3-22-2019

Instantaneous Bandwidth Expansion Using Software Defined Radios

Nicholas D. Everett

INSTANTANEOUS BANDWIDTH EXPANSION USING SOFTWARE DEFINED RADIOS

THESIS

Nicholas D. Everett, Captain, USAF

AFIT-ENG-MS-19-M-024

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-19-M-024

INSTANTANEOUS BANDWIDTH EXPANSION USING SOFTWARE DEFINED RADIOS

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Nicholas D. Everett, B.S.E.E.

Captain, USAF

March 21, 2019

AFIT-ENG-MS-19-M-024

INSTANTANEOUS BANDWIDTH EXPANSION USING SOFTWARE DEFINED RADIOS

THESIS

Nicholas D. Everett, B.S.E.E.
Captain, USAF

Committee Membership:

Dr. Peter J. Collins
Chair

Dr. Michael A. Temple
Member

Major J. Addison Betances, PhD
Member

AFIT-ENG-MS-19-M-024

Abstract

The Stimulated Unintended Radiated Emissions (SURE) process has been proven capable of classifying a device (e.g. a loaded antenna) as either operational or defective. Currently, the SURE process utilizes a specialized noise radar which is bulky, expensive and not easily supported. With current technology advancements, Software Defined Radios (SDRs) have become more compact, more readily available and significantly cheaper. The research here examines whether multiple SDRs can be integrated to replace the current specialized ultra-wideband noise radar used with the SURE process. The research specifically targets whether or not multiple SDR sub-band collections can be combined to form a wider composite band collection thereby achieving instantaneous bandwidth expansion. The goal is to achieve instantaneous bandwidth expansion without using a known a priori signal information or specialized circuitry. Simulations are conducted to develop a process for instantaneous bandwidth expansion and test the bandwidth expansion approach. Hardware tests are conducted to verify simulation results and demonstrate that the bandwidth expansion approach is successful in achieving instantaneous bandwidth expansion. The results here are based on combining collections from two Software Defined Radios (SDRs) having individual bandwidths of 1 MHz. The ability to achieve instantaneous bandwidth expansion up to 1.98 MHz is demonstrated using a cross-correlation approach that combines the multiple sub-band collections into a single wider band collection (without significant distortion or data loss).

Acknowledgements

I would first like to thank my amazing wife for all of the support during the countless nights I spent lost in thought or doing homework. I couldn't have done this without you! To my children, thank you for the comedic relief that would always provide me with a mental break from my research. Next, I would like to thank Dr. Peter Collins for always pointing me in the right direction when I would lose sight of where I was trying to go with my research. Your guidance and mentoring enabled me to complete this research and will continue to serve me in the future. I would also like to thank the rest of my committee and previous instructors. Your knowledge and open door policies were extremely helpful when I couldn't make sense of some results. Lastly, I would like thank my fellow students in the RAIL lab. Our discussions were always enjoyable and I hope our paths cross again in the future.

Nicholas D. Everett

Table of Contents

Page

List of Figures

List of Abbreviations

ADC	Analog to Digital Converter
AFIT	Air Force Institute of Technology
AWGN	Additive White Gaussian Noise
BANTAM	Broadband Antenna Near-field Test and Measurement
COTS	Commercial Off the Shelf
CTFT	Continuous Time Fourier Transform
DAC	Digital to Analog Converter
DFT	Discrete Fourier Transform
FFT	Fast Fourier Transform
GUI	Graphical User Interface
IDFT	Inverse Discrete Fourier Transform
IFFT	Inverse Fast Fourier Transform
LFM	Linear Frequency Modulation
LPA	Log-Periodic Antenna
MATLAB®	Matrix Laboratory
MSPS	Mega Samples Per Second
NoNET	Noise Radar Network
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RF-DNA	Radio Frequency Distinct Native Attribute
ROC	Receiver Operating Characteristic
SDR	Software Defined Radio
SNR	Signal-to-Noise Ratio
SURE	Stimulated Unintended Radiated Emissions

UWB	Ultra Wide Band
WSS	Wide-Sense Stationary

INSTANTANEOUS BANDWIDTH EXPANSION USING

SOFTWARE DEFINED RADIOS

I. Introduction

1.1 Research Motivation

With recent advancements in technology Software Defined Radios (SDRs) have become increasingly popular due to their low cost and flexibility allowing them to be used in a variety of applications ranging from medical devices to automotive radars. The low cost of the SDR is partly due to the lower sampling rate (lower bit count) of the Analog to Digital Converter (ADC) internal to the SDR which inherently limits the instantaneous bandwidth of the receiver. Due to the limited instantaneous receiver bandwidth, SDRs are typically only used in narrowband applications and are not suited for applications requiring the collection of wideband signals.

Previous research efforts [1–3] have focused on bandwidth expansion through multiple sub-band collections taken one after the other. To stitch the multiple collections together, some frequency overlap is required between consecutive sub-band collections as well as a known a priori signal which must be discernible across the entire collection bandwidth. This process works well for certain applications, particularly those that are Wide-Sense Stationary (WSS) (i.e. do not vary over time). However, applications that are non-WSS have data that may be present during one sub-band collection and not the next sub-band collection thus rendering any bandwidth expansion based on these techniques useless.

For bandwidth expansion to be effective with non-WSS applications, the consec-

utive sub-bands must be collected simultaneously to ensure an accurate snapshot of the collected data. This requires an instantaneous bandwidth expansion technique. The Stimulated Unintended Radiated Emissions (SURE) process is an example of one such non-WSS application. The SURE process uses a wideband signal to illuminate a device (e.g. a loaded antenna) and captures the reflected signal [4]. The reflected signal contains some unique characteristics from the device that are used with Radio Frequency Distinct Native Attribute (RF-DNA) fingerprinting techniques to enable the classification of a device as either operational or defective. Lukacs discovered the SURE process was more accurate at classifying a device correctly as the bandwidth of the transmitted and received signals increased [5]. This discovery drives the need for instantaneous bandwidth expansion that enables wideband collections. In previous research, the SURE process was implemented through the use of relatively expensive, one of a kind equipment that was designed specifically as a noise radar which is not very portable. It is desirable to achieve the same results using smaller, cheaper and Commercial Off the Shelf (COTS) available technology.

1.2 Problem Description

As mentioned, previous research efforts undertaken by Lukacs highlight the need for wideband signal collection for use in the SURE process. Lukacs discovered the best results were achieved when the interrogating signal bandwidth exceeded the bandwidth of the device being characterized [5]. For that requirement to be met, the receiver collecting the transmitted signal would require a wide instantaneous bandwidth. Due to the limited sampling rates of the ADCs, most SDRs are not able to facilitate the SURE process. To use SDRs for this purpose, a method of combining the receivers to effectively expand the instantaneous bandwidth of the receiver is required. Due to the non-WSS behavior of the SURE process, the sub-

band collections must be taken simultaneously which renders previous bandwidth expansion techniques useless.

This research aims to determine whether or not multiple narrowband SDRs can be utilized in a filter bank configuration for the collection of a wideband signal to be used in the SURE process. For this to be successful a few items must be considered. First the phase offset between SDRs used to collect separate bandwidths (i.e. sub-bands) must be accounted for or the combined signal will contain errors. Secondly, the SDRs used to collect the signals must have synchronized sampling or the sampling may be slightly different between radios at each time interval which would again cause the combined signal to contain errors and would hinder the estimation of the phase offset correction factor.

1.3 Background

Previous research efforts to be discussed in chapter II, used various techniques to stitch together multiple sub-bands to enable bandwidth expansion but all used a known a priori signal to enable the alignment in the frequency domain. All of those efforts focused on collecting the sub-bands at different times (one after the other) which is feasible if the signal is WSS. Previous efforts would then stitch the signals together by aligning the sub-band collections in the frequency domain and concatenating them together to form a wider bandwidth signal. Previous work with the SURE process has been conducted at Air Force Institute of Technology (AFIT). The SURE process relies on RF-DNA for the classification of a device. Extensive RF-DNA research conducted at AFIT has proven its effectiveness for device/system classification and discrimination.

1.4 Research Goals

The research goals for this effort are to determine if smaller COTS procured devices can be utilized for the SURE process instead of the Ultra Wide Band (UWB) noise radar (AFIT Noise Radar Network (NoNET)) that has been used in previous research with the SURE process. Recent technological advances with software defined radios should provide an avenue to reach that goal. One big hurdle to achieving that is whether or not a wider bandwidth signal can be formed from two receiver sub-band collections through instantaneous bandwidth expansion efforts. Once the instantaneous bandwidth expansion method is proven, an iterative process can be applied to determine if the SURE process is successful when using a wider bandwidth signal that has been formed through instantaneous bandwidth expansion techniques from multiple sub-band SDR collections.

This research effort focuses on instantaneous bandwidth expansion through sub-band combination in the frequency domain. Both stitching by concatenating sub-bands together and summation of the two sub-bands in the frequency domain are explored. Two approaches are examined for correcting any phase offset between the two sub-band collections. These approaches are evaluated in both simulations and hardware testing. After the best approach is identified, a Quadrature Phase Shift Keying (QPSK) signal is transmitted by a single SDR and received by two SDRs to demonstrate the bandwidth expansion results with a common communication signal. Suggestions for future research are outlined in section 5.3.

II. Background

This chapter provides some technical background on key concepts used in this research effort. Section 2.1 provides some background on the Fourier transform and the Fourier properties key to the proposed technique. Section 2.2 provides an overview of the Stimulated Unintended Radiated Emissions (SURE) process and highlights two key components of the SURE process: the noise radar and Radio Frequency Distinct Native Attribute (RF-DNA) processing. Section 2.3 discusses previous bandwidth expansion techniques and their limitations.

2.1 Fourier Transform

The Fourier Transform provides a relationship between the time domain and the frequency domain. The Continuous Time Fourier Transform (CTFT) enables the conversion between the time and frequency domains for continuous time signals $x(t)$. Typically the Discrete Fourier Transform (DFT) is more commonly used since in signal processing the signal has been sampled by an Analog to Digital Converter (ADC) resulting in a discrete signal $x[n]$. The DFT is defined as

$$X(e^{j\omega}) = \sum_{n=-\infty}^{\infty} x[n]e^{-j\omega n} \tag{2.1}$$

and is commonly implemented through a Fast Fourier Transform (FFT) which is a computational algorithm for calculating the DFT faster with the restriction that the number of samples must be a power of 2 [6]. The Inverse Discrete Fourier Transform (IDFT) is the invert of the DFT, thus converting from the frequency domain back to the time domain and is defined as

$$x[n] = \frac{1}{2\pi} \int_{-\pi}^{\pi} X(e^{j\omega})e^{j\omega n} d\omega. \tag{2.2}$$

Likewise, the IDFT also has a faster algorithm for calculation which is commonly used in its place and is referred to as the Inverse Fast Fourier Transform (IFFT) [6].

There are a couple of key Fourier Transform properties that are crucial to the proposed instantaneous bandwidth expansion technique. One of those properties is the scaling property which effectively states that "stretching a time signal will compress its Fourier transform" and "compressing a time signal will stretch its Fourier transform" [6]. The scaling property is defined as

$$y(t) = x(at) \overset{\mathcal{F}}{\longleftrightarrow} Y(j\omega) = \frac{1}{|a|} X(j\omega/a) \tag{2.3}$$

and is very helpful in describing the relationship between the time domain and the frequency domain of a signal [6]. As the duration of a signal decreases in the time domain, the bandwidth of the signal increases in the frequency domain and vice versa.

Another key Fourier property is the time delay property. The time delay property provides a relationship between a delay in the time domain and a phase offset in the frequency domain. The time delay property is defined as

$$x(t - t_d) \overset{\mathcal{F}}{\longleftrightarrow} e^{-j\omega t_d} X(j\omega) \tag{2.4}$$

and demonstrates that the Fourier transform of a time delay is just the Fourier transform of the given signal multiplied by a phase offset related to the time delay [6]. This property is particularly useful when trying to sync two signals together where the relationship of the phase between the two signals is unknown. It enables the correction of a phase offset through the use of a time shift in the time domain.

2.2 Stimulated Unintended Radiated Emissions Process

The word radar was originally an acronym that stood for radio detection and ranging. Radar systems have been used for decades to accomplish those tasks but modern radar systems have evolved to accomplish other tasks as well such as tracking, identifying, imaging, and classifying targets [7]. As time passes, new uses and applications of radar technology will most likely be developed. One such application is the SURE process. The SURE process is able to illuminate an antenna with a noise radar, capture the reflected signal and classify the state of a device (e.g. a loaded antenna) as either operational or defective [4].

The SURE process can be broken down into two main areas: RF-DNA (or fingerprint) generation and device/signal discrimination or classification. A noise radar is used as the transmitter and receiver for the Ultra Wide Band (UWB) signal. A cross-correlation of the transmitted and received signals provides an impulse response for the RF-DNA tools. Numerous impulse responses are collected for a given device and are provided to the RF-DNA tools to generate multiple fingerprints (similar to human fingerprints being attributable to a specific person) for the item under test. The RF-DNA tools use those fingerprints to classify the device into a specified category such as operational or defective [4]. Extensive research has been conducted at the Air Force Institute of Technology (AFIT) in the RF-DNA area. Some of this research includes detecting home automation network attacks using a Software Defined Radio (SDR) [8], resolving radar signal ambiguities in digital radio frequency receivers [9] and wireless intrusion detection [10] all through the use of RF-DNA.

Zeqolari demonstrated the ability to utilize a UWB noise radar to illuminate, collect signals and then apply RF-DNA to classify those signals. Zeqolari's work utilized the AFIT Noise Radar Network (NoNET) UWB noise radar [4]. Zeqolari was able to successfully fuse the previous work with the AFIT NoNET with the

previous RF-DNA research forming the foundation of the SURE process.

By utilizing a noise radar instead of a pulsed radar, the system is able to avoid any interference with other potential signals in the environment (such as those in a production environment). This low probability of interference is due to the inherent orthogonality of the noise waveform to interfering Radio Frequency (RF) signals in the environment [11]. Noise occurs naturally in any environment and since any sample of noise is orthogonal (or highly decorrelated) with any other noise sample, a noise radar is tougher to detect than a typical radar signal. The UWB also lowers the possibility of any interference by distributing the noise signals energy over a much larger bandwidth than that of a narrowband signal. This further reduces the risk of interference with a particular frequency range.

Lukacs advanced the SURE process by expanding upon Zeqolari's work through examining the effect of the interrogating signal bandwidth. As demonstrated previously in research conducted by Lukacs [4, 5, 12, 13], by using an UWB noise radar Lukacs was able to succesfully determine whether an amplifier was operational or defective over 95% of the time. While the setup used by Lukacs was effective, it is not very portable for potential use in a field testing environment and it relied heavily on a uniquely designed system (i.e. not Commercial Off the Shelf (COTS)). The Lukacs method also relied upon existing RF-DNA tools which did not allow for the modeling of devices.

Paul took the previous efforts of Lukacs and Zeqolari one step further by incorporating machine learning and modeling of devices into the SURE process [14]. Paul was able to convert most of the RF-DNA process into a neural net that is able to classify the inputs into categories such as operational or faulty. Under Paul's method, the desired signals are collected using an UWB noise radar similar to that of the previous efforts. The collected signals are then fingerprinted and fed into a trained

neural net. The neural net could have either been trained from actual fingerprints generated from the device under test or could have been trained through fingerprints generated from a model of the device under test. The neural net attempts to classify each fingerprint into a designated class such as operational or defective. The neural net approach streamlined the SURE process but still required the use of the AFIT NoNET UWB noise radar which again is not portable, not COTS procurable and is relatively expensive.

2.3 Bandwidth Expansion

The ability to expand the bandwidth of a receiver is not a new idea. Numerous research efforts have studied bandwidth expansion previously. Most of these approaches use a known a priori multisine (multiple tone) signal that spans over multiple bandwidth collections to assist in the frequency stitching. These approaches also require the sub-bands be collected at different times (one after the other) [1],[2]. The multisine signal is designed so the overlapping regions between collected sub-bands contain two to five tones. These tones are used to align the signals in the frequency domain and are utilized in a phase detrending process to eliminate any phase offset between the two signals. Figure 2.1 shows the multisine signal as well as two sub-bands. In this case, there are two tones in the overlapping region. The authors found the alignment and phase detrending results were better as the number of tones present in the overlapping region increased. The increase in the number of tones present requires more bandwidth to be allocated in the overlapping region which is not desired as it reduces the amount of bandwidth gained from the bandwidth expansion technique.

Other techniques use the aid of known a priori pilot tones over the frequency region of interest [3]. This technique varied from previous technique (Remley et al.) in that it does not require a multisine signal to span across the entire bandwidth

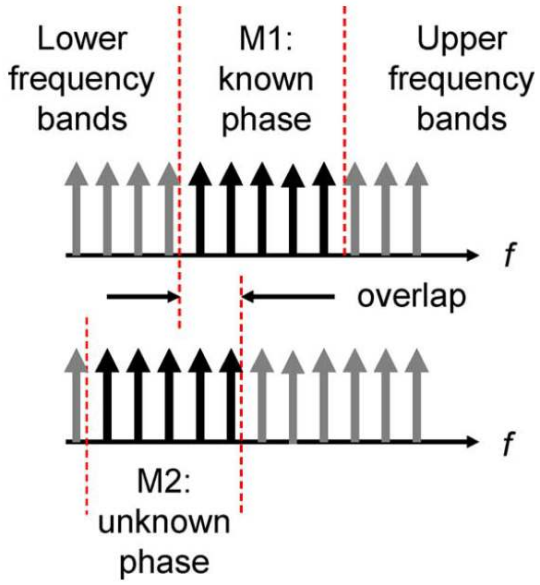

Figure 2.1. Collection process used by Remley et al. which highlights the use of a multisine signal to assist in the alignment of sub-band collections. In this case, two overlapping tones were used for phase alignment. [1]

to be collected, but would generate and inject pilot tones into the RF front end specific to the sub-bands being collected. Figure 2.2 contains the collection process used by Zenteno et al. [3]. As shown in figure 2.2, the pilot tone is generated to a specific frequency band that is being collected and injected into the receiver to enable the sub-band alignment. This method also requires the sub-band collections to be taken one after the other which is sufficient if the signal of interest is Wide-Sense Stationary (WSS). If the signal of interest is non-WSS though, such as those used with the SURE process, these previous techniques are insufficient.

Both of these previous methods have drawbacks by requiring an additional known signal to assist in the bandwidth stitching/combination. The use of a multisine signal or pilot tones contradicts the desired goals of this research effort (i.e. smaller/cheaper design), therefore this research effort will not use the aid of one. The goal of this research effort is also to support the collection of non-WSS signals, therefore all sub-band collections must be taken at the same time. This research effort explores

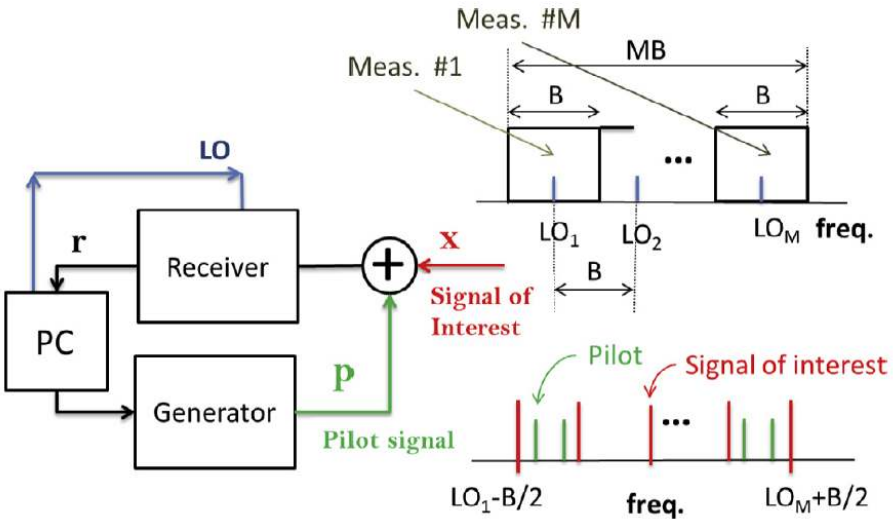

Figure 2.2. Collection process used by Zenteno et al. which highlights the use of a generated pilot signal that is specific to a specific sub-band collection to assist with sub-band alignment. [3]

methods that will enable a sub-band combination without the use of multisine signals or pilot tones while collecting all sub-bands at the same time.

Another research effort was able to achieve bandwidth expansion through the use of time-interleaving [15]. This effort developed a custom built SDR which contains 8 ADCs (figure 2.3). Each of the ADCs are set to sample at $\frac{1}{8}$ the sample rate of the transmitted signal. In order for this approach to be successful, very precise timing is required for each of the ADCs. After the signal is collected, the output of the ADCs are interleaved to increase the effective sample rate by a factor of 8 to form the transmitted signal. The authors found this method was successful in reconstructing the transmitted signal but was very prone to signal distortion. Signal distortion will render this technique useless for the SURE process. The SURE process attempts to identify slight variations in signal collections for successful classification and any signal distortion would most likely impair the results. More importantly though, this technique also relies on a custom built solution which is what this research is trying to eliminate.

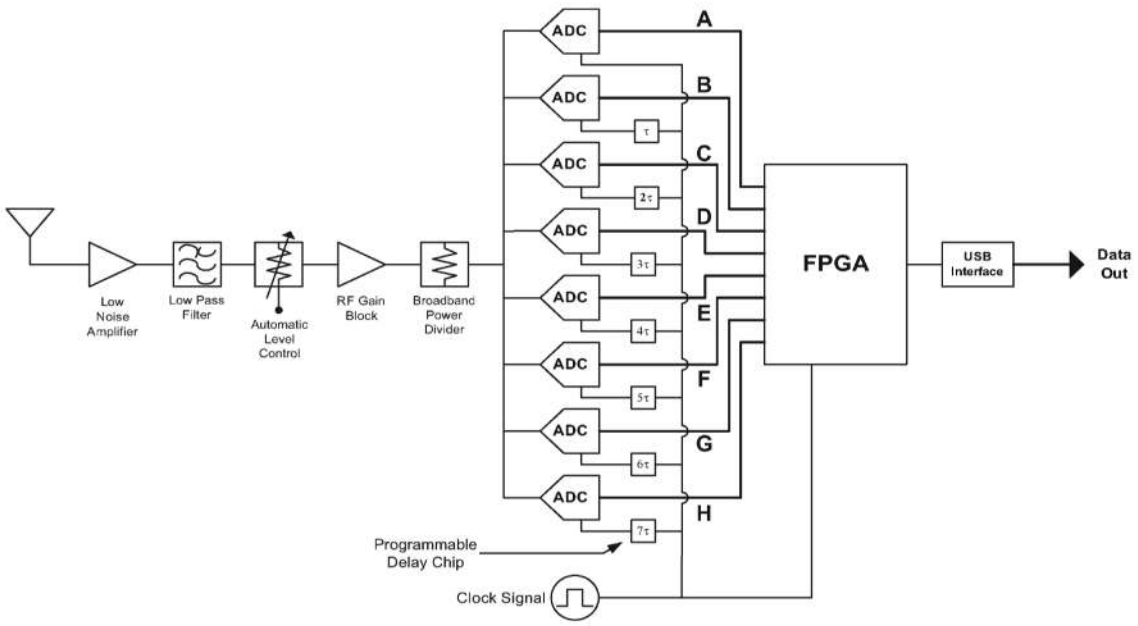

Figure 2.3. Custom designed SDR used by Anderson et al. for their time-interleaving approach. Each ADC samples the signal at different times thus enabling an increase in sampling rate through time-interleaving of the results. [15]

2.4 Summary

This section provided some fundamental background on key concepts to support this research effort. The Fourier properties discussed provide the framework for signal reconstruction using multiple sub-band collections. The SURE process describes the need for an instantaneous bandwidth expansion method and an explanation of why previous bandwidth expansion methods are not suitable for use with the SURE process is highlighted.

III. Design Methodology

This chapter lays out potential phase offset estimation methods and combination methods to achieve instantaneous bandwidth expansion. It also outlines the approach used to test the expansion methods starting with basic concept simulations and concluding with hardware testing.

3.1 Expansion Methods

The method for collecting and post-processing Software Defined Radio (SDR) data is critical to facilitate an increase in instantaneous bandwidth. A few different methods were examined with slight variations between them. Two of the methods vary the approach used to estimate the phase offset while the other two methods vary the approach used to combine the two sub-bands.

3.1.1 Phase Offset Estimation Methods.

One phase offset estimation method used here involves a time domain cross-correlation of the overlapping portions of the sub-band collections. By utilizing the portions of the sub-bands that overlap in the frequency domain, a cross-correlation is performed after using an Inverse Fast Fourier Transform (IFFT) to convert the signals to the time domain. The cross-correlation provides a lead or lag which is applied to one of the sub-bands in the time domain using equation (2.4) to correct for any phase offset between the two signals. Figure 3.1 outlines the process that can be used to estimate and correct for the phase offset using the cross-correlation method.

The other phase offset estimation method uses a phase slope comparison between the two sub-band collections. With this method, the phase slope is calculated for consecutive sub-band collections. Similar to the cross-correlation method, the phase

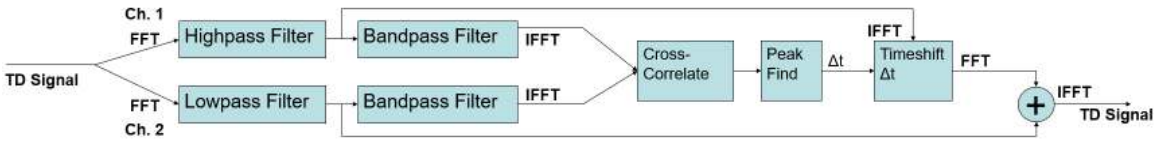

Figure 3.1. Bandwidth expansion method using time domain cross-correlation to estimate the phase offset.

slope comparison method only uses the overlapping portions of the sub-band collections. When comparing the phase of the two signals in the overlapping region, the difference in the slope of the two phases will provide the phase offset between the two sub-band collections. This phase offset is applied in the frequency domain as a phase shift at each individual frequency to correct for the phase offset as

$$F[x(t \pm t_0)] = X(j\omega)e^{\pm j\omega t_0}. \tag{3.1}$$

This phase offset is applied to one of the sub-band collections in the frequency domain to correct for the phase offset between the two sub-band collections. Figure 3.2 provides an outline of the process used. When compared to the previous method (cross-correlation), the phase slope comparison method requires significantly less processing power due to the fewer number of Fast Fourier Transforms (FFTs) and IFFTs required.

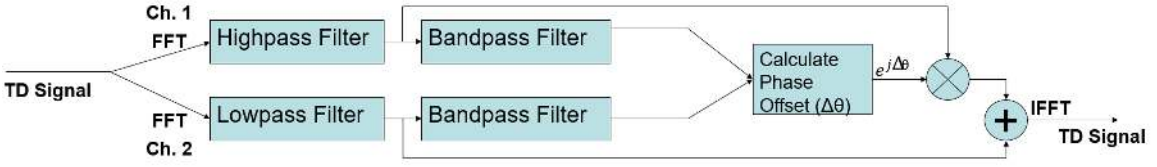

Figure 3.2. Bandwidth expansion method using phase offset estimation through a phase slope comparison between consecutive sub-band collections. The difference between phase slopes is applied as a phase offset correction in the frequency domain.

If hardware is to be utilized, both methods require a frequency offset correction be

implemented prior to estimating the phase offset. This is due to the slight differences in tuning between the two SDRs which can cause a frequency mismatch between the two sub-band collections. Any frequency mismatch between the center frequency the SDR is set to and the center frequency the SDR actually tunes to will cause a frequency misalignment between the two sub-band collections. Since both methods rely on comparing the phase at specific frequencies, the specific frequencies selected need to be identical from the two sub-band collections or the results will contain errors. Figure 3.3 outlines the process to correct for a slight frequency offset between consecutive sub-band collections from any hardware tuning differences and estimate the phase offset (using the cross-correlation method).

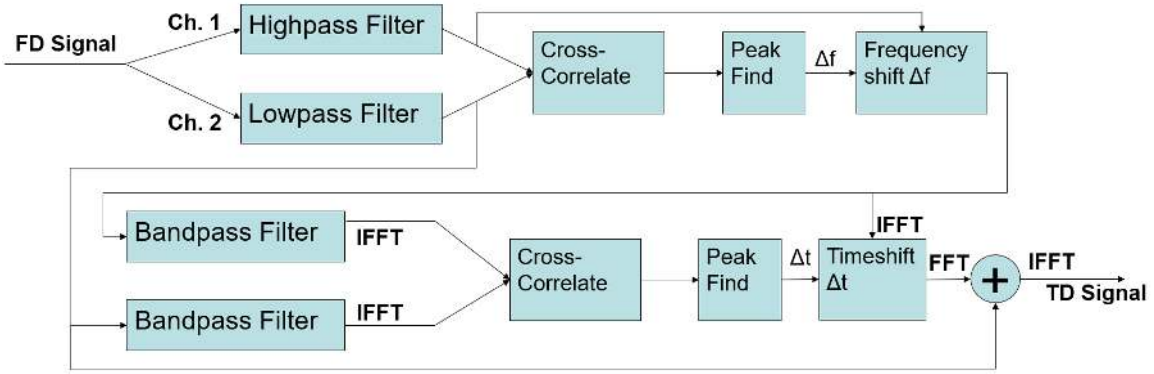

Figure 3.3. Bandwidth expansion method using time domain cross-correlation to estimate the phase offset that also corrects for a slight frequency offset between SDRs through the use of a cross-correlation in the frequency domain.

3.1.2 Combination Methods.

With the phase offset corrected and the two sub-band collections frequency aligned, two combination methods are explored in this research effort: summation and frequency stitching. The summation method involves adding the two sub-band frequency spectra together to form a single frequency spectrum. The frequency stitching method

involves concatenating the sub-bands together in the frequency domain where the end of one sub-band collection is the beginning of the next sub-band. The sub-bands are then stitched together to form a single bandwidth. For this research effort both methods are examined for all simulations and hardware experiments.

Both combining methods have advantages and disadvantages, which along with the signal of interest, will determine which method is best for a specific application. In theory, both methods are relatively simple to implement but the summation method may to be more tolerant for any frequency alignment errors between the sub-band collections than the stitching method. This would be due to the contribution of each sub-band to the combined signal in the overlapped regions. So if one sub-band is misaligned, the other one can compensate which may help with certain applications such as Quadrature Phase Shift Keying (QPSK) which are very dependent upon frequency indexing. With the stitching method, the combined signal will only contain a single sub-band collection at any frequency index. This may prevent any compensation for frequency alignment errors at the overlap region and could provide a very disjointed stitching point possibly resulting in data loss at that frequency bin. This could cause problems for an application such as QPSK.

In theory, the frequency stitching method should never result in any signal distortion by artificially amplifying the overlapped region of the combined signal since each frequency bin is comprised of a single sub-band collection. The summation method could result in signal distortion in the overlap region due to both sub-bands contributing to that portion of the frequency spectrum. This distortion could be minimized by utilizing the roll-off characteristics of the SDR filters. If the SDRs are tuned so that the roll-off from the filters comprise the overlap region, the summation may result in a signal that is close to that of the frequency bins outside of the overlap region. The amount of overlap required to achieve this should be small compared to

the overall sub-band collection but may vary depending on the characteristics of the SDR utilized.

3.2 Modeling and Simulation

Before working with any physical hardware, a modeling and simulation approach is necessary to ensure the instantaneous bandwidth expansion algorithm is successful under ideal conditions. The simulation results will also provide a reference to qualitatively compare any results obtained when utilizing physical hardware. The first phase of modeling and simulation is to demonstrate the cross-correlation response gets narrower as the bandwidth of a signal increases. Since the proposed expansion methods rely heavily on the cross-correlation function, these simulations will provide some insight on expected responses. This insight will help with debugging code and providing a quick check to determine if results are relatively close to what is expected. To demonstrate that relationship, two different waveform types are used: complex random noise signals of varying bandwidths and complex Linear Frequency Modulation (LFM) waveforms.

3.2.1 Bandwidth and Correlation Response.

For the first case, three complex random noise signals were generated using the **randn()** function in Matrix Laboratory (MATLAB®). Each of the signals were generated using different bandwidths through variations in the sampling rate. The sample rates chosen are 500 Hz, 5 kHz and 50 kHz. For the second case, LFM waveforms of different bandwidths were generated: 20 MHz, 50 MHz and 100 MHz. These three waveforms are compared against each other by use of their matched filter responses to demonstrate the relationship between bandwidth and correlation response. The matched filter response is commonly used in radar applications and

it continuously compares the received signal against the transmitted signal through the cross-correlation function. The matched filter response is the cross-correlation of the transmitted signal with the portion of the received signal that maximizes the Signal-to-Noise Ratio (SNR). Filtering a signal $s(t)$ with its matched filter impulse response corresponds to computing the continuous-time auto-correlation function [7] as:

$$\begin{aligned} y(t) &= \int_{-\infty}^{\infty} h(u)s(t-u)du \\ &= \int_{-\infty}^{\infty} s^*(T_M-u)s(t-u)du \\ &= \int_{-\infty}^{\infty} s(v)s^*(v+T_M-t)dv. \end{aligned} \tag{3.2}$$

The final result (3.2) is simply the auto-correlation of s evaluated at lag $T_M - t$.

3.2.2 Square Pulse.

Now that the relationship between bandwidth and correlation has been established the next step is to work towards the bandwidth expansion. To accomplish the overall goal of bandwidth expansion by combining the outputs of two SDRs, an incremental approach is taken which steps towards a simulation that is as close as possible to the actual hardware implementation. The goal of the first step is to create a signal that can be split into two different frequency portions, with some overlap, to demonstrate the ability to reconstruct the original signal from those two portions. Next, a random time delay is injected into the higher frequency portion to simulate a longer path length (e.g. longer cable length) to one of the receivers. This random time delay corresponds to a random phase offset in the frequency domain per the Fourier Time-Shift property (2.4). A 1 sec square pulse is chosen as the signal of interest due to its unique shape in the time domain and in the frequency domain (sinc function) which

provides an easy reference pictorially for reconstruction success or failure. The pulse, frequency response and phase are contained in Figure 3.4.

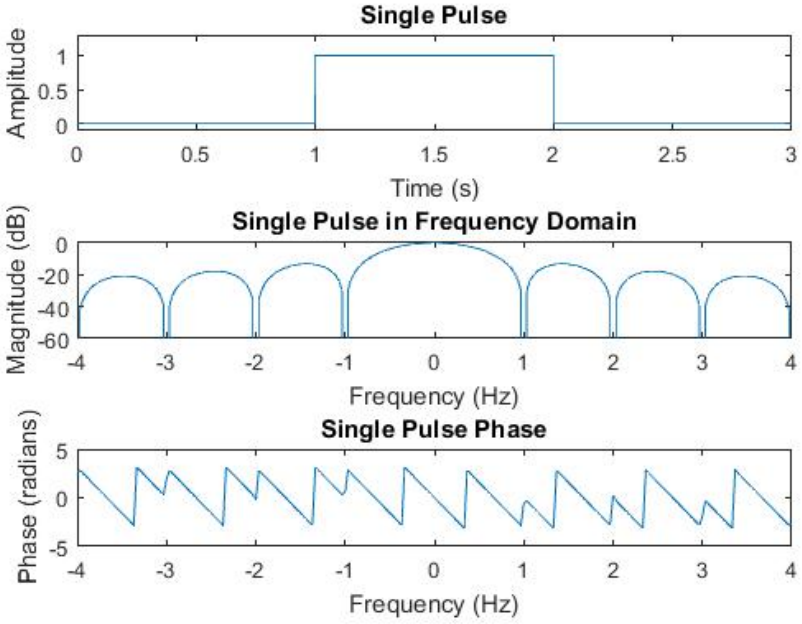

Figure 3.4. A 1 sec square pulse along with its frequency response and phase plots.

Two different approaches are used to try and approximate the random time delay that is injected into the highpass signal. The first approach utilizes the phase slope estimation method by using the difference between the slope of the lowpass phase and the slope of the highpass phase to calculate the phase offset present between the two signals.

The second approach utilizes the time domain cross-correlation between the overlapped portions of the lowpass and highpass signals as

$$s_{xy}[k] = x \circledast y = \sum_{n=-\infty}^{+\infty} x[n]y^*[n+k], -\infty < k < +\infty \tag{3.3}$$

where $\circledast$ denotes the convolution and $*$ denotes the conjugation. The output of the cross-correlation provides a lead or lag which is used to apply the appropriate time-

shift to either the lowpass or highpass signal to correct for the time offset between them. The goal of the time-shift is to eliminate any phase offset between the two signals in the frequency domain which will improve the reconstruction of the original signal in the frequency domain. The accuracy of the reconstruction is then examined by comparing the phase of the original signal with the phase of the reconstructed signal.

After both of the phase offset correction approaches are implemented, the next step is to combine the lowpass and highpass signals in the frequency domain. Since the signals are at baseband in the simulation, a simple summation of the two signals is not sufficient and will induce errors into the reconstructed signal unless the signals are frequency shifted by the appropriate amount. Instead of summing the lowpass and highpass signals, concatenation of the two is performed to achieve the proper reconstructed signal. It should be noted that either method is successful but the summation method requires an extra step of applying a frequency shift to one of the signals. Without frequency shifting, careful indexing is required to ensure the correct portions of the signal are chosen for the concatenation.

To select the correct frequency to splice the lowpass and highpass signals together, some filtering characteristics need to be considered. When an SDR is tuned to a specified center frequency, it also programs some front end filters to prevent any aliasing from occurring and to block any unwanted frequencies from entering the signal processing portion of the radio. In simulation, filters can have perfect cutoff frequencies which will ensure ideal signal quality right up to the stopband of the filter. However when actual hardware is used, that ideal cutoff is no longer achievable. The physical limitations of the hardware cause some rolloff near the stopbands of the filter. In other words, the signal tends to become degraded or weaker as the stopband is approached. To limit those effects on the reconstruction, the amount of

overlap will likely play a key role in the reconstruction when hardware is utilized. The amount of overlap required will also vary from one piece of hardware to another due to the different characteristics of each. For the case of two radios, the transmit center frequency, TX_c, is chosen as the frequency to splice the lowpass signal and the highpass signals together. This ensures the filter rolloff will have less impact and cause less degradation in the reconstructed signal. Once the lowpass and highpass signals are spliced together, the reconstructed signal is plotted in the time domain, the frequency domain, and in the phase domain for comparison with the original signal.

Next the previous simulation is repeated, but this time with Additive White Gaussian Noise (AWGN) injected into both the lowpass and highpass signals. The AWGN mirrors any noise that could be captured from the environment as well as any internal noise from the SDRs. Figure 3.5 shows the square pulse with the AWGN. The goal of the simulation is again to correct for any phase offset and reconstruct the original signal as well as possible. Once this simulation is successful, the next step is to repeat the simulation with AWGN, but instead of using a 1 sec square pulse, the simulation will use a 1 sec pulse of random noise as shown in Figure 3.6. As part of the 1 sec pulse of random noise simulation, a Monte Carlo simulation is conducted to determine how accurate the phase offset approximation is over a range of SNR values from -15 dB to 15 dB.

3.2.3 Gaussian Burst.

A similar simulation is conducted using a Gaussian burst as the signal of interest instead of the square pulse. A Gaussian pulse is generated by first creating a cosine signal with a frequency of 1 kHz and then applying a Gaussian window,

$$w(n) = e^{-n^2/2\sigma^2} \tag{3.4}$$

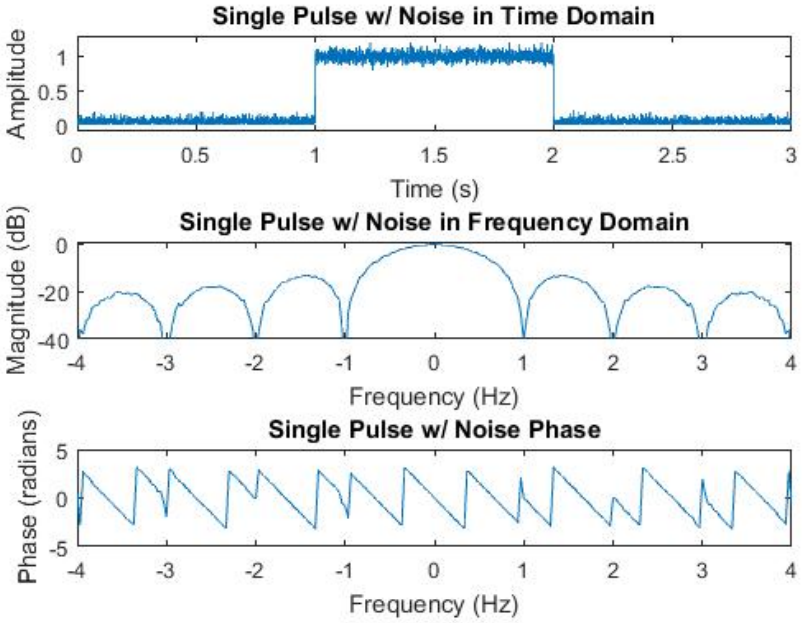

Figure 3.5. A 1 sec square pulse with AWGN along with its frequency response and phase plots.

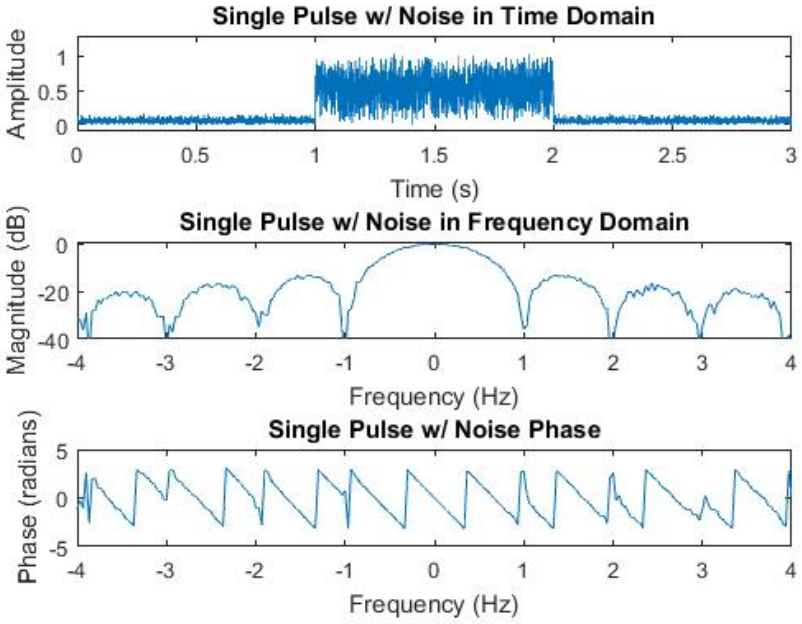

Figure 3.6. A 1 sec random noise pulse with AWGN along with its frequency response and phase plots.

where $\sigma = (N-1)/(2\alpha)$. N is defined as the number of samples in the cosine signal and α is fixed at a value of 16 to provide a narrow pulse shape as shown in Figure 3.7. This results in a -3 dB bandwidth of 9 Hz and a mainlobe bandwidth of 840 Hz. The lower bandwidth is a result of the alpha value selected. A larger value of alpha will make the pulse narrower and the bandwidth wider, but it will also require a higher sampling rate which will require more processing power. Less processing power enables the simulation to be run numerous times after making slight adjustments. After the Gaussian pulse is created and filtered into two sub-band spectrums, a time delay is injected into the highpass portion in the time domain (2.4) to simulate a phase offset between the two bandwidth collections (this would be representative of different signal path phase delays encountered in a real system). The Gaussian burst simulation provides assurance that the bandwidth expansion approach is applicable to a variety of signals instead of only a square pulse.

3.2.4 QPSK.

In an effort to determine if the stitching method will cause any errors in a realistic communication signal, a final simulation is conducted utilizing a 1000 bit (500 symbol) QPSK signal which is created and modulated to 3 GHz. The signal bandwidth (approximately 50 MHz in this case) was chosen to exceed that of a single SDR (approximately 25 MHz). AWGN is injected into the modulated signal to simulate noise from over the air transmission. The modulated signal is captured through the use of lowpass and highpass Butterworth filters acting as SDRs. Both filters are designed as 8th order Butterworth filters with a 25 MHz passband. The center frequencies of the filters are offset to provide a 5 MHz (20%) overlap in the collected bandwidths. This overlap portion enables a cross-correlation between the collected signals in the time domain to determine the phase offset between the lowpass and

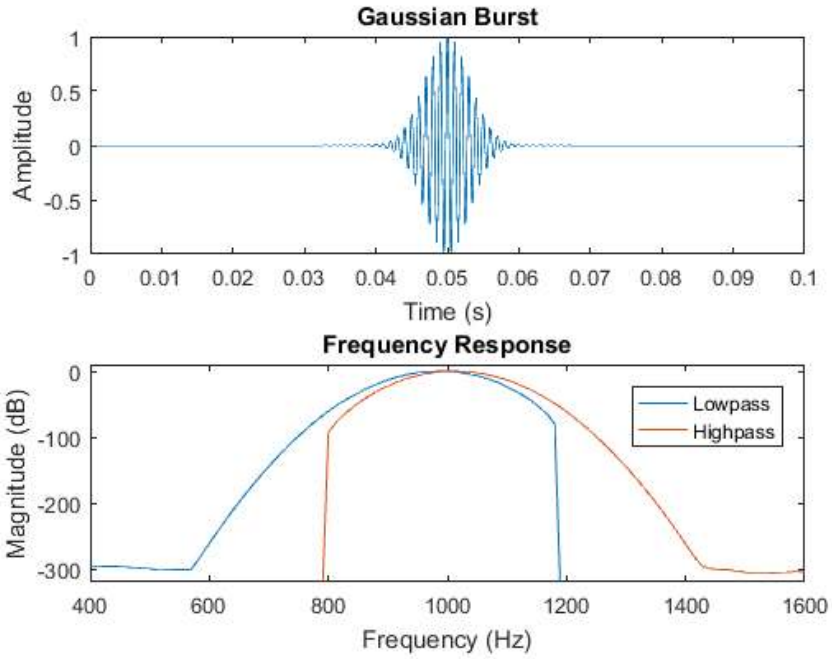

Figure 3.7. Simulated Gaussian pulse in both the time domain and the frequency domain. Frequency response is shown with both the lowpass and highpass portions to illustrate the different sub-bands to be stitched together.

highpass portions similar to the previous simulations.

3.3 Single Receiver Collections

Previous research suggests that a single radio collection will not be sufficient for the Stimulated Unintended Radiated Emissions (SURE) process to distinguish between antennas. A single radio collection hardware test will prove that suggestion and provide a baseline to compare the results from a multiple radio collection against. The comparison could demonstrate an improvement with the SURE process if the multi-radio collection is successful. Therefore the goal of this test is to determine if the SURE process is able to distinguish between different receiver antennas while using a single SDR to capture the transmitted signal. To conduct this test, an Ettus Research X310 (Figure 3.8) is utilized to transmit a random noise signal generated in MATLAB® and an Ettus Research B205 mini-i (Figure 3.9) is used to collect the signal.

Figure 3.8. Ettus Research X310

Figure 3.9. Ettus Research B205 mini-i

To properly configure the SDRs and ensure the GNU Radio Companion setup is correctly configured, the two SDRs are connected via an RF cable with a 30 dB attenuator. This configuration provides a controlled environment to ensure the SDR settings are correct and MATLAB® will be able to correlate the received signal with the transmitted signal. Various configurations are tested, most of which involves various sampling rates of the X310 and the B205. Initially, the X310 is set at 200 MSPS which is the maximum supported sampling rate. The B205 is set at 50 MSPS since it

is an even multiple of 200 MSPS and less than the maximum supported sampling rate of the B205 (56 MSPS). When this setup is executed in GNU Radio Companion, it displays numerous warnings about the B205 under-sampling and the cross-correlation is not successful (did not provide a large impulse response). Even when resampling the transmit signal by a factor of 3 with zeros (to ensure actual data every 4th sample, effectively 50 MSPS), the cross correlation is unsuccessful. This is most likely due to the B205 not sampling the correct samples (ones with the actual data), but possibly sampling the zeros (noise) instead.

After numerous testing configurations, it is discovered that a sampling rate of 20 MSPS on both the X310 and the B205 provided a strong cross-correlation. The 20 MSPS was chosen due to it being an even divisor of 200 (clock rate supported by the X310) and less than the maximum sampling rate of the B205. Any other non-even divisor will provide unstable results which will not cross-correlate. Due to those issues, 20 MSPS is used to move forward with the testing via antenna transmission. The GNU Radio Companion setup is shown in Figure 3.10.

For the remainder of the testing, the cable connecting the X310 and B205 is removed and each of the radios are connected to an antenna which are placed inside a Broadband Antenna Near-field Test and Measurement (BANTAM) chamber to protect against any unwanted signal interference. The X310 remains connected to a Log-Periodic Antenna (LPA) antenna (Model: WA5VJB, operating range: 850-6500 MHz, Figure 3.11) which is used as the transmitter antenna for the duration of the testing. The B205 is also connected to a LPA for the first set of data collection. Both SDRs are configured for a sample rate of 20 MSPS. As part of the SURE process, 100 fingerprints are generated through Radio Frequency Distinct Native Attribute (RF-DNA) fingerprinting for the LPA using MATLAB®. This entire procedure is repeated for a second LPA (Model: WA5VJB, operating range: 850-

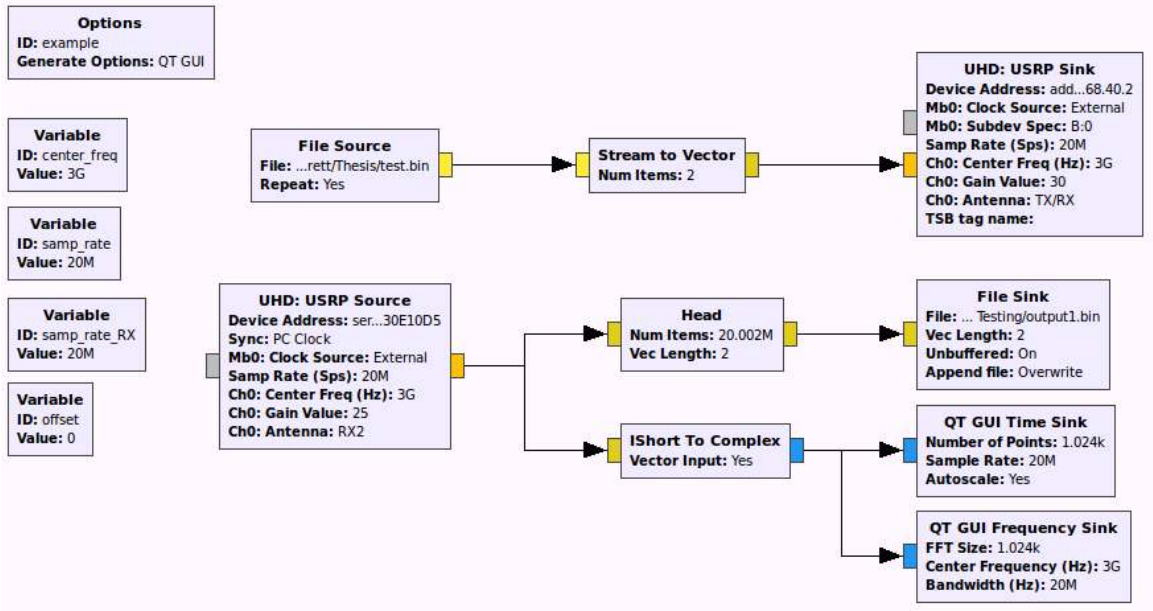

Figure 3.10. GNU Radio Companion setup to test the SURE process with a single receiver.

6500 MHz, Figure 3.11), a rectangular feed horn (Model: H-1498, operating range: 2-18 GHz, Figure 3.12), and a round feed horn (Model: AS-48461, operating range: 2-18 GHz, Figure 3.13) each connected to the B205 receiver for a total of 400 fingerprints (100 per receiver antenna). Those fingerprints are fed into the SURE process to determine if it can successfully distinguish between the different receiver antennas.

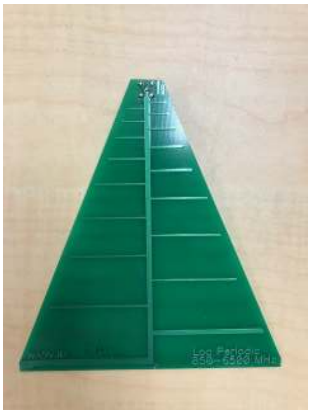

Figure 3.11. Log-Periodic Antenna

Figure 3.12. Rectangular Feed Horn

Figure 3.13. Round Feed Horn

3.4 Two Receiver Collections

The next two sections highlight the experiments that utilize two receivers for the collections. The first section outlines the approach for transmitting a Gaussian Burst signal and collecting it with two SDRs. The next section discusses the approach for transmitting and collecting a QPSK signal. The QPSK section details the variations in the hardware setup and how each of those setups will affect the bit error rate (P_b) calculations.

3.4.1 Gaussian Burst.

In an effort to verify the proposed solution to increase instantaneous receiver bandwidth and validate the simulation results, a hardware test is desired. Two Ettus Research B205 mini SDRs are selected for the receivers due to their availability (Commercial Off the Shelf (COTS)), cheap cost and history of use. A function generator provides a 10 MHz clock reference to synchronize the clocks of the SDRs. In an effort to compare hardware results with simulation results, a Gaussian pulse is chosen as the transmit signal (Figure 3.14). To form the pulse, a 200 kHz cosine is used as the base signal. A Gaussian window with $\alpha = 256$ is then applied to generate a 200 μs Gaussian pulse with a 13.5 kHz -3 dB bandwidth and approximately 140 kHz wide mainlobe centered at 200 kHz. The Gaussian pulse is uploaded to an arbitrary waveform function generator with a frequency of 5 kHz and mixed with a 3 GHz carrier signal from a signal generator (Figure 3.15).

After mixing the Gaussian pulse and 3 GHz carrier signal, the resulting signal is split and sent into both SDRs. Each SDR is tuned to 3.0002 GHz and programmed to collect a 1 MHz bandwidth. The 1 MHz bandwidth is more bandwidth than is required but is used to provide error checking and provide a comparison of what the signal would look like if the SDR had enough bandwidth to capture the entire signal. The

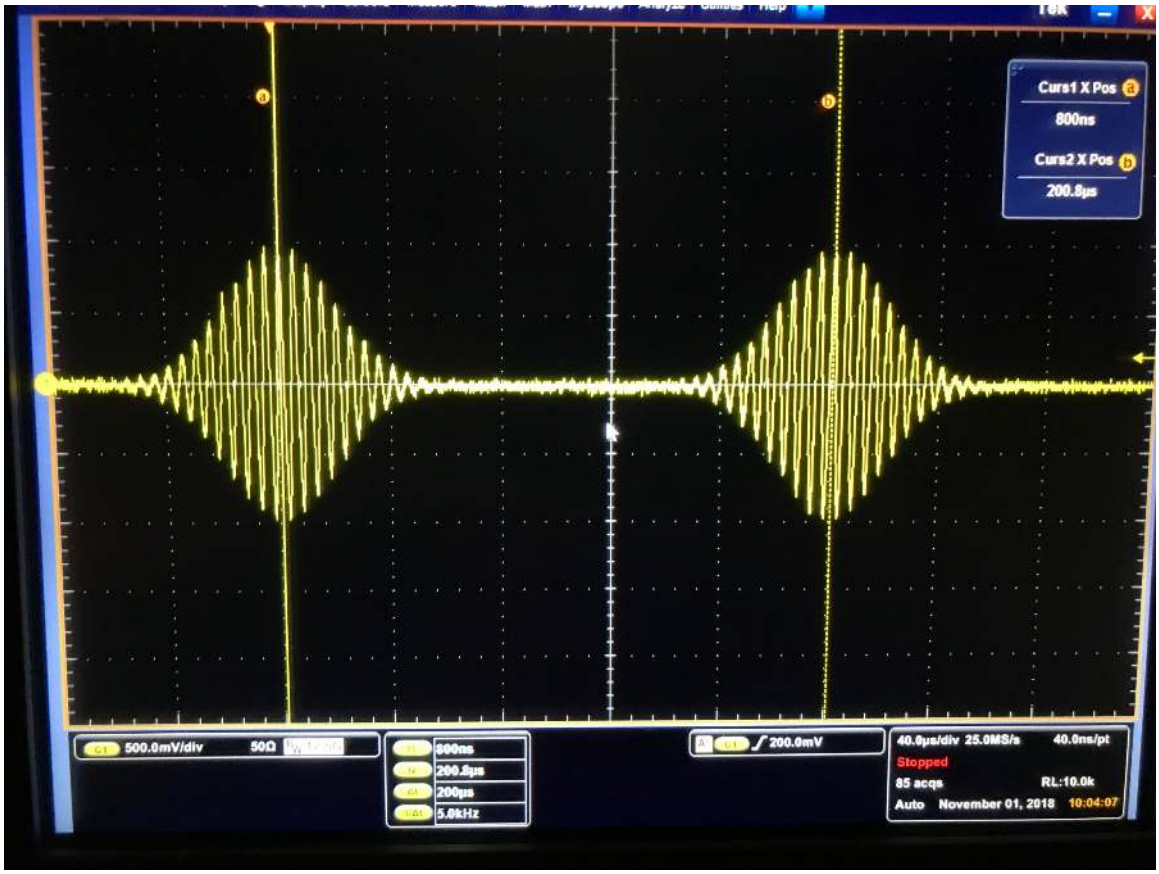

Figure 3.14. Oscilloscope capture of $200\ \mu$s Gaussian Burst signal formed from a 200 kHz cosine and transmitted with a frequency of 5 kHz.

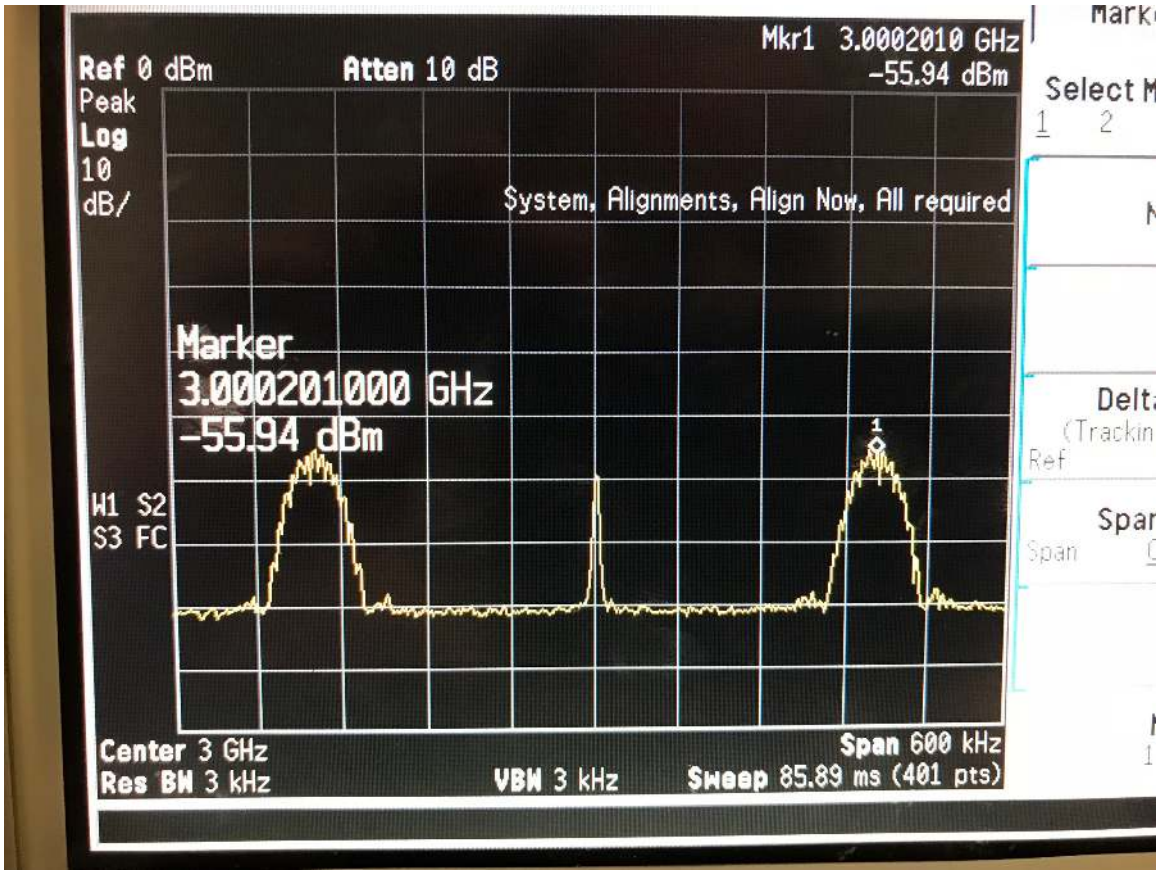

Figure 3.15. Frequency response of the Gaussian Burst captured by a spectrum analyzer highlighting the 200 kHZ offset from transmit center frequency.

collected signals from the SDRs are post-processed in MATLAB® to filter out 200 kHz portions as the lowpass and highpass collections. Prior to filtering out the 200 kHz portions, the signals are cross-correlated in the frequency domain to determine any tuning mismatch between the two SDRs. The cross-correlation provides the tuning mismatch between the two SDR that ensures the 200 kHz portions are aligned in the frequency domain. Once the lowpass and highpass portions are extracted, the phase offset is estimated through the cross-correlation approach. The phase offset is corrected for by applying a time-shift in the time domain and the two portions are concatenated in the frequency domain to complete the bandwidth expansion.

3.4.2 QPSK.

Using a similar approach to that of the Gaussian Burst, a QPSK signal is used to verify and validate the QPSK simulations. A QPSK signal provides an easy metric (P_b) for quantifying the results of the instantaneous bandwidth expansion methods on a communication signal. For this test, three Ettus Research B205 mini-i SDRs are utilized. One SDR transmits the signal while the other two SDRs receive the transmitted signal. Three different tests are conducted with this setup: one with the same center frequency and enough bandwidth to capture the entire signal (2 MHz per radio), one with the same center frequency but without enough bandwidth to capture the entire signal (1 MHz per radio), and one with different center frequencies (490 kHz offset) but without enough bandwidth to capture the entire signal (1 MHz per radio). The receivers are tuned to the same center frequencies and different center frequencies with different amounts of overlap in their frequency bands. The two receivers are connected to a 10 MHz clock source to synchronize the sampling intervals between the two. LPAs are used for both the transmit and receive paths. The two LPAs are positioned approximately 3 feet apart and are located inside a

BANTAM chamber. The receive antenna is connected to a power divider to provide the received signal to both of the receivers.

A QPSK signal is created in MATLAB® with a sample rate of 20 MHz and 4 samples per symbol which provides approximately 5 MHz of bandwidth (Figure 3.16). The signal is created with 200,000 random bits encoded into 100,000 QPSK symbols through the use of a raised cosine filter in MATLAB®. The QPSK signal is then zero padded to provide some buffer in the event the transmitter begins transmitting before the receivers begin collecting. The SDRs are all controlled through GNU Radio Companion. Figure 3.17 contains the GNU Radio Companion setup for the testing.

To simplify the signal processing, the sampling frequency of the transmitter, F_{s_T}, is fixed at 8 MHz and the sampling frequency of the receivers, F_{s_R}, are fixed at 1 MHz. The $F_{s_T} = 8$ MHz ensures the entire QPSK signal is being transmitted. The parameters chosen during the creation of the QPSK signal allow for some signal reconstruction with $F_{s_R} = 1$ MHz, but not a complete reconstruction (i.e. results in some bit loss). Complete signal reconstruction is expected with 2 MHz bandwidth. Since the QPSK signal is created with 20 MHz and it provides a 5 MHz bandwidth, any reduction in $F_{s_T} = 20$ MHz will appear to scale the bandwidth of the QPSK signal while maintaining the ratio of 4:1. For example if $F_{s_T} = 10$ MHz, the transmitted signal will appear to have only 2.5 MHz of bandwidth, but if it is upsampled by a factor of 2, to match its actual sample rate, it will still have 5 MHz of bandwidth. Therefore $F_{s_T} = 8$ MHz will provide a QPSK signal with 2 MHz bandwidth. To simplify the analysis, all results will be compared against the QPSK signal bandwidth of 2 MHz.

TX_c is fixed at 3 GHz which is within the operating range of the LPAs. The first test contains no offset where both $RX2_c$ and $RX2_c = 3$ GHz. This test demonstrates 1 MHz bandwidth is not enough to capture the entire QPSK signal. Next the receivers center frequency, $RX1_c$ (lower frequency receiver) and $RX2_c$ (higher

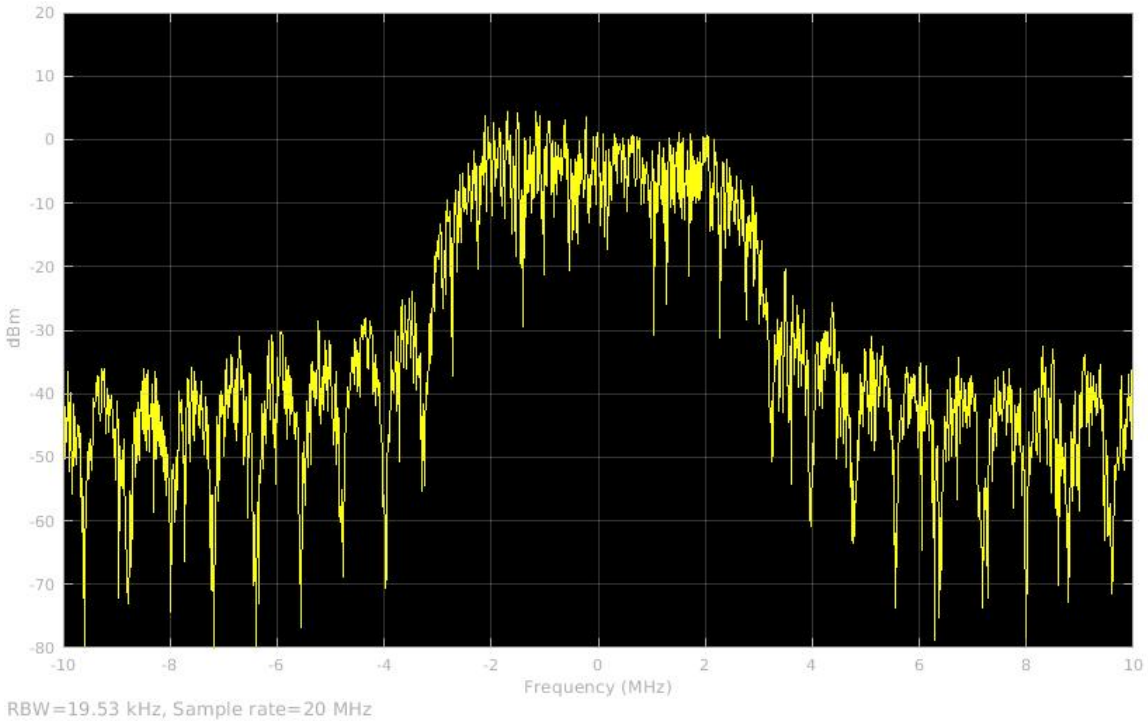

Figure 3.16. Frequency spectrum of the QPSK signal created for testing (shown at baseband) with a useable bandwidth of 5 MHz.

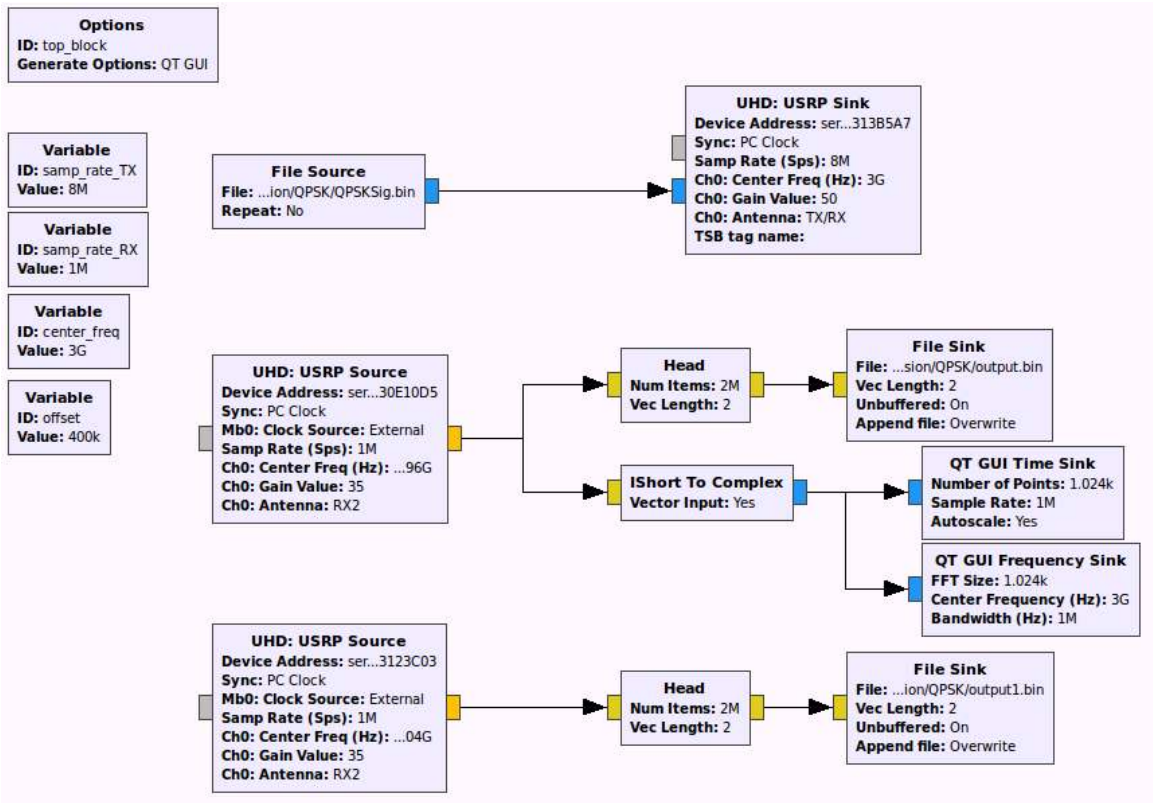

Figure 3.17. GNU Radio Companion setup to transmit and collect a QPSK signal.

frequency receiver), are offset from the transmit center frequency, TX_c, as much as possible while still maintaining some bandwidth overlap to assist in the alignment of the collected signals. A second test is conducted with an offset of 490 KHz which sets $RX1_c = 3$ GHz $-$ 490 KHz and $RX2_c = 3$ GHz $+$ 490 KHz. The combined instantaneous bandwidth, BW_c, can be calculated by

$$BW_c = Fs_R + (2x\text{offset}) \tag{3.5}$$

which in this case results in $BW_c = 1.98$ MHz. This test demonstrates an improvement in signal reconstruction from combining the instantaneous receiver bandwidths versus the performance when using a single receiver to collect the signal. Other tests are also conducted with different F_{s_R} and offsets to demonstrate the performance as receiver bandwidth increases.

Once the signal is collected by the receivers, some signal processing is performed to align and combine the two bandwidths to effectively expand the instantaneous bandwidth. The signal processing portion can be broken down as follows:

1. Interpolate the collected signals (F_{s_R}) to match F_{s_T}.
2. Correct for the phase offset between the collected signals.
3. Correct for the frequency offset to roughly align the collected signals.
4. Correct for the slight tuning differences of each receiver in the collected signals.
5. Combine the collected signals
6. Correct for any slight tuning error of the transmitter
7. Locate and extract the portion of the collected signal containing the QPSK signal.
8. Convert the QPSK signal back into symbols and bits for error checking

The interpolation step ensures the sample rates match which enables the demod-

ulation of the QPSK symbols without any issues and simplifies the interpretation of any plots. The phase offset correction between the two collected signals ensures no phase errors will be induced into the combined signal which is demonstrated in the modeling and simulation results. To correct for the phase offset, a time domain cross-correlation of the collected signals provides a time shift that can be applied to either of the signals through the Fourier time delay property (2.4). This time shift will align the collected signals in the time domain thus eliminating any phase offset between the two. A frequency shift equal to the frequency offset applied to each of the receivers roughly aligns the collected signals in the frequency domain since the collected signals are at baseband.

For the combination to be successful, the collected signals must be perfectly aligned in the frequency domain. The slight tuning differences of each receiver will be a bit more difficult to resolve. The slight tuning differences are a result of independent master oscillators in each of the receivers which are used in tuning each SDR to its designated center frequency ($RX1_c$ and $RX2_c$) and thermal instabilities in each radio. This slight tuning error causes $RX1_c$ and $RX2_c$ to be slightly different which must be corrected prior to combination. A cross-correlation of the overlapping bandwidths in the frequency domain provides the amount of mismatch between the two collected signals. A frequency shift can then be applied to correct for the mismatch and perfectly align them in the frequency domain. The collected signals can then be combined by summing the frequency components.

Once the signals are aligned and combined, the QPSK demodulation begins by estimating the center frequency of the collected signal. This estimation can be applied as a frequency shift to ensure the QPSK signal is centered in the frequency domain. This step corrects for any tuning error in the transmitter. To extract the QPSK portion of the signal, a cross-correlation between the known QPSK signal and the

combined signal will provide the starting index of the QPSK portion in the combined signal. It should be noted that while the known QPSK signal is used to locate and extract the QPSK portion in the combined signal, other methods exist to locate the signal without knowledge of the QPSK signal, but they are not trivial. Since signal detection is not the focus of this research effort, the known signal is used for simplification. Once the QPSK portion of the combined signal is extracted, demodulation and P_b calculations are performed to quantify the instantaneous bandwidth expansion results.

3.5 Summary

This chapter examined different approaches proposed to estimate and correct for any phase offset between SDRs used to capture the signal sub-bands. This phase offset is the main error source in the instantaneous bandwidth expansion techniques proposed in this thesis. It also described the modeling and simulation test scenarios using various pulses such as the square pulse and Gaussian burst. It then detailed the single radio collections and its application of the SURE process to distinguish between 4 different receiver antennas. Finally, it concluded with the two receiver collections detailing the Gaussian burst reconstruction and the QPSK reconstruction setups.

IV. Results

4.1 Bandwidth and Correlation Response Relationship

The bandwidth and correlation response simulation confirmed the relationship between the bandwidth of a signal and the shape of the correlation response. Figures 4.1 and 4.2 show the results of the simulation. As shown in Figure 4.1, as the bandwidth of the signal increases from 500 Hz to 50 kHz, the correlation response becomes narrower. This intuitively makes sense since higher bandwidth signals contain higher frequency signals. The higher frequency signals will have more variation from sample to sample over a specified time interval than that of lower bandwidth signals. The larger variation from sample to sample will result in a stronger correlation which will squeeze the correlation response making it narrower. Figure 4.2 shows the calculated bandwidth (using the Matrix Laboratory (MATLAB®) **obw()** function) for the 500 Hz complex random noise signal (494.771 Hz). The bandwidth calculations for the other two sampling rates (5 kHz and 50 kHz) were 4.957 kHz and 49.516 kHz respectively.

The results from the Linear Frequency Modulation (LFM) signals confirms the previous scenario results of the complex random noise signals. As the bandwidth of the LFM waveforms increased from 20 MHz to 100 MHz, the matched filter response becomes narrower. Figures 4.3 and 4.4 show the results of the simulation. The 20 MHz bandwidth signal has the narrowest bandwidth of the three LFM signals but has the widest matched filter response of the three signals. Similarly, the 100 MHz bandwidth signal has the widest frequency spectrum but the narrowest matched filter response. These results confirm that as signal bandwidth increases, the matched filter response (correlation) will become narrower.

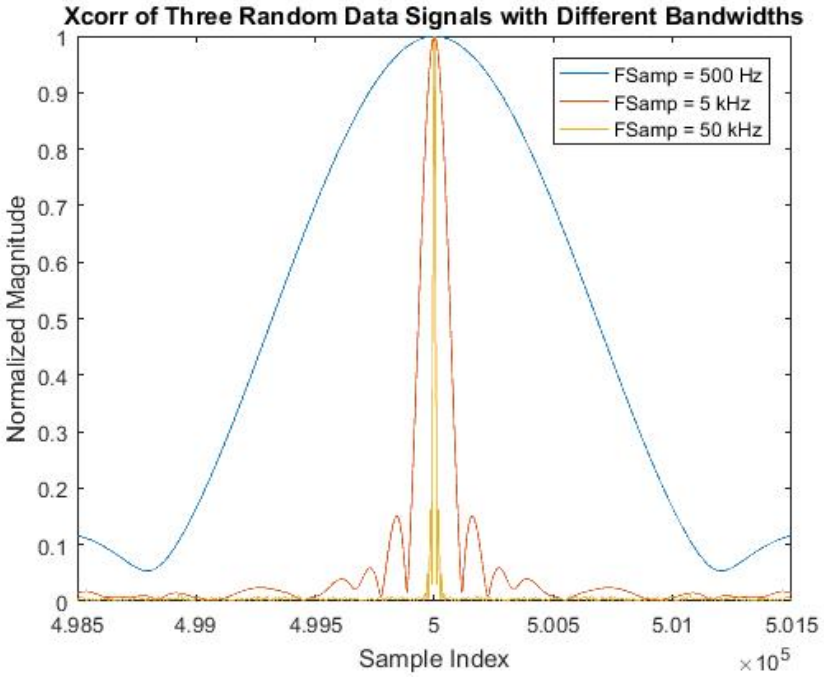

Figure 4.1. Normalized auto-correlation response of three random noise signals.

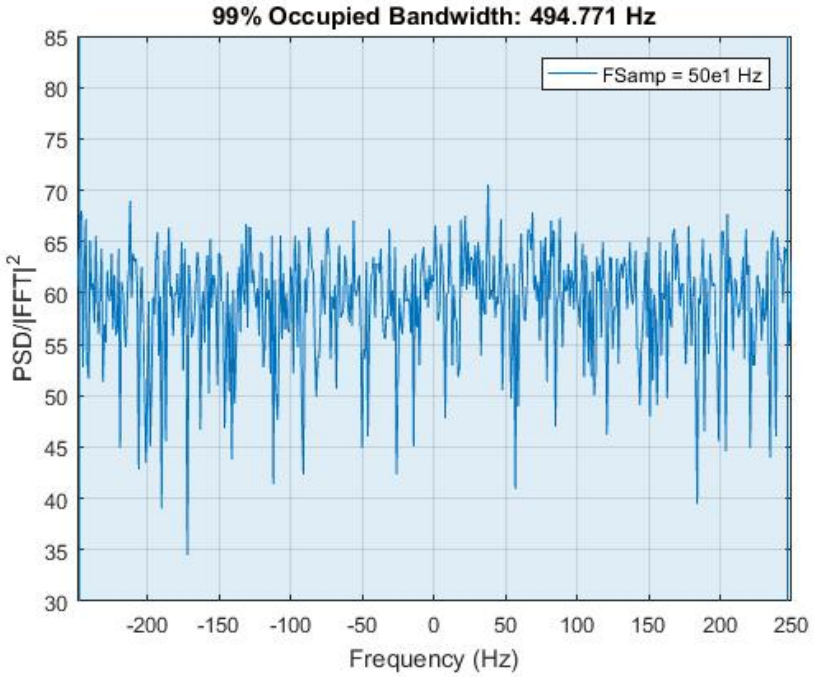

Figure 4.2. Bandwidth of the 500 Hz random noise signal.

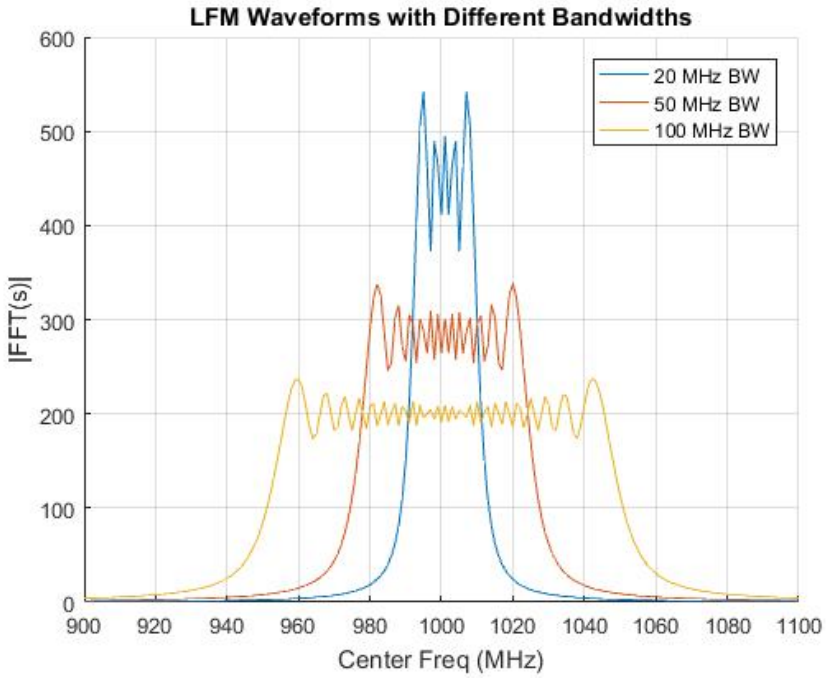

Figure 4.3. Three LFM waveforms with different bandwidths plotted in the frequency domain.

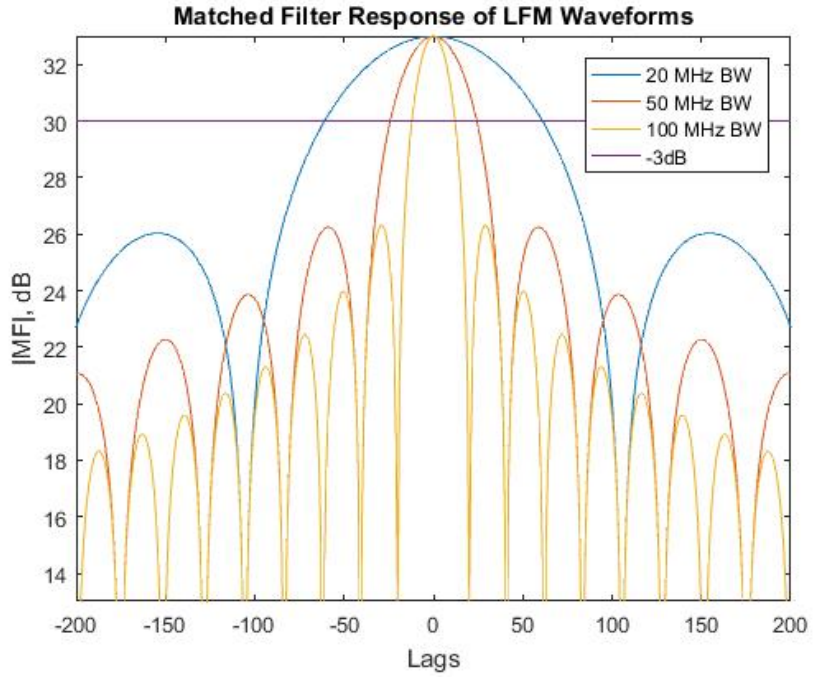

Figure 4.4. Matched filter response of three LFM waveforms with different bandwidths.

4.2 Bandwidth Expansion Simulations

Now that the relationship between bandwidth and correlation is understood, some MATLAB® simulations will help evaluate the proposed expansion methods. A square pulse simulation is conducted to demonstrate the phase offset issue. Then a Gaussian burst simulation is completed to demonstrate the bandwidth expansion approach on a different waveform. Finally a Quadrature Phase Shift Keying (QPSK) simulation is conducted to help quantify the results through bit error checking and ensure no data loss occurs when using a communication signal.

4.2.1 Square Pulse.

The first step of the bandwidth expansion simulations uses a 1 sec square pulse as the original signal. The square pulse was filtered into a lowpass and highpass portion. The highpass portion is then injected with a phase offset to simulate a longer path length. Figure 4.5 contains the attempt to reconstruct the original signal (Figure 3.4) using the uncorrected highpass portion which still contains the injected phase offset. As shown, the reconstructed pulse does not resemble a square pulse due to the phase offset. Per the Fourier Time-Shift property (3.1), the phase offset in the frequency domain results in a time shift in the time domain. This is evident from the top two plots in Figure 4.5. One can also observe the effect on the phase by comparing the phase of the signal with the ideal phase (phase of original signal). Figure 4.7 contains the comparison.

During the simulations, two approaches are examined to approximate and correct for the phase offset in the highpass signal. The phase slope approximation method initially works but once the Additive White Gaussian Noise (AWGN) is introduced, this approach becomes much less reliable than the other approach. The other approach is approximating the phase offset through the cross-correlation in the time

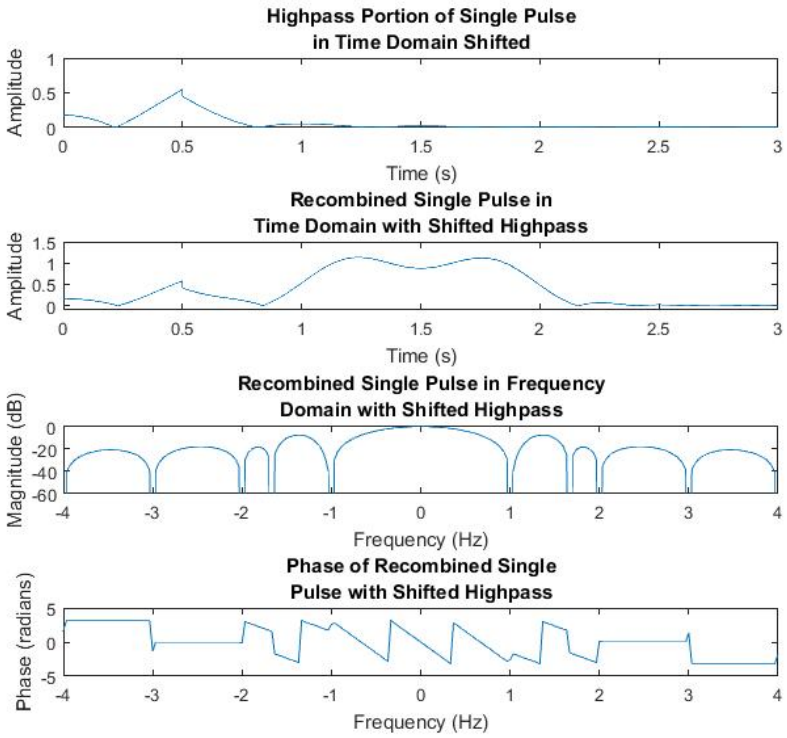

Figure 4.5. Reconstruction of signal using highpass containing phase offset. First plot is highpass signal with phase offset, second plot is reconstructed signal using highpass with phase offset, third plot is frequency domain spectrum of reconstructed signal and fourth plot is the phase.

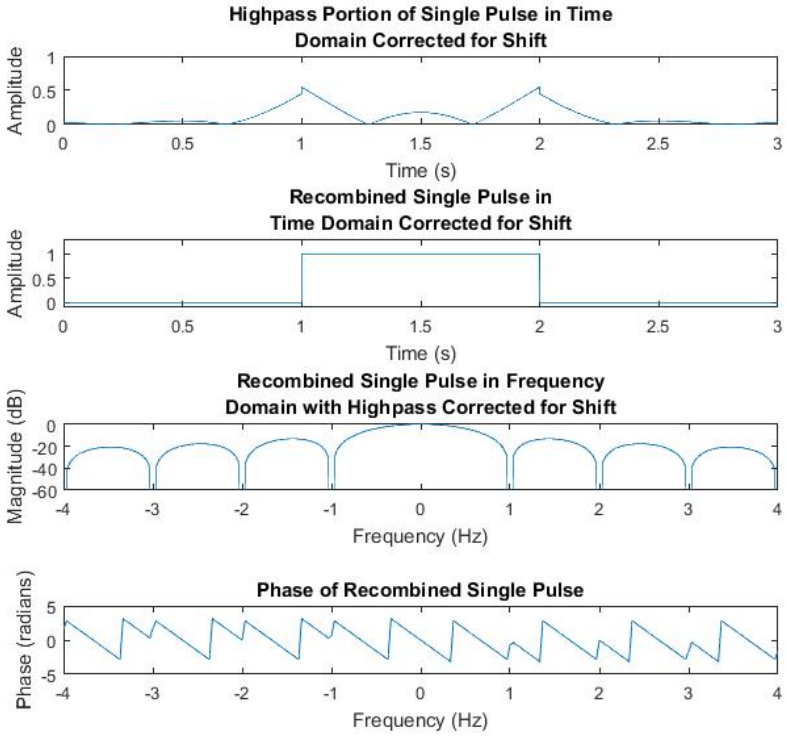

Figure 4.6. Reconstruction of signal using highpass signal with phase correction from cross-correlation. First plot is highpass signal with phase offset corrected by cross-correlation approximation, second plot is reconstructed signal using corrected highpass, third plot is frequency domain spectrum of reconstructed signal and fourth plot is the phase.

domain of the overlapped portions of the lowpass and highpass signals in the frequency domain. The cross-correlation approach provides more accurate results in the presence of AWGN. For this reason, most of the phase slope approximation results are omitted from this report. Figure 4.6 contains the reconstructed signal using the cross-correlation approximation approach. When comparing Figures 4.5 and 4.6, one can observe the square pulse now has the correct shape and the phase response is closer to that of the original signal. The effect the injected phase offset has on the phase of the reconstructed signal is highlighted in Figure 4.7. By examining Figure 4.7 it is evident that the cross-correlation approximation approach provides a better estimation to correct for the phase offset that was injected into the original signal.

The results of the next step in the simulations (1 ns pulse of random noise) produce similar results to that of the previous step (1 ns square pulse). The cross-correlation approximation approach is still more reliable than that of the phase slope approximation method. The phase offset correction results are also comparable to that of the previous simulation. This simulation ensures the random noise pulse does not have any effect on the ability to approximate the injected phase offset and correct for that phase offset. As shown in Figure 4.8, the phase offset approximation technique struggles to estimate the phase offset accurately, but the cross-correlation approximation technique is still able to correct for the phase offset relatively well. The Monte-Carlo simulations provide some insight on how the Signal-to-Noise Ratio (SNR) can affect the accuracy of the cross-correlation approximation approach as shown in Figure 4.9. From the results, it is clear that as the SNR decreases, the accuracy of the approximation technique begins to degrade at what appears to be an exponential rate.

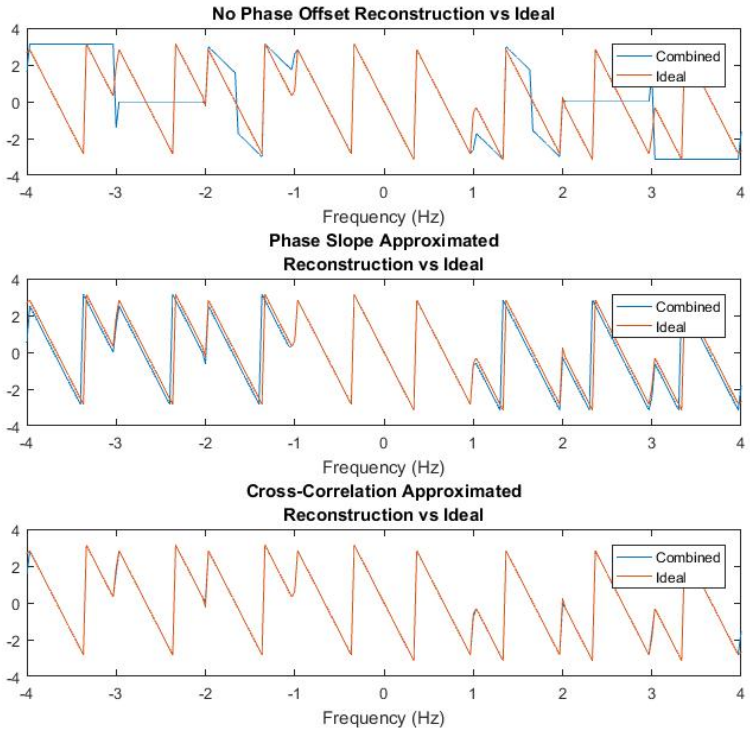

Figure 4.7. Phase offset comparison for the 1ns square pulse with no phase offset correction (top), phase offset corrected with phase slope approximation (middle), and phase offset corrected with cross-correlation approximation (bottom).

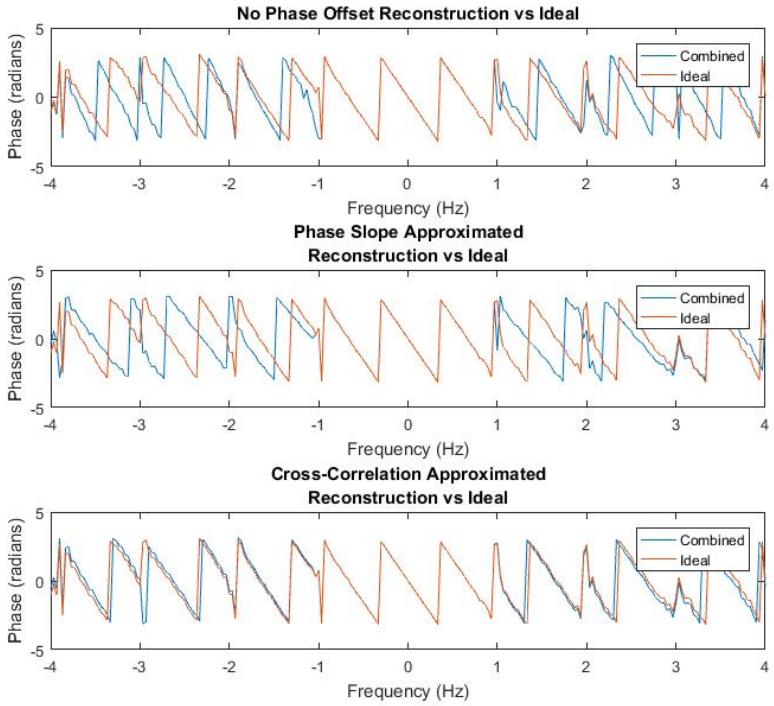

Figure 4.8. Phase offset comparison for the 1ns random noise pulse with AWGN and no phase offset correction (top), phase offset corrected with phase slope approximation (middle), and phase offset corrected with cross-correlation approximation (bottom).

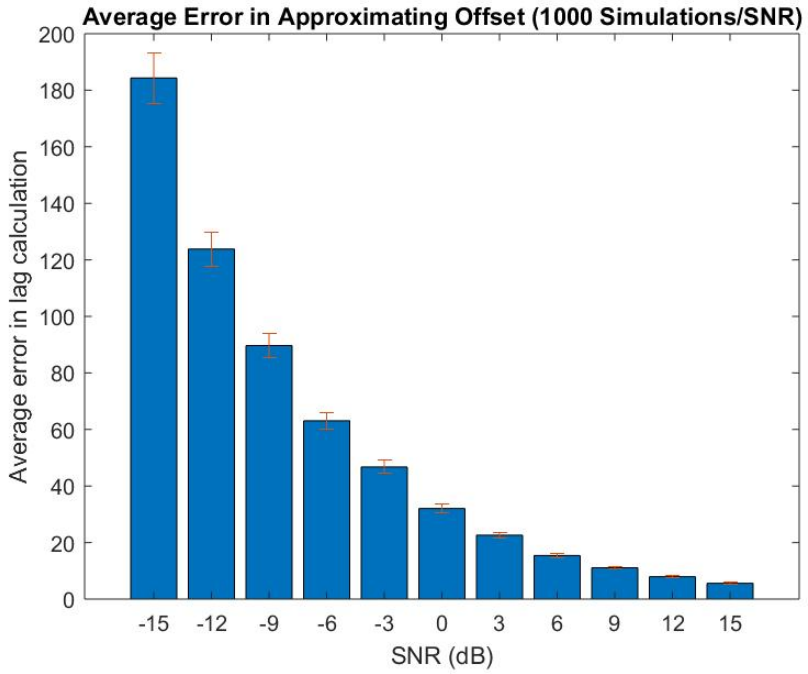

Figure 4.9. Monte Carlo simulation results for estimating the injected phase offset value with 95% confidence interval.

4.2.2 Gaussian Burst.

To prove the instantaneous bandwidth expansion method works with a variety of signals and confirm the results of the previous simulations, a Gaussian burst simulation is conducted as described in chapter 3. An attempt to stitch the two bandwidths together without any phase offset correction is taken. As shown in Figure 4.10, the combined frequency response contains errors in the form of frequency drop outs near the band edges of the high and low frequency sub-bands. By examining the constructed signal, it is clear that the lowpass and highpass portions are not time aligned. It is also evident that the phase offset has not been corrected when examining the phase plot in Figure 4.10. The results of this portion of the simulation confirm a phase offset correction needs to be applied prior to combining the sub-bands similar to the square pulse simulation results. To correct for the phase offset, a

cross-correlation between the overlapping portions of the signals in the time domain is performed. In this case, the cross-correlation accurately estimates the time lag that was injected. A time lag correction is applied to the highpass portion in the time domain to synchronize the two portions and eliminate the phase offset (2.4). Once the phase offset is corrected, the two sub-band spectrums are concatenated to form the complete spectrum. Figure 4.11 demonstrates this correction procedure results in the proper Gaussian pulse, frequency response, and phase response when compared with that of the original Gaussian pulse signal.

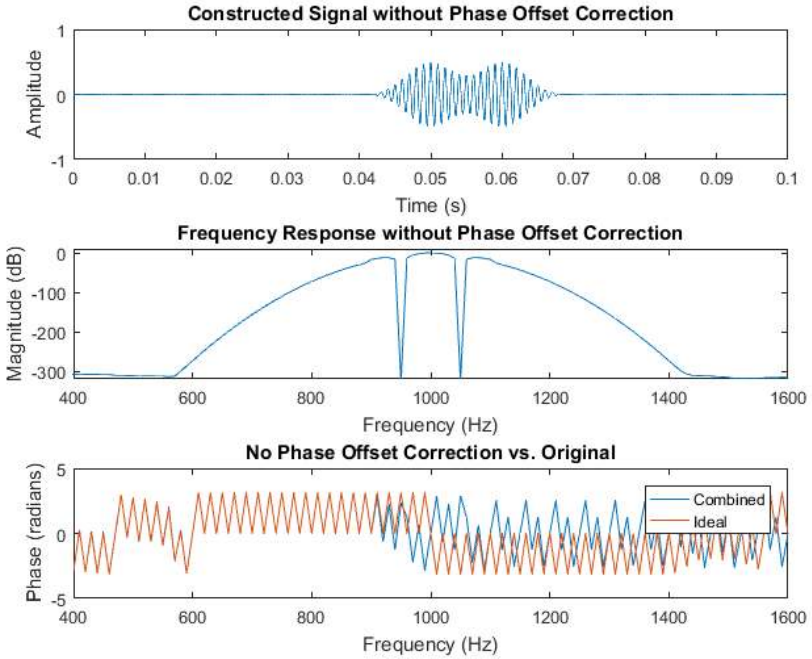

Figure 4.10. Constructed signal without any phase correction in the time domain (top), frequency response (middle), and a phase comparison of the constructed signal versus that of the original Gaussian pulse (bottom).

4.2.3 QPSK Simulation.

For the QPSK simulation described in chapter 3, the collected signals, after applying the lowpass and highpass filters, are shown in Figure 4.12. A smoothing filter

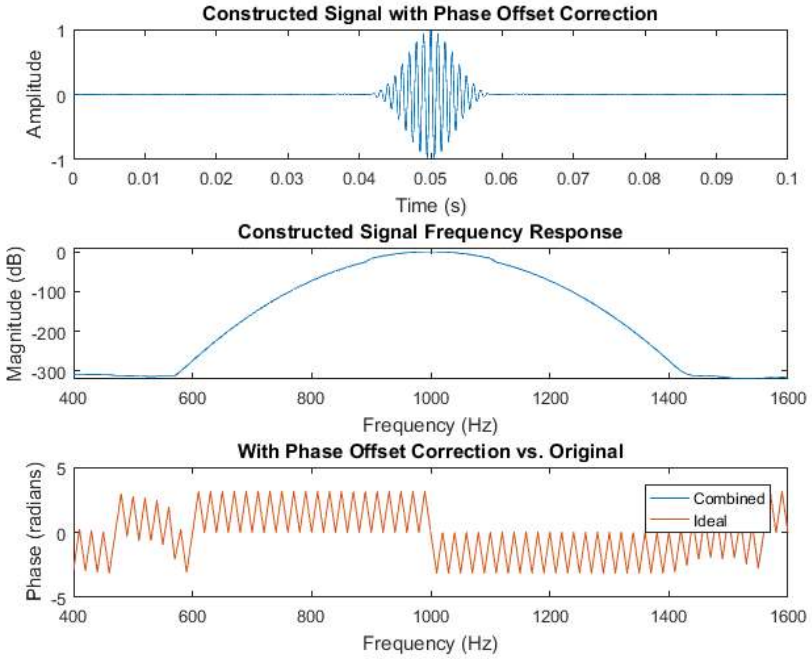

Figure 4.11. Constructed signal with phase correction in the time domain (top), frequency response (middle), and a phase comparison of the constructed signal versus that of the original Gaussian pulse (bottom).

is used to set the bandwidth at -20 dB of each signal. This threshold is chosen due to the amount of noise in the signal, the signal bandwidth, and the rolloff of the Butterworth filters used. Since this threshold is only being used to highlight the bandwidth before and after the combination, any arbitrary threshold could have been used.

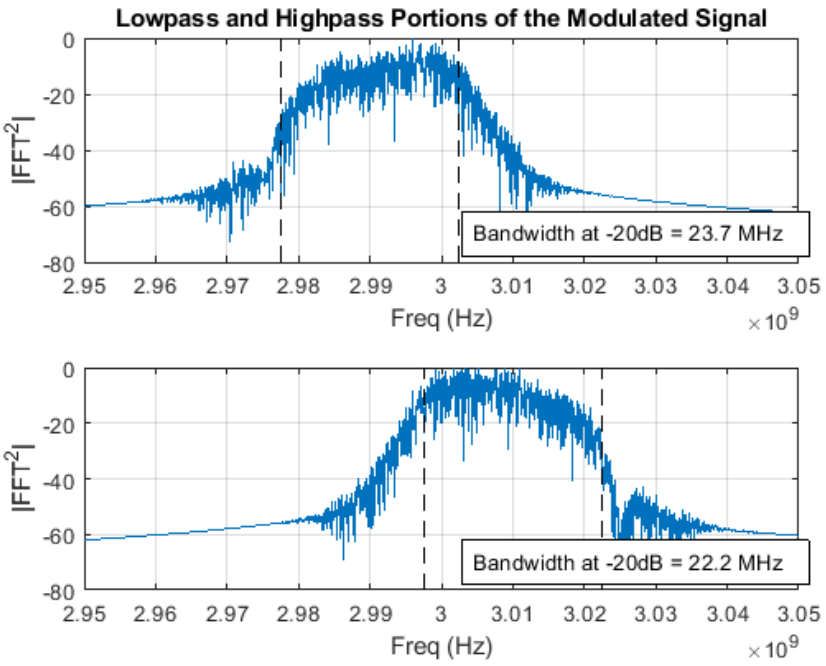

Figure 4.12. Lowpass filtered (top) and highpass filtered (bottom) portions of the modulated QPSK signal.

To correct for the phase offset in the frequency domain, the results from the cross-correlation are applied through the use of a time shift (2.4) similar to the Gaussian pulse simulation. For this simulation, two combination approaches are examined: combining the portions without any phase offset correction and combining the portions with a phase offset correction applied. Bit error calculations are conducted on both cases to determine the effect, if any, on the bit recovery. The results of the simulation verify bit errors will occur if the phase offset is not corrected prior to combining them. If the phase offset correction is applied before combining the two portions, it

results in zero bit errors, confirming the proposed solution is effective. Figure 4.13 highlights the difference between the phase of the original modulated signal and that of the combined signal with and without the application of the phase offset correction. Figure 4.13 demonstrates the need for a phase offset correction prior to applying any bandwidth expansion techniques unless significant phase distortion is desired.

Figure 4.14 contains a visual comparison of the original modulated QPSK signal with the result of the combination of lowpass and highpass portions with phase offset correction applied. As observed in Figure 4.14, the constructed signals bandwidth is slightly less than that of the original signal just past the filter cutoffs. This slight decrease in bandwidth is expected due to the rolloff characteristics of the Butterworth filters. But when comparing with the overall bandwidth of lowpass and highpass portions at -20 dB, it is practically what is expected with a 20% overlap in frequency spectrum between the two filters. The combined bandwidth of the lowpass and highpass portions is 23.7 MHz and 22.2 MHz = 45.9 MHz. After subtracting the 20% overlap yields 36.72 MHz, which is effectively the measured bandwidth (36.7 MHz).

To demonstrate the improvement of utilizing two Software Defined Radios (SDRs) instead of a single SDR, a Monte Carlo simulation is conducted with 100 trials per scenario. The Monte Carlo simulation utilized the QPSK scenario but added a bandpass filter centered directly over the mainlobe in the frequency spectrum. All three filters were designed with a bandwidth of 25 MHz which is not enough bandwidth to capture the entire QPSK signal individually. The goal of the simulation is to demonstrate an increase in bit loss as the lowpass and highpass portions are gradually tuned closer together until they are completely overlapped. The filters start with no overlap at the -3 dB point and are gradually tuned until centered over the mainlobe, like that of the bandpass filter. The results of the simulation confirm an increase in bit loss as the filters approached the bandpass configuration. Figure 4.15 shows that with 0%

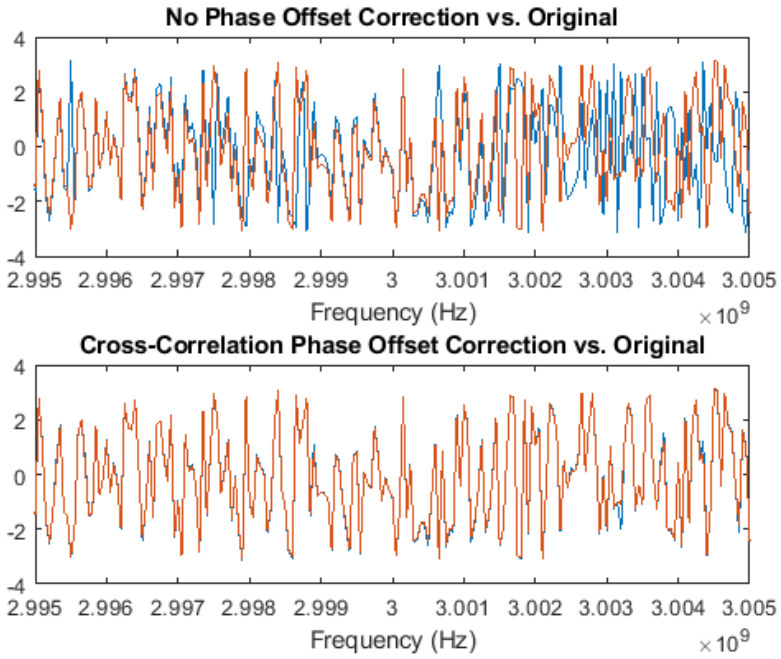

Figure 4.13. Phase comparison of the combined signal without any phase offset correction versus the original modulated QPSK signal (top) and the phase of the combined signal with phase offset correction versus the original modulated QPSK signal (bottom).

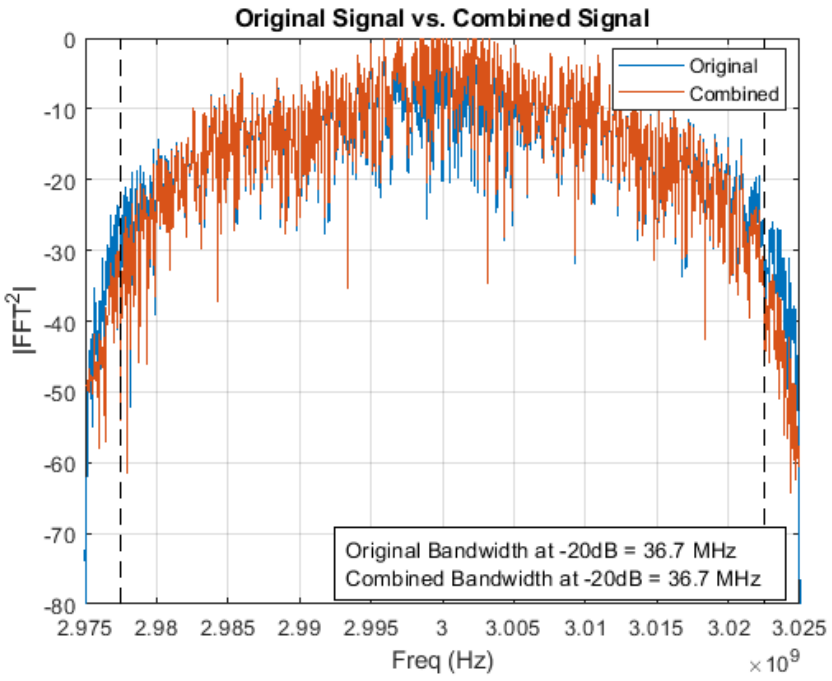

Figure 4.14. Original modulated QPSK signal versus the version constructed from the lowpass and highpass filtered portions.

overlap (50 MHz effective bandwidth) the simulations achieved the best results with nearly no bit loss compared to 100% overlap, where both the lowpass and highpass are acting as bandpass filters (25 MHz effective bandwidth), resulting in approximately the same results as the single bandpass SDR as expected. The slightly worse performance in the 70% to 100% range is believed to be from the relatively small number of trials conducted or possibly some distortion in the combined signal that occurs with significant bandwidth overlap while using the summation method. It is expected that the combined bit error rate will approach that of the bandpass SDR given a much larger number of simulations.

4.3 Antenna Classification with a Single SDR

For this portion of the research, the Stimulated Unintended Radiated Emissions (SURE) process is used to distinguish between 4 different recveiver antennas with only

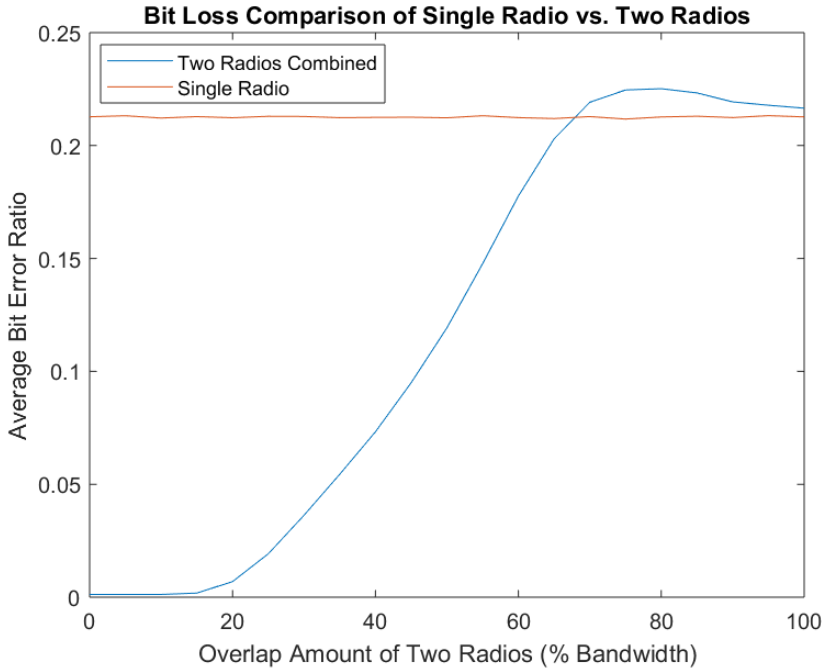

Figure 4.15. Bit loss ratio from a single radio centered over the mainlobe compared to the bit loss ratio of two radios combined at various percentages of overlap. 100 simulations were conducted with a 25 MHz bandwidth for each radio and SNR = 0.

using a single SDR as a receiver. Based on previous research mentioned in section 2.2, the SURE process may not be able to distinguish between two of the same antenna but may be able to distinguish between the different antenna types. Initially the results of the antenna classification using a single SDR are not very good (Figures 4.16 and 4.17). The SURE process is only achieving around 50% accuracy, but it is struggling to determine the difference between the Log-Periodic Antennas (LPAs) and the feed horns when classifies incorrectly. While analyzing these results, it is discovered that part of the neural net code within the SURE process uses the noise floor level of the collected signal, which is manually set in the Matlab code. The neural net uses the noise floor level to extract the portion of the signal above the noise floor level threshold to avoid any background noise from confusing the neural net. Initially the noise floor level was erroneously set at 0 dB, which caused the neural net to only use the upper portion of the impulse response which eliminates the beginning and end of the impulse response from being considered. Previous research highlights the transitions of the impulse response contain most of the distinguishing information to assist the neural net in deciding between the different classes [14]. So it makes sense that without that portion of the impulse response, the neural net will struggle to classify any of the different antennas correctly.

Once the issue with the noise floor level threshold was discovered, the noise floor value was set to -100 dB in the MATLAB® code ensuring the entire cross-correlation impulse response will be used for each of the collections. Since the signal used for the classification is the impulse response of the cross-correlation between the transmitted signal and the received signal, all of the information contained in the impulse response is desirable to help distinguish between the different antenna choices. Therefore it is perfectly acceptable to set the noise floor level to an extremely low level to ensure the entire impulse response is being utilized for classification. Once the noise floor level is

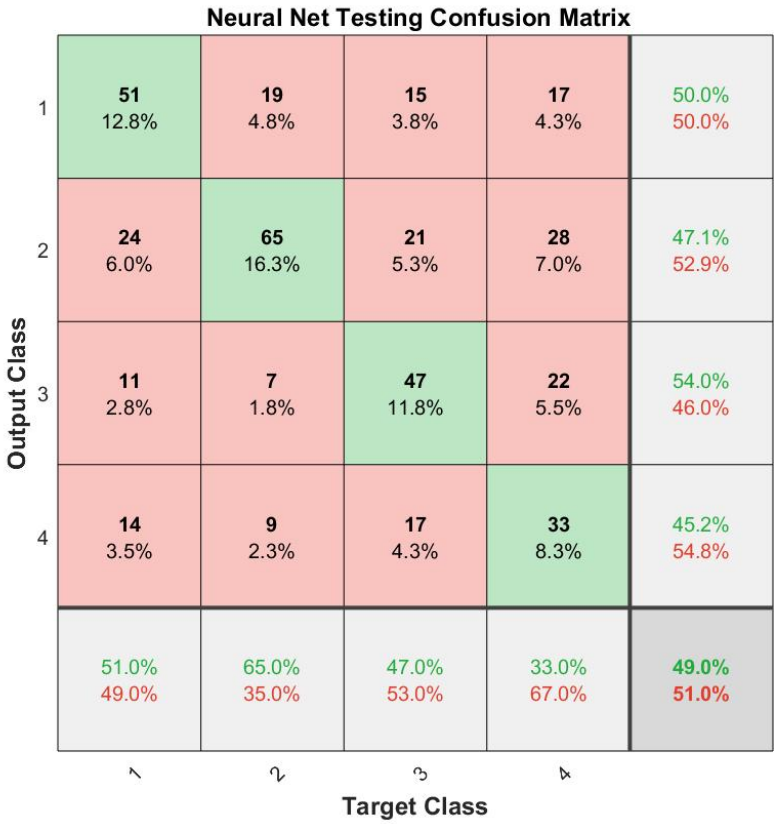

Figure 4.16. Confusion Matrix with Noise Floor at 0 dB

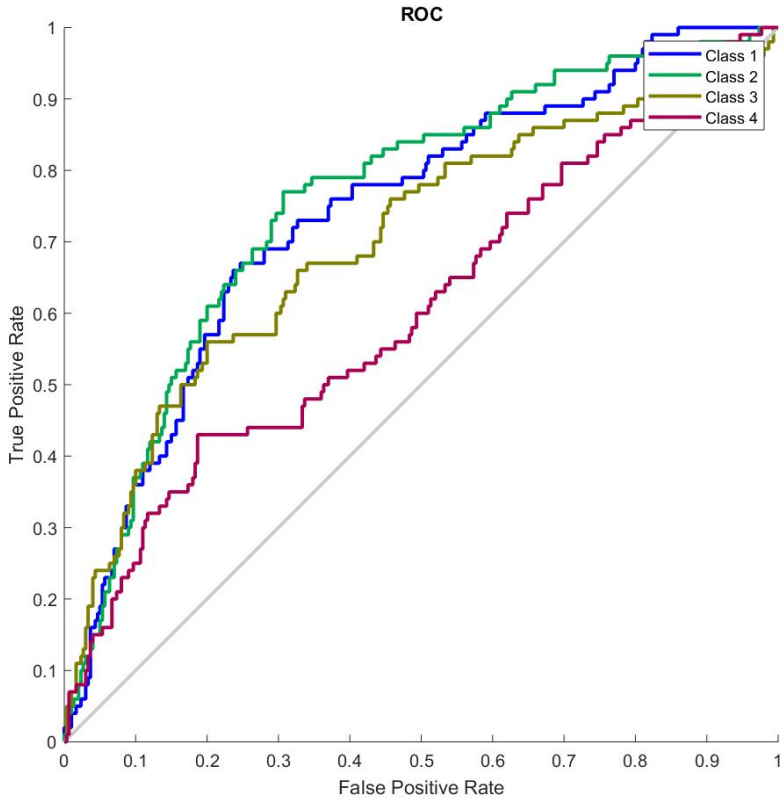

Figure 4.17. Receiver Operating Characteristic (ROC) Curve with Noise Floor at 0 dB

set at -100 dB, the neural net is much more successful at distinguishing between the different antenna types. Figures 4.18 and 4.19 show the results of the classification after the noise floor level setting is corrected. By comparing Figures 4.16 and 4.18, a remarkable improvement in classification is observed.

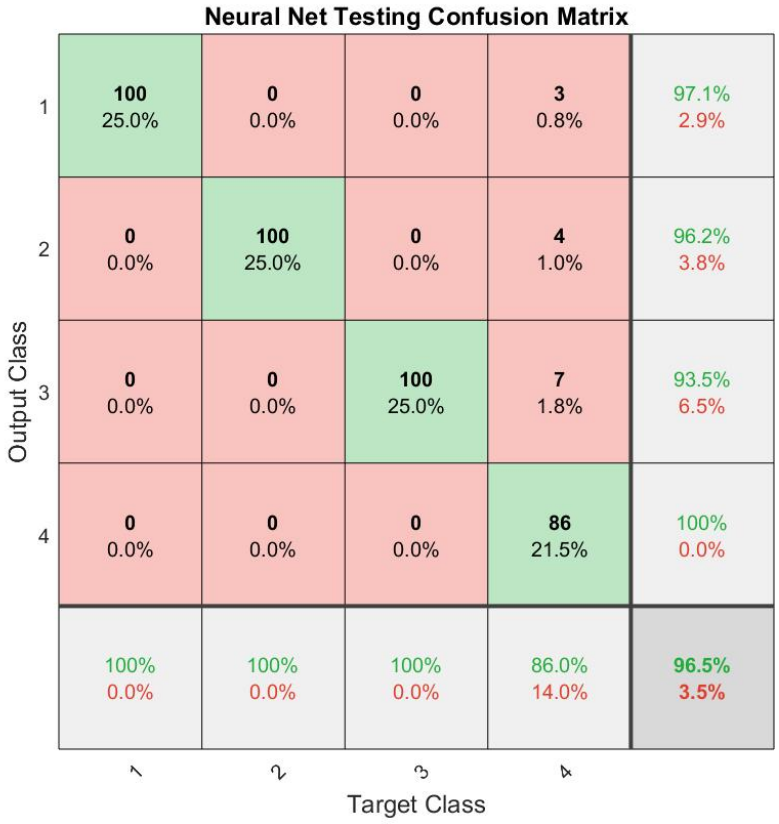

Figure 4.18. Confusion Matrix with Noise Floor at -100 dB

Given the different characteristics between the LPA and the feed horns, the Radio Frequency Distinct Native Attribute (RF-DNA) tools are expected to easily distinguish between the two types of antennas. The RF-DNA tools are expected to have more difficulty distinguishing between the two LPAs and between the two feed horns (which is what drove the selection of the four antennas). As shown in Figure 4.18, the neural net is able to classify both of the LPA antennas and the rectangular feed horn

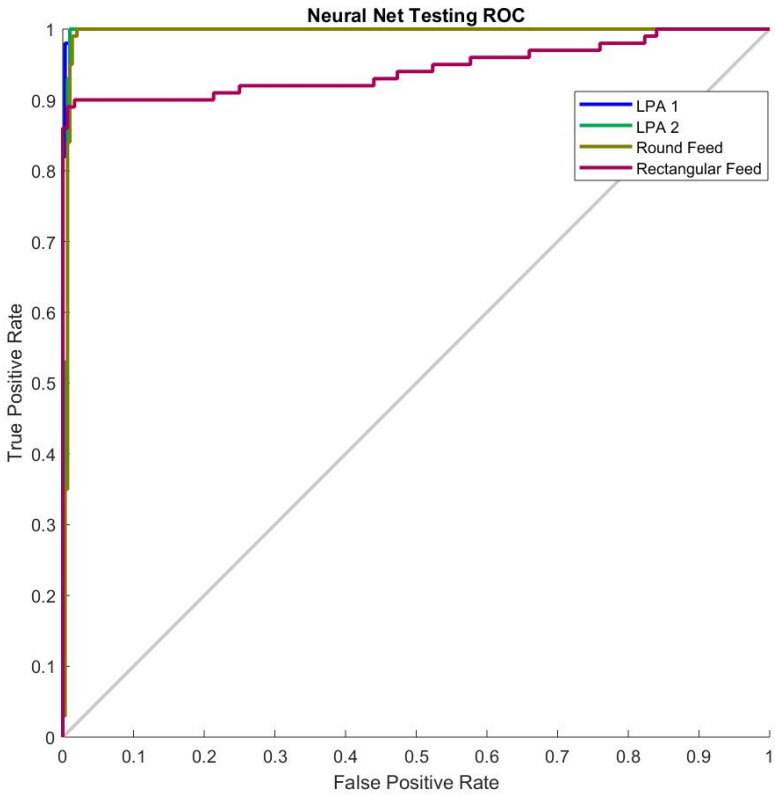

Figure 4.19. ROC Curve with Noise Floor at -100 dB

correctly 100% of the time. It is only slightly confused with classifying the round feed horn for some reason. It is surprising that the neural net is able to easily distinguish between the two LPA antennas. The results are somewhat concerning which warrants further investigation to determine why the SURE process is able to achieve those results. It is suspected that the two LPA antennas were at slightly different angles resulting in a stronger received signal for the neural net to cue in on, thus making the classification between the two easy.

To discern whether the angle of incidence of each antenna affected the results, the entire procedure is repeated with only two LPA antennas and a slight modification. The collection setup is slightly modified by collecting data on each LPA antenna at varying angles (Figure 4.20). A collection is taken at $-45, -30, -15, 15, 30$, and 45 degrees for each LPA. The various angles ensure the direction the antenna is facing will not be a factor in distinguishing one from the other. As shown in Figure 4.21, the neural net is not successful in distinguishing two LPAs and classified almost every collection as the first LPA. These results solidify the earlier belief that a slight difference in the angle of the two LPAs in the first data collection will provide enough of a discriminating factor for the neural net to easily classify them. Moving forward care will need to be exercised regarding the angle of incidence between the transmit and receive antennas. The results demonstrate that 20 MHz bandwidth is not enough for the SURE process to discriminate between the different antenna types which is expected based on previous research efforts. Collections using multiple SDRs is necessary to determine if this technique is successful with the SURE process.

4.4 Gaussian Burst using two SDRs

As described in section 3.4.1, a Gaussian burst is received with two SDRs. Figure 4.22 shows the distortion in the received signals from the lowpass and highpass

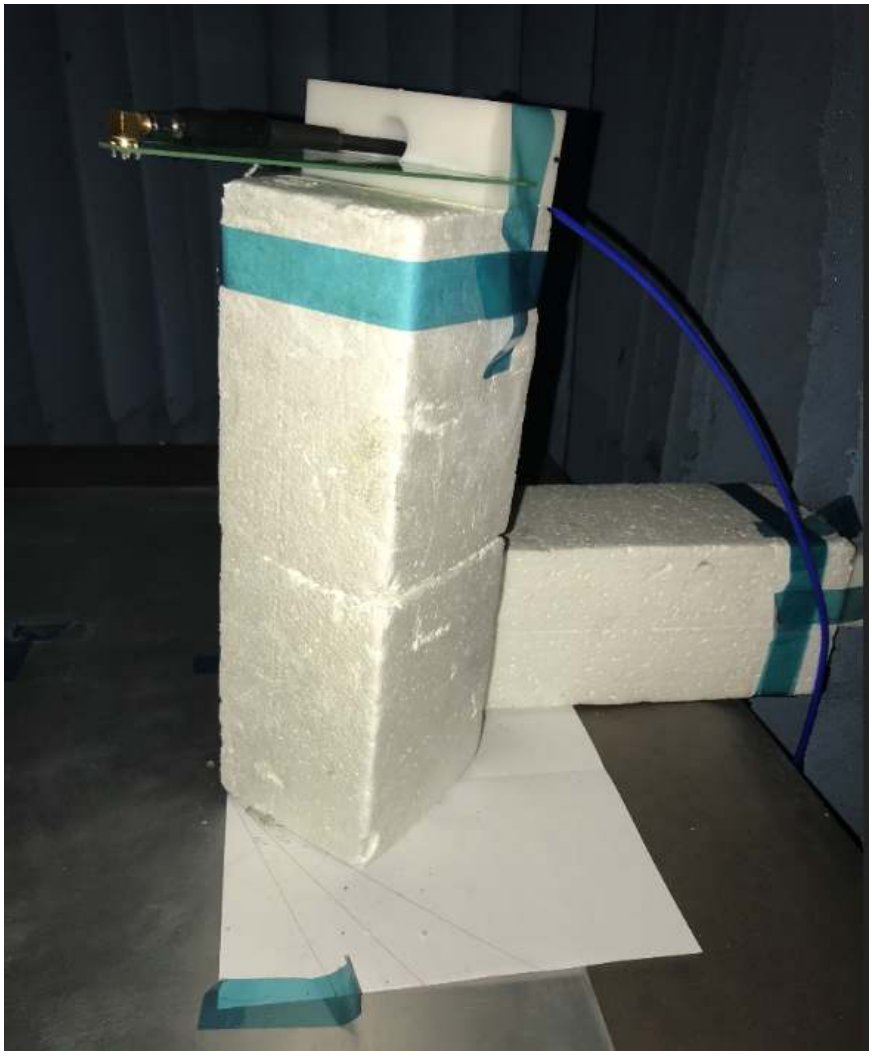

Figure 4.20. Collection Setup for Various Angles

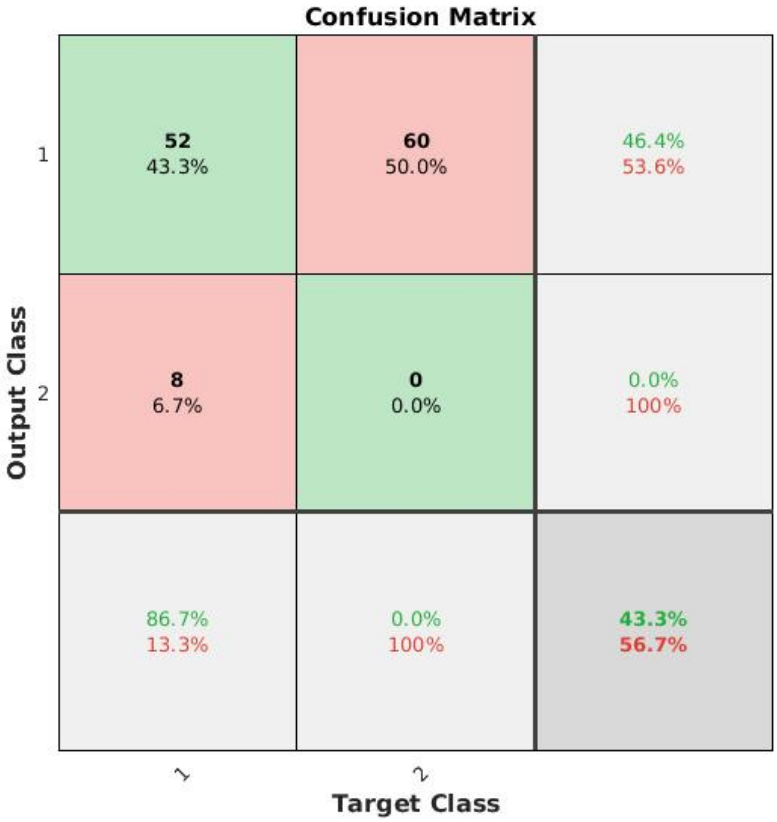

Figure 4.21. Testing Confusion Matrix of Various Angles

portions. The amplitude of each signal is reduced just like in the Gaussian pulse simulation (top plot of Figure 4.10). A slight overlap of the lowpass and highpass portions enables a cross-correlation in the time domain to correct for the phase offset as shown in the top portion of Figure 4.23. To simulate a single radio collection, like that of the bandpass filter in the simulations, a portion of the SDR collection is filtered as a 200 kHz bandpass to demonstrate that a single SDR is unable to collect enough bandwidth to capture the correct signal. The bottom half of Figure 4.23 shows the frequency spectrum of the bandpass filtered portion.

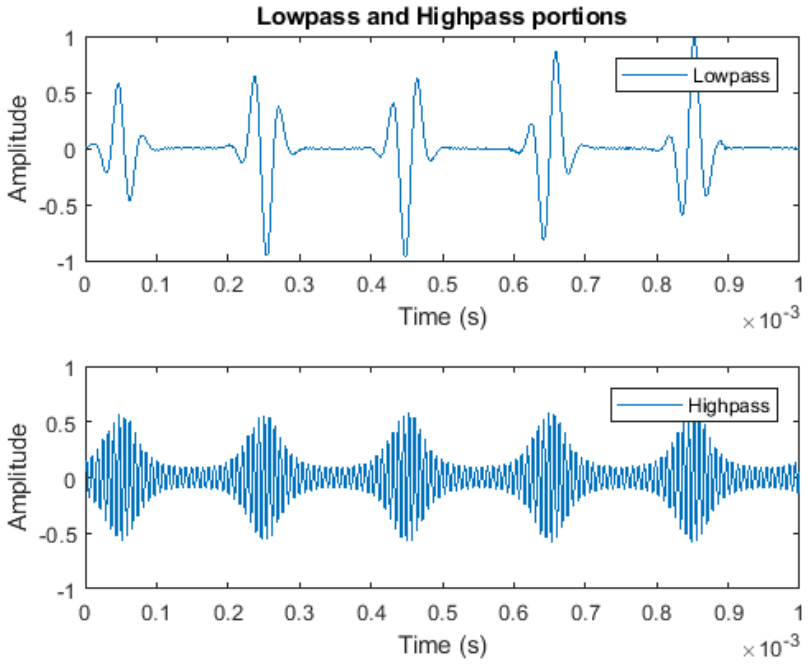

Figure 4.22. Five distorted Gaussian pulses from the lowpass filtered radio (top) and the highpass filtered radio (bottom).

One difference between the simulations and hardware testing involved the calculation of the exact center frequency of each SDR. With hardware, the collection is now prone to slight errors due to the small tuning difference between each SDR. This is easy to overcome through a cross-correlation of the overlapping frequency spectrum to properly align the collections in the frequency domain. This approach is similar

to previous techniques used for bandwidth expansion but does not require a known a priori signal to align the sub-bands. Once the frequency misalignment is corrected, the results confirm the proposed method is successful as shown in the top portion of Figure 4.24. The 200 μs period can be observed and the amplitude of the plot is normalized by the 1 MHz collection that collected the entire Gaussian burst as a reference. The peak of 1 to -1 demonstrates that the combined signal has the correct amplitude unlike that of each portion separately (Figure 4.22). Figure 4.24 also shows the signal distortion from the bandpass filtered signal proving that multiple sub-bands are required to capture the original signal. Again the results demonstrate that instantaneous bandwidth expansion is achievable using the cross-correlation approach.

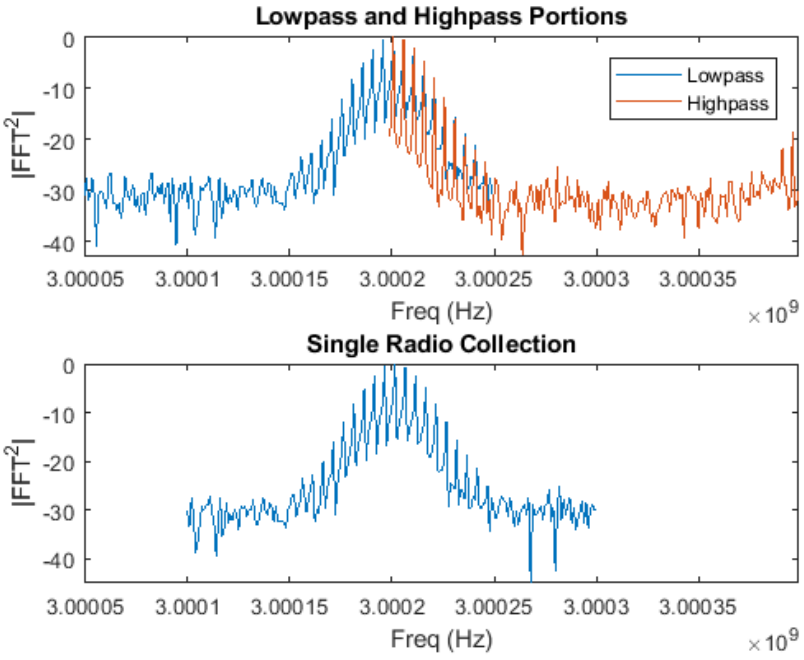

Figure 4.23. Spectrum of the stitched signal comprised of portions of the lowpass radio and highpass radio spectra each with a bandwidth of 200 kHz (top). Spectrum of a single radio collection (200 kHz) centered on the Gaussian spectrum (bottom).

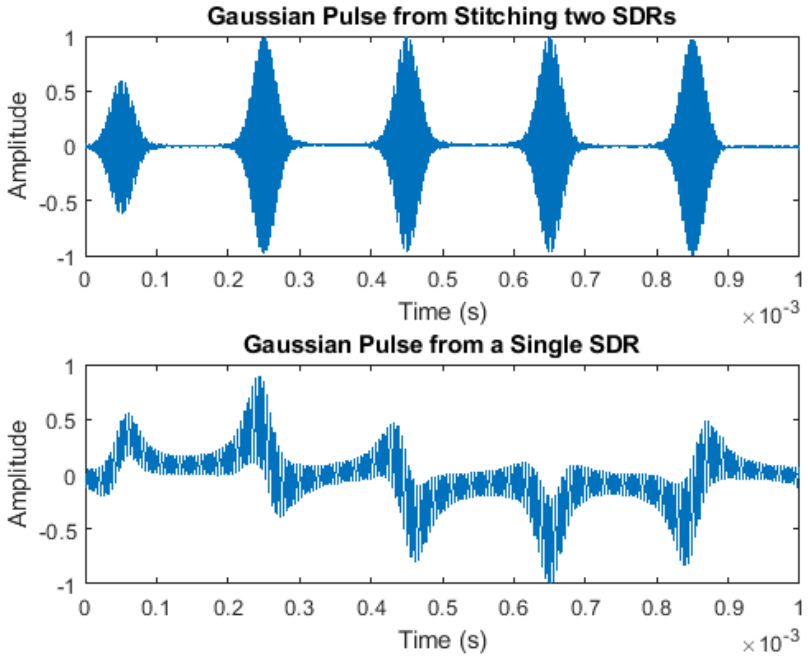

Figure 4.24. Time domain plots of the stitched signal containing the Gaussian pulses (top) and the single radio collection with the distorted Gaussian pulses (bottom).

4.5 QPSK using two SDRs

To quantify how effective the cross-correlation approach is, a QPSK signal is transmitted and received as outlined in section 3.4.2. The first test case examined is when $F_{s_T} = 8$ MHz and $F_{s_R} = 2$ MHz. Both of the receivers are tuned to collect at $TX_c = RX1_c = RX2_c = 3$ GHz (no offset). With this setup, each receiver should capture the entire QPSK signal. Following the process outlined in section 3.4.2, the receiver signals are interpolated by a factor of 4 to match F_{s_T}. Next the phase offset between the two collected signals is estimated through the use of a cross-correlation between the two. The cross-correlation response is shown in Figure 4.25. The peak of the correlation response is applied as a time shift to the $RX1$ signal to correct for the phase offset between the two collected signals.

Once the phase offset has been corrected, the next step would normally be to

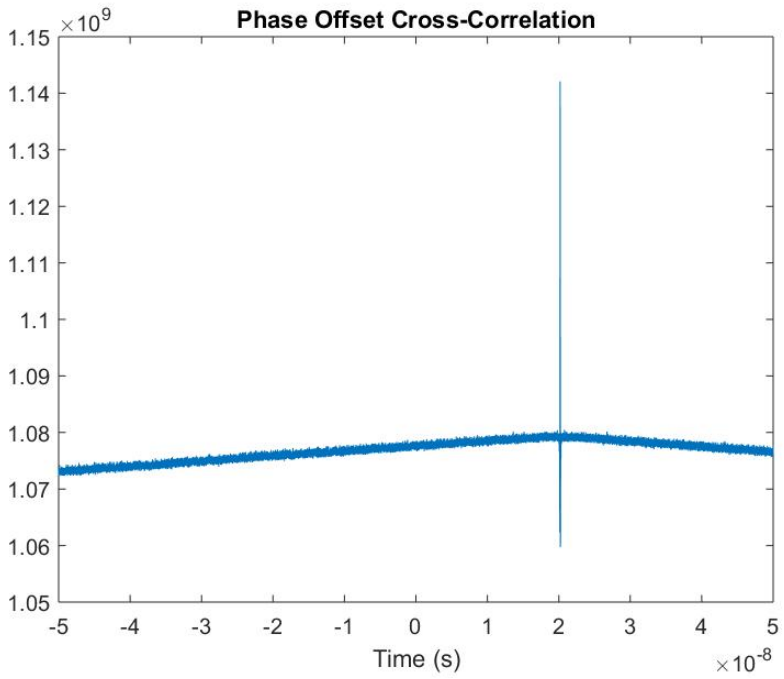

Figure 4.25. Cross-correlation response of receiver collections in the time domain to determine the phase offset between the two collections.

correct for the frequency offset that is applied to each of the receivers. However, in this test no offset was applied so this step is not necessary, but a correction for the slight tuning differences between the two receivers is. To correct for the small tuning difference, a cross-correlation of the two collected signals in the frequency domain provides the frequency difference between the two signals. This frequency difference is corrected by applying a frequency shift to one of the signals and aligning them. Figure 4.26 contains the correlation response.

Now that the phase offset has been corrected and the two collected signals are aligned in the frequency domain they are ready to be combined. In this case since there is no offset between the two receivers, the combination will not increase the instantaneous bandwidth and should perform the same as each individual receiver. Figure 4.27 shows the frequency spectrum of both receivers where the 2 MHz bandwidth can be observed. Figure 4.28 shows the frequency spectrum of the combined

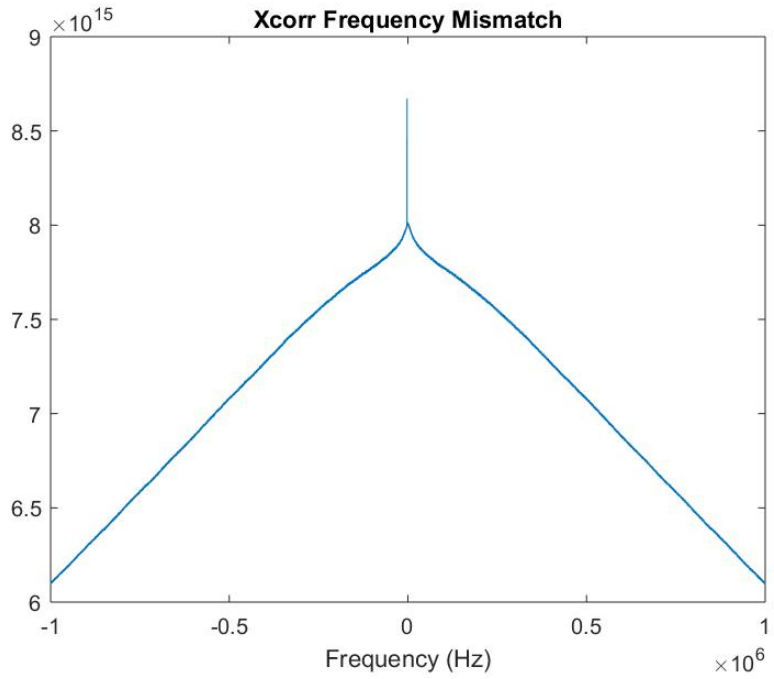

Figure 4.26. Cross-correlation response of receiver collections in the frequency domain to determine the frequency offset between the two collections.

signal after summing the two signals in the frequency domain. The DC term in the spectrum is due to some clock leakage into the TX port from the transmitter. This is common among cheaper radios which don't provide as much channel isolation as some more expensive radios do.

The final three steps are part of any QPSK demodulation. Since some frequency shifting is performed as part of the bandwidth expansion method, a frequency estimator is used to estimate where the center frequency of the combined signal is located. A frequency shift is then applied to correct for any slight tuning error in the transmitter. The portion of the combined signal containing the QPSK signal in the time domain is located and extracted. That portion is fed into a demodulator to decode the symbols, determine the phase of the QPSK signal and calculate a bit error rate. Figure 4.29 contains the decoded symbols prior to determining the phase of the signal. It is evident that the phase of the signal is unknown due to the rotation of the

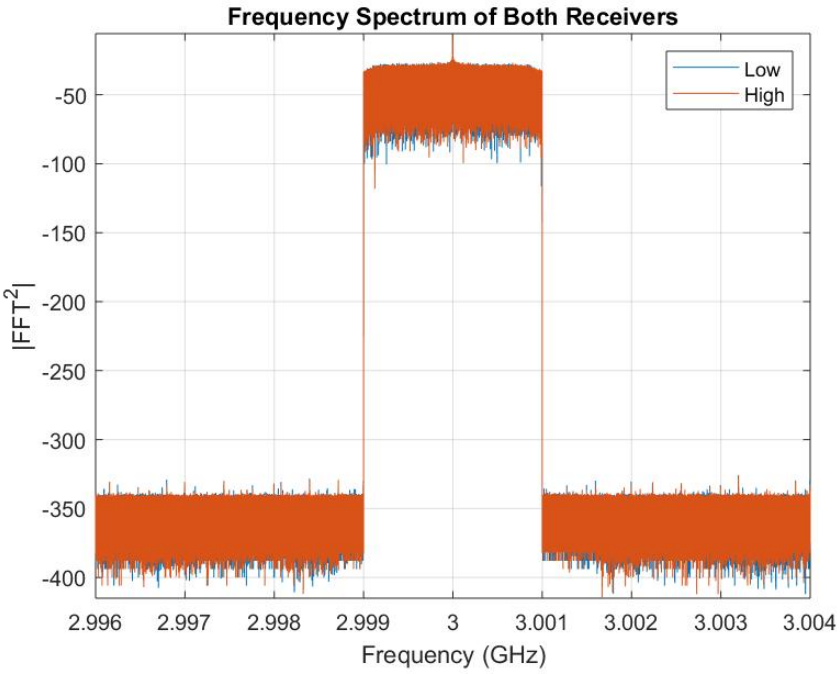

Figure 4.27. Frequency spectrum of two receivers centered at TX_c each collecting 2 MHz bandwidth.

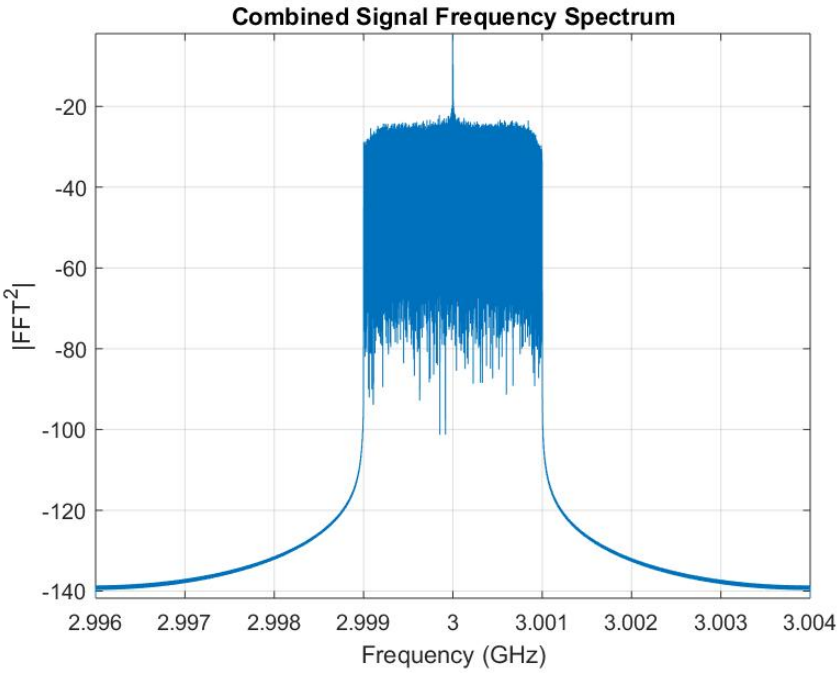

Figure 4.28. Frequency spectrum of the combined signal after summing the two receiver collections in the frequency domain.

symbols in the figure. Figure 4.30 shows the results after determining the phase of the signal and calculating bit error rates. By comparing Figures 4.29 and 4.30, the symbols are rotated once the phase of the signal is known and has been accounted for. This rotation ensures the bit error calculations are accurate. The diameter of the symbol groups (4 circles) is related to the SNR. The higher the SNR, the smaller the diameter will be and likewise a lower SNR will result in a larger diameter. Figure 4.30 confirms both predictions: $F_{s_T} = 2$ MHz is enough bandwidth to capture the entire QPSK signal and the combined signal does not improve the results since there is no increase in instantaneous bandwidth.

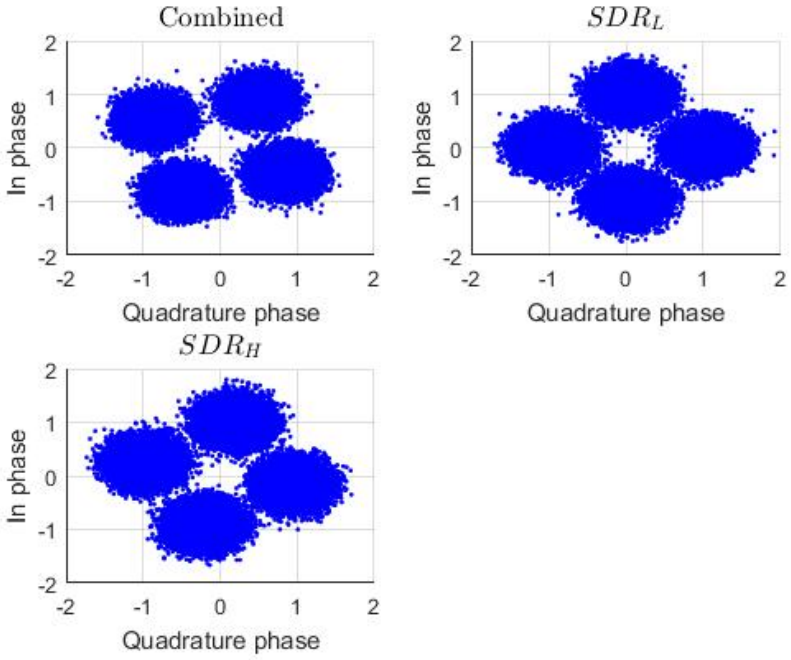

Figure 4.29. QPSK demodulation without phase correction for each of the three cases: combined collection, SDR_L receiver collection, and SDR_H receiver collection.

Since $F_{s_R} = 2$ MHz is successful at collecting the entire QPSK signal, a look at $F_{s_R} = 1$ MHz is warranted to prove it is not enough bandwidth to capture the entire QPSK signal. More data is collected exactly as before except with $F_{s_R} = 1$ MHz instead of 2 MHz. The expectation is each receiver will collect approximately half

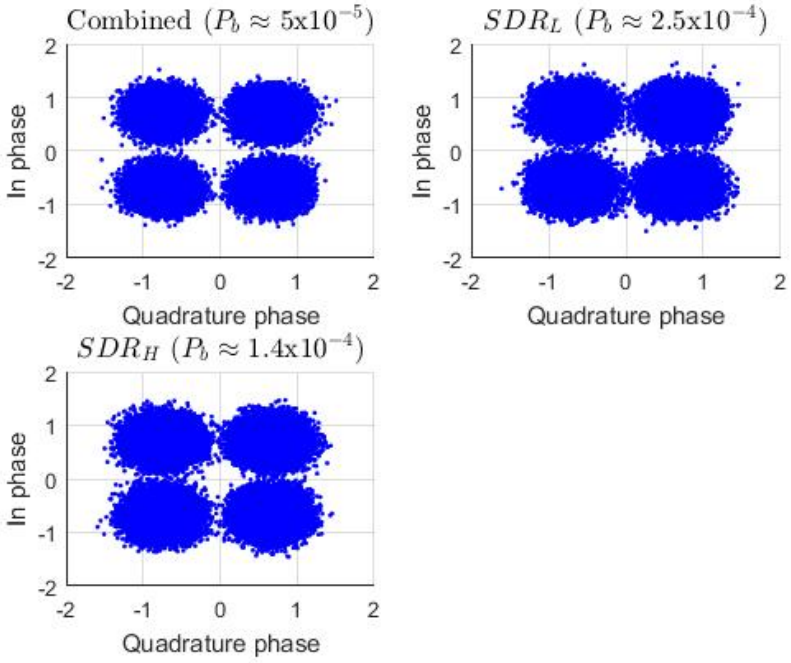

Figure 4.30. QPSK demodulation with phase correction along with P_b for each of the three cases: combined collection, SDR_L receiver collection, and SDR_H receiver collection.

of the QPSK signal and the combined signal will again result in no improvement since no frequency offset is used in the tuning of the two receivers. Figure 4.31 shows the frequency spectrum of the signals collected from both receivers. As shown, each receiver is collecting a 1 MHz bandwidth signal. The frequency spectrum of the combined signal is also 1 MHz as expected (Figure 4.32).

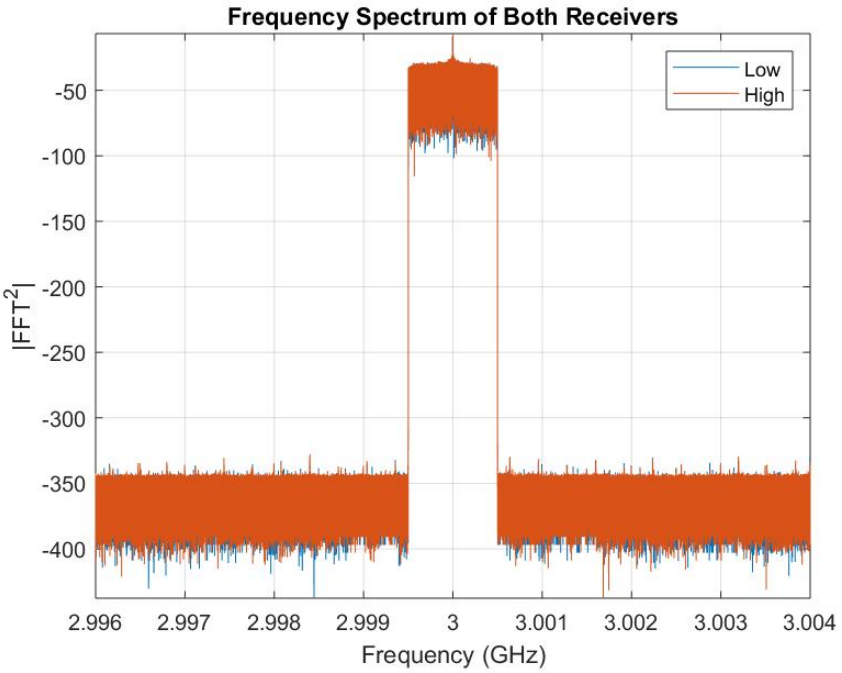

Figure 4.31. Frequency spectrum of two receivers centered at TX_c each collecting 1 MHz bandwidth.

The rest of the steps are applied and the QPSK symbols are again decoded. Figure 4.33 contains the final results of the collection. Each receiver results in $P_b \approx 2\text{x}10^{-1}$. With $P_b = 1/2$ being equal to that of a random guess, each receiver is demodulating just over half the bits correctly. These results match the prediction and prove that 1 MHz bandwidth is insufficient to collect the entire QPSK signal.

Now that the signal collection method is proven to require at least 2 MHz bandwidth to capture the entire QPSK signal, a new data collection is necessary to prove the proposed method to achieve instantaneous bandwidth expansion works. For the

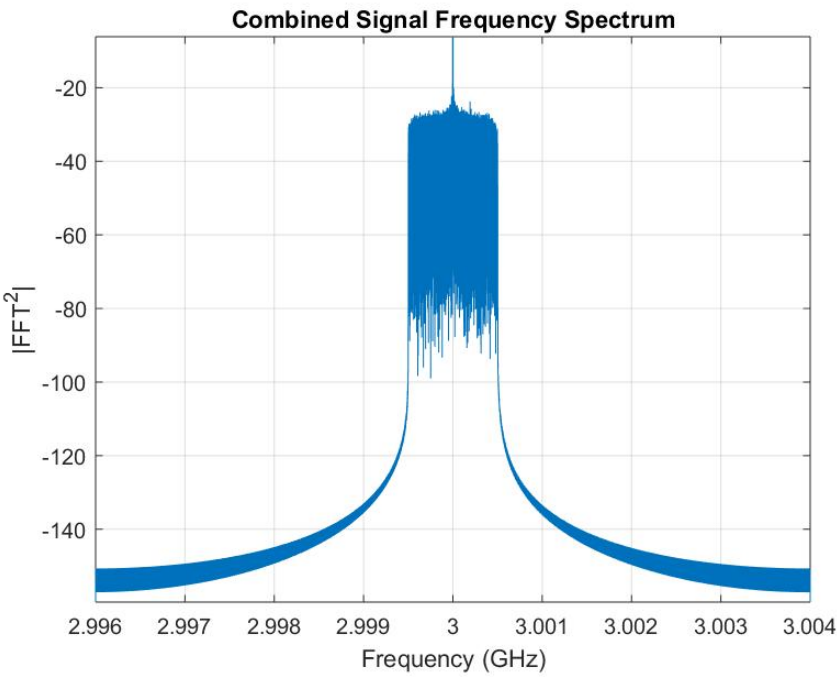

Figure 4.32. Frequency spectrum of the combined signal after summing the two receiver collections in the frequency domain.

final data collection each receiver is set to collect a 1 MHz bandwidth ($F_{s_R} = 1$ MHz) similar to the previous data collections. However for this collection each receiver is tuned 490 kHz off of TX_c. This results in $RX1_c = 3$ GHz - 490 kHz and $RX2_c = 3$ GHz + 490 kHz. This tuning will provide a 20 kHz overlap and a $BW_c = 1.98$ MHz after instantaneous bandwidth expansion. One can observe the frequency spectrums and see that after bandwidth expansion the combined signal would comprise nearly 2 MHz bandwidth in Figure 4.34. Figure 4.35 shows the frequency spectrum of the combined signal and demonstrates BW_c is nearly 2 MHz.

The results of the instantaneous bandwidth expansion can be observed in Figure 4.36. The combined signal results in $P_b = 0.02\%$ which is what the previous test achieved using a 2 MHz bandwidth centered at TX_c. The QPSK demodulation is not successful with either RX1 or RX2 by themselves since it is unable to estimate the center frequency of each signal. However, when the two bandwidths are combined

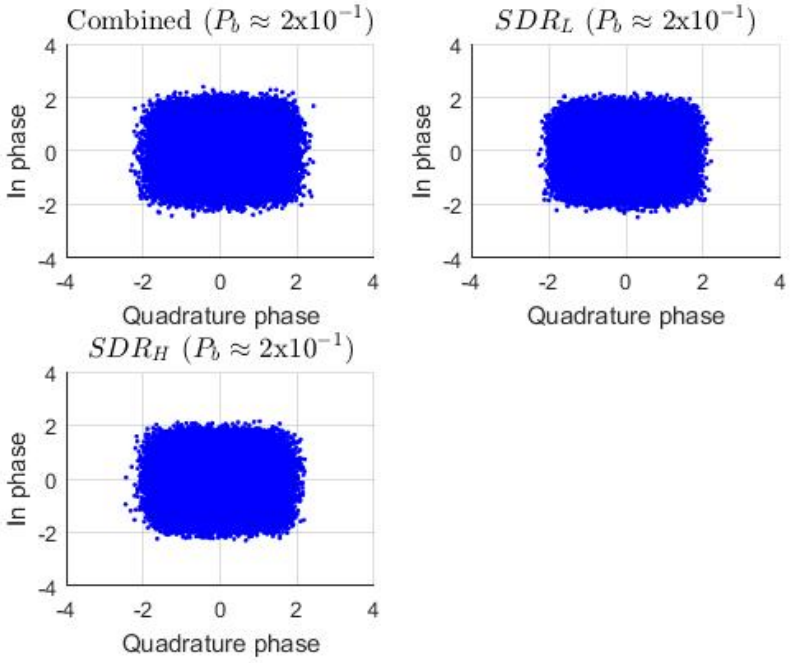

Figure 4.33. QPSK demodulation with phase correction along with P_b for each of the three cases: combined collection, SDR_L receiver collection, and SDR_H receiver collection.

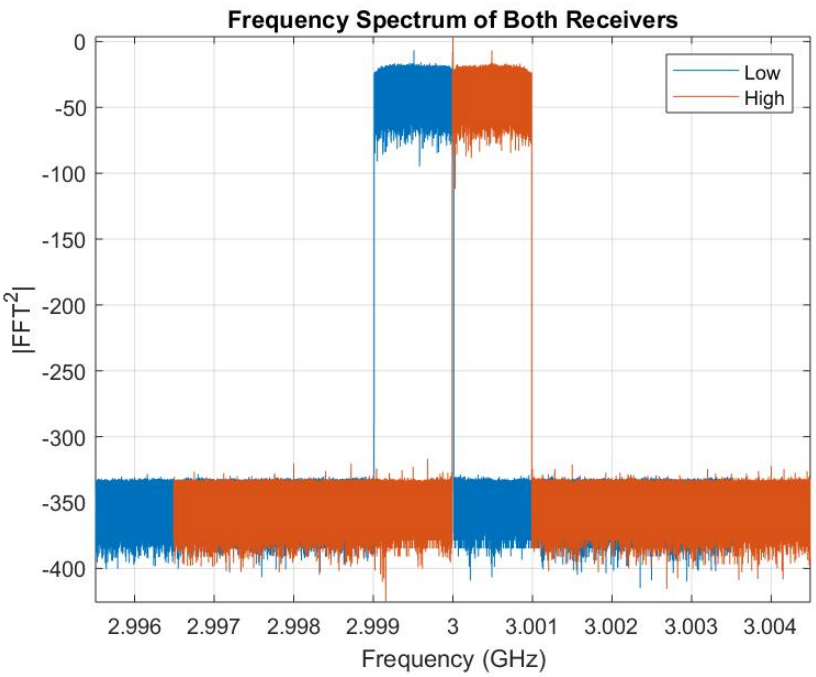

Figure 4.34. Frequency spectrum of two receivers offset from TX_c by 490 kHz each collecting 1 MHz bandwidth.

it is able to nearly decode all of the bits correctly. This confirms the instantaneous bandwidth expansion is successful at combining bandwidths while still preserving the data contained in the signal.

4.6 Summary

This chapter explored the relationship between signal bandwidth and correlation response and detailed the results of the bandwidth expansion simulations. The square pulse and Gaussian burst simulations demonstrated that the phase offset between the two signals needs to be corrected or distortion will occur in the combined signal. The QPSK simulation demonstrated the bandwidth expansion approach can be applied to a QPSK signal and can correctly combine the two signals without any data loss.

The hardware tests such as the antenna classification prove the Ettus Research B205 minis are capable of being used with the SURE process. It also demonstrates

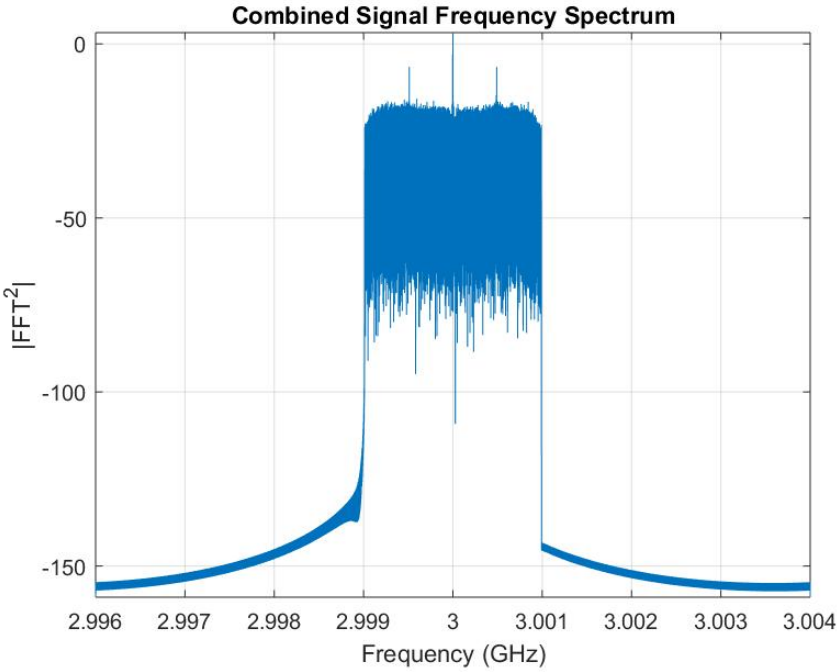

Figure 4.35. Frequency spectrum of the combined signal after summing the two receiver collections in the frequency domain. Each receiver has 1 MHz bandwidth with a 490 kHz offset between the two center frequencies.

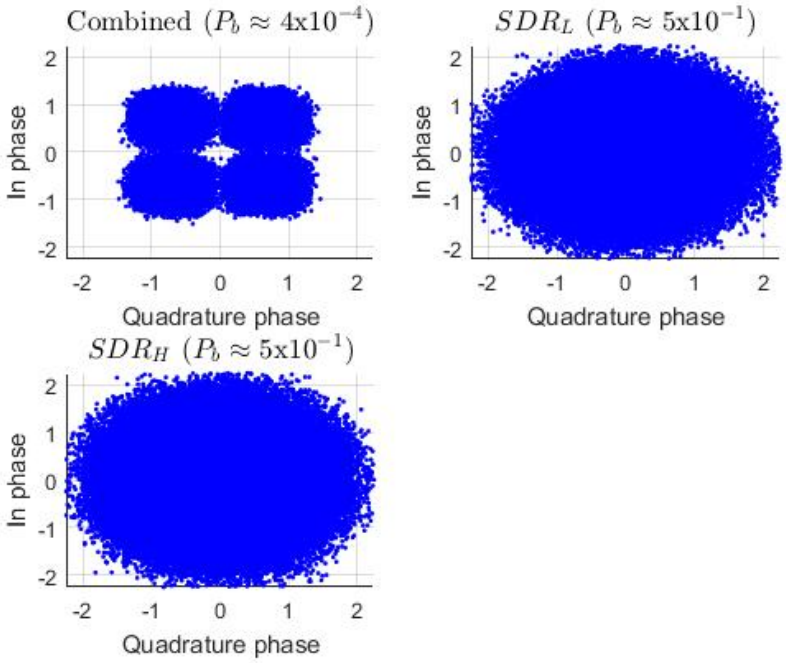

Figure 4.36. QPSK demodulation with phase correction along with P_b for each of the three cases: combined collection, SDR_L receiver collection, and SDR_H receiver collection. Each receiver has 1 MHz bandwidth with a 490 kHz offset between the two center frequencies.

the Ettus Research B205s do not have enough bandwidth to correctly distinguish between different antenna types. Lukacs was able to demonstrate good classification performance using the Air Force Institute of Technology (AFIT) Noise Radar Network (NoNET) which has around 500 MHz effective bandwidth [5]. If each B205 collects 50 MHz bandwidth, we would require around 11 B205s to successfully distinguish between the different antenna types.

The instantaneous bandwidth expansion efforts reinforced the simulation results. The Gaussian burst bandwidth expansion effort using hardware results in signal distortion similar to the simulation results if the phase offset is not corrected. The combination of two SDRs with the QPSK signal demonstrated that insufficient bandwidth in a single device can be overcome through the proposed instantaneous bandwidth expansion method while maintaining data integrity.

V. Conclusion

The Stimulated Unintended Radiated Emissions (SURE) process is an effective tool for distinguishing between devices (e.g. operational antenna vs. defective antenna) but requires large instantaneous bandwidth to be successful. Previous research has demonstrated the SURE process achieves increased performance as signal bandwidth increases. Previous applications of the SURE process utilized a relatively expensive, one of a kind piece of equipment that was designed specifically as a noise radar and is not very portable. These limitations create the desire to achieve the same results using smaller, cheaper, Commercial Off the Shelf (COTS) available technology. This research effort focused on the ability to use Ettus Research commercial Software Defined Radios (SDRs) to fill that role and demonstrates the ability to attain instantaneous bandwidth expansion using multiple SDRs. This is the first step to achieving the same SURE classification results with smaller, cheaper, COTS available technology by combining collections from two SDRs having individual bandwidths of 1 MHz. This chapter provides a review of the research goals and methodology, research contributions, and suggested areas of future research on this topic.

5.1 Research Goals and Methodology

The primary research goal was to determine whether the SURE process could be applied using smaller, cheaper, and commercially available SDRs. To determine that, the ability to combine multiple SDR collections to achieve an increase in instantaneous receiver bandwidth was crucial. This research began by laying out the foundation of bandwidth versus correlation response. Then simulations were conducted in Matrix Laboratory (MATLAB®) to demonstrate that two sub-bands could be combined without any signal distortion as long as the phase offset between the two sub-bands

was accounted for. Next simulations were completed using a Quadrature Phase Shift Keying (QPSK) signal to show no data loss would occur from the instantaneous bandwidth expansion.

To verify the simulation results and demonstrate that a single Ettus Research B205 mini could not collect enough bandwidth to distinguish between different antennas, hardware experiments were conducted. The single radio application of the SURE process proved that a single B205 mini was not suitable by itself to use the SURE process. The Gaussian burst experiment verified the simulation results and approach to correct the phase offset between the two sub-bands. The QPSK experiment demonstrated the instantaneous bandwidth expansion approach is effective at combining two sub-bands to achieve similar results to that of a single wider band collection.

5.2 Research Contribution

The results of this research effort demonstrate the ability to combine two sub-band SDR collections while correcting for any phase offset and frequency tuning differences between the two SDRs. This instantaneous bandwidth expansion method deviates from previous methods by not requiring the use of any known a priori signals and is suitable for applications that are non-Wide-Sense Stationary (WSS) such as the SURE process or data transmission applications. Through this work, we were able to demonstrate a 198% increase in bandwidth expansion over a single Ettus B205 SDR centered at 3 GHz using two Ettus B205 SDRs. This work resulted in first place at the IEEE APS/MTTS Graduate Poster Competition (Masters category) and has been submitted to the International Radar Conference 2019. This research represents the first step in using smaller, cheaper and COTS technology to replace expensive specially designed equipment in a wide range of applications.

5.3 Future Work

While this effort was able to successfully demonstrate instantaneous bandwidth expansion, there is much more work that could be done to move it forward. This section highlights suggested areas for future efforts regarding the SURE process.

5.3.1 Eliminate the TX_c Spike.

Many cheaper SDRs have some clock leakage into the TX port that is present in the transmitted signal and shows up as a spike at the TX_c. This spike could potentially make it easier for the cross-correlations to determine the phase offset and frequency mismatch between radios, but some transmitters may have more isolation which would not contain a spike. Any bandwidth combinations involving more than two SDRs will result in no spike from the transmitter in the overlap region. The transmit spike will instead be in the center of one of the receiver collections and will not be able to assist with the expansion process. Eliminate the transmit spike from the overlap region and determine if the bandwidth expansion process is still able to accurately estimate the phase offset and the frequency mismatch to combine the sub-bands. This will ensure the process is successful with any transmitted signal.

5.3.2 SURE Process with Multiple SDRs.

Apply the SURE process using multiple radios with increased bandwidths to determine if the results are successful. If duplicating this research effort, approximately 500 MHz bandwidth or roughly 11 B205s are recommended. This could be accomplished by attempting to duplicate previous research efforts such as classifying between different attenuators on an antenna which may require less bandwidth than classifying between antenna types. This will ensure the bandwidth expansion approach can achieve the same results.

5.3.3 Signal Processing Penalty.

As with most signal processing, there could be some penalty (i.e. signal degradation) using the bandwidth expansion approach used in this effort. Some of the signal processing techniques used could have degraded the Signal-to-Noise Ratio (SNR) of the resulting signal during the expansion effort. The current processing penalty is unknown and could be reducing the effectiveness of the current approach. Examine the processing penalty of the current bandwidth expansion approach and refine as necessary to reduce the processing penalty to improve results. The current process is capable of being run on a high-performance laptop. Could potentially look into more portable devices such as a raspberry pi or similar device.

5.3.4 Explore Bandwidth Overlap Requirements.

To correct for the frequency mismatch between radios, some bandwidth overlap is required, but the exact amount is unknown. Explore how much bandwidth overlap is required to achieve bandwidth expansion and examine the performance impact the amount of bandwidth overlap has. Whether or not the amount of overlap is dependent upon the wide-band waveform chosen could be examined as well. A metric such as P_b as a function of overlap (similar to figure 4.15) could be used to quantify the results. This information will assist in determining how many SDRs will be required to collect the desired overall bandwidth.

Bibliography

1. K. A. Remley, D. F. Williams, D. Schreurs, and M. Myslinski, "Measurement Bandwidth Extension using Multisine Signals: Propagation of Error," *IEEE Transactions on Microwave Theory and Techniques*, vol. 58, no. 2, pp. 458–467, 2010.

2. D. Wisell, D. Ronnow, and P. Händel, "A Technique to Extend the Bandwidth of an RF Power Amplifier Test Bed," *IEEE Transactions on Instrumentation and Measurement*, vol. 56, no. 4, pp. 1488–1494, 2007.

3. E. Zenteno, M. Isaksson, and P. Händel, "Pilot Tone Aided Measurements to Extend the Bandwidth of Radio Frequency Applications," *Measurement*, vol. 90, pp. 534–541, 2016.

4. M. W. Lukacs, A. J. Zeqolari, P. J. Collins, and M. A. Temple, "RF-DNA Fingerprinting for Antenna Classification," *Antennas and Wireless Propagation Letters, IEEE*, vol. 14, pp. 1455–1458, 2015.

5. M. Lukacs, P. Collins, and M. Temple, "Device Classification Performance Modeling using UWB Stimulated "RF-DNA" Fingerprinting," in *Radio Science Meeting (Joint with AP-S Symposium)*. IEEE, 2015, pp. 183–183.

6. J. H. McClellan, R. W. Schafer, and M. A. Yoder, *Signal processing first*. Pearson Education Upper Saddle River, NJ, 2003.

7. M. A. Richards, J. Scheer, W. A. Holm, and W. L. Melvin, *Principles of Modern Radar*. SciTech Publishing, 2010.

8. R. Ervin, M. Temple, A. Betances, and C. Talbot, "Detecting Insteon Home Automation Network Attacks Using a Software Defined Radio (SDR) Radio Fre-

quency Air Monitor," in *ICCWS 2018 13th International Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited, 2018, p. 200.

9. J. Rice, R. F. Mills, M. A. Temple, and J. D. Peterson, "Increased Ambiguity Resolution in Digital Radio Frequency Receivers," in *2015 IEEE International Conference on Microwaves, Communications, Antennas and Electronic Systems (COMCAS)*. IEEE, 2015, pp. 1–4.

10. B. W. Ramsey, B. E. Mullins, M. A. Temple, and M. R. Grimaila, "Wireless Intrusion Detection and Device Fingerprinting Through Preamble Manipulation," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 585–596, 2015.

11. T. Thayaparan, M. Daković, and L. Stanković, "Mutual Interference and Low Probability of Interception Capabilities of Noise Radar," *IET Radar, Sonar & Navigation*, vol. 2, no. 4, pp. 294–305, 2008.

12. M. Lukacs, P. Collins, and M. Temple, "Device Identification using Active Noise Interrogation and "RF-DNA" Fingerprinting for Non-Destructive Amplifier Acceptance Testing," in *2016 IEEE 17th Annual Wireless and Microwave Technology Conference (WAMICON)*, 2016, pp. 1–6.

13. M. Lukacs, M. Temple, and P. Collins, "Classification Performance using "RF-DNA" Fingerprinting of Ultra-Wideband Noise Waveforms," *Electronics Letters*, vol. 51, no. 10, pp. 787–789, 2015.

14. A. Paul, P. Collins, and M. Temple, "Nondestructive Evaluation of Radio Frequency Connector Continuity using Stimulated Emissions," *ASME Journal of*

Nondestructive Evaluation, Diagnostics and Prognostics of Engineering Systems, Feb 2019.

15. C. R. Anderson, S. Venkatesh, J. E. Ibrahim, R. M. Buehrer, and J. H. Reed, "Analysis and Implementation of a Time-Interleaved ADC Array for a Software-Defined UWB Receiver," *IEEE transactions on vehicular technology*, vol. 58, no. 8, pp. 4046–4063, 2009.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
21–03–2019	Master's Thesis	Sept 2017 — Mar 2019

4. TITLE AND SUBTITLE

Instantaneous Bandwidth Expansion Using Software Defined Radios

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Everett, Nicholas D, Capt, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-19-M-024

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Intentionally Left Blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Stimulated Unintended Radiated Emissions (SURE) process has proven capable of classifying a device (e.g. a loaded antenna) as either operational or defective. Currently, the SURE process utilizes a specialized noise radar which is bulky, expensive and not easily supported. With current technology advancements, Software Defined Radios (SDRs) have become more compact, more readily available and significantly cheaper. The research here examines whether multiple SDRs are able to replace the specialized Ultra-wideband noise radar used with the SURE process. The research specifically targets whether or not multiple SDR sub-band collections can be combined to form a wider band collection thereby achieving instantaneous bandwidth expansion. Simulations and hardware tests are conducted to verify the simulation results and prove the bandwidth expansion approach is successful. The results here demonstrate the ability to achieve instantaneous bandwidth expansion with the use of a cross-correlation approach to combine multiple sub-band collections into a single wider band collection without distortion or significant data loss.

15. SUBJECT TERMS

Instantaneous Bandwidth Expansion, Software Defined Radio, Stimulated Unintended Radiated Emissions

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Peter J. Collins, AFIT/ENG
U	U	U	UU	100	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636, x7256; peter.collins@afit.edu