THESIS OR DISSERTATION TITLE
TITLE LINE 2

by

Travis F. Collins

A Thesis
Submitted to the Faculty
of the
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements for the
Degree of Master of Science
in
Electrical and Computer Engineering
by

_____

December 2012

APPROVED:

_____

Professor Alexander Wyglinski, Major Advisor

_____

Professor Y

_____

Professor Z

Abstract

Since the advent of modern digital communications in the 20th century there has been an explosion in the demand for wireless spectrum. As a result spectrum is becoming an increasingly scare resource. This demand is a direct result of the availability and relatively inexpensive cost of such wireless device. Therefore in such environments as militaristic theatres the probability of interfering transmissions, intended and unintended, has steadily grown to a point where techniques need to be consider to combat such occurrences. More directly, in such situations when interfering signals are partially or completely understood measures can be taken to overcome such difficulties. Under these assumptions several well know techniques are can be applied to combat such scenarios. This research analyzes the feasibility of combining Antenna Subset Selection, Spectral Subtraction, and Blind Source Separation signal processing techniques to accomplish this goal. Together they provide multiple avenues of signal separation to remove such jamming effects, for both narrow and wide bands, without hindering the mobility of the nodes themselves.

Acknowledgements

Contents

Bibliography   **57**

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Since the advent of modern digital communications in the 20th century there has been an explosion in the demand for wireless spectrum. As a result spectrum is becoming an increasingly scare resource[46]. This demand is a direct result of the availability and relatively inexpensive cost of such wireless device. Therefore in such envirorments as militaristic theatres the probability of interfering transmissions, intended and unintended, has steadily grown to a point where techniques need to be consider to combat such occurrences. More directly, in such situations when interfering signals are partially or completely understood measures can be taken to overcome such difficulties.

In military theatres it is extremely common to observe friendly operated high-power broadband jamming signals[23]. Such devices exists as part of group convoys in several branches of the military and in many other forms in contested territories or war-zones. Unfortunately such devices block both friendly and hostile communications, and current anti-jamming techniques haven't provided a viable solution to this problem. Therefore new avenues should be considered, utilizing more flexible radio technologies.

Understanding how to overcome such challenges is a complex task; with vastly different

transmission enviroments and differing operating devices and operating standards. A new system that could combat such downfalls should rely on all friendly information, or be able to construct solutions of its own from a set of tools given to the radio. Such tools should be flexible and easily modified, changed, or improved. This ability to easily change or adapt is a key feature as the technical requirements can change from day to day, or between branches of the military itself. As such a solution should have the following attributes:

- **Flexible:** Easily adaptable to many situations and interference types, while still relying on the same hardware.

- **Efficient:** Relatively low hardware cost and low computational complexity

- **Hardened:** Designed to provide guaranteed performance gains even under severe channel conditions

1.2   State of the Art

Current implementations in anti-jamming technology lies on the strateling point of hardware and software in the communications world. This is true because hardware provides the speed and performance needed for digital data transmission, while software provides higher level intelligence and flexibility in such layers as the media access control layer and the network layer of the Open Systems Interconnect (OSI) model[61]. An outline of the model can be seen in figure 1.2. For anti-jamming applications, high intelligence allows for mobility again the jammer. Therefore a large implementation in software must be considered when investigating anti-jamming technics.

Current anti-jamming technics include channel hopping, spatial retreat, jammed area mapping, node escape, retreat restoration, frame masking, and many more[41]. All of these techniques use mechanisms of evasion or despection. These can be quite effective when attacked by generally narrowband, non-dynamic/non-learning jammers. In the case of wide and ultra-wide band jammers, they fail miserably. This wide-band enviorment is the primary situation of interest, and it generally considered a hopeless scenario. These anti-jam
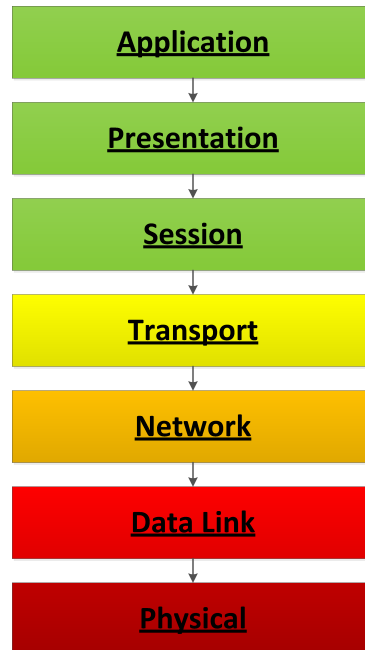
Figure 1.1: Open Systems Interconnection Model

technics are design for specific situations and jammers.

Let us first examine these anti-jamming technics which are broken down into three primary categories: Proactive countermeasures, Reactive countermeasures, and Mobile agent-base countermeasures[41]. Reactive countermeasures relies on a varying array of detection mechanisms first to determine if that node is being jammed. These detection methods must be coupled with a countermeasure or the scheme is in operable. Examples of these detection methods include a transmitter-based approach and a receiver-based detection. In a transmitter-based approach, such as ad-hoc networks, a decision algorithm is used based on four metrics: Packet Delivery Ratio (PDR), Received Signal Strength Indicator (RSSI), Physical rate, and Noise levels[16]. In the receiver-based detection additional information must be injected into frames to help the receiver determine the number of frames lost. Since frames can be easily lost in wireless transmissions, the receiver is handicapped when determining the number of retransmissions that have occurred. In the transmitter the PDR is deterministicly determined by the data-link layer, sequence numbers must be added to

frames for the receiver to accurately calculate the PDR[16]. Several other detection methods exist including using a detected detector, cooperative detection among nodes in a wireless network, and more sophisticated methods of RF fingerprinting[16].

Once the jammer has been detected the reactive countermeasures come into play. Many evasion techniques exists to combat narrowband jammers such as: channel hoping, spatial retreat, retreat restoration, hybrid attacks, and many cognitive radio approaches[8]. Many of these technics utilize the network itself to adapt to the jammer, which is an appropriate assumpt because without a network communications are irrelivant. Channel hopping is quite simple and can be considered easiet to implement. If a channel is begining jammed simply "hop" to another channel. This is easily defeated in two cases, the first the jammer follows you or the jammer is simply wideband capable. The second, spatial retreat, is a mechanism to physically evade the areas being jammed. Based on the detection algorithm all nodes in a network try to estimate the jammed region and flee physically in the direction of safer place. Based on their estimation about the jammed region, nodes will utilize shortest path algorithms to determine location of retreat[4]. Retreat restoration is focused around how to rebuild a network once the jammer has left. Retreat restoration can be done by coordinated or uncoordinated communication, and the transmissions are based on a pre planned hop patterns among nodes[52].

There also exists systems that are design to resist jamming proactively. These hybrid systems[48] utilize preventatives measure to resist jamming such as frequency hopping spread spectrum (FHSS). Spread-spectrum signals are highly resistant to narrowband jamming, unless the jammer has knowledge of the spreading key. In military applications the spreading key is generally created using a crytographic function[55]. More hybrid solutions include synchronous and asynchronous spectral multiplexing where intermediary nodes are used to communicate at multiple channels. When a node changes its channel because of jamming a neighbor will heal that connection by communicating with the node on its new channel and rest of the network on the old channel[38].

The largest problem with these techniques is they all have are designed to combat nar-

rowband jammers, and even friendly jammers. If high powered wideband jammers enter the equation, all of these solutions fall apart. Note these techniques primarily exploit the dimensionality of their envirmonent by simply avoiding the jammer, and all techniques require intelligent flexible hardware solutions. To implement such solutions requires suffisticated hardware implementations, that can be quite rigid for rapidly changing communication envirorments and adversaries. To compensate solutions that push more of the radio operations from their original rigid hardware implementations into the more flexible software domain, provide a more cost effective and elligent solution. These software focused radios, also know as Software defined radios, have provided a solid platform for very adaptive anti-jamming technologies under the name cogntive radios. These radios have the ability to easily learn and adapt to their envirorment, which is the primary requirement of anti-jamming devices.

As mentioned above, it is quite common for the military to self-jam its own channels. Unfortunately this can hinder their own use unintenially. These disrupted users are known as "disadvantage users". They are commonly small mobile hand held devices and cannot simply overcome the jammer computationally or in raw power; therefore, more manageable and eligent solutions must be considered for such disadvantaged users. Beside self-jammming, adversarial jammers must also be considered. Fortunately certain characteristics can be statistically exploited if these jammer abide by certain properties. Since adversarial jammers tend to inject random data or energy to block communication, if these transmissions can be shown to repeat they can be exploited. In the case of self-jamming, the signal characteristic can be know *a priori*; therefore they also can exploted or removed, negating the effects of such devices. Such scheme must consider the energy or symbols of the jammmer that are orthoganol and/or non-orthoganol to the symbols of the communication itself.

The goal of this project is to exploit a self-jammed and statiscially determistic adversarially jammed channel, throught the utilization of cognitive radio, implemented on a software defined radio platform. Software defined radios, defined as the intersection between hardware radios and computer software[40], provide a platform flexible enough to support highly intelligence operations such that anti-jamming requires. A proposed adaptive signal pro-

cessing software solution for mitigating the effects of both intentional and unintentional jamming (including wideband jamming) via the combination of antenna subset selection, spectral subtraction, and blind source separation (BSS) techniques in order to extract specific transmissions from a mixture of intercepted wireless signals. The goal of our proposed solution, called BLInd Spectrum Separation (BLISS), is to enable reliable, high throughput, and robust end-to-end wireless communications.

This work is a continuation of the work done through a collaberation of the United States Naval Academy, Worcester Polytechnic Insitute, and other external contractors. Primarily literature surveys and early simulations were completed or attempted before the transition of the project to the work done by this thesis. Credit is given to the following authors and there coensiding section or block as follows: Srikanth Pagadarai and Ryan Dobins Blind Source Separation, Robert Over Spectral Subtraction, Robert Capizzio Benjamin Hilbern and Dr. Christopher Anderson Antenna Subset Selection. This document examines the provided work dones by these individuals in detail, except for the topics in Antenna Subset Selection due to time constraints.

1.3   Thesis Contributions

This thesis will contribute the following to the wireless communications and signal processing research communities:

- A theoretical and simulated technique for non-orthoganol signal removal of undesired signals

- A theoretical and simulated technique for residual signal removal, primarily manifested as frequency selective fading

- A practical implementation using over the air communications of a anti-jamming sytem utilizing software defined radios. This implementation will tackle wideband

non-orthoganol and orthoganol jamming, and provide evidence of performance under specificied channel conditions.

1.4   Thesis Organization

This thesis will be organized into the following chapters. Chapter 2 provides the necessary background to understand basic communication system design, anti-jamming technics, and signal processing. Chapter 3 puts forward a theoritical simulations and a design of a physical anti-jamming system. Chapter 4 presents the results of the physical implement and analysis of its findings. Chapter 5 concludes the thesis, summarizing the accomplishments and outlines possible future work.

Chapter 2

Background

This chapter provides the background information needed to understand the chapters that follow. It examines the basic outline of a communication system and how non-idealities are compensated for, with addition of multiple input multiple output (MIMO) systems and a unique filtering technique called spectral subtraction. Secondly this chapter investigates common jammer scenarios and anti-jamming solutions. Finally it outlines the necessary hardware and software tools used in the implementation chapter.

2.1 Jamming

In 1899 Guglielmo Marconi successful transmitted radio messages across the English Channel, and nine months later Alexander Bell was discussing how this could be jammed during wartime[19]. Bell stated that such a wireless system can be easily disrupted with simple electromagnetic distrubances, "Its as easy as cutting the wires".[19] In the early days of wireless communication, such systems were very fragile but today they have become exponentially more resilient. In the simpliest form radio jamming is the transmission of electromagnetic signals that interfere with communications by decreasing the signal to noise ratio (SNR) between the transmitter and receiver. This jamming can be either deliberate or unintentional, and can either entirely disable the communication link or limit its capacity. A common example of unintentional jamming is, ironically, microwave ovens which operate at a wavelength of 122 millimetres which translates to 2.45GHz from equation (2.1). This

band directly interferes with channels defined under the IEEE 802.11 standard, also known as Wi-Fi[53]. Deliberate jamming on the otherhand, is generally more saphisticated and takes many different forms.

$$\lambda = \frac{v}{f} \tag{2.1}$$

Intentional communications jamming is usually aimed at radio signals in a militaristic setting, where consequences are insigificant or out of the relm of the law. In the most rudimentary designs, a jammer will simply tune their own frequency to that of their enemy and with a similar moduation scheme (and significant power) disrupt the enemies transmissions. The most common types of this form of signal jamming are: random pulses, stepped tones, warbler, tones, rotary, pulses, sparks, recorded sounds, gulls, sweep-through, and random noise[55]. These method obviously (or subtly) disrupt transmissions by inserting electronmagnetic energy into the transmission space of the receiver. In more technical terms, the jammer is producing randomly chosen data that is non-orthogonal to the data which the friendly transmitter is producing. Since this jammer's data is pseudo random when his transmissions are added to the 'enemy's', the result appears to be random as well. Therefore the signal is unrecoverable. As mentioned above, the jammer must produce signals that are non-orthogonal to the enemy of his jamming will have no effect. An example below shows random noise at a significant noise level is added to a previously destinquishable signal.

2.2   Anti-Jamming

Anti-jamming has been considerably outlined in the introductory chapter, therefore this section will examine more advanced narrowband and wideband techniques that involve filtering rather than avoidance. All of these approaches have various monitary costs, constraints, and power limitations. First narrowband mitigation techniques will be considered. These include adaptive filtering, time-frequency domain filtering, adaptive antennas and subspace processing. By combining several of the listed techniques, wideband jammers can
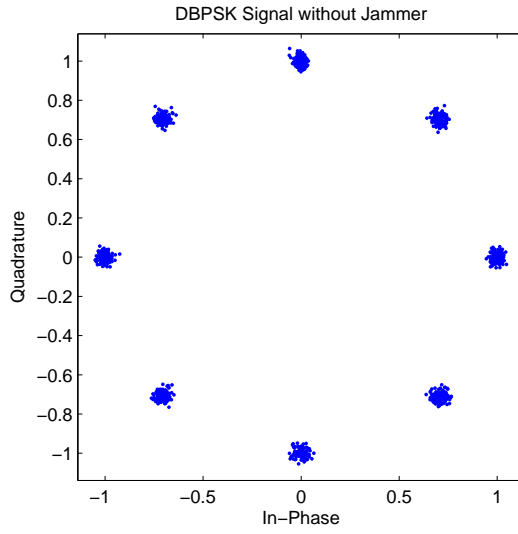
Figure 2.1: DBPSK signal uncorrupted by jammer
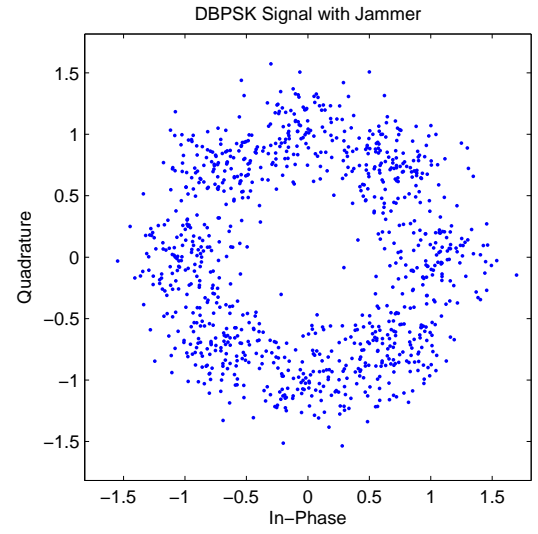
Figure 2.2: DBPSK signal corrupted by jammer

also be address, under certain conditions. Table 2.2 compares these techniques with various attributes.

Technique	Cost	Size	Flexibility	Complexity
Adaptive Filtering	low	small		
Time-Frequency Domain Filtering				
STFT	low	small	Environment Specific	low
Filter Banks	low	small	Environment Specific	low
Wavelet Transform	low	small	Environment Specific/Resolution Required	low
Subspace Processing	low	small		
Adaptive Antennas				
Null Steering	high	large		high
Beam Forming	high	large		high

Table 2.1: Comparision of Anti-Jamming Techniques

Adaptive filtering is a well defined solution in jammer mitigation, but it is to date the most limited. Most notably, the jammer must be a relatively narrowband and the period of the jammer must be relatively short. An example of an adaptive filtering technique is a suppression filter. Suppression filters assume statistically the signal is gaussian, which results in the optimal filter being linear. This filter essentially solves the Wiener equation

for an optimal filter, but generally a Least Means Squares (LMS) implementation is used instead of just inversing the channel estimate[27]. The technique of inverting the channel estimate or correlation matrix is traditionally called a zero forcing equalizer and is extremely unstable in the presence of small noise.

Next, time-frequency domain filtering attempts to represent the transform the received signal in such a way that it is possible to easily distinguish the jammer from the data signal. A Short-Time Fourier Transform (STFT) can be used to accomplish this goal. A STFT operates by sliding a window across a signal and taking the fast fourier transform (FFT) of that window. [17] uses the STFT to break a signal into its frequency components. From this information, with a narrowband jammer only a small number of frequency domain bins contain nearly all of the interferer. Therefore these bins can be simply nulled and an inverse FFT can be applied to the signal to regain its time domain version. This is very effective with the use of a spread spectrum signal with a narrowband jammer.

Filter banks is a second methodology that can be used to reduce spectral leakage in the frequency domain, which is the primary drawback with the STFT approach. One advantage of the filter banks approach is they do not inject interference when the jammer isn't present, which is a common problem when the jammer turns on and off frequently. Filter banks provide jammer suppression after their spectral decomposition stage, since at this point sub-band encoding can be accomplished this spectral modification can become excision for the jammer[32]. A similar decomposition is the wavelet transform. Unlike the STFT, the wavelet transform is much more flexible because the STFT has a fixed resolution for a given FFT size unlike the wavelet transform. Subspace processing, a wavelet transform, is applied in this way. The jammer subspace can be made orthogonal to the wanted signal subspace, nullifying the jammer's effects[59].

Besides these signal processing methods, physical techniques can also be use to do spatial filtering. These techiques make use of several antennas, and as an assumption the number of interferers must be equal to or less than the number of antennas. The first ap-

proach is called Null Steering. Null Steering constantly computes the weights in order to minimize the received energy level. In effect, this technique attempts to steer the antenna away from the jammer. The second approach is called Beamforming. Beamforming tries to adjust the antenna in order to maximize the SNR. In effect, the antenna beam is steered in the direction of the desired signal. It is of course, possible for the jammer's signal to be in the same direction as the signal source; therefore the postcorrelation technique is used in order to obtain the SNR. But, prior knowledge of the signal direction and the host location is required[33]. It is also important to note, that larger the number of elements in the array itself, the closer the jammer can physically be located to the desired transmitter.

Historically, all of these approaches historically were applied to spread spectrum communication systems because narrowband jammers fundamentally are considerably easier to deal with in this setting. They are more straightforward because the jammer effects only a fraction of the transmitter's transmission space; therefore, when wideband jammers exist many of these schemes fall apart. Other avenues or scenarios must be considered in such situations to overcome this limitation. Before a solution is chosen, additional signal processing and communication theory must be understood. These topics will be examined in the following sections.

2.3   Communication Systems

Modern wireless digital communication systems are based on a rich tradition of analog experimentation and theory. These signal technologies surround us constantly cellphones, car radios, GPS, and more. All these of these devices communicate over wireless links and are built upon the same building block of transmission and reception theory. Many perspectives can be taken, but a more generic observation should be taken at the system level. Depending on the level of sophistication these blocks can expand greatly, but still solve the same issue caused by the wireless transmission of digital access across their envirorment. Such non-idealities such as frequency offsets, doppler effect, signal echos, phase shifts, and

others must be compensated for to successful receive uncorrupted information.

Let us examine the transmitter first since it is less complicated than the receiver. The transmitter's primary goal is to send data in a resilient form, or structure, to create a more managable signal for the receiver. This is accomplished in several steps, and the function, or purpose, of the overall system determines the sophistication of the design. Figure 2.3 outlines the major building blocks of the transmitter; consisting of the coder, pulse-shape filter, and frequency translator. A filter is added after the coding block in some implementations to provide such effect as predistortion.
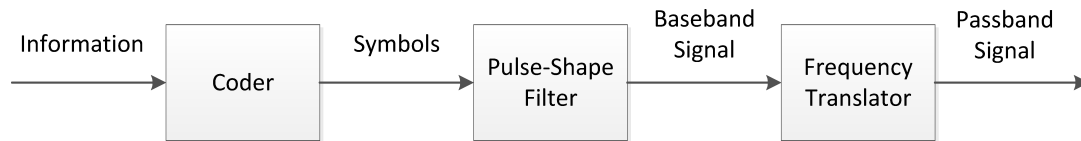
Information → **Coder** → Symbols → **Pulse-Shape Filter** → Baseband Signal → **Frequency Translator** → Passband Signal

Figure 2.3: Basic Transmitter Outline

The transmitter's sole purpose is the send data that is convient for the receiver to understand, and allow others to use the transmission medium as well. The coding phase of the transmitter can have many features and purposes, but simply it will encode data into a symbol with a form of redudancy or scheme that will help the receiver reconstructed the information more easily. Next the pulse-shape filter is used to help separate data and help maximize the SNR at the receiver. This filtering can be done with an asortment of filter shapes, but the most popular is the raised square-root cosine filter. After pulse-shaping, the signal is translated into frequency information and upconverted to a high RF with a carrier signal. The translation is done with a modulation scheme such a binary phase-shift keying (BPSK) or pulse amplitude modulation (PAM). The is upconverted by mixing the signal with a sinusoid, seen by equation (2.2). This done because low-frequency signals such as speech, music, or digital data can be much more efficiently transmitted at higher frequencies[15].

$$cos(x)cos(y) = \frac{(cos(x + y) + cos(x - y))}{2} \qquad (2.2)$$

Now let us discuss the receiver. At the system level, a modern digital receiver can be broken down into a small set of distinct categories or operations: carrier sychronization, timing synchronization, equalization, and frame synchronization; outlined in Figure 2.3. These sections work together in series to provide smooth transmission of data, and many techniques exist within theses categories to accomplish its goal. In most communication systems, after the radio frequency (RF) front-end, the first operation done on the received signal is frequency compensation and down conversion. This compensation needs to accomplished because non-idealities and differences exist between the transmitter's and receiver's oscillator. Therefore this is continually compensated for and corrected. Carrier recovery can be accomplished using several methods that include but are not limited to: squared difference loops, phase-locked loops, costas loops, and decision-directed phase tracking[15].
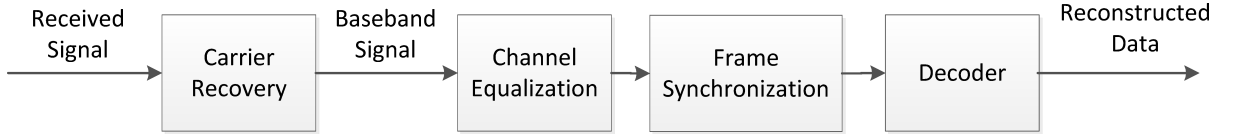

Figure 2.4: Basic Receiver Outline

After carrier recovery, the signal is pulse-shaped with the same filter shape used at the transmitter. This technique will help to maximize the SNR of the signal. Then the signal must be corrected again for timing. The purpose of timing recovery is to choose the instants at which to sample the incoming signal. This is generally done through a interpolation mechanism of the transmitted signal. Since at the transmitter the signal is upsampled to symbols, a single data point or bit is represented by several received data points. Therefore these points can be interpolated together for a more accurate estimate of the original data. Timing recovery also can be done with one of several methods including: output power maximization, Mueller-Muller method, or decision-directed. Generally they utlizie their own interpolation algorithm, such as sinc interpolation.

After this point the receiver designs can vary greatly, as the design in this thesis will present, because this is where most of the digital signal processing (DSP) will take place. This section, call Equalization, is responsible to correcting any effect the channel has on the signal. This includes multipath, noise, and other distortions that cause intersymbol interference (ISI). Equalizer implementations are designed to compensate for types of disturbances that occur using certain systems. The equalizer stage is most often coupled with the frame synchronization stage so the equalizer itself can adapt to changing conditions. This is known as soft decision making. Equalizer techniques include but are not limited to: LMS, decision-directed, dispersion-minimizing, viterbi, blind, and turbo equalizers.

2.3.1   Equalization

Equalizers can be considered the most complicated design of an entire communication system since they combat a series of distortions. The primary result of these distortions is called intersymbol interference (ISI). ISI simply means that symbols interact with one another in the channel space and cannot be considered independent from one another. Since this interference is generally considered a frequency selective disruption or disperation a filter needs to be employed to reverse such effects. This filter must be adaptable because the channel distortion cannot be know prior to transmission.

As listed in the previous section, many equalizers exists and operate under specific conditions. Here several linear equalizers will be discussed in detail including maximum-likelihood sequence detection, adaptively trained equalizer, and decision-directed linear equalization. The goal of all of these equalizers is to find a Finite Impulse Response (FIR) filter that when convolved with the received signal producing the original transmitted data $\hat{X} = Y * G$. Figure 2.3.1 outlines a typical FIR structure for which the equalizer will create the appropriate coefficents $b_0, b_1, ..., b_n$. These equalizers also examine the condition of an Additive White Gaussian Noise (AWGN) channel, and uncorrelated or independent interferers.
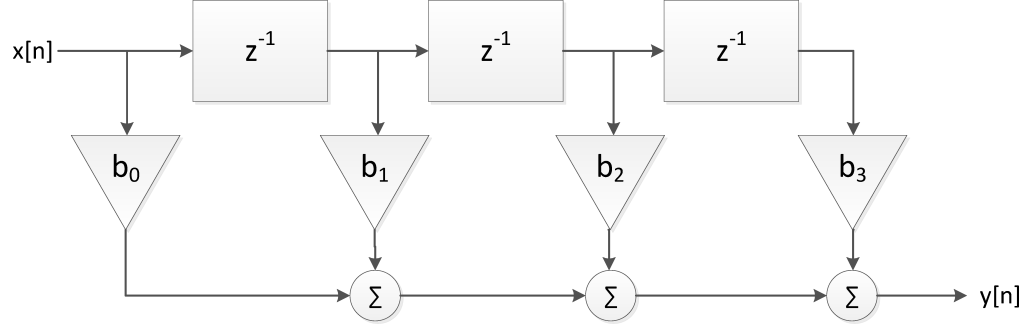
Figure 2.5: FIR Filter Structure

The Zero Forcing Equalizer (ZFE) uses peak distortion criteria to determine equalizer coefficents. If $H_c(f)$ is assumed to be the effects of the channel, the ideal equalizer would be $H_{eq}(f) = \frac{1}{H_c(f)}$. This can also be consider the inverse of the channel. The filter coefficents are modeled as weighted pulses convolved with the channel shown by equation (2.3).

$$p_{eq}(t) = \sum_{k=-M}^{M} w_k p_r(t - kT) \tag{2.3}$$

Unfortunately the ZFE has a large disadvantage, it cannot compensate for small amounts of noise. Technically, the ZFE will amplify all noise of the received signal, and if any elements of the channel matrix are considerably small, then the equalizer becomes unstable. Therefore this is generally considered a more theoretical or elementary equalizer formulation. To overcome this problem the zero ISI condition must be relaxed allowing for noise which if small can easily be overcome by such operations as quantization or decision making. The Linear Minimum Mean Squared Error Filter (LMMSE) takes this relaxation into account.

The LMMSE assumes that the symbols are uncorrelated with one another and uncorrelated from the noise in the channel. This approach tries to minimize the mean square error, a common measure of estimator performance. The estimator is defined as $\hat{x}_{MMSE}(y) = \exp x|y$. If x and y are jointly Gaussian, then the LMMSE will be linear. This function or equalizer design minimizes the mean square error. To simplify further an extension to random vectors can be examined. An estimate can be made for the original

vector x represented by $\hat{x}$, resulting in the linear equation $\hat{x} = Ay + b$. The LMMSE will minimize the mean square error $MSE = \|x - \hat{x}\|^2$.

Besides these linear equalizers outlined, an adaptive approach can also be considered. The Least Mean Squares (LMS) or Gradiant algorithm utilizes a traditional technique for minimizing the error in a signal. This method is historically known as the "Method of Steepest Decent" or "Newton's Method". By calculating the error of each received symbol, this can be fed back into the system for future symbols. This error will shape the equalizer's filter coefficents to match the inverse of the channel. The equations 2.4, 2.5, and2.6 outline the LMS algorithm.

$$y[n] = w[n]^H u[n] \tag{2.4}$$

$$e[n] = A_n - y[n] \tag{2.5}$$

$$w[n+1] = w[n] + \mu u[n] e^*[n] \tag{2.6}$$

In these equations μ acts as the algorithm's stepsize determining how quickly it will converge. It must also be considered that the larger the stepsize the higher the probability it may become unstable. As long as the channel's effects are slow changing, this equalizer can easily maintain up to date estimates while corrupting as little of the data as possible.

All of the methods proposed so far require *known* data to correct against. This data is called training data and generally comes in the form of a preamble in a frame. The preamble is added to the beginning of each frame so the equalizer can learn from the effects on that specific data. The preamble is the same for all frames and is always used so the equalizer will always be learning. But what happens when data is unknown in the frame; for example, the data portion of the frame. This is where blind equalization comes into play.
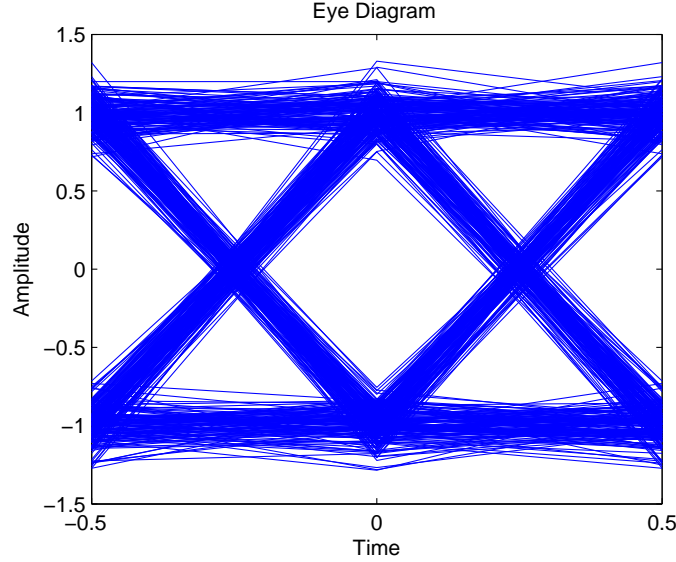
Figure 2.6: Good timing recovery produces open eye

Several blind equalizers exist but an extension of the LMS equalizer for blind situations will be examined here called the decision-direct equalizer. For a blind equalizer to operate an error generation mechanism must be evaluated, but since the data symbols are unknown, a decision device must be used inplace. This decision device is a quantization method and error is generated from this quantization. This error generation is extrapolated from the equation 2.7.

$$e = \frac{1}{2} \exp \left(sgn(y[k] - y[k])^2 \right) \tag{2.7}$$

This is quite similar to the original LMS implementation except instead of a known symbol the data is quantized using the sign function. This type of quantization using the sign function is only applicable with binary modulation schemes such as BPSK. This equalizer method is usually combined with a training equalizer method in practice; since if a nearly closed eye is observed, when using an eye diagram, this equalizer cannot open it by itself. An example of such an eye diagram is shown in figure 2.3.1, and clean/open eye diagram can be seen in figure 2.3.1.
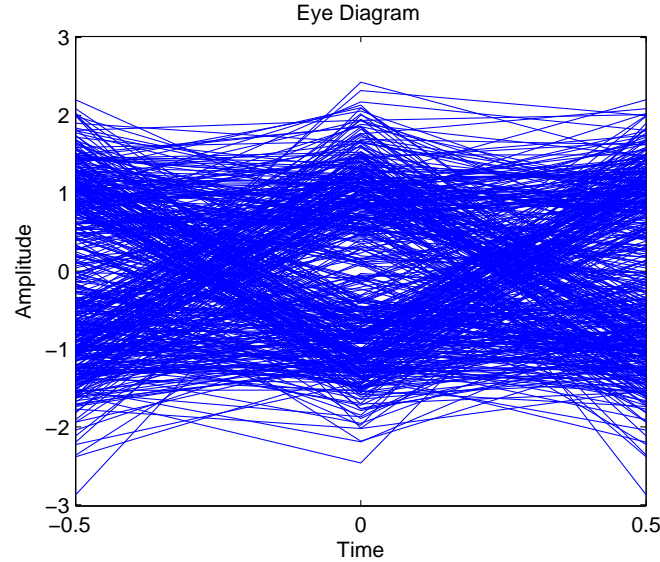
Figure 2.7: Poor timing recovery produces closed eye

In this section we have examined several equalizer technics while outlining their advantages and disadvantages. Most techniques require some training mechanisms to operate under heavy channel distortion, and blind techiques such as decision-directed equalization will fail under these conditions. Unforunately such training data can take considerable resources, and lower overall data throughput. In practice as much as 20% of frame information is training, therefore other techniques must be considered to help overcome this obsticle.

2.3.2 Superimposed Training Equalization

As mentioned in the previous section, many implementations exist for equalizer designs, but this thesis will examine the effectiveness of superimposed training symbols in frequency selective channels. In traditional equalizers, channel estimation is achieved through the use of training data or pilot symbols. These symbols are both known to the transmitter and receiver, providing the basis for an estimate. In these equalizers all training symbols are placed at the start of a frame,[5] shows that under high SNR training-based schemes are capable of capturing most of the channel capacity, while under low SNR they are highly

suboptimal. Superimposed equalizers try to overcome this problem along with others to provide more optimal estimates. Superimposed equalizers physically add training symbols to the data stream instead of concatinating symbols, saving precious bandwidyj bandwidth[5]. To accomidate such pilots, energy must be shared among the data and hidden pilots[24]. [21] shows that for a transmitter of fixed power, with an additive pilot sequence, the decrease in data signal power is equal to

$$K_{loss} = \frac{E[\|s(k)\|^2}{E[\|s(k)\|^2] + E[\|u(k)\|^2]}$$

equivalent to $10logK_{loss}dB$ in signal to noise ratio (SNR). Other disadvantages include an increased signal envelope fluctuation that can be undesireable in nonlinear transmit power amplifiers[60].

At the receiver, channel estimation can be done using several techniques in both the frequency and time domain. [60] examines a time domain approach for synchronized averaging of the received signal. It is important to note that this synchronization isn't related to transmitter and receiver synchronization. [60] and [43] both assume that the signal $x(n)$ and noise $v(n)$ have zero mean and $E[m_x(n)] = d(n) = p(n) * h(n)$. Therefore since $p(n)$ is the known superimposed periodic pilot sequence, $h(n)$ can be determined. $h(n)$ is generally considered frequency selective, and such channels can be quite difficult to deal with especially with multipath. Multipath interference is a distortion caused when copies of the original signal arrive at the receiver delayed ontop of the originally received non-delayed signal. This delayed signal essential took another path to the receiver, and this interference is commonly called ghosting in such applications as television broadcasts[18].

Superimposed equalizers are able to better compensate for large multipath channels because they can spread their training symbols throughout the signal itself. This spreading not only provides a spreading in time but also in other dimensions such a frequency. Therefore if the training symbols are chosen correctly and placed correctly, they can then be spread across the frequency spectrum efficently and capture its selectivity. Before the pilots can be examined, the channel must be defined. The channel will be of block length N, and the

channel is also time invariant across single blocks, but variable across blocks. The memory of this channel is of maximum length $L-1$, and the impulse response of the channel is defined as $\mathbf{h} = [h_0, ..., h_{L-1}]^T$. Since there are N blocks in the channel, the channel matrix H is modeled as an NxN circulant matrix, with the received signal as expressed as:

$$\mathbf{x} = H\mathbf{s} + \mathbf{v}$$

Here $\mathbf{v}$ is assumed to be zero mean white noise. The vector s is a combination of known training symbols and unknown data. The optimal placement for such training is where the channel undergoes nonergodic fading considered here [6]. [5] continues on to say that optimally, assuming symbols are placed in clusters of length $\alpha \geq 2L + 1$, this scheme is quasi-periodic. The variable α represents the cluser size in this scenario. It is also important to note that this placement makes sure that the training is always orthogonal.

Another consideration that must be considered is how these training symbols interfer with the data itself, and is the training symbols dependent on the data or even the modulation scheme.[24] examines this aspect and proposes solutions that provides a data independence condition. As explained, since the training data is periodic it can be placed in equispaced frequency bins, while data is spread across all frequency bins. Therefore the pilot must be designed to distort the data vector of the discrete fourier transform to zero. In the superimposed training data case, this is done by using the cyclic mean of the data. Therefore all that needs to be done is the removal of the cyclic mean $\mathbf{e} = \mathbf{Jw}$. $\mathbf{J}$ is the kronecker product of an identity matrix and the fractionally spaced locations of the pilot tones. Therefore at the pilot frequency only the training symbols are visible for the channel estimation. Formally here is the transmitted result including pilots and data: $\mathbf{s} = (I - \mathbf{J})\mathbf{w} + \mathbf{c}$.

In summary, modern research on superimposed training focuses primarily on the training symbol generation for a certain type of communication sytems design from single transmission to multiple-input multiple-output (MIMO). Unfortunately little to no physical implementations exists for such system. This is true because of the sychronization issue that exist when using superimposed training symbols. Since they are directly placed with transmit-

tion data it can be difficult to determine their locations in a sequence blindly, which is done in real world systems. This problem must be considered when phyiscal implementations are proposed.

2.4   Spectral Subtraction

New signal processing techniques are devised and evaluated in academica at an accelerated rate[**?**]. In this thesis a new application for a relatively standard technique was examined, called Spectral Subtraction (SS). The SS technique was first published in 1979 by Steven Boll[13]. SS is formally used to reduce ambient noise in audiable sources, improving the overall quality and intelligability of digitized speech. It is a dominant speech processing algorithm and many extension including [34], [57], [25], and many more improvements can be seen in the literature. Due to the large amount of litereature and investigation into the SS process it was assumed to be a solid option for removing unwanted signals in the spectrum.

SS primarily was designed for audio signal processing, small bandwidth signals roughly from 20Hz to 20,000Hz. Many forms of SS exists, but the approach examined here is Magnitude Spectral Subtraction (MSS). It works by first generating an estimate of the noise in the signal itself, which is usually attained at the first first few seconds of the signal itself. This noise is then subtracted, as the name suggests, from the rest of the signal. Mathematically let this be explained further. The received signal is assumed to be a combination of two signals, the transmitted and the noise itself $y(t) = x(t) + n(t)$. Next the power spectral densities (PSD) are calculated for these components $E\{|Y(e^{jw}|^2\} = E\{|X(e^{jw}|^2\} + E\{|N(e^{jw}|^2\} + 2E\{|X(e^{jw}|^2\}\{|N(e^{jw}|^2\}$ $E\{|Y(e^{jw}|^2\} = E\{|X(e^{jw}|\} + E\{|N(e^{jw}|\}$ Since at points when the desired is in present in the sprectum, a silent period, the measurement for N is taken and then subtracted from the entire received signal $E\{|X(\exp jw|\} = E\{|Y(\exp jw|\} - E\{|N(\exp jw|\}$. The is noise is amused to be quite stationary during the signal period, therefore the original estimate $\hat{N}$ can be quite accurate.

2.4.1   Residual Noise

As a result of the changes over time in the noise spectrum (whether power or magnitude) around its expected value, there is always some difference between the actual noise and its mean value. Hence some of the noise remains in the spectrum in the case that the value of noise is greater than its mean and some of the speech spectrum also is removed in the case that the estimate of noise tobe greater than the actual value of noise. The latter produces negative values in spectrum. These negative values are prevented or set to a floor (sometimes zero) using different techniques. The overall effect puts a noise in the output signal known as residual. The narrow band relatively long-lived portion of residual noise is sometimes referred to as musical noise:

A close examination of musical noise, shows that peaks and valleys exist in the shortterm power spectrum of white noise; these frequency locations for one frame are random and they vary randomly in frequency and amplitude from frame to frame. When a smoothed estimate of the noise spectrum is subtracted from the actual noise spectrum, all spectral peaks are shifted down while the valleys are set to zero. Therefore, after this subtraction sharp peaks reamin in the noise spectrum and pre-existing ones can be shapened. The wide peaks are generally estimated as time varying broadband noise. The narrower peaks, which are relatively large spectral distances because of the deep valleys that define them, are perceived as time varying tones which are generally referred to as musical noise[11].

Therefore [13] continues by introducing a 'smoothing' technique before the signal is convert back into the frequency domain. Two additional parameters are introduced: α the oversubtraction coefficent, and β the noise floor lower bound. α is used to provide a more aggresive subtraction to the signal, attacking high peaks which are generally a result of high noise and an inaccurate initial estimate. The second parameter β is used to fill in the valleys of the signal. Since if an oversubtraction takes too much signal it can cause valleys in the spectrum below or above the zero threshold. This value is used to simply quantize values within its +/- limits. As a result these operations together produce a smoother signal removing much of the residual noise from just a plain subtraction. [13] provides several

results examining the benefits of such a technique.

2.5 Software Defined Radio

For the past two decades there has been a peradyme shift is the definition of a radio device. The conversation has to do with the question of where hardware ends and where software begins. The term Software Defined Radio, coined by Dr. J. Mitola III, defined as a set of digital signal processing (DSP) primitives, a metalevel system for combining the primitives into communication system functions (transmitter, channel model, receiver, etc.), and a set of target processors on which the software radio is hosted for real-time communications[39]. Dr Mitola understood how software provided the flexibility that hardware never could, and as time made it more maliable SDR would become dominant.

SDR's can be flexible enough to avoid the "limited spectrum" assumptions of designers of previous kinds of radios, in one or more ways including: ultrawideband transceivers, cognitive radio, dynamic mesh networks, software-defined antenna arrays among others[54]. One of the first SDR implementations was a project called "SpeakEasy". The original purpose of SpeakEasy was to use programmable processing to emulate more than ten existing military radios, operating in frequency bands between 2 MHz and 2 GHz[36]. Therefore with this single radio, the operator could talk to ten radios operating under ten different standards. As simple enough idea, but unforunately the implementation left much to be desired. For example, physically the device encapsilated the entire back of a common pickup truck[36]. This might be great for a ground station that doesn't move, but for a mobile unit this was highly impractical. Secondly in 1992, field programmable gate arrays (FPGA) required significant time, compariatively to reflash or change their operational parameters. Again this also limited SpeakEasy's flexibility.

Today the prime implementations are within cellular basestations and other military applications such as the JTRS project. The JTRS or Joint Tactical Radio System, was

a program of the US military to produce radios that provide flexible and interoperable communications. Examples of radio terminals that require support include hand-held, vehicular, airborne and dismounted radios, as well as base-stations[35]. Again this project still has limited results and many setbacks have occured. Commerically, from a wide spread penetration standpoint, SDR is still many years away. The two barriers to this are speed and size. To provide enough data throughput, modern SDR's need to quite large physically, which is a serious drawback in many applications. Aside from these limitations, SDR's provide excellent flexibolity esspecially in a laboratory and proof of concept envirornmnet. Rapid protoyping is an obvious place where such radios shine, allowing massive changes without hardware modification. To support this flexibility several software packages have been constructed around the SDR concept, allowing for aggresive prototyping. The two examples discussed here were selected because of operability with the selected hardware, which will be discused future in chapter 3.

2.5.1   GNU Radio

The first software package to be discussed by this thesis is GNU Radio. GNU Radio provides the reconfigurable signal processing blocks that are necessary for software defined radios. GNU Radio is an open source project allowing for SDR developers to develop unique signal processing blocks and SDR systems. GNU Radio was started in 2001, originally forked from the SpectrumWare project developed at the Massachusetts Institute of Technology[14]. Since 2001 the codebase has undergone massive changes, containing almost no code from the original SpectrumWare project. Physically the code consist of three languages Python, C++, and SWIG. Python provides the overarching control of the system or program, while C++ provides the actual signal processing blocks and mathematics. SWIG is a wrapper for C++ which allows Python to dynamically wrap around C++ and control or compile with it. A diagram below better illustrates this architecture. It is also important to mention that there as significant paradyme shifts in the community, pushing more and more code to Python rather than C++, due to its easier programming syntax and structure.
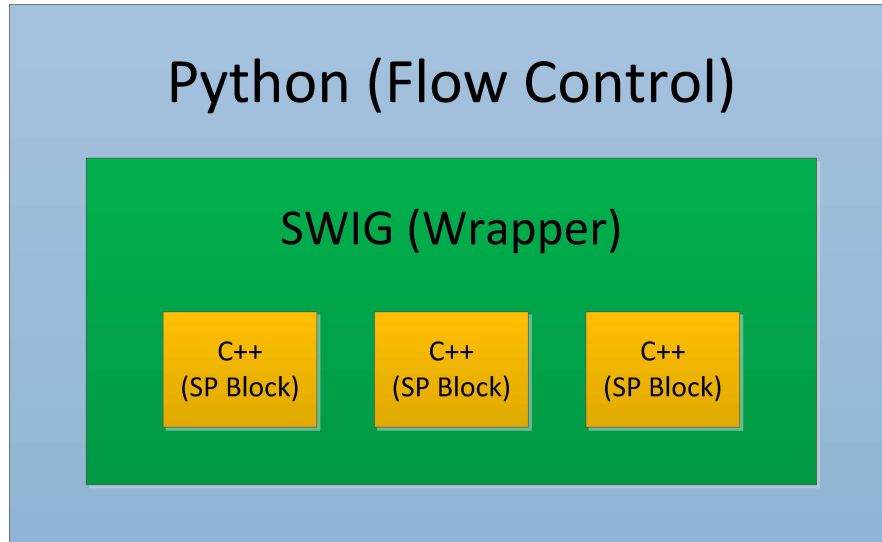
Figure 2.8: GNU Radio Code Structure

2.5.2   MATLAB

MATLAB is an extremely well known engineering, mathematical, biological, and financial software suite. MATLAB provide massive data leverage and advanced communication system models and algorithm for significant data processing. Since 2007, they have also provided hardware compilance with specific SDR platforms through their Simulink platform, and more recently within MATLAB itself[29]. This thesis primarily utilizes the signal processing and communication system aspects of matlab, since MATLAB cannot fully utilize all aspects of the chosen hardware. It is important to note under alternate constraints, MATLAB can provide adiquate performance directly interfacing with hardware, esspecially when accessing its targeting features seen here [30]. Figure 2.5.2 shows an example of a common MATLAB SDR model through Simulink.

2.5.3   Comparision

It is important to compare GNU Radio and MATLAB, from a user's perspective they perform quite differently. Firstly GNU Radio, is extremely fast, will the ability of sustaining the maximum throughput of the selected hardware. GNU Radio is also multi-threaded, and
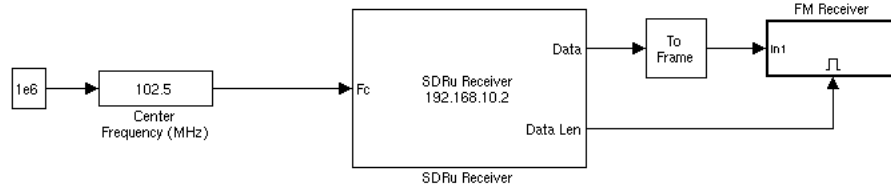
Figure 2.9: Sample SDRU MATLAB Model

while mainitaining high throughput and complete background tasks on mutlicore machines quite easily. This performance has a cost, comparitively GNU Radio has an extremely learning curve and debugging can be challenging. But if you need the performance GNU Radio is your option, can does provide significantly more advanced hardware support is SDR implementations. If data analysis is more heavily desired MATLAB is the obvious choice. MATLAB provides easy and advanced data visualization functionality, and built in tools for analysis. Since MATLAB doesn't compile itself normally, it can be much easier to debug and solve problems. MATLAB's syntax provide similar data manipulation, esspecially in communication system primatives. Therefore it can be a rather simple choice, speed or ease of use.

2.5.4   Summary

This chapter outlined and examined the topics of jamming and anti-jamming techniques, and provided a foundation in communication system theory and advanced equalizer design. Secondly it setup an understanding of Software-Defined Radio, the power of such an architecture, and examples of implementations and exisiting software for future designs. Next this thesis will consider a new anti-jamming technique and design an implementation of such a system. After the implemenation is investigated, the result of specific experiments on such an implementation will be analysed.

Chapter 3

Implementation

3.1 Overview

Now that a significant background has been provided, the problem this thesis combats will be futher framed and defined. This chapter outlines the proposed implementation of a receiver design, for wideband jammer scenarios and low-mobility situations. An adaptive signal processing software solution for mitigating the effects of both intentional and unintentional jamming (including wideband jamming) through a combination of three techniques. These include: antenna subset selection, spectral subtraction, and blind source separation (BSS), which work in conjuction with one another to extract specific transmissions from a mixture of intercepted wireless signals. The goal of the proposed solution, called BLInd Spectrum Separation (BLISS), is to enable reliable, high throughput, and robust end-to-end wireless communications, especially high capacity multimedia (voice, data, imagery) transmissions. In particular, the focus of the proposed work is the so-called "disadvantaged user". These users are generally considered limited in transmission and processing power such as small-deck combatants, submarines, unmanned air vehicles (UAVs), dispersed ground units in urban and radio frequency (RF) challenged environments. The previous research is also discussed for each section and implementation consideration are examined from this work.

The BLISS solution integrates three well-known adaptive signal processing algorithms

found in the open literature: antenna subset selection, spectral subtraction, and blind source separation. Each of these algorithms is employed within the BLISS framework in order to enable the process of extracting individual transmissions intercepted from several mixtures of wireless signals. Although blind source separation can readily extract transmissions under ideal conditions, the BLISS system is aimed at harsh spectral envirnorments consisting of many users and in some cases jamming devices. Therefore BSS will not provide adiquate signal separation for robust throughput. Hence, the other two algorithms, spectral subtractions and antenna subset selection will aid in this effort.

In previous sections it has been understood that current anti-jamming techniques cannot compensate in deterministic wideband jamming scenarios. These scenarios must be throughly understood before a practical solution can be provided. For this thesis, the worst case scenario will be considered for the jamming device. For simplification a narrowband jammer will be considered as an adversary, and the transceiving devices cannot frequency hop thus remaining on the same frequency as the jammer. The jammer has an identical modulation scheme as the friendly tranceivers and the constellation is in phase. Finally the jammer is assumed at a similar distance and transmit power as the friendly tranceiving devices. Under these conditions the jammer is completely orthogonal and historically impossible to remove.

This chapter is broken down into several sections which include a system level overview, the hardware and software choosen, signal removal evaluation, the superimposed equalizer design, and the antenna subset selection work. Each of the systems that makeup BLISS have different purposes and goals allowing them to tackle different problems that occur. It is important to note that these systems are at differing stages of development due to the limited time and initial development put into these blocks.

3.2 System

To provide a more straight forward explaination of the BLISS system it is appropriate to provided a system level overview. The system's original purpose was to remove the effects of narrow and wideband jamming. It accomplishes this goal through a series of processing blocks and a selection block. These blocks include: the antenna subset selection (AntSS) block, spectral subtraction block, and finally the blind source separation block. The figure below shows the interconnections between these blocks and certain modification were made from the original design of the system due to practical constraints. These changes will be brought fourth as the blocks themselves are discussed in detail. Since an external research group is responsible to the AntSS block, it will not be throughly discussed by this thesis, but its fundimental purpose will be examined.
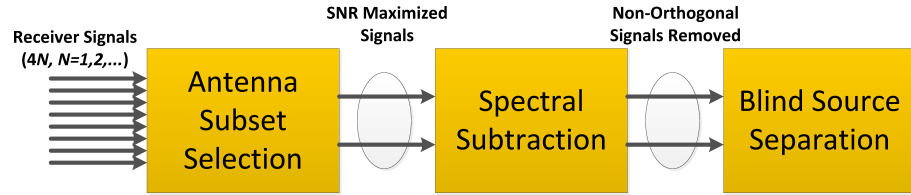

Figure 3.1: Overview of BLISS System

The first step in the BLISS system is to pass through the AntSS block. Physically this block is equipped with many antenna in groups of 4. As the block title portrays a subset of these antennas will be selected and they will be passed on to the next block. Precisely a $2^M - to - 2^N$ downselection from an array of receive antennas to a set of BLISS receiver inputs. Each individual AntSS board provides 4-to-2 antenna downselection through a set of RF switches. The goal of AntSS is to provide spatial separation through an array of antennas maximizing the SNR of the wanted signal. It is important to note that the antenna spacing must be adiquet to provide enough separation or independence, depending on the operating frequencies or wavelength of the signals themselves. Once the appropriate antennas are selected two signals are to the spectral subtraction block.

The spectral subtraction block is next, which is used to removal known unwanted signal from the spectrum so the source separation block and work properly. The original design of the spectral subtraction block is to use an existing audio technique of removing noise or signals in the frequency domain through a subtraction and smoothing technique. This technique was discussed previously in the background section, therefore its historical literature will not be examined futher. To enable removal of unwanted signals, the Spectral Subtraction block maintained a database of known power spectral densities (PSD) of common modulation schemes. A recognition system would be implemented to automatic identification of the interfering signal and the block would simply subtract it out, through its already known estimate from its database. Next the newly subtracted signal would be passed to the Source Separation System, where the signal would be unmixed.

The source separation block separates signals when only their mixtures are observed. The operation is called blind, since the signal sources and mixing procedure are unknown to the receiver. Under some conditions this constraint cannot be completely upheld. This is true because the solutions needed to solve such an event become generally intractable. An initial approach in this project was to use a technique called AMUSE (Algorithm for Multiple Unknown Signals Extraction)[37]. AMUSE works by first collecting an estimate of the covariance matrix of the received signal, computing the singular value decomposition of that covariance matrix, then performing several transforms on the received signal once the number of mixed received signals is known. Then a covariance is calculated from these transformed received signals which are offset by some instance τ, and a eigenvalue decomposition is done upon these covariances. From this decomposition the singular values are used with the transform matrix and the received signal to provide an estimate of the wanted source signal.

$$R_y = E[yy^t] \tag{3.1}$$

$$z = Cy \tag{3.2}$$

$$R_z = E[z(\tau)z(t - \tau)^t] \tag{3.3}$$

$$\hat{x} = VhattCy \tag{3.4}$$

It is important to note that for simplicity the mixing matrix for the original proposed solution involving AMUSE is generally constructed as a linear time invariant (LTI) system. There is some activity occuring with nonlinear mixing, but that was considered outside of the scope of this problem.

3.3   Hardware and Software Platforms

Before any implementation was considered a platform needed to be choosen for the end result. This selection provided the work flowpath for the implementation, eliminating many options. As discussed in previous chapters, the end result wants to leverage the power of Software-Defined radios (SDR). The hardware platform chosen was the USRP2 designed and built by Ettus Research[49]. These radios are readily available in the Wireless Innovation Laboratory and since the number of radios required for the design was still unknown, it was an obvious choice. There are several software packages that support the USRP2 hardware and several will be examined in this chapter.

The USRP2 or Universal Software Radio Peripheral are intended to be a comparatively inexpensive hardware platform for software radio, and is commonly used by research labs, universities, and hobbyists[42]. The USRP2 connects directly to a host computer through a Gigabit Ethernet link, which relays baseband sample that have been receiver or tobe translated. The motherboard provides the following subsystems: clock generation and synchronization, FPGA, ADCs, DACs, host processor interface, and power regulation. Several of these component are seen in the image below. These are the basic components that are required for baseband processing of signals. A modular front-end, called a daughterboard, is used for analog operations such as up and down conversion, filtering, and other signal

Figure 3.2: Full USRP2 Hardware with Daughtercard

conditioning. By replacing this RF daughtercard many different frequency ranges can be examined.

The information flow is important to understand within the phyiscal radio. This SDR block diagram shown below, outlines the common tasks done by the: daughtercard, FPGA, DAC/ADC, and host computer. Since the FPGA is programmable the operations can change if desire, but the three dominating software packages that utlize the USRP2 flow this structure. Beginning on the far left of the diagram and continuing to the right, at the daughtercard are RF emitions are received and transmitted. The daughter also contain mixers that translate the signal to an intermediate frequency. Next come the dual 100 MS/s 14-bit ADCs, dual 400 MS/s 16-bit DACs, two digital down-converters with programmable
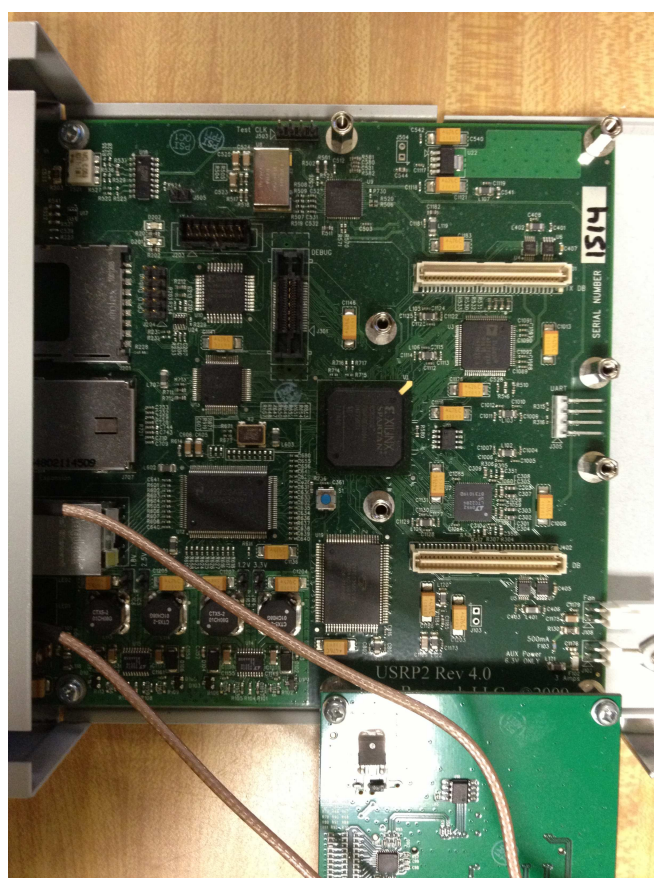
Figure 3.3: USRP2 Mainboard

decimation rates, and two digital up-converters with programmable interpolation rates[49]. These are located on the mainboard of the USRP2 itself. The FPGA is a Xilinx Spartan 3 XC3S2000, which with the current FPGA software is 59% free in general logic but only 3% free in memory. The FPGA also does not have any DSP resources. The limited memory left in the USRP2 FPGA severely limited any additional development. As a result on newer models, such as the N210, the FPGA has been upgrade.[50]
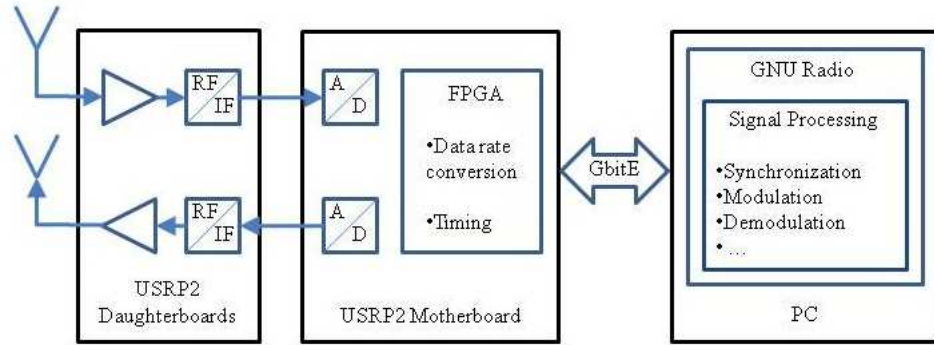

Figure 3.4: USRP System Block Diagram[1]

The data itself constain several pieces of metadata in a frame. RX metadata structure for describing sent IF data includes time specification, fragmentation flags, burst flags, and error codes. The receive routines convert IF data headers into metadata[20]. Such metadata can be used to indicate the position and FPGA timestamp associated with the sample that corresponds to the start of the underlying frame. By default, existing blocks will transparently propagate any attributes contained on their input streams to their output streams. Blocks that use the attributes can query their input streams to locate all (key, value, offset) tuples in the region of the stream that they are currently working on in their work method. Likewise, blocks can copy, add or delete attributes on their output streams[2]. This knowledge is extremely useful when doing multiple receive antenna arrays when alignment is necessary, or in any situation where fine timing information is required.

With the USRP hardware several software options are available including: GNU Radio,

MATLAB, LabVIEW, and several custom packages. MATLAB and GNU Radio have already been discussed, therefore the selection between them shall be discussed. Since this system is a MIMO implementation signal alignment is a requirement. MATLAB doesn't support sample alignment in a multiple USRP system. The sample alignment is possible through either external means through an external clock or through the option choosen here the MIMO cable. The MIMO cable, a picture of it can be seen in figure 3.3, is a standard 16-pole flatcable to connect tvrx, basic-rx or dbsrx boards. Of this 16pin flatcable only two pins are used (io15 and ground)[3]. An image also of the combined dual radio source block can be seen in figure 3.3 from GNU Radio. With this requirement GNU Radio must be used for direct access with the USRP2. Aswell full implementation of the systems blocks were first attempted with GNU Radio. Fortunately, if necessary, data can be passed to MATLAB for signal processing from GNU Radio through the use of the file blocks and a script located in Appendix A.
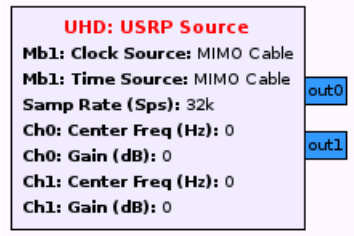

Figure 3.5: USRP2 MIMO Cable

Figure 3.6: GNU-Radio MIMO Enable Source Block

3.4 Spectral Subtraction

Now that the a formal system level approach has been presented and hardware setup chosen, a more detailed understanding of the blocks themselves can be examined. The goal of the spectral subtraction block is to removal signals to allow the blind source separation block to work properly. As discussed previously signals would first need to be identified and then removed based on information supplied in a precompiled database of known signals. The technique to remove such signals is called spectral subtraction, which primarily takes place in the frequency domain. This approach only relys on known PSD's of the interfering signal. Initially this technique seemed quite sound, but futher investigation proved otherwise.

Initial simulations were created to examine this spectral estimation technique at RF frequencies rather than the standard audio frequencies for which Spectral Subtraction is formally used. Only two signals were used in these simulations, both utilized the same modulation scheme and pulseshaping filters. The signals were chosen to be non-orthoganal, since when they are orthogonal The frequency of the interfering signal was varied, and so were the oversubtraction parameter α and quantization floor β. Through experimentation α worked best at a value greater than 10, and β worked best between 0.05 and 0.2. The graph in figure 3.4 shows the bit error rate (BER) as the interferer is shifted across the wanted signal in frequency.

As you can see this spectral subtraction technique operates extremely poor when the
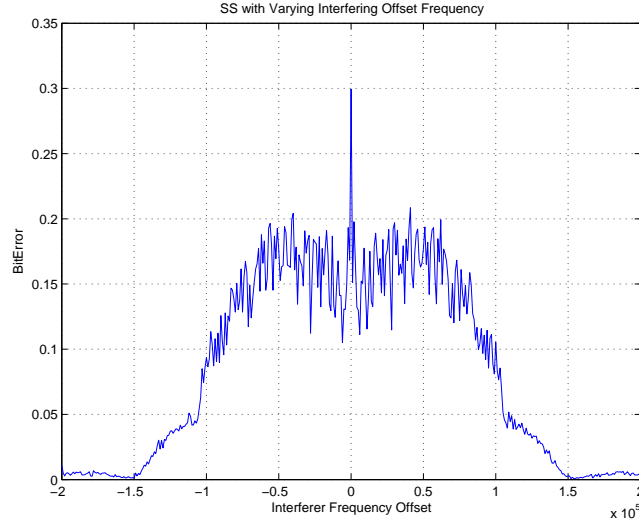
Figure 3.7: Original Spectral Subtraction Technique Results

signal are overlapping at all. The reason system performs well at large frequency shifts is due to the bandpass filter which is used before the signal is quantized. The reason the result is poor is because the estimate is largely incorrect. Since the subtraction only utilzes the PSD's of the signals, half of the information is completely ignored. This results in a completely inaccurate estimate. The problem with traditional Spectral Subtraction is that its results are subjectively evaluated or done, which isn't accurate enough in a digital communication system. Other evaluations uses such metrics as SNR, which can be quite deceptive esspecially in digital communications. Such examples can be seen here: [56], [9]

Since the initial simulations for traditional Spectral Subtraction proved inadiquated other optioned needed to be explored. First though, the problem needed to be an analyzed further for better understanding, then the appropriate solution could be formulated. Since the interfering signal and the wanted signal are non-orthoganal to one another they will share dimensional space, in this case the signals are inphase with one another. Therefore both planes real and imaginary must be considered. Non-orthoganal signal removal is a common task in communication system, which is done primarily by equalizers. Therefore an equalizer approach was considered next.

3.4.1 Equalizer Approach

The equalizer approach used in this Spectral Subtraction approach is a Least Means Square (LMS) equalizer, utilizing training data used in the front portion of each transmitted frame. This a common equalizer used in practice, allowing for future translation into a realized implementation. The LMS equalizer was also chosen for it robustness no noise, which is a weakness of such equalizers as the zero-forcing equalizer and requires no matrix inversion such as the Least Square (LS) equalizer. For proof of concept the entire datastream is used as training data, which provides the best results of any given channel for an adaptive equalizer, since the maximum knowledge is gained about the channel for each frame received. The results below show the BER as the signals pass over one another in frequency, similar to the previous evaluation using traditional Spectral Subtraction.
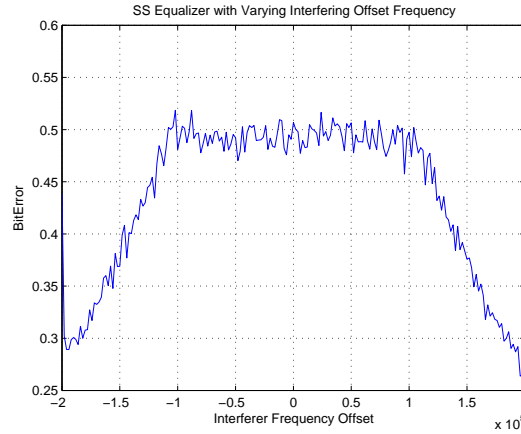

Figure 3.8: Spectral Subtraction Equalizer Test

As you can see the figure above, the equalizer approach doesn't provide any improve beyond the traditional Spectral Subtraction approach. The problem with using traditional adaptive equalizers is that they can only be used with a comparative slowly fading channel. Since knowledge learned from the training data can be applied at the earliest to the next frame, if the interference changes enough it can render the equalizer useless. This rapidly

changing spectrum or energy within the spectrum is unforunately a common characteristic of jammers. Even though this approach failed it provided an important observation and incite into the requirements and scenarios in which jammers can be overcome. For the sake of completeness an additional test was done with a small repeating sequence, smaller than the equalizer tap size, and as aspected the equalizer was able to overcome the interferer.

The important conclusion drawn from the previous experiment is that the when signals are orthogonal the receiver needs to be able to predict what data or energy is being transmismitted at a given time. Therefore the jammer problem must be constained future. As a result two jammer scenarios will be defined. The first scenarios is that the jammer's modulated data or energy is completely known to the receiver and the second is that the data sequence repeats with period being small. The larger the period the more resources the receiver will need to devote to its determination and evaluation. The sequence being completely known to the jammer is a reasonable assumption; primarily if the jammer is friendly, as discussed previously in this thesis, then that knowledge can be readily available.

Now that the jammer scenarios have been defined further they can be evaluated. The first will be when the data sequence of the jammer is completely known to the receiver. The approach here will be to synchronize with the interfering signal, so the interferer will simply be subtracted off. To synchronize the signals a mathematical tool called correlation will be used. Correlation is a common tool used in synchronization in communication systems when looking for known symbols in a stream of data. Equation 3.5 for cross-correlation simply passes signals over one another, the resulting sequence creates peaks where the data is most correlated.

$$R_{XY}(t_1, t_2) = E[X_{t_1} Y_{t_2}][26] \tag{3.5}$$

An example of two sequences being cross-correlated with one another can be seen below, with the peak being where the signal line up of share the most mutual information with one another. Therefore from this data the location of the start of the interfers data can

easily be located and removed. A simulation was created with this design in mind, with a unique result. Since the signals are frequency shifted over one another, when there frequencies match, it produces the best result, but as soon as they are offset, errors start to occur. This can easily be compensated for using a complex exponential multiplied by either the received or catalogued waveform. This will enduce a frequency shift cancelling out the shifting signal. Therefore the error is just a function of the noise itself.
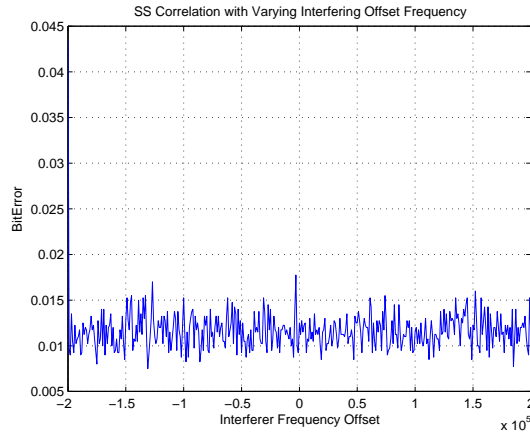

Figure 3.9: Spectral Subtraction Correlation method

This simulation was also repeated but this time was subtracted in the frequency domain. The result produced near identical results. Since using this approach requires two fourier transforms, into and out of the frequency domain, computationally it is much more involved and requires many more resources than the time domain approach. If the data was already the frequency domain from some other process or signal processing technique then the frequency subtraction would be a viable option.

Further analysis was done to provide a solid understand of the new requirements of the system and its limitations. The first is the precise understanding of the interfering signal itself. Since it is assumed that the signal modulation and data stream is known, attention can be shifted to the other issues that can occur, which are the non-idealities of the system. The first is the power constraint or effect. When subtracting the interferer specific power

must be measure of the interferer alone, so close to as little possible energy is subtracted from the joined signal that belongs to the desired signal. An examination of the incorrect estimation of the interfering signal was examined in 3.4.1.
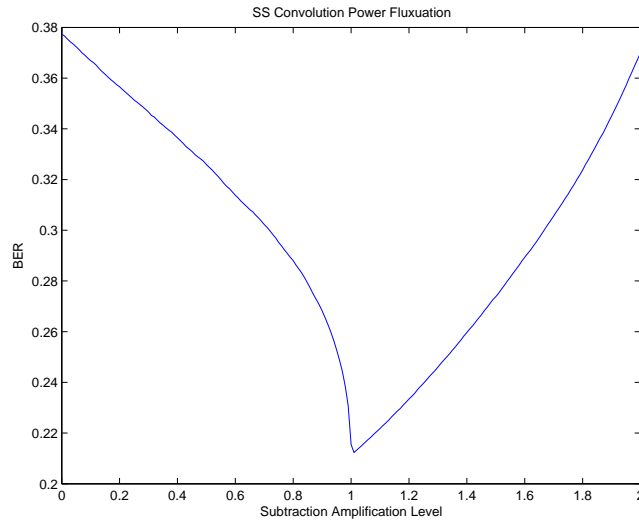

Figure 3.10: Spectral Subtraction Correlation Test with Varying Oversubtraction Level

Besides power, frequency and timing offsets were examined. These are especially concerning because the signal cannot be demodulated when in operation for feedback information, because it must be fed into the signal separation block for equalization. Therefore a timing recovery mechanism cannot downsample the signal either. The timing recovery and carrier recovery mechanism therefore needed to be unobtrusive as possible to the signal. As a result frequency and timing shifts were examined to understand the sensitivity of the subtraction, and how accurate the recovery mechanismed needed to be.

As you can see from figure 3.4.1, the subtraction mechanism is extremely sensitive to timing offsets, while frequency shifts the system is rather robust. If a full bitshift occures though, the entire system falls apart. This is a rather large problem and must be considered when attempting such operation on non-simulated data. This problem was forsean because of the time variance or sensitive of the signals themselves.

Moving on, now that a viable subtraction technique has been determined, the final
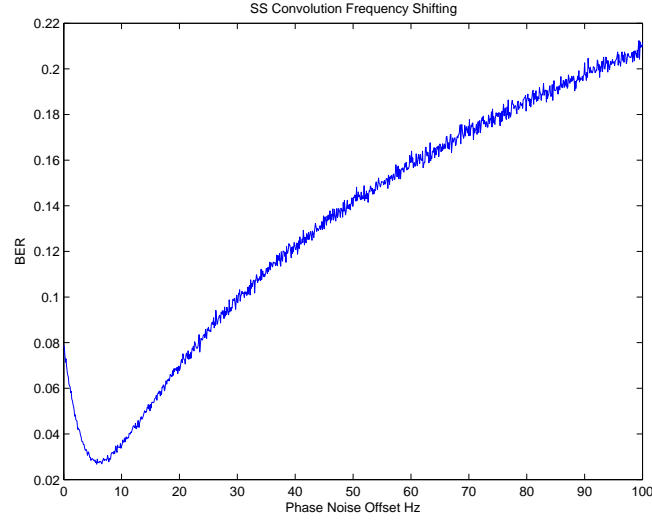
Figure 3.11: Spectral Subtraction with Phase Offsets of Interfering Signal

implementation for the Spectral Subtraction block can be realized. As discussed in the Hardware and Software Platform section of this thesis, GNU Radio was the first to be examined because of its realtime attributes. This was quite an involved process requiring many weeks of trial and error. The first implementation was entirely written in C++, which is the recommended language for signal processing blocks in GNU Radio.

Since C++ within GNU differs from many modern programming styles a code implementation or route was taken to ensure accuracy and speed up development. Therefore all coding was done with C++ itself, using no GNU Radio built-in libraries[47]. To allow for matrix operations the Aramdillo C++ Library[51] was imported and provided needed vector operations such as correlation and faster mathematical functions instead of having to rewrite common search operations. This library would also be needed for the Signal Separation block, therefore coding with Armadillo would provide the knowledge for future implementations needed in that block. From the standard C++ implementation results were compared with Matlab, and the code was ported into GNU Radio.

GNU Radio C++ are basically written by first creating test cases and writing your
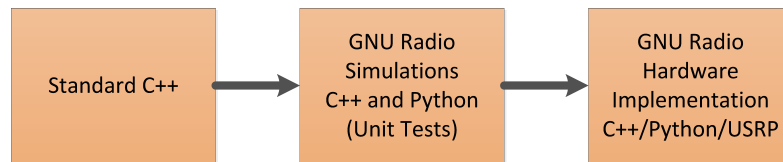
Figure 3.12: GNU-Radio Code Implementation Workflow

code until they are solved. This is a common practice among the programming community and provides a definitive endpoint to the code itself. The code was written and compiled successfully but unforunately the python wrapper called SWIG[10], which GNU Radio uses to interact with the C++ block through python, was unable to export the library. This is an undocumented problem within GNU Radio and was only identified through discussions directly with the GNU Radio core development team. Therefore another approach had to be considered.

The next option was to use python itself for signal processing. This is approach was primarily developed by Josh Blum, one of the core developer of GNU Radio. It isn't recommended due to speed issue, but it is quite easier to implement and debug for those familiar with python. As a result the previously C++ code was ported to python standards libraries and then to GNU Radio. The NumPy libraries were used within python. NumPy is the fundimental package for scientific computing in Python[31]. It like the armadillo library provides matrix operations such as correlation. Again under the Python standard libraries with NumPy the results were varified with MATLAB. Then the code was port to GNU Radio.

Again more problems occured, stonewalling all progress. The signal processing block was written as a subprocess using the queuing system built into GNU Radio. Queueing provides barriers between the connected blocks; therefore they can run freely, limiting bottlenecks. The system built would operate correctly for several hundred samples but would eventually segmentation fault. Several attempts to fix this error with even architectural changes to the code. Finally the lead developer of GNU Radio was consulted, Tom Rondeau [12], but he

was also unable to determine a solution. The assumed problem was a type casting occuring within the queue itself, that would eventually accumulate and cause a segmentation fault.

With these setbacks, it became necessary to look beyond GNU Radio and just utilize MATLAB for signal processing. Therefore the decision to load captured signals from GNU Radio and process them in MATLAB. It is nowhere near realtime, but it will process the data appropriately. The simple GNU Radio needs frontend is important because it allows tight synchronization between multiple receive antenna, which is a require of the original design of the system. The GNU Radio model can be seen in figure 3.4.1, the modulator block has been customized to remove the quantization, producing floating point results.
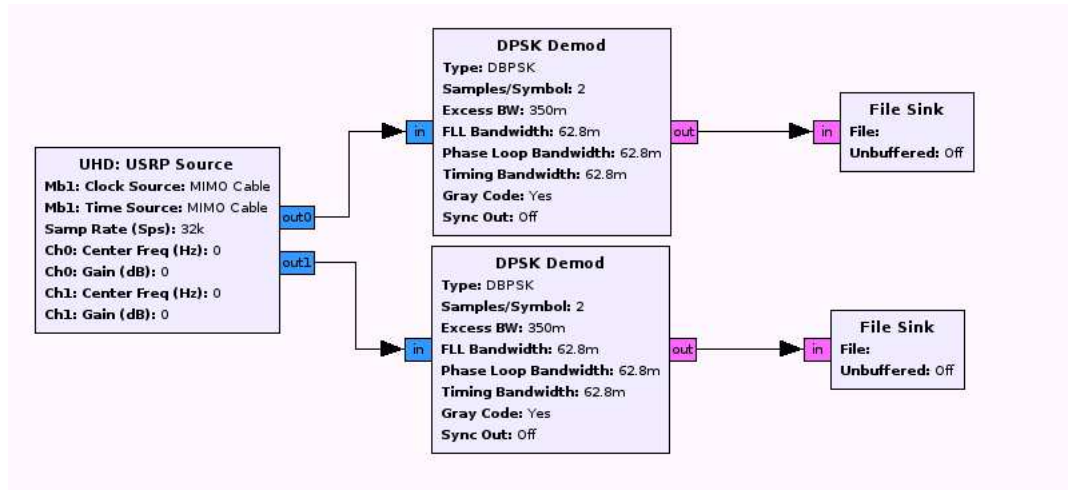

Figure 3.13: GNU-Radio Receiver Half Design

3.4.2 Non-deterministic Scenarios

For completeness it is important to discuss the scenarios when the interferer's modulated data is unknown but repetative with a small period. The approach to estimating short sequences is a rather obvious one, an autoregressive algorithm is used to predict samples. The simulation here, which was just used for proof of concept, uses a linear predictive filter. The filter determines coefficients of a forward linear predictor by minimizing the prediction

error in the least squares sense[28]. It finds the coefficients of a pth-order linear predictor (FIR filter) that predicts the current value of the real-valued time series x based on past samples.

$$\hat{x}[n] = -a(2)x(n-1) - a(3)x(n-2) - ... - a(p+1)x(n-p)$$

For the linear predictive filter to operate efficently the number of filter taps must be equal to or greater than the period of the repeated sequence. If the number of taps is smaller it cannot capture the randomness the in the interferer's data.

3.4.3   Over the Air Implementation Considerations

When moving towards a real implementation of the Spectral Subtraction block, the non-idealities introduced by the enviroment needed to be considered. These include frequency and phase shifts, as well as timing offsets. Certain considerations needed to be made as well, since instanteous changes occur when signals overlap. Therefore a more advanced control scheme needed to be constructed around the common signal compensation or correction. The basic idea used here is a receiver within a receiver, one for each signal received. This will be discussed in detail.

The system assumes that the jammer is always present within the enviroment therefore it was concluded that the jamming signal should be synchronized with first, be removed and then all that remains should be the wanted signal. There is were the receiver within a receiver design comes in, since first the interferer will be synchronized to, utilizing phase and frequency recovery and then timing recovery. Unforunately such an implementation isn't as straight forward as expected. Since when both signal are present in the spectrum it is impossible for these algorithm to operate correctly. This is due the fact that they cannot separate one signal from the other. For example, phase information cannot be accurately calcuated in the presence of two signals. Therefore modifications need to made, which is where a controlling mechanism comes into play.

When multiple signals are in the envirorment the compensation algorithm learn incorrectly; as a result, a decision was made to pause these algorithms when both signals were present and continue when the signal interferer was only present. This operation relys on two assumptions, the first is that both signals are present for short periods of time which can be controlled. The second is that the calculated offsets of cause by the envirorment don't rapidly vary during the periods of time for which the two signals are visible. This assumption is quite reasonable especially with relatively non-mobile transceivers, which was assumed in the original documentation.

To accomplish this algorithm holding mechanism, energy detection was chosen to be uses for its simplicity. Below you can see an image of the jammer signal by itself and the combined signals. A large increase in energy or step can be seen, which can easily numerically detected. Energy is calculated using the following equation: $E_s = |x(t)|^2 dt$. This was implemented with a moving average filter with a small window to reduce sperious changes due to signals gaps or outliers. In practice the average peak energy level of the interferer is first calculated, then when the power in the spectrum increases to a level roughly 1.5x of the original level, the compensation algorithms are halted. A simple technqiue technique, which is commonly uses but in the inverse fashion. An example of the combined and signals can be seen in figure 3.4.3. The final results of the Spectral Subtraction block are examined in the next chapter.

3.5 Superimposed Equalizer

Moving on, the next block to discuss is the signal separation block. The development of this block is very staggered and due to time requirements shortcuts needed to be made. The original desired result was to use a blind source separation technique outlined here [37], which is able to separate multiple signals from one another under specific constraints. For this process to work efficently an appropriate channel model needs to be created. Since the
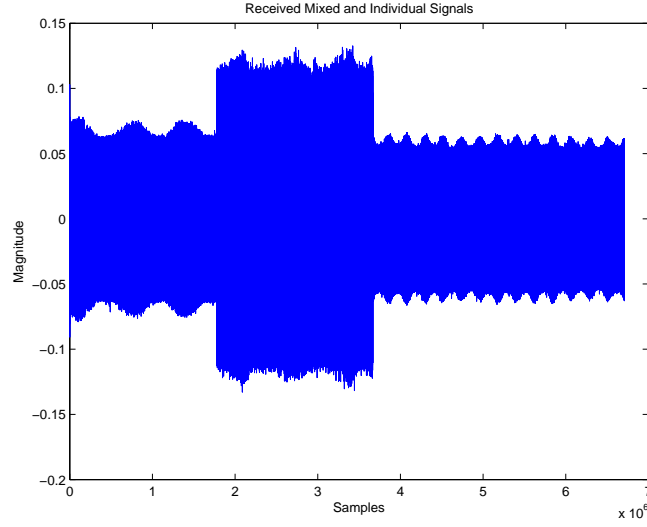
Figure 3.14: Received mixed and individual signals

goal of this system is to be very robust an estimator for very frequency selective channel is desired. The progession of the signal separation block will be examined in this sections and the limitations will be discussed. It is important to note that a large variation was taken in the system design due to implementation feasibility.

The original objective was the utilize a new signal separation technique called AMUSE, but a new avenue was taken with a more theoretical channel estimation problem in mind. This estimation evaluation will be discussed first. The first objective for channel estimation is to examine the channel mixing model which assumes a single-input multiple-antenna broadcast channel. A J-channel FIR system excited by K transmit antennas is considered. A quasi time-invariant multipath channel is assumed which remains constant during the transmission of a set of consecutive symbols, which are called slots. These slots are assumed independent from one another. The channel estimation is performed over each slot. Each symbol inside a slot is assumed to be the result of a known redundant precoder acting on an input transmit symbol vector drawn from an M-PSK constellation. Therefore the receiver receives signals not only from the intended transmitter but also from Q other interferers. The interferers are assumed to employ the same redundant precoder as the desired

signal[44].

With this model, [58] shows that no assumptions are necessary regarding the number of the transmit antennas of each of the interferers and the channel orders as long as they are smaller than the block size. The block size in this case is equal to the combination of the individual channel lengths and the number of transmit antenna used by the desired transmitter. But this evaluation rely on three assumptions:

1. The data sequence x_d is an i.i.d. sequence such that $x_d \sim \mathcal{CN}(0, \sigma_d^2)$

2. The distribution over the MIMO channel vector is $p(y; \theta)\ \mathcal{CN}(\mu_y, R_w)$, and the interference vector is distrbuted normal with covariance R_w

3. The transmitted symbols, the channel vector, and the interference vector are jointly independent

With these assumptions the mixing process can be undone but the channel estimation needs to be calculated first. Since this is a MIMO channel, frequency selective fading will need to be captured to providing appropriate channel knowledge. To accomplish this, the original research decided to utlize superimposed equalization, whose operation was heavily discussed in the background section of this thesis. In summary, [24] uses a superimposed symbol transmission scheme to estimate frequency-selective channels. Several points of the DFT of the data are set to known values. This operation can be easily implemented in the time domain when these DFT points are equispaced. The channel is estimated using the DFT of the received signal at these selected DFT points. The detection itself is done using an iterative method across these points. Unlike traditional equalizers, the proposed method does not require bandwidth for training. It instead trades spectral power for those symbols themselves, spreading its energy over the entire bandwidth capturing the entire spectrum space. [24] also proves that by placing the training symbols in quasi-periodic position they will not interfer with the data itself. It is important to note that this research discusses no sychronization mechanism, and now with the training data spread throughout the signal is very complex. This addition complexity was factored into the design decisions of the

implementation, which is discussed later in this section.

With our channel estimation method chosen, a simulation was created to prove the effectiveness of such a scheme. The result of this implementation were directly compared with the results of the paper to prove correctness.The results of this simulation are seen in figure 3.5. It examines a random frequency selective channel, with very high suppression with a across a number of SNR values. As expected there is a linear relationship between SNR and Error.
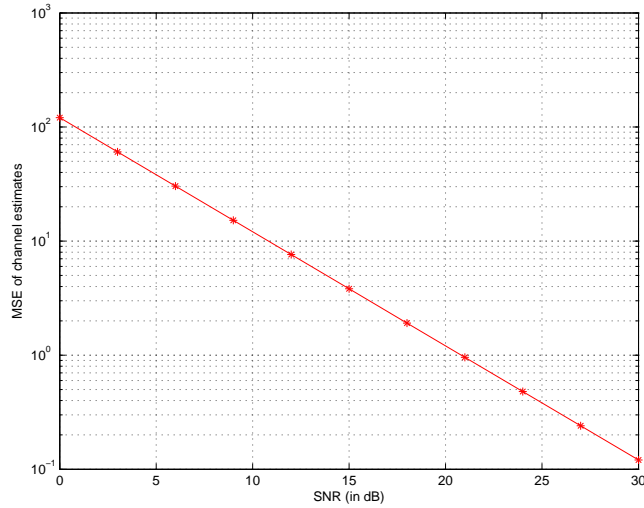

Figure 3.15: Superimposed Equalizer SNR Performance

From figure 3.5 you can see in a frequency selective fading channel is very well estimated by the superimposed equalizer. This was exactly the result that was desired, but symbol recovery after equalization still needed to be examined. This unfortunately is the drawback of this formulation. The first is the condition if the mixing matrix H is rank deficient, the channel become inestimiable, since there become an infinite amount of solutions to the actual unmixing process. The second is the equalizer, which is numerically intensive, and the alternative has limiting conditions [24]. This conclusion, which isn't discussed in [24], is when the equalized signal is very suppressed due to the incomplete channel estimate. The
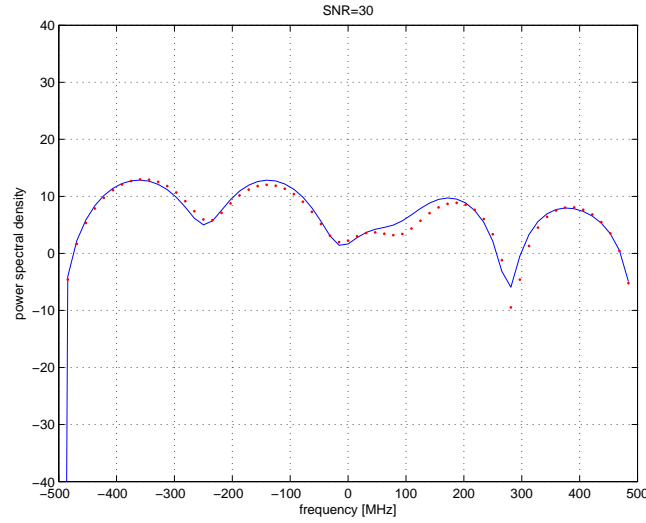
Figure 3.16: Superimposed Equalizer Channel Estimation Performance with High SNR

quantization feedback method overcome the previously received frame and dominated all future frames, essentually neglecting any information they have. Again this only in very suppresive channels. With these results the superimposed equalizer started to become less desirable due to it's complexity, but evaluations continued due to the amount of time invested into the topic already.

These simulations provide the necessary foundation to push towards the final implementation of the signal separation block. However, due to time constraints certain decisions needed to be made about this block and the feasibility of its operation. With that in mind the primary goal for the signal separation block was to provide signal separation or maximization from several received signals. Since the previous research provided substantial implemenation considerations and issue, a new direction needed to be considered. Therefore instead of the proposed AMUSE[37] technique, another MIMO cross-channel technique called Maxmimal Ratio Combining (MRC) was chosen as a viable alternative. This decision was made with both project managers.

Maximal Ratio Combining is a method of diversity combining in which the signal add

first weighted and then added together. These weights or gains are made proportional to the RMS signal level and are inversely proportional to the mean square noise level in that channel, and the same proportionality constant is used for all channels[22]. Therefore the channel with the best SNR provides the greatest impact on the resulting sequence. This process needs to explain more throughly. Assuming the received signal is an array of samples received the individual antennas $\boldsymbol{x}(t) = \boldsymbol{h}(t)u(t) + \boldsymbol{n}(t)$ and the individual channels $\boldsymbol{h} = [h_0, h_1, ..., h_{N-1}]^T$, and the additive noise $\boldsymbol{n} = [n_0, n_1, ..., n_{N-1}^T$. The equalized symbol $\hat{x} = x + (h^H n)/(h^H h)$ [7].

A simple evaluation of MRC was done to prove its capabilities, which is based on the simulations here [45].
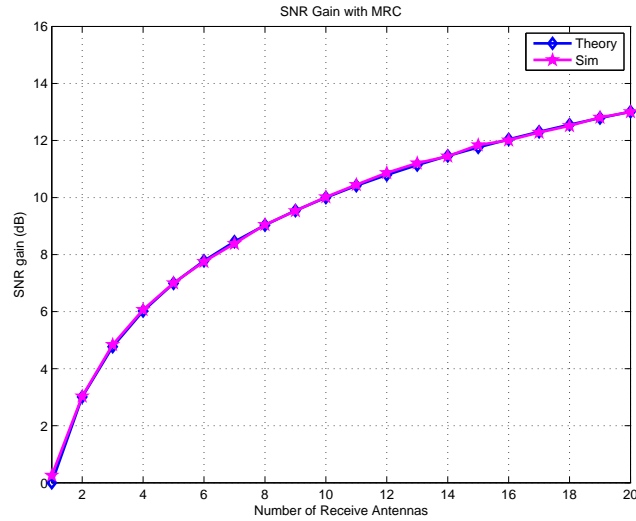

Figure 3.17: Maximal Ratio Combining gain acrossing varying number of antennas

As you can see as you increase the number of antennas in a frequency selective channel the better the result. Therefore MRC was introduce into the framework of the signal separation block, and the new model for this block can be seen in figure 3.5. This block first utlizes adaptive equalizers on the channels individually then uses MRC to combine there results maximizing the SNR of the desired signal. MRC was combined with the channel estimate approach using adaptive equalizers due to there known feasibility. From the knowledge learned in the previous with the implementation involving GNU Radio, the sig-

nal separation block was created entirely in MATLAB. The results of this operation will be discussed in the final chapter of the thesis.
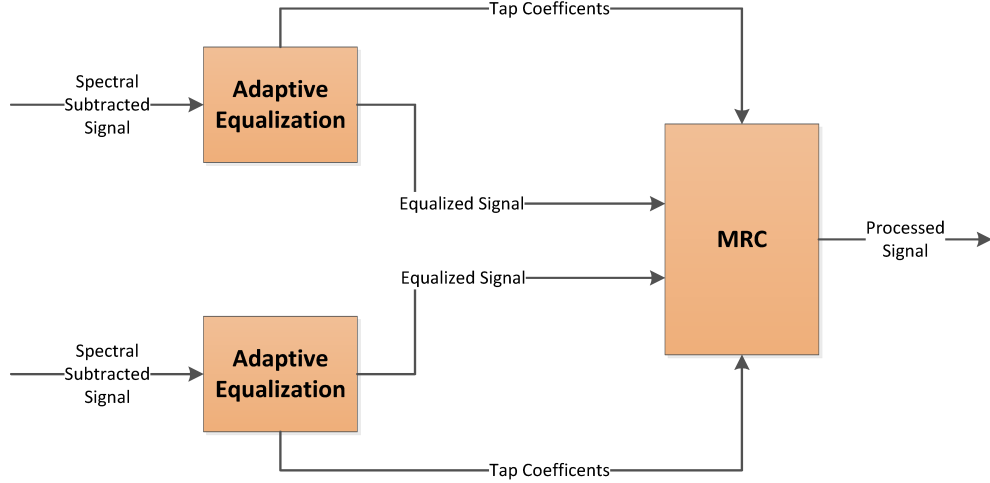

Figure 3.18: Maxmimal Ratio Combining Block design to replace original Super Imposed Equalizer design

3.6   Antenna Subset Selection

The Antenna Subset Selection (AntSS) block was fully contracted out to external contractors but unfortunately was never fully completed. It is important to understand the purpose of this block for future research, and how it should iteract with the other blocks of the system. The AntSS system itself consists of a series of AntSS boards that provides $2^M - to - 2^N$ downselection from an array of receive antennas to a set of BLISS receiver inputs. Each individual AntSS board provides 4-to-2 antenna downselection via a set of RF switches. A basic block diagram of an individual AntSS board is given in Figure 3.6. Each AntSS board has four receive paths. Each path consists of a bandpass filter and low-noise amplifier. The output of each receive path is connected to a switch matrix composed of a series of Single-Pole-Double-Throw (SPDT) RF Switches. The switch matrix is configured so that all possible permutations of the 4-to-2 downselection are possible. The switch matrix is controlled by software running on a simple PIC processor. The PIC interfaces with

the BLISS hardware platform via an RS-232 link that is connected from the BLISS receiver to all AntSS boards.
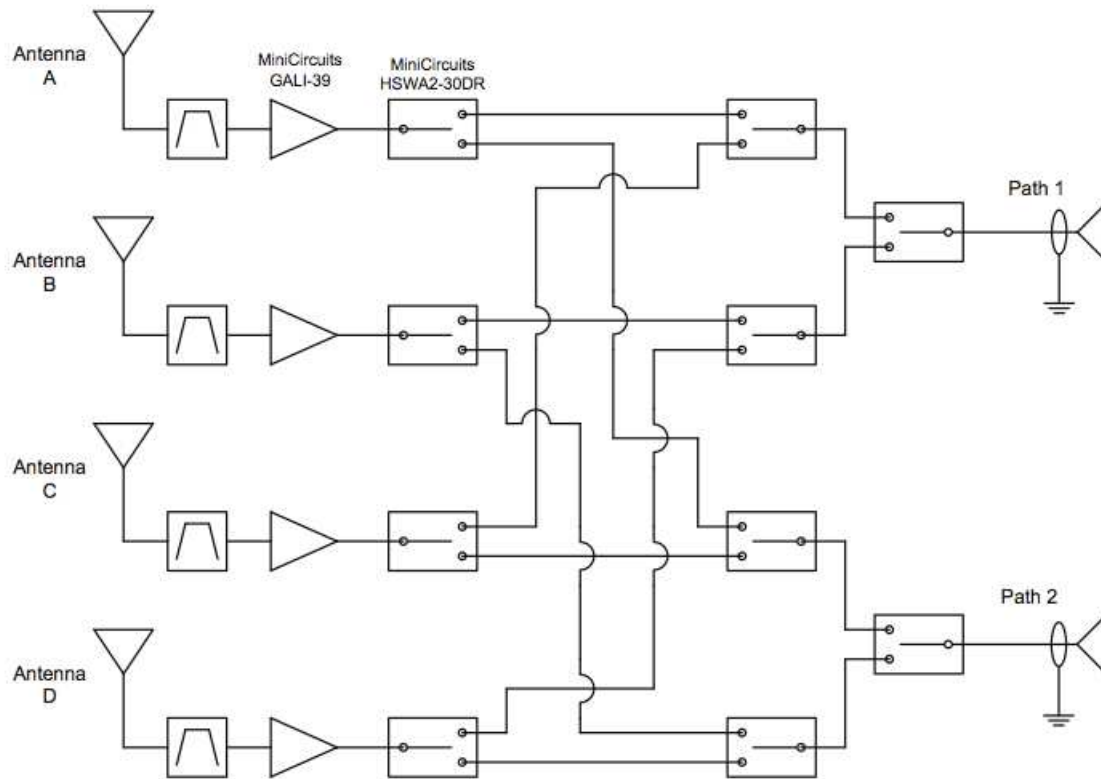

Figure 3.19: Antenna Subset Selection block outline

During operation, training information which was used also by the signal separation block is also used by AntSS. It uses this data to provide SNR values at each Antenna of the desired signal. Once all antennas have been evaluated the system then selects a subset of the best antennas, which is defined by the highest SNR levels. The signals from these antennas are then fed into the remain BLISS blocks. AntSS can have 2^M antennas, but will always deliever two signals. The antennas need to be space at least a single wavelength appart or they will not be considered independent of one another, reducing the effectiveness of AntSS. The physical boards have been built, which can be seen in figure 3.6 and their frequency response on the individual channels can be seen in Appendix ??.
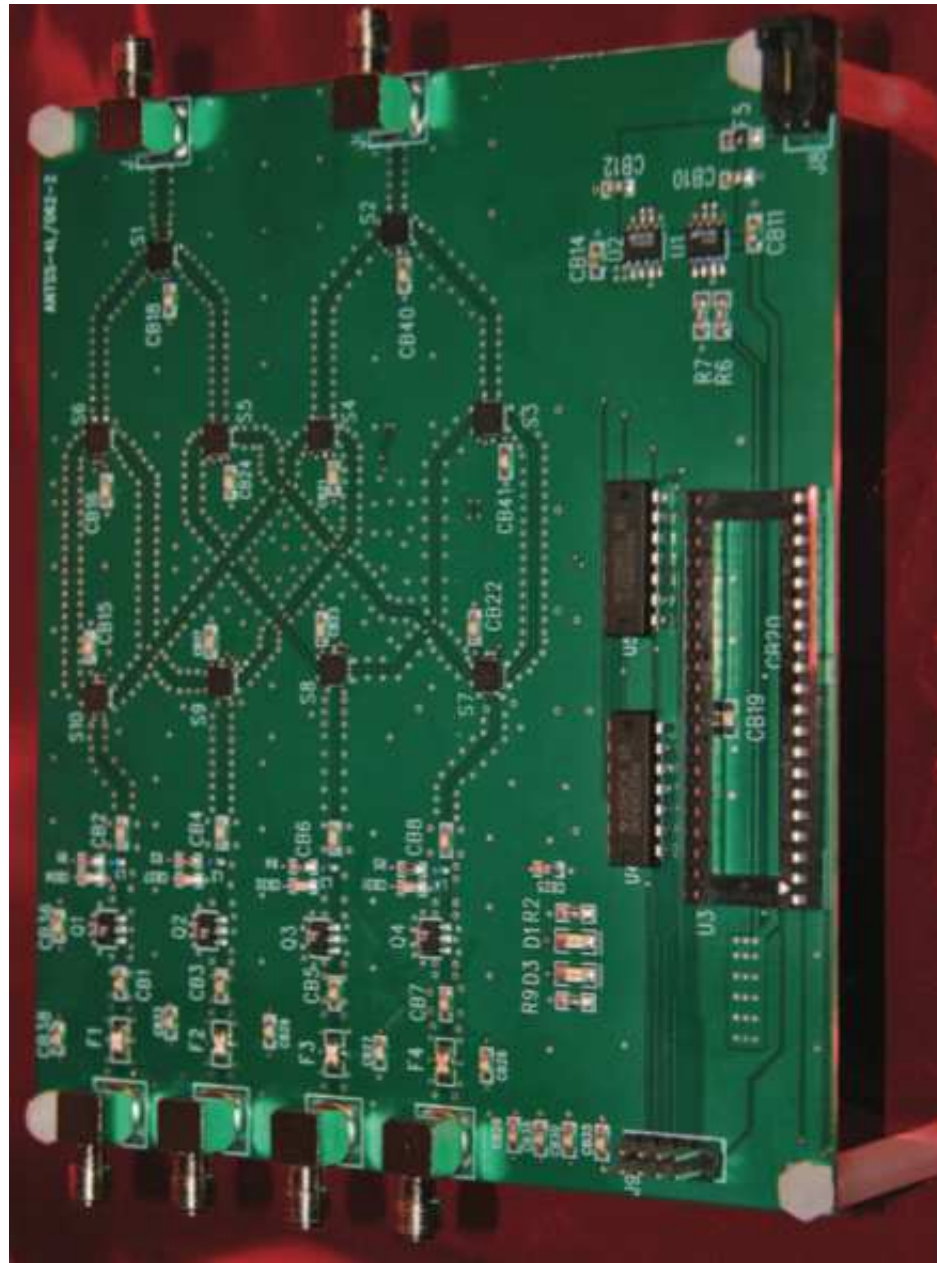
Figure 3.20: Single Antenna Subset Selection physcial board

Unfortunately none of the control mechanisms in software have been created, therefore AntSS couldn't be fully tested and effectiveness deteremined. This will be a reasonable avenue for future work.

3.7   Summary

This chapter discussed the implementation fallbacks and successes of the BLISS system. The entire BLISS system was outlined and structinized for feasilbility and operational performance. Spectral Subtraction and Signal Separation were transitioned from original research goals to more managable problems, with simplified solutions. Overall it can be said that optimality and technical complexity were sacrificed in the end for realiseability. Many directions needed to be changed, especially in the Signal Separation block, and constraints needed to be tightened on the Spectral Subtraction block. Although AntSS couldn't be realized a solid foundation exists for future work.

Bibliography

[1] March 2013.

[2] March 2013.

[3] March 2013.

[4] Mithun Acharya and David Thuente, *Intelligent jamming attacks, counterattacks and (counter)2 attacks in 802.11b wireless networks*, Proceedings of the OPNETWORK Conference, 2005.

[5] S. Adireddy, Lang Tong, and H. Viswanathan, *Optimal placement of training for frequency-selective block-fading channels*, Information Theory, IEEE Transactions on **48** (2002), no. 8, 2338 – 2353.

[6] Srihari Adireddy and Lang Tong, *Optimal placement of known symbols for nonergodic broadcast channels*, IEEE Trans. Info. Theory **2192** (2002), http://www.ece.corne.

[7] Raviraj Adve, *Receive diversity*.

[8] Faraz Ahsan, Ali Zahir, Sajjad Mohsin, and Khalid Hussain, *Survey on survival approaches in wireless network against jamming attack*, Journal of Theoretical and Applied Information Technology **30** (2011), no. 1, 55–67.

[9] B. BabaAli, H. Sameti, and M. Safayani, *Spectral subtraction in model distance maximizing framework for robust speech recognition*, Signal Processing, 2008. ICSP 2008. 9th International Conference on, Oct., pp. 627–630.

[10] Dave Beazley, *Swig (simplified wrapper and interface generator)*, 1996–.

[11] M. Berouti, R. Schwartz, and J. Makhoul, *Enhancement of speech corrupted by acoustic noise*, Acoustics, Speech, and Signal Processing, IEEE International Conference on ICASSP '79., vol. 4, apr 1979, pp. 208 – 211.

[12] Eric Blossom, *[discuss-gnuradio] s/eric/tom/g*, TheMailArchive, September 2010.

[13] Steven F. Boll, *A spectral subtraction algorithm for suppression of acoustic noise in speech*, Acoustics, Speech, and Signal Processing, IEEE International Conference on ICASSP '79 **4** (1979), 200–203.

[14] V. Bose, M. Ismert, M. Welborn, and J. Guttag, *Virtual radios*, Special Issue on Software Radios (1999).

[15] Jr. C. Richard Johnson, William A. Sethares, and Andrew G. Klein, *Software receiver design: uild your own digital communications system in five easy steps*, Cambridge University Press, 2011.

[16] Kwang-Cheng Chen and Ramjee Prasad, *Cognitive radio networks*, John Wiley and Sons, 2009.

[17] R.C. DiPietro, *An fft based technique for suppressing narrow-band interference in pn spread spectrum communications systems*, Acoustics, Speech, and Signal Processing, 1989. ICASSP-89., 1989 International Conference on, may 1989, pp. 1360 –1363 vol.2.

[18] Electus Distribution, *Solving tv reception problems*, 2002.

[19] F.W. Ellersick, D.L. Schilling, IEEE Communications Society, Institute of Electrical, Electronics Engineers, and IEEE Xplore (Online service), *Special issue on progress in military communications*, IEEE journal on selected areas in communications : a publication of the IEEE Communications Society, IEEE, 1985.

[20] Ettus Research, *Uhd documentation*.

[21] B. Farhang-Boroujeny, *Experimental study of semi-blind channel identification/equalization through pilot signals*, Signal Processing, 1996., 3rd International Conference on, vol. 1, oct 1996, pp. 618 –621 vol.1.

[22] Institute for Telecommunication Sciences, *Federal standard 1037c*.

[23] Michael R. Frater and Michael Ryan, *Electronic warfare for the digitized battlefield*, Artech Print on Demand, 2001.

[24] M. Ghogho, D. McLernon, E. Alameda-Hernandez, and A. Swami, *Channel estimation and symbol detection for block transmission using data-dependent superimposed training*, Signal Processing Letters, IEEE **12** (2005), no. 3, 226 – 229.

[25] Wang Guang-Yan, Zhao Xiao-Qun, and Wang Xia, *Musical noise reduction based on spectral subtraction combined with wiener filtering for speech communication*, Wireless Mobile and Computing (CCWMC 2009), IET International Communication Conference on, Dec., pp. 726–729.

[26] John A. Gubner, *Probability and random processes for electrical engineers*, Cambridge University Press, 2010.

[27] A. Haimovich and A. Vadhri, *Rejection of narrow-band interferences in pn spread spectrum systems using an eigenanalysis approach*, Military Communications Conference, 1994. MILCOM '94. Conference Record, 1994 IEEE, oct 1994, pp. 1002 –1006 vol.3.

[28] Simon Haykin, *Adaptive filter theory*, 4 ed., Prentice Hall, 2002.

[29] Mathworks Inc., 2013.

[30] ――――, January 2013.

[31] Eric Jones, Travis Oliphant, Pearu Peterson, et al., *SciPy: Open source scientific tools for Python*, 2001–.

[32] W.W. Jones and K.R. Jones, *Narrowband interference suppression using filter-bank analysis/synthesis techniques*, Military Communications Conference, 1992. MILCOM '92, Conference Record. Communications - Fusing Command, Control and Intelligence., IEEE, oct 1992, pp. 898 –902 vol.3.

[33] Anil Kandangath, *Jamming mitigation techniques for spread spectrum communication systems*, Tech. report, University of Arizona, 2003.

[34] Wooil Kim, Sunmee Kang, and Hanseok Ko, *Spectral subtraction based on phonetic dependency and masking effects*, Vision, Image and Signal Processing, IEE Proceedings - **147** (Oct), no. 5, 423–427.

[35] E. Koski and C. Linn, *The jtrs program: software-defined radios as a software product line*, Software Product Line Conference, 2006 10th International, 0-0 2006, pp. 10 pp. –191.

[36] R.I. Lackey and D.W. Upmal, *Speakeasy: the military software radio*, Communications Magazine, IEEE **33** (1995), no. 5, 56 –61.

[37] Rui Li and Fasong Wang, *Adaptive semiblind signal separation approach using temporal structure of sources*, Anti-counterfeiting, Security, Identification, 2007 IEEE International Workshop on, April, pp. 315–318.

[38] Karthikeyan Mahadevan, Sojeong Hong, and John Dullum, *Anti-jamming: A study*, December 2005.

[39] III Mitola, J., *Software radios: Survey, critical evaluation and future directions*, Aerospace and Electronic Systems Magazine, IEEE **8** (1993), no. 4, 25 –36.

[40] J. Mitola, *The software radio architecture*, IEEE Communications Magazine (1995), 26–38.

[41] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou, *A survey on jamming attacks and countermeasures in wsns*, IEEE Communications Surveys and Tutorials **11** (2009), no. 4, 42–56.

[42] Quinn Norton, *Gnu radio opens an unseen world*.

[43] A.G. Orozco-Lugo, M.M. Lara, and D.C. McLernon, *Channel estimation using implicit training*, Signal Processing, IEEE Transactions on **52** (2004), no. 1, 240 – 254.

[44] Srikanth Pagadarai, *Wireless communications and spectrum characterization in impaired channel environments*, Ph.D. thesis, Worcester Polytechnic Institute, 2012.

[45] Krishna Sankar Madhavan Pillai, *Maximal ratio combining effective snr*, apr 2009.

[46] Kathy Pretz, August 2012.

[47] The GNU Radio Project, *Gnu radio 3.6.4 c++ api documentation*.

[48] Kristopher W. Reese and Ahmed Salem, *A survey on jamming avoidance in ad-hoc sensory networks*, J. Comput. Sci. Coll. **24** (2009), no. 3, 93–98.

[49] Ettus Research, *Usrp2 the next generation of software radio systems*, 1043 North Shoreline Blvd, September 2010.

[50] ———, *Usrp n200/210 networked series*, 1043 North Shoreline Blvd, September 2012.

[51] Conrad Sanderson, *Armadillo: An open source c++ linear algebra library for fast prototyping and computationally intensive experiments*, Tech. report, NICTA, 2010.

[52] Jingpu Shi, Theodoros Salonidis, and Edward W. Knightly, *Starvation mitigation through multi-channel coordination in csma multi-hop wireless networks*, in CSMA Multi-hop Wireless Networks," in Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2006, pp. 214–225.

[53] IEEE Computer Society, *Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications*, Tech. report, IEEE, 2012.

[54] Regory Staple and Kevin Werbach, march 2004.

[55] Christopher H. Sterling, *Military communications: From ancient times to the 21st century*, ABC-CLIO, 2007.

[56] R.M. Udrea and S. Ciochina, *Speech enhancement using spectral over-subtraction and residual noise reduction*, Signals, Circuits and Systems, 2003. SCS 2003. International Symposium on, vol. 1, 0-0, pp. 165–168 vol.1.

[57] N. Upadhyay and A. Karmakar, *A perceptually motivated multi-band spectral subtraction algorithm for enhancement of degraded speech*, Computer and Communication Technology (ICCCT), 2012 Third International Conference on, Nov., pp. 340–345.

[58] Alexander Wyglinski, Christopher Anderson, and Srikanth Pagadarai, *Semi-blind estimation of correlated mimo channels using optimal training design in multiuser environments*, Tech. report, Office of Naval Research, 2011.

[59] Liang Zhao, M.G. Amin, and A.R. Lindsey, *Subspace projection techniques for anti-fm jamming gps receivers*, Statistical Signal and Array Processing, 2000. Proceedings of the Tenth IEEE Workshop on, 2000, pp. 529 –533.

[60] G.T. Zhou, M. Viberg, and T. McKelvey, *A first-order statistical method for channel estimation*, Signal Processing Letters, IEEE **10** (2003), no. 3, 57 –60.

[61] H. Zimmermann, *Osi reference model–the iso model of architecture for open systems interconnection*, Communications, IEEE Transactions on **28** (1980), no. 4, 425 – 432.