NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

USER EQUIPMENT-SIDE INITIATION FOR 5G COMMUNICATIONS

by

Jonathan D. Monti

September 2021

Thesis Advisor:	Frank E. Kragh
Second Reader:	Chad A. Bollmann

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2021	**3. REPORT TYPE AND DATES COVERED** Master’s thesis

4. TITLE AND SUBTITLE USER EQUIPMENT-SIDE INITIATION FOR 5G COMMUNICATIONS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Jonathan D. Monti	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The electromagnetic (EM) spectrum is an integral part of the modern battlefield, and the use of wireless connections presents both benefits and risks for U.S. forces. 5G New Radio (5G NR) represents the latest in wireless cellular technology and provides the foundation for a powerful network. However, the requirement for military communications to be low–probability of detection (LPD) and low–probability of intercept (LPI) makes 5G NR unsuitable for use in hostile environments in its current form. 5G NR initial access procedures were designed to provide a large area of coverage to a high number of users and results in substantial stray emissions. This research seeks to introduce a replacement procedure for 5G NR initial access utilizing a user equipment-side connection process (UECP). By capitalizing on the directionality of massive multiple-input multiple-output antenna arrays (MIMO) and utilizing a novel detection process known as passive array sweep listening (PASL), connections can be established between the user equipment (UE) and gNodeB (gNB) at ultra-low signal-to-noise ratios (SNRs). The performance of UECP was evaluated utilizing multiple simulations created in MATLAB. The ability of UECP to function at ultra-low SNRs, combined with the directionality of large antenna arrays, results in a substantial decrease of stray emissions normally found in 5G NR initial access, which greatly reduces the probability of intercept or detection.

14. SUBJECT TERMS 5G, connections, direction of arrival, DOA, user side, gNodeB, gNB, user equipment-side connection process, UECP, signal-to-noise ratio, SNR, passive array sweep listening, PASL, low–probability detection, LPD, low–probability of intercept, LPI, electromagnetic, EM, 5G New Radio, 5G NR, user equipment, UE	**15. NUMBER OF PAGES** 133
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

USER EQUIPMENT-SIDE INITIATION FOR 5G COMMUNICATIONS

Jonathan D. Monti
Captain, United States Marine Corps
BS, United States Naval Academy, 2012
MSME, Massachusetts Institute of Technology, 2014

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2021

Approved by: Frank E. Kragh
Advisor

Chad A. Bollmann
Second Reader

Douglas J. Fouts
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The electromagnetic (EM) spectrum is an integral part of the modern battlefield, and the use of wireless connections presents both benefits and risks for U.S. forces. 5G New Radio (5G NR) represents the latest in wireless cellular technology and provides the foundation for a powerful network. However, the requirement for military communications to be low–probability of detection (LPD) and low–probability of intercept (LPI) makes 5G NR unsuitable for use in hostile environments in its current form. 5G NR initial access procedures were designed to provide a large area of coverage to a high number of users and results in substantial stray emissions. This research seeks to introduce a replacement procedure for 5G NR initial access utilizing a user equipment-side connection process (UECP). By capitalizing on the directionality of massive multiple-input multiple-output antenna arrays (MIMO) and utilizing a novel detection process known as passive array sweep listening (PASL), connections can be established between the user equipment (UE) and gNodeB (gNB) at ultra-low signal-to-noise ratios (SNRs). The performance of UECP was evaluated utilizing multiple simulations created in MATLAB. The ability of UECP to function at ultra-low SNRs, combined with the directionality of large antenna arrays, results in a substantial decrease of stray emissions normally found in 5G NR initial access, which greatly reduces the probability of intercept or detection.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

5G NR	5th Generation Cellular - New Radio
ACF	Autocorrelation Function
AF	Array Factor
AUTHCODE	Authorization Code
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
C4I	Command, Control, Communications, Computers, and Intelligence
COC	Combat Operations Center
CPG	Commandant’s Planning Guidance
DOA	Direction of Arrival
DOS	Denial of Service
EABO	Expeditionary Advanced Base Operations
EDAC	Error Detection and Correction
EM	Electromagnetic
EL	Array Length
ESL	Effective Sequence Length
FR1	Frequency Range 1
FR2	Frequency Range 2
Gbps	Gigabit Per Second
GHz	Gigahertz
gNB	g-Node B
HPBW	Half Power Beamwidth
IID	Independent and Identically Distributed
KPI	Key Performance Indicator
LAN	Local Area Network
LPD	Low Probability of Detect
LPI	Low Probability of Intercept
MIMO	Multiple Input Multiple Output

MiTM	Man-in-the-Middle
MMWAVE	Millimeter Wave
MUSIC	Multiple User Signal Classification
PASL	Passive Array Sweep Listening
PSS	Primary Synchronization Signal
QPSK	Quadrature Phase Shift Keying
RACH	Random Access Channel
ROC	Receiver Operating Characteristics
SINR	Signal to Interference Noise Ratio
SL	Sequence Length
SNR	Signal to Noise Ratio
SSB	Synchronization Signal Block
SSS	Secondary Synchronization Signal
UE	User Equipment
UECP	User Equipment-Side Connection Process
ZC	Zadoff-Chu

ACKNOWLEDGMENTS

First and foremost, I want to thank God for giving me the energy, capacity, and ability to complete this work, as well as for providing me a sense of joy and fulfillment day by day that made this journey a sweet experience.

I want to thank my wife, Amanda, who has been through several moves, a deployment just before coming to graduate school, and while here at graduate school, two pregnancies, COVID, California wildfires, a few minor earthquakes, and more than a few days of me being sequestered to my closet-office, but has always kept a positive outlook, supported me in my work, and made sure that our home was a comfortable and wonderful place for our family every day. Her diligence and perseverance through some very unusual circumstances provided me the support I needed to put everything I had into this work. Thank you, Amanda, and I love you (you too, Lucas and baby Monti)!

I would like to thank Professor John Roth who guided me through over a year of this work. I genuinely appreciated the conversations we had that were a healthy mix of technical discussion, theoretical concepts, and random philosophical musings throughout our time working together. Thanks for giving me the freedom to explore topics and go down “rabbit holes” but also pulling me back and helping me find direction when needed. As a student, advisee, and friend, I was sorry to see you leave. I wish you and your family the best of luck in your future endeavors!

Additionally, I would like to thank Professor Frank Kragh and CDR Chad Bollmann for taking over the advisor and second reader roles in the 11th hour of my work, providing me with detailed and relevant feedback, and helping me get this work over the finish line. It was a pleasure working with you for the short time we had, and thank you!

Lastly, I would like to thank my fellow Marines in the Electrical Engineering program; Majors John Watkins and Vic Hollar and Captains Justin Bracci, Matthew Caspers, and Erik Henegar. Thank you for your support and friendship over the past few years (and most importantly, for being good group project partners!). Special shoutout to Matthew for always being there for me and my family. I really appreciate it!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OBJECTIVE OF RESEARCH

As of the beginning of 2019, the United States Marine Corps began an intensive internal overhaul of force design to better posture itself to meet the challenges of modern warfare. A primary initiative outlined in the *Commandant's Planning Guidance 2019* (CPG 2019), the central document which provides the strategic direction for the Marine Corps, is Expeditionary Advanced Base Operations (EABO). EABO is intended to counteract our enemy's desire to target "forward fixed and vulnerable bases" [1] by developing a force structure "not dependent on concentrated, vulnerable, and expensive forward infrastructure" [1]. An implicit requirement of this initiative is that forces must be highly mobile, as static units and command centers allow adversaries an advantage in the targeting process. An additional component of the *CPG 2019* is the requirement for the development of "low probability of intercept (LPI) / low probability of detection (LPD) communications" [1] as "communications nodes will be hunted and targeted…[and] careless and unmanaged [electromagnetic (EM)] signatures will invite destruction…[which] will require interoperable, low signature, secure communications" [1]. This thesis intends to address the issues of mobility, LPI/LPD, and secure communications by proposing a novel connection method that would allow commercial 5th generation mobile network – new radio (5G NR) technology to be incorporated into the Marine Corps' (and larger military's) command, control, communication, computers, and intelligence (C4I) infrastructure but still align with the desire for secure, LPI/LPD communications.

B. MOTIVATION OF RESEARCH

1. Risks Associated with Military Use of Wireless Communications

The United States Military has long been caught between the need and desire to incorporate advanced wireless technologies into its C4I infrastructure and the requirement to maintain secure communications. Two major areas of concern in implementing wireless technologies are the security of the communications, that is, the certainty that information relayed over wireless channels cannot be intercepted and used by an enemy, and the risks associated with the detection of wireless communications. Even if the information being transferred cannot be deciphered, detection alone can be catastrophic for a military unit as valuable information such as unit activity or geolocation data can be ascertained by detecting EM signals.

2. Mobility

Wireless technologies by their nature provide for increased mobility for the connected user or device. However, it is not simply the mobility of the user or device that is increased, it is the mobility of the system as well. A wireless system can be moved from location to location and either maintain or resume network operations orders of magnitude faster than its wired counterparts.

3. Flexibility

Wireless technology also provides a level of network flexibility not found in wired systems. Adjusting architecture, opening and closing connections, and expanding or contracting network size can all occur much faster and with less manpower required than wired systems.

4. Benefits of 5G NR over Previous Wireless Technology

5G NR offers many benefits over previous wireless technologies, most notably in the area of increased data rates, reaching speeds above one gigabit per second (Gbps) [2], physical layer security improvements over previous wireless technologies, and by taking a more holistic approach to security at all levels within the system [3]. Lastly, and most important to this research, is the implementation of massive multiple-input multiple-output (MIMO) technology in 5G NR which allows a system to “control how data maps into antennas and where to focus energy in space” [4]. The latter attribute, the ability to focus energy in space, is vital to endeavors involving LPI/LPD communications.

C. THESIS OVERVIEW

The remainder of this thesis will introduce the scenario/use case in which this research was meant to be applied, as well as an attack model used to develop a novel user-equipment (UE) side connection process. The classic "Alice/Bob/Eve" construct will be used to introduce the scenario and attack model, and system component names will be used throughout the detailed discussion of system operations. Through the scenario and attack model discussion key parameters and key performance indicators (KPI) are developed and subsequently used as the basis for decisions throughout the research. A broad overview of the UE-Side Connection Process (UECP) will be presented, followed by an in-depth analysis of critical elements and processes used throughout the connection process. A step-by-step explanation of performance criteria, analysis process, results, and decision point justifications will be provided throughout the document. Lastly, a summary and recommendations for follow-on work will be presented.

THIS PAGE INTENTIONALLY LEFT BLANK

II. ATTACK MODEL AND SCENARIO

This research is not intended to be applied to all 5G NR scenarios. This section is intended to clarify the proper use case or application of the novel UECP, as well as detail the attack model used to guide the focus of research and criteria for decisions throughout.

A. MODEL ACTORS AND SCENARIO OVERVIEW

1. Model Actors

The scenario/use case and proposed UECP process will be introduced using the "Alice/Bob/Eve" construct for clarity purposes. The main actors and what they represent are:

- Eve: Represents non-friendly forces, specifically those passively listening in the EM spectrum attempting to detect EM energy.

- Bob: Represents the g-Node B (gNB) base station used as the central hub for 5G NR connectivity for all Alices.

- Alice: Represent scattered devices (UE) that are connected to Bob, or attempting to connect to Bob, and close enough that a connection could be successful.

2. Scenario Overview

The fundamental scenario is that a wireless connection needs to be established between Bob and Alice (Figure 1), but Eve is constantly listening, and if she detects the transmissions from either Bob or Alice her ability to geolocate them improves. Neither Bob nor Alice is certain of the presence of the other, and both need a means of establishing the presence of the other without alerting Eve.

Eve exists within the environment, but her location is unknown to Bob or Alice. Eve is alerted when she detects a signal emanating from either Bob or Alice. There are three ways Eve can be successful in detecting Bob or Alice, and they will be discussed in a following section. Due to the nature of wireless connections, it is impossible to create a perfect connection between Bob and Alice with zero energy going in any undesired direction or fully stopping at the recipient; there will always be non-zero energy available for Eve to detect. Thus, the goal within the scenario is to establish a directed energy connection between Bob and Alice with the least amount of EM energy going in any direction not specifically towards Bob or Alice.

For the remainder of the scenario and attack model discussion, Eve's interaction with Bob will be the focal point; the reason for this will be explained in the UECP Process Overview section.

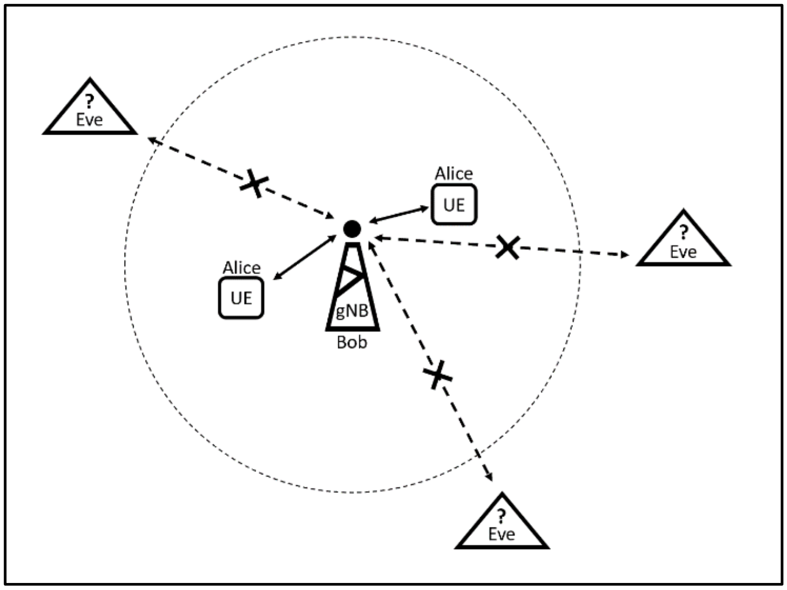


Figure 1. Scenario Overview

B. EVE CHARACTERISTICS

Eve's abilities within the attack model are vital in understanding the direction of this research, and the rationale for decisions made throughout the process. The following assumed capabilities and limitations were used to both scope the research and guide the development of UECP.

1. Capabilities

1. Eve's EM detection is not bounded to any specific region of the spectrum.

2. Eve can passively detect and capture signals.

3. Eve can actively transmit signals in the form of a local replay attack, where a signal from Alice in the scenario has been captured and is reused to try to solicit a response from Bob.

4. Eve can actively transmit signals in the form of a non-local replay attack, where a signal captured previously can be used to deceive Bob or Alice.

5. Eve can actively transmit signals in the form of a brute force attack, wherein randomly constructed signals are used to deceive Bob or Alice.

6. Eve can be any direction relative to Bob or Alice.

7. Eve can be at any distance with the exception that Eve will never be closer to Bob than any Alice.

8. Eve does not need to gain access to the underlying information in the signal, detection of signal energy from Bob or Alice is sufficient to ascertain their physical location.

9. Eve is passively listening at all times and can transmit at any time.

10. Eve has complete knowledge of how the systems work, with the exception of Limitation 3, below.

2. Limitations

1. Eve does not have the ability to establish a connection with Bob. Other protocols and safeguards exist outside the scope of this model that would prevent Eve from establishing a connection and accessing the network Bob is facilitating.

2. Eve cannot continuously transmit in an attempt to jam either Bob or Alice.

3. Eve does not have knowledge of the pre-shared key used by Bob and Alice.

C. EVE'S PATH TO VICTORY

Eve's goal within the scenario is to ascertain the physical location of either Bob or Alice. The simplest way this would occur would be for Eve to detect signal energy emanating from either Bob or Alice. The following paragraphs detail the various ways in which Eve can be successful in this endeavor and includes a basic discussion of each.

1. Passive Detection (Passive Eavesdropping)

The first path to victory for Eve is to passively detect a signal from either Bob or Alice. Inherent in the connection between Bob and Alice is the chance that stray EM energy could be detected by Eve; therefore, the likelihood of this occurring can never be reduced to zero as long as Alice or Bob is transmitting. However, compared to commercial systems, this probability can be greatly reduced while maintaining the ability for Bob and Alice to connect and share data.

2. Solicitation via Random Transmission (Active Eavesdropping)

The second path to victory for Eve is solicitation through random transmission. By using randomly generated transmissions, Eve could conceivably trick Bob or Alice into thinking she is a friendly device. This would resemble a brute-force attack, where random sequences are generated and transmitted with the desire for a randomly constructed signal to be similar enough to a valid signal that either Bob or Alice believes it to be a legitimate friendly signal. Theoretically, exploitation of this path also cannot always be prevented. However, steps can be taken to reduce the probability of this path being successful.

3. Solicitation via Replay Attack

The final path to victory for Eve is the solicitation of a response from Bob or Alice via replay attack. The underlying assumption of this path is that Eve has previously captured a signal and is going to use this signal to attempt to solicit a response from either a Bob or Alice who believes it to be a friendly solicitation.

4. Cyber and Communications Attacks Not Presented

There are many other common forms of attack on cyber and communications systems, such as denial-of-service (DoS), distributed-denial-of-service (DDoS), and man-in-the-middle attacks (MiTM) [5]. The reason DoS and DDoS are not presented as possible paths to victory for Eve is that these attacks attempt to degrade the capability of a network. Eve's goal within the scope of the attack model is not degradation, rather, detection of the friendly network. These types of attacks are worth exploring in future research but are not within the scope of the attack model presented. Another common attack, MiTM, is predicated on Eve's ability to get between Alice and Bob in a digital sense and to manipulate or simply observe the traffic flowing between them. For Eve to properly do that, she would have already detected the transmissions between Bob and Alice and satisfied the conditions for victory through passive detection (Path to Victory #1). Most forms of cyber or communications attack require certain levels of integration or access to a network that would only occur after the conditions for Eve's victory have already been met.

D. USE CASE OVERVIEW

The previous sections established the basic framework and rules for this scenario, however, a final important consideration for this research is an understanding of the real-world scenario in which it is intended to be used. One major difference between the commercial and military applications of 5G NR is that commercial systems are designed for the greatest connectivity and coverage possible. In contrast, military applications desire the least amount of coverage and connectivity required to perform the required underlying network and data transfer functions due to the risks associated with emanating EM energy in hostile environments. This research is not intended to apply to large-scale 5G NR implementations, and instead focuses on converting small-scale, local area networks (LAN) from wired to wireless systems utilizing 5G NR as the fundamental architecture. Figure 2 shows a typical military combat operations center (COC) with wired connections used for data connectivity between the various devices.

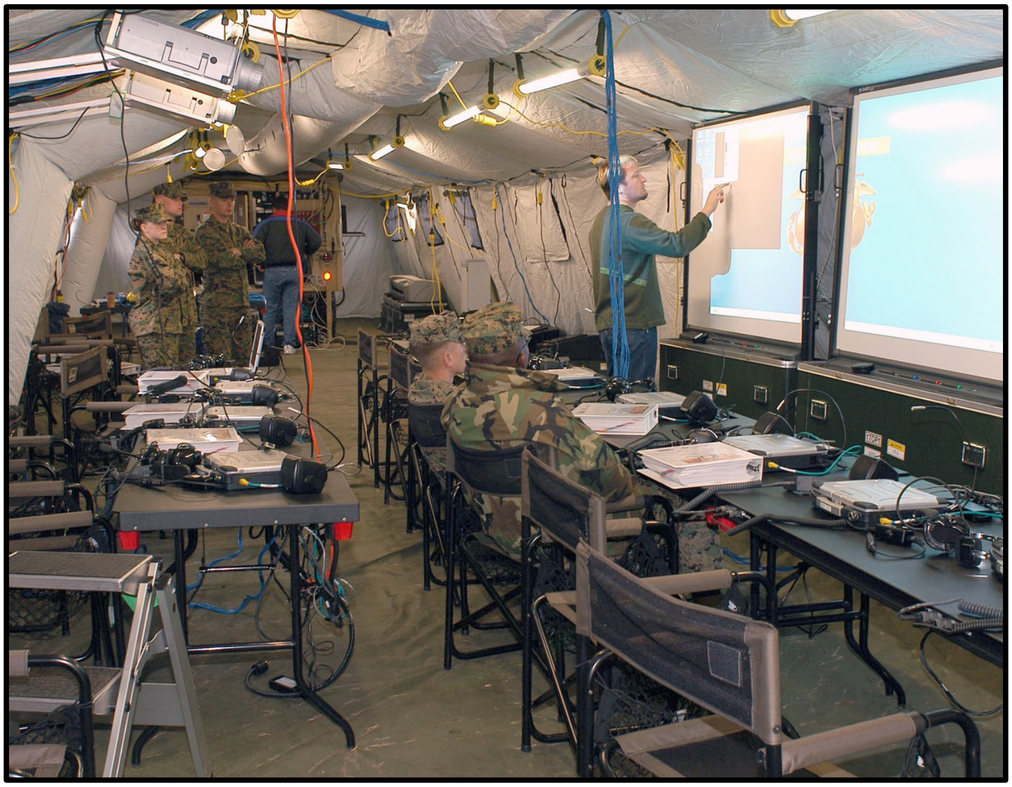


Figure 2. Typical Marine Corps Combat Operations Center. Source [6].

This research focuses specifically on adapting 5G NR to be used as a replacement for previously hard-wired connections present in a LAN. The importance of clarifying the intended use of this research is that the scope of implementation directly affected decisions made throughout this work. This research focuses on a network with a limited number of users and devices, a geographically small footprint, and static systems (relative to each other). There is not an exact number to each of these constraints, but the suitability of UECP diminishes as the number of users grows to the point where connection request transmission collisions occur, the geographic separation is great enough that transmit power becomes prohibitively high, or that mobility of UEs undermines the accuracy of direction of arrival estimates. A simple example of a use case would be a single router Wi-Fi and LAN setup, except the router is replaced with a gNB and the background network architecture is based on 5G NR technologies.

III. BACKGROUND

With the scenario, attack model, and use case established, there must be an investigation into how 5G NR currently operates to understand where risks, opportunities, and challenges exist. This section is intended to provide a basic understanding of 5G NR, several of its important features, and introduce critical elements and processes to be explored later in the work.

A. 5G NR OVERVIEW

5G NR is the latest wireless cellular technology standard commercially available throughout the world and has marked advantages over previous technologies. The three most important advantages and features for this research are its beam-centric design, high data rates, and usable spectrum. Beam-centric design is facilitated by multi-antenna arrays which allow energy to be directed to a specific location, increasing the spatial separation of individual wireless channels [4]. The underlying technology and use of bandwidth in 5G NR provides for extremely high data rates compared to other wireless technologies [7]. Lastly, 5G NR can operate over a wide section of the EM spectrum, and 5G NR has two primary frequency ranges; frequency range 1 (FR1) which encompasses all sub-6 GHz bands, and frequency range 2 (FR2) which includes 20 GHz to 60 GHz [8]. Additionally, 5G NR is capable of utilizing frequencies up to 300 GHz [9], which includes the millimeter wavelengths (mmWave) frequencies, although it is not currently operating at frequencies this high. A detailed analysis of the in-depth workings of 5G NR is beyond the scope of this work, however, the three attributes stated above make it a desirable network type for military operations and will be discussed in greater detail in the following sections.

B. 5G NR INITIAL ACCESS PROCEDURES

Although detailed operations associated with 5G NR are beyond the scope of this work, understanding the fundamentals of the start of the connection process is essential to this research. This process is outlined in this section is adapted summary from *ETSI TS 138 300 V15.8.0 (2020-01) 5G NR Overall Description Stage-2* [10] and *RF Wireless World – 5G NR Initial Access Procedure* [11].

Current 5G NR initial access procedure technology uses four steps to establish a physical layer connection between a gNB and a UE: beam sweeping, beam measurement, beam determination, and UE random-access channel (RACH) response. Beam sweeping entails the gNB broadcasting out multiple synchronization signal blocks (SSBs) in predetermined directions (Figure 3) at preset time intervals, with each SSB containing a primary synchronization signal (PSS) and a secondary synchronization signal (SSS). The UEs within the coverage area then receive one or multiple SSBs and perform beam measurement which includes analyzing the received SSB(s) to deduce specific performance metrics which are then used in beam determination to decide which SSB is most suitable for use. The UE then responds to the gNB with a RACH message which starts a series of transmissions between the two devices to establish a physical layer connection. Figure 4 shows the process in full, however, only the initial SSB process (labeled "PSS/ SSS" in the figure) is relevant to the remainder of this research.

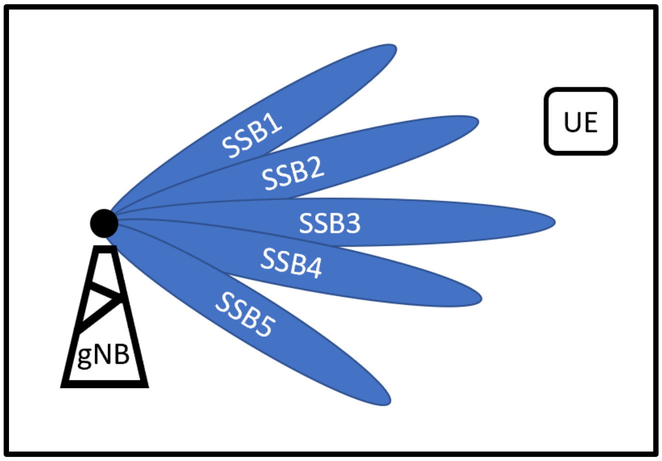


Figure 3. 5G NR SSB Sweep Illustration

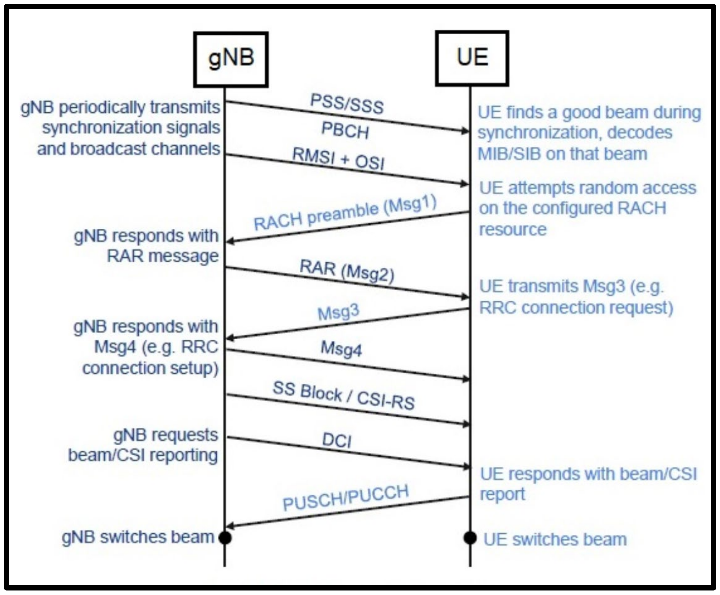

gNB
UE
gNB periodically transmits synchronization signals and broadcast channels
PSS/SSS
PBCH
RMSI + OSI
UE finds a good beam during synchronization, decodes MIB/SIB on that beam
UE attempts random access on the configured RACH resource
RACH preamble (Msg1)
gNB responds with RAR message
RAR (Msg2)
UE transmits Msg3 (e.g. RRC connection request)
Msg3
gNB responds with Msg4 (e.g. RRC connection setup)
Msg4
SS Block / CSI-RS
gNB requests beam/CSI reporting
DCI
UE responds with beam/CSI report
PUSCH/PUCCH
gNB switches beam
UE switches beam

Figure 4. 5G NR Initial Access Procedures. Source: [11].

C. MIMO AND ANTENNA ARRAY INTRODUCTION

Fundamentally, MIMO refers to the presence of multiple antennas working in concert at both the sending and receiving systems. An important feature of 5G NR is the utilization of not only MIMO technology but the expansion to massive MIMO, which greatly increases the number of antenna elements located at one or both ends of a connection. This technology provides a host of advantages: most important to this research is the ability of a system to beamform when transmitting [12]. It is important to consider the physical limitations of a system based upon application, and array sizes used for analysis may not be practical in a real-world scenario. However, a wide range of array sizes were used throughout this work to determine if trends existed regardless of specific array size.

Beamforming is the process by which a signal is sent from multiple antennae, but each antennae element can modify the signal to increase the energy sent in a specific direction, which in turn reduces the energy sent in a different direction. Figure 5 and Figure 6 illustrate the effects of beamforming. Figure 5 represents a simple omnidirectional antenna, and Figure 6 illustrates the impacts of the addition of a second antenna element at one-half wavelength distance along the x-axis. The resulting signal pattern shows increased amplitude along the y-axis and no energy along the x-axis. Although the resulting signal is running along the y-axis, it is possible to adjust the signal from each antenna to point the emitted energy in a specific direction in a process known as beam steering [12].

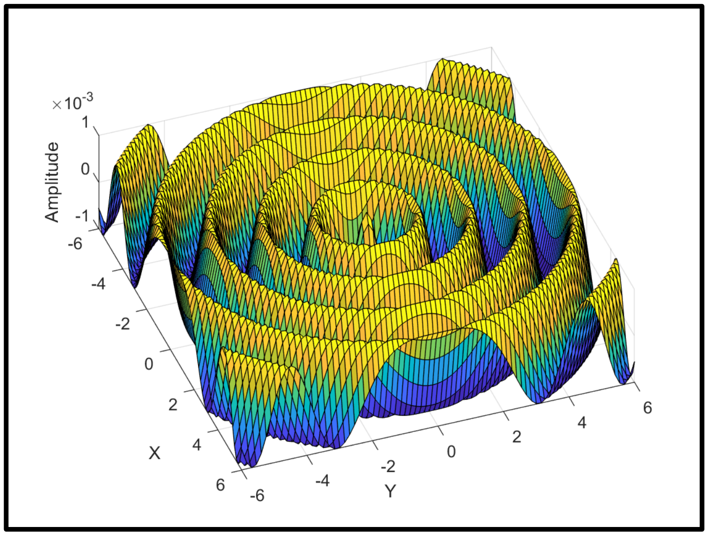


Figure 5. Omnidirectional Antenna Beam Pattern

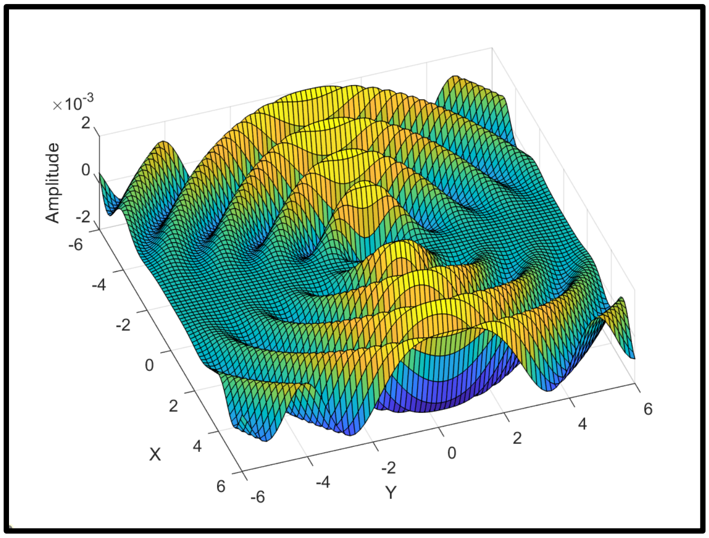


Figure 6. 2-Element Array Beam Pattern

Just as the energy from each element can be adjusted to direct the energy from an array to a specific location, the incoming signals can also be adjusted such that the gain in a particular direction is higher than any other direction. Theoretically, if an antenna array size were to go to infinity, the energy transmitted could be limited to a single, infinitely thin direction in space. The gain when receiving a signal transmitted from that direction would also go to infinity. These two attributes, along with the inclusion of massive MIMO in 5G NR, constitute major points within this research as they allow energy to be sent to, and received from, a single direction, thus reducing stray emissions. If the effects of multipath transmissions are also considered, and the number of paths increases, the energy being sent and received in any particular direction could be greatly reduced and would converge in-phase on a particular point in space. However, the effects of multipath are not included in this research due to the earlier-defined scope of the use case.

D. MILLIMETER WAVE CHARACTERISTICS

Another important feature of 5G NR is the ability to operate in the mmWave portion of the spectrum, which includes the 30 GHz to 300 GHz range [9]. This is an important aspect of 5G NR for several reasons. First, the lack of crowding in these frequency bands allows for wider spectrum use, thus increasing the data rate capability of the systems operating in this range. Second, and most importantly for military use, are the propagation characteristics of mmWaves. As a general trend, EM waves experience greater attenuation through the atmosphere as the frequency of a signal increases [13].

Beyond the general trend, certain areas within the mmWave range experience very high attenuation due to atmospheric interaction. Figure 7 shows the attenuation characteristics of signals ranging from 1 GHz to 350 GHz and shows several attenuation spikes, most notably around 60 GHz. This is an important feature for this research in that as the attenuation of a signal increases, the likelihood of detection by adversaries decreases as less energy is available for detection at a given distance. The specific regions of high attenuation could be exploited to allow the operation of close-range communications systems while reducing the detectable distance for those signals. This characteristic will not heavily affect the research in this work, as all processes and concepts explored are frequency independent. However, it does provide justification for 5G NR use in LPD/LPI scenarios and is a consideration for real-world implementation, especially if frequencies above 10 GHz are used.

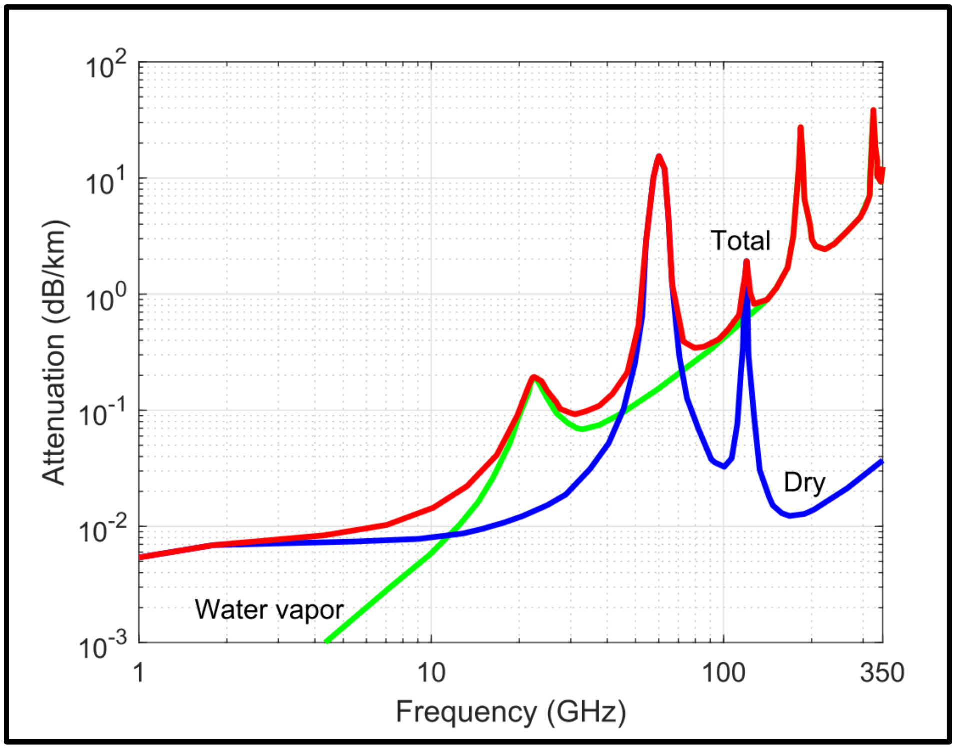


Figure 7. Attenuation Characteristics of Frequencies between 1 GHz and 350 GHz. Source: [13].

E. COMBINING THE ATTACK MODEL AND 5G NR

The attack model is useful in identifying critical areas of vulnerability within the current 5G NR processes. In this section, key elements of the attack model and relevant 5G NR processes are combined and examined to provide the basic framework for the remainder of this research.

1. Eve and 5G NR Initial Access

5G NR initial access is built upon the concept of providing the largest coverage and service to the highest number of users possible. This is facilitated by sending multiple SSBs in predetermined directions and using beamforming to increase the strength of each of those signals [7]. This process is immediately identifiable as undesirable when paired with the attack model, as it provides a high likelihood of signals being sent directly, or nearly directly, from Bob to Eve. This process would need to be modified for a 5G NR system to work within the constraints of the attack model. However, it is prudent to minimize modification to the 5G NR process as much as possible to reduce the time and resources required to modify the base technology for military use. The solution proposed in this research is to replace the SSB beam sweeping process with a directed energy approach that minimizes the stray emissions caused during the cell search procedure.

2. Eve and Signal Power

It is impossible to establish a wireless connection between Bob and Alice without any stray emissions. However, it is possible to reduce the energy of all stray emissions by reducing the signal power required to establish a connection. This signal energy can be reduced in two ways: reducing the duration of a signal and reducing the power of the signal. 5G NR massive MIMO provides a unique capability in pursuing both objectives. As the number of elements in an array increases the gain of the array increases as well. This gain allows for the detection of lower power signals and facilitates the use of shorter signal durations to establish a connection.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. UE-SIDE CONNECTION PROCESS OVERVIEW

A. HIGH-LEVEL UECP PROCESS FLOW

The proposed UECP does not interfere with 5G NR initial access procedures and instead replaces the SSB broadcast sweep with only a single SSB being transmitted from gNB to UE in an intentional direction. Figure 8 shows the previously established 5G NR initial access process (in blue text) with the addition of UECP (in red text).

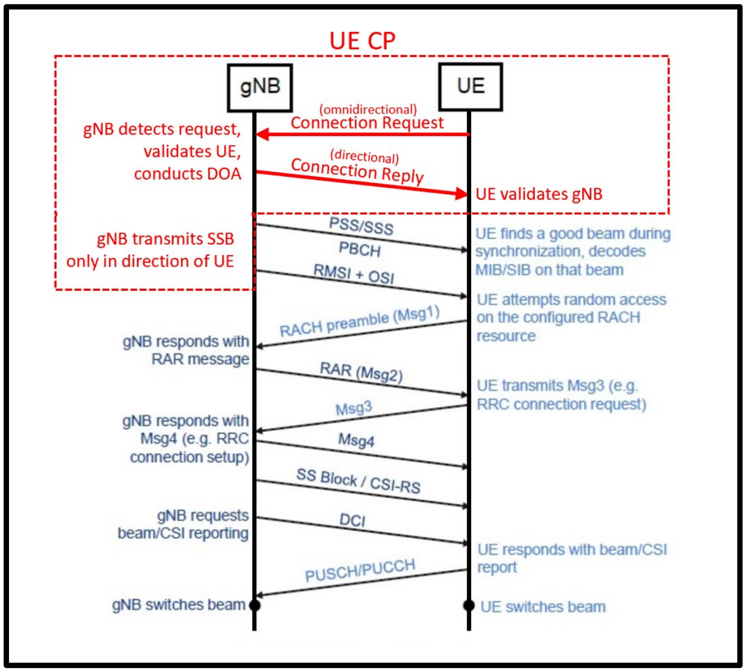


Figure 8. 5G NR Initial Access with UECP. Adapted From [11].

Figure 9 provides a process flow and illustration of the fundamental operations of UECP. A more detailed, step-by-step analysis of the process is provided in a Section D of this chapter.

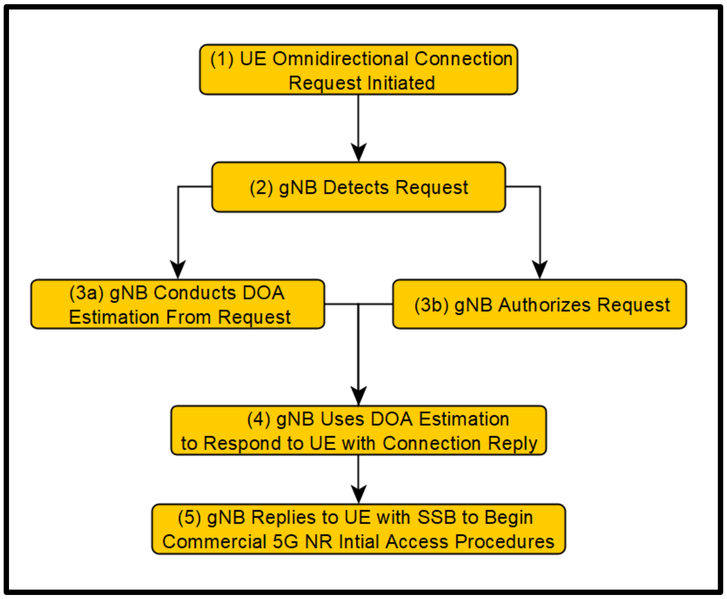

(1) UE Omnidirectional Connection Request Initiated
(2) gNB Detects Request
(3a) gNB Conducts DOA Estimation From Request
(3b) gNB Authorizes Request
(4) gNB Uses DOA Estimation to Respond to UE with Connection Reply
(5) gNB Replies to UE with SSB to Begin Commercial 5G NR Intial Access Procedures

Figure 9. UECP Process Flow

1. The proposed UECP would require the connection initiation to be done by the UE, rather than the gNB. Because neither the UE nor gNB has any information as to the direction to the other device, the initial connection request needs to be omnidirectional. The reason the connection request originates at the UE is because the gNB generally possesses much larger antenna arrays than the individual UEs, which provides greater gain when detecting the connection request. Although neither device knows the direction of an incoming signal, a process described later in this work allows the receiving device to scan through a series of possible directions of arrival to search if a signal is present. Also, the gain achieved by the larger arrays found at the gNB allows for the detection of a signal at lower transmit powers than could be achieved by a UE. Additionally, the large antenna arrays found at the gNB can more accurately direct a connection response to the requesting UE.

2. The gNB detects the request from the UE.

3. (a/b) Once the gNB detects the connection request it can use the received signal to conduct a direction of arrival estimation to use for the connection

response. Additionally, the gNB demodulates and decrypts the connection request, and subsequently uses the contained information to verify the authenticity of the request before sending a connection reply.

4. The gNB responds to the UE with a connection reply using the DOA estimate determined in step 3a. This response is now directional, thus reducing stray emissions. The larger antenna array of the gNB allows for tighter response beams which overcome the gain limitations of smaller arrays at the UEs which concentrate signal energy in a specific direction to overcome the desired reduction in transmitted energy. From this connection response, the UE can authenticate the gNB.

5. gNB responds to UE with SSB and begins standard 5G NR initial access procedures.

B. CONNECTION REQUEST/REPLY DEVELOPMENT

The goal of a UE-side connection is to reduce stray emissions and the likelihood of detection by Eve, which means it is important that the connection request contains just enough information that the gNB (Bob) can detect the connection request and authenticate both the request and sending UE (Alice). The following sections will detail the various ways in which the connection request needs to be modified to increase the likelihood of responding to a valid request and reducing the likelihood of responding to an invalid request. The "Alice/Bob/Eve" method will be used to explain the connection request development process.

1. Simple Connection

The simplest type of connection request would be the transmission of a known-value signal, referred to in this work as a "Hello" message. This process entails Alice sending a connection request in the form of an unencrypted "Hello" message to Bob, as illustrated in Figure 10. In this case, Eve can easily craft her own "Hello" message and solicit a response from Bob, as there is no distinction between the valid and invalid messages from Bob's perspective. This scenario will be our starting point for how to secure the process.

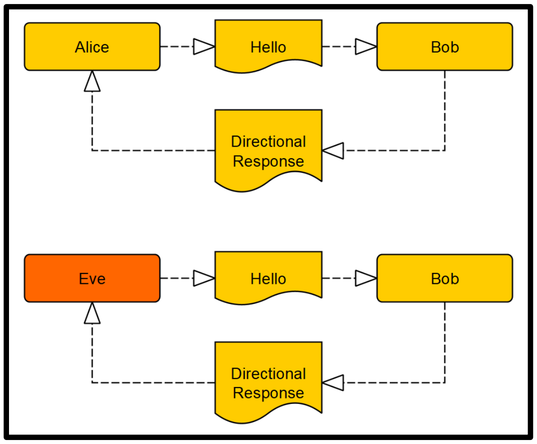


Figure 10. Simple Connection Request Process

2. Unique Authorization Code and Encryption

The simple "Hello" scenario demonstrates the need for a secure connection request to contain unique information. If we replace a simple "Hello" with an identifier unique to Alice, and Eve does not have knowledge of that identifier, then we can reduce the likelihood of Eve soliciting a response from Bob (Figure 11). However, if Eve ever captures the unique authorization code (AuthCode) for Alice through eavesdropping, she can use that code to craft a valid connection request in the future (Figure 12). This means protection is required to prevent Eve from being able to easily ascertain the AuthCode value. This can be accomplished by encrypting the message with a single pre-shared key that is shared by all devices in the scenario. This pre-shared key should not be confused with unique, device specific keys generally used in 5G NR connections, and exists only for use during this initial connection request.

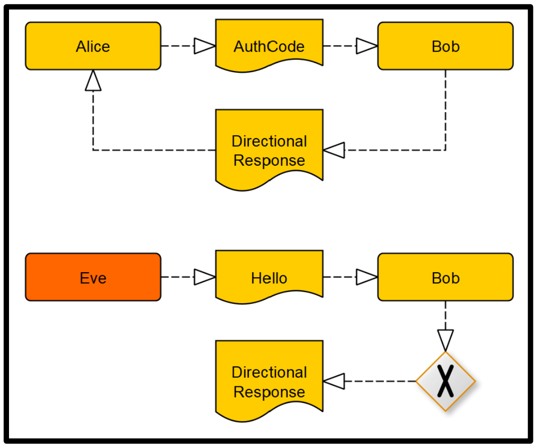


Figure 11. Connection Request Using Unique AuthCode

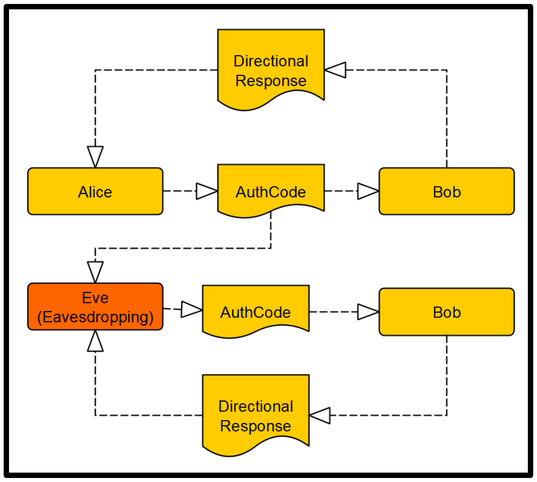


Figure 12. Eve Capturing AuthCode During Connection Request

3. Brute Force Attack

Even if Eve does not obtain a valid AuthCode through eavesdropping, she can create one via brute-force methods. This process would involve Eve cycling through possible AuthCode values until she randomly encounters a valid value, as seen in Figure 13. This situation indicates the need for an AuthCode long enough such that the ratio of valid values to all possible values is sufficiently low.

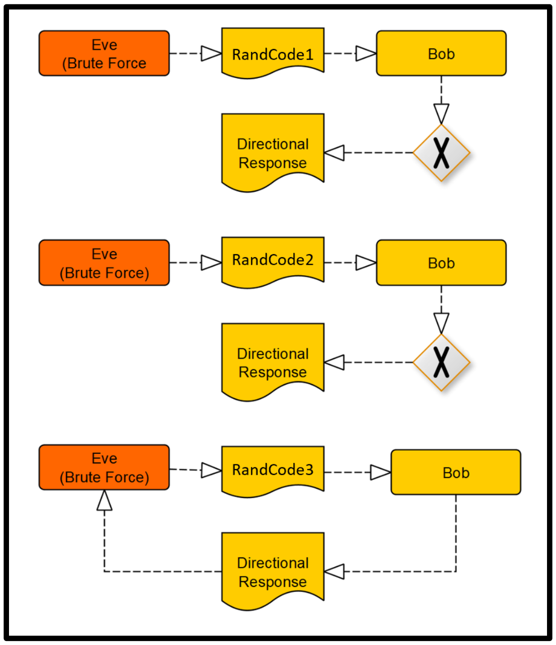


Figure 13. Eve Brute Force Solicitation Process

4. Capture of Signal

If Alice sends out an encrypted solicitation request, and Eve detects she may still be able to capture it and use it to craft a valid connection request from Bob's perspective without ever needing to gain access to the unencrypted information (Figure 14). This situation indicates the need for a nonce to be included in the connection request. A nonce, which is shorthand "a number used only once," is a number included in a message that once received is stored by the receiver. Should that message be captured and reused in a replay attack, the recipient can compare the nonce of the replay message to previously received nonces to determine if the message is original or the product of a replay attack. This nonce prevents Eve from being able to reuse the captured signal to solicit a response from Bob.

However, a nonce alone is not sufficient, as Bob must receive Alice's original message to be able to capture and store the nonce to prevent Eve from being able to reuse Alice's original message. This means that the nonce should be replaced by a time stamp, which itself can also act as a nonce. This allows Bob to determine whether that specific connection request has been previously received, or if he never received the original request, he could determine when the request was made and whether it falls within an acceptable time window (Figure 15). The use of an accepted time window for connection requests requires the systems to be previously time-synchronized.

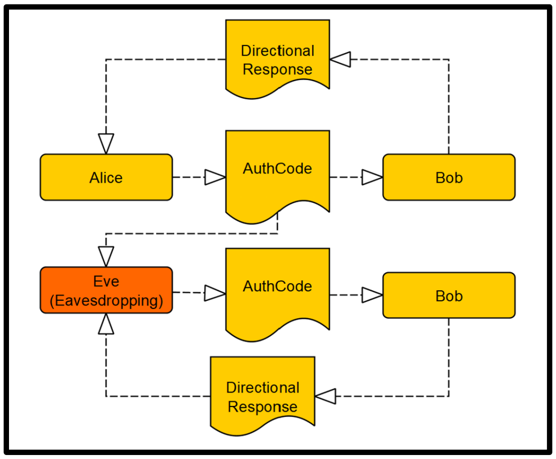


Figure 14. Eve Captures and Replays Valid Connection Request

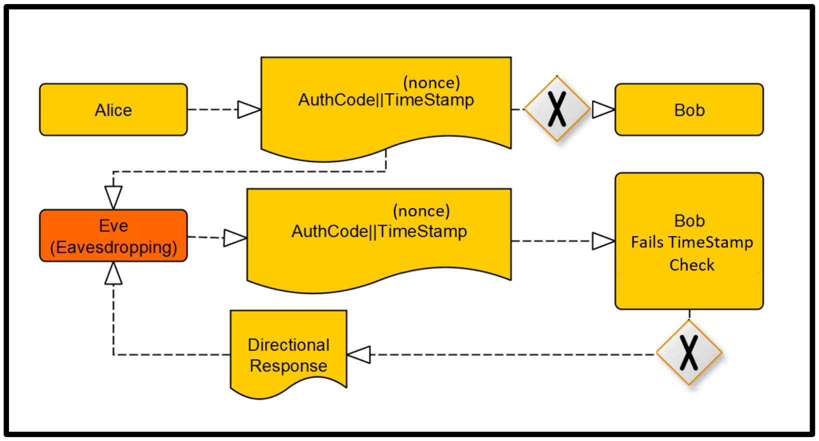

Alice
(nonce) AuthCode||TimeStamp
Bob
Eve (Eavesdropping)
(nonce) AuthCode||TimeStamp
Bob Fails TimeStamp Check
Directional Response

Figure 15. Result of Time Stamp Concatenated with AuthCode

5. Connection Request/Reply Summary

The preceding section detailed attack methods Eve can use to solicit a response from Bob. However, the same methods could be applied to solicit a response from Alice, meaning that both a connection request and a connection reply must contain specific attributes to prevent Eve from being able to solicit a response from either Bob or Alice.

For the solution proposed in this work, a connection request and reply must have four distinct properties to decrease the likelihood of Eve being able to solicit a response.

1. A connection request must use an AuthCode unique to the requesting Alice.

2. A connection request payload must be encrypted to prevent Eve from determining valid AuthCodes for future use.

3. A connection request must be of sufficient length such that Eve cannot be successful in soliciting a response via brute-force means. It is important to note this length requirement is affected by the use of a time stamp, as the smaller a valid time stamp window becomes, the fewer random requests can be generated within that window.

4. A connection request must have a nonce in the form of a time stamp to increase protection against replay attacks and increase the difficulty of a brute-force attack.

C. CONNECTION REQUEST/REPLY STRUCTURE

Figure 16 illustrates the proposed connection request and connection reply structure, which consists of two basic elements: the preamble and the payload. The preamble is primarily used for detection, synchronization, and DOA estimation, whereas the payload is used for authentication. The payload contains three sub-parts: AuthCode, time stamp, and error detection and correction (EDAC). Each element of the connection request/reply will be discussed in greater detail individually in the subsequent sections.

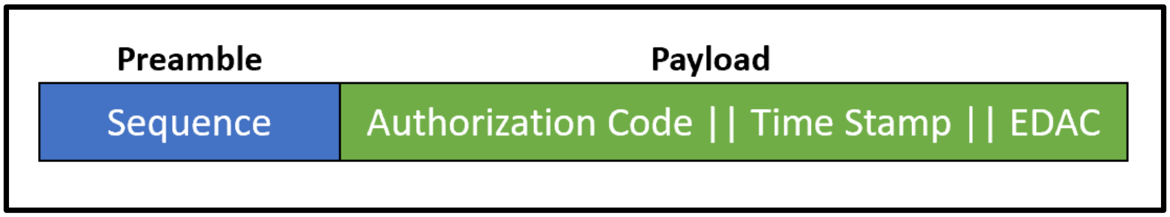
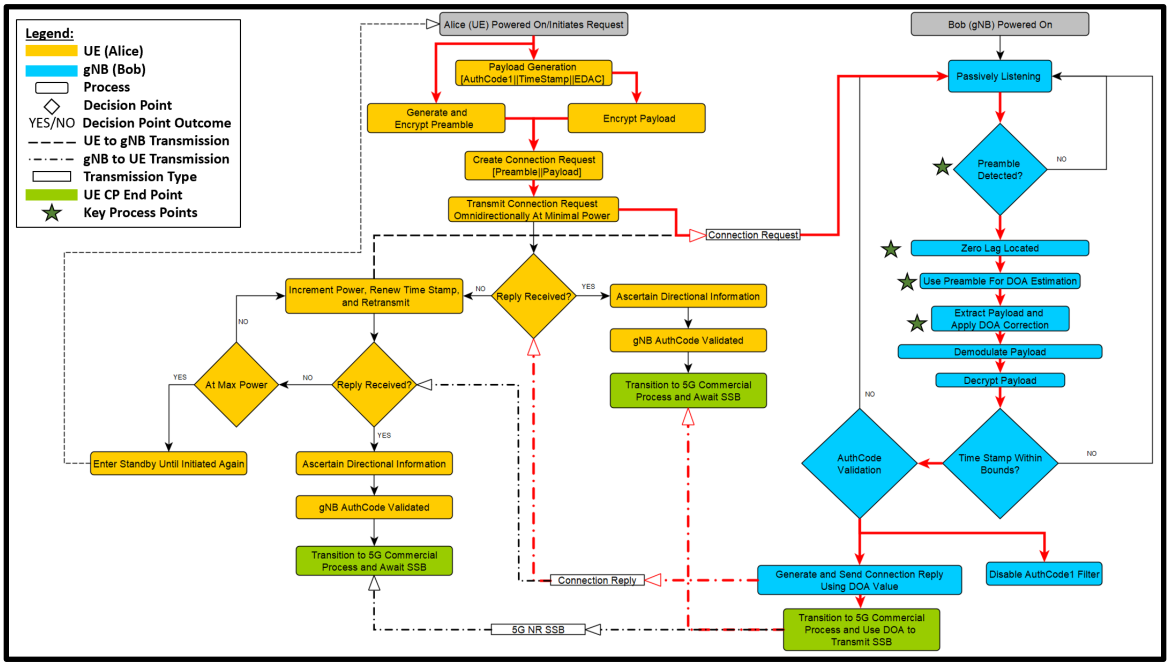


Figure 16. UECP Connection Request/Reply Structure

D. FULL UE-SIDE CONNECTION PROCESS AND CRITICAL PROCESS POINTS

The full UE-side connection process can be seen in Figure 17. Due to the presence of various decision points and branch process paths, a successful first-time connection will be explained first, and the various outcomes of decision points will be explained after. Critical process points are identified with a star in the process diagram and constitute the major processes that will be examined in depth later in this work.



Legend:
UE (Alice)
gNB (Bob)
Process
Decision Point
YES/NO Decision Point Outcome
UE to gNB Transmission
gNB to UE Transmission
Transmission Type
UE CP End Point
Key Process Points
Alice (UE) Powered On/Initiates Request
Payload Generation [AuthCode1||TimeStamp||EDAC]
Generate and Encrypt Preamble
Encrypt Payload
Create Connection Request [Preamble||Payload]
Transmit Connection Request Omnidirectionally At Minimal Power
Connection Request
Reply Received?
NO
YES
Increment Power, Renew Time Stamp, and Retransmit
Ascertain Directional Information
gNB AuthCode Validated
Transition to 5G Commercial Process and Await SSB
At Max Power
Reply Received?
Enter Standby Until Initiated Again
Ascertain Directional Information
gNB AuthCode Validated
Transition to 5G Commercial Process and Await SSB
Connection Reply
5G NR SSB
Bob (gNB) Powered On
Passively Listening
Preamble Detected?
Zero Lag Located
Use Preamble For DOA Estimation
Extract Payload and Apply DOA Correction
Demodulate Payload
Decrypt Payload
Time Stamp Within Bounds?
AuthCode Validation
Generate and Send Connection Reply Using DOA Value
Disable AuthCode1 Filter
Transition to 5G Commercial Process and Use DOA to Transmit SSB

Figure 17. UECP Full Process Diagram

A successful first-time connection process would proceed as follows (bolded red path in Figure 17):

1. gNB is manually powered on.

2. UE is manually powered on.

3. UE generates and encrypts the payload, which is a concatenation of the UE unique AuthCode, time stamp, and EDAC.

4. UE generates and encrypts the preamble.

5. UE generates the connection request which is the concatenation of the encrypted preamble and encrypted payload.

6. UE omnidirectionally transmits the connection request at minimum power.

7. gNB is passively listening for a connection request.

8. gNB detects the preamble (Critical process – Detection and Synchronization).

9. gNB finds preamble zero lag location (Critical process – Detection and Synchronization).

10. gNB uses preamble to conduct UE-to-gNB DOA estimation (Critical process – Direction of Arrival Estimation).

11. gNB extracts payload from connection request and uses UE-to-gNB DOA estimate to correct the payload (Critical process – Payload Correction).

12. gNB demodulates payload.

13. gNB decrypts payload.

14. gNB verifies request time stamp is within the acceptable time window.

15. gNB validates UE AuthCode against whitelist.

16. gNB disables UE AuthCode to reduce likelihood of successful replay attacks.

17. gNB generates a connection reply (same process as UE connection request).

18. gNB transmits connection reply using UE-to-gNB DOA estimate.

19. UE receives a connection reply and conducts gNB-to-UE DOA estimation.

20. UE validates the gNB’s AuthCode.

21. gNB transmits 5G NR SSB using UE-to-gNB DOA estimate and transitions to 5G NR initial access process.

Decision point outcomes (from Figure 17):

- UE does not receive a connection reply after the first connect request – UE increments transmission power and repeats the process.

- UE fails to receive connection reply after max power connection request transmission – UE enters standby until connection process is manually reinitiated.

- gNB does not detect preamble – gNB continues passively listening.

- Time stamp is not within bound – gNB returns to passive listening.

- AuthCode validation fails – gNB returns to passive listening.

1. Detection and Synchronization

Limiting the power of the incoming signal is not a concern in most wireless signal connection methods. However, in this scenario, the greater the energy of the connection request, the greater the likelihood of detection by Eve. This problem warranted a new approach to detecting and synchronizing signals at very low signal-to-noise ratios (SNRs). The key to creating an effective method for detection and synchronization without increasing transmitted energy involves increasing characteristics of the system that increase the likelihood of successful connection without increasing the likelihood of detection, such as antenna array size and connection request detection method.

2. Direction of Arrival Estimation

Direction of arrival estimation is a critical process in that it serves two purposes within UECP: determining response direction, and payload correction. DOA estimation involves applying one of several DOA estimation processes to a received signal to ascertain the direction from which the signal came. The DOA estimate is then used to steer the connection response from the gNB to the UE. The greater the fidelity of the DOA estimate, the more precisely the gNB can steer the response signal. This increases the likelihood the UE will receive the connection reply while also reducing stray emissions.

3. Payload Correction

The DOA estimate is also used to correct the payload before demodulation. Array reception of a signal requires that each element's received value needs to be phase-corrected before demodulation to maximize received gain and reduce the bit error rate (BER). This is especially true at very low SNRs where the BER can quickly become high enough that information cannot be reliably received.

E. KEY PERFORMANCE INDICATORS

Key performance indicators are developed from previous discussions in this work and will be used in the analysis process as the basis for decisions about process elements. The key performance indicators are as follows:

- Probability of detection and synchronization on the preamble.
- DOA estimation accuracy.
- BER of payload.

F. CONSTRAINTS, ASSUMPTIONS, DESIGN SPACE

As previously stated, this research is only intended to be applied to a specific use case consistent with a real-world scenario. Within the scenario and use case certain constraints and assumptions exist, along with practical considerations, that must be accounted for during analysis and utilization of this process. Additionally, a design space is intended to scope the value range of certain key parameters used throughout this research.

1. Constraints

- The proposed process must be compatible with 5G NR technology, but not limited to the current physical systems in use (e.g., array sizes).
- Process must not disrupt commercial 5G NR processes beyond removing the SSB sweep process.

2. Assumptions

- gNB and UE have a pre-shared key for encryption and decryption.
- There are no multipath effects to consider.
- Signal-to-interference noise ratio (SINR) is negligible.
- No two connection requests will occur at the same time.
- Relative motion between the UE and gNB is negligible.
- gNB and UE internal clocks have previously been synchronized (This is a requirement for the utilization of an acceptable time window, but time synchronization is not facilitated by UECP.).

3. Design Space

- SNR values at the receiver range from -20 dB to 0 dB.
- DOA values range from -60º to 60º, with 0º representing normal to the array.
- Array analysis is done solely in 2-D.
- Preambles will be transmitted in binary phase-shift keying (BPSK), and payloads will be transmitted in quadrature phase-shift keying (QPSK).

THIS PAGE INTENTIONALLY LEFT BLANK

V. DETECTION AND SYNCHRONIZATION

A. PURPOSE

1. Detection of Request

The detection of a connection request is primarily facilitated by the preamble. The gNB will always be passively receiving, matched filtering, and comparing the result to a threshold to determine if the expected preamble was detected. Once a request is detected, the gNB captures and stores the received signals of both the preamble and payload for later operations.

Many communications systems use unique preambles for each device with low cross-correlation characteristics to facilitate the reception and segregation of multiple signals simultaneously [14]. Because UECP is only utilized a single time at the initial establishment of a connection, a common preamble is shared by all UEs and would not be used again unless a new connection needed to be established. With UECP designed to support a small number of users, we will assume the likelihood of multiple connection requests occurring at precisely the same is negligible. This means the cross-correlation properties of a preamble are no longer relevant and having only a single signal used allows for detection at lower SNR.

2. Synchronization for Payload Capture

One critical element of the process is detecting the center lag location of the preamble to ensure the payload is properly captured, demodulated, and decrypted. If the connection request is detected but the gNB is not able to properly synchronize with the incoming signal both the DOA estimate and payload information will be degraded, with the primary concern being the payload degradation since those values are not correlated, but rather compared to known values to validate the authenticity of the request.

B. SELECTION CRITERIA

From all previous conversations in this work, certain criteria emerged that are relevant to the selection of a preamble.

1. Low Autocorrelation for Non-Zero Lag

The need for the gNB to properly synchronize on the connection request means that the preamble must have low autocorrelation for non-zero lag. For

$$R[n] \triangleq \langle x[m]x[m+n] \rangle, \tag{1}$$

$R[n]$ must be low at all non-center lag points, where $\langle \ \rangle$ is the time average over m, which ensures that the center lag time sample is clearly identifiable [15].

Using a preamble with high autocorrelation for non-zero lag increases the likelihood of the gNB orienting on a sample that is not center when additive white Gaussian noise (AWGN) is present. This can be seen in Figure 18 where Sequence 1 produces low side lobes, and Sequence 2 produces much higher sidelobes. Once AWGN is introduced, the higher side lobes in Sequence 2 cause the autocorrelation function (ACF) to exceed the given threshold at a point that does not represent full overlap, which would result in the payload not being properly captured.

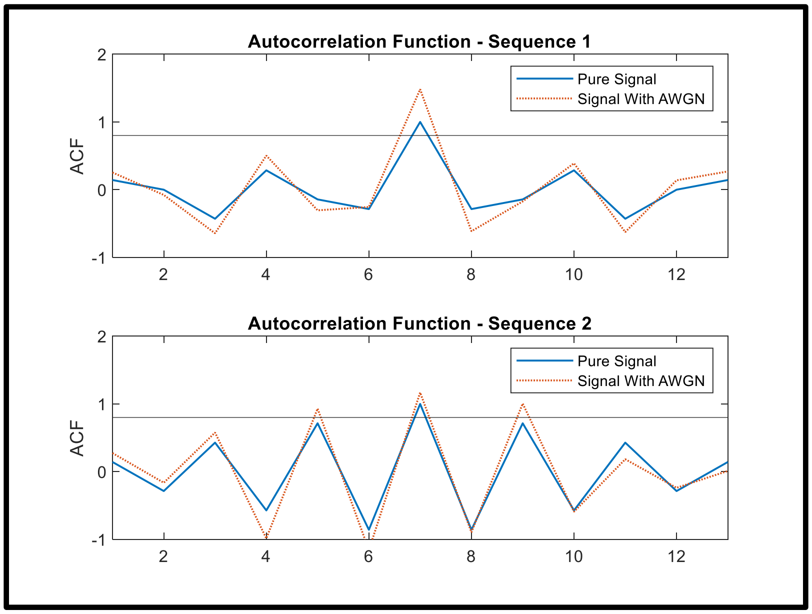


Figure 18. ACF Sidelobe Illustration

2. Length of Preamble

The longer a preamble is, the greater the processing gain and resilience to the effects of AWGN in the receiving system, but this comes at the cost of greater energy being emitted into the environment. UECP intends to reduce the amount of stray energy emitted, meaning the preamble length should be minimized while still fulfilling its central requirement of detection and synchronization.

3. Predictability

Although Eve possesses knowledge of how the system works, the presence of a pre-shared key means that important information can be obscured from her. Although the preamble is not used for UE or gNB authentication, it could be used by Eve to occupy critical resources in the gNB and prevent the detection of a valid connection request. Although jamming and denial of service (DOS) are not characteristics of the attack model, they are worth consideration due to the use case, and reducing the predictability of the preamble directly affects the ability of Eve to do either.

C. PREAMBLE TYPE PERFORMANCE

Three sequence types were tested for suitability within UECP: m-sequences, Zadoff-Chu (ZC), and randomly generated sequences. M-sequences and ZC sequences are two well-known sequence types commonly used as preambles due to their low sidelobe levels when autocorrelated [16]. It is worth noting the existence of the Barker sequence, which is another sequence type that could be considered for comparison. However, the desire for the system to operate at very low SNRs and the Barker sequences being limited to a sequence length of only 13 [17] means they are incapable of providing the processing gain required to be suitable for UECP.

1. M-Sequences

The following section is intended only as an introduction to m-sequences, and a more comprehensive and detailed discussion of use and correlation attributes can be found in *Introduction to Digital Mobile Communications* by Yoshihiko Akaiwa [18].

M-sequences are recursive binary sequences generated using linear feedback shift registers and are often used as preambles in communications systems due to the low sidelobe levels of the ACF. This behavior can be seen in Figure 19 with an $N = 15$ m-sequence.

Additionally, the normalized periodic ACF, when multiple m-sequences are sent in succession, exhibits a very specific behavior wherein the correlation value at full overlap is

$$R_m(n) = \begin{cases} 1 & \text{if } n = 0 \\ -\dfrac{1}{N} & \text{if } 0 < n < N \end{cases}, \tag{2}$$

where *n* represents lag and *N* is the total length of the sequence. This attribute can be seen for an $N = 15$ m-sequence in Figure 20. The resulting ACF is a very clear correlation profile in the receiving system but requires multiple sequences to be transmitted in succession, increasing the overall signal energy, an attribute not desirable for UECP.

A different approach would be to expand the matched filter impulse response to be a periodic m-sequence, however expanding the filter size increases the noise energy within the system, which is also not desirable due to the desire for UECP to function at low SNRs.

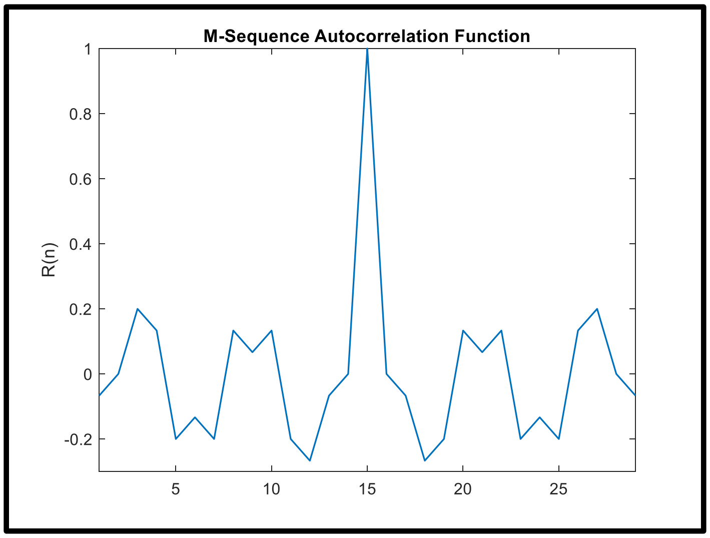


Figure 19. Autocorrelation of Single Period M-Sequence

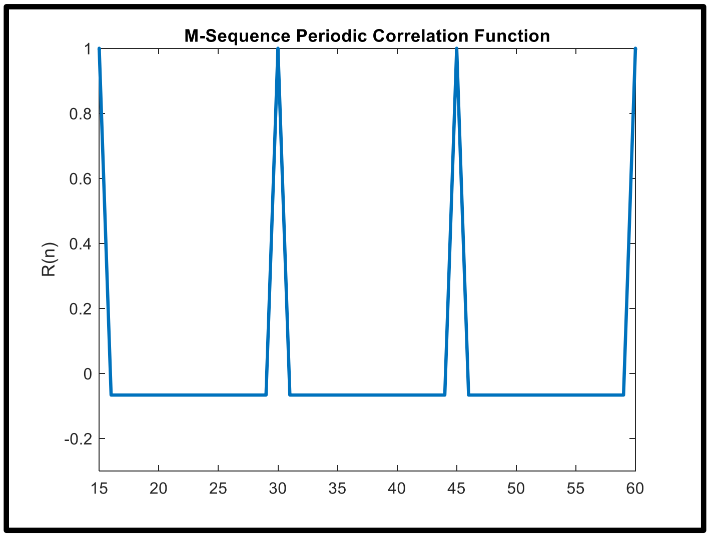


Figure 20. Autocorrelation of Periodic M-Sequence

2. Zadoff-Chu Sequences

This section is again intended only as an introduction to ZC sequences, and further discussion concerning the mathematics and application of ZC sequences can be found in *Preamble Detection Based on Cyclic Features of Zadoff-Chu Sequences for Underwater Acoustic Communications* by Qinyuan Tan and Yiyin Wang [19].

ZC sequences are another sequence type commonly used as preambles for communications systems due to low autocorrelation and periodic behavior of the sequence when a matched filter is used. The primary difference between ZC and m-sequences is that ZC utilizes complex values which result in a zero value at all points outside full overlap. The autocorrelation of a $N = 15$ ZC sequence can be seen in Figure 21. The periodic correlation value (when multiple sequences are sent in succession) is

$$R_{zc}(n) = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } 0 < n < N \end{cases}, \tag{3}$$

where n represents lag and N is the total length of the sequence. The periodic response behavior of an $N = 15$ ZC sequence can be seen in Figure 22.

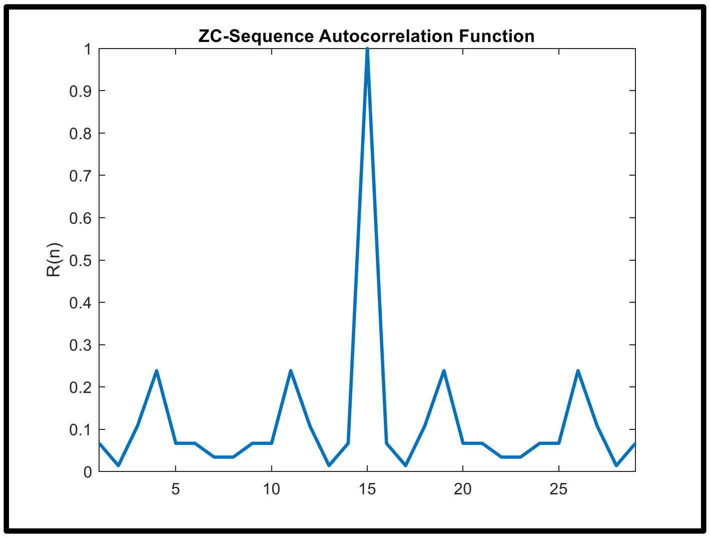


Figure 21. Autocorrelation of Single Period ZC-Sequence

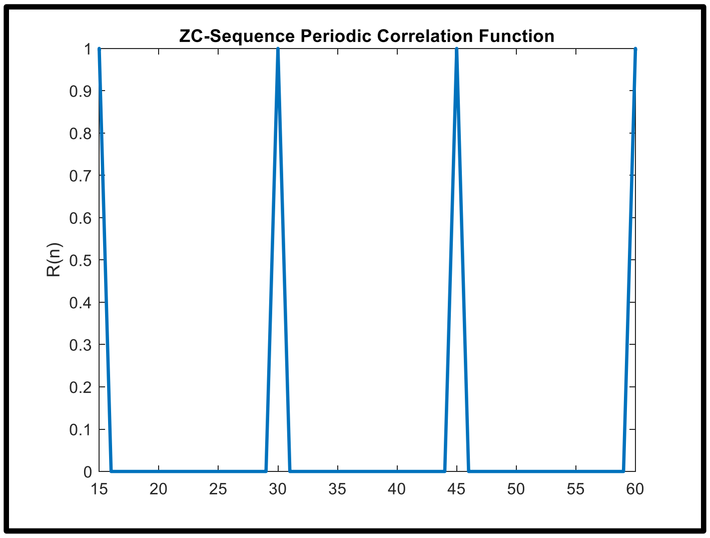


Figure 22. Autocorrelation of Periodic ZC-Sequence

3. Random Sequences

The final sequence type to be tested is a random binary sequence. The reason a random binary sequence is being examined is that it would allow a set preamble sequence to be masked using a single pre-shared key across all devices. Eve would need to capture the preamble encrypted with the pre-shared key before being able to falsify a detection within the gNB, and that captured preamble would only be valid for the duration of the time the pre-shared key is valid. Random sequences do not possess the same attributes of the m-sequences or ZC sequences. Generally, they do not possess low sidelobes when autocorrelated, as seen in Figure 23.

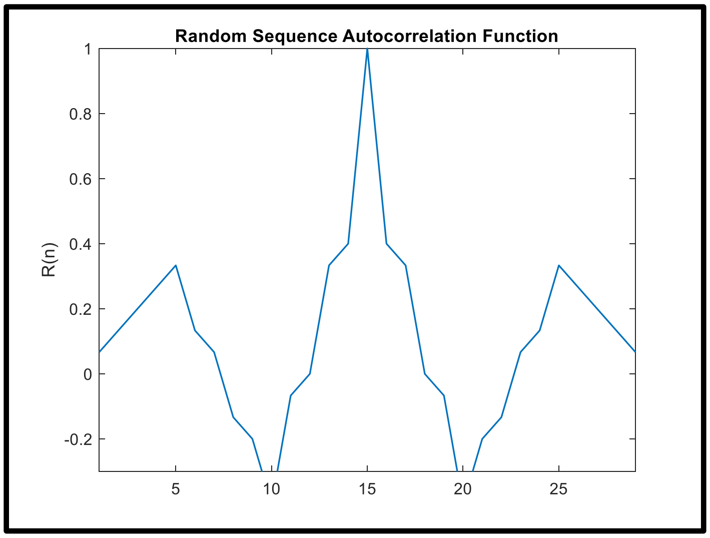


Figure 23. Autocorrelation Random Sequence (1 Realization)

Additionally, randomly generated sequences generally do not have low cross-correlation characteristics and do not exhibit an ideal behavior when periodically correlated (Figure 24). However, the two later characteristics, cross-correlation, and periodic correlation, are not of great concern since we assumed probability of simultaneous requests is low, and periodic correlation response requires multiple sequence transmissions which are not desired for our system. The critical point in analyzing the suitability of using a random sequence is determining the impacts of higher side lobes on the ability of the gNB to detect and synchronize with the incoming signal.

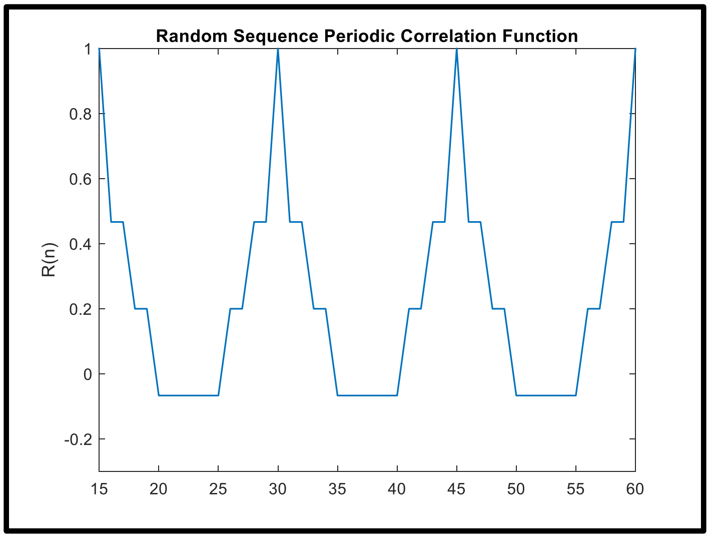


Figure 24. Autocorrelation of Periodic Version of Random Sequence (1 Realization)

D. PERFORMANCE AND COMPARISON OF SEQUENCE TYPES

1. Process and Simulation Explanation

The analysis of preamble types was done using a simulation built within *MATLAB*, and testing was done utilizing Monte Carlo simulations. Figure 25 shows the process flow for the simulation and step-by-step explanations are provided below.

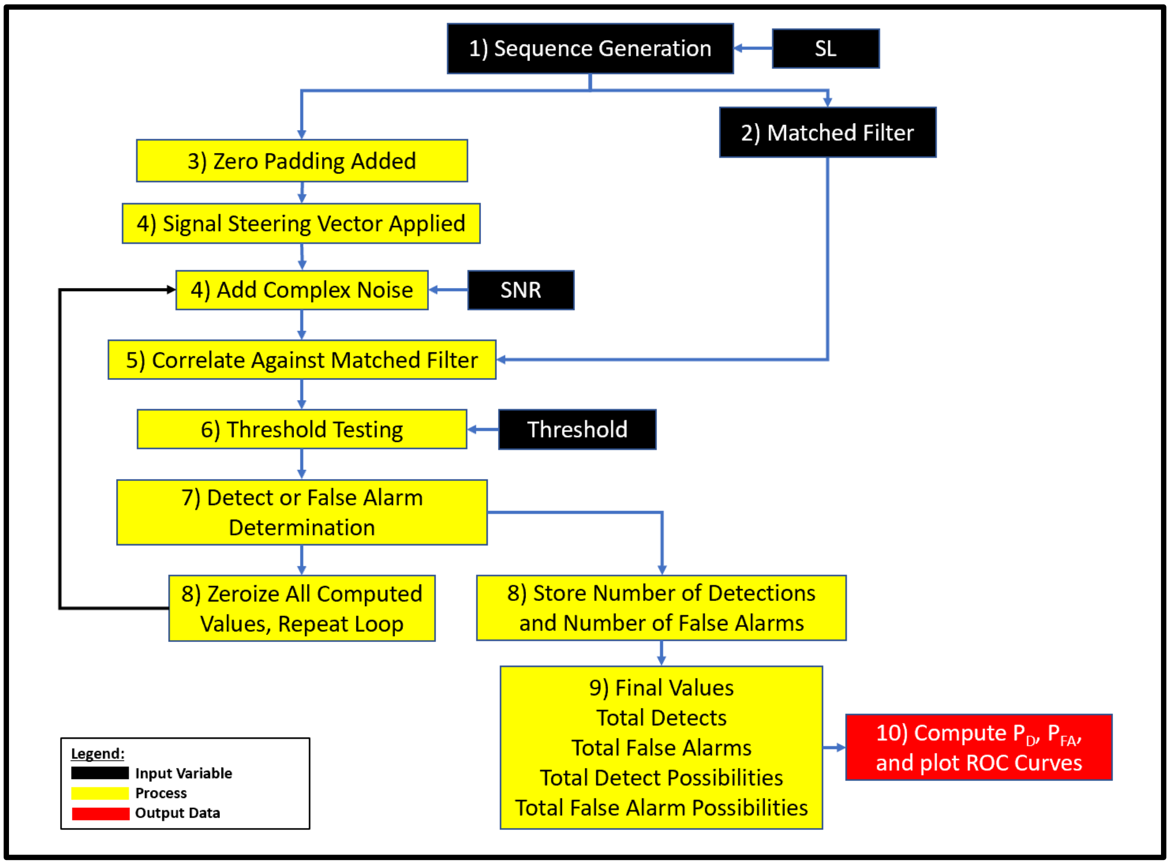

1) Sequence Generation
SL
2) Matched Filter
3) Zero Padding Added
4) Signal Steering Vector Applied
4) Add Complex Noise
SNR
5) Correlate Against Matched Filter
6) Threshold Testing
Threshold
7) Detect or False Alarm Determination
8) Zeroize All Computed Values, Repeat Loop
8) Store Number of Detections and Number of False Alarms
9) Final Values
Total Detects
Total False Alarms
Total Detect Possibilities
Total False Alarm Possibilities
10) Compute P_D, P_{FA}, and plot ROC Curves
Legend:
⬛ Input Variable
🟨 Process
🟥 Output Data

Figure 25. Preamble Testing Simulation Process

1. Sequence Generation: Depending on the type of sequence being tested, an m-sequence, ZC sequence, or random sequence was generated which will be expressed as y .

2. Matched Filter: The generated sequence from Step 1 was then stored for use as a matched filter impulse response during detection. The impulse response is the sequence reversed in time and can be expressed as $h_n = y_{N-n}$.

3. Zero Padding Added: Because the matched filter correlation against noise would have an impact at all points outside full signal and matched filter overlap, the system needed to simulate and capture that behavior. To

accurately represent that situation, zero padding of length equal to the sequence was added to both the front and the back of the generated sequence. This padding provided a realistic scenario where the matched filter would be correlated against noise only, as well as a preamble signal with the addition of noise. Since this process only occurs a single time, and a preamble will not always be present, it was important to determine the system characteristics with only noise present. The result of this step is the creation of y', which is the concatenation of zero padding, y, and zero padding.

4. Adding Complex Noise: Complex AWGN was generated using

$$\sigma_n^2 = \left(10^\wedge\left(\frac{-SNR}{10}\right)\right)P_s, \tag{4}$$

where σ_n^2 represents the noise variance, *SNR* is the signal-to-noise ratio of the given iteration in dB, and P_s is the signal power (which was held at 1 throughout all testing). The complex noise was then added to the original zero padded signal to produce $x = y' + noise$. *SNR* was varied throughout the series of simulations

5. Correlate Against Matched Filter: The matched filter impulse response saved in Step 2 was then convolved with the padded, noisy signal denoted as *x*. This correlation was computed using

$$R_{xh}(i) = \sum_{n=0}^{N-i-1} x(i-n)h(n) \text{ for } i \geq 0, \tag{5}$$

where *N* is the total signal length, *x* is the noisy signal, and *h* is the matched filter's impulse response.

6. Threshold Testing: A hypothesis test was applied to the correlation values produced in Step 6 to find all locations where $R_{xh}(i)$ exceeded a threshold. The hypothesis test used is

$$\begin{aligned} &H_{\gamma 0} : R_{xy}(i) < \gamma \\ &H_{\gamma 1} : R_{xy}(i) \geq \gamma \end{aligned}, \tag{6}$$

where $H_{\gamma 0}$ is no signal present, $H_{\gamma 1}$ is signal present, and γ represents the threshold value used. Because the outputs of this simulation were the probability of detection (P_D) and probability of false alarm (P_{FA}) in the form of a receiver operating characteristic (ROC) curve, the γ value was varied through the iterations.

7. Detect or False Alarm Determination: A second hypothesis test was applied to all values meeting the $H_{\gamma 1}$ test from Step 6. This was used to determine if the $H_{\gamma 1}$ value occurred only at the full overlap of the preamble and matched filter, which would mean the signal was both detected and synchronized. The hypothesis test used is

$$\begin{aligned} &H_{S0} : i \neq 2^m \\ &H_{S1} : i = 2^m \end{aligned}, \tag{7}$$

where i represents the location(s) of $H_{\gamma 1}$ found in Step 6, H_{S0} represents synchronization did not occur, H_{S1} represents synchronization did occur, and m is the power of 2 used to create the original sequence length. This hypothesis test is not standard and applies only to the specific location of full overlap between signal and matched filter impulse response as designed in this simulation.

8. Zero All Computed Values, Repeat Loop/Store Calculated Data: This step involved two separate processes, saving relevant computed values, then clearing all computed values to prepare for the next iteration of the Monte Carlo simulation. The values stored were the computed number of detections and false alarms, all others were cleared, and the only values held for the next iteration were the original sequence, matched filter impulse response, *SNR*, and γ values.

9. Final Values: This MC simulation was nested within multiple *for* loops within *MATLAB* to allow for multiple *SNR* and γ combinations to be tested to fully define the ROC curves. At the conclusion of each MC simulation the relevant values from each iteration were combined to determine the final values for each $SNR-\gamma$ combination.

10. Estimate P_D and P_{FA} Values: At the conclusion of each $SNR-\gamma$ combination, the sum of all detects and false alarms were used, along with all possible detect and false alarm opportunities to produce the P_D and P_{FA} estimates. The equations to solve for P_D and P_{FA} were

$$P_D = \frac{\sum_{i=0}^{M} D(i)}{M} \tag{8}$$

and

$$P_{FA} = \frac{\sum_{i=0}^{M} F_A(i)}{[2(2^m)-1]M}, \tag{9}$$

where *D* represents whether a detect occurred (a value of 1 for yes and a value of 0 for no), F_A represents if false alarms occurred (again, a value of 1 for yes and a value of 0 for no) on any given Monte Carlo iteration, and *M* is the number of Monte Carlo simulations conducted for a given $SNR-\gamma$ combination. Each iteration of the Monte Carlo simulation contained only a single opportunity for detection (detection, in this case, is defined as the combination of detection and synchronization), and a variable number of false alarm opportunities depending on the original sequence length. For any single iteration of the Monte Carlo simulation, there existed $2(2^m)-1$ possible false alarms, with the -1 value in the denominator of Equation 9 accounting for the single valid detection location. This value is then scaled by the total number of Monte Carlo iterations for a given $SNR-\gamma$ combination to determine total false alarm opportunities.

2. Probability of detection and Synchronization Results

Although Monte Carlo simulations were run for SNR values between -20 dB and 0 dB, at 5 dB increments, with sequence lengths (*SL*) of 2^m*-1* with $m=[3,7]$, and many plots created and studied, only a select number will be contained within this report. These plots are specifically chosen to demonstrate trends and illustrate important points that were discovered. The plots not contained in this work show the same behavioral trends and reinforced what will be discussed.

Figure 26 and Figure 27 show the ROC curves at $SNR=0$ dB, at two distinct *SL*s, 7 (Figure 26), and 127 (Figure 27). Several important observations can be seen between these two figures. First, as *SL* is increased, the processing gain results in improved ROC. This is the expected outcome as the increase in *SL* results in increased processing gain within the system, thus reducing the impact noise has on the detection process. The second major observation is that the ROC characteristics among all three sequence types are relatively consistent, with m-sequences showing a slight decrease in performance compared to the other two. This disparity, however, does not hold consistent as the *SNR* value decreases, as will be seen in the next set of plots.

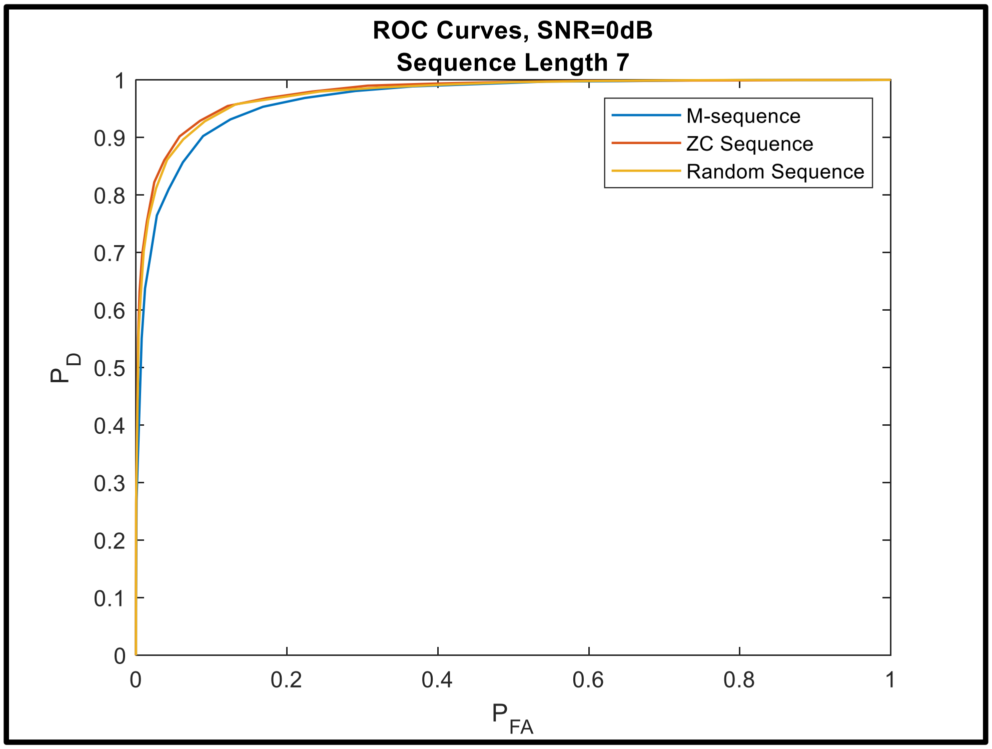


Figure 26. ROC Curve, *SNR* = 0 dB, *SL* = 7

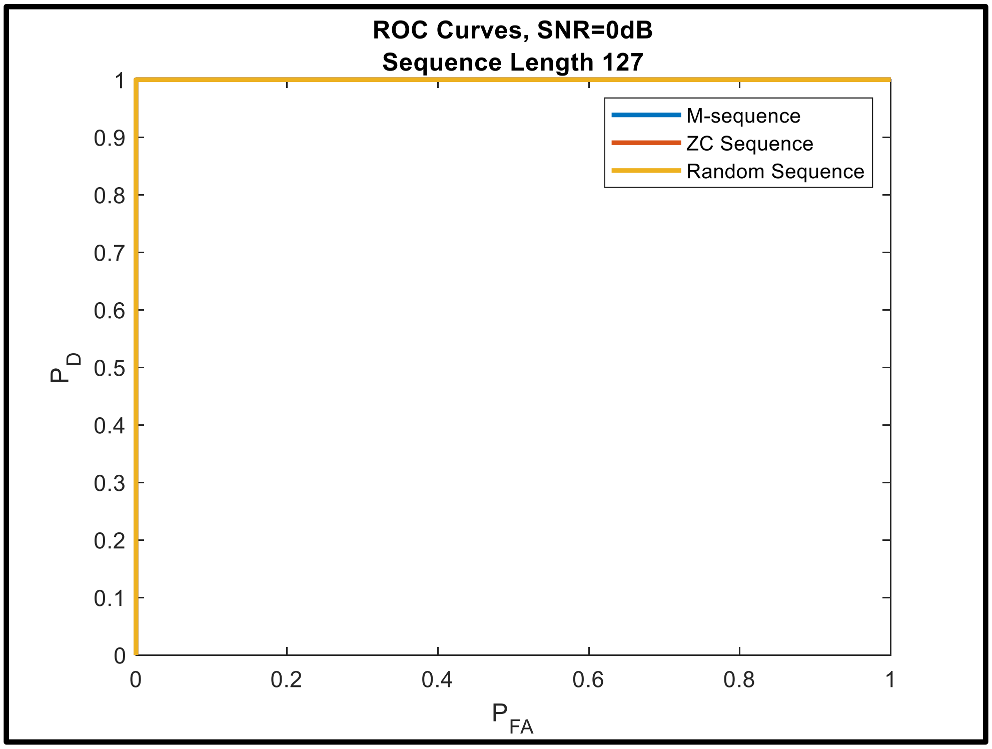


Figure 27. ROC Curve, *SNR* = 0 dB, *SL* = 127

Figure 28 and Figure 29 show the results of the simulation when *SNR* is decreased to -20 dB, with the *SL*s remaining at 7 and 127. There are several major points worth discussing between these two plots. First, as *SNR* decreases, the ROC decreases. As Figure 28 shows, with an *SL* of 7, detection becomes arbitrary. However, if we increase the *SL*, and thus increase processing gain, the ROC increases as well, as seen in Figure 29. The reason this is important to this research is that the impact of increasing *SL* is an increase in signal energy, thus increasing the likelihood of detection of the signal.

The second major point from these figures is that as *SNR* decreases, the performance variation between each sequence type becomes negligible. The results of the comparison between sequence types, specifically the performance of a random sequence compared to m-sequences and ZC sequences in this use case were not expected. This lack of performance separation warranted additional analysis.

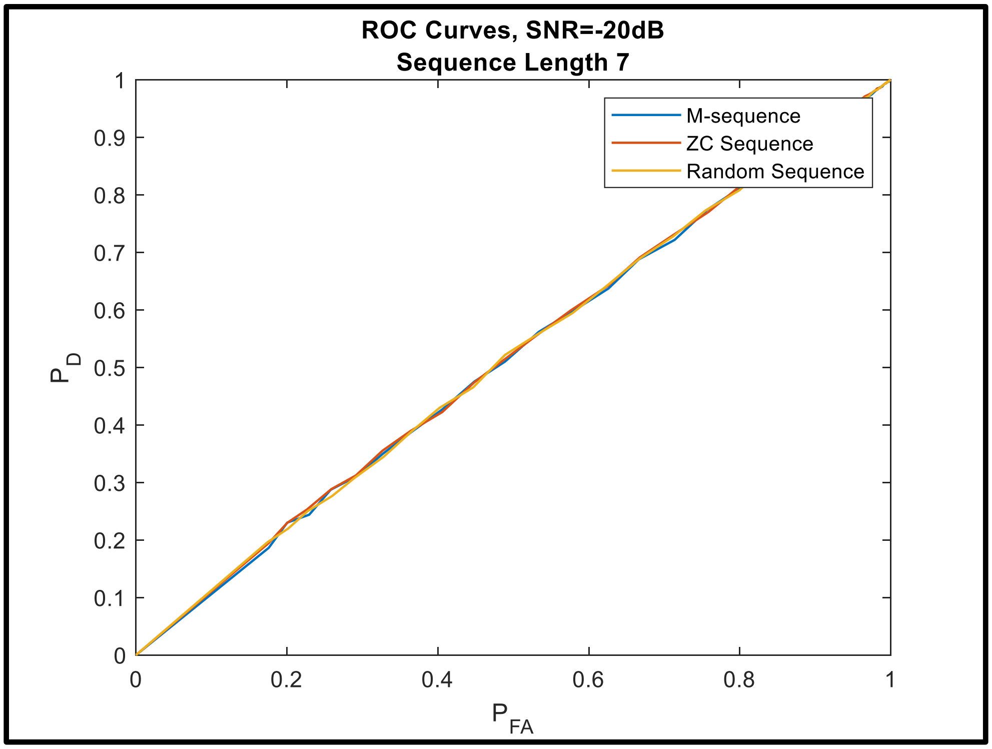


Figure 28. ROC Curve, *SNR* = -20 dB, *SL* = 7

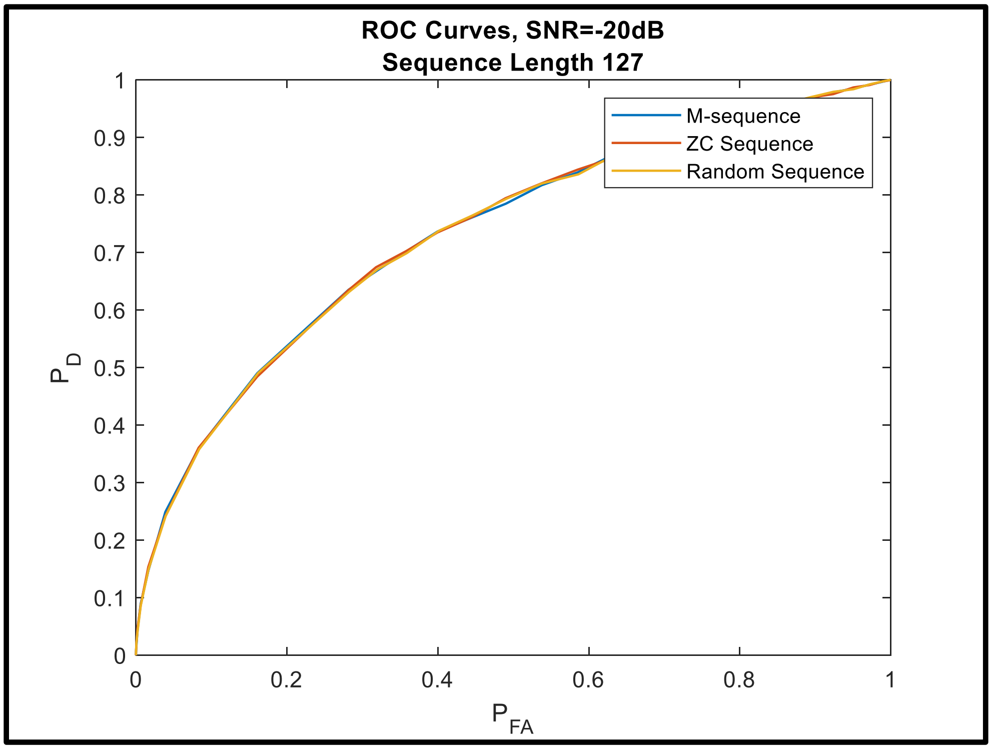


Figure 29. ROC Curve, *SNR* = -20 dB, *SL* = 127

3. Parity Between Sequence Types

As seen in the last section, all sequence types showed essentially equal performance as *SNR* decreased from 0 dB to -20 dB. This was not the expected result, and as such, warranted additional analysis to ensure the results were accurate. The first thing to consider is the autocorrelation results and sidelobes present from each sequence type. ZC and m-sequences are specifically designed to exhibit low side lobes in autocorrelation [16], whereas random sequences possess no such characteristic. Each random sequence will have its own sidelobe profile. Figure 30 shows the autocorrelation results of a random sequence, m-sequence, and ZC sequence. This particular randomly generated sequence shows two dominant side lobes, which, in the presence of noise, should decrease the likelihood of proper detection and synchronization. However, this illustrates only a single realization of a random sequence.

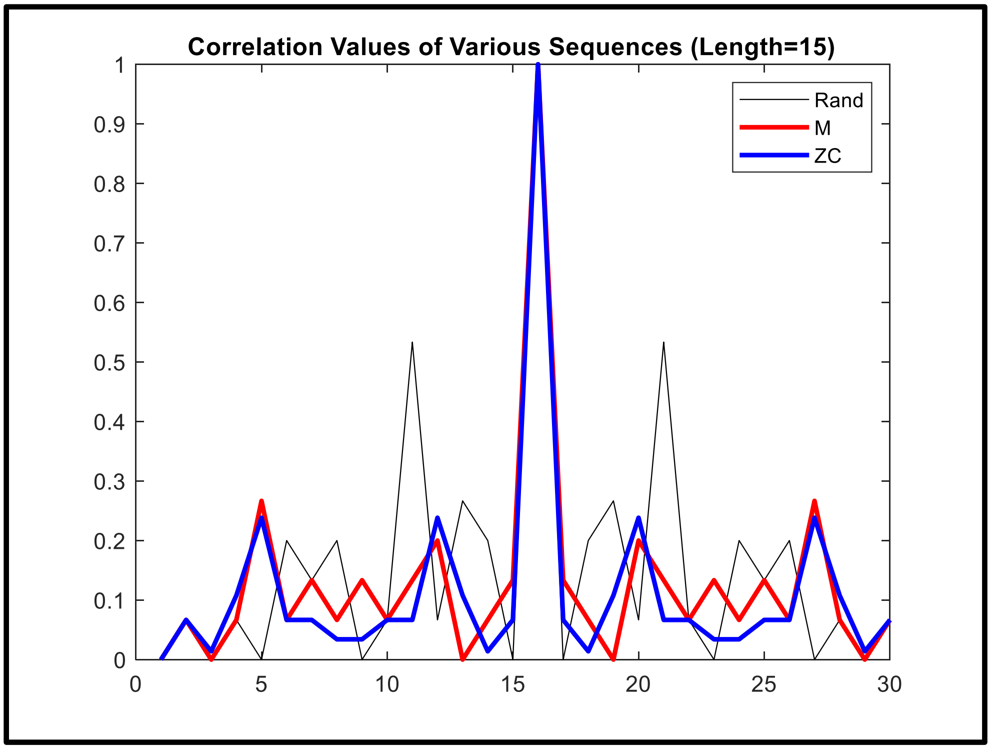


Figure 30. Autocorrelation Values of Various Sequence Types

To better understand the sidelobe behavior of a random sequence, and for illustrative purposes, a thousand realizations of random sequences of length 1023 ($SL = 1023$) were created and autocorrelated, then compared to the autocorrelation results of both ZC and m-sequences. Figure 31 shows the result of that study and several important things were discovered.

First, although ZC sequences generally result in very low correlation values, large sidelobes exist periodically. These large sidelobes present an opportunity for false alarms, and when this particular sequence was run through the detection simulation the result of these sidelobes was clearly visible in the ROC separation between the m-sequence and ZC sequence (Figure 32).

The second observation from Figure 31 is that although random sequences have higher sidelobes than an m-sequence, this plot is effectively showing the maximum sidelobe correlation values of the thousand random sequences in black, and not representative of the behavior of a single iteration.

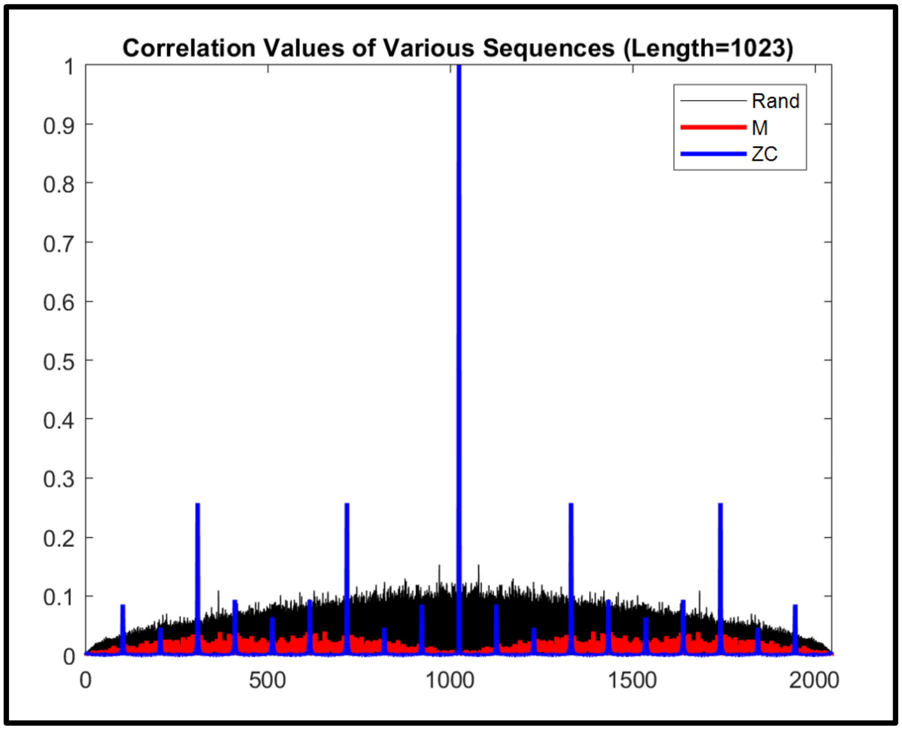


Figure 31. Combined Results of 1000 Random Sequence Autocorrelations

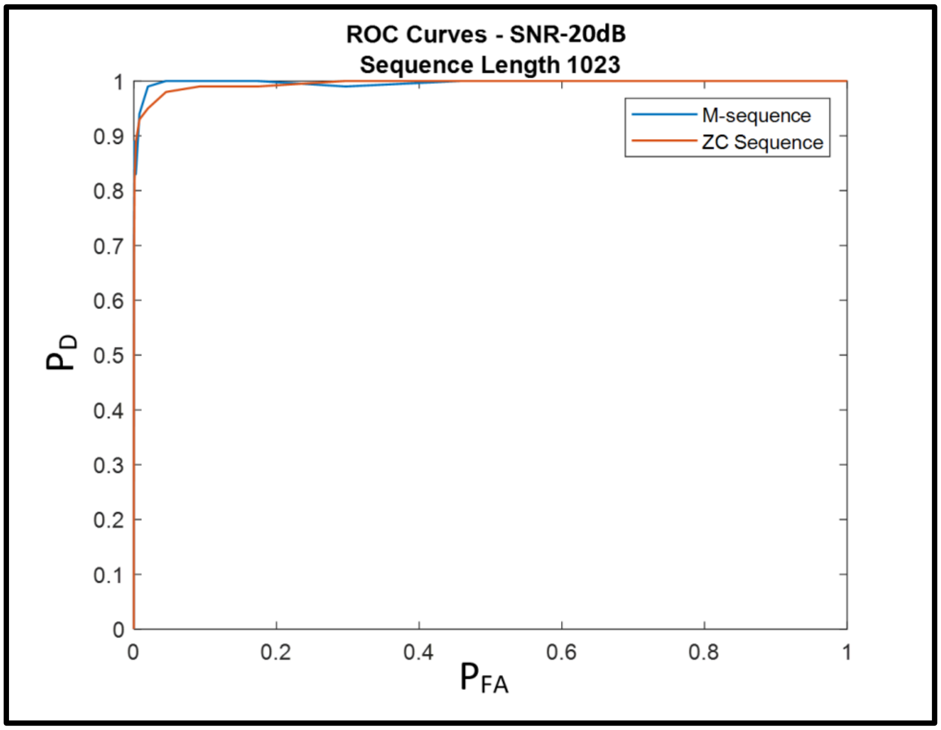


Figure 32. Impacts of Large ZC Sequence Sidelobes on ROC

What becomes clear is that two factors can cause one sequence to perform worse than another. The first, discussed previously, is the presence of unusually high sidelobes, which increases the likelihood that a specific location will cause a false alarm. The second is that the mean of the sidelobes of one sequence is greater than the mean of another, which would increase the likelihood of any random point causing a false alarm.

To better understand how the mean of the sidelobes would affect performance an additional simulation was conducted that measured the mean sidelobe level of each sequence, using one thousand realizations of each sequence's autocorrelation results. Figure 33 clearly shows a separation between the means of each sequence's autocorrelation values, but this separation cannot be used to draw a definitive conclusion about performance. Rather, mean separation compared to noise present is needed to determine performance. Figure 33 shows that at $SNR = 0$ dB there should be some performance difference, but with a mean value separation of less than 0.005, it is unlikely to be captured in the ROC curve unless the discrete γ values reach that granularity (which they did not in this simulation). Additionally, when the same study was conducted with $SNR = -20$ dB, it becomes clear the mean value separation is far less than the variance caused by noise within the system (Figure 34).

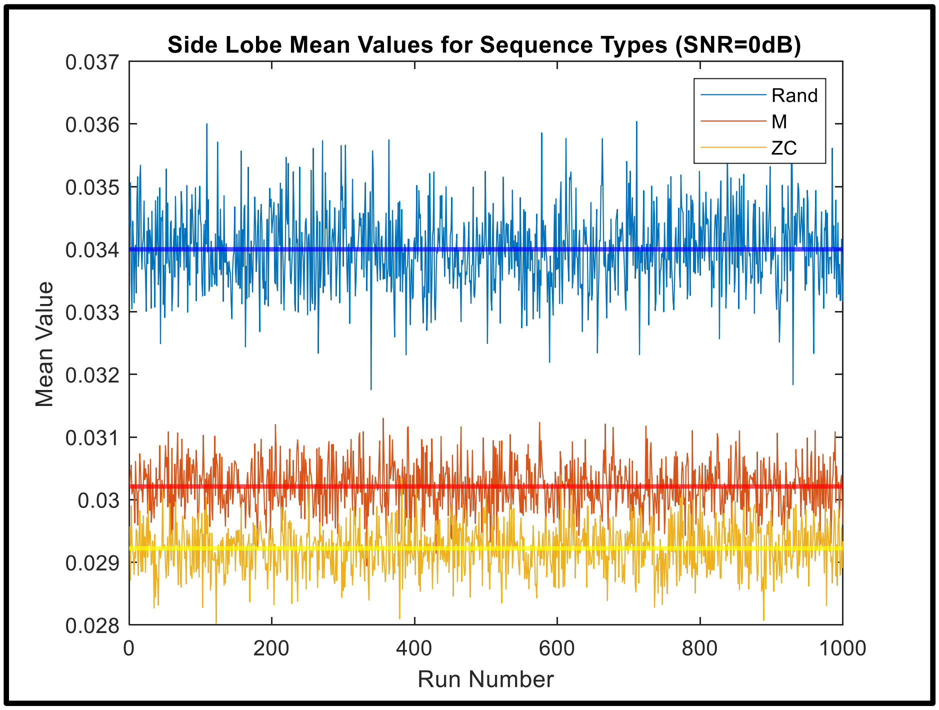


Figure 33. Autocorrelation Mean Values for Various Sequence Types (*SNR* = 0 dB)

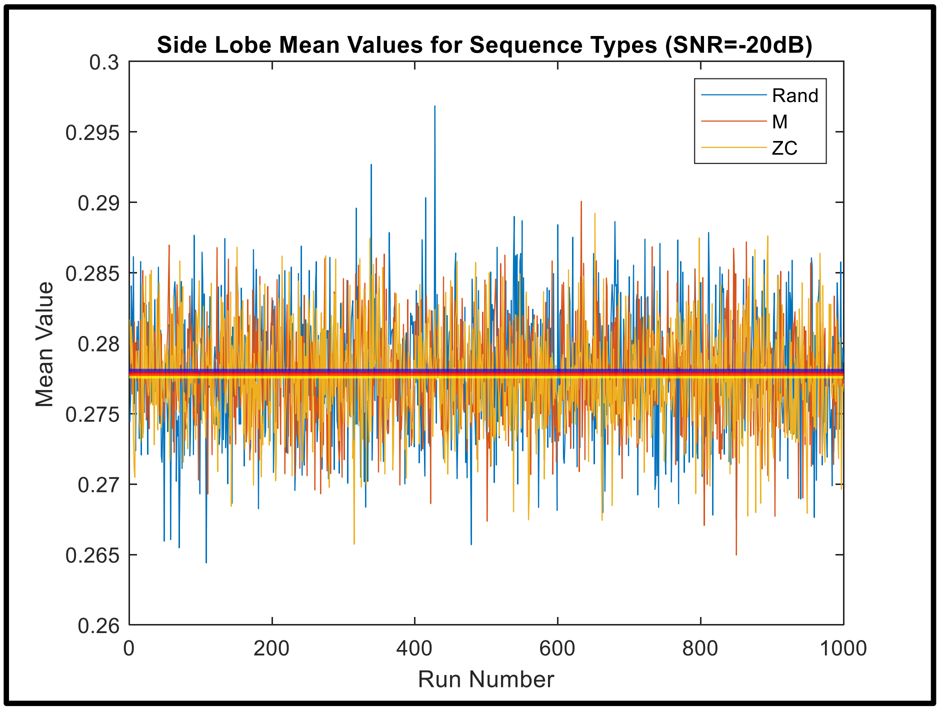


Figure 34. Autocorrelation Mean Values for Various Sequence Types (*SNR* = -20 dB)

E. DETECTION AND SYNCHRONIZATION CONCLUSION

The major results from this section are performance differences between random, ZC, and m-sequence types exist at higher SNRs, but as SNR decreases the performance difference becomes negligible. Because there are a limited number of ZC and m-sequences at a given SL, choosing either would make it easier for Eve to predict the specific sequence the UE or gNB is using and engage in coherent detection to improve her chances of detecting an omnidirectional connection request. Additionally, the use of a random sequence would allow the UE to encrypt a set preamble with a pre-shared key that changes periodically, thus randomizing the preamble structure with every new key used, preventing Eve from capturing it and using it indefinitely for either coherent detection or to craft a solicitation request. Because of these reasons, random sequences were chosen as the preamble sequence type for UECP analysis.

VI. PASSIVE ARRAY SWEEP LISTENING

A. PASSIVE ARRAY SWEEP LISTENING INTRODUCTION

The previous section simulated only a single antenna for analysis, but 5G NR wireless operations are facilitated primarily by antenna arrays [7]. Antenna arrays, as previously mentioned in this work, enable beamforming which increases the energy sent in a particular direction compared to others [20]. Although antenna arrays cannot increase the energy gained from a particular direction, they can combine the energy received at every antenna element in a way that increases the processing gain from a particular direction.

1. Array Gain Mathematics

Array gain allows antennas with multiple elements to increase the energy sent in a particular direction or to allow better reception of signals coming from a particular direction. To explore this further, we will look at the fundamentals of how array gain works. This section is not intended to be a full analysis of antenna array mathematics. All equations below, and more comprehensive derivations and analysis can be found in *Fundamentals of Applied Electromagnetics – Seventh Edition* [20].

Starting with a linear antenna array with equally spaced elements transmitting from all elements with uniform amplitude and phase, the array factor (AF), which represents the far-field radiation intensity of an array is

$$F_a(\gamma) = \frac{\sin^2(N\gamma / 2)}{\sin^2(\gamma / 2)} , \qquad (10)$$

$$\text{where } \gamma = \frac{2\pi d}{\lambda}\cos(\theta) , \qquad (11)$$

and N represents the number of antenna array elements, d is element spacing, λ is the wavelength, and θ is the angle of arrival/departure in radians ($\theta = \frac{\pi}{2}$ represents broadside). If we assume equal element spacing, $d = \frac{\lambda}{2}$ (an assumption used for the entirety of this research), and Equations 10 and 11 are combined, the resulting equations are

$$F_a(\theta) = \frac{\sin^2(N\pi\cos(\theta)/2)}{\sin^2(\pi\cos(\theta)/2)} \tag{12}$$

$$\text{and } F_{an}(\theta) = \frac{\sin^2(N\pi\cos(\theta)/2)}{N^2\sin^2(\pi\cos(\theta)/2)}, \tag{13}$$

where Equation 13 is the normalized array factor.

A plot of Equation 13 (Figure 35) illustrates the impacts of increasing the number of antenna elements by showing the gain pattern for $N = 4,\ 16,\ \text{and } 64$.

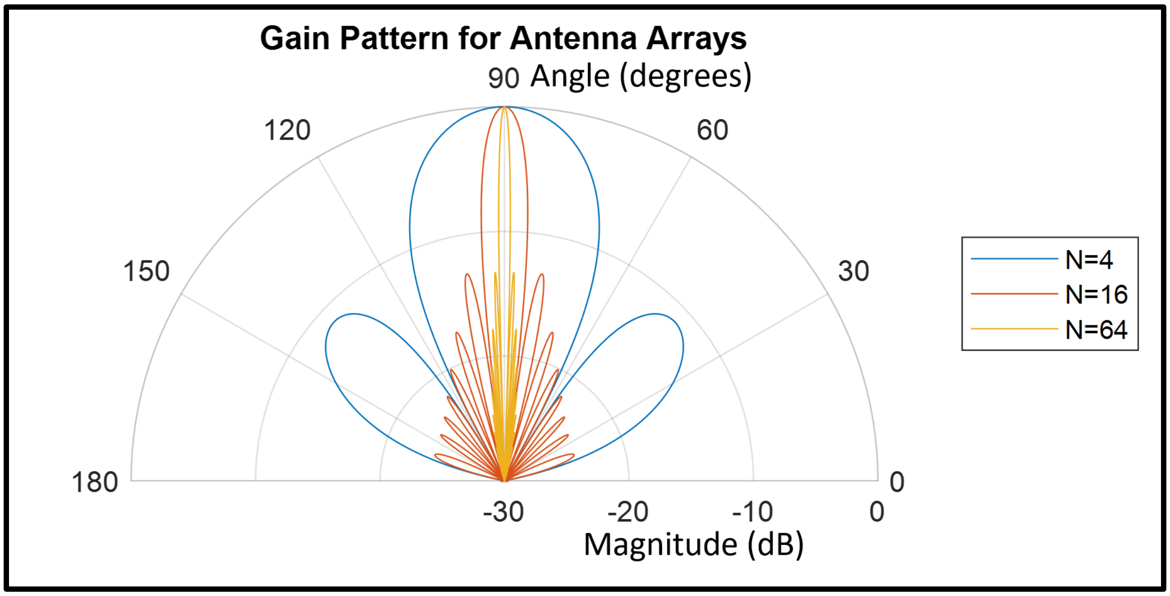


Figure 35. Antenna Array Gain Patterns for Various Array Sizes

As the number of antenna elements increases the half-power beamwidth (HPBW) decreases, the relative magnitude of the side lobes decreases, and the side lobe departure angles close around the main lobe. This phenomenon is good for this research for two reasons. First, the narrower the main lobe the greater the proportion of the transmitted energy directed at the receiving device, meaning less energy is required for the transmitted signal to be properly detected. Second, the magnitude and direction of the side lobes heavily affect the amount of energy classified as stray emissions in the connection process.

2. The Impacts of Massive MIMO

The previous section discussed the basics of array gain using smaller array sizes. Figure 36 clearly illustrates the impact if antenna array sizes are greatly increased by showing the gain pattern of an $N = 512$ array. An array of this size may not be practical at current 5G NR frequencies in FR1 or FR2 due to the spacing required for antenna elements ($d = \frac{\lambda}{2}$). However, as higher frequencies are utilized, the number of elements present in the same physical size array will increase linearly, allowing for much larger array sizes.

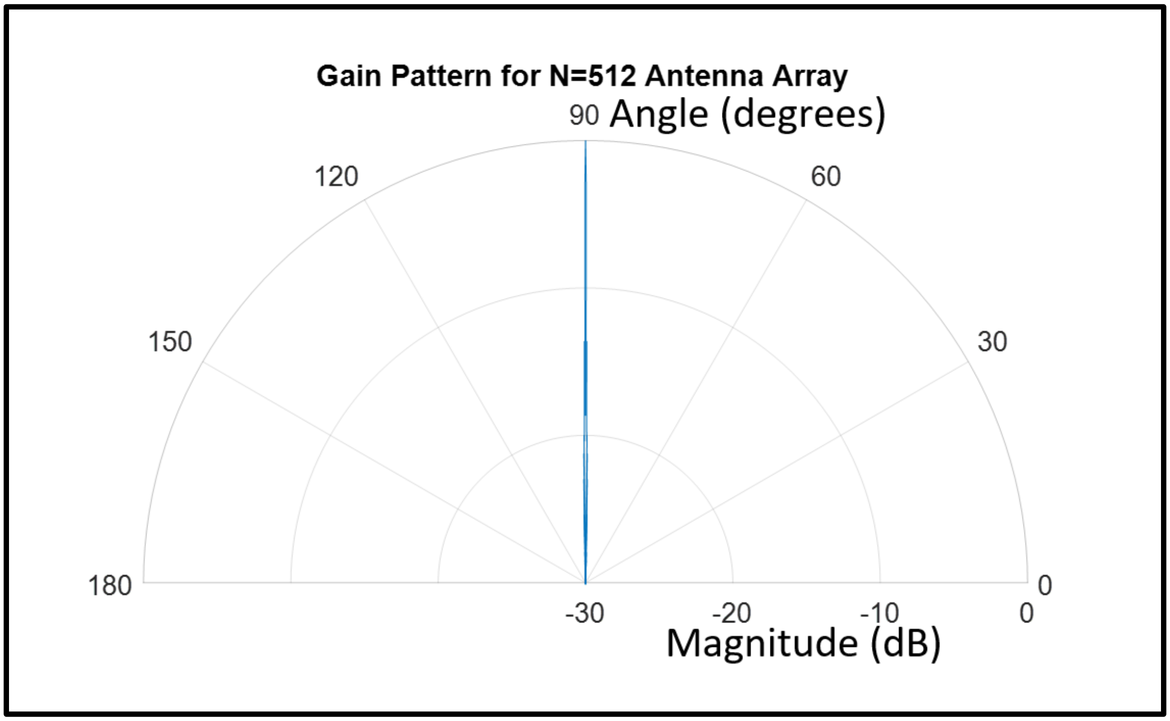


Figure 36. Gain Pattern of $N = 512$ Array

3. Electronic Scanning

The previous section showed the impacts of array sizes using uniform amplitude and phase at all antenna elements. However, the result of those constraints is that the main lobe will always be broadside to the array, that is, perpendicular to the face of the array. If the equal phase at all elements constraint is removed the array can steer the emitted energy in a specific direction. As before, only the equations relevant to this research are going to be presented, and more detailed mathematics and derivations can be found in *Fundamentals of Applied Electromagnetics – Seventh Edition* [20].

If the phase at all elements is not equal, Equation 11 is replaced by γ', which is

$$\gamma' = \frac{2\pi d\cos(\theta)}{\lambda} - \delta, \tag{14}$$

$$\text{where } \delta = \frac{2\pi d\cos(\theta_o)}{\lambda}, \tag{15}$$

and Equation 13 becomes $F_{an}(\gamma') = \dfrac{\sin^2(N\gamma'/2)}{N^2 \sin^2(\gamma'/2)}$ (16)

where θ_o is the angle of departure for the main lobe (in radians), also referred to as the scan angle.

Figure 37 illustrates the effects of applying a scan angle to the array and shows the main lobe moving to the scan angle location. Notice that *HPBW* increases as the scan angle moves from broadside to endfire (the significance of this will be discussed later).

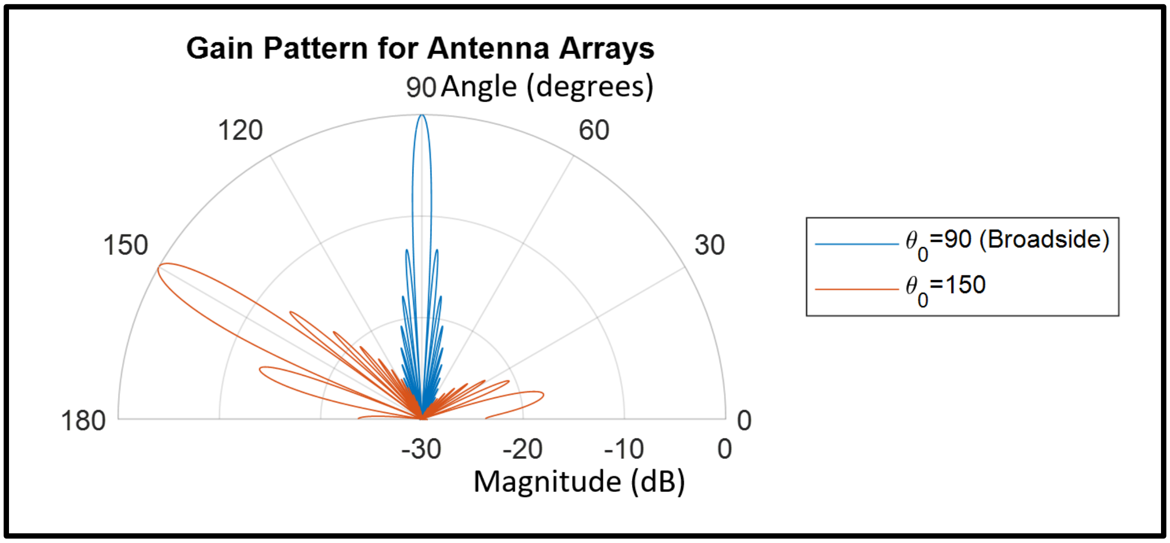


Figure 37. Effects of Scan Angle on Main Lobe HPBW

The previous equations showed the outgoing effects of applying a scan angle, but we also must understand how the array achieves gain on the receiving side. Figure 38 shows a uniform linear array of length *N* receiving an incident signal, s_p.

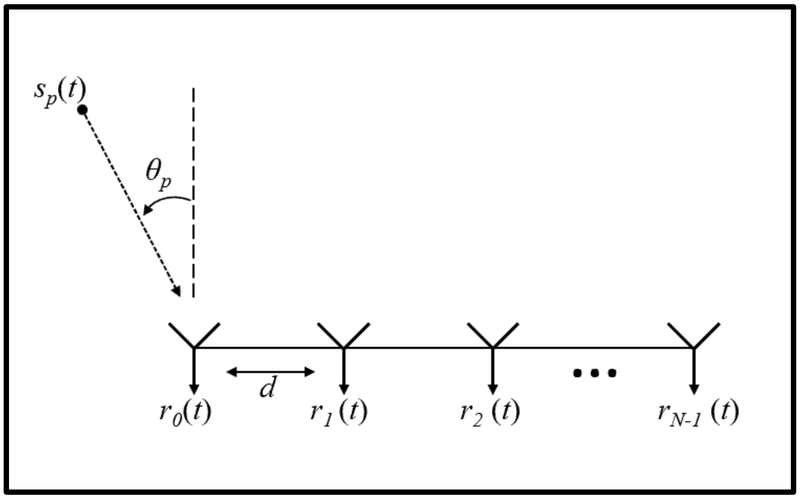


Figure 38. Uniform Linear Array with Incidental Signal

If the incident signal arrival direction, θ_p, is known, the signal received by the *k*th element at time *t*, $r_k(t)$, is

$$r_k(t) = s_p(t - kD), \tag{17}$$

$$\text{where } D = \frac{d\sin\theta_p}{c}, \tag{18}$$

and *kD* represents the time delay between when the zeroth element receives the signal and when the *k*th element receives it, which can also be regarded as a phase shift between the received signals.

The previous equations can be used to define the signal received at each element given a known signal and known direction of arrival. However, it is possible to utilize these relationships to determine the direction of arrival of a signal given the signal values are known in advance.

B. PASSIVE ARRAY SWEEP LISTENING PROCESS

Just as increasing a known signal's length can increase processing gain, should the direction of arrival be known, increasing the number of antenna elements can also increase the gain of the receiving system, as seen in Equation 12. In our scenario, the initial connection request is not coming from a known direction. There are various methods used to determine the received signal's DOA, and one of the most commonly used algorithms is Multiple User Signal Classification (MUSIC) [21]. MUSIC proved to be inadequate for this application, which will be explored in greater depth later in this work. The problem currently needing to be addressed is how to maximize array gain without a known direction of arrival. This challenge led to the development of the passive array sweep listening (PASL) method in this research. PASL applies multiple fundamental concepts to maximize the ability of a passively listening array to capture a known signal from an unknown location. The key to PASL is that the signal being received must be known in advance to allow for matched filtering.

1. PASL Process and Mathematics

Referencing back to Figure 38, an incident signal, s_p, is arriving at some angle off broadside, which will be used to explain the PASL process. Given the discrete incident signal s_p, the received signal, ignoring the presence of noise, can be characterized by the product of a steering vector and the original signal,

$$\mathbf{R}_r = \begin{bmatrix} a(\theta_p, k=0) \\ a(\theta_p, k=1) \\ \vdots \\ a(\theta_p, k=N-1) \end{bmatrix} \begin{bmatrix} s_p[0] & s_p[1] & \cdots & s_p[S-1] \end{bmatrix}, \tag{19}$$

and results in the $N\text{x}S$ matrix,

$$\mathbf{R}_r = \begin{bmatrix} a(\theta_p,0)s_p[0] & a(\theta_p,0)s_p[1] & \cdots & a(\theta_p,0)s_p[S-1] \\ a(\theta_p,1)s_p[0] & a(\theta_p,1)s_p[1] & \cdots & a(\theta_p,0)s_p[S-1] \\ \vdots & \vdots & \ddots & \vdots \\ a(\theta_p,N-1)s_p[0] & a(\theta_p,N-1)s_p[1] & \cdots & a(\theta_p,N-1)s_p[S-1] \end{bmatrix}, \tag{20}$$

where $a(\theta_p, k)$ are the individual steering values at each array element for the signal (the combination of all is referred to the steering array), N is the total number of antenna elements, and *S* is the total signal length. Notice that in the shift to discrete time the *t* variable from Equation 17 is replaced with *nT* where *n* is discrete time and *T* is the sample interval.

Next, the receiving system applies a series of unsteering vectors to the $\mathbf{R}_r$ matrix column-by-column. That is, it applies a steering vector intended to undo the effects of the original steering angle. This is accomplished using

$$\mathbf{r}_u(\theta_s) = \mathbf{r}_r[n] \cdot \mathbf{a}_{\theta_u}(\theta_s) \qquad \text{for } n\text{=0,1,2...}S\text{-1}, \tag{21}$$

$$\text{where } \mathbf{a}_{\theta_u}(\theta_s) = \begin{bmatrix} 1 \\ e^{-\frac{i2\pi d \sin\theta_s}{\lambda}} \\ \vdots \\ e^{-\frac{i2\pi d (N-1)\sin\theta_s}{\lambda}} \end{bmatrix} \qquad \text{for -}\frac{\pi}{2} \le \theta_s \le \frac{\pi}{2}, \tag{22}$$

and $\mathbf{r}_r[n]$ is the n^{th} column of the $\mathbf{R}_r$ matrix, and $\mathbf{a}_{\theta_u}(\theta_s)$ is the unsteering vector at each θ_s value used. The result, $\mathbf{r}_u(\theta_s)$, is a vector of unsteered signal values at every discrete θ_s used. As θ_s runs through the full range of possible values, the closer θ_s gets to the original incident angle, θ_p, the closer each element of the $\mathbf{r}_u(\theta_s)$ vector will get to the original $s_p(n)$ value. For every discrete θ_s, we can sum the absolute values of $\mathbf{r}_u(\theta_s)$ using

$$m(\theta_s) = \sum_{n=0}^{S-1} |\, \mathbf{r}_u(\theta_s) \,| \qquad \text{for -}\frac{\pi}{2} \le \theta_s \le \frac{\pi}{2}, \tag{23}$$

which results in a single scalar value, *m*, for every discrete θ_s value. As θ_s approaches θ_p, the value of *m* approaches a maximum possible value. Although the true maximum occurs when $\theta_s = \theta_p$ the discrete nature of θ_s means it is unlikely $m(\theta_s)$ will ever truly match the summed absolute value of s_p . Once the maximum $m(\theta_s)$ is found, the corresponding θ_s can be captured and will be referred to as $\theta_{s-\max}$ for the remainder of this work.

Although the previous mathematics work to determine the θ_s value where the largest signal value occurred, it does not consider whether a valid signal is present. Noise alone would always result in a maximum *m* value being found, and thus a $\theta_{s-\max}$ value, regardless of whether a signal was present.

To use this method fully in determining the presence of a signal, we need to use the $\theta_{s-\max}$ value found to unsteer the received signal and correlate against the matched filter. This is done using

$$\mathbf{r}_{\max} = \frac{\mathbf{r}_r[n] \cdot \mathbf{a}_{\theta_u}(\theta_{s-\max})}{N} \quad \text{for } n\text{=0, 1, 2,..., } S\text{-1}, \tag{24}$$

where *N* is the number of antenna elements and is used in the denominator to scale the resulting $\mathbf{r}_{\max}$ value. The process explained in Chapter V.D.1 of this work is then applied to the resulting $\mathbf{r}_{\max}$ vector to determine whether a preamble is present.

It is important to note that *N* in Chapter V refers to sequence length, not to be confused with *N* referencing array length in this chapter. Due to the concepts and topics being discussed in this work some confusion can arise as certain variables are commonly used across multiple fields of study and can mean very different things based on context. The variables used previously in this work were intended to align with the larger body of work in that particular field. However, the remainder of this work involves a combination of concepts that could cause such crossovers to become increasingly confusing. To prevent this, two new variables are used for the remainder of this work; the length of a signal is represented by *SL*, and the length of an array is represented by *EL*. It is important to be able to distinguish between these two variables as the central theme of this work is the trade space between them during the connection process.

2. PASL Sweep Angle Step Size

Now that the PASL process mathematics are established, this process can be applied to the specific scenario presented in this work. As seen previously in Figure 26 through Figure 29, the detection and synchronization capability of the system drops rapidly as *SNR* decreases when only a single antenna is used. However, the PASL process allows for much greater performance by utilizing the signals at all antenna elements in the array for detection and synchronization. Because AWGN is zero mean, as the number of antennas approached infinity, the sum of the noise would approach zero, leaving the received signal value as the dominant value.

Before that can be shown, it is important to consider some practical aspects of the PASL process. Observing Equation 22, the θ_s value is presented as continuous, but this is computationally impossible. The θ_s value must be broken up into discrete values in the computation process, and if the θ_s step size ($\Delta\theta_s$) is too large, we may fail to get close enough to the true θ_p value to result in $\mathbf{r}_{\max}$ producing a correlation value high enough for detection. Because the PASL process must be conducted with every new sample received, if the discrete $\Delta\theta_s$ values are too granular, the computation time required becomes too great to be practical for a real-world system.

The starting point for determining the optimum $\Delta\theta_s$ is to examine fundamental array gain mechanics. Figure 39 illustrates the beam pattern for two separate arrays, one with $EL = 4$ and the other with $EL = 8$.

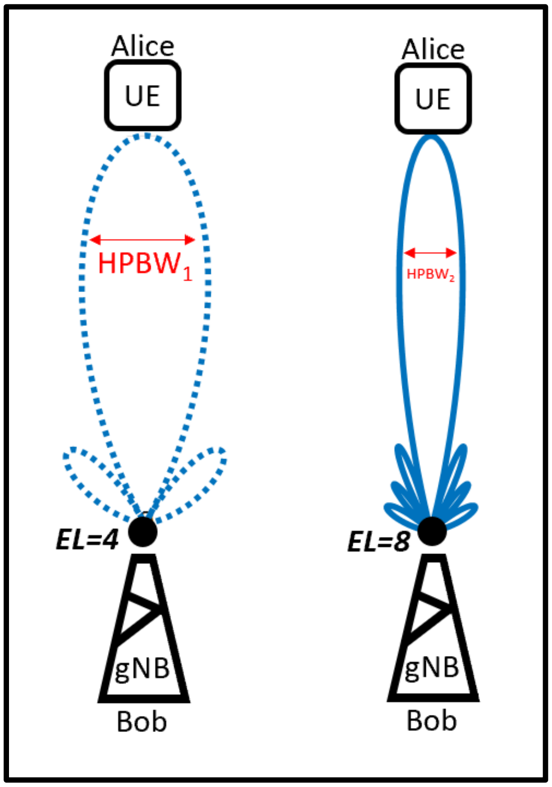


Figure 39. Beam Patterns for $EL = 4$ and $EL = 8$ Arrays

Notice that as the number of antenna elements (EL) increases, the $HPBW$ decreases. This is a good starting point to determine a $\Delta\theta_s$ required to properly capture the incoming signal. If the $\Delta\theta_s$ is larger than the $HPBW$, it has a chance of bypassing the main lobe of the received signal completely; if it is too small the computational time required becomes prohibitive. We now see that $\Delta\theta_s$ must be less than the $HPBW$ of the array itself, which is a function of the array size. Using the $HPBW$ approximation in radians (adapted from [12]),

$$HPBW(EL) \approx \frac{0.886\lambda}{EL(d\cos\theta_o)}, \tag{25}$$

where EL is the number of antenna elements, θ_o is the scan angle in radians ($\theta_o = 0$ represents normal or broadside to the array), and d is the element spacing, we can determine the $HPBW$ of various array sizes. Because the element spacing is locked at

$d = \frac{\lambda}{2}$, the *HPBW* becomes independent of frequency. Figure 40 illustrates the *HPBW* approximation through the range of values important to this research (+/- 60^o).

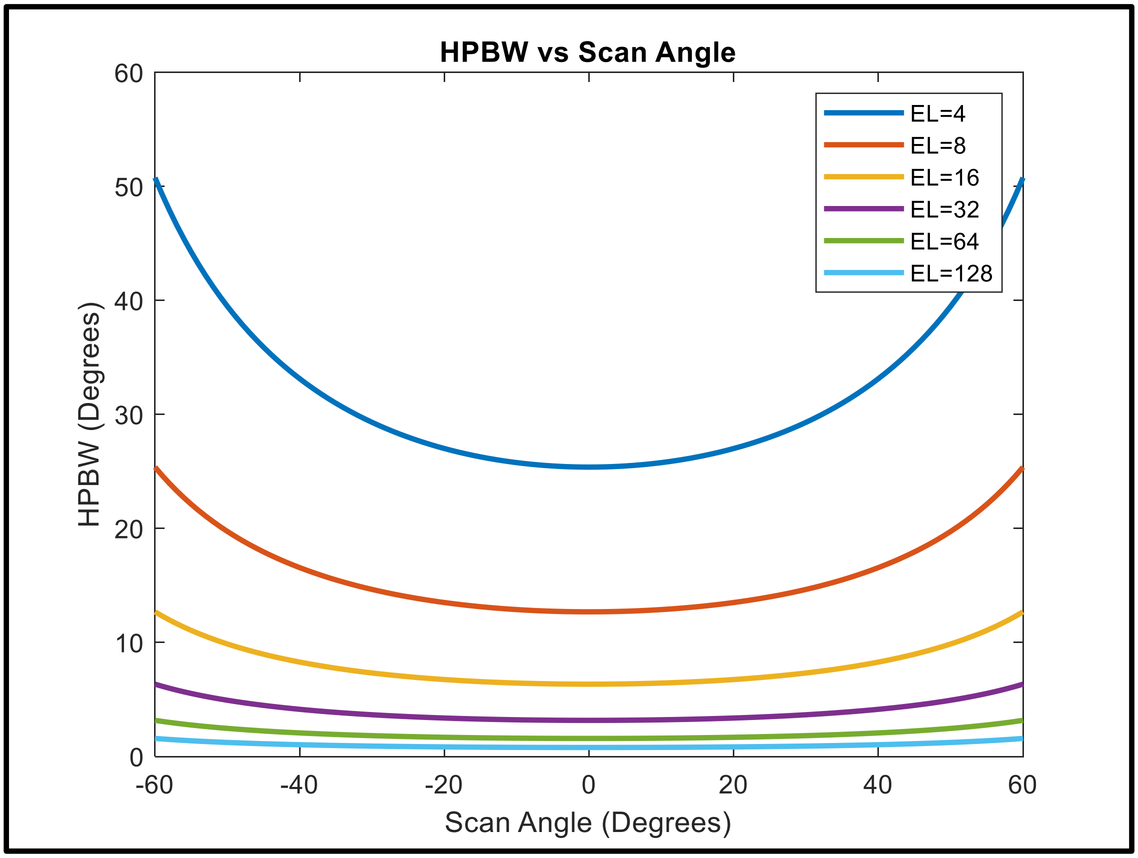


Figure 40. HPBW at Various Array Sizes (+/- 60^o Scan Angle)

The reason this is an approximation is that it is valid at broadside, but less accurate as θ_o approaches endfire. For the purposes of this research, this approximation is acceptable since the *HPBW* increases as the signal angle approaches endfire, and the goal is to ensure the $\Delta\theta_s$ is granular enough that it will not bypass the *HPBW*. If $\Delta\theta_s$ is built off a zero probability of missing the main lobe at broadside (0^o), then the probability of it missing the main lobe anywhere else is also zero.

The first set of analyses on the PASL process involved identifying the ideal step size for θ_s. To do this the PASL process was tested using the same process found in the

Preamble Process and Simulation Explanation found in Chapter V, using a random sequence and random arrival angle, with the inclusion of PASL between Steps 4 and 5. Note that for this analysis an array size of 8192 was used. Although this array size is not necessarily physically practical for small, mobile systems, it is used throughout this work as an upper theoretical bound for array length.

Figure 41 through Figure 46 illustrate the resultant ROC curves from a series simulation runs with $SL = 2$, $EL = 8192$, $SNR = -30$ dB, and the only variable was $\Delta\theta_s$ step size (as annotated on each plot). The three curves displayed are Array PASL, Array No PASL, and Single Element. Array PASL is the ROC curve resulting from an antenna array utilizing the PASL method described previously. Array No PASL is the ROC curve resulting from an array where PASL is not used, thus no direction of arrival estimation is performed and the received signal is merely the summation of incident signals at each element (Equation 21 with the $\mathbf{a}_{\theta_u}$ vector set to all ones). Single Element is the ROC curve produced if only a single antenna element was receiving the signal.

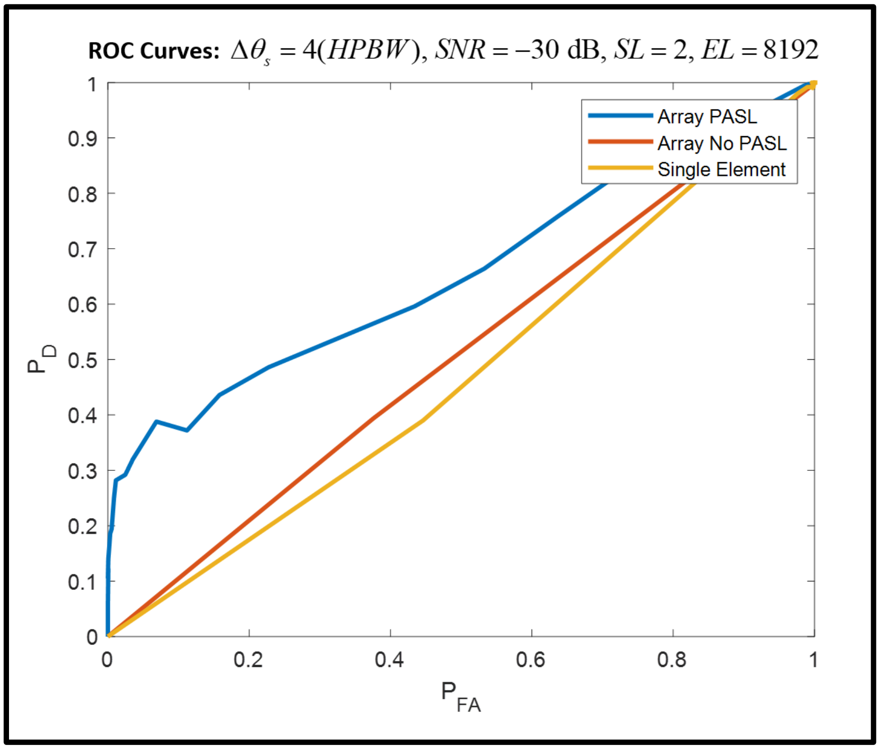


Figure 41. ROC Curves: $\Delta\theta_s = 4(HPBW)$

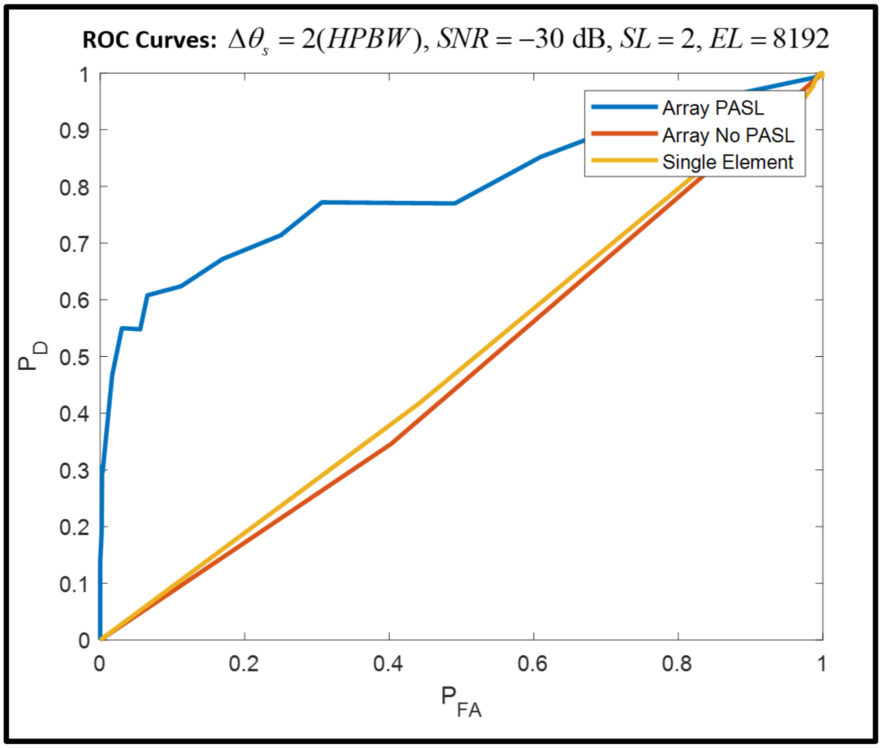


Figure 42. ROC Curves: $\Delta\theta_s = 2(HPBW)$

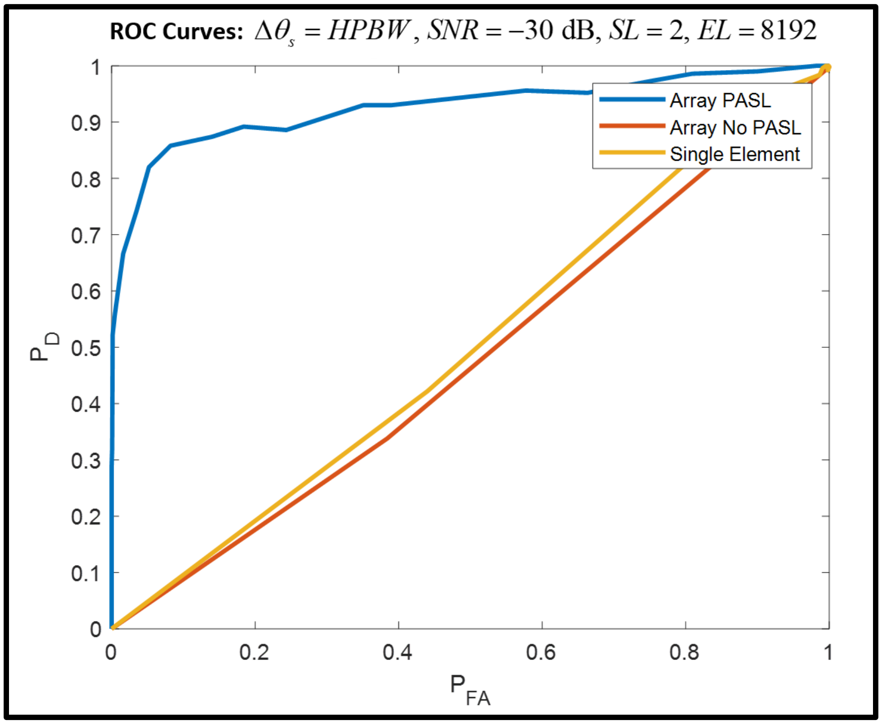


Figure 43. ROC Curves: $\Delta\theta_s = HPBW$

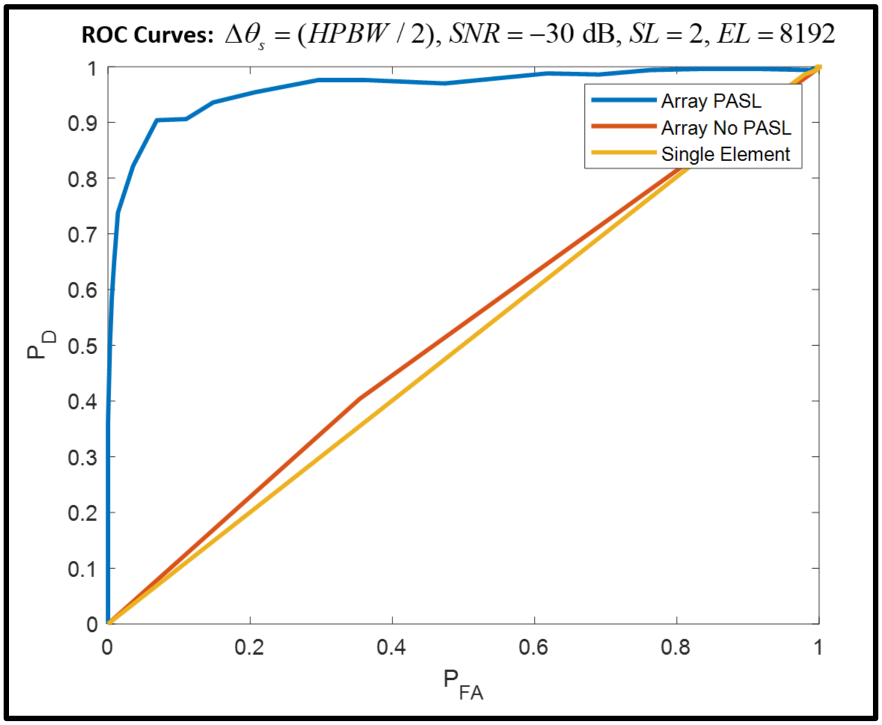


Figure 44. ROC Curves: $\Delta\theta_s = (HPBW/2)$

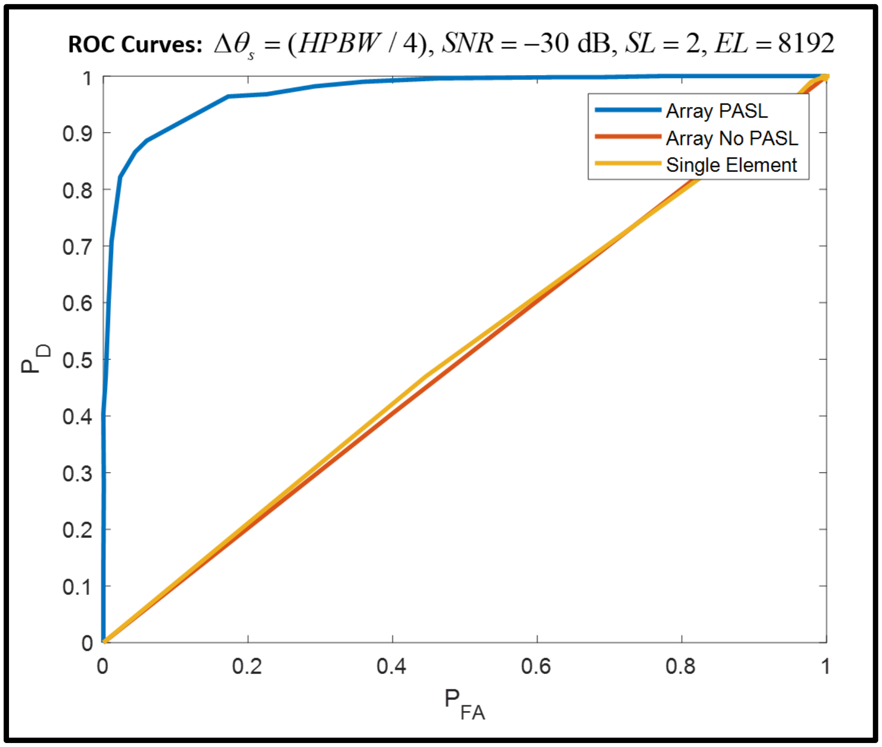


Figure 45. ROC Curves: $\Delta\theta_s = (HPBW/4)$

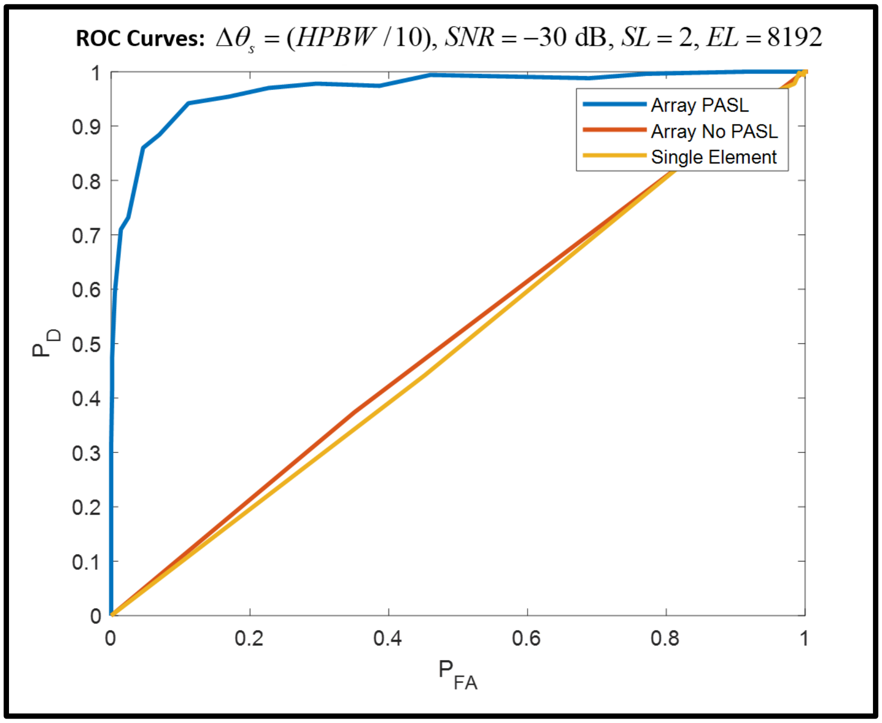


Figure 46. ROC Curves: $\Delta\theta_s = (HPBW/10)$

As can be seen in Figure 41 through Figure 43, the ability of the receiving system to detect and synchronize with the incoming preamble increase greatly as $\Delta\theta_s$ approaches the value of the *HPBW*. However, once $\Delta\theta_s$ equals ½ *HPBW*, the improvement achieved in the ROC curves by further reducing $\Delta\theta_s$ becomes negligible. The PASL process is computationally taxing, and the amount of discrete sweep angles is equal to $\frac{120}{\Delta\theta_s}$, meaning a decrease in step size is inversely proportional to the number of calculations required. The gains realized below $\Delta\theta_s = (HPBW/2)$ are not sufficient to justify the additional computational power required. Additionally, as is seen in Figure 41 through Figure 46, the application of the PASL method results in detection and synchronization performance that greatly exceeds the ability of a single antenna element or an array that is not conducting direction of arrival estimation.

3. Detection and Synchronization Performance Analysis

As illustrated and explained in the previous section, the PASL method can detect and synchronize with signals at far lower *SNR*s than a single antenna, or an array that does not estimate the direction of arrival of a signal. The key concept central to the capability of the PASL process is that the AWGN at each element is independent and identically distributed (IID) with a zero mean. This means as the number of array elements approached infinity, the average noise across all antenna elements would approach zero, leaving only the signal present. The same is true if we were to use a single antenna and a single-valued preamble of infinite length. Generally, increasing signal length is used to improve system performance as *SNR* decreases, but results in more EM energy emitted into the environment. By utilizing larger arrays, we can gain a similar benefit without violating a main tenant of this research, which is reducing EM energy emitted.

The first step in determining the performance of the PASL method is to define certain required performance characteristics. Figure 47 illustrates an ideal ROC curve (perfect classifier), where P_D is equal to 1 when P_{FA} is equal to zero, along with an arbitrary ROC curve (random classifier), where the likelihood of detection and false alarm are equal at any given threshold.

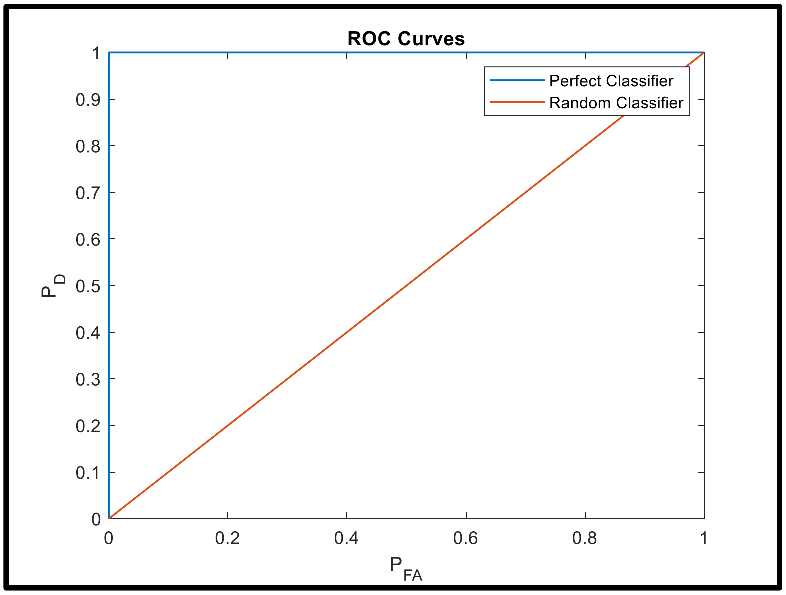


Figure 47. ROC Curve Types

Because the ROC curves for any given signal length, *SL*, number of antenna elements, *EL*, and *SNR* are different, a method of comparison was required to ascertain the performance of the system. One such method is to calculate the area under the ROC curve, where an area of 1 represents a perfect classifier and an area of 0.5 represents a random classifier. This method is achieved by using a right-hand Reimann sum [22] of the ROC curve. A right-hand Reimann sum was used because it provides a more conservative estimate of the area under the curve. Figure 48 illustrates the Riemann sum used and the equation (adapted from [22]) is

$$A_{ROC} = \sum_{n=1}^{R-1} P_D(n+1)(P_{FA}(n) - P_{FA}(n+1)), \qquad (26)$$

where R represents the total number of P_D and P_{FA} values computed, which is based on the amount of discrete threshold values used. The A_{ROC} term constitutes the area under the ROC curve for a given set of parameters.

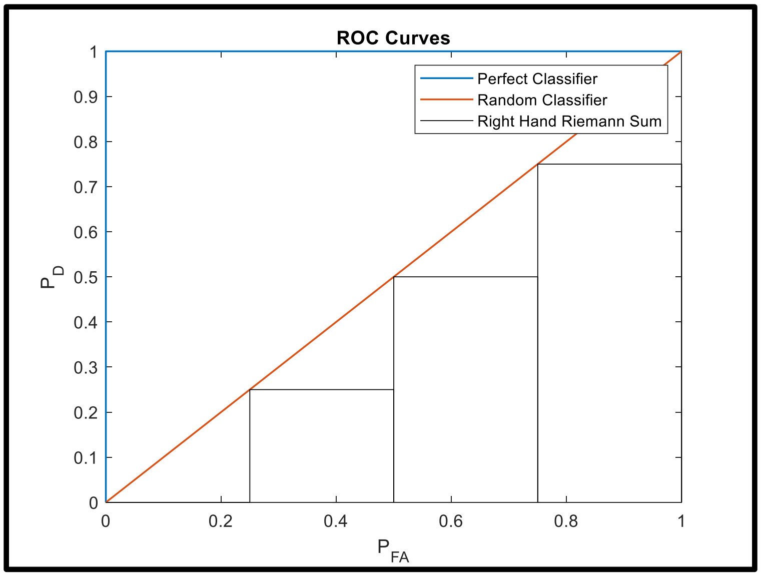


Figure 48. Riemann Sum of ROC Curves

Additionally, because the threshold values used start at zero and end at infinity, the first P_D and P_{FA} values start at (1,1) at a threshold of zero, and end at (0,0) at a threshold of infinity. This means the curve is progressing from right to left on the plot in Figure 48 as the threshold value rises, meaning the $(n+1)$ value seen in Equation 26 represents a point lower on the curve than n, making this a more conservative estimate of the area under the ROC curve. Now that a method has been established to characterize the performance of the system with any given set of parameters, an analysis of the PASL method's performance can be completed.

4. PASL Simulation

Figure 49 shows the simulation process used to analyze the performance of the PASL process. Outside a few modifications noted below Figure 49, this simulation mirrors that of the preamble testing simulation.

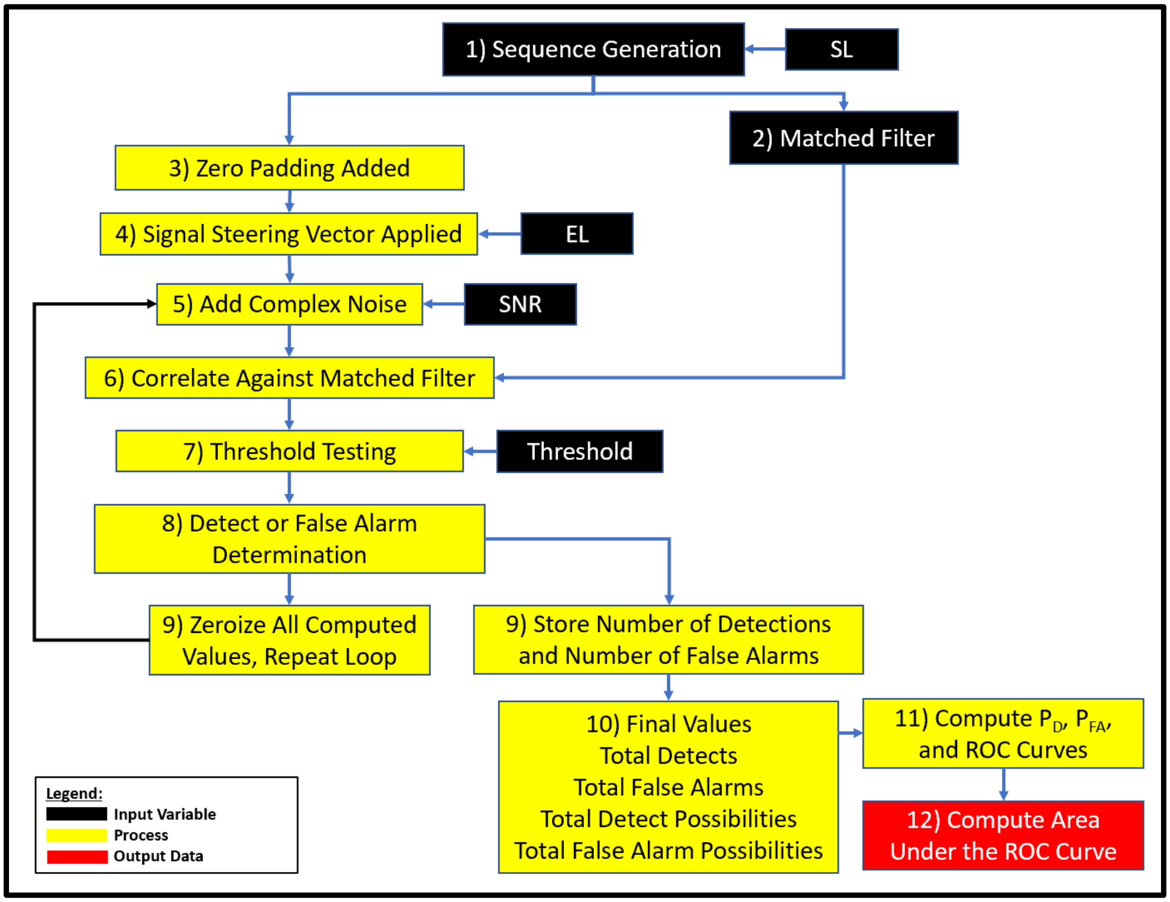

1) Sequence Generation
SL
2) Matched Filter
3) Zero Padding Added
4) Signal Steering Vector Applied
EL
5) Add Complex Noise
SNR
6) Correlate Against Matched Filter
7) Threshold Testing
Threshold
8) Detect or False Alarm Determination
9) Zeroize All Computed Values, Repeat Loop
9) Store Number of Detections and Number of False Alarms
10) Final Values Total Detects Total False Alarms Total Detect Possibilities Total False Alarm Possibilities
11) Compute P_D, P_FA, and ROC Curves
12) Compute Area Under the ROC Curve
Legend:
Input Variable
Process
Output Data

Figure 49. PASL Simulation Process

The first major change from the preamble simulation is the inclusion of a steering vector at Step 4, which is used in conjunction with a randomly generated DOA and steering vector based on *EL* to create the signal which will arrive at each antenna element. The other major modification is that the final output (Step 12) is no longer a ROC curve. Rather, it is the area under the ROC curve (A_{ROC}), which provides a numerical expression of the performance of the system.

5. PASL Applied to Detection and Synchronization

Table 1 shows the series of variables and range of values used to conduct the Monte Carlo simulations resulting in a total of 756 unique SNR-SL-EL simulation configurations with each configuration run one thousand times.

Table 1. PASL Monte Carlo Parameters

Variable	Min	Max	Step Size
SNR (dB)	-20	0	1
Sequence Length (SL)	4	128	2^m m= [2,7]
Array Elements (EL)	4	128	2^m m= [2,7]
Threshold	0	Infinity	Variable
Area Under ROC Curve	0.9 (90%)	0.999 (99.9%)	Variable

It is also important to introduce a new term at this time, effective sequence length (*ESL*), which is

$$ESL = SL(EL)\,, \tag{27}$$

where *SL* is the sequence length (preamble length in this case) and *EL* is the number of array elements. This term is important for characterizing the performance of the PASL system independent of the specific values of *SL* or *EL*, but only as a product of the combination of the two terms. If we determine the system operates with sufficient performance at an *ESL* of 1000, then any possible combination of *EL* and *SL* that result in an *ESL* of 1000 should perform the same. This is important because we are examining the trade space between signal length (which corresponds to the amount of energy emitted) and antenna array sizes. This concept, along with some limitations that exist with it, will be explored in greater detail later in this work.

The results of the comprehensive Monte Carlo simulation can be seen in Figure 50. It is important to note that the vertical axis scale of this plot is logarithmic and represents the product of the *SL* and *EL* terms (or *ESL*) for any given Monte Carlo simulation.

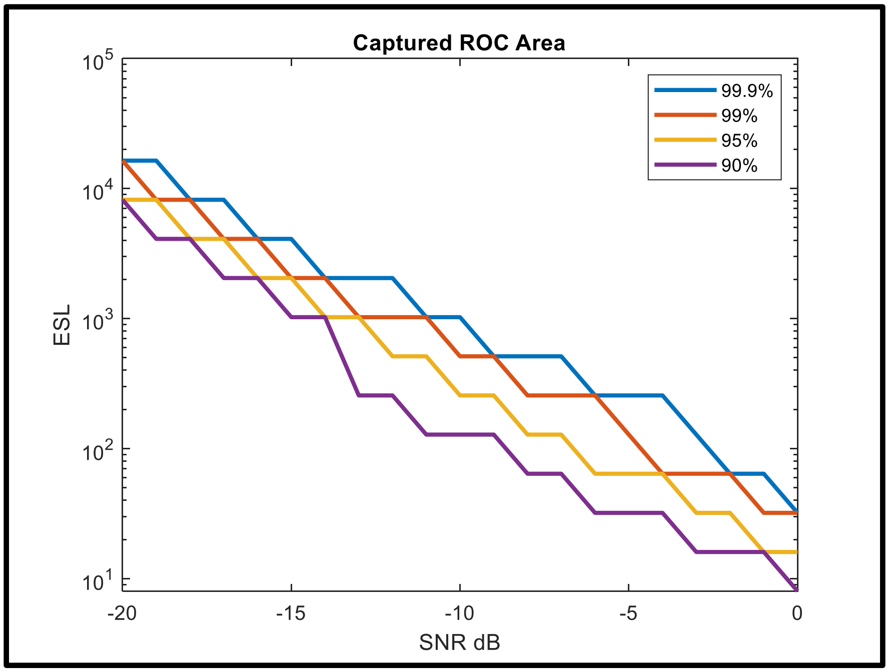


Figure 50. *ESL*s Required for Discrete A_{ROC} Performance Levels at Various *SNR*s

The curves of this plot show the *ESL* required to produce a ROC curve that captures a percentage of the total possible ROC curve area. The 90% line, for instance, equates to an A_{ROC} of 0.9, or 90% of the area value of a perfect identifier, which has an A_{ROC} equal to 1. As expected, larger *ESL* values are required to have better ROCs at any single *SNR* value, which is why the required *ESL* is higher for higher A_{ROC} percentages. The stairstep pattern of the graph is a byproduct of the discrete values used for the simulation, which also means the curves in Figure 50 do not represent the exact *ESL* values required at any given *SNR* and are better thought of as an upper bound. Figure 51 shows an expanded view of Figure 50, isolating the -5 dB to 0 dB *SNR* range, and the 32 to 256 *ESL* region.

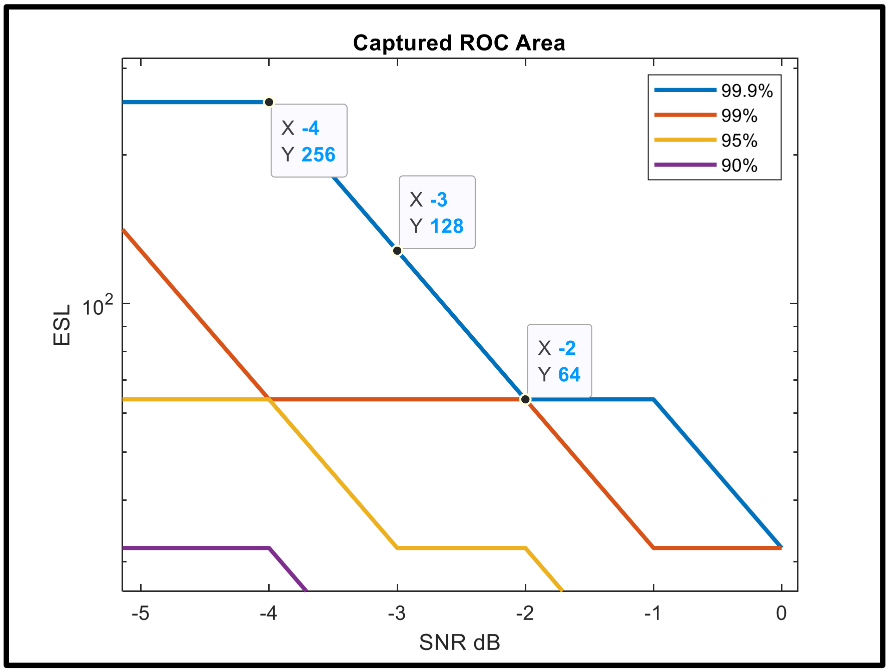


Figure 51. Expanded ESL vs. SNR Curves

Three points are annotated on this plot and show that for the ROC curve to capture 99.9% of the perfect identifier area at *SNR*s of -2 dB, -3 dB, and -4 dB, the *ESL* required is 64, 128, and 256, respectively. What can be identified from this plot is that at -4 dB it takes an *ESL* of no more than 256 for the ROC curve to capture 99.9% of the total perfect classifier area. What cannot be identified is precisely how low the *ESL* could be and still produce the required performance. However, we can see that at an *SNR* of -3 dB, an *ESL* of 128 was required, but an *ESL* of 128 was not sufficient to maintain the 99.9% performance at -4 dB. This means the true *ESL* required exists somewhere above 128 and at or below 256. This creates a region of ambiguity, but bounds the *ESL* required to achieve a specific performance level. An illustration of this bounded region can be seen in Figure 52.

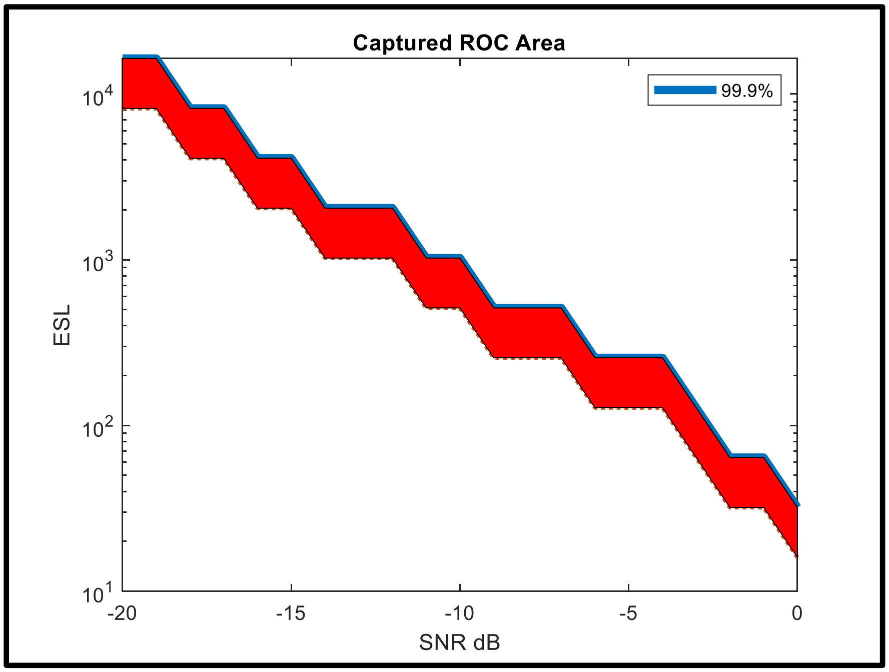


Figure 52. ESL vs. SNR Curves - Ambiguity Region

The primary intent of this analysis was to determine what the required *ESL* would be at a particular *SNR* value and determine if the *ESL* growth is steady as *SNR* drops. Referring to Figure 50, the curves show some irregularity above -14 dB but stabilize and grow consistently below -14 dB and can be characterized by the approximation equations

$$ESL_{99.9\%} \approx \begin{cases} 2^{-\left(\left(3-\frac{(-14-SNR_{dB})}{2}\right)+SNR_{dB}\right)} + 2^{-\left(\left(4-\frac{(-14-SNR_{dB})}{2}\right)+SNR_{dB}\right)} & \text{for even } \mathrm{SNR}_{dB} \le \text{-14dB} \\ 2^{-\left(\left(3-\frac{(-15-SNR_{dB})}{2}\right)+SNR_{dB}\right)} & \text{for odd } \mathrm{SNR}_{dB} \le \text{-15dB} \end{cases}, \qquad (28)$$

$$ESL_{99\%} \approx \begin{cases} 2^{-\left(\left(3-\frac{(-15-SNR_{dB})}{2}\right)+SNR_{dB}\right)} & \text{for even } \mathrm{SNR}_{dB} \le \text{-14dB} \\ 2^{-\left(\left(4-\frac{(-14-SNR_{dB})}{2}\right)+SNR_{dB}\right)} + 2^{-\left(\left(5-\frac{(-14-SNR_{dB})}{2}\right)+SNR_{dB}\right)} & \text{for odd } \mathrm{SNR}_{dB} \le \text{-15dB} \end{cases}, \qquad (29)$$

$$ESL_{95\%} \approx \begin{cases} 2^{-\left(\left(2-\frac{(-14-SNR_{dB})}{2}\right)+SNR_{dB}\right)} + 2^{-\left(\left(3-\frac{(-14-SNR_{dB})}{2}\right)+SNR_{dB}\right)} & \text{for even SNR} \le \text{-14dB} \\ 2^{-\left(\left(2-\frac{(-15-SNR_{dB})}{2}\right)+SNR_{dB}\right)} & \text{for odd SNR} \le \text{-15dB} \end{cases}, \qquad (30)$$

and

$$ESL_{90\%} \approx \begin{cases} 2^{-\left(\left(4-\frac{(-15-SNR_{dB})}{2}\right)+SNR_{dB}\right)} & \text{for even SNR} \leq \text{-14dB} \\ 2^{-\left(\left(5-\frac{(-14-SNR_{dB})}{2}\right)+SNR_{dB}\right)}+2^{-\left(\left(6-\frac{(-14-SNR_{dB})}{2}\right)+SNR_{dB}\right)} & \text{for odd SNR} \leq \text{-15dB} \end{cases}. \qquad (31)$$

The trendlines created with Equations 28 through 31 can be seen in Figure 53, and show that they are the high-end approximations for the required *ESL*, meaning lesser values may work, but the approximations are conservative enough to ensure the system works at the desired *SNR* and performance level.

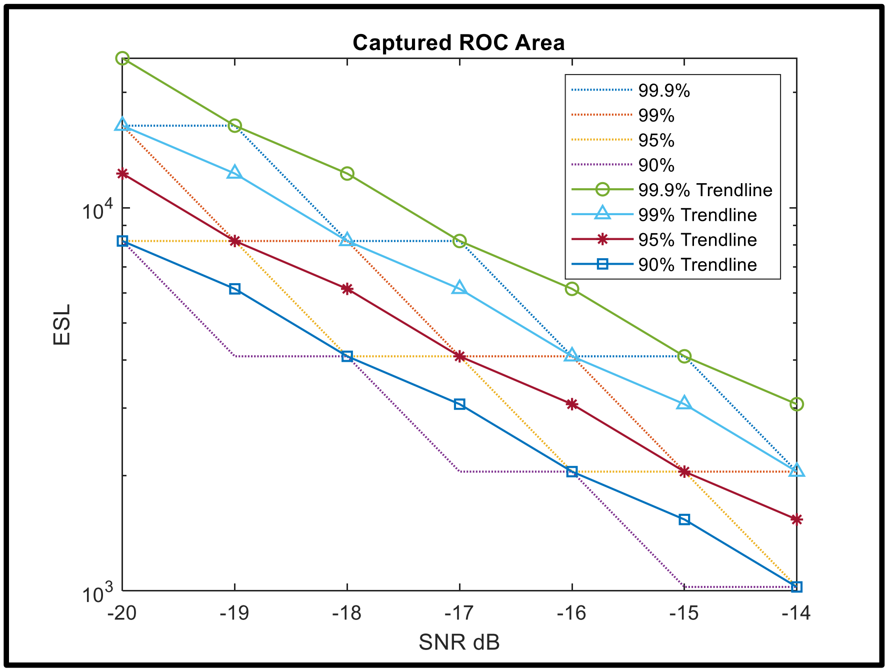


Figure 53. ESL Trendlines

Although Equations 28 through 31 accurately characterize the performance of the system below -14 dB, more analysis was required to understand why the system behavior was not as consistent when *SNR* was greater than -14 dB. The same data used to create Figure 50 was used again to better understand the interaction between the *SL* and *EL* values. Figure 54 shows the system behavior at $A_{ROC} = 0.999$ when one parameter (either *SL* or

EL) was locked into a set value, and the other parameter varied throughout the full range of possible values found in Table 1.

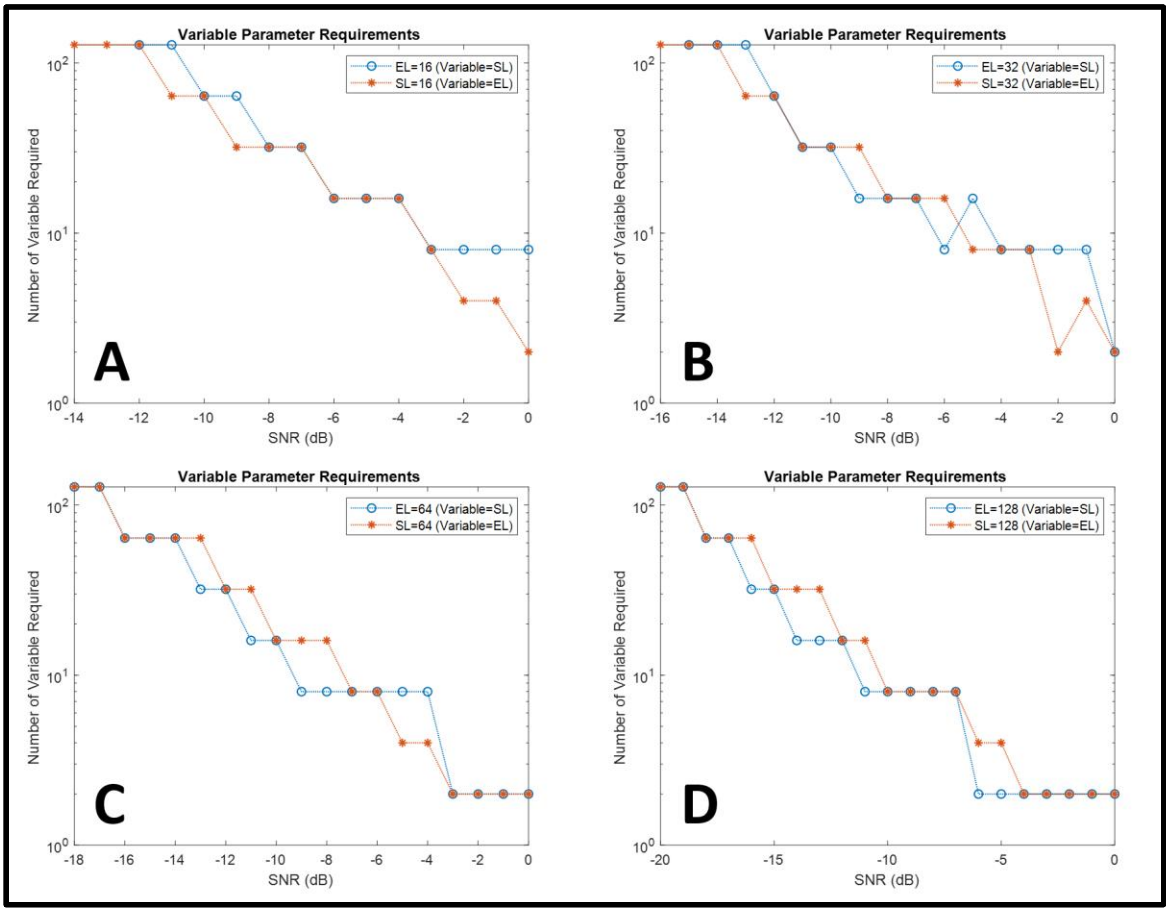


Figure 54. ESL Parameter Isolation

The four plots in Figure 54 represent four separate possible parameter values that were used to make either *SL* or *EL* a static value while the other parameter was varied. For instance, Figure 54: Subplot A illustrates the system performance between -14 dB and 0 dB when either the *EL* or *SL* value was locked at 16, and the other parameter varied between 4 and 128. Figure 54: Subplot A shows that at an *SNR* value of 0 dB, with an *EL* of 16, a minimum *SL* value of 8 is required for the system to operate properly, whereas an *SL* of 16 would support adequate system performance at 0 dB with an *EL* value of only 2. In this case we see that *SL* is the driving variable, that is, the variable which when set as static requires a larger *ESL* value than the *ESL* value required should the other variable be set as static at the same value. However, if we compare this to Figure 54: Subplot D we see that if *EL* is 128, then an *SL* of only 2 is required between -4 dB and -6 dB to achieve the desired system performance. However, if *SL* is 128 then an *EL* of only 4 is required, meaning *EL* in this case is the driving variable.

In all four subplots of Figure 54, the curve lower on the plot at a given *SNR* indicates that the variable locked to a static value to create that curve is the driving variable. What is important is that at lower *SNR*s, and thus lower *EL* and *SL* values, both the *EL* and *SL* variables trade places as the driving variable. However, as either variable increases to a certain threshold (approximately 32 based on the plots in Figure 54), the system stabilizes and neither variable is driving. This means that regardless of specific *SL* or *EL* values, as long as both are greater than 32, the system performance is adequately characterized by the combination of the two, which is the *ESL* value. Because the goal of this system is to achieve adequate system performance at the lowest *SNR* possible with the least amount of transmitted energy, *EL* can be increased to a maximum practical physical size, while reducing *SL*, which is directly related to transmitted energy, to the minimum length required to achieve specific system performance characteristics.

C. PASL CONCLUSION

This chapter introduced PASL as a possible method for antenna arrays to detect and synchronize with an incoming signal from an unknown direction. The PASL method maximizes the performance of large antenna arrays by taking advantage of the zero-mean nature of AWGN, and several mathematical processes, to determine the presence of a known signal. A series of high-end estimates for *ESL* required for various performance levels were created using the results of Monte Carlo simulations and provide a baseline for predicting *SL* and *EL* required to facilitate detection and synchronization at very low *SNR* values (<-20 dB).

Although the PASL process shows promise for the passive detection and synchronization of a signal, it is highly computationally intensive. For instance, a single run of the PASL process for system using an $SL = 256$ and $EL = 256$ takes an average of

2.4 seconds on a Surface Pro 6 computer. The largest computational requirement is the application of many steering vectors to each new sample received across an array. As array sizes grow, the number of individual antenna element samples increases and the step size of the sweep decreases, requiring a more powerful computational system to maintain real-time operation. However, should a system be capable of the computational load, and an array size large enough, the PASL process can theoretically achieve detection and synchronization at any *SNR* value.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. SIGNAL DOA ESTIMATION

A. PURPOSE

DOA estimation is a critical part of UECP and is used to determine the gNB response direction for the connection reply. Additionally, the DOA estimate is used to correct the phase shift of the signal received at each antenna element to reduce bit errors in the payload.

1. Estimation of Response Direction

The UE is sending an omnidirectional connection request because the relative location of the gNB is unknown. Once the gNB detects the preamble of the connection request it can estimate the DOA for the received signal and in return use that information in the connection response (Figure 55). Because multipath effects are assumed negligible in this scenario this DOA can be used to beam steer the response of the gNB directly to the UE. This is critical element in the UECP in that an inaccurate DOA would decrease the likelihood of the UE receiving the connection reply and increases the amount energy classified as stray emissions.

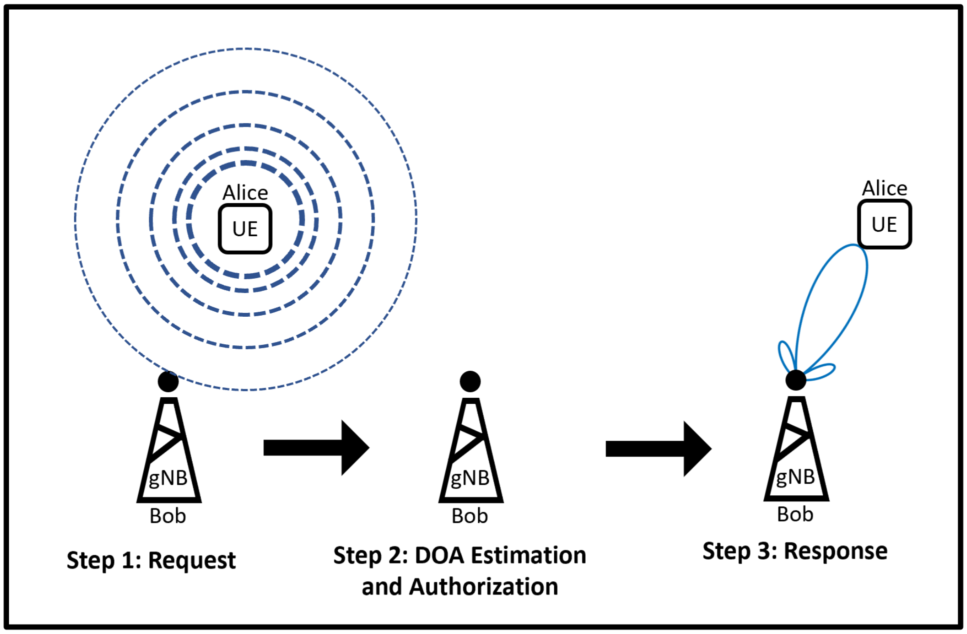


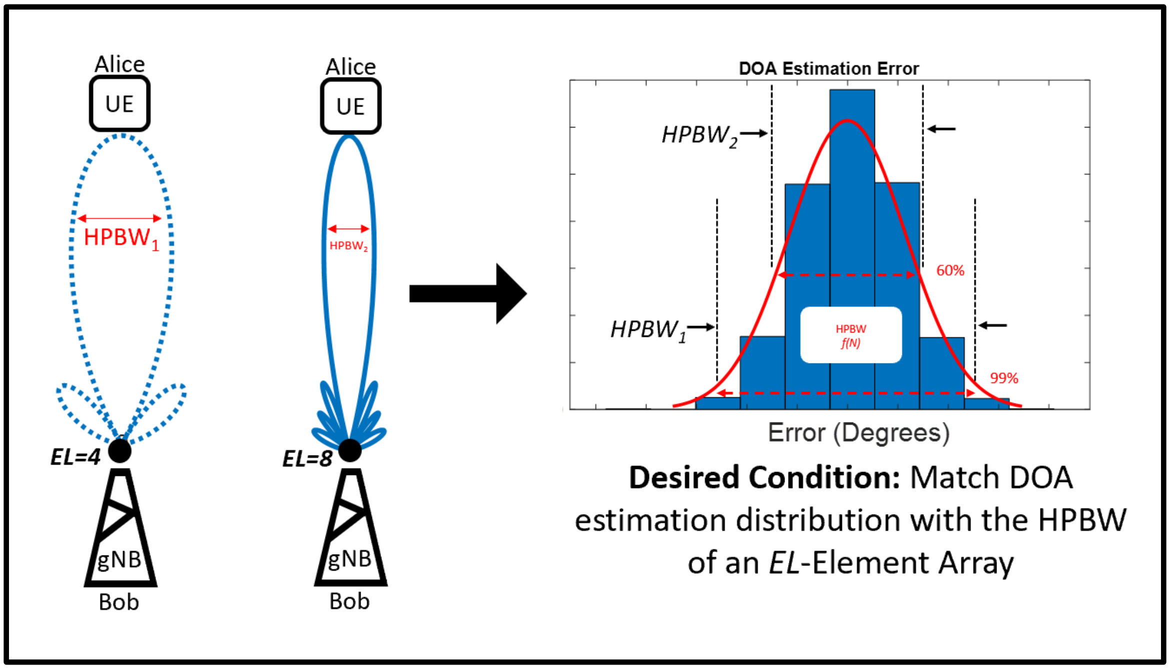
Figure 55. DOA Based Off Connection Request Illustration

2. Correction of Payload for Demodulation

Due to the requirement for the system to operate at low SNRs, BER is a fundamental concern within the payload. Because the signal is being received by an antenna array, vice a single element, the DOA can be used to correct the signal at each element before summation, which in turn decreases the BER of the payload. This will be discussed in greater detail in a subsequent section.

B. SELECTION CRITERIA

The DOA process both corrects the payload of the connection request and determines the return direction for a connection reply, which means a precise estimate is desired. However, increasing accuracy requires increasing computational power, processing time, or signal strength. Instead, a minimum suitable DOA estimate is required to ensure process efficiency. Referring to Figure 55, the connection reply must return directly to the UE. Should the connection reply not be directed properly at the UE, the amount of energy classified as stray emissions increases, and the likelihood of the UE properly receiving the reply decreases. Determining the minimum DOA estimate accuracy required to preserve the ability of the system to operate properly requires knowledge of the array size being used. Figure 56 shows a response to the UE occurring from a gNB with two separate array sizes: $EL = 4$ and $EL = 8$.



Desired Condition: Match DOA estimation distribution with the HPBW of an *EL*-Element Array

Figure 56. DOA Accuracy as a Function of Array Size

As the array size increases, the HPBW of the response signal decreases, requiring a more precise DOA estimate to prevent the main lobe of the response from missing the target UE. Therefore, the requirement for the accuracy of the DOA estimate must be based upon the size of the array being used by the gNB. If the HPBW of a specific array is used as the starting point $DOA_{error} \leq \frac{1}{2}HPBW$ is the requirement to ensure the main lobe of the response is sufficiently directed at the requesting UE.

Figure 56 also shows a mock DOA estimate error distribution along with the width of two separate HPBWs created by arrays of different sizes. For illustration purposes, each of the HPBWs was placed at a particular confidence interval on the DOA estimate error distribution. If this were the actual error distribution of a DOA estimation process, there is a 99% chance the DOA estimate would be sufficient to ensure the UE was in the main lobe of the connection response produced by the array responsible for $HPBW_1$. However, if the same error distribution existed for an array that produced $HPBW_2$, then there is only a 60% chance the DOA estimate would result in the UE being within the main lobe of the connection reply. Due to the impacts of AWGN on the random distribution of the DOA estimate error, 100% confidence cannot be achieved. However, for this research, the DOA estimate variance can be tied to a confidence interval that is equal to the HPBW. Performance will be based on 99.9%, 99%, 95%, and 80% confidence levels.

C. DIRECTION OF ARRIVAL PROCESSES

Although many algorithms exist for DOA estimation, only MUSIC was chosen for analysis and comparison against the PASL method of DOA estimation. MUSIC was chosen due to its widespread use and high-resolution DOA estimation capability [23].

1. Multiple User Signal Classification

MUSIC is an algorithm specifically designed for high-resolution DOA estimation and is based on utilizing the noise-subspace of a signal. Because this work is an application of MUSIC, this section is intended only as an introduction to the process. A more comprehensive explanation and associated mathematics can be found in *Multiple Emitter Location and Signal Parameter Estimation* [23] by Ralph Schmidt.

The effectiveness of MUSIC is based on the requirement that a known number of signals is present, and those signals are orthogonal. These requirements are acceptable for this analysis since a core assumption is that connection request transmissions collisions will not occur and only one connection request signal will be present at a time. Figure 57 shows the output of the MUSIC algorithm when a single signal is present, arriving at 30^{o} off broadside to the array.

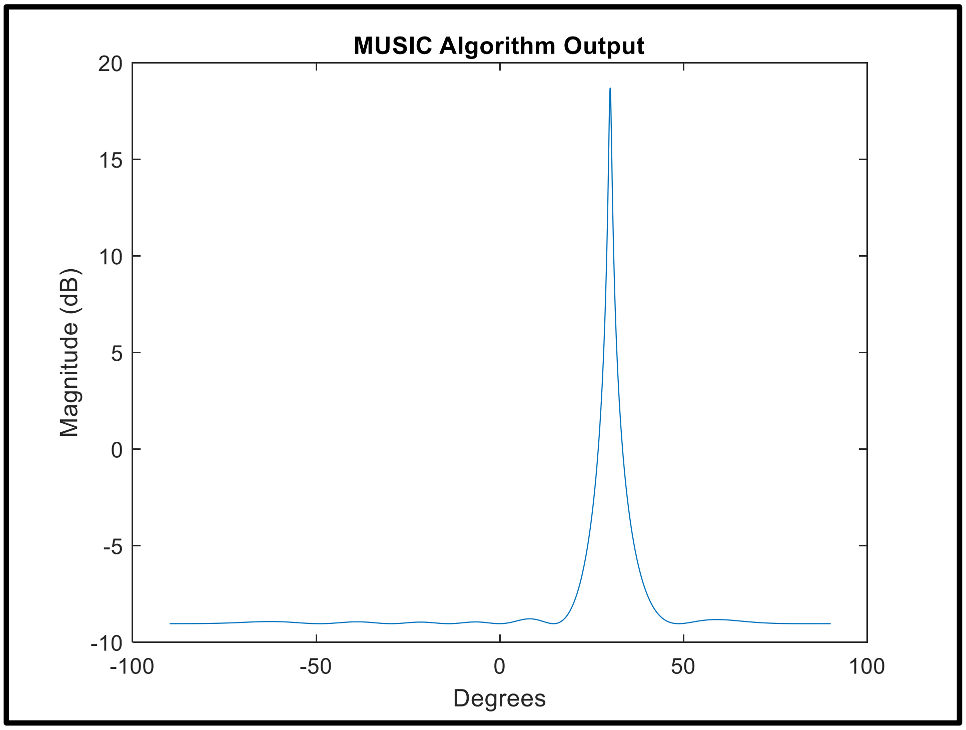


Figure 57. MUSIC Algorithm Output

The *SNR* for this plot was set at 10 dB, and there is a clear peak at 30^o in the output array. This peak is what will be stored for each iteration of a DOA Estimation Simulation and used to determine the DOA estimate variance. As the noise in the system increases this peak can become less pronounced and can lead to DOA estimation error.

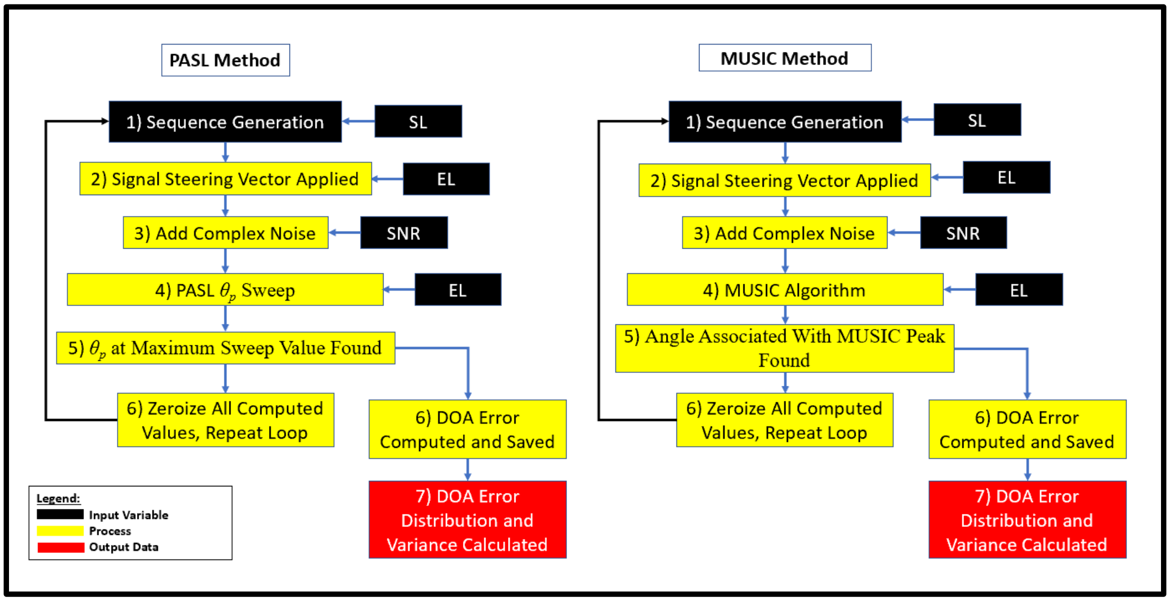
2. PASL Process Sweep Angle

From the previous PASL chapter, we see that the PASL process includes the creation of a series of steering arrays that are used to correct the incoming signal, from which a maximum signal value is determined. The θ_s angle at which the maximum signal value occurs (referred to as $\theta_{s-\max}$) can also be saved and used as a DOA estimate, and the variance of this estimate can be compared against the variance of the MUSIC DOA estimates.

D. PERFORMANCE AND COMPARISON OF DIRECTION OF ARRIVAL PROCESSES

1. Process and Simulation Explanation

Monte Carlo simulations were again used to characterize the DOA estimate variance of both the MUSIC and PASL methods. It is important to note that the variance produced in each method is a direct result of zero-mean AWGN which results in a zero-mean error distribution. Figure 58 shows the simulation process used for DOA estimation for both methods and is similar to the simulations used in preamble analysis and PASL detection and synchronization, with several modifications.



PASL Method
1) Sequence Generation
SL
2) Signal Steering Vector Applied
EL
3) Add Complex Noise
SNR
4) PASL θ_p Sweep
EL
5) θ_p at Maximum Sweep Value Found
6) Zeroize All Computed Values, Repeat Loop
6) DOA Error Computed and Saved
7) DOA Error Distribution and Variance Calculated
MUSIC Method
1) Sequence Generation
SL
2) Signal Steering Vector Applied
EL
3) Add Complex Noise
SNR
4) MUSIC Algorithm
EL
5) Angle Associated With MUSIC Peak Found
6) Zeroize All Computed Values, Repeat Loop
6) DOA Error Computed and Saved
7) DOA Error Distribution and Variance Calculated
Legend:
■ Input Variable
🟨 Process
🟥 Output Data

Figure 58. DOA Estimation Simulation Process

First, because this analysis is only meant to ascertain the DOA estimation capabilities of PASL and MUSIC, and not necessarily test the detection and synchronization results of those DOA estimations, the threshold input variable, leading/ lagging zero padding of the signal, and the matched filter used previously are no longer used. This isolates the DOA estimation processes as the only feature being tested for each process. The second major modification compared to previous simulations is that the output of this simulation is the DOA estimate error distribution and variance for each method.

If MUSIC produced a more accurate DOA estimate, that estimate could be used to unsteer the received signal (using Equation 24 with $\theta_{s-\max}$ replaced by the output of the MUSIC) and produce greater detection and synchronization performance. However, as will be demonstrated in this section, the DOA estimate produced by MUSIC is far less accurate than PASL given the specific attributes of the system being studied in this research (low signal energy and large array sizes). What this means is that the $\theta_{s-\max}$ angle produced during PASL will result in a corrected signal much closer to the original signal sent, and thus have far better detection and synchronization performance.

One other important note concerning this simulation is that both PASL and the MUSIC algorithms use an angular sweep to determine the angle at which a maximum occurs. Since a portion of the DOA estimate error, and therefore the variance, is caused by the granularity of the sweep angle step size, an equal step size of $\frac{1}{2}HPBW$ was used for both processes. Additionally, because both the MUSIC and PASL method's performance are affected by *SL* and *EL*, all simulations were run using equal input variable values for both methods.

2. Direction of Arrival Estimation Results

The MUSIC and PASL processes were compared using *SL* and *EL* ranges of 32, 64, and 128. The first analysis, seen in Figure 59, shows the DOA estimate variance of both processes at $SNR = 0$ dB. Each plot shows the results when either *EL* or *SL* is locked, and the other parameter varied. What is observed is that both processes are capable of very low DOA estimate variance regardless of the combination of parameters. However, UECP by design is required to function in very low SNR situations.

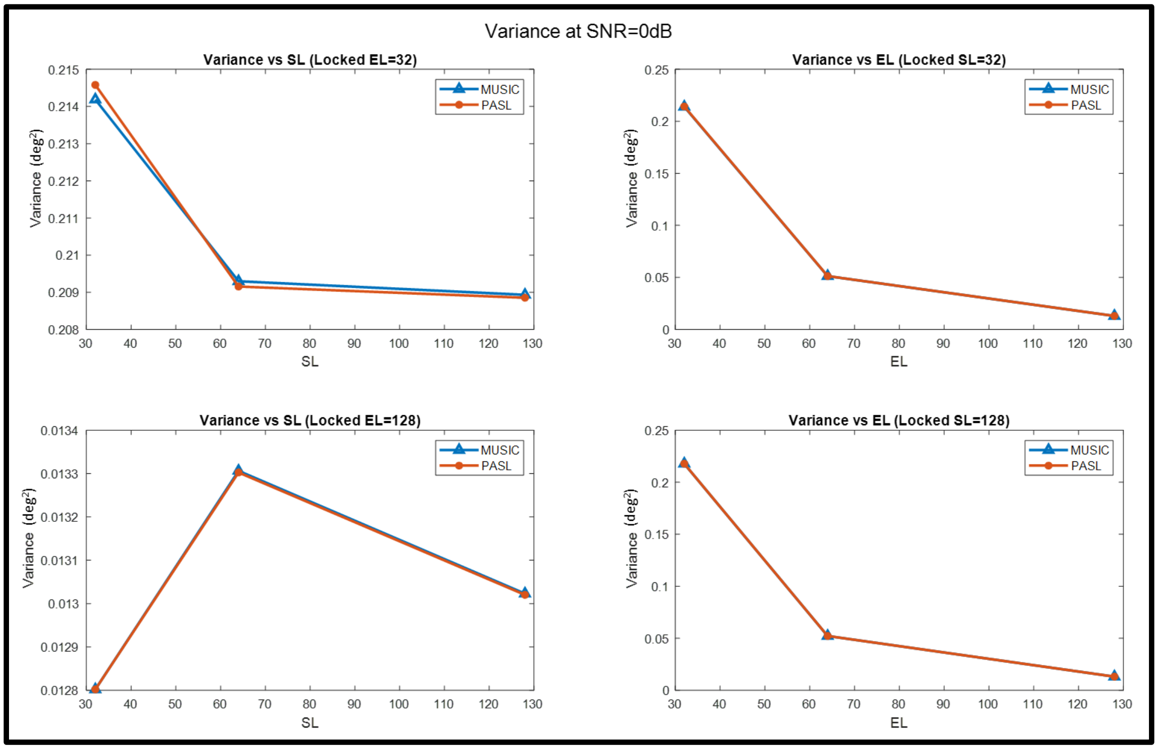


Figure 59. MUSIC and PASL DOA Variance at $SNR = 0$ dB

To understand the DOA estimation performance at low SNRs, the simulation was run again with *SNR* set to -20 dB. The results can be found in Figure 59 and show that as the *SNR* decreases, the DOA estimation performance of PASL greatly exceeds the performance of MUSIC. Even more importantly, we can see that when the *SL* is locked at a specific value, the performance increases of PASL are substantially higher than MUSIC as the *EL* value increases. With a locked *SL* of 32, and as *EL* increases from 32 to 128, the DOA estimation variance of MUSIC drops from 2298 to 1225 degrees squared, whereas PASL drops from 1842 to 120 degrees squared. Neither of these variances are sufficient for DOA estimation, but the trend shows PASL is far more effective when *EL* increases.

Observing the results when the *SL* is locked at 128, MUSIC drops from 1235 to 72 degrees squared, and PASL drops from 566 to 0.013 degrees squared. Additionally, at an *SL* of 128, PASL rapidly drops as *EL* increases from 32 to 64. This point will be addressed in greater depth in the following section. Because the goal of the system is to reduce signal energy by reducing *SL* (thus energy emitted), and capitalizing on the performance gains through raising *EL*, PASL shows a clear advantage over MUSIC in producing usable DOA estimates at lower SNRs.

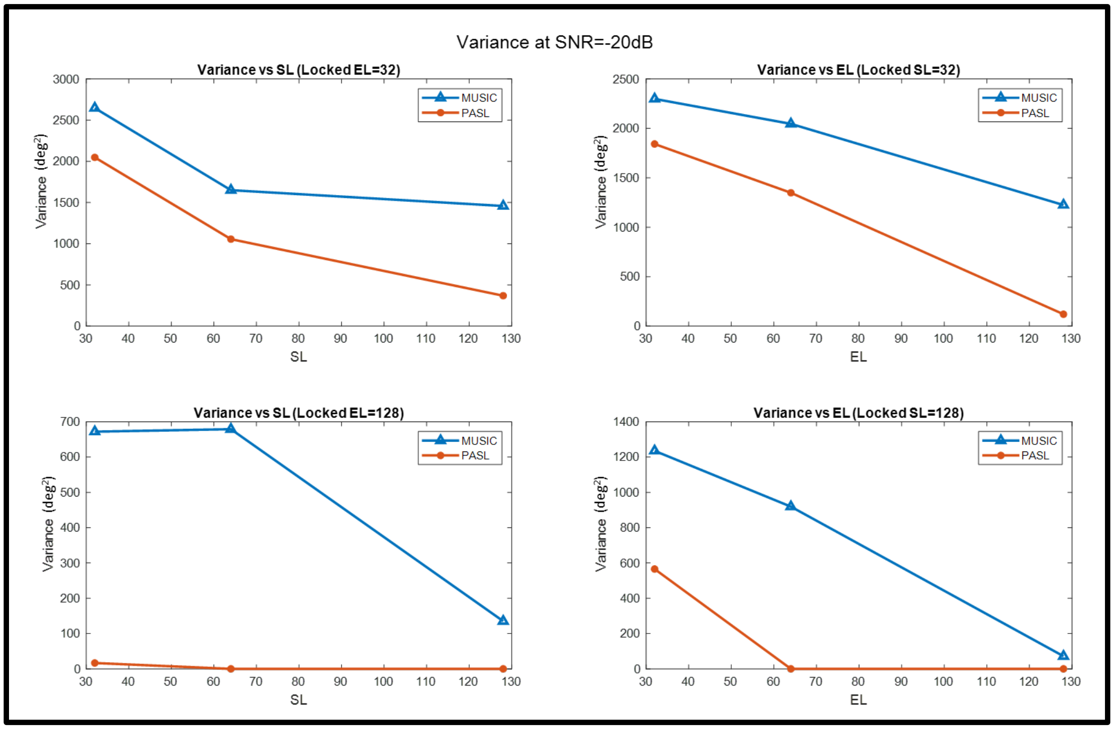


Figure 60. MUSIC and PASL DOA Variance at $SNR = -20$ dB

Now that PASL has been shown to produce more accurate at DOA estimates than MUSIC, specifically at the desired operating ranges and parameter values for UECP, it is important to determine if parity exists between the preamble detection and synchronization step and the DOA estimation step. To do this, we can compare the variance of PASL DOA estimates against the variance required to produce various confidence levels needed to ensure the UE is with the HPBW of the connection response. Variance for specific confidence levels was calculated using

$$\sigma_{CL}^2 = \left(\frac{HPBW\sqrt{n}}{z_{\alpha/2}}\right)^2 \text{(adapted from [24])}, \tag{32}$$

where *HPBW* is based on *EL* (computed using Equation 25), *n* is the number of Monte Carlo trials, and $z_{\alpha/2}$ is the critical value for the confidence level.

As with previous analyses, a multitude of Monte Carlo simulations were performed and plots for many different parameter values were analyzed, but only select plots are displayed to illustrate major points. All other parameter sets and resulting plots show the same behavior as those contained within this work. Figure 61 shows the DOA estimate variance of the PASL process with *EL* set to 32 and 128 and various *SL* values and *SNR* levels.

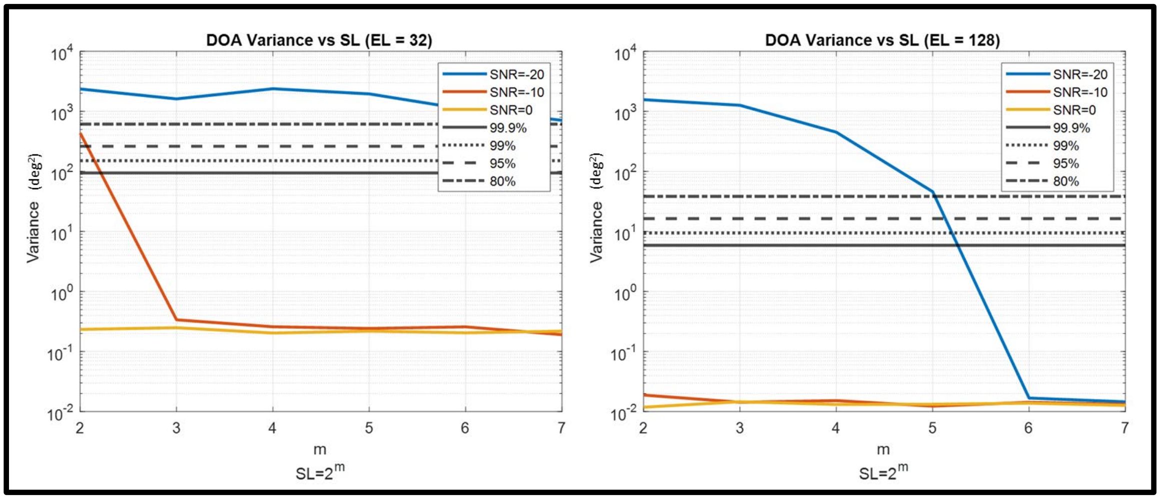


Figure 61. PASL DOA Variance vs. SL

As expected, at a given *EL* the variance of the DOA estimate decreases as *SL* increases. Referring back to Figure 50, we can see that at an *ESL* of 16384 the A_{ROC} is 0.999, and in Figure 60 an *ESL* of only 8192 (*EL*=128, *SL*=64) is required to adequately exceed the 99.9% confidence level for a DOA estimate. This means that if detection and synchronization occur the $\theta_{s-\max}$ value found during the PASL process is sufficiently accurate to use as the DOA estimate for the connection response signal.

E. DOA ESTIMATION CONCLUSION

This section detailed the two methods that can be used for DOA estimation: MUSIC, and PASL. MUSIC is a more powerful algorithm in that it can detect multiple orthogonal signals simultaneously, without prior knowledge of the signal, but is limited in its ability to detect a single unknown signal in a low SNR environment. PASL proved to be a more effective DOA estimation tool given its ability to estimate DOA by using a known signal value to correlate against a received signal that is steered through a series of possible DOA angles. Additionally, using PASL incurs no additional computational time. The $\theta_{s-\max}$ value found during the detection and synchronization step proved to be accurate enough to provide a high likelihood of the connection reply being directed towards the requesting UE.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. PAYLOAD CORRECTION AND USE

A. PURPOSE

The final critical element requiring analysis in UECP is the BER of the payload once detection and synchronization have occurred and the payload is demodulated and decrypted. The payload is important to the process in that it is used by the receiving device to authorize the sender and ensure a reply is appropriate. Errors within the payload decrease the ability of the gNB or UE to properly determine the validity of the connection request.

1. Maximum Gain in Direction of Arriving Signal

As discussed earlier in this work, the benefit of an array comes in the form of gain if the direction of the signal is known. The PASL process showed that by steering the incident signals on each antenna element and correlating the resulting signal against a known signal it can both determine the presence of a preamble, as well as produce a high-accuracy DOA estimate. Using this DOA estimate from the preamble, the system can steer the received payload such that maximum gain is achieved.

2. Authorization of UE and gNB

The payload contains the UE AuthCode, a time stamp, as well as EDAC (the purpose of which will be made clear in this section). If the BER is too high, the information needed to authorize the request, specifically the AuthCode and time stamp, will be corrupted and result in a failed authorization and thus no connection reply being sent. It is important to clarify the approach used to analyze BER within the context of this work. A perfect BER of zero would mean that if the AuthCode received is valid then there would be a zero probability of the requesting device not being validated. Any BER above zero would result in the possibility of a valid AuthCode not being validated if it is being compared directly to an authorized whitelist. The exact probability of a valid AuthCode being rejected would be a combination of the AuthCode length and BER in the system.

B. PERFORMANCE AND RESULTS

1. Process and Simulation

Monte Carlo simulations constructed in *MATLAB* were again used to analyze the effects of payload correction and the resulting BER of the payload. The simulation process can be seen in Figure 62.

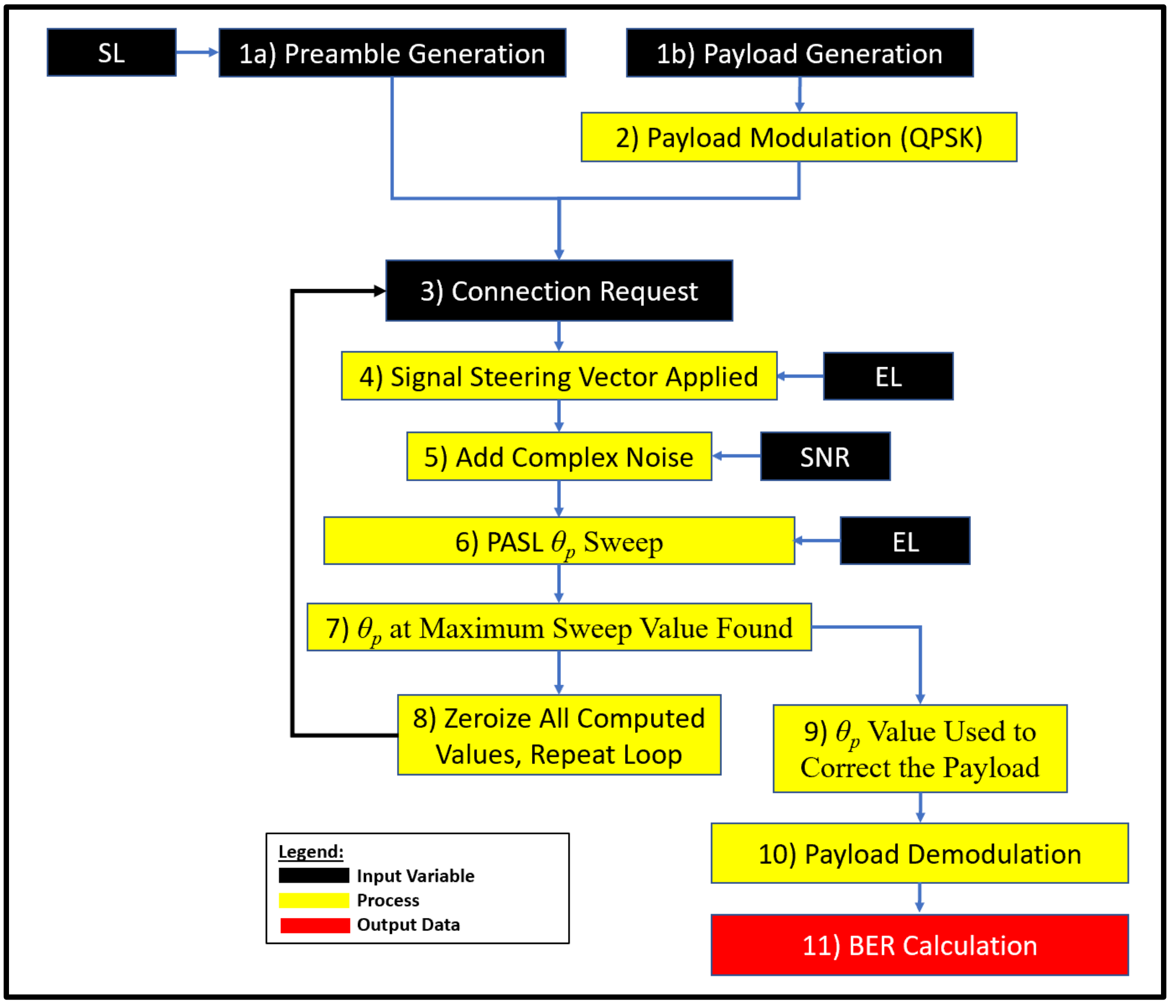


Figure 62. BER Testing Process

This simulation is similar to previous simulations run, with several modifications. First, along with preamble generation, there is also a payload generation, which is then modulated using QPSK. This modulation was used because QPSK shares the same BER as BPSK modulation but can transmit twice the information in the same signal length. Next, the preamble and payload are concatenated into a single connection request signal. The steering and reception of the signal follows previous simulation processes. For this simulation, however, once the $\theta_{s-\max}$ value is found from the PASL process, it is then used to correct the payload portion of the received signal (using Equation 24). Once that has occurred, the payload is then demodulated and compared against the original payload value to count bit errors and estimate BER.

2. Bit Error Rate Analysis

The first step in BER analysis is to determine the effectiveness of correcting the payload based upon the $\theta_{s-\max}$ value found during the PASL process. Figure 63 shows the BER simulation results for a PASL-corrected signal, an array that is not corrected, a single element, and lastly, the single element theoretical BER. Note that the horizontal axis is no longer *SNR*, but rather E_b / N_o since QPSK modulation was used, and because of this is shifted by -3 dB from the original *SNR* range of -20 to 0 dB. Theoretical *BER* was computed using

$$P_b \approx \frac{2}{\log_2 M} Q\left(\sqrt{\frac{2E_b \log_2 M}{N_0}} \sin\left(\frac{\pi}{M} \right) \right) \text{ [25],} \tag{33}$$

where *M* is the modulation order, E_b is the bit energy, and N_o is the noise power spectral density. With $M = 4$, as it is in this case, Equation 33 simplifies to

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0}} \right). \tag{34}$$

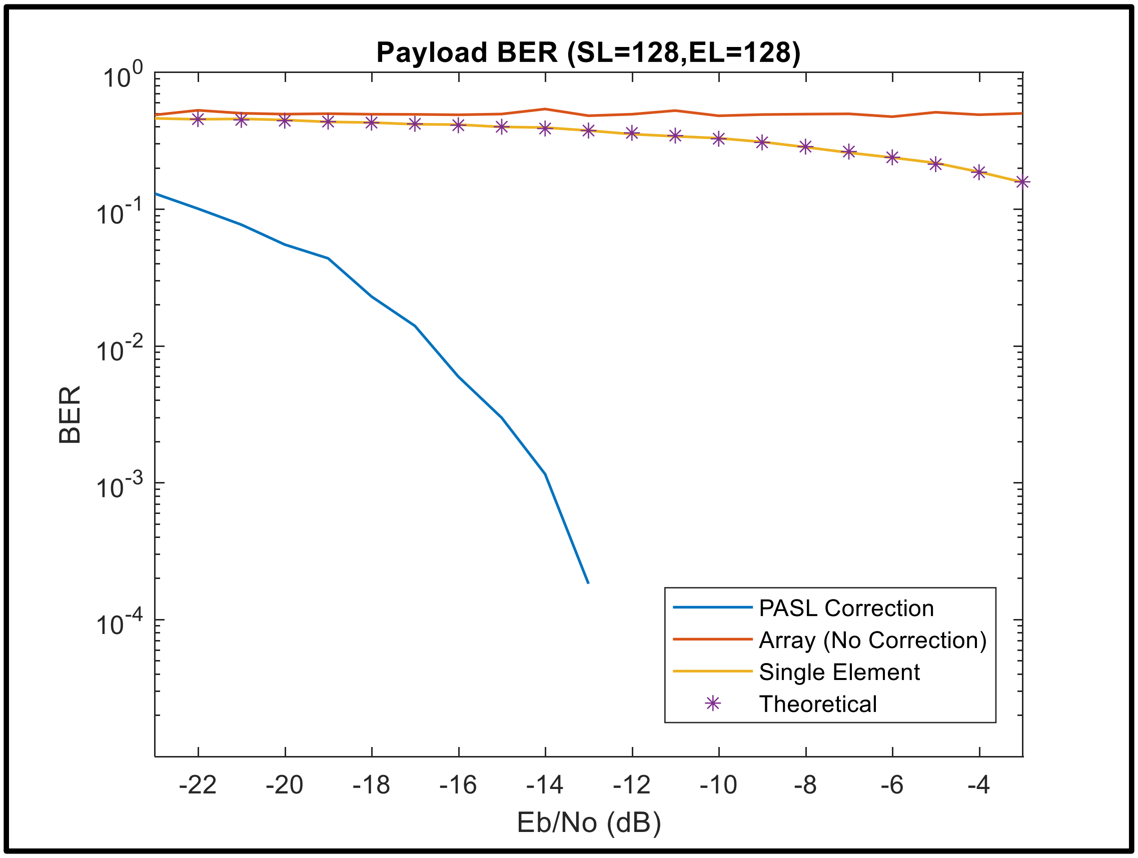


Figure 63. Payload BERs

The payload *BER* when no correction is applied is essentially 1/2, whereas the *BER* when PASL correction is applied is greatly reduced. It is also clear that the PASL correction has significant improvements over the *BER* when only a single antenna element was used. This analysis was done using only a set value for *SL* and *EL* (128), and a better understanding of the impacts of either parameter is important.

The next analysis sought to determine the impacts of either *SL* or *EL* on the *BER* of the payload by fixing one parameter at 32 and varying the other through a range of values from 8 to 256 (Figure 63).

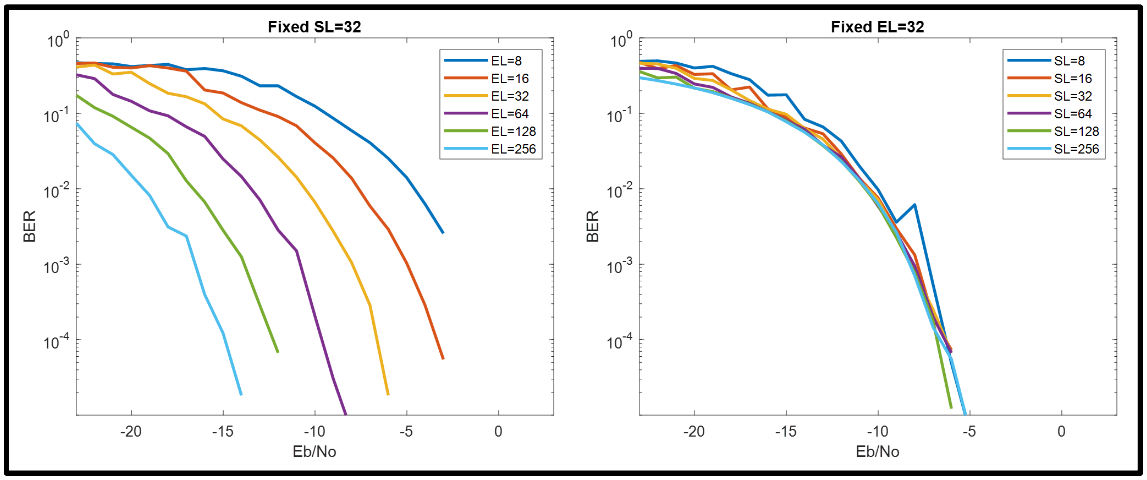


Figure 64. BER with Varying *SL* and *EL*

What is clearly seen is that at a fixed *EL*, increasing the *SL* of the preamble has very little impact on reducing the *BER* of the payload after it is corrected using the outcome of the PASL process. However, when the preamble length (*SL*) is fixed, increasing *EL* has significant impacts on reducing the *BER* of the payload. This is a very good characteristic in that UECP seeks to reduce signal energy (lower *SL*) and instead capitalize on very large arrays (larger *EL*) to maintain system usability.

The final point concerning Figure 64 is that the *BER*, even with very large *EL* values, is prohibitively high, and regardless of AuthCode length and validation method would result in the rejection of some percentage of valid AuthCodes. This work does not specify a BER requirement as that would be system specific attribute based on the specific system application and validation processes used.

C. PAYLOAD CORRECTION CONCLUSION

This section showed that BER can be improved by using the $\theta_{s-\max}$ value determined during the PASL process to correct the payload signals received at the array elements before demodulation. Additionally, BER showed very little improvement when *SL* (preamble length in this case) is increased but showed significant improvement as *EL* increased. This attribute aligns with the focus of this research in minimizing transmitted energy and instead capitalizing on the benefits of large antenna arrays. Lastly, even with payload correction before demodulation, the BER of the system is high enough to compromise the information contained in the payload and therefore requires EDAC to ensure proper authorization and response. The specific EDAC method used and BER requirement is going to be system dependent and beyond the scope of this work.

IX. SUMMARY, CONCLUSION, AND FOLLOW-ON WORK

A. SUMMARY AND CONCLUSION

The UECP process seeks to provide a new method for devices to connect in EM-sensitive environments while maintaining the functionality of the 5G NR architecture. The primary driver for developing a new method of initial access was to reduce the amount of energy classified as stray emissions that occur during commercial 5G NR operations. This can be accomplished in two steps. First, the 5G NR initial access procedures can be replaced with a process that eliminates the requirement for the transmission of periodic broadcast signals in the form of SSBs to search for UEs within the coverage area. Second, a novel process was required that was able to function at much lower SNRs than traditional 5G NR initial access procedures.

UECP replaces 5G NR UE search processes with a UE-side connection request, which a gNB can use to authorize the UE and estimate a DOA for the connection reply. By initiating the connection from the UE, we can capitalize on the larger antenna arrays that generally exist at the gNB. This greatly reduces the stray emissions created by a gNB during traditional 5G NR search processes. With this new method, however, came new challenges. Because the connection request must be transmitted omnidirectionally and should produce as little signal energy as possible, the gNB must be able to detect a request at very low SNRs. This was solved by the development of the novel PASL process, which uses various steering vectors to correct the incident signal across all antenna elements before correlating them against the known preamble signal value, improving detection and synchronization. The performance of this method was shown to be reliant on the size of the antenna array, given the incoming signal preamble met a minimum length requirement.

The PASL process also demonstrated higher fidelity DOA estimates when compared to the commonly used DOA algorithm, MUSIC, and is capable of estimating the DOA such that a requesting UE will be within the HPBW of the connection reply with a high level of certainty. The DOA estimate output of the PASL process can also be used to correct the payload signals received before demodulation, which greatly decreased the

BER. However, due to the SNR ranges this system should be operating in, the BER still proved to be prohibitively high and would require EDAC to ensure the information can be recovered and used for authorization.

Throughout this research, it was shown that all the processes and methods used would benefit from the creation and utilization of very large antenna arrays. As array sizes, frequencies used, and computational power of systems increase, the methods proposed in this work could facilitate initial access of 5G NR-based systems in environments where EM emissions need to be tightly controlled.

B. FOLLOW ON RESEARCH AND PRACTICAL CONSIDERATIONS

1. DDOS and Jamming Protection

Although the attack model in this work assumed Eve had the ability to craft and send a connection request, it assumed Eve did not have the ability to jam either the UE or gNB, or continually transmit in a denial-of-service type attack. These are important considerations for the battlefield environment and are worthy of study should this system ever be implemented.

2. EDAC for Payload

It was shown that despite the ability of UECP to detect, synchronize, and compute accurate DOAs, it is unable to reduce the BER of the payload enough to allow information to be recovered directly. There are many methods of EDAC used within commercial communications systems, and further study is required to determine which method of EDAC works most efficiently with the UECP process.

3. PASL Mathematics Efficiency

The PASL method is very effective in facilitating the connection of two devices within the constraints of the environment mentioned in this work. However, the PASL process is highly computationally intensive in its current form. Because PASL must occur in real-time, the efficiency of the mathematics is highly important. Although the currently proposed mathematical processes work, further study into optimizing and increasing the efficiency of the process is warranted.

4. Signal Length Optimization/Large Value Simulations

Throughout this work signal length and array length were two primary parameters used for analysis in each step. Although it was shown that a trade space exists between these two variables, there also exists a lower bound where UECP performance is difficult to predict. Additionally, as the signal length decreases, the array length must increase, but the exact performance of the system at ultra-high array lengths and ultra-low sequence lengths has not been fully explored. The PASL process is computationally intensive, and as either the sequence or array values get too large, the computational time required becomes prohibitive, and high-power computational platforms would be required to conduct the Monte Carlo simulations. Further analysis at these extreme values using a high-power computer would be prudent to determine if the characterizations presented in this work are valid in more extreme cases.

5. Signal Length and Time Stamp Analysis

The requirement for a time Stamp was presented earlier in this work, but a more definitive determination of the range of allowable values, based on the connection request length is required. As the signal length increases, the probability of Eve being able to randomly create a signal that could fool either the UE or gNB decreases. The larger the signal, the more time it would take Eve to test all possible signal values, but the greater the energy emitted during the connection request process. Decreasing signal length decreases the time it would take Eve to craft a valid connection request through random signal creation and would therefore force a decrease in the acceptable time stamp window. The practical application of UECP would require some knowledge of Eve’s ability to craft and transmit signals, as well as a probability threshold of Eve being able to craft a valid request through arbitrary connection request creation that could be used to determine the maximum allowable time stamp window.

6. Retransmission Optimization

UECP is built to work in low SNR environments, and part of this is the implementation of a signal power step increase each time a UE connection request fails to solicit a reply. Further exploration of the effects of a signal power increase on the system's ability to establish a connection and optimum power step size would be prudent prior to implementing UECP in a real-world environment.

7. Optimum Array Sizes

Throughout this work array sizes up to 8192 elements were used as a theoretical upper bound maximum. This size array, even at the upper end of 5G NR frequencies would still produce a physical array that is too large for practical use. Further study into the optimum array size to balance gains realized with real world physical size constraints

LIST OF REFERENCES

[1] D. H. Berger, “Commandant’s Planning Guidance - 38th Commandant of the Marine Corps,” United States Marine Corps, Quantico, VA, 2019.

[2] B. Turley, “Qualcomm’s Snapdragon X50 in the wild: Analyzing 5G mobile performance in U.S. cities,” SpeedTest, 14 August 2019. [Online]. Available: https://www.speedtest.net/insights/blog/qualcomm-snapdragon-x50-mobile-performance-us-cities/. [Accessed 16 June 2021].

[3] Ericsson, “A guide to 5G network security,” Kista, Sweden, 2018.

[4] Qualcomm, “How 5G massive MIMO transforms your mobile experience,” 20 June 2019. [Online]. Available: https://www.qualcomm.com/news/onq/2019/06/20/how-5g-massive-mimo-transforms-your-mobile-experiences. [Accessed 9 June 2021].

[5] J. Melnick, “Top 10 most common types of cyber attacks,” Netwrix Blog, 18 May 2021. [Online]. Available: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/. [Accessed 2 June 2021].

[6] D. Callaway, “U.S. national archives,” 2 November 2004. [Online]. Available: https://nara.getarchive.net/media/us-marine-corps-usmc-marines-assigned-to-the-2nd-marine-air-wing-attend-a-training-59751f. [Accessed 14 May 2021].

[7] “5G wireless access: An overview,” Ericsson, April 2020. [Online]. Available: https://www.ericsson.com/498a10/assets/local/reports-papers/white-papers/whitepaper-5g-wireless-access.pdf. [Accessed 20 June 2021].

[8] “What is 5G NR,” Verizon, 06 12 2019. [Online]. Available: https://www.verizon.com/about/our-company/5g/what-is-5g-nr. [Accessed 22 May 2021].

[9] K. Pretz, “IEEE spectrum,” 12 November 2019. [Online]. Available: https://spectrum.ieee.org/news-from-around-ieee/the-institute/ieee-member-news/will-5g-be-bad-for-our-health. [Accessed 22 May 2021].

[10] S. A. Cedex, “5G; NR; overall description; stage-2,” ETSI, France, 2020.

[11] “5G NR initial access procedure: 5G NR random access procedure,” RF Wireless World, [Online]. Available: https://www.rfwireless-world.com/5G/5G-NR-Initial-Access-Procedure.html. [Accessed 2 June 2021].

[12] R. J. Mailloux, *Phased Array Antena Handbook* - Second Edition, Norwood, MA: Artech House, 2005.

[13] J. F. Harvey, M. B. Steer and T. S. Rappaport, “Exploiting high millimeter wave bands for military communications, applications, and design,” *IEEE Access,* vol. 7, 2019.

[14] E. M. Silva, F. J. Harris and G. J. Dolecek, “On preamble design for timing and frequency synchronization of OFDM systems over Rayleigh fading channels,” in *18th International Conference on Digital Signal Processing*, 2013.

[15] C. W. Therrien, *Discrete Random Signals and Statistical Signal Processing*, Englewood Cliffs: Prentice-Hall, 1992.

[16] R.-A. Pitaval, B. M. Popovic, F. Berggren and P. Wang, “Overcoming 5G PRACH capacity shortfall by combining Zadoff-Chu and M-Sequences,” *IEEE International Conference On Communications,* vol. 05, pp. 1-6, 2018.

[17] P. Borwein and M. J. Mossinghoff, “Wieferich pairs and Barker sequences,” *LMS Journal of Computation and Mathematics,* vol. 17, no. 1, pp. 24-32, 2014.

[18] Y. Akaiwa, *Introduction To Digital Mobile Communications* - Second Edition, Hoboken, New Jersey: Wiley, 2015.

[19] Q. Tan and Y. Wang, “Preamble detection based on cyclic features of Zadoff-Chu Sequences for underwater acoustic communications,” *IEEE Signal Processing Letters,* vol. 26, no. 8, pp. 1192-1196, 2019.

[20] F. T. Ulaby and U. Ravaioli, *Fundamentals of Applied Electromagnetics* - Seventh Edition, Upper Saddle River, New Jersey: Pearson, 2015.

[21] T. E. Tuncer and B. Friedlander, *Classical and Modern Direction-of-Arrival Estimation*, Burlington, MA, USA: Elsevier, 2009.

[22] J. Stewart, Calculus - Early Transcendentals, Belmont, CA, USA: Thompson, 2008.

[23] R. O. Schmidt, “Multiple emitter location and signal parameter estimation,” *IEEE Transactions On Antennas and Propogation,* Vols. AP-34, no. 3, pp. 276-280, 1986.

[24] L. Gonick and W. Smith, *The Cartoon Guide to Statistics*, New York, New York, USA: HaperResource, 1993.

[25] T. Ha, *Theory and Design of Digital Communication Systems*, Cambridge, England: Cambridge University Press, 2010.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California