November 2023

Analog Cancellation of a Known Remote Interference: Hardware Realization and Analysis

James M. Doty
University of Massachusetts Amherst

ANALOG CANCELLATION OF A KNOWN REMOTE INTERFERENCE: HARDWARE REALIZATION AND ANALYSIS

A Thesis Presented

by

JAMES M. DOTY

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL AND COMPUTER ENGINEERING

September 2023

Electrical and Computer Engineering

ANALOG CANCELLATION OF A KNOWN REMOTE INTERFERENCE: HARDWARE REALIZATION AND ANALYSIS

A Thesis Presented

by

JAMES M. DOTY

Approved as to style and content by:

Robert W. Jackson, Co-chair

Dennis L. Goeckel, Co-chair

Stephen Frasier, Member

Christopher V. Hollot, Department Head
Electrical and Computer Engineering

DEDICATION

To the smile that keeps my feet on the ground,

the smile that brought me into this world,

and the smile that left us too soon.

ACKNOWLEDGMENTS

It wouldn't be possible for this thesis to have existed without the guidance, support, and constant advice of my committee co-chairs and advisors, Professor Bob Jackson and Professor Dennis Goeckel. Time and time again, they were able to call upon their vast knowledge to point me in directions I would never have even known to explore. Along the way, they have taught me how to form good questions from any problem and seek out the best possible answers. I am thankful for the position I landed in because of the encouragement provided by these two every single week. For all of their hard work, I am beyond thankful. Along with them, I would also like to thank Professor Stephen Frasier for his willingness to serve on my thesis comittee.

I also would not be here without the love and support of my parents and older sister. They instilled in me the passion for knowledge and work ethic needed to be successful. Equally as important to my success is Miranda, who has put her own life on hold numerous times in support of me chasing this life-long goal. The multi-hour round trips she has made in her time off have provided me the focus and stability, both mental and emotional, needed to reach this finish line. I owe them all the utmost love and thanks.

Lastly, I would like thank all of the friends who have helped me get here. To Ali, thanks for the random walk and lunch conversations that have helped me over many hurdles in my own work. To Connor, Colin, Marcus, and Frank, I would never have made it through my years in Amherst without your love and support. Lastly, to Connor, Noah, Joe, and Izzy, the dedication of this group to actively support, entertain, and lift each other up through so many crazy events over the last two years is something I will never take for granted.

ABSTRACT

ANALOG CANCELLATION OF A KNOWN REMOTE INTERFERENCE: HARDWARE REALIZATION AND ANALYSIS

SEPTEMBER 2023

JAMES M. DOTY

B.S., UNIVERSITY OF MASSACHUSETTS AMHERST

M.S.E.C.E., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Robert W. Jackson and Professor Dennis L. Goeckel

The onset of quantum computing threatens commonly used schemes for information secrecy across wireless communication channels, particularly key-based data-level encryption. This calls for secrecy schemes that can provide everlasting secrecy resistant to increased computational power of an adversary. One novel physical layer scheme proposes that an intended receiver capable of performing analog cancellation of a known key-based interference would hold a significant advantage in recovering small underlying messages versus an eavesdropper performing cancellation after analog-to-digital conversion. This advantage holds even in the event that an eavesdropper can recover and use the original key in their digital cancellation. Inspired by this scheme, a flexible software-defined radio receiver design capable of maintaining analog cancellation ratios consistently over 40 dB, reaching up to and over 50 dB, is implemented in this thesis. Maintaining this analog cancellation requires very precise time-frequency synchronization along with accurate modeling and simulation of the

channel effects on the interference. The key sources of synchronization error preventing this test bed from achieving and maintaining perfect interference cancellation, sub-sample period timing errors and limited radio frequency stability, are explored for possible improvements.

To further prove robustness of the implemented secrecy scheme, the testbed is shown to operate with both phase-shift keying and frequency-modulated waveforms. Differences in the synchronization algorithm used for the two waveforms are highlighted. Interference cancellation performance is measured for increasing interference bandwidth and shown to decrease with such.

The implications this testbed has on security approaches based on intentional interference employed to confuse eavesdroppers is approached from the framework proposed in the motivating everlasting secrecy scheme. Using analog cancellation levels from the hardware testbed, it is calculated that secrecy rates up to 2.3 bits/symbol are gained by receivers (intended or not) performing interference cancellation in analog rather than on a digital signal processor.

Inspired by the positive gains in secrecy over systems not performing analog cancellation prior to signal reception, a novel secrecy scheme that focuses on the advantage an analog canceller holds in receiver amplifier compression is proposed here. The adversary amplifier is assumed to perform linear cancellation after the interference has passed through their nonlinear amplifier. This is accomplished by deriving the distribution of the interference residual after undergoing an inverse tangent transfer function and perfect linear cancellation. Parameters of this scheme are fit for the radios and cancellation ratios observed in the testbed, resulting in a secrecy gain of 0.95 bits/symbol. The model shows that larger message powers can still be kept secure for the achieved levels of cancellation, thus providing an even greater secrecy gain with increased message transmission power.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Figure **Page**

CHAPTER 1

INTRODUCTION

In the age of information exchange over wireless communication channels, there will always be a need for increased information security over wrongdoers attempting to steal information. In the standard system model, the three entities at play are referred to by Alice - the information source or transmitter, Bob - the intended recipient of Alice's information, and Eve - an adversary eavesdropper on the broadly described communication channel. The most commonly known method of information security is encryption, where Alice's information is transformed at a data level by some encryption key such that the transformation can be easily undone by a key-informed Bob, but an uniformed Eve would need to perform computational processing well beyond current capabilities to recover that same information. However, unless the system is able to bound Eve's computational power for breaking the transformation, Alice cannot guarantee that her information was actually kept secret from Eve [8] [2].

The study of how secretive and resilient a communication system can be is a crucial area of information theory [1]. Fathered by Claude Shannon, it puts forth strict requirements for what may be defined as information-theoretic secrecy. These requirements can be summarized as the information in a transmission being entirely secure from an eavesdropper with unlimited resources, including time, power, and computational abilities. As stated above, the most common form of information security, encryption, is not resilient against an eavesdropper with a significant computational advantage over Alice and Bob. This means that encryption is not information-theoretic secure, only conditionally secure.

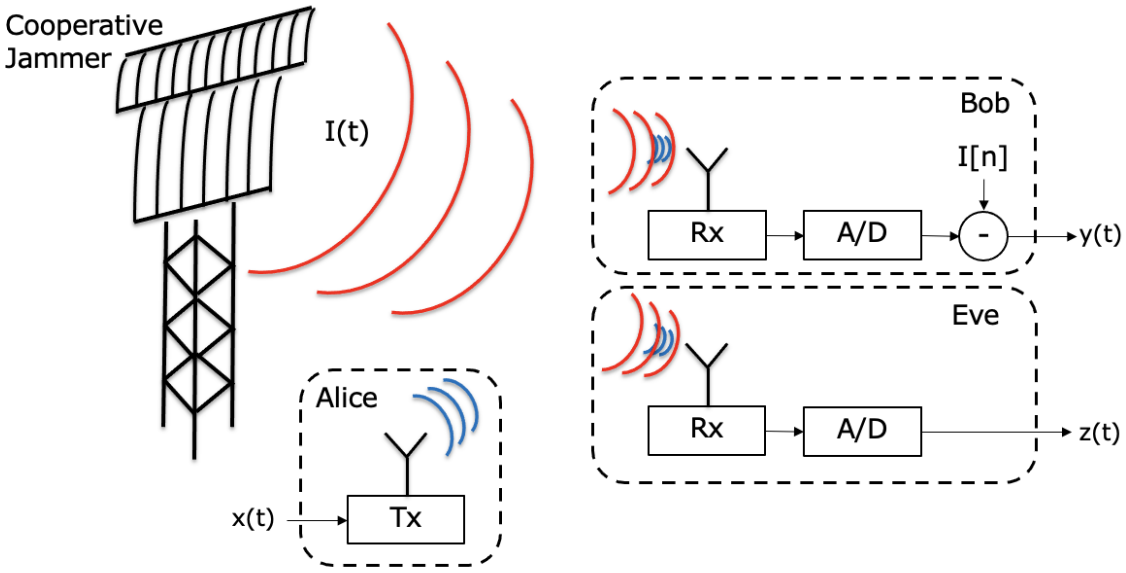


Figure 1.1: Block diagram of a standard cooperative jamming communication system.

Schemes that do provide information-theoretic secrecy over adversaries with unlimited resources have been extensively studied. Most notable is wiretap coding [9]. Unfortunately, the secrecy obtained through wiretap coding only holds under the assumption that the intended receiver, Bob, has some channel advantage, such as a higher received signal power, over the eavesdropper, Eve. This cannot be guaranteed for any practical system as the position of Eve is not bounded relative to Alice and Bob. If Eve is closer to Alice than Bob, i.e. closer to the information signal source, then Eve will actually have a channel advantage over Bob. This is commonly referred to as the "near Eve" scenario.

Physical layer security has been of significant interest in recent years to solve this issue at the signal level [10]. One proposed method of physical layer security, cooperative jamming (Figure 1.1), helps prevent Eve from ever hearing the message intended for Bob. This is accomplished by reducing the signal-to-noise (SNR) ratio of the channel as a whole (both Bob's and Eve's) by transmission of a large simultaneous interference. This interference is generated from a shared-key known by the

jammer and Bob, allowing Bob to exploit this knowledge to employ interference cancellation on their received signal prior to information recovery [11]. The powerful uncancelled interferer acts as an additional noise source in Eve's reception, masking the much smaller (lower power) information signal that they are attempting to recover. Performing reasonable cancellation of an intentionally-generated interferer at the intended receiver is a critical aspect of the aforementioned schemes. The greater the cancellation that Bob is able to maintain means a greater channel SNR advantage over Eve. This artificial gain in channel advantage held by Bob in the cooperative jamming scenario can be used to overcome the "near Eve" issue.

Interference cancellation encapsulates two distinct methodologies which can be used in isolation or conjunction. The first of the two, analog cancellation, often takes place at radio-frequency (RF) before downconversion and digitization by an analog-to-digital converter (ADC). Conversely, digital cancellation would occur in a discrete domain following conversion by an ADC. Work in known-interference cancellation for cooperative jamming has focused on architectures that employ digital cancellation, but full-duplex receiver research has shown various analog and hybrid analog/digital cancellation methods can work just as effectively [12]. Analog cancellation requires the additional step of interpolating and upconverting the generated cancellation signal to an analog carrier for RF cancellation, increasing complexity of the receiver design and adding an additional source of synchronization error.

Despite requiring a more complex receiver design, implementing cancellation before an ADC has significant advantages. It has been shown that the nonlinearity and finite resolution of an ADC - strict hardware limitations - can be taken advantage of by transmitting a message signal of interest (SoI) in the presence of much larger interference that is capable of saturating an eavesdropper's ADC. Forcing the eavesdropping ADC to operate at its full dynamic range leads to loss and distortion of lower energy received signals in the converter's digital output. This can also drive

a receiver's front-end amplifier into nonlinear operation, resulting in compression. Since compression is detrimental to any receiver, intended or not, on the cooperative jamming channel anyone who can prevent it via analog cancellation will have a significant. One way these advantages can be utilized is through design of the SoI such that it can be hidden by the interference and is entirely lost in the receiver's quantization noise. This non-invertible and thus permanent deformation of the digital reception provides everlasting secrecy even under the scenario in which an eavesdropper is able to obtain the interference sequence at a later time and utilize it with their digitized copy of the original transmission [2].

The work done in this thesis focuses on a practical implementation of such a secrecy scheme. Utilizing software-defined radios (SDRs), a hardware testbed supporting analog interference cancellation has been implemented. Signal processing methods used to achieve the necessary synchronization between interference and canceller will be described. Using this system, empirical results for cancellation ratios have been found for a binary phase-shift keying (BPSK) modulated interference and used to calculate applicable limits of everlasting secrecy rates theorized in [2]. In order to accommodate the necessity of a powerful transmitter for the interference source, dual use of an existing radar is suggested; therefore, differing synchronization methods and results will be presented for a frequency-modulated continuous-wave implementations as well. Lastly, the current theory for everlasting security will be expanded upon by considering the system model in which everlasting secrecy can be derived from the compression effects of an eavesdropper's receiver amplifier as it nears saturation due to the powerful incoming interference signal.

The contributions of this thesis are as follows.

- *SDR-based analog interference cancellation hardware testbed:* A receiver capable of performing over 40 dB of analog known-interference cancellation at RF was implemented using low-cost SDRs and external test equipment. The flexi-

bility of an SDR receiver is highlighted through the use of multiple interference waveforms.

- *Everlasting secrecy results for a practical realization:* This receiver was motivated by a previously developed theory for everlasting information-theoretic secrecy. It is based on analog cancellation of known interference prior to digitization. Using the cancellation results found here, realistic values for a system's secrecy rate are calculated that include hardware limitations in interference cancellation.

- *Improvements to existing cooperative jamming systems*: It is shown that secrecy can be achieved by an intended receiver performing analog cancellation of a large interferer prior to their receive amplifier, versus an eavesdropper performing cancellation later in the receiver chain with digital signal processing. Given that current cooperative jamming schemes often utilize digital cancellation after receiving and recording a signal, this provides a potential gain to any system performing interference cancellation after digitization if they were to instead perform their cancellation in the analog domain.

CHAPTER 2

BACKGROUND

2.1 Cryptographic Secrecy Systems

The type of secrecy systems most people will be familiar with is cryptographic secrecy. These systems will disguise their information or message, M, by performing some type of functional operation, T, upon it to transform it into something else. This function will be defined by a key, K, shared between the transmitter and intended receiver and will output the cryptogram E as defined in general below.

$$E = T_K M \tag{2.1}$$

The selection of this function T_K is critical. If an intended receiver hopes to have any chance of recovering the message itself, it must be possible to invert the transformation using the shared key. In a mathematical sense, this means that for the function T_K a unique inverse must exist such that $T_K T_K^{-1} = I$ where I is the identity matrix. This allows for the message recovery shown below.

$$M = T_K^{-1} E \tag{2.2}$$

In this definition from Shannon [1], it is assumed that an enemy cryptanalyst has knowledge of the type of transform being utilized, T_i, but not the particular shared key, K. This pessimistic assumption is used, because it must be assumed that eventually the enemy will figure out the workings of the cryptographic system. Therefore, the resiliency of a cryptographic secrecy system is only dependent on the

distribution of possible keys, with a large number of possibilities having uniform probability of use being the strongest.

2.2 Shared Key Exchange

In both the cryptographic secrecy system model as well as the cooperative jamming system, having shared information in the form of a key between Alice and Bob is crucial to developing an advantage over the adversary. While this key can simply be exchanged in some physical fashion prior to use, such as previous face-to-face communications, continued use of the same key increases the likelihood of the adversary figuring out the key and the secrecy system being broken. On the other hand, regularly having face-to-face communications to exchange new keys would defeat the purpose of wireless communication over distance. So the problem at hand is how can Alice and Bob develop a shared key over the wireless channel with an eavesdropper listening.

Luckily a number of solutions for this exist that involve nonlinear or assymetric operations. Examples include the Rivest–Shamir–Adleman (RSA) and Diffie-Hellman key systems [13, 14]. In this paper we suggest and will focus on the latter.

Diffie-Hellman works by the use of two separate sequences, a public key and a private key. Each Alice and Bob generate their own private key, A and B respectively, and use those keys in order to generate a public key, e^A and e^B. The two then will freely exchange the exponential based public keys with each other. This means that Eve now has access to the public keys as well. With that exchange, Alice and Bob agree to use the shared key e^{AB}. As shown in the equations below, Alice and Bob can generate this new key from the information they have and exponentiation, but Eve is required to compute a discrete logarithm in order to gain access to the same key. This process is computationally expensive for Eve to perform, meaning that while not secure against an adversary with unlimited time and computational power, regular

key exchanges between Alice and Bob can provide a shared key kept secret from Eve for the time it takes them to compute the logarithm.

$$\text{Alice: } (e^B)^A = e^{B*A} = e^{AB}$$

$$\text{Bob: } (e^A)^B = e^{A*B} = e^{AB}$$

$$\text{Eve: } e^{A*\ln e^B} = e^{AB}$$

2.3 Information-Theoretic Secrecy

Because of assumed computational limitations at Eve, most secrecy systems are not by definition theoretically secure, only conditionally. This is because they are susceptible to an adversary with unlimited resources. In order to be considered perfectly secret, information must not only be secure from the eavesdropper at the time of sharing, but also indefinitely from that point on. Shannon defines this as the notion that an adversary gains no advantage in trying to determine the secret message, M, from their intercepted signal, E. In other words, the eavesdropper on the channel receives no knowledge gain from listening to the cryptogram. Since an advanced adversary would be working with probabilities of the message content, information-theoretic secrecy can be summarized by Bayes Theorem.

$$P(M|E) = \frac{P(M)P(E|M)}{P(E)} \tag{2.3}$$

There exists two cases that meet the Bayes Theorem condition for perfect secrecy. The first of these is the trivial case in which $P(M) = 0$. This case is not actually valid since the message should have positive probability for any possible M. The only other case that meets this condition, therefore making it a necessary and sufficient condition for information-theoretic secrecy is:

$$P(E|M) = P(E) \tag{2.4}$$

For perfect secrecy this condition must hold for all messages and intercepted signals, M and E, respectively. This would mean E is independent of M. This independence, by definition, means an adversary who intercepts the signal E learns nothing about the probability of the message M, providing no advantage in identifying the original message over another adversary who did not intercept E.

In terms of keys, this condition can be summarized as the requirement that the total probabilities of any key defined transformation T_k transforming a message M_i into the cryptogram E, must also be the same as the total probabilities of all keys transforming a different message M_j into the same exact cryptogram E. This must be true for all possible combinations of messages M_i, M_j, and cryptograms E. For perfect secrecy to be achieved, $P(E|M) = P(E) \neq 0$ for any E or M. This leads to the condition that there must be as many possible cryptograms E as there are possible messages M, but the keys that relate each independent M to each independent E must be different. This means that for perfect secrecy from an eavesdropper who has noiseless access to the transmitted cryptogram, there needs to exist at least the same number of keys as number of possible messages, and that each of these keys need to map every message M in the set to a different one of the possible cryptograms E in the set. This can be easily visualized by Figure 2.1.

2.4 Entropy and Measuring Information

With the conditions of an information-theoretic secrecy achieving system established, an index of secrecy performance can now be defined. The amount of information needed to define (or the uncertainty in) a random or secret message M is measured by $H(M)$, the entropy of M. The definition for discrete-valued entropy is the following sum across all N possible messages, M_n. The greater the number of possible messages that exist, the larger the message's entropy will be as additional information would be needed to distinctly define every possibility.

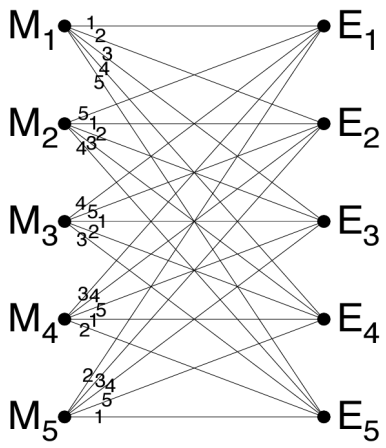


Figure 2.1: Relationship between message, cryptogram, and key sets in a perfectly secret system from [1].

$$H(M) = -\sum_{n=1}^{N} P(M_n) \log P(M_n) \tag{2.5}$$

Using conditional entropy, the amount of information about one random variable (the message or key) that is shared in having knowledge of another random variable (the cryptogram) can be calculated. This is known as equivocation. It can be defined based on the joint probability of all possible messages and cryptograms and the conditional probability of perfect secrecy for the message given a cryptogram. Both the equivocation of the message and key based upon knowledge of the cryptogram generated from them are of interest and are denoted by $H(M|E)$ and $H(k|E)$ respectively, where N is the total number of possible messages and L is the total number of cryptograms.

$$H(M|E) = -\sum_{n=1)}^{N} \sum_{l=1}^{L} P(M_n, E_l) \log P(M_n|E_l) \tag{2.6}$$

$$H(k|E) = -\sum_{n=1}^{N} \sum_{l=1}^{L} P(k_n, E_l) \log P(k_n|E_l) \tag{2.7}$$

These indexes describe the uncertainty (an unknown quantity of information) remaining in the message M assuming an adversary has received the exact cryptogram

E. This means that a larger equivocation relative to the entropy of the message designates a given variable that shares less information with the argument variable. That being said the inequality $H(M|E) \leq H(M)$ must always be true as it is not possible for one variable to share more information about a second variable than that second variable actually contains. Therefore for a cryptogram E that provides absolutely no information about the original message M, $H(M|E) = H(M)$.

2.5 The Wiretap Channel

Building upon the metrics defined by Shannon for information-theoretic secrecy, Wyner introduced the idea of a wiretap channel [9], shown in Figure 2.2. The wiretap channel assumes a general scenario where an information source, Alice, is encoding and transmitting their message over a memoryless channel between themselves and an intended receiver Bob. This is known as the main channel. Unbeknownst to Alice, there is a wiretapper, Eve, listening to the transmission across the channel between Alice and Eve. This is known as the wiretap channel. Wyner showed that if the intended receiver has a higher quality channel than the wiretapper, then information can be encoded at too fine of a resolution for Eve to decode.

In the example shown by Figure 2.3, Alice transmits a message that has been modulated to fit the 16-point constellation on the left. When she transmits the modulated signal, Bob has a high quality channel and is able to identify each of the 16 different points of the constellation or symbols. Eve on the other hand, has a much noisier channel leading to a greater variance in their received symbols. Eve is able to locate in which quadrant each symbol is located, but is unable to determine which of the four possible symbols in the quadrant was sent. Accounting for this advantage, Alice would be able to purposefully encode the message into the bits that only Bob can recover, leaving Eve to decode only meaningless filler bits. In this scenario, perfect secrecy for the message bits is achieved by Alice and Bob from Eve.

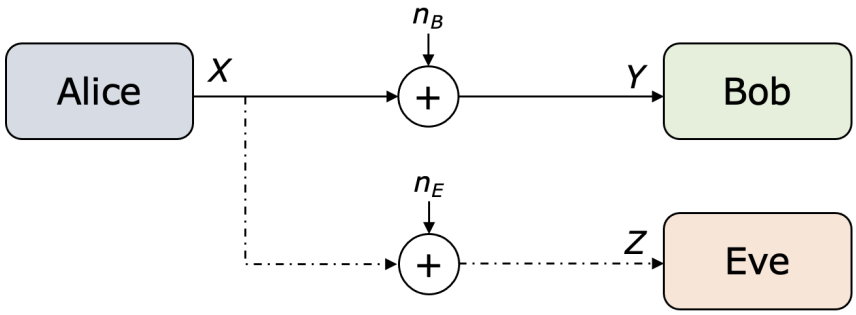


Figure 2.2: Block diagram of the generic Wiretap Channel Scenario.

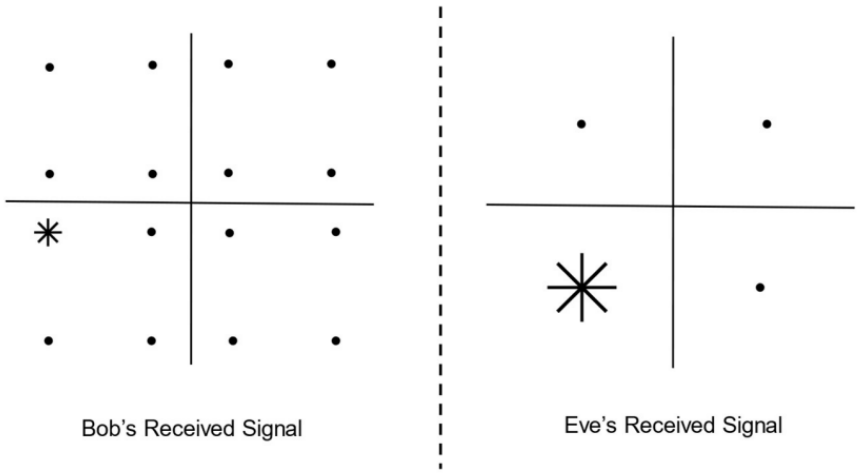


Figure 2.3: Example of wiretap coding via modulation resolution.

It has been shown for the stationary memoryless wiretap channel, any secrecy rate,

$$R_s < \max_{X \to YZ} [I(X;Y) - I(X;Z)] \tag{2.8}$$

is achievable [15], where $I(X;Y)$ and $I(X;Z)$ are the mutual information between X and Y and X and Z respectively, as defined by (2.9). The secrecy rate of a system is the maximum capacity at which information can be transmitted while maintaining perfect secrecy.

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \\ &= \sum_{y \in \mathcal{Y}} \sum_{x \in \mathcal{X}} P_{(X,Y)}(x,y) \log \frac{P_{(X,Y)}(x,y)}{P_X(x)\, P_Y(y)} \end{aligned} \tag{2.9}$$

The wiretap channel provides a useful and implementable method for meeting Shannon's requirements for an information-theoretic secrecy system. It does come with the crucial caveat of Bob needing a channel advantage over Eve. In the most basic system, one without noise sources other than the channel noise impacting Bob and Eve, it is generally not possible to guarantee Bob's channel advantage over Eve. Since the position of an adversary Eve, relative to the transmitter Alice, cannot be bounded, Eve could very well be closer to Alice than Bob is. In this scenario, there would be no channel advantage for Alice and Bob to leverage into wiretap coding. This is commonly referred to as the "near Eve" problem. Emphasizing the effect of an unknown Eve's location, imagine a scenario where Alice and Bob were to assume they had a channel advantage over Eve to share a message via wiretap coding. It could turn out this assumption was incorrect, allowing Eve to decode the secret message without error. This all occurs unbeknownst to Alice and Bob since they have no

prior information about Eve's channel or whereabouts. This makes wiretap coding unreliable in most practical scenarios.

2.6 Cooperative Jamming

Based on the wiretap channel shown by Wyner, it is possible to realize communication systems that will achieve information-theoretic secrecy, but the system requires that a intended receiver have a signal advantage over the eavesdropper. This advantage needs to be enough in order to prevent Eve from acquiring any new information about the message intended for Bob. Unfortunately, due to the unknown nature of Eve's channel as described in the "near Eve" scenario before, it is not practical to simply assume Bob's channel is superior to Eve's in order to support secrecy.

Cooperative jamming has been proposed as a solution to this issue. Cooperative jamming is a method by which a powerful key-based interference signal is transmitted alongside the weaker message signal. Prior to transmission, the key used to generate the interference at the cooperative jammer is shared with Bob, providing him with the ability to generate the same interference pattern at his receiver. The interference affects both the main and wiretap channels of Bob and Eve, respectively, by acting as an additional source of noise in demodulating the message signal. Since Bob knows the interference key and is expecting it, they are capable of generating a cancellation signal from the shared key and using it to subtract the interference from their received signal. Without the interference to bother Bob's demodulation process, they now hold a significant signal advantage over Eve, who is unable to recover the message from their jammed wiretap channel. Bob's clean main channel provides the necessary advantage needed to implement wiretap coding techniques and achieve perfect secrecy.

Cooperative jamming is widely accepted as a secure secrecy system, but unfortunately it still has a weakness. This is because existing systems have focused on implementations that utilize digital cancellation methods in their intended receiver

and often only consider passive eavesdroppers. In digital cancellation schemes, Bob captures the entire signal (interference and message) at their receiver. After amplification and analog-to-digital conversion by their front end, Bob performs digital signal processing in order to remove the interference and isolate the message signal before demodulation. This all happens in the digital domain. A passive Eve simply means that the eavesdropper does not attempt to process their reception other than decoding, subjecting their demodulator to the entire span of the interference.

Since the channel advantage is gained from the post-digitization signal processing, Bob does not hold a physical advantage in his reception of the signal; their advantage is purely from having knowledge of the interference pattern. Eve is just as capable as Bob at capturing the signal, which consists of the being interference and message. Therefore if Eve were able to find out the key and perform cancellation of their own, Eve could also recover the underlying message.

Recall that one of Shannon's requirements for information-theoretic secrecy is that it holds up against an adversary with unlimited resources. To be pessimistic, it should be assumed that Eve records their captured signal to memory for continued processing. Given unlimited time and computational ability, Eve would be able to identify the key-based interference pattern and perform their own cancellation, allowing them to break the secrecy scheme at some later time. Once again, we are left with a system that is only conditionally secure.

2.7 Everlasting Secrecy Based on Jamming

Cooperative jamming presents to us a system of physical layer security, that like traditional cryptography, only provides us with conditional security when up against an active adversary with unlimited time and computational abilities. While it is possible to delay the adversary's ability to decode the message using cooperative

jamming, as long as they are capable of recording the message as cleanly as an intended receiver, everlasting secrecy cannot be achieved.

Work into methods of developing a signal advantage for Bob that holds up against a powerful Eve has continued. Sheikholeslami in particular [2], presents a theory, shown in Figure 2.4 that takes advantage of an overlooked component in existing cooperative jamming schemes: the innate nonlinear operations of an analog-to-digital converter in the front end of an RF receiver. In this system, it is proposed that Bob subtract the interference signal in analog, meaning prior to their conversion and recording. An active Eve on the other hand would have to perform these operations in the reverse order, conversion and recording followed by digital subtraction. This forces Eve to operate their ADC at a much larger span than Bob, losing the low power message signal in the quantization noise of their converter. In this scenario, it was shown that positive secrecy rates can be achieved over an eavesdropper that not only has access to the transmitted combination of message and interference via a non-disadvantaged channel, but also gains access to the key used to generate the interference following transmission and uses it to perform perfect digital cancellation. Therefore the secrecy rates derived from this method meet the everlasting condition required for information-theoretic secrecy.

The challenge in this system is that it requires Bob to perform analog cancellation at RF. This process requires a more sophisticated receiver as Bob now needs to simultaneously receive the transmitted signal, while also up-converting and transmitting his own interference cancellation signal that has been tuned in software to destructively interfere with the transmitted signal's interference component. Like digital cancellation systems, this still requires a rigorous synchronization process in order to maintain large enough cancellation ratios and hold a significant advantage over the eavesdropper. The everlasting secrecy rates achievable by this system depends on the number of key bits that can be successfully cancelled by Bob as can be seen in Figure

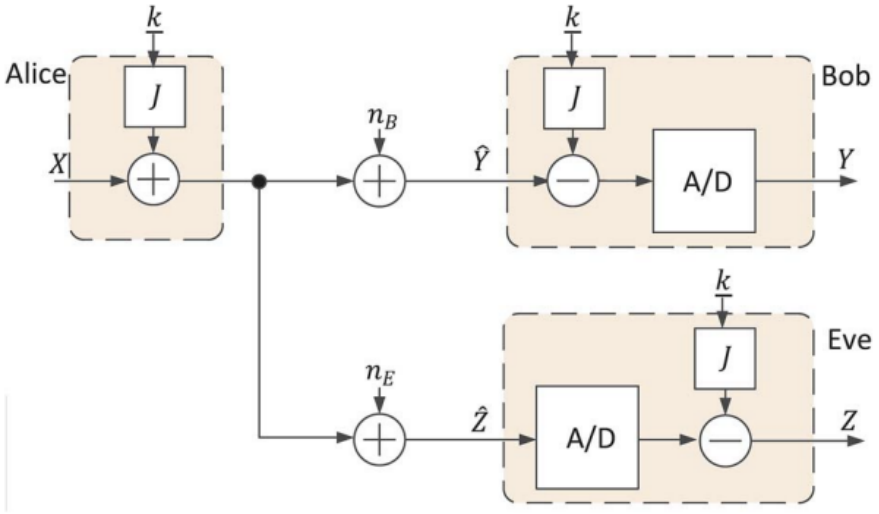


Figure 2.4: Block diagram of the proposed method for everlasting secrecy from [2].

2.5. These values are presented assuming the intended receiver, Bob, implements a 10-bit analog to digital converter while the resolution of Eve's could vary.

2.8 Compression Avoidance

Another benefit to performing analog cancellation comes in the form of reduced receiver compression. Receiver compression is most prevalent when there is a large ratio between the highest power and lowest power signal components passing through an amplifier. This important ratio is referred to as the dynamic range of the overall signal. When a signal with a wide dynamic range passes through a front-end amplifier, the higher power portions of the signal can drive the device past its linear operating region. At this point, the assumed linear gain slope of the amplifier response starts to drop off dramatically as shown by the actual response curve in Figure 2.6. This results in a reduced gain of the high power terms, while the lower power terms still receive the expected linear gain of the amplifier. This distortion of wide dynamic range signals is referred to as compression. A receiver that is subjected to decoding a compression distorted signal will have a disadvantage in recovering the underlying

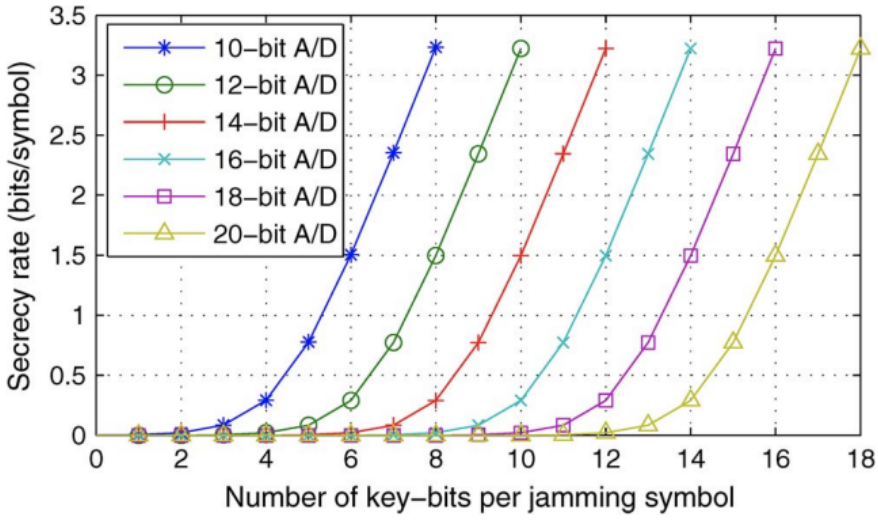


Figure 2.5: Achievable secrecy rates versus the number of key bits when Bob employs a 10-bit ADC and Eve employs ADCs of various quality from [2]. In this model, Bob achieves perfect analog cancellation while Eve achieves perfect digital cancellation. Despite entirely removing the interference, Eve is still limited by the increased quantization noise forced upon their ADC.

message. The only way to prevent this disadvantage for a given receiver is to reduce the dynamic range input to a receiver's front end.

This issue is prevalent in all receiver systems, but is directly linked to cooperative jamming and often overlooked in theory. The combination of using a powerful interference to mask a weaker message signal is undoubtedly a wide dynamic range signal. In the traditional digital cancellation schemes, the intended receiver is capturing the full span, the full dynamic range, of the interference and message signals. Naturally this subjects them to compression due to innate amplifier limitations in their front end. This compression can cause numerous difficulties in their digital processing techniques following capture as the signal linearity that is assumed to achieve perfect interference cancellation is no longer the case. This means even after an interference cancellation stage, the message signal can remain distorted by these compression effects, increasing the probability of errors in decoding the original message.

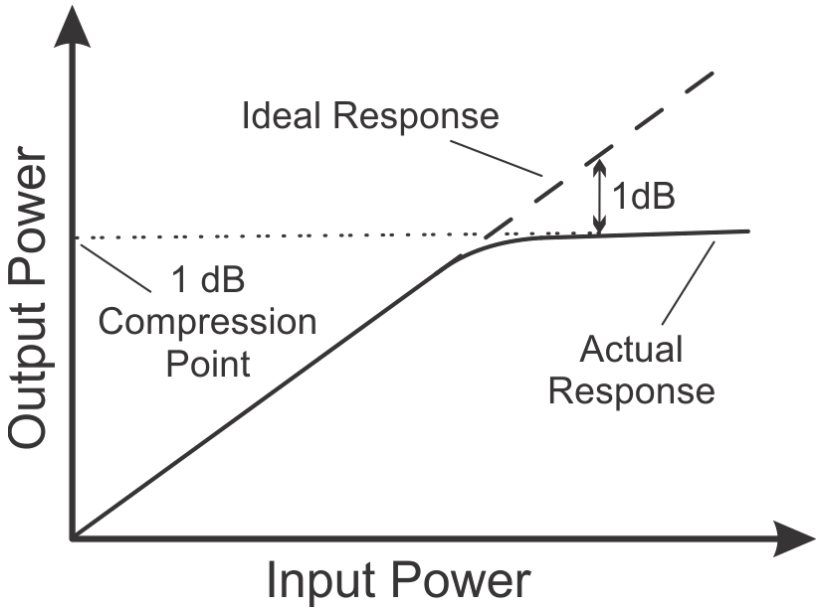


Figure 2.6: Ideal and approximate actual response of an amplifier plotted against input power from [3].

An intended receiver performing analog cancellation has an advantage in this sense. Since they are generating an analog RF cancellation signal to be combined with the received signal, they are drastically reducing the interference power level and therefore the dynamic range of the signal reaching their amplifier. This results in their amplifier remaining in its linear operating range during message transmission, providing them a clean, uncompressed capture of the message signal.

2.9 Software-Defined Radios

The system being analyzed in this thesis utilizes software-defined radios (SDRs). SDRs utilize signal processing to perform as much of traditional radio functions as possible. Whereas a traditional RF front end would connect an antenna to complex chains of various expensive and specialized hardware components in order to tune, adjust, and filter the received signal, SDRs reduce hardware to a minimum. Reduced specialized hardware allows SDRs to be much more flexible in their implementations. These improvements include tuning to a wide variety of operating frequencies,

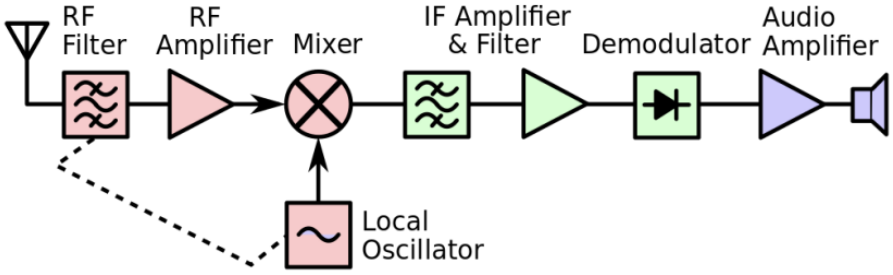


Figure 2.7: A block diagram of a typical RF front end of radio receiver from [4].

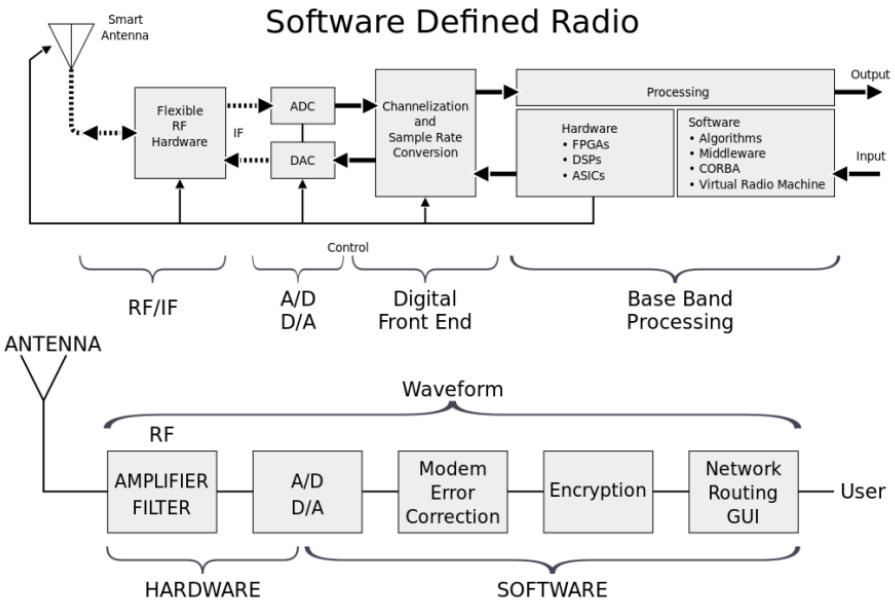


Figure 2.8: A block diagram of a typical SDR front end and example use case from [5].

performing any kind of modulation and demodulation techniques, and adjusting to changing protocol all using their flexible hardware and software programming. Typical structures of the two types of radios can be seen in figures 2.7 and 2.8.

Each block in the typical RF front end (Figure 2.7) would typically be its own integrated circuit or analog filter functionally specific to that use case. The SDR structure requires much less hardware. It still requires a minimal RF front end in order to handle amplification and mixing of high-frequency signals. This is because signals with frequencies commonly on the order of GHz are unable to be sampled at

rates large enough to meet the Nyquist-Shannon sampling theorem. This theorem states that if a signal is not sampled at a frequency greater than twice its highest frequency component, then information will be lost. A lightweight and flexible mixing stage before the SDR software processing solves this issue by down-converting radio frequency carriers to much lower intermediate frequencies or baseband. Once shifted down to near baseband, an analog-to-digital converter is capable of sufficiently sampling the signal into the discrete domain where it is quantized into binary data and managed in software. A SDR transmitter works in the opposite way. The desired signal is designed in software as discrete samples, and a digital to analog converter transforms them into an analog waveform at base-band. It is then up-converted to a desired carrier frequency and amplified to be transmitted.

CHAPTER 3

SYSTEM OVERVIEW

The proposed cancellation scheme is an improvement on traditional cooperative jamming; therefore, the same three characters are still at play: Alice (the message transmitter), Bob (the intended receiver of the message), and Eve (an adversary eavesdropper on the channel recording everything that is transmitted). Also on the channel is the cooperative jammer. Figure 3.1 provides an overview of the system operation during transmission of the SoI.

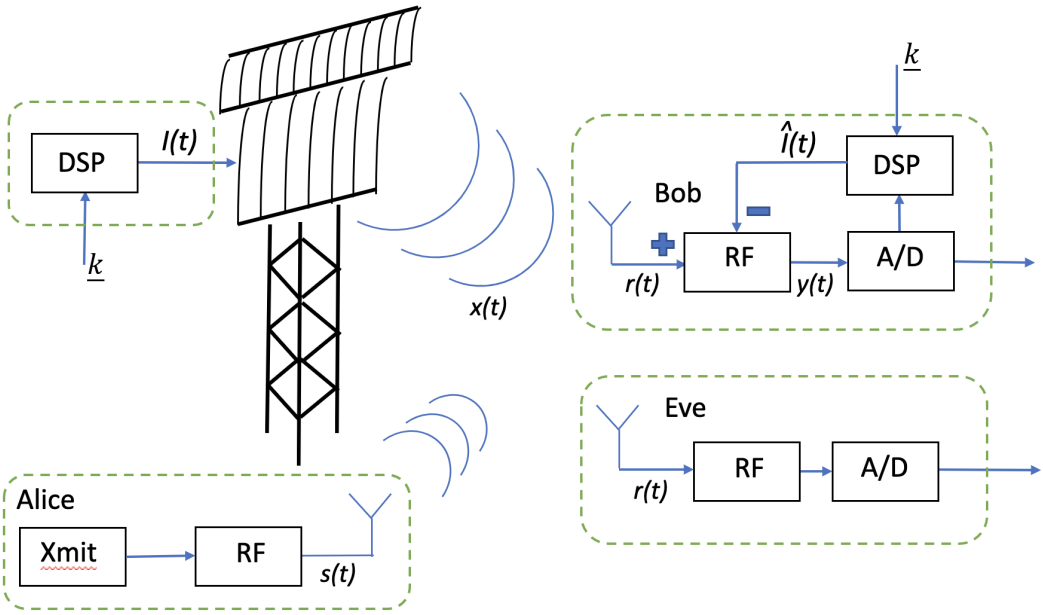


Figure 3.1: A block diagram describing the analog known interference cancellation system function. The message signal transmitted from Alice, $s(t)$, is hidden by the much larger interference, $I(t)$. Having knowledge of the shared key used to generate the interference, $\underline{k}$, Bob is capable of constructing the approximate interference, $\hat{I}(t)$, to perform analog cancellation before their ADC. Conversely, Eve's ADC is not protected from saturation by cancellation, resulting in a compressed reception of the message.

Accurate channel estimation and synchronization between the transmitter and jammer are crucial to the ability to generate a cancellation signal that matches the interference. To maintain cancellation in real time, the transmitter and receiver must generate their interference and cancellation signals, $I(t)$ and $\hat{I}(t)$, simultaneously based on the shared cryptographic key, $\underline{k}$. For a given SoI, $s(t)$, the transmitted signal is:

$$x(t) = s(t) + I(t) \tag{3.1}$$

This thesis will discuss the use of a binary phase-shift keying (BPSK) modulated and frequency-modulated continuous-wave (FMCW) signals generated from the shared key as the interference. Furthermore, the interference bandwidth is assumed small enough for the channel to be frequency-nonselective. This simplifies the channel parameterization to:

$$r(t) = h_s s(t - \tau_s) e^{j2\pi(t-\tau_s)f_s} + h_i I(t - \tau_i) e^{j2\pi(t-\tau_i)f_i} \tag{3.2}$$

where $r(t)$ is the RF signal at the receiver. The parameters h_s and τ_s as well as h_i and τ_i are the complex gains and real time delays of the SoI and interference channels, respectively. The carrier frequencies f_s and f_i of the two transmitters can differ from that of the receiver.

In cooperative jamming, a synchronization and channel estimation period is adopted prior to transmission of the interference and SoI. This will be referred to as the learning period. In order to reduce transmitter downtime during the learning period, we propose that the transmitter is implemented as a dual-use system. In particular, the transmitter would utilize a cyclic transmitted learning sequence, $I_l(t)$, for normal operation during the receiver's estimation. Here, the intended receiver iterates over the learning sequence to model the channel parameters. During the learning period,

there should be no SoI added to the transmission such that the received signal $r_l(t)$ is as follows.

$$r_l(t) = h_i I_l(t - \tau_i) e^{j2\pi(t-\tau_i)f_i} \tag{3.3}$$

In this model we propose using a radar system as the cooperative interference transmitter, so its normal sensing operation can be used as a learning sequence. Then, at a predetermined time, both the interference transmitter and receiver will switch over from the learning sequence to the interference sequence. Simultaneously, the transmitter will also begin generating a low power SoI, $s(t)$, to be combined with the interference transmission. With the channel already modeled from the learning sequence, the receiver is able to maintain cancellation of the interference and receive the uncompressed SoI.

Here, the eavesdropper, Eve, is just as capable as the receiver Bob but lacks the key. Hence, the advantage comes from the single-use shared key based, large interferer. Without access to the key beforehand, Eve is unable to perform real-time analog cancellation of the interferer. With their receiver saturated by the interference, even if perfect digital cancellation of the signal is achieved, they are relegated to digital processing of a message that has been significantly degraded by the saturation and compression of their ADC.

CHAPTER 4

THE HARDWARE TESTBED AND SIMPLE MODULATION PERFORMANCE

In this chapter, the analog cancellation architecture is explored and implemented in hardware using low-cost software-defined radios (SDR). We show that large cancellation ratios can be achieved using BPSK modulated learning and interference signals despite challenges in modeling and compensation. Limitations to this architecture are discussed.

4.1 Hardware Testbed

The testbed is shown in Figure 4.1. It features two inexpensive SDRs from Ettus Research, USRP B210s. The B210 utilizes an onboard 2x2 transceiver RFIC, the AD9361. The AD9361 provides two transmit and two receive channels each with individually tunable gain and frequency settings [16] [17]. The USRP B210 must be connected to a host PC, where most of the digital sample processing occurs. The transmitter and receiver (see Figure 4.1) also each use a Mini-Circuits ZFSC-2-11+ RF splitter/combiner to combine signals. Both radios utilize the reference output signal of a Keysight N9000B signal analyzer. Stable references are required to minimize carrier frequency drift, the effects of which will be discussed later.

Sample generation, processing, and radio control is handled via GNURadio, a free and open source radio environment that can be implemented via companion GUI, C++, or Python programming languages [18]. The Python control scheme is utilized in these experiments because its hybrid nature provides greater autonomous control

over processing and radio settings than the GUI companion. Through GNURadio, the B210 on-board FPGAs are only utilized for sample handling between the host PC and internal RF transceiver IC. Thus, a sufficiently powerful host processor is required to handle all sample generation and estimation algorithms described later in this chapter.

The repeated learning pattern used is a 16-bit binary phase-shift keying (BPSK) sequence that is modulated and upconverted to the carrier frequency. Experiments were run for a variety of carrier frequencies, but results for 100 MHz and 1 GHz carriers will be shown and compared. Data for 1 GHz carrier will be shown using a wireless channel via radios about 10 feet apart, while 100 MHz results will focus on a coaxial cable channel due to cancellation ratios being limited by propagation capabilities rather than estimation error. The interference signal has a 94 kHz bandwidth at a 3 MHz sample rate. The narrow bandwidth allowed for improved time domain resolution relative to the symbol period and for the system to operate assuming a frequency non-selective (flat) fading channel in wireless testing.

RF radio settings are also crucial to testing the maximum cancellation capabilities, as the transmitter needs to propagate an appropriately large SNR. The achievable cancellation is also limited by transmitter intermodulation distortion; since nonlinearities within commercial power amplifiers (PA) are not consistent [19], intermodulation distortion caused by a saturated transmitter gain stage cannot be consistently canceled. Therefore, it is crucial for the transmitter to operate in a gain region that maximizes transmitter power while adequately attenuating the digital-to-analog converter output to avoid PA saturation and maintain linearity. Similarly, it is important for the receiver low noise amplifier to also operate in a linear stage. If the receiver gain is too large, increased intermodulation distortion will drive down the SNR preventing accurate channel and frequency offset estimation. In order to achieve interference cancellation to the receiver noise floor, the third-order intermodulation products can-

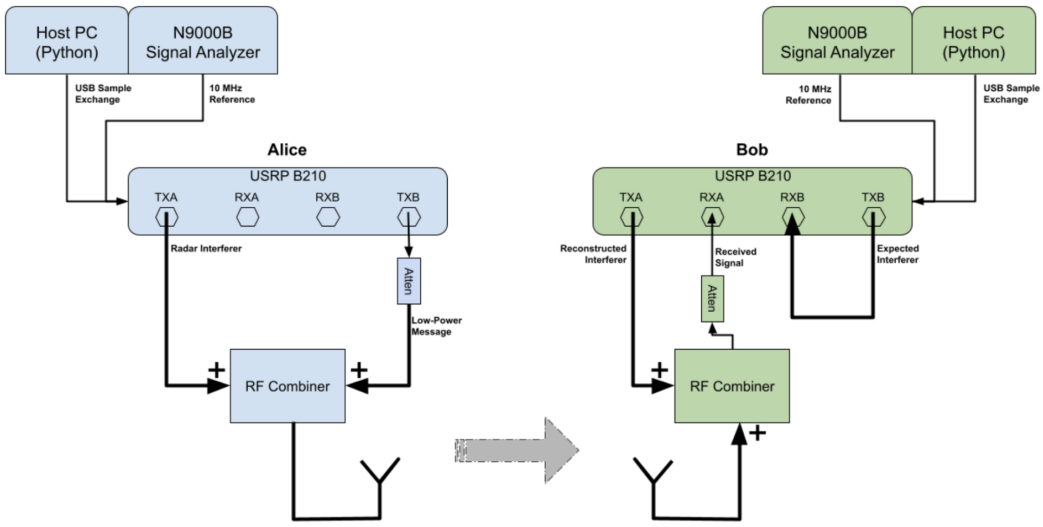


Figure 4.1: Hardware diagram of the implemented testbed. Each B210 SDR utilizes its own host PC and reference source, entirely isolating them from one another. Intended receiver, Bob, loops an analog copy of expected interference out and back into one of their receivers to solve an indeterminate sample timing delay issue introduced by the single-stream USB interface.

not be too far above that floor. This corresponds to a transmit PA back-off of roughly 22 dB. This guarantees spur-free transmission of the interference. The receiver LNA should operate with similar levels of back-off for the best carrier frequency synchronization.

4.2 Receiver Design and Implementation

As discussed above, fine synchronization of carrier frequency offset and channel parameters is required to achieve large cancellation ratios. This is accomplished by digital signal processing of the learning sequence as it is repeatedly transmitted prior to transmission of the cryptographic interference and SoI. The following estimators are employed.

4.2.1 Carrier Frequency Synchronization

Since the transmitter and receiver must generate their RF carriers from separate non-ideal reference oscillators, there is an innate offset between the two that is passed along to their generated carriers. If this offset is not sufficiently compensated, then cancellation is diminished or not at all possible [20]. This offset is estimated using a common phase-shift keying (PSK) architecture, the Costas Loop. The Costas Loop is a second order phase locked loop (PLL) that is capable of tracking the instantaneous phase and frequency offsets of a received PSK signal. It is one of the preferred methods of frequency synchronization in PSK systems as it does not require any pre-processing of the received signal to approach its performance limits [21].

This PLL iterates over the received signal and updates its frequency offset estimate $f_o = f_i - f_r$, where f_r is the carrier frequency generated by the receiver. The estimate f_o is employed by the receiver to frequency shift the baseband signals before and after upconversion and downconversion, respectively.

4.2.2 Channel Gain and Time Delay Estimation

The channel effects on the interference include attenuation, phase, and time delays. These effects can be described by two parameters, a time delay d_i and a complex channel gain h_i. Without identical (or close to) simulation of these parameters on the reconstructed interference at the receiver, cancellation is rapidly diminished or not at all possible [22].

Since the time delay of the channel is largely dependent on the physical distance between transmitter and receiver, this parameter will not change rapidly over time. Therefore it is sufficient to make a single accurate estimate of this parameter rather than tune over time as is done with channel gain. The channel time delay estimate, $\hat{d}$, is calculated by maximizing the correlation function of the digitized received signal before cancellation begins, $r[n] = r(nT_s/M)$, and the digital signal expected to be

received, $I[n] = I(nT_s/M)$, as shown in (4.1), where T_s is the radio sample period, M is an interpolation factor greater than one, and N is the period of the cyclic interference in samples before interpolation. Interpolating the signals allows the correlation based estimator to measure a sub-sample period delay.

$$\hat{d} = \arg\max_{d} \frac{1}{M} \sum_{n=1}^{M*N} r[n] * I_l[n-d] \tag{4.1}$$

The channel time delay τ_r is not always an exact multiple of the sampling period, which results in a floating point estimate $\hat{d}$. For sub-sample period time delays, a bandlimited digital fractional-delay filter (FDF) is used. This design utilizes a finite impulse response approximation of the Nyquist-Shannon ideal FDF for a fractional delay, $d_f = \hat{d} - \lfloor \hat{d} \rfloor$, between 0 and 1. The FDF impulse response is shown in (4.2) [22] [23].

$$h_f[n, d_f] = \text{sinc}[n - d_f] = \frac{\sin[(n-d_f)\pi]}{(n-d_f)\pi} \tag{4.2}$$

As there is no perfect digital implementation for non-bandlimited filters, the realizable approximation introduces inter-symbol interference (ISI) to the cancellation signal. The ISI results in a reduction in cancellation capability relative to how large of a fractional delay the filter is adjusting for [24].

Unlike time delay, the attenuation and phase delay of the received signal is influenced by environmental changes due to multipath and thus varies more rapidly with time. Thus, the complex gain of the fading channel is iteratively estimated from the residual signal following interference cancellation. The gain estimate $\hat{h}$ is updated over time by the learning rule in (4.3). The learning rate α controls how quickly the gain estimate can track a changing channel. Too large of a learning rate causes unstable estimates (and unstable cancellation) in a constant or near-constant channel. This rule is based on the estimation circuit for the full-duplex receiver described in [25] and mean-squared error channel tracking [26].

$$\hat{h}_{N+1} = \hat{h}_N + \alpha[y(nT_s t) * I_l(nT_s t)^*] \tag{4.3}$$

4.2.3 Cancellation Signal Correction

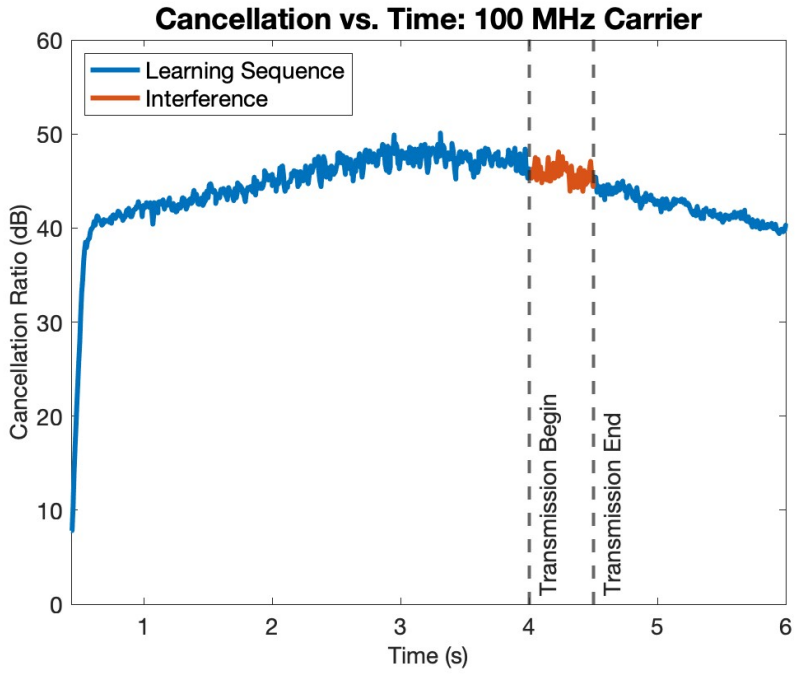
The cancellation signal at the receiver is generated from the same symbol sequence as the interference at the transmitter. This is so that without any channel simulation, the cancellation signal is also $I(t)$, the expected interference signal. As the channel parameter estimates are updated, they are applied to the cancellation according to (4.4) resulting in the reconstructed analog interference signal $\hat{I}(t)$, where $f_r + f_o$ is the assumed carrier frequency of the originally transmitted interference.

$$\hat{I}(t) = \hat{h} I(t - \hat{d}) e^{j2\pi(t-\hat{d})(f_r+f_o)} \tag{4.4}$$

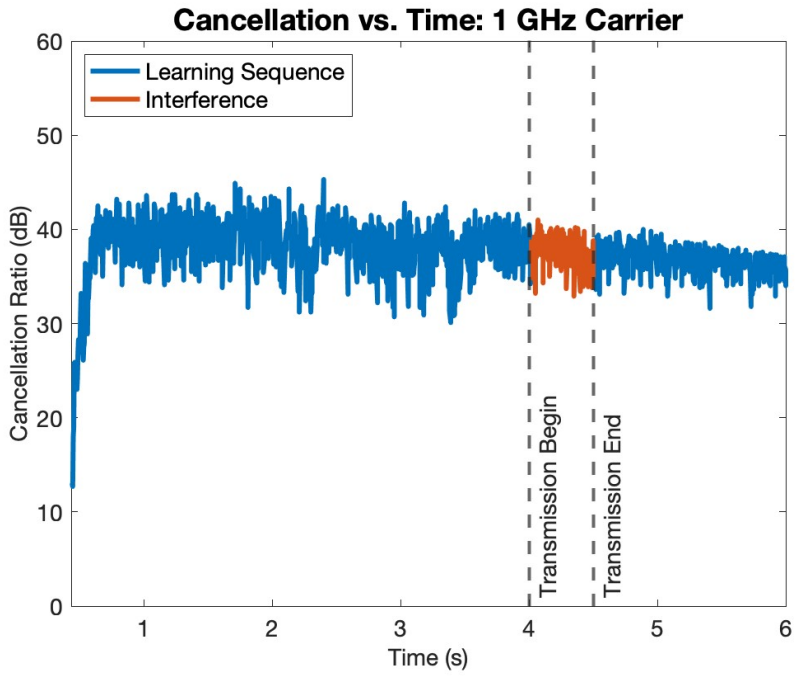
4.3 Cancellation Capability and Limitations

As shown below, under these circumstances peak cancellation ratios for the 100 MHz and 1 GHz carriers of 52 dB and 42 dB were observed, respectively. Cancellation for either frequency varied over time, but could be maintained over 40 dB and 30 dB, respectively, for extended periods of time.

Highlighted by the orange sections of Figure 4.2, cancellation is maintained across the predetermined transmitter switch between the cyclic learning sequence and key-based interference. This is crucial, as if Eve is able to learn the pattern during a repeated transmission, then the compression advantage Bob has over them is lost. Therefore, the interference must be able to be cancelled at Bob in a one-off fashion immediately following the learning sequence. The time axis begins upon the start of time and channel estimation, which follows the carrier frequency estimation period.



(a)



(b)

Figure 4.2: Cancellation ratio versus time plotted for (a) the 100 MHz carrier and (b) the 1 GHz carrier. The time axis begins upon the start of time and channel estimation, which follows the carrier frequency estimation period. The window of time highlighted from 4 to 4.5 seconds shows where the both transmitter and receiver simultaneously switch from the learning sequence to the shared-key based interference.

The window of time from 4 to 4.5 seconds shows where the both transmitter and receiver simultaneously switch from the learning sequence to the shared-key based interference. Because the channel effects are independent of the signal itself, the channel model built from the learning sequence works for the interference as well. This results in a seamless transition with maintained cancellation when going between learning and interference sequences.

Figure 4.3 compares the power spectral density of the received signal before and after cancellation for the 100 MHz carrier. It shows the interference which an intended receiver (black) and a eavesdropper (blue) would receive. Without cancellation, the SoI can be hidden by the more powerful interference (blue) from Eve. The receiver capable of performing analog cancellation can reduce the interference down to a much smaller residual (black) that allows the SoI to be received.

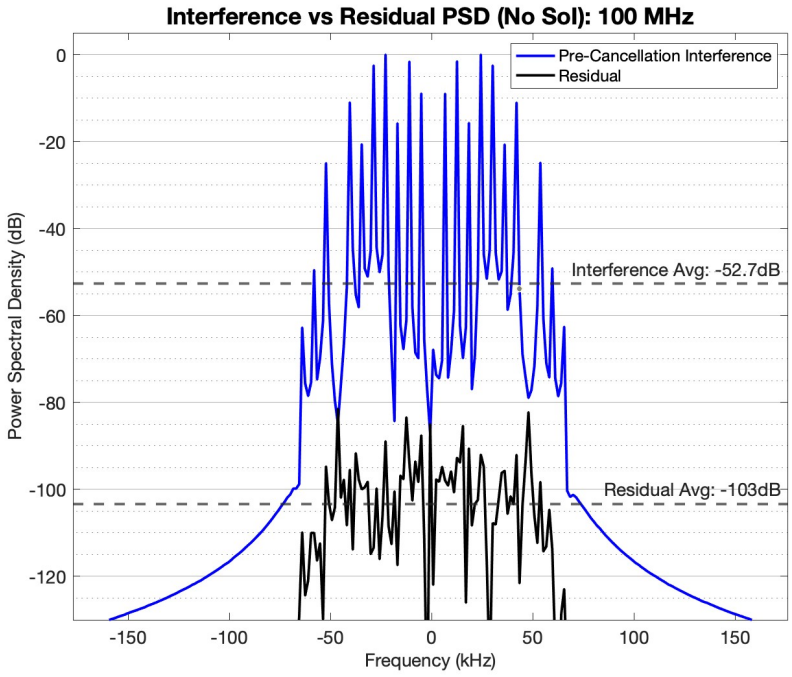


Figure 4.3: A frequency domain view of the receiver's analog cancellation capability. In blue is the pre-cancellation interference received by Bob. The black trace shows the remaining residual received by Bob's ADC during cancellation.

The analog known interference cancellation architecture shown above not only achieves peak cancellation values comparable to recent digital systems [11], but does so despite a prominent challenge in analog cancellation systems: frequency stability. In this analog architecture, cancellation is occurring at RF but processing occurs at base-band in the receiver. Because of this, frequency estimation occurs with a given chunk of samples, but then a base-band cancellation signal is generated using that estimation and upconverted to the carrier frequency to cancel the proceeding RF signal. In this window between estimation and cancellation, the carrier frequency of the interference may have drifted a small amount. Therefore, the frequency alignment between interference and cancellation (at RF) is not perfect. It is not possible to resynchronize the carrier frequencies actively during cancellation as the signal that estimation is based on is being severely attenuated. Based on the frequency sensitivity of interference cancellation shown by Guo in [22], to achieve a 50+ dB cancellation ratio, the frequency error must be on the order of 10^{-6} of the interference bandwidth. For this implementation the error must be less than 0.1 Hz. Comparatively, a OFDM signal (with 30dB SNR) approaches the noise limit of its bit-error rate at frequency offsets greater than 10^{-3} of it's subcarrier spacing [27]. That makes the analog cancellation performed here more sensitive to frequency-error than OFDM by a factor of 10^3. Since frequency drift is proportional to carrier frequency, lower carrier frequencies will produce reduced drift and therefore reduced carrier frequency error, as shown by increased peak cancellation and cancellation stability in the 100 MHz carrier results.

A more advanced receiver could be able to help solve this issue by splitting a portion of the received interference prior to the analog cancellation stage. This would require an additional receive channel at Bob exclusively for carrier frequency estimation. In return, it would allow for continuous carrier frequency tracking of the uncancelled interference portion while the channel intended for message reception

performs cancellation. The cancellation channel would be able to make small adjustments to its carrier offset correction based upon estimates from the new channel.

Fractional time error is also impactful, and a limitation of SDRs and digital signal processing for this application is time delay resolution. If the channel time delay is estimated to be between multiples of the SDR sample period, the receiver is unable to perfectly synchronize to that time delay without introducing ISI to the cancellation signal. Guo shows that cancellation degradation due to ISI in fractional delay tuning is relative to the interference's symbol period [22].

4.4 Further Analysis of Time-Frequency Impact on Cancellation

As laid out above, the two biggest factors limiting cancellation and its stability over time are the discrete-time domain resolution of the signal processing system and natural frequency drift of the reference oscillators. The best solution found to prevent carrier frequency drift is to improve the test bench with more stable reference oscillators as there would be no performance trade offs anywhere else in the system. The ones used in these experiments are sourced from high quality test equipment. For discrete-time resolution, improvement is more complicated.

The easiest way to improve discrete-time domain resolution and reduce the need for imperfect fractional-delay filtering is to increase the SDR sample rate without changing the bandwidth of our interference or learning signals. This would mean we are further oversampling the signals, increasing the number of clean samples we have to process or generate the signals with in a given window of time. This provides finer time delay steps for our cancellation signal without having to use a FDF. Unfortunately, the sample rate of the system is limited by host computer processing power and the interface being used to exchange samples with the SDRs (see Appendix A), and the testbed was already pushing this limit. Attempting to increase the sam-

ple rate further resulted in the radios not receiving any samples on time and just returning error messages repeatedly.

Since the sample rate cannot be pushed any higher, the only other option is to oversample another way. This can be done by interpolation in the modulation stage of signal generation at both the transmitter and intended receiver. Interpolation here allows for the selection of the number of samples to represent each symbol in the interference sequence. By increasing this samples per symbol (SPS) parameter for the constant sample rate, the signal is being extended in the time domain. This provides greater flexibility in the time domain as is desired, but comes with a trade off. Extending the signal in the time domain, slowing it down, naturally creates a real signal with a reduced bandwidth. Essentially, only a fraction of the sample rate is being used for meaningful data. As discussed earlier, it has been shown that the cancellation ratio's stability vs carrier frequency offset is relative to the interference bandwidth. As the bandwidth is decreased by increasing SPS, the symbol period is increased. Since frequency error between two signals results in a linearly increasing phase difference over time, a larger symbol period results in a greater phase error across a set of symbols. This means that without being able to increase the system sample rate any further, there is a forced trade off between time and frequency error effects in the system. Increasing the SPS provides an improved ISI-free time delay correction resolution, but it comes at the cost of system performance with imperfect reference oscillators and carrier drifting.

Figure 4.4 shows this frequency stability tradeoff in action. Since the frequency sensitivity of the cancellation ratio is also relative the cancellation at that moment (meaning a small change in carrier frequency will have a much greater effect at 40 dB of cancellation than at 20 dB), the data was chosen to compare similar cancellation ratios for different SPS parameters. This can be done since the time domain resolution limit does not set an upper bound for cancellation, only a lower one. What this means

is that while the wider bandwidth signal has a worse time delay step resolution, if by chance the uncontrollable fractional delay of the channel happens to be small, large cancellation ratios are still possible, but are not guaranteed. In the plot, it is visible at peak cancellation that the orange trace representing 16 SPS and wider bandwidth, is more consistent as it follows a smoother cure. The 32 SPS trace is much more jagged at its peak, highlighting how much more sensitive to small frequency drifts it is.

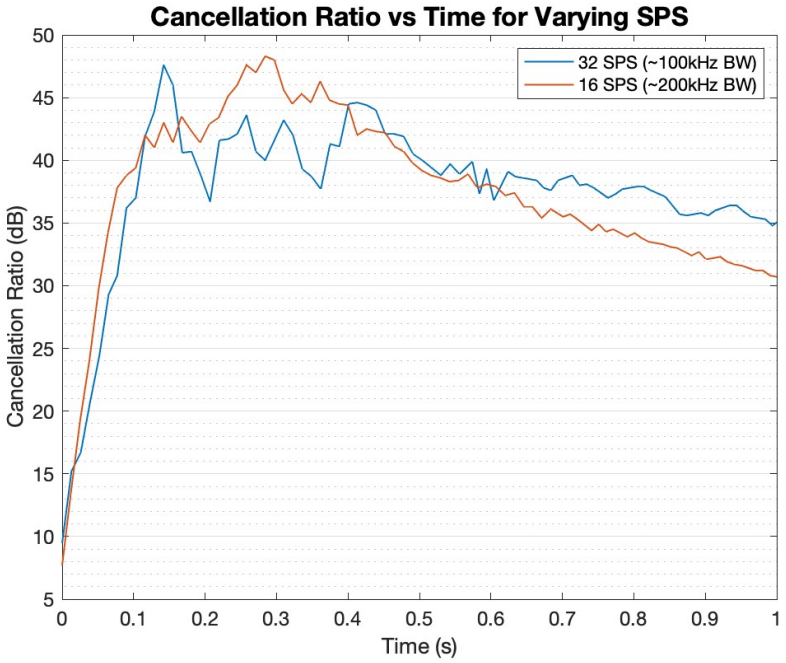


Figure 4.4: Cancellation ratio plotted versus time for two different sample per symbol rates.

Another potential method to reduce this problem is to update the estimated channel gain (particularly phase) more often. This would decrease the number of symbols that the phase difference is assumed constant for. Since this estimate is updated via a feedback loop, increasing the update rate too far will result in instability of the channel estimation loop. This occurs when new estimates and corrections are made before the effects of previous updates have yet to propagate through the system.

CHAPTER 5

COEXISTENCE OF FMCW RADAR

This novel interference cancellation method's limitations in terms of carrier frequency drifting sensitivity discussed in the prior chapter point to a reasonable implementation of this method for achieving information-theoretically secret communications requiring a transmitter (and receiver) with highly stable reference oscillators. Rather than designing new and costly high power systems just to transmit an interference signal, it may be possible to take advantage of existing systems that can meet the requirements to achieve reasonable secrecy rates. An example of such design could be a local radar system.

Despite the dual-utility of a radar transmitter in such a scenario, it is clearly undesirable to entirely lose operation of an important sensing system to allow for the necessary learning and message transmission periods described in Chapter 3. In order to minimize downtime of a cooperative radar system, the intended receiver can complete their channel learning processes while the radar performs its normal operation. That would mean the intended receiver must be capable of using the radar system's transmitted waveform as the learning signal in the described cancellation scheme. In order for a suggestion of coexistence with a normally operating radar to be reasonable, the system proposed here should be compatible with common radar waveforms such as those shown in Figure 5.1.

Of these waveforms, compatibility with the proposed interference cancellation method has been shown for pulsed wave and PSK-coded waveforms by the periodic BPSK interference used with the testbed from Chapter 4. The remaining waveform

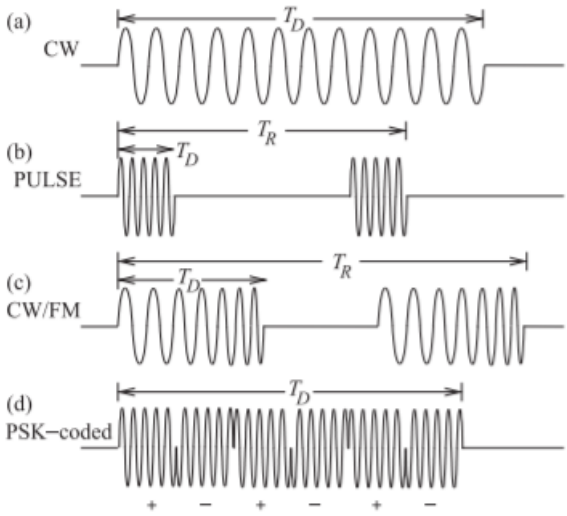


Figure 5.1: Examples of common radar waveforms given in [6]: (a) continuous-wave; (b) pulsed wave; (c) frequency-modulated continuous-wave; and (d) phase-encoded (PSK-coded) waveform.

is frequency-modulated continuous-wave (FMCW). The rest of this chapter will address the necessary changes to the hardware testbed's synchronization algorithms to accommodate an FMCW learning signal as well as the achieved performance of the testbed in performing channel modeling and therefore analog cancellation of the new waveform.

5.1 The FMCW Waveform

FMCW waveforms provide a number of advantages over traditional pulsed radar that make them desirable. Since they measure the distance of a target via the frequency difference between the transmitted and reflected signals they can achieve a greater range resolution than traditional pulse systems that rely on timing or phase differences of reflections. FMCW systems can range targets at much shorter distances than pulse systems as well. These advantages come at the cost of bandwidth and maximum range as pulse radar uses narrower bandwidth signals that perform better over long ranges. Doppler shifts, the changes in reflected frequency by fast

moving targets, can also cause inaccuracies in the target distance estimated with an FMCW waveform.

Frequency-modulated continuous-wave signals consist of a single tone but the frequency of that tone is increased or decreased over time according to some modulation pattern, $f_m(t)$. This means that the instantaneous frequency of the signal is $f_i = f_0 + f_m(t)$, where f_0 is the carrier frequency, resulting in the transmitted signal below.

$$s(t) = \cos(2\pi f_i t + \phi) \tag{5.1}$$

In this equation, ϕ is the reference phase of the transmitter. When the tone frequency is swept linearly, like example c in Figure 5.1, the waveform is called a chirp. Many FMCW waveforms use a saw-tooth pattern for their modulation and operate under some fractional duty cycle. For true continuous-wave, meaning no interruptions or downtime between chirps, a saw-tooth pattern can be undesirable as the sharp transitions in frequency can cause bandwidth expansion, distorting the transmitted waveform. In this case, a triangular frequency modulation pattern, meaning a chirp up followed immediately by a chirp down, can be used, resulting in a base-band waveform such as the one in Figure 5.2.

Unlike the phase-shift keying used previously, which was a digital modulation scheme, FMCW is an analog modulation scheme. This means that the carrier signal is adjusted based on an analog input (in this case the frequency sweeping pattern) rather than the binary data or pattern determining the BPSK signal's phase changes. This means that the bandwidth and time domain resolution of the generated signal are no longer explicitly tied together, allowing for much more control over the learning sequence modulation's bandwidth, periodicity, and resolution. This can prove useful in showing how these various parameters influence cancellation capability.

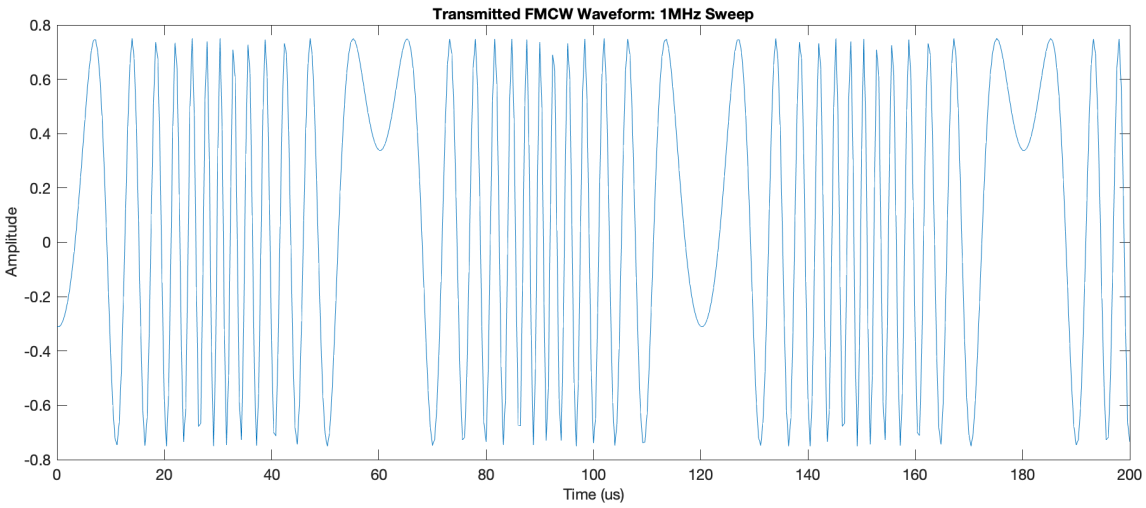


Figure 5.2: A time domain plot of the triangular FMCW signal used in testing.

5.2 Data-Aided Carrier Frequency Estimation

As with the pulsed radar waveform learning period, the FMCW learning period will require some form of time, complex gain, and carrier frequency synchronization in order to achieve cancellation. Fortunately, the time and gain estimators used in the previous chapter are both defined for estimating time and gain errors of general signals, meaning they can still be used in synchronization of the FMCW waveforms. Conversely, the digital Costas loop architecture implemented for carrier frequency offset estimation is exclusive for phase-shift keying modulation schemes. This means a new carrier frequency estimator is necessary for this learning sequence.

Since the learning sequence is periodic, and known by the intended receiver performing synchronization prior to the process beginning, this information can be used to allow for a simple carrier frequency estimation algorithm. The data aided estimator measures the phase difference between periods of the real received signal over time in order to estimate the frequency offset from Bob's baseband. The carrier frequency offset estimate, f_o is described by (5.2), where arg[$\cdot$] denotes the value of the argument normalized between $-\pi$ and π, and L is the period of the learning sequence [28].

$$f_o = \frac{1}{2\pi L} \arg \left[\sum_{n=0}^{L-1} r[n] r^*[n-L] \right] \tag{5.2}$$

5.3 Cancellation Performance with FMCW Waveforms

Since it was seen to be the best performance option in the prior test experiments, the FMCW work here will focus on cancellation using a 100 MHz carrier frequency. Using the 100 MHz carrier frequency again required the system be operated using coaxial cables rather than over-the-air transmission. The signal characteristics chosen to best match the previously used BPSK signal's bandwidth and period are summarized in Table 5.1.

Parameter	Value
Carrier Frequency	100 MHz
Frequency Sweep (BW)	100 KHz
Sweep Period	100 µs

Table 5.1: FMCW signal parameters used to match BPSK signals in Chapter 4.

Using the new carrier frequency offset estimation method, and the previously described channel time delay and gain estimation and correction methods, analog cancellation was achieved between a transmitter and intended receiver using separate reference oscillators. The cancellation of this learning sequence was consistently over 35 dB, with peaks seen up to 47.9 dB. The windows of time over which peak cancellations were maintained were shortened as slightly less stable reference oscillators were used in these experiments. Similar decreases in the cancellation consistency were also seen when using BPSK waveforms with this set of reference oscillators, so it can be concluded that they are the main contribution to this drop in stability. If the oscillators used in Chapter 4 were implemented here, it is likely an increase in both consistent and peak cancellation ratios would be seen.

Taking advantage of the freedom of signal design granted by the analog modulation scheme, data was also collected for increased frequency sweeps. These increased bandwidths were larger than was possible with BPSK while also maintaining a minimum time domain resolution to produce large cancellation ratios. Increasing the frequency sweep to 500 KHz (keeping carrier frequency and sweep period constant) saw an immediate drop in cancellation capability. The peak cancellation seen in these drops down to 25.6 dB, with 1 second windows of cancellation never getting over 13 dB. This drastic drop-off in performance called for further investigation as it went against the conclusions for BPSK waveforms that larger bandwidth signals should experience a greater cancellation stability in the event of frequency error or drift.

In order to attempt to isolate the predominantly contributing parameter of the reduced cancellation performance, the carrier frequency error was removed from the experiment by linking the Alice and Bob radios together via a shared reference oscillator. By doing this, it could be narrowed down whether or not the drop in cancellation capability was due to the waveforms or not. Without the constantly changing carrier frequency error, the cancellation ratio levels out to a maximum value rapidly as the synchronization algorithm runs and converges to a locked channel model as shown in Figure 5.3. A compilation of these locked cancellation values over multiple runs of varying bandwidths is shown in Figure 5.4.

The fluctuations in cancellation performance for individual bandwidths even under the frequency locked scenario is due to the fractional time delay error that is not being corrected for in this experiment. This correction was left out here as the fractional-delay filters implemented in previous experiments only behave as perfect all-pass filters for narrow fractional bandwidths. Using these narrow time delay filters would introduce more error in the wide-band signals. It is visually evident in Figure 5.4 that the decreased cancellation performance observed for larger frequency sweeps is still present and therefore independent of carrier frequency drift.

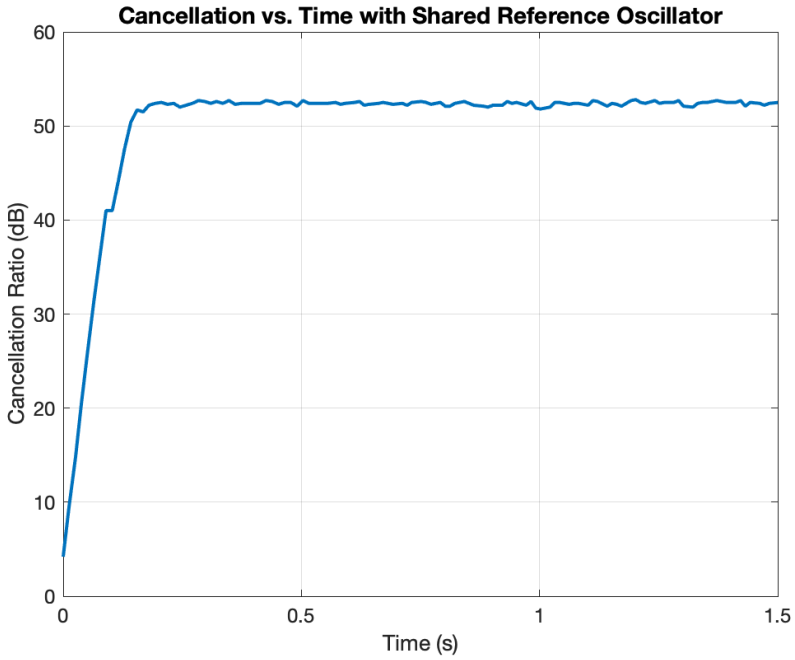


Figure 5.3: An example of the cancellation ratio leveling out to a constant value when there is no frequency drifting.

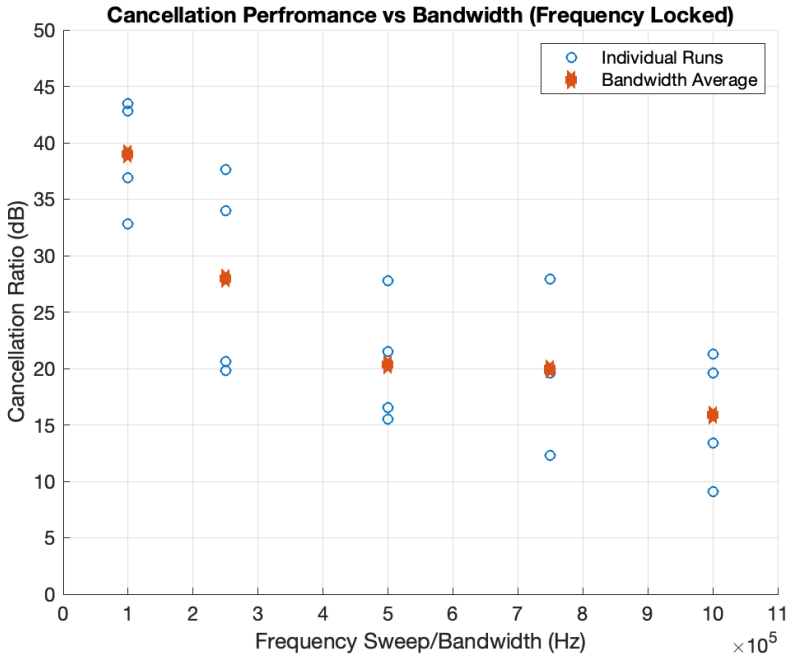


Figure 5.4: A comparison of cancellation performance for FMCW signals of varying bandwidths with a shared reference (frequency locked).

Another possible cause of this drop in performance could be that the cancellation of higher frequency tones in the wider bandwidth sweep are more sensitive to fractional time delay error or the channel gain error in general. This was tested by comparing cancellation of single tones at both 100 KHz (the narrow sweep max) and 1 MHz (the wide sweep max). In this comparison, both tones were consistently reduced by 43 dB or greater across multiple runs and fractional time delay errors, ruling out those possibilities.

At this time it can be concluded that increasing the frequency sweep while holding the sweep period constant impacts cancellation. This ratio of sweep frequency to sweep period is known as the waveform's chirp rate. The next step in untangling this decrease in cancellation would be to compare cancellation performances across constant chirp rates, meaning increasing the sweep period along with the frequency length of the sweep rather than increasing the chirp rate and frequency sweep as we did here. This would show whether chirp rate or the bandwidth is the limiting factor. Unfortunately this experiment was unable to be performed with the current testbed due to the necessary computational power. As the sweep period of the signal is increased, the synchronization algorithms need to operate over larger numbers of samples to accurately model the channel. Since for analog cancellation, this must be a real-time running process, the speed at which these operation can be performed is crucial. Without a powerful enough host PC to simultaneously run the synchronization algorithm and generate samples for the radios, the experiment cannot be run in analog as intended.

CHAPTER 6

EVERLASTING SECRECY AND IMPROVEMENTS UPON DIGITAL CANCELLATION SCHEMES

As previously mentioned, the motivation behind developing this testbed for analog cancellation of remote interference is everlasting information-theoretic secrecy. Using the realistic values of the analog interference cancellation from the testbed, the next logical step is to return to theory in order to map this performance to secrecy rates. The secrecy rates calculated in this section will inform the capacity at which everlastingly secure information can be transmitted in a practical system. Secrecy rate is defined by the mutual information between the message transmitted by Alice, X, and the received signals at Bob and Eve, Y and Z respectively, in (6.1).

$$R_s = I(X;Y) - I(X;Z) \tag{6.1}$$

This just means that the information of X that is present in Bob's reception, Y, but not present in Eve's reception, Z, is kept secret between Alice and Bob.

By being pessimistic and assuming that the eavesdropper is achieving perfect digital cancellation of the interference signal, the adversary model used in this thesis closely matches the model of intended receivers used in existing cooperative jamming works. For example, in [11] the intended receiver performs interference cancellation in post-digitization processing. This means that the secrecy results derived in this work can be viewed not only as an independent everlasting secrecy scheme, but also as a potential gain over the implementation of [11] if the author's intended receiver were to choose to cancel their interference in analog instead.

6.1 Advantage Due to Limited Adversary Analog to Digital Converter

The testbed was built with a specific secrecy implementation in mind, as derived by Sheikholeslami in [2]. That paper states that a powerful interferer can force an adversary's analog-to-digital converter to operate in a low gain regime to avoid saturation, thus reducing its small signal resolution. This results in permanent loss or deformation of the underlying message signal during digitization. Even in the event that Eve can discover the interference key shared between Alice and Bob and perform interference cancellation on their digitized reception, the message cannot be recovered. All of the message information is lost in the nonlinear process of digitzation. Analog interference cancellation allows for an intended receiver to operate with a narrower ADC span and reduce quantization noise; this is an advantage held by this receiver over an adversary eavesdropper in the scheme.

An exact secrecy analysis based on the exact distributions of the transmitted and residual signals is beyond the scope of this research. However, by assuming that the SoI follows a Gaussian distribution with power spectral density characterized by the results using the testbed from the previous chapter and that the jamming is uniform with similarly characterized power spectral density, rough estimates for the gain can be calculated.

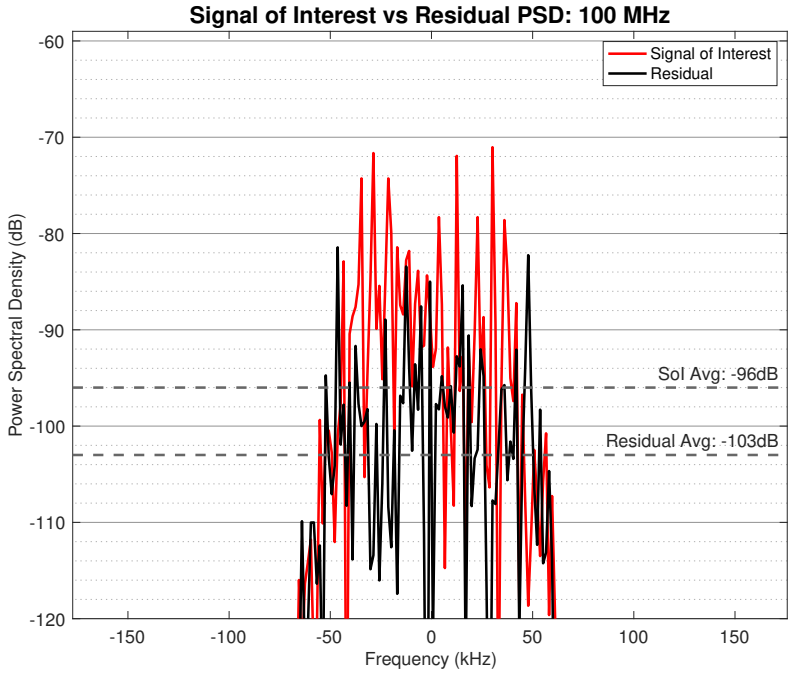
The results from Sheikholeslami were shown under the assumption that any amount of interference can be cancelled at the intended receiver, thus producing significant secrecy rates even against a superior adversary receiver. In practice, as highlighted throughout this work, interference cancellation is far from a perfect operation. Using the interference and SoI power levels, P_I and P_S, results generated using the testbed described in Chapter 4 and shown by Figure 6.1b, the necessary parameters to find secrecy rate can be calculated. The power of a uniform interference spanning from $-c$ to c can be found as the second moment of its distribution, $P_I = \int_{-c}^{c} \frac{1}{2c} x^2 \, dx = \frac{c^2}{3}$. From

here, the interference amplitude can be calculated from the known P_I as $c = \sqrt{3P_I}$. Eve's ADC span which maximizes the mutual information between the signal and her reception turns out to be $2l\sigma$, where sigma is the standard deviation of the SoI, and $l = 2.5$ [2]. This gives $2l\sigma = 5\sqrt{P_S}$. These values are used to determine k, the number of key-bits per interference symbol that can be successfully cancelled.

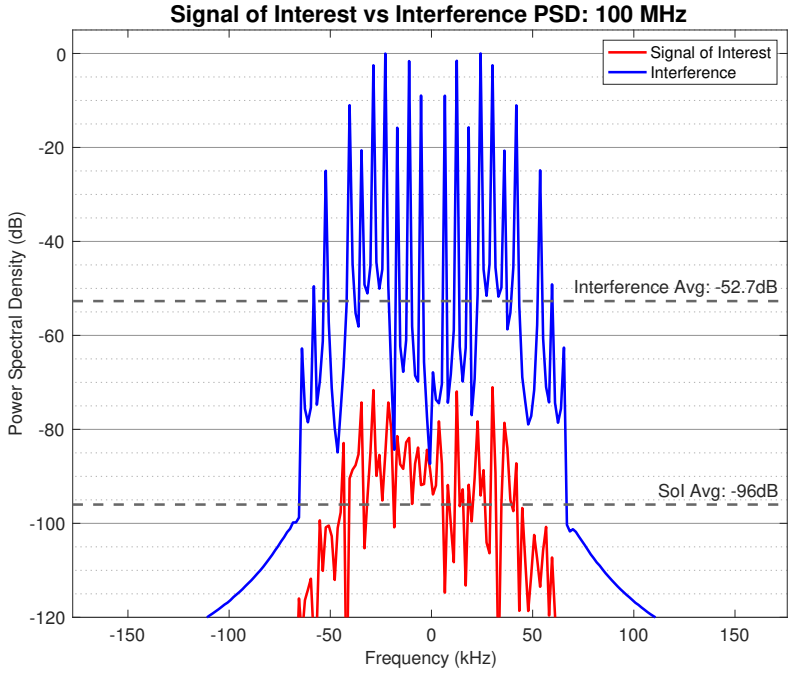
$$(2^k - 1) \times 2l\sigma = 2c \tag{6.2}$$

From (6.2), the ADC-attacking secrecy architecture is capable of supporting cancellation of about $k = 6.8$ key-bits per jamming symbol for an interference-to-SoI ratio of 43 dB. From results in [2] shown by Figure 2.5, this corresponds to a secrecy rate of approximately 2.3 bits/symbol over an eavesdropper performing perfect digital cancellation with the same number of ADC bits as the intended receiver, or an enhancement of the secrecy rate in standard cooperative jamming schemes by the same amount. It is important to note that the derivation in [2] considers idealistic Gaussian, and thus maximum channel capacity achieving, message signals. A real system would not achieve such a high capacity for the intended receiver without ideal Gaussian message, meaning that the rates given here represent an upper bound on secrecy rates seen in practice.

In Figure 6.1, the power levels depicted for each signal are relative to the interference (blue curve) power level. Since Bob performs analog cancellation, his receiver sees a red message signal that is more powerful than the black residual interference (Figure 6.1a); thus, information can be recovered with relative ease. Eve, without any cancellation stage before their receiver, is relegated to recovering the red SoI from underneath the more powerful blue interference (Figure 6.1b).



(a)



(b)

Figure 6.1: Frequency domain representations of the signals received by the intended receiver, Bob (a), and the eavesdropper, Eve (b).

6.2 Forcing an Adversary Amplifier into Saturation

6.2.1 The Model

Given the success in achieving everlasting secrecy by attacking the nonlinearity of an adversary ADC trying to digitize a small message in the presence of a large interferer, could the nonlinear behavior of their receive amplifier be similarly taken advantage of? If an adversary is to perform digital interference cancellation through a nonlinearity, after passing the received interference and message combination, then they would need to overcome additional noise introduced by the nonlinear interaction with the interferer. While in the previous section, perfect digital cancellation of the received interference is assumed, meaning there is no residual noise leftover from the process, that would require either an idealistic linear (and therefore compression-less) amplifier in their front end, or intensive nonlinear modeling of their amplifier performance taken into account when performing cancellation.

Even when the amplifier input is backed off of the saturation point, large signals passing through an amplifier are subject to some gain compression. This is the event where the amplifier does not provide linear gain for a given input power level. This results in a distorted output compared to the expected linear gain model usually assumed in a system.

This is an issue that the intended receiver is not subjected to as it performs analog cancellation prior to the signal reaching its receive amplifier. Even if the initial reception of the learning sequence does have some level of compression to it, the distortion is quickly diminished as the cancellation attenuates the incoming interference causing the compression. This provides yet another advantage to the intended receiver performing analog interference cancellation over an adversary performing cancellation in digital, post-transmission. The wiretap channel model representing the nonlinear amplification advantage held by an intended receiver is shown in Figure 6.2, where

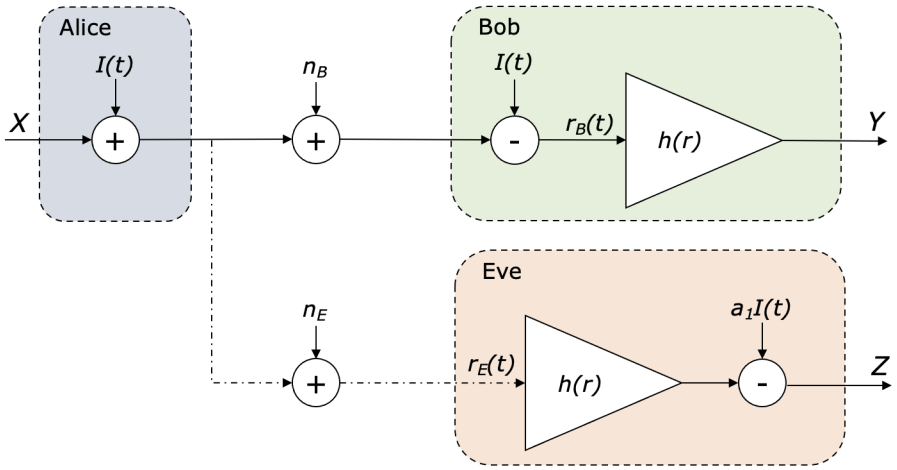


Figure 6.2: Wiretap block diagram of the nonlinear amplifier compression model.

$h(r)$ is the nonlinear transfer function of the receiver amplifier and a_1 is the first-order (linear) coefficient of $h(r)$ used by Eve to model the amplifier.

As derived in what follows, the mutual information needed to calculate the secrecy rate of this wiretap channel from (6.1) depends on various probability density functions (PDFs) of the corresponding signals. In order to make this derivation possible, numerous assumptions are made about the wiretap channel. First, assume that the message signal X will always be small enough to be treated with only the localized linear (compression-less) gain of the amplifier transfer function about $r = 0$. In this scenario, the message signal will not contribute to any residual noise in Eve's reception. This is reasonable, as by design of this system, the message signal will be orders of magnitude smaller than an interference signal that is already backed off the amplifier saturation point (but still in compression). It is also assumed that Eve models the amplifier's gain as an ideal amplifier whose gain is the same local linear fit about $r = 0$ for the entire range of the amplifier input. When performing digital cancellation after recording, Eve will achieve perfect cancellation of any and only first-order interference terms in the amplifier output. The amplifier transfer function used in this derivation (6.3) is the best performing model when compared to actual

data in [29].

$$h(r) = \frac{2}{\pi} V_s \arctan(\alpha r) \tag{6.3}$$

In this model, V_s is the saturation voltage of the amplifier while α is a coefficient that determines the gain of the model. The values of these parameters are determined by best fitting the function $h(r)$ to the commonly used third-order amplifier model, $h_3(r)$, that can be defined using the gain, k_1 and input third-order intercept point (IIP3). IIP3 and k_1 are operating specifications provided of a given system, where IIP3 is defined with respect to the system impedance, Z_o.

$$h_3(r) = k_1 r - k_3 r^3 \tag{6.4}$$

$$k_3 = \frac{3k_1}{\text{IIP3} \times 8Z_0} \tag{6.5}$$

Finally, the linear gain assumed by Eve, A_E, under this model can then be found by taking the coefficient of the first-order term in the Taylor-series expansion of $h(r)$ around $r = 0$, such that $A_E = \frac{2}{\pi} V_s \alpha$.

These assumptions allow for the outputs of the wiretap model to be simplified to the forms (6.6) and (6.7). Here, n_B and n_E are Bob and Eve's respective channel noises, but from this point forward they are assumed to have the same statistics. N_A is the residual interference left over after Eve has performed first-order cancellation of their amplifier output.

$$Y = A_E(X + n_B) \tag{6.6}$$

$$Z = A_E(X + n_E) + N_A \tag{6.7}$$

6.2.2 Derivation of Mutual Information

Calculating the exact mutual information between two distributions is straightforward if their joint distribution is known. Even when it is not, conditional entropy

provides a way forward without joint probabilities defined by the differential entropy relation in (6.8).

$$\begin{aligned} I(X;Y) &= h(Y) - h(Y|X) \\ &= \int_{-\infty}^{\infty} -f_Y(y)\log(f_Y(y))\,dy \\ &\quad - \int_{-\infty}^{\infty} f_X(x) \int_{-\infty}^{\infty} -f_{Y|X=x}(y)\log(f_{Y|X=x}(y))\,dydx \end{aligned} \tag{6.8}$$

The same expression can be used to find the mutual information between X and Z, $I(X;Z)$, by substituting Z in for Y. With this useful definition, the only information needed to calculate the secrecy rate of this wiretap channel are the PDFs of the three key signals, $f_X(x)$,$f_Y(y)$,$f_Z(z)$, and the conditional PDFs of the outputs in regards to a known input, $f_{Y|X=x}(y)$ and $f_{Z|X=x}(z)$.

The channels between Alice and the two receivers are modeled as AWGN. Like the previous section, a statistical analysis using exact signal distributions for X and I is beyond the scope of this work. Therefore, it was decided to model the message signal X and the interference signal I as zero-mean Gaussian signals. The known PDF of a Gaussian $\mathcal{N}(\mu,\sigma^2)$ is defined in (6.9), where μ is the mean of the distribution and σ^2 is its variance.

$$\phi(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \tag{6.9}$$

By making $X \sim \mathcal{N}(0,\sigma_X^2)$ and $n_B \sim \mathcal{N}(0,\sigma_n^2)$, their PDFs are known. The PDF of X, $f_X(x)$, is of particular significance as it is one of the necessary functions for calculating mutual information. From (6.6), Y is a linear combination of these two Gaussian distributions. By the properties of Gaussian random variables, the linear combination of the two is also Gaussian. That means Y has a Gaussian PDF that can be found from the mean and variances of the two components. Therefore it is known that $Y \sim \mathcal{N}(0, A_E^2(\sigma_X^2+\sigma_n^2))$ and:

$$f_Y(y) = \frac{1}{\sqrt{2\pi A_E^2(\sigma_X^2 + \sigma_n^2)}} \exp\left(-\frac{y^2}{2A_E^2(\sigma_X^2 + \sigma_n^2)}\right) \tag{6.10}$$

The only necessary PDF remaining to calculate the mutual information between X and Y is the conditional PDF of $(Y|X = x)$. For any $X = x$, the PDF of the message becomes localized at the value x. This essentially means $X \sim \mathcal{N}(x, 0)$. Applying this to the derivation used for $f_Y(y)$ above, then $(Y|X = x) \sim \mathcal{N}(x, A_E^2\sigma_n^2)$ and:

$$f_{Y|X=x}(y) = \frac{1}{\sqrt{2\pi A_E^2\sigma_n^2}} \exp\left(-\frac{(y-x)^2}{2A_E^2\sigma_n^2}\right) \tag{6.11}$$

In deriving the PDFs $f_Z(z)$ and $f_{Z|X=x}(z)$, the properties of Gaussian random variables no long provide a simple approach, as it is unknown if (and not expected) that the residual noise left after Eve's cancellation, N_A, follows a Gaussian distribution. As was done for the PDFs of Y, $f_Z(z)$ should be defined first. It is assumed that Bob and Eve have similar channels and therefore Eve has to deal with channel noise following similar statistics, $n_E \sim \mathcal{N}(0, \sigma_n^2)$. This gives the new formula $Z = Y + N_A$. The PDF of the sum of two independent random variables is the convolution of those two variables' PDFs. With the PDF of Y, $f_Y(y)$, known from above, $f_Z(z)$ can be numerically calculated if there is a tractable PDF for N_A.

From (6.3), and Eve's assumption that $A_E = V\alpha$, where $V = \frac{2}{\pi}V_s$, N_A can be modeled as (6.12).

$$N_A = V \arctan(\alpha I) - V\alpha I \tag{6.12}$$

Note that because of the requirement that X is much smaller than I, it is assumed in this thesis to pass through a perfectly linear amplifier, and not contribute to the nonlinear output of the amplifier, $V \arctan(\alpha I)$.

From an initial derivation, it known that the PDF for N_A should be zero-mean and symmetric around zero. This means that the PDFs of N_A and $-N_A$ are identical. In order to simplify the signs that carry through this derivation, it will be completed for

$N_A = -N_A = V\alpha I - V\arctan(\alpha I)$, knowing that the resulting PDF will be exactly the same.

Before continuing with the derivation, a useful function, $D(x)$, is defined in (6.13). Even though an inverse function for $D(x)$ cannot be written as a simple function, it is a monotonically increasing function (shown by Figure 6.3) and therefore is invertible. This can also be proven as the derivative of $D(x)$, $\frac{\partial D}{\partial x}(x) = 1 - \frac{1}{1+x^2}$, is positive for all values of x. This means a function $D^{-1}(y)$ does exist such that $D^{-1}(D(x)) = x$.

$$D(x) = x - \arctan x \tag{6.13}$$

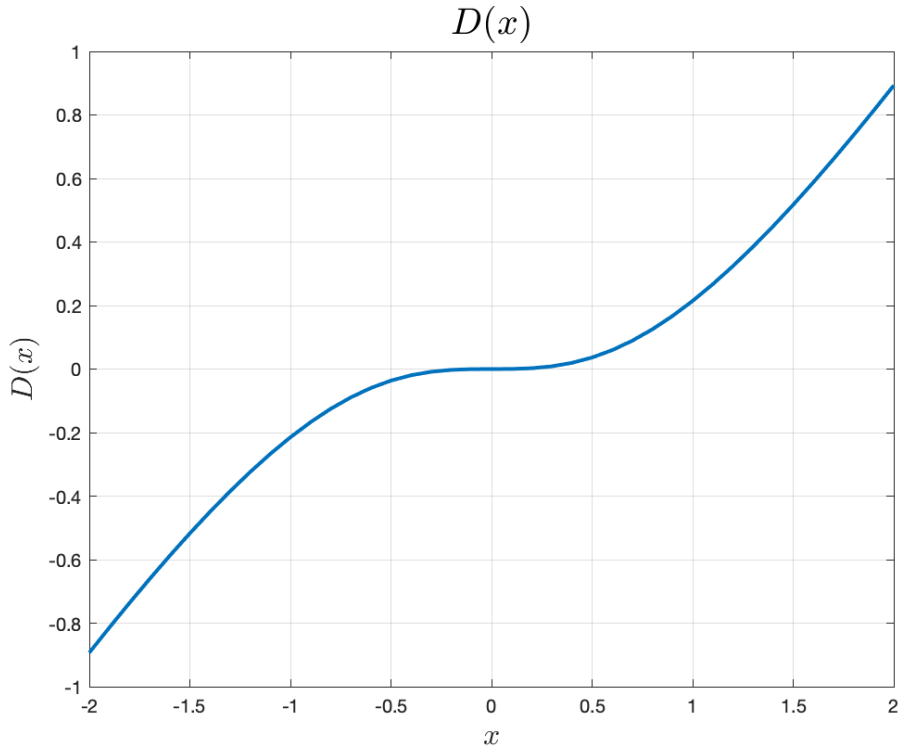


Figure 6.3: A plot of $D(x)$. The function is monotonically increasing, therefore is invertible.

A direct approach is taken in finding the PDF of N_A. That is starting by defining its cumulative distribution function (CDF), $F_{N_A}(n)$ and then taking the derivative.

$$
\begin{aligned}
F_{N_A}(n) &= P\{N_A \leq n\} \\
&= P\{V[\alpha I - \arctan(\alpha I)] \leq n\} \\
&= P\{VD(\alpha I) \leq n\} \\
&= P\left\{I \leq \frac{1}{\alpha} D^{-1}\left(\frac{n}{V}\right)\right\} \\
&= F_I\left(\frac{1}{\alpha} D^{-1}\left(\frac{n}{V}\right)\right)
\end{aligned}
$$

Since it has been assumed $I \sim \mathcal{N}(0, \sigma_I)$, $F_{N_A}(n)$ can be written in terms of the general Gaussian CDF, Φ.

$$
F_{N_A}(n) = \Phi\left(\frac{D^{-1}(\frac{n}{V})}{\alpha\sigma_I}\right) \tag{6.14}
$$

From (6.14), the PDF $f_{N_A}(n)$ can be calculated by differentiating the CDF of N_A with respect to n.

$$
\begin{aligned}
f_{N_A}(n) &= \frac{\partial}{\partial n} F_{N_A}(n) \\
&= \frac{\partial}{\partial n} \Phi\left(\frac{D^{-1}(\frac{n}{V})}{\alpha\sigma_I}\right) \\
&= \frac{1}{V\alpha\sigma_I} \phi\left(\frac{D^{-1}(\frac{n}{V})}{\alpha\sigma_I}\right) \times \frac{\partial D^{-1}(\frac{n}{V})}{\partial n}
\end{aligned}
$$

In the above, ϕ, is the Gaussian PDF expressed in (6.9). This leaves the unknown terms $D^{-1}(\frac{n}{V})$ and its derivative with respect to n. The one-to-one nature of the forward function $D(x)$ guarantees that a one-to-one inverse does exist. Even though this inverse is not definable as a simple function, its value for any input can be found using a lookup table much like other trigonometric functions. Using partial differentiation, the derivative of the inverse function can also be calculated by taking the inverse of the derivative of the forward function as shown below.

$$\begin{aligned}\frac{\partial D^{-1}(\frac{n}{V})}{\partial n} &= \left(\frac{\partial D(x)}{\partial n}\right)^{-1}\Bigg|_{x=D^{-1}(\frac{n}{V})} \\ &= \left(1-\frac{1}{x^2+1}\right)^{-1}\Bigg|_{x=D^{-1}(\frac{n}{V})} \\ &= \frac{\left[D^{-1}(\frac{n}{V})\right]^2+1}{\left[D^{-1}(\frac{n}{V})\right]^2}\end{aligned}$$

With the final missing term in f_{N_A} defined, the PDF (6.15) can be solved numerically for a range of possible values of n. Figure 6.4 shows this PDF using the values for V_s and α that best fit the USRP B210 model based on published performance specifications [30]. The interference power, σ_I^2, is chosen to match that used in the experimental results of Figure 6.1b.

$$f_{N_A}(n) = \frac{1}{V\alpha\sigma_I}\phi\left(\frac{D^{-1}(\frac{n}{V})}{\alpha\sigma_I}\right)\frac{\left[D^{-1}(\frac{n}{V})\right]^2+1}{\left[D^{-1}(\frac{n}{V})\right]^2} \tag{6.15}$$

Interestingly, as n approaches zero, the PDF is asymptotic, approaching infinity. Since this is a real, implementable signal that can be modeled accurately in simulation, it is unexpected for it to behave this way. In order to make the PDF tractable, and therefore useful in calculating the secrecy rate of the wiretap model, the asymptote is terminated. The termination value is determined such the the PDF meets the axiom of probability that its total probability should integrate to one. This termination results in a PDF that still matches the distributions of simulation results using large random sample sets.

As expected, $f_{N_A}(n)$ is zero-mean and symmetric about zero. While the amplitude of N_A is small, the amplitude of the message X is as well, and thus N_A can still impact Eve's ability to receive the message. This will be shown by the reduced mutual information between X and Z compared to X and Y. To calculate $I(X;Z)$, $f_Z(z)$ is

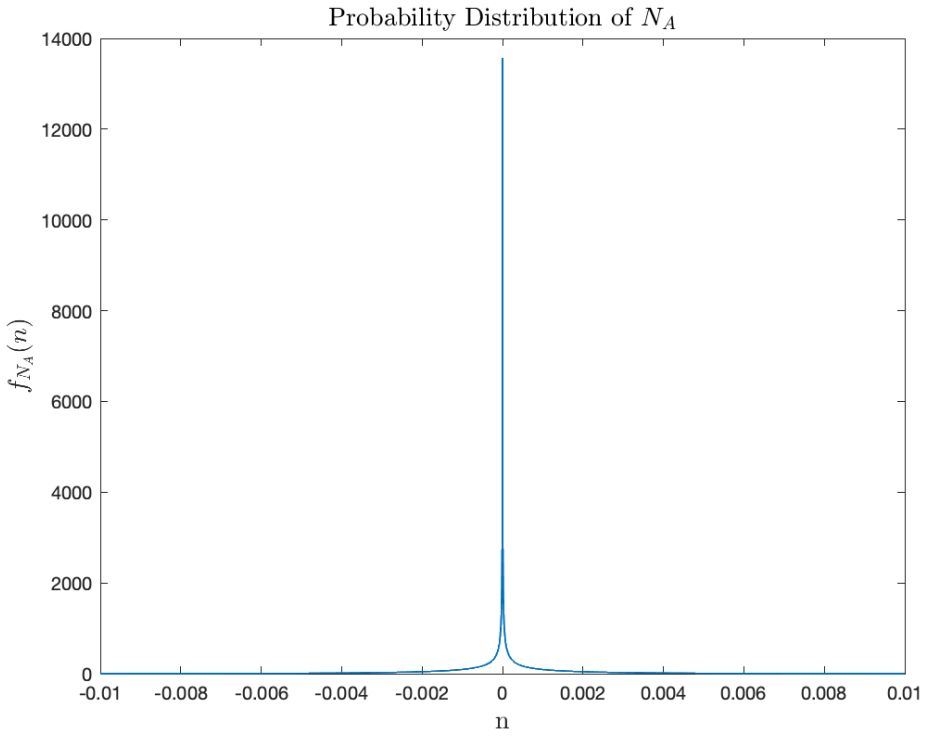


Figure 6.4: The probability density function of N_A plotted for $V_s = 0.02$, $\alpha = 360$, and $\sigma_I = 0.00177$.

still needed. Since $Z = A_E(X + n_E) + N_A = Y + N_A$ and the PDFs of Y and N_A are both known, then the PDF of Z can be calculated in (6.16), where $f_Y(y)$ is the zero-mean Gaussian PDF of Y defined in (6.10).

$$f_Z(z) = f_Y(y) * f_{N_A}(n) \tag{6.16}$$

As for $f_{Z|X=x}(z)$, the derived Gaussian PDF for $Y|X = x$ can also be used again. For any given $X = x$, Z can be written as $(Z|X = x) = (Y|X = x)+(N_A|X = x)$, but since N_A was modeled without the inclusion of the message signal, it is independent from X; therefore $(Z|X = x) = (Y|X = x) + N_A$, and:

$$f_{Z|X=x}(z) = f_{Y|X=x}(y) * f_{N_A}(n) \tag{6.17}$$

Substituting (6.10) and (6.11) into (6.8) provides a numerical value for $I(X;Y)$ in bits/symbol. The same can be done for $I(X;Z)$ by substituting in (6.16) and (6.17) instead. By (6.1) the difference of these two values provides the secrecy rate of the compression-avoidance analog cancellation scheme, also in bits/symbol.

Figure 6.5 displays the achievable secrecy rates of this scheme as the message and interference power levels are adjusted. There are a couple key observations to note. First, since the model used here assumes perfect cancellation of the interference at Bob in analog, the interference to noise ratio (INR) should be chosen to be the limit of a systems analog cancellation capability. The green mark on the surface represents the power levels from Figure 6.1 that were used to calculate the secrecy rate of the ADC-targeting scheme in Section 6.1. It corresponds to about 0.95 bit/symbol. Also note the leveling out of secrecy rate as INR increases (yellow region). This flattened region represents where $I(X;Z)$ goes to zero; thus, the secrecy rate is approaching Bob's channel capacity, $I(X;Y)$. On the other hand, the secrecy rate flattening out to zero as INR decreases (purple region) represents when the interference is not large enough to drive Eve's amplifier into compression. In this scenario, no advantage is gained in performing analog cancellation over digital cancellation post-recording.

When compared to the ADC attacking scheme discussed earlier in this chapter, the secrecy performance for the given signal powers is much lower. Interestingly, the position of the green mark shows that the message power level used in that experiment would not be optimal. Under this scheme, increasing the message power continues to increase the mutual information of X and Y at a quicker rate than that of X and Z, resulting in better secrecy rates. This shows that with a more optimal message power chosen, the given INR can still produce secrecy rates up over 2.3 bits/symbol. Even though Figure 6.5 suggests that this relationship between secrecy rate and message power should continue indefinitely, the model is only valid for small message powers, thus, conclusions should not be implied past the limits of the figure.

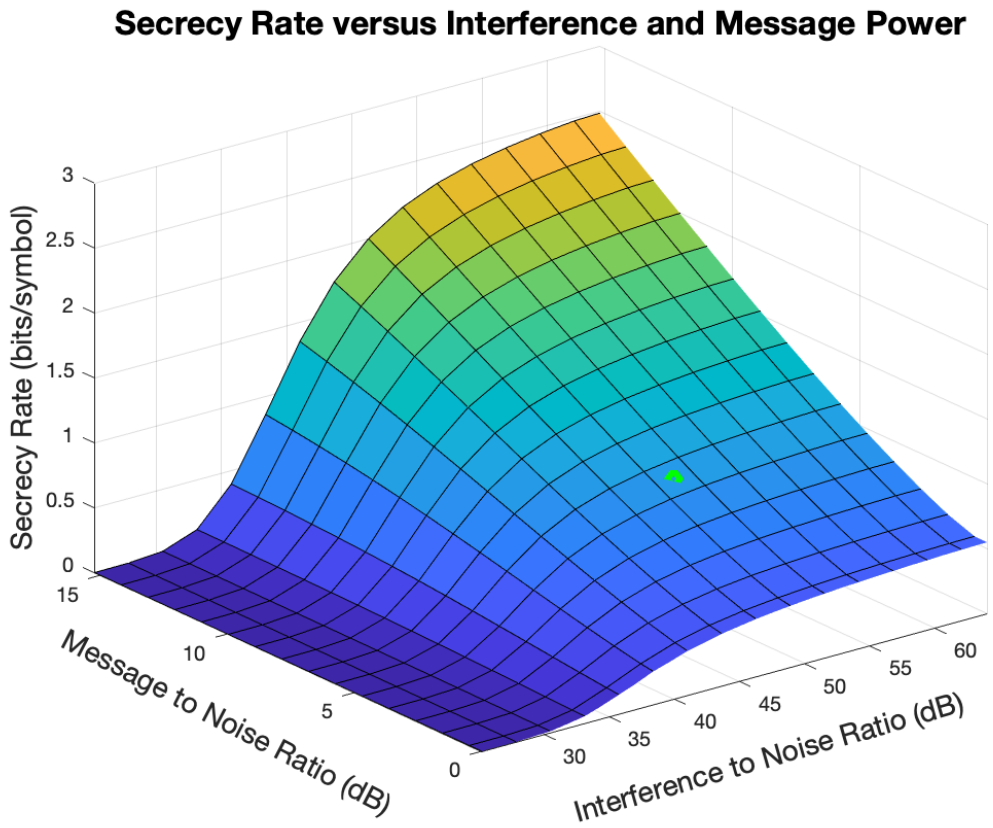


Figure 6.5: Secrecy rate of the compression-avoidance analog cancellation scheme for varying interference and message to noise ratios. The green mark indicates the signal levels that were used in the testbed and their corresponding secrecy rate in the cancellation scheme.

CHAPTER 7

CONCLUSION

This thesis work further explored a cooperative jamming scheme for secret communication scenarios between a message transmitter Alice, their intended receiver Bob, and an adversary eavesdropper listening in, Eve. Here, Alice employs the help of a cooperative system providing an interference known by Bob. With their knowledge of the interference, Bob is able to use interference cancellation techniques to gain an advantage over Eve in recovering the original message.

Inspired by an analog interference cancellation scheme for everlasting secrecy, a hardware testbed was built to characterize the scheme's potential in application. Designed for flexibility with software-defined radios, the testbed performed necessary synchronization algorithms to properly align a cancellation signal's carrier frequency, time delay, phase, and amplitude with that of an incoming known interferer for destructive interference to occur between the two radio frequency signals. Using binary phase-shift keying (BPSK) modulated waveforms, the testbed was capable of maintaining an interference power reduction over 40 dB (with peaks up to 52 dB) at the intended receiver for a 100 MHz carrier frequency. Increased carrier frequencies showed reduced interference cancellation ratios as carrier frequency drift becomes large enough to disrupt the alignment of the interference and cancellation waveforms.

In order to prove robustness of the suggested scheme in the event of a radar-based cooperative jamming transmitter, the testbed was adjusted to measure cancellation performance using frequency-modulated continuous-wave (FMCW) waveforms. This change required implementation of a new carrier frequency estimation method. For

FMCW signals with the same 100 MHz carrier and similar bandwidth and periodicity as the BPSK signals used in the prior experiments, cancellation was once again seen over 40 dB. Increasing the bandwidth (frequency sweep) of the interference waveform quickly diminished cancellation capability, even without the effects of carrier frequency drift on the system. This points to the conclusion that increased FMCW chirp rate, the ratio of frequency sweep to time domain period of the modulation, causes decreased cancellation potential of the system. While beyond the capability of this work, further experiments could isolate the contributions of chirp rate and signal bandwidth individually to this diminished performance.

With the functional testbed providing experimentally achievable interference cancellation levels, focus returned to the motivating theory for everlasting secrecy. Using the framework put forth in the theory, cancellation capability was related to achievable secrecy rates. The testbed performance with BPSK signals suggests everlasting secrecy capacity up to 2.3 bits/symbol over an eavesdropper with the same number of ADC bits as the intended receiver.

Further research was done into how a similar analog cancellation secrecy approach would attack an eavesdropper's receive amplifier instead of their ADC. By deriving the probability density function of a large interference passing through the nonlinear amplifier of an adversary who performs digital cancellation under the assumption that their amplifier operates in its linear regime, everlasting secrecy could be proven to be gained by a receiver performing analog cancellation prior to their own amplifier stage. The nonlinear amplifier model chosen in this study was an inverse tangent based function whose parameters were fit to match published performance of the software-defined radios used in the testbed. Once again matching the proven cancellation capabilities of this testbed to secrecy performance, this new scheme suggested a secrecy capacity around 0.95 bits/symbol. Interestingly, the results of this scheme also suggests that the message signal power could be increased further without an

eavesdropper receiving much information gain. If the message power were to be increased accordingly, the same interference cancellation capability could once again result in secrecy rates near 2.3 bits/symbol.

Future research into this topic could move further into hardware, signal processing, or information theory. In terms of hardware, the test bench could be upgraded to try and improve upon sub-sample period time delay errors. A combination of upgraded host PCs and SDRs, with faster interfaces than USB (such as Ethernet), would allow for greater sampling rates and increased signal bandwidths without losing any fractional time delay resolution. As more powerful SDRs are implemented, work from the host PC could be passed to on-board FPGAs. In particular, cancellation signal correction could be done entirely on the FPGA at interpolated sample rates to achieve better fractional time-delay correction than the digital fractional-delay filter used in the testbed. As signal bandwidths are increased, synchronization algorithms will need to be upgraded to account for multipath of over the channel as well. This would include synchronization using a multi-tap channel model with varying gain, phase, and time delays across the taps. Finally, the theory used to derive secrecy rates with this testbed can be expanded upon. This could range from implementing more representative statistical models for each of the signals involved (rather than assuming Gaussian distributions), to further investigating the asymptotic PDF used for residual interference in Section 6.2.

APPENDIX A

SDR SAMPLE RATES

software-defined radios are designed to seamlessly interface analog and digital signals. In order to process analog data digitally, it must be quantified into samples which is accomplished by the radios analog-to-digital converter. The number of samples needed to accurately represent analog data is set by the Nyquist sampling theorem. This theorem gives that an analog signal must be sampled at twice the rate of its highest frequency component in order to accurately reproduce it.

For most all SDRs, the sampling rate is a controllable setting. The trade off for using increasingly large sample rates is the necessity to deal with the increasing number of samples in timely fashion. This is of particular importance when using real-time signal processing as is needed for analog cancellation.

The USRP B210 SDR utilized in this testbed relies on a host computer to manage all of the signal processing as it does not have a dedicated processor on board to do so itself. While this can be accomplished with a powerful enough host connected to the SDR, there is also the issue of getting samples exchanged between the computer and radio. The B210 is designed as a rapid development device, as such it uses the standard universal serial bus (USB) 3.0 interface for communicating with a host. While this provides convenient compatibility with the large majority of computers, it also presents a bottleneck in the sample exchange pipeline.

The USB 3.0 interface theoretically provides the necessary data streaming rates to handle the B210s maximum sample rate of 56 MHz. Unfortunately this is only the case for 1x1 operation of the B210, meaning when the radio is only used as a single

channel transmitter or a single channel receiver. This is because USB only provides a single data path that must operate in a half-duplex fashion, splitting achievable data rates between samples being received from the radio and samples being sent to the radio for transmission, cutting the achievable single channel sample rate in half [31].

To further complicate the sample exchange, the B210 is based off of a 2x2 (two transmit and two receive channels) RF transceiver integrated circuit, the AD9361. All four of these RF channels are used by the intended receiver in order to achieve analog interference cancellation. This means that the host computer, via GnuRadio, and USB interface need to be capable of both sustaining sample generation and processing and maintaining real time sample exchange rates for four individual streams of samples, just for the intended receiver to function. It was observed that adding more than one transmit or receive channel to the GnuRadio flowgraph resulted in a nonlinear decrease in maximum sample rate achieved by the host PC. For example, a flowgraph that only sent or received "dummy" samples to or from a single channel could reach stable sample rates over 21 MHz. Adding a second channel to this set up dropped the maintainable sample rate down to 7 MHz. The drop in performance continues as the other additional channels are added. The decrease is likely due to additional overhead needed to address and process each channel individually over a single USB interface.

APPENDIX B

IQ BALANCING IN ZERO-IF SDRS

The software-defined radios used in this work, the Ettus Instruments USRP B210, like many other software-defined radios implement a zero intermediate frequency (zero-IF) or homodyne receiver architecture. This means that the incoming radio frequency (RF) signal, is mixed with an carrier frequency that downconverts the signal drectly to or near baseband, meaning zero hertz. This architecture requires fewer frequency dependent components, such as filters and amplifiers, promoting lower costs and flexibility in implementations [7]. This simple design comes with one major downside for quadrature (IQ) signals, imaging.

Imaging is when a up converted or down converted signal that is supposed to exist in the positive frequency domain is also reflected into the negative frequency domain. This is due to the cosine or sine waveform used when mixing with a carrier naturally exist in both the positive and negative frequency domains. Under ideal conditions, there should not be a problem with IQ implementations as the images of the in-phase and quadrature mixing stages will be summed together and cancel each other out. Unfortunately, in real systems this is not the case as, just like with the cancellation performed here, any small difference in the phase delay or attenuation of the in-phase and quadrature receive paths will result in imperfect cancellation.

How well a given system can actually perform this cancellation is known as its image rejection ratio. The USRP B210's transceiver chip is designed to achieve around 50 dB of image rejection for single carrier and narrow band waveforms [7]. The testing done for this work with FMCW waveforms did not reach those limits of

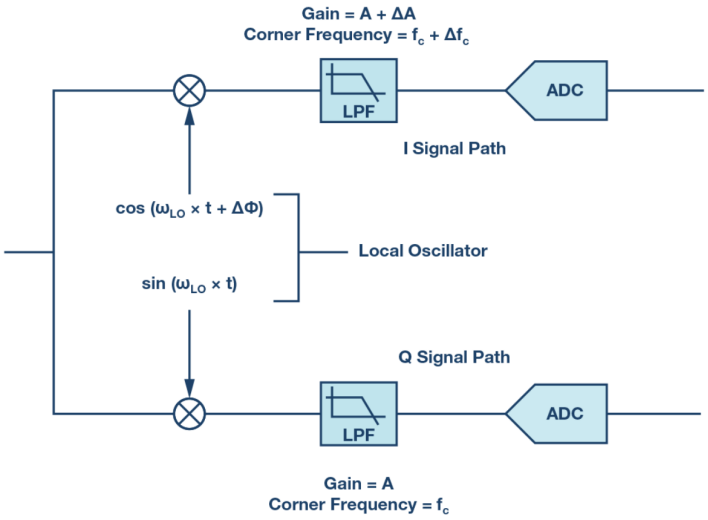


Figure B.1: A simplified zero-IF quadrature receiver architecture from [7].

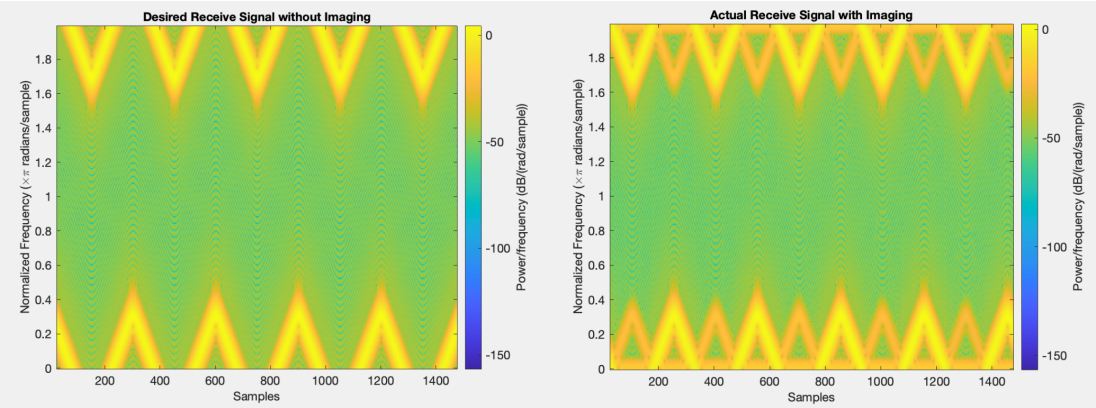


Figure B.2: Example of imaging in received FMCW waveform using USRP B210.

image reduction as shown in Figure B.2. In the figure, the bright yellow triangles are the intended signal being received. The duller yellow triangles between each pair of intended signals are the images. From the scale on the right, the images in the spectrum are only 25-30 dB below the intended signal level. This is a result of the digital image rejection algorithm not performing to the levels suggested by Analog Devices, for the triangular FMCW waveform.

APPENDIX C

GNURADIO FLOWGRAPH AND HARDWARE CONFIGURATION

This appendix serves to provide a pathway for any researcher picking up this project or attempting to accomplish something similar. All of the software work was done using GnuRadio version 3.7. More up to date versions of the library are available, but utilize a different file format which breaks compatibility with the older versions.

The top half of the flowgraph in Figure C.1 shows the message and interference generation and cancellation correction flow. The bottom half of the flowgraph deals with Bob's reception where a Costas loop is used for frequency synchronization. The other synchronization algorithms and sequence controlling take place within the EstimateSync block. This block is an embedded Python block. Sample Python code from the EstimateSync block can be found in Appendix D. Manual adjustments were made to the Python files generated by the companion application in order to allow the top block variables to be shared and adjusted by the EstimateSync block. This is accomplished by making a reference to the parent topblock object within EstimateSync block via the get_from_outerscope function at the top of Appendix D. This function requires the topblock Python file to be run from a dedicated python compiler, as GnuRadio companion does not recognize the get_from_outerscope function. Figure C.2a and C.2b show the two software-defined radios used in the testbed along with their corresponding external hardware components. Note that Bob loops an analog copy of expected interference out and back into their second receiver to solve

an indeterminate sample timing delay issue introduced by the single-stream USB interface.

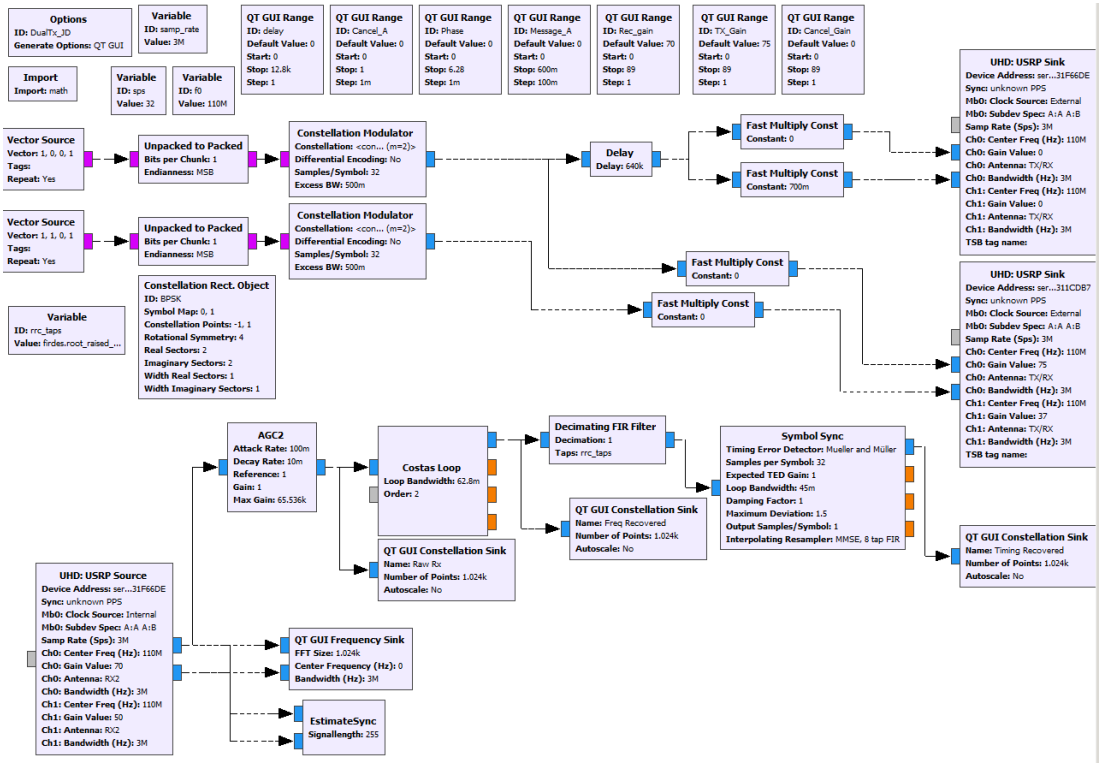
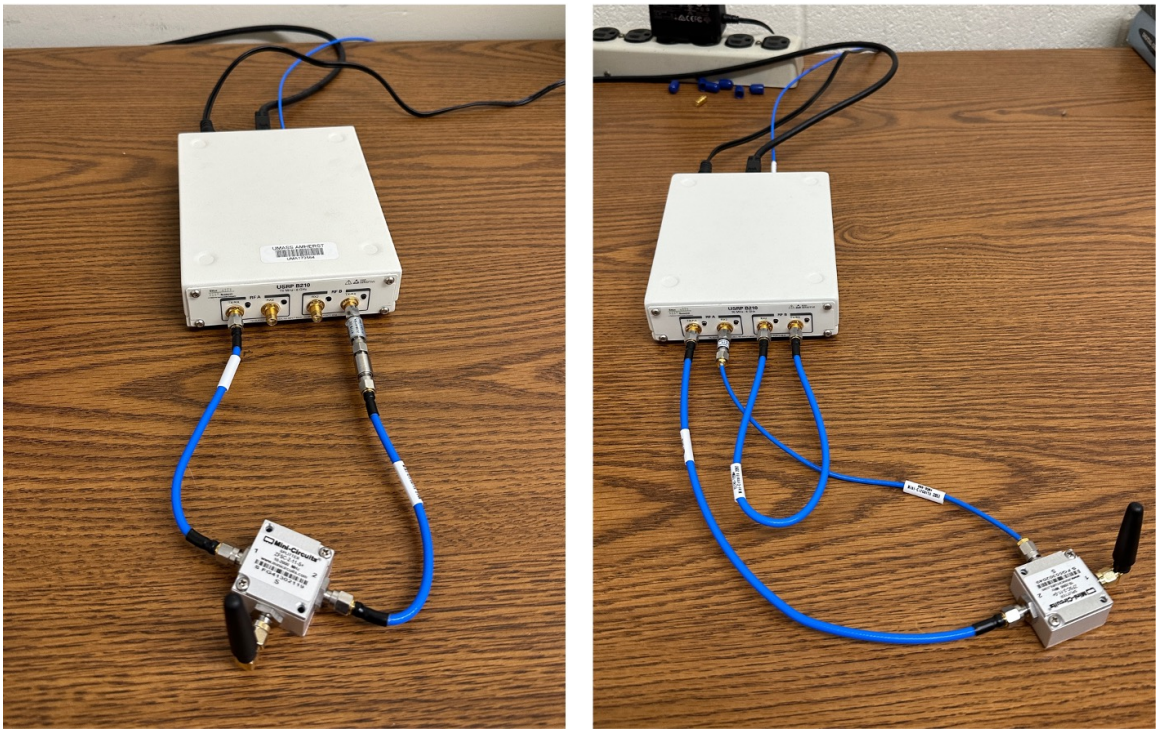


Figure C.1: The original GnuRadio companion flowgraph used in the described testbed.



(a) (b)

Figure C.2: Pictures of the USRP B210s and external components used as (a) Alice and (b) Bob in the test bed.

APPENDIX D

SAMPLE PYTHON CODE OF ESTIMATESYNC BLOCK

```
import math
import numpy as np
import scipy.signal
from gnuradio import gr
import sys
import time

def get_from_outerscope(var_name):
    """Function that will use python's underlying frame functions to return a reference
     to an object further up in the call stack (i.e DualTx_JD)"""
    frame = sys._getframe(2)
    return frame.f_locals[var_name]

class CancelSyncBlock(gr.sync_block):
    """Cancellation Sync Block - Will measure the incoming raw Rx and adjust flowgraph variables
    (delay, phase, cancel_amp) such that the incoming interference is minimized,
    thus the receiver is ready to capture the message"""

    def __init__(self, signal_length=1000):  # only default arguments here
        """arguments to this function show up as parameters in GRC"""
        # Define parent as self from outerscope (The class attempting to initiate this block)
        # Also verify that parent is of the right type
        self.parent = get_from_outerscope("self")
        assert type(self.parent).__name__ == "DualTx_JD"
        # Constructor
        gr.sync_block.__init__(
            self,
            name='Sync',   # will show up in GRC
            in_sig=[np.complex64, np.complex64],
            out_sig=[]
        )
        # Define all of the different variables and flags that will need to
        be remembered between chunks of samples
        self.signal_length = signal_length
        self.done = False
        self.wait = True
        self.waitSamples = 3e6 * 1
        self.cancelOn = False
        self.samplesStored = False
        self.delayCoarseSynced = False
        self.delayFineSync = False
        self.phaseCoarseSynced = False
        self.phaseFineSynced = False
        self.sampleAlign = False
        self.raw_rx = np.zeros(self.signal_length, dtype=np.complex64)
        self.cancel = np.zeros(self.signal_length, dtype=np.complex64)
        self.numSamMeas = self.signal_length
        self.delay = 0
        self.bestDelay = 0
        self.phase = 0
        self.bestPhase = 0
        self.cancelAmp = 0.7
        self.bestCancelA = 0
        self.passedSamples = 0
        self.startTime = 0
        self.startPwr = 1
        self.startPwrdB = 0
        self.cancelGain = self.parent.get_Bob_cancel_gain()
        self.startRxGain = self.parent.get_Rec_gain()
        self.testarray = []
        self.tuneTime = 0
        self.fdftuneTime = 0
        self.freqSync = False
        self.cancelArray = []
        self.previousPower = 0
        self.phaseTurn = True
        self.bestCancellation = 0
        self.Cancellation = 0
        self.heldPowers = []
        self.N = 0
        self.minresidual = []
        self.F = 0
```

```
        self.dF = -0.7
        self.fdftaps = []
        self.fdfSet = False
        self.phaseCompensation = self.parent.phaseCompSwitch()
        self.longCancel = []
        self.longRx = []
        self.appendTime = 0
        self.learningPattern = True
        self.fineFreqSync = True
        self.phaseArray = []

    def ignoresamples(self, numsamples, input_items):
        # print "~~~~~Ignoring " + str(numsamples) + " samples~~~~~"
        self.passedSamples = self.passedSamples + len(input_items[0])
        if self.passedSamples >= numsamples:
            self.passedSamples = 0
            self.wait = False
        return len(input_items[0])

    def avgAmp(self, signal):
        return np.mean(abs(signal))

    def correlation_Array(self, cancel, rx, L = 1):
        SL = self.signal_length * L
        corrArray = np.zeros(SL * 2)
        rx_mag = abs(rx)
        rx_mag = scipy.signal.resample_poly(rx_mag, L, 1)
        cancel_mag = abs(cancel)
        cancel_mag = scipy.signal.resample_poly(cancel_mag, L, 1)
        for i in range(0, 2 * SL):
            corrArray[i] = np.dot(rx_mag[i:SL+i-1], cancel_mag[0:SL-1])
        np.savetxt("CorrArray.csv", corrArray, delimiter=",")
        d = np.mod(np.argmax(corrArray) / float(L), self.signal_length)
        dint = int(round(d))
        dfrac = round((d - dint), 1)
        self.fdftaps = np.sinc(np.linspace(-10, 10, num=21) - dfrac)
        self.parent.set_FDFtaps(self.fdftaps)
        print "\n", np.argmax(corrArray), dfrac, dint, "\n"
        self.bestDelay = dint #np.mod(d_int, self.signal_length)
        self.parent.set_delay(self.bestDelay)
        self.delay = self.bestDelay
        self.delayCoarseSynced = True
        self.wait = True
        self.waitSamples = 5000 * 20
        return int(np.floor(d))

    def test_FDF(self, cancellation):
        if self.dF <= 0.7:
            t = time.time() - self.fdftuneTime
            if t >= 1:
                self.dF += 0.1
                fdfTaps = np.sinc(np.linspace(-10, 10, num=21) - self.dF)
                self.parent.set_FDFtaps(fdfTaps)
                # self.parent.set_FD(self.dF)
                self.fdftuneTime = time.time()
            else:
                self.testarray.append([self.dF, t, cancellation])
        else:
            np.savetxt("Test2.csv", self.testarray, delimiter=",")

    def phaseSyncMMSE(self, input_items):
        # Get Initial Estimate of Phase using MMSE Channel Estimation
        c = np.copy(input_items[0])
        r = np.copy(input_items[1])
        res = r - c
        w = np.matmul(np.transpose(np.conjugate(c)), res)
        res = r - c * w/abs(w)
        for i in range(50):
            I = np.matmul(np.transpose(np.conjugate(c)), res)
            w+= 0.05*I
            cancelo = c * w
            res = r - cancelo
        H = w
        self.bestPhase = np.angle(H) + self.phaseCompensation
        self.parent.set_Phase(self.bestPhase)
        self.phase = self.bestPhase
        self.Pdiff = self.phase
        self.phaseCoarseSynced = True

    def storeInputstoSelf(self, input_items):
        if len(input_items[0]) >= 2 * self.numSamMeas and len(input_items[1]) >= 2 * self.numSamMeas:
            amp = self.avgAmp(input_items[0])
            if amp > 0:
                self.raw_rx = np.copy(input_items[1])
                self.cancel = np.copy(input_items[0])
                self.samplesStored = True
                self.startTime = time.time()
                return len(input_items[1])
        else:
            return 0

    def initTuneCancelAmp(self, input_items):
```

```
        if len(input_items[1]) >= self.signal_length:
            refPower = np.mean(abs(input_items[0][0:2*self.signal_length])**2)
            self.startPwr = np.mean(abs(input_items[1][0:2*self.signal_length])**2)
            self.previousPower = self.startPwr
            self.startPwrdB = 10 * np.log10(self.startPwr)
            rcvrPathLoss = 5+3.35+0.1  # 5+3.35+0.1
            pwrAtComb = self.startPwr * 10**((rcvrPathLoss)/10)
            ratio = pwrAtComb/refPower
            self.cancelAmp = 0.7 * math.sqrt(ratio)
            # print refPower, self.startPwr, self.startPwrdB, rcvrPathLoss, pwrAtComb, ratio, self.cancelAmp
            while self.cancelAmp >= 0.7:
                self.cancelAmp = self.cancelAmp / 1.122
                self.cancelGain += 1
            self.bestCancelA = self.cancelAmp
            self.parent.set_Bob_cancel_gain(self.cancelGain)
            self.parent.set_Cancel_A(self.cancelAmp)
            self.cancelOn = True
            self.wait = True
            self.waitSamples = 500000
            print self.bestDelay, self.bestPhase, self.bestCancelA, self.cancelGain
            return len(input_items[0])
        else:
            return 0

    def updateChannelGain(self, input_items):
        # Timo Huusari, Wideband Self-Adaptive RF Cancellation Circuit for Full-Duplex Radio
        W = np.complex(self.cancelAmp * np.cos(self.phase), self.cancelAmp * np.sin(self.phase))
        res = input_items[1]
        can = input_items[0] * np.complex(np.cos(-self.phaseCompensation), np.sin(-self.phaseCompensation))
        I = np.sum(np.conjugate(can)*res)
        W += 0.05 * I
        self.waitSamples = 35000  # 10000
        if np.abs(W) <= 0.8:
            self.cancelAmp = np.abs(W)
        else:
            self.parent.set_Bob_cancel_gain(self.parent.get_Bob_cancel_gain()+1)
        self.parent.set_Cancel_A(self.cancelAmp)
        self.phase = np.angle(W)
        self.parent.set_Phase(self.phase)
        self.wait = True

    def collectData(self, input_items):
        powerW = np.mean(np.abs(np.square(input_items[1])))
        powerdB = 10 * np.log10(powerW)
        self.Cancellation = cancel = self.startPwrdB - powerdB
        t = time.time()
        tlapse = t - self.startTime
        self.cancelArray.append(
            [tlapse, cancel, self.previousPower, powerW, self.cancelAmp, self.phase])
        self.phaseArray.append(self.phase)

    def work(self, input_items, output_items):
        if self.wait:
            return self.ignoresamples(self.waitSamples, input_items)
        self.freqSync = True
        if not self.freqSync:
            if time.time() - self.tuneTime > 0.1:
                self.parent.tune_Bob_LO()
                array = self.parent.freqEstimateArray
                L = len(array)
                freqDiff = abs(array[L-1] - array[L-2])
                if L > 20 and freqDiff < 0.01:
                    self.freqSync = True
                    self.parent.tune_Bob_LO(Rx=True)
                if L == 4:
                    self.parent.set_Loop_BW(0.0001)
                elif L == 6:
                    self.parent.set_Loop_BW(0.00001)
                elif L == 8:
                    self.parent.set_Loop_BW(0.0000001)
                self.tuneTime = time.time()
        elif not self.samplesStored:
            return self.storeInputstoSelf(input_items)
        elif not self.delayCoarseSynced:
            self.correlation_Array(self.cancel, self.raw_rx, L=16)
            return len(input_items[1])
        elif not self.phaseCoarseSynced:
            rx = input_items[1]
            cancel = input_items[0]
            self.phaseSyncMMSE(input_items)
        elif not self.cancelOn:
            return self.initTuneCancelAmp(input_items)
        else:
            # return len(input_items[1])
            if not self.phaseFineSynced:
                self.updateChannelGain(input_items)
            self.collectData(input_items)
        return len(input_items[1])
```

BIBLIOGRAPHY

[1] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, October 1949.

[2] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Jamming based on an ephemeral key to obtain everlasting security in wireless environments," *IEEE Transactions on Wireless Communications*, vol. 14, no. 11, pp. 6072–6081, November 2015.

[3] J. Freet, "Disentangle rf amplifier specs: output voltage/current and 1db compression point," *TI E2E Design Support*, Jun 2016. [Online]. Available: e2e.ti.com

[4] W. Commons. (2021) Superheterodyne receiver block diagram. [Online]. Available: https://en.m.wikipedia.org/wiki/File:Superheterodyne_receiver_block_diagram_2.svg

[5] T. Tuukkanen. (2009) Software defined radio scheme - adopted by ltcdr topi tuukkanen, project manager, finnish software radio demonstrator from various scientific articles, studies, conference papers etc in public domain. [Online]. Available: https://commons.wikimedia.org/wiki/File:SDR_et_WF.svg

[6] M. B. Steer, *Radar Systems*. NC State University, 2019, ch. 5.

[7] P. Wiers, "Mirror, mirror on the wall-understanding image rejection and its impact on desired signals," www.analog.com/en/analog-dialogue, Aug 2017.

[8] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Everlasting secrecy by exploiting non-idealities of the eavesdropper's receiver," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1828–1839, September 2013.

[9] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[10] E. R. Alotaibi and K. A. Hamdi, "Optimal cooperative relaying and jamming for secure communication," *IEEE Wireless Communications Letters*, vol. 4, no. 6, pp. 689–692, December 2015.

[11] W. Guo, H. Zhao, and Y. Tang, "Testbed for cooperative jamming cancellation in physical layer security," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 240–243, February 2020.

[12] J. W. Kwak, M. S. Sim, J. S. P. I. W Kang, J. Park, and C. B. Chae, "A comparative study of analog/digital self-interference cancellation for full duplex radios," in *53rd Asilomar Conference on Signals, Systems, and Computers*, 2019, pp. 1114–1119.

[13] S. J. Aboud, "An efficient method for attack rsa scheme," in *Second International Conference on the Applications of Digital Information and Web Technologies*, 2009, pp. 587–591.

[14] S. Goldwasser, J. C. Lagarias, A. M. Odlyzko, K. S. McCurley, and A. K. Lenstra, "The discrete logarithm problem," in *Cryptology and computational number theory*, C. Pomerance, Ed. Providence, R.I, Colorado: American Mathematical Society p. 49, 1990.

[15] M. Bloch and J. N. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *46th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, 2008, pp. 818–825.

[16] *USRP B200/B210 Bus Series*, Ettus Research.

[17] *RF Agile Transceiver*, Analog Devices, November 2016.

[18] "Mainpage," March 2022. [Online]. Available: wiki.gnuradio.org.https://wiki.gnuradio.org/index.php/Main_Page

[19] S. Dolatshahi, A. Polak, and D. L. Goeckel, "Identification of wireless users via power amplifier imperfections," in *2010 Conference Record of the Forty Fourth Asilomar Conference on Signals, Systems and Computers*, 2010, pp. 1553–1557.

[20] W. Guo, H. Zhao, W. Ma, C. Li, Z. Lu, and Y. Tang, "Effect of frequency offset on cooperative jamming cancellation in physical layer security," in *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018, pp. 1–5.

[21] C. R. Johnson, W. A. Sethares, and A. G. Klein, *Carrier Recovery*. Cambridge University Press, 2011, ch. 10, pp. 192–225.

[22] W. Guo, C. Li, H. Zhao, R. Wen, and Y. Tang, "Comprehensive effects of imperfect synchronization and channel estimation on known interference cancellation," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 457–470, 2020.

[23] T. Laakso, V. Valimaki, M. Karjalainen, and U. Laine, "Splitting the unit delay [fir/all pass filters design]," *IEEE Signal Processing Magazine*, vol. 13, no. 1, pp. 30–60, 1996.

[24] C. Li, H. Zhao, F. Wu, and Y. Tang, "Digital self-interference cancellation with variable fractional delay fir filter for full-duplex radios," *IEEE Communications Letters*, vol. 22, no. 5, pp. 1082–1085, 2018.

[25] T. Huusari, Y.-S. Choi, P. Liikkanen, D. Korpi, S. Talwar, and M. Valkama, "Wideband self-adaptive rf cancellation circuit for full-duplex radio: Operating principle and measurements," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, 2015, pp. 1–7.

[26] H. Arslan and G. E. Bottomley, "Channel estimation in narrowband wireless communication systems," *Wireless Communications and Mobile Computing*, vol. 1, no. 2, pp. 201–219, 2001. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.14

[27] Z. Jie, Z. Yun, S. Ling, and Z. Ping, "Effects of frequency-offset on the performance of ofdm systems," in *International Conference on Communication Technology Proceedings, 2003. ICCT 2003.*, vol. 2, 2003, pp. 1029–1032 vol.2.

[28] U. Mengali and M. Morelli, "Data-aided frequency estimation for burst digital transmission," *IEEE Transactions on Communications*, vol. 45, no. 1, pp. 23–25, 1997.

[29] X.-B. Zeng, Q.-M. Hu, J.-M. He, Q.-P. Tu, and X.-J. Yu, "High power rf amplifier's new nonlinear models," in *2005 Asia-Pacific Microwave Conference Proceedings*, vol. 2, 2005.

[30] "B200 rf performance," May 2016. [Online]. Available: http://kb.ettus.com/File:B200_RF_Performance.pdf

[31] "About usrp bandwidths and sampling rates," May 2016. [Online]. Available: https://kb.ettus.com/About_USRP_Bandwidths_and_Sampling_Rates