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

Put your abstract here.

Acknowledgements

Contents

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(Insert citation). 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 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(citation). 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 OSI model (insert citation of OSI model.) 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.

Insert figure of OSI model

Current anti-jamming technics include channel hopping, spatial retreat, jammed area mapping, node escape, retreat restoration, frame masking, and many more[8]. All of these techniques use mechanisms of evasion or despection. These can be quite effective when attacked by generally narrowband, non-dynamic/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[8]. 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: PDR (Packet Delivery Ratio), RSSI (Received Signal Strength Indicator), Physical rate, and Noise levels[4]. 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[4]. 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[4].

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[2]. 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 ẗhoptẗo 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[10].

There also exists systems that are design to resist jamming proactively. These hybrid systems[9] 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(NEED citation). 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[6].

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. 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[7], 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.

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 during 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[5]. Bell stated that such a wireless system can be easily disrupted with simple electromagnetic distrubances. "Its as easy as cutting the wires".[5] 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 defined as the transmission of radio signals that disrupt communications by decreasing the signal to noise ratio (SNR) between the transmitter and receiver(s)(need citation). This jamming can be either deliberate or unintentional. A common example of unintentional jamming is a microwave oven ironically. Microwave oven operate with a wavelength of 122 millimetres which translates to 2.45GHz from the equation shown below. This directly interferes with channels defined

under the IEEE 802.11 standard, also known as Wi-Fi(insert citation). 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 noise, random pulse, stepped tones, warbler, random keyed modulated CW, tone, rotary, pulse, spark, recorded sounds, gulls, and sweep-through(insert citation). These method obviously or subtly disrupt transmissions by inserting electronmagnetic energy into the transmission space of the receivers. Mathematically what is occuring is that 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.

INSERT FIGURE OF Modualated and noisy modulated DBPSK Signals

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 of all 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 also be address, under certain conditions. The table below compares these techniques with various attributes.

INSERT TABLE

Adaptive filtering is a well defined solution in jammer mitigation, but is considerably the most limited. Most notably the jammer must be 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 inverting the correlation matrix[**?**]. The matrix inversion of the correlation matrix is considered a zero forcing equalizer and is extremely unstable in the presence of small noise.

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. [**?**] 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 is applied to the signal to regain its time domain version. This is very effective with the use of 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 a large problem with the STFT approach. Also filter banks don't inject interference when the jammer isn't present, which is a common problem when the jammer turns on and on. Filter banks provide jammer suppression after their spec-

tral decomposition stage, since at this point sub-band encoding can be accomplished this spectral modification can become excision for the jammer[**?**]. A similar decomposition is the wavelet transform. The wavelet transform is much more flexible than a STFT because STFT has a fixed resolution for a given FFT size unlike the wavelet transform. Subspace processing can also be applied in this way. The jammer subspace can be made to orthogonal to the wanted signal subspace, nullifying the jammer's effects[**?**].

Besides these signal processing methods, physical techniques can be use to do spatial filtering. These techiques make uses 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. Beam Forming 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 however, possible to end up in situations where the jammer is in the same direction as the signal source. This is a postcorrelation technique since the desired signal has to be correlated in order to obtain the SNR. Also, prior knowledge of the signal direction and the host location is required(insert citation).

2.3 Communication Systems

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

phase shifts, and several more. These must be compensated for to successful receive uncorrupted information.

Before the receiver, which is the most complicated part of a communication pair, the transmitter must be examine. 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.

At the system level, a modern digital communication system can be broken down into a small set of distinct categories or operations: carrier sychronization, timing synchronization, equalization, and frame synchronization. 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 system, after the radio frequency (RF) front-end, the first operation done on the received signal is frequency compensation and done conversion. When a transmission is made, the transmitter mixes the modulated information with a sinusoid to push the signal up to a much higher frequency. This done because low-frequency signals such as speech, music, or digital data can be much more efficiently transmitted at higher frequencies[3].

2.3.1

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] 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.

[3] 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.

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

[5] Fred W. Ellersick and Donald L. Schilling, *Guest editorial scanning the issue*, IEEE Journal on Select Areas in Communications **3** (1985).

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

[7] J. Mitola, *The software radio architecture*, IEEE Communications Magazine (1995).

[8] 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.

[9] 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.

[10] 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.