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

List of Figures **v**

List of Tables **vi**

1 Introduction **1**
1.1 Motivation . . . 2
1.2 State of the Art . . . 3
1.3 Thesis Contributions . . . 7
1.4 Thesis Organization . . . 7

2 Background **8**
2.1 Jamming . . . 8
2.2 Anti-Jamming . . . 9
2.3 Communication Systems . . . 12
2.3.1 Equalization . . . 15
2.3.2 Superimposed Training Equalization . . . 18
2.4 Spectral Subtraction . . . 22
2.4.1 Residual Noise . . . 23
2.5 Software Defined Radio . . . 24
2.5.1 GNU Radio . . . 25
2.5.2 MATLAB . . . 26
2.5.3 Comparision . . . 27
2.5.4 Summary . . . 27

Bibliography **29**

List of Figures

1.1 Open Systems Interconnection Model 3

2.1 DBPSK signal uncorrupted by jammer 10
2.2 DBPSK signal corrupted by jammer 10
2.3 Basic Transmitter Outline 13
2.4 Basic Receiver Outline 14
2.5 FIR Filter Structure 16
2.6 Good timing recovery produces open eye 19
2.7 Poor timing recovery produces closed eye 19
2.8 GNU Radio Code Structure 26

List of Tables

2.1 Comparision of Anti-Jamming Techniques 10

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[30]. 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[14]. 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 envirorments 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:**
- **Resilient:**
- **Hardened:** in changing enviroments

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[39]. 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.

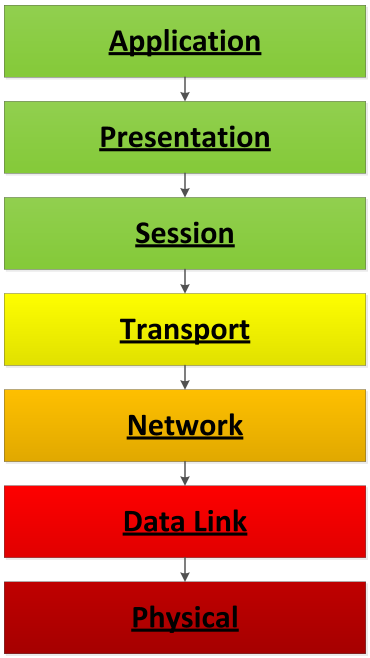

Figure 1.1: Open Systems Interconnection Model

Current anti-jamming technics include channel hopping, spatial retreat, jammed area mapping, node escape, retreat restoration, frame masking, and many more[28]. 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 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[28]. 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[9]. 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[9]. 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[9].

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[4]. 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[1]. 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[32].

There also exists systems that are design to resist jamming proactively. These hybrid systems[31] 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[35]. 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[25].

The largest problem with these techniques is they all have are designed to combat narrowband 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. Un-

fortunately 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[27], provide a platform flexible enough to support highly intelligence operations such that anti-jamming requires. A proposed adaptive signal processing 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 basis for blind source separation of define subset of signals, and tools on estimating and removing those signals.
- 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 probability of operational.

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[12]. Bell stated that such a wireless system can be easily disrupted with simple electromagnetic distrubances, "Its as easy as cutting the wires".[12] 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[33]. Deliberate jamming on the otherhand, is generally more saphisticated and takes many different forms.

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

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[35]. These method obviously (or subtly) disrupt transmissions by inserting electron-magnetic 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

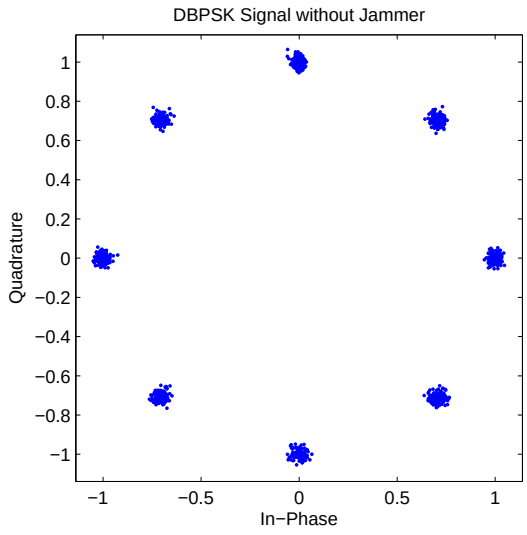

Figure 2.1: DBPSK signal uncorrupted by jammer

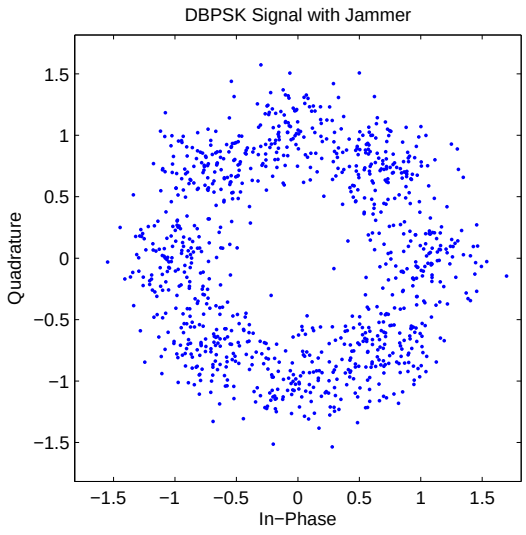

Figure 2.2: DBPSK signal corrupted by jammer

subspace processing. By combining several of the listed techniques, wideband jammers can 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[17]. 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. [10] 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[20]. 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[37].

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 approach 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[21]. 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.

Figure 2.3: Basic Transmitter Outline

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.

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[8].

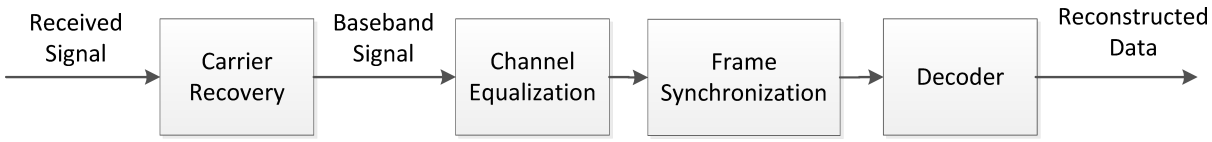

Figure 2.4: Basic Receiver Outline

$$cos(x)cos(y) = 1/2(cos(x+y) + cosine(x-y)) \tag{2.2}$$

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[8].

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

$$\hat{\boldsymbol{X}} = Y * F$$

. Figure 2.3.1 outlines a typical FIR structure for which the equalizer will create the appro-

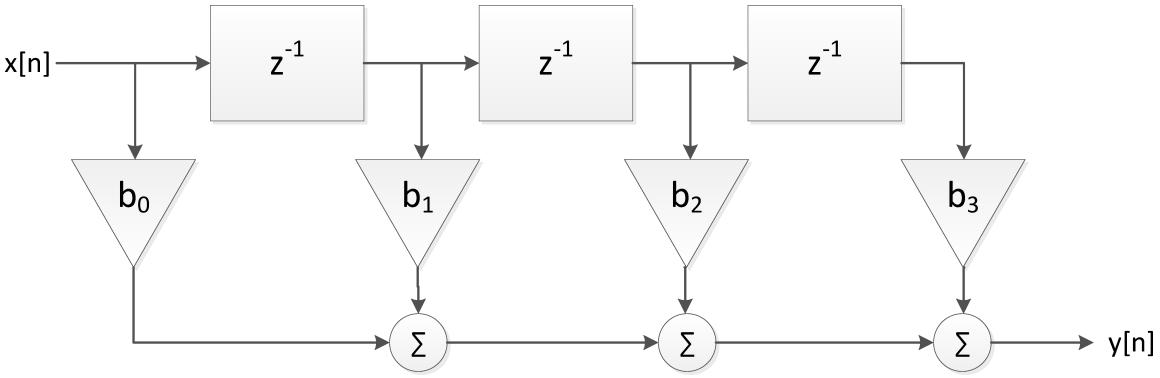

Figure 2.5: FIR Filter Structure

priate 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.

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 show be the equation below.

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

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 Squaed Error Filter (LMMSE) takes this relaxation into account.

The LMMSE assumes that the symbols are uncorrelated with one another and uncorre-

lated from the noise in the channel. This approach tries to minimize the mean square error, a common measure of estimator qualities. 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 $\|x - \hat{x}\|^2$.

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 are outlined here:

$$y[n] = w[n]^H F[n]e[n] = A_n - y[n]w[n+1] = w[n] + \mu[n]F[n] \tag{2.4}$$

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.

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 2.5.

$$e = \frac{1}{2} \exp\left(sign(y[k] - y[k]\right)^2 \tag{2.5}$$

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.

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

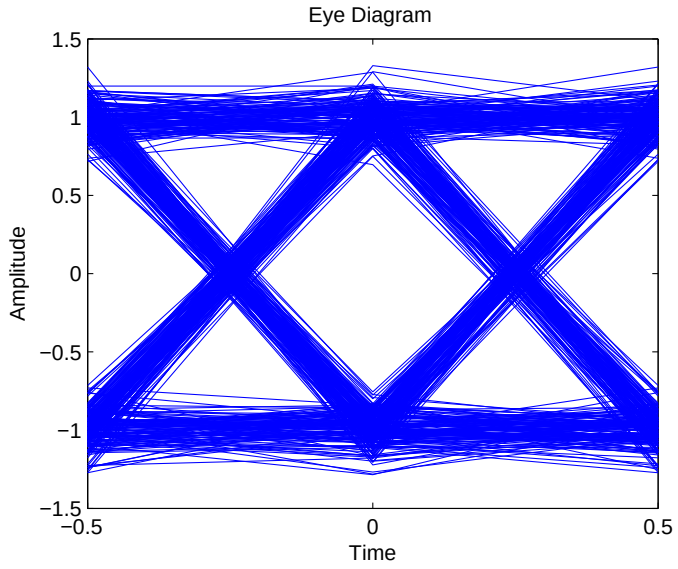

Figure 2.6: Good timing recovery produces open eye

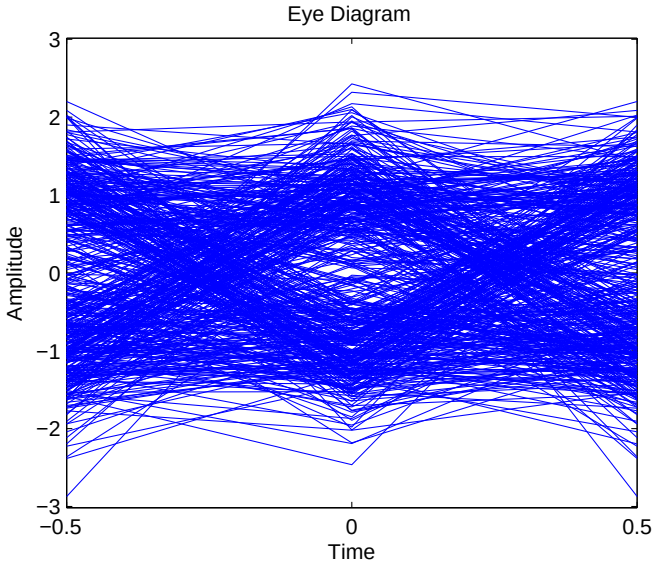

Figure 2.7: Poor timing recovery produces closed eye

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,[2] 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[2]. To accomidate such pilots, energy must be shared among the data and hidden pilots[15]. [13] 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 $10 log K_{loss} dB$ in signal to noise ratio (SNR). Other disadvantages include an increased signal envelope fluctuation that can be undesireable in nonlinear transmit power amplifiers[38].

At the receiver, channel estimation can be done using several techniques in both the frequency and time domain. [38] 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. [38] and [29] 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[11].

Superimposed equalizers are able to better compensate for large multipath channels be-

cause 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 [3]. [2] 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.[15] 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 $\mathbf{e} = \mathbf{J}\mathbf{w}$. 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: $s = (I-J)w+c$.

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 transmittion 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[6]. 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 [22], [36], [16], 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[5].

Therefore [6] 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. [6] 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[26]. 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[34]. 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[24]. 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[24]. 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[23]. 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

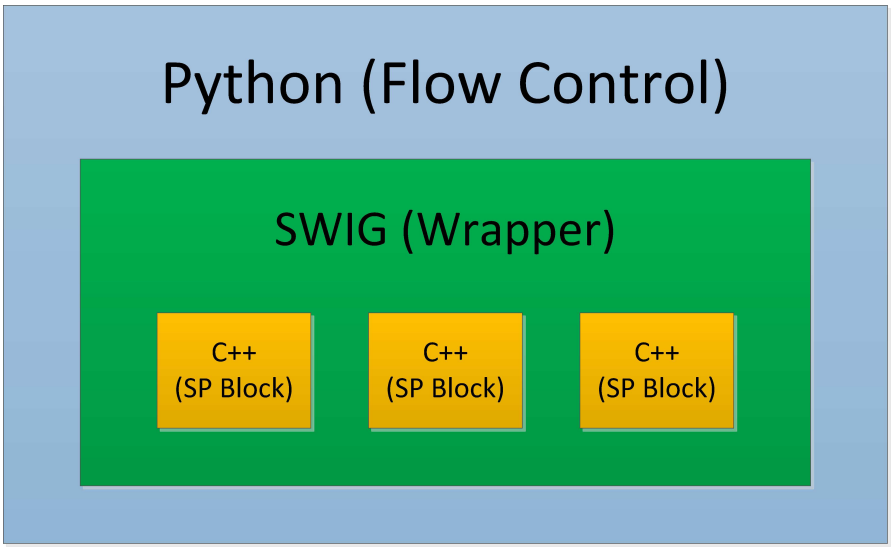

Figure 2.8: GNU Radio Code Structure

Technology[7]. 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.

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[18]. This thesis primarily utilizes the signal processing and communication system aspects of matlab, since MATLAB cannot fully uti-

lize 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 [19]. Below shows an example of a common MATLAB SDR model through Simulink.

INSERT PICTURE OF SDR Model

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 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.

Bibliography

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

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

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

[10] 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.

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

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] Mathworks Inc., 2013.

[19] ———, January 2013.

[20] 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.

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

[22] 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.

[23] 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.

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

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

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

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

[28] 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.

[29] 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.

[30] Kathy Pretz, August 2012.

[31] 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.

[32] 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.

[33] 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.

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

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

[36] 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.

[37] 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.

[38] 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.

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