ECE4305: Software-Defined Radio Systems and Analysis

Laboratory 4: Spectrum Sensing Techniques

C-Term 2011

Objective

With advanced digital communication systems such as *cognitive radio* being used in a growing number of wireless applications, the topic of spectrum sensing has become increasingly important. This laboratory will introduce the concept, fundamental principles, and practical applications of spectrum sensing. In the experimental part of this laboratory, you will implement two different primary signal detectors and then observe their performance during over the air transmission. This is followed by a Simulink implementation of those two detectors. Finally, the open-ended design problem will focus on a commonly-used form of wireless access scheme referred to as *carrier sense multiple access with collision avoidance* (CSMA/CA).

Contents

1 Theoretical Preparation

Spectrum sensing is a radio process for determining whether a signal is present across a specified RF bandwidth. This process has many applications and usages, including *dynamic spectrum access networks*, which are designed to maximize spectrum efficiency and capacity within congested wireless transmission environments. Dynamic spectrum access temporarily utilizes spectral white spaces in order to transmit data. What this means is that if a licensed (primary) user is allocated a predetermined frequency to operate on, an unlicensed (secondary) user can temporarily "borrow" the unoccupied spectrum for transmission.

In a system consisting of many primary users and secondary users, the secondary users need to be able to jump into and utilize the unused spectrum of the primary users as it becomes available. In order to accomplish this action, spectrum sensing techniques are employed to avoid spectral collisions. This laboratory discusses both energy detection and cyclostationary feature detection, and goes into detail about energy detectors.

1.1 Power Spectral Density

To analyze a signal in the frequency domain, the power spectral density (PSD), $S_x(f)$, is often used to characterize the signal, which is obtained by taking the Fourier Transform of the autocorrelation $R_x(\tau)$ of the signal $X(t)$. The PSD and the autocorrelation of a function, $R_x(\tau)$, are mathematically related by the Einstein-Wiener-Khinchin (EWK) relations, namely:

$$S_x(f) = \int_{-\infty}^{\infty} R_x(\tau) e^{-j2\pi f\tau}\, d\tau \tag{1}$$

$$R_x(f) = \int_{-\infty}^{\infty} S_x(\tau) e^{+j2\pi f\tau}\, df \tag{2}$$

Using the EWK relations, we can derive some general properties of the power spectral density of a stationary process, such as:

- $S_x(0) = \int_{-\infty}^{\infty} R_x(\tau) d\tau$
- $E\{X^2(t)\} = \int_{-\infty}^{\infty} S_x(f) df$
- $S_x(f) \geq 0$ for all f
- $S_x(-f) = S_x(f)$
- The power spectral density, appropriately normalized, has the properties usually associated with a probability density function:

$$p_x(f) = \frac{S_x(f)}{\int_{-\infty}^{\infty} S_x(f) df} \tag{3}$$

Using $H(f)$ to denote the frequency response of the system, we can relate the power spectral density of input and output random processes by the following equation:

$$Y(f) = |H(f)|^2 X(f), \tag{4}$$

where $X(f)$ is the PSD of input random process and $Y(f)$ is the PSD of output random process.

1.2 Collecting Spectral Data

Although spectrum sensing is a rather intuitive process, its implementation possesses several engineering trade-offs. One of the key considerations when designing a spectrum sensing system is how to collect and store spectrum measurements via a spectrum sweep.

A spectrum analyzer can be employed to provide an instantaneous snapshot of a bandwidth via the sampling of intercepted signals at some rate. Considerations when parameterizing a spectrum sweep include the *sweep time* and *sweep resolution*, *i.e.*, the speed and detail at which the spectrum sweeps are obtained. Higher resolution sweeps result in much longer sweep times, but provide a much more accurate estimate of the spectrum. The sweeps used later in this laboratory are the average of thousands of spectrum sweeps of a single bandwidth. This process can take minutes to hours depending on the frequency resolution of the sweep. Figure 1 shows the PSD of a pulse shaped QPSK signal collected by the spectrum analyzer.

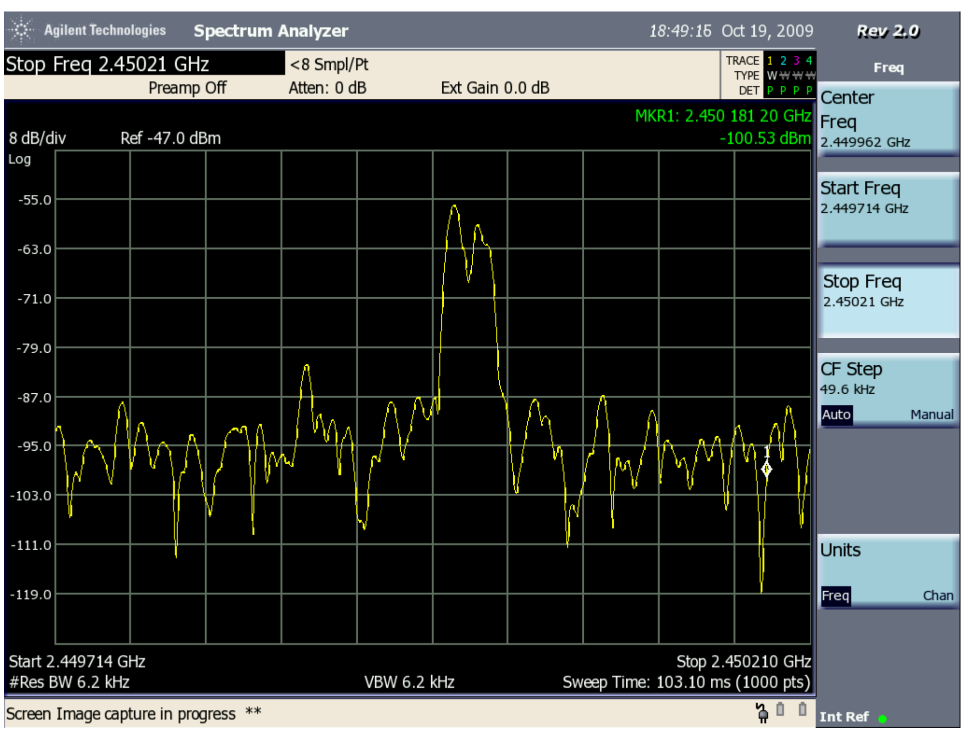


Figure 1: Power Spectral Density of a Pulse Shaped QPSK Signal.

1.3 Primary Signal Detection

In this laboratory, we discuss the detection of wireless signals, which constitutes the basic step in 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:

$$\mathcal{H}_0 \quad \text{(idle)} \quad \text{vs.} \quad \mathcal{H}_1 \quad \text{(busy)} \ . \tag{5}$$

Under the idle scenario, the received signal is essentially the ambient noise in the RF environment, and under the busy scenario, the received signal would consist of the PU signal and the ambient noise. Thus, this yields the following mathematical representation:

$$\begin{aligned} \mathcal{H}_0 : &\quad y(k) = w(k) \\ \mathcal{H}_1 : &\quad y(k) = s(k) + w(k) \end{aligned}$$

for $k = 1, .., n$, where n is the number of received samples, $w(k)$ represents ambient noise, and $s(k)$ represents the PU signal. Intuitively, the received signal will have more energy when the channel is busy than when it is idle, thus forming the underlying concept in the energy detector which we discuss in detail in Section 1.3.1. When aspects of the signal structure are known one can exploit the structure; a special case leads to the cyclostationary detector discussed in Section 1.3.2.

Regardless of the precise signal model or detector used, sensing errors are inevitable due to additive noise, limited observations, and the inherent randomness of the observed data. False alarms (Type I errors) occur if an idle channel is detected as busy. On the other hand, missed detections (Type II errors) occur when a busy channel is detected as idle. Consequently, a false alarm may lead to a potentially wasted opportunity for the SU to transmit while a missed detection could potentially lead to a collision with the PU, leading to wasted transmissions for both PU and SU.

The performance of a detector is characterized by two parameters, the *probability of missed detection* (P_{MD}) and the *probability of false alarm* (P_{FA}), which are defined as:

$$\begin{aligned} \epsilon &= P_{FA} = \text{ Prob } \{\text{Decide } \mathcal{H}_1 | \mathcal{H}_0\}; \\ \delta &= P_{MD} = \text{ Prob } \{\text{Decide } \mathcal{H}_0 | \mathcal{H}_1\} \ . \end{aligned}$$

A typical *receiver operating characteristic* (ROC), which is a plot of $1-\delta$, the probability of detection (P_D), versus P_{FA}, is shown in Figure 2.

To motivate the practical aspects of spectrum sensing in the latest wireless communication standards, the proposed sensing requirements of the IEEE 802.22 Wireless Regional Area Network (WRAN) standard are summarized in Table 1 [8, 2].

[1] In this situation, we refer to the "channel" in a general sense, where it represents a signal dimension (time, frequency, and code, etc.) that can be allocated to a particular user.

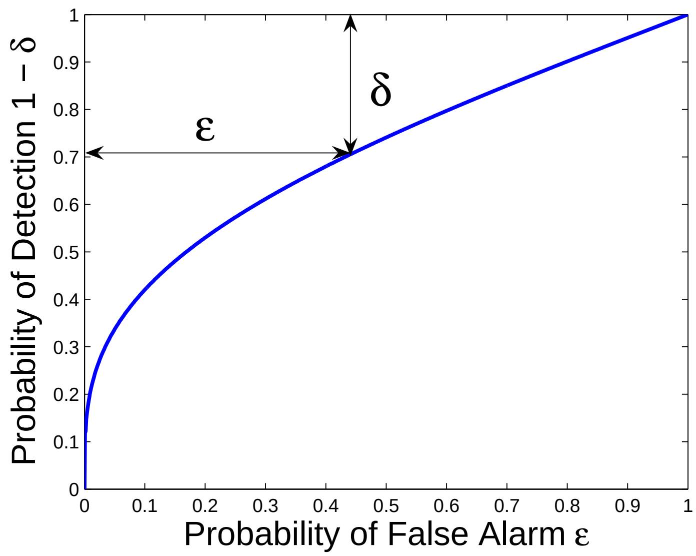


Figure 2: Typical receiver operating characteristic.

1.3.1 Energy Detector

Energy detection uses the energy spectra of the received signal in order to identify the frequency locations of the transmitted signal.

Energy detection approach relies only on the energy present in the channel. Since the energy of a signal is defined as $\int_{\infty}^{\infty} |f(t)|^2 dt$, no phase information is required. The underlying assumption is that with the presence of a signal in the channel, there would be significantly more energy than if there was no signal present. Therefore, energy detection involves the *application* of a threshold in the frequency domain, which is used to decide whether a transmission is present a specific frequency, as shown in Figure 3. Any portion of the frequency band where the energy exceeds the threshold is considered to be occupied by a transmission.

Since different transmitters employ different signal power levels and transmission ranges, one of the

Table 1: Sensing Requirements in the IEEE 802.22 draft standard.

Parameter	Digital TV	Wireless Microphone (Part 74)
Channel Detection Time	$\leq$ 2 sec	$\leq$ 2 sec
Channel Move Time	2 sec	2 sec
Detection Threshold (required sensitivity)	- 116 dBM (over 6 MHz)	- 107 dBm (over 200 KHz)
Probability of detection	0.9	0.9
Probability of false alarm	0.1	0.1
SNR	- 21 db	- 12 dB

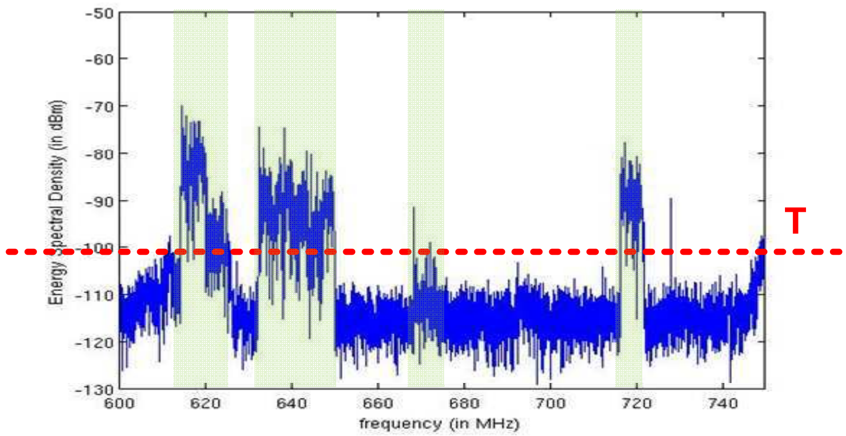


Figure 3: Energy detection threshold level, denoted as red T. Any portion of the frequency band where the energy exceeds the threshold is considered to be occupied by a transmission.

major concerns of energy detection is the selection of an appropriate threshold. A threshold that may work for one transmission may not be sufficient for another. Figure 5 shows two typical detection errors caused by inappropriate energy detection threshold. In Figure 4(a), the threshold is too low, so some noise is considered as primary signal, resulting in false alarm. While in Figure 4(b), the threshold is too low, so some primary signals are ignored, incurring the missed detection.

1.3.2 Cyclostationary Feature Detector

Cyclostationary feature detection relies upon periodic redundancy introduced into a signal by sampling and modulation. It uses the non-random periodic statistics of these signals to detect and possibly even classify a signal of interest. Cyclic detection is a robust spectrum sensing technique since it relies on what are called cyclostationary processes.

A random process is cyclostationary if its mean and autocorrelation vary periodically in time. Modulated information is a cyclostationary process, while noise is not. As a result, cyclic detectors can successfully operate in extremely low SNR environments.

A cyclic detector operates by calculating the cyclic autocorrelation function (CAF) given by:

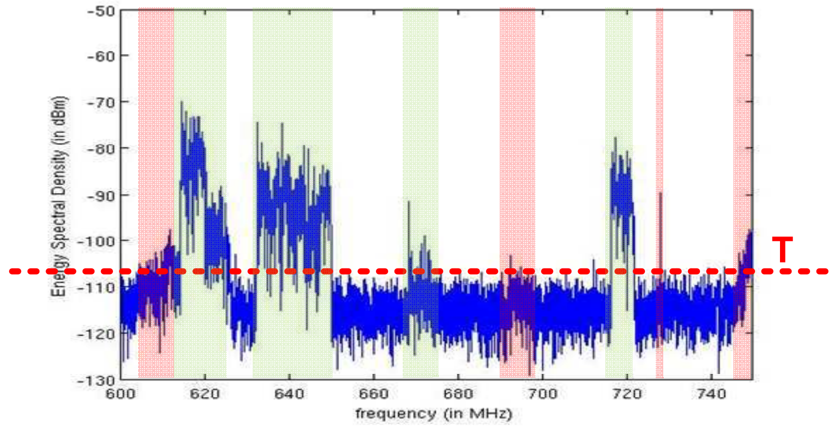
$$R_x^\alpha(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_T x\left(t+\frac{\tau}{2}\right) x^*\left(t-\frac{\tau}{2}\right) e^{-j2\pi\alpha t}\, dt. \tag{6}$$

The Fourier transform of the CAF, which is equal to the spectral correlation function (SCF), is given by:

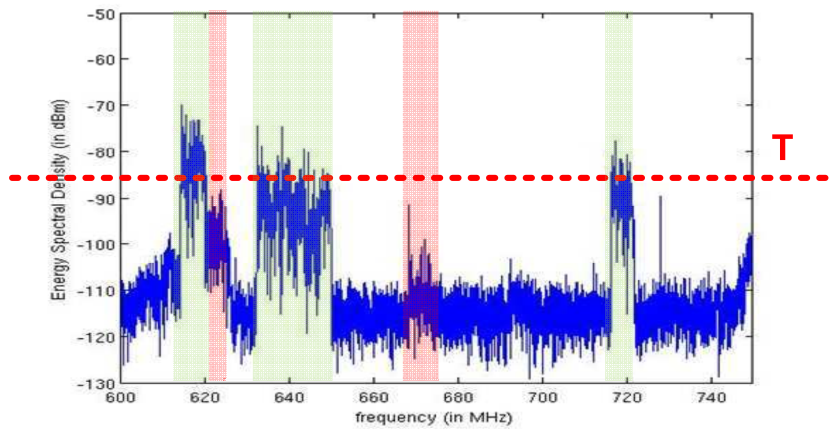
$$S_x^\alpha(f) = \int_{-\infty}^{\infty} R_x^\alpha(\tau) e^{-j2\pi f\tau} d\tau. \tag{7}$$

To derive a normalized version of the SCF, the spectral coherence function (SOF) is given by:

$$C_X^\alpha(f) = \frac{S_X^\alpha(f)}{[S_X^0(f+\alpha/2)\times S_X^0(f-\alpha/2)]^{1/2}}. \tag{8}$$



(a) Energy detection threshold level yielding *false alarms*.



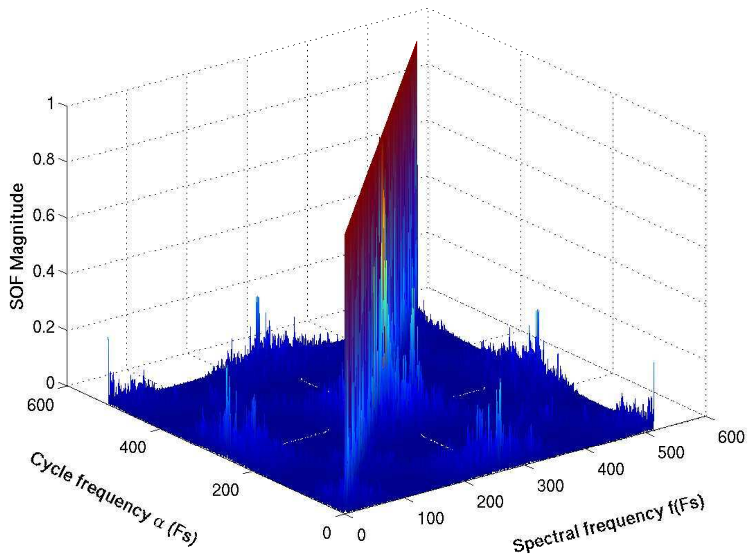
(b) Energy detection threshold level yielding *missed detection*.

Figure 4: Inappropriate energy detection threshold levels.

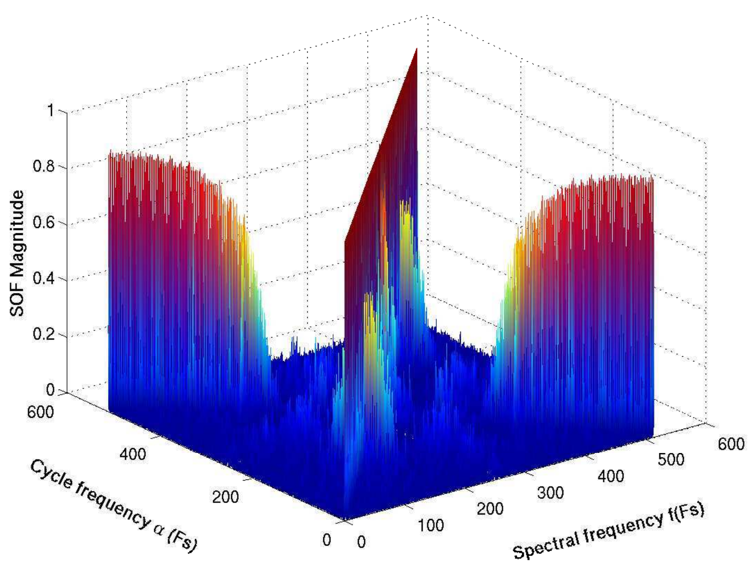
From this equation, it extracts the cyclic features of the signal. Different modulation schemes have different features. In fact, the difference between some modulation schemes is so distinct that these profiles can be used to accurately classify the physical layer parameters of the signal.

The magnitude of the SOF varies from "0" to "1" and represents strength of second order periodicity within the signal. The SOF contains the spectral features of interest. These features are non-zero frequency components of the signal at various cyclic frequencies. All modulation schemes contain a range of spectral components at different cyclic frequencies, thus distinguishing them from other modulation schemes, *i.e.*, the spectral components form a spectral fingerprint for the specific modulation scheme. The SOFs of two typical modulation schemes, QPSK and 4PAM, are shown in Figure 5(a) and Figure 5(b). Notice how the SOF for each modulation scheme generates a highly distinct spectral image. These distinctions allow signals to be classified from cyclic analysis.

Cyclostationary feature detector is easily implemented via FFTs. Knowledge of the noise variance is not required to set the detection threshold. Hence, the detector does not suffer from the "SNR wall" problem of the energy detector. However, the performance of the detector degrades in the presence of timing and frequency jitters (which smear out the spectral lines), and RF non-linearities (which



(a) SOF of QPSK signal in an AWGN channel at 10 dB SNR.



(b) SOF of 4PAM signal in an AWGN channel at 10 dB SNR.

Figure 5: Distinctive cyclic features of different modulation schemes.

induce spurious peaks). Representative papers that consider the approach are [1, 4, 6].

1.4 Suggested Readings

Although this laboratory handout provides some information about the spectrum sensing techniques, the reader is encouraged to review the material from the following references in order to gain further insight on these topics.

- Overview of Primary Signal Detection
  - Section 4.2 in [9]
- Overview of Cyclostationary Detection
  - Section 2.2 in [5]
- Introduction to Higher Order Cyclostationary Detection
  - Section 2.3 in [5]

1.5 Problems

1. Calculate and plot the PSD of a 100MHz sinusoidal tone. How would you expect this to look on a spectrum analyzer?

2. Consider the problem of detecting between two real Gaussian random variables with means μ_i and variance σ_i^2, $i = 0, 1$. Show that the P_{FA} is given by $\text{P}(Z > \tau | \mathcal{H}0) = Q(\frac{\tau - \mu_0}{\sigma_0})$, where $Q(\tau) := \frac{1}{\sqrt{2\pi}} \int_\tau^\infty e^{-t^2/2} dt$ is the standard Gaussian tail function.

3. If x(t) is wide-sense cyclostationary, its mean and autocorrelation are periodic. Express $R_x(t - \frac{\tau}{2}, t + \frac{\tau}{2})$ as a Fourier series. If x(t) is cyclostationary, what does that imply about frequency components at m/T_0, where m is an integer?

4. Given Eq. (6) and using the Einstein-Wiener-Khintchine (EWK) relation, derive the spectral autocorrelation function of a wide sense cyclostationary process.

2 Software Implementation

2.1 Spectrum Sensing using Energy Detection

2.1.1 Signal Generation

The first step of this experiment is to generate signals belonging to different families of modulation schemes. This is done in order to highlight how certain modulation schemes can vary spectrally while others possess similar characteristics.

Open the `datagen.mdl` file available on the course website, as shown in Figure 6.

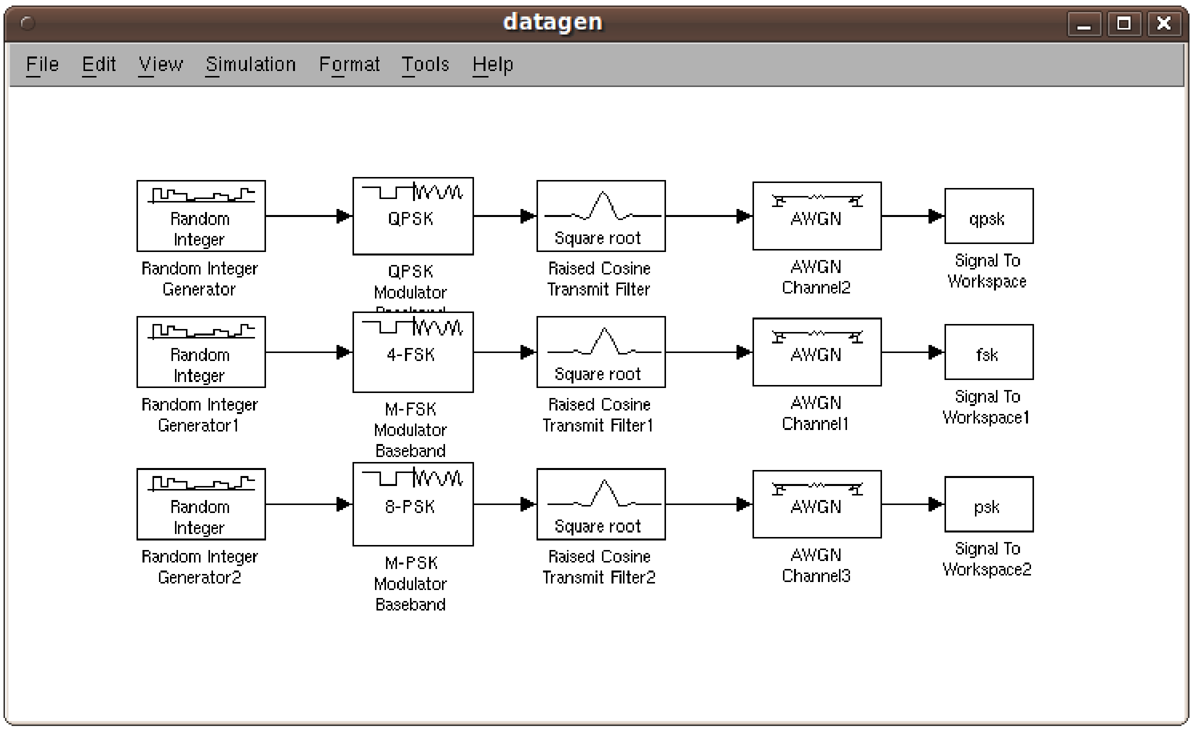


Figure 6: Data generation model.

This model features three very basic modulation schemes that are pulse shaped for over the air transmission. Vectors of each transmission are saved to the MATLAB workspace.

Run the model once and go to the MATLAB workspace. Begin by observing the output of each channel on an `fftscope` block. Next vary the SNR of the channel. At what point does the signal become unobservable due to noise?

2.1.2 Energy Detector Construction

We will now proceed with the construction of a simple energy detector that analyzes the signals in the workspace and determines whether or not a signal is present based on a threshold. Recall that an energy detector uses the energy spectra of the received signal in order to identify the frequency

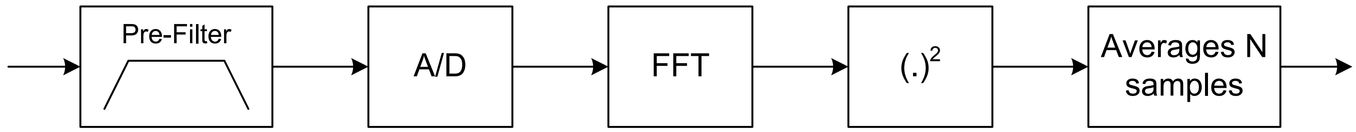


Figure 7: Schematic of an energy detector implementation employing pre-filtering and a square-law device.

locations of the transmitted signal. As a result, the following steps that are also illustrated in Figure 7 will assist in producing the frequency representation of the intercepted signal.

1. *Pre-filtering* of intercepted signal extracts frequency band of interest.
2. *Analog-to-digital conversion* (ADC) converts filtered intercepted signal into discrete time samples.
3. *Fast Fourier transform* (FFT) provides the frequency representation of the signal.
4. *Square-law device* yields the square of the magnitude of the frequency response from the FFT output.
5. *Average* N samples of the square of the FFT magnitude.

Please note that the first two steps depend on the software-defined radio equipment itself and is not under your control.

2.1.3 Energy Threshold Selection and Hypothesis Testing

To perform the actual energy detection, we need to apply a threshold in the frequency domain, which is used to decide whether a transmission is present a specific frequency. As a result, any portion of the frequency band where the energy exceeds the threshold is considered to be occupied by a transmission since energy detection is a binary decision making process consisting of two hypotheses: $\mathcal{H}_0$ (idle) or $\mathcal{H}_1$ (occupied). However, one of the primary challenges of energy detection is the selection of an appropriate threshold. This is due to the fact that the threshold may work for one transmission but may not be sufficient for another since the transmitters might be employing different signal power levels or the transmission ranges may vary altogether.

Since Simulink only supports baseband modulation, we will need to implement all of the signals at baseband as well. We will now conduct a series of ten trials across a range of SNR values. For each trial:

1. Compute the probability of false alarm (the number of times we incorrectly say that there is a signal present, when in fact there isn't).
2. Compute the probability of missed detection (the number of times we did not find the signal).
3. What threshold values did you employ in your energy detection implementations?

Which modulation scheme is most often detected? Which modulation scheme is most often not detected?

2.2 Understanding Cyclostationary Detectors

Let us now examine the spectral coherence of the three signals generated in the previous Section 2.1.1. The spectral coherence is a measure of the correlation between each cyclic frequency and ranges in magnitude from 0 to 1. High coherence terms indicate some periodicity within the signal being examined. Reset the parameters of each channel in `datagen.mdl` to the following:

SNR: 100 dB
β: 0.5

Run the model and open `cyclic.m`, use the following lines of code for the QPSK (qpsk), FSK (fsk), and PSK (psk) signals:

```
[SCF Cx] = cyclic(qpsk);
Cxplot = surf(abs(Cx));
set(Cxplot, 'edgecolor','interp');
```

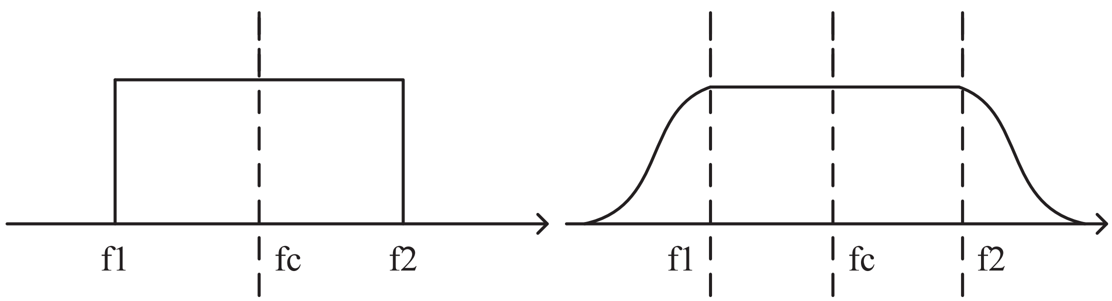
Using this code, answer the following questions:

1. Generate an AWGN vector and plot its coherence. Does this plot support the conclusion that cyclic detectors are robust to Gaussian noise? Why?
2. Why might cyclic detectors be susceptible to frequency selective fading?
3. Adjust the roll-off factors of the pulse shaping filters and re-examine the coherence functions. What effect does the excess bandwidth have on the effectiveness of the detector?

3 USRP2 Hardware Experimentation

In Simulink, the frequency range you can observe using the spectrum scope is limited. If you want to consider a communication system over a wideband channel, you can divide that channel into K narrowband subchannels. In this section, you will implement a wideband spectrum sensing using two types of "sliding window". Please perform the following tasks:

- Step 1: Take the Simulink design of energy detection from Section 2.1.2 and incorporate into it the USRP2 receiver block.
- Step 2: Develop a "sliding window" approach to the energy detection spectrum sensing implementation from Step 1 such that it can cover a wide frequency band, such as 200 MHz. Use two types of windows, namely,
  - A *rectangular window*, as shown in Figure 8(a).
  - A *tapered window* such as a Hamming window [3], as shown in Figure 8(b).



(a) Rectangular window. (b) Hamming window.

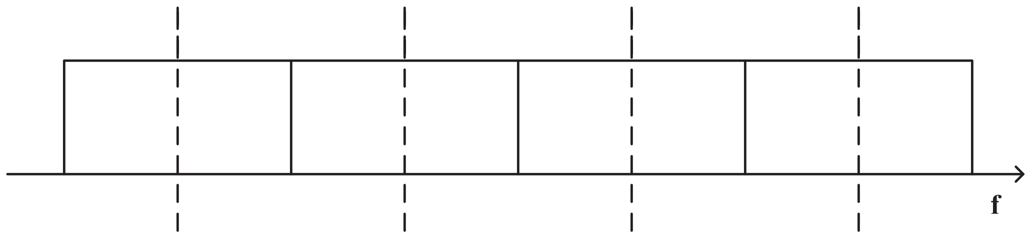
Figure 8: Two types of windows.

  The goal is to sweep individual segments of a much wider frequency range using these two types of windows, and then post-process them into a single frequency sweep result, as shown in Figure 9. One of the advantages of tappered windows is that they have gradual transitions between bands.

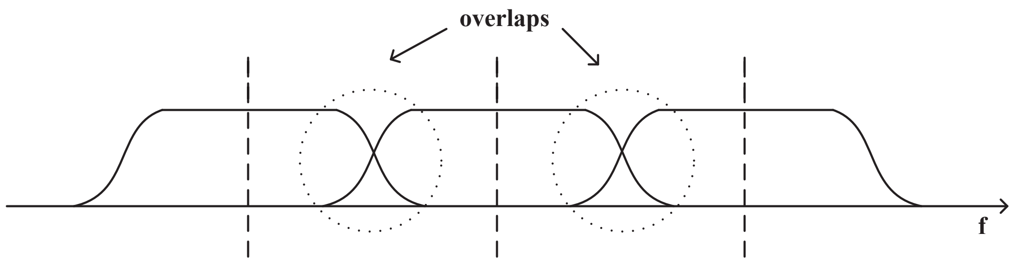
- Step 3: Apply the two types of multi-band spectrum sensing approaches for 5.1 GHz to 5.3 GHz and repeat 25 times. Average the result of both approaches. What do you observe?
- Step 4: Now transmit a sinusoidal signal in that frequency range and perform the test again. Do you see the sinusoidal signal?

Please answer the following questions:

- How long does it take to sweep 200 MHz of spectrum?
- Is there a relationship between sweep time, FFT size, and frequency resolution?
- What do you notice about the quality of your spectrum sweep when you average more sweeps?



(a) A single frequency sweep result using rectangular window.



(b) A single frequency sweep result using Hamming window. Note there are overlaps in transition areas.

Figure 9: A single frequency sweep result from two types of windows.

- What is the impact of the individual window size when sweeping a large frequency band?
- Is it possible to obtain the frequency response of a wideband spectral range using a single FFT and no windowing? If yes, is there a trade-off with frequency resolution? If no, please explain the reason.

4 Open-ended Design Problem: CSMA/CA

4.1 Carrier Sense Multiple Access

Carrier sense multiple access (CSMA) is a probabilistic media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus, or a band of the electromagnetic spectrum [7]. CSMA is composed of two logically defined components:

- *Carrier sense* describes the fact that a transmitter uses feedback from a receiver that detects a carrier wave before trying to send. That is, it tries to detect the presence of an encoded signal from another station before attempting to transmit. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission.
- *Multiple access* describes the fact that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations using the medium.

4.2 Collision Avoidance Variant

Carrier sense multiple access with collision avoidance (CSMA/CA) is a variant of CSMA. Collision avoidance is used to improve CSMA performance by not allowing wireless transmission of a node if another node is transmitting, thus reducing the probability of collision due to the use of a random binary exponential backoff time.

In this protocol, a carrier sensing scheme is used, namely, a node wishing to transmit data has to first listen to the channel for a predetermined amount of time to determine whether or not another node is transmitting on the channel within the wireless range. If the channel is sensed "idle", then the node is permitted to begin the transmission process. If the channel is sensed as "busy", the node defers its transmission for a random period of time. A simple example of CSMA/CA is shown in Figure 10, where Node 1 wants to transmit, but the channel is sensed as "busy", so Node 1 defers its transmission for 5 slots.

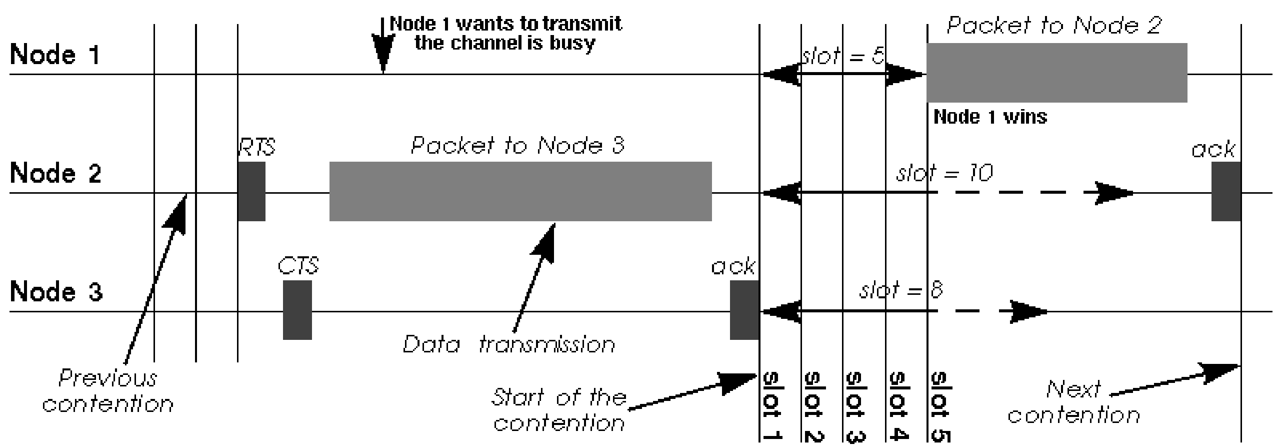


Figure 10: An example of a 3-node communication system employing CSMA/CA protocol.

4.3 Implementation Approach

In this laboratory, you are required to implement a communication system consisting of two transceivers (Radio 1 and Radio 2). These two radios are sharing a common communication channel and they are using CSMA/CA protocol. Since they are transceivers, they can swithch between *transmit* and *receive* modes. You can define the duration of each mode.

Your system should perform the following three stages, as shown in Figure 11:

- Stage 1:
  - Radio 1 is in *transmit* mode. It switches between transmitting a random number of "Hello world" frames and listening for a codeword from Radio 2.
  - Radio 2 does the spectrum sensing using energy detection. If the channel is sensed as "busy", Radio 2 enters a random backoff time. If the channel is sensed "idle", Radio 2 begins to transmit a codeword to Radio 1 and the system enters Stage 2.
- Stage 2:
  - Radio 2 is in the *transmit* mode. It repeats sending a random number of "Change" to Radio 1.
  - Radio 1 is in the *receive* mode and it does the spectrum sensing using energy detection. If the channel is sensed as "busy", Radio 1 keeps receiving the incoming message. If the channel is sensed "idle", Radio 1 begins to decode the message it has received and the system enters Stage 3.
- Stage 3:
  - If Radio 1 can get at least one "Change" in its decoded message, Radio 1 begins to broadcast "Goodbye" and their communication ends.
  - If Radio 1 doen not get any "Change" in its decoded message, the whole system returns to the origin and starts from Stage 1.

4.4 Hints

- Use energy detection to determin whether the channel is idle or busy. You should select an reasonable threshold.
- Implement an exponential random number generator. This is to be used as the backoff time for CSMA/CA protocol while the system is running.
- The number of "Hello world" frames and the number of "change" codewords are also exponential random variables. They can be defined before the system is running.

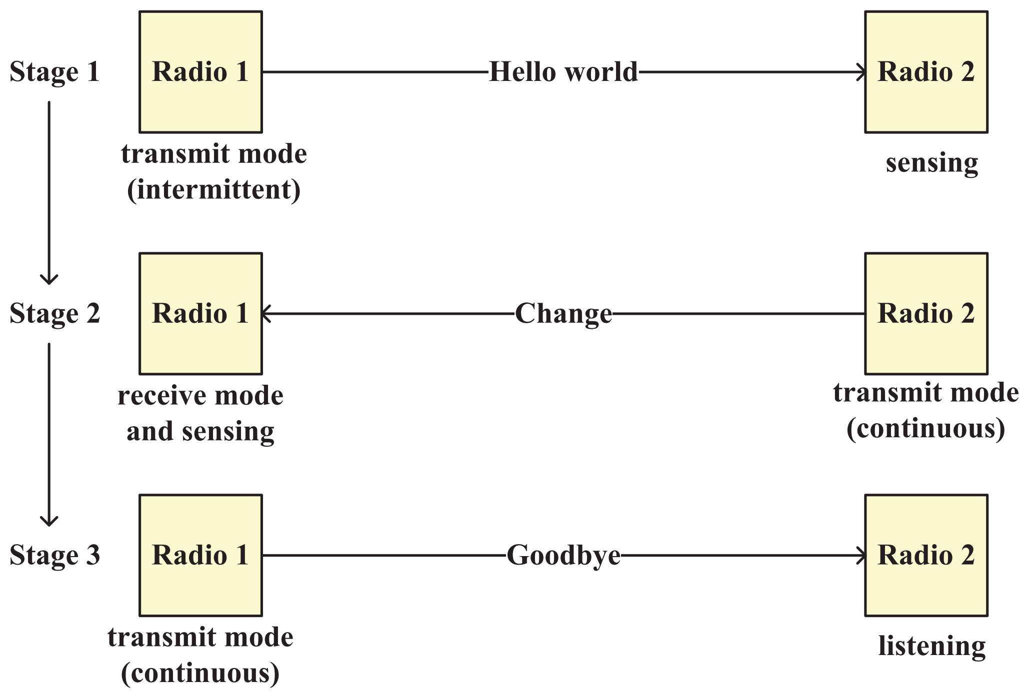


Figure 11: Three stages in CSMA/CA protocol implementation.

5 Lab Report Preparation & Submission Instructions

Include all your answers, results, and source code in a lab report formatted as follows:

- Cover page: includes course number, laboratory title, names and student numbers of team, submission date
- Table of contents
- Pre-lab
- Responses to laboratory questions and explanation of observations
- Responses to open-ended design problem
- Source code

Please include images and outputs wherever possible, as well as insights on your laboratory.

Each group is to submit a single report electronically (in PDF format not exceeding 2MB) to `alexw@ece.wpi.edu` by scheduled due date. Reports that do not meet these specifications will be returned without review.

References

[1] D. Cabric, S.M. Mishra, and R.W. Brodersen. Implementation issues in spectrum sensing for cognitive radios. In *Proceedings of the Asilomar Conference on Signals, Systems and Computers*, November 2004.

[2] C. Cordeiro, K Challapali, D. Birru, and N. Sai Shankar. IEEE 802.22: The first worldwide wireless standard based on cognitive radios. In *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Baltimore, MD, USA, November 2005.

[3] Richard W. Hamming. *Digital Filters*, chapter Windows. Dover Publications, 3rd edition, July 1997.

[4] K. Kim, I.A. Akbar, K.K. Bae, J.-S. Um, C.M. Spooner, and J.H. Reed. Cyclostationary approaches to signal detection and classification in cognitive radio. In *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, Ireland, April 2007.

[5] Eric Like, Vasu D. Chakravarthy, Paul Ratazzi, and Zhiqiang Wu. Signal classification in fading channels using cyclic spectral analysis. *EURASIP Journal on Wireless Communications and Networking*, 2009, 2009.

[6] P.D. Sutton, K.E. Nolan, and L.E. Doyle. Cyclostationary signatures in practical cognitive radio applications. *IEEE Journal on Selected Areas in Communications*, January 2008.

[7] Andrew S. Tanenbaum. *Computer Networks*, chapter The medium access control sublayer. Prentice Hall, 4th edition, August 2002.

[8] U.S. Federal Communications Commission. Fcc et docket-03-122, November 2003.

[9] Qing Zhao and Ananthram Swami. *Cognitive Radio Communications and Networks: Principles and Practice*, chapter Spectrum Sensing and Identification. Elsevier, 2009.