6-28-2019

Ultra-Wideband Secure Communications and Direct RF Sampling Transceivers

Dimitrios Siafarikas
Florida International University, dsiaf001@fiu.edu

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

ULTRA-WIDEBAND SECURE COMMUNICATIONS AND DIRECT RF SAMPLING TRANSCEIVERS

A dissertation submitted in partial fulfillment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY

in

ELECTRICAL AND COMPUTER ENGINEERING

by

Dimitrios Siafarikas

2019

To: Dean John L. Volakis
College of Engineering and Computing

This dissertation, written by Dimitrios Siafarikas, and entitled Ultra-wideband Secure Communications and Direct RF Sampling Transceivers, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Stavros Georgakopoulos

Elias A. Alwan

Ioannis Zisis

John L. Volakis, Major Professor

Date of Defense: June 28, 2019

The dissertation of Dimitrios Siafarikas is approved.

Dean John L. Volakis
College of Engineering and Computing

Andres G. Gil
Vice President for Research and Economic Development
and Dean of the University Graduate School

Florida International University, 2019

DEDICATION

To all the people out there struggling to find a meaning in life.

I am rooting for you.

ACKNOWLEDGMENTS

I would like to express my utmost and undying gratitude to my advisor, Professor John Volakis, for his mentorship, for trusting me to deliver all the projects and for undertaking the onerous task of shaping me into a successful engineer. I cannot even begin to describe my appreciation for all the guidance and support you showed me over the past five years. My future endeavors will be due in large part to you. You will never be forgotten. But most importantly, I want to thank you for not giving up on me. I would also like to thank Professor Elias A. Alwan for helping me take my first steps in the academic world and Professors Waleed Khalil and Ayman Fayed from The Ohio State University and Nir Corse from Motorola Solutions for the trove of knowledge they transferred to me.

A special thank you note goes to Anestis Arampatzis (tootski?), Harris Orfanidis (E nai!) and Anestis Iliadis. Without them, the nights in Miami would have been completely different. The once-in-a-lifetime experiences will never be forgotten. You will be missed.

I want to extend my deepest gratitude to Club Space and all the amazing artists for the magical moments on the terrace and all the sunrises that took place. I do hope that all #SpaceInvaders will continue supporting this community for years to come. A special thanks to Eric Estornel aka Maceo Plex aka Mariel Ito aka Maetrik. You have been the greatest source of inspiration I could have asked for. Even When the Lights Are Out you can find me diving into Mutant Series and Solar. Keep doing what you are doing best!

I would like to thank all my classmates I had the pleasure to interact with. I feel lucky I shared a multicultural environment with (in alphabetic order): Abe Akhiat, Shubhendu Bhardwaj, Yonathan Bonan, Max Carvahlo, Ushe Chipengo, Daerhan, Brock DeLong, Alfredo Gonzalez, Alexander Hovsepian, Alexander John-

son, Cedric Lee, Daniel Lepkowski, Daron Mac, Mahmoud Sharafi Masouleh, Matt Nichols, Anthony Nunez, Dimitris 'D1' Papantonis, Md Rakibur Rahman, Nicholas Russo, Yousuf Shafiq, Satheesh Bojja Venkatakrishnan, Dieff Vital, Steve Watt, Constantine Zekios, Jingni Zhong, Rashed Zuboraj.

My dearest thank-you notes go to Dimitris Kakarontzas and Mark Tousias for all the laughs, all the tears, all the joy we shared together since we were kids. You are the brothers I never had.

Kelly Kostala for following me on my very first steps into this journey. You will always have a special place in my heart.

Thank you Simona Lekht for supporting me through all the difficult moments. Our bond will never fade away.

Christos Bouzounis, Petros and Nikos Avradopoulos for their support during all these years. You were like fathers to me and I will make sure you will live forever.

To all the people that directly and indirectly contributed and shaped my personality that I have forgotten to mention, thank you for your contributions.

But, most importantly I would like to thank my beloved family: Pavlos, Yioula and Athina for their continued support, for always believing in me, supporting my education, and providing me with guidance as I face difficult decisions in life.

-Thank you

Dimitris 'Rafe' Siafarikas

ABSTRACT OF THE DISSERTATION

ULTRA-WIDEBAND SECURE COMMUNICATIONS AND

DIRECT RF SAMPLING TRANSCEIVERS

by

Dimitrios Siafarikas

Florida International University, 2019

Miami, Florida

Professor John L. Volakis, Major Professor

Larger wireless device bandwidth results in new capabilities in terms of higher data rates and security. The 5G evolution is focused on exploiting larger bandwidths for higher though-puts. Interference and co-existence issues can also be addressed by the larger bandwidth in the 5G and 6G evolution.

This dissertation introduces a novel Ultra-wideband (UWB) Code Division Multiple Access (CDMA) technique to exploit the largest bandwidth available in the upcoming wireless connectivity scenarios. The dissertation addresses interference immunity, secure communication at the physical layer and longer distance communication due to increased receiver sensitivity.

The dissertation presents the design, workflow, simulations, hardware prototypes and experimental measurements to demonstrate the benefits of wideband Code-Division-Multiple-Access. Specifically, a description of each of the hardware and software stages is presented along with simulations of different scenarios using a test-bench and open-field measurements. The measurements provided experimental validation carried out to demonstrate the interference mitigation capabilities. In addition, Direct RF sampling techniques are employed to handle the larger bandwidth and avoid analog components. Additionally, a transmit and receive chain is designed and implemented at 28 GHz to provide a proof-of-concept for future 5G

applications. The proposed wideband transceiver is also used to demonstrate higher accuracy direction finding, as much as 10 times improvement.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background

In the past few years, we have witnessed a dramatic increase in data transfers using wireless devices. Additionally, there is a growing and steady demand for high speed communications and for data services, particularly for Internet-of-Things (IoT) devices. According to a recent report [del], mobile data traffic in the US will quadruple between 2016 and 2021. Notably, the report suggests that an investment of about $130 billion to $150 billion could be required over the next seven years. It can be said that the current infrastructure is not adequate to support the expected growth in wireless data.

Wireless communication systems have come a long way since their inception back in 1980. Nevertheless, the ever increasing demand from end-users particularly for higher resolution video streaming and smaller latency has led to much research and investment. Fig. 1.1 show the path to 5G/mmWave communications and presents a comparison between applications and the typical data rates for each generation. Next-gen systems such as 5G NR promise much higher data rates and capacity. Specifically, 5G systems are expected to deliver 100 times increase in data rates, a 1000 times increase in system capacity, less than 1 ms latency (base station to end end-user), 100 times more energy efficient systems and a 1000 times more dense environment.

With the advent of new protocols and standards, wireless communications are developing rapidly. To keep their systems up to date, wireless systems manufacturers and service providers must respond to changes as they occur by upgrading systems to incorporate the latest innovations.

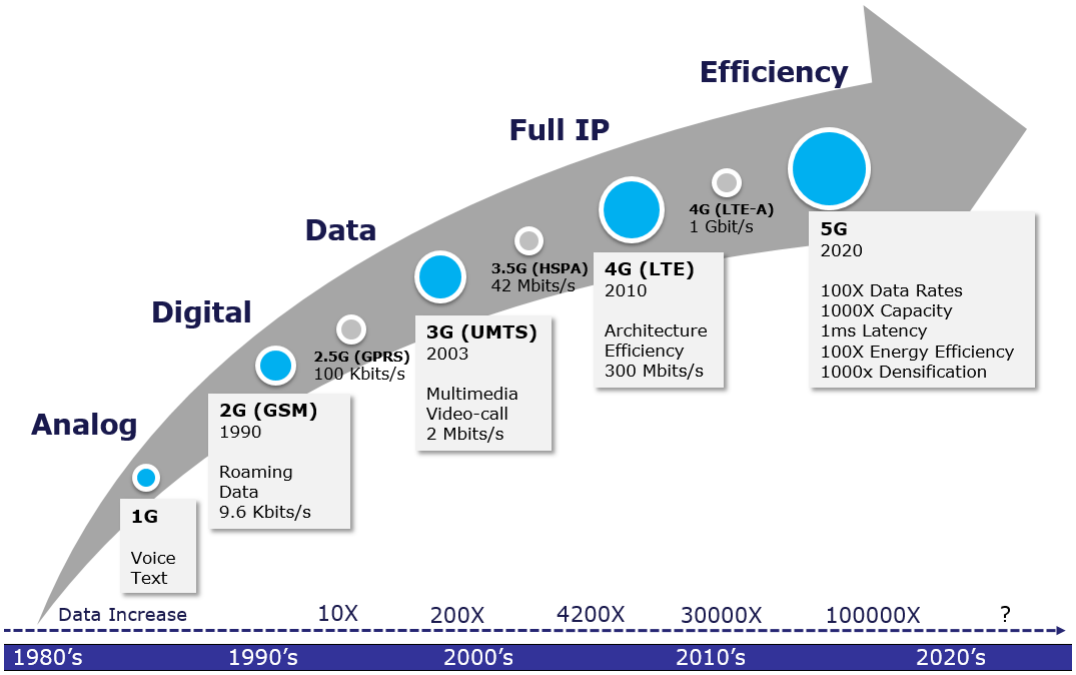

Figure 1.1: Path to 5G and mmWave communications (data sourced from 3GPP specifications [3GP].

A solution to the aforementioned issues can be the use of software radios or software-defined radios (SDRs). Joe Mitola first introduced the term Software-defined radio when referring to re-programmable radios back in 1991 [Mit95]. Currently, there is no existing definition of SDR nor the level of reconfigurability that would constitute a radio as software-defined. However, it is common to see system parameters such as frequency range, bandwidth and amplifier gain controlled by software through some kind of interface with a host controller. This controller can be a Field-Programmable-Gate-Array (FPGA) or an Application-Specific-Integrated-Circuit (ASIC).

There are quite a few benefits from adopting Software Defined Radio techniques for communication systems. First of all, a common set of hardware offers the ability to receive and transmit various modulation methods and coding schemes without

the need of redesign. Simply, a software update can provide the end-user the option to connect, transmit and receive within a different network.

The ability to reconfigure or reprogram some or all of the functionalities of the device itself without the need of a redesign can result in a multi-functional device capable of operating at different frequency bands using multiple protocols and standards. For example, it is not uncommon to see devices that connect to Wi-Fi, Bluetooth, LTE and GPS at the same time. This level of agility paves the way for Cognitive Radios (CR) and future communication systems will be able to "sense" the environment and decide the best possible communication interface for maximum performance. Additionally, SDR being a "smart" platform, is able to detect, recognize and avoid interference from other users or devices to deliver reliable communication.

For commercial applications, a family of radio products, may be implemented using a common platform architecture, allowing new products to be more quickly introduced into the market. Software can be reused across radio "products", reducing development costs. Over-the-air or other remote reprogramming allows for "bug fixes" while the radio is in service, to reduce the time and costs associated with operation and maintenance.

However, current SDR devices are bandwidth limited. Commercially available boards such as that from Ettus Research [ett] can accommodate bandwidth on the order of tens of megahertz. However, over the past few years, companies began offering boards with multi-gigahertz operation. Technologies such as Direct RF sampling, that rely on single Analog-to-Digital (AD) and Digital-to-Analog (DA) Converters will likely dominate the wireless industry in the future due to their low complexity and superior performance over previous generation transceivers.

Besides UWB back-ends, advances in the area of Tightly-Coupled-Dipole-Arrays (TCDAs) resulted in UWB antennas with an impressive 14.2:1 bandwidth and an efficiency of 70% [MSV13] while maintaining superior scanning performance. This takes us a step closer to the UWB Software-radio which can be configured to operate at any frequency range.

1.2 Advantages of Ultra-wideband Systems

Since ultra-wideband transceivers and antennas are now available, future designs can accommodate the available bandwidth. According to the FCC, a wireless system can be classified as an UWB system if it is able to cover a continuous bandwidth of more than 500 MHz or a fractional bandwidth of at least 0.25. Modern system employing Direct RF sampling techniques can easily match or surpass this number. Below, we describe some of the advantages of UWB systems:

- Increase in channel capacity

Probably the most important benefit of using ultra-wideband systems is the increase in channel capacity. The Hartley-Shannon equation predicts this theoretical capacity limit [Sha48]:

$$C = Blog_2(1 + \frac{S}{N}) \tag{1.1}$$

where C is the max data capacity in bits/sec, B is the bandwidth and $\frac{S}{N}$ is the Signal-to-Noise Ratio of the system. This formula shows that capacity increases linearly as Bandwidth increases. Thus, employing multi-gigahertz bandwidth systems implies large data rates (a thousand to tens of thousands faster).

- Spectrum sharing

Employing ultra-wideband systems may give the designers the opportunity to accommodate multiple users without interfering with each other. The transmitted power requirement set by the FCC is about 41 dBm/MHz, equal to 80 nanowatts/MHz for UWB systems. This amount of power falls into the category of unintentional transmitters, such as TV sets and computer screens. This power density allows UWB wireless systems to operate below the noise floor of a narrowband receiver and enables UWB signals to coexist with current radio services with minimal or no interference.

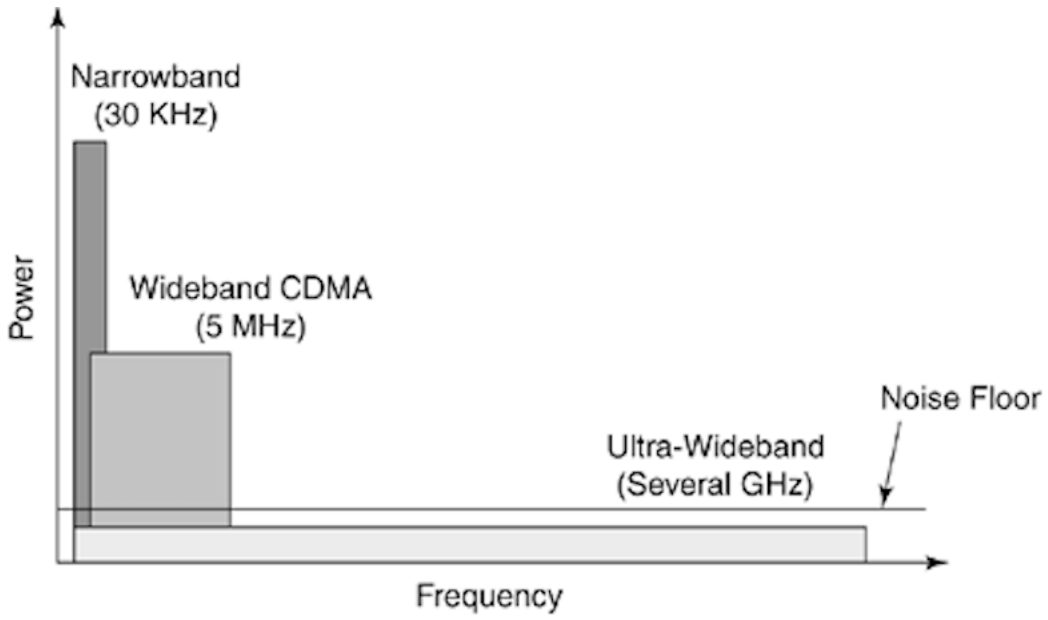

Figure 1.2: Typical wireless systems coexisting with UWB systems [Nek05]

- Covert Communications

As discussed earlier, lower transmitted power density results in a signal lying close to the noise floor. A potential eavesdropper will have to be either really close to the source of the transmitted information or employ high-gain directional antennas which would also require prior knowledge of the transmitter's location. In case of systems transmitting extremely short pulses, an additional layer of security

is added because detection of the picosecond pulses (without any other information about the incoming signal) is fairly impossible. Low probability of intercept is an attractive solution for military and other critical applications.

- Immunity to interference

Spread spectrum systems have the ability to mitigate strong interfering signals. The de-correlation process at the receiver will convert any uncorrelated signals into low-power noise close to the noise floor. A term used to describe the amount of interference mitigation is Processing Gain (PG), calculated as follows:

$$PG_{dB} = 10log_{10}\left(\frac{Spread\ Bandwidth}{Bit\ Rate}\right) \qquad [dB] \tag{1.2}$$

Indeed, the frequency diversity resulting from higher processing gain makes UWB systems immune to intentional and unintentional blocking. This is because no interferer can block the entire UWB band at once. Therefore, if some of the frequencies are interfered with, the majority of the band remains undisturbed.

- Resistance to multi-path effects

Communication in a multi-path environment can cause serious degradation in system performance. For example, urban environments might prove to be challenging since the high density of buildings can generate tens or hundreds or reflected signals. However, Direct Sequence Spread Spectrum (DSSS) systems have the ability to discard multi-path products generated by the reflection of the transmitted signals. Such systems work by performing correlation of the received signals against known sequences. A multi-path rich propagation environment would generate many correlation peaks. However, the signal with the strongest correlation would be preserved (as it might not be the Line-of-Sight component) discarding the rest of the signals in the process.

- Operation in low Signal-to-Noise ratio (SNR)

The Hartley-Shannon equation (1.1) also shows that the channel capacity is dependent on signal-to-noise ratio (SNR). That being said, it is possible to trade bandwidth for SNR and thus maintain or increase the capacity of the communication link.

1.3 Beamforming

Advanced beamforming capabilities, resulting from digital transceivers, give SDRs the advantage to dynamically adjust with environmental changes, high gain, high interference mitigation, to achieve spatial filtering, and reliability across a wide bandwidth. Adaptive multi-band multi-beam performance of smart antennas is achieved by dynamically adapting the weights of the signal from each antenna element to maximize antenna gain in one direction and improve signal-to-noise ratio (SNR). Smart antennas require advanced digital signal processing algorithms, available using SDRs.

To realise beamforming, phase or time delay of each array element signal needs to be adjusted. Traditionally, phase shifters/True-time-delay (TTD) components can be used at the RF/analog front-end or at the digital back-end. Therefore, beamforming can be performed in different ways:

- using phase shifters or true time delay components behind each antenna (RF beamforming).
- adjusting the phase of the local oscillators (LO - phase shifting).
- post processing after digitization (digital beamforming).

The first two techniques constitute analog beamforming. Here, we focus on digital beamforming.

1.4 Pros and Cons of Beamforming Schemes

In a conventional analog beamforming system, phase shifters or TTD components are used at the RF front-end to realize beamforming. However, due to phase limitations, phase shifters can resolve only one spatial direction at a time, presenting bottlenecks in applications requiring Multiple-Input-Multiple-Output (MIMO) configurations [VJJ07]. Also, phase shifters tend to be lossy and bulky resulting in increased size, weight and complexity of the system. However, an advantage of this scheme is that only one local oscillator (LO) is required. Another way to realize beamforming in the analog domain is to perform phase shifting at the local oscillator. This approach does not affect the sensitivity of the receiver since lossy phase shifters are not required. However, limitations pertaining to phase noise and synchronization between LOs make this option less attractive.

In digital beamforming, the signals are detected and digitized at the element level. The now-available RF data converters are wide enough to capture the signals directly at RF frequencies bypassing the need for mixers and analog stages which limit bandwidth and degrade receiver sensitivity. Furthermore, the ongoing decrease in cost make this approach more and more attractive to systems designers. Subsequently, the signals captured directly by the RF converters are post-processed digitally to form the desired beam. In this way, all information of the aperture is preserved allowing the end-user to form any beam they desire without suffering the limitations of the analog schemes. Digital beamforming includes quite a few advantages such as [Ste87]:

- Improved adaptive pattern nulling
- Multiple beams which can be closely spaced
- Array element pattern correction
- Antenna self-calibration and ultra-low sidelobes
- Increased resolution
- Multi-purpose RADAR systems

1.5 Multiple-In-Multiple-Out (MIMO) Systems

Multiple-In-Multiple-Out (MIMO) Systems take advantage of multiple transmitting and receiving elements. Besides beam-forming, MIMO systems are attractive for future communications systems by exhibiting time, frequency, and spatial diversity. Coupling MIMO capabilities with ultra-wideband waveforms gives the possibility of dramatic increase in security by providing multi-gigabit rates for individual streams to each user.

Besides antenna element configurations (such as SIMO, MISO, MIMO) and depending on how data is transmitted across the given channel, there are two ways of implementing MIMO systems. Multiple antennas in a system, means ability to create several propagation paths. By sending same data across the different propagation paths, the reliability of the system is greatly improved. Such scheme is known as spatial diversity or simply diversity. If the goal it to improve the data rate of the system, different portions of the data may be transmitted on different propagation paths. Such scheme is called spatial-multiplexing. These two systems are listed below.

- Diversity

Data are sent concurrently across different channels to mitigating distortion from fading. Each copy of the information will suffer a different level of distortion since each block propagates through different fading channel. This scheme uses the advantage that at least one copy will be distorted much less as compared to rest of the transmitted blocks. Overall, this improves the reliability of the system. For a set of N_t transmit antennas and N_r receive antennas, the total amount of diversity gain is $N_t \times N_r$.

- Spatial multiplexing

In spatial multiplexing, each spatial stream carries independent information to increase the data rate. In a multi-path rich environment, several independent streams can be created in the same allocated bandwidth. Thus, the multiplexing gain comes at no additional cost on bandwidth or power. The multiplexing gain is also knows as Degree-of-Freedom. The number of degrees of freedom in a multiple antenna configuration is equal to $min(N_T, N_R)$, where N_T is the number of transmit antennas and N_R is the number of receive antennas. The degrees of freedom in a MIMO configuration dictate the overall capacity.

MIMO techniques, beamforming and ultrawide-band systems are the means to the next generation of communication systems which will be able to achieve unprecedented performance. Bundled with Direct RF sampling, will result in the ultimate future radio.

1.6 Contribution of this Dissertation

This dissertation focuses on presenting a new way of designing communication systems with minimal design and maintenance effort. Although traditional software defined radios have been discussed in research and commercial applications [MGV+15,

LWR+18, BHG+14, BSB+11, RBL+12, Ulv10, RDB+08, SK12, CNMG14], they still lack bandwidth and reconfigurability for the next generation of systems.

With this in mind, a novel architecture based on Direct RF Sampling techniques is presented bypassing these limitations. Specifically, by using Direct RF sampling, analog mixing is no longer required, thus, providing access to large bandwidth to implement next-generation wireless and wired systems. As a proof of concept, a novel Code-Division-Multiplexing system is implemented with increased immunity to interference at the physical layer and higher peak data rates as compared to previous generation systems. This system operates across a bandwidth of 1.3 GHz with a center frequency of up to 6 GHz. Various measurements were conducted to test the performance of the system against interference (static and non-static). Table. 1.3 shows a comparison between previous generation systems and this work. The proposed Direct RF sampling system was tested at millimeter-wave frequencies. This was done using a transmit and receive chain, designed and implemented for operation at 28 GHz with of-the-self components achieving 2.13 dB of noise figure on average.

1.7 Outline of the Dissertation

The next chapter presents the novelty of the proposed secure communication system. Specifically, this chapter focuses on the theory of Spread Spectrum systems, Code Division Multiplexing techniques and Direct Sequence generators. The dissertation presents simulations to illustrate the concept.

Chapter 3 describes the hardware realization of the proposed system using software defined set-ups with Ultra-wideband (UWB) data converters. A detailed description of each stage, their challenges and limitations are highlighted in this dis-

	IS-2000	UMTS	Ultra Mobile Broadband	LTE	LTE Advanced	This work
Technology	CDMA	W-CDMA	OFDMA	OFDM/MIMO/SC-FDMA	MIMO OFDMA/SC-FDMA (Uplink)	UWB-CDMA
Generation	3G	3G	4G	4G	4G	5G
Year	2000/2002	2001	2008 (Abandoned)	2009	2011 Release 8	2019
Channel BW	1.228 MHz	5 MHz		20 MHz max	Up to 100 MHz	1.27 GHz (Up to 8 per channel)
Symbol Rate				18 Msps		10 Msps
Data Rate	3 Mbps	2 Mbps 42 Mbps for HSPA+	275 Mbps (Downlink)	50 Mbps	300 Mbps	60 Mbps Per user (64-QAM)
Chip Rate	1.2288 MHz SF = 64	3.84 SF = 4		3.84 SF = 4	N/A	1.27 GHz SF = 127
Code Sequences	Walsh codes Lc = 128	OVSF Code Variable length		OVSF Code Variable length	N/A	Gold Codes Lc = 127
Channel Coding	Turbo Codes	1/3 Turbo		Turbo Codes	Turbo Codes	Turbo Codes

Figure 1.3: Comparison of previous generation systems versus the proposed UWB spread spectrum system. IS-2000 [PO98], UMTS [Mol12], Ultra Mobile Broadband [Goz07], LTE [ADF+09], LTE Advanced [GRM+10].

sertation. A description of the test-bench configuration along with measurements in presence of static interference is given in chapter 3. Measurements including multiple sources of interference emulating different communication environments are also included.

The next part of the dissertation (chapter 4) addresses Direct RF Sampling for UWB communications. Specifically, traditional implementations are discussed along with limitations. Subsequently, Direct RF Sampling Receiver and Transmitter topologies are presented along with state-of-the-art hardware implementations for UWB communications.

Chapter 5 presents a new way of Direction finding process that exploits ultra-wideband signals using Direct RF sampling. Simulations and measurements using a prototype system are presented.

Chapter 6, provides some specific applications at millimeter-wave. Custom RF transmitter and receiver chains are designed for the 28 GHz band to test the CDM system. Measurements are presented.

Future directions of this research beyond 5G are discussed in the last chapter.

CHAPTER 2

SECURE COMMUNICATION LINKS WITH UWB TRANSCEIVERS

2.1 Introduction to Secure Communications

The need for secure communications has always been the center of attention for wireless and wired systems designers. The problem of eavesdropping and Man-in-the-Middle (MitM) attacks is an inherit issue of communications and researchers go to great lengths to provide the world with solutions that protect the identify and integrity of two or more parties wishing to exchange information. Telecommunications technology continues to advance with great pace and momentum and as the technology expands, so do the threats to these communications. This "forever ending" battle will keep taking place between the ones wishing to protect their lines of communications and the ones trying to intercept them. The burden will always fall on the shoulders of researchers trying to maintain an edge and provide the world with protection against threats.

There are quite a few different methods of securing a communications network such as encryption, stenography, identity based networks etc. All these methods operate at higher levels of the Open Systems Interconnection (OSI) model. However, to maintain the edge in secure communications it is important to provide the maximum level of security. That being said, security measures at the physical layer is an additional step to this goal.

Psychical layer, also known as PHY, refers to the first and lowest layer of the OSI model. The physical layer consists of the electronic circuit transmission technologies of a network. It is a fundamental layer underlying the higher level functions in a network. The physical layer defines the means of transmitting raw bits or symbols rather than logical data packets over a physical data link connecting net-

work nodes. The series of bits or symbols are converted to a physical signal that is transmitted over a transmission medium. The physical layer can be an electrical, mechanical (or a combination of both) interface to the transmission medium. There are many functions operating at the PHY layer. Major ones include: Bit-by-bit delivery, modulation, encoding, bit synchronization, clock recovery, multiplexing, carrier sense and collision detection, equalization, pulse shaping, channel estimation and pilot training, forward error correction and channel coding. Examples of technologies existing in PHY layer are: GSM air interface, Bluetooth physical layer, Ethernet physical layer, ISDN, USB physical layer, LoRa, IEEE 802.15.4, IEEE 802.15.7 (visible light communications), DSL, and others.

Due to the increase in densification in future communication systems, increased measures have to be taken to mitigate the resulting interference from the sheer number of devices in a given area and PHY layer is, as discussed above, responsible for interference mitigation and multiplexing. There are several methods in the literature to mitigate signal interference in radio frequency (RF) communications. In addition to filtering, other methods may employ active interference cancellation to suppress interference at the receiver front-end [WSWH10, RGTL05, KGK11, CH08, Yam04]. Among available methods, interference cancellation techniques can be classified into several approaches [Chi15]: space, time, frequency, time-frequency, and code domains. Space domain methods use antenna arrays with adaptive beamforming [Jon11] to suppress interfering signals by steering the beam to different directions or by placing nulls along the direction of the interfering signals [ZA12, GLG$^+$10, LWL13, IM85]. In time-domain methods, adaptive filtering is performed using finite impulse response (FIR) and infinite impulse response (IIR) filters [BCP08, RP94, CHHL00]. However, these interference cancellation methods are limited to narrowband interferers and incur hardware complex-

ity. Also, frequency domain methods have been proposed for interference rejection [WLT09, ZYCY09, Chi13, CHYT10]. A major drawback for the latter is hardware complexity due to requiring Fast Fourier transform (FFT), inverse FFT, or wavelet transform blocks as part of the hardware. Additionally, windowing blocks are needed to avoid significant spectral leakage [CHHL00], implying higher costs. Further, time-frequency excision techniques require an estimate of the interferer instantaneous frequency [Coh95], implying even more complex hardware. A sophisticated orthogonal-like Gabor expansion may also be required to estimate the interferer signal prior to subtracting it from the input [SPR13].

Most of the above interference suppression techniques are limited in terms of their spectral and spatial filtering, and suffer from limitations in hardware and digital cancellation techniques [RGTL05, KGK11, WSWH10, CH08]. That is, in presence of high interference levels, these techniques, if implemented individually, fall short to achieving enough suppression. Also, most require previous knowledge of the interferer's position, channel, and signal identity [KGK11]. Of course, in realistic scenarios, and when communicating across wide bandwidths, interferers are unknown to the receiver. Therefore, more advanced techniques are required to suppress interference and avoid signal fratricide.

2.2 Spread Spectrum (SS) Systems

One of the techniques that can be used to secure the physical layer is Spread Spectrum (SS). It was first introduced by the prolific Serbian-American pioneer, Nikola Tesla. On 17th of March 1903, U.S. patent No. 723,188 named "Method of Signaling filed by him described essentially a method of frequency hopping however did not use the same words for it [Tes03]. An excerpt of the patent submitted reads

”to enable a great number of transmitting and receiving stations to be operated selectively and exclusively and without any danger of the signals or messages being disturbed, intercepted, or interfered with in any way is the object of my present invention.”

It wasn’t until June 10th 1941, when Hedwig Eva Maria Kiesler, known as Hedy Lamarr, a Holywood actress, who introduced the spread spectrum system during second world war as a means to further secure communications between allies and also suppress interference from adversaries [Sch83]. The patent was filled under her second husband’s name Markey Kiesler [KG42]. There are three spread spectrum methods:

- Frequency hopping spread spectrum (FHSS)

In FHSS the data is transmitted over pseudo-random series of frequency tones or bands. For this, a large amount of frequency channels is allocated. Transmitter and receiver must be able to maintain perfect synchronization after each frequency hop in order to successfully recover the data transferred. This techniques provides a layer of interference mitigation since a potential blocker would have to essentially guess the frequency hops at each point in time. However, if the frequency hop rate is slow, which is a challenge for designers, a interferer may be able to rapidly follow the frequency components and momentarily block the systems.

- Time Hopping Spread Spectrum (THSS)

Although, strictly speaking, Time Hopping Spread Spectrum is not a spread spectrum technique, spreading can be achieved by other means. Specifically, the duty cycle of the transmitted pulses changes in a pseudo-periodic manner which provide a wide frequency response. This can constitute a spread spectrum mechanism. In this method however elaborate code acquisition techniques are required

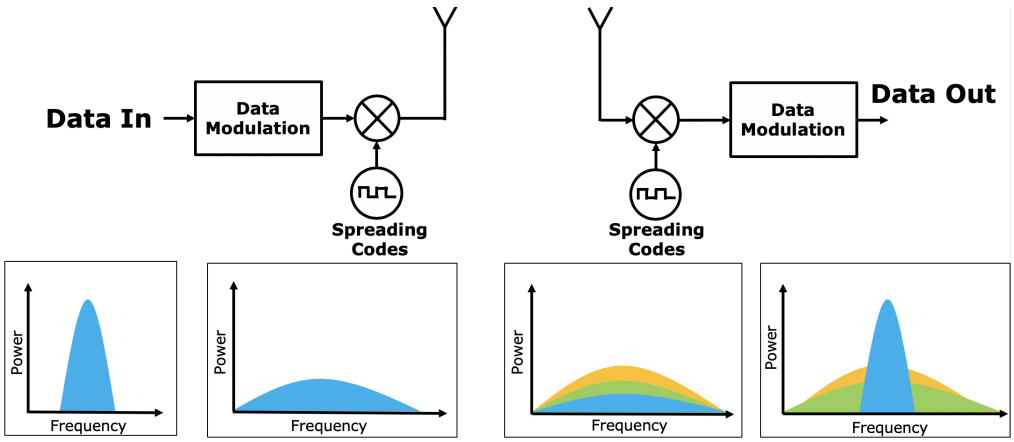

Figure 2.1: Direct Sequence Spread Spectrum (DSSS) scheme.

which increase the complexity and additionally Forward Error Correction codes are also required.

- Direct Sequence Spread Spectrum (DSSS)

In the simplest form it is a multiplication of the data with another unique and faster sequence shared only with the transmitter and the receiver [PR04]. This results in a noise-like signal appearing to be spread in frequency domain. Fig. 2.1 illustrates the concept. In more details, the data are modulated using one of the available modulation schemes. After this stage, the resulting signal is multiplied with a spreading sequence. Examples of spreading sequences are Pseudo-Noise (PN) [Mut96], Kasami [ZLH07], Gold [Gol67] and Zadoff-Chu [HM16]. At the receive side, the signal is multiplied again with the same unique sequence (assuming synchronization is has been achieved). After this stage, the signal is ready to be demodulated. Depending on the application, different sequences shall be used. For example, a system that requires low probability of intercept and some degree of interference immunity but with no need of multiple access communication may employ PN sequences which are simple to implement, provide good auto-correlation properties but lack near-zero cross-correlation, as shown in Fig. 2.2. Further, Walsh sequences

are a good candidate when there is synchronous communication. For asynchronous communication, Gold codes may be used due to their minimal cross-correlation. Their code length is $2^{N-1}-1$, where N is an even integer. Kasami codes are similar to Gold codes but their length is $2^{N}-1$, where N is an even integer. The correlations of this figure were calculated using the equation 2.1:

$$(f \otimes g)(\tau) = \int_{\infty}^{-\infty} \overline{f(t)} g(t+\tau) dt \tag{2.1}$$

where $\overline{f(t)}$ denotes the complex conjugate of $f(t)$, and τ is the displacement, also known as lag.

Three major advantages when employing DSSS are:

- Anti-jamming performance.
- Low probability of intercept.
- Multiple Access communications

These effects were primarily of military interest but later were adapted to provide benefits to civilian systems. These are:

- Interference immunity.
- Low transmit power density.
- Multiple simultaneous transmissions.

Popular communication systems typically use code domain for interference cancellation. For instance, Wi-Fi, CDMA2000, and Global Positioning System (GPS) use Barker codes [AKK16], a combination of Walsh and Gold codes [Wil00], and long Gold codes [HBW15], respectively. The key advantage of spread spectrum modulation is immunity to noise and multipath distortion, including interference

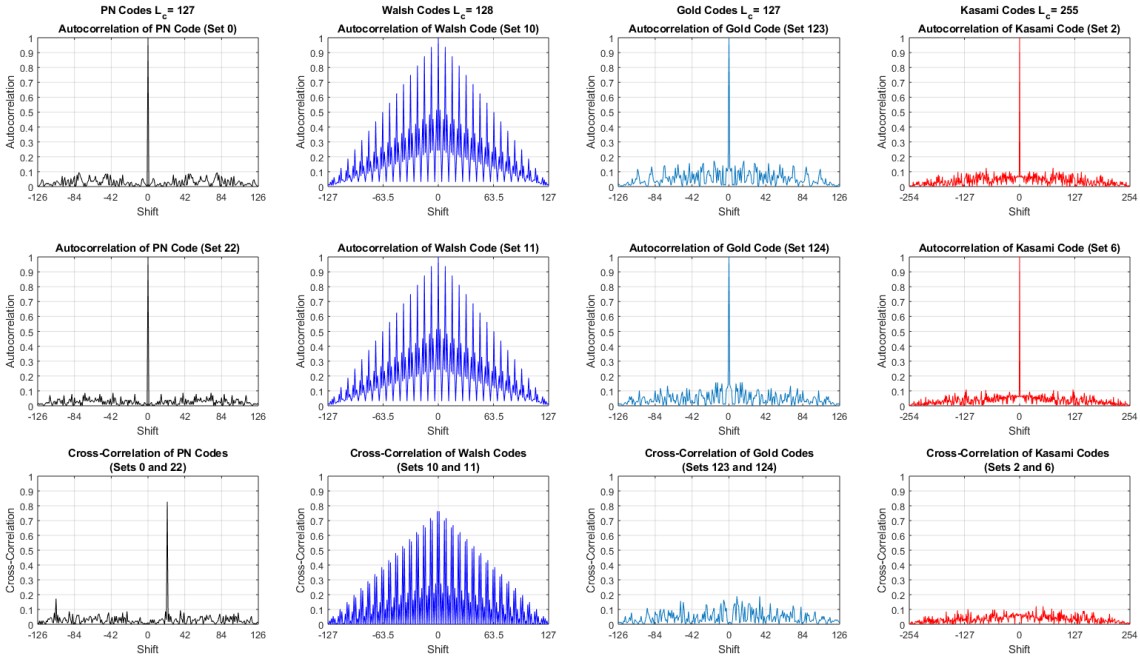

Figure 2.2: Plots showing auto-correlation and cross-correlation of two PN, Walsh, Gold and Kasami sequences.

mitigation. Also, Code Division Multiplexing (CDM) is known for its high spectral efficiency as compared to other double-sided modulation schemes [HYKY03]. CDM is also known to be robust against narrowband interference. Further, the random properties of CDM code sequences make them attractive when deployed in fading channel environments [HYKY03]. This is because it can discard the samples generated by multipath propagation [HYKY03]. In addition, protection against channel perturbation can be achieved when implementing CDM with channel coding, which provides error detection and correction features. That is, coding gain increases the interferer's power margin and receiver's resilience against high power malicious attacks [CF07, Ple86, GKD07, TJC99].

Although spread spectrum systems add an additional layer of security, they cannot be considered impenetrable. A malicious user with high speed hardware correlators might be able to determine the spreading sequences (equivalent to a private key in encrypted systems) used by the system by running all possible combinations in real-time. Of course, the longer the sequences the more difficult it would be to identify them. An additional step towards increased security is the ability of the DSSS system to adaptively change the spreading sequences when a breach is detected in the network. There are two possible situations in case of a network beach:

- Active adversary

In this scenario the malicious user acquired the spreading sequences and tries to actively transmit within the same network perpetrating another user (spoofing attack) or simply flood the network with data, an attack known as Denial-of-Service (DoS). In this case, an increase in the overall Signal-to-Interference would be detected instantly. The system should be able to detect and mitigate this attack

by changing the spreading sequences and issue a broadcast alert to all nodes to effectively ban the user transmitting using the said configuration.

- Passive adversary

In this case, a malicious user has acquired the spreading key but instead of transmitting, this time acts as a passive listener. This would constitute a "sniffing" attack and it is a lot more difficult to mitigate since there is no indication of a system breach. To mitigate a possible passive attack, we could proactively change the spreading sequences frequently. Specifically, the keys should randomly change in a predetermined way to avoid notifying the malicious users of an impending change. Additionally, the change should be fast enough in order to hamper the efforts of the adversary without disturbing the proper operation of the network.

The proposed system was designed with these two possible attacks in mind. In more details, the Medium Access Control (MAC) Layer adaptively changes the configuration of the system and communicates the changes to the rest of the legitimate users. The frame structure (described in more details in section 3.2) are reserved a total of 14 bits for this purpose.

A major drawback however of spread spectrum systems is the excessive bandwidth they tend to require. For example, if the original signal of a DSSS system occupies 10 MHz, after the spreading process with a sequence length of 127, the resulting signal will occupy about 1270 MHz which, up until recently, was prohibitive due to the lack of hardware to support such wide frequency of operation. One of the limiting components withing the transmit and receive chains was the data converters. However, recently high-speed ADCs and DACs emerged able to accommodate multi-GHz bandwidth of operation and thus allowing DSSS with increased Processing Gain.

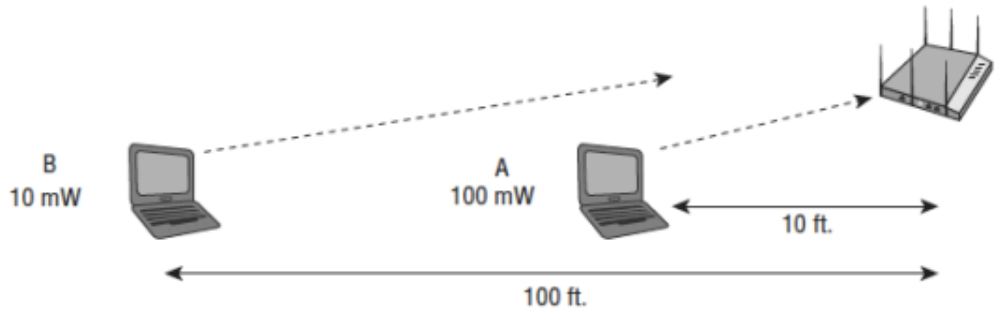

Figure 2.3: Diagram exhibiting the Near-far problem.

Another challenge of DSSS systems is the "Near-Far" problem. In such systems, all the signals are transmitted on the same frequency band at the same time. However, the power of nearby transmitters arriving at the receiver can overwhelm the signal from transmitter located further away. Fig. 2.3 illustrates the issue. Essentially, transmitter A acts a wideband interferer for transmitter B. In severe cases, the interference margin would have to be more than 40 dB, a value that is difficult to achieve for high data rate systems.

2.3 Processing Gain

A term used to describe one of the unique properties of Spread Spectrum systems is Processing Gain (PG). In more details, it is a measure of performance advantage of spread spectrum against narrowband signaling. Spread spectrum systems are dual-modulated systems. First step is by using traditional modulation techniques such as PSK, QAM, etc. and then, for a second time with the wideband modulation of choice, i.e. Frequency Hopping (FH), Direct Sequence (DS) or others. The wideband modulation scheme spreads the signal power over a wider range of frequencies. This spreading procedure is what provides Processing Gain.It can be seen as the ratio

of the spread (or RF) bandwidth to the unspread (or baseband) bandwidth and is usually expressed in decibels (dB):

$$PG_{dB} = 10log_{10}\left(\frac{Spread\ Bandwidth}{Bit\ Rate}\right) \qquad [dB] \tag{2.2}$$

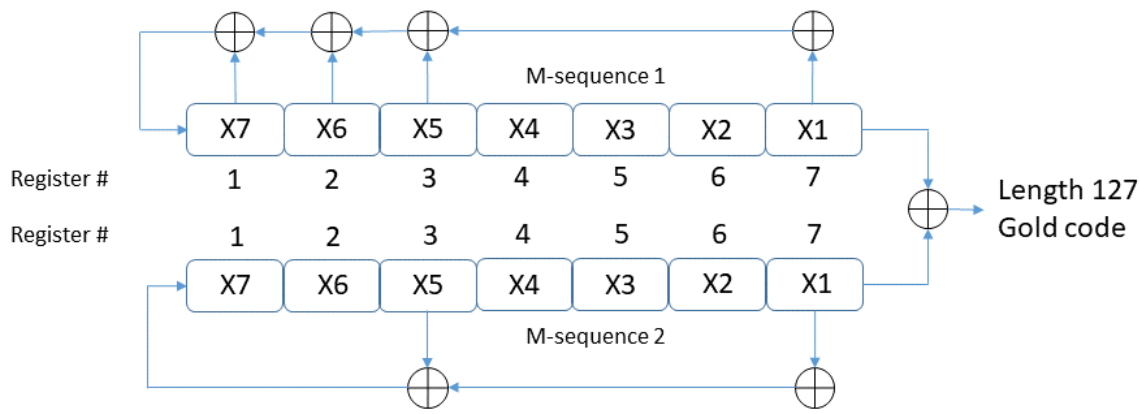

Figure 2.4: Length 127 Gold sequence generator.

Many spreading sequences exist in literature with each one providing different benefits for different applications. For the proposed system, Gold codes were chosen primarily because of easier synchronization at the receiver (more details on chapter 3). They are binary sequences for spread spectrum applications and were named after Robert Gold [Gol67]. Fig. 2.4 shows the implementation of a 127-length Gold code generator. Two M-sequence generators are used (with the preferred pairs [7,3,2,1],[7,3] in this example) that are XOR'ed to produce the final sequence. The resulting sequence has a chip rate (i.e bit rate of the spread spectrum system) 127 times faster than the bit rate of the raw data at the input.

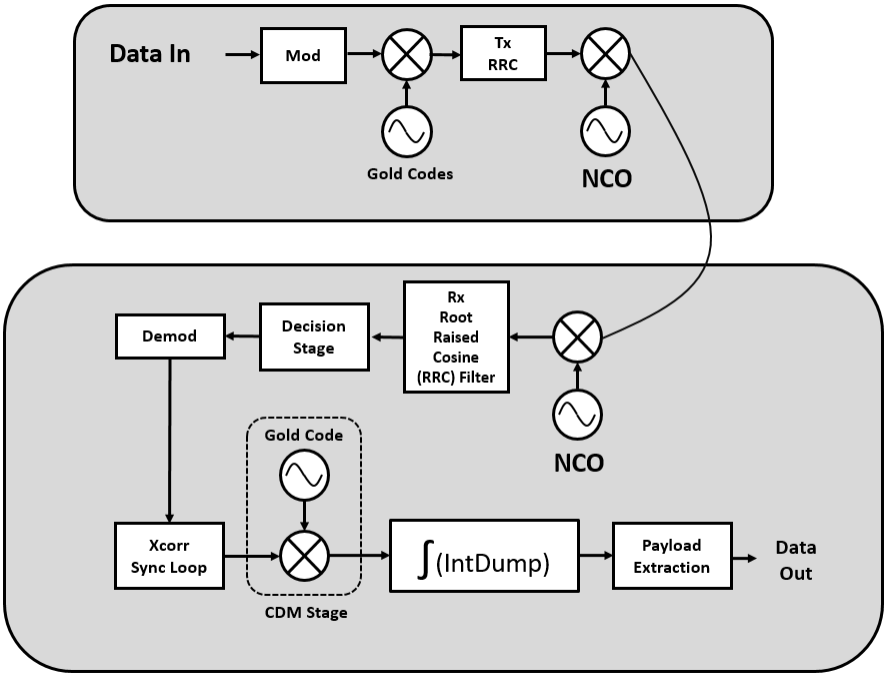

Figure 2.5: Simulation testbench of the UWB spread spectrum system using MATLAB.

2.4 Simulations

As already mentioned, one of the advantages of DSSS is the option to have multiple users communicating using the same frequency band. To illustrate the performance of such environment simulations were performed for different code lengths and different number of concurrent users. The simulation test-bench is shown in Fig. 2.5 and it was implemented in MATLAB. Fig. 2.6, 2.7 and 2.8 show Bit-Error-Rates (BER) versus Eb/N0 for 2, 4, 8 users when using Gold codes of length 31. It shows that a small degradation of 0.4 dB, 0.9 dB and an average of 2.3 dB occurs, for 2, 4 and 8 users, respectively. This test proves that many users can occupy the same bandwidth to communicate without significant degradation.

Another simulation performed pertains to the performance of the system under the effects of a single high-power interferer trying to block the system at an

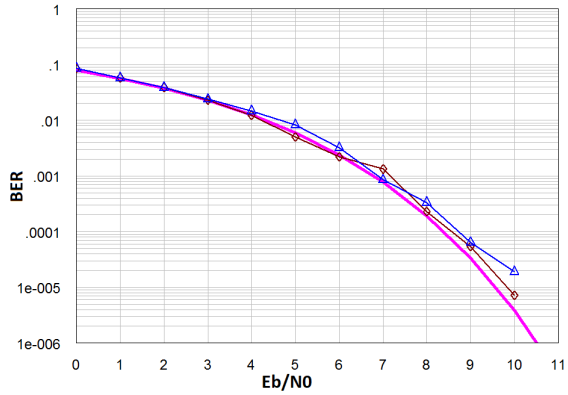

Figure 2.6: BER vs E_b/N_0 plot of two users communicating within the same frequency band using Gold codes of length 31.

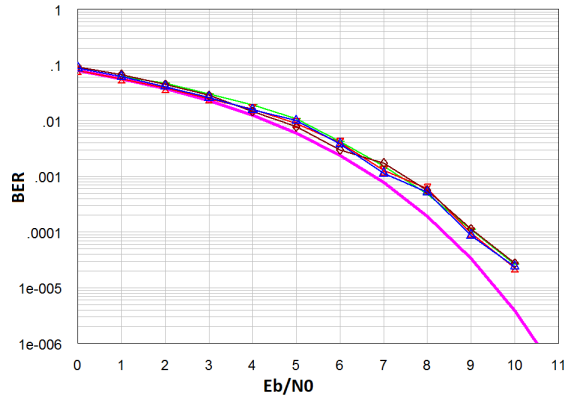

Figure 2.7: BER vs E_b/N_0 plot of four users communicating within the same frequency band using Gold codes of length 31.

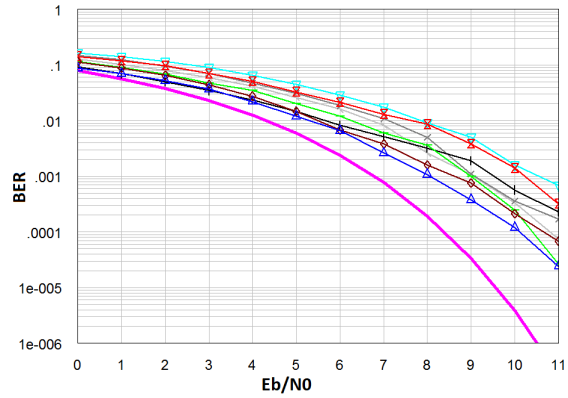

Figure 2.8: BER vs E_b/N_0 plot of eight users communicating within the same frequency band using Gold codes of length 31.

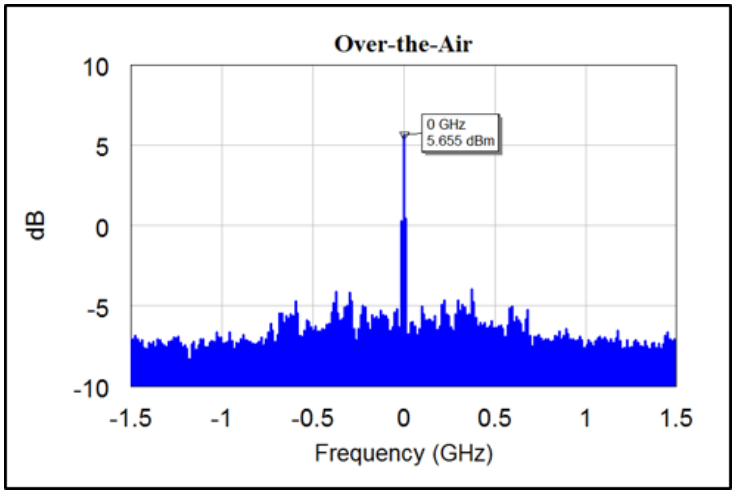

Figure 2.9: Over-The-Air (OTA) frequency plot of the simulated transmitted signal close to the noise floor and a high power interferer.

Interferer-to-Signal ratio of 10 dB. For this test, the length of the code was increased to 127, resulting in a total bandwidth of 1.27 GHz. The Over-The-Air frequency domain is shown in Fig. 2.9. Notably, the transmitted signal lies very close to the noise floor providing some privacy to the communication system.

The test was preformed for three different scenarios. The first one included two users communicating at the same time utilizing the same frequency band. The second test included four users and the last test included eight users. In all occasions, perfect synchronization was assumed. The results are plotted in Fig. 2.10, 2.11 and Fig. 2.12.

Furthermore, the same test was conducted for different Interferer-to-Signal ratios. Fig. 2.13 presents the data from all the tests. Notably, degradation for 8 users is only 0.8 dB more than the degradation for 4 users. This is due to the nature of the spread signal. In other words, the resulting spread signal does not have a flat frequency response and is affected differently depending on the interferers frequency of operation.

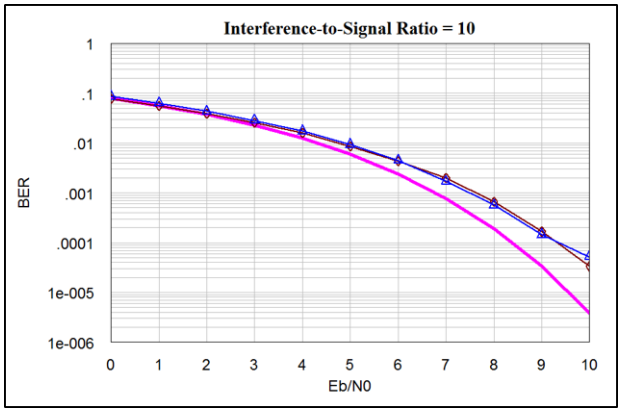

Figure 2.10: BER vs E_b/N_0 of 2 users utilizing the same frequency band.

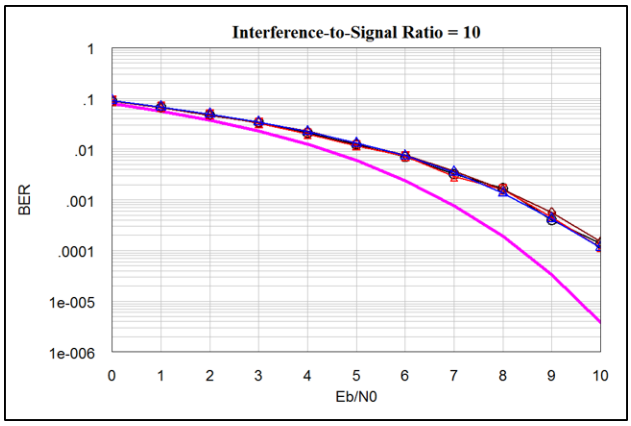

Figure 2.11: BER vs E_b/N_0 of 4 users utilizing the same frequency band.

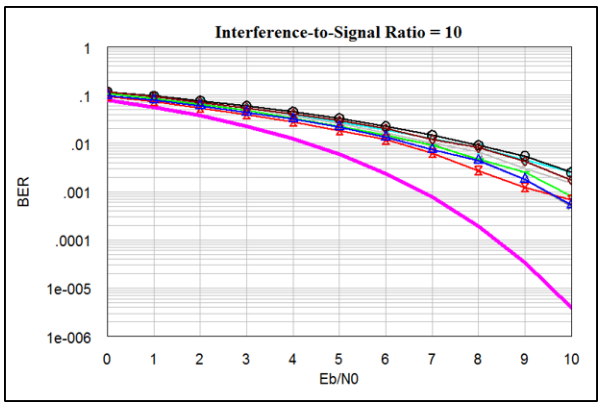

Figure 2.12: BER vs E_b/N_0 of 8 users utilizing the same frequency band.

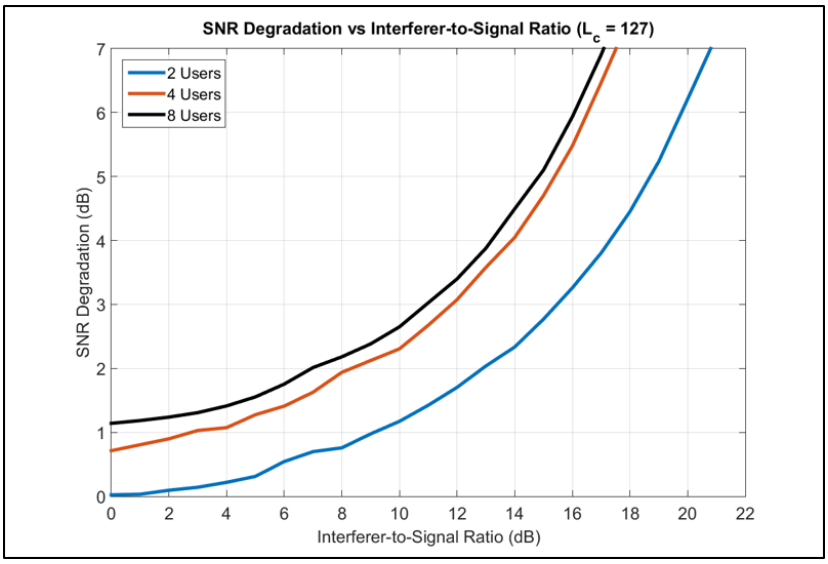

Figure 2.13: Signal-to-Noise Ratio (SNR) degradation vs Interferer-to-Signal Ratio (ISR)

CHAPTER 3

EXPERIMENTAL DEMONSTRATION OF SECURE LINKS WITH UWB TRANSCEIVERS

In this chapter a new approach towards transceivers utilizing ultra-wideband spectrum is introduced which could enable a fusion between massive machine type and ultra reliable communications. Benefits of this approach include increased densification (meaning more and more devices in a crowded area), longer range communications, increased security at the the psychical layer and increased throughput. We proceed below with the transmitter architecture.

3.1 Transmitter Architecture

The proposed system was implemented in a software-defined fashion to minimize cost and to allow for easier integration and maintenance. Software defined radios (SDR) have been in existence for almost a decade however their bandwidth was rather limited and in the order of 100 MHz. Nowadays, with the advent of high speed ADCs/DACs we are capable of utilizing multi-GHz available spectrum for UWB communications. Additionally, the large bandwidth of the newly introduced devices can also be used to digitally up/down convert the baseband signal to RF frequencies without the need for complex RF-front ends. More details can be found in chapter 6.

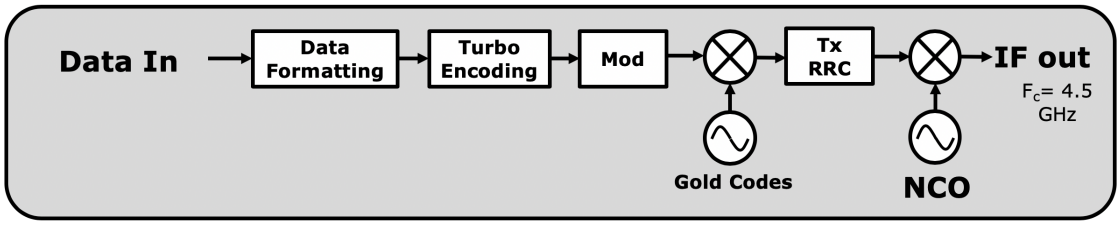

Figure 3.1: Ultra-wideband transmitter architecture

Input to the system is a digital file, i.e. audio, video or raw data. The data needs to be formatted in a certain way in order to be ready for the subsequent stages. For this reason, the Data Formatting stage exists. It essentially reshapes the constant stream of zeros and ones into a single payload of data. Additionally, at this stage, a preamble is added at the start of the payload in order to allow for easy frame synchronisation at the receiver side. For this implementation, Barker codes were used which are known to produce the highest auto-correlation [CCGR16]. All the knows Barker codes to this day are shown in Table 3.1.

Furthermore, to increase the total combined gain of the system, we employ channel coding using Turbo Codes. Turbo codes are considered a set of codes to closely approach the Shannon limit of -1.59 dB.

After the channel coding comes the modulation of the actual data. Essentially, it is a mapping process where 0s translate to 1s and 1s to -1s. The resulting data is multiplied by a unique code at the next stage.

For the proposed system, Gold codes were chosen primarily because of easier synchronization at the receiver (more details on the next section). They are binary sequences for spread spectrum applications and were named after Robert Gold [Gol67]. Fig. 2.4 shows the implementation of a 127-length Gold code generator. Two M-sequence generators are used (with the preferred pairs [7,3,2,1],[7,3] in this

Length	Codes	
2	+1 -1	+1 +1
3	+1 +1 -1	
4	+1 +1 -1 +1	+1 +1 +1 -1
5	+1 +1 +1 -1 +1	
7	+1 +1 +1 -1 -1 +1 -1	
11	+1 +1 +1 -1 -1 -1 +1 -1 -1 +1 -1	
13	+1 +1 +1 +1 +1 -1 -1 +1 +1 -1 +1 -1 +1	

Table 3.1: All available Barker codes.

example) that are XOR'ed to produce the final sequence. The resulting sequence has a chip rate (i.e bit rate of the spread spectrum system) 127 times faster than the bit rate of the raw data at the input.

The next steps involve a transmit Root Raised Cosine (RRC) filter matching the receive filter and a Digital Up-Conversion (DUC) stage. The latter up-converts the baseband signal to RF frequency for sub-6 GHz operation or to an IF frequency for an additional up-conversion to 28 GHz.

3.2 Medium Access Control (MAC) Layer Design

Since there has never been a wireless system employing such a large bandwidth before, the design of a new custom transmission frame architecture is required to achieve communication between the transmitter and the receiver. Low latency and high reliability are of concern, thus, we opted for a relatively small payload. Fig. 3.2 shows the structure of the UWB-CDMA transmit frame. As discussed earlier, the Preamble section of the frame is reserved for the preamble detection using Barker codes.

The next two blocks are used for routing of the frame to the proper user. Specifically, 16 bit addresses are used to determine the source and destination of the message. Since this system is aiming for high density environments, the number of unique devices that may connect to the network is 65,536.

The following section of the frame is the Header. The Header contains information about the Frame ID (in case the frame is lost and a re-transmission is required), the protocol type and the protocol version being used. Additionally, the last 128 bits contain information about the current state of the channel (Channel State Information, CSI). In more details, a channel transmission matrix of a four-by-four

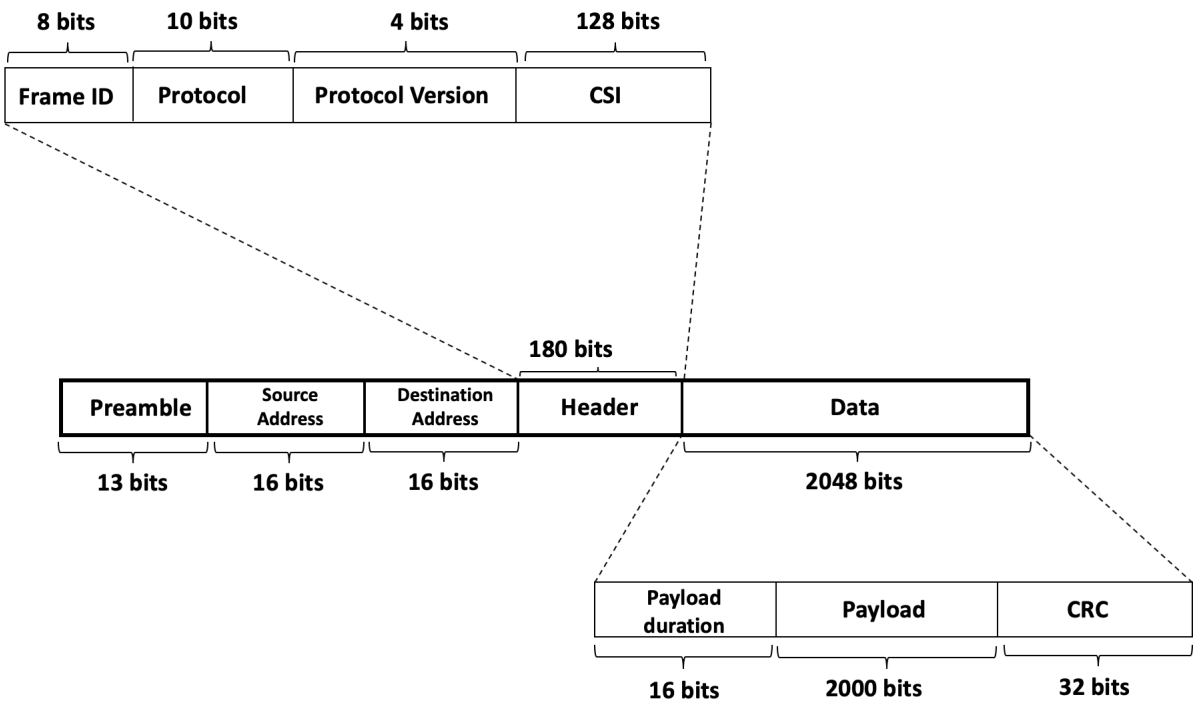

Figure 3.2: UWB-CDMA frame structure.

MIMO system is transmitted. The matrix can be used at the receiver side to offset the effects of channel distortion. Available algorithms may be used to precode the transmitted signal in order to cancel out the channel imperfections and provide an additional boost in signal integrity. Finally, the last part of the frame involves the actual transmitted data. 2048 bits are reserved for this section. The first 16 bits refer to the total length of the payload. It is needed since the payload length can vary and the receiver does not have information about the number of payload bits transmitted. The next 2000 bits contain the actual data transmitted by the user. The payload of its frame is coded using Turbo codes rate 1/2 to provide additional channel coding gain. Notably, the decoding process happens after the payload is extracted and usually is implemented separately in a different stage of the receiver. Lastly, the last 32 bits of the receiver are reserved for the Cyclic Redundancy Check (CRC). It is an error detecting code commonly found in many modern wireless

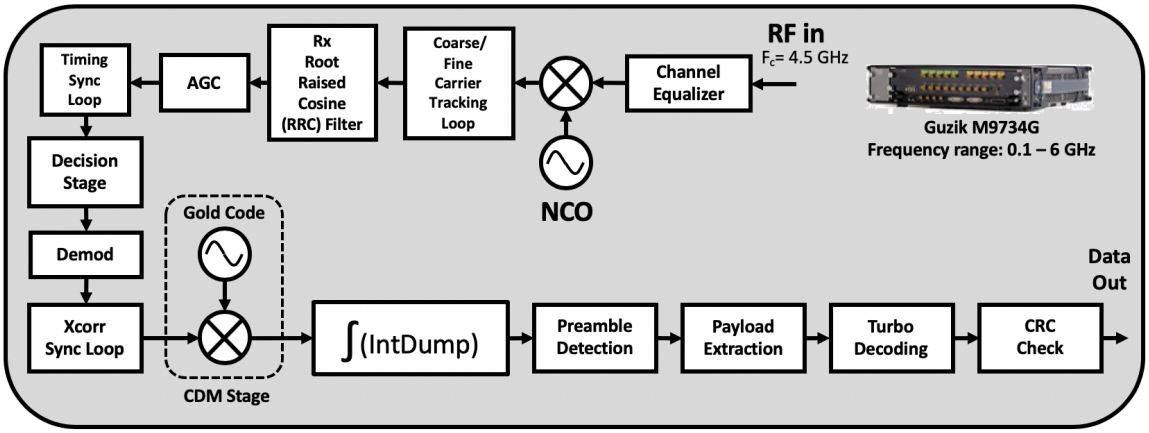

Figure 3.3: Ultra-wideband receiver architecture

protocols. The proposed system utilizes the variant CRC-32 algorithm to detect possible errors during the transmission.

3.3 Receiver Architecture

In this section we will present a detailed description of each stage of the receiver architecture.

As already mentioned, the signal is captured at RF without the need for external mixers and analog filtering by employing direct RF sampling. This results in easier integration and reconfigurability. However, the ADC/DAC of the system does not produce a flat frequency response throughout the 1.3 GHz of bandwidth. Thus, equalization is required to recover the slightly distorted signal. Next, the desired signal needs to be down-converted to baseband. For this purpose, a Numerically Controlled Oscillator (NCO) is used. Basically, an NCO is a digital signal generator same as an analog signal generator and combined with a low-pass filter and a down-sampler is tasked to perform Digital Down-Conversion (DDC).

In wireless communications the most difficult task is, as widely accepted by designers [Dix94], is the transmitter/receiver synchronization. The first step is to have a coarse estimate of the frequency offset between the transmitted and received signal. For that, we are using a closed-loop compensator that uses the PLL-based algorithm described in [LR95]. Next, for the residual frequency offset and carrier synchronization we are using the algorithms described in [Ric09].

The next two stages are the receive Root-raised cosine (RRC) filter and Automatic Gain Control (AGC). The RRC filter simply matches the Transmit RRC filter resulting in an increase in SNR. The AGC block is a closed-loop feedback block with a purpose of maintaining a suitable signal amplitude at its output, regardless of any variation of the signal amplitude at the input due to variation in received power.

The next level of synchronization involves the clock skew between the transmitter and the receiver. For this task, a few algorithms exist and they fall in two categories: non-data-aided timing error detector (TED), such as the Gardner Method and the Early-Late method, which uses received samples without any knowledge of the transmitted signal and a decision-directed TED, such as the Zero-Crossing Method and the Mueller-Muller, which uses the sign function to estimate the in-phase and quadrature components of received samples [Men13]. Different methods perform more efficient in different applications. For example, the Zero-Crossing (decision-directed) and Mueller-Muller (decision-directed) methods estimate the timing error based on the sign of the in-phase and quadrature components of signals passed to the synchronizer. As a result, the decision-directed methods are not recommended for constellations that have points with either a zero in-phase or quadrature component. For example, QPSK modulation with a zero phase offset having points at 1+0i, 0+1i, -1+0i, and 0 - 1i would not be suitable for these methods.

The following two stages involve the decision making process and subsequent demodulation of the received data. At this point, the complex IQ data is converted

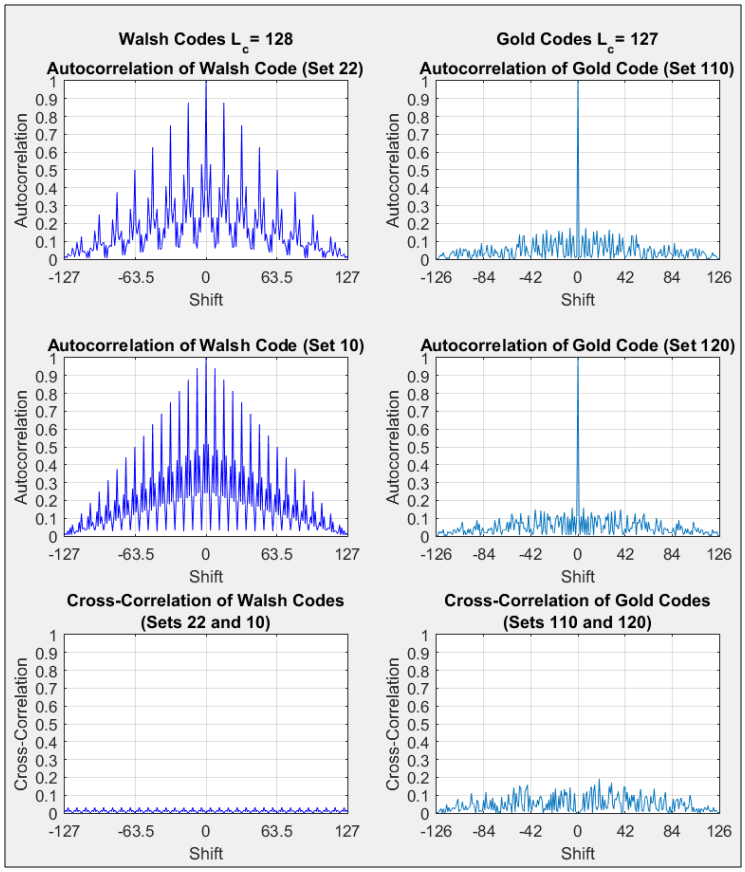

Figure 3.4: Correlation properties of Gold and Walsh codes.

to bipolar raw data (ones and minus ones).

The cross-correlation sync loop plays a very important role of synchronizing the transmitter to the receiver. To do so, real-time cross-correlation is first performed with the purpose of identifying the time difference (lag) between the received signal and Gold code that is already saved on the receiver side. We note that Gold codes were favored over Walsh codes because of the superior auto-correlation properties. Fig. 3.4 shows the auto-correlation of two random set of Walsh and Gold codes and their cross-correlation. In case of a synchronous communication system (meaning perfect synchronization between transmitted and received signal), Walsh codes would be the perfect choice. The zero cross-correlation between different sets of

codes at zero lag would result in no interference between different signals. However, the proposed system supports asynchronous communication between different users. In this case, Walsh codes would result in multiple auto-correlation peaks (as shown in figure) which would in turn make impossible to measure the time difference and subsequently align the signals. Therefore, another set of codes was selected which provide a single auto-correlation peak for synchronization purposes and minimal interference between different users communicating at the same time (on average 0.1 or less on a normalized scale).

Once the time difference (lag) is identified by the cross-correlation of the transmitted and received signal, the two signals are aligned and formatted for the next stage which is the de-spreading process. At this point, we perform a one-to-one bit multiplication of the received signal with the previously saved Gold code sequence.

Integration and Dump is the next stage and is one of the most critical components in the receiver. It is the stage where processing gain is realized. Essentially, it is a process of integrating energy from 127 pulses to output a single bit. It is equivalent to matched filtering at the sampling points.

At this point, the data coming out of the Integration and Dump process is raw digital data (zeros and ones). However, the receiver does not have any information of the start and the end of the payload. Another procedure is needed to identify these. During the preamble detection process, a cross-correlation of the received data and the Barker codes that were used is performed. This leads to payload extraction and subsequently to Turbo decoding. Finally, a cyclic redundancy check (CRC) is performed to detect accidental changes and errors in the received payload. The CRC number must match the CRC number during transmission for a perfectly recovered payload.

3.4 Test-bench Description

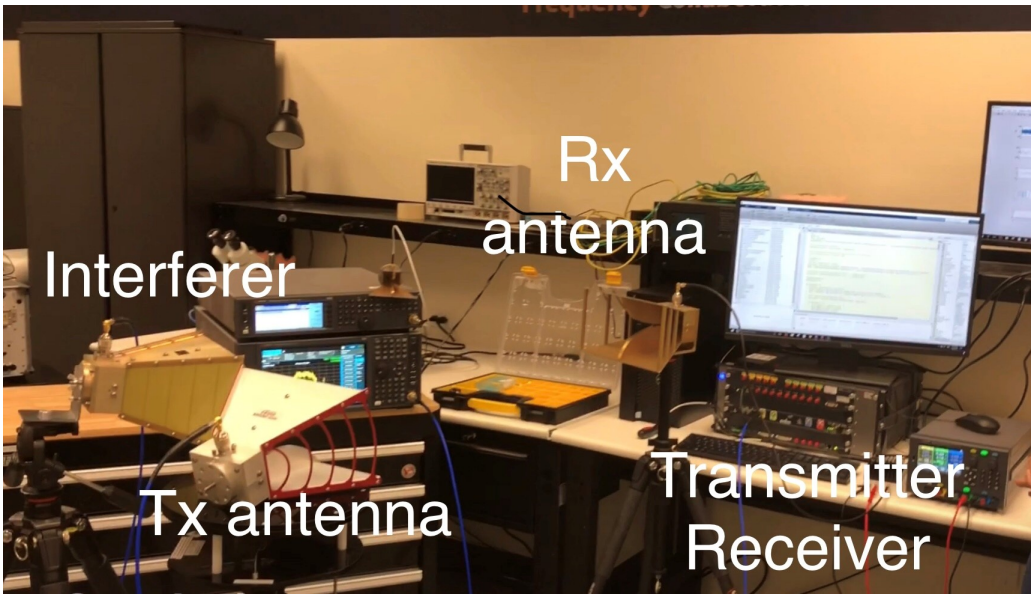

Figure 3.5: Measurements hardware setup.

In this section, we carry out measurements in order to assess the feasibility and performance of the UWB spread spectrum system. For this purpose, a complete communication system was created as a proof-of-concept. Specifically, we employed equipment setup from Keysight (M8190A [keyb] as transmitter which allows up to 6 GHz bandwidth and Guzik Technologies equipment (M9734G [guz]) as a receiver, allowing operation across 6.5 GHz. Both the transmitter and receiver were designed in a software defined fashion to minimize cost. Further, Direct RF sampling was used to remove the bottleneck of complex RF front-ends for ultra-wideband signals. For this experiment, we focused on the interference suppression capabilities of the link. Therefore, we used a single antenna at the transmitter and receiver.

The transceiver operation is as follows: After creating the signal in baseband as described in the previous section, the Keysight M8190 Arbitrary Waveform Generator was used to Digitally Up-Convert (DUC) and transmit the signal at 4.5 GHz

center frequency as shown in Fig. 3.1. A standard horn antenna was then used to transmit the signal. The receiver architecture was implemented using the M9734G digitizer as shown in Fig. 3.3. Notably, this digitizer employs interleaved ADCs to achieve 20 GSPS sampling rates. A photo of the actual hardware setup is shown in Fig. 3.5. As already mentioned, the channel bandwidth is approximately 1.3 GHz and, as noted, multiple users can readily occupy the same bandwidth without appreciable BER degradation.

Below we describe BER measurements to assess processing gain using CDM spreading across 1.3 GHz bandwidth. First, we carry out measurements without interference and then in presence of an interferer. Measurements with channel coding are also conducted in this study.

3.5 Measurements in Presence of Static Interference

In this section, data from multiple test scenarios are shown. The primary metric employed to asses the performance of digital wireless/wired communications systems is the Bit-Error-Rate (BER). BER is a measure of frequency of errors occurring during a transmission period. Such errors can be a result of noise, interference, distortion, bit synchronization errors, multi-path effects or a combination of them. Commercial Bit-Error-Rate-Testers (BERTs) are currently offered, however they can be only used for baseband digital circuits. Currently, BERTs for RF communication systems are not available. For this reason, a custom BERT system was implemented in order to measure the error rate of the proposed system.

A BER test works by comparing transmitted bits to received bits in a synchronous manner. The device under test has to be able to recover as many bits as possible without having a systematic error in the received bits. An example of sys-

tematic error could be an increased BER when the transmitted sequence is a series of zeros or even a certain sequence of zeros and ones. For this reason, the devised test included the transmission of not only random sequences, but also repetitive patterns and bit sequences consisting only of zeros or ones. In all the tests, the system designed did not incur any systematic error.

3.5.1 Processing Gain Measurement

Fig. 3.6 shows the measured BER data in absence of an interfering signal. These measurements were obtained using randomized set of codes and by recording BER across various SNR values for several hours. As seen, CDM spreading across a 1.3 GHz bandwidth implies significant reduction in BER. Specifically, the reduced BER implies a measured processing gain of 16 dB at BER = 10^{-4}. That is, the receiver sensitivity was improved by 16 dB. By comparison, the "ideal" computed processing gain is $10log(127) = 21\ dB$, where 127 refers to the code length. The difference in processing gain is likely due to imperfections (cable losses, mismatches) and due to the non-optimized implementation of the system (timing loops, symbol tracking loops, etc).

3.5.2 Interference Margin Measurement

Next, we introduced a high-power interferer in the communication link to assess Interference Margin. For this experiment, the transmitted power is kept constant while the power of the interferer is varied. Specifically, the Signal-to-Interference-Plus-Noise-Ratio (SINR) was varied by 14 dB at f = 4.5 GHz, viz. in the middle of the operational bandwidth. Measurements for this study are given in Fig. 3.7. It is shown that a margin gain of 14 dB is achieved, implying that the system can

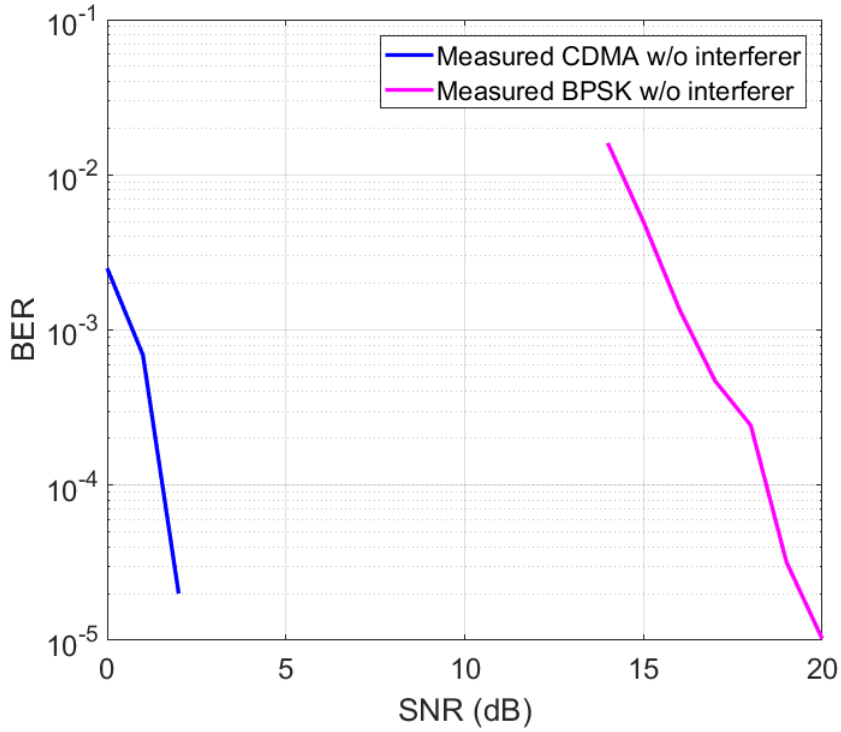

Figure 3.6: Measured BER with and without CDMA coding in absence of a single high-power interferer.

withstand an additional 14 dB of interference as compared to conventional BPSK transmission link.

But what does a 14 dB look like in a real world scenario? A typical application of a wireless communication system is the transmission of video between two devices. To show the result, a black-and-white image was transmitted using a simple BPSK system and subsequently the proposed system. In both cases, an interferer was blocking the transmission. The resulting received images from the two systems are shown in 3.8 and 3.9 respectively.

In the following sections, results from different interference scenarios are shown including swept, barrage and base interference.

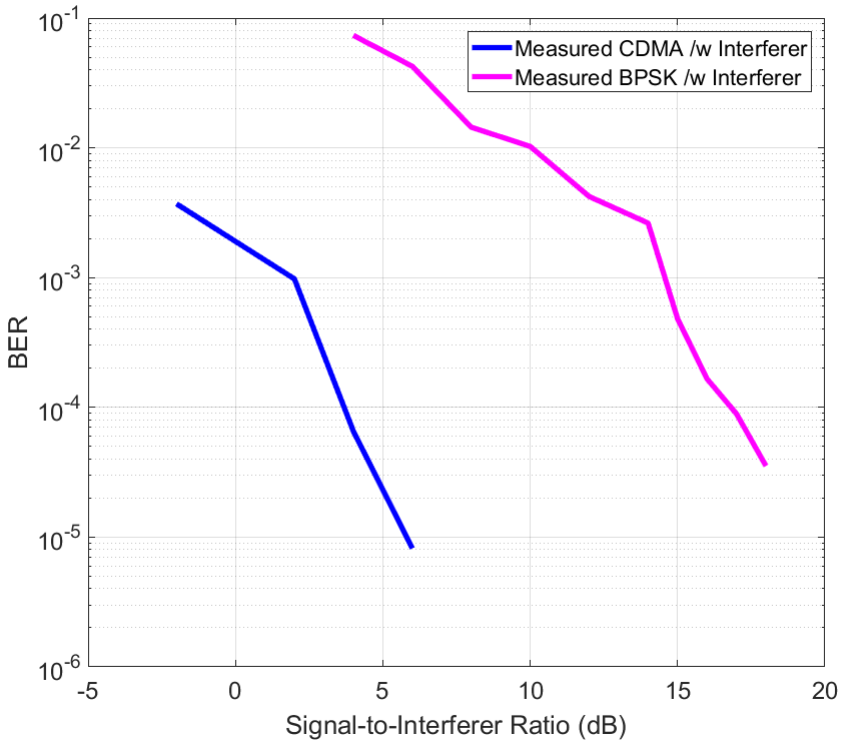

Figure 3.7: Measured BER with and without CDMA coding in presence of a single high-power interferer.

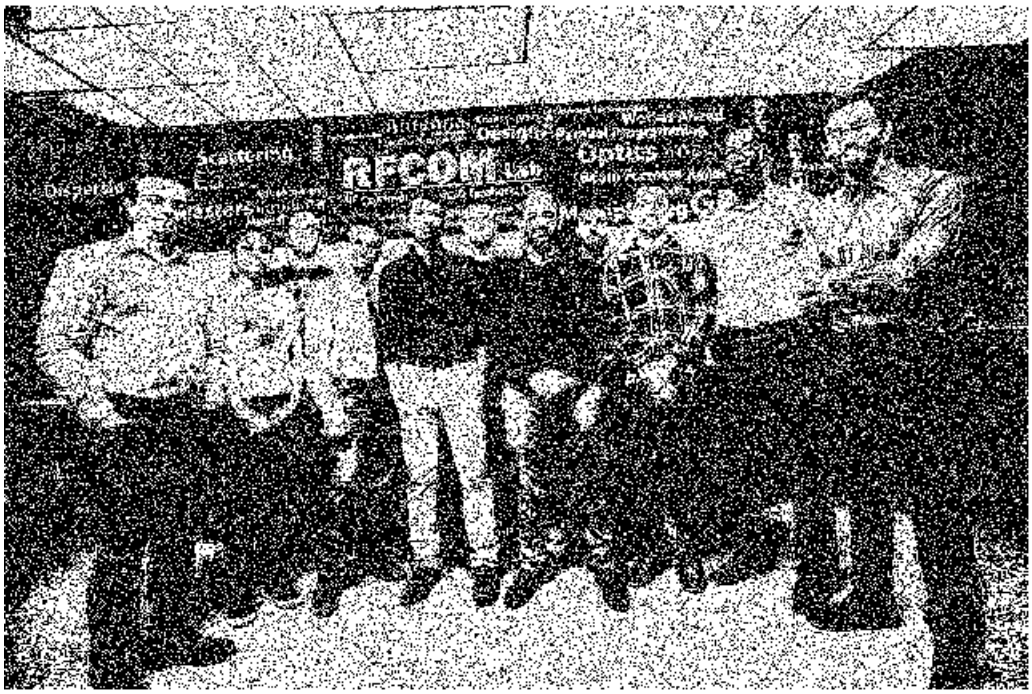

Figure 3.8: Sample image transmitted without any coding.

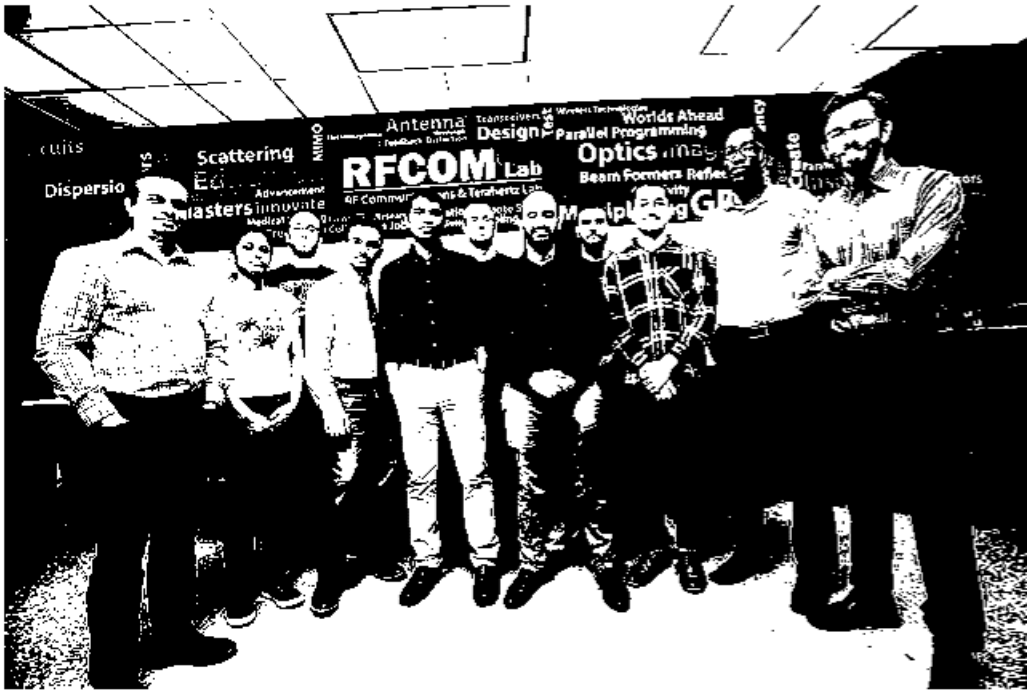

Figure 3.9: Sample image transmitted through the proposed spread spectrum system.

3.6 Measurements in presence of dynamic interference

In a world of high wireless congestion, the frequency spectrum is rarely static. Dynamic spectrum allocation, inter-modulation products and arbitrary interference can block wireless communication systems, in a non-predictive way. That being said, static interference scenarios are not enough to understand their impact. In the following sections we present results from dynamic interference scenarios including sweep interference, barrage interference, base interference.

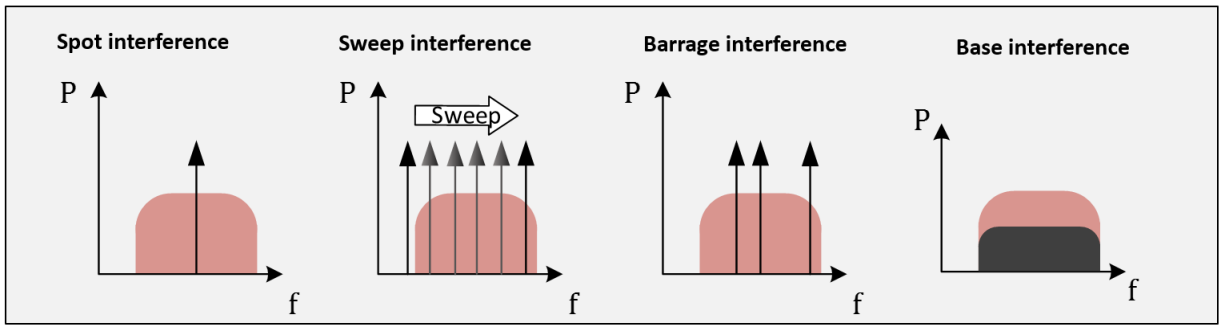

Figure 3.10: Interference scenarios.

3.6.1 Measurement in Presence of a Single Swept Interference

In this scenario, we assumed a single high power interferer trying to block the system. This time the blocker is not at a fixed frequency but was being swept across the entire bandwidth of the desired transmitted signal. Specifically, the interferer was generated using a Keysight signal generator and swept between 3.35 GHz and 4.65 GHz. The sweep time was 5 ms. This interval was based on a hypothetical Bluetooth system transmitting at the same frequency (Bluetooth employs frequency hopping as a means to reduce interference from other wireless systems and it hops at about

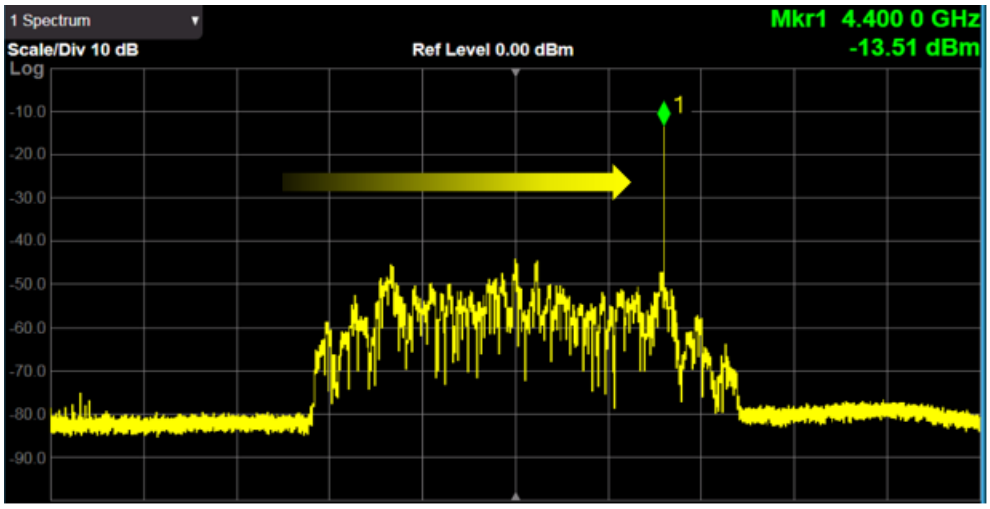

Figure 3.11: OTA spectrum of the transmitted signal and the swept interfering signal.

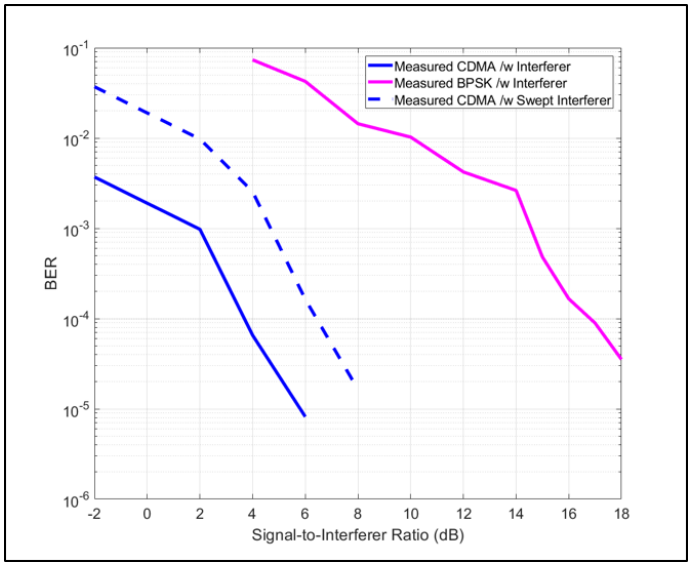

Figure 3.12: BER vs SNR of the proposed CDMA system in presence of both static and dynamic interference (solid and dashed curve respectively) and the uncoded BPSK system.

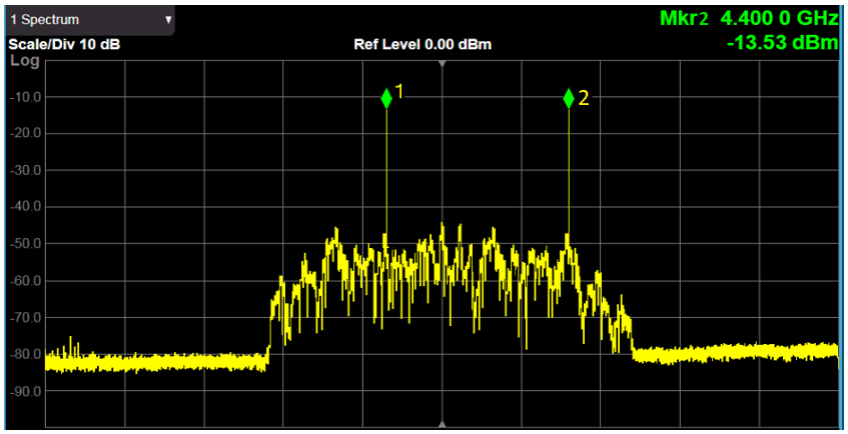

Figure 3.13: OTA spectrum of the transmitted signal and two interfering tones.

the same frequency as the interferer in this test). Fig. 3.11 shows the OTA spectrum of the desired signal and the swept interferer. Fig. 3.12 presents the measured BER. It can be seen that when the interferer is being swept, there is an additional 3 dB of degradation. This is likely due to the fact that the system is being blocked at very small intervals and in the entirety as opposed to a small fraction of the entire band (shown in the previous section).

3.6.2 Measurement in Presence of Multiple Static Interference

For this scenario, the same test as in the previous chapter was conducted but with two interferers instead of one. Due to equipment availability, we could not conduct the experiment with more than two sources of interference. In more details, the two sources of interference were two separate Keysight signal generators transmitting identical, between each other, power throughout the duration of the test. The signals were combined using a power combiner and then fed to the same horn as in the previous experiment. Fig. 3.13 shows the OTA spectrum of two high power

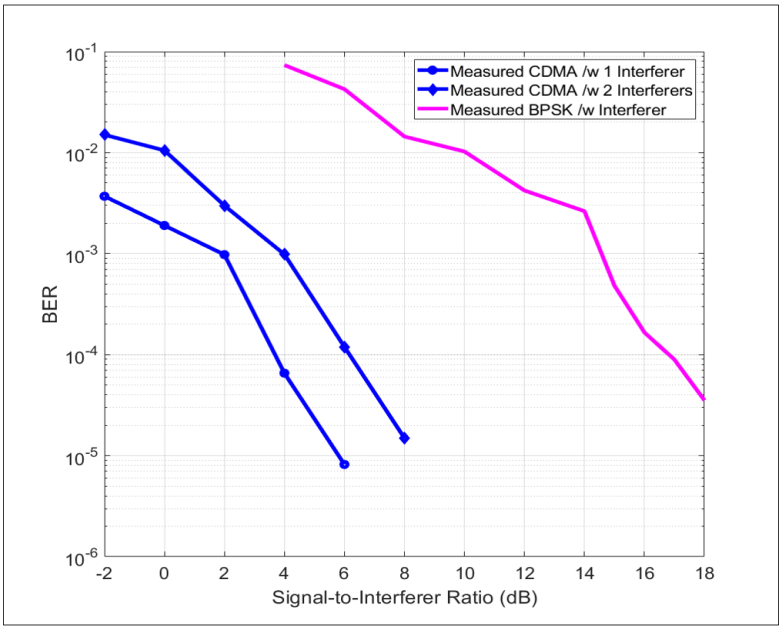

Figure 3.14: BER vs SIR of the UWB-CDMA system in presence of one and two interferers.

interferers blocking the desired spread signal. The resulting BER is shown in. Fig. 3.14.

3.6.3 Measurement in Presence of Base Interference

In this scenario base interference is considered. In this case, the interferer bandwidth is not a single frequency tone (as shown in the previous chapter) but it can cover

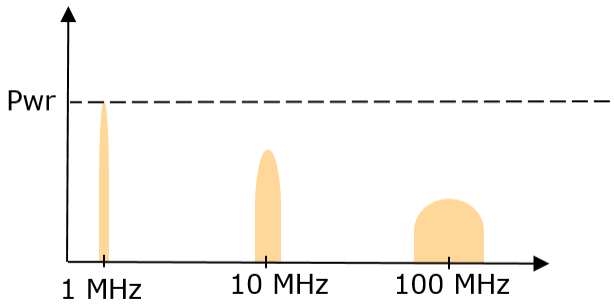

Figure 3.15: Varying power density of base interferer.

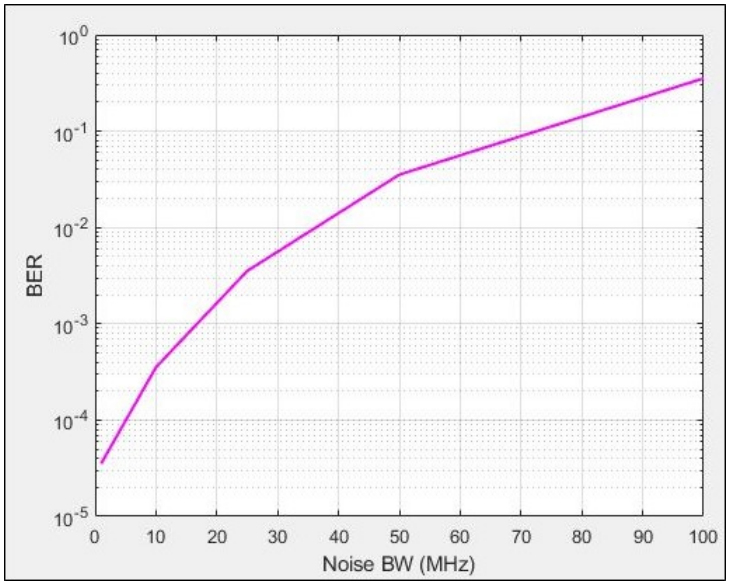

Figure 3.16: BER versus different noise bandwidth.

the entire band of interest of a fraction of it. In order to study the effects of base interference, a new interferer was designed. Specifically, the second channel of the Keysight Arbitrary Waveform Generator was employed to create a noise-like signal with various bandwidths. During the design process it was found that the device cannot provide constant power density. The maximum transmitted power is finite and is allocated according to bandwidth transmitted. In fact, the power density drops by 10 dB per decade increase in bandwidth. Fig. 3.15 shows examples of the bandwidth of the transmitted noise-like signal and the respective power density. The resulting BER versus different bandwidth of the base interferer are shown in Fig. 3.16.

An additional measurement was performed in order to study the effects of a base interferer having constant power density. Since the Keysight equipment has a limit on maximum power transmitted, a different approach was made. For this measurement, the maximum power density was identified when a noise like signal was transmitted occupying 100 MHz of bandwidth. Subsequently, when the bandwidth

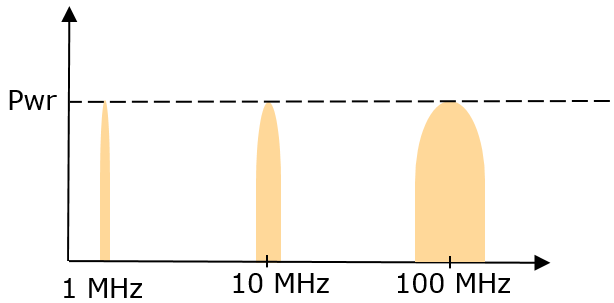

Figure 3.17: Constant power density of base interferer.

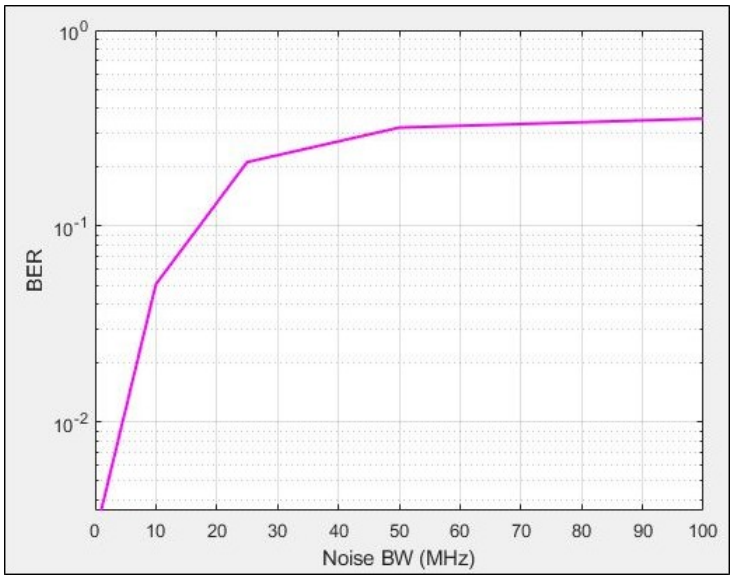

Figure 3.18: BER versus different noise bandwidth.

of the signal is decreased, a 10 dB attenuator per decade was added at the output of the front-end. The resulting power density is shown in Fig. 3.17. The resulting BER versus different noise bandwidth are shown in Fig. 3.18. Notably, both tests were performed in a high SNR environment in order to discard the effects of AWGN noise and focus only on the effects of base interference.

Finally, a set of measurements was conducted to provide a comparison between previous experiments. That is, the same test was performed at the same SNR as the previous tests. The results are shown in Fig. 3.19.

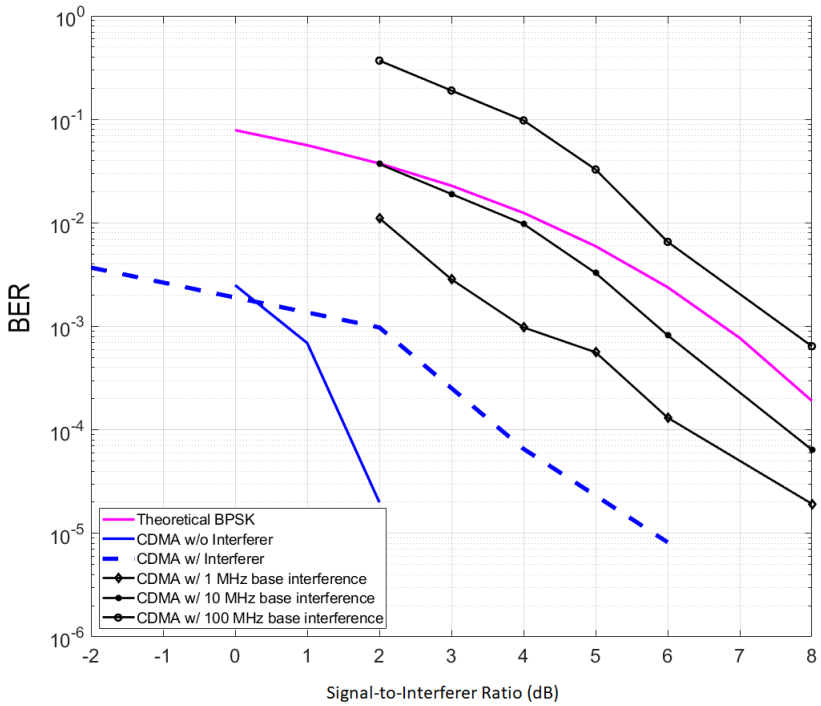

Figure 3.19: BER versus SNR of various interference modes.

CHAPTER 4

DIRECT RF SAMPLING TRANSCEIVERS FOR UWB COMMUNICATIONS

The need for data growth and higher throughput provide an impetus for a new class of digital radio transceivers with more efficient data converters can provide the needed data throughputs. These transceivers employ direct RF sampling and could be used in a production environment to enable software-defined radios. Specifically, Direct RF sampling captures the desired signal without a need for an analog RF front-end. As a result, all processing can be handled digitally, implying drastic reduction in hardware and power requirmenet. Until recently, commercial Analog-to-Digital Converters (ADCs) were limited to a speed of about 10 Gigasamples per second. Therefore Direct RF sampling could theoretically be achieved up to S-band (4 GHz). Currently, ADCs exceeding 256 GSPS may be found embedded in test/measurement equipment and optical networking systems [UXR] but are not available for general-purpose devices. The well-established approach of heterodyne receivers is to mix and downconvert the RF signal to a lower frequency prior to digitization. However, analog mixers are associated with nonlinearities resulting in distortions to the desired signal and may also generate extraneous spurious signals that cannot be easily removed. This issue becomes even more challenging at higher frequency bands. Therefore, ADCs/DACs implementations that offer up to 18 GHz bandwidth are highly attractive as they can provide coverage up to K-band without need of analog mixers.

This section serves as an introduction to direct RF sampling technology. It presents advantages and challenges of this approach. Below, we start by discussing traditional transmitters/receivers and their advantages/disadvantages depending on the application. Direct RF transceivers and their potential are discussed afterwards.

4.1 Traditional Heterodyne Receivers

Heterodyne have been traditionally employed for radar applications and RF communication systems. This architectures use a Local Oscillator (LO) with a mixer to down-convert the incoming signal to IF for digitization using lower speed ADCs. This process is referred to as heterodyning and is depicted in Fig. 4.1. An apparent disadvantage of this architecture is the generation of unwanted signals at the output of the mixer. Specifically, upon mixing the incoming signal, centered at f_c, with the LO sinusoid signal, the sum and difference of these signals as well as higher order harmonics and intermods are generated. In addition, heterodyne receivers suffer from the image problem. To filter out unwanted signals, more sophisticated designs are required implying increased complexity and additional hardware.

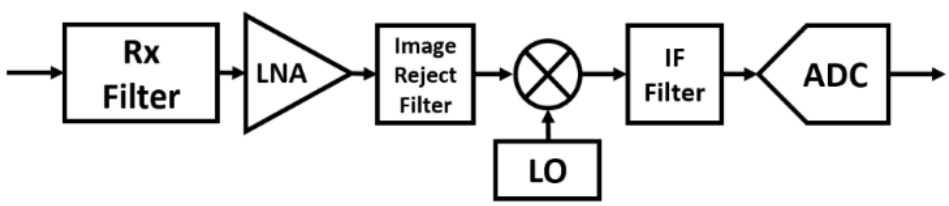

Figure 4.1: Heterodyne receiver architecture and associated mixing process before digitization.

The frequency plan for a heterodyne receiver is shown in Fig. 4.2. The desired wideband signal is centered at frequency f_c and, upon mixing, it is down-converted to an IF frequency depending on the LOs center frequency. Typically, down-conversion shifts the signal to $f_{IF} = f_c - f_{LO}$ where f_{LO} is the center frequency of the LO.

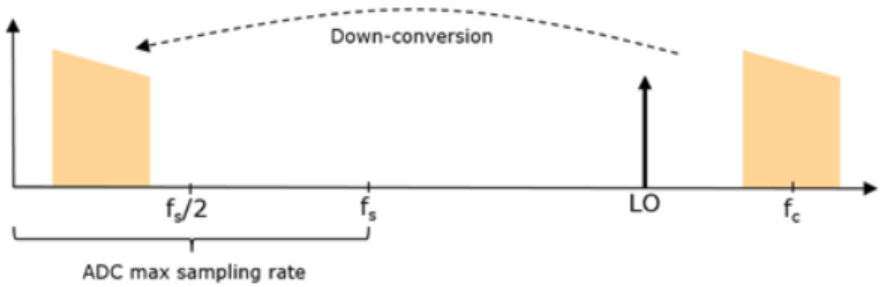

Figure 4.2: Frequency Plan of Heterodyne Receivers.

4.2 Direct Conversion Receivers

To overcome the aforementioned issues, Direct conversion methods can be employed using quadrature modulation/demodulation, as depicted in Fig. 3. Unlike heterodyne architectures, direct conversion receiver does not suffer from the image-frequency problem, implying fewer components and less cost. The advantages of the direct conversion receiver architecture made it attractive to IC designers. The frequency plan of the Direct conversion receiver is shown in Fig. 4. As usual, the LO is used to mix the desired signal and convert it to baseband. After filtering, the resulting quadrature baseband signal is fed to the dual ADCs.

The direct conversion receiver does have some limitations. Specifically, the high power local oscillator signal can leak back to the antenna causing self-mixing. This can result in large DC components and can even cause issues if leakage occurs into the low noise amplifier. To overcome this, we down-convert to a lower-IF frequency. This approach eliminates the DC offset but causes image signal components. Further, any phase and amplitude imbalances within the In-phase and Quadrature (IQ) chains can lead to other signal degradation.

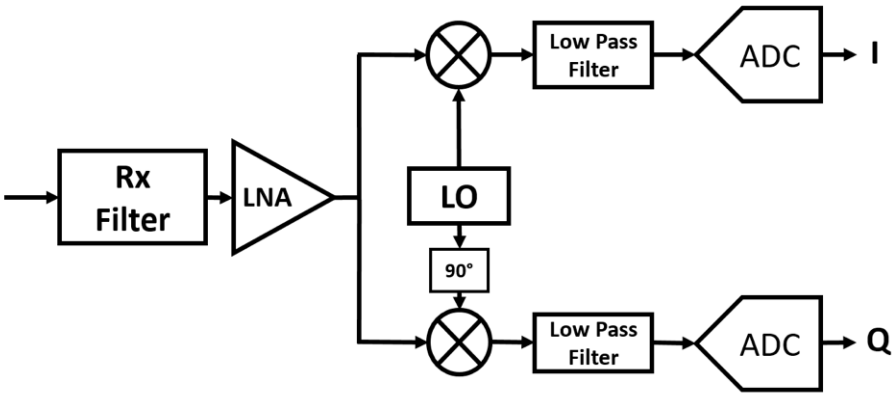

Figure 4.3: Direct Conversion receiver block diagram using quadrature modulation.

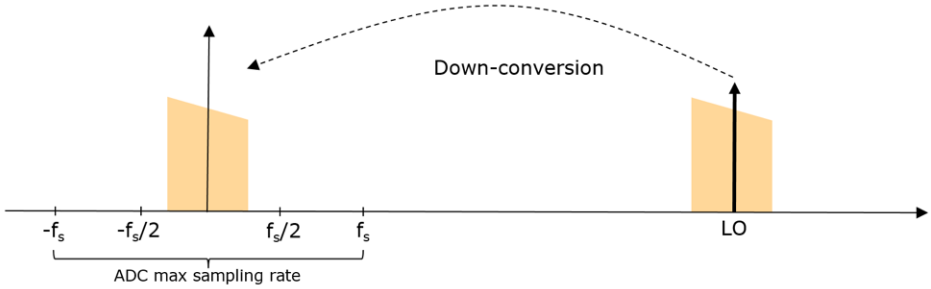

Figure 4.4: Frequency planning of the Direct Conversion receiver.

4.3 Direct RF Sampling Receivers

The aforementioned issues, including image signals, frequency dependent components, and DC offsets can be circumvented via direct digitization at the RF domain. To do so, much faster data converters are required. Indeed, ADCs with sampling rates of 65 GSPS [guz] or even 70 GSPS [IQa] employing the 14nm FinFET process are now available. Such extreme sampling speeds were achieved with the advent of a new interleaved time-domain ADC architecture known as Traveling Pulse Wave Quantizer (US Patent No. US9098072B1, 2015). This architecture is four times faster than conventional Successive Approximation Register (SAR) cores, and thus improving power efficiency by requiring fewer cores. Using these fast digitizers, in-

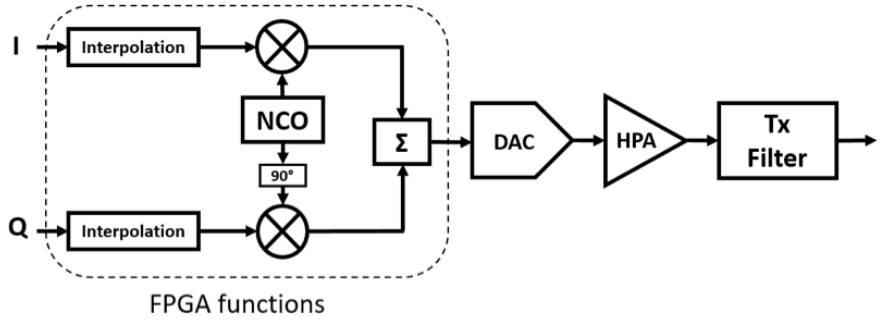

Figure 4.5: Direct RF sampling transmitter architecture.

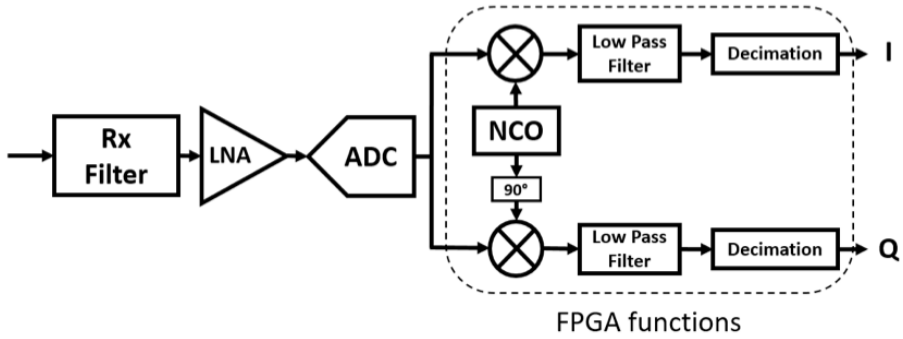

Figure 4.6: Direct RF sampling receiver architecture.

stead of down-converting to IF and then sample, digitization can occur at the RF stage, right after the antenna. Fig. 4.6 illustrates the architecture of the Direct RF sampling receiver.

Typical Direct RF sampling receivers consist of an antenna, a band-select filter, a Low Noise Amplifier (LNA), a channel select filter, a ADC followed by a Field-Programmable-Gate-Array (FPGA). The latter handles post-processing functions such as digital down-conversion, demodulation, digital filtering and decimation.

Fig. 4.7 shows the frequency plan for a Direct RF receiver. This technique was previously unavailable due to the lack of high-speed ADCs. However, new commercially available high-speed ADCs can capture/digitize the desired signal at RF, regardless of bandwidth. Once digitized, the signal is digitally down-converted to baseband using a Numerically Controlled Oscillator (NCO) implemented in the

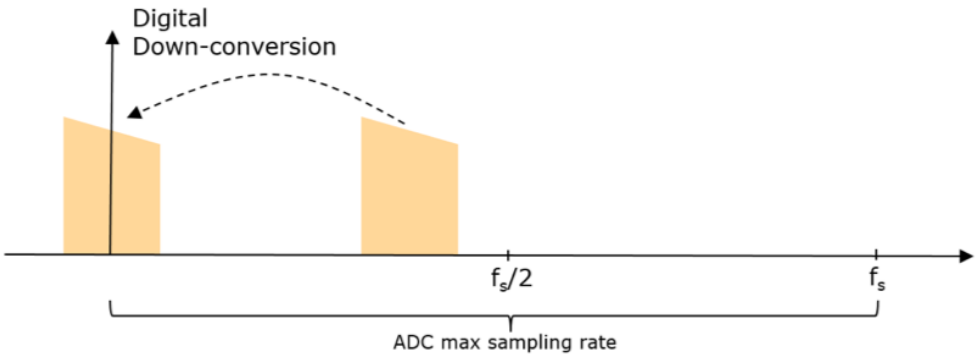

Figure 4.7: Frequency plan for the Direct RF sampling receiver.

FPGA. Filtering and decimation is also carried out to clean the signal prior to post-processing. As noted, an advantage of Direct RF sampling receivers is the elimination of analog mixers. By using faster ADCs, we can also eliminate some filters from the receive chain since aliasing from unwanted signals will not fold back to the desired band.

At the moment, one of the fastest ADC topologies relies on interleaving sampling [guz], to achieve 32 GSPS with 10-bit resolution. Using this approach, as many as 160 ADCs can be stacked to sample at shifted locations across the period as depicted in Fig. 4.9. The block diagram of a 4-channel ADC is depicted in Fig. 4.8. Notably, this ADC has a total available sampling rate of 64 GSPS which can either be divided in 2 32GSPS channels or 4 16GSPS channels. For the four channel configuration, FPGAs provided by Intel are responsible for the control of the core and acquisition of the data. Due to the massive amount of the captured data, which is not possible to be transferred in real-time to a host computer, four DDR 4 RAM banks are available to store the data temporarily in order to be off-loaded later using another FPGA. This FPGA, located at the bottom of the block diagram (see Fig. 4.8) acts as a bridge between the incoming data and the PCI express bus which provides connectivity between the ADC and the host computer.

Alternatively, a faster Optical Data interface can provide streaming data. However, the sheer amount of data may be difficult to process in real-time. As such, some form of decimation is necessary.

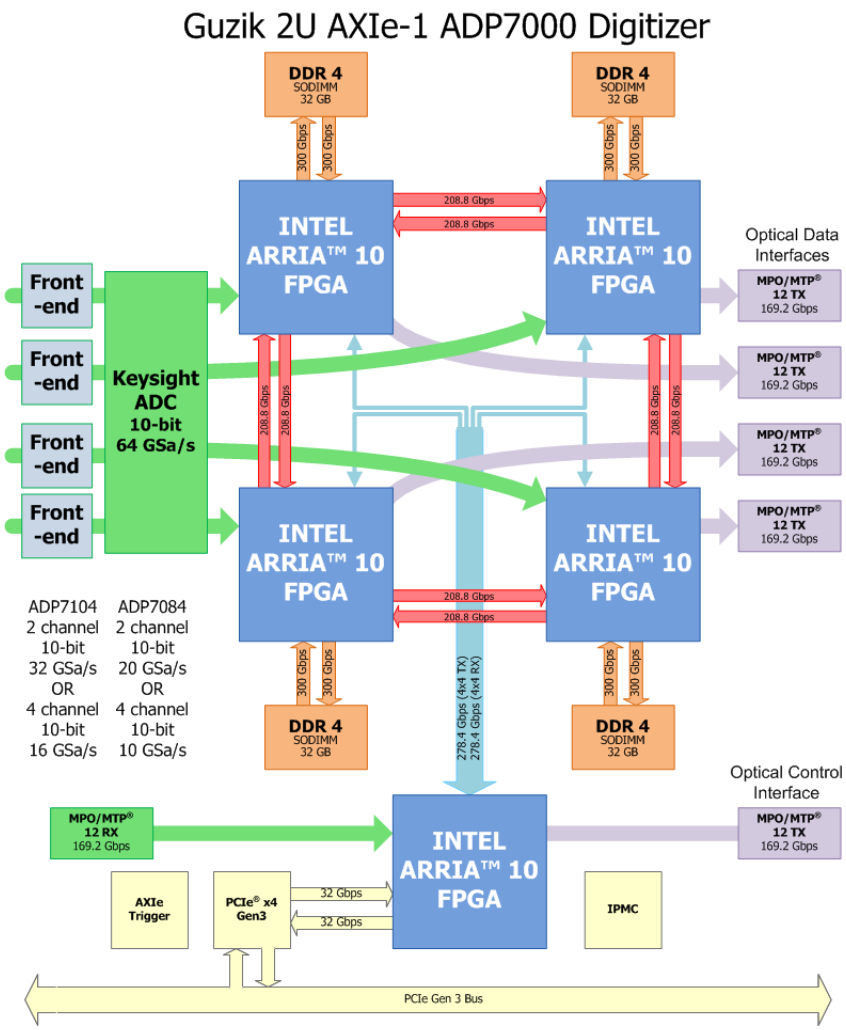

Figure 4.8: Block diagram of the four-channel ADC [ADP]

The Keysight ADC core has some limitations. For instance, challenges exist with mismatches between interleaved signals, as depicted in Fig. 4.9. These mismatches manifest as spurious components, referred to as interleaving spurs. For example, a 2-way interleaving ADC may have variations in gain among the 2 channels. This gain imbalance is likely to generate gain spurs at $f_s/2$ that could lead to an amplitude

modulated signal. Similarly, other signal mismatches or timing offsets may generate interleaving spurs. To mitigate interleaving spurs mismatch calibration is required. Channel randomization may also be used to decrease spurs. Signal misalignments are often corrected using equalization methods and are known to reduce spurs by as much as 18 to 33 dB (USA Patent No. US7408495B2, 2006).

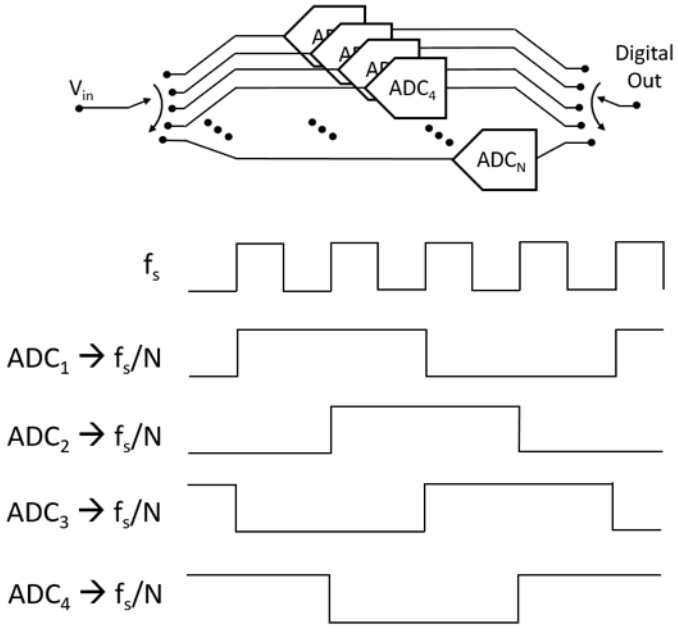

Figure 4.9: Interleaving sampling for faster ADCs.

4.4 Oversampling and Undersampling Considerations

Due to the large available bandwidth in Direct RF Sampling transceivers, the actual signal of interest will occupy a bandwidth that is smaller than the Nyquist bandwidth. As a result, oversampling occurs and the Signal-to-Quantization Noise ratio (SQNR) needs to be adjusted. Specifically, a correction factor must be included to account for the SQNR increase. The SQNR for an ADC is given by [SDX05]:

$$SQNR = 6.02N + 1.76dB + 10log\left(\frac{f_s}{2 * BW}\right) \tag{4.1}$$

where N is the number of bits per quantization level, f_s is the sampling rate, and BW is the bandwidth of the signal. The process of sampling a signal at a rate which is greater than twice its bandwidth is referred to as oversampling, and f_s/BW is the oversampling ratio. The in-band quantization noise is inversely proportional to the oversampling ratio, resulting in 1/2-bit (3.01 dB) improvement in resolution for every factor of 2 higher than the sampling frequency. The anti-aliasing filter and the reconstruction filter of the ADC are relaxed, resulting in more linear phase. This allows multiple adjacent channels to be subsumed simultaneously into the digital domain for digital channel selection and post-processing. In addition, it allows decimation and interpolation filtering in the digital domain.

Undersampling can also be used to shift the signal to lower frequencies. In this case, the signal of interest lies in a higher Nyquist zone above the baseband and is intentionally aliased into the first Nyquist zone. However, when undersampling, the wideband thermal noise from the sample/hold and ADC, leads to an inherent 3.01 dB per octave noise penalty. Nevertheless, the penalty from aliasing wideband thermal noise is not severe relative to the benefit of lower jitter due to a lower incoming frequency content into the sampler (assuming a low-IF digital receiver).

4.5 Direct RF Sampling Transmitters

As is the case with receivers, by resorting to digital up-converters, analog components can be minimized, leading to simpler and wideband transmitter implementations. Currently, an 8-bit Digital-to-Analog converter (DAC) is available at a rate of 92 GSPS [keya]. This implies an effective bandwidth of 32 GHz (limited by the

front-end) with up to 90 dBc Spurious Free Dynamic Range (SFDR). As in the case of the receiver, the DAC-FPGA interface (or host computer) can be a potential bottleneck. Specifically, current streaming data rate using available digital technology is 600 Mbyte/sec. For a 10-bit ADC this translates to a 120 MHz of bandwidth at the receiver end. As far as Digital Up-Conversion (DUC) is concerned, the maximum modulation bandwidth that can be up-converted is 1920 MHz within the FPGA. Another technique for designers to consider relates to Soft-DUC, a process of performing DUC in software, rather than in the FPGA. Such option can avoid the throughput bottlenecks with existing FPGAs.

4.6 Challenges and Design Considerations

Despite the benefits of Direct RF sampling techniques, there are a few challenges that must be considered. First of all, RF converters at the moment require much higher power. The following equation describes the Figure-of-Merit between power consumption at a certain sampling rate and ENOB.

$$FOM = \frac{P}{f_s * 2^{ENOB}} \tag{4.2}$$

where P is the consumed power, f_s is the sampling rate, and $ENOB$ is the Effective Number of Bits. It is obvious that by increasing sampling rate and ENOB, the above FOM degrades significantly. This FOM refers to the converter core and does not include necessary circuitry such as buffers, sample and hold, clock distribution, etc. These additional circuits may exceed the power consumed by the core itself. For reference, the AD9213 from Analog Devices has a sampling rate of 10 GS/s and an 8.3 bits ENOB at $f_s = 4$ GHz and the entire chip consumes more than 4 W of

power. Furthermore, such high conversion speeds require high speed digital signal processing which also consumes high power.

The dynamic range of the receiver is another critical aspect of the system and could and should be considered towards a design. Current RF converters offer a maximum resolution of 10 bits. This translates to a dynamic range 62 dB. For some applications this amount of dynamic range might not be adequate enough as traditional receivers require typically at least 12 bits. For example, for applications such as electronic warfare, strong interfering signals could potentially block communication due to the inability of the receiver to capture weaker signals. Another challenge associated with high speed RF converters is the need for wideband filters and amplifiers. Of course, wideband amplifiers are difficult to design while maintaining linearity and low noise across large spectrum. The integration of noise across the larger spectrum degrades the resolution of the converter due to higher thermal noise and higher sampling jitter. On the other hand, RF converters require extremely low jitter sampling clocks at RF frequencies. A metric that describes the relationship between jitter and sampled frequency at the input is the following:

$$SNR_{jitter} = 20log10(\Delta t_{RMS} 2 f_{in}) \tag{4.3}$$

where Δt_{RMS} is the standard deviation of the jitter. From this, a value of $\Delta t_{RMS} = 100\ femtosec$ implies SNR = 64 dB at $f_{in} = 1\ GHz$. But this value reduces to SNR = 30 dB at $f_{in} = 50\ GHz$.

Certainly, high-speed DACs and ADCs are expensive at the moment and also come with relatively high-power consumption, but these costs are likely to be reduced as 5G products emerge. The overall trend is a two-fold increase of FoM every 2.6 years which can be seen in the Fig. 4.10.

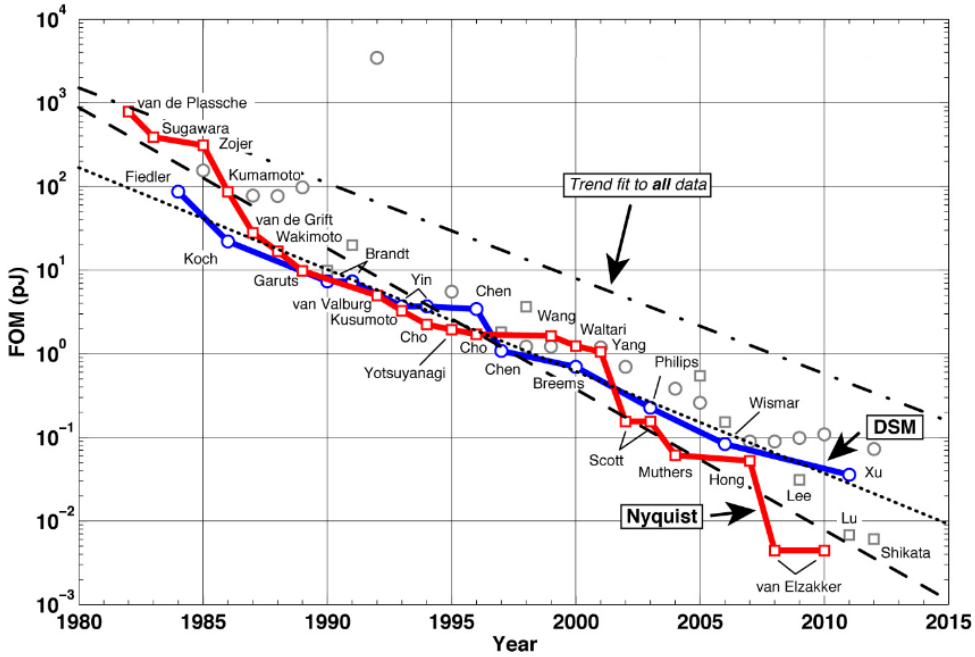

Figure 4.10: Analog-to-Digital converters over the past 30 years [jon].

As it is well known, such bandwidths are available in the upcoming 5G bands allowing for wideband high data rate communications. Furthermore, large bandwidth and Digital Up/Down Conversion using Direct RF Sampling could be beneficial to other areas such as advanced digital beamforming, multi-mode RADARs and electronic warfare systems. Some of the applications are discussed below. However, being able to access such large frequency of operation and receive multi-GHz signals presents us with another serious issue. That is, the amount of computational power required to process the sheer amount of data received be the ADC. A typical 20 GSPS 8-bit receiver, would require a processor being able to transfer through an interface and process 20 Gigabytes of raw data per second. For a single-band frequency of operation and relatively small bandwidth this would not be a problem since decimation would decrease the amount of data. Nonetheless, for a multi-purpose radio, being able to operate across all the bands with large bandwidth at the same time, the amount of data would be staggering. A cluster of computers added at the back-

end would be an easy solution, but this would also result in additional cost and complexity. Alternatively, artificial intelligence (AI) and machine learning (ML) techniques could be useful to determine which channels are and should be used by the users and determine the relevant information in the ocean of data being received and transmitted.

4.7 Ultra-wideband Communications

Recently, the FCC announced 3.85 GHz of licensed spectrum and 7 GHz of unlicensed millimeter wave spectrum. The licensed spectrum includes the bands: 27.5 - 28.35 GHz, 37 - 38.6 GHz and 38.6 - 40 GHz. The unlicensed spectrum refers to the 57-64 GHz band which was introduced in 2013. In addition, FCC allocated the adjacent 64 - 71 GHz band. The latest 5G New Radio (NR) specification (38.101-1) suggests that frequencies below 6 GHz can also be used for 5G communications [IEE].

The aforementioned added bandwidth can possibly deliver 1000-fold higher data rates. To enable these added speeds, Direct RF sampling transceivers and wideband RF front-ends are required. Below, we assess the utility of Direct RF front-ends, considering the transmission of ultra-wideband CDMA signal (see Fig. 4.11). The considered signal is coded using Gold codes and occupies approximately 1.3 GHz after pulse shaping. For transmission, this signal is digitally up-converted to 4.5 GHz (see Fig. 4.5) and transmitted via a wideband horn antenna. For our case, the transmitter was emulated using the Keysight M8190A Arbitrary Waveform Generator. At the receiver, the received passband signal is directly captured using the Guzik M9734G digitizer and subsequently down-converted to baseband. The received signal is then aligned and despread. Then, cross-correlation is used in a

software fashion. Clock recovery, carrier synchronization, timing synchronization and payload extraction are all performed in real-time on the host computer.

As expected, the use of large bandwidth allows for longer codes, more complex modulation schemes and therefore higher speeds and greater security. Specifically, by employing the maximum bandwidth that ADCs can currently provide (approximately 10 GHz [guz]) and dropping the bit rate to 0.5 Mbps, we can provide a processing gain of 43 dB, as calculated using Eq. 1.2. This implies improved sensitivity, higher security and longer distance communications.

Notably, the resolution of an ADC improves by 6 dB (one bit) for every 4X factor of decimation. This can help the designer directly trade-off sample rate for increased resolution in case lower frequency of operation is desired.

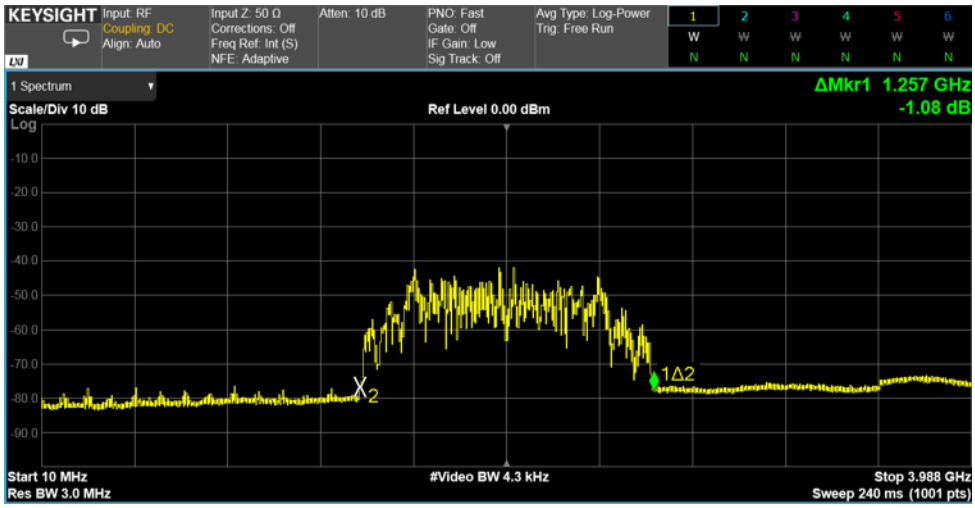

Figure 4.11: Over-the-Air (OTA) CDMA signal spanning across 1.3 GHz.

In the next chapter, we will present a method of performing Direction of Arrival (DoA) for ultra-wideband signals using Direct RF sampling. Traditional methods and algorithms will be described along with their limitations and challenges in implementing a practical system. Additionally, a practical system will be presented utilizing the coded signal of the proposed communication system to determine the

position of an unknown transmitter using Direct RF sampling and four receiving sensors.

CHAPTER 5

DIRECTION FINDING OF UWB SIGNALS USING DIRECT RF SAMPLING

5.1 Introduction to Direction Finding

Identifying the direction of arrival (DoA) of an incoming signal has been a topic of significant interest. DoA estimation techniques have a wide application in radar, sonar, wireless communications, and radio navigation [SM97, NGW11, BCH08]. In addition, law enforcement authorities have a strong need for a technology for radio monitoring applications such as finding the source of interference and unauthorized emitters. In the military world, there has also been a significant interest towards detection of adverse activities and information gathering. Similarly, Radio astronomy and remote-sensing are areas that could be benefited from Direction Finding (DF) methods.

One of the applications of the proposed Utra-Wideband CDMA system, described in the previous chapters, is low-power communication. Such system should be able to transmit at the lowest power configuration possible in order to save power resources. Another application is the ability to transmit at the noise floor, or even below it, as a means to covert communication. Both cases require a priori knowledge of the transmitter since the wideband signal at the noise floor can only be allocated to a specific emitter if the direction is known. Therefore, DoA estimation is an important step, particularly since reading the contents of such emissions is usually impossible.

Antenna arrays can be utilized to increase the gain to certain directions and recover low-power signals. To do so, the direction of such signals has to be estimated. With the advent of low-cost back-ends and Digital Signal Processors, direction find-

ing can now be performed using antenna processing algorithms by utilizing the information about the incident wave derived directly from the antenna elements. Factors to be considered when designing a direction finding system are: Accuracy, Sensitivity, Bandwidth and frequency range, Minimum signal duration Operation in multipath-rich environment, Scanning speed, especially for Frequency hopping systems.

There are 3 techniques to estimate the direction of arrival of a signal:

- Beam-forming methods
- Subspace method such as MUSIC and ESPRIT
- Element Correlation

5.2 Beamforming methods for Direction Finding

Historically there have been many Direction Finding systems, employing mainly some kind of beamforming technique [KMCV07]:

1. Circularly Displayed Antenna Array (CDAA)

   This type is sometimes referred to as a The Wullenweber (the original name introduced by Dr. Hans Rindfleisch was Wullenwever) and it was an improvement done by the University of Illinois around 1950 [KMCV07]. It is a large circular antenna array used for radio direction finding at high frequencies. It was used for military purposes to triangulate radio signals for radio navigation. A spinning rotor, capacitively coupled ontiguous elements of the stator at any moment in time, provided both summed and differenced outputs. Thus, the spinnig rotor acted both as a commutator switching between antenna elements and as a beamformer.

2. Pseudo-Doppler Direction Finding System [EG47]

   This system measures signal phase changes at switched sequential elements located on the circumference of a circle. When every antenna element is sampled, the signal phase will appear spatially shifted, thus producing a bearing estimate on the received signal. The pseudo-Doppler relies upon capturing very short sampling time from each antenna element. The original method used a single antenna that physically moved in a circular fashion but modern approaches use multi-antenna circular arrays with each antenna sampled in sequentially.

3. Watson-Watt Direction Finding System

   The Watson-Watt uses two orthogonal Adcock beamforming arrays to perform an amplitude comparison on the incoming signal. An Adcock antenna pair is a pair of monopole or dipole antennas that takes the difference of the received signal at each antenna [Kes03]. In the receiver, the AOA θ is estimated by taking the arctangent of the voltages from these two RF pairs.

4. Brueninger Direction Finding System

   The Brueninger system is essentially an improvement over the Watson-Watt system. It employs a reference antenna to distinguish signal phase which resolves ambiguities. The omni-antenna can be a separate antenna or a sum of all Adcock antenna elements. More antenna elements can be combined to create the beam patterns pairs. Phase-amplitude correlation methods are used instead of taking the arctangent of voltages from the RF pairs.

5. Butler Direction Finding Systems

   The Butler matrix can be used in many applications to generate a number of staring beams. It consists of fixed phase shifts interconnected to hybrids

and yields orthogonal beams [But66, BMSS02]. Butler matrix is the analog implementation of the Fast Fourier Transform (FFT). But it is developed before the FFT. There is an important difference between FFT and Butler matrix, i.e., a Butler matrix processes signals in the analog domain, whereas the FFT processes signals in the digital domain. Currently, the largest possible Butler matrix is 64x64 and is limited to permitivity microstrip technology is used [HV90].

Other examples of beamforming methods is the minimum-variance distortionless-response (MVDR) beamformer [Cap69] [Cap79] [LB05]. The latter is also called the Capon beamformer. It belongs to the family of constrained optimization beamformers and it works by maximizing the Signal-to-Noise Ratio (SNR) of the incoming signal. If the direction of the incoming signal lies withing the given direction, then maximum power is received and hence the emitter can be located. However, as one could imagine, this method greatly depends on achieving high SNR and can only be applied to narrow-band signals.

5.3 MUSIC/ESPRIT Algorithms

In this section, we highlight the MUSIC and ESPRIT algorithms. MUltiple SIgnal Classification (MUSIC) algorithm is such an example. This method works by estimating the frequency content of the incoming signal and its auto-correlation matrix using an eigenspace method [Sch86]. It provides high resolution, however, there are some key limitations. MUSIC algorithm is based on Pisarenkos method for harmonic decomposition [Pis73]. This method requires a priori knowledge of the components, which limits the methods usefulness. Furthermore, searching through all the available angles to generate the spatial spectrum requires large computational power and

storage. Another limiting factor is the bandwidth of the signal that can be resolved. An incoming signal of about 80 MHz would require approximately 100 Gigabytes of RAM on a standard host computer. For next-gen systems, which would employ channel bandwidth in the order of gigahertz, this would clearly be an issue. Additionally, the analog components required to operate in multi-gigahertz operation do not currently exist. Another popular method for DoA is the Estimation of Signal Parameters via Rotational Invariant Techniques (ESPRIT). The ESPRIT method is faster and less computational expensive than MUSIC but requires twice the number of sensors as compared to MUSIC algorithm in order to achieve the same accuracy. However, as in the case of MUSIC, the required storage is still prohibitive. For instance, a signal of 80 MHz would require about 60 Gigabytes of RAM.

5.4 Time Difference of Arrival (TDOA) for UWB signals

A solution to the aforementioned limitations could be the implementation of Time-Difference-of-Arrival (TDOA) [KMCV07] using Direct RF sampling. TDOA estimates the time difference between the received signals of different receivers by performing cross-correlation. Traditionally, TDOA has not been a favorable option since the accuracy was rather low for narrowband signals. To time-align the received signal at each sensor, the signal must contain nonrandom, non-repeating structure. Many interference sources emit white noise, which lacks the structure necessary to align the signal. Simple emitters, such as a sine wave generator, produce a repeating pattern that has structure, but the repeating pattern does not allow for a unique time-alignment. Repeating patterns can be aligned at multiple positions with no means of distinguishing a correct time-shift. That is, for narrowband signals the cross-correlation of the received signals does not generate a sharp

correlation peak. Modulated signals contain a structure that can be aligned in time using cross-correlation. Good examples of modulated signals are FM radio broadcasts and cell phone signals. For this reason, TDOA is typically used to locate rogue broadcast signals, and other communication signals that are out-of-band or otherwise unexpected. On the other side, next-gen systems employing UWB signals will produce a very sharp peak hence improving the accuracy dramatically since their structure contains a less repeating pattern. Furthermore, by employing Direct RF sampling, we enable access to multi-gigahertz bandwidth of operation, which was previously not available due to the lack of available components.

Guzik digitizers provide synchronized ADCs which can measure a time difference of 2 picoseconds at SNR = 0 dB when using a 4 GHz Frequency Modulated (FM) chirped signal by cross-correlating two received signals. Averaging 50 repetitions would decrease the difference to 0.3 picoseconds. This level of resolution makes this method a prime candidate. Alternatively, Gold codes, which are already being used by our UWB-CDMA system, can be employed giving an added benefit to the entire platform. To illustrate the concept of increased resolution using larger bandwidth, simulations of various bandwidth signals were performed. Fig. 5.1 shows the cross-correlation of the two received signals. Both signals are FM modulated chirp with 10 MHz bandwidth. The simulated delay is 0.3 microseconds at SNR = 0 dB. The cross-correlation is given by:

$$(f \otimes g)(\tau) = \int_{\infty}^{-\infty} \overline{f(t)} g(t+\tau) dt \tag{5.1}$$

where f and g are the two signals that are correlated.

In Fig. 5.1, the plot exhibits a peak at the simulated delay. However, the resolution is not adequate enough for direction of arrival estimation. That is, the resulting cross-correlation cannot be employed for succesful direction finding since the low

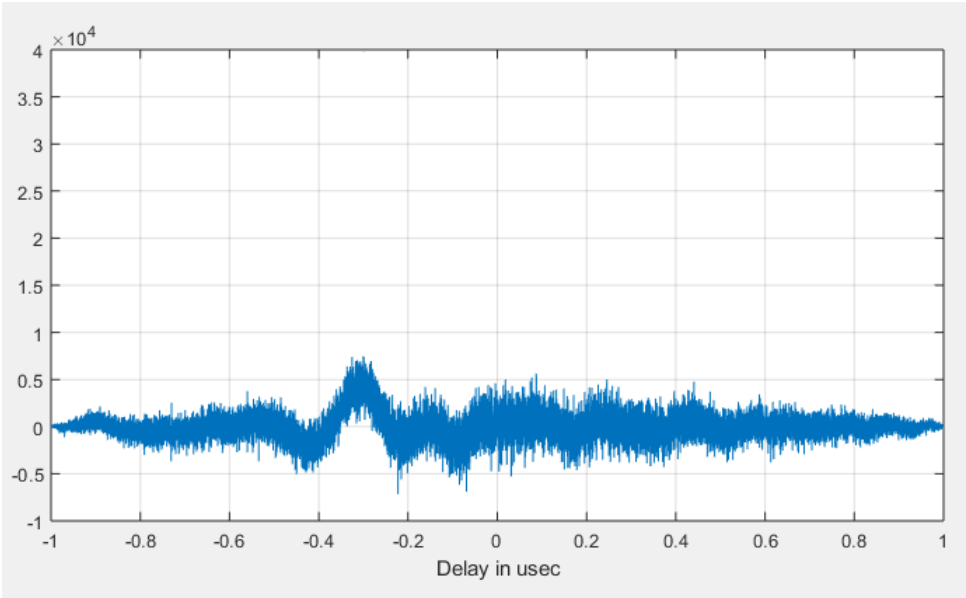

Figure 5.1: Correlation of two incoming chirped signals of 10 MHz bandwidth.

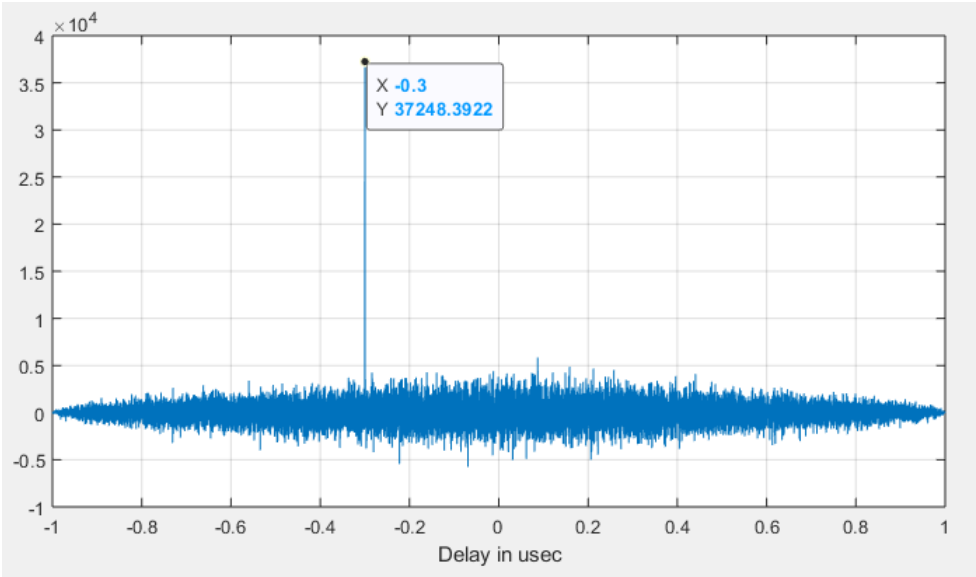

Figure 5.2: Correlation of two incoming chirped signals of 4 GHz bandwidth.

resolution would create a large offset error. The same test was repeated using a 4 GHz FM modulated chirp signal at same SNR. Fig. 5.2 shows the correlation of the two signals. The plot exhibits a sharp peak at exactly the same simulated delay with perfect accuracy. This test indicates the benefits of UWB signals for DoA applications.

As a practical application, we considered DoA estimation of an incoming signal using four receivers. Specifically, DoA is assessed for a real-world UWB signal below the noise floor. As already mentioned, current architectures and algorithms, such as MUSIC and ESPRIT, are unable to determine angle-of-arrival (AoA) for UWB signals as these techniques are limited to few MHz.

It should be noted that TDOA accuracy really depends on the quality of the signal. Signal strength is not normally an issue, as long as the signal is clearly present and presents a discernable I/Q diagram, but it can be rather noisy. However, higher signal strength will not necessarily produce better resolution. Multipath signals can degrade the system and make it more difficult to find the proper time alignment. If the strongest component of the signal is a reflection off of some nearby surface, then the distance calculation will be the reflected signal path, rather than the Line-of-Sight path between the sensor and emitter.

Another important aspect of a TDOA is sensor synchronization. For collocated receivers, this should not present us with problems since they can be easily synchronized using a common clock. However, for sensors located far away from each other, precise synchronization is required, as the slightest drift in time would cause large error offsets. GPS synchronization may be used in this case. Typically, synchronization every one second is enough to provide good results.

Sample rate is a key factor in determining spatial resolution. Sample rate is the number of I/Q data pairs collected per second. This is by definition the temporal

resolution: the spacing in time of the sample data points. The time separation is multiplied by the speed of light to get the distance separation, so the spatial resolution is directly proportional to the temporal resolution. As a specific example, consider a sampling rate of 50 kHz for a typical FM signal. This rate yields a time resolution of $\frac{1\ sec}{50{,}000\ samples} = 0.2\ \mu s$. A 0.2 μs time resolution gives $0.2\mu s * 3x10^8 m/sec = 6\ km$ per data point. A spatial resolution of 12 km is not very good. If we employ the max sample rate of the Direct RF sampling receiver is 20 GHz, then the resolution is effectively 0.015 meters. One would assume that just by increasing the sample rate to increase the spatial resolution would be a successful endeavour. However, there is a practical limit to how much you can increase the spatial resolution by increasing the sampling rate. This is determined by the underlying modulation rate of the signal of interest. Samplnig at extreme rates would not increase the resoltuion since the sampled signal will contain mostly noise anyway, so there is a practical limit to the usefulness of sampling at higher and higher rates. A good rule of thumb is to sample at 20 points per period.

Finally, TDOA may also be used for lower bandwidth signals (i.e. in the order of kHz). Averaging is a method to increase the resolution. This can accomplished by repeating the measurement several times and averaging for each sensor pair. This number will vary from measurement to measurement due to statistical noise and uncertainty in the measurement data. As an example (using 250 kHz as the sampling rate), the expected uncertainties are calculated and shown here in Table 5.1 [anr]. In this figure, N is the number of measurements taken in the averaging process.

N	Uncertainty (m)
1	600
3	346
5	268
10	190
15	150
20	134
50	85

Table 5.1: Expected location uncertainty for a sample rate of 250 kHz.

5.5 Experimental Demonstration

To carry out the direction of arrival estimation using a Direct RF sampling receiver, we adopted a time difference of arrival (TDOA) method using four channels. This technique requires high speed ADCs as is the case with our Guzik ADC receiver. To illustrate TDOA using a Direct RF sampling receiver, we demonstrate below the DoA estimation of a 1.3 GHz bandwidth signal at a carrier frequency of 3 GHz. To emulate delay from different antennas we used coaxial cables with various lengths. A transmitter was emulated using Keysight's DAC. The signal transmitted is the same 1.3 GHz Gold coded signal which was used for all the previous experiments. On the receive side, once all four signals are digitized, they are down-converted digitally. After that, correlations between all four channels are perform using MATLAB to determined the relative delay Δt. The angle of arrival is then found using:

$$\theta = sin^{-1}\frac{\Delta t \times c}{d} \tag{5.2}$$

where d is the distance between the antenna elements and c is the speed of light. As depicted in Fig. 5.3, direct RF sampling receivers are not only capable of providing accurate estimate of direction of arrival but can also process and resolve the direction of arrival of UWB signals.

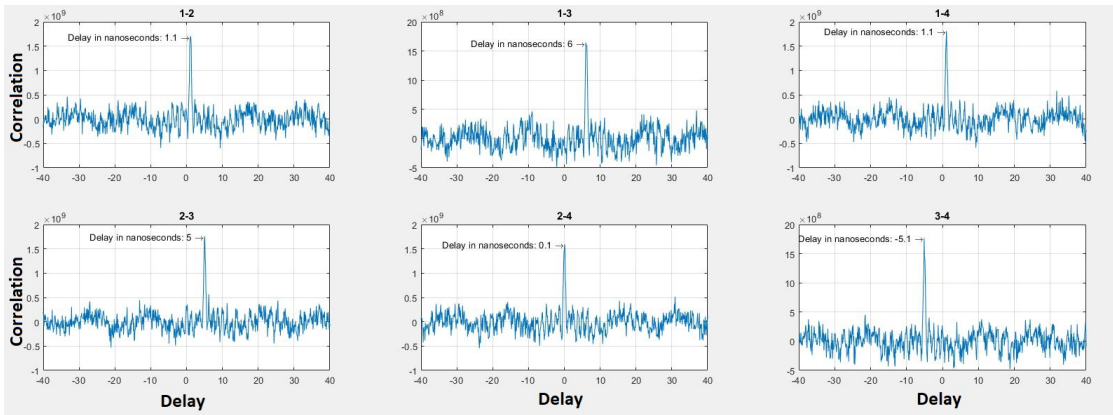

Figure 5.3: Example signals showing the relative delay between four UWB signals.

In more details, six unique combinations of correlations between the four receivers are shown in Fig. 5.3. These delays can be used to plot hyperbolas of constant delays between two receiving sensors. The intersection of these plots will yield the precise location of the transmitter. In more details, once the signal is received by two receivers, the difference in arrival time can be used to calculate the difference in distances between the target and the location of the sensors. This difference can be calculated using:

$$\Delta d = c * (\Delta t) \tag{5.3}$$

where c is the speed of light and Δt is the difference in arrival times at each sensor point. In two dimensions, this leads to the following equation:

$$\Delta d = \sqrt{(x_2 - x)^2 - (y_2 - y)^2} - \sqrt{(x_1 - x)^2 - (y_1 - y)^2} \tag{5.4}$$

where (x_1, y_1) and (x_2, y_2) are the known positions of the sensors. Using nonlinear regression, this equation can be converted to the form of a hyperbola [SM16]. Analytically, (5.4) can be written in the form of a hyperbolic conic section, such as:

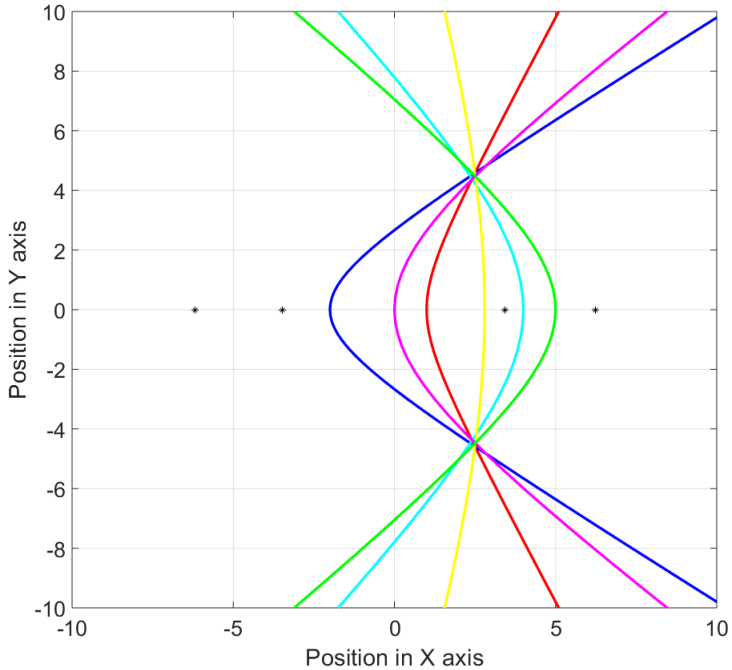

Figure 5.4: Hyperbolas representing constant delays between two sensors. The intersection is the location of the transmitter. The stars represent the locations of the receiving sensors.

$$\frac{x^2}{a} - \frac{y^2}{b} = 1 \tag{5.5}$$

As a practical proof-of-concept experiment, we assumed a linear array receiving the signal of a transmitter with unknown location. Again, due to lack of available antennas, we utilized cables with various lengths to emulate various propagation delays. Fig. 5.4 shows the hyperbolas. The stars represent the location of the receiving sensors. The ambiguity can be resolved by placing the sensors in a different topology.

Solving the non-linear system of equations yields the location of the transmitter, viz. the intersection of the hyperbola curves. Alternatively, image recognition

may be used to extract the location of the transmitter by estimating visually the coordinates of the intersecting curves.

Time-Difference-Of-Arrival methods can be advantageous for direction finding of UWB signals, which as shown above, can clearly provide good resolution with low-complexity, especially in open space environments. However, in multipath-rich propagation, TDOA may yield wrong results. This is because TDOA measurements are based on the assumption that the signal propagates from the transmitter to the sensor along the shortest path, or Line of Sight (LOS). When the primary path is not the direct one, the possible signal, resulting from a multipath environment, will arrive along a longer path, which results in a later time and incorrect transmitter location. This problem is not uncommon in radio-navigation systems. For example, GPS systems lose signal in tunnels and dense urban areas. Indoor Positioning Systems' performance also degrades due to walls, furniture, or people [YKBF03]. Several solutions have been proposed for this problem, including modeling the Non-Line of Sight path and using low-interference signals like Ultra-Wideband waveforms [GPH+15].

Overview of the algorithm:

- A modulated signal is received from an unknown location.
- The signal is captured at three or more sensors at various locations.
- The signal captured by each sensor is shifted in time to find a position of maximum alignment using cross-correlation.
- The relative time difference of each signal is multiplied by the speed of light to get a distance difference between each sensor.
- The distance difference is plotted as a set of hyperbolic curves.
- The intersection of the lines indicates the location of the emitter.

To conclude, we demonstrated a method of localizing the location of unknown transmitter. The increased level of accuracy and resolution is achieved by utilizing UWB signals. The only method able to resolve the direction of arrival of such wideband signals is TDOA. MUSIC/ESPRIT algorithms and their variations may also be used, however the extreme computational cost make them prohibitive for such applications requiring wideband signals. Furthermore, this technique was demonstrated employing Direct RF sampling receivers which are able to tune in any frequency and employ any bandwidth making them a versatile option for direction finding systems.

CHAPTER 6

APPLICATIONS AT MILLIMETER-WAVE (MMWAVE) BANDS

The FCC announced millimeter wave (mmWave) spectrum bands for future 5G applications. The new frequency bands include: 27.5 - 28.35 GHz, 37 - 38.6 GHz and 38.6 - 40 GHz. Next-gen wireless systems such as 5G New Radio (NR) aim to solve the exponential growth by utilizing UWB systems and millimeter wave (mmWave) frequency bands. These bands are capable of accommodating much larger bandwidth than the sub-6 GHz bands making them prime candidates for the proposed UWB-CDMA system. In this chapter, we will demonstrate the efficacy of the proposed system in mmWave bands and the challenges associated.

6.1 5G New Radio (NR)

The newly accepted Radio Access Technology (TAR) termed "5G NR" divides the market in three distinct categories: 1) Enhanced Mobile Broadband (eMBB), 2) Massive Machine-Type Communication (mMTC), and 3) Ultra Reliable Low Latency Communication (URLLC). Applications that fall into these three categories are shown in Fig. 6.1.

1. **Enhanced Mobile Broadband (eMBB)**

   Enhanced Mobile Broadband is an evolution to existing 4G networks which will provide faster data rates and therefore a better user experience than current mobile broadband services. 5G in this case promises to deliver:

   Higher capacity broadband access in densely populated areas, both indoors and outdoors, such as urban environments, office buildings or public venues. Enhanced connectivity broadband access everywhere to provide a consistent

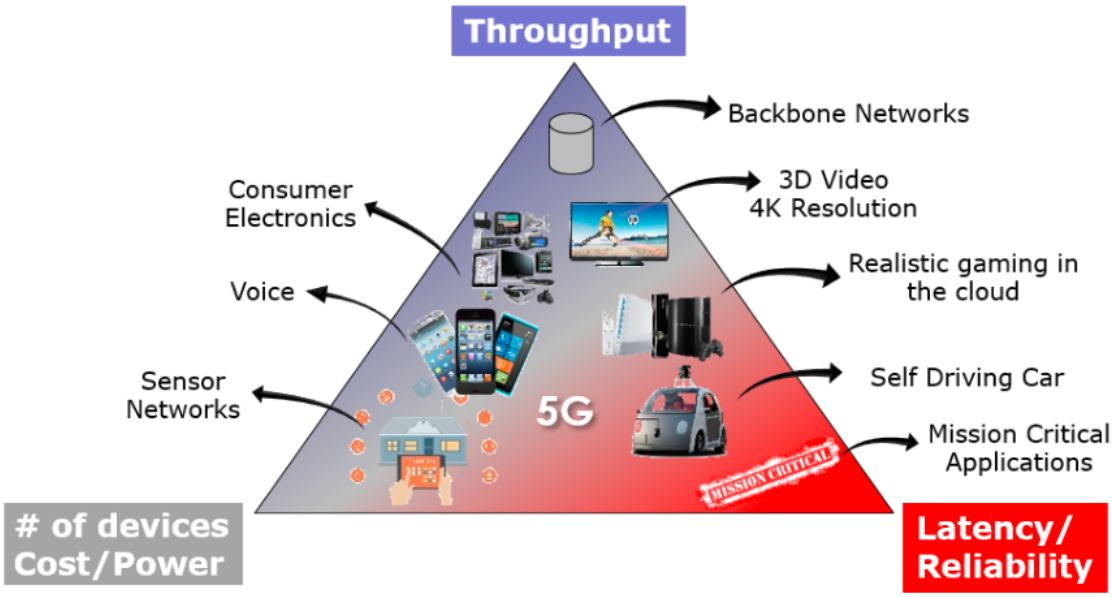

Figure 6.1: Three pillars of 5G representing different use cases.

user experience. Higher user mobility mobile broadband services in moving vehicles including cars, buses, trains.

In order to deliver these requirements, it is expected that 5G NR will support: Traffic capacity of 10-20 Gbps peak data rates with wide channels and massive MIMO. Data transfer rates experienced by the user of up to 1Gbps and total traffic of at least 1 Tbps/sq^2. Additionally, high mobility up to 500km/hour in high-speed trains and up to 1,000km/hour in airplanes is also promised. Latency of 1ms for user experienced data exchange. Connection density of up to one million connections per square kilometre.

2. **Massive Machine-Type Communication (mMTC)**

   Machine to Machine (M2M), as stated in [DSWM14], is a term used to describe technologies enabling computers, smart sensors, and mobile devices to communicate with one another, take measurements and make decisions - often without human intervention. A native inclusion of M2M communication

in 5G involves satisfying three different requirements associated with different classes of low-data-rate services: 1) support of a massive number of low-rate devices, 2) sustaining a minimal data rate in virtually all circumstances, and 3) very-low-latency data transfer. Addressing these requirements in 5G requires new methods and ideas at both the component and architectural levels [BHJL+13].

Typical requirements include the following:

(a) Small packets potentially going down to a few bytes.

(b) Large number of users, for example, up to 300.000 devices in a single cell.

(c) Uplink - dominated transmissions.

(d) Low user data rates (approximately 10kb/s per user).

(e) Sporadic user activity, i.e. mixed traffic models with period and event driven traffic.

(f) Low complexity and battery constrained (low energy) devices.

3. **Ultra Reliable Low Latency Communication (URLLC)**

Another critical aspect of next-gen networks is ultra-low latency of communication, i.e. the time required for transmitting a message from node to node. The typical latency within a 4G network lies around 40ms. However, in some instances this number can dramatically increase to several seconds [LBK+15].

There is a general consensus for future services dictating that many industrial, traffic, medical and internet services will depend on wireless connectivity with guaranteed and consistent latency of 1ms or less [nok]. Examples of such services include Tele-surgery, Intelligent Transportation, Industry Automation and more.

Requirements for this use-case scenario include:

(a) Ultra responsive <1 ms air interface latency.

(b) 5 ms End-to-End (E2E) latency.

(c) Ultra reliable and available (99.9999%).

(d) Low to medium data rates (50 kpbs 10 Mbps). High Speed mobility.

A major challenge at mmWave frequencies is the very high propagation loss, which can significantly limit the communication distance. Specifically, the attenuation at these frequencies is almost an order of magnitude larger as compared to sub-6 GHz bands. Due to oxygen and water vapor at the mmWave and THz frequency bands [JA11], respectively, the absorption peaks create spectral windows, which have different bandwidths and drastically change with the variation of the distance, as shown in Fig. 6.2. In addition, the very high path loss also arises from the spreading loss, which increases quadratically with the frequency, as defined by Friis law [JA11].

Many methods to combat the distance problem in the millimeter wave frequencies exist in literature. Such methods include: 1) Distance-Adaptive Design, 2) Massive Multiple-In-Multiple-Out systems, 3) Reflectarrays, 4) HyperSurfaces

1. Distance-Adaptive Design [HBA15]

   As shown in Fig. 6.2, the entire spectrum has "windows" which can be divided into narrower but still broadband sub-windows and allow parallel multi-wideband transmissions. This attribute can be exploited in 2 ways, distance-adaptive multi-wideband waveform design and distance-aware bandwidth-adaptive resource allocation. This is shown in, [HBA15], where the waveforms can be

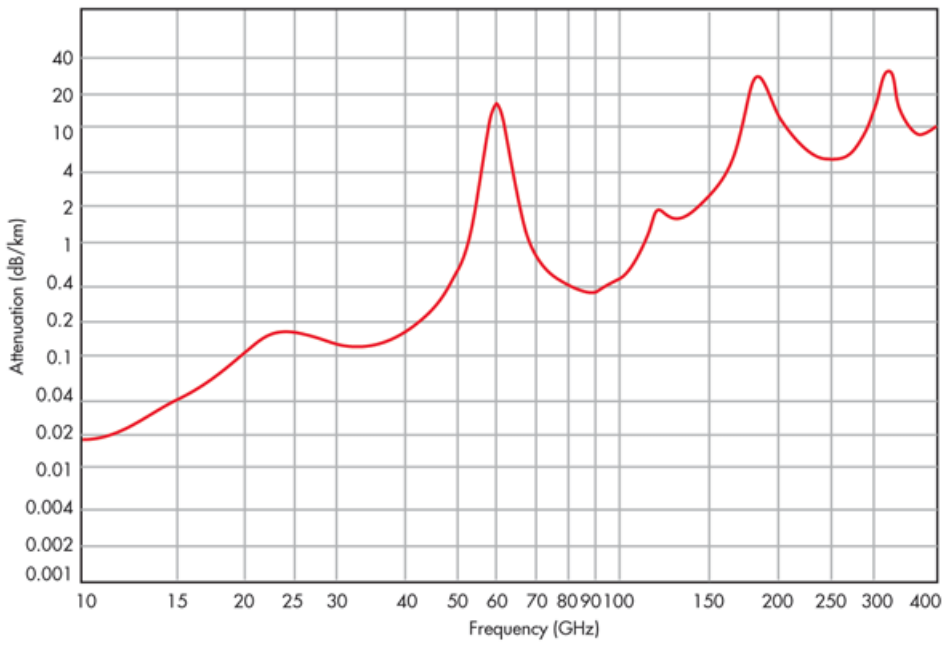

Figure 6.2: Path loss of the Line-of-Sight and multipath channels in the mmWave band [mmW].

dynamically adapted to match the windows. It is shown that the communication distance can be effectively improved as the transmit power and the number of frames increase, sacrificing power consumption and data rate.

2. Massive Multiple-In-Multiple-Out systems

   The concept of massive MIMO has been introduced in recent years [MVL+17], in which antenna arrays with hundreds of elements are employed to increase the bandwidth efficiency and to realize beam-forming. Combined with UWB antenna arrays, this approach can significantly increase the distance at mmWave by focusing the transmitted signals in space and in frequency. By properly feeding the antenna array elements, dynamic array modes can be adaptively created. The large number of antenna arrays can be grouped together and generate steering high directivity narrow beams toward the strongest propagation path as beamforming. This design can effectively overcome very high

attenuation at the mmWave band and, importantly, enhance communication distance.

3. Reflectarrays

   Reflectarrays have been explored in the past in applications such as satellite communications, radars, point-to-point links due to their flexibility and low implementation cost [HPC13]. Like phased arrays, tunable reflectarrays can generate adaptive patterns. Specifically, the phase of each element in the reflectarray can be shifted digitally to form a pattern to receive or transmit to or from specific directions. Importantly, reflectarrays are much simpler than phased arrays and easier to mass produce. They also have higher efficiency since transmission lines are not needed. In addition, in applications with multi-path rich environments at mmWave, reflectarrays can be used to extend the transmission range. For example, in an indoor situation where the line-of-sight (LoS) path from a transmitter to a receiver is blocked, a reflectarray can be employed as a reflector to bounce the signal off to reach the receiver. The reflectarray can dynamically tune the phase of the elements that can sense the transmitted signal to direct the reflected rays toward the users, without requiring any complex ditigal signal processing. Additionally, since multiple reflectarray elements will form sharp beams targeting specific users, the interference among users will be mitigated. However, reflectarrays also exhibit limitations. The efficiency of digital tuning is dependent on the array size and the characteristics of the environment. Also, movement in the environment can distort the signal transmission paths. Additionally, the time efficiency and accuracy of channel estimation is critical in providing adequate link coverage to receivers.

4. HyperSurfaces

   The concept of HyperSurfaces or software-defined meta-surfaces has been proposed [LTP+15] to improve the transmission distance. Application scenarios include indoor rooms or hallways. Metasurfaces can control the incident electromagnetic waves with high resolution. Hypersurfaces can manipulate incident waves in ways that are not possible with reflectarrays, including wave steering, wave absorption, and wave polarization [LTP+15]. A typical scenario would include many tiles inside wall areas. When in use, those tiles can identify the best possible path in terms of angles in azimuth and elevation to maintain high SNR, minimize path loss, mitigate undesired multipaths, thus increasing the transmission distance. However, a network of such tiles would require special structural design and an intricate network with a complex signal processing back-end.

Alternatively, direct-sequence-spread-spectrum and the ensuing processing gain involved can be used to increase the sensitivity of the receiver. By transmitting the same power density over the larger bandwidth available in mmWave band, users can take advantage of the processing gain and increase the overall SNR and the transmission distance. As shown eariler, the 16 dB of processing gain that was achieved using our sub-6 GHz systems, described in the previous chapters, implies a 16 dB improvement in SNR. This method is independent of carrier frequency and therefore can be adapted for use in mmWave frequencies. As a proof of concept, a transmit and receive chain were design and fabricated using components-off-the-shelf (COTS) to show the method at the 28 GHz band. The following sections provide a detailed description of the system.

6.2 mmWave Transmitter Front-end

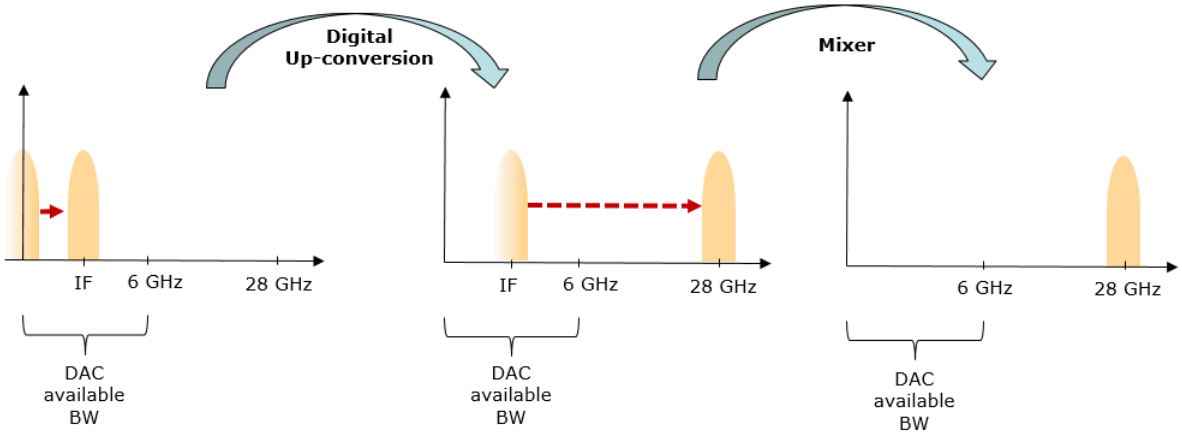

Figure 6.3: mmWave transmit chain block diagram.

Current commercial Direct RF sampling converters do not offer operation at mmWave frequencies. Until such devices are available, it is required to up-convert the desired signal using analog mixers. Combining Direct RF sampling and a single stage of up-conversion for mmWave, still offers the benefit of having to use only one analog mixing stage instead of two. More into detail, the system, described in Chapter 3, is used to digitally up-convert the signal to an IF frequency of 4.5 GHz. Subsequently, the mmWave RF front-end is used to upconvert the signal to the RF frequency of choice, as shown in Fig. 6.3. In Fig. 6.4, we illustrate the block diagram of the mmWave transmitter chain. The system was optimized to accommodate all the 5G frequency bands that FCC has allocated by combining different IF and LO frequencies. Specifically, the frequency range spans from 26.5 GHz to 49 GHz. Depending on the RF frequency of operation, a respective RF filter after the power amplifier is employed (not shown in the diagram).

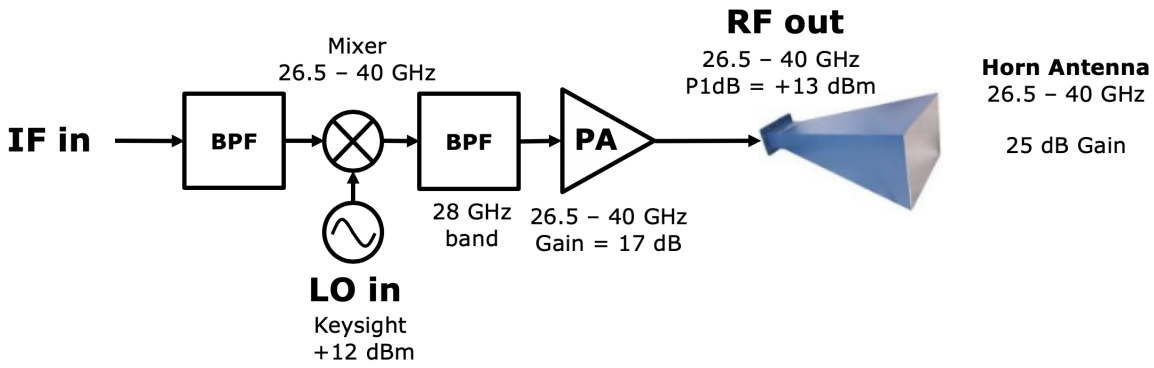

Figure 6.4: mmWave RF front-end block diagram (transmitter).

6.3 mmWave Receiver Front-end

Similarly, the receive chain was implemented using a combination of Direct RF sampling and a stage of analog mixing. The desired signal, received by the horn antenna, is fed into the LNA to boost the SNR at an early stage and decrease the cascaded noise figure (NF). The Image Reject Filter (IR Filter) cancels out image components which could potentially fold into the desired band after the mixing stage. Subsequently, the mixers down-converts the signal from RF to an IF of 4.5 GHz and the IF filter further rejects non-necessary frequency components. Finally, the desired signal is fed to the ADC (described in chapter 3) where Digital Down-conversion is performed.

The (NF) of the RF front-end depends on the combination of LO frequency and desired RF signal. It was measured and found to be on average 2.13 dB. Fig. 6.7 shows plots of the NF in different LO and RF frequencies of operation.

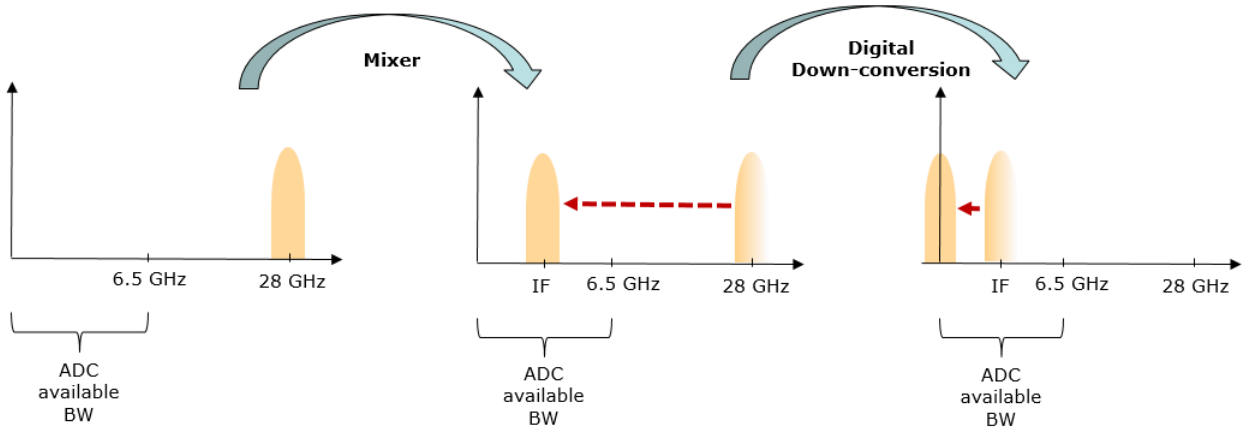

Figure 6.5: mmWave receive chain block diagram.

6.4 Link Budget of a 28 GHz Link

A link budget is a sum of all of the gains and losses throughout a communication system. It accounts for cable mismatches, efficiency, attenuation of the transmitted signal due to propagation, fading margin, body loss, polarization mismatch, amplifier gains, antenna gains, and other possible imperfections from the transmitter to the receiver.

The proposed communication system may be used for cell-to-cell communication. Such system can serve as a back-haul network that transfers large amounts of data through different base station controllers. Here, we demonstrate a typical real-world

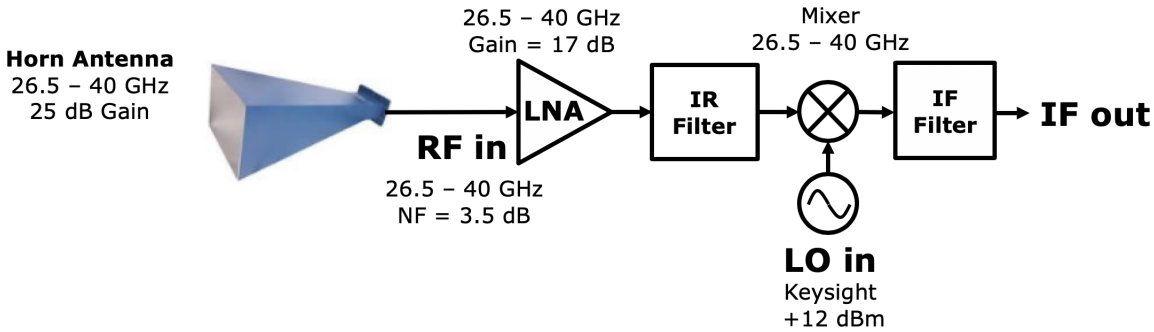

Figure 6.6: mmWave RF front-end block diagram (receiver).

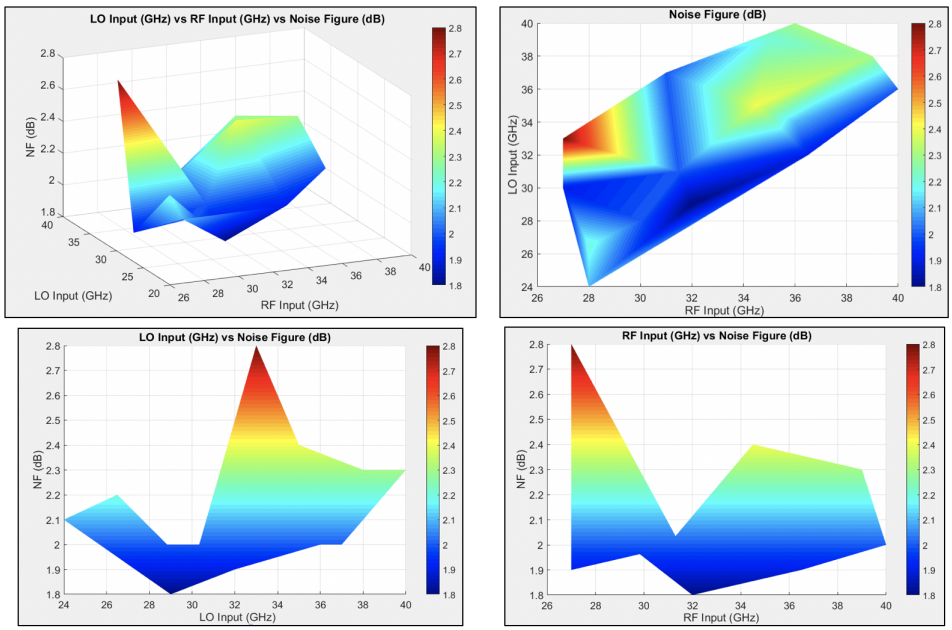

Figure 6.7: mmWave receive chain block diagram.

example of such application. The link-budget for a 28 GHz mmWave, 1 kilometer, point-to-point link is shown in Fig. 6.8.

The total transmitted Equivalent Isotropically Radiated Power (EIRP), which is the product of transmitter power and the antenna gain in a given direction is $T_x + G_{Tx_{Antenna}} = 35dBm$. The transmitted bandwidth of 1.3 GHz yields a processing gain of 21 dB. The measured NF of the receiver RF Front-end has a typical value of 2.1 dB. The number was rounded to 2.5 dB to account for cable mismatches at the IF stage. The amount of thermal noise at the input of this system is $-174 + 10 * log(1.3 \times 10^9) = -82\ dBm$. If Noise Figure (NF) of 2.5 dB is added, the resulting number, which refers to the minimum detectable signal, is -79.5 dB. To estimate the required SNR for BPSK modulation using 1/2 Forward-Error-Correction codes a simulation was conducted. Specifically, an AWGN channel was emulated have an uncoded BPSK signal transmitting a random signal. The green curve shows the Bit-Error-Rate vs Signal-to-Noise Ratio. Next, the same channel was emulated, but

Parameter	Assumptions	Value
Tx EIRP		+35 dBm
Bandwidth	CDMA signal	1.3 GHz
Thermal Noise		-82 dBm
NF	2.1 dB typ/2.8 dB max	2.5 dB
Min Detectable Signal		-79.5 dB
Required SNR	BPSK ½ FEC	6 dB
Antenna Gain	Horn Antenna	25 dB nominal
Min signal required		-98.5 dBm
Estimated Path Loss	1km ISD	133 to 160 dB
Margin		-26.5 to -0.5 dB
Processing Gain	L_c= 127	21 dB
Final Margin		**-5.5 to 20.5**

Figure 6.8: Link budget of a 28 GHz mmWave point-to-point link.

this time using a channel-coded BPSK using Turbo codes. The red curve shows the respective response. It is shown that channel coding gain resulted by employing Turbo codes is approximately 6 dB (for a Bit-Error-Rate of around 5×10^{-9} as shown in Fig. 6.9). Adding the coding gain to the minimum detectable signal yields the minimum required power for successful recovery of the BPSK waveform, which is -73.5 dBm. Furthermore, the antenna has a nominal gain of 25 dB. This brings the minimum required signal power at the RF front-end to -98.5 dBm. Taking into account the path loss and the processing gain of the system, we estimate a final margin of -5.5 to 20.5 dB. This range can be shifted by changing the configuration of the system such as the forward error correcting codes and the length of the spreading sequences. For example, if we utilize 10 GHz of bandwidth and drop the bit rate to 0.5 Mbps, we can provide a processing gain of 43 dB. This technique is useful for long-range communication applications that do not require high data rates such as the Global Positioning System and the Deep Space Network (DSN) [Moy05].

Millimeter wave frequencies can provide the necessary bandwidth to accommodate spread spectrum systems. As shown earlier, spread spectrum systems have significant advantages, such as increased receiver sensitivity and multi-user communication. This link-budget scenario also demonstrates the ability of the system to operate at distances of 1 km without having to use any range extenders or repeaters. This could save operators and telecommunication companies the need of such devices and decrease the operational costs of the network. That being said, this method could create a fusion between Massive Machine-Type Communication (mMTC) and Ultra Reliable Low Latency Communication (URLLC) where large amount of User Equipment (UE) is present in the same cell and require lower user data rates. Additionally, we demonstrated the efficacy of single heterodyne architecture instead of super heterodyne. To do so, we employed Digital Up/Down conversion employing Direct RF sampling. This can result in lower implementation costs, decreased power due to fewer components which can result in size reduction.

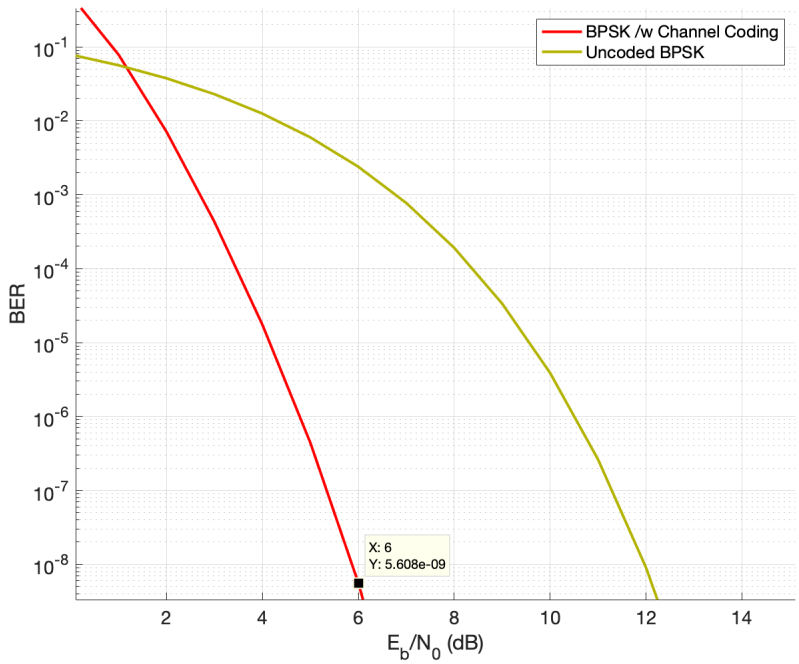

Figure 6.9: BER of uncoded BPSK and Turbo coded BPSK signals. There is a 6 dB coding gain as a result of channel coding.

CHAPTER 7

CONCLUSIONS AND FUTURE WORK

7.1 Conclusion

Recent developments in the are of wireless communications point towards an all-connected future. Every electronic devices will have the ability to communicate through massive networks. The explosion of the interconnected devices, therefore, requires new architectures to sustain this massive growth. Simpler architectures and access to mmWave frequencies could be the solution to this problem.

Along these lines, Chapter 1 provided an introduction into Ultra-wideband systems, Beamforming and Multiple-In-Multiple-Out wireless communication techniques. Merits and de-merits of each technique is stated and compared against each other.

In Chapter 2, the concept of secure communications in the physical layer was explained. The chapter describes different techniques and methods to secure wireless systems along with their advantages and disadvantages. Spread spectrum techniques are described in detail. Challenges and considerations are explained along with processing gain evaluations. Simulations of different codes and lengths are also presented.

Chapter 3 presented the complete communication system that was developed. Specifically, the workflow, design and implementation of the entire wireless system is described in detail. Furthermore, each stage and reasoning behind each design decision was explained. In this chapter, measurements were also presented in presence of different interference scenarios. These scenarios included static and dynamic blockers in various power levels.

Next, Chapter 4 described the concept of Direct RF sampling transceivers and their application for UWB communications. An introduction to previous generation

systems and their limitations was shown among with possible solutions to those using Direct RF sampling methods.

In chapter 5, we explored the are of direction finding. Specifically, we described the limitations of previous techniques, such as MUSIC and ESPRIT, regarding bandwidth and frequency of operation. A prototype was designed which successfully measures the time difference of arrival of UWB signals and can resolve the direction of the transmitter regardless of bandwidth.

Chapter 6 described applications to millimeter-wave frequency bands. For these applications, a mmWave transmitter and receiver front-end was designed and implemented using components-of-the-shelf. Also, Details about the future 5G NR radio access network were described along with a design of a 28 GHz point-to-point link for base stations.

7.2 Future Work

The work presented in this dissertation paves the way for continued research along these lines; opportunities such as in the area of communications, as well as in the development of spectrum management and user allocation platforms.

As already mentioned, the sheer amount of data that have to be processed and transmitted between connected devices increase the computation complexity and require processing power that currently does not exist or requires an immense amount of DSP resources to run efficiently, especially in mobile devices that are battery powered. That being said, another approach should be considered to manage the network data. Machine learning and artificial intelligence could be a solution to the aforementioned problem. Specifically, by training a network with predetermined

signals/waveforms, the back-haul system could classify different users and networks without having to process and subsequently determine the raw data of the frame.

The work in [Côt18] presents results from an application using unsupervised machine learning in a real network. The system can detect anomalies at multiple network layers, including the optical layer, how it can be trained to anticipate anomalies before they become a problem. In [KLC19], a machine learning-based beamforming design was presented for two-user MISO interference channels. The numerical results show that the machine learning-based beamforming design well finds the best beamforming combination and achieves the sum-rate more than 99.9% of the best beamforming combination.

Finally, machine learning may be used to efficiently sense the spectrum and create networks based on the needs of the current environment. Specifically, waveforms and modulations can be created on the fly to minimize the interference between users and also increase the system throughput without increasing the complexity. Dynamic resource allocation and adaptive power control is another step to create even more efficient wireless networks by allocating only the required amount of processing power per user, thus saving resources and power.

7.2.1 Machine Learning for Classification and Interference Suppression

In the search for alternative techniques to suppress noise and interference from unintentional or deliberate sources, we considered the use of machine learning and artificial intelligence to recover the desired signal.

Machine learning (ML) is an application of Artificial Intelligence (AI) aiming to perform a certain process employing pattern recognition and inference techniques.

To do so, ML algorithms generate a "mathematical" model based on given sample data, called "training data", to predict or decide without being explicitly programmed externally to execute a task. ML techniques can be found in many areas, such as spam filtering, and computer/robotic vision.

There are typically four stages in every ML application, as shown in Fig. 7.1. The Input stage refers to data collection process and is by far the essential first step. Specifically, it is the procedure in which the data are fed into the system in order to "teach" it accordingly. It is important for this step to have as much data as possible as the ML system will only be as good as the quality of data collected.

The next step is Feature Extraction. It is an attribute reduction process which transforms the attributes and features into linear combinations of the original attributes. The feature extraction process results in a much smaller and richer set of attributes. [JMN+18].

Classification is a system that inputs a vector of discrete and/or continuous feature values and outputs a single discrete value, the class. For example, a spam filter classifies email messages into spam or not spam, and its input may be a Boolean vector. The test of the learner is whether this classifier produces the correct output for future examples (e.g., whether the spam filter correctly classifies previously unseen emails as spam or not spam). [Dom12].

Finally, the output stage presents results in a meaningful way using various plots,

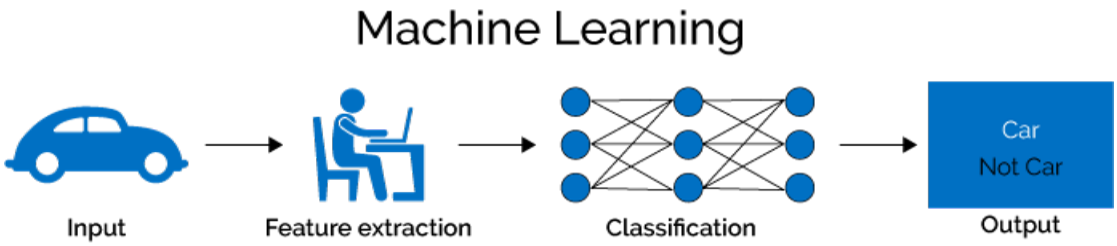

Figure 7.1: Machine Learning (ML) implemented in four steps.

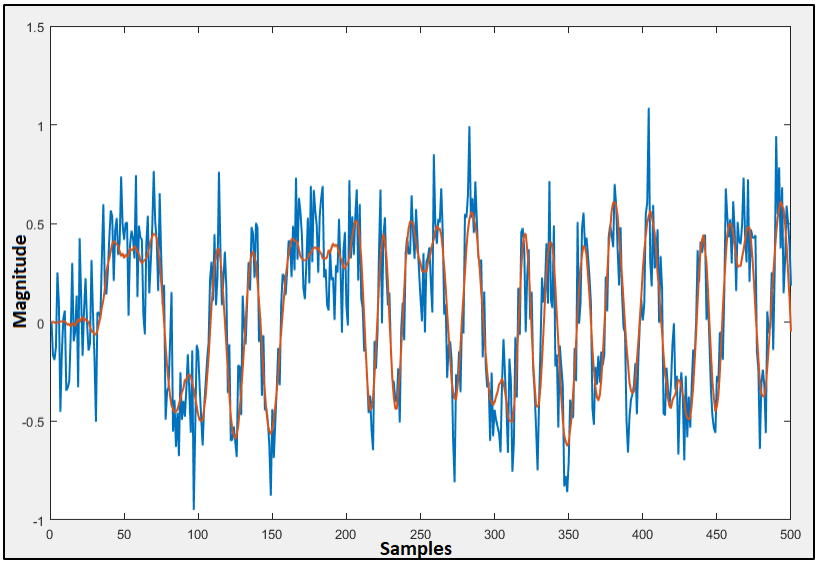

Figure 7.2: Data used to train the ML network. Red plot represents the transmitted signal and the blue plot represents the same signal with 3 dB SNR.

graphs and curves. It can be used to provide results that are either predictive such as forecasting or prescriptive such as a course of action recommendation. This output information may be saved for analysis or fed as input into other systems Also, this stage yields the confidence level of the prediction.

To assess the performance of the ML algorithms in recovering signals buried in noise, tests were conducted. As a first step, the network has to be "taught" using training data as mentioned earlier. To do so, we created many different signals and the equivalent noisy ones. Fig. 7.2 shows an example signal generated with MATLAB and was used to train the network. The red signal represents the transmitted signal with no added noise and the blue signal represents the same signal at 3 dB SNR. At first a relatively small amount of data was fed to train the system. After the network was trained, we tried to perform signal recovery from a noisy sample. Fig. 7.3 shows the input noisy signal (top) and the recovered signal overlaid with the original transmitted signal (bottom). For the most part the signal recovered from the noisy input matches the transmitted signal. However, there are some parts,

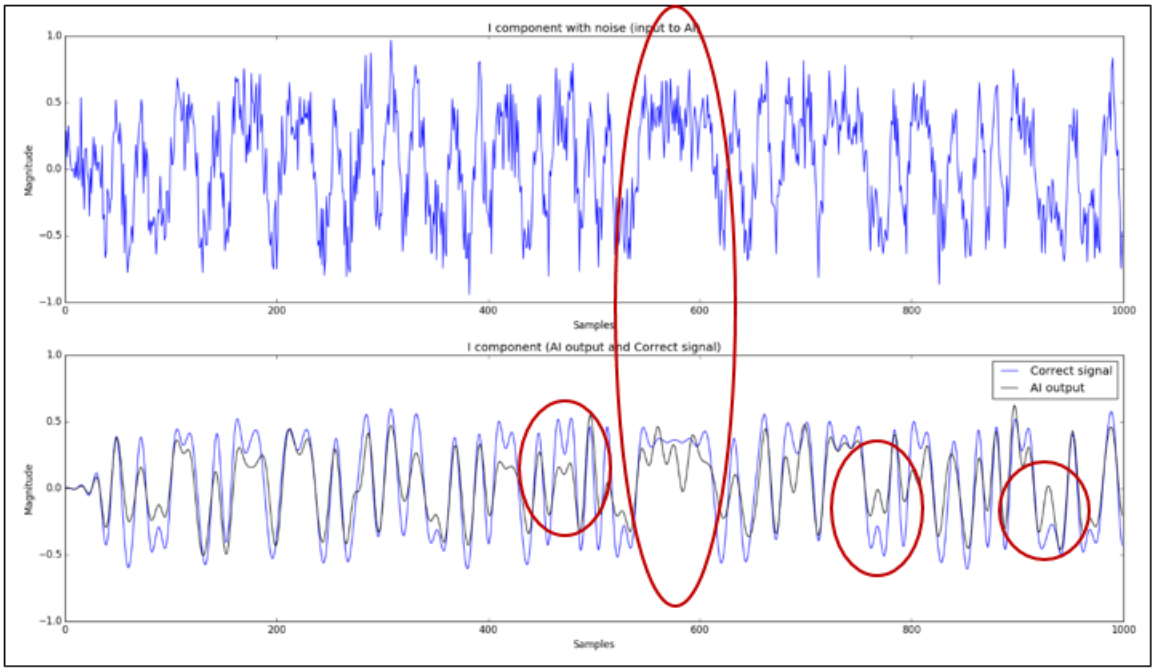

Figure 7.3: Input noisy signal (top) and the recovered signal overlaid with the original transmitted signal (bottom). Red circles highlight problematic areas.

highlighted with red circles, having poor performance. This is due to the relatively small amount of data used to train the ML network. To solve this issue we increased the amount of data to a total of 200 billion samples (close to 400 gigabytes of raw data). Fig. 7.4 shows the input and output of the system that was trained with a larger amount of data. Clearly, no errors are found and the recovered signal almost perfectly matches the correct transmitted signal.

Another interesting area where machine learning and artificial intelligence can be beneficial is again in the physical layer. Using this approach, we can perform modulation classification which can have superior accuracy over other methods [OH17]. In this paper, the authors used convolutional neural networks (CNNs) to classify modulation schemes of a received signal. To train the network, several sample data sets were used including different modulation schemes, such as AM, FM, PSK, QAM, etc. The signals suffered various channel impairments and were taken at different

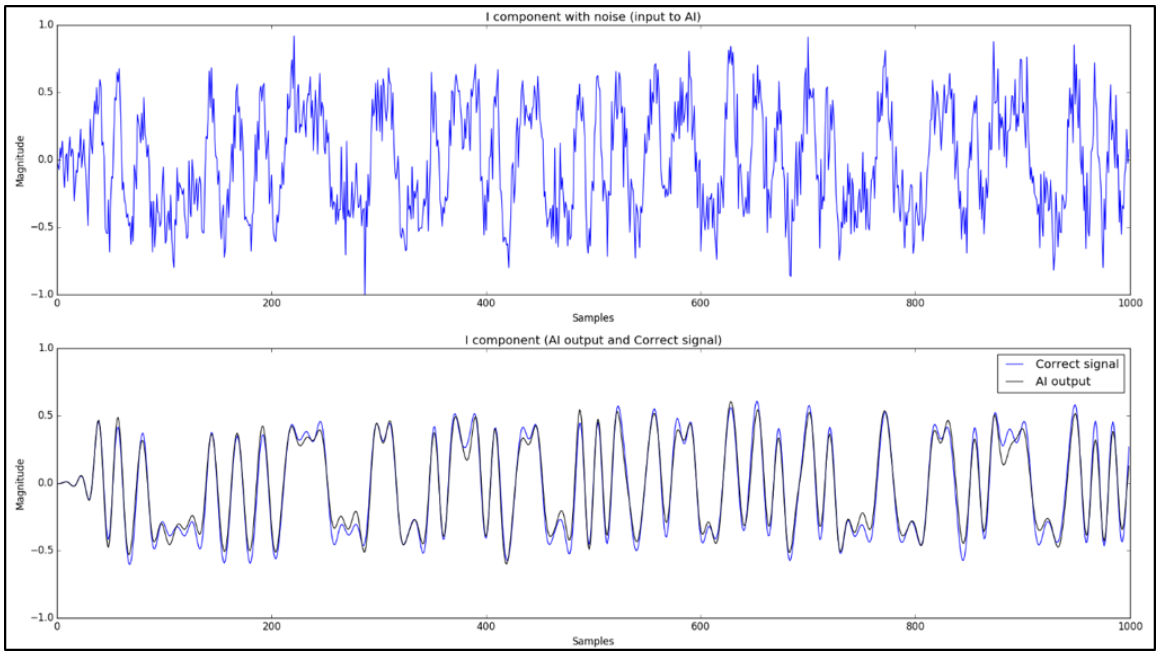

Figure 7.4: Input and output of the system that was trained with a larger amount of data.The signal is perfectly recovered.

SNRs ranging from -20 to 18 dB. Fig. 7.5 shows the confusion matrix of the trained CNN at an SNR of 10 dB. As shown, there are confusing cases between QAM16 and QAM 64. This is mainly due the small observation window.

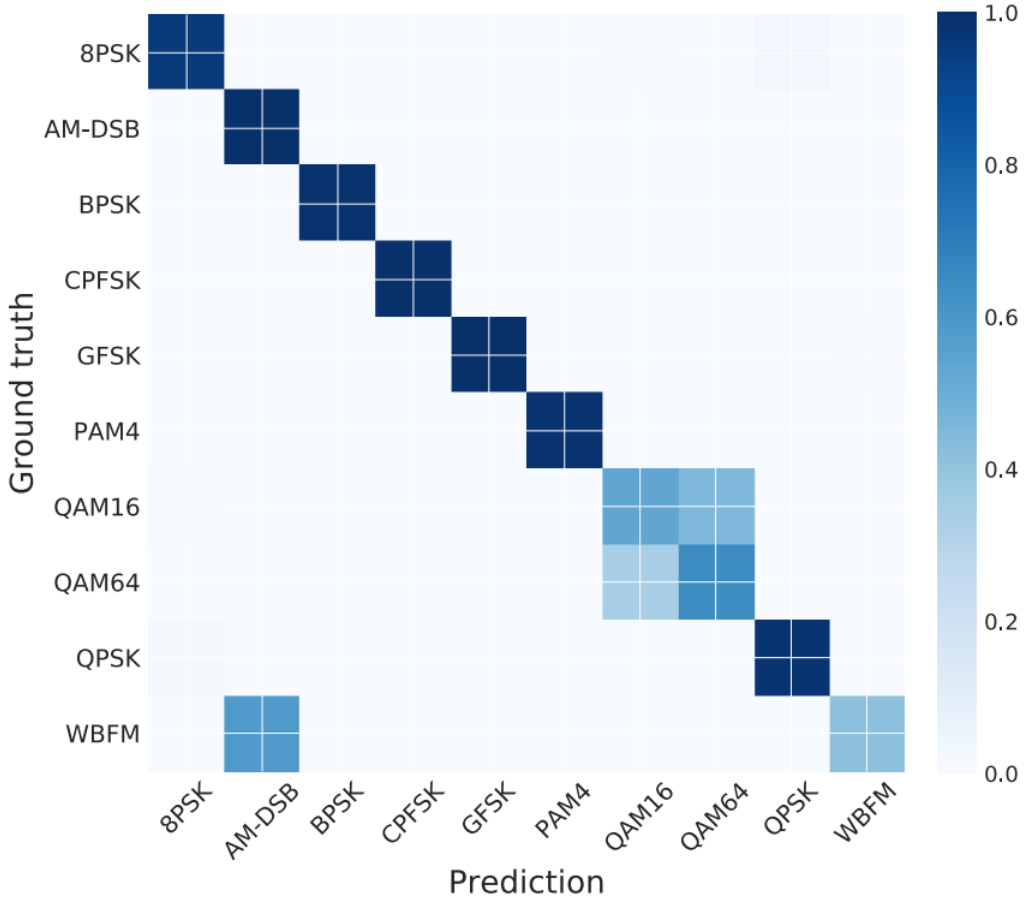

Figure 7.5: Confusion matrix of the CNN (SNR = 10 dB) [OH17].

7.2.2 6G and beyond

As 5G networks are starting to roll out, there has been a start of a movement about the future of wireless communications. Research regarding 6G and even 7G networks started to emerge and current topics of discussion refer to higher frequency of operation, larger bandwidth, and multiple antenna systems [Hea19]. Assuming that consumers' demand will increase, the logical step forward is to employ Super-wideband (SWB) systems at even higher frequencies. Early reports suggest terabit-per-second speeds, true microsecond delay and virtually unlimited bandwidth [Hea19]. Currently, there is no direction towards the frequency range of operation for future generation systems. Fig. **??** shows several bands between 100 and 300 GHz that look promising.

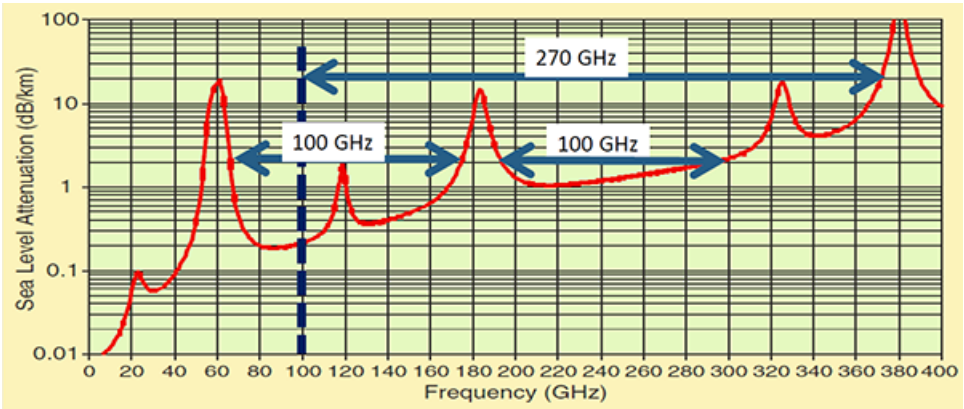

Figure 7.6: "FasterThanFiber: The Future of Multi-Gb/s Wireless" [Wel09].

A potential band of operation for 6G generation systems employing SWB signals could be the D-band and specifically the 120 to 170 GHz. As shown in Fig. **??**, this band has relatively low attenuation and is wide enough to support multi-gigahertz frequency of transmission. To test the operation at such frequencies and demonstrate a practical system, we assembled a test-bench for pre-6G applications. Specifically, a real-time Over-The-Air (OTA) communication link is presented operating at a

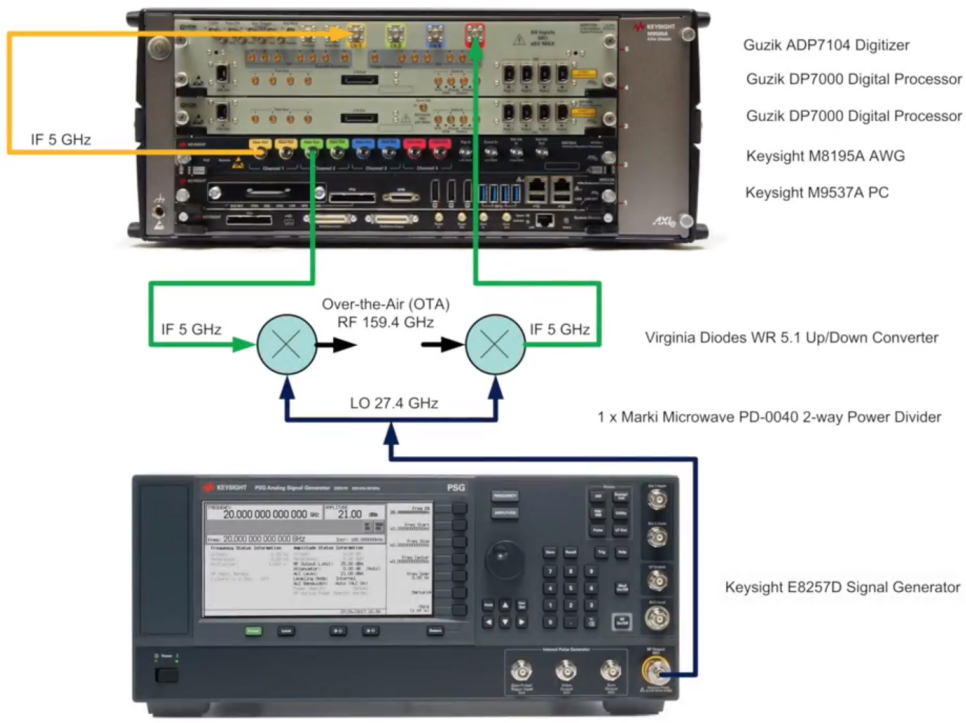

Figure 7.7: Experimental setup of the pre-6G system.

center frequency of 159.4 GHz (D-band) and employing a large bandwidth of 5 GHz using 64-QAM modulation. Fig. 7.7 and Fig. 7.8 show the block diagram and system implemented. More into details, the UWB signal was generated using Keysight's M8195A AWG. The signal was digitally up/down-converted to an IF frequency of 5 GHz. Then using Keysight's E8257D signal generator and mixers from VDI, the UWB signal was up/down-converted to RF = 159.4 GHz. The signal was transmitted using standard waveguide horn antennas. The resulting Error-Vector-Magnitude (EVM) was less than 2.6% RMS. The maximum, end-to-end peak data throughput recorded was approximately 30 gigabits/second which at the writing of this thesis is a record transmission in D-band.

The experiment was conducted again, this time employing the maximum available continuous bandwidth offered by the Arbitrary-Waveform-Generator (AWG)

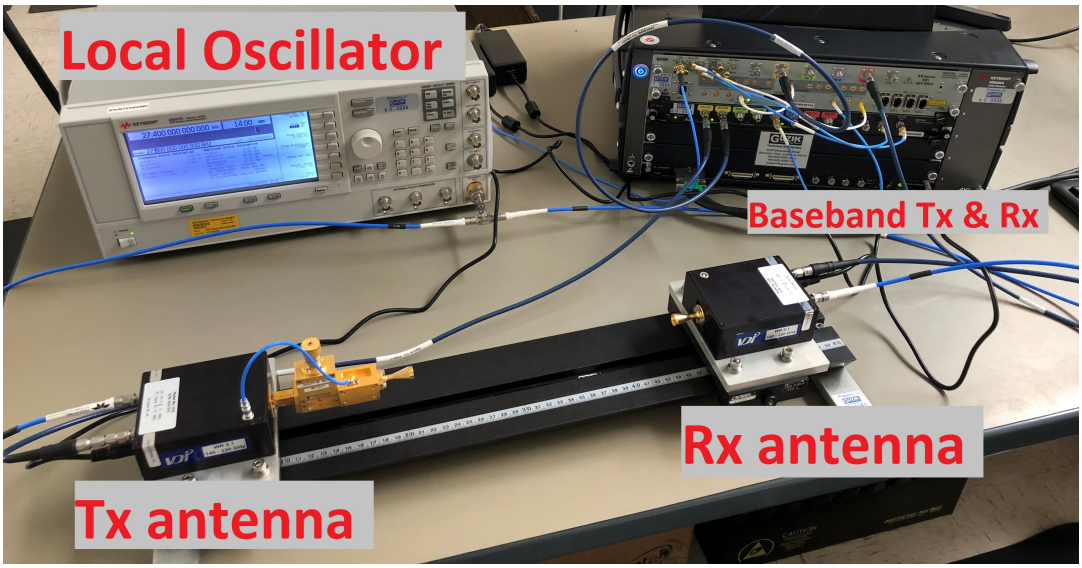

Figure 7.8: Photo of the actual pre-6G test-bench used to achieve high-data rates at D-band.

which was 10 GHz. It was found that the Tx and Rx filters were severely distorting the edges of the spectrum, therefore we opted for 8 GHz instead. Performing the test with the same 64-QAM modulation resulted in a peak throughput of 48 gigabits/second. However, the connection exhibited frequent disruption. This was due to the instability of the carrier synchronization loop which could be the object of further research in the area of UWB systems. Data rates are expected to be increased on the order of 100s of gigabits with the help of more linear systems and better baseband algorithms. It should be noted that future generation wireless networks will most probably affect the backbone connectivity of the entire platform and not the base-station - to - user equipment (UE). This is due to the fact that mobile devices are unable to physically generate the enormous amount of data that the wireless link can support.

Future communication systems will also require some sort of direction-finding capability to realize beamforming in order to surpass propagation losses. That being said, we tested the ability to perform Time-Difference-of-Arrival for future SWB

applications. The same hardware configuration was employed as in the previous experiment but this time using a 10 GHz FM chirped signal as the transmitted waveform. The cross-correlation occurred in real-time and as it can be seen in Fig. 7.9 and Fig. 7.10 the time difference measured is in the order of 10 femtoseconds which translates in a measurement accuracy of 1 μm. This extreme resolution can be beneficial to applications requiring increased accuracy of direction finding and accurate distance measurement. The increased resolution could be beneficial towards phased array systems that are required to precisely locate the direction of arrival of a transmitter.

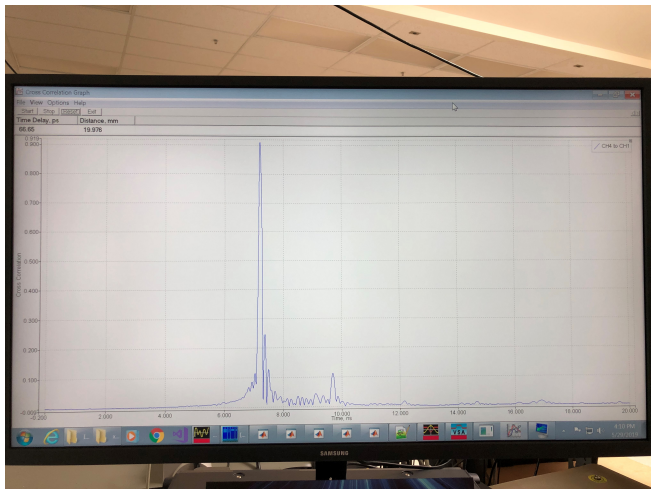

Figure 7.9: Cross-correlation of a 10 GHz. (screen capturing was disabled on the computer).

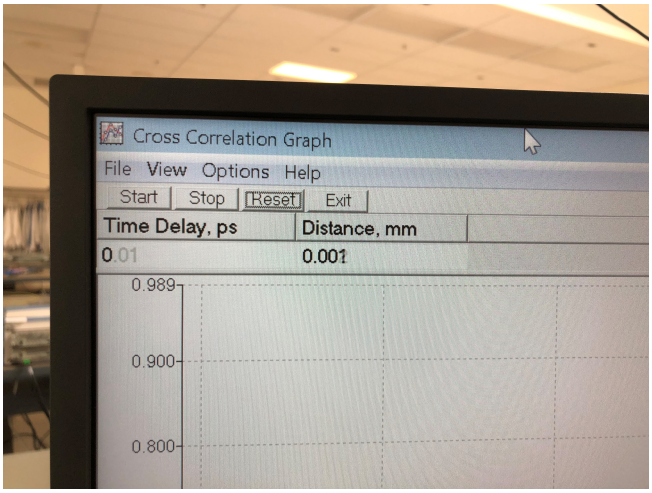

Figure 7.10: Measurement resolution of 10 femtoseconds translating to a distance of 1 μm. (screen capturing was disabled on the computer).

BIBLIOGRAPHY

[3GP] The mobile broadband standard 3gpp, https://www.3gpp.org/specifications, available: Online.

[ADF+09] David Astély, Erik Dahlman, Anders Furuskär, Ylva Jading, Magnus Lindström, and Stefan Parkvall. Lte: the evolution of mobile broadband. *IEEE Communications magazine*, 47(4):44–51, 2009.

[ADP] Adp7000 series 10-bit digitizer, https://www.guzik.com/product/adp7000-series-10-bit-digitizers/ [accessed on 02/19/2019].

[AKK16] S. Ahmed, M. Khurram, and M. A. Khan. Matlab based implementation of IEEE 802.11b DSSS transmitter. In *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pages 624–630. IEEE, 2016.

[anr] Time difference of arrival (tdoa), https://www.rcrwireless.com/wp-content/uploads/2017/06/78a06980-cb97-4351-9baa-036b686b0aa5-anritsu-whitepaper-time-difference-of-arrival-tdoa.pdf, available: Online.

[BCH08] Jacob Benesty, Jingdong Chen, and Yiteng Huang. *Microphone array signal processing*, volume 1. Springer Science & Business Media, 2008.

[BCP08] D. Borio, L. Camoriano, and L. L. Presti. Two-pole and multi-pole notch filters: a computationally effective solution for GNSS interference detection and mitigation. *IEEE Systems J.*, 2(1):38–47, 2008.

[BHG+14] Jason Bonior, Zhen Hu, Terry N Guo, Robert C Qiu, James P Browning, and Michael C Wicks. Software-defined-radio-based wireless tomography: Experimental demonstration and verification. *IEEE Geoscience and Remote Sensing Letters*, 12(1):175–179, 2014.

[BHJL+13] Federico Boccardi, Robert W Heath Jr, Angel Lozano, Thomas L Marzetta, and Petar Popovski. Five disruptive technology directions for 5g. *arXiv preprint arXiv:1312.0229*, 2013.

[BMSS02] M Bona, L Manholm, JP Starski, and B Svensson. Low-loss compact butler matrix for a microstrip antenna. *IEEE Transactions on Microwave Theory and Techniques*, 50(9):2069–2075, 2002.

[BSB+11] Gianmarco Baldini, Taj Sturman, Abdur Rahim Biswas, Ruediger Leschhorn, Gyozo Godor, and Michael Street. Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead. *IEEE Communications Surveys & Tutorials*, 14(2):355–379, 2011.

[But66] Jesse L Butler. Digital matrix and intermediate frequency scanning. *Microwave scanning antennas*, 3:241, 1966.

[Cap69] Jack Capon. High-resolution frequency-wavenumber spectrum analysis. *Proceedings of the IEEE*, 57(8):1408–1418, 1969.

[Cap79] J Capon. Maximum-likelihood spectral estimation. In *Nonlinear methods of spectral analysis*, pages 155–179. Springer, 1979.

[CCGR16] D Diego Andres Cuji, Paul Andres Chasi, Fernando Guerrero, and Fredy Rivera. Frame synchronization through barker codes using sdrs in a real wireless link. In *2016 International Conference on Electronics, Communications and Computers (CONIELECOMP)*, pages 68–72. IEEE, 2016.

[CF07] D. J. Costello and G. D. Forney. Channel coding: The road to channel capacity. *Proceedings of the IEEE*, 95(6):1150–1177, 2007.

[CH08] J. T. Chiang and Y. C. Hu. Dynamic jamming mitigation for wireless broadcast networks. In *INFOCOM 2008. The 27th Conference on Computer Communications*. IEEE, 2008.

[CHHL00] P. T. Capozza, B. J. Holland, T. M. Hopkinson, and R. L. Landrau. A single-chip narrow-band frequency-domain excisor for a global positioning system (GPS) receiver. *IEEE J. Solid-State Circuits*, 35(3):401–411, 2000.

[Chi13] Y. Chien. Hybrid successive continuous wave interference cancellation scheme for global positioning system receivers. *The Journal of Engineering*, 1(1), 2013.

[Chi15] Y. Chien. Design of GPS anti-jamming systems using adaptive notch filters. *IEEE Systems Journal*, 9(2):451–460, 2015.

[CHYT10] Y. Chien, Y. Huang, D. Yang, and H. Tsao. A novel continuous wave interference detectable adaptive notch filter for GPS receivers. In

Global Telecommunications Conference (GLOBECOM 2010),, pages 1–6. IEEE, 2010.

[CNMG14] William J Chappell, Eric J Naglich, Christopher Maxey, and Andrew C Guyette. Putting the radio in software-defined radio: Hardware developments for adaptable rf systems. *Proceedings of the IEEE*, 102(3):307–320, 2014.

[Coh95] L. Cohen. *Time-frequency analysis*, volume 778. Prentice hall, 1995.

[Côt18] David Côté. Using machine learning in communication networks. *Journal of Optical Communications and Networking*, 10(10):D100–D109, 2018.

[del] 2018 Telecommunications Industry Outlook. Retrieved from A new era of connectivity is on the horizon, [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/ Documents /technology-media-telecommunications/us-tmt-2018-telecom-industry-outlook.pdf [Accessed: 25-Jun-2018].

[Dix94] Robert C Dixon. *Spread spectrum systems with commercial applications*. Wiley, 1994.

[Dom12] Pedro M Domingos. A few useful things to know about machine learning. *Commun. acm*, 55(10):78–87, 2012.

[DSWM14] Osman Sezgen David S. Watson, Mary Ann Piette and Naoya Motegi. Machine to machine (m2m) technology in demand responsive commercial buildings. *Lawrence Berkeley National Laboratory*, 2014.

[EG47] CW Earp and RM Godfrey. Radio direction-finding by the cyclical differential measurement of phase. *Journal of the Institution of Electrical Engineers-Part IIIA: Radiocommunication*, 94(15):705–721, 1947.

[ett] Ettus reserach products [online]. available:https://www.ettus.com/product [accessed on 02/19/2019.

[GKD07] A. Gabay, M. Kieffer, and P. Duhamel. Joint source-channel coding using real BCH codes for robust image transmission. *IEEE Trans. Image Process.*, 16(6):1568–1583, 2007.

[GLG+10] I. J. Gupta, T. Lee, K. A. Griffith, C. D. Slick, C. J. Reddy, M. C. Bailey, and D. DeCarlo. Non-planar adaptive antenna arrays for GPS receivers. *IEEE Antennas Propag. Mag.*, 52(5):35–51, 2010.

[Gol67] Robert Gold. Optimal binary sequences for spread spectrum multiplexing (corresp.). *IEEE Transactions on Information Theory*, 13(4):619–621, 1967.

[Goz07] Javier Gozalvez. Ultra mobile broadband [mobile radio]. *IEEE Vehicular Technology Magazine*, 2(1):51–55, 2007.

[GPH+15] Enrique García, Pablo Poudereux, Álvaro Hernández, Jesús Ureña, and David Gualda. A robust uwb indoor positioning system for highly complex environments. In *2015 IEEE International Conference on Industrial Technology (ICIT)*, pages 3386–3391. IEEE, 2015.

[GRM+10] Amitava Ghosh, Rapeepat Ratasuk, Bishwarup Mondal, Nitin Mangalvedhe, and Tim Thomas. Lte-advanced: next-generation wireless broadband technology. *IEEE wireless communications*, 17(3):10–22, 2010.

[guz] Guzik Technical Enterprises. ADC6000 Series 8-bit Digitizers - Guzik Technical Enterprises,http://www.guzik.com/product/adc6000-series-8-bit-digitizers/ [Accessed: 25-Jun-2018].

[HBA15] Chong Han, A Ozan Bicen, and Ian F Akyildiz. Multi-wideband waveform design for distance-adaptive wireless communications in the terahertz band. *IEEE Transactions on Signal Processing*, 64(4):910–922, 2015.

[HBW15] M. M. Hafidhi, E. Boutillon, and C. Winstead. Reliable gold code generators for GPS receivers. In *2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 1–4. IEEE, 2015.

[Hea19] Robert W Heath. Going toward 6g [from the editor]. *IEEE Signal Processing Magazine*, 36(3):3–4, 2019.

[HM16] Mashud Hyder and Kaushik Mahata. Zadoff–chu sequence design for random access initial uplink synchronization in lte-like systems. *IEEE Transactions on Wireless Communications*, 16(1):503–511, 2016.

[HPC13] Sean Victor Hum and Julien Perruisseau-Carrier. Reconfigurable reflectarrays and array lenses for dynamic antenna beam control: A review. *IEEE Transactions on Antennas and Propagation*, 62(1):183–198, 2013.

[HV90] PS Hall and SJ Vetterlein. Review of radio frequency beamforming techniques for scanned and multiple beam antennas. In *IEE Proceedings H (Microwaves, Antennas and Propagation)*, volume 137, pages 293–303. IET, 1990.

[HYKY03] L. Hanzo, L. Yang, E. L. Kuan, and K. Yen. *Single-and multi-carrier DS-CDMA: multi-user detection, space-time spreading, synchronisation, standards and networking*. John Wiley & Sons, 2003.

[IEE] 3GPP Release 15 Overview,https://spectrum.ieee.org/telecom/wireless/3gpp-release-15-overview [Accessed: 25-Jun-2018].

[IM85] R. Iltis and L. Milstein. An approximate statistical analysis of the Widrow LMS algorithm with application to narrow-band interference rejection. *IEEE Trans. Commun.*, 33(2):121–130, 1985.

[IQa] Iqanalog, nxt-f1000., online: https://www.iqanalog.com/nextsemi/products/nxt-f1000// [accessed on 02/19/2019].

[JA11] Josep Miquel Jornet and Ian F Akyildiz. Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band. *IEEE Transactions on Wireless Communications*, 10(10):3211–3221, 2011.

[JMN+18] Deepali J Joshi, Mohit Makhija, Yash Nabar, Ninad Nehete, and Manasi S Patwardhan. Mental health analysis using deep learning for feature extraction. In *Proceedings of the ACM India Joint International Conference on Data Science and Management of Data*, pages 356–359. ACM, 2018.

[jon] Adc performance evolution. adms design ab.

[Jon11] M. Jones. The civilian battlefield: Protecting GNSS receivers from interference and jamming. *Inside GNSS*, 6(2):40–49, 2011.

[Kes03] Walt Kester. *Mixed-signal and DSP Design Techniques*, chapter 2. Burlington MA:Newnes, 1 edition, 2003.

[keya] Keysight technologies 5G Goals, On-line Webinar, online, available: https://www.keysight.com/us/en/events/engineering-webinar-series.html.

[keyb] M8190a 12 *gsa/s* arbitrary waveform generator, https://www.keysight.com/en/pd-1969138-pn-m8190a/12-gsa-s-arbitrary-waveform-generator?cc=uslc=eng.

[KG42] Markey Hedy Kiesler and Antheil George. Secret communication system, August 11 1942. US Patent 2,292,387.

[KGK11] G. Karawas, K. Goverdhanam, and J. Koh. Wideband active interference cancellation techniques for military applications. pages 390–392, 2011.

[KLC19] Hyung Jun Kwon, Jung Hoon Lee, and Wan Choi. Machine learning-based beamforming in two-user miso interference channels. In *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, pages 496–499. IEEE, 2019.

[KMCV07] Robert L Kellogg, Eldon E Mack, Cathy D Crews, and J Volakis. Direction finding antennas and systems. *Antenna engineering handbook(McGraw-Hill Press, 1961, 4th*, pages 1403–1435, 2007.

[LB05] Robert G Lorenz and Stephen P Boyd. Robust minimum variance beamforming. *IEEE transactions on signal processing*, 53(5):1684–1696, 2005.

[LBK+15] Natalie Larson, Džiugas Baltrunas, Amund Kvalbein, Amogh Dhamdhere, Ahmed Elmokashfi, et al. Investigating excessive delays in mobile broadband networks. In *Proceedings of the 5th Workshop on All Things Cellular: Operations, Applications and Challenges*, pages 51–56. ACM, 2015.

[LR95] Marco Luise and Ruggero Reggiannini. Carrier frequency recovery in all-digital modems for burst-mode transmissions. *IEEE Transactions on Communications*, 43(2/3/4):1169–1178, 1995.

[LTP+15] Christos Liaskos, Ageliki Tsioliaridou, Andreas Pitsillides, Ian F Akyildiz, Nikolaos V Kantartzis, Antonios X Lalas, Xenofontas Dimitropoulos, Sotiris Ioannidis, Maria Kafesaki, and CM Soukoulis. Design and development of software defined metamaterials for nanonetworks. *IEEE Circuits and Systems Magazine*, 15(4):12–25, 2015.

[LWL13] D. Lu, R. Wu, and H. Liu. Global positioning system anti-jamming algorithm based on period repetitive CLEAN. *IET Radar, Sonar & Navigation*, 7(2):164–169, 2013.

[LWR+18] Hanjiang Luo, Kaishun Wu, Rukhsana Ruby, Yongquan Liang, Zhongwen Guo, and Lionel M Ni. Software-defined architectures and technologies for underwater wireless sensor networks: a survey. *IEEE Communications Surveys & Tutorials*, 20(4):2855–2888, 2018.

[Men13] Umberto Mengali. *Synchronization techniques for digital receivers*. Springer Science & Business Media, 2013.

[MGV+15] Daniel F Macedo, Dorgival Guedes, Luiz FM Vieira, Marcos AM Vieira, and Michele Nogueira. Programmable networksfrom software-defined radio to software-defined networking. *IEEE communications surveys & tutorials*, 17(2):1102–1125, 2015.

[Mit95] Joe Mitola. Software radios. *IEEE Communications magazine*, 33(5):24–25, 1995.

[mmW] Millimeter waves will expand the wireless future, https://www.electronicdesign.com/communications/millimeter-waves-will-expand-wireless-future.

[Mol12] Andreas F Molisch. *Wireless communications*, volume 34. John Wiley & Sons, 2012.

[Moy05] Theodore D Moyer. *Formulation for observed and computed values of Deep Space Network data types for navigation*, volume 3. John Wiley & Sons, 2005.

[MSV13] William F Moulder, Kubilay Sertel, and John L Volakis. Ultrawideband superstrate-enhanced substrate-loaded array with integrated feed. *IEEE Transactions on Antennas and Propagation*, 61(11):5802–5807, 2013.

[Mut96] RN Mutagi. Pseudo noise sequences for engineers. *Electronics & communication engineering journal*, 8(2):79–87, 1996.

[MVL+17] Steffen Malkowsky, Joao Vieira, Liang Liu, Paul Harris, Karl Nieman, Nikhil Kundargi, Ian C Wong, Fredrik Tufvesson, Viktor Öwall, and Ove

Edfors. The worlds first real-time testbed for massive mimo: Design, implementation, and validation. *IEEE Access*, 5:9073–9088, 2017.

[Nek05] Faranak Nekoogar. *Ultra-wideband communications: fundamentals and applications*. Prentice Hall Press, 2005.

[NGW11] Ali Abdul-Elah Noori, Sadiq Kamel Gharghan, and Ali Jaber Abdul Wahhab. Study of signal estimation parameters via rotational invariance technique by using ants colony optimization algorithm. *Engineering and Technology Journal*, 29(4):736–749, 2011.

[nok] 5g for mission critical communicationachieve ultra-reliability and virtual zero latency, white paper, nokia netw., 2016. [online]. available: https://www2.deloitte.com/content/dam/deloitte/us/ documents /technology-media-telecommunications/us-tmt-2018-telecom-industry-outlook.pdf [accessed on 01/19/2019.

[OH17] Timothy OShea and Jakob Hoydis. An introduction to deep learning for the physical layer. *IEEE Transactions on Cognitive Communications and Networking*, 3(4):563–575, 2017.

[Pis73] Vladilen F Pisarenko. The retrieval of harmonics from a covariance function. *Geophysical Journal International*, 33(3):347–366, 1973.

[Ple86] V. Pless. Decoding the golay codes. *IEEE Trans. Inf. Theory*, 32(4):561–567, 1986.

[PO98] Ramjee Prasad and Tero Ojanpera. An overview of cdma evolution toward wideband cdma. *IEEE Communications Surveys*, 1(1):2–29, 1998.

[PR04] M. B. Pursley and T. C. Royster. Coding alternatives for high-rate direct-sequence spread spectrum. In *Military Communications Conference, 2004. MILCOM 2004*, volume 2, pages 892–898. IEEE, 2004.

[RBL+12] Andre Luiz Garcia Reis, Andre Felipe Barros, Karlo Gusso Lenzi, Luis Geraldo Pedroso Meloni, and Silvio Ernesto Barbin. Introduction to the software-defined radio approach. *IEEE Latin America Transactions*, 10(1):1156–1161, 2012.

[RDB+08] Francois Rivet, Yann Deval, Jean-Baptiste Begueret, Dominique Dallet, Philippe Cathelin, and Didier Belot. A disruptive receiver architecture

dedicated to software-defined radio. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 55(4):344–348, 2008.

[RGTL05] A. Raghavan, E. Gebara, E. M. Tentzeris, and J. Laskar. Analysis and design of an interference canceller for collocated radios. *IEEE Trans. Microw. Theory Techn.*, 53(11):3498–3508, 2005.

[Ric09] Michael Rice. *Digital communications: a discrete-time approach*. Pearson/Prentice Hall Upper Saddle River, 2009.

[RP94] L. A. Rusch and H. V. Poor. Narrowband interference suppression in cdma spread spectrum communications. *IEEE Trans. Commun.*, 42(234):1969–1979, 1994.

[Sch83] Robert Scholtz. Notes on spread-spectrum history. *IEEE Transactions on Communications*, 31(1):82–84, 1983.

[Sch86] Ralph Schmidt. Multiple emitter location and signal parameter estimation. *IEEE transactions on antennas and propagation*, 34(3):276–280, 1986.

[SDX05] Zheng Shenghua, Xu Dazhuan, and Jin Xueming. Adc limitations on the dynamic range of a digital receiver. In *2005 IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications*, volume 1, pages 79–82. IEEE, 2005.

[Sha48] Claude Elwood Shannon. A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423, 1948.

[SK12] Sam Shearman and James Kimery. Software defined radio prototyping platforms enable a flexible approach to design [application notes]. *IEEE microwave magazine*, 13(5):76–80, 2012.

[SM97] Petre Stoica and Randolph L Moses. *Introduction to spectral analysis*, volume 1. Prentice hall Upper Saddle River, NJ, 1997.

[SM16] Guowei Shi and Ying Ming. Survey of indoor positioning systems based on ultra-wideband (uwb) technology. In *Wireless Communications, Networking and Applications*, pages 1269–1278. Springer, 2016.

[SPR13] S. Savasta, L. L. Presti, and M. Rao. Interference mitigation in gnss receivers by a time-frequency approach. *IEEE Trans. on Aerospace and Electronic Syst.*, 49(1):415–438, 2013.

[Ste87] Hans Steyskal. Digital beamforming antennas. *Microwave journal*, 30(1):107–124, 1987.

[Tes03] Nikola Tesla. Method of signaling., March 17 1903. US Patent 723,188.

[TJC99] V. Tarokh, H. Jafarkhani, and A. R. Calderbank. Space-time block codes from orthogonal designs. *IEEE Trans. Inf. theory*, 45(5):1456–1467, 1999.

[Ulv10] Tore Ulversoy. Software defined radio: Challenges and opportunities. *IEEE Communications Surveys & Tutorials*, 12(4):531–550, 2010.

[UXR] Infiniium uxr-series real-time oscilloscopes, https://www.keysight.com/en/pcx-2935671/uxr-series-real-time-infiniium-oscilloscopes?nid=-31885.0cc=uslc=eng [accessed on 02/19/2019].

[VJJ07] John Leonidas Volakis, Richard C Johnson, and Henry Jasik. *Antenna engineering handbook*, volume 1755. McGraw-Hill New York, 2007.

[Wel09] Jonathan Wells. Faster than fiber: The future of multi-g/s wireless. *IEEE microwave magazine*, 10(3):104–112, 2009.

[Wil00] S. Willenegger. CDMA2000 physical layer: An overview. *J. Commun. and Netw.*, 2(1):5–17, 2000.

[WLT09] Z. Wang, M. Lv, and B. Tang. Paper application of partial coefficient update LMS algorithm to suppress narrowband interference in DSSS system. In *Communication Software and Networks, 2009. ICCSN'09. International Conference on*, pages 275–278. IEEE, 2009.

[WSWH10] T. D. Werth, C Schmits, R. Wunderlich, and S. Heinen. An active feedback interference cancellation technique for blocker filtering in RF receiver front-ends. *IEEE J. Solid-State Circuits*, 45(5):989–997, 2010.

[Yam04] H. Yamaguchi. Active interference cancellation technique for MB-OFDM cognitive radio. In *Microwave Conference, 2004. 34th European*, volume 2, pages 1105–1108. IEEE, 2004.

[YKBF03] Derek P Young, Catherine M Keller, Dan W Bliss, and Keith W Forsythe. Ultra-wideband (uwb) transmitter location using time difference of arrival (tdoa) techniques. In *The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, 2003*, volume 2, pages 1225–1229. IEEE, 2003.

[ZA12] Y. D. Zhang and M. G. Amin. Anti-jamming GPS receiver with reduced phase distortions. *IEEE Signal Process. Lett.*, 19(10):635–638, 2012.

[ZLH07] Xiangyong Zeng, John Qingchong Liu, and Lei Hu. Generalized kasami sequences: the large set. *IEEE Transactions on Information Theory*, 53(7):2587–2598, 2007.

[ZYCY09] L. Zhang, S. Yuan, Y. Chen, and J. Yang. Narrowband interference suppression in DSSS system based on frequency shift wavelet packet transform. In *Electronic Measurement & Instruments, 2009. ICEMI'09. 9th International Conference on*, pages 2–333. IEEE, 2009.

VITA

DIMITRIOS SIAFARIKAS

May 11, 1991	Born, Larissa, Greece
2015	Diploma, Electrical and Computer engineering Democritus University of Thrace Xanthi, Greece
2017	M.S., Electrical and Computer engineering The Ohio State University Columbus, Ohio
2018–2019	RF Systems / RFIC Design engineer Motorola Solutions Plantation,Florida
2019–Present	Wireless Systems Engineer Apple Cupertino,California

PUBLICATIONS AND PRESENTATIONS

Siafarikas, Volakis, J.L., (2019). *Towards Direct RF Sampling for Communications*. IEEE Microwave Magazine (Submitted).

Siafarikas, D., Volakis, J.L., (2019). *Experimental Results of Interference Mitigation using Ultra-Wideband Spreading.*. Government Microcircuit Applications and Critical Technology Conference (GOMACTech), Albuquerque, NM

Siafarikas, D., Alwan, E.A, Volakis, J.L., (2019). *Interference Mitigation for 5G Millimeter-Wave Communications*. IEEE Access.

Siafarikas, D., Volakis, J.L., (2019). *Experimental Validation of Interference Mitigation for 5G Millimeter Wave Communication Links.*. IEEE National Radio Science Meeting (NRSM), Boulder, CO.

Siafarikas, D., Volakis, J.L., (2018). *5G Millimeter-Wave Communications using Direct RF sampling techniques.*. IEEE International Symposium on Antennas and Propagation (APSURSI), Boston, MA.

Siafarikas, D., Volakis, J.L., (2018). *Direction Finding of Ultra-Wideband Signalsusing Direct RF Sampling.*. IEEE International Symposium on Antennas and Propagation (APSURSI), Boston, MA.

Siafarikas, D., Alwan,E.A, Volakis, J.L., (2018). *Interference Mitigation for 5G Millimeter Wave Communications.*. IEEE National Radio Science Meeting (NRSM), Boulder, CO.

Siafarikas, D., Alwan,E.A, Volakis, J.L., (2018). *Processing Gain Using CDMA in Ultra-Wideband Multi-Channel Digital Beam-Formers.*. Government Microcircuit Applications and Critical Technology Conference (GOMACTech), Miami, FL

Siafarikas, D., Alwan,E.A, Volakis, J.L., (2017). *Processing Gain Using CDMA in Ultra-Wideband Multi-Channel Digital Beam-Formers.*. IEEE International Symposium on Antennas and Propagation (APSURSI), San Diego, CA.

Siafarikas, D., Volakis, J.L., (2017). *Synchronization issues in Ultra-Wideband Multi-channel Digital Beam-formers.*. IEEE International Symposium on Antennas and Propagation (APSURSI), San Diego, CA.

Alwan, E.A, Siafarikas, D., Volakis, J.L., (2016). *Ultra-wideband transceiver with high interference mitigation for secure high data rate communication.*. URSI International Symposium on Electromagnetic Theory (EMTS), Espoo, Finland.

Siafarikas. D., Alwan, E.A., Volakis, J.L., (2016). *Millimeter wave transceivers with coding gain for secure high data rate communication.*. IEEE International Symposium on Antennas and Propagation (APSURSI), Fajardo, Puerto Rico.

Siafarikas. D., Alwan, E.A., Volakis, J.L., (2016). *High data rate multi-path transmit/receive system with on-site coding.*. International Workshop on Antenna Technology (iWAT), Cocoa Beach, FL.

Siafarikas. D., Samourkasidis, A., Arampatzis, A., (2014). A Cost-Benefit Analysis of Indexing Big Data with Map-Reduce.. SFHMMY 7, Thessaloniki, Greece.