



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2022-09

USAGE OF 5G IN UAV MISSIONS FOR ISR

Leviton, Melissa C.

Monterey, CA; Naval Postgraduate School

<https://hdl.handle.net/10945/71075>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

USAGE OF 5G IN UAV MISSIONS FOR ISR

by

Melissa C. Leviton

September 2022

Thesis Advisor:

Co-Advisor:

Chad A. Bollmann

Darren J. Rogers

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>
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 2022	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE USAGE OF 5G IN UAV MISSIONS FOR ISR			5. FUNDING NUMBERS
6. AUTHOR(S) Melissa C. Leviton			
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) Traditionally, UAVs operate on a one-to-one transmission mode where the UAVs have one data link between one ground command and control station. Therefore, the radius at which the UAV can travel is limited. The bandwidth of the traditional link is limited to less than 8Mbps and the quality of the video is below 1080p. 4G technology has been applied to the UAV data link to solve some of these more traditional problems. However, the 4G data link also comes with its own limitations such as downlink interference and can only be useful in scenarios with a high delay tolerance. 5G technology solves the spatial coverage problem by increasing the number of antenna modules and fusing the antenna module and radio hardware. The result is a three-dimensional beam. The UAV itself can be used as a base station for the 5G network, so that all ground stations can be connected as the UAV continues its flight path. UAVs can also be used as aerial nodes in a larger swarm network to offer coverage over larger areas. Additionally, the use of the OpenStack architecture can allow the Navy to customize protocols as desired. The proposed research includes investigating how current UAV to ship/shore communications are conducted. The objective of this thesis is to determine if 5G communications are possible between UAV and ship/shore assets, to successfully connect a UAV to the 4G and possibly 5G network and to determine if UAVs can send data between each other to the ground station.			
14. SUBJECT TERMS 5G, UAV			15. NUMBER OF PAGES 129
			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

Approved for public release. Distribution is unlimited.

USAGE OF 5G IN UAV MISSIONS FOR ISR

Melissa C. Leviton
Lieutenant Commander, United States Navy
BS, United States Naval Academy, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

**NAVAL POSTGRADUATE SCHOOL
September 2022**

Approved by: Chad A. Bollmann
Advisor

Darren J. Rogers
Co-Advisor

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Traditionally, UAVs operate on a one-to-one transmission mode where the UAVs have one data link between one ground command and control station. Therefore, the radius at which the UAV can travel is limited. The bandwidth of the traditional link is limited to less than 8Mbps and the quality of the video is below 1080p. 4G technology has been applied to the UAV data link to solve some of these more traditional problems. However, the 4G data link also comes with its own limitations such as downlink interference and can only be useful in scenarios with a high delay tolerance.

5G technology solves the spatial coverage problem by increasing the number of antenna modules and fusing the antenna module and radio hardware. The result is a three-dimensional beam. The UAV itself can be used as a base station for the 5G network, so that all ground stations can be connected as the UAV continues its flight path. UAVs can also be used as aerial nodes in a larger swarm network to offer coverage over larger areas. Additionally, the use of the OpenStack architecture can allow the Navy to customize protocols as desired.

The proposed research includes investigating how current UAV to ship/shore communications are conducted. The objective of this thesis is to determine if 5G communications are possible between UAV and ship/shore assets, to successfully connect a UAV to the 4G and possibly 5G network and to determine if UAVs can send data between each other to the ground station.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1	Introduction	1
1.1	Motivation and Context	1
1.2	Research Questions	1
1.3	Background	2
1.4	Scope and Limitation.	2
1.5	Overview of Equipment and Network Setup.	2
1.6	Overview of Methodology.	3
1.7	Overview of Results	4
1.8	Conclusion.	4
2	Background and Literature Review	5
2.1	Overview of 5G Networks.	5
2.2	Subscriber Identification Module Cards	10
2.3	International Mobile Equipment Identity	12
2.4	Comparison to 4G	12
2.5	Use Case Classifications	13
2.6	Selected Prior 5G Throughput Testing	14
2.7	Overview of Unmanned Aerial Vehicles used in the U.S. Military	16
2.8	Current Limitations of UAV to Ship/Shore Assets	21
3	Experimental Design	23
3.1	Equipment	23
3.2	Experiment Connection Set Up.	32
3.3	Experimentation Constraints	32
4	Results	35
4.1	Use Case Scenario.	35
4.2	Methodology of Experimentation	35

4.3	Analysis of 4G Experiments	42
4.4	Analysis of 5G Experiments	44
4.5	Improvements for Future Tests	65
5	Conclusion and Future Work	67
5.1	Summary	67
5.2	Application and Benefit of Use/Conclusion	68
5.3	Future Work	69
	Appendix A Payload Assembly and Configuration	71
A.1	Physical Assembly.	71
A.2	Configure 5G Hat	77
A.3	Enable Camera	79
	Appendix B Configuring the Amarisoft Network	81
B.1	Quarterly Update Installation Instructions.	81
B.2	4G LTE Network Configuration	82
B.3	4G LTE Band Configuration	83
B.4	5G Network Configuration	84
B.5	5G Band Configuration	86
B.6	Changing the nodeB Pointer Configuration File	87
B.7	Location of 4G and 5G Configuration Files	89
	Appendix C Uplink and Downlink Testing	91
C.1	Uplink Testing	91
C.2	Throughput Testing	95
C.3	MATLAB Code and Testing Data Files Location.	97
	List of References	99
	Initial Distribution List	105

List of Figures

Figure 2.1	U.S. Air Force Global Hawk. Source: [32]	17
Figure 2.2	U.S. Navy Triton. Source: [36]	18
Figure 2.3	U.S. Air Force Scan Eagle. Source: [40]	19
Figure 2.4	U.S. Navy Fire Scout. Source: [43]	20
Figure 3.1	Amarisoft Callbox Classic. Source: [47]	23
Figure 3.2	Amarisoft Callbox Classic Inner View. Source: [47]	24
Figure 3.3	Amarisoft Sample SIM Cards	25
Figure 3.4	Raspberry Pi 4. Source: [49]	27
Figure 3.5	Raspberry Pi Camera Model 2 NoIR. Source: [52]	28
Figure 3.6	SIM8200EA-M2 5G Hat for Raspberry Pi. Source: [53]	29
Figure 3.7	FreeFly Alta X. Source: [4]	31
Figure 3.8	Network Diagram	32
Figure 4.1	Theoretical Signal Power Received vs Distance	39
Figure 4.2	Downlink Throughput Test Results - Raw Data	41
Figure 4.3	Downlink Throughput Test Results - Formatted Data	42
Figure 4.4	1x1 SISO Configuration Signal Power vs Theoretical Signal Power	46
Figure 4.5	1x1 SISO Configuration Signal Power	47
Figure 4.6	2x2 MIMO Configuration Signal Power	48
Figure 4.7	4x4 MIMO Configuration Signal Power	50
Figure 4.8	5 MHz Bandwidth Received Signal Power	52

Figure 4.9	10 MHz Bandwidth Received Signal Power	53
Figure 4.10	15 MHz Bandwidth Received Signal Power	54
Figure 4.11	20 MHz Bandwidth Received Signal Power	55
Figure 4.12	1x1 SISO Configuration Throughput	57
Figure 4.13	2x2 MIMO Configuration Throughput	58
Figure 4.14	4x4 MIMO Configuration Throughput	59
Figure 4.15	5 MHz Bandwidth Throughput	60
Figure 4.16	10 MHz Bandwidth Throughput	61
Figure 4.17	15 MHz Bandwidth Throughput	62
Figure 4.18	20 MHz Bandwidth Throughput	63
Figure A.1	Assembled Payload	71
Figure A.2	Installation of 5G Hat and Raspberry Pi: Equipment Required. Source: [66]	72
Figure A.3	Installation of 5G Hat and Raspberry Pi: Steps 1-3. Source: [66]	73
Figure A.4	Installation of 5G Hat and Raspberry Pi: Steps 4-5. Source: [66]	74
Figure A.5	Installation of 5G Hat and Raspberry Pi: Steps 6-7. Source: [66]	75
Figure A.6	Installation of 5G Hat and Raspberry Pi: Step 8. Source: [66]	76
Figure A.7	Raspberry Pi 4 OS Install	77
Figure A.8	Waveshare Instructions for 5G Hat Driver Install. Source: [68]	77
Figure A.9	RNDIS Dial-up Command. Source: [69]	78
Figure A.10	ifconfig -a wwan0. Source: [68]	78
Figure A.11	Minicom Installation Commands. Source: [68]	79
Figure A.12	AT Command from RNDIS Instructions. Source: [69]	79
Figure A.13	5G Networking Commands. Source: [68]	79

Figure A.14	Camera Enable Instructions. Source: [67]	80
Figure B.1	Screenshot of Amarisoft Files Folder	81
Figure B.2	Screenshot of LTE Status	82
Figure B.3	4G LTE Default Configuration Options	83
Figure B.4	4G LTE Band 3 in Configuration File	83
Figure B.5	4G LTE Band 7 in Configuration File	84
Figure B.6	Top of 5G Configuration File with a 1x1 SISO with a 5MHz bandwidth configuration	85
Figure B.7	2x2 MIMO Configuration with 50 MHz Bandwidth	85
Figure B.8	4x4 MIMO Configuration with 15 MHz Bandwidth	86
Figure B.9	5G Bands	87
Figure B.10	eNodeB Configuration Pointer File	88
Figure B.11	eNodeB Default Configuration File	88
Figure B.12	Screenshot of changing eNodeB Pointer to gnb-sa.cfg	89
Figure C.1	Command to Start Video Streaming on Payload. Source: [70]	91
Figure C.2	Command to Open Minicom	92
Figure C.3	Minicom Timestamp Added	92
Figure C.4	CSQ Script	93
Figure C.5	Minicom CSQ Script	93
Figure C.6	Minicom CSQ Script Output in Minicom	94
Figure C.7	Minicom CSQ Script	94
Figure C.8	iPerf Server Start Command on Raspberry Pi	95
Figure C.9	ENB Trace Example for Downlink Testing	96

Figure C.10 iPerf Client Start Command on Amarisoft Callbox Classic 96

List of Tables

Table 2.1	4G vs 5G. Source: [27]	13
Table 2.2	5G-DRIVE Warsaw, Poland NSA Test Results. Source: [30]	16
Table 3.1	Amarisoft Test SIM Card Data	26
Table 3.2	SIM Card ICCID	26
Table 3.3	Google Pixel 4a. Source: [54].	30
Table 3.4	Google Pixel 3a. Source: [56]	30
Table 3.5	OnePlus A6003. Source: [58]	31
Table 4.1	Minicom Signal Power Quality Ranges and Classifications. Source: [63]	40
Table 4.2	4G Phone Testing Data Using Band 3	43
Table 4.3	4G Phone Testing Data Using Band 7	43
Table 4.4	1x1 SISO 0 m and 1 m Signal Power Measurements	44
Table 4.5	2x2 MIMO 0 m and 1 m Signal Power Measurements	45
Table 4.6	4x4 MIMO 0 m and 1 m Signal Power Measurements	45
Table 4.7	Average Commercial Download Speeds. Source: [65]	56

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

3GPP	3rd Generation Partnership Project
5GC	5G core
AF	application function
AMF	access and mobility management function
API	application programming interface
APN	access point name
ARFCN	absolute radio-frequency channel number
AUSF	authentication server function
CA	carrier aggregation
CC	component carrier
CCW	Center for Cyber Warfare
COTS	commercial off-the-shelf
DN	data network
eMBB	enhanced Mobile Broadband
eNodeB	evolved node B
EO	electro-optical
EPC	evolved packet core
eSIM	embedded subscriber identification module
EU	European Union

FDD	frequency division duplex
FIAC	fast inshore attack craft
FLIR	forward looking infrared
FR1	frequency range 1
FR2	frequency range 2
gNodeB	5G new radio base station
GSM	Global System for Mobile Communications
HD	high-definition
HDMI	high-definition multimedia interface
HISAR	Hughes integrated surveillance & reconnaissance
ICCID	integrated circuit card identity
ID	identification
IMEI	international mobile equipment identity
IMINT	imagery intelligence
IMS	internet protocol multimedia subsystem
IMSI	international mobile subscriber identity
IoT	internet of things
IP	internet protocol
IR	infrared
ISR	intelligence, surveillance, and reconnaissance
ITU	International Telecommunications Union
LAN	local area network

LCS	littoral combat ship
LRE	launch and recovery element
LTE	long term evolution
MBMS	multimedia broadcast multicast service
MBMSGW	multimedia broadcast multicast service gateway
MCC	mobile country code
MCE	mission control element
MFAS	multi-function active sensor
MIMO	multiple input, multiple output
MME	mobility management entity
mMTC	massive machine-type communications
MNC	mobile network code
MNO	mobile network operator
MSIN	mobile subscription identification number
MTI	moving target indicator
MU-MIMO	multi-user multiple input, multiple output
NEF	network exposure function
NF	network function
NPS	Naval Postgraduate School
NR	new radio
NRF	network function (NF) repository function
NSA	non-standalone

NSSF	network slice selection function
OFDM	orthogonal frequency-division multiplexing
OS	operating system
PCF	policy control function
PIN	personal identification number
PRACH	physical random access channel
PUCCH	physical uplink control channel
PUK	personal unblocking key
RAM	random access memory
RAN	radio access network
RF	radio frequency
SA	standalone
SAR	search and rescue
SAR	synthetic aperture radar
SD	secure digital
SDN	software-defined networking
SDR	software defined radio
SIGINT	signals intelligence
SIM	subscriber identification module
SISO	single input, single output
SMF	session management function
SNR	signal-to-noise ratio

SU-MIMO	single-user multiple input, multiple output
TAO	Tactical Action Officer
TCP	transmission control protocol
TDD	time division duplex
TRX SDR	transceiver software defined radio (SDR)
UAV	unmanned aerial vehicle
UDM	unified data management
UDP	user datagram protocol
UE	user equipment
UPF	user plane function
URLLC	ultra-reliable low-latency communications
USB	universal serial bus

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

Thanks to all the professors who worked with me during COVID-19 and my time here at NPS. To CDR Bollmann, thank you for taking on a thesis student you had never met and for your guidance throughout the thesis process. To Darren Rogers, thank you for somehow always having the exact equipment I need on hand and readily available, and for being a sounding board as I talked my way through my design and experiment.

I would also like to thank my family. To Evelyn, thank you for building circuits with me, and for knowing what a resistor was at two years old, so you could return the resistors you put in your Minnie Mouse train. To Ezra, thank you for always being happy and for being a subject of my video stream testing. To Cory, thank you for being my lackey while I conducted the experiments. Thank you for editing my thesis and not laughing too hard when I handed you pages with incomplete thoughts and sentences. Also, thank you for taking the lead on cooking meals so the smoke alarm wouldn't go off and scare Evelyn because mommy was making dinner. To my parents and aunts, thank you for listening to me ramble on about my thesis, school work and life in general when stuck in traffic.

Finally, thank you to coffee. We all know my life revolves around coffee.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1: Introduction

This thesis focuses on developing 4G long term evolution (LTE) and 5G new radio (NR) networks with the end goal of sending higher-quality data from an unmanned aerial vehicle (UAV) to ship and/or shore assets. This introduction covers the motivation for the thesis and research questions examined. It also includes background on 4G and 5G networks, scope and limitations, experimental design, methodology of analysis, results, conclusions and future work.

1.1 Motivation and Context

The motivation for this thesis came from the author's experience with UAVs during deployments. UAVs are used for overhead intelligence, surveillance, and reconnaissance (ISR) support while conducting strait transits. Fast inshore attack craft (FIAC) often approach U.S. Navy warships conducting strait transits. Tactical Action Officers (TAOs) watch live feed from the UAVs to determine how many personnel and weapons are on the FIACs, and if the weapons are covered or uncovered. However, this live feed is grainy and slightly time late, making it difficult to provide actionable intelligence to the Commanding Officer of the ship.

1.2 Research Questions

Based on this motivation, three research questions were developed:

1. Can a UAV be connected to a locally controlled 4G LTE and/or 5G network?
2. Are 5G communications with adequate throughput and signal power between UAV and ship/shore assets possible?
3. Can UAVs send data between each other to the ground station?

1.3 Background

5G is the fifth generation of wireless networks. 5G networks provide higher data rates, lower latency, and more reliability over 4G networks [1].

5G networks are comprised of three basic components: the 5G core, the radio access network (RAN), and user equipment (UE) [2]. Two frequency ranges are used in 5G: frequency range 1 (FR1) which operates between 600 MHz – 6 GHz and frequency range 2 (FR2) which operates between 24 – 100 GHz [2]. This thesis uses FR1.

Carrier aggregation (CA) concatenates multiple carriers resulting in an increased bandwidth and an increase in the data rate of the system [3]. This thesis uses CA of 1x1 single input, single output (SISO), 2x2 multiple input, multiple output (MIMO) and 4x4 MIMO. This thesis uses five test subscriber identification module (SIM) cards to provide network access to the UEs. The three main use cases for 5G are: enhanced Mobile Broadband (eMBB), massive machine-type communications (mMTC) and ultra-reliable low-latency communications (URLLC). This thesis focuses on the eMBB use case.

1.4 Scope and Limitation

Limitations of this thesis includes using commercial off-the-shelf (COTS) equipment to keep operating costs low. Our selected COTS provider was Amarisoft. Our Amarisoft license limits the CA to a 120 MHz bandwidth. An up-down converter would have been required to conduct testing in FR2; therefore, only FR1 is used during this thesis.

The UAV used has a maximum weight limit of 35 lbs [4]. The UAV could only be flown in line-of-sight due to flight restrictions at the Monterey Bay Academy.

1.5 Overview of Equipment and Network Setup

The 4G LTE and 5G standalone (SA) networks were configured using the Amarisoft Callbox Classic. Four COTS phones were used in conjunction with the 4G LTE network:

1. Pixel 4a
2. Pixel 3a
3. OnePlus A6003 (2 phones)

The payload consisted of a Raspberry Pi NoIR Camera V2, SIMCOM8200EA-M2 5G hardware attached on top, commonly referred to as a hat; and a Raspberry Pi 4 Model B. The 5G hat allowed the Raspberry Pi 4 to connect to the 5G SA network. Video was streamed from the camera through the 5G SA network to the receiving device on the ground, which was a personal laptop.

The FreeFly Alta X UAV was used to provide power to the payload and to fly the payload.

We first conducted 4G LTE testing to verify proper operation of the payload and to isolate faults to the payload for troubleshooting.

1.6 Overview of Methodology

This experiment was divided into three parts:

- 4G LTE network connection verification and video streaming from the payload
- 5G SA network uplink signal power measurement while video streaming from payload
- 5G SA network downlink throughput measurement

The phones were tested to determine if a connection could be achieved, if sending and receiving text messages was possible, if the internet could be searched for data, and finally if a video could be streamed.

The 5G SA tests were conducted using frequency band n7 and CA of 1x1 SISO, 2x2 MIMO, and 4x4 MIMO. The bandwidth varied between 5 – 20 MHz in 5 MHz increments. The payload was placed at a distance of 5 – 40 m from the Amarisoft Callbox Classic, in 5 m increments.

The first test conducted using 5G SA was the uplink signal power test. Video was streamed from the camera on the payload, through the network, to the receiving device. Received signal power was measured using the minicom serial communications program on the payload. The average received signal power was compared to the theoretical received signal power calculated.

Next, the 5G SA downlink throughput testing was conducted using the payload as a server and the Amarisoft Callbox as a client. The average throughput was calculated and compared

to the experimental values at the various configurations.

Due to the short ranges achieved during ground testing, we decided to cancel the flight tests using the FreeFly Alta X.

1.7 Overview of Results

The 4G LTE network experiment using band 3 resulted in all phones except one OnePlus phone being able to establish connection, send and receive text messages, search the internet for data, and stream video. There was no change in test results between band 3 and band 7 for the Pixel 3a and both OnePlus phones. However, the Pixel 4a was unable to connect in band 7. It is believed that band 7 was simply out of range for the Pixel 4a.

The 5G SA uplink signal power results followed the theoretical signal power calculations. Received signal power decreased as distance was increased between the payload and Amarisoft Callbox. Also, as the bandwidth increased by 5 MHz, the received signal power decreased. Received signal power increased as the CA increased. The signal quality was considered to be good during the majority of the tests.

The 5G SA downlink throughput tests showed a trend where throughput decreased as distance increased. However, no trend could be seen where the throughput increased or decreased as a result of CA. In some tests with sufficient signal-to-noise ratio (SNR), the experimental average throughput matched average throughput seen in the real-world.

1.8 Conclusion

This thesis verified that UAVs could be connected to ship/shore assets using 4G LTE and/or 5G SA networks, with 5G communications being possible between UAV and ship/shore assets. However, adequate throughput and signal power was not achieved at larger distances that would typically be required during ISR missions. More transmission power and higher-quality antennas are required to achieve required signal quality and data throughput at the required ranges.

Due to time constraints, we were unable to demonstrate that UAVs could send data between themselves and the ground station.

CHAPTER 2: Background and Literature Review

This chapter provides an overview of 5G networks, the components that comprise 5G networks, and the main principles that drive 5G technology as applicable to this research. The use cases of eMBB, mMTC, and URLLC are discussed to include the main users and the technical specifications. 5G testing and associated results are laid out as a comparison basis for this thesis. For practical application of 5G research, four military UAVs are described by their missions, technical specifications, and limitations.

2.1 Overview of 5G Networks

5G is the fifth generation of wireless networks. 5G follows fourth generation networks (4G) and provides higher data rates, lower latency, and more reliability [1]. The design of 5G networks aims to connect more individuals, machines and devices to create the wider internet of things (IoT) with its massive network capacity.

2.1.1 5G 3rd Generation Partnership Project (3GPP) Standards

The 3GPP unites several telecommunications development organizations to develop protocols and international standards for all mobile communications companies. If an entity is claiming to sell 5G equipment, the expectation is that various device protocols will conform to 3GPP standards. Since 5G is still in the development stages, 3GPP continues to release standards which companies developing 5G equipment must meet or exceed in order for those networks to be considered 5G. From the 5G 3GPP Release 15, the requirements for peak data rates are 20 Gbps for downlink and 10 Gbps for uplink [5]. User plane latency is the time required to transmit a packet until the receiver receives the packet at the application layer [6]. Per 3GPP, the requirement for user plane latency is 4 ms for eMBB, discussed later in this chapter. The user experienced data rate requirement is 100 Mbps for downlink and 50 Mbps for uplink. The bandwidth requirements are greater than 100 MHz for both FR1 and FR2 and up to 1 GHz for FR2.

2.1.2 5G Components

Three basic components are required for a 5G network: the 5G core, the RAN, and the UE [2].

Multiple networking components are required for the 5G core to operate. The 5G core includes elements such as the: user plane function (UPF), data network (DN), core access and mobility management function (AMF), authentication server function (AUSF), session management function (SMF), network slice selection function (NSSF), network exposure function (NEF), network function (NF) repository function (NRF), policy control function (PCF), unified data management (UDM), and application function (AF) [2]. These functions are out of the scope of the thesis and are not discussed further.

There are two different configurations of 5G networks. The first is a 5G non-standalone (NSA) architecture. The NSA architecture includes an LTE core called the evolved packet core (EPC) [2]. The NSA architecture also includes the LTE RAN, 5G core, and 5G RAN. When operating in NSA mode, the device first connects to the 4G network and, if available, uses 5G for additional bandwidth. This NSA mode is expected to become more common as the 5G physical architecture is put in place [2].

As sufficient 5G infrastructure is built, the network will evolve into 5G SA [2]. The 5G SA architecture is a pure 5G network with no 4G components. This network provides the same functionality as the NSA network. The 5G SA network includes the 5G core and 5G RAN. In this architecture, the UE connects over the RAN and to the core [2]. This thesis uses a 5G SA network.

2.1.3 Frequency Bands

5G frequency bands consist of two main ranges, FR1 and FR2 set by 3GPP. For this thesis, FR1 mid-band is used.

FR1 consists of low-band and mid-band [2]. The low-band frequency range is from 600 MHz – 2 GHz. Low-band has a maximum bandwidth of 50/100 MHz with a sub carrier spacing of 15 kHz [5]. The main usage for the low-band is wide area and in-depth indoor coverage. The mid-band is between 2 – 6 GHz [2]. Mid-band has a maximum bandwidth of 50/100/200 MHz with sub carrier spacing of 15/30/60 kHz [5]. Mid-band is best used in

urban and suburban areas and provides peak rates in the hundreds of Mbps [2].

FR2, also referred to as mmWave, consists of all frequencies above 6 GHz, specifically between 24 – 100 GHz [2]. FR2 has a maximum bandwidth of 200/400 MHz and subcarrier spacing of 60/120/240/480 kHz. FR2 is used in cases where high data rates are required [5]. FR2 is mostly used for short range and dense urban communications [2].

2.1.4 Internet protocol (IP) Multimedia Subsystem

The internet protocol multimedia subsystem (IMS) is an architecture that allows for the transport and delivery of IP multimedia services over IP networks [7]. IMS consists of three layers: application, control and transport. The application layer executes services provided to the users. The control layer directs traffic between the transport layer and the service or application layer. The transport layer acts as a gateway between the access layer and control layer. The control layer is often referred to as the IMS core. Users can connect to the IMS through the use of phones, computers and similar devices [7].

2.1.5 Multimedia Broadcast Multicast Service

Multimedia broadcast multicast service (MBMS) is comprised of the broadcast service and the multimedia service [8]. The broadcast service is where all users in the same geographic area can receive the same information. The multicast service is when only specific users who have subscribed to the service and are within the geographical area can receive the information [8]. Both the broadcast service and multimedia service are point-to-multipoint transmissions of multimedia data [9].

2.1.6 Orthogonal Frequency-Division Multiplexing

5G leverages orthogonal frequency-division multiplexing (OFDM). OFDM modulates a digital signal across multiple different channels to reduce interference [1]. OFDM uses subchannel frequencies that are orthogonal to each other, so that the channels overlap and use the same frequency, but the signal is modulated so that the interference between the subchannels is canceled out [10]. By using OFDM and higher frequencies, large throughput capacity can be reached with low latency.

2.1.7 Time Division Duplex and Frequency Division Duplex

5G uses both time division duplex (TDD) and frequency division duplex (FDD). TDD uses one frequency band for uplink and downlink, switching between the two from one time interval to the other. FDD uses one frequency band for downlink and one frequency band for uplink [11]. FDD is typically used to obtain better coverage while TDD is used to obtain better capacity [12].

2.1.8 Carrier Aggregation

CA concatenates multiple carriers resulting in an increased bandwidth and an increase in the data rate of the system [3]. 5G supports CA with 16 component carriers (CCs). When using CA, two or more CCs are aggregated. CA can be used in both TDD and FDD typologies and helps improve network efficiency [3]. This thesis compares three different types of carrier aggregation: 1x1 SISO, 2x2 MIMO, and 4x4 MIMO.

2.1.9 Single Input, Single Output

SISO transmissions use one antenna at the transmitter and one antenna at the receiver, per channel [13]. The downside to SISO is that the capacity is limited by the radio resources vice channel conditions in some cases [13]. SISO is typically used in satellites and Global System for Mobile Communications (GSM) [14].

2.1.10 Multiple Input, Multiple Output

Due to the SISO limitations, MIMO might be more suitable in some circumstances. MIMO is the transmission of the same content to the same user over multiple antennas [13]. MIMO can be used for single-user multiple input, multiple output (SU-MIMO) or multi-user multiple input, multiple output (MU-MIMO). SU-MIMO can increase the data rate that a user can achieve by transmitting multiple layers of data on the same resources. MU-MIMO allows for the transmission of different radio frequency (RF) streams from multiple antennas to multiple receiving antennas, using the same spectral resources. These signals can be separated by the receiving antennas and pass on to the different users [13].

2.1.11 Beamforming

Beamforming is the concept of shaping the signal radiating from the antenna to direct the energy in a specific direction to result in an improved signal quality to the UE [13]. Beamforming is accomplished by changing the phase and amplitude of the transmission for each element [13].

FR2 suffers from heavy path loss during transmission [15]. The use of beamforming is more common with FR2 because the directing of a transmission to a single UE improves the SNR, thereby increasing the signal range. In order for beamforming to be effective, the antenna arrays used must be highly capable [15].

2.1.12 Network Slicing

Network slicing allows the creation of multiple networks, both virtualized and independent, on top of the physical infrastructure [16]. Each “slice” can be allocated based on the specific needs of the customer or use case. Three main slice examples exist [2]:

1. The mobile broadband slice is for communication, entertainment, and the internet.
2. The massive IoT slice is for retail, shipping, and manufacturing.
3. The mission critical IoT slice is for automotive, medical, and infrastructure.

Other slices can be built as required for specific application requirements.

2.1.13 Software Defined Networking

Software-defined networking (SDN) brings 5G into the virtual realm. SDN uses software-based application programming interfaces (APIs) to coordinate with the hardware infrastructure to direct traffic on the network [17]. Rather than using hardware such as routers and switches to control network flow, SDN can control a virtual network using software and route data packets through a centralized server. The advantages of SDN include greater control of speed, increased flexibility, and an extremely customizable network infrastructure.

SDN requires three main components to operate: the applications, controller, and networking devices. The applications request resources and information, the controllers decide how to route the data packets, and the networking devices receive the information from the controller and route packet accordingly [17].

2.1.14 Edge Computing

Small data centers positioned close to the cell towers at the edge of the network enable edge computing [2]. By having the information stored closer to the end user, the requested information does not have to travel across a large network or into a data center for processing. Edge computing helps achieve low latency and high bandwidth by bringing network computation capabilities closer to the end user [2].

2.2 Subscriber Identification Module Cards

SIM cards store information such as the customer's identification (ID), phone number, address book, and settings, and help associate the customer with a physical UE [18]. SIM cards provide the stored information to the wireless network so that the UE is granted access to the network [19]. This network access provides the ability to make phone calls, send text messages, and use mobile internet services.

Physical SIM cards can be swapped between devices, making it easier for customers to change phones or devices [18]. Likewise, customers can purchase additional SIM cards for international travel and simply swap the SIM cards while using the same UE. This gives customers the ability to access the mobile network of an international country while traveling abroad, and then simply switch to their original SIM card upon returning home to access their normal mobile network [18].

While swapping SIM cards is convenient for travel, there is an inherent security risk [18]. If a customer loses the physical SIM card, that individual can contact their mobile network provider and request the SIM information be transferred to a new SIM card. Attackers take advantage of this by pretending to be the customer who lost the SIM card and orchestrating the SIM card data being put on a new card. Pretending to be the customer is easy in the social media age where basic security question answers can be found online, such as what street you lived on growing up and your mothers' maiden name. The attacker can install the SIM card into a new UE and gain access to the mobile network. At this point, the customer loses access to the mobile network on the legitimate UE while the attacker can use the text messaging feature to provide two-factor authentication to the customers' bank account and conduct other nefarious activities [18].

To protect against the SIM card swapping attack, most providers have implemented the use of personal identification numbers (PINs) to add a layer of security [18]. Should the customer lose the physical SIM card and request the mobile company swap the SIM card data to a new physical SIM, the customer must provide the correct PIN to the company in order to authenticate the swap [18].

If a customer enters their PIN incorrectly multiple times, the SIM card will be blocked [20]. For this reason, SIM cards have a personal unblocking key (PUK) that can be entered to unblock the SIM card. If the PUK is entered incorrectly multiple times, the SIM card is disabled. The number of times the PIN and PUK can be entered too many times varies for each network provider. Typically, the card will be blocked if the PIN is entered incorrectly three times, and the card is disabled if the PUK is entered incorrectly ten times [20].

Some SIM cards have two PINs, one to access all features on the SIM and one that only allows for access to a portion of the information on the SIM [21]. Accordingly, there would be two PUKs. Users must utilize PUK1 to unblock PIN1, and PUK2 to unblock PIN2 [21].

An embedded subscriber identification module (eSIM) is a digital SIM card that is directly soldered to the phone's board, cannot be easily moved from one UE to another, and can be reprogrammed through software [22]. The functionality and information stored is the same as on a traditional SIM card. The use of an eSIM allows the user flexibility when it comes to switching phone plans. Eliminating extra hardware in the form of a physical SIM card makes the eSIM very desirable from a future technology perspective [22].

Located on the SIM card is an international mobile subscriber identity (IMSI) which is a unique number that mobile network operators (MNOs) use to identify individual subscribers [23]. IMSI numbers are typically 15 digits long with three sets of numbers. The first set of numbers is typically two to three digits and corresponds to the mobile country code (MCC) which defines the country the customer operates within. The second set of numbers is typically one to three digits and corresponds to the mobile network code (MNC) the specific MNO the customer is associated with. The final set is typically nine or ten digits and is the mobile subscription identification number (MSIN) that is unique to the subscriber. The IMSI number can be found on the physical card that comes with the SIM card. It can also be found by following the phone manufacturer instructions with the SIM card installed on the device.

Each SIM card has an associated integrated circuit card identity (ICCID). An ICCID is an 18 to 22 digit code that is uniquely associated and serves as an identifier to the SIM card [24]. When the UE attempts to connect with a mobile network, the UE sends the ICCID to the network. The mobile network verifies the ICCID is unique and allows the SIM card to be used. The ICCID can be found on the physical card that came with the SIM card, or in the installed UE manufacturers' instructions [24].

The ICCID is comprised of four sets of numbers to represent the industry code, MCC, MNC, and unique SIM identifier [25]. The first two digits are typically '89' to represent the product is for the telecommunications networks. The MCC, established by the International Telecommunications Union (ITU), is one to six digits long. The MNC is one to four digits long and is associated with the MNO that issues the SIM card. The rest of the digits is unique to each SIM card. This allows networks to identify a unique subscriber to activate, cancel a service, or provide further customer service support [25].

2.3 International Mobile Equipment Identity

International mobile equipment identity (IMEI) is a 15 to 17 digit code that every mobile device has [26]. Mobile service providers use the IMEI to uniquely identify devices that are valid. The IMEI is printed on the device, whether inside the casing or on the back of the UE. It can also be found listed in the software of the device by following the phone manufacturers' instructions. If a UE is lost or stolen, the customer can provide the IMEI number to the network provider and have the device located or flagged should it be detected trying to access network resources. Some devices have two numbers, one for each SIM card, either physical or digital [26].

2.4 Comparison to 4G

4G is the fourth generation mobile networking technology and the predecessor to the 5G network discussed in this thesis. The four main differences between 4G and 5G networks are: latency, download speeds, OFDM, and cell density [27]. As shown in Table 2.1, 4G latency ranges between 60 – 98 ms, where the minimum 5G latency is only 5 ms. The download speed of 4G has the potential to be up to 1 Gbps, but 5G has the potential to be 20 Gbps [27]. Average data rates for 4G are around 30 Mbps, where 5G is 100+ Mbps [1].

The OFDM encoding for 4G is in 20 MHz channels, but is in 100 – 800 MHz channels for 5G [27]. The user capacity of user per cell tower is 200 – 400 in 4G and is 100 times greater for 5G.

Table 2.1. 4G vs 5G. Source: [27].

	4G	5G
Latency Range	60 – 98 ms	5 ms
Download Speed	1 Gbps	20 Gbps
Average Data Rates	30 Mbps	100+ Mbps
OFDM Encoding Channel Bandwidth	20 MHz	100 – 800 MHz
Users per Cell Tower	200 – 400	100x greater than 4G

2.5 Use Case Classifications

Different use cases have different requirements and obstacles. The three main use cases for 5G are: eMBB, mMTC, and URLLC [28].

2.5.1 Enhanced Mobile Broadband

The eMBB use case focuses on human-centric access to multimedia content, services and data such as video to include ultra-high definition video, and augmented reality [28]. In short, eMBB aims to provide high data rates, wide area coverage, improved user experience, and higher user mobility [5]. 5G will be expected to support 1080p, 2K, 4K, and 8K full high-definition video resolution. The 5G eMBB use case is expected to support peak data rates of 20 Gbps for downlink and 10 Gbps for uplink with area traffic capacity of 10 Mbps per square meter. The energy efficiency is expected to increase by 100 times as compared to 4G. Peak spectral efficiency should be 30 bps/Hz for downlink and 15 bps/Hz for uplink. The user experienced data rate is expected to be 100 Mbps for downlink and 50 Mbps for uplink. eMBB should support high mobility of a UE that travels at maximum speeds of 500 – 1000 km/h. Lastly, eMBB is expected to support less than 1 ms of mobile interruption time [5].

2.5.2 Massive Machine-Type Communications

The mMTC use case is for large numbers of devices transmitting a small volume of sensitive data that requires no delay, such as smart grids and smart cities [28]. The aim here is that up to 50 billion machines will be able to communicate between themselves without human intervention [5]. Examples of the mMTC use case are: automated driving cars, health monitoring, factory automation, smart metering, surveillance and security. The uplink flow of data will require much more data than the downlink. The main features for the mMTC use case are wider coverage, low-cost IoT, high connection density of one million devices per square kilometer, and high mobility of 10 km/h for indoor, 30 km/h for dense urban and 500 km/h for rural areas. These types of communications require more reliability and security than the previous human-to-human communications of the previous generation of networks. The use of FR2 and beamforming is more common in dense urban areas for the mMTC use case [5].

2.5.3 Ultra-Reliable Low-Latency Communications

The URLLC use case is for mission-critical applications or industry automation [28]. Due to the nature of the use case, the requirements for latency, availability, and throughput are stricter. Examples of URLLC uses include industrial automation to include drone delivery and remote driving, remote surgery, intelligent transportation, and smart-grid automation [5]. The end goal for URLLC systems is to ensure a low latency of 1 ms per packet with a high reliability of 99.999%. The requirements also include a control plane latency up to 10 – 20 ms and <1 ms of mobile interruption time [5].

2.6 Selected Prior 5G Throughput Testing

2.6.1 Huawei Testing

Huawei, a leading global provider of information and communications technology infrastructure and smart devices, conducted tests using the eMBB use case with a frequency of 2.3 GHz [29]. During this test, the system bandwidth was set to 100 MHz, using TDD and five CCs. The testing was conducted while stationary and with multiple users. The coverage reached 75 meters with a peak spectral efficiency of 49.9 bps/Hz [29]. Other testing has

been done in FR2 but is not relevant to this thesis because of the hardware limitations noted in Chapter 3.

2.6.2 5G-DRIVE Testing

5G-DRIVE the 5G Harmonised Research and Trials for Service Evolution between the European Union (EU) and China, conducted trials for the eMBB use case at 3.5 GHz at the EU trial sites [30]. The NSA trials were conducted outdoors at the Surrey, UK and Warsaw, Poland sites. The SA trials were only conducted indoors and are not mentioned in this thesis, since the trials for this thesis will be conducted outdoors only.

The first set of NSA trials were conducted at the 5GIC trial site in Surrey, UK. The evolved node B (eNodeB) operated at a frequency of 2.6 GHz, while the 5G new radio base station (gNodeB) operated at a frequency of 3.5 GHz. The nine gNodeB antennas were placed at a height of 5 or 10 meters. This trial used different types of 5G UEs. iPerf3, a tool to test network bandwidth and throughput, was used to generate the maximum network traffic.

These NSA outdoor tests were stationary, meaning the UEs were moved to a location and remained at that location for 2 minutes. Testing was conducted to determine the data rate at each location. The UEs were then moved to a different location, and the testing was repeated. Tests were conducted to determine the UE peak data rate for both uplink and downlink. The downlink single UE peak data rate was 824 Mbps while using user datagram protocol (UDP), and were 724 Mbps while using transmission control protocol (TCP).

Drive tests were also conducted to compare the results to the stationary measurements. The drive tests resulted in about 95% of the sample points providing more than 200 Mbps in downlink data rate, and 48.6% of the sample points providing more than 400 Mbps in downlink data rate.

Another set of NSA trials were conducted at the Orange trial site in Warsaw, Poland. The eNodeB operated in band 1 with a frequency of 2100 MHz using a 5 MHz bandwidth. The gNodeB operated in band 42 with a frequency of 3400 – 3840 MHz using an 80 MHz bandwidth. This test conducted measurements at four stationary points, at approximately 50, 100, 150 and 200 meters away from the test gNodeB. A Samsung Galaxy A42 5G phone

was used as the UE. At each stationary point, downlink and uplink tests were conducted by downloading or uploading 2 GB files for 60 seconds from or to a server. Table 2.2 shows the downlink and uplink average and maximum throughput at each of the stationary distances [30].

Table 2.2. 5G-DRIVE Warsaw, Poland NSA Test Results. Source: [30].

Distance (m)	DL Avg (Mbps)	DL Max (Mbps)	UL Avg (Mbps)	UL Max (Mbps)
50	382.47	671.94	63.61	65.37
100	231.14	431.71	63.58	64.71
150	328.39	518.41	63.47	67.30
200	211.50	386.26	63.57	66.46

These tests are illustrative of the impacts of using COTS vice high-end commercial equipment. In most cases, our results in Chapter 4 demonstrate lower throughput at range.

2.7 Overview of Unmanned Aerial Vehicles used in the U.S. Military

UAVs are heavily used by the military for ISR to keep personnel out of harm’s way. UAVs also provide an advantage since human factors such as fatigue, acceleration, and weight do not have to be considered for the design and usage [31]. This gives UAVs more maneuverability and longer endurance times. UAVs can also be smaller than manned airplanes, providing a much smaller target area for adversaries to find, fix, and target [31].

The UAVs listed below are UAVs the author has worked with.

2.7.1 RQ-4 Global Hawk

The RQ-4 Global Hawk, shown in Figure 2.1, is an unmanned aerial vehicle used by the Unites States Air Force to provide persistent ISR [32].



Figure 2.1. Global Hawk. Source: [32].

The Global Hawk can reach high altitudes and stay on station for more than 30 hours. The Global Hawk is also able to provide communications relay support [32]. The Global Hawk provides coverage using imagery intelligence (IMINT), signals intelligence (SIGINT), and moving target indicator (MTI) sensors [33].

The Global Hawk requires launch from an aircraft base with a launch and recovery element (LRE) and a mission control element (MCE) [33]. The LRE is manned by one pilot and is responsible for getting the aircraft off the deck, to and from the target area, and back on the ground. The MCE is manned by one pilot and one sensor operator and is responsible for the control over the target area. The MCE pilot coordinates with outside entities for the mission as required [33].

The Block 30 Global Hawk features a multi-intelligence platform that carries electro-optical (EO), infrared (IR), synthetic aperture radar (SAR), and high and low band SIGINT sensors [33].

The Hughes integrated surveillance & reconnaissance (HISAR) sensor system is based on the ASARS-2 package developed for the Lockheed Martin U-2. It is lower cost than the ASARS-2, and integrates a SAR-MTI system and an EO/IR imager. The sensor data is

transmitted using a speed up to 50 Mbps [34]. The sensor system operates in the X-band with frequencies between 8 – 12 GHz [34].

The Global Hawk has a 130.9 feet wing span, weighs 14 950 pounds and can carry up to 3000 pounds of payload [33]. The Global Hawk can reach a speed of 310 knots, a range of 12 300 nautical miles, and reach a ceiling of 60 000 feet. There are currently 33 Global Hawks in operation as of the date of this thesis [33].

2.7.2 MQ-4C Triton

The MQ-4C Triton, shown in Figure 2.2, also provides real-time ISR, concentrating on ocean and coastal regions [35].



Figure 2.2. Triton. Source: [36].

The Triton was based on the Northrop Grumman Global Hawk and focuses on providing the U.S. Navy with maritime domain awareness [35]. Physically, the Triton is equipped with gust load protection, de-icing, and lightning protection systems to allow the aircraft to operate in harsh maritime weather. As the Triton must descend and ascend rapidly to gain

in-close views of ships and other targets, it is specially equipped to navigate these rapidly changing environmental conditions [35].

The Triton main mission is ISR, but the Triton is also able to conduct SIGINT gathering, SAR, and communications relay [35]. The Triton is crewed by five ground station personnel to include an Air Vehicle Operator, Tactical Coordinator, two Mission Payload Operators, and a SIGINT coordinator [37].

The Triton surveillance sensor is the AN/ZPY-3 multi-function active sensor (MFAS), and operates in the X-band frequencies between 8 – 12 GHz [38]. The Triton EO/IR sensor is a Raytheon MTS-B which can live stream video to ground forces [38].

The Triton can fly for more than 24 hours at altitudes above 10 miles, and has an operational range of 8200 nautical miles [35]. The wingspan is 130.9 feet and has a maximum takeoff weight of 32 250 pounds [37].

2.7.3 Scan Eagle

Scan Eagle, shown in Figure 2.3, provides ISR primarily for U.S. Air Force security forces expeditionary teams [39].



Figure 2.3. Scan Eagle. Source: [40].

Scan Eagle does not require a runway for launch and recovery, making it the most portable

ISR asset available [39]. Scan Eagle is able to conduct missions over land and sea [40].

Scan Eagle launches by a catapult launcher and is retrieved by a SkyHook recovery system [40]. Scan Eagle has the ability to fly in a range of environments and has a suite of ISR tools that can be configured quickly to collect images in the field. ISR tools include an EO camera and an IR camera for night operations. Scan Eagle requires two Airmen to operate in addition to two maintenance personnel [39].

Scan Eagle payload includes EO and IR sensors, and has a 2.4 GHz S-band downlink for video transmission [41]. The DRS E6000 high resolution uncooled thermal imager module provides 640x480 pixels [41]. The E0950 multi-feed imager produces an output of 960x720 pixels [42].

Scan Eagle has a wingspan of 10.2 feet, weighs 37.9 lbs, and has a speed of 55-80 mph [39]. Scan Eagle can operate up to 19 500 feet and can loiter over a mission area for 24+ hours [40].

2.7.4 MQ-8B Fire Scout

The MQ-8B Fire Scout, shown in Figure 2.4, is an autonomous helicopter system that provides real-time ISR, target-acquisition, and battle space management to users without having to rely on manned assets [43].



Figure 2.4. Fire Scout. Source: [43].

The smaller Fire Scouts have been deployed on smaller vessels such as frigates and the littoral combat ship (LCS) [43].

The Fire Scout has the ability to autonomously take off and land from landing zones and aviation capable ships [43]. The Fire Scout has the ability to fly, navigate, and avoid collisions in the same air space with other manned aircraft [43].

The Fire Scout uses the forward looking infrared (FLIR) Systems Brite Star II EO/IR payload. The Brite Star II has a 640x480 pixel infrared thermal imager [44].

The Fire Scout has an overall length of 31.5 ft, a maximum speed of 85 knots and a service ceiling of 12 500 ft [45]. The standard endurance with a 300 lb payload is 5.5 hours and can provide coverage for 110 nautical miles [45].

2.8 Current Limitations of UAV to Ship/Shore Assets

While the use of UAVs has reduced the number of military personnel put at risk, there are still major disadvantages to consider. The primary disadvantages are the requirement for large bandwidths for communications and potential vulnerability to jamming [31]. UAVs such as the Global Hawk, Triton, and Scan Eagle require large amounts of bandwidth for command and control in addition to the payload feedback loop of near real-time information to the operators. The need for a larger bandwidth for data flow means the UAV is more vulnerable to adversary detection and jamming [31].

While the Fire Scout does not require a remote pilot to fly, it is still vulnerable to jamming attacks and is unable to tell the ground station if it comes under attack [31].

Time on station and payload size is a limitation for all UAVs. Larger payloads require a heavier frame to carry the payload and more fuel to remain on target.

Both the Scan Eagle and Fire Scout IR imagers have a resolution of 640x480 pixels [44]. Scan Eagle has a second imager with a 960x720 pixel imager [42]. High-definition TVs have a 1280x720 pixel resolution while standard 4K TVs today have a resolution of 3840x2160 pixels [46]. This means that the military UAVs are using image resolutions that are one third or less of standard TVs.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3: Experimental Design

This chapter discusses the equipment used in this thesis. We begin by describing the equipment used in this work. Next we discuss the network set up. Finally we describe the limitations and constraints applied to this thesis.

3.1 Equipment

3.1.1 Amarisoft Callbox Classic

The work described in this thesis was the first at the Naval Postgraduate School (NPS) to explore and use the Amarisoft 5G-capable products.

The Amarisoft Callbox Classic, shown in Figure 3.1, is a solution for a 4G or 5G network in a box. It operates and permits tests in 5G SA and 5G NSA, and 4G LTE modes. The internals include an EPC, 5G core (5GC), eNodeB, gNodeB, software defined radios (SDRs), IMS, and MBMS [47]. The callbox uses a Fedora Linux 34 operating system with technical specifications that state support of up to 1000 UEs [47].



Figure 3.1. Amarisoft Callbox Classic. Source: [47].

The callbox SDRs provide coverage from 500 MHz – 6 GHz (i.e. FR1), and support a bandwidth <200 kHz – 56 MHz [48]. The callbox SDRs also support both TDD and FDD operations [48].

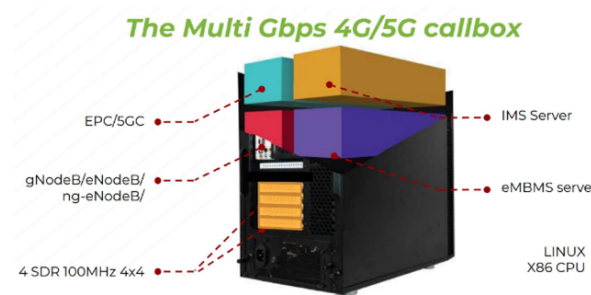


Figure 3.2. Amarisoft Callbox Classic Inner View. Source: [47].

The Amarisoft company releases quarterly updates to the software and configuration files. This thesis uses a standard Amarisoft license purchased by the NPS Center for Cyber Warfare (CCW). The standard license allows the use of the Amarisoft configuration files with one hardware device, in this case the callbox.

Five physical SIM cards were provided along with the callbox, as shown in Figure 3.3.



Figure 3.3. Amarisoft Sample SIM Cards

Each SIM had the same PIN, PIN2, PUK, PUK2, and IMSI. Each SIM card had a unique ICCID, with the first 16 numbers being the same. Table 3.1 shows the SIM Card Data and Table 3.2 shows the different last 3-digit ICCIDs for the test SIM Cards.

Table 3.1. Amarisoft Test SIM Card Data. The first 16 digits of the ICCIDs remains the same for all SIM cards. The last three digits are noted in Table 3.2.

PIN	1234
PIN2	1234
PUK	12345678
PUK2	12345678
IMSI	001010123456789
ICCID	8988211910000029XXX

Table 3.2. Last three digits of each SIM Card ICCID. The first 16 digits remain the same for all SIM cards and is noted in Table 3.1.

747
754
762
770
788

3.1.2 Raspberry Pi

The Raspberry Pi 4 Model B, shown in Figure 3.4, has a high-performance 64-bit quad-core processor with two micro-high-definition multimedia interface (HDMI) ports that support up to 4K resolution [49]. The Raspberry Pi has 4 GB of random access memory (RAM), supports both 2.4 GHz and 5.0 GHz wireless local area network (LAN) transmission, Bluetooth 5.0, and has four universal serial bus (USB) 3.0 ports [49]. The Raspberry Pi 4 is powered by a USB-C port with 5.0 volts [50].

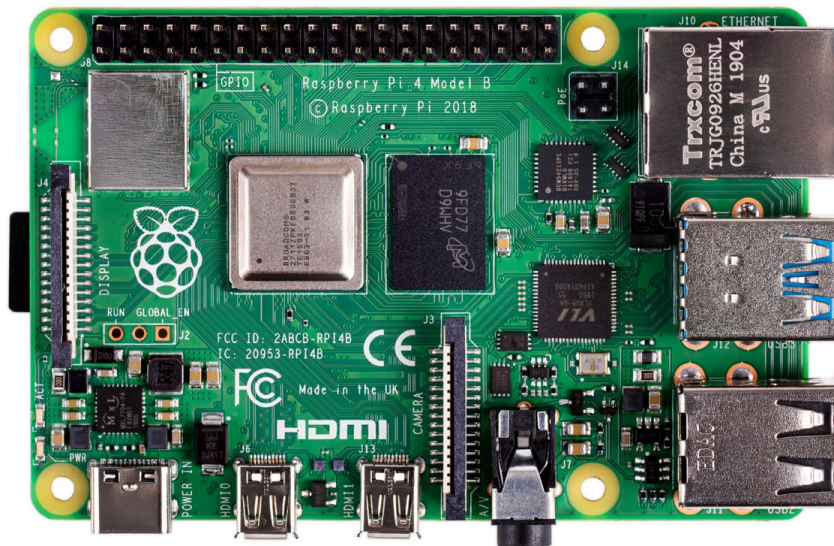


Figure 3.4. Raspberry Pi 4 Model B. Source: [49].

3.1.3 Raspberry Pi Camera Model 2 NoIR

The Raspberry Pi Camera Module 2 NoIR, shown in Figure 3.5, connects to all Raspberry Pi modules. The module 2 NoIR has a Sony IMX219 8-megapixel sensor but, unlike other Raspberry Pi cameras, does not have an infrared filter (hence no-IR) [51].

This camera is capable of taking 4K high-resolution photographs and high-definition (HD) 1080p video [52].



Figure 3.5. Raspberry Pi Camera Model 2 NoIR. Source: [52].

3.1.4 Waveshare SIM8200EA-M2 5G Hat

The SIM8200EA-M2 5G Hat for Raspberry Pi, shown in Figure 3.6, is used to connect the Raspberry Pi to the callbox network. The SIM8200EA-M2 5G Hat comes with a core module which supports multi-mode multi band and 3G/4G/5G connectivity [53]. The SIM8200EA-M2 module supports 5G SA and 5G NSA mode and is applicable for regions with 5G FR1 signal coverage. The SIM8200EA-M2 can provide data rates up to 2.4 Gbps for downlink and 500 Mbps for uplink. The SIM8200EA-M2 5G hat has a SIM card slot that supports a 1.8V and 3V SIM card [53].

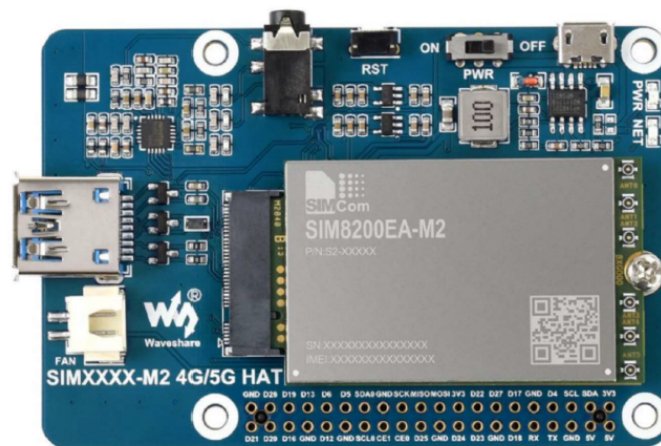


Figure 3.6. SIM8200EA-M2 5G Hat for Raspberry Pi. Source: [53].

3.1.5 Phones used in this Thesis

We used the phones to verify network operability and functionality of the payload, which consisted of the camera, 5G hat and the Raspberry Pi. Four phones were used in this thesis.

The Google Pixel 4a 5G phone was released in 2020 and is 4G and 5G capable [54]. The Pixel 4a has one physical SIM card slot and is eSIM capable [54]. The chipset is Qualcomm Snapdragon 730G with 800 Mbps peak download speeds and 150 Mbps peak upload speeds [55]. There are two IMEI numbers, meaning the Pixel 4a can support one physical SIM card and one eSIM card. Users can set which IMEI pairs with which SIM card [26].

Table 3.3. Google Pixel 4a. Source: [54].

Network Compatibility	4G and 5G
Chipset	Qualcomm Snapdragon 730G
IMEI 1	358116104953882
IMEI 2	358116104953890
eSIM Capable	Yes
Number of Physical SIM Card Slots	1

The Google Pixel 3a was released in 2019 and uses one physical SIM card and is eSIM capable [56]. The Pixel 3a is equipped with a Qualcomm Snapdragon 670 chipset, which provides 600 Mbps peak download speeds and 150 Mbps peak upload speeds [57]. It can support 2G, 3G, and 4G communications [56]. Similar to the Pixel 4a, the Pixel 3a has two IMEI numbers which users can pair with the physical or digital SIM card [26].

Table 3.4. Google Pixel 3a. Source: [56].

Network Compatibility	4G
Chipset	Qualcomm Snapdragon 670
IMEI 1	359643090946728
IMEI 2	359643090946736
eSIM Capable	Yes
Number of Physical SIM Card Slots	1

The OnePlus A6003 was released in 2018 [58]. The OnePlus A6003 has a dual-SIM card slot to hold two physical SIM cards [58]. The internal chipset is a Qualcomm Snapdragon 845 that supports 1.2 Gbps peak download speed and 150 Mbps peak upload speed [59]. Two OnePlus phones were used in this work.

Table 3.5. OnePlus A6003. Source: [58].

Network Compatibility	4G
Chipset	Qualcomm Snapdragon 845
(Phone 1) IMEI 1	869295032458974
(Phone 1) IMEI 2	869295032458966
(Phone 2) IMEI 1	869295032457711
(Phone 2) IMEI 2	869295032457703
eSIM Capable	No
Number of Physical SIM Card Slots	2

3.1.6 FreeFly AltaX

The FreeFly Alta X, shown in Figure 3.7, is a UAV with a 50-minute flight time [4]. The FreeFly Alta X is able to carry a payload up to 35lbs. The FreeFly Alta X is extremely portable with its ability to fold to half its normal size for storage and transportation, going from 89.4 in unfolded with propellers to 34.5 in folded. The Alta X has a gimbal to mount onto the bottom to carry payloads. The Alta X features three XT-90 battery voltage outputs which can power the payload [4].



Figure 3.7. FreeFly Alta X. Source: [4].

3.2 Experiment Connection Set Up

The four phones were used for network operability and functionality checks. Each phone had an Amarisoft SIM card installed.

The payload, which consists of the camera, Raspberry Pi 4 and 5G hat, was assembled and configured in accordance with Appendix A. The SIM card with ICCID ending in 9762 was installed in the 5G hat.

The callbox was updated with the latest software update, in accordance with Appendix B.1.

For the 4G LTE testing, the callbox network was configured to 4G in accordance with Appendix B.2 and B.3. For the 5G testing, the network was configured to 5G SA in accordance with Appendix B.4 and B.5. Appendix B.6 was used to switch between 4G and 5G network configurations, as required. The location of the configuration files used in this thesis is found in Appendix B.7.

The callbox is directly plugged into the AT&T hotspot to provide backhaul service to the internet.

Figure 3.8 shows the network configuration used during these tests.

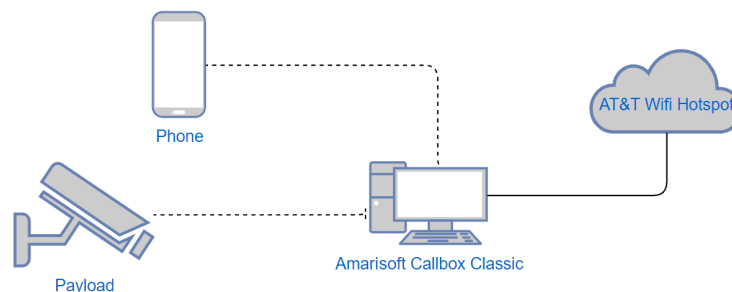


Figure 3.8. Network Diagram

3.3 Experimentation Constraints

The Amarisoft Callbox Classic license only allows a maximum of 120 MHz bandwidth carrier aggregation. The total aggregation is calculated by the sum of cells bandwidth

multiplied by the number of MIMO layers. The license constraints limited the testing of 2x2 MIMO to bandwidths of 60 MHz and below, and limited the testing of 4x4 MIMO to bandwidths of 30 MHz and below.

The SDR cards limited the RF bandwidth to 56 MHz and below, meaning all SISO and MIMO configurations could not have a bandwidth of more than 56 MHz [48].

Testing in FR2 was not conducted due to not having an up-down converter box required to configure the callbox to FR2.

The Raspberry Pi and 5G hat required a mobile power source light enough to fit within the FreeFly Alta X 35lb payload limit. The FreeFly Alta X has a limited flight time that decreases with the increase of the payload weight [4]. Due to flight restrictions at the Monterey Bay Academy in La Selva, the FreeFly Alta X can only be flown in line of sight, which is around one mile.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4: Results

This chapter describes the use case scenario for this thesis, outlines the methodology of experimentation, and analyzes the experimentation results.

4.1 Use Case Scenario

As discussed in Section 2.5.1, this thesis focuses on the eMBB use case scenario which provides the user with high data rates, wide area coverage, and higher user mobility. In this thesis, we use COTS equipment for the payload, network, and UAV. The payload streams video using high data rates, from a moving platform to the user on the ground.

4.2 Methodology of Experimentation

The data collection and evaluation portion of this thesis was divided into three experiments:

- 4G LTE network with phone connection and video streamed from the payload
- 5G SA network uplink signal power with video streamed from payload
- 5G SA network downlink throughput with payload

4.2.1 4G LTE Network Tests

The 4G LTE testing was conducted to verify proper operation of the payload. The Amarisoft Callbox Classic is configured for a 4G LTE network out of the box. This meant the payload could be tested with the 4G network and faults could be isolated to the payload for troubleshooting.

During this test, each of the four phones described in Chapter 2 had an Amarisoft SIM card installed. The final Amarisoft test SIM card was installed in the 5G hat in the payload.

The payload video stream was started in accordance with Appendix C.1.1.

All phones were connected to a Google Voice account with a virtual phone number. Each phone was tested to confirm it could send/receive text messages, search the internet for data,

and stream the payload video feed.

At first, the callbox was configured to the 4G network using band 3. Once the testing was completed with all phones on band 3, the 4G configuration was changed to use band 7 in accordance with Appendix B.3 and the same tests were run.

4.2.2 5G SA Uplink Signal Power Tests

We then configured the Amarisoft Callbox Classic to a 5G SA network in accordance with Appendix B.4. The configuration of the downlink and uplink antennas were varied between 1x1 SISO, 2x2 MIMO, and 4x4 MIMO.

While the Amarisoft Callbox Classic carrier aggregation was limited to no more than 120 MHz due to licensing limitations, the experiments should have been able to run between 5 – 50 MHz bandwidths at 5 MHz intervals for the 1x1 SISO and 2x2 MIMO configurations, and between 5 – 30 MHz bandwidths for the 4x4 MIMO configuration. However, for all SISO and MIMO configurations, the 25 – 50 MHz bandwidth tests had no connectivity between the payload and Amarisoft Callbox Classic.

Possible reasons for failed connectivity include interference from outside sources. This interference could be destructive interference caused by transmissions from campus buildings and surrounding areas. They could also be due to interference from physical objects or other sources near the testing site. In attempt to remove interference, the experiment set up was moved from outside the building to inside an office on the fourth floor to limit the outside interference. Connectivity was evaluated and tested at the zero-meter, one-meter and five-meter marks indoors. No connection was achieved. The network was then moved into the large conference desk area in the CCW with no change in results.

After change in location did not yield connection, the troubleshooting guidelines in the Amarisoft LTE eNodeB documentation were followed. Specifically, chapter 6 section 5 was followed since the initial physical random access channel (PRACH) signal was not received by the callbox. The absolute radio-frequency channel numbers (ARFCNs) were verified in the 5G SA configuration file for both bands used. The ARFCN in the configuration file for band n7 was 536 020 and within the required range of 524 000 – 538 000 for downlink [60]. The ARFCN in the configuration file for band n78 was 632 628 and within the required

range of 620 000 – 653 333 for downlink and uplink [60].

The UE configuration was verified to ensure the ability to support the frequency bands in the 5G SA configuration file. The UE supports bands n7 and n78 and was able to transmit on the same frequency band during previous testing using smaller bandwidths.

The distance between the UE and the callbox was increased and decreased in one-meter increments with no change in connection status. The 5G SA configuration was changed to use band n78, but no connection was achieved. The *cell_id* in the configuration file was changed, which forced the UE to search for another frequency. Connection was still not achieved.

Lastly, the ARFCN for band n7 was changed to 526 020 and the ARFCN for band n78 was changed to 622 628. Both ARFCNs were within the required range for the respective bands. Neither resulted in connection.

Based on troubleshooting steps and experimentation results, the lack of connectivity is determined to be due to payload antenna saturation when using more than 20 MHz bandwidth.

We were unable to isolate the high bandwidth connectivity problem to specifically the callbox or the UE. However, since both nodes were able to communicate in the 5 – 20 MHz bandwidths, we adapted our constraints for the remaining experiments. Therefore, for the 1x1 SISO, 2x2 MIMO and 4x4 MIMO configurations, the bandwidth was varied between 5 – 20 MHz in 5 MHz increments.

The distance between the payload and callbox was varied from 5 – 40 m, in 5 m increments. The received signal power was measured for each configuration setting at each 5 m increment. This was done by following the instructions in Appendix C.1.2. The payload was held at each increment for one minute and the time at the location was recorded manually to associate the data during result analysis.

The uplink testing was conducted while streaming a video from the payload to the YouTube video streaming platform, as described in Appendix C.1.1.

Once testing was completed, the average received signal power for all configurations at all meter intervals was calculated from the data collected and provided as parameters to the

MATLAB code. Both the MATLAB code and testing data can be found in Appendix C.3.

The received signal power data was collected using the minicom serial communication program. While the minicom serial communication program is not most accurate, minicom was used to keep the experiment design cost low by using COTS equipment and keep the experiment design similar to the field network design where the payload is attached to the UAV. The granularity of the minicom program signal power is 2 dBm, meaning signal power fluctuations are at a minimum of 2 dBm. These fluctuations provide minor inconsistencies when plotting the data points. As such, we focus our subsequent analysis on observed trends vice specific data points.

The collected data was compared to the theoretical values calculated. (4.1) shows the received signal power calculation in dBm [61].

$$P_{rx} = P_{tx} + G_{tx} + G_{rx} - L_{tx} - L_{rx} - L_m - L_{fs} \quad (4.1)$$

Received signal power is calculated from the transmitted power, plus the transmitter and receiver gains, minus the transmitter, receiver and miscellaneous losses, minus the free space path loss.

In this experiment, the receiver and transmitter gains are assumed to be zero since the antennas are simple omnidirectional antennas. The transmitter and receiver losses are also assumed to be zero, since there is an insignificant amount of cabling between the antenna and radio. Miscellaneous losses are also assumed to be zero. To calculate the received signal power, the only remaining terms were the transmit power and the free space path loss, as shown in (4.2).

$$P_{rx} = P_{tx} - L_{fs} \quad (4.2)$$

The transmit power was determined by the Amarisoft installed SDR cards. The maximum transmit power is -4 dBm for the frequency used in this experiment [48].

Free space path loss is calculated from the frequency in MHz and the distance in meters, as

shown in (4.3) [62].

$$L_{fs} = -27.55 + 20\log(\text{frequency}) + 20\log(\text{distance}) \quad (4.3)$$

The uplink frequency used in this experiment is 2560.1 MHz. From (4.2) and (4.3), the theoretical received signal power was calculated for each meter increment and is shown in Figure 4.1.

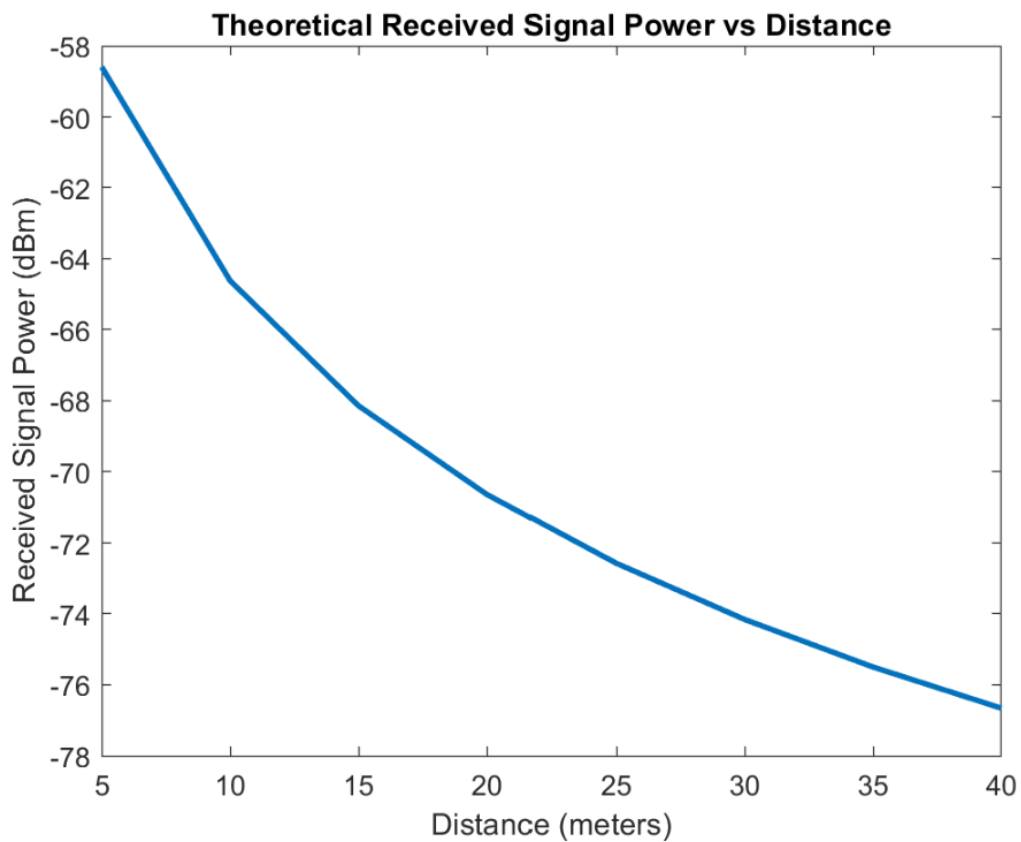


Figure 4.1. Theoretical Signal Power Received vs Distance

Using the minicom AT command quality signal report ranges shown in Table 4.1, any received signal power between -53 and -73 dBm is considered excellent connection quality. Any received signal power between -75 and -83 dBm is considered good quality, while any received signal power between -85 and -93 dBm is considered OK quality. Received signal powers between -95 and -109 dBm are considered to be marginal connection quality. Based on Figure 4.1, we expect to see excellent connection quality until 40 m where we will drop into the good connection quality category.

Table 4.1. Minicom Signal Power Ranges and Classifications. Source: [63].

Received Signal Power (dBm)	Connection Quality
-53 to -73	Excellent
-75 to -83	Good
-85 to -93	OK
-95 to -109	Marginal

4.2.3 5G SA Downlink Throughput Tests

Finally, the downlink throughput tests were conducted similarly to the uplink tests for configuration, distance and payload placement. The throughput was measured for each configuration setting at each meter interval by following the instructions in Appendix C.2.

The Amarisoft Callbox Classic did not record data if zero throughput was received. Therefore, this data point was not taken into consideration when calculating the average. However, the callbox would record minimal throughput in the kbps or bps range. These data points were used in calculating the average throughput.

Once all testing was completed, the data in the saved downlink testing files was formatted to remove extraneous labels that Amarisoft records. Since most of the bitrates were reported in Mbps, as denoted by the letter “M” in the bitrate column, all other bitrates were manually converted to be in Mbps. Figure 4.2 shows the raw data collected during the testing.

Figure 4.3 shows the file after being cleaned up. This was done for ease of importing the data into MATLAB. MATLAB calculations were conducted to obtain the average throughput for each configuration setting and each meter mark using the MATLAB code. The testing data and MATLAB code can be found in Appendix C.3.

```

testDL1-5M.txt - Notepad
File Edit View
[root@CBC-2021101900 enb]# cd /root/enb
[root@CBC-2021101900 enb]# /root/lteots-linux-2022-03-19/ltelaunch.sh ENB
Base Station version 2022-03-19, Copyright (C) 2012-2022 Amarisoft
This software is licensed to NAVAL POST GRADUATE SCHOOL.
Support and software update available until 2022-09-29.

RF0: sample_rate=5.760 MHz dl_freq=2680.100 MHz ul_freq=2560.100 MHz (band n7) dl_ant=1 ul_ant=1
(enb)
(enb) log file.rotate=250M,file.path=/var/log/lte/
(enb) [2022-06-22 10:43:37.971] TRX port #0 underflows=0% (206)
[2022-06-22 10:43:37.991] TRX port #0 overflows=0% (1)
cell phy
[gnb0012345] PLMN=00101 gNB_ID=0x12345
-----Global-----DL-----UL-----SSB-----
Cell RAT BAND BW P ARFCN ANT NL SCS QAM ARFCN ANT NL SCS QAM ARFCN SCS
0x001 NR n7 5 0 536020 1 1 15 256 512020 1 1 15 256 535930 15
(enb) t
Press [return] to stop the trace
PRACH: cell=01 seq=3 ta=5 snr=22.2 dB
-----DL-----UL-----
UE_ID CL RNTI C cqi ri mcs retx txok brate snr puc1 mcs rxko rxok brate #its phr pl ta
3 001 4603 1 15 1 20.9 95 1552 13.7M 19.3 - 18.3 15 50 53.6k 1/3.3/5 38 75 0.3
3 001 4603 1 13 1 20.9 19 1849 16.3M 15.7 - 13.7 10 52 35.3k 1/2.7/5 38 74 0.3
3 001 4603 1 14 1 21.3 25 1843 16.6M 1.2 - 6.7 19 57 34.8k 1/2.9/5 32 88 -0.5
3 001 4603 1 12 1 21.0 86 1783 15.8M 20.0 - 2.5 6 57 27.2k 1/2.2/5 36 77 -0.1
3 001 4603 1 13 1 20.6 27 1840 15.9M 16.8 - 7.6 2 52 34.1k 1/2.1/5 38 76 -0.4
3 001 4603 1 15 1 21.8 30 1842 16.9M 16.0 - 7.0 9 53 33.9k 1/2.5/5 38 77 -0.4
3 001 4603 1 14 1 21.1 20 1848 16.6M 12.1 - 2.8 6 57 29.2k 1/2.1/5 32 82 -0.4
3 001 4603 1 14 1 17.4 20 1852 13.7M 11.6 - 0.6 14 55 23.7k 1/2.7/5 32 79 -0.4
3 001 4603 1 13 1 22.2 38 1830 17.3M -1.7 - 3.0 2 54 30.5k 1/2.2/5 30 85 -0.4
3 001 4603 1 15 1 20.8 38 1829 16.1M 5.3 - 3.9 9 55 32.1k 1/2.3/5 32 81 -0.4
-----DL-----UL-----
UE_ID CL RNTI C cqi ri mcs retx txok brate snr puc1 mcs rxko rxok brate #its phr pl ta
3 001 4603 1 14 1 21.1 27 1839 16.4M 15.2 - 2.9 6 54 31.1k 1/2.2/5 36 78 -0.4
3 001 4603 1 14 1 21.3 23 1844 16.6M 18.7 - 2.4 0 56 30.0k 1/1.8/5 34 79 -0.4
3 001 4603 1 15 1 22.8 17 1849 18.1M 8.1 - 0.8 2 58 26.2k 1/1.5/5 32 85 -0.5
3 001 4603 1 14 1 21.7 55 1815 16.6M 9.4 - 0.7 7 62 26.2k 1/1.8/5 32 82 -0.4
3 001 4603 1 13 1 20.6 261 1590 13.9M 20.4 - 3.3 1 55 28.3k 1/1.3/5 34 76 -0.4
3 001 4603 1 13 1 16.9 26 1843 12.9M 14.7 - 6.6 0 53 34.1k 1/1.6/3 32 78 -0.4
3 001 4603 1 13 1 19.5 60 1808 14.8M 9.3 - 3.5 0 57 32.0k 1/1.8/3 32 78 -0.4
3 001 4603 1 14 1 20.0 26 1842 15.5M 18.7 - 3.9 0 53 32.5k 1/1.8/3 34 77 -0.4
3 001 4603 1 13 1 18.8 198 1652 13.1M 18.5 - 3.9 0 50 30.8k 1/1.9/3 32 77 -0.4
3 001 4603 1 12 1 17.5 58 1805 13.3M 18.5 - 3.6 0 54 31.7k 1/1.7/3 32 79 -0.4
-----DL-----UL-----
UE_ID CL RNTI C cqi ri mcs retx txok brate snr puc1 mcs rxko rxok brate #its phr pl ta
3 001 4603 1 12 1 17.9 166 1672 12.8M 9.7 - 5.1 0 51 32.0k 1/1.8/3 34 79 -0.4

```

Figure 4.2. Downlink Throughput Test Results - Raw Data

Table 4.2. 4G Phone Testing Data Using Band 3

Phone	IMEI	Connection Status	Text Message	Internet Data	Video Stream
Pixel 4a	3882	Connected	Yes	Yes	Yes
Pixel 3a	6728	Connected	Yes	Yes	Yes
OnePlus	7711	Connected	Yes	Yes	Yes
OnePlus	8974	Connected	No	No	No

Table 4.3 shows the results of the 4G LTE testing with the four phones using band 7. The Pixel 3a and both OnePlus phones had the same test results in band 7 as they did in band 3. The Pixel 4a failed to connect to band 7; therefore, the Pixel 4a was not be able to send or receive text messages, browse the internet, or stream videos.

The Pixel 4a is able to communicate using FDD center frequencies of 1800 MHz, 1900 MHz, and 2600 MHz, among more [54]. The frequency used in band 3 for this experiment was 1842.5 MHz, which is directly in the middle of 1800 MHz and 1900 MHz, both of which the Pixel 4a supports. However, the frequency used in band 7 was 2680 MHz, which is at the top end of the 2600 MHz frequency the Pixel 4a supports in FDD. We assess that band 7 is simply out of the Pixel 4As capable frequency range.

Table 4.3. 4G Phone Testing Data Using Band 7

Phone	IMEI	Connection Status	Text Message	Internet Data	Video Stream
Pixel 4a	3882	Not Connected	No	No	No
Pixel 3a	6728	Connected	Yes	Yes	Yes
OnePlus	7711	Connected	Yes	Yes	Yes
OnePlus	8974	Connected	No	No	No

4.4 Analysis of 5G Experiments

4.4.1 5G SA Uplink Signal Power with Payload

Tables 4.4, 4.5, and 4.6 show the zero-meter and one-meter measurements for received signal power in the 1x1 SISO, 2x2 MIMO, and 4x4 MIMO configurations, respectively. For readability, these measurements are not plotted in the subsequent graphs. These measurements were taken to provide a baseline received signal power for the different configurations. We should not expect to see better signal power than the zero-meter measurements, as this is the closest the payload can get to the transmitting antennas. The losses for free space is negligible when the payload is zero-meters from the transmitting antenna. The amount of interference from outside sources is also negligible. As the bandwidth increases, we consistently see the received signal power decrease for all configurations. All one-meter measurements are at or below the zero-meter measurements, consistent with expected signal power decrease as the distance between the payload and callbox increases. All zero- and one-meter measurements are considered to be excellent signal quality.

Table 4.4. 1x1 SISO 0 m and 1 m Signal Power Measurements

Bandwidth	0 m	1 m
5 MHz	-53 dBm	-57 dBm
10 MHz	-53 dBm	-61 dBm
15 MHz	-55 dBm	-63 dBm
20 MHz	-57 dBm	-65 dBm

Table 4.5. 2x2 MIMO 0 m and 1 m Signal Power Measurements

Bandwidth	0 m	1 m
5 MHz	-53 dBm	-55 dBm
10 MHz	-53 dBm	-57 dBm
15 MHz	-53 dBm	-59 dBm
20 MHz	-55 dBm	-61 dBm

Table 4.6. 4x4 MIMO 0 m and 1 m Signal Power Measurements

Bandwidth	0 m	1 m
5 MHz	-53 dBm	-53 dBm
10 MHz	-53 dBm	-53 dBm
15 MHz	-53 dBm	-55 dBm
20 MHz	-55 dBm	-55 dBm

Figure 4.4 and Figure 4.5 show signal power as a function of distance for the 1x1 SISO configuration, varying between 5 – 20 MHz bandwidth in 5 MHz intervals, with measurements taken every 5 m between 5 – 40 m. Figure 4.4 also shows the theoretical received signal power as a comparison. Further graphs will not display the theoretical calculations for readability purposes.

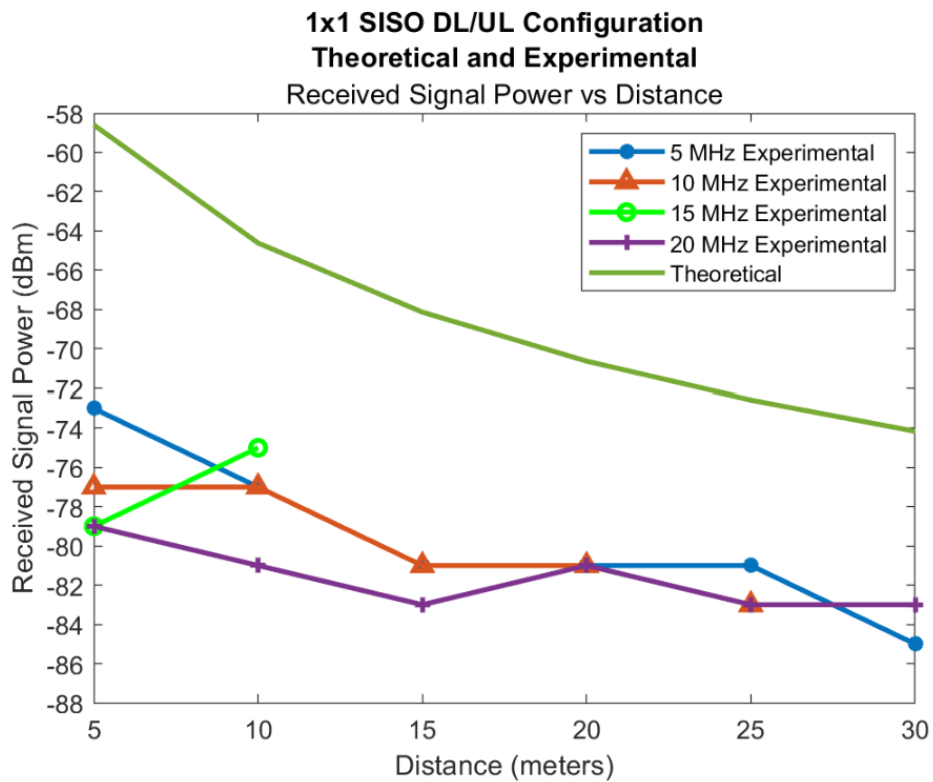


Figure 4.4. 1x1 SISO Configuration Signal Power vs Theoretical Signal Power

For the 1x1 SISO configuration shown in Figure 4.4 and Figure 4.5, the received signal power decreases as the bandwidth increases. This trend was also seen during the zero- and one-meter measurements, where the received signal power decreased by about 2 dBm as the bandwidth increased by 5 MHz. The experimental received signal power followed the same downward trend as the theoretical received signal power. The 15 MHz test is an outlier because as the distance increased, the signal power increased and then connection is lost. The rapid increase of signal power then connection loss is not seen during any other tests. The connection quality seen during the test is assessed as good, where we expected to see an excellent connection quality. The signal quality dips into the OK category at the 30 m mark for the 5 MHz configuration. At every bandwidth tested, the connection was lost at or before 30 m. Based on the theoretical signal power calculations, the payload should have remain connected to the network until approximately 40 m. The connection loss is likely due to inadequate transmit power from the SDR.

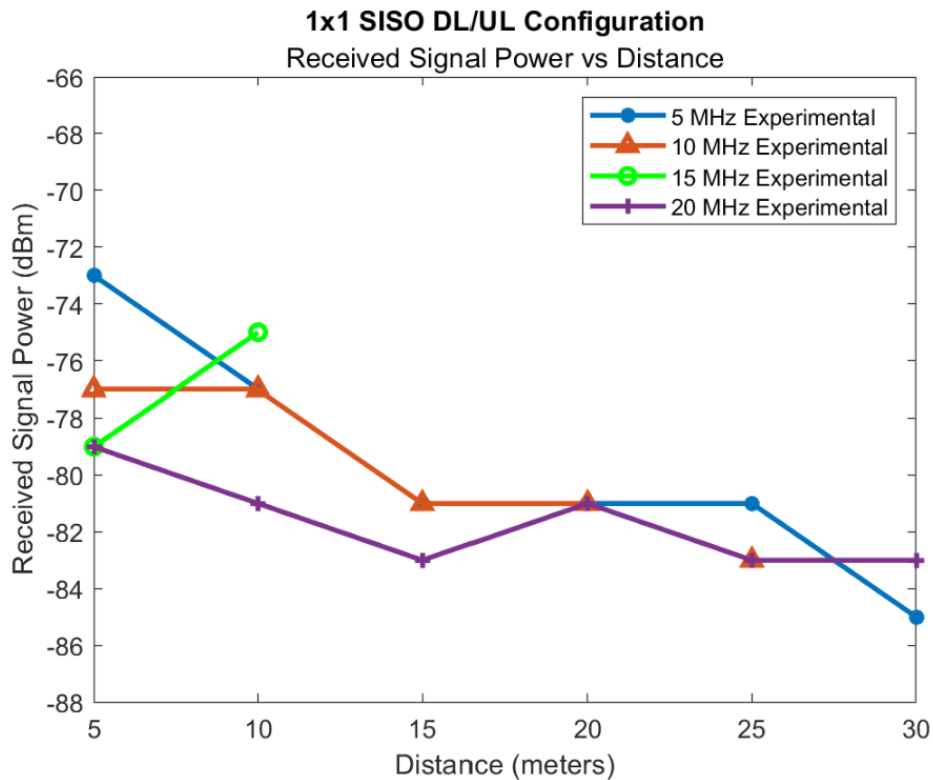


Figure 4.5. 1x1 SISO Configuration Signal Power

Figure 4.6 shows the 2x2 MIMO configuration with varying bandwidths between 5 – 20 MHz at 5 MHz intervals. The received signal power follows the theoretical trend of a decrease in signal power with an increase in distance. Similar to the 1x1 SISO configuration tests, there is a decrease in signal power of 2 dBm as the bandwidth increases in 5 MHz increments. The fluctuations seen in the 5 MHz and 20 MHz configuration are likely due to equipment sensitivity granularity of 2 dBm. The fluctuations could have been due to human interference such as people walking by the testing site. The connection quality is considered good, while we expected to see an excellent connection quality. Only in the 5 MHz bandwidth configuration did the connection remain until the 40 m mark, while the 10 MHz, 15 MHz, and 20 MHz bandwidths lost connection at 25 or 30 m.

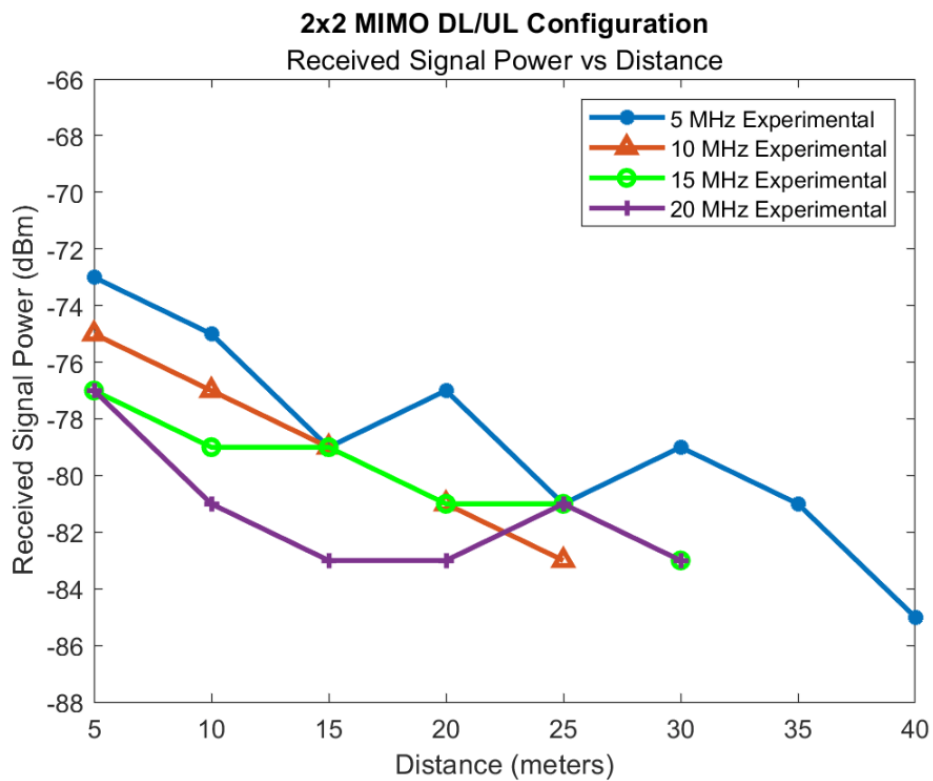


Figure 4.6. 2x2 MIMO Configuration Signal Power

Figure 4.7 shows the 4x4 MIMO configuration test results, while varying bandwidths between 5 – 20 MHz at 5 MHz intervals. This test follows the trend of received signal power decreasing as distance increases. This test also follows the trend of signal power decreasing by approximately 2 dBm as the bandwidth increases by 5 MHz. One exception is the 10 MHz test at the 5 m mark where we saw a lower received signal power than expected. This could have been due to interference unaccounted for by physical objects or other sources near the testing site between the payload and callbox. During this test, only the 5 MHz test lost connectivity before the 40 m mark. The loss of connectivity is likely an aberration since the transmitter power is the same as the other bandwidths, which all maintained connection until 40 m. The 4x4 MIMO test is the only test where we see an excellent connection quality at the 5 m mark with the 5 MHz, 15 MHz and 20 MHz bandwidths. The signal quality slowly moves into the good range that we see in the 1x1 SISO and 2x2 MIMO configurations.

When testing was first conducted, the 4x4 MIMO configuration using a 20 MHz bandwidth was unable to achieve connection and was not tested. After troubleshooting, the 20 MHz connection was achieved, and tests were conducted weeks after the rest of the tests in this thesis. As such, we provide the 20 MHz test points only as a reference as we cannot decisively compare the 20 MHz results with the rest due to the changes in experimental conditions and the large fluctuations observed in the data. This test will need to be repeated (as future work) to determine if the 20 MHz bandwidth follows the trend as the other bandwidths in the 4x4 MIMO configuration.

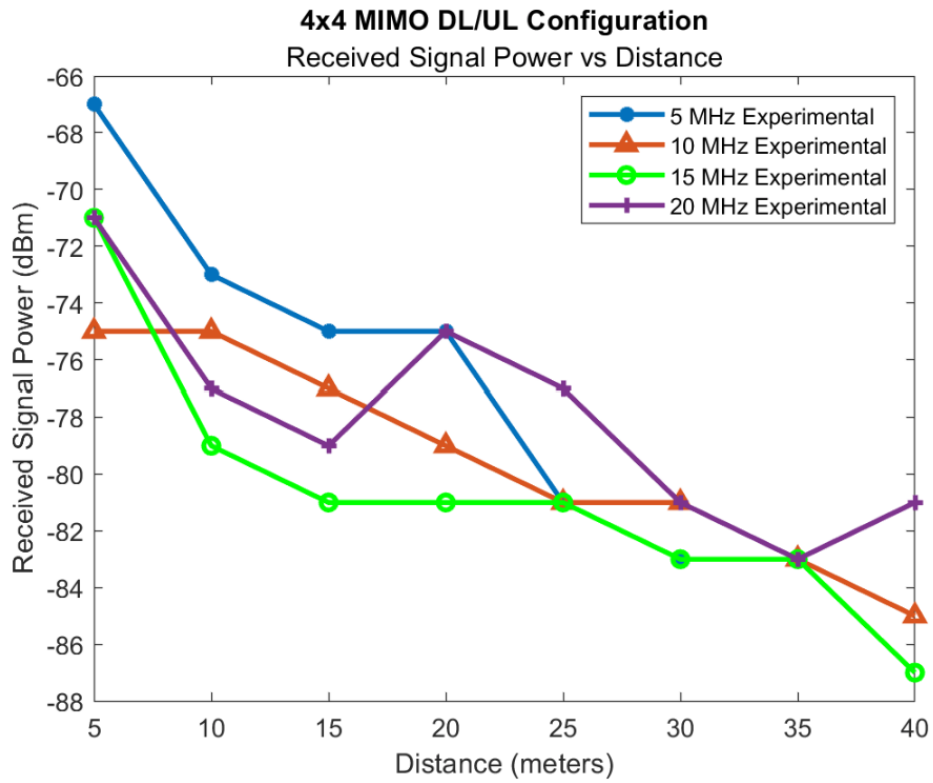


Figure 4.7. 4x4 MIMO Configuration Signal Power

Figure 4.8 is an alternative presentation of previous results showing received signal power as a function of distance and different SISO and MIMO configurations at a 5 MHz bandwidth. As seen before, these tests follow the trend of the received signal power decreasing as distance increases. This alternative presentation format makes it clear that as the carrier aggregation is increases, the received signal power increases. The higher carrier aggregations use more SDRs, providing more transmit signal power, which subsequently increases the received signal power. The 2x2 MIMO configuration signal power fluctuations are likely due to equipment sensitivity since the abnormal fluctuations appear to be within a range of about 2 dBm, which is the granularity limit for our equipment. As expected, the 4x4 MIMO received signal power remained higher than the 1x1 SISO and 2x2 MIMO between 5 m and 20 m. All three configurations have the same received signal power at 25 m, and have a good connection quality. Both the 1x1 SISO and 4x4 MIMO drop connection at 30 m and 35 m, respectively. The connection quality for 1x1 SISO and 2x2 MIMO configurations are in the OK category at 30 m and 40 m respectively. Only the 2x2 MIMO configuration continues to have connection at 40 m. This is likely due to low transmit power from the SDR being used.

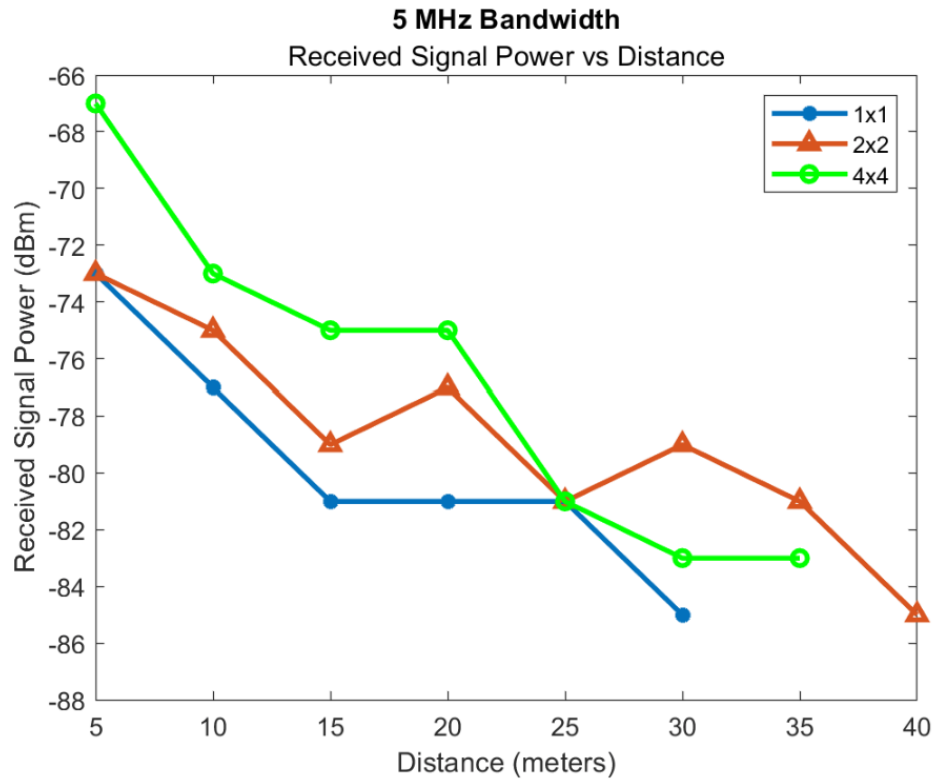


Figure 4.8. 5 MHz Bandwidth Received Signal Power

Figure 4.9 shows the results of the signal power received for different SISO and MIMO configurations at a 10 MHz bandwidth. We continue to see the trend of the received signal power decreasing as the distance increases. Similar to before, as carrier aggregation is increased, the signal power also increases. These tests remain close in received signal power throughout, providing the smoothest trend lines of all tests thus far. Channel diversity maintained connectivity by using more SDRs and subsequently increasing received signal power. The 2x2 MIMO configuration lost connection at 25 m, and the 1x1 SISO connection was lost at 20 m. Only the 4x4 MIMO configuration remains connected until 40 m, but the connection quality dips into the OK category. The 4x4 MIMO connection likely persists, even below the loss connection threshold for the other signals, due to the diversity gains from using extra channels.

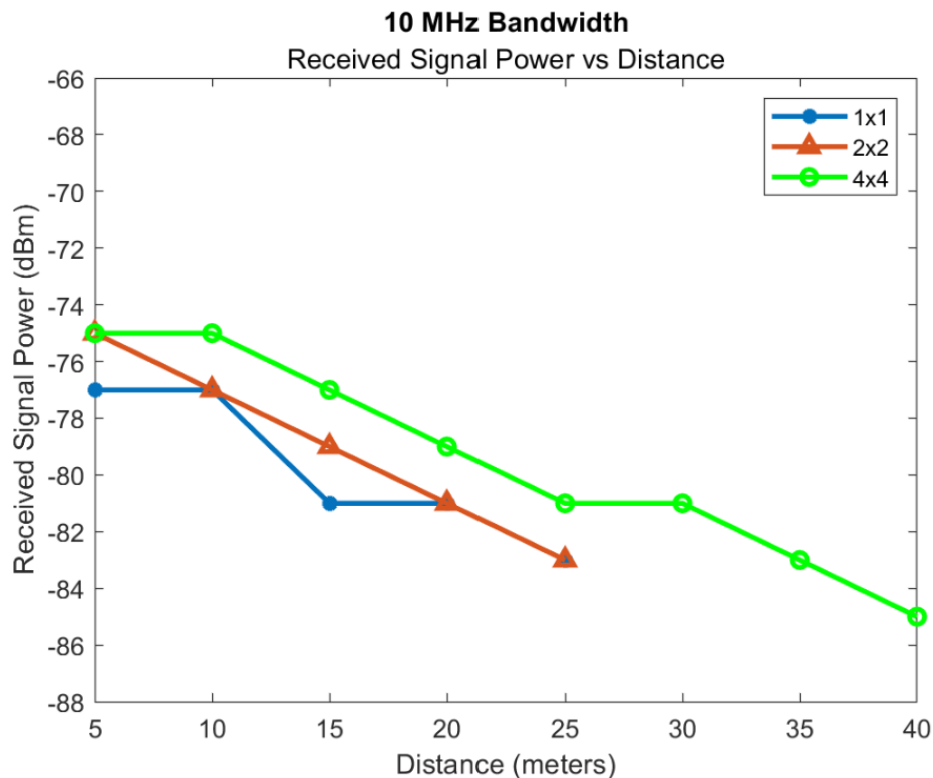


Figure 4.9. 10 MHz Bandwidth Received Signal Power

Figure 4.10 shows the results of the signal power received for different SISO and MIMO configurations at a 15 MHz bandwidth. The trend of the received signal power decreasing as the distance increases is followed in this figure. Similar to before, as carrier aggregation is increased, the signal power also increases. However, the 1x1 SISO configuration test should be repeated because it lost connectivity at 10 m, much earlier than any other test and the increase in received signal power does not conform to the downward theoretical trend nor the experimental trends we have seen with the rest of the experiments. Test was not repeated due to time constraints. The 2x2 MIMO configuration drops connection early at 20 m. Again, only the 4x4 MIMO configuration remains connected to 40 m.

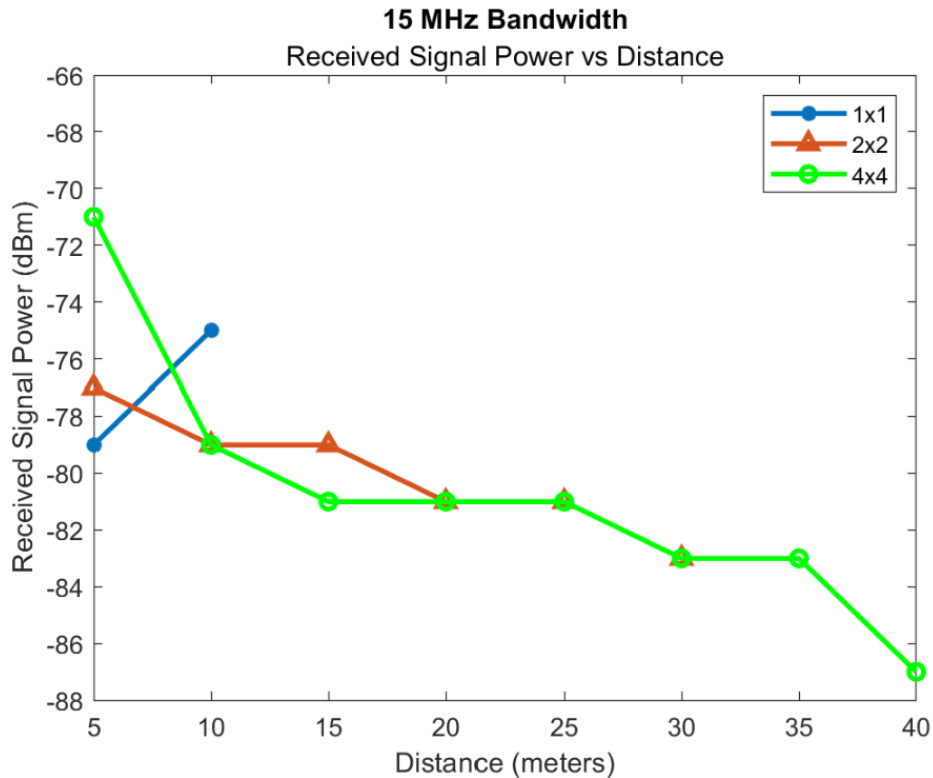


Figure 4.10. 15 MHz Bandwidth Received Signal Power

Figure 4.11 shows the results of the signal power received for the different SISO and MIMO configurations using a 20 MHz bandwidth throughout the meter intervals. We continue to see the trends of received signal power decreasing as distance increases, and signal power increasing as carrier aggregation increases. The 15 MHz and 20 MHz bandwidth tests have the same received signal power at 5 m, meaning antenna saturation likely occurs when using more than 15 MHz bandwidth. The connection quality for all configurations remains in the good category throughout this test, similar to what we have seen in previous tests. Both the 1x1 SISO and 2x2 MIMO configurations drop after 30 m but the 4x4 MIMO configuration remains connected out to 40 m.

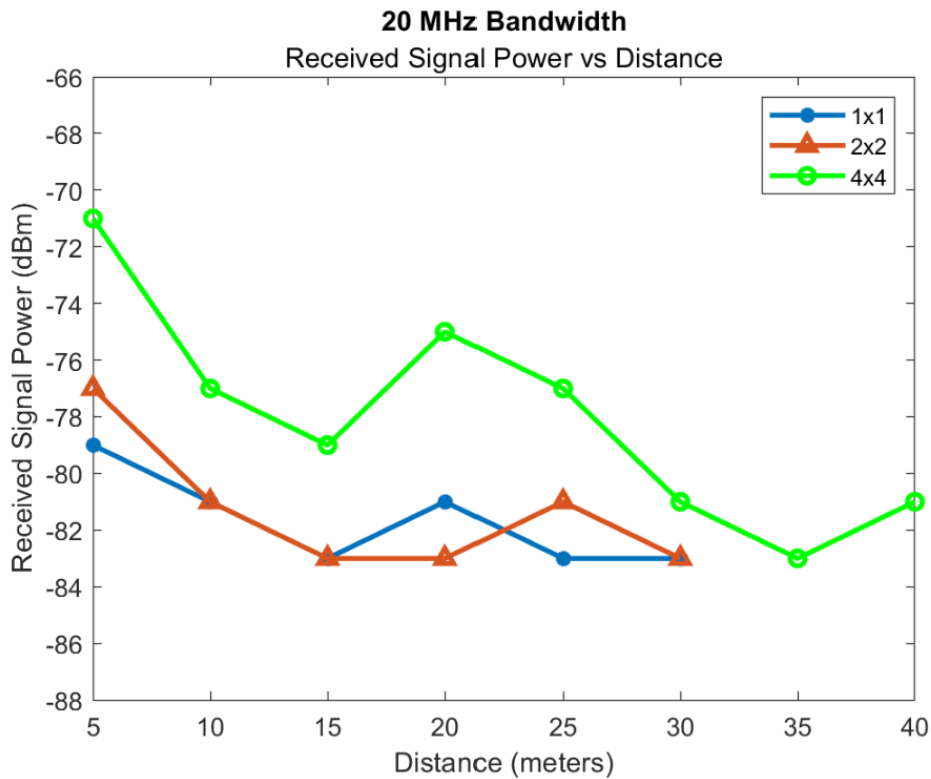


Figure 4.11. 20 MHz Bandwidth Received Signal Power

4.4.2 5G SA Downlink Throughput with payload

The throughput command in Appendix C.2 requests 150 Mbps from the server. Therefore, the expected throughput for all tests is 150 Mbps. This theoretical maximum is not graphed to make the graphs more readable.

5G theoretical throughput speeds are 1 – 10 Gbps while average real-world speeds are currently 50 Mbps [64]. Table 4.7 shows the average download speeds of various commercial 5G networks.

Table 4.7. Average Commercial Download Speeds. Source: [65]

Commercial Partner	Average 5G Download Speed
AT&T	75.6 Mbps
Sprint	70 Mbps
T-Mobile	71 Mbps
Verizon	67.1 Mbps

The SIMCOM8200EA-M2 5G Hat is capable of supporting speeds of 2.4 Gbps downlink and 500 Mbps uplink [53].

Figure 4.12 shows the throughput results for the 1x1 SISO configuration. A similar decreasing trend in throughput is seen as the distance increases. As expected, throughput increased as bandwidth increased for the majority of the tests. Throughout the test, the 20 MHz bandwidth throughput is approximately four times the throughput of the 5 MHz bandwidth tests and is approximately double the throughput of the 10 MHz bandwidth tests. The 15 MHz bandwidth throughput fluctuates oddly and does not follow expected trends. This is likely due to degraded signal quality, as shown in the Figure 4.5, where the 15 MHz test increased in received signal power and then lost connection. Given more time, the 15 MHz bandwidth tests should be conducted again to determine if this is an outlier or a trend for 15 MHz when using the 1x1 SISO configuration or possible equipment design issue. Connectivity stops for all bandwidths except 5 MHz before 35 m. As the bandwidth is increased, the same amount of power is spread through the larger frequency range, reducing the effectiveness of the radiated power. Therefore, a smaller bandwidth would produce a slower but steadier throughput.

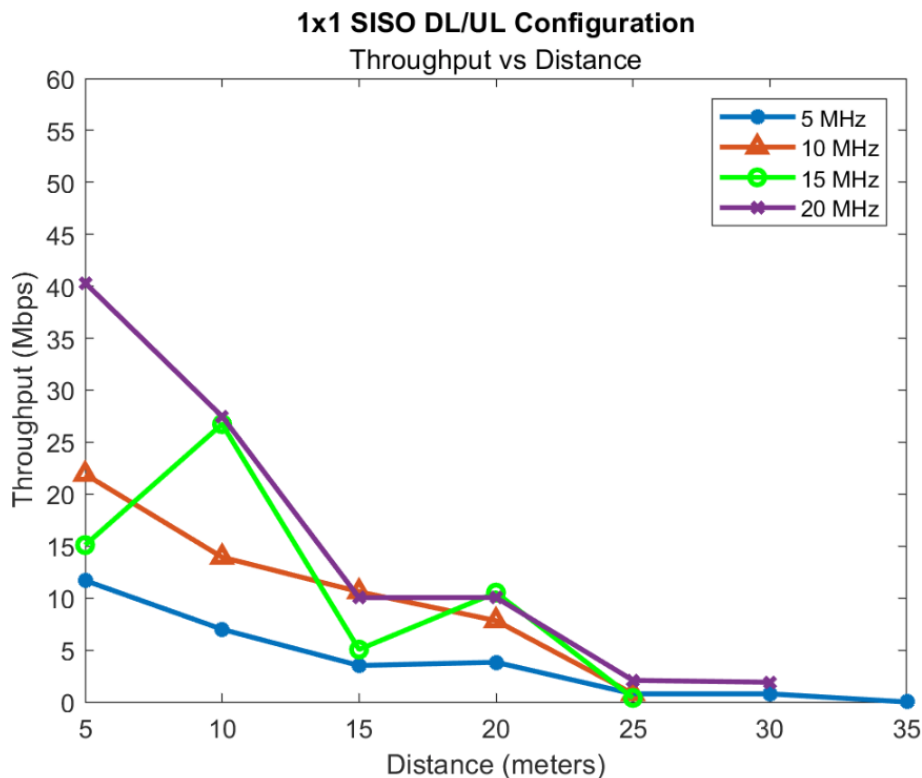


Figure 4.12. 1x1 SISO Configuration Throughput

Figure 4.13 shows the throughput results for the 2x2 MIMO configuration, using a 5 – 20 MHz bandwidth at intervals of 5 MHz. This configuration follows the same downward trend as the 1x1 SISO configuration in which the throughput decreases as the distance increases. We also observed the throughput increase as the bandwidth increased for the majority of the tests. In the same manner as the 1x1 SISO configuration, the 5 MHz bandwidth remains connected longer than the other, still having a connection at the 40 m mark. As seen in the signal power experiments, the drop in connection for the 15 MHz and 20 MHz tests could be due to antenna saturation. Interestingly, the 10 MHz bandwidth has a higher throughput at 5 m than the 15 MHz bandwidth. More tests and data points could provide more insight into causes, but time constraints and COVID limited experimentation.

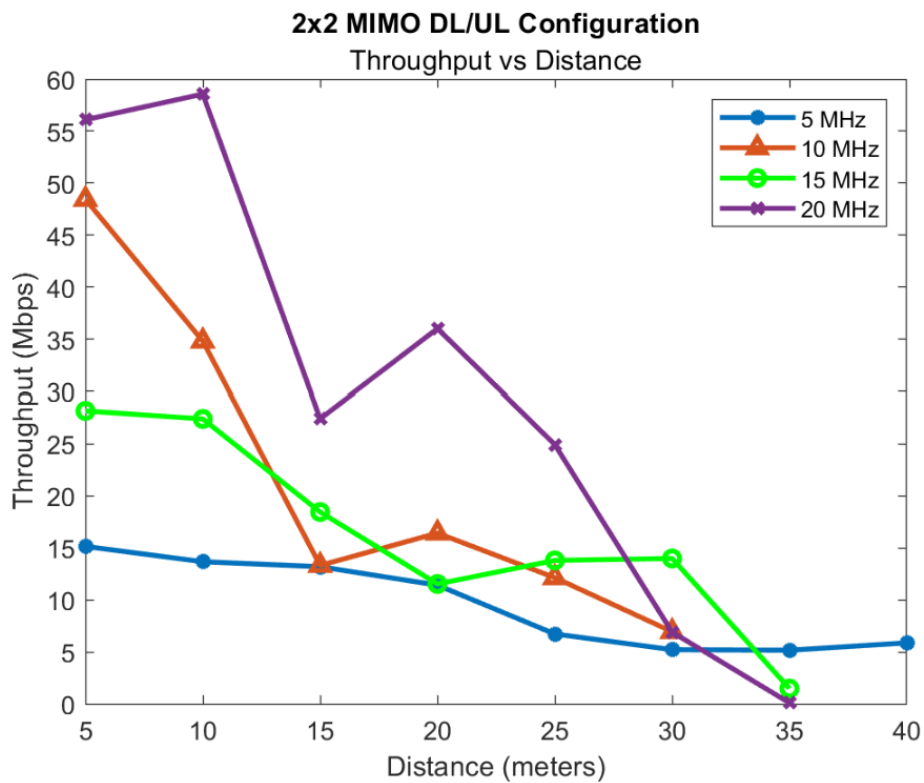


Figure 4.13. 2x2 MIMO Configuration Throughput

Figure 4.14 shows the throughput results for the 4x4 MIMO configuration, using a 5 – 20 MHz bandwidth at intervals of 5 MHz bandwidth; trends remain constant. Similar to the 1x1 SISO and 2x2 MIMO configurations, the 5 MHz bandwidth test stayed connected longer than the rest. The 20 MHz test throughput rapidly increases and decreases, likely due to human interference.

At 5 m, the 4x4 MIMO configuration has the highest throughput of all configurations. The 4x4 MIMO configuration uses more SDRs, allowing more data to be received by the callbox. The higher bandwidths of 15 MHz and 20 MHz allow more data to be sent through the network. As stated previously, the 4x4 MIMO configuration using a 20 MHz bandwidth test was conducted after the rest of the experiments. As such, we provide the 20 MHz test only as a reference.

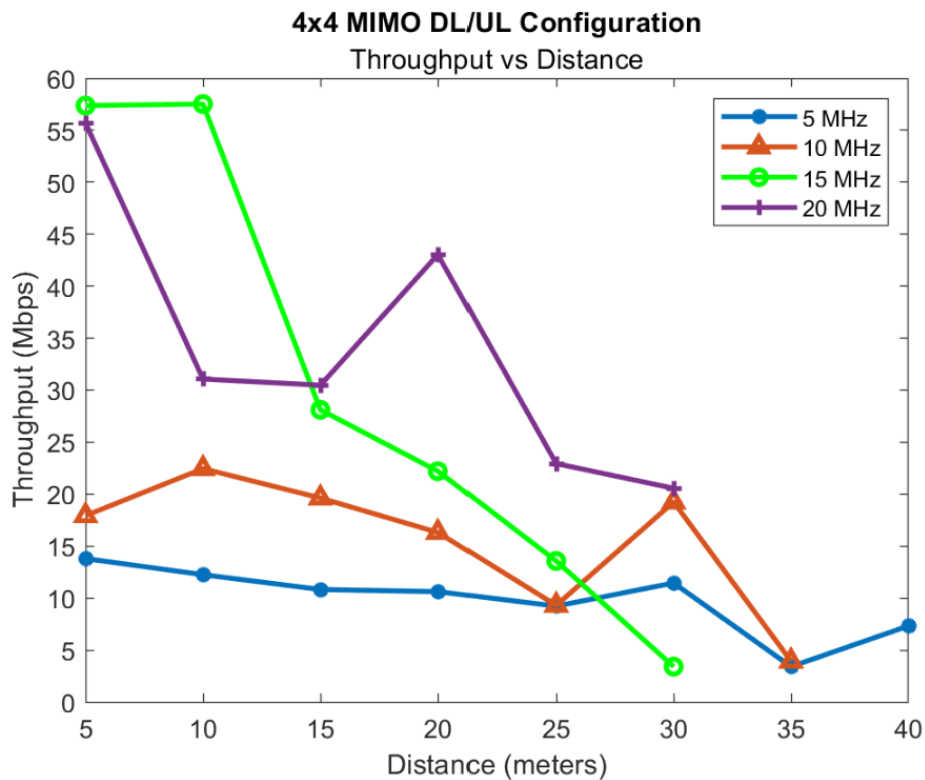


Figure 4.14. 4x4 MIMO Configuration Throughput

Again, we now present previous results in a different format. Figure 4.15 shows throughput as a function of distance and different SISO and MIMO configurations at a 5 MHz bandwidth. We continue to see the trend of throughput decreasing as distance increases.

Very little throughput is achieved when using 5 MHz bandwidth, but the 5 MHz bandwidth is the only bandwidth where connection continued until 40 m and there were no sharp increases or decreases in throughput. This is due to the power being spread over a small bandwidth, meaning the effective radiated power is higher than when using larger bandwidths. While using a 5 MHz bandwidth maintains connection at larger distances, it does not provide adequate data transfer because of the extremely low data rates.

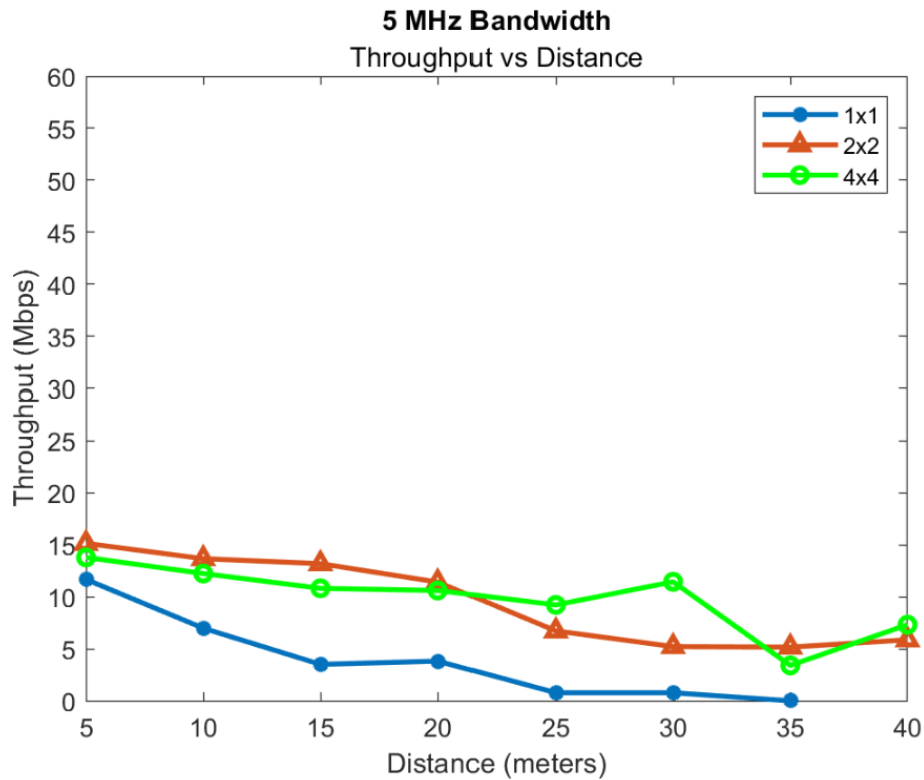


Figure 4.15. 5 MHz Bandwidth Throughput

Figure 4.16 shows the results of the throughput for different SISO and MIMO configurations at a 10 MHz bandwidth. Using a 10 MHz bandwidth increases the data received as compared to the 5 MHz bandwidth, which is to be expected because more data can be sent when using a larger bandwidth. We continue to see the trend of throughput decreasing as distance increases. While the throughput for the 2x2 and 4x4 MIMO configurations is higher than the throughput for the 1x1 SISO configuration, there is no distinct trend where the throughput increases as the carrier aggregation increases. Similar to the 5 MHz bandwidth, the 2x2 and 4x4 MIMO tests interchange as for which test has a higher throughput. Two outlying data points occur at 15 m for the 2x2 MIMO configuration and 30 m for the 4x4 MIMO configuration. These are likely due to interference unaccounted for by physical objects or other sources near the testing site between the payload the Amarisoft. All connections drop at or before 35 m. We also see this in Figure 4.9 where signal for the 1x1 SISO and 2x2 MIMO configurations is lost at or before 25 m.

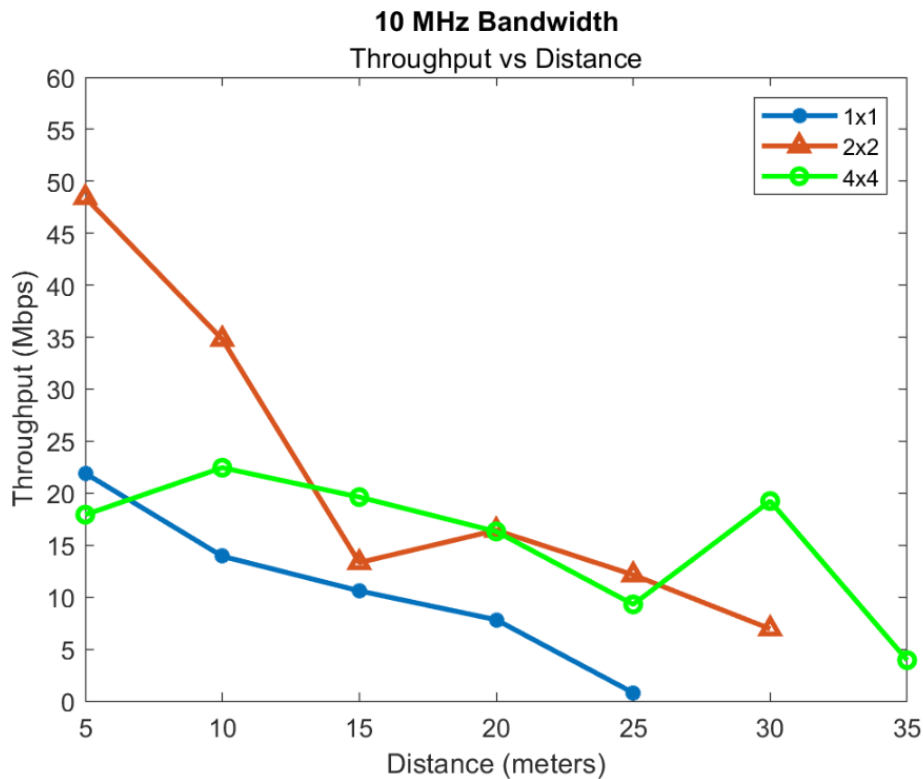


Figure 4.16. 10 MHz Bandwidth Throughput

Figure 4.17 shows the results of the throughput for different SISO and MIMO configurations at a 15 MHz bandwidth. As carrier aggregation increases, throughput mostly increases. All configurations using 15 MHz bandwidth lost connection after 35 m. This is likely due to the antenna saturation. This test shows the highest throughput achieved of 58 Mbps when configured using 4x4 MIMO. This maximum throughput is likely achieved due to using multiple SDRs and a larger bandwidth to send data. Using half of the SDRs used in the 4x4 MIMO configuration, the 2x2 MIMO configuration, the 2x2 MIMO configuration results in around 29 Mbps throughput, half of the throughput of the 4x4 MIMO configuration. Likewise, the 1x1 SISO configuration resulted in around 15 Mbps throughput, about half of the 2x2 MIMO configuration and a quarter of the 4x4 MIMO configuration. However, there is not enough evidence to suggest that using a 4x4 MIMO configuration would provide a larger throughput than using a 2x2 MIMO configuration at longer distances.

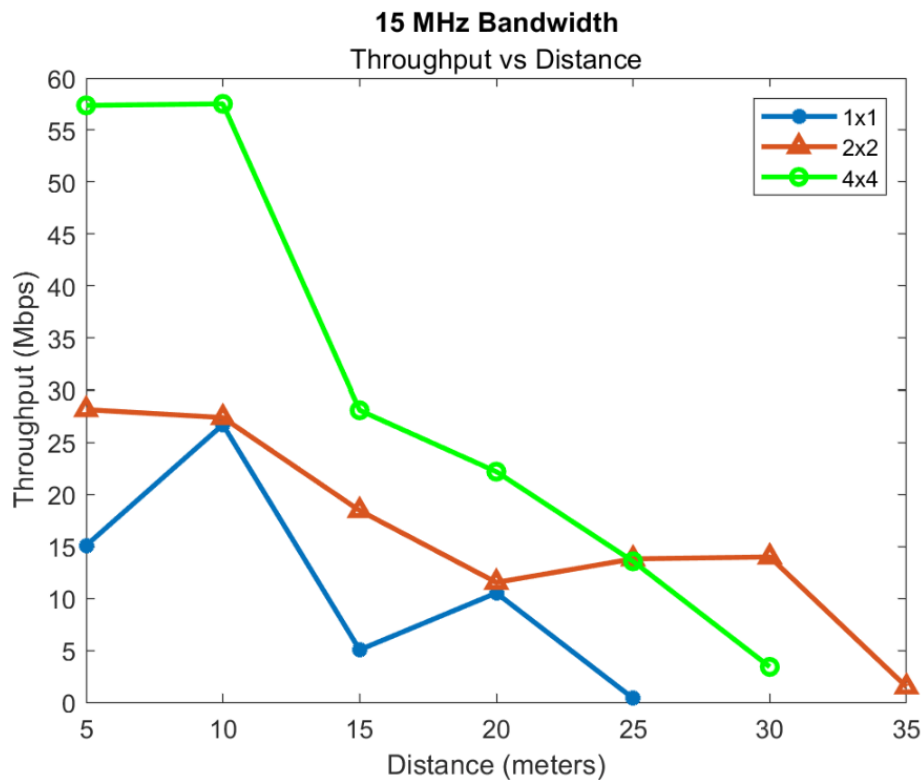


Figure 4.17. 15 MHz Bandwidth Throughput

Figure 4.18 shows the results of the throughput for the different SISO and MIMO configurations at a 20 MHz bandwidth. The throughput continued to decrease as the distance increased. As carrier aggregation increased, the throughput does not necessarily increase. This is also seen in the 5 MHz and 10 MHz bandwidths. All connections stopped at or before 35 m, in keeping with the trends we have seen in previous 15 MHz and 20 MHz tests where antenna saturation occurred. Due to the limited radiation power and antenna saturation, a throughput of higher than 57 Mbps was not achieved. An increase in power and better-quality antennas would likely see an increase in throughput.

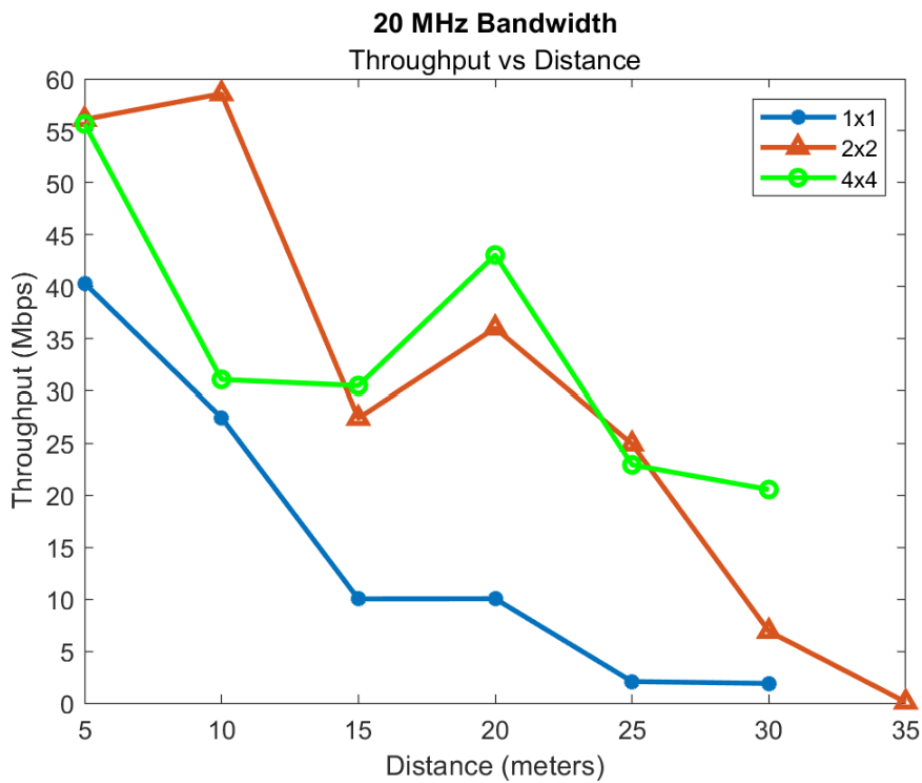


Figure 4.18. 20 MHz Bandwidth Throughput

At 25 m, the throughput for the 2x2 and 4x4 MIMO configurations is approximately 25 Mbps vice 15 Mbps when using 15 MHz bandwidth. This implies there is an issue with the 15 MHz configuration in either software or at the UE, and is worth investigating in future work. As stated previously, the 4x4 MIMO configuration using a 20 MHz bandwidth test was conducted after the rest of the experiments. As such, we provide the 20 MHz test only

as a reference as we cannot compare this test with the rest due to the large fluctuations.

4.4.3 Conclusion of 5G Experiments

During the signal power experiments, we saw the experimental received signal power follow the theoretical signal power trend. The signal power decreased as the distance increased. As the bandwidth increased by 5 MHz, we saw a decrease of received signal power by about 2 dBm. We also saw the trend of the signal power increasing as the carrier aggregation increased. A few configurations dropped connection before the 40 m mark when we expected the connection to remain, likely due to low SNR or low transmit power. Increasing the transmit power would increase the received signal power and could result in connectivity at further distances.

Most signal qualities remained in the good category, with two outliers falling into the OK category. We expected the signal quality to remain in the excellent category based on our theoretical received signal power calculations. However, this testing was not conducted in a shielded box so outside interference is expected and perfect signal quality cannot be achieved. We also observed antenna saturation when using 20 MHz bandwidth, meaning a 20 MHz bandwidth is likely the largest bandwidth this UE can support.

During the throughput experiments, we saw the trend where throughput decreased as distance increased. Generally, at greater distances, throughput was greater at higher carrier aggregations. All throughput tests were less than half of the expected 150 Mbps. Average 5G throughput speeds in previous real-world experiments are 50+ Mbps, which we achieved using larger bandwidths and shorter distances [64]. Table 4.7 shows the average download speeds of various commercial 5G networks.

Higher throughput can be achieved by obtaining perfect radio channels with more radiated power. Higher throughput could be experienced if the experiment was done in a shielded box, so as to cancel out any interference. However, that is not practical for this thesis and the distances being tested.

4.5 Improvements for Future Tests

Future tests with the 4G LTE network and phones should include a 4G network configuration of TDD. The TDD configuration might be able to support the band 7 connection since the Pixel 4a can support a 2600 MHz and 3600 MHz center frequencies in TDD, where at the tested FDD can only support 2600 MHz center frequency [54].

Future 5G SA tests should include running these same tests at a higher frequency and using TDD, such as band n78 which has a transmit frequency of around 3500 MHz. This higher frequency should allow for more data throughput and for better signal quality further away from the transmit source.

A spectrum analyzer can be used in future tests to achieve more granular signal power results.

Further research needs to be conducted to determine why the throughput did not increase steadily as the carrier aggregation increased.

Future tests should be conducted at different locations to eliminate any physical and electromagnetic interference that occur around the testing area. Conducting more tests would create more data points and smoother trends for analysis.

If connection and high throughput at further distances are achieved during stationary ground testing, further testing should be conducted with the FreeFly Alta X for mobility testing.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5: Conclusion and Future Work

This chapter summarizes the experiments conducted, results, application, benefit of use, and the future work required to further this research.

5.1 Summary

During this thesis both 4G LTE and 5G SA networks were tested.

The 4G LTE tests were conducted to ensure proper operation of the network and payload prior to conducting the 5G SA tests. The 4G LTE network was configured to use band 3, then reconfigured to use band 7. Four phones were tested to determine if connectivity could be achieved, text messages could be sent, data could be searched on the internet, and video data could be streamed.

The Pixel 3a and OnePlus with IMEI 7711 were able to successfully complete all tests in both band 3 and band 7. The Pixel 4a was able to complete all tests in band 3, but failed to connect in band 7 and was therefore unable to complete any tests in band 7. We assess that band 7 is out of range for the Pixel 4a. The OnePlus with IMEI 8974 was unable to complete any tests in band 3 or 7, but was able to connect to both networks.

In the 5G SA tests, the Amarisoft Callbox Classic was configured to use 1x1 SISO, 2x2 MIMO, and 4x4 MIMO carrier aggregation, with a varied bandwidth of 5 – 20 MHz in 5 MHz increments, at a distance of 5 – 40 m in 5 m increments.

The 5G SA tests were conducted in two parts. First, uplink testing was conducted to collect received signal power by streaming video from the payload through the 5G SA network to a laptop on the ground. In general, the experimental received signal power followed the theoretical signal power trend where the signal power decreased as the distance increased. As the bandwidth increased by 5 MHz, the received signal power decreased by approximately 2 dBm. The trend of the received signal power increasing as the carrier aggregation increased was also observed. Several configurations dropped connection before the 40 m mark when the connection was expected to remain, likely due to low SNR or low transmit power.

Increasing the transmit power would increase the received signal power and could result in connections at further distances. Most signal qualities remained in the “good” category, with two outliers falling into the “OK” category. The signal quality was expected to remain in the “excellent” category based on our theoretical received signal power calculations. However, this testing was not conducted in a shielded box; outside interference was expected and perfect signal quality could not be achieved. Antenna saturation was also observed when using a 20 MHz bandwidth, meaning a 20 MHz bandwidth is likely the largest bandwidth this SIMCOM8200EA-M2 5G hat can support.

The next 5G SA test used iPerf3 to determine the throughput for the varying configurations. In general, the trend where throughput decreased as distance increased was observed. However, there was no trend where throughput increased as carrier aggregation increased. All throughput tests achieved less than half of the expected 150 Mbps. Average 5G throughput speeds in previous real-world experiments is approximately 50 Mbps, which we achieved using larger bandwidths and smaller distances [64]. Higher throughput should be achievable in future work by using more perfect radio channels with less interference and more radiated power. Higher throughput could be experienced if the experiment was done in a shielded box as to cancel out any interference. However, that is not practical for our use case and the distances being tested.

5.2 Application and Benefit of Use/Conclusion

The motivation behind this research was the author’s experiences using ISR UAVs during deployments. The UAVs video feeds streamed to the U.S. warships were near real-time with low video quality, making it difficult to provide actionable intelligence to Commanding Officers to increase battle space awareness. The goal of this thesis was to use emerging technology to support sending better quality video at a faster rate to U.S. warships.

Three research questions were derived from the motivation:

1. Can a UAV be connected to a locally-controlled 4G LTE and/or 5G network?
2. Are 5G communications with adequate throughput and signal power between UAV and ship/shore assets possible?
3. Can UAVs send data between each other to the ground station?

This thesis proved that UAVs could be connected to a 4G LTE and/or 5G SA network. In this thesis, a payload was constructed using a Raspberry Pi NoIR Camera, SIMCOM8200EA-M2 5G hat, and Raspberry Pi Model 4. This payload is able to be powered and carried by the FreeFly Alta X UAV. An Amarisoft Callbox Classic was configured for a 4G LTE and separate 5G SA network. The payload was connected to the 4G and 5G networks using Amarisoft test SIM cards. All equipment was COTS in order to keep experimentation costs low.

Next, tests were conducted in order to determine if communications are possible between a UAV and ship/shore assets. Signal power was tested by streaming video from the payload through the network to a laptop on the ground. Throughput was tested by conducting downlink tests. These tests proved that while communications are possible between UAVs and ship/shore assets, modifications to the equipment must be made. Increased transmitting power is required to achieve longer distances since increasing transmitted power would increase SNR for several configurations. Higher quality antennas are required for the both the payload and callbox in order to reduce antenna saturation. Reducing antenna saturation would enable a connection using more than 20 MHz bandwidth. At shorter distances, received signal power achieved was considered excellent and throughput was comparable to current real world averages. However, as distances increased the signal power and throughput decreased to a level that is inadequate for ISR in current military operations.

Due to time constraints, the final research question was not attempted.

5.3 Future Work

Further research needs to be conducted to provide connectivity between the payload and the callbox at higher bandwidths, such as the 25 – 50 MHz bandwidth range where connection should have occurred but was not successful during these trials. It is believed that antenna saturation occurred after 20 MHz and that higher quality antennas are required to use higher bandwidths. Once the system is able to achieve connection at the higher bandwidths, licensing could be acquired to use more than 120 MHz of carrier aggregation. All of these changes should provide greater throughput approaching commercial 5G limits. These tests should be analyzed with tests previously conducted to confirm or deny trends already seen.

5G SA testing in band n78 should be conducted. Band n78 uses TDD and a center frequency of 3500 MHz. Band n78 is supported on both the SIMCOM8200EA-M2 5G Hat and the Pixel 4a phone. The higher frequency would allow more data to be transmitted through the network.

FR2 testing can be conducted by acquiring an up-down converter for the Amarisoft Callbox Classic. A different payload will be needed as the SIMCOM8200EA-M2 5G hat does not support FR2.

Future work may be conducted to determine if the payloads can send data between each other and to different base stations on the ground. Another Amarisoft Callbox Classic or an Amarisoft Callbox Mini could be used. These Amarisoft networks can be connected to each other to facilitate handovers of the payload.

Finally, multiple devices should be connected with the Amarisoft Callbox Classic, which has technical specifications stating it can support up to 1000 active UEs. The same throughput and signal power tests should be conducted to determine the impact multiple UE connections may cause.

APPENDIX A: Payload Assembly and Configuration

A.1 Physical Assembly

The payload, shown in Figure A.1, consists of the SIM8200EA-M2 5G hat, Raspberry Pi 4 and the Raspberry Pi Camera NoIR.

Assemble the camera mount and camera in accordance with manufacturers' instructions. Install camera mount onto top of black acrylic case panel of 5G hat, noted in item 10 of Figure A.2 [66]. Thread camera cable through opening in top of black acrylic case panel and insert into camera slot of Raspberry Pi. Ensure silver contacts of cable are facing the HDMI port [67].

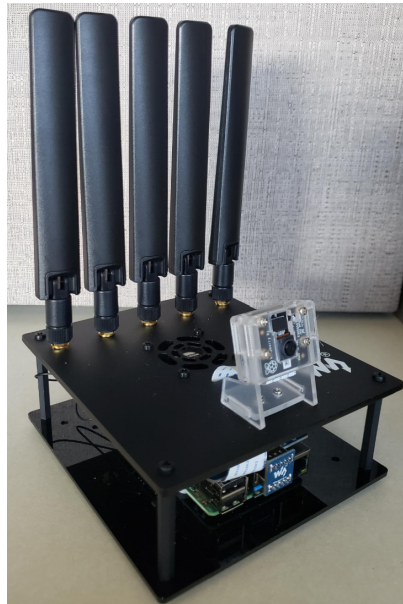
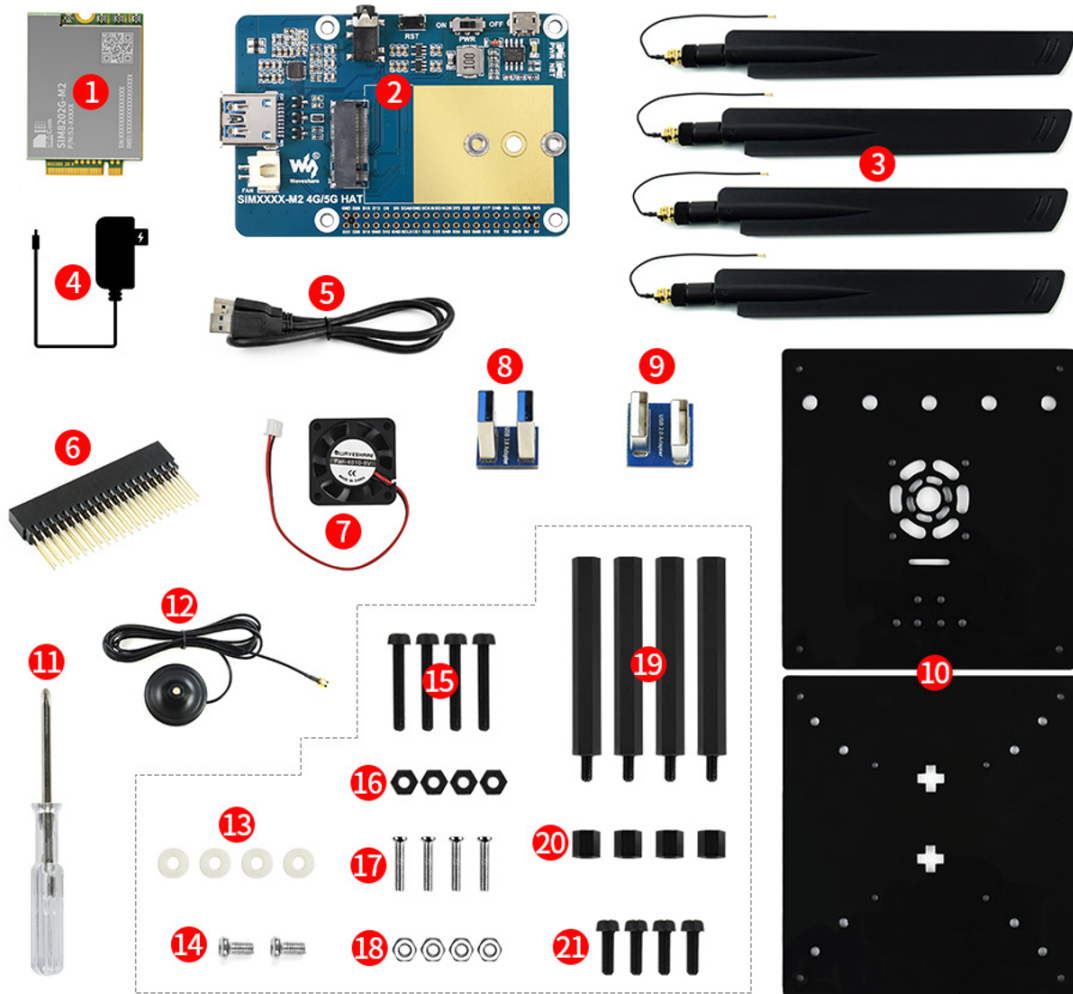


Figure A.1. Assembled Payload

Instructions to physically assemble the 5G Hat and Raspberry Pi were found at reference [66] and are listed in Figures A.3 – A.6.

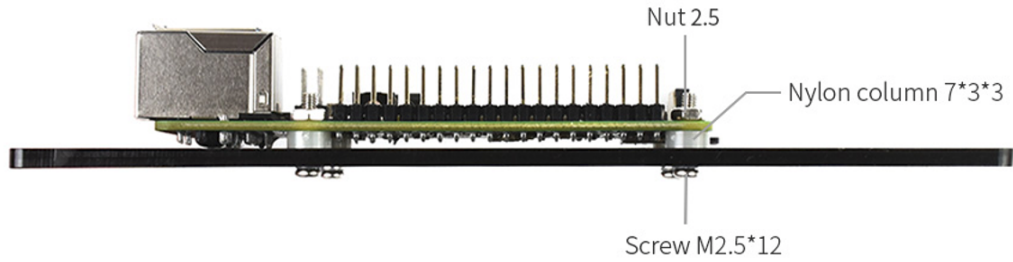


- | | | |
|--|------------------------------|--------------------------------|
| 1. SIMXXXX-M2 | 8. USB3.0 Adapter | 15. Black nylon screws M3*20 |
| 2. SIMXXXX-M2 4G/5G HAT | 9. USB2.0 Adapter | 16. Black nylon nut M3 |
| 3. 5G/4G/3G/GNSS External Antenna | 10. Black acrylic case panel | 17. Screw M2.5*12 |
| 4. Power adapter 5V 3A Micro | 11. Screwdriver | 18. Nut 2.5 |
| 5. Power adapter 5V 3A MicroUSB3.0 dual plug cable | 12. Antenna sucker base | 19. Black nylon column M3*45+6 |
| 6. 2x20PIN pin header | 13. Nylon column 7*3*3 | 20. Black nylon column M3*5 |
| 7. 4010 cooling fan | 14. Round head screw M3*5 | 21. Black nylon screws M3*10 |

Figure A.2. Installation of 5G Hat and Raspberry Pi: Equipment Required.
Source: [66].

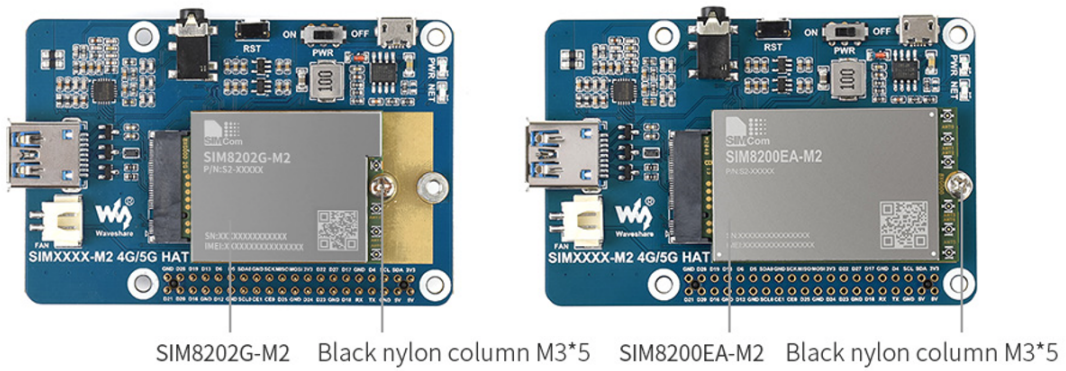
Step 1

Install the Raspberry Pi into the black acrylic base.



Step 2

Install the SIMXXXX-M2 main board into the SIMXXXX-M2 4G/5G HAT base board.



Step 3

Install SIMXXXX-M2 4G/5G HAT base into the Raspberry Pi.

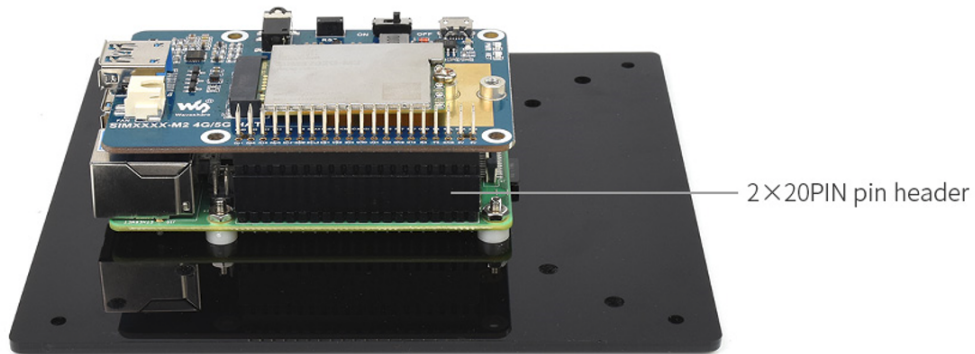
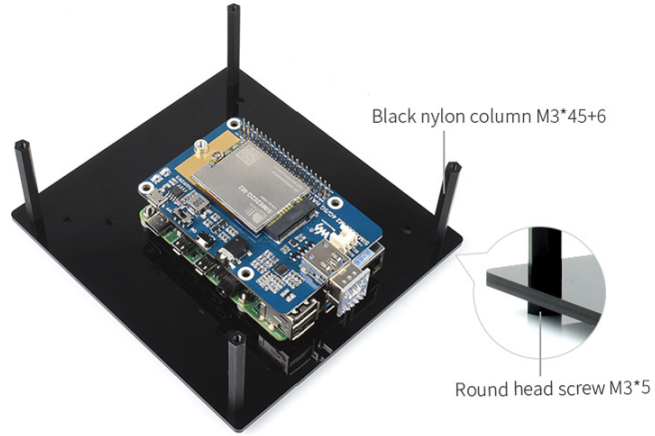


Figure A.3. Installation of 5G Hat and Raspberry Pi: Steps 1-3. Source: [66].

Step 4

Install Black nylon column M3*45+6 into the black acrylic base board.



Step 5

Install 4010 cooling fan and Antenna adapter cable into Black acrylic upper cover board.

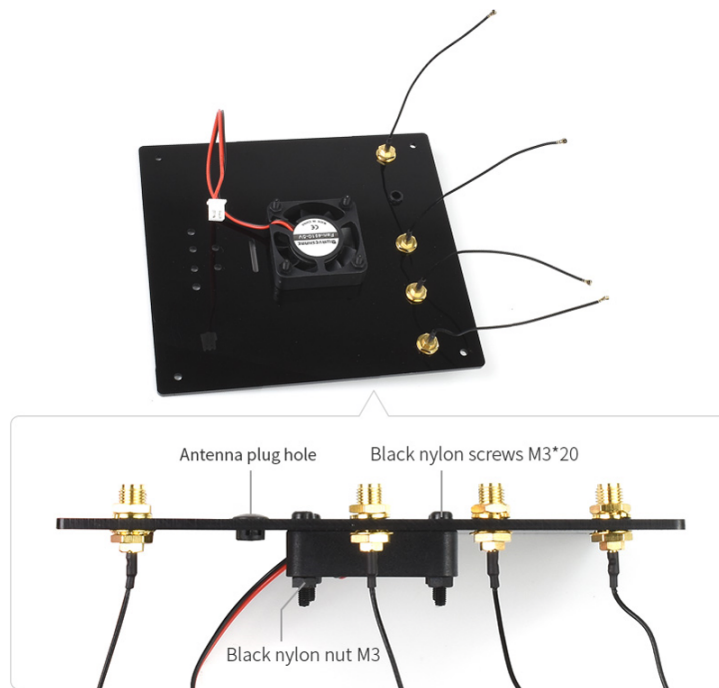
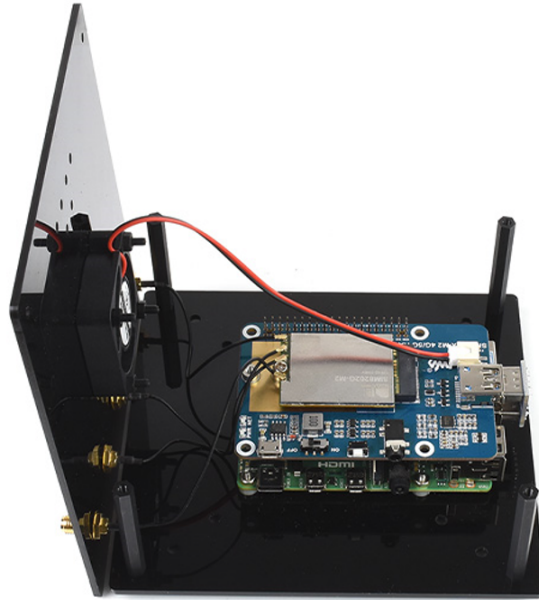


Figure A.4. Installation of 5G Hat and Raspberry Pi: Steps 4-5. Source: [66].

Step 6

Connect the Antenna adapter cable to the SIMXXX-M2 main board;
Connect the cooling fan to the SIMXXX-M2 4G/5G HAT base board.



Step 7

Assemble the black acrylic cover and fix with screws.



Figure A.5. Installation of 5G Hat and Raspberry Pi: Steps 6-7. Source: [66].

Step 8

Install the External Antenna. Finish!

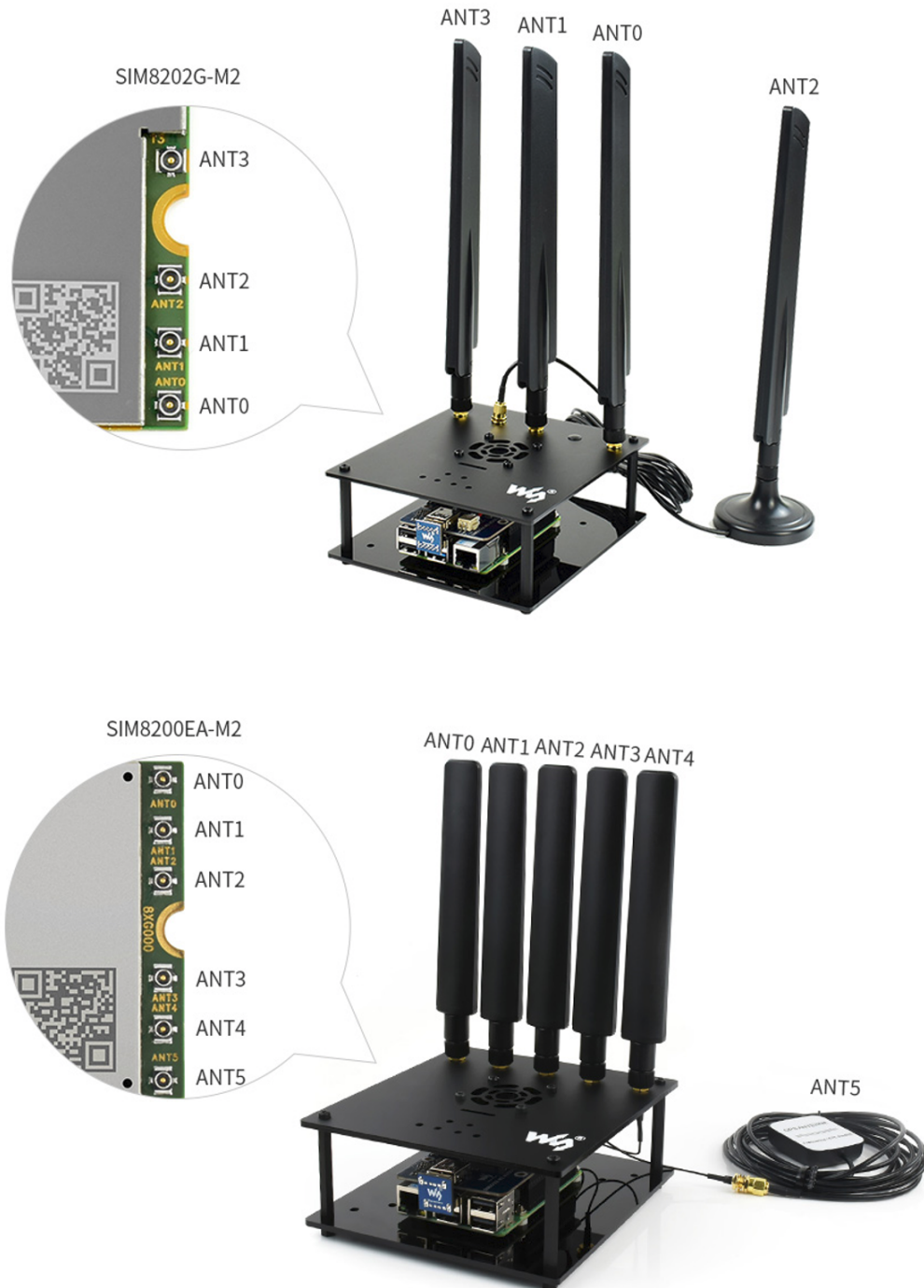


Figure A.6. Installation of 5G Hat and Raspberry Pi: Step 8. Source: [66].

A.2 Configure 5G Hat

The micro-secure digital (SD) card slot of the Raspberry Pi holds a 32-bit SD card with the Raspberry Pi Legacy operating system (OS) Debian Buster, as shown in Figure A.7.

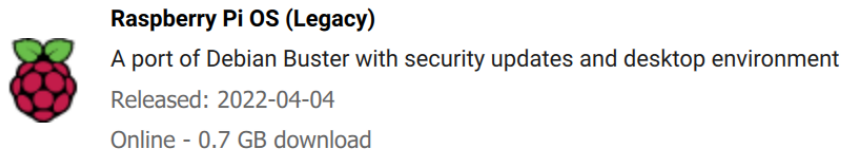


Figure A.7. Raspberry Pi 4 OS Installation to Debian Buster

Power on the Raspberry Pi 4 and 5G hat. Connect Raspberry Pi 4 to a display monitor. Connect the Raspberry Pi 4 to the AT&T WiFi hotspot. Follow the SIM8200EA-M2 5G hat driver installation instructions listed at [68].

During installation, errors were encountered after entering the commands in Figure A.8 into a terminal window on the Raspberry Pi.

```
sudo apt-get install p7zip-full
wget https://www.waveshare.com/w/upload/f/fb/SIM8200-M2_5G_HAT_code.7z
7z x SIM8200-M2_5G_HAT_code.7z
sudo chmod 777 -R SIM8200-M2_5G_HAT_code
cd SIM8200-M2_5G_HAT_code
sudo ./install.sh
```

Figure A.8. Waveshare Instructions for 5G Hat Driver Install. Source: [68].

Technical support was contacted and advised to install the SIM820X RNDIS Dial-up in accordance with [69]. After completing the commands in Figure A.9, the device was able to ping *www.google.com*.

```
wget https://www.waveshare.net/w/upload/1/1e/SIM820X_RNDIS.zip
sudo apt-get install python3-pip
sudo pip3 install pyserial
sudo apt-get install unzip
unzip SIM820X_RNDIS.zip
sudo chmod 777 SIM820X_RNDIS.py
sudo python3 SIM820X_RNDIS.py
```

Figure A.9. RNDIS Dial-up Commands. Source: [69].

At this point, wwan0 was not listed after running the *ifconfig -a* command as noted in Figure A.10.

```
pi@raspberrypi:~ $ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.3.131 netmask 255.255.255.0 broadcast 192.168.3.255
    inet6 fe80::d244:10b2:68b5:7245 prefixlen 64 scopeid 0x20<link>
    ether dc:a6:32:15:53:ae txqueuelen 1000 (Ethernet)
    RX packets 3432 bytes 749255 (731.6 KiB)
    RX errors 0 dropped 1 overruns 0 frame 0
    TX packets 2684 bytes 517939 (505.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 720 (720.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 720 (720.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.3.18 netmask 255.255.255.0 broadcast 192.168.3.255
    inet6 fe80::72f2:4bda:904:bedd prefixlen 64 scopeid 0x20<link>
    ether dc:a6:32:15:53:af txqueuelen 1000 (Ethernet)
    RX packets 392 bytes 60128 (58.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 469 bytes 93530 (91.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wwan0: flags=4291<UP,BROADCAST,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 169.254.160.22 netmask 255.255.0.0 broadcast 169.254.255.255
    inet6 fe80::b771:2b43:17d9:2ac6 prefixlen 64 scopeid 0x20<link>
    ether 22:3a:ef:1c:81:fa txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14 bytes 3379 (3.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure A.10. *ifconfig -a wwan0*. Source: [68].

Follow the instructions to install minicom by entering the commands listed in Figure A.11 [68].

```
sudo apt-get install minicom
sudo minicom -D /dev/ttyUSB2
```

Figure A.11. Minicom Installation Commands. Source: [68].

Restore default settings of the module through the serial port by running the command in Figure A.12 [69].

```
at+cusbcfg=usbid,1e0e,9001
```

Figure A.12. AT Command from RNDIS Instructions. Source: [69].

Open a new terminal window. Run the *ifconfig -a* command again and verify *wwan0* is listed as shown in Figure A.10.

Enable 5G networking by entering the commands in Figure A.13 [68].

```
cd Goonline
make
sudo ./simcom-cm
```

Figure A.13. 5G Networking Commands. Source: [68].

Turned off WiFi network connection and restart the Raspberry Pi and 5G hat. The 5G hat is now configured to work with the Raspberry Pi 4 and the Amarisoft Callbox Classic network.

A.3 Enable Camera

Power on Raspberry Pi and open a terminal window. Follow the steps in Figure A.14.

1. Ensure your system is up-to-date and reboot it.
2. Run `sudo raspi-config`.
3. Navigate to `Interface Options` and select `Legacy camera` to enable it.
4. Reboot your Raspberry Pi again.

Figure A.14. Camera Enable Instructions. Source: [67].

APPENDIX B: Configuring the Amarisoft Network

B.1 Quarterly Update Installation Instructions

Installation is completed by following the instructions in the lteenb.pdf files downloaded with the latest Amarisoft software update. The Callbox Classic is configured to provide 4G LTE network capability by default upon installation of the configuration files. This includes configuration files for the eNodeB, mobility management entity (MME), multimedia broadcast multicast service gateway (MBMSGW), IMS and transceiver SDR (TRX SDR). Figure B.1 shows the files created after downloading the quarterly Amarisoft update.

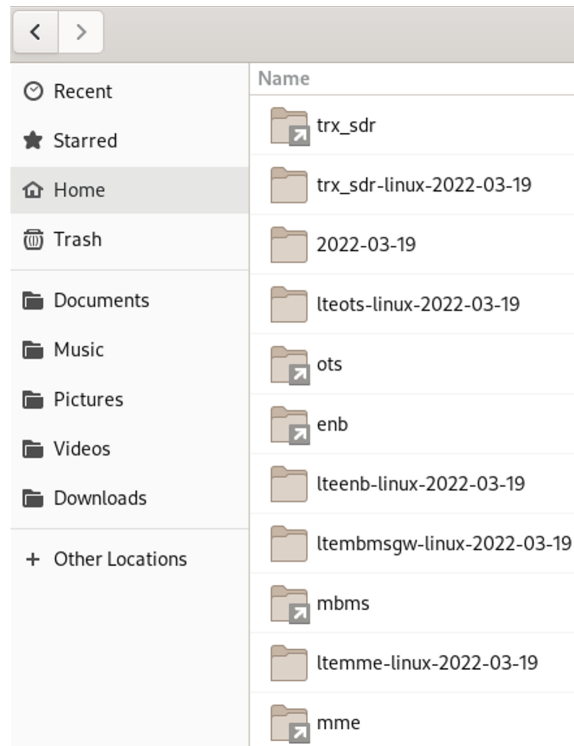
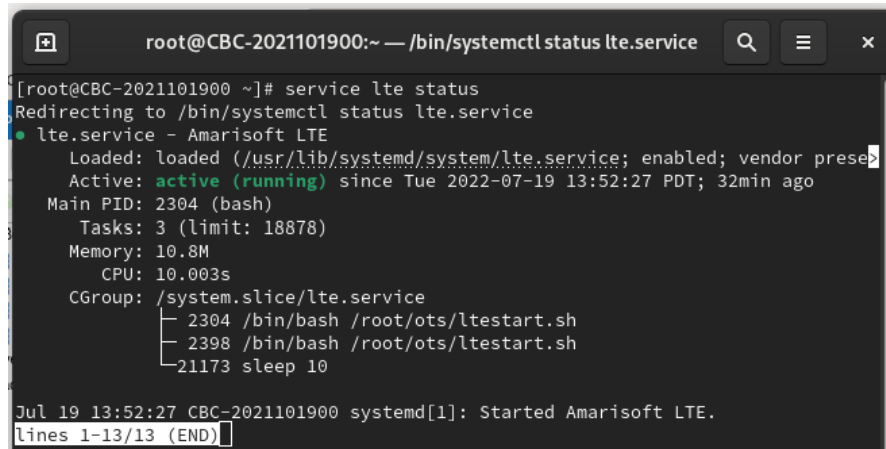


Figure B.1. Files Downloaded with the quarterly update

B.2 4G LTE Network Configuration

Upon startup of the Callbox Classic, LTE services are automatically started. This can be verified by opening a terminal window and entering the command `service lte status` and verifying that "active(running)" is returned, as shown in Figure B.2.



```
root@CBC-2021101900:~ — /bin/systemctl status lte.service
[root@CBC-2021101900 ~]# service lte status
Redirecting to /bin/systemctl status lte.service
● lte.service - Amarisoft LTE
   Loaded: loaded (/usr/lib/systemd/system/lte.service; enabled; vendor prese
   Active: active (running) since Tue 2022-07-19 13:52:27 PDT; 32min ago
   Main PID: 2304 (bash)
     Tasks: 3 (limit: 18878)
    Memory: 10.8M
       CPU: 10.003s
   CGroup: /system.slice/lte.service
           └─ 2304 /bin/bash /root/ots/ltetestart.sh
              2398 /bin/bash /root/ots/ltetestart.sh
             21173 sleep 10

Jul 19 13:52:27 CBC-2021101900 systemd[1]: Started Amarisoft LTE.
lines 1-13/13 (END)
```

Figure B.2. Steps required to verify the LTE Service is running

The default 4G LTE service uses the `enb.default.cfg` configuration file. Basic configurations can be changed at the top of the `enb.default.cfg` file as shown in Figure B.3. These configurations are:

- TDD or FDD
- Different values of resource block for downlink
- The number of antennas used for downlink and uplink
- Enable or disable channel simulator
- Enhanced version of the eNodeB

None of these settings were changed in this thesis work due to focusing on the 5G network configuration.

```

enb.default.cfg
~/enb/config
1 /* lte4n configuration file version 2022-03-19
2 * Copyright (C) 2015-2022 Amarisoft
3 */
4
5 #define TDD                0 // Values: 0 (FDD), 1(TDD)
6 #define N_RB_DL            25 // Values: 6 (1.4 MHz), 15 (3MHz), 25 (5MHz), 50
   (10MHz), 75 (15MHz), 100 (20MHz)
7 #define N_ANTENNA_DL      1 // Values: 1 (SISO), 2 (MIMO 2x2)
8 #define N_ANTENNA_UL      1 // Values: 1, 2
9 #define CHANNEL_SIM       0 // Values: 0 (channel simulator disabled), 1 (channel
   simulator enabled)
10 #define NG_ENB            0 // 1 for ng-eNB

```

Figure B.3. 4G LTE Default Configuration Options

B.3 4G LTE Band Configuration

To switch between 4G LTE bands, open the enb.default.cfg file on the Amarisoft Callbox Classic. Uncomment the line with the band to be used. Comment out the line of all bands not to be used. Figure B.4 shows band 3 being used for 4G LTE. Figure B.5 shows band 7 being used for 4G LTE.

```

85 #if TDD == 1
86     //dl_earfcn: 38050, /* 2600 MHz (band 38) */
87     dl_earfcn: 40620, /* 2593 MHz (band 41) */
88     //dl_earfcn: 42590, /* 3500 MHz (band 42) */
89 #else
90     //dl_earfcn: 300, /* DL center frequency: 2132 MHz (Band 1) */
91     //dl_earfcn: 900, /* DL center frequency: 1960 MHz (Band 2) */
92     dl_earfcn: 1575, /* DL center frequency: 1842.5 MHz (Band 3) */
93     //dl_earfcn: 2150, /* DL center frequency: 2130 MHz (Band 4) */
94     //dl_earfcn: 2525, /* DL center frequency: 881.5 MHz (Band 5) */
95     //dl_earfcn: 3350, /* DL center frequency: 2680 MHz (Band 7) */
96     //dl_earfcn: 6300, /* 806 MHz (Band 20) */
97     //dl_earfcn: 38050, /* 2600 MHz (band 38) */
98     //dl_earfcn: 40620, /* 2593 MHz (band 41) */
99     //dl_earfcn: 42590, /* 3500 MHz (band 42) */
100 #endif

```

Figure B.4. 4G LTE Band 3 in Configuration File

```

85 #if TDD == 1
86     //dl_earfcn: 38050, /* 2600 MHz (band 38) */
87     dl_earfcn: 40620, /* 2593 MHz (band 41) */
88     //dl_earfcn: 42590, /* 3500 MHz (band 42) */
89 #else
90     //dl_earfcn: 300, /* DL center frequency: 2132 MHz (Band 1) */
91     //dl_earfcn: 900, /* DL center frequency: 1960 MHz (Band 2) */
92     //dl_earfcn: 1575, /* DL center frequency: 1842.5 MHz (Band 3) */
93     //dl_earfcn: 2150, /* DL center frequency: 2130 MHz (Band 4) */
94     //dl_earfcn: 2525, /* DL center frequency: 881.5 MHz (Band 5) */
95     dl_earfcn: 3350, /* DL center frequency: 2680 MHz (Band 7) */
96     //dl_earfcn: 6300, /* 806 MHz (Band 20) */
97     //dl_earfcn: 38050, /* 2600 MHz (band 38) */
98     //dl_earfcn: 40620, /* 2593 MHz (band 41) */
99     //dl_earfcn: 42590, /* 3500 MHz (band 42) */
100 #endif

```

Figure B.5. 4G LTE Band 7 in Configuration File

After making any network configuration changes, the network must be restarted by entering the command *service lte restart* in a terminal window.

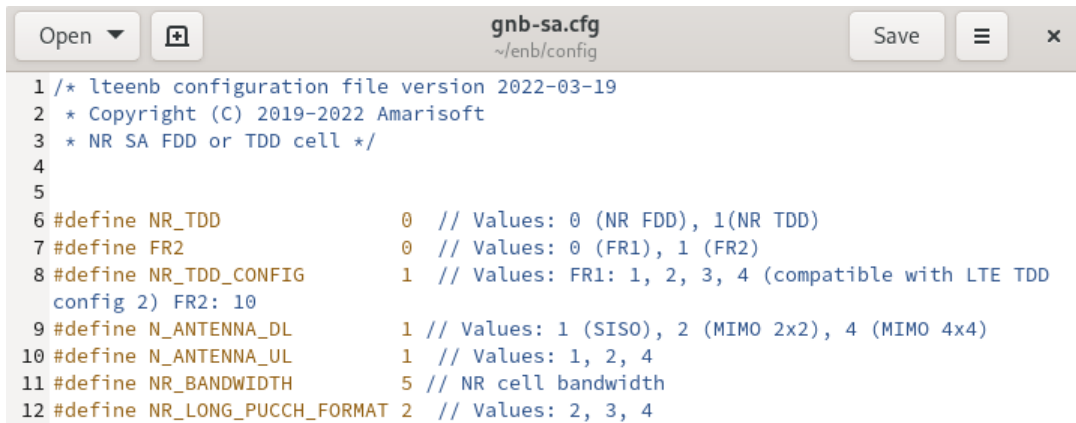
B.4 5G Network Configuration

This thesis uses the 5G SA configuration found in the `gnb-sa.cfg` file. Basic configurations can be changed at the top of the configuration file as show in Figure B.6. These configurations are:

- TDD or FDD
- FR1 or FR2
- Pre-defined TDD configuration patterns
- The number of antennas used for downlink and uplink
- Bandwidth used
- Bits per symbol for physical uplink control channel (PUCCH) Format

In this thesis, configurations were changed for the `N_ANTENNA_DL`, `N_ANTENNA_UL`, and `NR_BANDWIDTH` only.

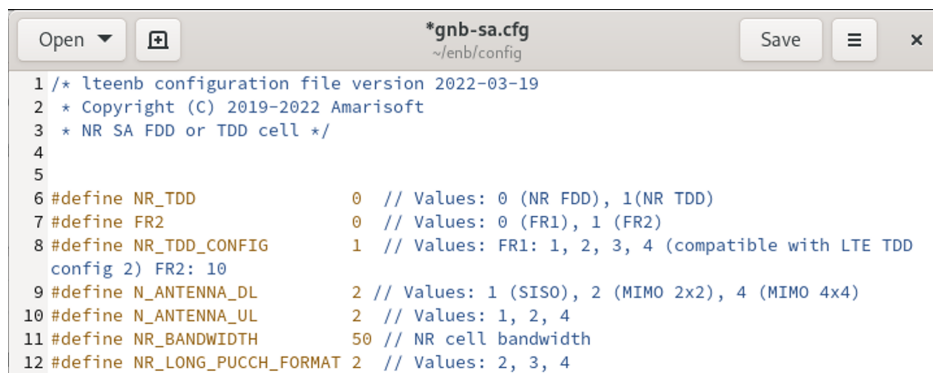
Figure B.6 shows a 1x1 SISO configuration with a 5 MHz bandwidth.



```
1 /* lte-nb configuration file version 2022-03-19
2 * Copyright (C) 2019-2022 Amarisoft
3 * NR SA FDD or TDD cell */
4
5
6 #define NR_TDD          0 // Values: 0 (NR FDD), 1(NR TDD)
7 #define FR2             0 // Values: 0 (FR1), 1 (FR2)
8 #define NR_TDD_CONFIG  1 // Values: FR1: 1, 2, 3, 4 (compatible with LTE TDD
   config 2) FR2: 10
9 #define N_ANTENNA_DL   1 // Values: 1 (SISO), 2 (MIMO 2x2), 4 (MIMO 4x4)
10 #define N_ANTENNA_UL  1 // Values: 1, 2, 4
11 #define NR_BANDWIDTH  5 // NR cell bandwidth
12 #define NR_LONG_PUCCH_FORMAT 2 // Values: 2, 3, 4
```

Figure B.6. Top of 5G Configuration File with a 1x1 SISO with a 5 MHz bandwidth configuration

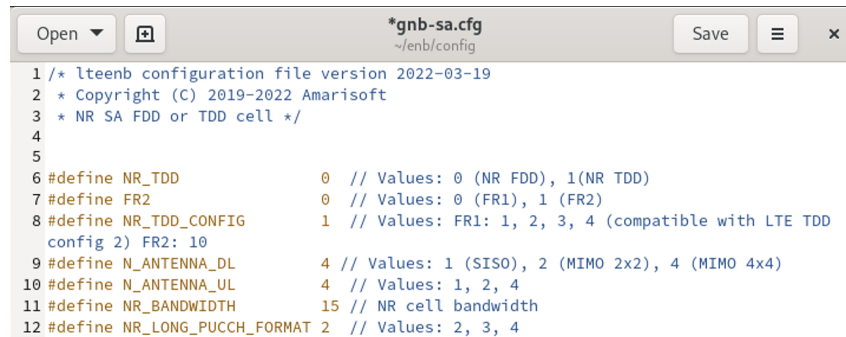
Figure B.7 shows a 2x2 MIMO configuration with 50 MHz bandwidth.



```
1 /* lte-nb configuration file version 2022-03-19
2 * Copyright (C) 2019-2022 Amarisoft
3 * NR SA FDD or TDD cell */
4
5
6 #define NR_TDD          0 // Values: 0 (NR FDD), 1(NR TDD)
7 #define FR2             0 // Values: 0 (FR1), 1 (FR2)
8 #define NR_TDD_CONFIG  1 // Values: FR1: 1, 2, 3, 4 (compatible with LTE TDD
   config 2) FR2: 10
9 #define N_ANTENNA_DL   2 // Values: 1 (SISO), 2 (MIMO 2x2), 4 (MIMO 4x4)
10 #define N_ANTENNA_UL  2 // Values: 1, 2, 4
11 #define NR_BANDWIDTH  50 // NR cell bandwidth
12 #define NR_LONG_PUCCH_FORMAT 2 // Values: 2, 3, 4
```

Figure B.7. 2x2 MIMO Configuration with 50 MHz Bandwidth

Figure B.8 shows a 4x4 MIMO configuration with a 15 MHz bandwidth.



```
1 /* lteemb configuration file version 2022-03-19
2 * Copyright (C) 2019-2022 Amarisoft
3 * NR SA FDD or TDD cell */
4
5
6 #define NR_TDD          0 // Values: 0 (NR FDD), 1(NR TDD)
7 #define FR2             0 // Values: 0 (FR1), 1 (FR2)
8 #define NR_TDD_CONFIG  1 // Values: FR1: 1, 2, 3, 4 (compatible with LTE TDD
  config 2) FR2: 10
9 #define N_ANTENNA_DL   4 // Values: 1 (SISO), 2 (MIMO 2x2), 4 (MIMO 4x4)
10 #define N_ANTENNA_UL   4 // Values: 1, 2, 4
11 #define NR_BANDWIDTH   15 // NR cell bandwidth
12 #define NR_LONG_PUCCH_FORMAT 2 // Values: 2, 3, 4
```

Figure B.8. 4x4 MIMO Configuration with 15 MHz Bandwidth

After making any network configuration changes, the network must be restarted by entering the command `service lte restart` in a terminal window.

B.5 5G Band Configuration

To change the default TDD and FDD frequency bands, edit the band, `dl_nr_arfcn`, `subcarrier_spacing`, and `ssb_pos_bitmap` to be the correct data for the desired frequency band as shown in Figure B.9. This thesis uses FDD for testing, therefore uses frequency band 7.

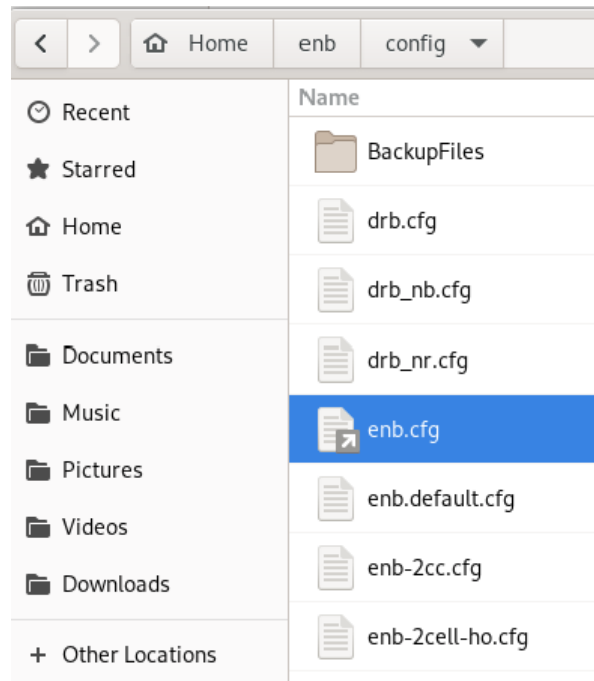


Figure B.10. eNodeB Configuration Pointer File Location

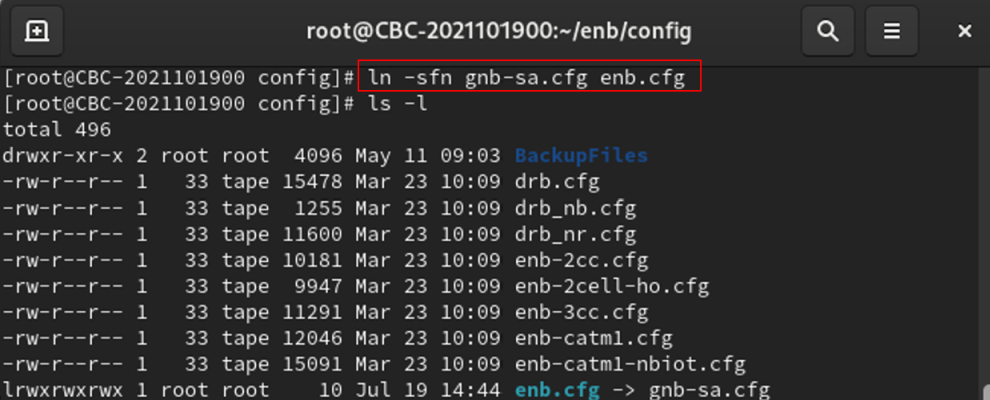
The default eNodeB configuration file is labeled "enb.default.cfg", and shown in Figure B.11. The file used for the 5G SA testing is labeled "gnb-sa.cfg".

```

root@CBC-2021101900:~/enb/config
[root@CBC-2021101900 ~]# cd enb/config/
[root@CBC-2021101900 config]# ls -l
total 496
drwxr-xr-x 2 root root 4096 May 11 09:03 BackupFiles
-rw-r--r-- 1 33 tape 15478 Mar 23 10:09 drb.cfg
-rw-r--r-- 1 33 tape 1255 Mar 23 10:09 drb_nb.cfg
-rw-r--r-- 1 33 tape 11600 Mar 23 10:09 drb_nr.cfg
-rw-r--r-- 1 33 tape 10181 Mar 23 10:09 enb-2cc.cfg
-rw-r--r-- 1 33 tape 9947 Mar 23 10:09 enb-2cell-ho.cfg
-rw-r--r-- 1 33 tape 11291 Mar 23 10:09 enb-3cc.cfg
-rw-r--r-- 1 33 tape 12046 Mar 23 10:09 enb-catm1.cfg
-rw-r--r-- 1 33 tape 15091 Mar 23 10:09 enb-catm1-nbiot.cfg
lrwxrwxrwx 1 root root 15 Jul 19 14:44 enb.cfg -> enb.default.cfg
  
```

Figure B.11. eNodeB Default Configuration File Pointer

To switch the pointer, open a terminal window and enter the command `ln -sfn <new configuration file> enb.cfg` where `<new configuration file>` is the file to be used, as show in Figure B.12.



```
root@CBC-2021101900:~/enb/config
[root@CBC-2021101900 config]# ln -sfn gnb-sa.cfg enb.cfg
[root@CBC-2021101900 config]# ls -l
total 496
drwxr-xr-x 2 root root 4096 May 11 09:03 BackupFiles
-rw-r--r-- 1 33 tape 15478 Mar 23 10:09 drb.cfg
-rw-r--r-- 1 33 tape 1255 Mar 23 10:09 drb_nb.cfg
-rw-r--r-- 1 33 tape 11600 Mar 23 10:09 drb_nr.cfg
-rw-r--r-- 1 33 tape 10181 Mar 23 10:09 enb-2cc.cfg
-rw-r--r-- 1 33 tape 9947 Mar 23 10:09 enb-2cell-ho.cfg
-rw-r--r-- 1 33 tape 11291 Mar 23 10:09 enb-3cc.cfg
-rw-r--r-- 1 33 tape 12046 Mar 23 10:09 enb-catm1.cfg
-rw-r--r-- 1 33 tape 15091 Mar 23 10:09 enb-catm1-nbiot.cfg
lrwxrwxrwx 1 root root 10 Jul 19 14:44 enb.cfg -> gnb-sa.cfg
```

Figure B.12. Changing eNodeB Pointer to gnb-sa.cfg

After making any network configuration changes, the network must be restarted by entering the command `service lte restart` in a terminal window.

B.7 Location of 4G and 5G Configuration Files

The full 4G and 5G configuration files are located on the NPS GitLab, under the project “LevitonThesis_5G and Drones”.

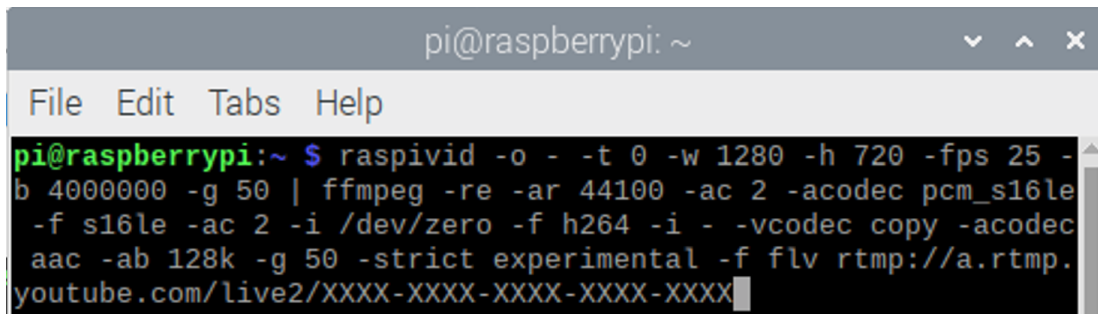
THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C: Uplink and Downlink Testing

C.1 Uplink Testing

C.1.1 Video Stream

Figure C.1 shows the command entered into a terminal window on the Raspberry Pi to start the video stream. The XXXX-XXXX-XXXX-XXXX-XXXX in the command refers to the stream key used to live stream the video to an account on YouTube and has been redacted from this thesis.

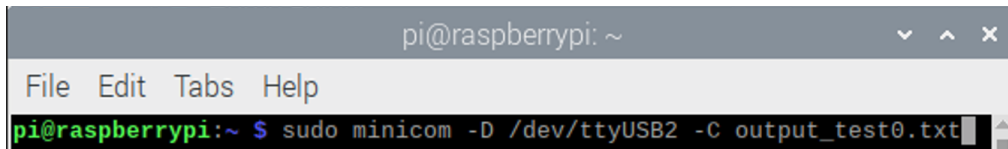


```
pi@raspberrypi: ~  
File Edit Tabs Help  
pi@raspberrypi:~ $ raspivid -o - -t 0 -w 1280 -h 720 -fps 25 -  
b 4000000 -g 50 | ffmpeg -re -ar 44100 -ac 2 -acodec pcm_s16le  
-f s16le -ac 2 -i /dev/zero -f h264 -i - -vcodec copy -acodec  
aac -ab 128k -g 50 -strict experimental -f flv rtmp://a.rtmp.  
youtube.com/live2/XXXX-XXXX-XXXX-XXXX-XXXX
```

Figure C.1. Command to Start Video Streaming on Payload. XXXX-XXXX-XXXX-XXXX-XXXX in the command refers to the personal stream key used to live stream to an account on YouTube and has been redacted from this thesis. Source: [70].

C.1.2 Signal Power Data Collection

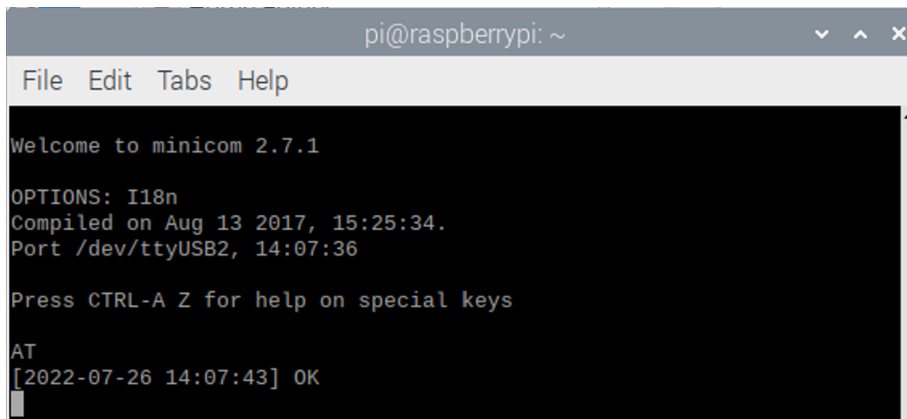
To measure the signal power at the payload, a minicom serial terminal was opened on the Raspberry Pi, with output going to a text file, as shown in Figure C.2.

A terminal window titled 'pi@raspberrypi: ~' with a menu bar containing 'File Edit Tabs Help'. The command 'sudo minicom -D /dev/ttyUSB2 -C output_test0.txt' is entered at the prompt.

```
pi@raspberrypi: ~  
File Edit Tabs Help  
pi@raspberrypi:~ $ sudo minicom -D /dev/ttyUSB2 -C output_test0.txt
```

Figure C.2. Open Minicom Command

Once the minicom terminal was opened, a timestamp was added by pressing *ctrl+N*, as shown in Figure C.3. As the payload was at each meter interval, the time was manually recorded for correlation during result analysis.

A terminal window titled 'pi@raspberrypi: ~' with a menu bar containing 'File Edit Tabs Help'. The output shows the minicom version, options, compilation date, port, and a timestamp added after pressing Ctrl+N.

```
pi@raspberrypi: ~  
File Edit Tabs Help  
Welcome to minicom 2.7.1  
OPTIONS: I18n  
Compiled on Aug 13 2017, 15:25:34.  
Port /dev/ttyUSB2, 14:07:36  
Press CTRL-A Z for help on special keys  
AT  
[2022-07-26 14:07:43] OK
```

Figure C.3. Minicom Timestamp Added

A script was created to request a quality signal report every ten seconds, as show in Figure C.4

```
script.txt - Mousepad
File Edit Search View Document Help
verbose on
timeout 900
start:
  send AT+CSQ
  expect "OK"
  sleep 10
  goto start
```

Figure C.4. CSQ Script

In minicom, the script was run, as shown in Figure C.5.

```
pi@raspberrypi: ~
File Edit Tabs Help
Welcome to minicom 2.7.1
OPTIONS: I18n
Compiled +-----[Run a script]-----
Port /dev|
Press CTR| A - Username      :
          | B - Password     :
          | C - Name of script : script.txt
AT       |
[2022-07-| Change which setting? (Return to run, ESC to stop)
+-----
```

Figure C.5. Running the CSQ script in minicom

The results are a continuous output to the terminal window, as shown in Figure C.6 with the same information saved in the text file referenced in Figure C.2 and the output shown in Figure C.7.

```
pi@raspberrypi: ~
File Edit Tabs Help
Welcome to minicom 2.7.1
OPTIONS: I18n
Compiled on Aug 13 2017, 15:25:34.
Port /dev/ttyUSB2, 14:07:36
Press CTRL-A Z for help on special keys
AT
[2022-07-26 14:07:43] OK
[2022-07-26 14:08:06] AT+CSQ
[2022-07-26 14:08:06] +CSQ: 28,99
[2022-07-26 14:08:06] OKAT+CSQ
[2022-07-26 14:08:16] +CSQ: 28,99
[2022-07-26 14:08:16]
[2022-07-26 14:08:16] OK
```

Figure C.6. Minicom CSQ Script Output in Minicom

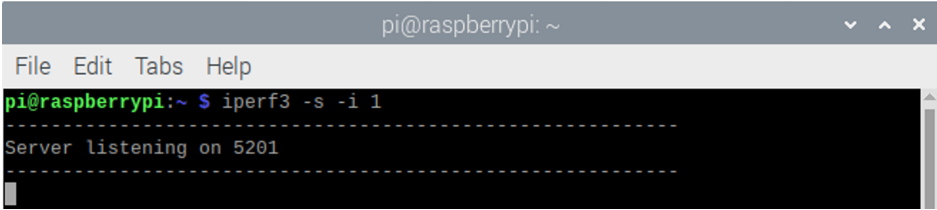
```
output_test0.txt - Mousepad
File Edit Search View Document Help
AT
[2022-07-26 14:07:43] OK
[2022-07-26 14:08:06] AT+CSQ
[2022-07-26 14:08:06] +CSQ: 28,99
[2022-07-26 14:08:06] OKAT+CSQ
[2022-07-26 14:08:16] +CSQ: 28,99
[2022-07-26 14:08:16]
[2022-07-26 14:08:16] OK
```

Figure C.7. Minicom CSQ Script

C.2 Throughput Testing

The downlink throughput testing was conducted using iPerf, a tool for active measurements of various parameters [71].

An iPerf server was started on the Raspberry Pi by entering the command in Figure C.8 in to a terminal window.



```
pi@raspberrypi: ~  
File Edit Tabs Help  
pi@raspberrypi:~ $ iperf3 -s -i 1  
-----  
Server listening on 5201  
-----
```

Figure C.8. iPerf Server Start Command on Raspberry Pi

On the Amarisoft Callbox Classic, the eNodeB logs were accessed by attaching a screen to the LTE service by typing `screen -x lte` into a terminal window and navigating to the ENB tab by pressing `ctrl+a +l`. To verify the network configuration, enter `cell phy` into the ENB log, as shown in Figure C.9. A trace of all connections can be started by entering `t` into the ENB log. This test focuses on the downlink bitrate provided by the trace as shown in Figure C.9.


```

root@CBC-2021101900:~ — screen -x lte

[root@CBC-2021101900 enb]#
[root@CBC-2021101900 enb]# cd /root/enb
[root@CBC-2021101900 enb]# /root/lteots-linux-2022-03-19/lte!aunch.sh ENB
Base Station version 2022-03-19, Copyright (C) 2012-2022 Amarisoft
This software is licensed to NAVAL POST GRADUATE SCHOOL.
Support and software update available until 2022-09-29.

RF0: sample_rate=17.280 MHz dl_freq=2680.100 MHz ul_freq=2560.100 MHz (band n7) dl_ant=1 ul_ant=1
(enb)
(enb) log file.rotate=250M,file.path=/var/log/lte/
(enb) cell phy
[gnb0012345] PLMN=00101 gNB_ID=0x12345
-----Global-----DL-----UL-----SSB---
Cell  RAT BAND BW P  ARFCN ANT NL SCS  QAM  ARFCN ANT NL SCS  QAM  ARFCN SCS
0x001  NR  n7  15  0  536020  1  1  15  256  512020  1  1  15  256  535450  15
(enb) t
Press [return] to stop the trace
PRACH: cell=01 seq=3 ta=3 snr=25.2 dB
-----DL-----UL-----
UE_ID  CL RNTI C  cqI  rI  mcs  retx  txok  brate  snr  pucl  mcs  rxko  rxok  brate  #its  phr  pl  ta
3 001 4603 1  5  1  6.0  0  3 29.1k 11.1  - 14.0  0  2 14.2k 2/2.5/3 38 84 -0.1
3 001 4603 1 15  1 26.0  0  7 3.70k 11.3  - 12.3  1  3 1.82k 2/3.0/5 38 82 0.0
3 001 4603 1 15  1 26.0  0  4 2.06k 11.3  -  -  0  0  0  - 38 82 -
3 001 4603 1 15  1 25.5  1  3 1.54k 11.3  -  -  0  0  0  - 38 82 -
3 001 4603 1 15  1 25.0  0  4 2.06k 11.3  -  -  0  0  0  - 38 82 -
3 001 4603 1 15  1 24.7  2  4 2.04k 11.3  -  -  0  0  0  - 38 82 -
PRACH: cell=01 seq=6 ta=2 snr=26.3 dB
4 001 4604 1 15  1 15.1  1  9 4.06k 13.8  - 12.5  0  5 2.54k 1/1.8/2 38 80 0.8
4 001 4604 1 15  1 26.0  0  4 2.06k 13.8  -  -  0  0  0  - 38 80 -
4 001 4604 1 15  1 25.2  2  4 2.06k 13.8  -  -  0  0  0  - 38 80 -
4 001 4604 1 15  1 25.0  0  4 2.06k 13.8  -  -  0  0  0  - 38 80 -

```

Figure C.9. ENB Trace example for Downlink Testing

The iPerf client was started on the Amarisoft Callbox Classic by entering the command in Figure C.10 in to a terminal window.

```

root@CBC-2021101900:~ — iperf -c 192.168.2.2 -u -b 150M -i 1 -t 60
[root@CBC-2021101900 ~]# iperf -c 192.168.2.2 -u -b 150M -i 1 -t 60 | tee testDL0-5M.txt
-----
Client connecting to 192.168.2.2, UDP port 5001
Sending 1470 byte datagrams, IPG target: 74.77 us (kalman adjust)
UDP buffer size: 208 KByte (default)
-----
[ 1] local 192.168.2.1 port 49015 connected with 192.168.2.2 port 5001
[ ID] Interval      Transfer      Bandwidth
[ 1] 0.00-1.00 sec  18.8 MBytes  157 Mbits/sec

```

Figure C.10. iPerf Client Start Command on Amarisoft Callbox Classic

Once the command executed fully, the trace in the ENB log file was stopped by pressing the *enter* button while in the ENB log file terminal window. The data recorded was copied and pasted into the file opened during the client iPerf testing.

C.3 MATLAB Code and Testing Data Files Location

The MATLAB code used for data analysis and graphing are located on the NPS GitLab, under the project “LevitonThesis_5G and Drones”. This site also holds the data for the Uplink Signal Power and Downlink Throughput testing data.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

- [1] Qualcomm, “Everything You Need to Know About 5G,” Accessed Jul. 14, 2022 [Online]. Available: <https://www.qualcomm.com/5g/what-is-5g>
- [2] H. Remmert, “What Is 5G Network Architecture?” Digi, Mar. 19, 2021 [Online]. Available: <https://www.digi.com/blog/post/5g-network-architecture>
- [3] RF Wireless World, “5G NR Carrier Aggregation (CA) Basics | Carrier Aggregation Frequency Bands,” Accessed Jul. 14, 2022 [Online]. Available: <https://www.rfwireless-world.com/5G/5G-NR-Carrier-Aggregation-basics.html>
- [4] Free Fly, “Introducing the All New Alta X,” Accessed Jul. 21, 2022 [Online]. Available: <https://freeflysystems.com/alta-x>
- [5] A. Dogra, R. K. Jha, and S. Jain, “A Survey on Beyond 5G Network With the Advent of 6G: Architecture and Emerging Technologies,” *IEEE Access*, vol. 9, pp. 67 512–67 547, 2021.
- [6] “5G NR User Plane Latency,” TechPlayOn, Jun. 20, 2019 [Online]. Available: <https://www.techplayon.com/5g-nr-user-plane-latency/>
- [7] C. Bock, “What is an IP Multimedia Subsystem (IMS core),” NG-Voice, Sep. 13, 2021 [Online]. Available: https://www.ng-voice.com/what-is-an-ip-multimedia-subsystem-ims-core/?utm_source=rss&utm_medium=rss&utm_campaign=what-is-an-ip-multimedia-subsystem-ims-core
- [8] Dialogic, “Multimedia Broadcast/Multicast Service (MBMS),” Accessed Jul. 22, 2022 [Online]. Available: <https://www.dialogic.com/glossary/multimedia-broadcastmulticast-service-mbmsi>
- [9] “LTE MBMS Delivering Broadcast and Multicast Services at LTE Speed,” RCR Wireless News, May 9, 2014 [Online]. Available: <https://www.rcrwireless.com/20140509/fundamentals/lte-mbms>
- [10] G. Wright and J. Burke, “Orthogonal Frequency-Division Multiplexing (OFDM),” Accessed Jul. 27, 2022 [Online]. Available: <https://www.techtarget.com/searchnetworking/definition/orthogonal-frequency-division-multiplexing#:~:text=Orthogonal%20frequency%2Ddivision%20multiplexing%20is,a%20single%20Wideband%20channel%20frequency.>

- [11] C. Craven, "What Is the 5G Spectrum? Definition," sdxcentral, Jan. 18, 2020 [Online]. Available: <https://www.sdxcentral.com/5g/definitions/what-is-5g/what-is-5g-spectrum/>
- [12] C. S. Nin, "Understanding FDD/TDD Carrier Aggregation for 5G," rcwireless, Apr. 20, 2021 [Online]. Available: <https://www.rcwireless.com/20210420/5g/understanding-fdd-tdd-carrier-aggregation-for-5g>
- [13] Viavi Solutions, *Understanding 5G, A Practical Guide to Deploying and Operating 5G Networks*, 2nd ed. USA: Viavi Solutions Inc, 2021.
- [14] RF Wireless, "MIMO vs SISO-Difference Between SISO and MIMO Techniques," Accessed Jul. 21, 2022 [Online]. Available: <https://www.rfwireless-world.com/Articles/difference-between-SISO-and-MIMO.html>
- [15] AVNET, "5G Beamforming: An Engineer's Overview," Accessed Jul. 21, 2022 [Online]. Available: <https://www.avnet.com/wps/portal/abacus/solutions/markets/communications/5g-solutions/5g-beamforming/>
- [16] Viavi, "5G Network Slicing," Accessed Jul. 14, 2022 [Online]. Available: <https://www.viavisolutions.com/en-us/5g-network-slicing>
- [17] VMware, "What is Software-Defined Networking (SDN)?" Accessed Jul. 18, 2022 [Online]. Available: <https://www.vmware.com/topics/glossary/content/software-defined-networking.html>
- [18] T. Xu, "What is a SIM Card? Why Do We Still Use Them?" Built-in, Mar. 30, 2021 [Online]. Available: <https://builtin.com/hardware/what-is-a-sim-card>
- [19] R. Kayne, "What is a SIM Card?" Built-in, Jul. 16, 2022 [Online]. Available: <https://www.easytechjunkie.com/what-is-a-sim-card.htm>
- [20] D. A. Roe, "3 Ways to Get the PUK Code of Your SIM Ccard," Built-in, Jul. 30, 2020 [Online]. Available: <https://www.digitalcitizen.life/get-puk-code-sim-card/>
- [21] Just Ask Thales, "What is the difference between PUK1 and PUK2 codes?" Accessed Jul. 21, 2022 [Online]. Available: <https://justaskthales.com/en/difference-puk1-puk2-codes/>
- [22] S. Segan, "What is an eSIM Card?" PC Mag, Mar. 8, 2021 [Online]. Available: <https://www.pcmag.com/how-to/what-is-an-esim-card>
- [23] EMnify, "What is an International Mobile Subscriber Identity (IMSI)?" Accessed Jul. 22, 2022 [Online]. Available: <https://www.emnify.com/iot-glossary/imsi>

- [24] Dukeson, “What is ICCID Number and Why Is It Important for Your SIM Card?” Cellular News, Feb. 5, 2021 [Online]. Available: <https://cellularnews.com/cellular-network/what-is-iccid-number-and-why-is-it-important-for-your-sim-card/>
- [25] EMnify, “What is an ICCID Number?” Accessed Jul. 22, 2022 [Online]. Available: <https://www.emnify.com/iot-glossary/iccid-number>
- [26] Tech Target, “IMEI (International Mobile Equipment Identity),” Accessed Jul. 22, 2022 [Online]. Available: <https://www.techtarget.com/whatis/definition/IMEI-International-Mobile-Equipment-Identity>
- [27] M. Goss, “5G vs. 4G: Learn the Key Differences Between Them,” Accessed Jul. 14, 2022 [Online]. Available: <https://www.techtarget.com/searchnetworking/feature/A-deep-dive-into-the-differences-between-4G-and-5G-networks>
- [28] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, “A Survey on 5G Usage Scenarios and Traffic Models,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 905–929, 2020.
- [29] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, “5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice,” *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1201–1221, 2017.
- [30] N. Yi, S. Horsmanheimo, L. Tuomimäki, S. Mehnert, T. Chen, A. Kostopoulos, A. Kourtis, H. Zhu, P. Assimakopoulos, G. Frangulea, and S. Kuklinski, “5G Harmonised Research and Trials for service Evolution between EU and China; Final Report of eMBB Trials,” *5G-Drive*, 2021.
- [31] Glade, David Lt Col USAF, “Unmanned Aerial Vehicles: Implications for Military Operations,” Center for Strategy and Technology Air War College, 2000 [Online]. Available: <https://apps.dtic.mil/sti/pdfs/ADA425476.pdf>
- [32] Northrop Grumman, “Global Hawk,” Accessed Jul. 15, 2022 [Online]. Available: <https://www.northropgrumman.com/what-we-do/air/global-hawk/>
- [33] Air Force, “RQ-4 Global Hawk,” Accessed Jul. 15, 2022 [Online]. Available: <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/>
- [34] Academic, “RQ-4 Global Hawk,” Accessed Aug. 02, 2022 [Online]. Available: <https://en-academic.com/dic.nsf/enwiki/23373>
- [35] Northrop Grumman, “Triton,” Accessed Jul. 15, 2022 [Online]. Available: <https://www.northropgrumman.com/what-we-do/air/triton/>

- [36] H. Reyes, "US Navy Tests Upgraded MQ-4C Triton Drone," *The Defense Post*, Aug. 2, 2021 [Online]. Available: <https://www.thedefensepost.com/2021/08/02/upgraded-triton-drone/>
- [37] Navy, "MQ-4C Triton," Accessed Jul. 15, 2022 [Online]. Available: <https://www.navair.navy.mil/product/MQ-4C/>
- [38] Aircraft Fandom, "Triton," Accessed Aug. 02, 2022 [Online]. Available: [https://aircraft.fandom.com/wiki/Northrop_Grumman_MQ-4C_Triton#Design\[edit\]](https://aircraft.fandom.com/wiki/Northrop_Grumman_MQ-4C_Triton#Design[edit])
- [39] Air Force, "Scan Eagle," Accessed Jul. 15, 2022 [Online]. Available: <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104532/scan-eagle/>
- [40] Boeing, "Scan Eagle," Accessed Jul. 15, 2022 [Online]. Available: <https://www.boeing.com/defense/autonomous-systems/scaneagle/index.page>
- [41] Naval Technology, "ScanEagle – Mini-UAV (Unmanned Aerial Vehicle)," Accessed Aug. 02, 2022 [Online]. Available: <https://www.naval-technology.com/projects/scaneagle-uav/>
- [42] Insitu, "EO950 Mult-Feed Turret," Accessed Aug. 02, 2022 [Online]. Available: https://www.insitu.com/wp-content/uploads/2020/12/EO950_ProductCard_DU120420.pdf
- [43] Northrop Grumman, "Fire Scout," Accessed Jul. 15, 2022 [Online]. Available: <https://www.northropgrumman.com/what-we-do/air/fire-scout/>
- [44] FLIR Systems, "BRITE Star II," Accessed Aug. 02 2022 [Online]. Available: http://www.edesgroup.com/files/FlirAir_-_BRITESTar_II.pdf
- [45] Navy, "MQ-8B Fire Scout," Accessed Jul. 15, 2022 [Online]. Available: <https://www.navair.navy.mil/product/mq-8b/>
- [46] G. Morrison, "From 4K to UHD to 1080p: What you should know about TV resolutions," *CNET*, Jan. 25, 2022 [Online]. Available: <https://www.cnet.com/tech/home-entertainment/from-4k-to-uhd-to-1080p-what-you-should-know-about-tv-resolutions/>
- [47] Amarisoft, "Amarisoft Callbox Classic," Accessed Jul. 17, 2022 [Online]. Available: <https://www.amarisoft.com/app/uploads/2021/10/AMARI-Callbox-Classic.pdf>
- [48] *PCI Express SDR Board*, Amarisoft, 2022-03-19, pp. 1–16.
- [49] Raspberry Pi, "Raspberry Pi 4," Accessed Jul. 17, 2022 [Online]. Available: <https://datasheets.raspberrypi.com/rpi4/raspberry-pi-4-product-brief.pdf>

- [50] Raspberry Pi, “Raspberry Pi 4,” Accessed Jul. 17, 2022 [Online]. Available: <https://www.raspberrypi.com/products/raspberry-pi-4-model-b/>
- [51] Raspberry Pi, “Raspberry Pi Camera Module 2 NoIR,” Accessed Jul. 21, 2022 [Online]. Available: <https://www.raspberrypi.com/products/pi-noir-camera-v2/>
- [52] Raspberry Pi, “Introducing the Raspberry Pi Cameras,” Accessed Jul. 21, 2022 [Online]. Available: <https://www.raspberrypi.com/documentation/accessories/camera.html>
- [53] Waveshare, “SIM8200EA-M2 5G HAT for Raspberry Pi, 5G/4G/3G Support, Snapdragon X55, Multi Mode Multi Band,” Accessed Jul. 21, 2022 [Online]. Available: <https://www.waveshare.com/sim8200ea-m2-5g-hat.htm>
- [54] IMEI Info, “Google Pixel 4A 5G Specs,” Accessed Jul. 22, 2022 [Online]. Available: <https://www.imei.info/phonedatabase/google-pixel-4a-5g/>
- [55] Qualcomm, “Snapdragon 730G Mobile Platform,” Accessed Jul. 22, 2022 [Online]. Available: <https://www.qualcomm.com/products/application/smartphones/snapdragon-7-series-mobile-platforms/snapdragon-730g-mobile-platform>
- [56] IMEI Info, “Google Pixel 3A XL Specs,” Accessed Jul. 22, 2022 [Online]. Available: <https://www.imei.info/phonedatabase/google-pixel-3a-xl/#basic>
- [57] Qualcomm, “Snapdragon 670 Mobile Platform,” Accessed Jul. 22, 2022 [Online]. Available: <https://www.qualcomm.com/products/application/smartphones/snapdragon-6-series-mobile-platforms/snapdragon-670-mobile-platform>
- [58] IMEI Info, “OnePlus 6 Specs,” Accessed Jul. 22, 2022 [Online]. Available: <https://www.imei.info/phonedatabase/oneplus-6/>
- [59] Qualcomm, “Snapdragon 845 Mobile Platform,” Accessed Jul. 22, 2022 [Online]. Available: <https://www.qualcomm.com/products/application/smartphones/snapdragon-8-series-mobile-platforms/snapdragon-845-mobile-platform>
- [60] TechPlayOn, “5G NR-ARFCN Calculation,” Tech On Play, Jul. 3 2018 [Online]. Available: <https://www.techplayon.com/5g-absolute-radio-frequency-channel-number-nr-arfcn/>
- [61] Electronics Notes, “Radio Link Budget: details & formula,” Accessed Jul. 31, 2022 [Online]. Available: <https://www.electronics-notes.com/articles/antennas-propagation/propagation-overview/radio-link-budget-formula-calculator.php>
- [62] Electronics Notes, “Free Space Path Loss: details & calculator,” Accessed Jul. 31, 2022 [Online]. Available: <https://www.electronics-notes.com/articles/antennas-propagation/propagation-overview/free-space-path-loss.php>

- [63] M2MSupport, “AT+CSQ Command,” Accessed Aug. 02, 2022 [Online]. Available: <https://m2msupport.net/m2msupport/atcsq-signal-quality/>
- [64] C. de Looper and M. Jansen, “Is 5G as fast as they’re saying? We break down the speeds,” Accessed Aug. 19, 2022 [Online]. Available: <https://www.digitaltrends.com/mobile/how-fast-is-5g/>
- [65] Tom’s Guide Staff, “5G speed: 5G vs. 4G performance compared,” Tom’s Guide, Jun. 01, 2021 [Online]. Available: <https://www.tomsguide.com/features/5g-vs-4g>
- [66] Waveshare, “SIM8202G-M2-5G-HAT-Assembly-en.jpg,” Accessed Jul. 22, 2022 [Online]. Available: <https://www.waveshare.com/wiki/File:SIM8202G-M2-5G-HAT-Assembly-en.jpg>
- [67] Raspberry Pi, “Introducing the Raspberry Pi Cameras,” Accessed Jul. 22, 2022 [Online]. Available: <https://www.raspberrypi.com/documentation/accessories/camera.html#installing-a-raspberry-pi-camera>
- [68] Waveshare, “SIM8200EA-M2 5G HAT,” Accessed Jul. 22, 2022 [Online]. Available: https://www.waveshare.com/wiki/SIM8200EA-M2_5G_HAT#Assembly_drawing
- [69] Waveshare, “SIM820X RNDIS Dial-Up,” Accessed Jul. 22, 2022 [Online]. Available: https://www.waveshare.com/wiki/SIM820X_RNDIS_Dial-Up
- [70] Raspberry Pi, “Infrared Bird Box,” Accessed Jul. 31, 2022 [Online]. Available: <https://projects.raspberrypi.org/en/projects/infrared-bird-box/10>
- [71] iPerf, “What is iPerf / iPerf3 ?” Accessed Jul. 29, 2022 [Online]. Available: <https://iperf.fr/>

Initial Distribution List

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California