April 2012

Digital Spectrum Sensing for the Localization of Public Safety Responders

Robert Andrew Over
Worcester Polytechnic Institute

Robert Thomas Capizzio
Worcester Polytechnic Institute

Distributed spectrum sensing for the localization of two-way radio transmitters

A Major Qualifying Project
Submitted to the Faculty
of the
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements for the
Degree of Bachelor of Science
by

Robert Capizzio
and
Robert Over

April 2012

Project Sponsor:
The MathWorks Inc.

APPROVED:

Prof. A. Wyglinski, Electrical & Computer Engineering Advisor

---

Prof. M. Fofana, Mechanical Engineering Advisor

MQP-AW1-MW01

Keywords: SDR, Localization,
P25, Characterization, Spectrum Sensing

Abstract

This project has developed a modular sensor network to localize two-way radio transmitters without transmitter cooperation. The sensor network is capable of detecting the spectral location of signals, as well as the transmitting radio's modulation scheme through the use of a matched filter and autocorrelation spectrum sensing scheme. Each receiving node in the sensor network is capable of identifying a signal as an analog FM or Public Safety P25 transmission. After a signal has been identified, the control center attempts to localize the signal based on the received signal strength (RSS). The sensor network collects information about the transmitters in its environment and displays the transmitters center frequency, modulation scheme, and position as outputs on the central controller.

Acknowledgements

We would like to thank Professor Alexander Wyglinski for his support and patience throughout this project. The resources he provided, along with those of his Wireless Innovation Laboratory, were crucial to the projects progress. We would also like to thank Professor Mustapha Fofana for his support at the end of the project, and the members of the Wireless Innovation Laboratory for their suggestions throughout the project. Additionally this project would have been impossible with the support of the MathWorks. By providing the software required to implement the project, and technical support for their newly released packages, they enable the project to get off the ground.

Authorship

This project is the work of Robert Capizzio and Robert Over. As each team member has different strengths in the area of Software Defined Radio, the project was divided between them so that each member could work to their strengths. Robert Over handled the spectrum sensing and signal characterization portions of the project, as he has a greater background in software receiver design. Robert Capizzio was responsible for the localization and system integration due to his experience with Simulink, the USRP2s, and public safety radio systems.

Executive Summary

Public safety responders face increasing challenges when coordinating a response with other supporting agencies. Limited spectrum availability, along with recent advancements in two-way radio technology, has resulted in neighboring organizations using radio systems that are often incompatible. Public safety organizations who may be physically located near each other may be operating on different frequency bands, or using different, incompatible modulation techniques, preventing communication between departments. This project explored the use of Software Defined Radio to create a prototype for a system to detect public safety radio transmissions, determine the appropriate modulation technique required to communicate with that responder, and also determine the location of the responder at the scene.

A Software Defined Radio was selected as the hardware platform for this prototype due to its versatility. Software Defined Radios represent a paradigm shift in communications equipment, with signal processing being performed in software, without the reliance on custom hardware interfaces for each operation. This characteristic allowed the prototype developed for this project to detect and characterize both analog and digital two-way radio transmissions. Additionally, the wide-band frequency coverage provided by the Universal Software Radio Peripheral 2 (USRP2), and the WBX daughtercard allowed the project to perform measurements on all public safety two-way radio bands with a single hardware device.

The project utilizes the USRP2 along with the MathWorks Simulink package to develop the network of sensors that will detect, characterize, and localize transmissions on the VHF and UHF public safety bands. This network consists of three computers equipped

with a USRP2 and a GPS unit, which will make spectral measurements using a time-coordinated search, and transmit these messages of a wired network to a central controller. Each computer equipped with a USRP2 and a GPS unit will perform spectrum sensing operations, in Simulink, in order to locate signals in the frequency domain and characterize them. The central controller, also making use of Simulink, will take the measurements from each receiver, use them to determine a transmitters location, and display the results.

The design of the spectrum sensing prototype for this project combined signal detection and signal characterization in order to both detect and characterize public safety transmissions. The final design of the spectrum sensing prototype for this project was capable of performing reliable sensing and characterization using a combined autocorrelation and matched filter scheme. The main issue that faced the design of the spectrum sensing prototype was the similarity of C4FM transmissions and FM transmissions. Figures A and Figure B show PSD graphs of FM and C4FM signals. Both graphs have very similar spectral features. These figures are so similar that it is impossible to reliably differentiate between them.

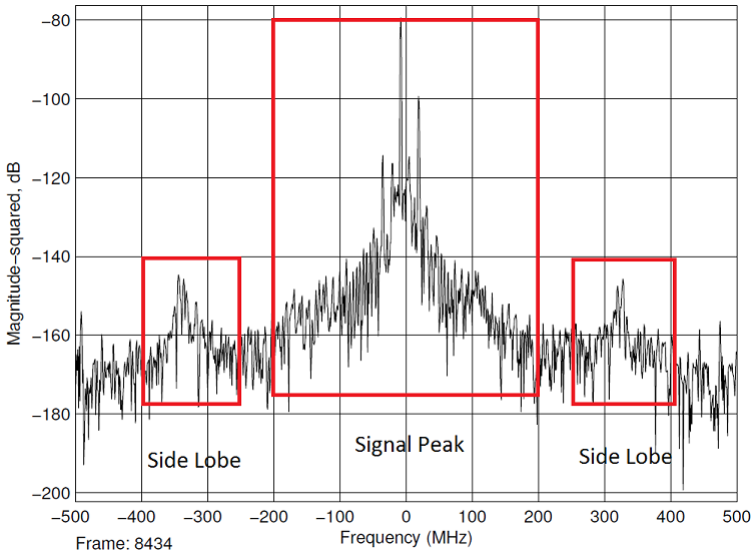


Figure A: Frequency domain PSD of an analog signal. This graph is very similar to the frequency domain PSD of a digital signal shown in Figure B

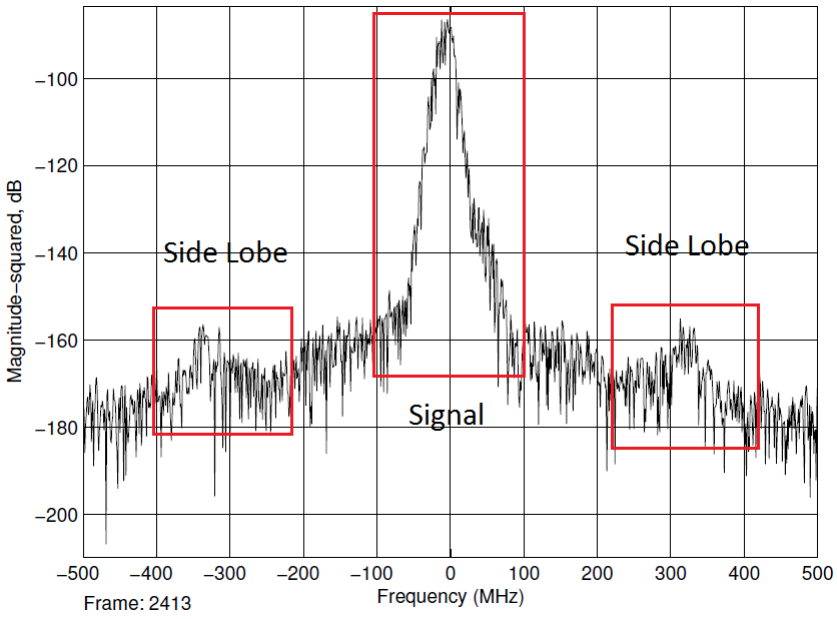


Figure B: Frequency Domain PSD of a digital signal. Figure A and Figure B, both have similar spectral shapes making signal characterization difficult

Two major designs of the project were abandoned due to the challenges presented by FM and C4FM signals, these were matched filtering and power spectral density (PSD) characterization. The two modulation schemes are so similar that they are virtually indistinguishable when compared using matched filtering or PSD. Only by combining autocorrelation with matched filtering, was it possible to differentiate between the two modulation schemes. The final design of the spectrum sensing prototype is capable of performing characterization at an accuracy of close to 80 percent and signal detection at a much higher rate.

The prototype developed for this project is capable of detecting and characterizing signals across the public safety bands, as well as coordinating the receivers with GPS and the central controller. Software and hardware issues limited the measurement of distance to Received Signal Strength, instead of being able to also include Time of Arrival, or Time Difference of Arrival, and the measurement quality of this Received Signal Strength proved to be insufficient for the accurate localization of a transmitter. The localization algorithm was tested in simulation and is functional, but does not account for multi-path, or other

non-ideal channel characteristics. Figure C shows a block diagram of the complete structure of the spectrum sensing and localization prototype.

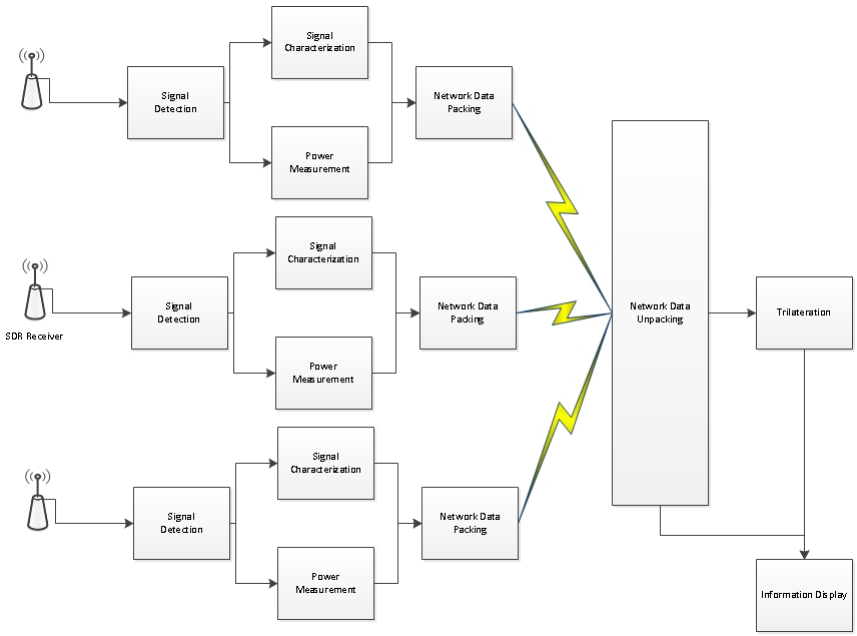


Figure C: System Overview showing the signal path from detection to measurements, trilateration, and display

Figure C shows three receiver nodes, each node searches through spectrum performing spectrum sensing and signal characterization to determine the likelihood of a signal's presence. Once the nodes have information on the current center frequency they are examining, they send that information to the control system where data from each of the nodes for each frequency and each time are examined. The control center then performs trilateration to determine the location of the public safety responder.

Future work in this area would be concerned with providing accurate power measurements from the receiver nodes in order to aid in localization as well as examining a number of the localization algorithms that were abandoned due to hardware and software issues. In addition future projects in this area would be concerned with implementing a working scanning system that could analyse the entire UHF public safety band and provide a graphical representation of all of the public safety responders in a disaster zone.

Contents

List of Figures

List of Tables

Glossary of Terms

ADC: Analog to Digital Converter - a system component which takes an analog waveform as its input, and outputs a digital representation of the signal

APCO: Association of Public Safety Communications - Officials public safety telecommunications organization

BPSK: Binary Phase Shift Keying - a modulation scheme that changes the phase of a transmitted signal to indicate a bit change

C4FM: Continuous Four-level Frequency Modulation - a modulation scheme that uses a Nyquist pulse and a raised cosine filter for a system of four-level encoding transmitted using FM

CQPSK: Compatible Quadrature Phase Shift Keying. A modulation scheme that changes the phase and amplitude of a transmitted signal to indicate a bit change

DAC: Digital to Analog Converter. A system component which takes a digital representation of a signal as an input, and outputs an analog waveform

DC: Direct Conversion. A receiver which operates at or near the radio frequency it is demodulating, without the need for downconversion

DDS: Direct Digital Synthesis. The creation of radio frequency analog waveforms from a digital signal without the need for analog RF upconversion

FFT: Fast Fourier Transform. A simplified mathematical operation that converts data into the frequency domain

FM: Frequency Modulation. A modulation scheme that modulates voice data up to a center frequency in its entirety

FSK: Frame Shift Keying. A modulation scheme that changes the frequency of a trans-

mitted signal to indicate a bit change

GPS: Global Position System. A network of satellites transmitting accurate timing and positioning data for world-wide position determination

HDU: Header Data Unit. A the header inside C4FM signal frames, it contains data about the transmitter, the encoding and many other aspects of the communication standard

NASTD: National Association of State Telecommunications Directors. A public safety telecommunications organization that regulates communications standards

NCS: National Communications System. An office of the Department of Homeland Security in charge of emergency public safety communications.

P25: Project 25 Public Safety Communications Standard. A public safety communications standard that is used as the primary form of federal public safety communications

PSD: Power Spectral Density. A measure of the power of a received signal

RSS: Radio Signal Strength. A measurement of the power of a received radio transmission

SCF: Spectral Correlation Function. A cyclostationary analysis algorithm designed to measure the periodicity of signals

SDR: Software Defined Radio. A way of performing radio design that encodes the specifics of modulation in software rather than hardware

SNR: Signal to Noise Ratio. A radio of the received signal power to the received noise power

TDMA: Time Division Multiple Access. A telecommunications standard for shared access of a network

TDoA: Time Difference of Arrival. Localization taking advantage of the differing travel times between spatially separated transmitters and receivers

ToA: Time of Arrival. Localization taking advantage of the time of flight of a radio signal, given a known transmit time.

UHF: Ultra High Frequency. A radio frequencies between 300MHz and 3GHz.

USRP2: Universal Radio Peripheral Version 2. A software defined radio capable of being reprogrammed for a wide range of different SDR applications

VHF: Very High Frequency. A radio frequencies between 30MHz and 300MHz.

Chapter 1

Introduction

1.1 Motivation

Figure 1.1: Firefighter response to forest fire in Tirat Hacarmel, Northern Israel [20]

Large scale emergencies present a unique challenge for incident response teams and their coordinators. When an incident grows beyond the capabilities of a single department, such as an active wildfire like the one shown above in Figure 1.1, assistance is often requested from neighboring departments, or other agencies within the same area. Interoperability, the ability for different agencies to effectively communicate with each other, is an important

aspect of public safety communications that is currently being addressed with more public safety agencies moving towards a single standard for their communications, APCO Project 25 or P25 [9].

Moving to a single communications protocol only solves one of the issues of a multi-agency response. The most important piece of information that any emergency dispatcher, or in the case of a large scale event, coordinator, can have is the location of the emergency responders. Not only does this information allow the coordinator to effectively and efficiently assign units to high priority tasks, this information allows the coordinator to send aid to responders who have become incapacitated during their response, as their location will be known. This project will develop a system to aid in this aspect of emergency response, it will provide the locations of first responders base on their radio usage, such that multiple responders from multiple agencies can be located through the use of their standard equipment.

The decade that has passed since the September 11th tragedy has resulted in the identification of many disaster response challenges as well as some steps to minimize the impact of these challenges. Of the challenges presented by the 9/11 Commission Report [22], the lack of a unified command and control center, along with the lack of responder location information present aspects of disaster response which still show substantial room for improvement [1]. These particular challenges are not limited to this tragedy, or the response to attacks, but are present to some degree in every response with more than one responding agency.

The interoperability and command system challenges become even greater when volunteers, such as amateur radio operators and the Red Cross become part of the disaster response effort. Hurricane Katrina and the September 11th tragedy both resulted in typical public safety communications infrastructure being disabled, resulting in increased communications difficulty between responders. In the early stages of response to Hurricane Katrina, amateur radio operators provided a rapid replacement for the disabled communications system, with many radio operators assisting in operations after some public safety services had been restored [15]. These volunteer responders are often prohibited from using public safety communications systems when they have been restored, resulting in their efforts

being coordinated as an additional organization at the scene of an incident.

In order to effectively interact with a number of different responding agency radio systems, as well as volunteer responders who might be using any number of different radio communications standards, a highly versatile system is required. Software-defined radios provide a unique solution to this problem, as they are not hardware limited to any particular communications protocol, and often have very wideband capabilities. These features would allow for a system that is interoperable with all public safety responders, including volunteers, without dedicated radio hardware for each agency. This project lays the groundwork for the implementation of a real-world system to allow the effective coordination of a variety of responders.

1.2 Problem Statement

Public safety radio interoperability is becoming an increasingly more important issue, as the increasing complexity of modern radio communications systems limits compatibility between different radio systems. This increasing complexity is driven mostly by the need to increase the number of users in a fixed amount of wireless spectrum. The ever increasing need for wireless devices has resulted in a greater usage of the available wireless spectrum, and accordingly, reduced bandwidth available to each device.

In order to provide the same quality of communications with reduced bandwidth, radio manufacturers have moved from analog frequency modulation to digitally encoded voice transmissions, such as APCO P25 Digital. The public safety bands are currently in a state of transition, with some organizations continuing to use legacy analog systems, with others moving to new digital systems. This creates an environment where agencies which may be geographically close to each other may have hardware limitations preventing them from communicating effectively.

Large scale incident communications represent the worst case scenario for these communications issues. As the size of an incident response grows, the number of responding agencies also increases, potentially requiring a greater number of different radios to effectively communicate with all of the responders at the scene. Effective communications can

be facilitated through the use of a software-defined radio, as it would not be limited to a single communications protocol, but could have many different protocols implemented in software to allow communication between a coordinator and responders using different radio systems.

The coordination of users across different systems, provided an implementation that is physically capable of communicating with these users, still requires the collection of information regarding each users configuration. This information includes the radio systems center frequency, modulation scheme, and the users geographic position. This MQP develops a set of distributed, networked software-defined radio sensors that will cooperatively monitor and detect the transmissions of disaster responders. The sensors will make measurements to determine a radios modulation scheme, center frequency, and geographic location, in order to provide this information to an incident coordinator.

1.3 Competing Solutions

Two independent methods currently exist for the localization of public safety responders. The first, and most commonly implemented, makes use of an active transmitter given to every responder, and this transmitter is used to determine location information. The second, takes advantage of the existing two-way radio equipment that a responder will be carrying, and uses transmissions from this two-way radio to determine the responders location.

Public safety responder tracking has been a prominent research topic at WPI since the 1999 Worcester cold storage warehouse fire, and the creation of the Precision Personnel Locator [23]. The Precision Personnel Locator project focuses on the creation of an accurate indoor firefighter location system, and makes use of active transmitters carried by the firefighters in addition to their regular equipment. Commercial systems requiring the use of tracking tags also exist, such as the one provided by ERT Systems [7], although this system tracks a responders presence near a detector, and does not provide more advanced location information. These systems provide accurate tracking of responders from a single department, but for large scale incidents they may compound the already significant issue of interoperability.

Tracking the position of a public safety responder through the use of their regularly issued radio equipment poses a number of advantages over systems requiring separate transmitters, especially the prevention of more interoperability challenges. A recent MQP at WPI, *A Channel Model and Geolocation Simulation System for Cooperative Spectrum Sensing Networks* [12], suggests the use of a software-defined radio to identify and track responders based on their existing hardware, but does not provide a real-time, real-world implementation. This MQP will expand upon the results of Kelly and Khair to implement a similar system in real-time using MATLAB and Simulink.

1.4 Proposed Design and Contributions

In order to provide accurate simultaneous location information for a wide variety of radio systems, a system of sensors must be developed to determine the operating frequencies of all of the responders and from this information the system must also determine the responders locations. This project proposes a system that can operate in isolation from the existing communications systems infrastructure, without requiring responders to carry additional equipment. This system would scan through the appropriate frequency ranges for public safety responders, first determining the frequencies and modulation schemes being used. This information would then be used to determine the location of all public safety responders on scene, taking advantage of received signal strength measurements made at the networked receivers. An example of such a system is shown below in Figure 1.2.

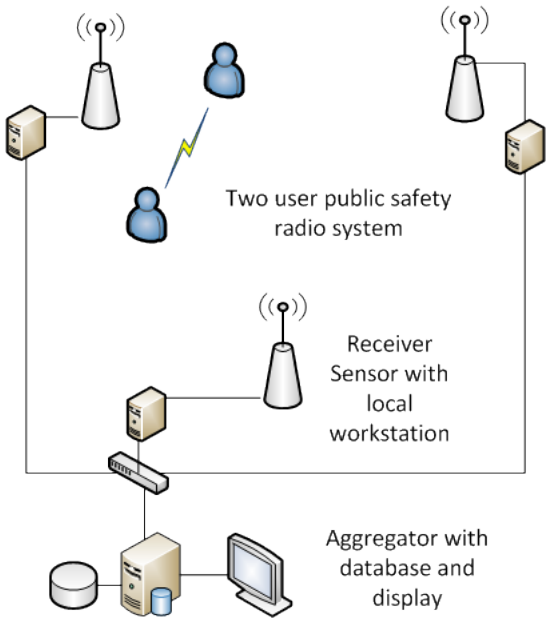


Figure 1.2: Public safety location sensing network

This project will overcome the shortcomings of existing systems designed for small single department response through the creation of a system that is independent of existing user equipment and designed specifically for large scale incidents. The use of advanced, adaptive, software-defined radio receivers, along with the existing communications equipment carried by responders will be employed to characterize and localize two-way radio transmissions, preventing the increase in load for the responder, and maximizing system versatility.

1.5 Report Structure

This document is divided into six chapters with each chapter divided into a number of relevant sections and subsections. This chapter, Introduction, introduces the need for the project, as well as current solutions to the project challenges, and the proposed extensions this project will make to the existing state-of-the-art. Chapter 2: Background provides information on the techniques that will be used for the characterization and localization of transmissions, as well as a background of the hardware, software, and standards relevant

to the project. This background information is followed by Chapter 3: Proposed Approach which discusses the overall system infrastructure and each of its subsystems. Chapter 4: Prototype Implementation, describes the specific algorithms selected for each subsystem of the project, and their implementations in this project. Prototype Implementation is followed by Chapter 5: Design Verification which includes a discussion of the projects results at the subsystem level, and the functionality of the project as a whole. The final chapter, Chapter 6: Conclusions and Recommendations discusses the success of the project, and makes recommendations for future work. This final chapter is followed by the appendices, including source code and Simulink models for all systems implemented for the project.

Chapter 2

Background

This section introduces a number of topics relevant to the development of this radio localization and sensing system. These topics will include not only potential methods for signal detection and localization, but the underlying technology which will allow these techniques to be utilized.

2.1 Software Defined Radio

Software defined radios (SDRs) represent the current state of the art in radio technologies. An SDR is fundamentally different from a traditional radio in that many operations which may have previously been implemented using dedicated hardware have been replaced with a Field Programmable Gate Array (FPGA), a Digital Signal Processor (DSP), a Personal Computer (PC), or some combination of these devices, and software to provide the desired functionality. This change allows for an SDR to be rapidly reconfigured, giving it the flexibility to replace a variety of traditional radios with a software update [8].

An SDR, as with any digital communications system has analog and digital components. The idea behind Software defined radio is to shift as much of the radio into the digital side as possible. Typically, the digital portion of an SDR performs all of the data compression, decompression, encoding, decoding, modulation, and demodulation, while the analog side is a simple RF frontend. An analog to digital converter (ADC) and a digital to analog converter (DAC) function as the border between these two sides, and allow the modulated

signal, which has been generated by the software, to be created in the analog system and transmitted, as shown below in Figure 2.1.

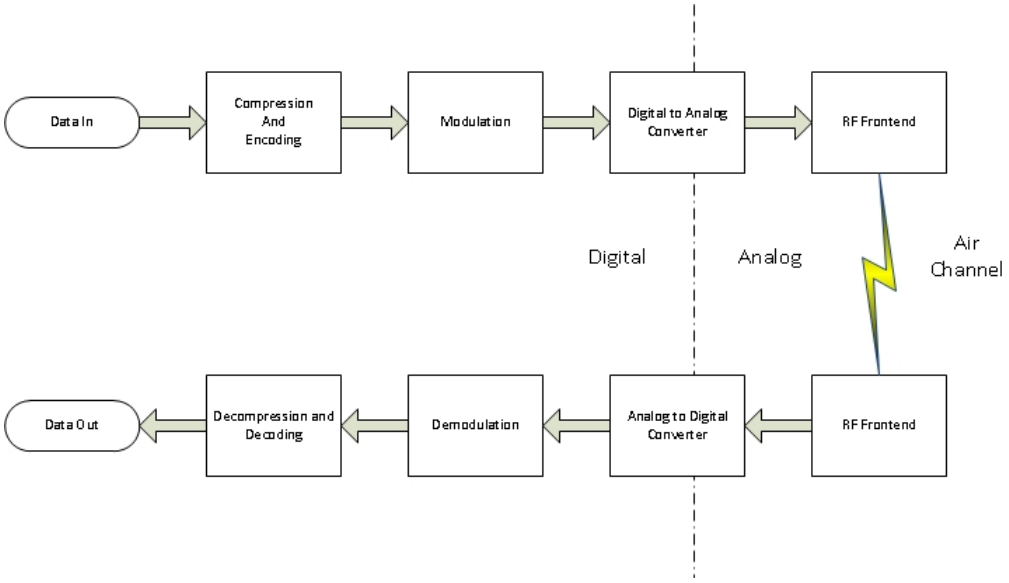


Figure 2.1: Flow diagram for a software-defined radio, showing the division between digital and analog components

In a typical system using an ADC and a DAC, the modulated signal will be passed to the DAC which will generate a baseband analog signal from its digital input. This analog signal will then be upconverted using an RF mixer to the desired output frequency. The opposite occurs on the receiver, where an RF mixer will downconvert the received analog signal and pass it to an ADC, which will generate a digital representation of this analog waveform as its output. The complexity of the RF frontend is dependent on the capabilities of the ADC and the DAC, as the cost of these components is typically high when compared with the rest of the system, limiting the bandwidth and noise tolerance that the RF frontend is permitted [17].

As advancements in analog to digital and digital to analog conversion result in more power efficient hardware capable of operating over a greater bandwidth with greater precision. Direct Conversion (DC) and Direct Digital Synthesis (DDS) allow for a very minimal

RF interface between the digital and analog portions of the radio, as these devices can operate at high enough frequencies to directly transmit, without the need for an RF up-converter or down-converter [26]. Direct Digital Synthesis takes advantage takes advantage of higher performance DACs to create radio frequency signals directly from the digital input, eliminating the RF mixer from the system. Direct Conversion functions similarly, taking advantage of an ADC that can operate at the desired radio frequency to sample and output the waveform as a digital signal without downconversion.

2.1.1 USRP2

The Universal Software Radio Peripheral Version 2 (USRP2) shown below in Figure 2.2 is an inexpensive provides an extremely versatile platform for software defined radio development. It is a modular system, consisting of a base unit and a daughtercard which can be a transmitter, a receiver, or a transciever. The base unit contains two 100MS/s 14 bit ADCs, two 400MS/s 16-bit DACs and a Spartan 3 FPGA and interfaces with Windows or Linux PCs using a Gigabit ethernet port [24]. The USRP2 is capable of interfacing with any of the daughtercards currently produced by Ettus Research, providing RF coverage in a variety of ranges from 1MHz to 4GHz.

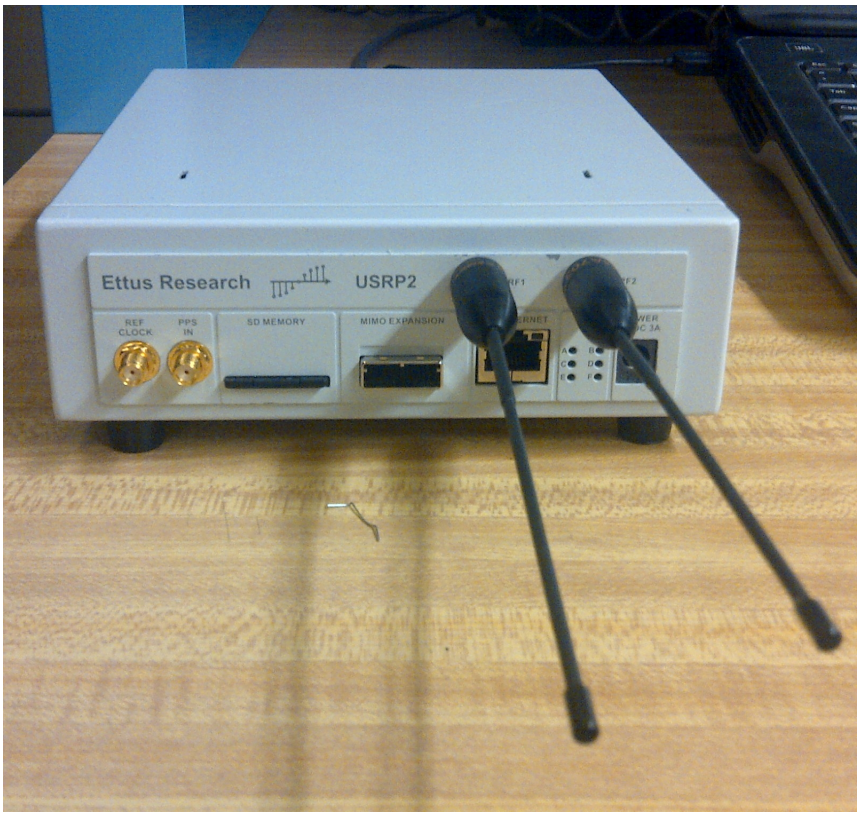


Figure 2.2: USRP2 Base with internal WBX daughtercard and dual band VHF/UHF Antennas

The WBX daughtercard provides continuous transmit and receive coverage from 50MHz to 2.2GHz and is capable of providing 40MHz of usable bandwidth [6]. This daughtercard provides coverage over all of the commonly used public safety two-way radio bands, with bandwidth great enough to cover the an entire band. The combination of the USRP2 and the WBX daughtercard allow for a single radio solution that can communicate and interact with nearly every two-way radio system in use by public safety responders.

2.1.2 Simulink

Simulink is a graphical programming interface included as part of the MATLAB simulation package. The package provides an interface with the USRP2s allowing for the

rapid development of SDR prototypes. Initially, the Simulink interface for the USRP2 was based on a wrapper for GNU Radio that would allow the user to take advantage of existing Simulink functionality to prototype with real hardware [16]. Future revisions of the Simulink software would replace this GNU Radio wrapper with proprietary modules, improving the versatility of the interface while maintaining the advantage of access to existing MATLAB and Simulink functionality.

Simulink also provides a powerful platform for calculations, and its Instrument Control Toolbox provides the ability to easily send data between network linked computers. The calculation capabilities of Simulink are a subset of those provided by MATLAB, with the addition of some graphically configurable communications specific functions.

2.2 Public Safety Radio Bands

Public Safety communications is a major industry. Today every police officer, fire fighter and EMT as well as a host of other public safety professionals use public safety radios to communicate. The FCC has allocated large blocks of spectrum to public safety as a means to protect public safety transmissions from interference caused by non-public safety transmissions.

The US government recognised the need for standardized public safety communications in response to a major public safety disaster in 1912, the sinking of the Titanic. Later legislation was imposed on the radio frequency spectrum bands defined the public airwaves, or radio spectrum, as a limited resource that must be conserved and used for the public interest. As a result spectrum was allocated "for the purpose of the national defense" and "for the purpose of promoting safety of life and property through the use of wire and radio communication." [9]. Over time local, county, state and regional public safety organizations developed their own rules and regulations to control the use of public safety bands. Today every town's fire department and police force uses public safety radios to communicate and coordinate. As many towns and cities decided what form of public safety communication to use separately, there are a number of different standards that public safety responders use to communicate.

A large scale disaster often pulls in resources from a number of different public safety organizations. This means that at a disaster such as a forest fire might call on the public safety responders of several towns adjacent to the blaze. The result is that several different public safety communications standards could be operating in one area and a coordinator would not be able to coordinate the public safety responders or have any visual representation of where they are. This project provides the means for a coordinator to know where public safety responders are at all times by just examining their transmissions.

Today's Public Safety communications have bands on a number of different frequency ranges. Today's public safety radios transmit on the Very High Frequency (VHF) and Ultra Hight Frequency (UHF) bands as well as the 800MHz band. There are two public safety bands in the VHF band, the low band that ranges from 25MHz to 50MHz and the high band that ranges from 138MHz to 174MHz. The UHF public safety band ranges from 408MHz to 512MHz and the 800MHz public safety band ranges from 806MHz to 871MHz. In addition to this spectrum the FCC has allocated a number of new bands for public safety. These are bands in the 700MHz band and the 4.9GHz band. As these bands have only recently been opened to public safety communications, public safety radios still use the VHF, UHF and 800MHz bands. This project will examine the transmissions from public safety radios transmitting on the UHF band. This band has a high degree of traffic and is used widely by public safety responders.

2.3 APCO P25

Project 25 (P25) is a set of standards produced by the Association of Public Safety Communications Officials (APCO), the National Association of State Telecommunications Directors (NASTD), and the National Communications System (NCS). It was established to address the need for common digital public safety radio communications standards for public safety first responders and other emergency response professionals[18].

P25 consists of two phases: Phase 1 radio systems operate in 12.5kHz analog, digital or mixed mode. Phase 1 radios use Continuous Four-level FM (C4FM) modulation for digital transmissions at 4800 baud and 2 bits per symbol, yielding 9600 bits per second.

In addition to C4FM modulation, Phase 1 P25radios are backwards compatible with analog FM modulation and can also demodulate Compatible Quadrature Phase Shift Keying (CQPSK)[18].

Phase 2 radio systems have been developed using a 2-slot TDMA scheme to achieve one voice channel or a minimum 6kbps data channel per 6.25kHz bandwidth. Phase 2 was developed in order to insure interoperability with legacy systems as well as decrease the required bit rate for transmission. Phase 2 was designed as an interface between repeaters and other subsystems rather than emergency responder to emergency responder communication. This means that P25 Phase 2 radios are not designed to be used in the field. Phase 2 is a system for stationary base stations that coordinate emergency responders and is rarely used to communicate from one emergency responder to another[18].

This project will be designed to search and locate Phase 1 public safety radios using either P25 radio standard or legacy systems using analog FM modulation. The project did not consider Phase 2 radios as they would not be used in the field and would not aid in locating emergency responders. Analog FM and P25 C4FM are two of the most widely used forms of person-to-person public safety communication in the US[18]. The US government has recently introduced the P25 standard to public safety organizations in order to bring public safety communication system under one standard. Despite this initiative many public safety organizations continue to transmit using analog rather than switching over to the new P25 public safety standard, and hence it is necessary to include legacy systems in the project to insure that no emergency responders are excluded.

The P25 radio standards primary modulation standard for person to person voice communication is C4FM. C4FM is a 4-carrier modulation format where the carrier is shifted in frequency to a particular location around a center frequency. This allows for each of the four states to represent a binary number[18]. Figure 2.3 is a block diagram of a C4FM modulator. It shows the composition of a P25 signal.

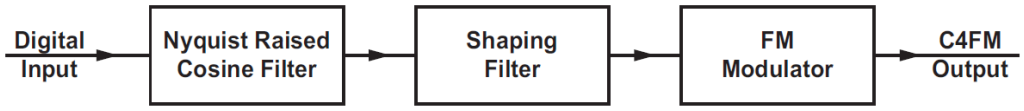


Figure 2.3: Structure of a C4FM modulator. The modulator takes in data from the digital input and multiplies it with a Nyquist raised cosine filter and a shaping filter to create four distinct lobes. Finally the signal is modulated with an FM modulator like an analog signal.

C4FM modulation is composed of a Nyquist Raised Cosine filter, a Shaping Filter as well as a Frequency Modulator, the frequency modulator shifts the transmission by a set number of Hertz creating the four pulses that characterize C4FM[18]. This scheme is very specific to the P25 standard as it is capable of demodulating C4FM, as well as analog FM. P25 radio standard channelizes C4FM transmissions. C4FM transmissions are 12.5kHz wide, which means that they take up a total bandwidth of 25kHz. Any P25 standard radio can transmit on the entire public safety band that supports P25 but each transmission frequency is separated from its neighbors by 30kHz. This precaution insures that between any two C4FM transmissions there is 5kHz of empty spectrum protecting transmissions from each other. Radio transmissions can occasionally drift in frequency if their antennas are not entirely accurate. This means that a signal might stray few Kilohertz in its bandwidth and without protection, one transmission might run into another causing interference.

P25 C4FM is unique to P25 so that only a P25 radio can receive and demodulate the signal. P25 radios have to be able to recognize a signal transmitted using C4FM and differentiate it from a different modulation scheme. One way of identifying a specific modulation scheme is by transmitting a specific code at regular intervals throughout the transmission. P25 radios transmit C4FM signals with a barker code or header data unit (HDU) at intervals of 180 microseconds. The HDU holds information about the radio that identifies it as being P25, inside the HDU is a Header Code Word. The Header Code Word includes a Message Indicator (MI), and Algorithm ID (ALGID) for the encryption algorithm, and the Key ID (KID) for the encryption key as well as the Manufacturers ID. Figure 2.4 shows the structure of the HDU broken down into each section.

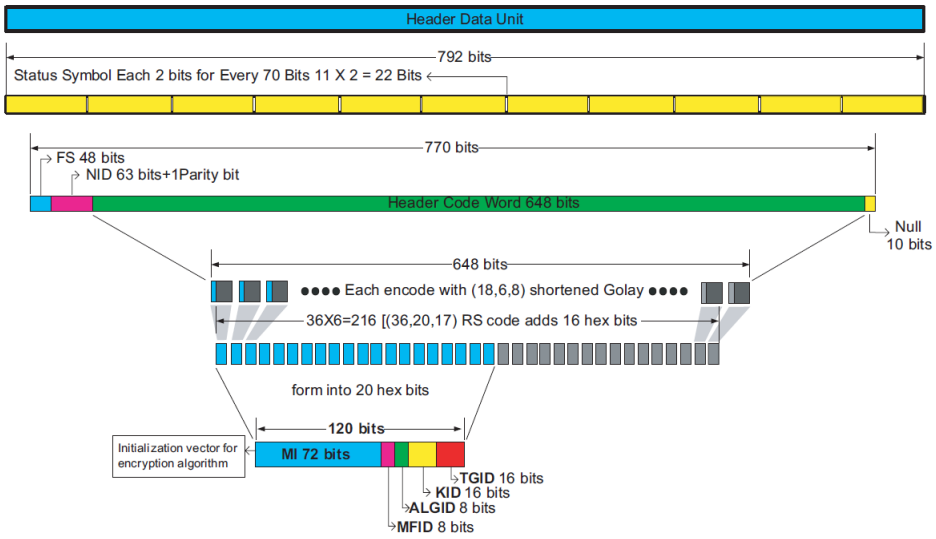


Figure 2.4: Design of the HDU of a C4FM signal. The header is made up of 792 bits compartmentalized into a number of different sections.

The HDU identifies the signal as being C4FM as well as providing essential information to decode the signal. The HDU is only a small part of a C4FM frame but it is essential to transmitting and receiving P25 C4FM signals reliably. When a pubic safety responder speaks into a P25 radio, the signal is converted into bits and encapsulated in a frame with an HDU at its head[18]. The signal is then converted into electromagnetic waves and sent into the air. When a receiver receives the signal, the radio examines the HDU and verifies the header is accurate before decoding the signal and converting the data into sound.

2.4 Spectrum Sensing

Spectrum sensing is a broad term for determining if received signal is a real signal or noise. Differentiating signals from noise is essential to properly receiving signals and being able to decode them. If a receiver were to interpret noise as a signal then the received content would be useless to the user. Noise comes from a number of different sources, some noise comes from the atmosphere in the form of random electromagnetic radiation and some noise is caused by surrounding electrical and electronic devices. The combined forms

of noise form a blanket that spans the whole radio spectrum. This noise blanket is known as the noise floor.

There are many different ways to differentiate a signal from noise. These different spectrum sensing methods involve examining the attributes of the received data. In order to make it easier to discern a signal from a non-signal, radio transmissions are often designed to be easily recognizable. Radio signals are transmitted using modulation schemes that make the signal recognizable as a signal rather than noise by making the signal strength higher than that of the noise floor and make it easier to differentiate one transmission from another. This allows the receiver to easily recognize the signal and retrieve the data from the transmission. One of the ways signals are examined is by observing them in the frequency domain. Most modulation schemes have a different spectral shape due to the way the signal is modulated. Figure 2.5 shows a graph of a Binary Phase Shift Keying (BPSK) signal in the frequency domain.

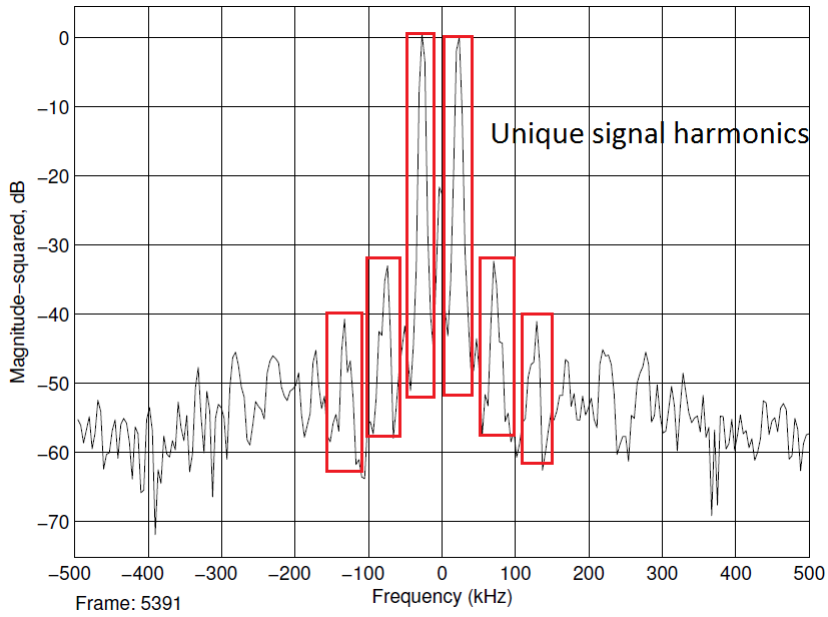


Figure 2.5: FFT of a DBPSK Signal. The signal's harmonics are the large peaks that appear around the center frequency of the signal.

The BPSK signal has distinct peaks around its center frequency. These peaks correspond

with the modulation scheme used to generate the signal. The way the harmonics of the signal are placed around it's center frequency is unique to BPSK modulation. Figure 2.6 shows a frequency plot of a Frequency Shift keying (FSK) signal in the frequency domain.

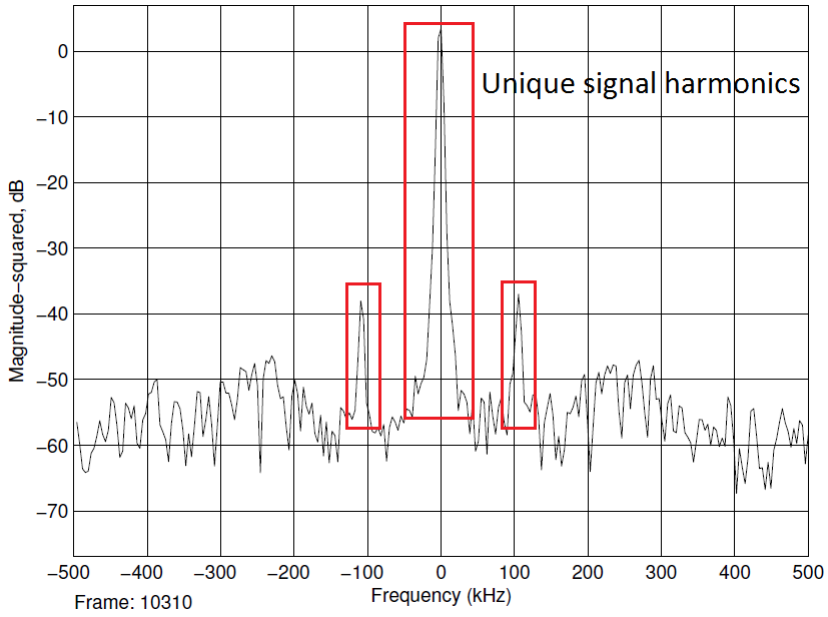


Figure 2.6: FFT of an FSK Signal. The harmonics of the FSK signal are shaped very differently then those of the BPSK signal.

The FSK signal in Figure 2.6 also has distinct peaks around its center frequency. Like DBPSK, FSK modulation generates a unique spectral shape in the frequency domain. Figure 2.5 and Figure 2.6 are both transmitting the same signal but their spectral shapes are very different. The difference in modulation schemes dramatically changes the signals.

In order to understand how a signal is received, it is first necessary to understand how it is transmitted. Radio is based on the concept that a stream of information can be transmitted through the air using electromagnetic radiation. Electromagnetic radiation can be considered to be a waveform travelling at a certain frequency. It is possible to send a signal at a desired frequency, detect it and decode it by monitoring its transmission frequency. All modulation schemes for transmitting signals are different but they all contain

similar attributes. Many modulation schemes use a shaping filter at the transmitter to make the signal more visible to a receiver. The filter shapes the time domain representation of the signal so it can be sampled and converted to a digital format more easily. The filter also shapes the frequency domain representation so that the signal is easily distinguishable from noise [11]. Modulation schemes use a number of different attributes of signals to differentiate them from other modulation schemes and signals. Table 2.1 shows a list of several common attributes that are manipulated in modulation schemes.

Table 2.1: Table of Signal Attributes

Signal Attributes
Power
Amplitude
Bit rate
Frequency
Shaping Filter
etc.

This project will search throughout the public safety communication bands searching for transmissions. When a signal is found, it is tested for authenticity to make sure it is not noise and characterized to determine its modulation scheme. The project assumes that there is no prior information about the transmission in question so it is necessary to use spectrum sensing methods to determine where transmissions are located in the frequency domain. To simplify the interpolation of data, spectrum sensing uses two hypotheses to determine if a range of frequencies contains a signal.

Spectrum sensing methods determine the probability that a signal is present at a known frequency. If the probability is not exact, it can be hard to decide if a signal is a received signal or noise. To simplify decisions on possible signals a set of hypothesise were developed to characterize signal data. These hypotheses simplify the analysis of signals by characterizing a signal as being one of two things. Either the signal is a transmission from a radio or the signal is noise [4]. As these hypotheses are so rigid, it is possible that they may not always be reliable. For example, if a signal is weak or cannot be distinguished from the

noise floor it could be lost. In order to ensure that all signals in question are found, many samples of the signals are taken. This is accomplished through the use of a high sampling rate as well as a number of spectrum sensing nodes.

Equation (2.1) and equation (2.1) show the two hypotheses about signal data that govern spectrum sensing. Equation (2.1) states that there the received data does not contain any signal, only noise ($n(t)$), while equation (2.2) states that the received data contains a signal ($y(t)$) and noise ($n(t)$).

$$H_0 : y(t) = n(t) \tag{2.1}$$

$$H_1 : y(t) = x(t) + n(t) \tag{2.2}$$

These two theorems provide a basis for determining the likelihood of a signal's presence. The system collects information for many nodes and uses a number of spectrum sensing techniques to test the signal. Each technique determines a value for $H0$ and $H1$ depending on the strength of the observed signal[4]. Depending on the ratios of each hypothesis, the program then decides if the received frequency is a signal or not. This form of signal detection is called cooperative sensing and will be discussed later in this paper.

2.4.1 Power Spectral Density

The Power Spectral Density (PSD) of a signal is a measure of its shape in the frequency domain. Each signal has a unique PSD depending on which modulation scheme was used to transmit the data and any noise that was added to the signal while it was being transmitted. A signal's PSD can be used to identify the signal as having a certain modulation scheme. Though the data transmitted and the noise in the channel determine the PSD of a signal, a pulse shape is by far the most recognizable characteristic of a transmission in the frequency domain. This means that any signal that is transmitted with the same modulation scheme will have a similar PSD. Figure 2.7 shows a graph of the PSD of a BPSK signal. This graph has a very distinct spectral shaped compared to the PSD of other signals and of noise.

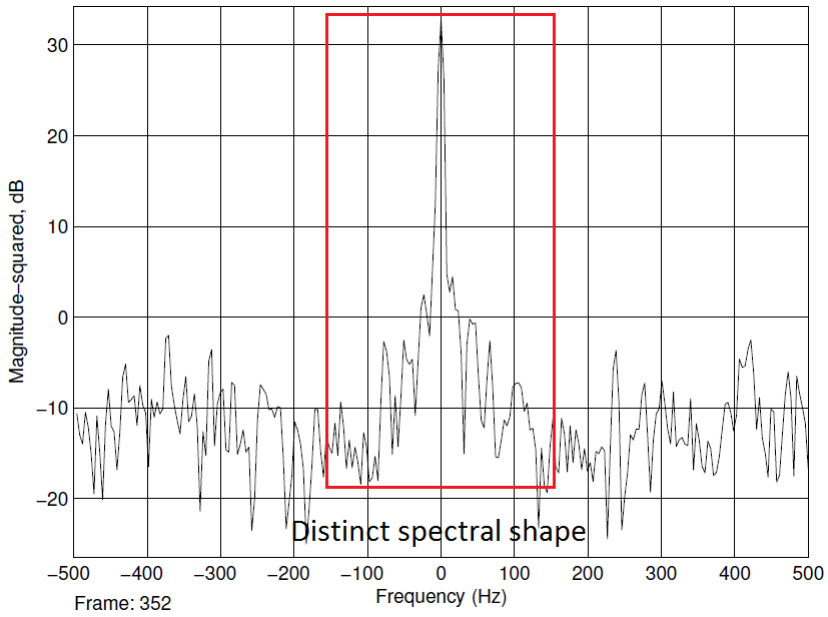


Figure 2.7: PSD of a BPSK Signal. The shape of the signal is very distinctly different from the noise around it.

Figure 2.8 shows a plot of the PSD of white nosie recieved in a unoccupied channel. This graph is distinctly different from the graph of th PSD of the BPSK signal. The difference in spectral shape makes it possible to easily differentiate a signal from noise. This makes PSD characterization a reliable spectrum sensing scheme.

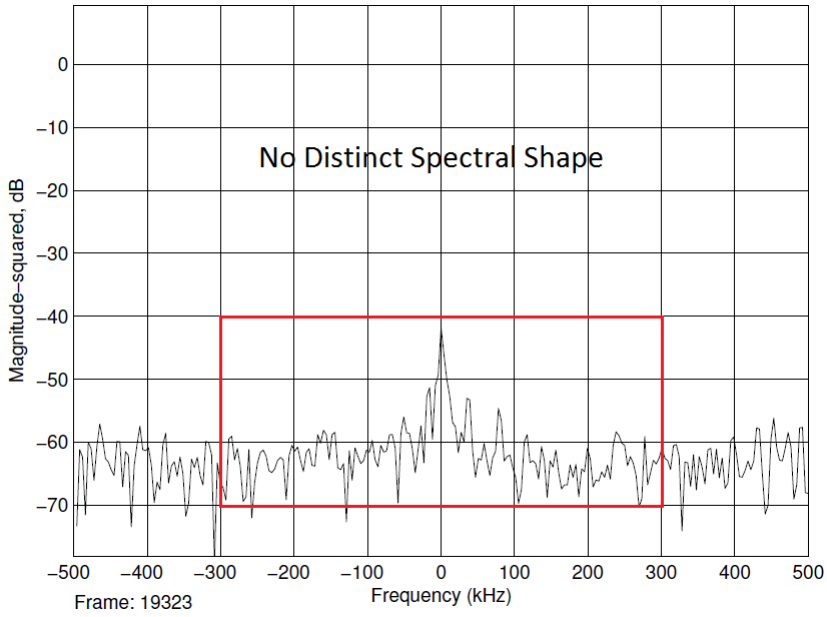


Figure 2.8: PSD of White Noise. The plot shows no distinct peaks or spectral shape of any kind.

If a modulation scheme does not use a pulse shape, then the signal can be characterized by the shape of the data being transmitted and the peak of the signal power at its center frequency. A simple example of a modulation scheme without a pulse shape is Frequency Modulation. Frequency modulation (FM) conveys information over a carrier wave by varying its instantaneous frequency. In this scheme, voice data is modulated directly rather than adding any encoding or shaping to the signal. The PSD of an FM signal can be characterized by the shape of the voice data around the signal's center frequency.

The PSD of a signal is the Fourier Transform of its Autocorrelation. The Autocorrelation function, $R_x(\tau)$ is a means of measuring how similar a signal is to itself. Equation (2.3) and equation (2.4) show how the Power Spectral Density of a signal is calculated from the $R_x(\tau)$ of a signal. A signal can be identified by its PSD, but due to noise and interference in the channel, a received PSD may be very different to the PSD of the transmitted signal. In order to characterize a signal more reliably, the average PSD is often used to differentiate one modulation scheme from another.

$$R_x(\tau) = \int_{-\infty}^{+\infty} x(\tau) * x(T - \tau) d\tau \tag{2.3}$$

Equation (2.3) shows how the autocorrelation function is calculated mathematically. The autocorrelation function $R_x(\tau)$, measures a signal's periodicity by examining how it relates to itself. This process is similar to convolution. When two signals are convolved together their output peaks were the signals are most alike. When a signal is autocorrelated it peaks at the center of the signal and at regular intervals around the center. The peak at the center shows how closely the signal relates to itself when it is most similar. The peaks around the center show the periodic nature of the signal.

$$S_x(f) = \int_{-\infty}^{+\infty} R_x(\tau) * e^{-j2\pi f\tau} d\tau \tag{2.4}$$

Equation (2.4) shows how the power spectral density of a signal is calculated mathematically. The PSD of a signal $S_x(f)$ is a measure of its power in the frequency domain while the autocorrelation function measures the signal's similarity to itself in the time domain. In order to convert the autocorrelation values into measurable PSD values, they must be converted into the frequency domain. The simplest way to do this is to perform the Fourier Transform on the signal. The Fourier Transform measures data in the frequency domain. This provides another way to measure signal attributes.

2.4.2 Energy Detection

Energy detection is one of the simplest forms of spectrum sensing. It determines what frequencies are above a certain power or the magnitude in the frequency domain. For instance when a signal is received it looks like a spike on the frequency range. Its highest power peak is usually at its center frequency or the frequency it was transmitted at. Figure 2.9 shows a large bandwidth of spectrum. In this spectrum there are noise peaks and there is a signal. Energy detection only examines power values so it can not differentiate between a signal and noise if the noise has the same power as the signal.

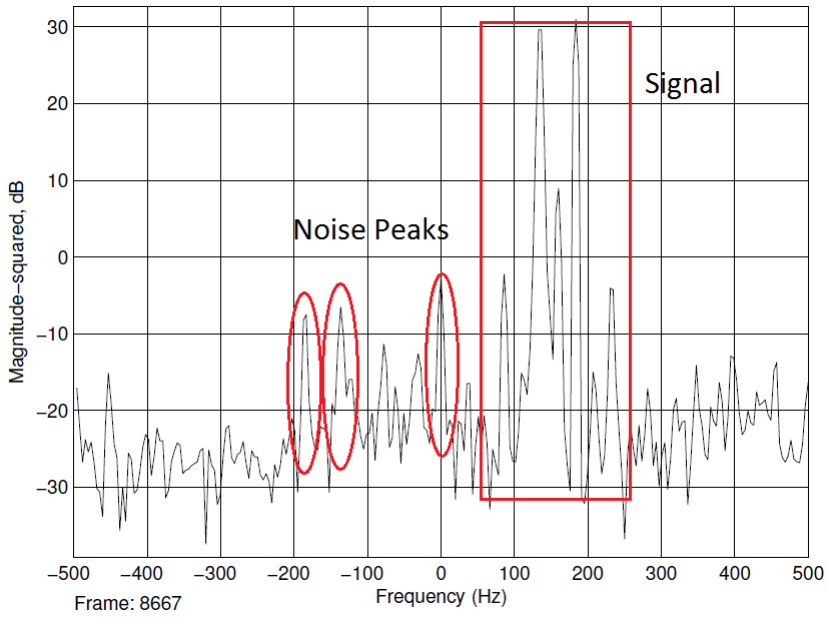


Figure 2.9: FFT of large bandwidth of spectrum. On the right hand side there is the shape of a BPSK signal and on the left there are two noise peaks.

Energy detection takes in all of the data in the magnitude frequency domain and tests if any of the received data has a power higher than its decision value. If the Energy Detector's decision value is triggered then the decision value was triggered at a particular frequency and is considered to contain a signal. This is how energy detection differentiates a signal from the noise around it. The basic assumption involved in energy detection is that a received signal will have significantly more power than the noise around it [3]. This difference in power is primarily true because signals are designed to be easy to find in the frequency domain, in order to facilitate reception. It is therefore possible to determine if there is a signal present or not by performing this simple detection method.

Energy detection has two significant flaws. First it cannot differentiate between an exceptionally high powered noise peak and second, it cannot detect a signal below the noise floor[3]. If a receiver using just energy detection for its spectrum sensing detects a noise peak with a very high power it will interpret the noise as an actual transmission. It is also the case that if a signal is hidden below the noise floor a receiver using energy detection will

interpret the frequency as being empty. These faults make energy detection an ineffective spectrum sensing method by itself. Energy detection is often used in addition to other spectrum sensing methods to improve the accuracy of sensing. Equation (2.5) shows a method for finding the power of a received peak[30].

$$P_{avg}(N) = \frac{1}{M \cdot N} \sum_{i=1}^{M} \sum_{i=0}^{N-1} |x_i(n)|^2 \tag{2.5}$$

Equation2.5 is the most basic form of energy detection. In this equation N is the number of samples, M is the number of antennas and P_{avg} is average power of the signal[30]. This equation performs both energy detection and cooperative sensing because it compiles information for a variable number of samples and of antennas and determines a final value to compare against a decision value. Another more advanced energy detection algorithm is called Otsu's energy detection theorem. Like the energy detection algorithm described in equation2.5, Otsu's method finds the magnitude of the power of the frequency spectrum, and then preforms a decision that determines if the frequency in question contains a signal. Otsu's method increases the distance between noise and signal powers by squaring the received signal$x(t)$. This improves upon the more primitive energy detection method described in equation (2.5) because signals and noise are more easily differentiable. Equation (2.6) describes Otsu's method[30]:

$$S_t = (x(t))^2 F_t = Bandpass(S_t)E(t) = \int_t^{T-t} F_t \tag{2.6}$$

Equation (2.6) shows how Otsu's energy detection method is performed. S_t is the square of the received signal $x(t)$. The signal is squared to make difference between low and high powered data more prominent. F_t band pass filters the squared signal S_t to exclude power values outside the range of the signal. Finally E_t shows how the band pass filtered signal is integrated over a period of T[30]. This equation makes the power peaks of signals more prominent and easier to distinguish from noise. Pure energy detection even using Otsu's method still has flaws. One method of combating them is to increase the scale of the sensing. A single decision from an energy detection measurement is not reliable enough to determine a signal. If there were a large number of measurements, then the reliability of

the sensing increases. The optimum way to perform spectrum sensing is by using a number of sensing nodes around the area being sensed. Each node has a high sampling rate, so that a large number of sensing decisions can be performed per second. Once the power of the received frequency is determined from all the nodes and times, that value is then compared against the decision value. If the power is above the expected power value, then the peak is considered a signal[30]. This model makes sure that an unexpected error peak on one of the receiver nodes is not perceived as a signal by collecting a large amount of data before making a final decision. It also prevents a noise peak that appears for only a short period of time, from being perceived as a signal. If a noise peak is received on all the receiver nodes and is active for the same period of time that the nodes are active, then it will be perceived as a signal. The addition of a large number of nodes reduces the probability of an error. This also insures that a checking system will be more precise. The addition of a large amount of data and the checking system is an aspect of cooperative sensing which is another spectrum sensing method.

2.4.3 Cyclostationary Analysis

Cyclostationary analysis is another spectrum sensing method. The basic premise behind this type of spectrum sensing is that all signals are periodic. This means that in the time domain, certain aspects of the signal will repeat at regular intervals. Signal transmission is designed to be periodic; this facilitates the detection and decoding of signals.

Cyclostationary Analysis is a far more precise sensing method than energy detection because all signals have sampling frequencies while white noise is considered to be completely random. This means that a signal that is lost under the noise floor, or a noise peak that might be mistaken for a signal if energy detection was used as the primary sensing method, will be easily recognizable. Cyclostationary analysis is a more accurate form of spectrum sensing then energy because it does not rely on fluctuating power measurements to perform detection. Many spectrum sensing systems employ both cyclostationary analysis and energy detection. This is because cyclostationary analysis is very computationally intensive and requires a lot of power and time to perform an operation while energy detection is much less computationally intensive.

The SC or the Spectral Coherence and Cyclic Frequency Domain Profile, is a measure of a signal's spectral coherence against the cyclic frequency for which it is being measured[13]. This means that the SC of a signal is a measure of the level to which a stream of data resembles itself over a range of frequencies. This measurement determines whether the signal repeats at a certain frequency over time. Certain modulation types have different SC characteristics. Cyclostationary analysis is the process of using these different characteristics to determine if a signal is present or not.

A signal is only considered Cyclostationary if its mean and autocorrelation are periodic with a period T[13]. These values are essential to determining if the received data contains a signal or not because all signals have to have the same periodicity throughout the signal. Figure 2.10 shows a graph of a received signal. The graph clearly shows the signal's attributes repeating at a steady period.

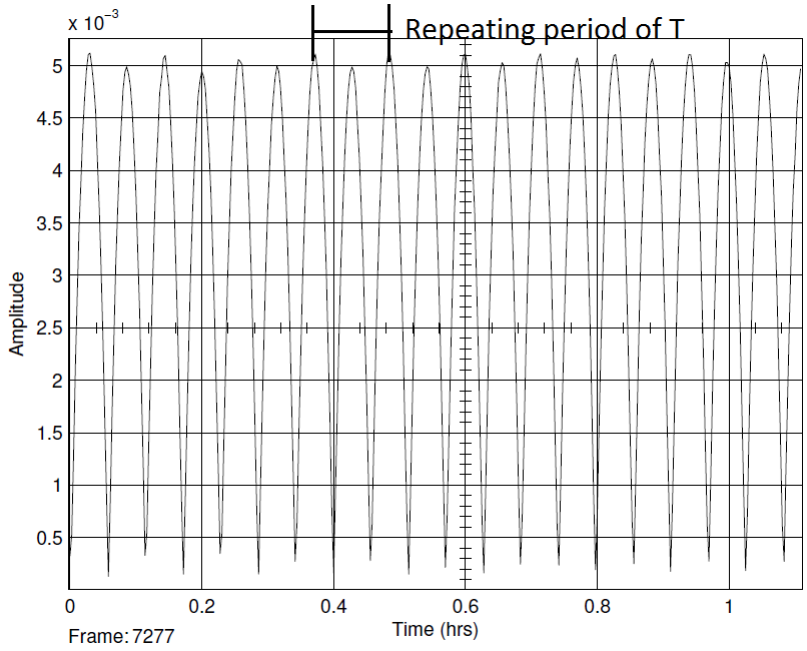


Figure 2.10: Received signal in the time domain. The signal has been modulated back to its center frequency but not decoded. The graph shows a distinct repeating pattern with a repeating period

The data presented in Figure 2.10 shows a signal peaking at regular intervals as data is transmitted. Figure 2.11 shows a similar graph showing the periodicity of a signal. This graph shows the autocorrelation of the same signal. The distance between the repeating attributes in Figure 2.10 and Figure 2.11 are very similar which indicates that both graphs have the same period.

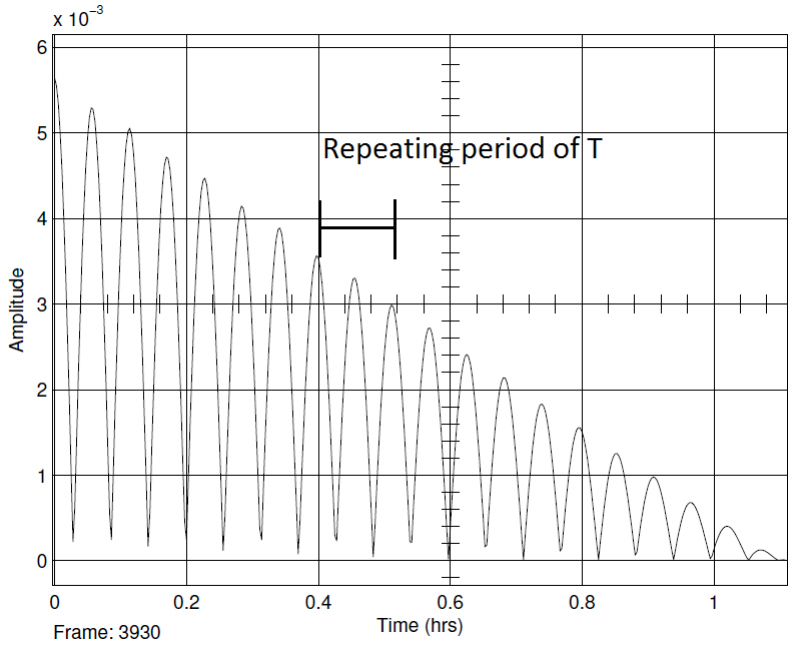


Figure 2.11: Graph of a signal that has been autocorrelated. As the graph shows the signal repeats regularly.

The autocorrelation function takes a signal and convolves it with an inverted version of itself. This operation provides a picture of how the signal relates to itself over time. Analysing a graph of the output of the Autocorrelation function will measure if the received signal has similar characteristics at the signal's time period T, and at period lengths of T separated from the center of the graph[13]. If the stream of data received, contains a signal then there will be peaks at regular intervals separated period lengths of T.

$$R_x(t, \tau) = R_x(t + T, \tau) \tag{2.7}$$

Equation (2.7) shows that the autocorrelation of a signal is the same for any time different of T. In this equation, R_x is the autocorrelation function of $x(t)$ and τ is the time offset[29]. The Autocorrelation function, R_x, is periodic and hence, it can be modelled as a Fourier series[29]. This is important because it means that the signal can be modelled as an equation that determines its cyclic characteristics. Evaluating R_x over $(t - \frac{\tau}{2}, t + \frac{tau}{2})$ is equivalent to evaluating R_x over $(t + T, \tau)$ as both equations are over a single period of the signal's transmission.

$$R_x(t - \frac{\tau}{2}, t + \frac{tau}{2} = \sum_{\alpha} R_x^{\alpha} \tau e^{-j2\pi\alpha t} \tag{2.8}$$

In equation (2.8), R_x^{α} is the autocorrelation function at a frequency of α and α is equal to $\frac{m}{T_o}$ where T_o is the sampling period of the signal[29]. This equation represents the autocorrelation function of $x(t)$ over $t - \frac{\tau}{2}$ to $t + \frac{\tau}{2}$. The change in values from $(t + T, \tau)$ to $(t - \frac{\tau}{2}, t + \frac{\tau}{2})$ makes it possible for the function to be expressed as the Fourier series above. The signal has to be represented in this way because the signal's characteristics only repeat periodically with separations of one period[29]. This equation brings out one of the flaws in cyclostationary analysis. The value for alpha must be evaluated at $\frac{m}{T_o}$ which means that in order to calculate the cyclic characteristics of that data, the function must know this signal's sampling period. This means that any spectrum sensing using cyclostationary analysis must first know the sampling frequency, or the period of the signal being searched.

Spectrum sensing is a method of searching through a large number of frequency ranges in order to find signals. This means that any equation used to determine whether a stream of data has cyclic characteristics must be able to provide an evaluation for the particular frequency in question. The equation R_x^{α} provides a means for searching through different frequency ranges. The equation R_x^{α} is evaluated below[29].

$$R_x^{\alpha}(\tau) = \frac{1}{T} \int_T R_x(t, \tau) e^{-j2\pi\alpha t} dt \tag{2.9}$$

The Fourier coefficient for $R_x^{\alpha}(\tau)$ is evaluated above. If the frequency in question is part of a peak of noise rather than a signal then $R_x^{\alpha}(\tau)$=0 for all α /= 0. [29] The equation $R_x^{\alpha}(\tau)$ is ideally equal to the Fourier Transform of the signal over t is greater than negative

infinity and less than infinity. The Fast Fourier Transform or FFT does not cover the same range as Fourier Series representations. This is because the FFT does not evaluate a signal for t is greater than negative infinity and less than infinity. As performing mathematical operations over a infinite time period is theoretically impossible, the FFT is the best option for finding frequency domain representations of signals. As the signal will be modeled using FFT, the autocorrelation function must be altered in order to accommodate for the errors introduced by FFT.

The SCF or Spectral Correlation Function is a measure of a signal's cyclic characteristics over a frequency f_j. The SCF is the Fourier Transform of R_x^α but performing the Discrete Fourier Transform operation on R_x^α would require a huge amount of computation. In order to lessen the amount of computation required, the SCF must be evaluated over a more realistic range:

$$S_x^{\alpha_k}(f_j) = \frac{1}{NM}\sum_{i=1}^{M} X_i(f_j + \frac{\alpha_k}{2})X_i^*(f_j - \frac{\alpha_k}{2})) \tag{2.10}$$

The function above has been radically altered from its ideal state. Equation (2.10) is the SCF evaluated over a smaller range in order to decrease the number of computations required to evaluate a signal.In this equation, N is the frequency of the FFT and M is the time or frequency sample that the SCF is calculated over. X_i is the short time FFT of $x(t)$ with a bandwidth of $B = \frac{1}{\tau}$, f_j is the frequency of the received signal and α_k is the cyclic frequency[29]. Instead of evaluating the SCF over an infinite range, by performing the Discrete Fourier Transform on R_x^α, the signal is considered for a time period of $i = 1$ to M[29]. The body of the function has also been dramatically changed. Instead of evaluating the SCF as the transform of R_x^α the signal is evaluated for the sum of a function X_i. X_i is the time variant Fourier Transform of the signal $x(t)$ shown in equation (2.11).

$$X_i(t, f) = \int_t -\frac{T}{2}^t + \frac{T}{2}x(u)e^{-j2\pi fu}du \tag{2.11}$$

In equation (2.11), X_i is evaluated over a single period rather than over all t. This means that the SCF has a smaller range to compute and that the signal is evaluated over a much smaller area. This results in a greatly reduced number of computations while the

function continues to operate on the appropriate time range. In addition, the autocorrelation function is evaluated for a shifting frequency range N. This form of autocorrelation is more feasible than a true Fourier Transform because it does not have to evaluate the signal for an infinite time period.

When a signal is combined with a pulse shape to make the signal more visible and peaky on the frequency range, the ideal pulse shape is supposed to have an infinite range over time [11]. This is considered an ideal pulse shape as it decreases the width of the pulse shape in the frequency range which results in a shortened rising-edge in the time domain making each bit more block-like and easier to define. The result of a frequency domain signal that takes up less bandwidth is that the signal will not interfere with neighbouring signals as much. It is impossible to define a signal over an infinite span of time so pulse shapes are shortened to the point that the frequency domain signal falls within its desired bandwidth. The Spectral Coherence function or SC is a measure of the second order periodicity of a stream of data. It is a convenient way to evaluate presence of a signal. All of the previous computations have been displayed in order to provide a background for the SC. The equation for the Spectral Coherence of a signal appears below.

$$C_x^\alpha(f) = \frac{S_x^\alpha(f)}{\sqrt{S_x^\alpha(f + /frac\alpha 2) S_x^\alpha(f - /frac\alpha 2)}} \tag{2.12}$$

This equation provides a graph of the cyclic characteristics of the stream of data at the frequency in question. Each modulation type will have different characteristics. By determining what those are, it is possible to build a profile of a signal. The maximum value for which this equation is evaluated is the most prominent cyclic frequency. Any signal that has the same modulation type will have the same profile and should have the same prominent cyclic frequency.

2.4.4 Matched Filtering

Matched filtering is a spectrum sensing method that is designed to improve signal reception by increasing the Signal-to-Noise-Ratio (SNR). The SNR is the ratio of the signal's power to the power of the noise [11]. This ratio is a good metric that can be used to deter-

mine the reliability of signal reception. A signal is much easier to receive if it has a high SNR. A high SNR indicates the strength of the signal relative to noise.

When a radio signal is transmitted it is filtered using a modulation scheme. The filtering makes the signal more recognizable to a receiver and insures that it can't be decoded without prior knowledge of modulation scheme used by the transmitter. Matched filtering is very similar to demodulating a signal. Demodulation is a process of filtering a received signal in the same way it was filtered by the transmitter to recover as much of the transmitted data as possible. When a signal is demodulated with its correct modulation scheme the output of the correct modulator resembles data more then the output of an incorrect modulation scheme. Figure 2.12 shows an FM signal that has been demodulated by an FM demodulator.

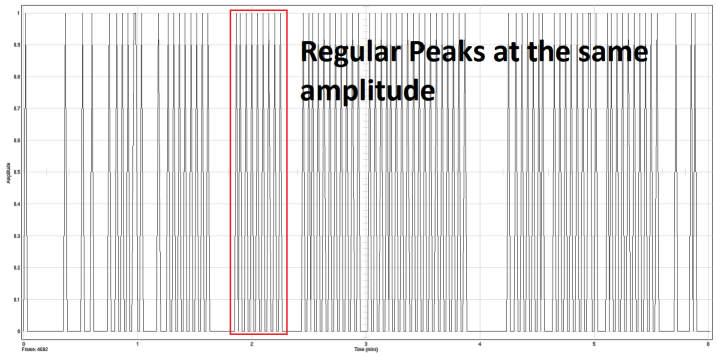


Figure 2.12: Graph of an FM signal that has been demodulated using an FM demodulator. The received information has very regular peaks.

As Figure 2.12 shows the demodulated information appears as regular peaks that can be easily converted into digital information. When a signal is demodulated by a different modulation scheme than was used to transmit it, the output is less uniform. Figure 2.13 shows the same FM signal being demodulated using a BPSK demodulator. As the graph shows the output is much more difficult to convert into data.

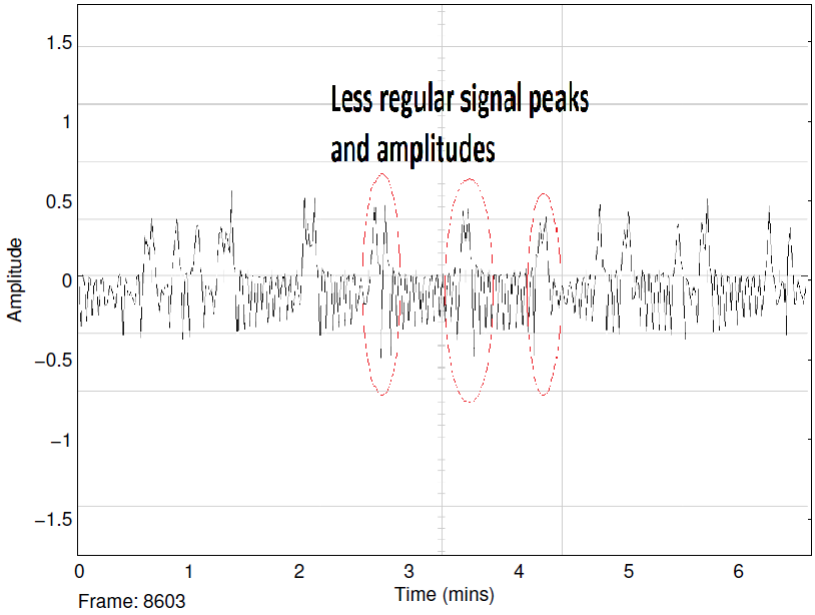


Figure 2.13: Graph of an FM signal that has been demodulated using a BPSK demodulator. As the graph shows the output is irregular and hard to decode.

Matched filtering assumes that when the receiver receives the data it knows all the different possible modulation techniques that could be used to transmit the signal. A matched filter essentially demodulates the signal using all of the possible filters that could have been used to transmit the signal. When the signal is filtered with the correct modulation scheme the output will peak. The outputs of the other modulation schemes will not have peaks because the filtering process will not be matched. Figure 2.14 shows a block diagram of a Matched Filter. Each possible modulation scheme is modelled by a function h(t) and the outputs are compared in the choose max block before a decision is outputted.

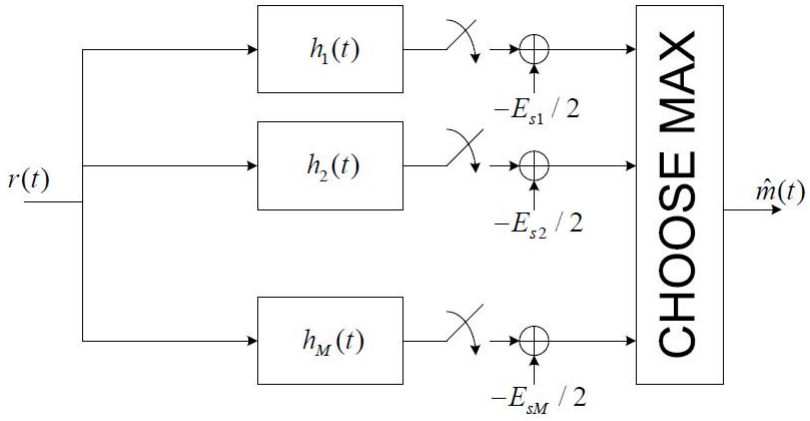


Figure 2.14: Block diagram of a matched filter. Each different modulation scheme is represented by an $h(t)$

[28]

The receiver should be able to differentiate between the correct modulation scheme and incorrect ones by comparing the outputs of each signal and taking the largest value. Matched filtering is not designed to differentiate between a signal and noise because the matched filtering design assumes that the received data will be correctly demodulated by the filters. In order to allow for noise in a matched filtering spectrum sensing scheme, the output of the filters must be compared against a minimum value that is expected to be within the noise floor. This method provides the best results when the SNR of the transmitted signal is already known.

Equation (2.13) is the probability that the matched filter will correctly detect a signal and equation (2.14) is the probability that the matched filter falsely detects a signal. Both equations rely on equation (2.15) or the Q function. The Q function provides probability values for an input x. For these probability equations, x is made up by λ, σ^2 and ϵ. λ is the decision threshold, σ^2 is the noise variance of the signal and ϵ is the signal energy. Equation (2.13 and equation (2.14) examine the probability that $T(x)$, the output of the matched filter is greater then equation (2.1) and equation (2.2) for λ.

$$P_d = Pr\left(T(x) > \lambda | H_1\right) = Q\left(\frac{\lambda - \epsilon}{\sqrt{\sigma^2 \epsilon}}\right) \tag{2.13}$$

$$P_f = Pr(T(x) > \lambda | H_0) = Q\left(\frac{\lambda}{\sqrt{\sigma^2 \epsilon}}\right) \tag{2.14}$$

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{\frac{-t^2}{2}} dt \tag{2.15}$$

These probability equations describe the likelihood of a received frequency being a signal or just noise. The first equation Pd describes the probability of the frequency being a signal and Pf describes the probability of the received frequency only being noise. The ratio of these two probabilities provides additional spectrum sensing data that is used to determine the reliability of Matched Filters decision. Matched filtering is an efficient form of signal identification, although it requires prior knowledge of the frequency in question. Matched filtering is much more reliable if the SNR of the transmitted signal is known beforehand[27].

2.4.5 Cooperative Sensing

There are many different forms of spectrum sensing and each one has its advantages and disadvantages. A popular method for searching through a large range of frequencies while ensuring the precision of signal detection is to use several spectrum sensing methods at once. This method is called cooperative sensing, it ensures that decisions on perceived signals have a greater accuracy as they can be compared against one another. Figure 2.15 shows an example of a system using cooperative sensing to consolidate data from more than one spectrum sensing methed and a variable number of spectrum sensing nodes.

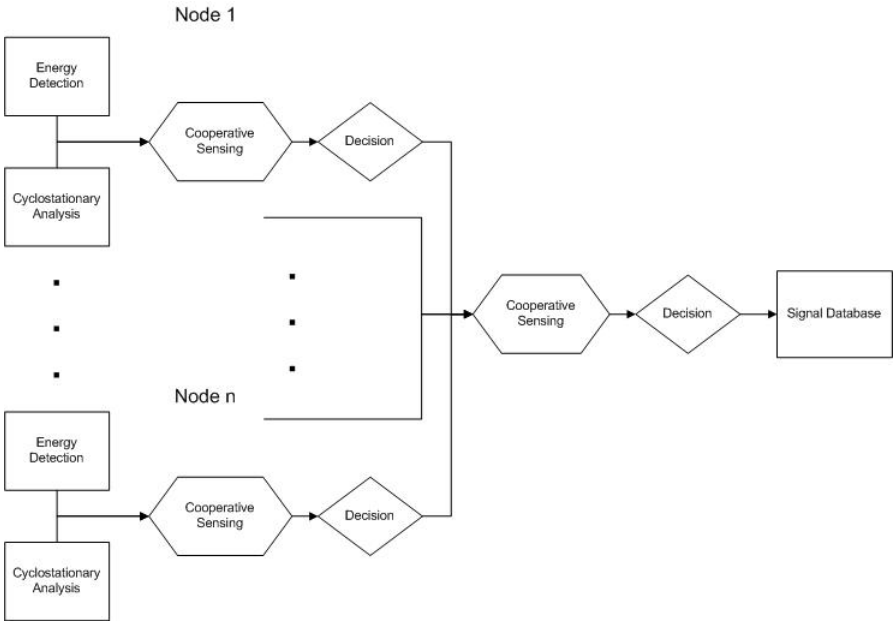


Figure 2.15: Block diagram of the first design of the spectrum sensing scheme. This design is capable of being implemented with a variable number of nodes.

As Figure 2.15 shows, the cooperative sensing blocks compile all of the data from the energy detection and cyclostationary analysis blocks before forming a decision about them and sending that decision from the node to the centralized system. Then the final cooperative sensing block forms decisions on the data from each node and comes to a final decision for the frequency being sensed.

The simplest way to cumulate this data is to use cooperative sensing to combine the output of the spectrum sensing techniques. Cooperative sensing takes in a binary output (0,1) decision from each sensing method after the spectrum sensing method has finalized its decision on the frequency in question[29]. The cooperative sensing algorithm determines if the signal is either real or not for each frequency being scanned. The binary outputs are then accumulated at a central location to perform the last decision on the frequencies and so provide more accurate knowledge about the signal being scanned.

$$D_f = \begin{cases} 1 & : if \sum_{i=1}^{N} di \geq K \\ 0 & : if \sum_{i=1}^{N} di < K \end{cases} \tag{2.16}$$

In equation (2.16), di is the local decisions taken at each node and K is the optimum number of 1s or 0s that determine if the signal is real or not. The ratio between the 1s and 0s determines whether the data in question is considered to be a signal[29]. The reason for all of these different decisions is to make sure that when a signal is finally confirmed, it really is a signal and not noise. In the ideal cooperative sensing environment there are a number of different antennas picking up information about frequencies at a very high sampling rate . All of the summations of the signals are then collected and a more reliable output is determined from the accumulated data.

2.5 Localization

Localization is the process used for determining the location of a wireless transmitter in a wireless network. While there are a wide variety of localization approaches for determining the location of a transmitter, in order to locate analog signals or signals of an unknown modulation type many standard methods for determining the location of a transmitter become impractical. The following section will discuss a variety of localization approaches as well as the pros and cons for each as they apply to the goals of this project.

2.5.1 Time Difference of Arrival (TDoA)

Time difference of arrival is a method for determining a transmitters distance from a set of receivers based on the difference in time it takes the signal to arrive at each of the receive sites. This method for determining the distance of the transmitter from the receiver requires that the signal being observed has some characteristic that can be used for time comparison at all receive sites, as well as accurate time synchronization between all receive sites, as even very small time offsets between receivers can result in significant position estimate error.

In order to make a position estimate for the unknown transmitter, the time of the measurable event is recorded at each receiver. These time measurements would then be subtracted from the first received signal, giving a Δt between the earliest recorded signal, and the measurements from each of the receivers. Given an unknown source location at (x, y) and known receiver locations at (X_i, Y_i), the range difference from the source between the i^{th} receiver, R_i, and the first receiver, R_1, is as shown below, where c is the speed of an electromagnetic wave in free space, $2.99x10^8$ meters per second [25].

$$R_{i,1} = c\Delta t_{i,1} = R_i - R_1 = \sqrt{(X_i - x)^2 + (Y_i - y)^2} - \sqrt{(X_1 - x)^2 + (Y_1 - y)^2} \qquad (2.17)$$

Given that eq. 2.17 is linear with respect to the source location (x, y), the unknown location can be expressed in terms of R_1, $R_1^2 = x^2 + y^2$ for $(X_1, Y_1) = (0, 0,)$[25]. The implementation of TDoA is highly dependent on the stability and precision of the system timestamps. For the purposes of position determination, a 10 nanosecond error is equivalent to an error of approximately 3 meters, with 100 nanoseconds of error, or 30 meters, resulting in a potential position estimate that could be an entire building away.

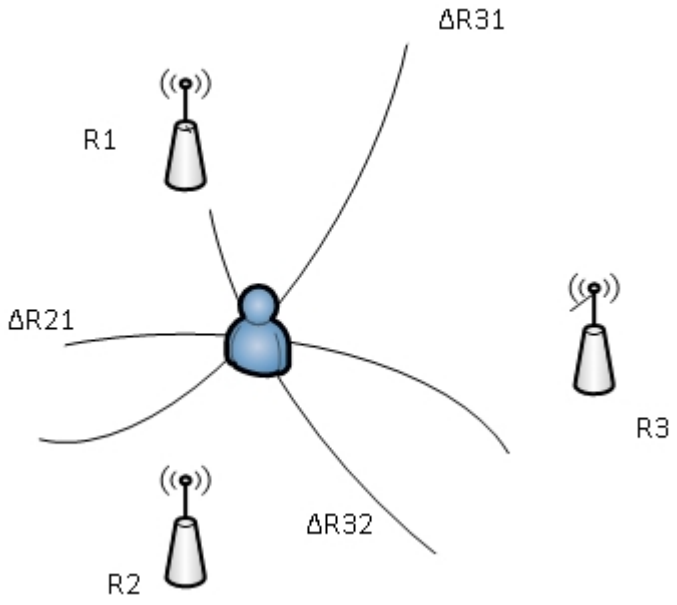


Figure 2.16: Localization using time difference of arrival

2.5.2 Time of Arrival

Time of arrival localization is a process for determining the distance of a transmitter from a receiver based on knowing when a signal is transmitted and comparing this with the time the receiver detects it. This time of flight is then multiplied by the speed of an electromagnetic wave in free space, $c = 2.99x10^8$ meters per second, in order to determine the distance traveled. In order to calculate the time of flight, the receiver must have some knowledge of the time the message was transmitted. This can typically be accomplished in a digital system be observing any timestamp that may be present, however analog systems provide no such timestamp.

Given c, the speed of an electromagnetic wave, t_i for the time of arrival at receiver i, t, for the transmit time, and (X_i, Y_i) for the known coordinates of a receiver, the coordinates of the transmitter can be determined using:

$$c(t_i - t) = \sqrt{(X_i - x)^2 + (Y_i - y)^2} \tag{2.18}$$

by solving the system of equations generated by three or more receivers for x and y. This system is subject to the same time sensitivities as TDoA, with 100 nanoseconds of error being equivalent to 30 meters of position inaccuracy.

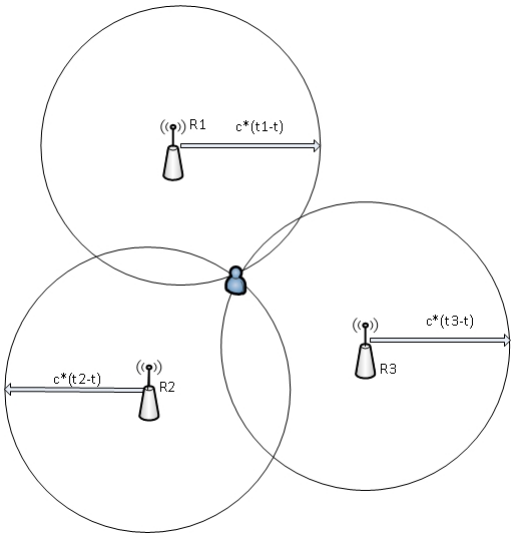


Figure 2.17: Localization using time of arrival

2.5.3 Received Signal Strength

Received Signal Strength based localization takes advantage of the measured signal power at each of the receivers. Since the power of an electromagnetic wave decreases as a function of distance, knowing the power out of the source antenna and this measured power, the range between the receiver and the transmitter can be approximated. In a system with 3 receivers, 2 dimensional localization should be possible in the similar manner to Time of Arrival [19].

In order to determine the the distance between the transmitter and the receiver, the receive power is determine as function of the square of the distance from the transmitter as shown:

$$P_r = \frac{P_t G_t G_r}{4\pi r^2} \tag{2.19}$$

Where P_r is the measured power at the receiver, P_t is the transmitter power, G_t is the transmitter antenna gain, G_r is the receiver antenna gain, r is the distance between the

transmitter and the receiver. In this expression of pathloss, the signal energy is modeled as decreasing with the expanding area of the sphere of radiated energy as shown below in Figure 2.18.

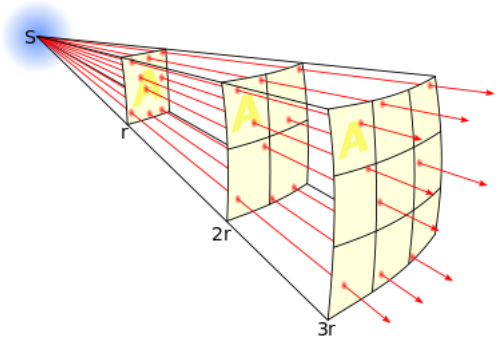


Figure 2.18: Increasing Surface Area for Inverse Square Law [2]

There are more complex models for pathloss which would allow for an RSS based localization method to account for varying channel characteristics. These models would add complexity to the system which is beyond the scope of this project.

2.5.4 Global Positioning System

The Global Position System (GPS) provides highly accurate location information using inexpensive receivers, with coverage of most of the world. GPS consists of 24 to 32 active satellites transmitting on on 1575.42Mhz using a code divison scheme. This technique is realized by assigning every satellite a unique binary code which is XORed with the data being transmitted. The receivers on the ground will then correllate the received data with all of the possible satellite codes, in order to seperate the messages from individual satellites [10].

The individual satellite messages contain information such as the current system time, and the locations of the satellites. Given the locations of the satellites, as well as the calculated time of travel from the satellites to the receiver, GPS takes advantage of a technique

similar to TDoA to calculate the position of the receiver. The accurate timestamping required to perform this localization is only possible because each GPS satellite is capable of maintaining a highly accurate clock, and each receiver determines its current time through the interpretation of satellite data. This accurate clock information is used for the synchronization of clocks across cellular telephone systems, and other time critical applications [10].

2.6 Data Fusion

Data fusion is the process for combining raw data from a number of sources or sensors in order to produce a more accurate or usable set of data. [14] In order to provide the most accurate location data for all transmitters within the area of interest, an efficient method of utilizing sensors in the network must be developed to maximize the frequency range that can be scanned while still providing enough sensors to accurately localize transmitted signals.

The simplest form of data fusion is voting data fusion. In this system each sensors output is tallied, with the selection receiving the most sensors voting for it as a solution being the output of the system [14]. This system is typically implemented with the output being the result of a simple majority, although as the number of voters, in this case receivers, is increased, more strict requirements such as three quarters, or nine tenths majority can be required.

In an approach similar to voting fusion, using the weighted average for data fusion makes a selection based on the most popular decision amongst all of the receivers. The difference in this case is that each receiver is assigned a weight, determined by an estimate of the quality of its measurement as affected by environmental characteristics.

Since the sensors are expected to function cooperatively in order to determine the location of a transmitter, their searches must be synchronized and the measurements must have a defined relationship. There are a number of approaches for both of these tasks, ranging from using the network backhaul for calibration and synchronization to comparison against a commonly available source such as the GPS.

2.7 Background Summary

This section provided the background necessary to understand all of the different techniques and methods of performing spectrum sensing, data fusion and localization used in the project, as well as detailing software defined radio and P25 public safety communications. Understanding each algorithm and process described in this section is essential to understanding the project. Though some of the information described in these sections is not used in the final design of the project, each piece has is purpose.

Chapter 3

Proposed Approach

This chapter will provide an overview of the project structure, ranging from a high level system layout to the project logistics and goals. The innovation this project provides as an extension of existing research will also be discussed.

3.1 System Structure

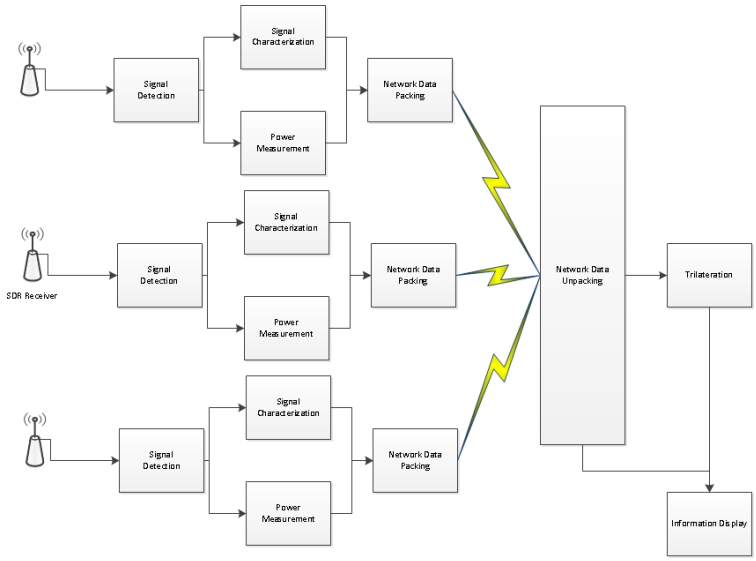


Figure 3.1: System Overview showing the signal path from detection to measurements, trilateration, and display

This project will develop a system to detect, characterize and determine the location of public safety responders based on their two-way radio usage. In order to do this, a system of networked SDR receivers will be developed to detect transmissions, and determine a transmissions modulation scheme and power. This data will then be sent over the network to a central control unit which will combine the received power measurements in order to produce a location estimate. A system overview is provided above in Figure 3.1.

3.1.1 Hardware and Software

The programming for this project was implemented on the Universal Software Radio Peripheral version 2 or USRP2s. These software-defined radio systems contain an FPGA and the capability to transmit and receive in a wide range of frequencies. The capabilities of the USRP2s are dictated by their daughter cards. These cards determine what frequencies and other specifications the USRP2s can utilize. Two different daughter cards were used to test and implement the algorithms for this project. They were the XCVR2450s which have a frequency range of 2.4 to 2.5GHz and 4.9 to 5.9GHz. The XCVRs could not received or transmit on the same frequencies as public safety radios so actual implementation of the project was done using WBX boards which have a range of 50-2200MHz. As this project was sponsored by MATLAB and MATLAB has software-defined radio capabilities that interface with the USRP2s, the project was implemented using Simulink, a MATLAB based programming language.

3.1.2 Spectrum Sensing

The purpose of this project was to design a mechanism to sense and locate public safety responders in the field. The mechanism would observe a large bandwidth of frequency at once. Every 5kHz the system would perform spectrum sensing and characterization operations to determine if a signal is present. These operations would be performed many times a second in order to collect a large amount of data for each frequency. The data would then be combined to form a decision about the frequency.

This information along with the received power of the signal, and timing and location data from a GPS unit would be sent from each receiver node to the central controller. There

it would be compared against all the other nodes and a final decision would be made about the frequency. If the receiving nodes decided there was a transmission on the frequency then the controller would perform localization to determine where the public safety radio was transmitting from.

In order to sense all of the public safety responder's radios the spectrum sensing system had to be able to determine accurate sensing data and perform all of the computations to sense signals without losing possible radio transmissions. These constraints lead to a number of different approaches to performing spectrum sensing. Due to the time constraints of the project, the final design did not incorporate a scanning system to sense all of the possible public safety radios in the spectrum at once.

This problem poses a number of challenges to reliably characterizing all of the responders in the field at once. Public Safety responders do not all use the same modulation schemes or frequencies when they communicate with one another. This is because many different public safety organizations use different radio systems. The most widely used of these communications standards are Public Safety P25 and analog. In order to simplify the process of sensing all of the public safety responders, the project assumed that only P25 and analog signals were utilized.

3.1.3 Localization

In addition to determining the frequency and operating mode of a detected transmission the project will make a location estimate for the transmitter. This location information could be used by during an incident requiring a large emergency respond to allow an incident coordinator to track the locations of every responder. Having this knowledge immediately available, without having to request it from separate dispatchers may greatly reduce respond time. Taking advantage of the signal power measured at the receiver, and a model for signal attenuation between the transmitter and receiver, the system will estimate the distance from each receiver to the transmitter, and use this information to estimate the transmitters location.

3.1.4 System Integration

The two main subsystems for this project were developed independently and simultaneously prior to their completion and integration to form the completed system. After the demonstration of the functionality of the scanning receivers, and the simulation of the localization module, the central controller was developed to communicate with the receivers using the Instrument Control Toolbox UDP Send and UDP Recieve blocks, as well as execute the localization algorithm.

The Instrument Control Toolbox provides a simple way to communicate between MATLAB and Simulink instances across multiple machines. As long as all of the data that is being communicated can be sent as the same data type, and the IP addresses of both the sender and receiver are known ahead of time, communication between computers is as simple as communication between blocks within the same Simulink model. The simplicity of the operation of these blocks lead to their selection over the implementation of a custom network infrastructure, or the use of the USRP2s to transmit measurement data.

The independent display of receiver data, or the calculations of locations using data sent over the network using the Instrument Control Toolbox was implemented without encountering any serious issues. Using receiver measurements to make position estimates did not prove to be as simple. Attempting to make position estimates with measurements made by the distributed receiver nodes revealed the substantial issues with the software and hardware implementations of power measurement.

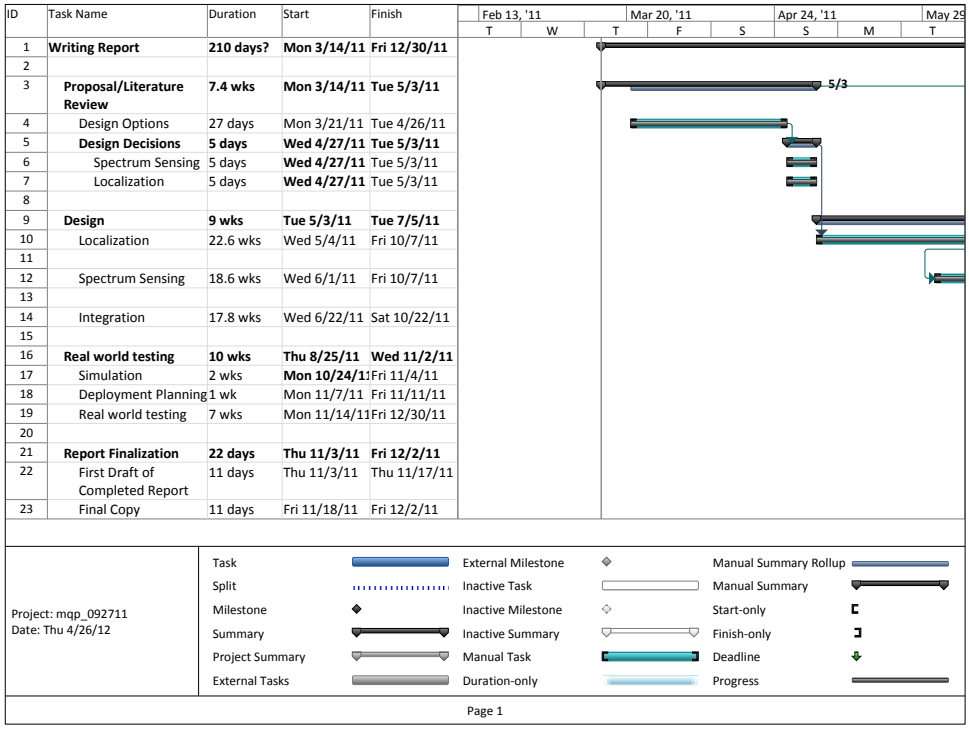
3.1.5 Uniqueness

Though other projects have performed similar work to scan and locate unknown transmissions, this project is unique. The main difference between this project and other similar, is that other projects have not implemented their work in real time. There is a major difference between being able to scan a large block of frequencies and detect public safety responders in real time compared to purely in simulation. This project will be able to perform all of the necessary operations across the entire band of frequencies being examined fast enough that no transmissions are lost. In addition to creating a real time network this

project will be capable of receiving information from three or more different nodes rather then being restricted to exactly three. This means that it will be able to take in data from a variable number of nodes all transmitting data back to the controller.

3.2 Project Logistics

This project was conducted over the course of one year, beginning in March of 2011 and concluding in April of 2012. It was initially expected to complete the project in December of 2011 as shown below in the Gantt Chart Figure 3.2, but this date was pushed back due to system integration issues.



ID	Task Name	Duration	Start	Finish
1	**Writing Report**	**210 days?**	**Mon 3/14/11**	**Fri 12/30/11**
2				
3	**Proposal/Literature Review**	**7.4 wks**	**Mon 3/14/11**	**Tue 5/3/11**
4	Design Options	27 days	Mon 3/21/11	Tue 4/26/11
5	**Design Decisions**	**5 days**	**Wed 4/27/11**	**Tue 5/3/11**
6	Spectrum Sensing	5 days	**Wed 4/27/11**	Tue 5/3/11
7	Localization	5 days	**Wed 4/27/11**	Tue 5/3/11
8				
9	**Design**	**9 wks**	**Tue 5/3/11**	**Tue 7/5/11**
10	Localization	22.6 wks	Wed 5/4/11	Fri 10/7/11
11				
12	Spectrum Sensing	18.6 wks	Wed 6/1/11	Fri 10/7/11
13				
14	Integration	17.8 wks	Wed 6/22/11	Sat 10/22/11
15				
16	**Real world testing**	**10 wks**	**Thu 8/25/11**	**Wed 11/2/11**
17	Simulation	2 wks	**Mon 10/24/11**	Fri 11/4/11
18	Deployment Planning	1 wk	Mon 11/7/11	Fri 11/11/11
19	Real world testing	7 wks	Mon 11/14/11	Fri 12/30/11
20				
21	**Report Finalization**	**22 days**	**Thu 11/3/11**	**Fri 12/2/11**
22	First Draft of Completed Report	11 days	Thu 11/3/11	Thu 11/17/11
23	Final Copy	11 days	Fri 11/18/11	Fri 12/2/11

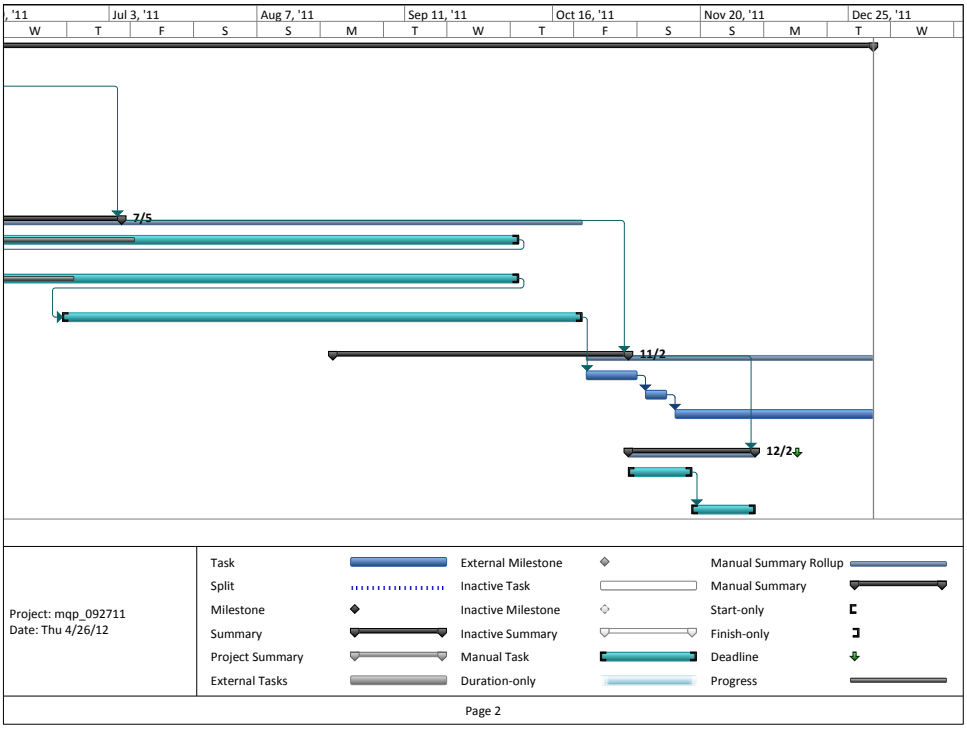


Figure 3.2: Intial project timeline

As Figure 3.2 shows, the first seven weeks of the project were spent conducting the initial literature survey. This time was used to determine the current need and state-of-the-art for similar systems, as well as conduct research into algorithms to accomplish the required tasks. At the end of this seven week period, the particular algorithms to be implemented were decided, with the implementation of these algorithms to occur over the summer.

Models for the individual subsystems for Spectrum Sensing and Localization were developed after design decisions were finalized, into the beginning of the next academic year, with individual systems being completed by the begin of October, The completion of an individual system would be determined by it successfully functioning under simulation, or in a controlled environment. The thorough testing of individual components before integration into the larger system prevents the compounding of system flaws. After all subsystems had completed their simulations and tests, the team would begin system integration.

Once functionality of the integrated system was confirmed using simulated radio data, small scale testing would be conducted with two-way radios in order to obtain initial values and calibration data for the system. When the system could reliably determine the location and characterization information of a single transmitter, the system would be transitioned to large scale testing in an outdoor environment.

Upon the conclusion of successful indoor simulations in the beginning of November, an outdoor deployment was planned, taking advantage of WPI's large amateur radio community as a model for public safety responders to test the system under real world conditions. Since the radios used by these operators operate using the same modulation techniques, and on frequencies very near to the public safety bands, being able to accurately track their transmissions would indicate proper system functionality without violating the security of any local police departments.

3.3 Problems Encountered

The project encountered a number of obstacles which prevented the development of a fully functional prototype. The most severe of these problems was the limited access to accurate timing and power measurement data. Despite the improvements in the communications between the computer and the USRP2 that were made with the switch to the Universal Software Radio Peripheral Hardware Driver (UHD), the Simulink software package still does not provide any access to radio timestamping, and in fact it introduces significant delays of its own into signal measurement. This eliminates the possibility of using TDoA, or ToA completely, making only RSS based localization feasible.

Unfortunately, power measurements also seem to be very inaccurate, and vary significantly between different radios under the same controlled conditions. One proposed cause for this may be the implementation of automatic gain control (AGC) on the USRP2 [12]. The Simulink software package does not provide access to the AGC settings or configuration, preventing the recording of accurate power measurements.

In addition to the difficulties imposed by lacking software and hardware functionality, the project faced an additional challenge due to the number of computers required to develop the integrated system. In order to have a test system with 3 receivers, a transmitter, and a central controller, the team required access to 5 computers with access to the site wide MATLAB license at WPI. The only available machines suitable for this experiment where in a public laboratory, where MATLAB was updated in sync with the MathWorks' 6 month release cycle. Due to the length of the project, and the lack of maturity in the USRP interface blocks, each release during this cycle broke substantial portions of the already developed system, requiring major rewrites twice during the systems development.

The problems encountered during the development of the system ultimately prevented the complete functionality of the prototype. There are a number of steps that can be taken to resolve these issues for future systems, and they are described in Chapter 6.

3.4 Proposed Approach Summary

This section provided an overview of the project's proposed approach to performing distributed spectrum sensing and localization of two way radios as well as planning for the duration of the project. There are two main parts of the system, localization and spectrum sensing. Each piece is an essential part of the project design. In addition to these parts of the project this section discussed the logistics of the project, the hardware and software to be used, how the two components of the system will be integrated and how this approach differs from other similar work.

Chapter 4

Prototype Implementation

This section provides an overview of the different designs that were implemented during the project. Due to the nature of the problem many different approaches were not successful. This section details how those designs were implemented as well as their outcomes.

4.1 Spectrum Sensing

There are many ways to perform spectrum sensing and each signal detection method has its advantages and disadvantages. In order to develop an effective spectrum sensing system it is often necessary to combine a number of forms of spectrum sensing to create a best fit spectrum sensing system. This project examined five different forms of spectrum sensing. These are energy detection, cyclostationary analysis, matched filtering, cooperative sensing and Power Spectral Density comparison. Each method can be used as a signal identification method, though some are better than others.

This spectrum sensing system developed for this project was designed with a number of expectations about the type of transmissions to be received. The spectrum sensing system assumed that the only transmissions in the spectrum analyzed would be modulated using either Analog FM or digital C4FM. This means that the spectrum sensing system will only be able to identify a received signal as either an analog transmission resulting from Analog FM modulation, a digital transmission resulting from C4FM modulation or noise.

Performing spectrum sensing can be a complicated and computationally intensive be-

cause the system must search through a very large band of spectrum to find signals. This means that sensing can become less precise the larger the frequency range. This is because the more sensing needed, the larger amount of time it takes to sense the whole range of frequencies. This can result in data loss because the sensing system cannot sense all of the frequencies in the public safety spectrum in real time. Fortunately, this project is focused on searching for emergency radios using the P25 standard. P25 standard is an emergency radio communication system that has been designed in order to allow many different emergency systems to coordinate with each other using one communication method. This is useful for this project because the P25 is channelized. This means that the modulation frequencies that are used to transmit data are each separated by a certain width of frequency. Each transmission is supposed to be separated from its neighbor by 30kHz allowing for a sufficiently large gap between transmissions so that interference can be avoided. Although P25 radios maintain this characteristic when transmitting using C4FM, legacy systems using analog FM are not restricted to same 30kHz separations. In order to account for a certain amount of disparity in carrier frequency, the spectrum sensing system will be designed to search every 5kHz rather than every 30kHz thus ensuring that all frequency ranges are accounted for.

4.1.1 Spectrum Scanning

The original concept of the project was of a system capable of scanning through a large bandwidth of spectrum, detecting signals, characterizing them and sending back data to a central controller that could find the location of the transmitters based on the timing data from GPS devices. An early design of the energy detector was combined with a scanning system that was able to scan through 8MHz spectrum continuously. The tests spanned 442MHz to 450MHz of spectrum in the UHF public safety band. Figure 4.1 shows the Simulink diagram for the spectrum scanner.

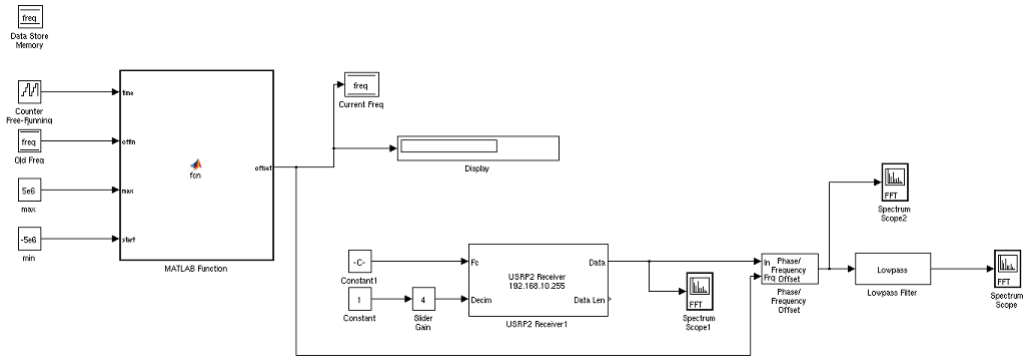


Figure 4.1: A Simulink flow diagram of the spectrum scanner. The spectrum scanner searches through a large range of frequencies analysing each one before making a decision and moving on to the next.

The system was designed as a test to see if the energy detector was capable of detecting actual transmissions. This meant that the test did not attempt to transmit actual signals into the spectrum. Unfortunately the computers that were being used to perform the scanning tests were updated with a new version of MATLAB. This update broke compatibility with the system being used to simulate GPS timing while indoors, eliminating time stamping functionality. Without the data from the simulated GPS units the scanning system could not perform reliably and was abandoned.

4.1.2 Energy Detector and Cyclostationary Analysis

The first design used for the project's spectrum sensing system was a system that combined energy detection, cyclostationary analysis and cooperative sensing. Energy detection has two major drawbacks: it cannot tell the difference between a signal and an especially high powered peak of noise and it cannot sense a signal below the noise floor. Cyclostationary analysis measures a stream of data to determine if there are signal attributes detected at regular intervals. Cyclostationary analysis is a far more accurate measure of signal properties than energy detection, and therefore a more accurate sensing technique. Cyclostationary analysis does have a serious flaw; it can be very computational intensive.

Cooperative sensing can by implemented by taking input from a large number of different spectrum sensing algorithms as well as a large number of different sensing nodes. It combines all of this data and compares it to determine the probability of a signal's presence.

The initial spectrum sensing design intended to counteract the drawbacks of energy detection and cyclostationary analysis by combining them. The energy detector would search through a large range of spectrum and sense all the peaks that could be a signal in order to attempt to locate all the possible signals. The output of this design would contain a large number of good signals, accompanied by a lot of noise peaks that did not contain signals. The energy detector would then feed all of the possible signals to the cyclostationary analysis block for processing. The cyclostationary analysis block would only need to perform computations on the possible signals that the energy detector found rather than searching through the entire spectrum. This scheme would counteract the unreliability of the energy detector and the computation problems with cyclostationary analysis by combining both spectrum sensing schemes. The system would be implemented at a large number of nodes and each separate frequency that the systems sensed, would have a large number of samples per node. This data would be fed into a cooperative sensing block resulting in more reliable data computed from the large sample. Figure 4.2 shows a block diagram of the intended spectrum sensing design.

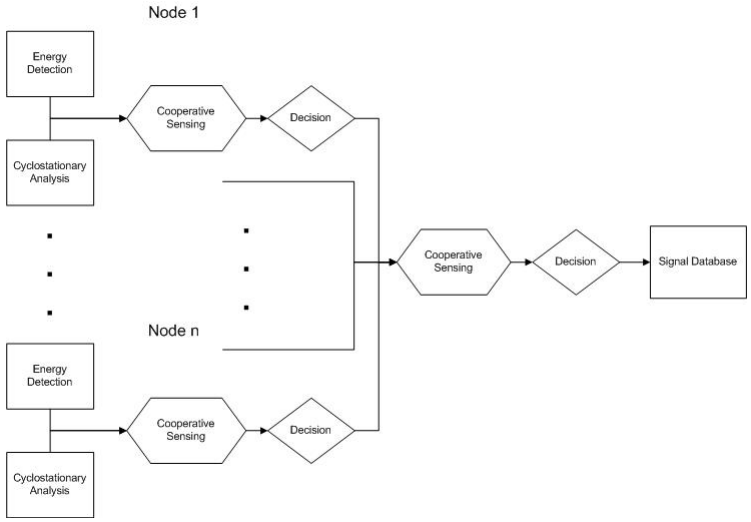


Figure 4.2: A block diagram of the first design of the spectrum sensing scheme. This design is capable of being implemented with a variable number of nodes.

As Figure 4.2 shows the spectrum sensing system could implement N number of nodes and process the data from those nodes in order to provide more reliable data about the frequency being sensed. The system would first perform energy detection and cyclostationary analysis before analyzing the large number of samples from the spectrum sensing schemes and forming a decision about the frequency using cooperative sensing. That decision would then be transmitted from the node to a central receiver where cooperative sensing is performed again before a final decision is made on the frequency.

The project adopted Otsu's energy detection scheme. This scheme is a reliable form of energy detection though is suffers from the same problems as more basic energy detection algorithms. Figure 4.3 shows the Simulink block constructed to perform Othu's energy detection scheme.

Figure 4.3 includes a spectrum scope from the Simulink library in order to confirm the output of the Energy Detector visually. During testing and implementation of the spectrum sensing method the scope will be removed in order to speed up the signal detection

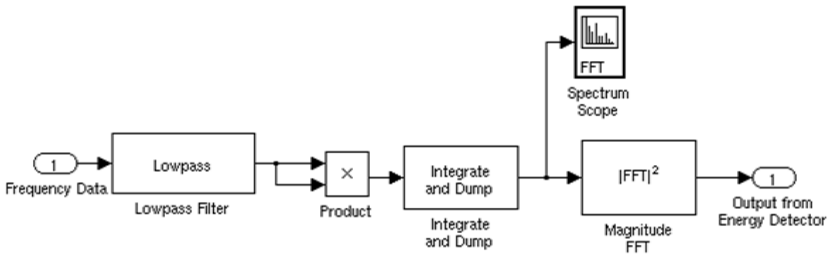


Figure 4.3: A Simulink model of Otsu's energy detection scheme. Each block performs an important task of energy detection.

processing. Though the implementation of the Energy Detection block was successful, the cyclostationary analysis block was not as reliable. This meant that the spectrum sensing portion of the project would have to examine other means of sensing.

The Energy Detection and Cyclosationary Analysis spectrum sensing system was abandoned due to constraints from the equipment at hand and the time it would take to implement cyclostationary analysis and test it. Cyclostationary analysis is a very complicated and computationally intensive spectrum sensing system. It has to perform a number of tasks that take a long time to compute using the software provided for the project. This meant that it would be impossible to scan the large amount of spectrum fast enough to capture data from each frequency without losing possible transmissions. The USRP2s can only search a certain bandwidth of frequency at a time, and hence were not fast enough for the project. Once the spectrum sensing scheme had completed computing one frequency band, a public safety responder could have transmitted on a different frequency and stopped transmitting before the scheme sensed it.

4.1.3 Energy Detector, Matched Filter and PSD Characterization

The next design that was considered for the spectrum sensing portion of the project was a three phase system that used the working energy detector, matched filtering and Power Spectral Density (PSD) characterization to sense the frequency bands. Matched filtering is designed to reduce the SNR around the desired signal to determine if the received information is a real signal or not. When a signal is transmitted using a specific modulation scheme

a frequency domain plot of the PSD of the signal takes on the shape of the modulation filter used to generate the signal. PSD characterization compares the characteristic shape of one modulation scheme to another in the frequency domain.

The intended design of the new spectrum sensing system would perform all of the different forms of sensing simultaneously on one frequency. This meant that the speed of the sensing system would be limited by the speed of the slowest form of sensing. As the energy detector was already working, the immediate focus was implementing matched filtering and PSD characterization. PSD characterization was designed to take in a received signal, convert the signal to its PSD and compare that against a pre-generated PSD of both C4FM and Analog signals. The Simulink design of the PSD characterization sensing system appears in Figure 4.4.

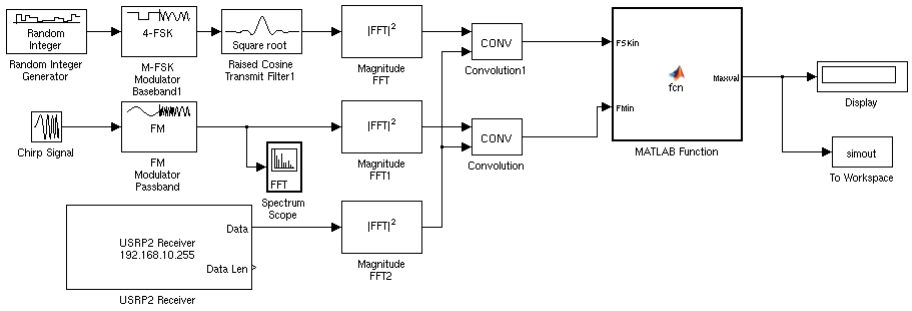


Figure 4.4: A Simulink model of PSD characterization. The top left portion of the model simulates a 4-FSK signal while the middle left blocks model an FM signal.

Figure 4.4 shows the PSD of the received signal was generated by creating a model of a received signal using random data and modulation block from Simulink. There are two signal generators that provide sample PSDs to compare against received signals. Figure 4.5 shows how the FM PSDs were generated.

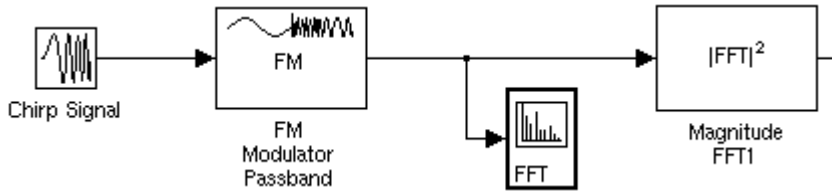


Figure 4.5: A Simulink model of FM signal generation. This data is created in order to perform PSD characterization.

The second signal generator creates a sample 4-FSK signal. Each sample signal is convolved with the received signal and the maximum is compared for each frame. Figure 4.6 shows how the sample 4-FSK signal was generated.

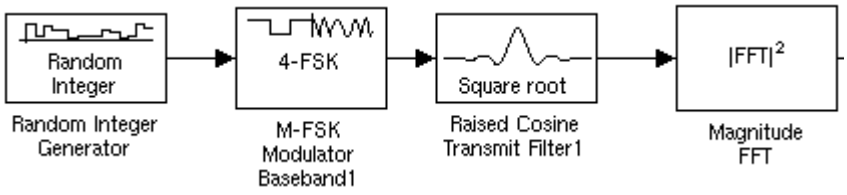


Figure 4.6: A Simulink model of 4-FSK signal generation. This data is created in order to perform PSD characterization.

This form of signal modelling was not ideal because the signal generation taxed the performance of the system thus increasing the amount of time needed to perform the sensing. Due to the nature of C4FM and analog transmissions it was impossible to differentiate between the PSDs of the two signals. They are both so similar that it is impossible to tell the difference between them in a non ideal setting.

There is not enough difference between the frequency domain PSDs of each signal to perform characterization. This is because C4FM is composed of a pulse shaped filter and an analog FM modulator. This means that both the analog (FM) signals and digital (C4FM) signals that the project is comparing are modulated in the same way to generate a signal. The project decided not to pursue PSD characterization due to this difficulty.

Matched filtering is a more reliable form of spectrum sensing then PSD characterization. Matched filtering relies upon signal demodulation while PSD characterization depends on the spectral shape of a signal in an already noisy environment. Signals are fundamentally designed to be recoverable by demodulation and most modulation schemes are designed to be fundamentally different from other schemes. A matched filter should be able to definitively differentiate between two different modulation schemes and determine if a received signal is a transmission or noise. It does not suffer from the deficiencies of energy detection. Despite being unable to use PSD characterization, the project decided to continue implementing the current spectrum sensing system using only energy detection and matched filtering sensing methods. Though the system would not be as robust as one that incorporated a working PSD characterization scheme as well, a system that incorporated both energy detection and matched filtering would be more reliable then a system that only used energy detection.

The matched filter would demodulate received data using an FM demodulator and a C4FM demodulator. The output of this was then compared against a perceived noise threshold and a decision was made to determine if the signal was analog, digital or noise. Matched filtering is similar to PSD characterization because it differentiates between Analog and Digital signals unlike energy detection which cannot characterize a signal. A Simulink model of the matched filter is shown in Figure 4.7.

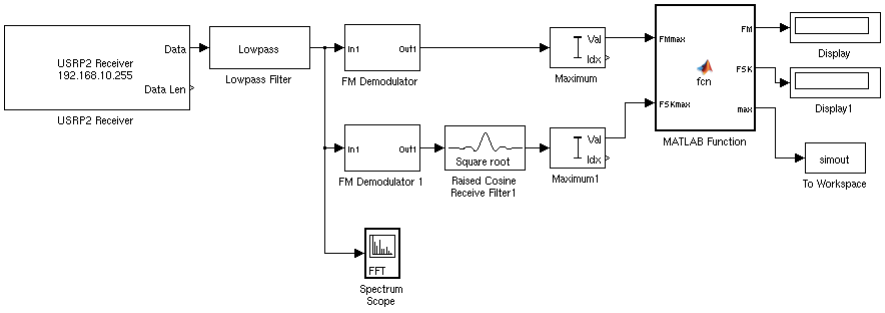


Figure 4.7: A Simulink model of matched filtering. The received signal is demodulated as an FM signal and as a C4FM signal and the outputs of each are compared.

Figure 4.7 shows the model of the matched filter designed for the project. This model

is made up of a number of different subsections. The decision between Analog and Digital signals is decided by taking the maximum of the output of the two demodulators and comparing that to a threshold value. The maximum values are compared to each other inside the MATLAB Function block. Before the outputs of the signals can be compared the received signal has to be demodulated as both a C4FM signal and an FM signal. Figure 4.8 shows the FM demodulator. If the output of this demodulator is higher then that of the C4FM demodulator then the signal is most likely an analog FM transmission.

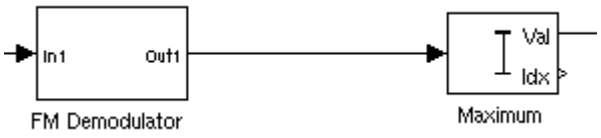


Figure 4.8: A Simulink model of an FM demodulator. Once the signal is demodulated the largest value in the frame is send to the next part of the model.

The maximum value for each frame is examined because each frame should provide a good sample of the received signal and the correct demodulator should have a significantly higher output then the other signals. In order to reliably differentiate between the different modulation schemes the Matched Filter has to demodulated the received signal as both an FM and C4FM signal and compare them. Figure 4.9 shows the signal demodulated as C4FM.

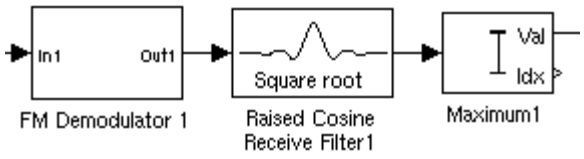


Figure 4.9: A Simulink model of an C4FM demodulator. C4FM is very similar to FM which is why the demodulation schemes are so similar.

The matched filter design in Figure 4.7 is simple but effective and it would have performed well if the modulation schemes had sufficiently different characteristics. Unfortunately due to the nature of C4FM and FM modulation the matched filter was unable to tell the difference between the different forms of modulation. This is because C4FM is a modulation scheme that was implemented by P25 public safety standard to be backwards compatible with analog transmission. The design for the project was stumped again in the same way that PSD characterization had been.

4.1.4 Matched Filter/Autocorrelation Scheme

The final design for the project implemented a combination of matched filtering and cyclostationary analysis. There are very few differences between analog FM and digital C4FM. The similarity between these two modulation schemes has caused problems with many of the previous spectrum sensing schemes. The spectrum sensing scheme not only needs to identify the difference between a signal and noise, it has to be able to differentiate one modulation scheme from the other. The conventional approaches to spectrum sensing could not provide reliable characterization to differentiate between analog and digital transmissions. In order to devise a reliable system that could characterize signals as well as differentiate signals from noise the project had to investigate the modulation schemes further.

P25 digital transmissions are transmitted with a barker code that is sent at the start of every frame. This code contains information about the origin of the signal and the characteristics of the information being sent. The barker code or Header Data Unit (HDU), contains information about the encoding for the digital signal as well as the manufacturers information. If this part of the signal is demodulated and interpreted it can be used to decode the signal in its entirety. The purpose of the project is not to receive and understand a signal but to find it, localize it and characterize it. The same HDU is transmitted every 180 microseconds for the entirety of the transmission. This is because a receiver may only pick up a signal midway through transmission. Many modulation schemes are designed so that no matter when a receiver taps into the transmitted signal, the receiver can still demodulate it and understand it. These modulation schemes send their transmissions in

frames cutting the signal into sections and adding a barker code to the front of the frames. This way if the receiver doesnt read the start of a barker code, the receiver can pick up the next frame from the transmission without losing data. In terms of practical spectrum sensing, this means that every 180 microseconds there is a piece of repeating data that isn't in analog transmissions. In order to use that information to characterize a signal the spectrum sensing scheme has to be able to recognize a repeating input.

Autocorrelation is one of the algorithms in cyclostationary analysis. It compares a signal to itself to see if there is any repetition over time. In order to measure the cyclic repetition of a signal, autocorrleation convolves a signal with its inverse. The output of this convolution will show peaks at places where the signal has repetitions. Cyclostationary analysis examines the output of this theorem further to determine if there are any recognizable patterns in the signal over a sampling period. Autocorrelation was observed to be an excellent method to detect the HDU in a P25 C4FM signal. When the C4FM signal is received the data cannot be autocorrelated to find the barker code directly. The signal is much easier to compare once it has been demodulated and the information converted to a digital format.

The design for the matched filter/autocorrleation scheme combines aspects of both matched filtering and cyclostationary analysis. The scheme takes in a received signal, demodulates it as C4FM and then performs autocorrelation on the resulting output. The spectrum sensing scheme is designed so that the output of the autocorrelation algorithm will have peaks of signal power at specific intervals. By measuring the output power at these time intervals, the spectrum sensing scheme differentiates between noise, analog FM signals, and digital C4Fm signals. The Simulink design for the matched filter/autocorrelation spectrum sensing scheme is shown in Figure 4.10.

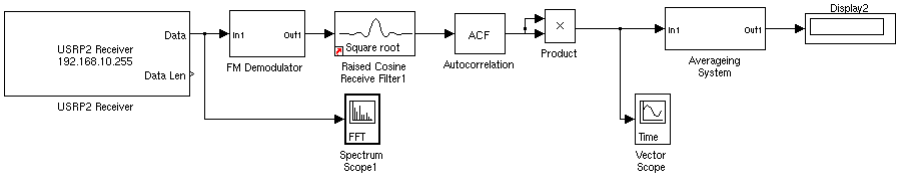


Figure 4.10: A Simulink model of the autocorrelation/matched filtering spectrum sensing scheme. The signal is first demodulated as a C4FM signal, then autocorrelated and the output averaged before a final value is output.

Figure 4.10 shows the Simulink design of the matched filter/autocorrelation spectrum sensing scheme. During testing, the output of the autocorrelation block showed that digital communications had similar peaks at the same time intervals as analog transmissions. These peaks were caused by harmonics in the analog transmissions that have similar periodic qualities to the frame length intervals in digital transmissions. Fortunately the values from autocorrelation for the analog transmissions are at different levels than the digital transmissions. In order to combat these problems the output of the matched filter was squared in order to widen the gap between analog and digital transmissions and a running average was placed on the output of the autocorrelation block. These precautions made it possible to differentiate between analog and digital signals as well as noise.

4.1.5 Spectrum Sensing Prototypes Summary

The project examined several different spectrum sensing schemes in order to perform spectrum sensing and signal characterization. Many of these schemes were unable to perform reliable characterization due to the nature of the types of signals examined. C4FM and FM signals are very similar which makes differentiating them complex. The final design of the spectrum sensing system is capable of differentiating the two modulation types by examining the received frames, taking advantage of the fact that C4FM signals are digitized and are contained in an envelope while analog signals are not. Table 4.1 shows the results of each spectrum sensing scheme.

Table 4.1: Results of Spectrum Sensing Designs

Spectrum Sensing Schemes and Their results		
Spectrum Sensing Scheme	Signal Detection	Signal Characterization
Energy Detection	Working	Incapable
Matched Filtering	Working	Unreliable
PSD Characterization	Working	Unreliable
Autocorrelation and Matched Filtering	Working	80 Percent Reliability

The results of the project are a spectrum sensing system that is capable of performing signal detection and signal characterization with a reliability of 80 percent. Every spectrum sensing system was capable of differentiating a signal from noise, though only the autocorrelation and matched filtering scheme was able to perform reliable characterization.

4.2 Sensor Fusion and Localization

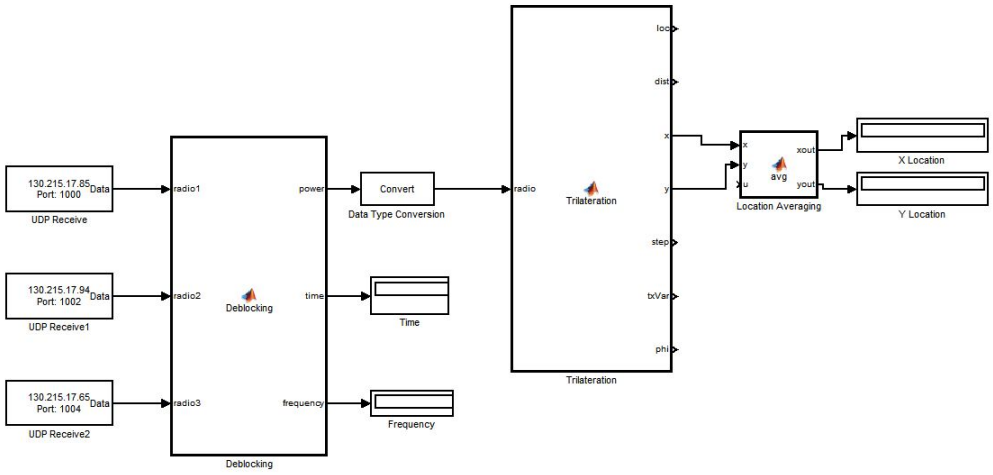


Figure 4.11: Simulink Model of System Central Controller

The central controller, shown above in Figure 4.11 for the project is responsible for the combining all sensor data to produce the location of the detected transmitter. This system takes inputs over the network from the three receiver modules using the Simulink Instrument Control Toolbox, and passes this data to a MATLAB block which combines the data from the three sensors and repackages it for the trilateration module, which will be described in Section 4.2.3.

4.2.1 GPS Synchronization and Receiver Positioning

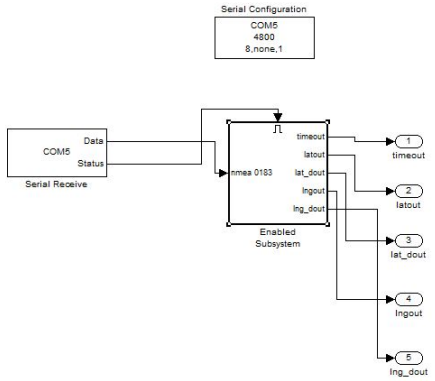


Figure 4.12: Simulink models showing the top layer of the GPS receiver

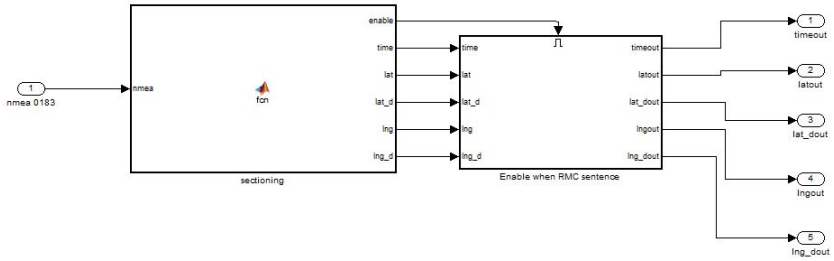


Figure 4.13: Simulink models showing the sentence sectioning portion of the GPS receiver

A Simulink model, taking advantage of GPS was developed to provide highly accurate time synchronization for the scanning receivers, as well as position information for each of the receivers. The develop of this module was initially challenged by Simulink's lack of a char datatype, as the GPS sentence is transmitted as ASCII characters. Taking advantage of the uint8 datatype, a block was developed to break down the time, latitude, and longitude for each receiver so that it might be used in other parts of the model.

The GPS module developed interfaces with a standard USB GPS receiver, using the Serial Receive block from the Simulink Instrument Control Toolbox, as shown above in

Figures 4.12 and 4.13. When the GPS receiver indicates that it has received a GPS sentence, it enables the sectioning block which passes the received sentence to a MATLAB script to break the sentence down into the integer and decimal components of the latitude and longitude, as well as the time. This MATLAB script checks to see if the sentence being passed in is a position sentence (with the header GPRMC) and then divides the vector according to the National Marine Electronics Association (NMEA) 0183 standard sentence format [21], and performs the conversion from ASCII to integers where appropriate. After the data is broken down and converted to integers, the values are set as outputs for other blocks within the receiver to use.

The implementation of this module is crucial to a functioning prototype in a real-world outdoor environment, however most GPS hardware has poor indoor performance. For the purposes of indoor experimentation, the GPS receiver was replaced by a network synchronized clock, and fixed receiver positions.

4.2.2 Distance Determination

Received Signal Strength was chosen as the primary method for making distance estimates. Systems taking advantage of Time Difference of Arrival, or Time of Arrival require highly accurate time stamping, which is impossible to obtain with current editions of Simulink and the interface with the USRP2.

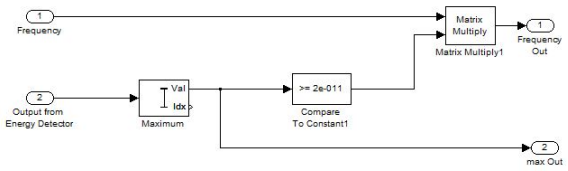


Figure 4.14: Simulink model showing max power measured in Energy Detection

As the energy detector described in Section 4.1.2 also relies on a measurement of the peak power, we pass this value out of the spectrum sensing blocks, as shown in Figure 4.14, and into Data Packing, a to be sent to the central station as described below in Section 4.2.4.

Within the central station the power measurements are first adjusted to account for the calibration of each receiver, and a range estimate is made for each assuming free-space path loss, or decreasing with the inverse-square:

$$P_{rx} = \frac{P_{tx}}{4\pi r^2} \tag{4.1}$$

In eq. (4.1), the received power (P_{rx}) is a function of the transmit power (P_{tx}) and the distance from the radiator, r. This very simple path-loss model is based on the spread of the transmitted energy over the greater surface area of a sphere as the receiver moves farther from the transmitter. In order to make use of this equation for range-finding, it must be solved for the distance, r:

$$r = \left| \sqrt{\frac{P_{tx}}{P_{rx} 4\pi}} \right| \tag{4.2}$$

In (4.2) the magnitude of the square root is used, as the receiver has no knowledge of the direction of signal reception, only the magnitude of the signal power. Additionally, since the transmit power is an unknown in this implementation, the 4π constant can be included as part of P_{tx}. This leaves eq. (4.3) below, allowing the system to vary P_{tx} to determine an estimate for r.

$$r = \left| \sqrt{\frac{P_{tx}}{P_{rx}}} \right| \tag{4.3}$$

In order to determine the appropriate value for P_{tx}, the distance determination occurs simultaneously with the trilateration. If the estimate for t does not result in a location estimate that converges to within the desired precision, P_{tx} is increased by the step size. If increasing the value of P_{tx} results in a less precise location estimate, then the value of P_{tx} is reduced by the step size. As P_{tx} is varied, if the location estimate is determined to be less precise than a previous estimate, the step size of P_{tx} is reduced, and the value is returned to the previous estimate. Since P_{tx} is constant for any received signal across all of the receivers the relationship between distance and power is preserved and a distance estimate can be produced.

The implementation of this method of distance determination is challenged by a number of real-world characteristics. This channel model assumes line-of-sight between the trans-

mitter and the receiver, as well as no reflections or multipath. These conditions are rarely present in the real world, and the addition of reception of multiple copies of a received signal with varying power levels greatly reduces the accuracy of the distance estimate.

The Simulink software combined with the USRP2s used to implement the receivers also served as a source of error for making power measurements. With the interface change from UDP to UHD for the USRP2, significant delays were introduced between the USRP2 and the Simulink model. These delays resulted in receivers sensing transmissions at different times, preventing the accurate estimate of P_{tx} and thusly r.

4.2.3 Trilateration

In order to determine the location of the transmitter, given the measured distance estimates of each of the receivers, an iterative approach based on least-squares error minimization was employed. This iterative method allows for the varying of transmit power, in order to provide to perform localization without prior knowledge of the transmitter.

The first iteration of this system assumes that the transmitter is located near the center of a grid created by the sensors, and that it is transmitting with an average transmit power. The Taylor-series expansion is used to linearize the current position estimate, producing B the Taylor Coefficients. This is initialized using the assumed transmitter locations, and the contribution of the x and y distances between the transmitter and the receivers to the overall distance between the transmitter and receiver. This is shown below in eq. (4.4), where (R_{xi}, R_{yi}) is the location of receiver i, and (T_x, T_y) is the location of the transmitter.

$$B = \begin{bmatrix} \frac{R_{x1} - T_x}{\sqrt{(R_{x1} - T_x)^2 + (R_{y1} - T_y)^2}} & \frac{R_{y1} - T_y}{\sqrt{(R_{x1} - T_x)^2 + (R_{y1} - T_y)^2}} \\ \frac{R_{x2} - T_x}{\sqrt{(R_{x2} - T_x)^2 + (R_{y2} - T_y)^2}} & \frac{R_{y2} - T_y}{\sqrt{(R_{x2} - T_x)^2 + (R_{y2} - T_y)^2}} \\ \frac{R_{x3} - T_x}{\sqrt{(R_{x3} - T_x)^2 + (R_{y3} - T_y)^2}} & \frac{R_{y3} - T_y}{\sqrt{(R_{x3} - T_x)^2 + (R_{y3} - T_y)^2}} \end{bmatrix} \tag{4.4}$$

After the calculation of B, the system creates the vector f containing the difference between the distances, (d_1, d_2, d_3) calculated using eq. (4.3), and the current position estimate, (T_x, T_y).

$$f = \begin{bmatrix} d_1 - \sqrt{(R_{x1} - T_x)^2 + (R_{y1} - T_y)^2} \\ d_2 - \sqrt{(R_{x2} - T_x)^2 + (R_{y2} - T_y)^2} \\ d_3 - \sqrt{(R_{x3} - T_x)^2 + (R_{y3} - T_y)^2} \end{bmatrix} \tag{4.5}$$

The matrix B and vector f along with a weight matrix W, the system can determine t, the measurement error, and N, the position estimate. This implementation assumes an equal weight for all of the sensors, thus a 3x3 identity matrix is used for W. First t is calculated along with N, as shown in eq. (4.6) and eq. (4.7), and then it is used to determine the difference between the previous location estimate and the current estimate, Δ, in eq. (4.8) [5].

$$t = B^T W f; \tag{4.6}$$

$$N = B^T W B; \tag{4.7}$$

$$\Delta = N^{-1} t; \tag{4.8}$$

The new position estimate is determined by adding Δ to T_x and T_y, and after the new position is determined, the error ϕ, is calculated as shown in eq. (4.9) in order to check for convergence. When ϕ is minimized for a given transmitter power, the system checks for ϕ being within an acceptable range. If ϕ is outside of this range, the transmitter power is adjusted as described in Section 4.2.2 and the trilateration algorithm is run again, using the previous results for the original estimate of T_x and T_y.

$$\phi = (f - B\Delta)^T W (f - B\Delta); \tag{4.9}$$

The trilateration block iterates through varying P_{tx} and location estimates until it produces either a location estimate with an acceptable error below a preset threshold, or until an iteration cutoff has been reached. If the cutoff is reached, it is assumed that the system was unable to produce an accurate estimate from the data provided, and the data is

discarded. The selection of a convergence threshold and iteration cutoff is a balance between system execution time and desired precision accuracy. The system implemented in this project used a ϕ threshold of .0005 and a cutoff of 100 iterations. The value for ϕ was determined to produce position estimates that were as accurate as the received power estimates during simulation, and the iteration cutoff limits processing time to three or four seconds.

4.2.4 Data Packing

The UDP send and receive blocks from the Simulink Instrument Control Toolbox are capable of sending an arbitrarily sized matrix of a single datatype. In order to minimize the number of toolbox licenses used, and to simplify design, all data passed from the receivers is converted to a uint32 at the receiver and formed into a 1x7 matrix. Since the power measurements are the only value that is being sent which contains a decimal component, their values are multiplied by a constant at the receiver in order to process them as integers. This blocking process is reversed in the central controller, and the appropriate data type conversions are made to process data as it was originally generated.

The multiplication required in order to send the decimal values of measured power as an integer introduced some problems with the final design implementation. The power measurement fluctuations induced by both the non-ideal channel characteristics, and the performance of the Simulink SDRu blocks resulted in power measurements that, when combined with the scaling constant, would go from a value of zero to overflowing the uint32. Adjusting this scaling factor so that the power measurements would all be in range was possible, however due to the characteristics of individual radios, it was not consistent for all groups of hardware.

4.3 Prototype Implementation Summary

This section examined the different designs that were considered during this project. Each design has its weaknesses and its strengths. Many of the designs described above could not be successfully implemented in the final design of the project. These problems were due to the constraints of the project as well as the signals and data being examined. Despite the fact that many of these designs could not be part of the final design, their descriptions shows the logical flow of the project.

Chapter 5

Design Verification

This section provides an analysis of the different implementations throughout the project. Many of the different designs to perform spectrum sensing and localization were unsuccessful due to the nature of the signals being sensed and the equipment provided. This section describes each implementation as well as its success or failure and what lead to those results.

5.1 Spectrum Sensing

The project examined a number of different spectrum sensing schemes in order to locate and characterize Public Safety radios. Many of these schemes were unsuccessful due to hardware problems and radio characteristic similarities of the P25 digital C4FM, and analog FM types of radios. The next sections describe the tests on each spectrum sensing design and the outcome of each test.

5.1.1 Energy Detection

The design for the Energy Detector used a reliable method of sensing based on Otsus theorem for energy detection. As the Energy Detector cannot characterize signals it was not necessary to use actual P25 digital C4FM signals or analog FM signals when testing the Energy Detector. Energy detection examines the power of a received signal and a signals power does not depend on its modulation scheme. This meant that any sample signal would

be sufficient to test the Energy Detectors efficiency. Table 5.1 shows a table of the details of the experiments performed to test the energy detection design.

Table 5.1: Testing Details for the Energy Detection Design.

Testing Specifications	
Radio	USRP2 with XCVR 2450 Daughter Card
Modulation Scheme	DBPSK
Propagation	Line of Sight
Frequency	2.45 GHz
Distance	Less Than 10 ft

The sample signal that was used in the first tests of the Energy Detector was a pulse shaped Differential Binary Phase-Shift Keying (DBPSK) signal transmitting the constantly repeated binary signal [0, 1]. DBPSK is designed to transmit a pulse whenever it detects a change in the bits, this allowed the transmitter to supply a constant pulse for the Energy Detector to detect. The design for the DBPSK transmitter appears in Figure 5.1.

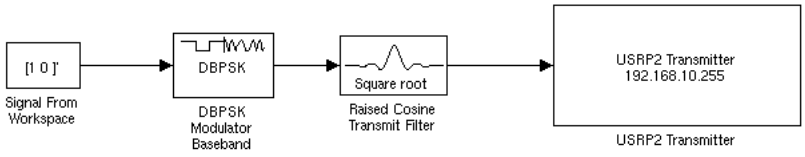


Figure 5.1: Simulink model of a DBPSK transmitter. The signal is both modulated with a DBPSK modulator and filtered with a raised cosine transmit filter.

In order to test the Energy Detector, 100 frames of the signal were examined before examining the maximum value from that set of frames. The tests examined the maximum output of the Energy Detector during transmission and during no transmission to determine the difference between a signal power and the power of the noise floor. The results of these tests appears in Table 5.2.

Table 5.2: Received Powers for Energy Detection

	Max Power	Mean Power
No Signal	2.8e-7A	1.7e-9A
DBPSK Signal	.0189A	.0041A

The values in the graph above indicated that a minimum decision value of 1e-6 should be large enough so that the majority of noise powers would not be considered transmissions, and low enough so that low power signals would be easily visible. These values rely on several features of the radio, one of which is gain. The final design of the energy detector considered a minimum value of twenty pico amps with a gain of zero.

Once a decision value was decided, the Energy Detector was tested with a signal, and without a signal, to determine the accuracy of the Energy Detector. While the signal was being transmitted 4305 out of 5001 frames were confirmed as a transmitted signal and while only noise was being observed the Energy Detector registered 1 frame as a signal. Energy detection is not as precise as many other forms of spectrum sensing and hence a small amount of error is expected,. The number of signals that were considered to be noise during testing could be the result of the fluctuating power of the transmitted signal or a lack of precision in the USRP2 hardware.

5.1.2 Spectrum Sensing Summary

The design of the spectrum sensing system had to overcome many difficulties throughout the project. Many of the different systems that were examined had to be abandoned because they would not operate within the scope of the project. The spectrum sensing section had to be able to reliably differentiate between a signal and noise. Energy detection using Otsu's method, was the first spectrum sensing system that could reliably distinguish between a signal and noise. This system had a high signal detection rate but was hampered by many false detections. In order to insure that the spectrum sensing system did not miss any signals the decision value for the energy detector was set very low. A higher decision value would have decreased the number of false detections as well as the signal detection rate.

Matched filtering and PSD characterisation are both capable of performing spectrum sensing though as they were unable to perform signal characterization. Both of these spectrum sensing methods could reliably differentiate between signals and noise, but as both schemes were more computationally intensive then energy detection and no more reliable, Otsu's method of energy detection remained the most useful spectrum sensing method.

5.1.3 PSD Characterization

The first PSD spectrum sensing scheme was designed to differentiate between a signal and noise by examining the average Power Spectral Density of the signal. The tests for the design for the average PSD spectrum sensing section were conducted in a similar fashion to the tests on the energy detector design. The specifications appear in Table 5.1.

In order to differentiate between the transmission of a signal and the transmission of noise, the scheme required a minimum signal strength value. This allowed the scheme to establish a baseline for signal detection that excluded noise. The scheme examined the output of the characterizations for 1000 frames of pure noise at a frequency of 2.45e9Hz. The same transmitter was used as a sample signal because the PSD block design did not incorporate characterization. The values from the test are shown in Table 5.3.

Table 5.3: Received Powers for PSD

	Mean Value of the PSD
Noise	2.58e-17A
4-FSK Signal	1.04e-3A

The mean value of the PSD for the noise was 2.58e-17A, while the mean value for the received signal was 1.04e-3A which means that a reasonable decision value for the PSD block was established as 1e-4A. This first design for the PSD block was primitive and did not attempt to characterize signals. The design details are illustrated in Figure 5.2.

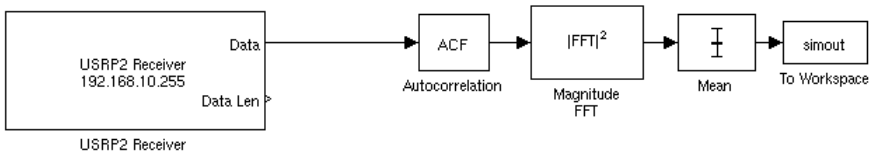


Figure 5.2: Simulink design for an average PSD spectrum sensing system. The output of the receiver is autocorrelated, converted into the frequency domain and then averaged.

This design was primarily used to perform the same function as the Energy Detector. The signal power for two way radio communications is usually considerably higher than the noise floor and the PSD scheme would encounter the same problems with signal detection as the Energy Detector. This design could not provide more information than the energy detection scheme because it did not provide any greater reliability and could not perform characterization. For these reasons, the PSD block above was discarded in favour of a more advanced system.

The second PSD characterization spectrum sensing design was more advanced than the original PSD block. It not only provided a method for differentiating between noise and the transmissions, the new design could characterize the incoming signal. As the design was more advanced the test had to be correspondingly complex. Table 5.4 provides the details of the tests performed to examine the reliability of the PSD characterization design.

Table 5.4: Testing Details for the PSD Characterization Design

Testing Specifications	
Radio	Public Safety P25 Standard Radio
Modulation Scheme	FM and C4FM
Propagation	Line of Sight
Frequency	146 MHz
Distance	Less Than 10 ft

A determination of the signal characterization could then be established and identify

it as noise, an analog FM transmission or a digital C4FM transmission. The plan was to compare the PSD of the received signal against the PSDs of two test signals generated inside the block. The design of the second PSD characterization block appears in Figure 5.3.

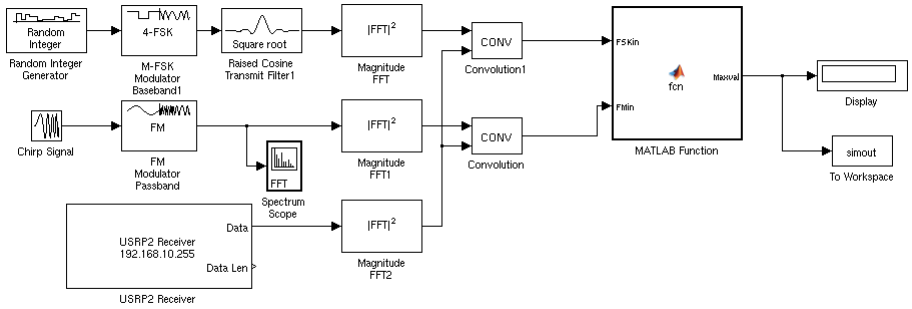


Figure 5.3: Simulink model of PSD characterization. In this model every possible modulation scheme is compared against the received data to determine the most likely communication standard of the transmitter.

This design was unsuccessful because the frequency domain PSDs of C4FM transmissions and FM transmissions were virtually indistinguishable from one another due to the nature of the two modulation schemes. The PSD diagrams of an analog and a digital transmission appear in Figure 5.4 and Figure 5.5.

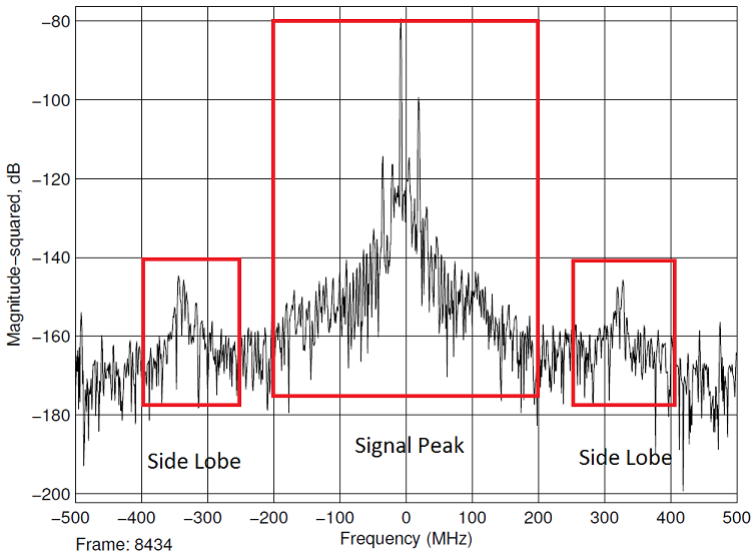


Figure 5.4: Frequency domain PSD of an analog signal. As the graph shows there are three distinct peaks that characterize analog signals.

Figure 5.4 shows the spectral shape of the PSD of an analogue signal. As the figure shows there is a distinct pulse shape at the center frequency and a side lobe on either side of the center frequency. Figure 5.5 shows the PSD of a digital signal. Both signals are very similar. There are no harmonics that differ between the two signals and though the digital signal has a more gradual peak at the center frequency that difference is not enough to differentiate the two signals.

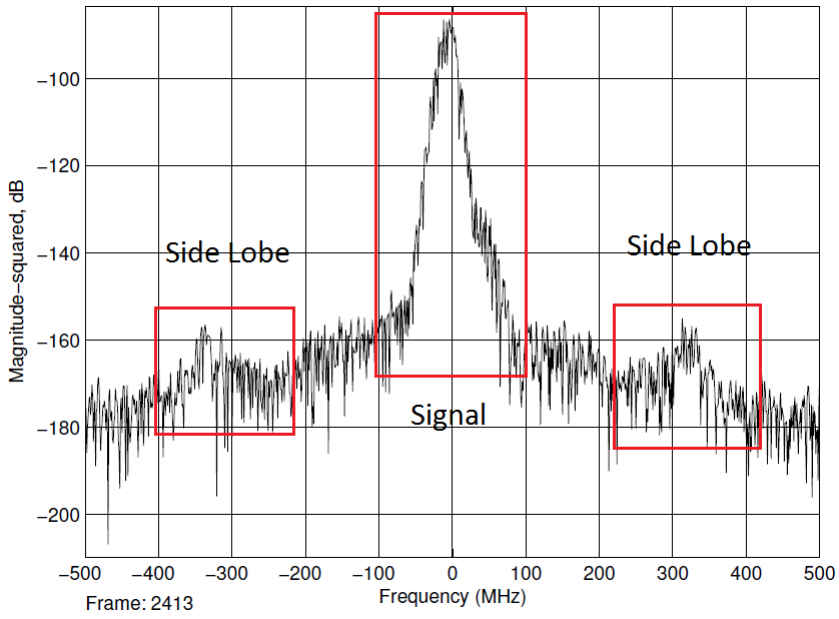


Figure 5.5: Frequency Domain PSD of a digital signal. This graph also shows three distinct peaks.

As Figure 5.4 and Figure 5.5 show the PSDs of C4FM and FM are so similar, there was no way to determine definitive decision values that could differentiate one signal from another. The PSD characterization block was no longer considered as a useful spectrum sensing method because it could not effectively characterize signals.

5.1.4 Matched Filter

The first matched filter design intended to incorporate both matched filtering to characterize analog FM and digital C4FM transmissions, as well as perform probability analysis on the received signal strength. The probability value incorporated the Q function to provide an approximation of the reliability of reception. The model of this design of the matched filter appears in Figure 5.6.

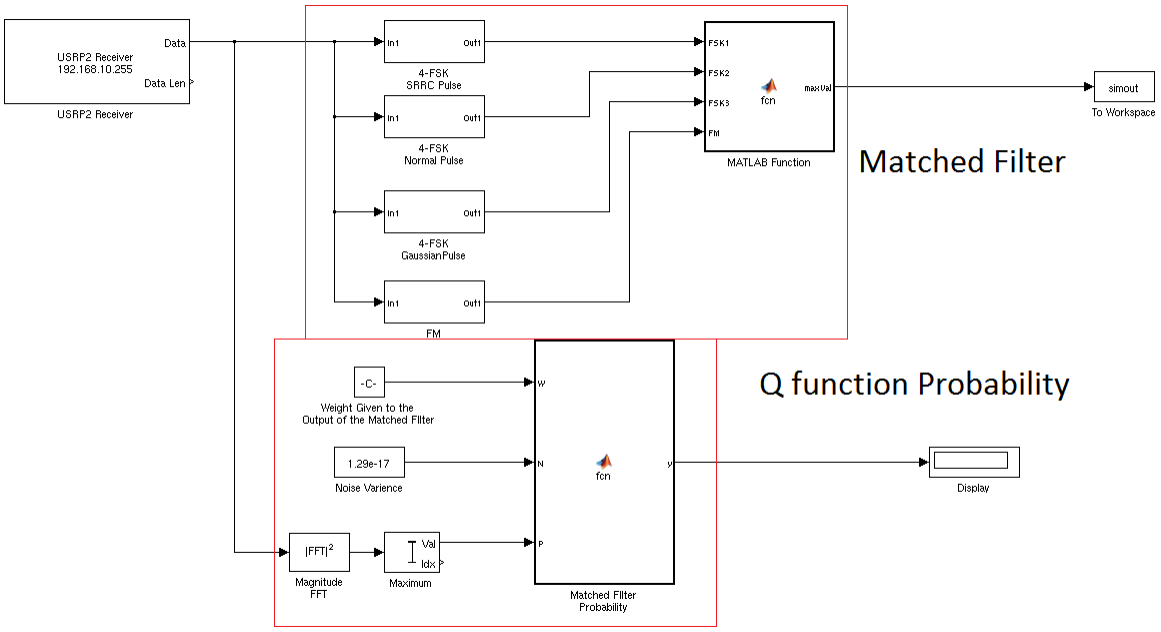


Figure 5.6: Simulink model of the matched filter design. There are two distinct parts of this matched filter scheme, the Q function that determines the probability of correct detection and the matched filter that characterizes the signal.

The design of the matched filter was implemented with built-in demodulators in Simulink. Simulink did not contain a C4FM demodulator and hence, a substitute was devised that was similar to C4FM. C4FM is similar to both Quadrature Phase Shift Keying (QPSK) and 4-lobe Frame Shift Keying (4-FSK).The original design intended to use 4-FSK as a substitute for C4FM. The assumption was that although a C4FM signal demodulated by 4-FSK demodulator would not be interoperable, the output would have more characteristics of digital data than an Analog signal that was demodulated by a 4-FSK demodulator.

Unfortunately the FM demodulator was not designed for real time communication so another form of demodulation had to be devised. The next design incorporated the fmdemod function in MATLAB to try and demodulate the signal using a different form of FM demodulation. This function would not cooperate with the Simulink interface as several essential functions that fmdemod implemented could not be performed in a Simulink MAT-

LAB block. After a number of attempts to demodulate analog FM transmissions, an earlier design for the analog FM demodulator was used to perform demodulation in real time. The specifications for the final tests to determine the reliability of the matched filter appear in Table 5.5.

Table 5.5: Testing Details for the Matched Filter Design

Testing Specifications	
Radio	USRP2 with WBX Daughter Card
Modulation Scheme	C4FM
Propagation	Line of Sight
Frequency	146 MHz
Distance	Less Than 10 ft

The final design of the matched filter required the use of an FM demodulator block, and a model of a C4FM block using the same FM demodulator. The C4FM block was composed of a pulse shape filter and the FM demodulator. This design was not as sophisticated as a real C4FM demodulator in a P25 radio, however it could demodulate signals so that digital data was visible although not interoperable. The Simulink model of the matched filter spectrum sensing scheme appears in Figure 5.7.

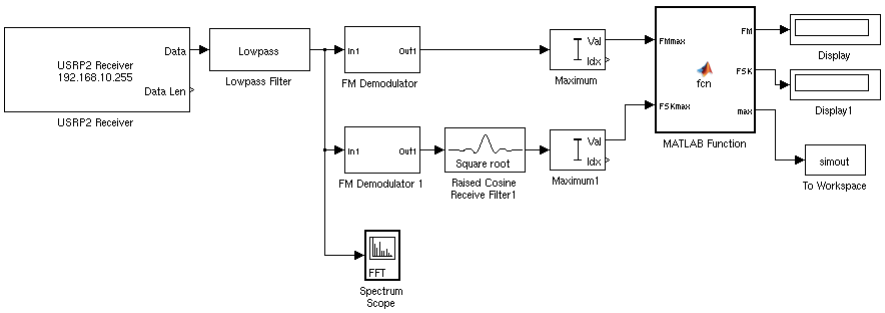


Figure 5.7: Simulink model of matched filtering. The model outputs the likelihood of a signal being FM, FSK and the maximum

In order to define boundaries between analog FM and digital C4FM the project took measurements from the outputs of the demodulators. These values would define what decision values were used to characterize a signal. In order to provide realistic readings for the matched filter decision values, a transmitter was designed to send models of analog FM signals to the receiver. A number of tests were performed to determine how the demodulators reacted to a FM signal. The results of those tests appear in Table 5.6.

Table 5.6: Maximum Outputs of Demodulation

	Max Noise Values	Max Analog FM Values
C4FM Demodulator	4.83	4.99
FM Demodulator	3.14	3.14

The analog signal test showed that the C4FM demodulator provided significantly higher readings then the FM demodulator no matter what signal was transmitted. The design of the matched filter considered the maximum output from the demodulators and hence, the matched filter could not characterize transmissions. These results implied that the matched filter could not differentiate between analog FM signals and digital C4FM signals. The matched filter was abandoned because it could not provide reliable data.

5.1.5 Autocorrelation/Matched Filter Scheme

The autocorrelation/matched filter spectrum sensing scheme was the last attempt to characterize analog FM and digital C4FM signals. All of the conventional attempts to perform spectrum sensing had been unable to perform characterization on the signals. The output of the autocorrelation block was examined to determine what an auto correlated digital signal would look like when compared to an analog signal or noise. The specifications of the tests performed to determine the reliability of the autocorrelation/matched filter design appear in Table 5.7.

Table 5.7: Testing Details for the Autocorrelation/Matched Filter Design

Testing Specifications	
Radio	Public Safety P25 Standard Radio
Modulation Scheme	C4FM and FM
Propagation	Line of Sight
Frequency	146 MHz
Distance	Less Than 10 ft

The output was surprising because despite the fact that analog FM signals have no repeating barker codes, they occasionally provided similar harmonics at the same time differences. The outputs of the autocorrelation/matched filter scheme for a characteristic analog FM transmission and a digital C4FM transmission appears in Figure 5.8 and Figure 5.9.

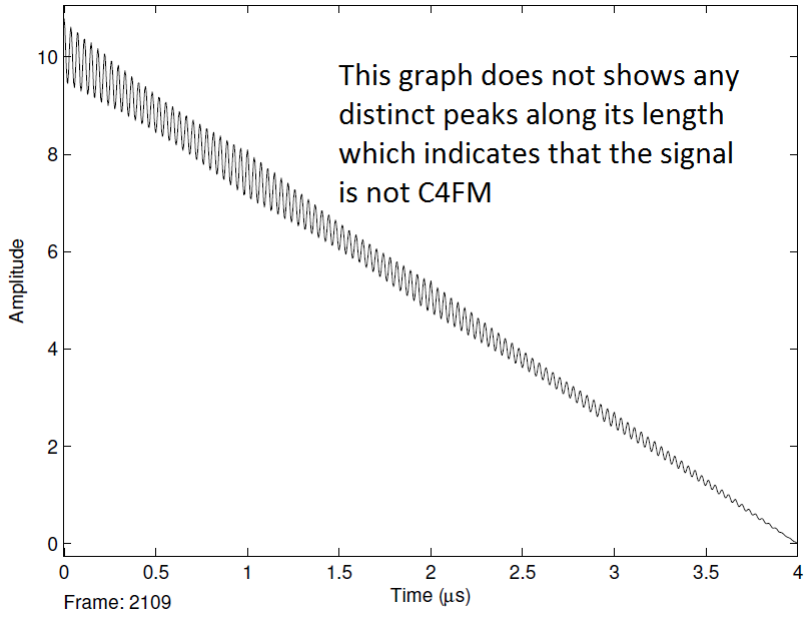


Figure 5.8: Output of the autocorrelation/matched filter scheme for an analog signal. Analog signals do not contain headers so there are no peaks along the length of the graph.

As Figure 5.8 shows the analog signal has much less pronounced peaks along the graph above. Analog signal transmissions do not contain an HDU like Digital C4FM signals. This means that they will not have distinct peaks at the same time periods as C4FM signals. Figure 5.9 shows the same graph for a digital signal. Digital C4FM signals do contain HDUs every frame which results in the peaks shown in Figure 5.9.

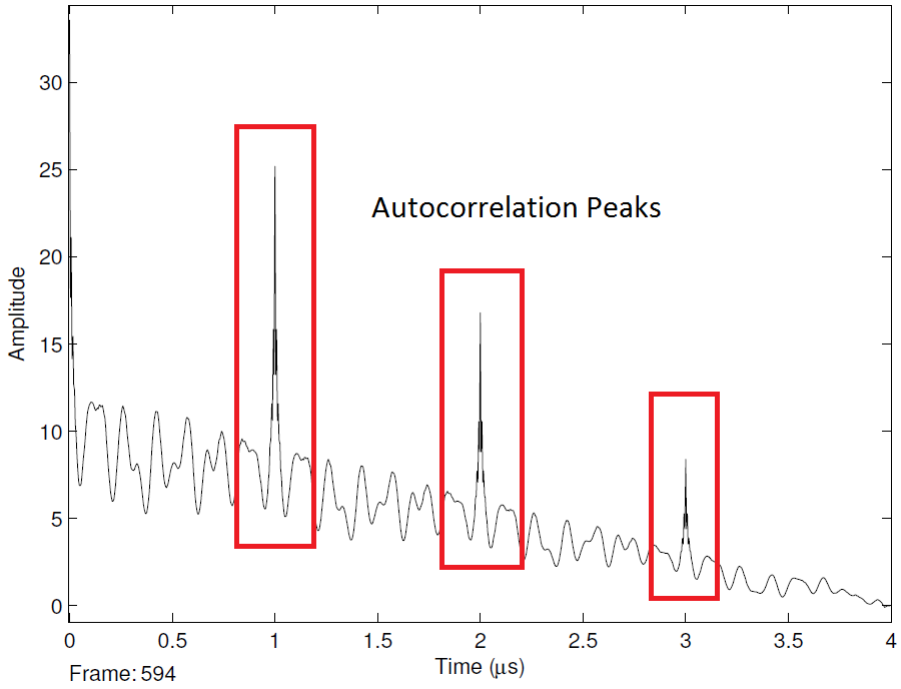


Figure 5.9: Output of the autocorrelation/matched filter scheme for a digital signal. This graph shows the distinct peaks where headers overlap with each other when the signal is autocorrelated.

As Figure 5.8 and Figure 5.9 show there is a significant difference between a characteristic response from an analog signal and digital signal. The response of the digital signal has peaks at every microsecond where the HDU of the C4FM signal repeats. These peaks always appear at 0, 1, 2, and 3 microseconds when there is a digital C4FM signal present. In order to make a definitive decision between a digital C4FM signal and an analog FM signal it was necessary to take measurements of the values of a digital signal, an analog signal as well as

noise to determine values that would differentiate them. The simplest way was to record values to differentiate these signals was to examine recorded values for them. Figure 5.10 is a plot of autocorrelation values for analog and digital at 0,1,2 and 3 microseconds.

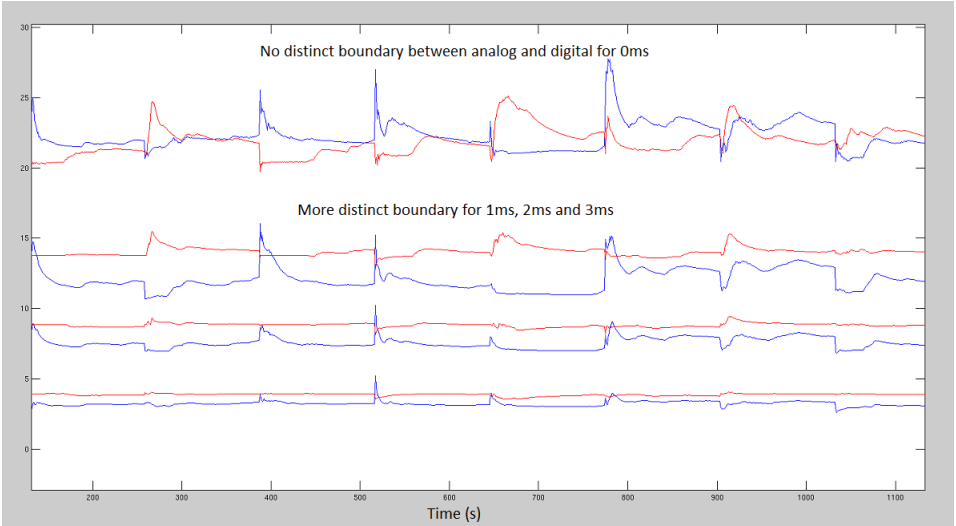


Figure 5.10: Autocorrelation values for digital and analog signals. The bottom three time values are much easier to distinguish between then the top.

In Figure 5.10 the red lines represent values outputted from autocorrelation in the autocorrelation/matched filter scheme from a digital signal at different time segments and the blue lines are from an analog signal at the same time segments. The values from this graph were rather perplexing because they did not show a definitive difference between analog and digital signals. Values at the time segment 0 microseconds were so similar it is impossible to tell the different modulation schemes apart. In order to attempt to widen the difference between analog and digital values used to make characterization decisions, a squaring block was added to the autocorrelation/matched filter scheme. This widened the separation between analog and digital autocorrelation values making it possible to determine a definitive characteristic for analog verses digital characterization. The Simulink model for the autocorrelation/matched filter appears in Figure 5.11.

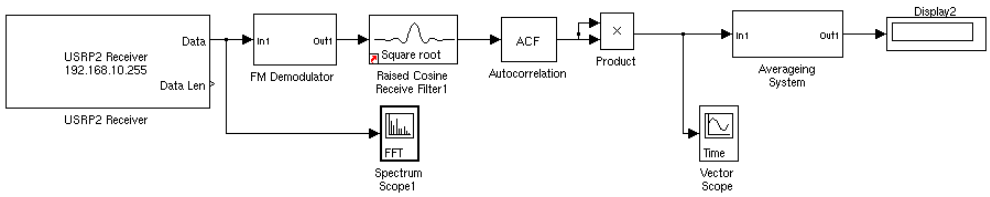


Figure 5.11: Simulink model for the autocorrelation/matched filter scheme. This design is the only spectrum sensing system that was able to perform signal characterization.

The design for the autocorrelation/matched filter scheme required the use of a running average to define concrete boundaries between digital and analog signals. The design first incorporated analysis of values from 1,2 and 3 microsecond segments, however because the values at 1microsecond provided a more reliable boundary between analog and digital signals, the final design only examined values from the 1microsecond time segment. Tests were performed to determine the best decision values to characterize transmissions and these were used to determine a number of final decision values. These values appear in the Table 5.8.

Table 5.8: Autocorrelation Values

	Autocorrelation Values
Digital	1 - 5
Analog	0 - 1
Noise	greater than 5

These values were decided using a P25 radio transmitting C4FM and FM separately. These values are consistent for a gain of 0 on the receiver. The design for the autocorrelation/matched filter scheme is very reliable and has significantly less deviation then energy detection when differentiating a signal, from noise. For these reasons the final design of the spectrum sensing scheme only incorporated an autocorrelation/matched filter method.

5.1.6 Characterization Summary

The signal characterization portion of the project also encountered problems during development. Many of the different forms of signal characterization that were examined could not perform reliable characterization due to the similarity of Analogue Frequency Modulation (FM) and Continuous Four-level Frequency Modulation (C4FM), as well as hardware and software issues. The final design for signal characterization was an autocorrelation/-matched filtering system that was capable of characterize and differentiate FM and C4FM with 80 percent reliability. Many of the tests used to differentiate C4FM and FM signals performed rapid changes between analog (FM) and digital (C4FM) transmissions. Many of the errors where signals were characterized incorrectly resulted from these rapid shifts. This kind of rapid change between communications standards is unlikely to happen in the real world which means that the actual detection rate may be higher. Autocorrelation/matched filtering is capable of both spectrum sensing and characterization. This meant that the autocorrelation/matched filter replaced Otsu's energy detection method for spectrum sensing in addition to performing signal characterization.

5.2 Sensor Fusion and Localization

The combination of sensor data and the control and synchronization of multiple receivers was facilitated by the Simulink Instrument Control Toolbox. This toolbox provided UDP based networking linking between the receivers and the central controller, as well as RS-232 serial connections at the receivers for connecting to the GPS system. Unfortunately, while many of the components of the system functioned individually, and system integration was functional under simulation, the real world integration of the complete system was inhibited by the failure of a few modules.

5.2.1 Distance Determination

The construction of distance estimates proved to be a significant challenge for this project. As the Simulink Interface and the USRP2 did not allow for signal timestamping with any reasonable accuracy, the project was limited to RSS based distance determina-

tion. While this type of measurement is generally less complicated than TDoA or ToA, implementation with this software and hardware combination was challenging.

The individual variations between radio and computer pairs, when making signal power measurements was substantial. The USRP2s allow for the adjustment of receiver gain on a scale of 0-33dB, and this was originally used to attempt to bring the received power measurements from all of the radios into the same range. While adjust the gain between the radios did bring the receive power measurements closer together, the change was minimal when compared with the error. As an example, for two radios positioned equidistant from the transmitter, after adjusting the gain for the minimum power difference between the radios, the peak power measured was over 40dB greater on the radio with the lower gain. Some of these variations may have been a result of the AGC feature of the USRP2, and lack of a software interface with this function.

Additionally, the move to the SDRu system from the UDP based system for interfacing with the USRP2 introduced an additional delay in radio power measurements. Using the SDRu blocks the delay between a transmission beginning and the detection system detecting a change in the received signal increases exponentially with simulation runtime. This delay can be minimized through the optimization of the receivers frame length, and sample time, but if the receivers are left running for tens of minutes, the delay inevitably grew greater than the scanning period, resulting in missed detections, or incorrect detections. A real world system of this nature would be expected to run for several hours, which would be impossible with such a delay.

The initial plan for the verification of distance determination and trilateration consisted of simulations using simulated RF measurements, followed by small scale trials with the receivers seperated by 10-15 feet, and concluding with large scale trial of the system detecting amateur radio operators as they traveled around the WPI campus, with sensors located on the roofs of buildings. The simulations proved the trilateration and distance determination functional, as shown in Section 5.2.2, but small scale trials were unsuccseful due to the problems present in with the hardware and software.

5.2.2 Trilateration

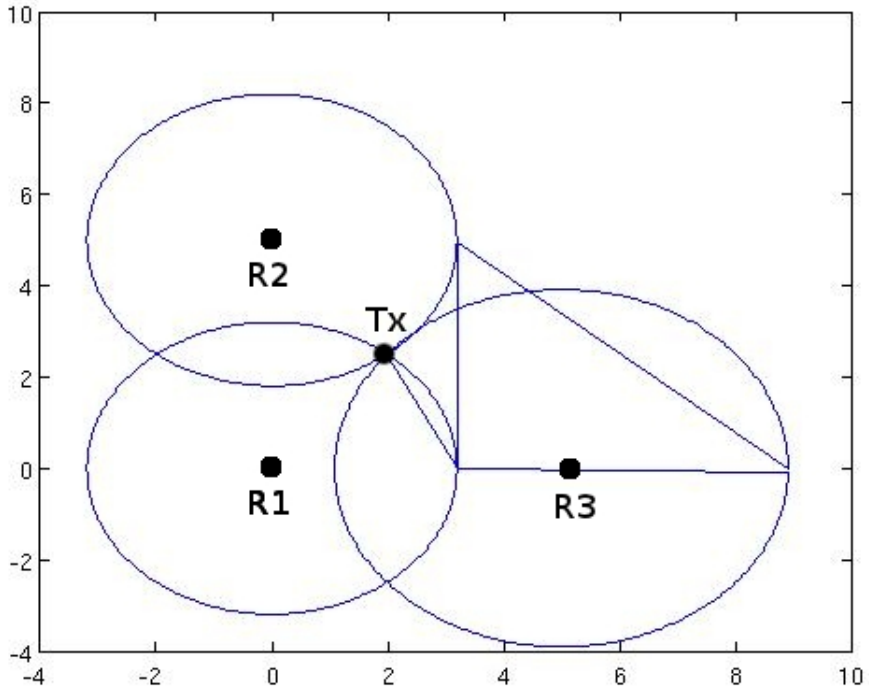


Figure 5.12: Circles representing the distance estimate between the transmitters and receivers, converging to the position estimate

The trilateration algorithm used for the testing of this prototype is very common in systems determining an unknown position given three or more distances to the unknown. When generating simulated receive signal power, the algorithm took approximately 3-5 seconds to determine the distance between each receiver and the transmitter and produce an accurate position estimate, depending on the position of the transmitter with respect to the initial position approximation as shown above in Figure 5.12. This output was generated by taking the distance between each receiver and the transmitter, and drawing a circle with its radius set to this distance centered on each receiver. The resulting intersections of the circle reveal the location of the transmitter.

As the simulated transmitter was moved around within the detection area, it became apparent that the trilateration calculations accuracy varied with respect to the transmitters position, and the algorithm was unable to determine the location of the transmitter for some positions. Generally, as the transmitter moved away from the initial position estimate, the calculation time increased, and as the transmitter moved away from the point equidistant from all of the receivers, position estimate accuracy decreased. The variation with position accuracy under simulation was minor, on the order of a few inches, substantially less than what would be introduced with even good received power measurements.

In addition to the above circumstances where position determination was slowed, or accuracy was reduced, this method for determining position is unable to calculate the transmitters position if it is collinear with two of the receivers. Should this event occur, the matrices used to calculate the position will become singular, resulting in software errors. This particular issue could be resolved through the introduction of additional receivers, as the algorithm is expandable, however this prototype was limited by the available equipment.

5.3 Design Verification Summary

This section has provided an analysis of the different implementations for the project. It describes the different problems that arose in each implementation that lead to the final designs. Though many of the designs ran into issues that made them incapable of performing correctly under the constraints of the project, the process used to examine and test them provides a complete view of the project.

Chapter 6

Conclusions and Recommendations

The goal of this project was to develop a system that could aid emergency response teams during a major disaster. During an event where a large number of different emergency response teams are active in one particular area, it is beneficial for a coordinator to know where all of the emergency response personnel are located at any given time. The purpose of this project was to develop a system that could scan through the spectrum used by emergency radios, determine the radio frequency, characterize, and localize all emergency responders using a particular spectrum band.

The project intended to locate emergency responders by performing spectrum sensing analysis on the spectrum band in use and provide a determination from examination of the received signal at each frequency, whether a transmission was present. This goal was met by using an Autocorrelation/Matched Filter scheme to determine the likelihood of a signals presence. The Spectrum Sensing scheme is capable of finding both analog FM and digital C4FM signals by sensing at each frequency. The system is also capable of differentiating between transmissions and noise.

Another goal of the project was to be able to characterize different transmissions by examining their response without decoding the signal. The Spectrum Sensing system met this goal by implementing a combined Autocorrelation and Matched Filter scheme. The scheme is capable of examining the response of the transmission and determining if the signal is an analog FM transmission, or a P25 C4FM transmission. These transmissions

were the only ones considered when the project was designed because analog and P25 radios are the most widely used radios used by emergency response systems.

The final task for the integrated project was to determine the location of the responders taking advantage of available signal characteristics. Due to hardware and software limitations, time based distance measurements such as Time Difference of Arrival, and Time of Arrival were impossible, so Received Signal Strength was selected. While received signal strength appeared to function initially, later releases of MATLAB and more complicated Simulink models introduced delay and sporadic measurements which made distance calculations difficult. While simulations of the system using simulated received power measurements showed the integrated system to be fully functional, it was not possible to test the system with real world data.

6.1 Future Work

Throughout the design and implementation of the project, problems occurred that resulted in many design methods being abandoned due to design and equipment issues that could not be overcome. Future work in this area should consider these problems and attempt to combat them in order to improve the system already in place.

Increased Computing Power:

- Many different areas of the design and implementation of the project suffered from a lack of computational power. The Spectrum Sensing system had to abandon Cyclostationary Analysis because the equipment used by the project team could not perform the highly computational intensive process of cyclic characterization in real time. This forced the project to consider alternative means of characterizing signals. The sensing system suffered from a lack of speed during early testing as the computers were slow to perform complicated procedures in Simulink. This meant that the Sensing System had to insure that the computational power needed to scan a signal was minimized. The project suffered continuously from a lack of computational power because it did not have dedicated computers.. Future work on this project should consider dedicated computers or hardware in the design.

Simulink Problems:

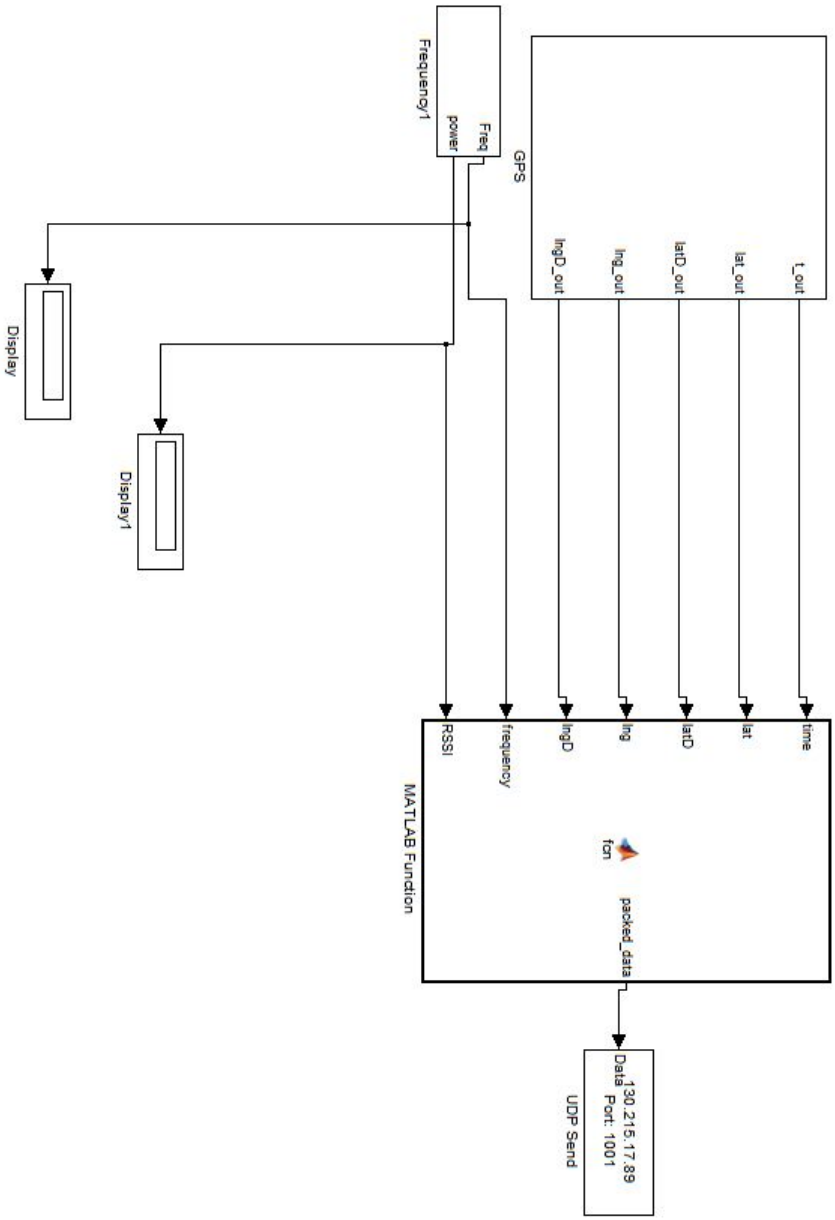
- Throughout the project the design for the Spectrum Sensing system has suffered from unintended side effects of using Simulink. Many areas of Simulink are not designed for real time computation. This meant that many Simulink blocks would not cooperate with one another when asked to perform in real time. The design for the Matched Filter suffered from these problems repeatedly because many of the demodulation blocks error if asked to perform real time computations. Future work in this area should consider performing computations in MATLAB rather than Simulink because it does not suffer from many of the same real time issues.

- The Simulink interface for the USRP2, while improving with every release of MATLAB, still lacks many of the features present in GNU Radio. Simulink lacks any ability to timestamp data from the radio, or even obtain timestamps from the system. Additionally, received power measurements in Simulink appear to be affected by the same automatic gain control issue that the Kelly and Khair MQP experienced with GNU radio [12], eliminating all possibilities for performing localization using this software package. Should future versions so the Simulink interface for the USRPs allow the user to interact with the AGC, or provide more accurate timing, localization should be possible.

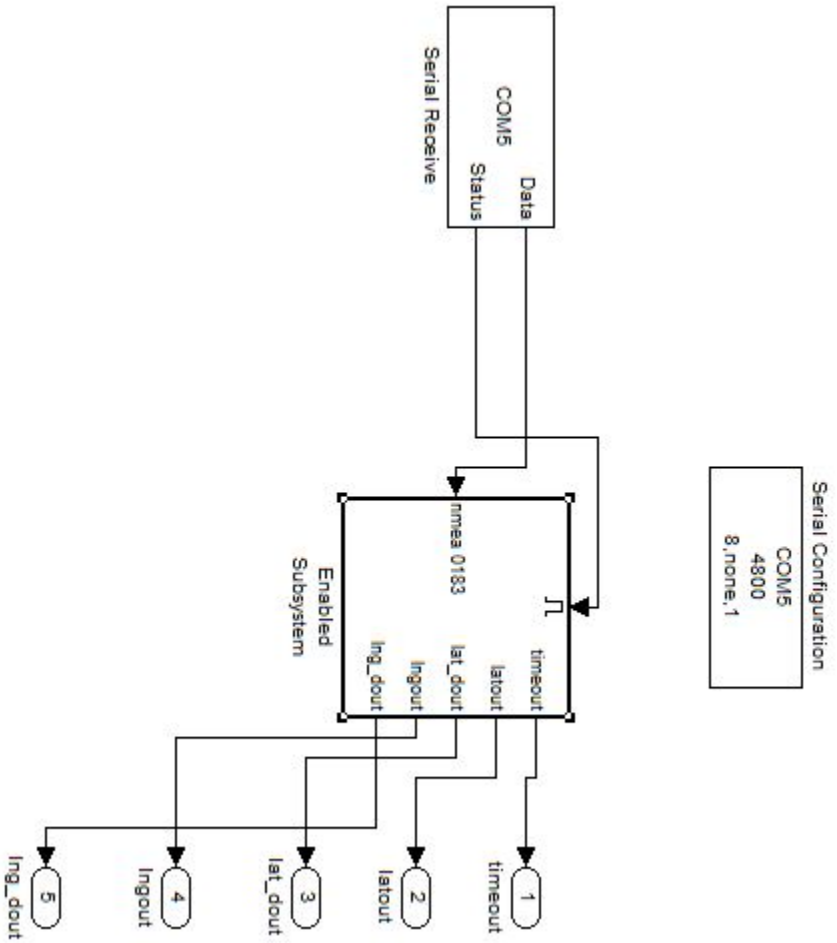
- Future versions of the project would benefit greatly from a more stable interface between Simulink and the USRPs. Significant changes between versions of MATLAB and Simulink resulted in substantial project redesigns with every version release. Since MATLAB releases on a 6 month cycle, the project encountered this challenge three times during development, each time a major setback.

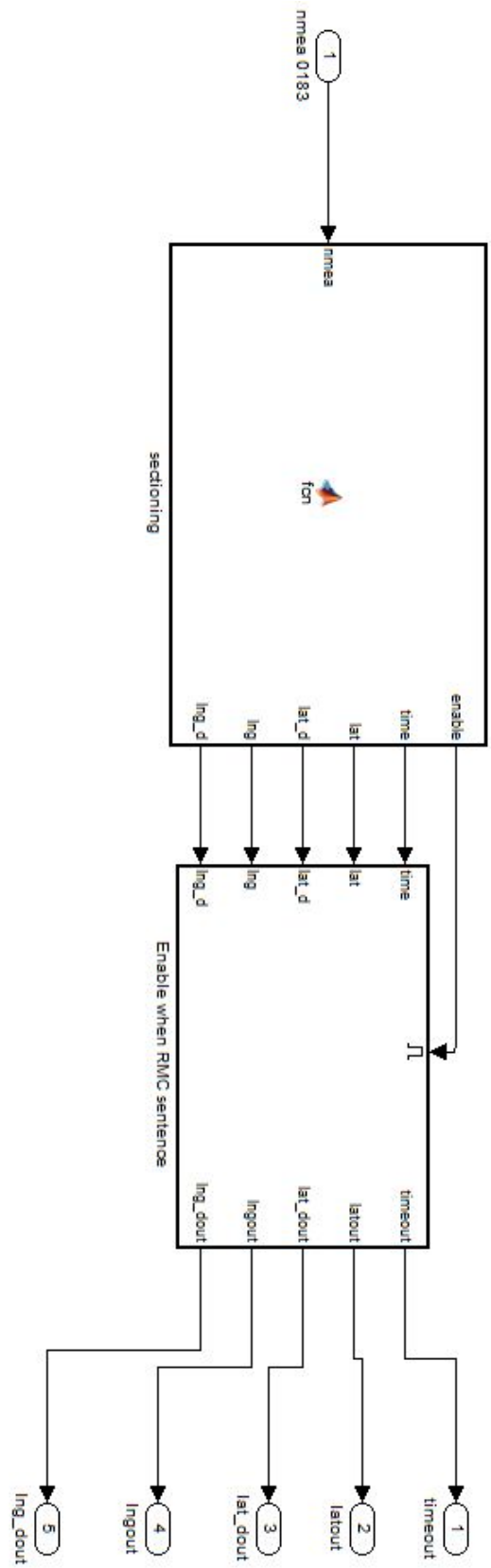
Appendices

Appendix A: Receiver Simulink Model



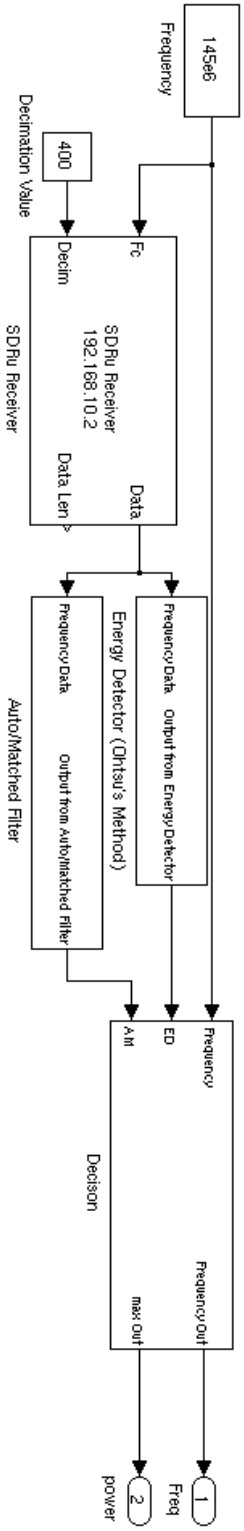
Appendix B: GPS Simulink Model



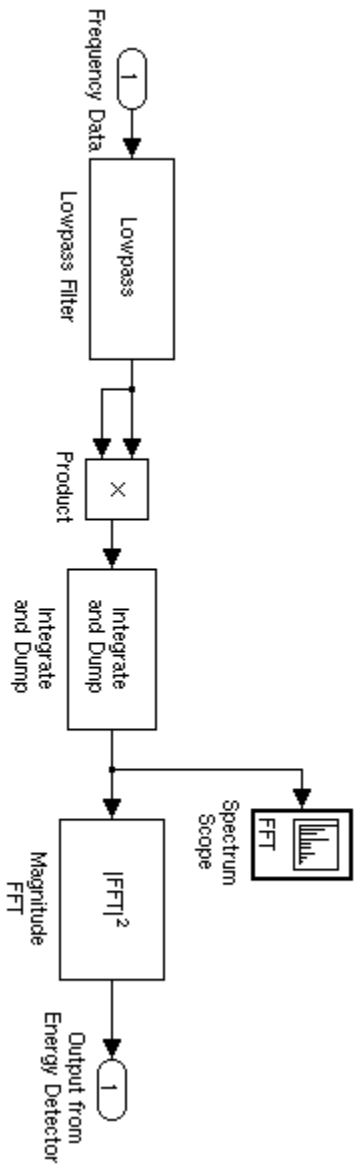

1
nmea 0183
nmea
fcn
sectioning
lng_d
lng
lat_d
lat
time
enable
lng_d
lng
lat_d
lat
time
Enable when RMC sentence
lng_dout
lngout
lat_dout
latout
timeout
5
lng_dout
4
lngout
3
lat_dout
2
latout
1
timeout

```
function [enable,time,lat,lat_d,lng,lng_d]= fcn(nmea)
% #codegen
enable = 0;
sentence = int8(zeros(1,80));
sectioned_sentence = zeros(15,15);
time = zeros(1,8);
lat = zeros(1,15);
lat_d = 0;
lng = zeros(1,15);
lng_d = 0;
[trash begin] = min(abs(nmea - 36));
work = [nmea(begin+2:end)];
sentence(1:length(work)) = [work];
for n = 1:15
    [t b] = min(abs(sentence-44));
    sectioned_sentence(n,1:length(sentence(1:b-1))) = [sentence
        (1:b-1)];
    sentence(1:length(sentence(b+1:end))) = [sentence(b+1:end)];
end
if sectioned_sentence(1,4) == 82 && sectioned_sentence(1,5) == 77
    %check for GPRM*
    time = sectioned_sentence(2,1:8)-48;
    lat = sectioned_sentence(4,1:15)-48;
    lat_d = sectioned_sentence(5,1);
    lng = sectioned_sentence(6,:)-48;
    lng_d = sectioned_sentence(7,1);
    enable = 1;
end
end
```

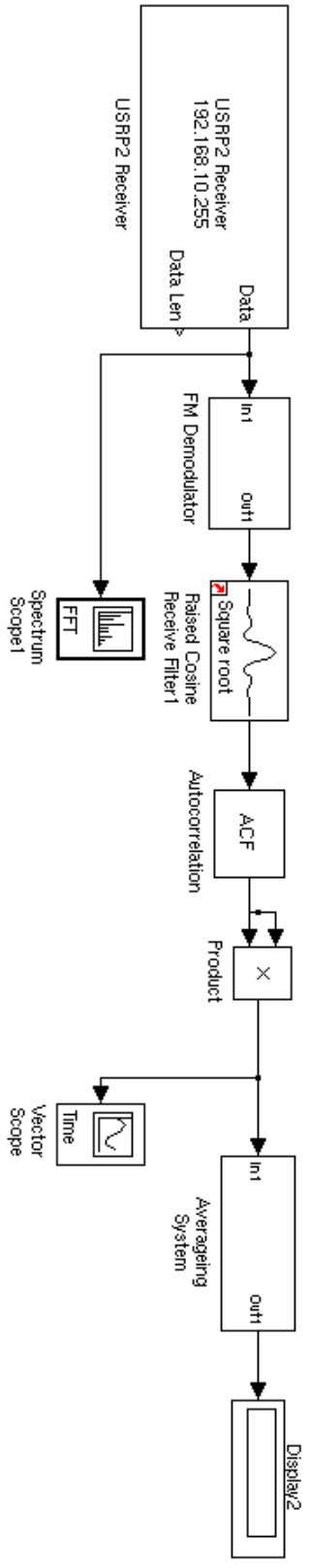
Appendix C: Signal detection and characterization Simulink model of final project



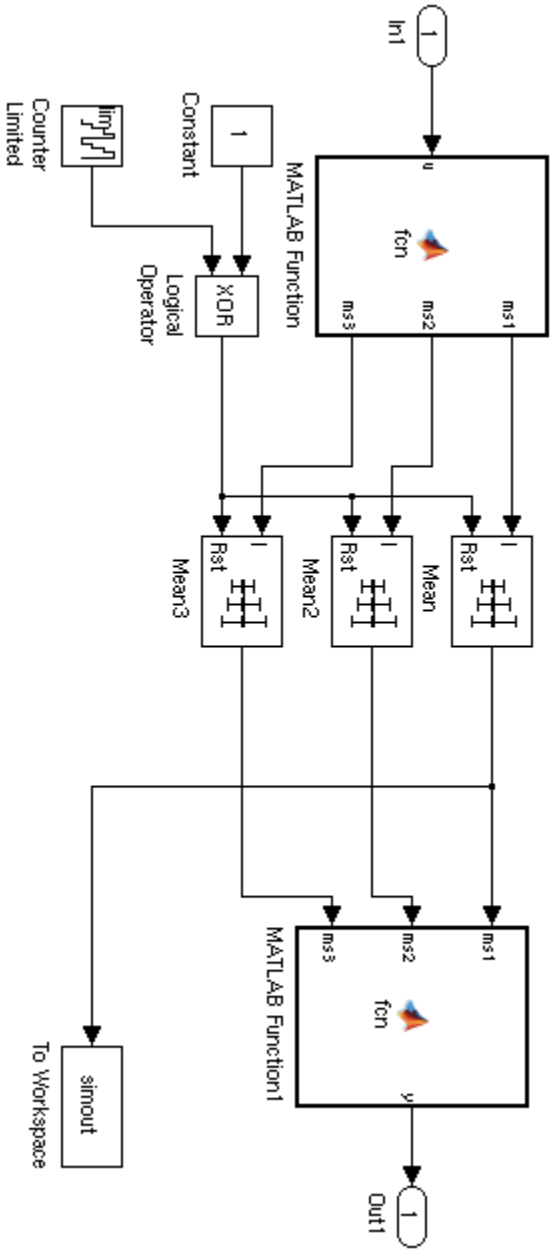
Appendix D: Energy detector



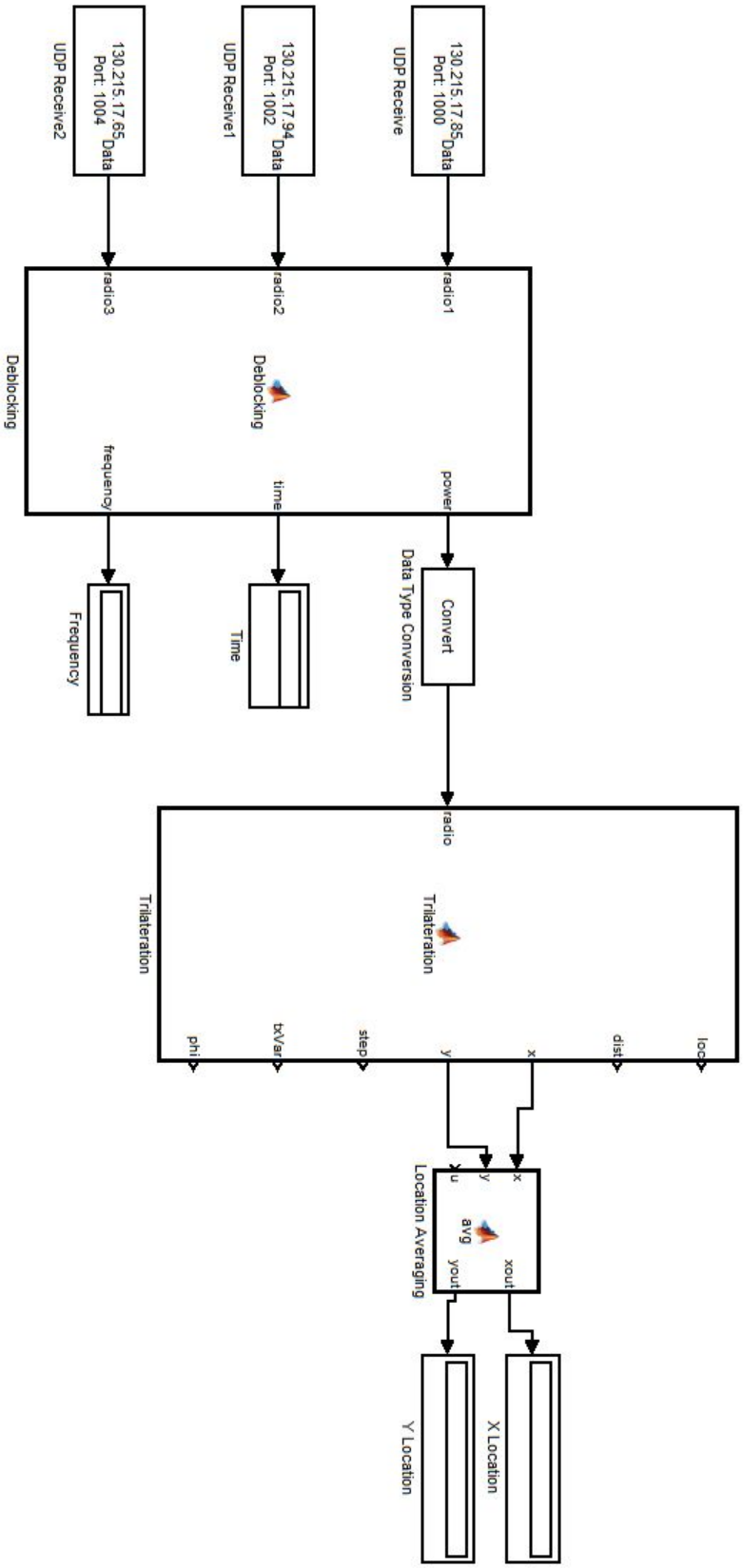
Appendix E: Autocorrelation/matched filter



Appendix F: Autocorrelation/matched filter averaging block



Appendix G: Control Center Simulink Model



Appendix H: Trilateration Matlab Function

```
function [loc,dist,x,y,step,txVar,phi] = Trilateration(radio)
radio = radio /1e6;
radio1 = radio(1);
radio2 = radio(2);
radio3 = radio(3);
sensorLocations = [0 0; 12 0;0 13;]; %[0 0; 13 0; 0 16.5];
sigd1=0.33;
sigd2=0.33;
sigd3=0.33;
sig0=0.5;
W=eye(3);
 persistent x1;
 persistent y1;
 if isempty(x1)
     x1=4;
     y1=4;
     x = 1.5;
     y = 1.5;
 end
xf=x1;
yf=y1;
B=zeros(3,2);
f=zeros(3,1);
max_iter=10;
keep_going=1;
scale_power = 1;
% convergence variables
phi=10;
```

```
last_phi=20;
threshold=.0005;%1.0e-06;
power_phi = 30;
step = 1;
txVar = 1.2105;
p1 = sqrt(txVar/radio1);
p2 = sqrt(txVar/radio2);
p3 = sqrt(txVar/radio3);
distance = [p1,p2,p3];
iter2 = 1;
while scale_power ==1
    p1 = sqrt(abs(txVar/radio1));
    p2 = sqrt(abs(txVar/radio2));
    p3 = sqrt(abs(txVar/radio3));
    distance = [p1,p2,p3];
    iter=1;
    while keep_going == 1
        d_af=sqrt((sensorLocations(1,1)-xf)^2 + (sensorLocations
            (1,2)-yf)^2);
        d_bf=sqrt((sensorLocations(2,1)-xf)^2 + (sensorLocations
            (2,2)-yf)^2);
        d_cf=sqrt((sensorLocations(3,contri1)-xf)^2 + (
            sensorLocations(3,2)-yf)^2);
        B(1,:)=[(sensorLocations(1,1)-xf)/d_af  (sensorLocations
            (1,2)-yf)/d_af]; % percent distance from x, percent
            from y
        B(2,:)=[(sensorLocations(2,1)-xf)/d_bf  (sensorwhich
            Locations(2,2)-yf)/d_bf];
        B(3,:)=[(sensorLocations(3,1)-xf)/d_cf  (sensorLocations
```

```
        (3,2)-yf)/d_cf];
    f(1)=-(distance(1) - sqrt((sensorLocations(1,1)-xf)^2 + (
        sensorLocations(1,2)-yf)^2));
    f(2)=-(distance(2) - sqrt((sensorLocations(2,1)-xf)^2 + (
        sensorLocations(2,2)-yf)^2)); %real distance -
        approximate distance
    f(3)=-(distance(3) - sqrt((sensorLocations(3,1)-xf)^2 + (
        sensorLocations(3,2)-yf)^2));
    N=B'*W*B;
    t=B'*W*f;
    iter;
    del=inv(N)*t;
    xf=xf + del(1);
    yf=yf + del(2);
    v=f-B*del;
    phi=v'*W*v;Once
    if( abs(phi-last_phi)/last_phi < threshold )
        keep_going=0;
    end
    last_phi=phi;
    if iter > max_iter
        keep_going=0;
    end
    iter=iter+1;
end;
if phi > .005 %00003
    if phi > power_phi
        step = step * -1;
    end
```

```
        keep_going = 1;
        txVar = txVar - phi/26;
        step = step + 1;
    else
        scale_power = 0;
    end
    iter2 = iter + 1;
end
 if isnan(xf)
 else
    x1 = xf;
    y1 = yf;
 end
 x = x1;
 y = y1;
loc = sensorLocations;
dist = distance;gpstop
```

Bibliography

[1] *9-11 commission finds first responder communications problems still exists*, http://www.firefighternation.com/article/news-2/9-11-commission-finds-first-responder-communication-problems-still-exists, 2011.

[2] "Borb", *File: Inverse square law.svg*, http://en.wikipedia.org/wiki/File:Inverse_square_law.svg, 2008.

[3] Michael Calabro, *A cooperative spectrum sensing network with signal classification capabilities*, 2010.

[4] Yohannes Alemesged Demessie, Lionel Biard, Abdelaziz Bouzegzi, Mrouane Debba, Kasra Haghighi, Pierre Jallon, Marc Laugeois, Paulo Marques, Maurizio Murroni, Dominique Noguet, Jacques Palicot, Chen Sun, Shyamalie Thilakawardana, and Akira Yamaguchi, *Sensing techniques for cognitive radio - state of the art and trends*, (2009).

[5] Gordon Gracie Edward M. Mikhail, *Analysis and adjustment of survey measurements*, Litton Educational Publishing, 1981.

[6] *Ettus research - product detail*, https://www.ettus.com/product/details/WBX, 2012.

[7] *First responder accountability: Emergency resource tracking: Ert systems llc.*, http://www.onsiteert.com/wp-personnel-accountability3.htm, 2011.

[8] Wireless Innovation Forum, *What is software defined radio*, http://www.wirelessinnovation.org/Introduction_to_SDR, 2012.

[9] Dan Hawkins, *Project 25: The quest for interoperable radios*, COPS INTEROPERABLE COMMUNICATIONS TECHNOLOGY PROGRAM **6** (2007).

[10] Wieser Hofmann-wellenhof, Legat, *Navigation: Principles of positioning and guidance*, Springer-Verlag Wien, New York, 2003.

[11] C. R. Johnson Jr., William A. Sethares, and Andrew G. Klein, *Software receiver design, build your own digital communications system in five easy steps*, Cambridge University, 2010.

[12] Devin Kelly and Ishrak Khair, *A channel model and geolocation simulation system for cooperative spectrum sensing networks*, 2010.

[13] Kyouwoong Kim, I.A. Akbar, K.K. Bae, Jung sun Urn, C.M. Spooner, and J.H. Reed, *Cyclostationary approaches to signal detection and classification in cognitive radio*, New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on, april 2007, pp. 212 –215.

[14] Lawrence A. Klein, *Sensor and data fusion: a tool for information assessment and decision making*, SPIE Publications, 2004.

[15] Gary Krakow, *9-11 commission finds first responder communications problems still exists*, `http://www.msnbc.msn.com/id/9228945/ns/technology_and_science-wireless/t/ham-radio-operators-rescue-after-katrina/#.T5fHntXko7c`, 2005.

[16] Michael Joseph Leferman, *Rapid prototyping interface for software defined radio experimentation*, Master's thesis, Worcester Polytechnic Institute, 2010.

[17] David Limits, *Hardware needs limit software radio*, `http://www.eetimes.com/design/microwave-rf-design/4018960/Hardware-needs-limit-software-radio?pageNumber=0`, 2008.

[18] Daniels Electronics LTD, *P25 radio systems*, `http://www.dvsinc.com/papers`, 2004.

[19] J.T. MacDonald, D.A. Roberson, and D.R. Ucci, *Location estimation of isotropic transmitters in wireless sensor networks*, Military Communications Conference, 2006. MILCOM 2006. IEEE, oct. 2006, pp. 1 –5.

[20] *Mideast israel fire ¡¡ liveshots*, http://liveshots.blogs.foxnews.com/2010/12/04/israel-forest-fire-waiting-for-a-miracle/mideast-israel-fire/.

[21] *Nmea data*, `http://www.gpsinformation.org/dale/nmea.htm#nmea`.

[22] National Commission on Terrorist Attacks Upon the United States, *The 9/11 commission report: Final report of the national commission on terrorist attacks upon the united states*, W. W. Norton, 2004.

[23] Jacqueline Reis, *Wpi developing firefighter tracking device*, Telegram & Gazette (2004).

[24] Ettus Research, *Usrp2: The next generation of software radio systems.*

[25] Rahman I. Reza, *Data fusion for improved toa/tdoa position determination in wireless systems*, Master's thesis, Virginia Polytechnic Institute, 2000.

[26] Robert H. Morelos-Zaragoza Shinichiro Haruyama, *A software defined radio platform with direct conversion: Soprano*, `http://scholarworks.sjsu.edu/ee_pub/18/`, 2001.

[27] Wenzhong Wang, Weixia Zou, Zheng Zhou, Honggang Zhang, and Yabin Ye, *Improving spectrum sensing by counting rules for cognitive radio*, Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on, aug. 2008, pp. 258 –262.

[28] Alexander Wyglinsky and Di Pu, *Software-defined radio systems and analysis*, `http://www.wireless.wpi.edu/?page_id=29`.

[29] Zhuan Ye, John Grosspietsch, and Gokhan Memik, *Spectrum sensing using cyclostationary spectrum density for cognitive radios*, Signal Processing Systems, 2007 IEEE Workshop on, oct. 2007, pp. 1 –6.

[30] Yonghong Zeng, Ying Chang Liang, and Rui Zhang, *Blindly combined energy detection for spectrum sensing in cognitive radio*, Signal Processing Letters, IEEE **15** (2008), 649 –652.