to 5,900 kg/m3 with iron additives or up to 8900 kg/m3 with lead additives. Heavy concrete provide very effective protection against neutrons. [82]

Also, Carbon-fiber laminate woven materials are known to be used for shielding purposes [83], [84]. Lead aprons are used for personal protection of physicians and patients from X-ray (gamma) radiation during medical operations.

11.2 EMI and Shielding Effectiveness

Electromagnetic interference shielding (EMI) is an undesired electromagnetic (EM) induction triggered by extensive use of alternating current/Voltage which tries to produce corresponding induced signals (Voltage and current) in the nearby electronic circuitry, thereby trying to spoil its performance. The mutual interference among electronic gadgets, business machines, process equipments, measuring instruments and appliances lead to disturbance or complete breakdown of normal performance of appliances. The EM disturbances across communication channels, automation, and process control may lead to loss of time, energy, resources and also adversely affect human health.

Therefore, some shielding mechanism must be provided to ensure undisturbed functioning of devices even in the presence of external electromagnetic (EM) noises. For efficient shielding action, shield should possess either mobile charge carriers (electrons or holes) or electric and/or magnetic dipoles which interact with the electric (E) and magnetic (H) vectors of the incident EM radiation. In case of nuclear power plants, we also should shield EM radiated from the nuclear (e.g gamma rays - alpha rays).

11.3 Shielding definitions and phenomenon

EMI shield is essentially a barrier to regulate the transmission of the electromagnetic EM wave across its bulk. In power electronics, term shield usually refers to an enclosure that completely encloses an electronic product or a portion of that product and prevents the EM

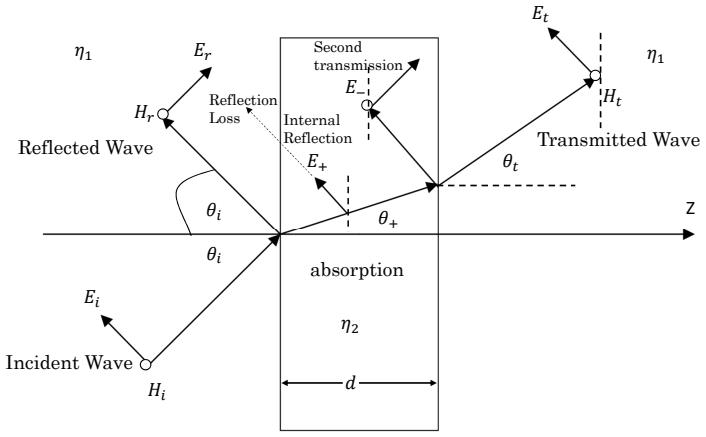


Fig. 11.1 Incident TM wave on a sheet.

emission from an outside source to deteriorate its electronic performance. In nuclear power plants, it means to enclosure all EM beams and secure the surroundings.

Mathematically shielding effectiveness SE_T can be expressed in logarithmic scale as per expressions:

$$SE_T(dB) = SE_R + SE_A + SE_M = 10\log_{10}(\frac{P_T}{P_I}) = 20\log_{10}(\frac{E_T}{E_I}) = \log_{10}(\frac{H_T}{H_I}) \qquad (11.1)$$

where P_I (E_I or H_I) and P_T (E_T or H_T) are the power (electric or magnetic field intensity) of incident and transmitted EM waves respectively. As shown in Fig. 11.1, three different mechanisms namely reflection (R), absorption (A) and multiple internal reflections (MIRs) contribute towards overall attenuation with SE_R, SE_A and SE_M as corresponding shielding effectiveness components due to reflection, absorption and multiple reflections respectively.

11.3.1 Shielding theory

This section presents the shielding basics based on the transmission line theory (Schelkunoff, 1943) and the plane wave shielding theory (Schulz et al,1988). Assume a uniform plane wave characteristic by E and H that vary within a plane only with x direction as showed in Fig. 11.2. The Maxwell's curl equations give:

$$\frac{dE}{dx} = -j\omega\mu H \quad \textbf{and} \quad \frac{dH}{dx} = -(\sigma + j\omega\varepsilon)E \qquad (11.2)$$

where μ is the permeability of the material and $\mu = \mu_o\mu_r$. μ_o and μ_r are the permeabilities of air (or free space) and shield material respectively, σ is the conductivity of material in S/m. where ε is the permittivity of the material and $\varepsilon = \varepsilon_o\varepsilon_r$. ε_o and ε_r are the permittivities

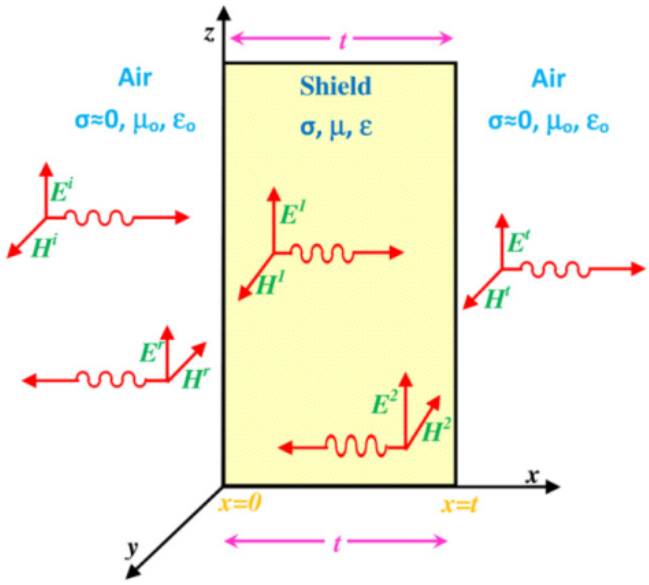


Fig. 11.2 Propagation of electromagnetic waves and its interaction with the shield material.

of air (or free space) and shield material respectively, $\omega = 2\pi f$. $\omega(f)$ is angular frequency (linear frequency) in Hz. All homogenous materials are characterized by a quantity known as the intrinsic impedance:

$$\eta = \sqrt{\frac{j\omega\mu}{\sigma + j\omega\varepsilon}} \tag{11.3}$$

When an electromagnetic wave propagates through the material, the wave impedance approaches the intrinsic impedance of the material. For dielectric material, the conductivity is extremely small $\sigma \ll \omega\varepsilon$ and the intrinsic impedance of Eq. 11.3 becomes:

$$\eta = \sqrt{\frac{\mu}{\varepsilon}} \tag{11.4}$$

For a conductor used below optical frequencies defined by $\sigma \gg \omega\varepsilon$, the intrinsic impedance of Eq. 11.3 can be written as:

$$\eta = \sqrt{\frac{j\omega\mu}{\sigma}} = (1+j)\sqrt{\frac{\pi\mu f}{\sigma}} \tag{11.5}$$

It is customary to define propagation constant γ in the media such that:

$$\gamma = (\alpha + j\beta) = \sqrt{j\omega\mu(\sigma + j\omega\varepsilon)} \tag{11.6}$$

where α is attenuation constant and β is phase constant. A good conductor is a medium for which $\sigma/\omega\varepsilon \gg 1$. Under this condition the Eq. 11.6 becomes:

$$\gamma = \sqrt{j\omega\mu} = (1+j)\sqrt{\pi\mu f\sigma} \tag{11.7}$$

Therefore, we can write $\alpha = \beta = 1/\delta = \sqrt{\pi\mu f\sigma}$, where quantity δ represents skin depth which is defined as the distance required by the wave to be attenuated to $1/e$ or 37% of its original strength. For a dielectric plane sheet $\sigma/\omega\varepsilon \ll 1$ and Eq. 11.6 becomes:

$$\gamma = \sqrt{-\omega^2\mu\varepsilon} = j\omega\sqrt{\mu\varepsilon} \tag{11.8}$$

The impedance of a homogeneous barrier of thickness d is

$$Z = \eta\frac{Z(d)\cosh(\gamma d) + \eta\sinh(\gamma d)}{\eta\cosh(\gamma d) + Z(d)\sinh(\gamma d)} \tag{11.9}$$

$$H(d) = \frac{\eta}{\eta\cosh(\gamma d) + Z(d)\sinh(\gamma d)}H(0) \tag{11.10}$$

$$E(d) = \frac{Z(d)}{\eta\sinh(\gamma d) + Z(d)\cosh(\gamma d)}E(0) \tag{11.11}$$

where $Z(0)$ is the impedance at interface 0 looking into the plane and $H(d)$ is the impedance at interface d looking into the right of the plane at $x = d$. If $Z(d) \neq \eta$, reflection occurs at the boundary $x = d$. Let E^i and H^i are the incident electric and magnetic fields, E^r and H^r the reflected fields, and E^t and H^t the transmitted fields as shown in Fig. 11.2. With the continuity of the tangential field component at a boundary we can write:

$$E^i + E^r = E^t \quad \textbf{and} \quad H^i + H^r = H^t \tag{11.12}$$

The electric and magnetic fields of a plane wave are related by the intrinsic impedance of the medium

$$E^i = \eta H^i, \quad E^r = -\eta H^r \quad \textbf{and} \quad E^t = Z(l)H^i \tag{11.13}$$

Solving the above equations, the expression of reflection coefficients can be written as:

$$q_E = \frac{E^r}{E^i} = \frac{Z(d) - \eta}{Z(d) + \eta} \tag{11.14}$$

$$q_H = \frac{H^r}{H^i} = \frac{\eta - Z(d)}{Z(d) + \eta} = -q_E \tag{11.15}$$

The corresponding transmission coefficients can be written as:

$$p_E = \frac{E^t}{E^i} = \frac{2Z(d)}{Z(d)+\eta} = 1+q_E \tag{11.16}$$

$$q_H = \frac{H^t}{H^i} = \frac{2\eta}{Z(d)+\eta} = 1+q_H \tag{11.17}$$

When two mismatched interfaces must be considered in the same plane, the net transmission coefficients is the product of the transmission coefficient across the two boundaries i.e.:

$$p = p_E = p_H = p_E(0)p_E(d) = p_H(0)p_H(d) \tag{11.18}$$

Considering the re-reflection effect, the transmission coefficients across the plane are:

$$T_H = \frac{H(d)}{H^i} = \frac{H(d)}{H^0}\frac{H(0)}{H^i} \tag{11.19}$$

$$T_E = \frac{E(d)}{E^i} = \frac{Z(d)}{Z_\omega}\frac{H(d)}{H^i} = \frac{Z(d)}{Z_\omega}T_H \tag{11.20}$$

where $E(0)$, $E(d)$, $H(0)$ and $H(d)$ are the actual values at interfaces i.e. at $x = 0$ and $x = d$. Z_ω is the impedance of the incident wave. Using 11.9, 11.10 and 11.11 for the plane of the thickness 0 and d

$$\frac{H(d)}{H(0)} = \frac{\eta}{\eta\cosh(\gamma d)+Z(d)\sinh(\gamma d)} \tag{11.21}$$

$$\frac{E(d)}{E(0)} = \frac{Z(d)}{Z(d)\cosh(\gamma d)+\eta\sinh(\gamma d)} \tag{11.22}$$

From 11.14 and 11.15 we may write:

$$\frac{H(d)}{H^i} = \frac{2Z_\omega}{Z(0)+Z_\omega} \tag{11.23}$$

$$\frac{E(d)}{H^i} = \frac{2Z(0)}{Z(0)+Z_\omega} \tag{11.24}$$

where $Z(0)$ is the impedance at interface $x = 0$ looking into the plane. By substituting 11.23 and 11.24 into equations 11.19 and 11.20 we get:

$$T = T_E = p_H(1-q_H e^{-2\gamma d})e^{-\gamma d} \tag{11.25}$$

where

$$p_H = \frac{4Z_\omega \eta}{(Z_{\omega+\eta})(Z(d)+\eta)} \tag{11.26}$$

$$q_H = \frac{(Z_{\omega-\eta)(Z(d)-\eta)}}{(Z_{\omega+\eta})(Z(d)+\eta)} \tag{11.27}$$

when $Z(d) = Z_\omega$, taking $k = Z_\omega/\eta$ we can write:

$$p = p_H = \frac{4k}{(k+1)^2} \tag{11.28}$$

$$q = q_H = \frac{(k-1)^2}{(k+1)^2} \tag{11.29}$$

$$T_E = T_H = T = p(1-qe^{-2\gamma d})e^{-\gamma d} \tag{11.30}$$

$$SE_T(dB) = 20\log_{10}|T| = 20\log_{10}\left|p(1-qe^{-2\gamma d})e^{-\gamma d}\right| \tag{11.31}$$

$$\begin{aligned} SE_T &= SE_R + SE_A + SE_M \\ SE_T(dB) &= 20\log_{10}|p| + 20\log_{10}\left|e^{-\gamma d}\right| + 20\log_{10}\left|(1-qe^{-2\gamma d})\right| \end{aligned} \tag{11.32}$$

Therefore, after careful comparison of δ with shield thickness d two situations can be visualized:

- When ($d \ll \delta$): which occurs either at low frequencies or in case of electrically thin sample where actual shield thickness is much less than skin depth. In such a case the absorption which is a bulk (or thickness) related phenomenon, can be neglected and attenuation occurs almost exclusively by reflection. The total shielding becomes frequency independent and can be expressed in terms of free space impedance ($Z_o = 377\Omega$) as:
$$SE(dB) = -20\log_{10}[1 + \frac{Z_o}{2} d\sigma_T] \tag{11.33}$$
- When ($d \gg \delta$) which is valid in our case and generally occurs at higher frequencies where skin depth becomes much less as compared to actual shield thickness i.e. in case of electrically thick samples. In such regime, attenuations due reflection, absorption and multiple internal sub-phenomenon becomes a straight forward exercise after making good conductor approximation i.e. $\sigma_T/\omega\varepsilon \gg 1$.

11.3.2 Reflection loss

The reflection loss (SE_R) is related to the relative impedance mismatch between the shield's surface and propagating wave. The magnitude of reflection loss under plane wave (far field conditions) can be expressed as (Saini et al, 2011):

$$SE_R(dB) = -10\log_{10}(\frac{\sigma_T}{16\omega\varepsilon_o\mu_r}) \tag{11.34}$$

where σ_T is the total conductivity, f is the frequency in Hz, μ_r is the relative permeability referred to free space; The above expression shows that SE_R is a function of the ratio of conductivity (σ_T) and permeability (mu_r) of the shield material i.e. quantity (σ_T/μ_r). Further for a given material (i.e. fixed σ_T and μ_r), SE_R decreases with increase in frequency.

11.3.3 Absorption loss

As shown in Fig. 11.1, when an electromagnetic wave pass through a medium its amplitude decreases exponentially. This decay or absorption loss occurs because currents induced in the medium produce ohmic losses and heating of the material, and E_t and H_t can be expressed as $E_t = E_i e^{d/\delta}$ and $H_t = H_i e^{-d/\delta}$ (Ott, 2009). Therefore, the magnitude of absorption term (SE_A) in dB can be expressed by following equation:

$$SE_A(dB) = -20\frac{d}{\delta}\log_{10} e = -8.68d(\frac{\sigma_T\omega\mu_r}{2})^2 \tag{11.35}$$

where d is shield thickness in inches and f is frequency in Hertz. The above expression revealed that SE_A is proportional to the square root of the product of the permeability (μ_r) times the conductivity (σ_T) of the shield material i.e. quantity $(\sigma_T\mu_r)^{1/2}$ (Saini et al, 2009a, 2011). Further, for a given material, absorption loss increases with increase in frequency. Therefore, a good absorbing material should possess high conductivity and high permeability, and sufficient thickness to achieve the required number of skin depths even at the lowest frequency of concern.

11.3.4 Multiple Internal Reflections (MIRs)

If the shield is thin, the reflected wave from the second boundary is re-reflected from the first boundary and returns to the second boundary to be reflected again and again as shown in Fig. 11.1. The attenuation due these multiple internal reflections i.e. SE_M can be mathematically

expressed as (Ott, 2009, Saini et al, 2011):

$$SE_M = 20\log_{10}(1-e^{-2d/\gamma}) = 20\log_{10}\left|1-10^{-SE_A/10}\right| \tag{11.36}$$

Therefore, it can be seen from the above expression that SE_M is closely related to absorption loss (SE_A). SE_M is also important for porous structures and for certain type of filled composites or for certain design geometries. It can be neglected in the case of a thick absorbing shield due high value of SEA so that by the time the wave reaches the second boundary, it is of negligible amplitude. For practical purposes, when $SE_A is \geq 10$ dB (Saini, et al 2009a, 2011) SE_M can be safely neglected. Usually SE_M is important only when metals are thin and are used at very low frequencies (kHz range). However, for highly absorbing materials or at very high frequencies (GHz or high), condition $|SE_A| \geq 10$ dB gets satisfiedand re-reflections can be safely ignored i.e. $SE_M \approx 0$.

11.4 Numerical Calculations of Shield Effectiveness

In this section, we consider an incident TM wave with frequency more than 10 THz falling on a thin sheet of different materials such as Mumetal, Aluminum, and Plumbum (Lead) “Pb". We calculate Shield Effectiveness (SE) for each of these materials, which is considered one of the most important parameter for radiation protection in nuclear reactor stations where the main purpose is to reduce the radiation exposure to persons and staff in the vicinity of radiation sources. Also, different polymer materials, such as Polytetrafluoroethylene (PTFE), can be used as the base material for design of shields for microwave frequencies (100 MH-10 GHz).

11.4.1 Simulations and Results

MATLAB simulations are performed to calculate SE of three materials which are, Mumetal ($\sigma_r = 0.0305$ and $\mu_r = 30000$), Aluminum ($\sigma_r = 0.58$ and $\mu_r = 1$), and Lead “Pb" ($\sigma_r = 0.0763$ and $\mu_r = 0.98$). Where σ_r is the relative conductivity, relative conductivity is defined with respect to Copper ($\sigma_{Copper} = 5.96 \times 10^7$), and μ_r is the relative permeability with respect to free space. Thickness of the sheet is 10 μm and it is on a distance of 30 cm from the source of radiation. The simulations also have shown that, the variation of incident angles will slightly change the total SE by a fraction of 1 dB which can be negligible.

From simulations, it is obvious that Mumetal has the highest SE for approximately all higher frequencies. Aluminum, Lead, and other Ferritic materials will exist between

Mumetal and Nichrome which has the lowest acceptable conductivity. Dielectric material and semiconductors maybe used for shielding but after doping to manipulate in their structure.

Theoretically a few hundreds dB SE can be reached at low frequencies even with a few micrometer thick shield against electrical interfering sources, but this may be as low as 0 dB for the magnetic sources as seen in Fig. 11.3. Starting from low frequencies, SE decreases with frequency for electrical shielding and increases with frequency for magnetic shielding.

In practice, depending on the critically of the problem under consideration, SE values of 30-60 dB are considered acceptable, whereas SE values in the range of 70-90 dB represent quite high shields. The shielding performance of a metal box with no holes, slots, joints, vents, windows, or other discontinuities, the SE can only be as good as allowed by such shielding imperfections.

We can notice these results:

- Shielding mostly occurs because of reflections and absorption at low and high frequencies respectively.
- High conductivity is good for both reflection and absorption while high permeability causes high absorptions but low reflections.

In brief, SE performance of a sheet depends on the material permeability μ, conductivity σ, sheet thickness d, distance from source of radiation, and frequency of the incident wave.

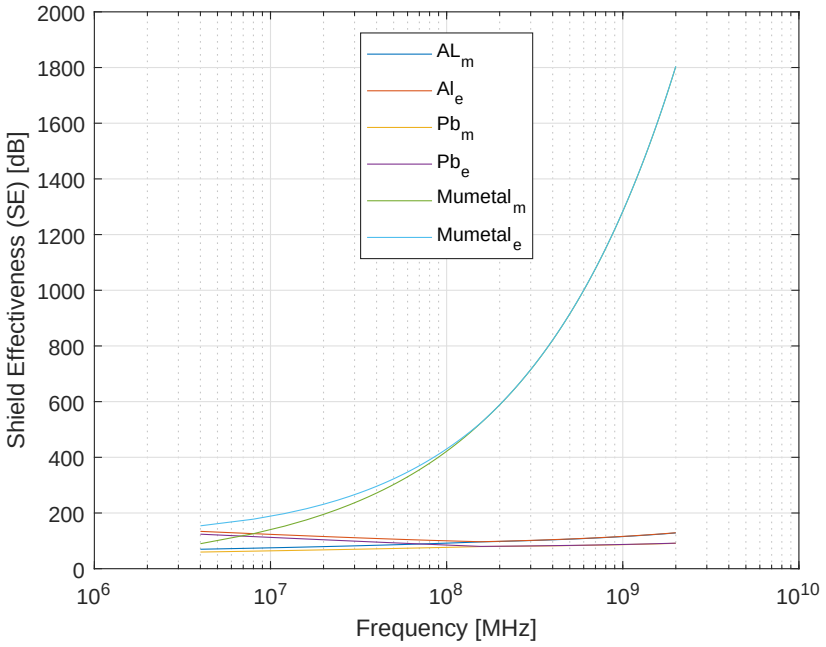


Fig. 11.3 Shield Effectiveness vs. frequency of different metals.

11.4.2 Detection and Shielding of Gamma Radiation

In nuclear power plants there are several methods that are used for fast neutron detection. In [85], they used Teflon (PTFE) to detect fast neutrons with energies $E_n > 3$ MeV.

Effective shielding of gamma radiation is in most cases based on use of materials with two following material properties: (a) high-density of material, and (b) high atomic number of material (high Z materials). However, low-density materials and low Z materials can be compensated with increased thickness, which is as significant as density and atomic number in shielding applications.

A lead (Pb) is widely used as a gamma shield. Major advantage of lead shield is in its compactness due to its higher density. On the other hand depleted Uranium 235 is much more effective due to its higher Z. Depleted Uranium 235 is used for shielding in portable gamma ray sources.

11.4.3 Polytetrafluoroethylene (Teflon)

Polytetrafluoroethylene (PTFE), also known as Teflon, is a commonly used material in a spacecraft design, automotive and semiconductor industry. Reported applications are associated to the fact that PTFE has excellent chemical inertness, high thermal stability and low frictional coefficient [86],[87]. Therefore, it is broadly used in a range of industrial sectors where severe conditions as radiation, high temperature or lack of protection atmosphere occurs [88]. Materials subjected to aforementioned conditions are of great importance when it comes to safety assurance in nuclear facilities.

Also, different polymer materials, such as Teflon or thermoplasts, can be used as the base material for design of shields for microwave frequencies (100 MH-10 GHz). Teflon is almost non-dispersive in the frequency range of interest, and its loss factor can be neglected. The dielectric constant of the Teflon is taken as 2.2.

Over a wide range of frequencies, Teflon coatings have a high dielectric strength, low dissipation factor, and high surface resistivity. Dielectric strength is the highest voltage that the coating can withstand before it breaks down. The dissipation factor is the percentage of electrical energy absorbed and lost when current is applied to the coating. A low dissipation factor means that the absorbed energy dissipated as heat is low. Adding fillers to certain coatings can make them electro-conductive enough to be used as an anti-static coating. In addition, it can be used for shielding.

References

[1] E. Grayver, *"Implementing Software Defined Radio"*. New York: Springer Science + Business Media, 2013.

[2] J. Mitola, "Cognitive radio an integrated agent architecture for software defined radio," Master's thesis, Royal Institute of Technology (KTH), 2000.

[3] C. R. Stevenson and G. Chouinard, "Ieee 802.22: The first cognitive radio wireless regional area network standard," *IEEE Communications Magazine*, vol. 47, pp. 130–138, 2009.

[4] A. Khattab, D. Perkins, and M. Bayoumi, *"Cognitive Radio Networks From Theory to Practice"*. New York: Springer Science+Business Media, 2013.

[5] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 201–220, 2005.

[6] T. R. D. M. C. W. B. D. Scaperoth, B. Le and S. Harrison, "Cognitive radio platform development for interoperability," *in Military Communications Conference*, Oct. 2006.

[7] L. E. D. T. W. R. B. L. K. E. Nolan, P. D. Sutton and C. W. Bostian, "Demonstration and analyses of collaboration, coexistence, and interoperability of cognitive radio platforms," *IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, USA, Jan. 2007.

[8] M. C. V. I. F. Akyildiz, W. Y. Lee and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Elsevier Computer Networks Journal*, vol. 50, pp. 2127–2159, Sept. 2006.

[9] M. Nekovee, "Quantifying the availability of tv white spaces for cognitive radio operation in the uk," *IEEE International Conference on Communications*, June 2009.

[10] M. J. Marcus, "Unlicensed cognitive sharing of tv spectrum: The controversy at the federal communications commission," *IEEE Communications Magazine*, vol. 43, pp. 24–25, May 2005.

[11] L. B. Le and E. Hossain, "Resource allocation for spectrum underlay in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 5306–5315, Dec. 2008.

[12] R. Zhang and Y. Liang, "Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, pp. 88–102, Feb. 2008.

[13] M. R. N. A. Attar, O. Holland and A. H. Aghvami, "Interference-limited resource allocation for cognitive radio in orthogonal frequency-division multiplexing networks," *IET Communications*, vol. 2, pp. 806–814, July 2008.

[14] T. A. Weiss and F. K. Jondral, "Spectrum pooling: An innovative strategy for the enhancement of spectrum efficiency," *IEEE Communications Magazine*, 2004.

[15] S. D. M. G. R. D. Steenkiste, P., *"Future directions in cognitive radio network research"*. NSF Workshop Report, 2009.

[16] A. H. Gorcin, A., *"Public safety and emergency case communications: Opportunities from the aspect of cognitive radio"*. Chicago, IL: IEEE DySPAN, 2008.

[17] V. A. K. H. F. S. Rehmani, M.H., "A cognitive radio based internet access framework for disaster response network deployment," *INRIA*, July 2012.

[18] H. Goldstein, *"Engineers help NGOs get online after Haiti quake"*. IEEE Spectrum, 2010.

[19] P. V. V. J. Guijarro, L., *"Competition in cognitive radio networks: Spectrum leasing and innovation"*. Las Vegas, NV: IEEE CCNC, 2011.

[20] T. R. P. T. H. W. F. M. A. M. Xu, L., *"DRiVEing to the internet: Dynamic radio for ip services in vehicular environments. In: Proceedings of the 25th Annual Conference on Local Computer Networks"*. Tampa, FL: LCN'00, 2000.

[21] M. K. L. T. W. M. Tnjes, R., *"OverDRiVE spectrum efficient multicast services to vehicles. In: Proceedings of IST Mobile and Telecommunicatiosn Summit"*. Greece: Thessaloniki, 2002.

[22] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Processing Magazine*, vol. 24, pp. 79–89, May 2007.

[23] Q. Zhao and A. Swami, "A decision-theoretic framework for opportunistic spectrum access," *IEEE Wireless Communications Magazine*, vol. 14, pp. 14–20, Aug. 2007.

[24] Q. Zhao, "Spectrum opportunity and interference constraint in opportunistic spectrum access," *IEEE International Conference on Acoustics*, Apr. 2007.

[25] Q. Z. Y. Chen and A. Swami, "Joint design and separation principle for opportunistic spectrum access in the presence of sensing errors," *IEEE Transactions on Information Theory*, vol. 54, pp. 2053–2071, May 2008.

[26] W. R. Q. Zhao and A. Swami, "Spectrum opportunity detection: How good is listenbefore-talk?," *Proceedings of the Asilomar Conference on Signals, Systems, and Computers*, Nov. 2007.

[27] T. Sheldon, *Encyclopedia of Networking and Telecommunications*. New York, NY, USA: Osborne/McGraw-Hill, 2001.

[28] Q. Z. W. Ren and A. Swami, "Power control in cognitive radio networks: How to cross a multi-lane highway," *IEEE Journal on Selected Areas in Communications, Special Issue on Stochastic Geometry and Random Graphs for Wireless Networks*, vol. 27, pp. 1283–1296, Sept. 2009.

[29] F. C. Commission, *"Memorandum opinion and order"*. FCC 07-99, May 2007.

[30] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," *IEEE International Workshop on Mobile Multimedia Communications*, vol. 1, pp. 3–10, Nov. 1999.

[31] R. A. J. Perez-Romero, O. Salient and L. Giupponi, "A novel on-demand cognitive pilot channel enabling dynamic spectrum allocation," *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 46–54, April 2007.

[32] R. Tandra and A. Sahai, "Snr walls for signal detection," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, pp. 4–17, Feb. 2008.

[33] R. Tandra and A. Sahai, *"Noise calibration, delay coherence and SNR walls for signal detection"*. in Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Oct. 2008.

[34] J. D. Poston and W. D. Horne, "Discontiguous ofdm considerations for dynamic spectrum access in idle tv channels," *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 607–610, Nov. 2005.

[35] S. Kondo and L. Milstein, "Performance of multicarrier ds cdma systems," *IEEE Transactions on Communications*, vol. 44, pp. 238–246, Feb. 1996.

[36] A. M. W. G. J. M. R. Rajbanshi, Q. Chen and J. B. Evans, "Quantitative comparison of agile modulation technique for cognitive radio transceivers," *IEEE Consumer Communications and Networking Conference*, pp. 1144–1148, Jan. 2007.

[37] M. R. N. A. Attar and A. H. Aghvami, "Cognitive radio transmission based on directsequence mc-cdma," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 1157–1162, April 2008.

[38] M. R. N. A. Attar and A. H. Aghvami, "Sharing with legacy rans using cognitive mc-cdma," *in Proceedings of the IEEE International Symposium on Personal*, Sept. 2008.

[39] M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, pp. 439–441, May 1983.

[40] P. M. N. Devroye and V. Tarokh, "Achievable rates in cognitive radio channels," *IEEE Transactions on Information Theory*, vol. 52, pp. 1813–1827, May 2006.

[41] M. Z. Win and R. A. Scholtz, "Impulse radio: How it works," *IEEE Communication Letters*, vol. 2, pp. 36–38, Feb. 1998.

[42] R. P. A. J. V. L. A. W. J. K. S. Gilhousen, I. M. Jacobs and C. E. W. III, "On the capacity of a cellular cdma system," *IEEE Transactions on Vehicular Technology*, vol. 40, pp. 303–312, May 1991.

[43] R. M. B. R. Menon and J. H. Reed, "Outage probability based comparison of underlay and overlay spectrum sharing techniques," *IEEE Transactions on Vehicular Technology in Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, vol. 1, pp. 101–109, Nov. 2005.

[44] L. Wang and C. Tellambura, "Narrowband interference suppression in time-hopping impulse radio ultra-wideband communications," *IEEE Transactions on Communications*, vol. 54, June. 2006.

[45] S. U. C. Rose and R. D. Yates, "Wireless systems and interference avoidance," *IEEE Transactions on Wireless Communications*, vol. 1, pp. 415–428, July 2002.

[46] A. P. R. Etkin and D. Tse, "Spectrum sharing for unlicensed bands," *in Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, vol. 1, pp. 251–258, Nov. 2005.

[47] U. Berthold and F. K. Jondral, "Guidelines for designing ofdm overlay systems," *in Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, vol. 1, pp. 626–629, Nov. 2005.

[48] B. E. Hoffmeyer, Stewart and Frantz, "Standard definitions and concepts for dynamic spectrum access—terminology relating to emerging wireless networks, system functionality, and spectrum management," *tech. rep., IEEE 1900.1 Standar*, Oct. 2008.

[49] T. W. Rondeau and C. W. Bostian, "Cognitive techniques: physical and link layers," *Cognitive Radio Technology (B. A. Fette, ed.):Elsevier Science and Technology Books*, 2006.

[50] F. C. Commission, "Facilitating opportunities for flexible, efficient and reliable spectrum use employing cognitive radio technology," Mar. 2005.

[51] I. T. Union, "New broadband statistics," Jan. 2005.

[52] I. W. G. on Wireless Regional Area Networks, "[online]: www.iee802.org/22," Feb. 2009.

[53] I. of Electrical and I. Electronic Engineerings, "Ieee 802.16 working group on broadband wireless standards [online]: http://wirelessman.org.,"

[54] A. Mody, "Protocol reference model enhancements in 802.22," July 2008.

[55] I. T. Union, "Method for point-to-area prediction for terrestrial services in the frequency range 30 mhz to 3000 mhz," ITU-R P.1546-1, Oct. 2005.

[56] G. C. M. M. S. Shellhammer, V. Tawil and M. Ghosh, "Spectrum sensing simulation model," IEEE 802.22-06/0028r6, June 2006.

[57] G. Chouinard, "Wran reference model spreadsheet," IEEE 802.22-04-0002r12, June 2006.

[58] Z. L. W. H. S. J. S. C. R. Stevenson, G. Chouinard and W. Caldwell, "Ieee 802.22: The first cognitive radio wireless regional area network standard," *IEEE Communication Magazine*, Jan. 2009.

[59] I. . WG, "Ieee p802.22/d0.1 draft standard for wireless regional area networks part 22: Cognitive wireless ran medium access control (mac) and physical layer (phy) specifications: Policies and procedures for operation in the tv bands," *IEEE docs*, May 2006.

[60] K. Bian and J.-M. J. Park, "Security vulnerabilities in ieee 802.22," *WICON '08: Proceedings of the 4th Annual International Conference on Wireless Internet*, pp. 1–9, 2008.

[61] Y. T. H. A. M. Wyglinski, M. Nekovee, "Cognitive radio communications and networks: Principles and practice," Dec. 2009.

[62] K. Dogancay and D. A. Gray, "Closed-form estimators for multi-pulse tdoa localization," *in Proceedings of the Eighth International Symposium on Signal Processing and Its Applications*, pp. 543–546, Aug. 2005.

[63] D. Niculescu and B. Nath, "Ad hoc positioning system (aps)," *in Proceedings of the IEEE Global Telecommunications Conference*, pp. 2926–2931, Nov. 2001.

[64] R. W. T. Locher and A. Zollinger, "Received-signal-strength-based logical positioning resilient to signal fluctuation," *in Proceedings of the First ACIS International Workshop on Self-Assembling Wireless Sensor Networks*, May 2005.

[65] Y. X. L. Zhang and Y.-C. Liang, "Power allocation for multi-antenna multiple access channels in cognitive radio networks," *in Proceedings of the Annual Conference on Information Sciences and Systems, Princeton*, Mar. 2007.

[66] M. J. S. T. K. A. N. Mody, R. Reddy and D. J. Shyy, "Security and the protocol reference model enhancements in ieee 802.22," *IEEE Document: IEEE 802.22-08/0083r04*, June 2008.

[67] MESA, "Project mesa: Statement of requirements[online]: projectmesa.org/ftp/," 2008.

[68] P. T. I. Group, "P25 homepages," *[Online]: www.project25.org/*, 2009.

[69] T. Forum, "Tetrapol homepage," *[Online]: www.tetrapol.net/*, 2009.

[70] T. T. M. A. Ltd., "Terrestial trunked radio, radio communication standards, tetra private digital mobile radio pmr," *[Online]: www.tetra-association.com/*, 2009.

[71] C. Oosting, "De vuurwerkramp—eindrapport," 2001.

[72] D. C.-O. F. G. E. M. C. Guerrero, E. Berthoumieux and S. Andriamonje, "A new set-up for the simultaneous measurement of neutro-induced capture and fission reactions," *in Proceedings of the 2nd International Conference on Advancements in Nuclear Instrumentation Measurement Methods and Their Applications (ANIMMA'11), Ghent, Belgium*, June 2011.

[73] I. D. e. a. I. Bolshakova, V. Chekanov, "Methods and instrumentation for investigating hall sensors during their irradiation in nuclear research reactors," *in Proceedings of the 1st International Conference on Advancements in Nuclear Instrumentation, Measurement Methods and Their Applications (ANIMMA'09), Marseille, France,*, June 2009.

[74] R. I. Scherpelz and J. E. Tanner, "Neutron measurements at nuclear power reactors," *Nuclear Instruments and Methods in Physics Research A*, vol. 476, 2002.

[75] A. L. e. a. D. Fourmentel, J.-F. Villard, "Combined analysis of neutron and photon flux measurements for the jules horowitz reactor core mapping," *in Proceedings of the 2nd International Conference on Advancements in Nuclear Instrumentation, Measurement Methods and Their Applications (ANIMMA'11)*, Ghent, Belgium, June 2011.

[76] H. G. Brixy, "Temperature measurement in nuclear reactors by noise thermometry," *Nuclear Instruments and Methods*, vol. 97, 1971.

[77] T. Bily and L. Sklenka, "Neutronic design of instrumentation for thermal effects measurement on vr-1 reactor," *in Proceedings of the 1st International Conference on Advancements in Nuclear Instrumentation, Measurement Methods and Their Applications (ANIMMA'09), Marseille, France*, June 2009.

[78] J. E. D. e. a. J. L. Rempe, D. L. Knudson, "Enhanced in-pile instrumentation at the advanced test reactor," *in Proceedings of the 2nd International Conference on Advancements in Nuclear Instrumentation, Measurement Methods and Their Applications (ANIMMA'11), Ghent, Belgium*, June 2011.

[79] M. C. e. a. A. Porta, V. M. Bui, "Reactor neutrino detection for non-proliferation with the nucifer experiment," *IEEE Transactions on Nuclear Science*, vol. 57, 2010.

[80] D. F. J. F. Villard, S. Fourrez and A. Legrand, "Improving high-temperature measurements in nuclear reactors with mo/nb thermocouples," *International Journal of Thermophysics*, vol. 29, 2008.

[81] B. B. G. Cheymol and J. F. Villard, "Fibre optics for metrology in nuclear research reactors applications to dimensional measurements," *in Proceedings of the 1st International Conference on Advancements in Nuclear Instrumentation, Measurement Methods and Their Applications (ANIMMA'09), Marseille, France*, June 2009.

[82] R. from, "Nuclear power for everybody," *www.nuclear-power.net/nuclear-power/reactor-physics/atomic-nuclear-physics/radiation/shielding-of-ionizing-radiation/.*

[83] D. W. D. L. E. O. Rea, S. P. and J. McConnell, "Emi shielding of woven carbon flbre composites," *IEEE High Frequency Postgraduate Student Colloquium, 205-210, UMIST, Manchester, UK*, Sep. 6-7, 2004.

[84] S. P. R. E. O. Ding, J. and J. McConnell, "Mixture properties of carbon fibre composite materials for electronics shielding in systems packaging," *Electronics System-Integration Technology Conference*, Sep. 5-7, 2006.

[85] S. Kahane and R. Moreh, "Optimizing the teflon thickness for fast neutron detection using a ge detector," *Department of Physics, Ben-Gurion University, 84120, Beer-Sheva, Israel*, vol. 13, August 2017.

[86] Q. W. T. W. Mei Lv, Fei Zheng and Y. Liang., "Surface structural changes, surface energy and antiwear properties of polytetrafluoroethylene induced by proton irradiation, mater," *Nucl. Instrum. Methods Phys*, vol. 85, 2015.

[87] T. M. A. S. T. T. Akane Kitamura, Tomohiro Kobayashi, “Control of cell behaviour on ptfe surface using ion beam irradiation,” *Nucl. Instrum. Methods Phys*, 2009.

[88] A. G. Z. Y. Shuling Liu, Congli Fu, “Structural changes of polytetrafluoroethylene during irradiation in oxygen,” *Radiat. Phys.*, vol. 109, 2015.

Appendix A

MATLAB code explanation

MATLAB code

```
t = 0:0.00001:0.001;
% we've taken 5 carrier frequencies Fc1 = 1000, Fc2 = 2000, Fc3 = 3000, Fc4=4000 & Fc5
= 5000
% keeping the user message/data signal frequency as 1000.
Fc1 = 1000;
Fc2 = 2000;
Fc3 = 3000;
Fc4 = 4000;
Fc5 = 5000;
Fs = 12000;
y1 = 1; y2 = 0; y3 = 0; y4 = 0; y5 = 0; Y = 0; y = 0;
x1 = cos(2*pi*1000*t); % every user's base band data signal
% once user 1's data arrive, it is modulated at the first carrier Fc1, similarly as the 2nd user's
% data arrives; it is modulated at the 2nd carrier Fc2, so on till fifth user is assigned the Fc5
% band. If any user's data isn't present his frequency band remains empty which is called a
Spectral Hole. in_p = input('\nDo you want to enter first primary user Y/N: ','s');
if(in_p == 'Y' || in_p == 'y')
y1 = ammod(x1,Fc1,Fs);
end
in_p = input('Do you want to enter second primary user Y/N: ','s');
if(in_p == 'Y' || in_p == 'y')
y2 = ammod(x1,Fc2,Fs);
end
```

in_p = input('Do you want to enter third primary user Y/N: ','s');
if(in_p == 'Y' || in_p == 'y')
y3 = ammod(x1,Fc3,Fs);
end
in_p = input('Do you want to enter fourth primary user Y/N: ','s');
if(in_p == 'Y' || in_p == 'y')
y4 = ammod(x1,Fc4,Fs);
end
in_p = input('Do you want to enter fifth primary user Y/N: ','s');
if(in_p == 'Y' || in_p == 'y')
y5 = ammod(x1,Fc5,Fs);
end
% once all the assignment is complete we add all the signals to create a carrier signal which will be analyzed for empty slots as the channel.
y = y1 + y2 + y3 + y4 + y5;
while(1)
% Now we'll estimate the power spectral density of our carrier signal using the periodogram();
% function and the values are stored in an array Pxx. Pxx is the distribution of power per unit frequency. This value is then stored in a dsp data object and then plotted.
Pxx = periodogram(y);
Hpsd = dspdata.psd(Pxx,'Fs',Fs);
plot(Hpsd);
in_p = input('\nDo you want to enter another primary user Y/N: ','s');
if(in_p == 'Y' || in_p == 'y')
tp=0;
% we've obtained five points for all users in the array Pxx which multiplied by 10000 should be
% above 8000 if there's no spectral hole. //this just an observation which is working so far, the
% technical aspects will be addressed later in the presentation.
chek1 = Pxx(25)*10000;
chek2 = Pxx(46)*10000;
chek3 = Pxx(62)*10000;
chek4 = Pxx(89)*10000;
chek5 = Pxx(105)*10000;
% now if there is a new user entering the channel, we'll check the array Pxx, at certain

location and assign user the first spectral gap as coded below
if(chek1 < 8000)
disp('Assigned to User 1 as it was not present.');
y1 = ammod(x1,Fc1,Fs);
elseif (chek2 < 8000)
disp('Assigned to User 2 as it was not present.');
y2 = ammod(x1,Fc2,Fs);
elseif(chek3 < 8000)
disp('Assigned to User 3 as it was not present.');
y3 = ammod(x1,Fc3,Fs);
elseif(chek4 < 8000)
disp('Assigned to User 4 as it was not present.');
y4 = ammod(x1,Fc4,Fs);
elseif(chek5 < 8000)
disp('Assigned to User 5 as it was not present.');
y5 = ammod(x1,Fc5,Fs);
else
disp('all user slots in use. try again later,');
tp=1;
end
figure
y = y1 + y2 + y3 + y4 + y5 ;
Pxx = periodogram(y);
Hpsd = dspdata.psd(Pxx,'Fs',Fs);
plot(Hpsd);
if(tp==1)
% then we've the slot emptying algorithm which will empty the already occupied bands by
% asking user to choose a slot and executing the following code.
inp_t=input('Do you want to empty a slot: ','s');
if(inp_t=='Y'||inp_t=='y')
inp_t=input('Which slot do you want to empty for your entry: ','s');
switch(inp_t)
case ('1')
y1=0;
disp('slot1 is fired');
y = y1 + y2 + y3 + y4 + y5;

```
Pxx = periodogram(y);
Hpsd = dspdata.psd(Pxx,'Fs',Fs);
plot(Hpsd);
case('2')
y2=0;
disp('slot2 is fired');
y = y1 + y2 + y3 + y4 + y5;
Pxx = periodogram(y);
Hpsd = dspdata.psd(Pxx,'Fs',Fs);
plot(Hpsd);
case('3')
y3=0;
disp('slot3 is fired');
% then we repeat the above plotting procedure that was done after the assignments.
% To add noise to our signal I've used the simpler awgn(); function.
y = y1 + y2 + y3 + y4 + y5;
Pxx = periodogram(y);
Hpsd = dspdata.psd(Pxx,'Fs',Fs);
plot(Hpsd);
case('4')
y4=0;
disp('slot4 is fired');
y = y1 + y2 + y3 + y4 + y5;
Pxx = periodogram(y);
Hpsd = dspdata.psd(Pxx,'Fs',Fs);
plot(Hpsd);
case('5')
y5=0;
disp('slot5 is fired');
y = y1 + y2 + y3 + y4 + y5;
Pxx = periodogram(y);
Hpsd = dspdata.psd(Pxx,'Fs',Fs);
plot(Hpsd);
otherwise disp('Invalid slot entered');
end
end
```

```
end
inp_t=input('Do you want to add noise: ','s');
if(inp_t=='y'||inp_t=='Y')
d = input('Enter the SNR in dB: ');
figure
Y = awgn(y,d);
Pxx1 = periodogram(Y);
Hpsd = dspdata.psd(Pxx1,'Fs',Fs);
plot(Hpsd);
end
% to attenuate our signal the system asks for the percentage of attenuation required followed
% by the plot of the attenuated carrier signal. The percentage divided by hundred is subtracted
% from 1 and the remaining number is multiplied with the signal.
temp = input('Do you want to attenuate the signals? [Y/N]: ','s');
if(temp == 'Y' || temp == 'y')
aF = input('Enter the percentage to attenuate the signal: ');
figure
tem = aF/100;
tm = 1-tem;
Z = y.*tm;
disp('attenuating');
grid;
plot(Z);
Pxx4 = periodogram(Z);
Hpsd = dspdata.psd(Pxx4,'Fs',Fs);
plot(Hpsd);
end
end
temp = input('Do you want to re-run the program? [Y/N]: ','s');
if(temp == 'Y' || temp == 'y')
disp('\n\nEnter the users again.\n\n');
else
break;
end
end
```