2021-06

IMPLICATIONS FOR LOCATION PRIVACY IN 5G

Foster, Kayla R.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPLICATIONS FOR LOCATION PRIVACY IN 5G

by

Kayla R. Foster

June 2021

Thesis Advisor:	John D. Roth
Second Reader:	Murali Tummala

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

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

4. TITLE AND SUBTITLE
IMPLICATIONS FOR LOCATION PRIVACY IN 5G

5. FUNDING NUMBERS

6. AUTHOR(S) Kayla R. Foster

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)

As cellular technology continues to advance, Fifth Generation (5G) delivers a network capacity and speed to mobile devices unmatched by its predecessors. This heterogeneous network has improved efficiency that connects multiple platforms to create a new experience for its users. The new improvements introduced by 5G also include the increased bands into mmWave and beamforming capabilities that significantly improve the efficiency of 5G. With these improvements, location-based services are more accurate, but also lead to increased vulnerabilities. Location-based attacks via the uplink timing management commands have been studied in previous networks and are susceptible in 5G due to the nearly unchanged timing management structure and increased location accuracy. This thesis comprehensively analyzes cellular positioning, which leverages the 5G timing advance and beamforming for the end user's location. We evaluated the efficiency of varying remote radio heads in an environment to find the most precise location error with the new addition of beamforming. Additionally, we demonstrate how architectural density affects the position estimate in the 5G environment.

14. SUBJECT TERMS	15. NUMBER OF PAGES
beamforming, location-based services, location privacy, 5G	67
	16. PRICE CODE

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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

IMPLICATIONS FOR LOCATION PRIVACY IN 5G

Kayla R. Foster
Lieutenant, United States Navy
BS, Tennessee Wesleyan College, 2011

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ENGINEERING SCIENCE
(ELECTRICAL ENGINEERING)

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: John D. Roth
Advisor

Murali Tummala
Second Reader

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As cellular technology continues to advance, Fifth Generation (5G) delivers a network capacity and speed to mobile devices unmatched by its predecessors. This heterogeneous network has improved efficiency that connects multiple platforms to create a new experience for its users. The new improvements introduced by 5G also include the increased bands into mmWave and beamforming capabilities that significantly improve the efficiency of 5G. With these improvements, location-based services are more accurate, but also lead to increased vulnerabilities. Location-based attacks via the uplink timing management commands have been studied in previous networks and are susceptible in 5G due to the nearly unchanged timing management structure and increased location accuracy. This thesis comprehensively analyzes cellular positioning, which leverages the 5G timing advance and beamforming for the end user's location. We evaluated the efficiency of varying remote radio heads in an environment to find the most precise location error with the new addition of beamforming. Additionally, we demonstrate how architectural density affects the position estimate in the 5G environment.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

2G	Second Generation
3G	Third Generation
3GPP	3rd Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
AAS	Advanced Antenna Systems
AI	Artificial Intelligence
AoA	Angle of Arrival
AR	Augmented Reality
BBU	Baseband Unit
BS	base station
C-RAN	Cloud-Radio Access Network
CEP	circular error probable
CPRI	Common Public Radio Interface
D2D	Device to Device
DoD	Department of Defense
E-911	Enhanced 911
eCPRI	Enhanced Common Public Radio Interface
FCC	Federal Communication Commission

FDD Frequency Division Duplex

FR1 Frequency Range 1

FR2 Frequency Range 2

IoS Internet of Skills

IoT Internet of Things

ISI intersymbol interference

LBS Location-Based Services

LTE Long-Term Evolution

M2M Machine To Machine

MAC medium access control

MBB Mobile Broadband

MIMO Multiple Input, Multiple Output

MLE Maximum Likelihood Estimate

mmWave Millimeter wave

MSE mean square error

MTC Machine Type Communications

MU-MIMO Multiple User MIMO

NLLS Non-Linear Least Squares

NR New Radio

OFDM Orthogonal Frequency-Division Multiplexing

OFDMA Orthogonal Frequency-Division Multiple Access

OSI Open Systems Interconnection

PLS	Physical Layer Split
RAN	Radio Access Network
RF	radio frequency
RRH	Remote Radio Head
RSS	Received Signal Strength
SCS	Sub-Carrier Spacing
SINR	Signal to Interference+Noise Ratio
SIR	signal to interference
SNR	signal to noise ratio
SU-MIMO	Single User MIMO
TA	Timing Advance
TAG	Timing Advance Group
TDD	Time-Division Duplex
ToA	Time of Arrival
UE	User Equipment
URLLC	Ultra-Reliable Low Latency
V2X	Vehicle to Everything
VoIP	Voice over Internet Protocol
VR	Virtual Reality

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

First and foremost, I would like to give all my glory to God, who continues to bless me with power, love, and self-discipline.

I would also like to thank my family for their support through this process. I truly could not have done this without your love and encouragement.

Finally, I would like to thank my advisor, Dr. John Roth. Thank you for being gracious with your time and encouragement. Your teaching methods have helped me recognize my abilities and have allowed me to trust myself and the process. Thank you for your support and for instilling a greater knowledge and passion in this field.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

1.1 Motivation

Since its beginning in the mid-1990s, cellular technology has adapted and grown with each generation of cellular networks' increased goals to push the limits of cellular capability. The goal of large-scale circuit switched networks was used in Second Generation (2G) but evolved as data on wireless devices were added to the circuit-switched networks in Third Generation (3G). With higher data rates needed, Fourth Generation (4G) moved to packet-switched networks and incorporated newer technologies, such as Internet of Things (IoT) and Vehicle to Everything (V2X). In the era of Fifth Generation (5G), higher bandwidth and efficiency, higher data rates, and massive IoT have driven this 5G New Radio (NR) to push limits that reach beyond the initial start of the IoT and V2X [1]. 5G is pushing the limits of Internet of Skills (IoS), Virtual Reality (VR), Augmented Reality (AR), and Artificial Intelligence (AI).

The idea of privacy is at the forefront of every individual's mind but seems to lose its stamina when paired with the convenience of life applications. With the increase and advancement of technology, debates over digital privacy are becoming even more important as private life is more transparent than before. Location-Based Services (LBS) are utilized so frequently that they have become ubiquitous in our everyday lives. Services such as ride-share, food delivery, maps, emergency calls, and various other cell phone applications continuously calculate one's location to provide the user with a better service. The IoT also uses LBS to run its applications to serve the user better. With 5G, LBS are used in the Federal Communication Commission (FCC)'s Enhanced 911 (E-911), the health industry, autonomous driving, and other trafficking control systems [1].

The evolution of 5G creates an environment enriched with large amounts of cellular capabilities with known and unknown vulnerabilities. It is projected that by 2023 over 70 percent of the global population will have mobile connectivity, 29.3 billion networked devices, and over 10 percent of those networked devices (roughly 1.4 billion) will be 5G devices [2].

Technology can be viewed in many ways but often breaks down into two schools of thought. First, the benefits of the LBSs mentioned above outweigh the loss of privacy. The other side sees that this loss of privacy and the dangers that the evolving technology brings without proper protections are creating vulnerabilities that will not be reversed. Location privacy is vulnerable to leaks in the 5G network by access point algorithms [3] and also shows vulnerabilities in its unencrypted timing management signaling that can exploit the location of the target User Equipment (UE) [4]. The 5G network also introduces Sub-Carrier Spacing (SCS), known as "numerologies", that support a range of deployment scenarios. With the increase of capabilities in 5G, the Department of Defense (DoD) must utilize these capabilities while also ensuring that those systems are robust, protected, resilient, and reliable [5].

1.2 Objective

As mobile users go through their everyday routines, their mobile devices actively connect to a numerous amount of base stations. While this daily routine happens, we may not fully consider the concept of location privacy. New concepts are implemented to provide the services that are in demand as 5G continues its set up throughout the United States. These services are created to encompass high data rates, low latency, and other additions to allow the user to get the best network services to date. Although these services are engineered to be the best network option, those creating these services and the mobile users who utilize the network must be cognizant of our location privacy and approach this issue in an ethical and measured way. What are the new changes that affect our location privacy? The 5G network made changes to the base waveform, the directionality associated with base stations, and their communications that boost signal to noise ratio (SNR) to create a more robust and more reliable network. However, there are also consequences to these changes with location privacy. This thesis takes a geometric view of this phenomenon and quantifies the discoveries for location privacy in 5G. With this, we aim to form better decisions about our privacy as we move into this new era.

1.3 Approach and Chapter Breakdown

Chapter 2 will first look at the unique differences between 4G Long-Term Evolution (LTE) and 5G. It will also include discussions on LBS, the technical evolution of 5G, the newly

implemented beamforming, and the architectural density in the 5G environment. Chapter 3 will look at questions that this thesis is based on and the methodology approach taken for the 5G simulation. The final results of the simulations and answers to the posed questions from Chapter 3 will be discussed in Chapter 4. Chapter 5 will consist of the final thoughts, limitations, and recommendations for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Background

2.1 Changes to Location-based Services in 5G

The changes in 5G technology have included the promise of higher bandwidths, large capacities, and low latencies. Positioning services, architecture, emergency calling, and 3rd Generation Partnership Project (3GPP) positioning requirements are directly affected by the move to 5G. In this section, we will discuss how positioning is used in LBS and multilateration techniques used to compute the position estimate of an end user.

2.1.1 Positioning and LBS

Devices are exposed with location data, even when powering on. Our devices trust the network as it connects, and our real-time location information is provided to the cellular provider. Trust in the network creates vulnerabilities that could be exploited for various reasons [6]. Historically, positioning in cellular technology was utilized for emergency calls and services. The localization of UE started in 1996 as the FCC mandated standardized accuracy requirements for E-911 calls [7]. As the requirements continue to be revised, the accuracy requirements are becoming more precise with each iteration. 4G LTE built on the technology to expand on other uses such as navigation, maps, health and fitness, and fraud prevention. 4G LTE continued this trend with other commercial applications that would enhance the way people use mobile technology with the demand for faster, more accurate services. In doing so, LTE became the forefront of positioning technology [1]. The results of these requirements have numerous effects on the use of users' location data.

2.1.2 Trilateration

The five fundamental positioning techniques utilizing radio signals as identified by Rosado et al. [8] are trilateration, triangulation, proximity, scene-analysis, and hybrid. This thesis will focus on trilateration, or more generally known as *multilateration*, and *multiangulation*. Multiangulation is the approach used that is based on the angle measurements [9]. The process of multilateration is the intersection of geometric constructs based on measurements

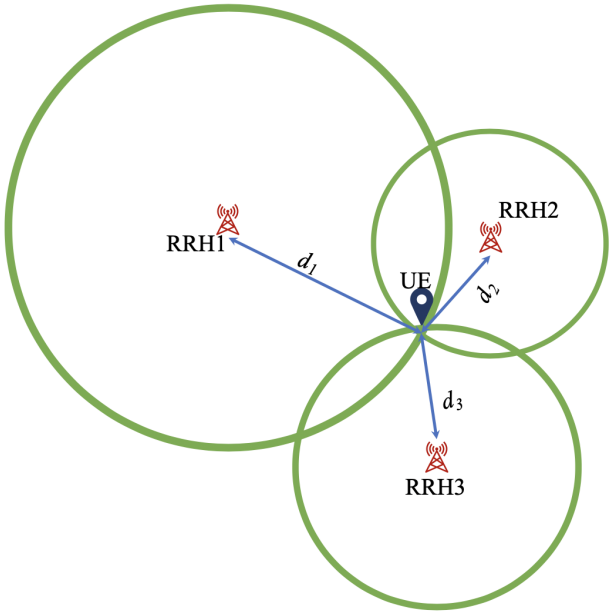

Figure 2.1. Example of trilateration in a wireless network. Source: [11].

that are calculated between the UE and the reference transmitter/receiver, such as Time of Arrival (ToA), Received Signal Strength (RSS), Angle of Arrival (AoA), etc. to find its position solution. Figure 2.1 is an illustration that shows this method. Research continues to be conducted on the network and mobile-based trilateration techniques to meet regulatory requirements [10].

2.2 Technical Evolution from 4G to 5G

As mobile users move from one location to the next, their connection to the network is not interrupted as they move away from a cell tower to which they are connected. The development of 4G gave users seamless transition services and the ability to use their mobile equipment in various ways no matter their position or time. To create this seamless transition, 4G would no longer use circuit-switch capabilities but would instead transition to Voice over Internet Protocol (VoIP) [12]. It was years later when LTE evolved its compatibility to work in areas without coverage through Device to Device (D2D) and Machine To Machine (M2M) communications that changed the way cellular technology would be used [13]. 5G altered its architecture and spectrum to allow for the change in technology but made slight changes in

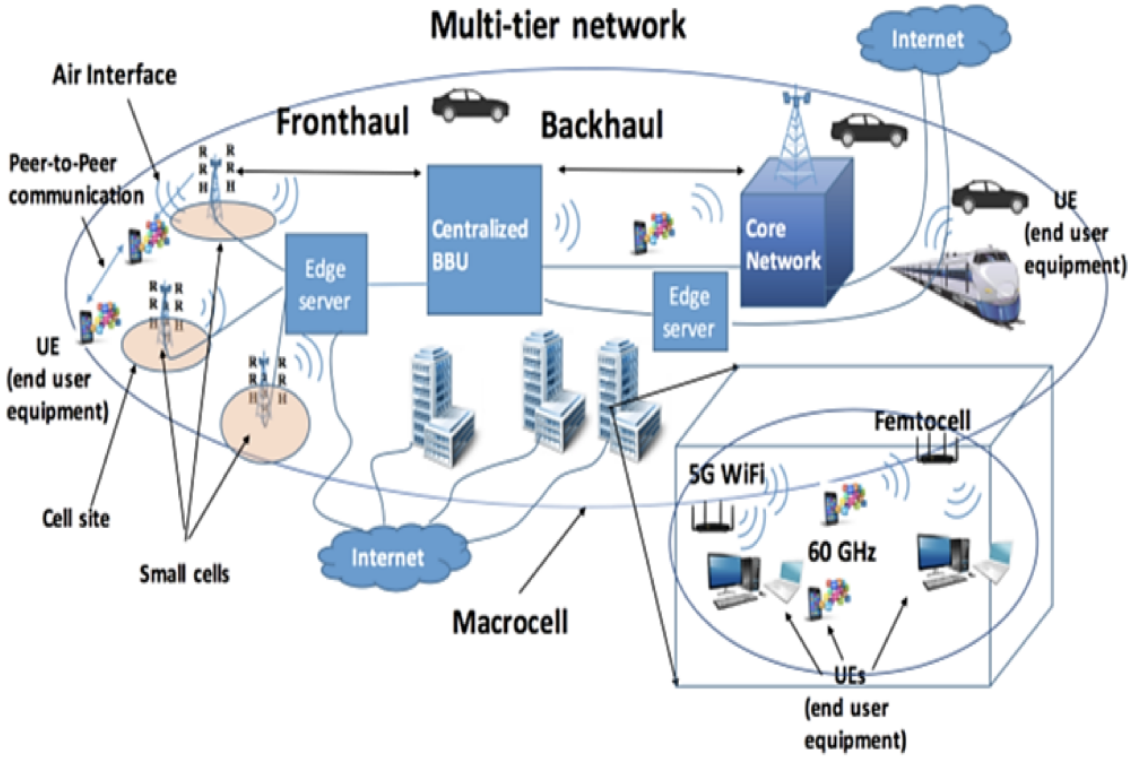

Figure 2.2. 5G Multi-tier Network. Source: [14].

its timing management. These concepts will be discussed more in the following subsections. Figure 2.2 [14] shows an example of a multi-tier 5G network which shows the complexity of the macro and small cells, Remote Radio Head (RRH)s, Baseband Unit (BBU)s, UEs, and a core network. A fronthaul/backhaul connection is visible in Figure 2.2, which will be discussed in Section 2.2.1. We will first look at the changes in the 5G architecture to better understand how the network is connected.

2.2.1 Architecture

The 5G network strives to improve upon the 4G LTE architecture to allow for services that push the limits of reliability. The 5G architecture takes on 4G LTE primary services of Mobile Broadband (MBB) and Machine Type Communications (MTC) but is also including the service of Ultra-Reliable Low Latency (URLLC) [15]. The use of URLLC creates

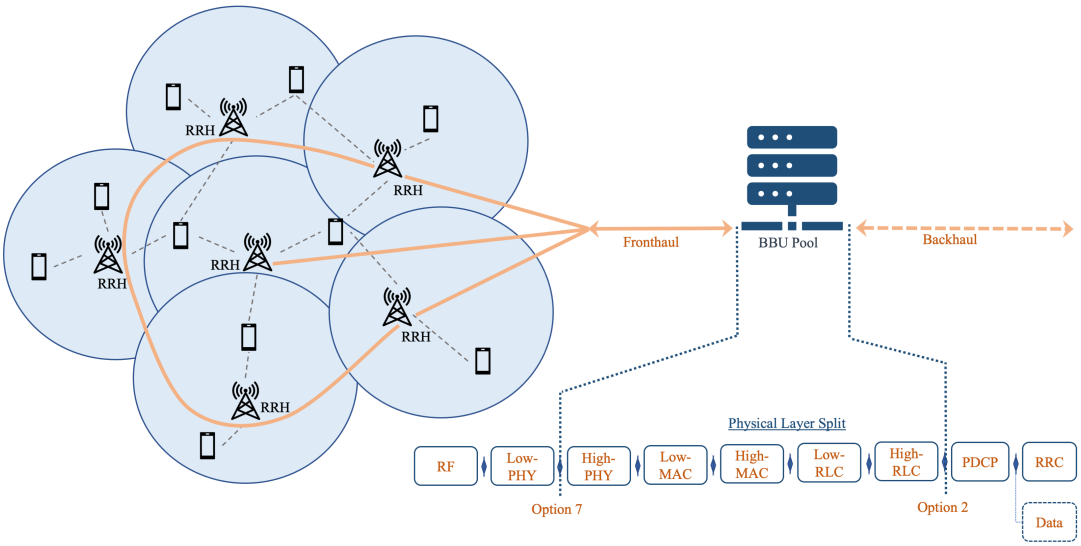

Figure 2.3. Example of C-RAN Architecture with physical layer splits identified. Source: [11].

high reliability with low latency for V2X, remote surgery, video surveillance, medical and health services, and other safety-critical applications [1]. The Cloud-Radio Access Network (C-RAN) architecture was created from the previous 4G LTE network architecture and protocols, Radio Access Network (RAN), which is implemented in 5G. The architecture was created to allow as many base station (BS)s that the network needs by way of virtualization [16]. The C-RAN design differs in two primary categories: physical restructuring of the network and interface updates.

As depicted in Figure 2.3, the physical restructuring of the network comprised of a grouping of centrally located BBUs, better known as "BBU pools," and their affiliated RRHs. In the traditional LTE network, the BBUs and RRHs are conjoined as the BS. In 5G, each BBU is located in its serving geographic region and is connected to various RRHs that are distributed near the UEs. This connection between the BBUs and RRHs is called a fronthaul network. There are many physical layer proposals to connect the BBU pools to the RRHs [17].

It was essential to create an interface update to implement key metrics in 5G. Many LTE

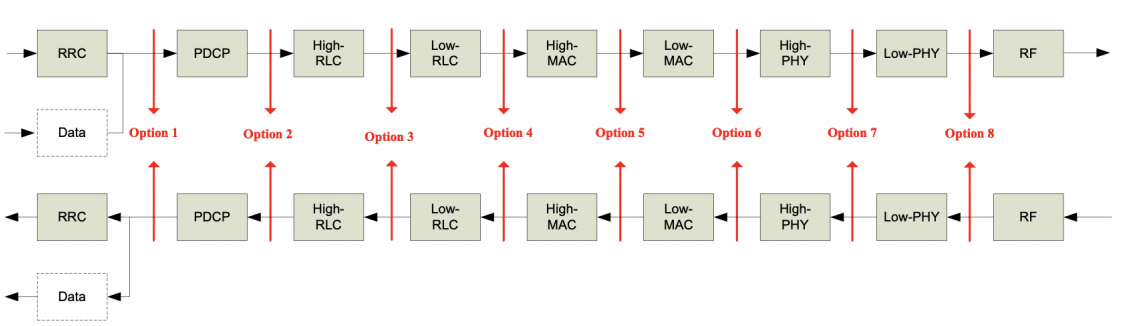

Figure 2.4. Physical Layer Split. Source: [19].

connections utilized the Common Public Radio Interface (CPRI) protocol but with 5G are evolving to Enhanced Common Public Radio Interface (eCPRI). The LTE split fronthaul was intended to be for one use case and proves to be too restrictive for connections that must be flexible. The proposed eCPRI will desegregate the network, allowing high levels of virtualization, and use packet-based synchronization. This will allow 5G to support various needs of users on the same network, at the same time [18]. The 5G fronthaul architecture has eight functional deployment options, which vary on benefits and possible drawbacks when depicting latency, complexity, and capacity. As seen in Figure 2.4, the options are defined at the points between the Physical, Data, and Network layers found in the Open Systems Interconnection (OSI) model. Option 8 is depicted as the current CPRI configuration where the high-level split is found between the low Physical layer of the BBU and the RRH [20]. The Physical Layer Split (PLS) architecture presented by 3GPP gives the network engineers options for how they want to set out responsibilities between the BBU and RRH. In this option, the BBU maintains all radio link control and media access control layer functions. It also maintains the lower physical layer functions, such as modulation and fast Fourier transforms, which are delegated to the RRH [21]. The BBU will be conducting most of the digital baseband radio functions, as the RRH carries out mostly analog radio frequency tasks. This will allow for the most cost-effective spatial separation that is desired [17]. The BBU supports a large number of RRHs and variables that are needed to be optimized, such as beamforming vectors, in a dense C-RAN. The BBU computes beamforming-vectors that are compressed for each RRH [22].

This section has emphasized how the new 5G architecture has allowed for a more reliable

network with low latency with its physical restructuring. Next, we will discuss how the changes to the base waveform and the increased spectrum provide a more improved network.

2.2.2 Spectrum

The 5G network increased the use of the spectrum and implemented changes to the base waveform to increase spectrum efficiency and reduce intersymbol interference (ISI) for mobile users. In 5G, the use of the spectrum in cellular technology allows for an increase of capacity and decreased congestion. LTE was one of the first designs to show spectrum flexibility with the ability to have a joint Frequency Division Duplex (FDD)/Time-Division Duplex (TDD) and multi bandwidth support. This allowed LTE to utilize carrier aggregation and have access to unlicensed spectra to adhere to higher bandwidths and fragmented spectra. LTE supports licensed spectra at 3.5 GHz and unlicensed at 5 GHz. 5G significantly expanded the frequency range with its radio-access technology in its support to the licensed spectrum by dividing the spectrum into two ranges. Frequency Range 1 (FR1) includes bands from below 6 GHz, and Frequency Range 2 (FR2) includes bands from 24.25 GHz up to 52.6 GHz [13].

Millimeter wave (mmWave) uses the radio frequency (RF) spectrum from approximately 30 to 300 GHz. 5G is able to operate at mmWave frequencies which allows for high traffic and extreme data rates due to the large amounts of the spectrum use and wide transmission bandwidths. The ability for 5G to operate in these ranges are needed due to the large quantities of the spectrum that are available at high-frequency ranges. Another reason for 5G to operate in this spectrum are for the spatial degrees of freedom that are used with high-dimensional antenna arrays, which are possible due to the smaller size of antenna elements at these higher frequencies [23]. Using mmWave frequencies creates limitations because of poor isotropic propagation and shadowing at the higher frequencies. However, by using directional antennas that have high gain, overcoming these limitations is possible [23]. Section 2.3 will further discuss how beamforming in 5G is an effort to neutralize these limitations.

Modulation schemes in 5G will mirror those in LTE, which utilizes Orthogonal Frequency-Division Multiplexing (OFDM) and Orthogonal Frequency-Division Multiple Access (OFDMA). A visual representation of the time and frequency domain view of OFDM can

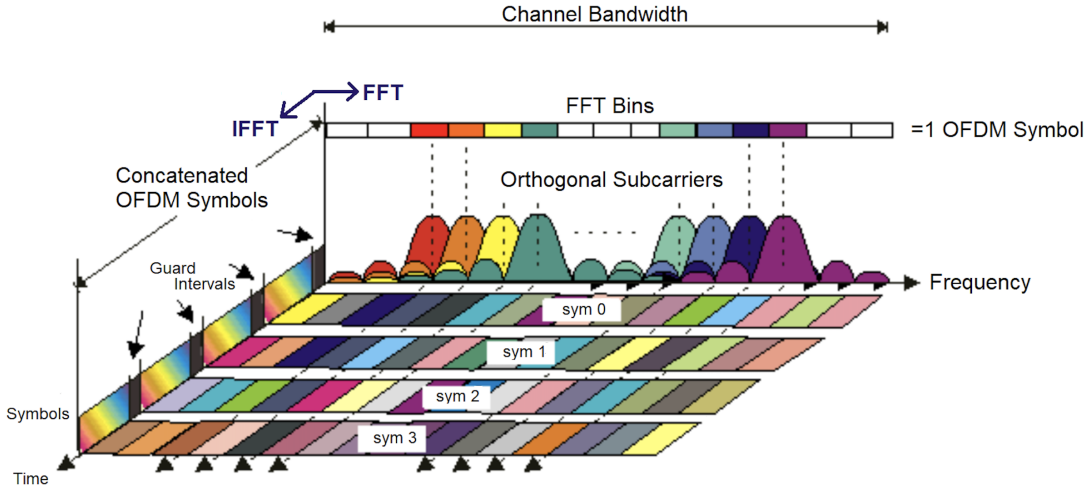

Figure 2.5. Frequency and Time of OFDM. Source: [26].

be seen in Figure 2.5. 5G NR's highly flexible spectrum establishes multiple numerologies μ, defined by the specific SCS [24]. The SCSs are evaluated as

$$\Delta f_{SCS} = 15 \times 2^{\mu} \text{ kHz for } \mu \in [0, 4], \tag{2.1}$$

and allows for a novel SCS range of 15 (standard LTE) to 240 kHz. Generally, higher SCS is used for shorter transmission time intervals required for mmWave while lower SCS is optimal for higher throughput performance [25]. Increasing this flexibility of SCS allows for more efficient use of the available spectrum.

2.2.3 Timing Management

Timing management in the OFDMA construct is vital to creating a successful network operation. It is necessary in cellular systems to ensure that the transmissions from the UEs are synchronized when received by the RRH. It is a requirement by OFDMA that the uplink frames arrive at the cell towers that a specific user is scheduled. Without this requirement, the uplink frames are susceptible to inter-symbol interference, which would degrade the wireless link [27]. Cellular networks must incorporate propagation delay into its scheduling in order to prevent inter-symbol interference, since that delay between the user and the RRH

will not be constant. To do this, a Timing Advance (TA) parameter is used as a control element in the medium access control (MAC) layer to modify the users uplink burst timing to allow for adjustments in the propagation delay [27]. Like LTE, the 5G TA command is made up of two prominent parts, the timing advance value N_{TA} and the Timing Advance Group (TAG) [28]. The TA command must ensure that a UE is able to move within a serviceable environment as its transmissions arrive at the RRH in its given time slot. The propagation time for its transmissions will change as the UE moves, significantly at times, requiring some synchronization method.

TAG, a 2-bit field, allows for a unique association of the TA command to a particular RRH to specifically account for communication with multiple RRHs. This is done through carrier aggregation [13] and the high unlikelihood that they are equal distance from the UE. N_{TA} has an associated fixed time value due to the unchanging basic time in LTE, T_s, detailed in

$$T_s = \frac{1}{\Delta f_{ref} \times N_{f,ref}} = \frac{1}{15 \times 10^3 \times 2048} \approx 32.6 \text{ nsec}, \tag{2.2}$$

where Δf_{ref} is the LTE SCS and $N_{f,ref}$ the maximum number of subcarriers. The TA values are represented as integers and account for 16 sample time units such that

$$N_{TA} = 16T_s. \tag{2.3}$$

Equations (2.2) and (2.3) are used to calculate the one-way distance resolution as shown

$$r = \frac{cN_{TA}}{2} = 78.125 \text{ meters}. \tag{2.4}$$

To employ the NR numerologies, the new base unit of time is employed in [29]

$$T_c = \frac{1}{\Delta f_{max} \times N_f} = \frac{1}{480 \times 10^3 \times 4096} \approx .51 \text{ nsec}, \tag{2.5}$$

where Δf_{max} is the maximum SCS and N_f the maximum number of subcarriers. The

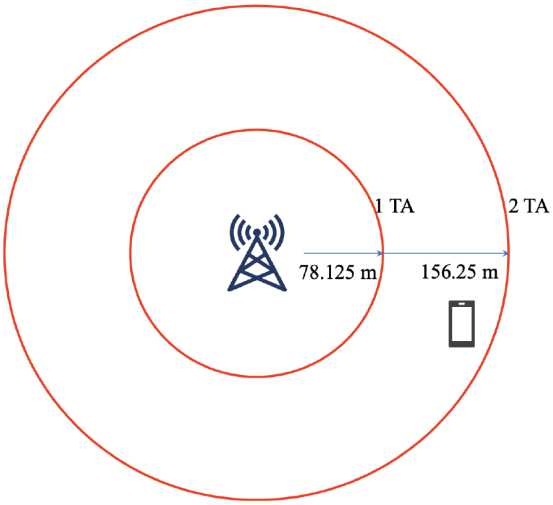

Figure 2.6. Visual representation of a TA command with TA = 2 and the associated distances with $\mu = 0$. Source: [11].

relationship between T_c and T_s previously stated in [24], which introduces κ defined as

$$\kappa = \frac{T_s}{T_c} = 64. \tag{2.6}$$

The basic slot time in 5G is redefined as

$$T_s = \frac{1}{\Delta f_{ref} \times N_{f,ref}} = \frac{1}{15 \times 10^3 \times 2^{\mu} \times 2048}, \tag{2.7}$$

where Δf_{ref} is the standard LTE SCS. It is then multiplied by 2^{μ} for various numerologies while $N_{f,ref}$ is the same as (2.2). N_TA is now defined as

$$N_{TA} = \frac{16\kappa T_c}{2^{\mu}}. \tag{2.8}$$

Based on equation (2.6), T_c is nullified which leaves

$$N_{TA} = \frac{16T_s}{2^{\mu}}. \tag{2.9}$$

Thus, using the equations (2.4) and (2.9), the distance resolutions are now calculated as

$$r = \frac{cN_{TA}}{2} = \frac{78.125}{2^{\mu}} \text{ meters}, \tag{2.10}$$

which directly shows the dependence of 5G TA distance resolutions on the associated numerology. Table 2.1 summarizes these new resolutions and Figure 2.6 exhibits a visual understanding of the TA.

Table 2.1. 5G NR Numerology Distance Resolutions. Adapted from [30] and [31].

μ	**Distance Resolution (m)**	**Subcarrier Spacing (kHz)**	**OFDM Symbol Duration (μ)**	**Slot Duration (ms)**
0	78.125	15	66.67	1
1	39.06	30	33.33	0.5
2	19.53	60	16.67	0.25
3	9.77	120	8.33	0.125
4	4.88	240	4.17	0.0625

2.3 Beamforming in 5G

To improve on 4G LTE communication from the eNB to the user, 5G changed the directionality associated with each RRH by way of beamforming. Although beamforming is new to cellular technology starting in 5G, the concept of RF beams has been around for many years. Beamforming is the controlled interference of multiple waves to increase the strength of transmitted signals in a specific direction [32]. The beams are used to identified the best data-delivery route to the UE and that will also reduce interference [13]. This increase in spectrum efficiency is especially useful in mmWave technology [13]. As cellular signals are transmitted, signals can be blocked or weakened over long distances. While using beamforming techniques, the signal is sent in a concentrated direction to a specific user, which allows for the strengthening of a signal and allows for improved probability of interference.

There are multiple ways to deploy this technology in 5G depending on the equipment the user has available [33].

2.3.1 Motivation

5G NR utilizes multiple steerable antenna elements or arrays of radiators to capture or radiate energy in a specific direction over its aperture to transmit and receive data [34]. These antennas make it possible for mmWave devices to overcome propagation effects [23]. The higher-frequency bands are primarily used for beamforming for extended coverage, while the lower-frequency bands are used to enable massive Multiple Input, Multiple Output (MIMO) and interference avoidance [13]. All NR channels and signals have been designed for beamforming support. Analog beamforming is possible at high frequencies where the receiver and transmit beams can be one-directional at a given time [13]. Beam-sweeping is method that is utilized because the same signal is repeated in multiple OFDM symbols. Beam-sweeping ensures that any signal can be transmitted with a narrow beam and a high gain to reach the coverage area [13].

High propagation losses in FR2 create the need for improvement in the link budget and enable this frequency range for 5G cellular networks. 5G NR uses a large number of beams to cover legacy networks' spatial areas as seen in Figure 2.7. 5G uses multiple beams for transmitting and receiving signals in different directions allows for higher antenna gain than the previous LTE use of beamforming.

2.4 Massive MIMO

MIMO is the use of multiple transmitters and receivers on a device to increase performance. Massive MIMO extends beyond MIMO by adding a significant number of antennas on base stations. The added antennas focus more energy to increase throughput and efficiency for 5G [35].

2.4.1 Massive MIMO and Beamforming

A type of legacy beamforming design, known as Advanced Antenna Systems (AAS), uses static beamforming in the radio and is applicable in limited coverage networks. 5G networks

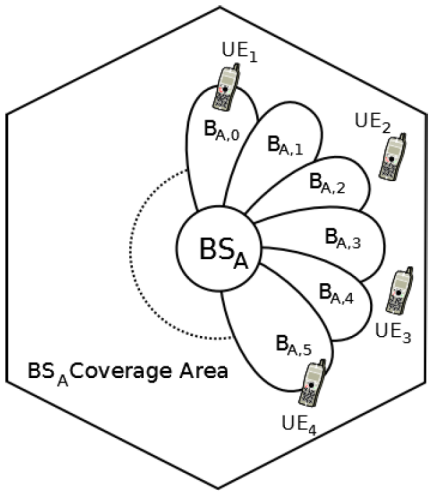

Figure 2.7. Beamforming Deployment. Source: [13].

utilize digital beamforming to obtain the maximum spectral efficiency improvements. Massive MIMO adds a spatial dimension to frequency and time dimensions to boost spectral efficiency. By adding spatial dimensions, the SNR is improved because of the array gain and orthogonality of multiple beams. This allows the frequency and time allocations to be reused by other users [36]. Figure 2.8 shows a comparison of AAS and massive MIMO.

2.4.2 Variations of MIMO

Spatial processing for 5G NR is based on beamforming, Single User MIMO (SU-MIMO), and Multiple User MIMO (MU-MIMO). Beamforming concentrates energy to the UE and reduces interference with other UEs. MIMO beamforming techniques compensate for high attenuation caused by theoretical free space path loss, which is governed by Friis' equation as discussed in [37] and [23]. Theoretical free space path loss is proportional to the square of the frequency and results in the magnitude of power received for a mmWave signal being over 30 dB less than the conventional cellular systems [37] [23]. The antenna size and spacing compacts to millimeters and then packs hundreds of elements onto cell base stations and handheld devices in mmWave. The smaller antennas allow for integrating multiple arrays onto the mobile devices to stay connected, even if the signal is blocked from one array [23]. SU-MIMO splits Signal to Interference+Noise Ratio (SINR) between multiple layers to the target UE to improve user throughput. MU-MIMO shares SINR between multiple data

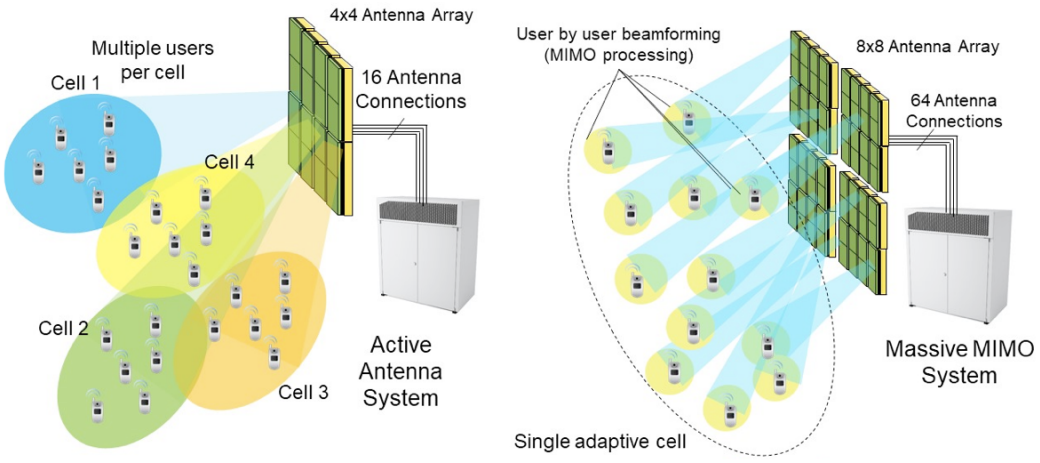

Figure 2.8. AAS vs massive MIMO. Source: [36].

layers to multiple UEs where each layer is separately beamformed to improve capacity and throughput for the user [38]. Figure 2.9 shows the spatial processing.

2.5 Base Station Density in 5G

Base station density is increasing as 5G continues to be established in the United States. To ensure that the network capacity increases in 5G, decreasing cell sizes have proven to be most effective. In shrinking the cells, spectrum reuse is utilized to allow a reduction in the number of users needing to compete for resources at their respective BS. Cells are able to shrink without sacrificing the signal to interference (SIR), proven in [39]. Because of this, every BS is able to use its resources and backhaul connection to a small number of users [40].

The shift to higher frequencies in 5G, namely mmWave that range from 24GHz to nearly 53 GHz, creates disadvantages, such as the frequencies can only be used at shorter distances and are susceptible to obstructions in its path. Significant obstructions that affect mmWave include buildings, trees, humidity, and rain [41]. Because of these obstructions for higher frequencies, the 5G network must utilize many more base stations than the previous LTE network.

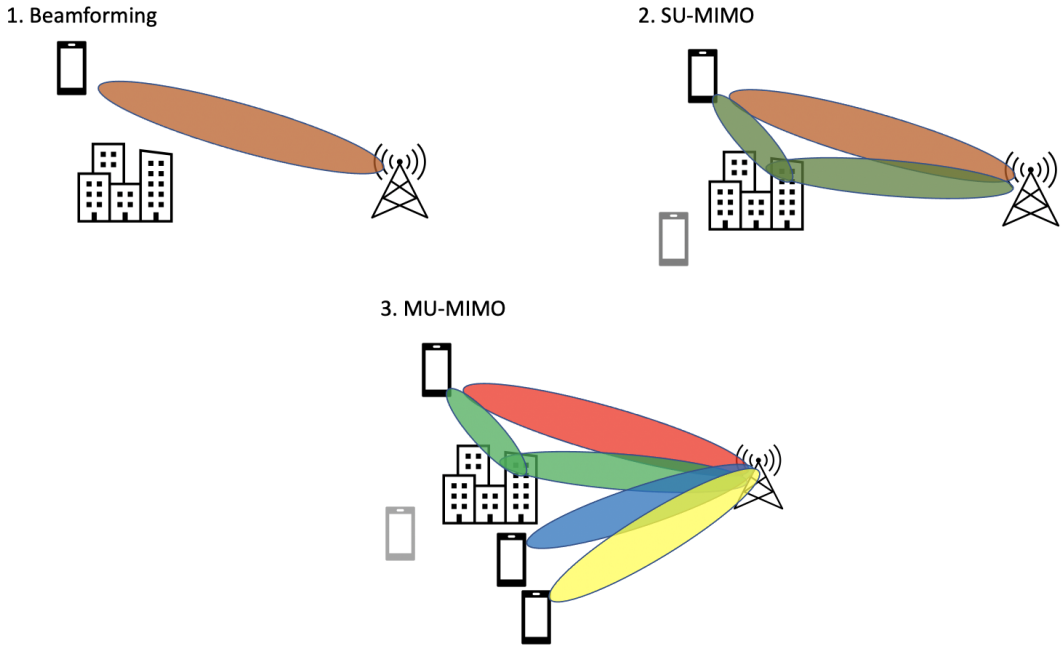

Figure 2.9. Beamforming and MIMO. Adapted from [38].

2.6 Summary

This chapter discussed the fundamental topics for 5G for comprehension of the simulation parameters, methods of testing, and the final results. We gave an overview of LBS and its advances in 5G that include positioning. We followed with a look at the technical changes that included the architecture, spectrum, and timing advance. We then reviewed beamforming followed by a deeper dive into massive MIMO. We ended this chapter with 5Gs base station density that will impact areas across the United States. In the next chapter, we will present the methodology processes that were derived from our guiding questions as presented in Chapter 3.

CHAPTER 3:
Methodology

In this chapter, we will describe the processes used to create our schemes based on the background information previously discussed in Chapter 2. We will further discuss our scheme, equations, and our methodology to evaluate questions presented about the 5G environment. Simulations that we created were based on finding accurate results to the following questions:

1. At what point do the number of servicing RRHs not provide a significant improvement in the positioning performance, both with and without beamforming?
2. How do results change per numerology used?
3. How does architectural density marginalize the benefit of a multilateration approach to a location estimate? To demonstrate this we show at what point, if ever, would the position estimate be more accurate by utilizing the closest servicing RRH in a 5G environment.

3.1 Position Estimates based on RRH and Numerology Simulation Without Beamforming

This scheme was partially set up in [11] and modified for this thesis. To answer the first question, we have to first use a range of RRHs that our UE will be communicating with and evaluate that data per numerology being used. The range of RRHs tested range from 3 to 11 with one UE located at (0,0). This range started at 3 RRHs, based on the trilateration techniques and ended at 11 RRH, which allowed a large range to observe the changes in our scheme. The RRHs were randomly placed throughout a 1,000,000 m^2 area. We then calculated the TA for each RRH to the UE. Each TA has associated rings of the uncertainty of equal distance, depending on the numerology used as seen previously in Table 2.1. The rings are used to find the possible location that the UE could be located. Non-Linear Least Squares (NLLS) was the method used to find the position estimate of the UE. After calculating the true distances from the RRH to the UE, Gaussian noise was added and formed our distance estimates, $\hat{d}_i$. The estimates were then quantized into the appropriate

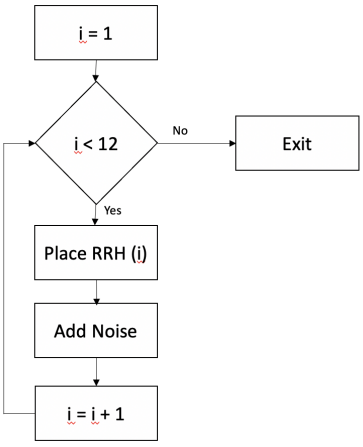

Figure 3.1. A basic example of populating RRHs in a 5G environment with the addition of noise.

TAs. This process can be seen in Figure 3.1, where i represents the number of RRHs in the 5G environment. The known range values for each TA were then used to calculate the target's position Maximum Likelihood Estimate (MLE), $\hat{\boldsymbol{p}}$, through the employment of the NLLS method presented in [42], and [43], and [11]. This involves the minimization of $\boldsymbol{x} = [x, y]^T$ in the following

$$\hat{\boldsymbol{p}} = \arg\min_{\boldsymbol{x}} \sum_{i=1}^{N} [d_i - \|\boldsymbol{x} - \boldsymbol{x_i}\|]^2 \tag{3.1}$$

where the position estimate is represented by $\hat{\boldsymbol{p}} = [\hat{x}, \hat{y}]^T$, d_i represents the distance from the center of the TA to each RRH, $\boldsymbol{x_i} = [x_i, y_i]^T$ represents the positions of each RRH, and i is an integer ranging from 1 to the total number of RRHs. The squared distance error solution from (3.1) is calculated by squaring the distance between $\hat{\boldsymbol{p}}$ and the true UE position $\boldsymbol{p}$.

3.2 Position Estimates with Beamforming

We now include beamforming to test the proposed scheme's positioning performance. Beamforming, based on AoA, is used in the geometric approach for angle-based positioning performance. The range and angle of this positioning system follows a geometric approach

for localization and uses measured distances or angles from one node (UE) to the anchor node (RRH) [44]. The distances based localization utilizes the lateration methods to find the approximate location of a certain node [44]. In a geometric localization system, an incident signal's AoA is represented by straight lines [44]. The intersection of lines from its respective anchor node represents the location of that UE.

In addition to the RRHs and novel 5G numerologies found in Section 3.1, zero mean Guassian noise was added before the calculations of the angles of arrival. This noise was implemented in the x and the y coordinates by adding Gaussian noise with standard deviation sigma to all coordinates in the RRHs. The standard deviation sigma was found by taking the distance resolutions found in Table 2.1 and dividing it by a fixed annulus previously found in [45].

The range of RRHs tested were again looked at in the range of 3 to 11 with the UE located at (0,0). The RRHs were randomly placed throughout a 1,000,000 m^2 area that was identical to the scheme without the beamforming. We then calculated the TA for each RRH to the UE. Each TA has associated rings of uncertainty of equal distance, depending on the numerology used. We again calculated the true distances from the RRH to the UE with the added Gaussian noise and formed our distance estimates, $\hat{d}_i$. The estimates were then calculated into the appropriate TAs. The known range values for each TA were then used to calculate the target's position MLE, $\hat{\hat{\boldsymbol{p}}}$, through the employment of the NLLS method presented in [42], and [43], and [11]. In addition to the previous NLLS, we utilized the AoA for estimating the position of the UE. Figure 3.2 shows the basic concept of calculating the AoA to (3.1) for the added calculation of beamforming. An overview of this model can be seen in Figure 3.3. Figure 3.4 shows a closer look at 3.3 and the beams being discussed.

We first accounted for the slope, m, of each line from the RRH to the position estimate of the UE. The perpendicular of the slope, $\hat{m}$, was found by using the negative reciprocal of m, $\hat{m}$. We then continued our calculations with the added beam. This involves the minimization of $\boldsymbol{x} = [x, y]^T$ in the following

$$\hat{\hat{\boldsymbol{p}}} = \arg\min_{\boldsymbol{x}} \sum_{i=1}^{N} ([d_i - \|\boldsymbol{x} - \boldsymbol{x_i}\|]^2 + (\epsilon_i)^2), \tag{3.2}$$

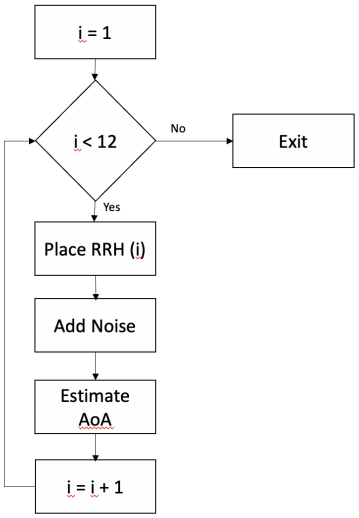

Figure 3.2. A basic example populating RRHs in 5G environment with the addition of noise and beamfoming.

where $\hat{\boldsymbol{p}} = [\hat{x}, \hat{y}]^T$, d_i represents the distance from each RRH to the center of its TA ring, $\boldsymbol{x_i} = [x_i, y_i]^T$ represents the positions of each RRH, and i is an integer ranging from 1 to the total number of RRHs. The squared distance error solution from (3.2) is calculated by squaring the distance between $\hat{\boldsymbol{p}}$, the true UE position $\boldsymbol{p}$, and the magnitude of the line segment perpendicular to the beam and that contains the beam and the point x as its endpoints, ϵ_i.

3.3 Architectural Density in the 5G Environment

The scheme in Section 3.1 was modified to examine the density of base stations placed within a city-like environment. To answer the last question posed in this thesis, we first had to use a range of RRHs that our UE will be communicating with and then observe the outcome of the data per numerology being used. The range of RRHs tested again ranged from 3 to 11 with one UE located at (0,0). This range started at 3 RRHs, which we found to be the most effective starting point for multilateration since any number of RRHs less than three will not have an unambiguous solution. Our range ended at 11 servicing RRHs since we found that the data does not show any significant change after this range. The location of the RRHs were uniformly random and placed throughout a 1,000,000 m^2 area.

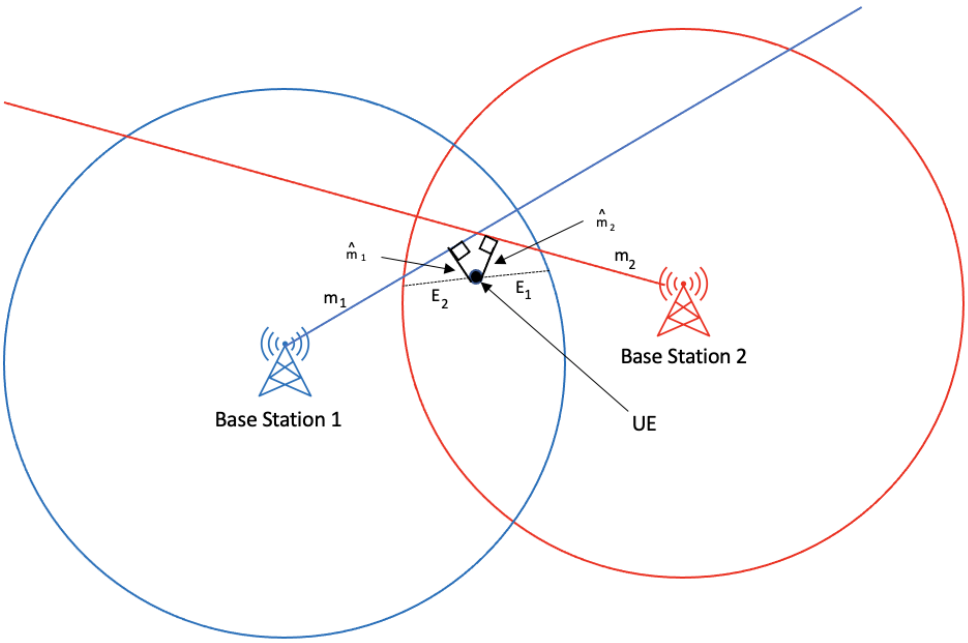

Figure 3.3. A basic example of two RRHs with beamforming to visualize the 5G location estimate. The beams are shown with the slopes represented by m_1 and m_2, starting from the RRHs to the estimated UE location.

In this approach, we varied the density of RRHs placed within our simulated area. We started with ten RRHs and tested up to 250 RRHs placed in the area. The large amount of RRHs was used to simulate a city-like location where an abundance of RRHs could be found, such as businesses, housing communities, and other various locations. We used this environment to compare two options. The first option would be for the UE to connect to the closest RRH. The second option would be for the UE to connect to the closest 3 to 11 RRHs, utilizing multilateration discussed in Chapter 2.

Following this, Equation (3.1) was used to find the position estimate of the UE. True distances from the RRH to the UE were again calculated, and Gaussian noise was added as used in the previous Equation (3.1) to form our estimated distance, $\hat{d}_i$. The estimates were again quantized into the appropriate TAs. The known range values for each TA were then used to calculate the target's position MLE, $\hat{\boldsymbol{p}}$, through the employment of the NLLS as seen in Section 3.1 and equation (3.1). We then find the MLE and the mean square error (MSE) of both options.

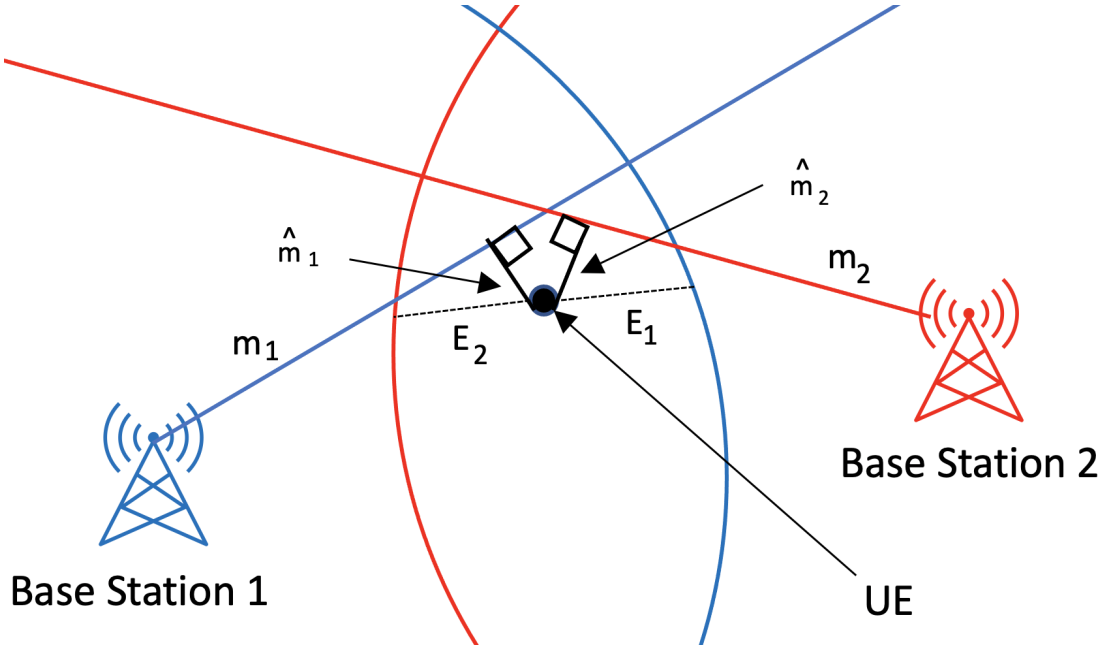

Figure 3.4. A basic example of two RRHs with beamforming to visualize the 5G location estimate. The beams are shown with the slopes represented by m_1 and m_2, starting from the RRHs to the estimated UE location.

3.4 Summary

In this chapter, we proposed three schemes to answer the guiding questions stated at the beginning of this chapter: at what point do the number of servicing RRHs not provide a significant improvement in the UEs positioning performance, how do results change per numerology used, how does architectural density marginalize the benefit of a multilateration approach to a location estimate, and at what point, if ever, would the position estimate be more accurate by utilizing the closest servicing RRH in a 5G environment? We will now move to our results found and the implications for 5G in Chapter 4.

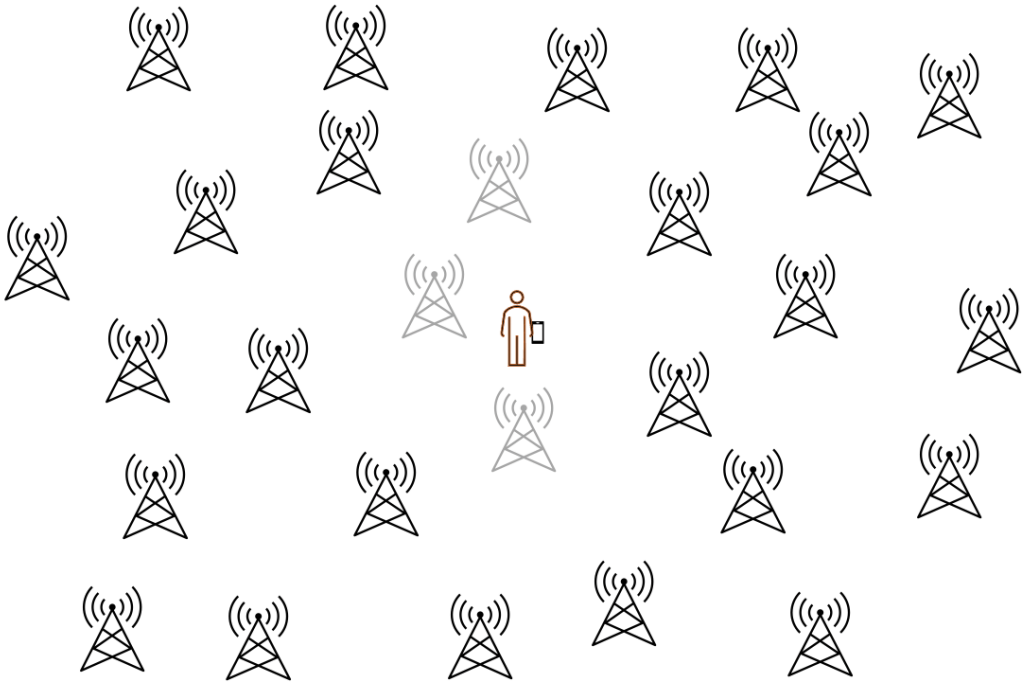

Figure 3.5. Image to depict cell tower density in 5G environment. The light colored antennas show the three nearest RRHs to the end user.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Results

This chapter describes the development and evaluation of the results found in the dense 5G environment created from the questions formulated in Chapter 3. We organized our results into two categories: the simulation of RRH and numerology, and the architectural density simulation. Each of these Monte Carlo simulations were calculated no less than 1,000 times.

4.1 Simulation of RRH and Numerology

We had anticipated that our simulations for the position accuracy would increase as the number of RRHs increased and as well as when the SCS became larger. As seen in Figures 4.1 and 4.2, our results showed that our expectations were correct. It is evident in the results showed that as the numerology increases, the MSE decreases per BS. Not only does the MSE become halved for each numerology when there are 3 RRHs, the MSE from 5G without a beam is nearly halved when a beam is added. As the number of RRHs increase, the margin of MSE between the data with and without beamforming decrease. Beamforming adds significant value to minimizing the location error when compared to simulations without beamforming when there are less than 6 servicing RRHs. In answering our first question, the position estimate difference in MSEs with and without beamforming per numerology became negligible at 9 RRHs for $\mu = 0$ and 1, at 8 RRHs for $\mu = 2$ and 3, and 7 RRHs when $\mu = 4$.

We then found the 90% and 95% circular error probable (CEP) for each RRH shown in Tables 4.1-4.3. The CEP creates a ring of precision around a target that relates the location distance error and confidence location error. A chosen percentage of location estimates are contained in the ring of precision (90% and 95% respectively). The radius of this circle is equal to the furthest location distance error among those contained points [11] [46]. As the numerology, μ, increases, the data shows that the location error decreases by nearly half for each RRH tested. Beamforming also significantly decreases the location error, especially when there are 3 to 5 RRHs. The most accurate scenario is when $\mu = 4$ and beamforming is used.

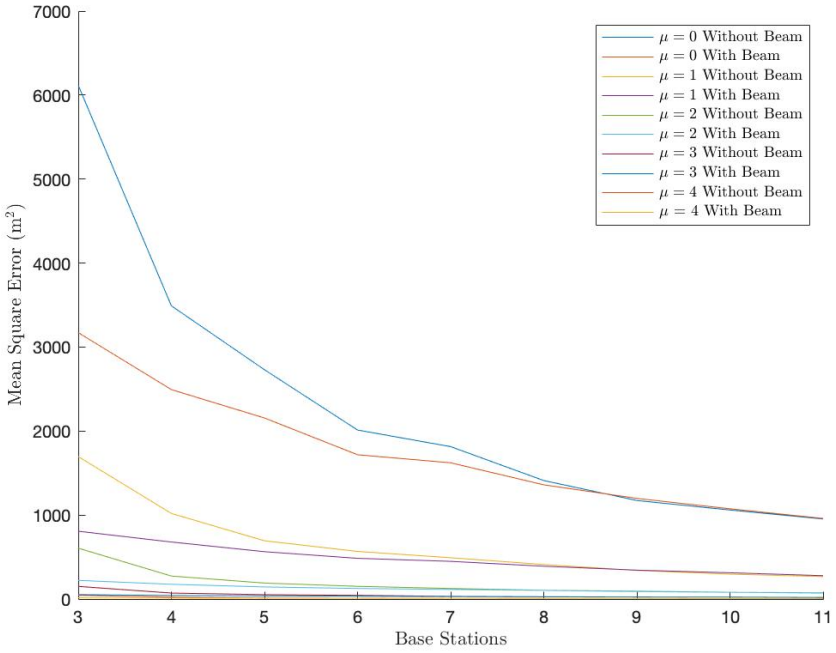

Figure 4.1. Mean square error for the position estimate for all numerologies when estimating distances from only servicing RRHs and both RRHs and beams.

4.2 Architectural Density Simulation in the 5G Environment

We had anticipated that at some point, the saturation of remote radio heads would create an environment that would make the UE location less accurate. However, Figures A.1-A.7 found in Appendix A show a closer look at our dense 5G environment. It is visible that at each numerology tested, the UE selecting the closest RRH will always have a higher MSE as compared with the UE selecting 3 to 11 of the closest RRHs for its location estimate. Figures A.1 and A.7 presented in Appendix A show zoomed out images where the top blue line represents the UE selecting the closest remote radio head, and below, the 3 through 11 of the closest RRHs selected by the UE. Figures A.3-A.6 also presented in Appendix A show a zoomed-in image for their respective μ.

Overall, as seen in the previous images presented in Appendix A and in Tables B.2-B.6

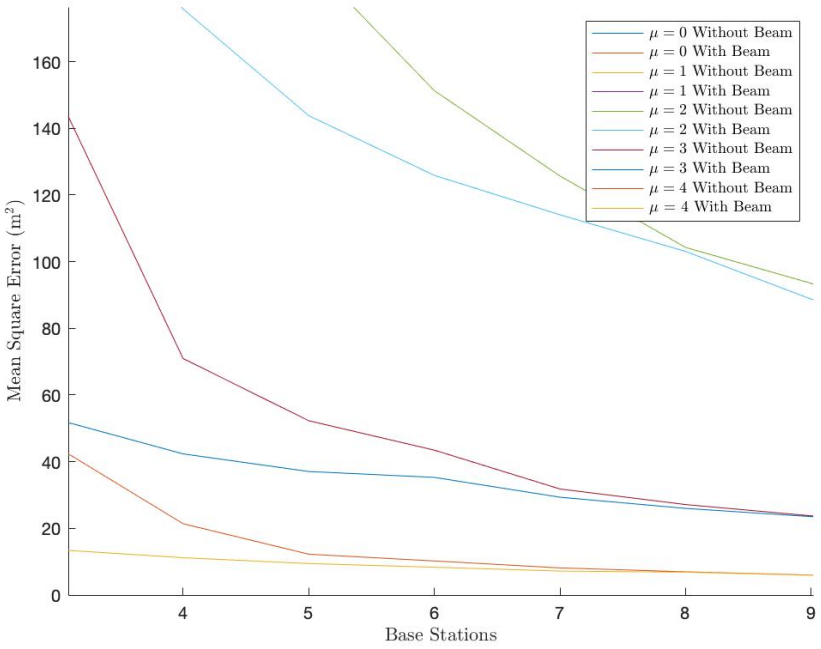

Figure 4.2. This image is the close-up of Figure 4.1. The mean square error for the position estimate of the UE for all numerologies when estimating distances from only servicing RRHs and both RRHs and beams. μ= 0 and 1 not pictured.

found in Appendix B, it is evident that the MSE is lowest when a UE can utilize more servicing RRHs for a more accurate location estimate. The results in Table B.2 show the location error results when μ = 0. The difference between the MSE of the closest RRH to the UE compared to the UE selecting the 3 closest RRH was a larger deficit than expected. As the density of these increases, it is still significant that choosing the closest 3 RRHs would give a much smaller MSE than choosing the single closest. This difference is even more drastic when comparing the selection of the closest 11 RRHs to the closest UE.

The comparisons found in Table B.2 become more severe as the MSE continues to rapidly decrease as the numerology increases. These relationships can be seen in Tables B.3-B.6. When μ = 4, it is a striking difference in the location error, as the |acMSE of the closest 3 RRHs is under 35 m^2, no matter how dense the infrastructure deployment, and even more accurate at MSE of the closest 11 RRHs that is under 5 m^2.

3 Remote Radio Heads					
		90% CEP		95% CEP	
μ	SCS (kHz)	Beamforming	Without Beamforming	Beamforming	Without Beamforming
0	15	66.37	77.49	71.27	92.68
1	30	33.27	40.23	37.00	46.23
2	60	17.10	21.51	18.83	24.86
3	120	8.39	10.72	9.22	12.68
4	240	4.29	5.24	4.69	5.97

Table 4.1. Circular error probable for 3 RRHs per numerology. Comparison of 90% and 95% CEP both with and without beamforming.

5 Remote Radio Heads					
		90% CEP		95% CEP	
μ	SCS (kHz)	Beamforming	Without Beamforming	Beamforming	Without Beamforming
0	15	58.72	63.64	65.29	74.47
1	30	31.19	34.06	34.60	39.57
2	60	15.58	17.25	17.25	19.70
3	120	7.82	8.51	9.08	9.97
4	240	3.91	4.35	4.55	5.30

Table 4.2. Circular error probable for 5 RRHs per numerology. Comparison of 90% and 95% CEP both with and without beamforming.

Other observations found in this simulation is the point at which selecting a certain number of RRHs will not affect the MSE. At its most dense point of 250 RRHs, when $\mu = 0$, the range of MSE between 3 and 11 RRHs is from 514 m^2 to 368 m^2 respectively. This range becomes more accurate as the numerology increases, as seen when $\mu = 4$ where 3 and 11 RRHs have a MSE of nearly 32 m^2 and 4 m^2, respectively.

Lastly, as expected, it can be seen in the previous tables and figures that the density is affected more when at a lower numerology. As expected, when $\mu = 0$, the lowest MSE was with 11 selected RRHs in a highly dense environment of nearly 250 RRHs. The MSE for these parameters was about 368 m^2. Comparing this result to $\mu = 4$, the average MSE for

9 Remote Radio Heads					
		90% CEP		95% CEP	
μ	SCS (kHz)	Beamforming	Without Beamforming	Beamforming	Without Beamforming
0	15	46.92	47.46	52.61	53.91
1	30	25.34	24.83	28.40	29.08
2	60	12.91	12.82	14.14	14.59
3	120	6.56	6.50	7.39	7.53
4	240	3.35	3.39	3.66	3.85

Table 4.3. Circular error probable for 9 RRHs per numerology. Comparison of 90% and 95% CEP both with and without beamforming.

11 RRHs is 4 m^2. This is a significant difference in location error.

4.3 Summary

Looking back at the questions posed in Chapter 3, we are able to summarize our findings based on the parameters and results of the simulations conducted. Our first simulation objective was to observe the point at which the number of servicing RRHs stop providing a significant improvement in the UEs positioning performance. We conducted this both with and without beamforming in the 5G environment. We found that as the number of RRHs increase, so too does the accuracy of our location estimates. With these results, we were also able to see that as the numerology increased, the MSE decreased, making our location estimate even more accurate. Beamforming made our results much more accurate when there were 3 and 4 servicing RRHs. As the numerology increases, our accuracy of finding our UE position increases, both with and without beamforming.

Our final question that we simulated set out how BS density affected our location estimate and at what point, if ever, would the UE become easier to find utilizing the closest RRH. Our results showed that no matter how dense the RRHs become, the location accuracy will increase accuracy with more RRH options available.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5:
Conclusion and Recommendations

The purpose of this thesis was to determine whether the TA localization method results in a low MSE with 5G beamforming, how beamforming changes the 5G environment, and how dense RRH areas affect location privacy. We have shown that by using the multiple unencrypted TA commands of a target UE, an adversary can calculate the user with a small margin of error with the proper equipment. We believe that with the preciseness of beamforming, the location error is lowered in areas with fewer RRHs for the user to utilize. We also were able to find that a user is vulnerable to more accurate position estimates in RRH dense areas. With our findings, we believe that end-user privacy is at greater risk with the evolution of 5G technology.

5.1 Limitations

There were limitations with the implementations of this thesis. Beamforming in 5G is a significant concept utilized in its most basic form for this thesis. Beam management, specifically beam-sweeping, measurement, determination, and reporting, was not discussed in-depth or simulated. The element patterns and array factors were also not discussed or simulated for this thesis. Another limitation was the two-dimensional simulation setting. Beamforming utilized in urban areas creates an interesting dynamic as antennas are utilized at various heights that depend on environmental factors.

5.2 Follow-on Research Recommendations

Follow-on recommendations for this thesis are based on the limitations found in this thesis and the logical "next step" to this research. The first recommendation would be to create a three-dimensional version of this study and add a dynamically moving UE to test how well the algorithms can localize the target. Conducting this research in an operational 5G environment would allow the algorithm to be tested in a true environment with real signals to test the accuracy of locating the end user.

A final recommendation would be to analyze the data found in the 5G beamforming mini-

mization equation 3.2 to determine whether or not it is a MLE that includes beamforming. Future research should include detailed mathematical analysis of finding this objective MLE function.

APPENDIX A:
Figures of Mean Square Error Results for Location Error

Each figure in this section show the results found from the simulations detailed in Chapter 3 and Chapter 4. Each figure displays the resulting MSE for the location error of each μ with increasing architectural density.

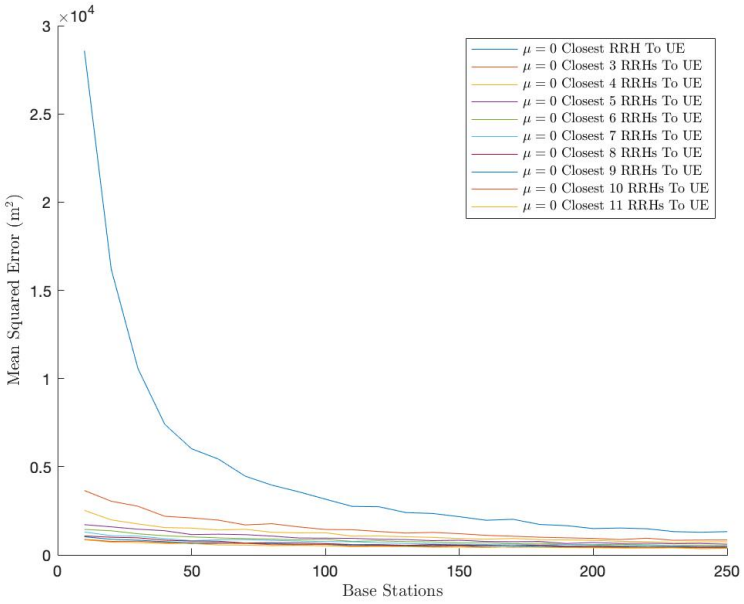

Figure A.1. This image shows the mean square error of location error when $\mu = 0$. The RRHs in the given area range from 3 to 250.

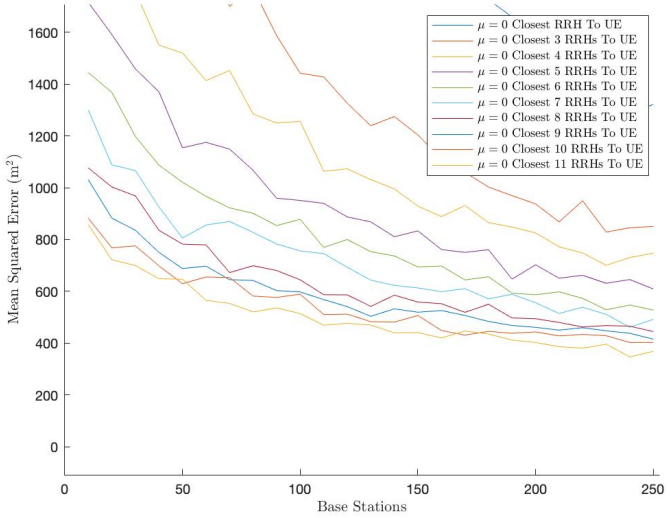

Figure A.2. Above is a close-up of the mean square error for the location error when $\mu = 0$. The RRHs in the given area range from 3 to 250.

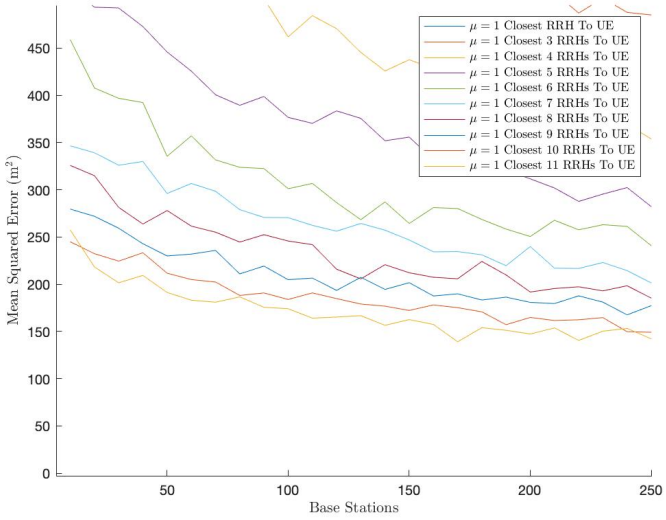

Figure A.3. Above is the zoomed in view of mean square error for the location error when $\mu = 1$. The RRHs in the given area range from 3 to 250. Closest RRH to UE and closest 3 RRHs to UE not pictured.

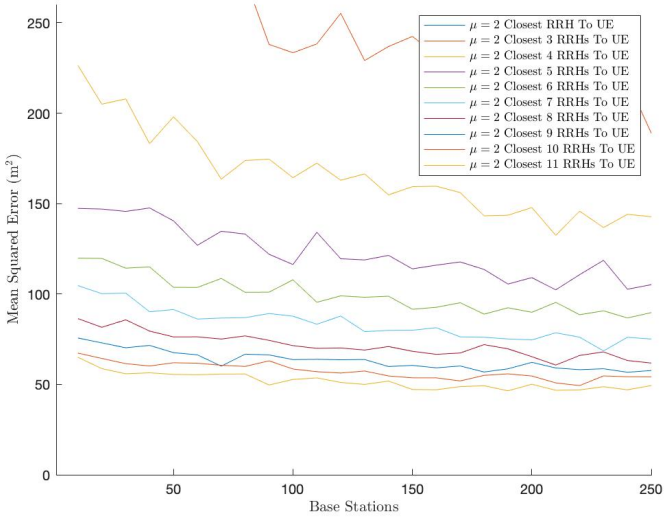

Figure A.4. The zoomed in view of mean square error for the location error when $\mu = 2$. The RRHs in the given area range from 3 to 250. Closest RRH to UE not pictured.

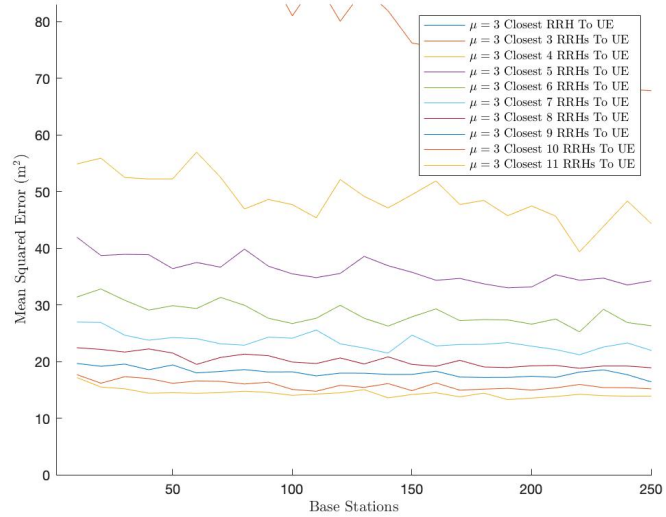

Figure A.5. The zoomed in view of mean square error for the location error when $\mu = 3$. The RRHs in the given area range from 3 to 250. Closest RRH to UE not pictured.

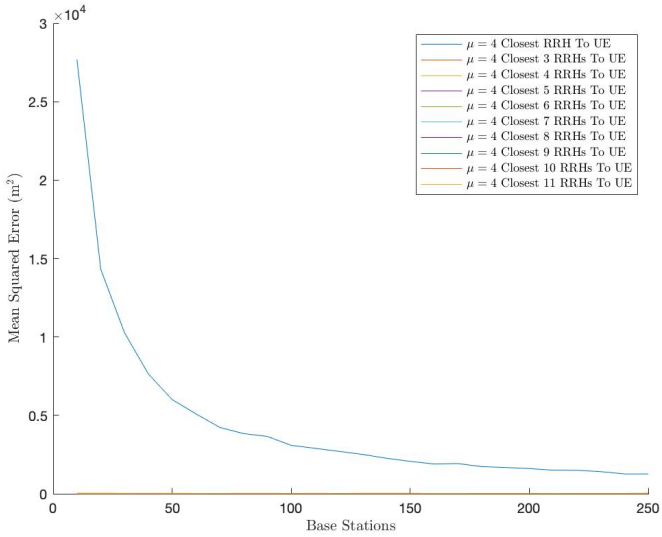

Figure A.6. Mean square error of location error when $\mu = 4$. The RRHs in the given area range from 3 to 250.

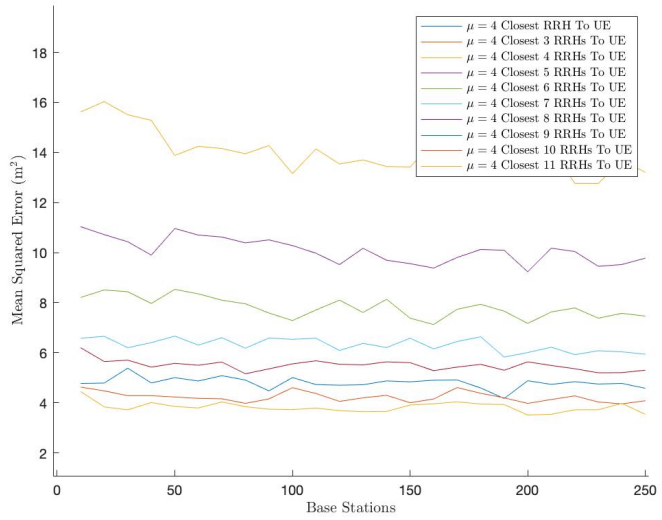

Figure A.7. The zoomed in view of mean square error for location error when $\mu = 4$. The RRHs in the given area range from 3 to 250. Closest RRH to UE not in picture. Closest RRH to UE and closest 3 RRHs to UE not pictured.

APPENDIX B: Tables of Mean Square Error Results for Location Error

The tables in this section show the results found from the simulations detailed in Chapter 3 and Chapter 4. Each table describes the resulting MSE for the location error of each μ with increasing architectural density.

Location Error when μ=0			
Density of RRHs	MSE of Closest RRH to UE (m^2)	MSE of Closest 3 RRHs to UE (m^2)	MSE of Closest 11 RRHs to UE (m^2)
10 RRHs per 1 km^2	28580.70	3158.52	1322.05
100 RRHs per 1 km^2	3648.96	1442.16	850.49
250 RRHs per 1 km^2	857.11	514.14	368.43

Table B.1. Mean Square Error Results for the location error when μ=0 for density of 10, 100 and 250 RRHs in a given area.

Location Error when μ=0			
Density of RRHs	MSE of Closest RRH to UE (m^2)	MSE of Closest 3 RRHs to UE (m^2)	MSE of Closest 11 RRHs to UE (m^2)
10 RRHs per 1 km^2	28580.70	3158.52	1322.05
100 RRHs per 1 km^2	3648.96	1442.16	850.49
250 RRHs per 1 km^2	857.11	514.14	368.43

Table B.2. Mean Square Error Results for the location error when μ=0 for density of 10, 100 and 250 RRHs in a given area.

Location Error when μ=1			
Density of RRHs	MSE of Closest RRH to UE (m^2)	MSE of Closest 3 RRHs to UE (m^2)	MSE of Closest 11 RRHs to UE (m^2)
10 RRHs per 1 km^2	31356.60	1191.89	257.36
100 RRHs per 1 km^2	3292.96	691.47	174.05
250 RRHs per 1 km^2	1273.24	484.98	142.10

Table B.3. Mean Square Error Results for the location error when μ=1 for density of 10, 100 and 250 RRHs in a given area.

Location Error when μ=2			
Density of RRHs	MSE of Closest RRH to UE (m^2)	MSE of Closest 3 RRHs to UE (m^2)	MSE of Closest 11 RRHs to UE (m^2)
10 RRHs per 1 km^2	29014.4	339.24	64.97
100 RRHs per 1 km^2	3054.19	233.45	52.74
250 RRHs per 1 km^2	1281.62	188.89	49.38

Table B.4. Mean Square Error Results for the location error when μ=2 for density of 10, 100 and 250 RRHs in a given area.

Location Error when μ=3			
Density of RRHs	MSE of Closest RRH to UE (m^2)	MSE of Closest 3 RRHs to UE (m^2)	MSE of Closest 11 RRHs to UE (m^2)
10 RRHs per 1 km^2	28524	110.79	17.16
100 RRHs per 1 km^2	3081.94	80.99	14.02
250 RRHs per 1 km^2	1208.77	67.80	13.89

Table B.5. Mean Square Error Results for the location error when μ=3 for density of 10, 100 and 250 RRHs in a given area.

Location Error when μ=4			
Density of RRHs	MSE of Closest RRH to UE (m^2)	MSE of Closest 3 RRHs to UE (m^2)	MSE of Closest 11 RRHs to UE (m^2)
10 RRHs per 1 km^2	27692.8	33.18	4.45
100 RRHs per 1 km^2	3087.95	21.69	3.73
250 RRHs per 1 km^2	1264.45	31.69	3.54

Table B.6. Mean Square Error Results for the location error when μ=4 for density of 10, 100 and 250 RRHs in a given area.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

[1] A. C. Garcia, S. Maier, and A. Phillips, *Location-Based Services in Cellular Networks from GSM to 5G NR*, 1st ed. Boston, MA, USA: Artech House, 2020.

[2] CISCO, "Cisco annual internet report (2018-2023)," CISCO, Tech. Rep., 2020.

[3] I. Ahmad, M. L. Tanesh Kumar, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," in *IEEE Communications Mag.*, 2018, pp. 36–43.

[4] C. Drane, M. Macnaughtan, and C. Scott, "Positioning GSM telephones," in *IEEE Communications Mag.*, 1998, pp. 46–59.

[5] *Department of Defense 5G Strategy*, Under Secretary of Defense, Washington, DC, USA, 2020. Available: https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf

[6] National Security Agency, "Limiting location data exposure," NSA Cybersecurity Information, Aug. 2020. [Online]. Available: https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF

[7] Federal Commun. Commission, "Report and Order and Further Notice of Proposed Rulemaking on Revision of the FCC Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems," pp. 96–264, 1996.

[8] J. A. del Peral-Rosado, R. Raulefs, J. A. López-Salcedo and G. Seco-Granados, "Survey of cellular mobile radio localization methods: From 1G to 5G," in *IEEE Communications Surveys Tutorials*, 2018, pp. 1124–1148.

[9] F. E. L. M. Dardari, Davide. Elsevier, 2012. Available: https://app.knovel.com/hotlink/toc/id:kpSTRPTAS1/satellite-terrestrial/satellite-terrestrial

[10] Federal Commun. Commission, "Fourth Report and Order on Wireless E911 Location Accuracy Requirements," pp. 15–9, Jan. 2015.

[11] A. Schacht, K. Foster, and J. Roth, "Location privacy in the era of 5G," in *in Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021. [Online]. Available: https://doi.org/10.24251/HICSS.2021.826

[12] E. Hajlaoui, A. Zaier, A. Khlifi, J. Ghodhbane, M. B. Hamed, and L. Sbita, "4G and 5G technologies: A comparative study," in *5th International Conference on Advanced Technologies For Signal and Image Processing*, 2020.

[13] E. Dahlman, S. Parkvall, and J. Skold, *5G NR The Next Generation Wireless Access Technology*, 1st ed. San Diego, CA, USA: Academic Press, 2018.

[14] R. Q. Shaddad, F. S. Al-kmali, M. A. Noman, N. K. Ahmed, E. M. Marish, A. M. Al-Duais, A. A. Al-Yafrsi, and F. A. Al-sabri, "Planning of 5G millimeterwave wireless access network for dense urban area," in *2019 First International Conference of Intelligent Computing and Engineering (ICOICE)*, 2019.

[15] A. Karimi and K. I. Pedersen, "On the multiplexing of data and metadata for ultra-reliable low-latency communications in 5G," in *IEEE Transactions on Vehicular Technology*, 2020.

[16] T. Salman and R. Jain, "Cloud RAN: Basics, advances and challenges," Washington University in St. Louis, Apr. 2016. [Online]. Available: https://www.cse.wustl.edu/~jain/cse574-16/ftp/cloudran.pdf

[17] S. Perrin, "Evolving to an open c-ran architecture for 5G," Fujitsu, Tech. Rep., 2017.

[18] D. T. Kiet, T. M. Hieu, N. Q. Hung, N. V. Cuong, V. T. Van, and P. N. Cuong, "A survey on TOA based wireless localization and NLOS mitigation techniques," in *2020 4th International Conference on Recent Advances in Signal Processing, Telecommunications Computing (SigTelCom)*, 2020.

[19] 3GPP TS 38.801, release 14, (v2.0.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; Physical layer procedures for control," July 2016.

[20] Viavi Solutions, "What is fronthaul?" VIAVI Solutions Inc., Apr. 2021. [Online]. Available: https://www.viavisolutions.com/en-us/fronthaul

[21] eCPRI Specification V1.2, "Common Public Radio Interface; eCPRI Interface Specification," June 2018. [Online]. Available: http://www.cpri.info/downloads/Requirements_for_the_eCPRI_Transport_Network_V1_2_2018_06_25.pdf

[22] C. Pan, M. Elkashlan, J. Wang, J. Yuan, and L. Hanzo, "User-centric c-ran architecture for ultra-dense 5G networks: Challenges and methodologies," arxiv, Sep, 2017. [Online]. Available: https://arxiv.org/pdf/1710.00790.pdf

[23] M. Mezzavilla, M. Zhang, M. Polese, R. Ford, S. Dutta, S. Rangan, and M. Zorzi, "End-to-end simulation of 5G mmwave networks," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2237–2263, 2018.

[24] 3GPP TS 38.213, release 16, (v16.1.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; Physical layer procedures for control," Apr. 2020.

[25] N. Patriciello, S. Lagen, L. Giupponi, and B. Bojovic, "5G new radio numerologies and their impact on the end-to-end latency," in *2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2018, pp. 1–6.

[26] B. Witte, "The basics of 5G's modulation, OFDM," 5G Technology World, Apr, 2020. [Online]. Available: https://www.5gtechnologyworld.com/the-basics-of-5gs-modulation-ofdm/

[27] J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "Location privacy in LTE: A case study on exploiting the cellular signaling plane's timing advance," in *IEEE Communications Surveys Tutorials*, 2017.

[28] 3GPP TS 36.321, release 16, (v16.0.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification," Apr. 2020.

[29] 3GPP TS 38.211, release 16, (v16.1.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; Physical channels and modulation," Apr. 2020.

[30] A. Schacht, J. Long, and J. Roth, "Timing management in 5G and its implications for location privacy," in *53rd Hawaii International Conference on System Sciences*, 2020. Available: https://doi.org/10.24251/HICSS.2020.773

[31] Abuu B. Kihero and Muhammad Sohaib J. Solaija and Hüseyin Arslan, "Inter-Numerology Interference for Beyond 5G," Oct. 2019.

[32] T. Maksymyuk, J. Gazda, O. Yaremko, D. Nevinskiy, and L. Polytechnic, "Deep learning based massive mimo beamforming for 5g mobile network," in *2The 4th IEEE International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems*, 2018, pp. 241–244.

[33] A. Nordrum, K. Clark, and I. Spectrum, "5G bytes: Beamforming explained," IEEE Spectrum, Jul. 15, 2017. [Online]. Available: https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-beamforming-explained

[34] S. Kutty and D. Sen, "Beamforming for millimeter wave communications: An inclusive survey," in *IEEE Communications Surveys Tutorials*, 2016.

[35] M. Shukair, "How 5G massive MIMO transforms your mobile experiences," Qualcomm OnQ Blog, Jun, 2019. [Online]. Available: https://www.qualcomm.com/news/onq/2019/06/20/how-5g-massive-mimo-transforms-your-mobile-experiences

[36] P. Newson, H. Parekh, and H. Matharu, "Realizing 5G new radio massive MIMO systems," EDN, Jan, 2018. [Online]. Available: https://www.edn.com/realizing-5g-new-radio-massive-mimo-systems/

[37] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, N.J, USA: Prentice-Hall, 2002.

[38] "Advanced antenna systems for 5G," 5G Americas White Paper, Aug, 2019. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Americas_Advanced-Antenna-Systems-for-5G-White-Paper.pdf

[39] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of k-tier downlink heterogeneous cellular network," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, 2012.

[40] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, 2014.

[41] VIAVI, "5G technology," VIAVI Solutions, May, 2021. [Online]. Available: https://www.viavisolutions.com/en-us/5g-technology

[42] I. Guvenc and C. Chong, "A survey on TOA based wireless localization and NLOS mitigation techniques," in *IEEE Communications Surveys Tutorials*, 2009.

[43] J. J. Caffery and G. L. Stuber, "Overview of radiolocation in CDMA cellular systems," in *IEEE Commun. Mag.*, 1998, pp. 38–45.

[44] Stijn Wielandt and Lieven De Strycker, "Indoor Multipath Assisted Angle of Arrival Localization," *Sensors*, Nov. 2017.

[45] J. Roth, "Analysis and augmentation of timing advance-based geolocation in lte cellular networks," Ph.D. dissertation, Dept. of Electrical and Computer Engineering, Naval Postgraduate School, Monterey, CA, USA, 2016.

[46] D. J. Torrieri, "Statistical theory of passive location systems," in *IEEE Trans. Aerosp. Electron. Syst.*, 1984, pp. 183–197.

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California