Sorbonne University
Doctoral School of Informatics, Telecommunications and Electronics of Paris
EURECOM

Localization and Sensing in 5G NR and beyond

Presented by **Rakesh Mundlamuri**

Dissertation for Doctor of Philosophy in Information and Communication Engineering

Directed by **Prof. Florian Kaltenberger**

The Jury committee is composed of:

Prof. Kaushik Chowdhury	(University of Texas at Austin, USA)	Reviewer
Prof. Henk Wymeersch	(Chalmers University of Technology, Sweden)	Reviewer
Prof. Luc Deneire	(Côte d'Azur University, France)	Jury President
Dr. Mari Kobayashi	(Habilitation at Paris-Sud University, Germany)	Examiner
Prof. Dirk Slock	(EURECOM, France)	Examiner
Prof. Florian Kaltenberger	(EURECOM, France)	Thesis Director

Sophia Antipolis, 26 June, 2025

Sorbonne Université
École Doctorale Informatique, Télécommunications et Électronique de Paris
EURECOM

Localisation et Sensing dans la 5G NR et au-delà

Présenté par **Rakesh Mundlamuri**

Thèse de doctorat en Sciences de l'Information et de la Communication

Dirigée par **Prof. Florian Kaltenberger**

Le jury est composé de :

Prof. Kaushik Chowdhury	(Université du Texas à Austin, USA)	Rapporteur
Prof. Henk Wymeersch	(Université de technologie Chalmers, Suède)	Rapporteur
Prof. Luc Deneire	(Université Côte d'Azur, France)	Président du Jury
Dr. Mari Kobayashi	(Habilitation à Université Paris-Sud, Allemagne)	Examinatrice
Prof. Dirk Slock	(EURECOM, France)	Examinateur
Prof. Florian Kaltenberger	(EURECOM, France)	Directeur de Thèse

Sophia Antipolis, 26 Juin, 2025

Abstract

Accurate localization and environmental sensing capabilities are crucial for developing intelligent, autonomous, and connected systems. Apart from offering high data rates and low latency communication, next-generation cellular networks, such as 5G and beyond, are expected to provide precise localization and environmental sensing capabilities. These capabilities rely on the accurate estimation of the channel state information (CSI). However, in practice, the estimated CSI suffers from impairments such as clock drift and timing correction loops. The clock drift occurs when the clocks on the base station (gNB) and the user equipment (UE) run asynchronously, leading to drift over time. To mitigate this issue, timing correction loops are incorporated into the cellular protocol stack to correct the clock drift periodically. While cellular systems were traditionally designed for communication purposes, the effect of clock drift and timing correction loops is negligible on the communication performance. In contrast, these factors significantly affect the performance of the localization and sensing. Specifically, they introduce variability in the delay estimates of the multipath components obtained from the CSI across different time slots. As a result, even when the UE is static and the gNB has access to multiple channel measurements, the delay estimates of the multipath components estimated from the CSI vary over time.

In this dissertation, we design a system and propose signaling schemes that allow us to obtain CSI that is robust to clock drift and timing correction loops within a cellular system. Additionally, we propose a system that leverages sensing information to improve the performance of the communication system. Specifically, we introduce a system framework that facilitates the fusion of sensing information into the communication system, thereby reducing the pilots in channel estimation. We also provide a framework to evaluate the performance of our proposed localization algorithms in a digital twin using the Colosseum platform. Furthermore, we demonstrate a drone-based localization and sensing application for search and rescue missions, emphasizing the importance of backhaul connectivity to the cellular network in such scenarios. Finally, we highlight that most of our work has been validated using OpenAirInterface (OAI).

Résumé

La localisation précise et les capacités de sensing environnementale sont essentielles au développement de systèmes intelligents, autonomes et connectés. En plus d'offrir des débits élevés et une communication à faible latence, les réseaux cellulaires de nouvelle génération, tels que la 5G et au-delà, devraient également fournir des capacités de localisation et de sensing environnementale précises. Ces capacités reposent sur une estimation précise de l'état du canal, connue sous le nom d'informations d'état du canal (CSI – Channel State Information). Cependant, dans la pratique, le CSI estimé est affecté par des perturbations telles que la dérive d'horloge et les boucles de correction temporelle. La dérive d'horloge se produit lorsque les horloges de la station de base (gNB) et de l'équipement utilisateur (UE) ne sont pas synchronisées, entraînant une dérive au fil du temps. Pour atténuer ce problème, des boucles de correction temporelle sont intégrées dans la pile protocolaire du réseau cellulaire afin de corriger périodiquement la dérive d'horloge. Alors que les systèmes cellulaires ont été conçus à l'origine pour des fins de communication, l'effet de la dérive d'horloge et des boucles de correction temporelle sur les performances de communication reste négligeable. En revanche, ces facteurs ont un impact significatif sur les performances de localisation et de sensing. Plus précisément, ils introduisent une variabilité dans les estimations de délai des composantes de trajets multiples extraites du CSI à différents instants. En conséquence, même lorsque l'UE est statique et que la gNB dispose de multiples mesures de canal, les estimations de délai des composantes multipaths dérivées du CSI varient dans le temps.

Dans cette dissertation, nous concevons un système et proposons des schémas de signalisation permettant d'obtenir un CSI robuste face à la dérive d'horloge et aux boucles de correction temporelle au sein d'un système cellulaire. Par ailleurs, nous proposons un système exploitant les informations de sensing afin d'améliorer les performances du système de communication. Plus précisément, nous introduisons un cadre systémique facilitant la fusion des informations de sensing dans le système de communication, réduisant ainsi le besoin de pilotes pour l'estimation du canal. Nous présentons également un cadre d'évaluation des performances de nos algorithmes de localisation proposés dans un jumeau numérique, à l'aide de la plateforme Colosseum. De plus, nous démontrons une application de localisation et de sensing basée sur drone pour des missions de recherche et de sauvetage, en soulignant l'importance de la connectivité dorsale au réseau cellulaire dans ce type de scénarios. Enfin, nous soulignons que la majorité de nos travaux a été validée en utilisant OpenAirInterface (OAI).

Acknowledgments

This work would not have been possible without the support of many people who helped me along the way.

I am especially thankful to my supervisor, Prof. Florian Kaltenberger. We first connected while I was at IISc, and his encouragement led me to pursue both my master's and doctoral studies. His constant guidance and support have shaped my research and helped me grow both as a scholar and as a person.

I'm grateful to Prof. Chandra Murthy and Christo Thomas for their early encouragement. Their belief in me inspired me to take on this doctoral journey. Special thanks to Rajeev Gangula for his steady support and many helpful discussions, which helped me grow both in my research and as a person.

I also thank my collaborators, Raymond Knopp, Omid Esrafilian, and Christo Thomas, for sharing their knowledge and making our work together enjoyable.

I am grateful to Prof. Tommaso Melodia and everyone at Northeastern University for welcoming me as an exchange student. Working at the Colosseum facility was a great experience that helped my research.

I am deeply grateful to my family for their unwavering love and support. My parents, Srinivasulu and Ramadevi, made many sacrifices for me, and my brother, Bala Yeshwanth, always gave me the strength I needed. I also thank my uncle Ramesh and his family for their care and encouragement.

I also want to thank my friends Sri Hari, Viswa, Sireesha, Sandeep, Cedric, Melek, Jayanth, Nitha, Pavani, and Meghana for being there for me through all the ups and downs.

Thank you.
Rakesh

Contents

List of Figures

List of Tables

Glossary

2G	second-generation
3D	three dimensional
3G	third-generation
3GPP	third generation partnership project
4G	fourth-generation
5G NR	fifth-generation new radio
5GC	5G core
6G	sixth-generation
AC	air-conditioner
ADC	analog-to-digital conversion
ADoA	angle difference of arrival
ADoD	angle difference of departure
AI	artificial intelligence
AMF	access and mobility management function
AoA	angle of arrival
AoD	angle of departure
AR	augment reality
AUSF	authentication server function
BAP	backhaul adaptation protocol
CDF	cumulative distribution Function
CFR	channel frequency response
CIR	channel impulse response
COTS	commercial off-the-shelf
CS	compressed sensing
CSI	channel state information
CSI-RS	channel state information reference signal
CU	centralized unit
CU-CP	CU control plane
CU-UP	CU user plane
DAC	digital-to-analog conversion
DARPA	defense Advanced research projects agency
dBFS	decibels relative to full scale
DC	direct current
DCI	downlink control information
DFT	discrete Fourier transform
DL	downlink
DRX	diversity receive antenna

DSB	double sideband
DU	distributed unit
E	expectation
E-CID	enhanced cell ID
EDGE	enhanced data rates for GSM evolution
EM	expectation maximization
eMBB	enhanced mobile broadband
F1AP	F1 application protocol
FCC	federal communications commission
FDD	frequency division duplex
FFT	fast Fourier transform
FIR	finite impulse response
FPGA	field programmable gate array
FR	frequency range
GERAN	GSM EDGE radio access network
GHz	gigahertz
gNB	base-station
GPRS	general packet radio service
GPS	global positioning system
GPU	graphics processing unit
GSM	global system for mobile communications
GTP	general packet radio service tunneling protocol
IAB	integrated access and backhaul
IDFT	inverse discrete Fourier transform
IF	intermediate frequency
IFFT	inverse fast Fourier transform
IQ	in-phase and quadrature-phase
KHz	kilohertz
LBS	location-based services
LMF	location management function
LNA	low-noise amplifier
LO	local oscillator
LoS	line-of-sight
LPHAP	low power high accuracy positioning
LPP	LTE positioning protocol
LS	least squares
LTE	long-term evolution
LXC	linux container
M	maximization
m	meter
MAC	medium access control
MAP	maximum a posteriori
MCHEM	massive channel emulator
MF	threshold based matched filter
MGEN	multi-generator
MHz	megahertz
MIB	master information block

MIMO multi-input multi-output
ML machine learning
MLH maximum likelihood
MMTC massive machine-type communications
mmWave millimeter wave
MPC multipath component
ms milliseconds
MSBL multiple measurement vector SBL
MT mobile terminal
NAS network attached storage
NLS non-least squares
NMSE normalized mean square error
NRF network repository function
NRPPa NR positioning protocol annex
nrUE user equipment
ns nano seconds
NSF national science foundation
NSSF network slice selection function
O-RAN open radio access network
OAI OpenAirInterface
OFDM orthogonal frequency division multiplexing
OMP orthogonal matching pursuit
OTFS orthogonal time frequency space
PA power amplifier
PBCH physical broadcast channel
PD threshold based peak detector
PDCCH physical downlink control channel
PDCP-C control plane packet data convergence protocol
PDCP-U user plane packet data convergence protocol
PDSCH physical downlink shared channel
PHY physical
PRACH physical random access channel
PRS positioning reference signal
PSG programmable signal generator
PSS primary synchronization signal
QPSK quadrature phase shift keying
RA random access
RACH random access channel
RAN radio access network
RAR random access response
RB resource block
RE resource element
RF radio frequency
RIC RAN intelligent controller
RLC radio link control
RNTI radio network temporary identifier
RRC radio resource control

RSS received signal strength
RToA relative time of arrival
RTT round-trip time
RU radio unit
RX receiver
Rx-Tx receive-transmit
SAR search and rescue
SBL sparse Bayesian learning
SCS subcarrier spacing
SDAP service data adaption protocol
SDR software-defined radio
SIB system information block
SMF session management function
SMO service management and orchestration
SNR signal-to-noise ratio
SRN standard radio node
SRS sounding reference signal
SSB synchronization signal block
SSS secondary synchronization signal
SUL supplementary uplink
SUMO simulation of urban mobility
SWOMP simultaneous weighting orthogonal matching pursuit
TA timing advance
TDD time division duplex
TDoA time difference of arrival
TGEN traffic generator
THz terahertz
TRX transmit/receive
TX transmitter
Tx transmit
UAV unmanned aerial vehicle
UDM unified data management
UDR unified data repository
UE user equipment
UL uplink
UPF user plane function
URLLC ultra-reliable low-latency communications
URS uplink reference signal
USRP universal software radio peripheral
UTMS universal mobile telecommunications system
V2X vehicle-to-everything
VDI virginia diodes, Inc.
VR virtual reality
ZC zadoff-chu

Chapter 1

Introduction

Localization in cellular networks enables the base stations to determine a user's location, while sensing enables the network to sense the surrounding environment besides offering cellular connectivity. These technologies have drawn significant attention in recent years as they enhance the global positioning system (GPS) outdoors and act as a viable alternative in low-visibility, indoor, and GPS-denied environments. Furthermore, they also act as a viable alternative to radar systems without the need for additional infrastructure or frequency spectrum. This chapter is composed of three sections. The first section motivates the need to study and develop cellular-based localization and sensing systems. Section 1.2 provides an overview of the localization and sensing frameworks in fifth-generation new radio (5G NR) and beyond, as well as the state-of-the-art positioning and sensing techniques. The final section provides an outline of the contributions of this dissertation.

1.1 Motivation

Precise localization and environment sensing capabilities play a crucial role in the development of intelligent, autonomous, and connected systems [1, 2, 3, 4]. Beyond providing cellular connectivity, next-generation cellular networks–such as 5G NR and beyond–leverage large bandwidths and massive antenna arrays to enable highly accurate and reliable positioning and sensing capabilities [5, 6, 7].

1.1.1 Localization in Cellular Networks

Cellular-based localization serves as a complement to the GPS in outdoor scenarios and acts as a viable alternative in low-visibility, indoor, and GPS-denied environments. These advanced localization capabilities have led to numerous applications spanning both civilian and tactical scenarios.

In industrial environments, robots and automated manufacturing equipment rely on precise location awareness for autonomous operation. Additionally, workers can monitor tools and assets using cellular-based location tags, resulting in faster workflows and a more productive environment, as employees spend less time searching for equipment.

Beyond civilian applications, localization plays a crucial role in emergency response and tactical operations. Police and emergency services can use cellular-based localization to locate emergency calls quickly, enhancing dispatch systems. For instance, search and rescue (SAR) missions can utilize drone-based localization to locate individuals lost in remote areas, such as hikers in dense forests or skiers trapped in avalanche-prone zones.

1.1.2 Sensing in Cellular Networks

Cellular-based sensing serves as an alternative to radar systems for environmental sensing, eliminating the need for additional infrastructure and frequency spectrum. These advanced sensing capabilities have led to numerous applications spanning both civilian and tactical scenarios.

In futuristic smart homes, cellular networks can function as occupancy sensors, detecting human presence to autonomously adjust temperature and lighting for improved energy efficiency. Moreover, with the rise of artificial intelligence (AI), personalized AI assistants such as Siri (Apple), Alexa (Amazon), and Google Home can leverage these capabilities to follow users from room to room to provide seamless assistance. Furthermore, cellular-based sensing enhances workplace safety by establishing virtual boundaries in manufacturing plants, issuing alerts when employees enter hazardous zones. These capabilities also extend to weather monitoring, including rainfall detection and flood risk assessment. Additionally, these technologies enhance situational awareness in military scenarios by monitoring enemy movements when handling hostage situations, tracking troop positions in GPS-denied environments, and detecting rogue drones in restricted airspaces.

Apart from these applications, the situational awareness of the user devices in a cellular network greatly enhances its connectivity [8, 9, 10]. Several applications of sensing-aided communication utilize situational awareness of the user devices for channel estimation, beam prediction, and refinement.

1.2 State-of-the-Art and Literature Survey

In this section, we summarize the state-of-the-art localization and sensing frameworks in the 5G NR and beyond cellular networks. We also provide the applications of sensing to aid cellular connectivity. Finally, we highlight the impact of hardware impairments in the localization and sensing performance.

1.2.1 Cellular based Localization

The localization feature in cellular systems was initially developed to determine the location of users making emergency calls, ensuring timely rescue operations. This capability was first introduced as location-based services (LBS) in second-generation (2G) networks, including global system for mobile communications (GSM), general packet radio service (GPRS), and enhanced data rates for GSM evolution (EDGE). Collectively, these technologies formed the GSM EDGE radio access network (GERAN) [11]. LBS was also integrated into third-generation (3G) universal mobile telecommunications system (UTMS) networks [12], and the accuracy requirements were further refined in fourth-generation (4G) long-term evolution (LTE) networks [13]. In LTE, higher localization accuracy became essential due to the growing demand for location-specific applications, such as vehicle-to-everything (V2X) communication and cellular-assisted navigation [6, 14, 15, 16, 17]. These requirements have been further enhanced in 5G NR to improve the localization of users making emergency calls, particularly from indoor environments, where most emergency calls originate [18]. Starting from Release-16, the third generation partnership project (3GPP) has begun defining the target positioning accuracy for various scenarios in 5G NR. New positioning signals, measurement procedures, and architecture enhancements have been introduced in [19, 20, 21, 22, 23].

Localization techniques in cellular networks typically involve estimating parameters such as time, angle, received signal strength (RSS) at the base-station (gNB), and user equipment (UE) from the received reference signals, as shown in Figure 1.1. Timing-based methods estimate the time difference of arrival (TDoA) and round-trip time (RTT). Angle-based techniques leverage multiple antennas to obtain angular information, such as the angle of departure (AoD) and angle of arrival (AoA), as well as the angle difference of departure (ADoD) and angle difference of arrival (ADoA). RSS-based techniques measure

the power of received signals to estimate distance. Hybrid approaches combine multiple parameters–such as time, angle, and RSS–to enhance localization accuracy.

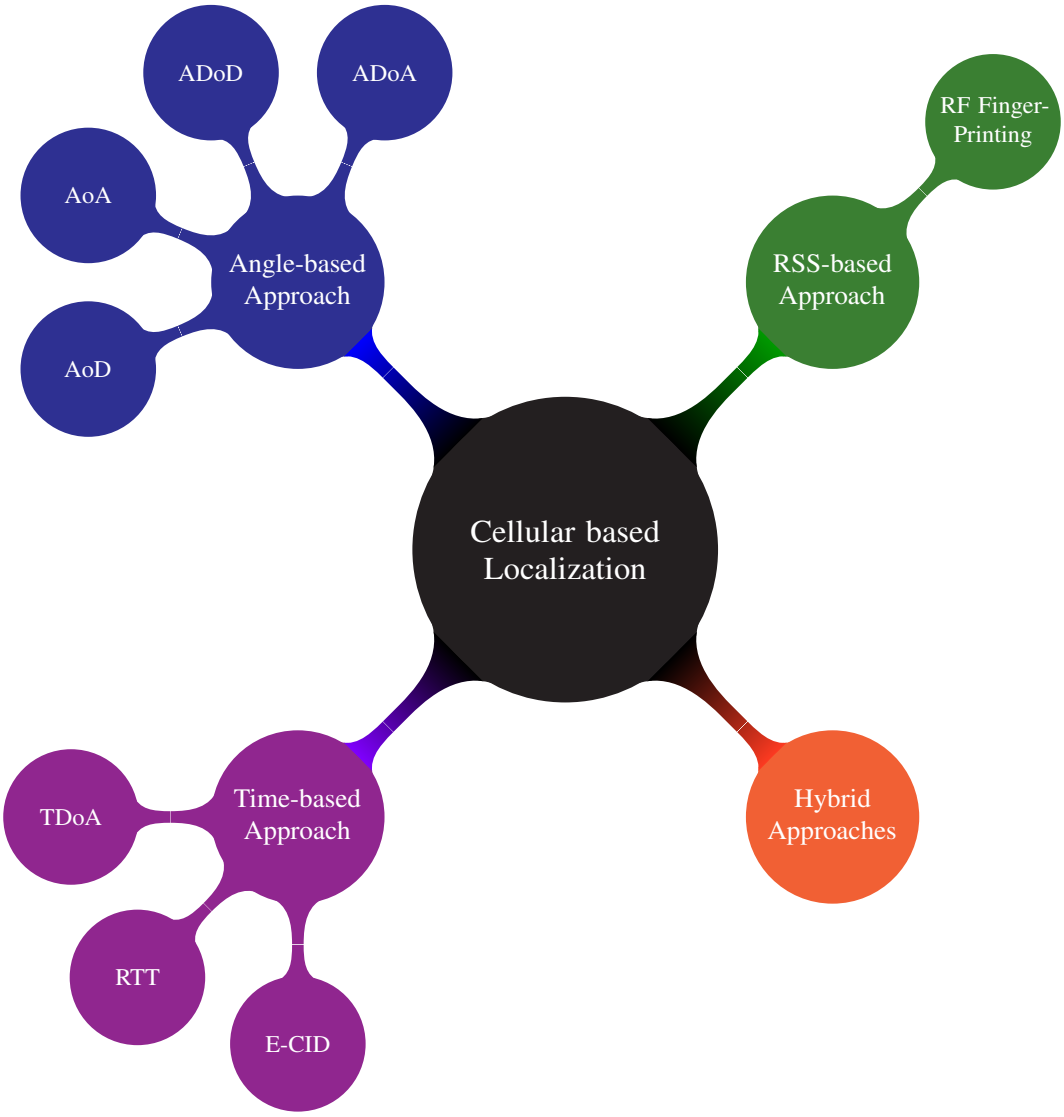


Figure 1.1: Characterization of various cellular based localization techniques.

In 5G NR, the process of localizing a UE involves single/multiple gNBs and a component of the 5G core (5GC) network, known as the location management function (LMF). During this process, both the gNBs and the UEs report measurements such as time, angle, and RSS via the NR positioning protocol annex (NRPPa) and LTE positioning protocol (LPP), as illustrated in Figure 1.2. Note that the measurements from the UE reported to the LMF using LPP are tunneled via gNB and access and mobility management function (AMF). Similarly, the measurements from gNB reported to LMF using NRPPa are tunneled via AMF. Once these measurements reach the LMF, a localization algorithm is applied to determine the location of the UE.

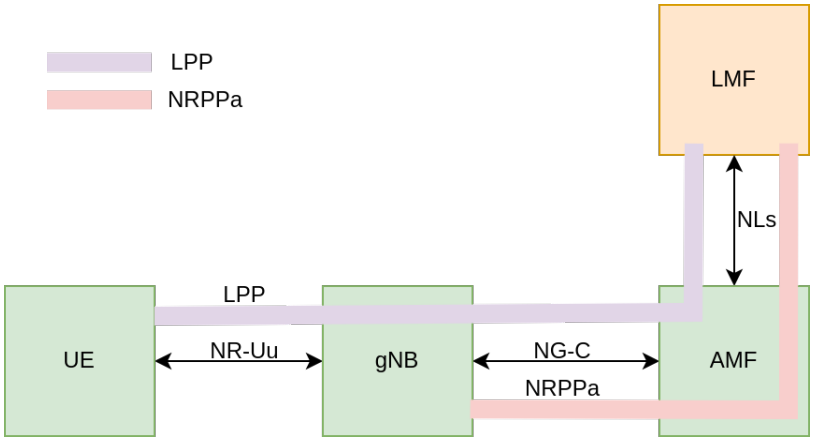


Figure 1.2: 5G Localization Architecture.

Focusing on timing-based localization techniques, two primary methods used in 5G NR are based on TDoA and RTT.

1.2.1.1 Time Difference of Arrival

TDoA-based localization in 5G NR involves multiple gNBs that are tightly synchronized and utilized in both downlink (DL) and uplink (UL) scenarios. In the downlink, TDoA is estimated using positioning reference signal (PRS), while in the uplink, it is estimated using sounding reference signal (SRS).

For DL-TDoA, the relative time of arrival (RToA) measurements estimated at the UE using PRS from multiple gNBs are reported to the LMF via LPP. The LMF then applies a localization algorithm to determine the UE location. To demonstrate how a UE can be localized using TDoA in the downlink with an example, we consider a scenario with four gNBs and a UE, as depicted in Figure 1.3. The three dimensional (3D) locations of the four gNBs in cartesian form are known and are defined as follows: $[x_1, y_1, z_1]$, $[x_2, y_2, z_3]$, $[x_3, y_3, z_3]$, and $[x_4, y_4, z_4]$. The estimated RToA from each of the four gNBs to the UE is represented as t_1, t_2, t_3, and t_4, respectively. These RToA measurements are reported to the LMF via LPP, where the LMF computes the TDoA by taking t_1 as a reference as follows,

$$t_{12} = t_1 - t_2,$$
$$t_{13} = t_1 - t_3,$$
$$t_{14} = t_1 - t_4.$$

The corresponding distances of these TDoA measurements t_{12}, t_{13}, t_{14} are denoted as d_{12}, d_{13}, d_{14} respectively. where, $d_{12} = t_{12}c$, $d_{13} = t_{13}c$, $d_{14} = t_{14}c$ and c is the speed of light. Finally, the location of the UE, represented as $[x, y, z]$, can be estimated from the distances d_{12}, d_{13}, d_{14} and the known gNB locations

$[x_1, y_1, z_1]$, $[x_2, y_2, z_3]$, $[x_3, y_3, z_3]$ and $[x_4, y_4, z_4]$ using the following equations:

$$\begin{aligned}
\sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2} - \sqrt{(x-x_2)^2+(y-y_2)^2+(z-z_2)^2} &= d_{12}, \\
\sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2} - \sqrt{(x-x_3)^2+(y-y_3)^2+(z-z_3)^2} &= d_{13}, \\
\sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2} - \sqrt{(x-x_4)^2+(y-y_4)^2+(z-z_4)^2} &= d_{14}.
\end{aligned} \tag{1.1}$$

These equations represent three hyperbolas, and by solving the equations in (1.1) for $[x, y, z]$, we can determine the location of the UE. Several works solving these non-linear equations can be found in [24]. Prior works in [25, 26, 27, 28, 29] have demonstrated the use of PRS in performing DL-TDoA.

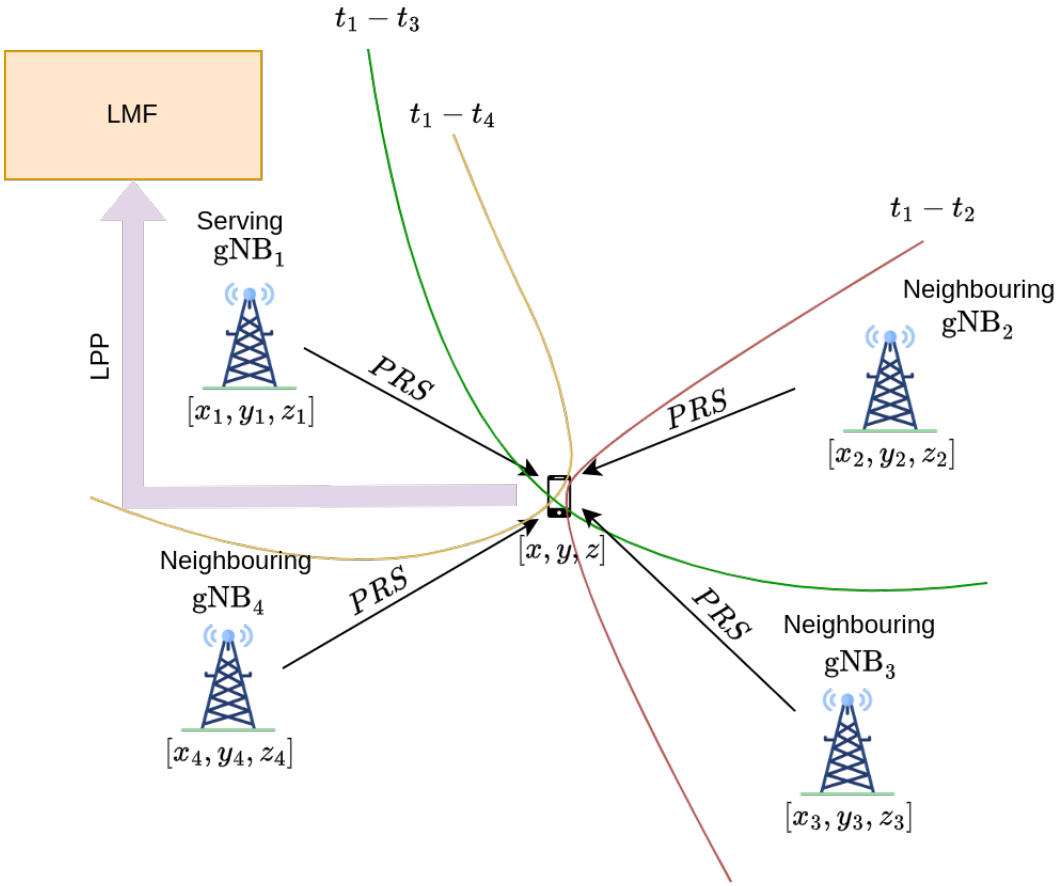


Figure 1.3: Downlink Time Difference of Arrival Localization Scenario.

Similarly, for UL-TDoA, RToA measurements based on SRS, estimated at multiple gNBs, are reported to the LMF via the NRPPa protocol, as shown in Figure 1.4. These RToA measurements from all four gNBs can be used to compute TDoA at the LMF and form equations similar to (1.1), and solving these equations allows us to determine the location of the UE. Prior works in [30, 31] have demonstrated using SRS in performing UL-TDoA for localization.

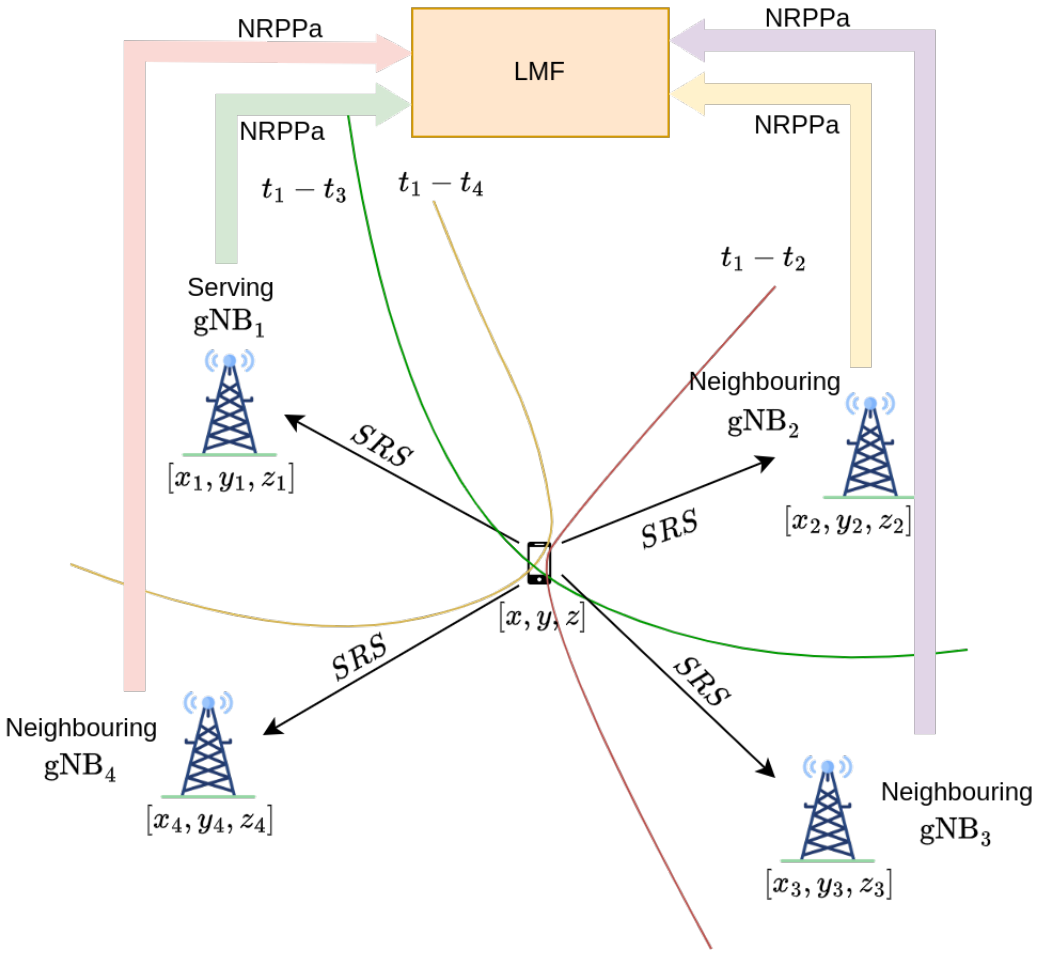


Figure 1.4: Uplink Time Difference of Arrival Localization Scenario.

1.2.1.2 Round Trip Time

RTT-based localization in 5G NR can be categorized into coarse and precise methods. A coarse RTT method referred to as enhanced cell ID (E-CID) is derived from the timing advance (TA) in the random access channel (RACH) during random access (RA) procedures. However, the accuracy of this procedure is limited due to the low bandwidth of the RACH, and RA is only performed during initial access or in the event of uplink synchronization failure. A precise RTT can be estimated using wideband reference signals like PRS and SRS. To compute RTT, both the UE and gNB measure the receive-transmit (Rx-Tx) time difference, as shown in Figure 1.5. The RTT is calculated as,

$$\text{RTT} = \text{UE Rx-Tx time difference} + \text{gNB Rx-Tx time difference}.$$

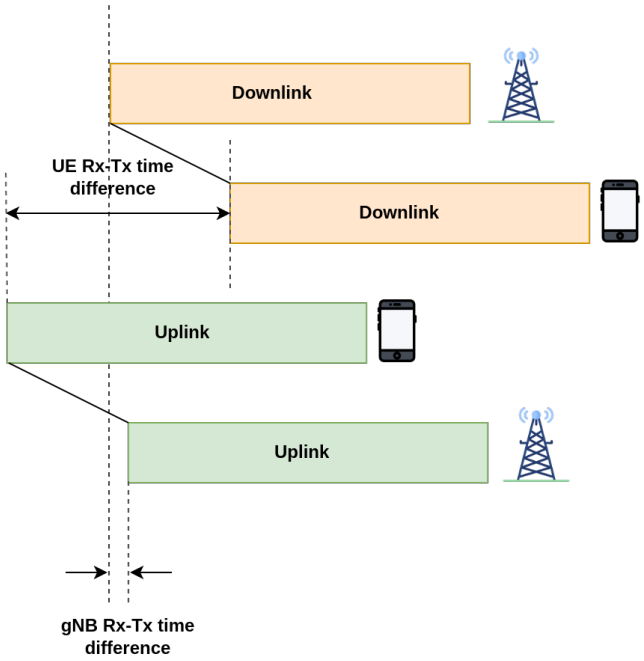


Figure 1.5: RTT estimation from Rx-Tx time difference in 5G.

This method is used in the multi-RTT scheme in 5G NR [32, 33]. Similar to TDoA-based localization, Rx-Tx time difference measurements estimated at the gNB and UE are reported to the LMF via NRPPa and LPP, where RTT is computed. Detailed reporting procedures for Rx-Tx time difference measurements to the LMF are outlined in [34]. Note that the RTT method does not require multiple gNBs to be synchronized.

Further, to demonstrate how a UE can be localized using RTT with an example, we consider a scenario with three gNBs and a UE, as depicted in Figure 1.6. The 3D locations of the three gNBs in cartesian form are known and are defined as follows: $[x_1, y_1, z_1]$, $[x_2, y_2, z_3]$, and $[x_3, y_3, z_3]$. The estimated RTT from each of the three gNBs to the UE is represented as t_1, t_2, and t_3, respectively. The distances computed from these RTT measurements, are denoted as d_1, d_2, and d_3, represent the distance between the corresponding gNB and the UE. where, $d_1 = \frac{t_1}{2}c$, $d_2 = \frac{t_2}{2}c$, $d_3 = \frac{t_3}{2}c$ and c is the speed of light. Finally, the location of the UE, represented as $[x, y, z]$, can be estimated from the distances d_1, d_2, d_3 and the

known gNB locations $[x_1, y_1, z_1]$, $[x_2, y_2, z_3]$, $[x_3, y_3, z_3]$ using the following equations:

$$\begin{aligned}(x-x_1)^2+(y-y_1)^2+(z-z_1)^2 &= d_1^2,\\ (x-x_2)^2+(y-y_2)^2+(z-z_2)^2 &= d_2^2,\\ (x-x_3)^2+(y-y_3)^2+(z-z_3)^2 &= d_3^2.\end{aligned} \tag{1.2}$$

These equations represent three circles, and by solving the equations in (1.2) for $[x, y, z]$, we can determine the location of the UE. These non-linear equations in (1.2) can be further reduced to linear equations and can be solved using least-squares and non-linear least-squares techniques as described in [35]. Note that even when a single multi-antenna gNB is available, the distance between the gNB and UE estimated from RTT can be combined with UL-AoA measurements to localize the UE. In contrast, localization with a single gNB is not possible in the case of TDoA-based localization.

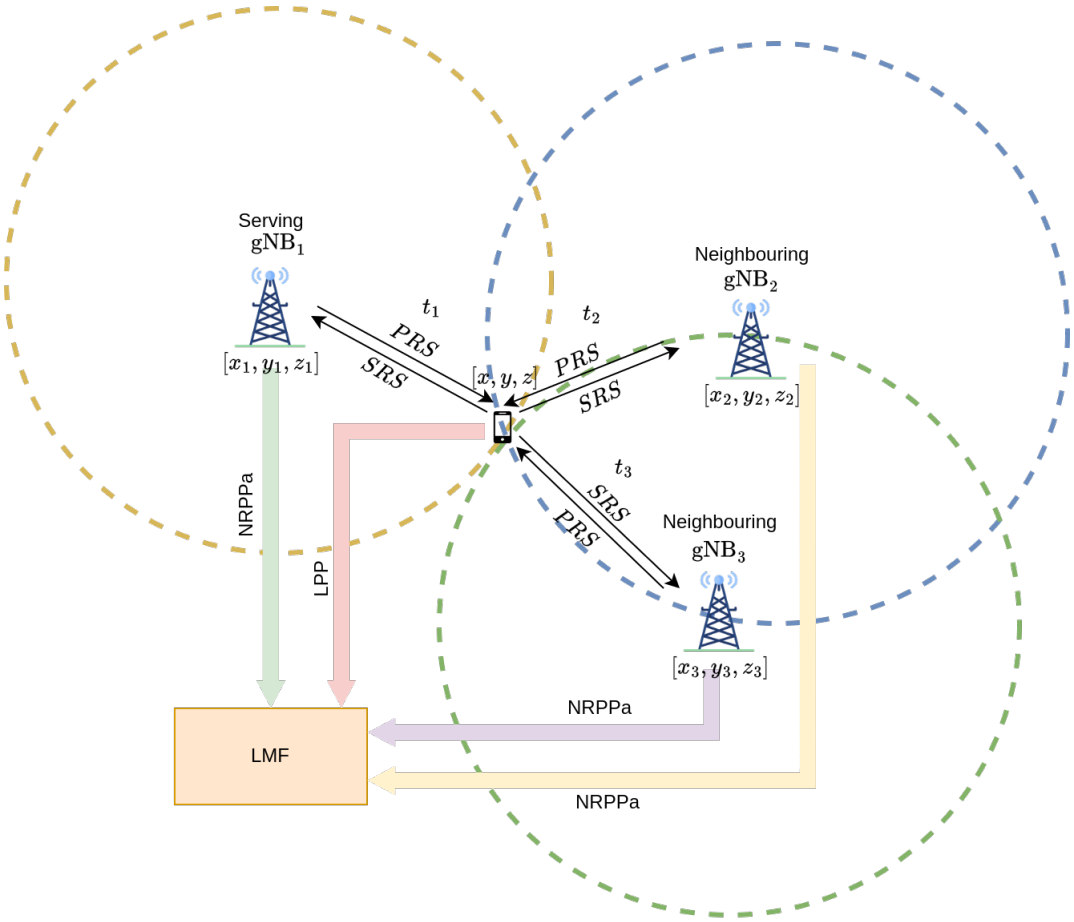


Figure 1.6: Multiple Round Trip Time Localization Scenario.

1.2.2 Cellular based Sensing

The sensing feature in cellular networks leverages existing infrastructure to enhance environmental perception and situational awareness. While traditionally designed for communication, cellular networks are now being explored for sensing applications, allowing for the detection of objects, tracking movements, and analyzing environmental conditions without needing additional hardware and frequency spectrum.

Sensing applications rely on estimating parameters such as signal strength, delay, doppler shift, and angle information, collectively known as sensing information from scattered and/or reflected radio frequency signals that are transmitted and received by gNBs or UEs. Sensing information can be obtained either from communication signals or from non-3GPP sensors like radar. Several works estimating the sensing information from communication signals, such as orthogonal frequency division multiplexing (OFDM) and orthogonal time frequency space (OTFS) waveforms, are discussed in [36, 37, 38, 39, 40]. Starting with Release-19, 3GPP began considering sensing capabilities in 5G NR cellular networks. They classified sensing systems into two types based on the relative positions of the transmitter and receiver. The first type features a collocated transmitter and receiver, while the second type comprises a separated transmitter and receiver [41].

Sensing systems can also be categorized based on the transmission source, whether the gNB or UE is transmitting. These are classified as downlink sensing and uplink sensing. If the sensing information is derived from the radio signals transmitted by the gNB, it is known as downlink sensing. Conversely, if the sensing information is derived from the radio signals transmitted by the UE, it is called uplink sensing. Depending on the number of gNBs involved, the transmission source (gNB or UE), and the location of the transmitter and receiver, various sensing modes can emerge, including mono-static mode, bi-static mode, and multi-static mode [42, 43], as shown in Figure 1.7.

In the mono-static mode, only downlink sensing is possible with a single gNB and a collocated transmitter and receiver operating in full-duplex mode as illustrated in Figure 1.8. However, this mode presents challenges, such as self-interference, that must be addressed. In contrast, both downlink and uplink sensing is possible in bi-static and multi-static modes. In bi-static mode for downlink sensing, two gNBs are required, where the transmitted signal from one gNB reaches the other gNB for sensing. In contrast, bi-static uplink sensing requires a single gNB and a UE, where the signal transmitted by the UE is received by the gNB for sensing. Illustrations of both bi-static downlink and uplink sensing scenarios are provided in Figures 1.9a and 1.9b, respectively. For multi-static downlink sensing, multiple gNBs are necessary, where a signal transmitted from one gNB is received by several other gNBs for sensing purposes. Multi-static uplink sensing involves multiple gNBs and a UE, where the signal transmitted by the UE is received by multiple gNBs to carry out sensing. These multi-static downlink and uplink sensing scenarios are also illustrated in Figures 1.10a and 1.10b, respectively. In all modes, the sensing information estimated at the gNBs is sent to the wireless sensing service as illustrated in Figures 1.8, 1.9 and 1.10, where object detection and tracking algorithms are applied to achieve environmental perception.

Furthermore, environmental perception and situational awareness achieved through sensing capabilities in cellular networks can improve connectivity. Several applications of sensing-aided communication utilize sensing information for channel estimation, beam prediction, and refinement. The works in [44, 45, 46, 47] use situational awareness for channel estimation, while the works in [48, 49, 50, 51, 52, 53, 54] use situational awareness for beam prediction and refinement.

In the next section, we discuss the impact of hardware impairments on localization and sensing.

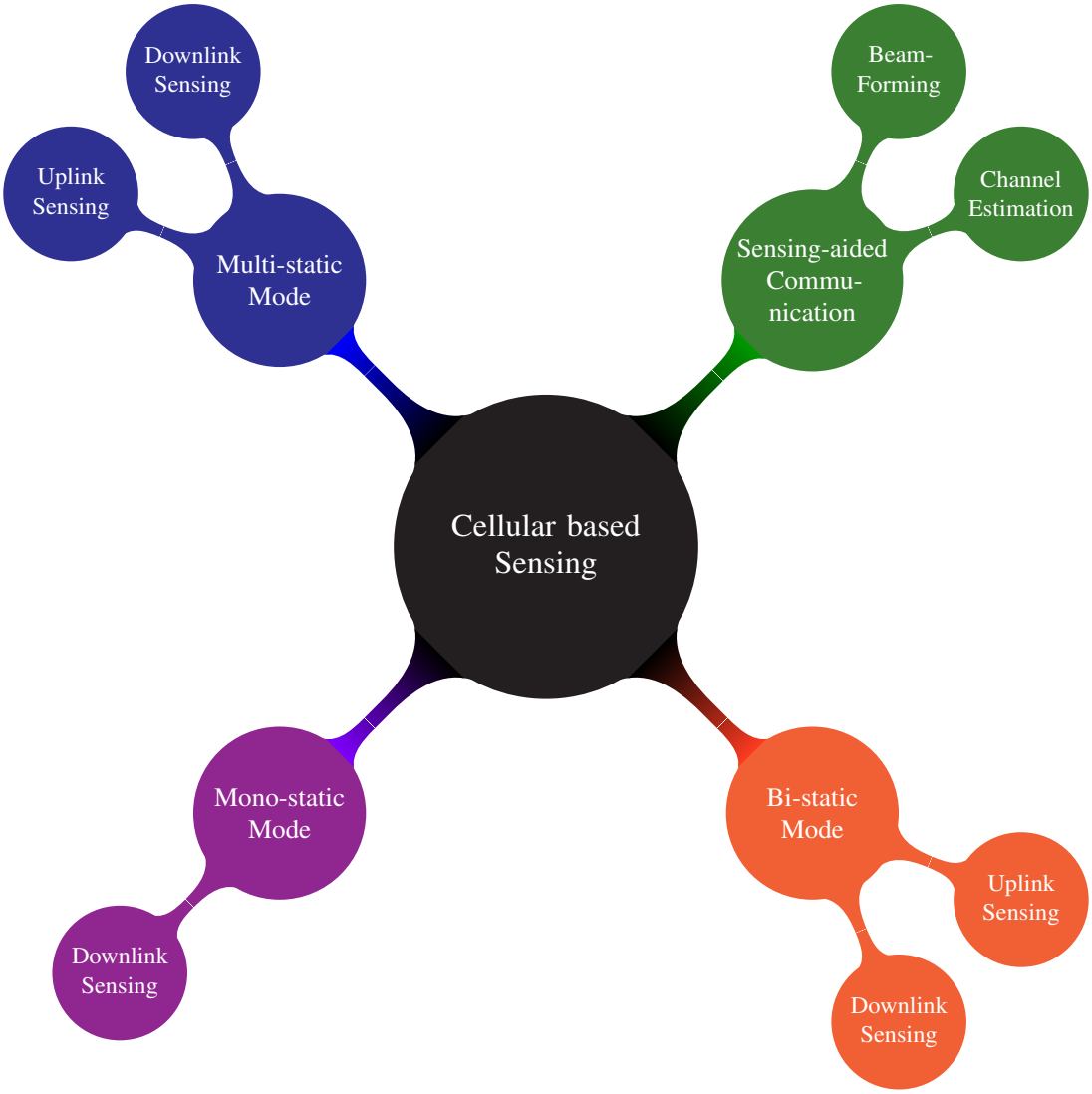


Figure 1.7: Characterization of various cellular based sensing techniques and its applications.

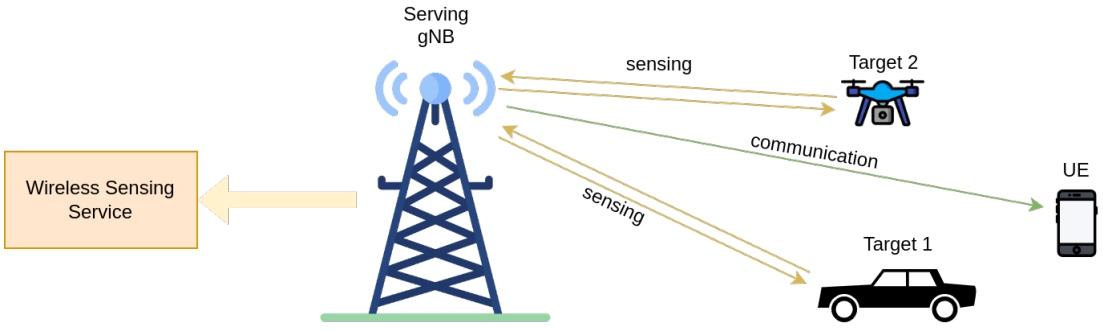
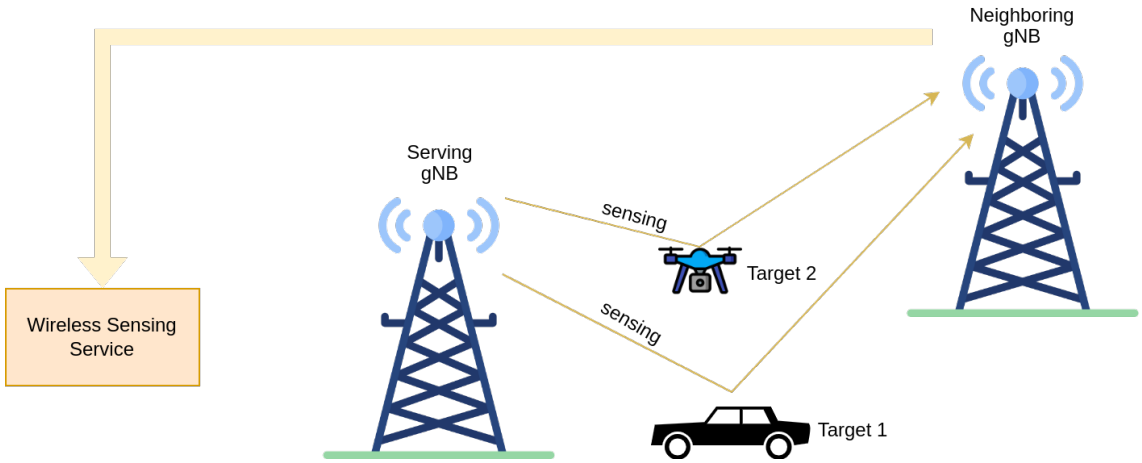
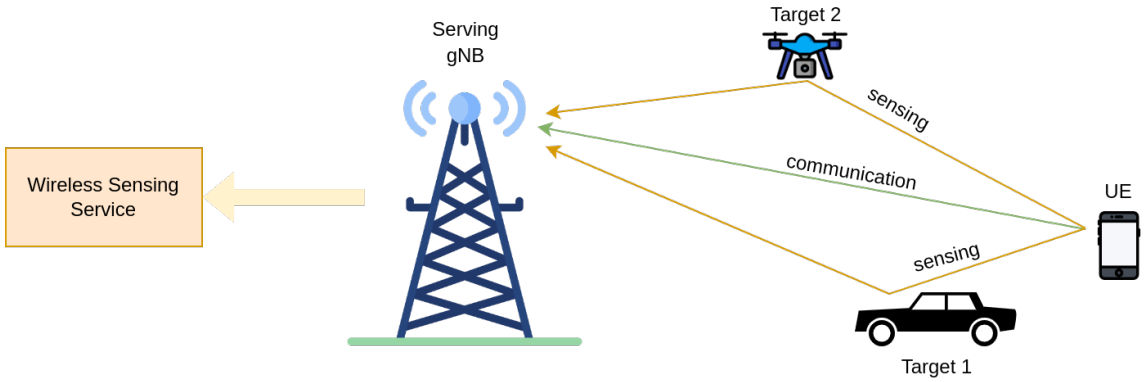


Figure 1.8: Mono-static Downlink Sensing Scenario.

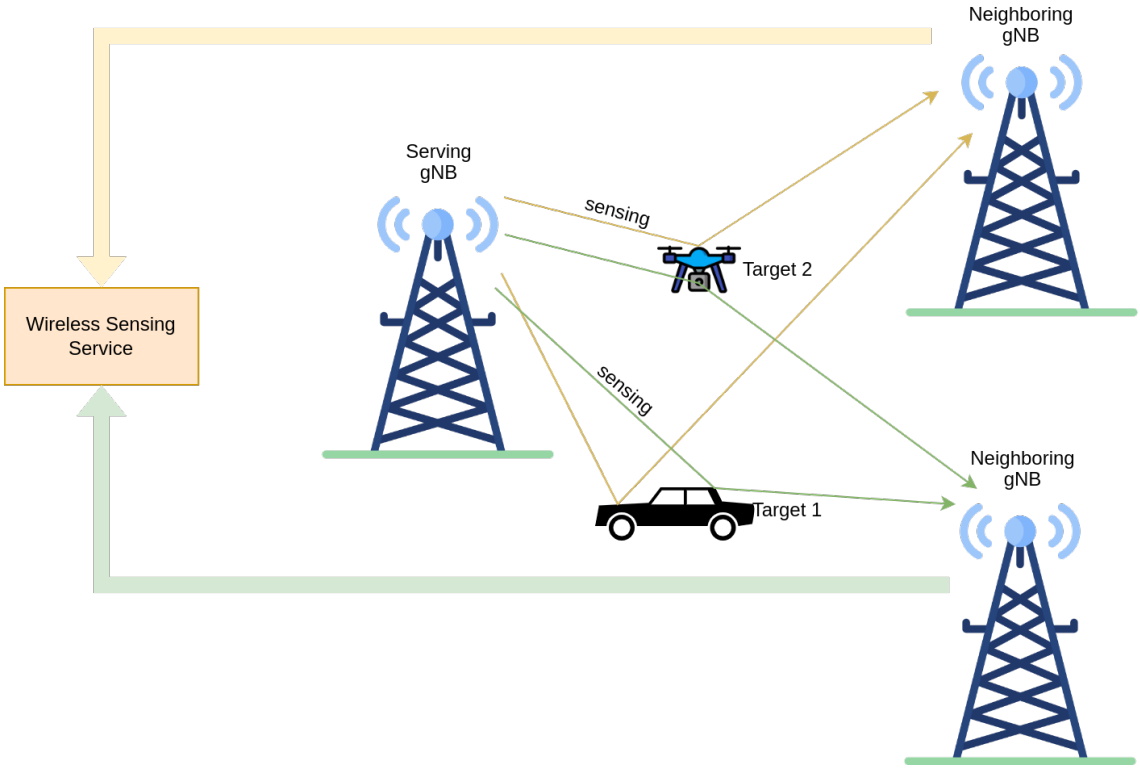


(a) Downlink Sensing Scenario

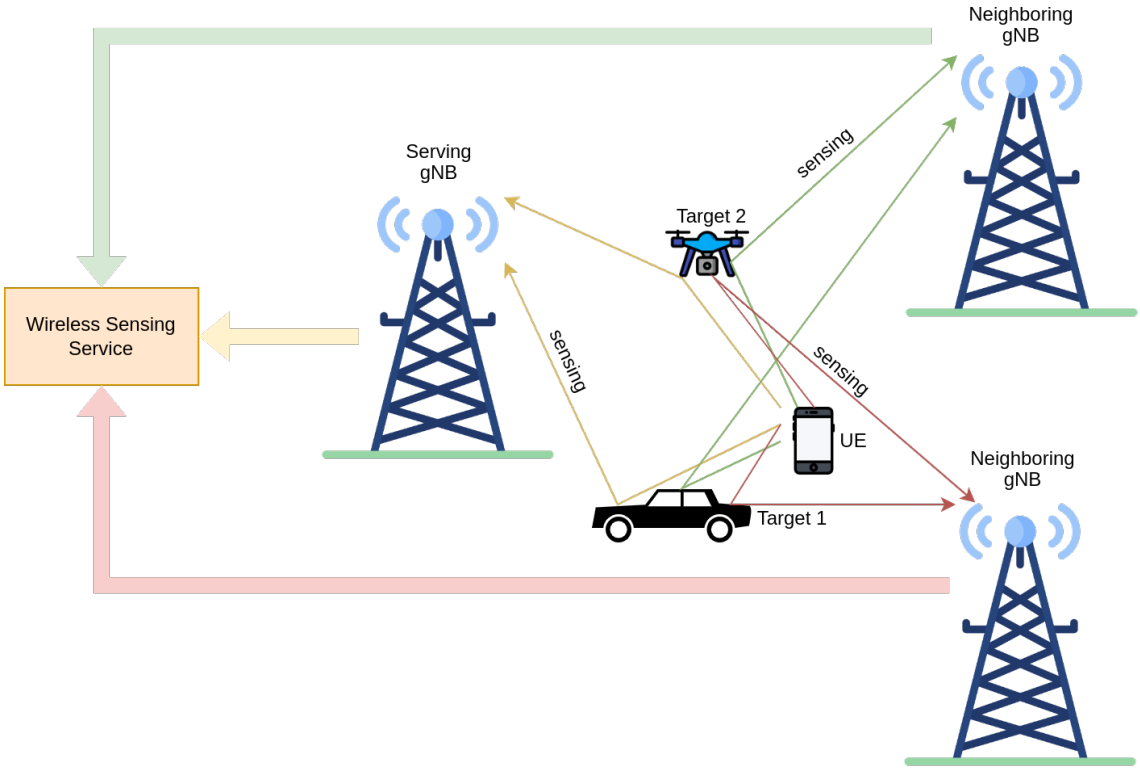


(b) Uplink Sensing Scenario

Figure 1.9: Bi-static Sensing Scenario.



(a) Downlink Sensing Scenario



(b) Uplink Sensing Scenario

Figure 1.10: Multi-static Sensing Scenario.

1.2.3 Localization and Sensing under Hardware Impairments

The localization and sensing performance of a cellular system relies on the accurate estimation of channel state information (CSI). In most prior works, evaluating the performance of localization and sensing algorithms was restricted to system-level simulations without hardware impairments. However, in practice, hardware impairments can significantly impact overall system performance, affecting the estimation of CSI. Common hardware impairments include clock drift, in-phase and quadrature-phase (IQ) imbalance, phase noise, and antenna array calibration [55].

In this dissertation, we focus on the clock drift among the hardware impairments. The clock drift occurs because the clocks on the gNB and UE run asynchronously, leading to drift over time. To address this issue, timing correction loops are incorporated into the cellular protocol stack to correct clock drift periodically. Since cellular systems were traditionally designed for communication purposes, the effect of clock drift and timing control loops is negligible on communication performance. However, the effect of clock drift and timing control loops are significant in the performance of the localization and sensing. These factors create variability in the delay estimates of the multipath components obtained from the CSI in different time slots. Therefore, even when the UE is static and the gNB has access to multiple channel measurements, the delay estimates of the multipath components vary over time. For example, the impact of clock drift and timing loops in 5G NR on the estimated distance by tracking the line-of-sight (LoS) component obtained from the uplink CSI over time with a commercial UE (Quectel RM500-GL) at a fixed location can be seen in Figure 1.11. Such variations of the delay estimates of the multipath components obtained from the CSI over time with a fixed distance between the gNB and UE are unreliable for localization and sensing purposes.

In this dissertation, we focus on designing a signaling mechanism in the 5G NR and beyond cellular networks that is robust to the effects of clock drift on the estimated uplink CSI used for localization and sensing purposes. Further, we discuss the outline of the dissertation.

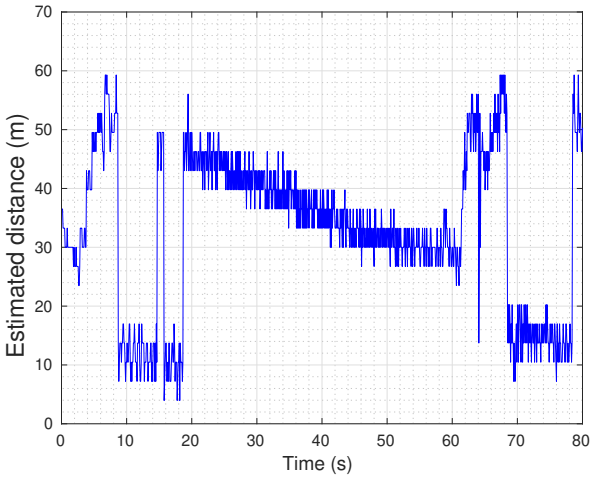


Figure 1.11: Effect of clock drift and timing loops on RTT in a commercial UE.

1.3 Outline of the Dissertation

The primary focus of this dissertation is to design a system that enhances positioning and sensing capabilities in 5G NR and beyond cellular networks. Precisely, we design a system and propose signaling schemes that allow us to obtain channel state information that is robust against clock drift and timing correction loops within a cellular system, which is essential for positioning and sensing. Furthermore, we evaluate the performance of these proposed schemes in real-time using OpenAirInterface. Additionally, we propose a system that leverages sensing information to improve the performance of the communication system. Specifically, we introduce a system framework that facilitates the fusion of sensing information into the communication system, thereby reducing the pilots in channel estimation. We also demonstrate the applications of the backhauls, including aerial integrated access and backhaul and a THz backhaul.

An outline of the dissertation along with a brief summary of the contributions of each chapter is provided below.

Chapter 2 - 5G New Radio using OpenAirInterface: Tools and Methodologies for Positioning

In this chapter, we present the essential background, tools, and methodologies to implement positioning schemes in 5G New Radio using OpenAirInterface.

The work in this chapter has resulted in the following publication:

- **Rakesh Mundlamuri**, Rajeev Gangula, Florian Kaltenberger and Raymond Knopp, "5G NR Positioning with OpenAirInterface: Tools and Methodologies", *IEEE Wireless On-demand Network systems and Services Conference (WONS)*, 2025.

Chapter 3 - Novel Round Trip Time Estimation in 5G NR and beyond

Most prior works assume that the CSI available in the uplink is robust to clock drift and the internal timing correction loops of a cellular system. However, in practice, the CSI is always prone to impairments like clock drift and internal timing loops, making most of the localization and sensing algorithms utilizing this CSI unreliable. Therefore, a natural question to ask is

- How do we obtain an uplink CSI that is robust to these impairments?

In this chapter, we propose various signaling schemes in a cellular system that enable us to obtain an uplink CSI robust to clock drift and internal timing correction loops. With this reliable uplink CSI, we can accurately determine the distance between the gNB and a UE, further enabling uplink sensing. Furthermore, we evaluate these schemes for distance estimation in real-time using OpenAirInterface.

The work in this chapter has resulted in the following publications:

- **Rakesh Mundlamuri**, Rajeev Gangula, Omid Esrafilian, Florian Kaltenberger, Raymond Knopp, David Gesbert, Sebastian Wagner, and Kien Le Trung, "System and a method for improved round trip time estimation", *EUROPEAN PATENT* 23306847.7, October, 2023.
- **Rakesh Mundlamuri**, Rajeev Gangula, Florian Kaltenberger and Raymond Knopp, "Novel Round Trip Time Estimation in 5G NR", *IEEE Global Communications Conference (GLOBECOM)*, 2024.
- **Rakesh Mundlamuri**, Rajeev Gangula, Florian Kaltenberger and Raymond Knopp, "Demo: Novel Round Trip Time Estimation in 5G NR", *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2024.
- Rajeev Gangula, Tommaso Melodia, **Rakesh Mundlamuri** and Florian Kaltenberger, "Round Trip Time Estimation Utilizing Cyclic Shift of Uplink Reference Signal", *IEEE International Conference on Communications (ICC)*, 2025.

Chapter 4 - Sensing aided Channel Estimation in Wideband MIMO Systems

In this chapter, we propose a framework that leverages sensing information available at the base station as side information to enhance the performance of the communication system in the uplink. Specifically, this approach aims to reduce the number of pilots required for channel estimation in the uplink. The proposed framework is robust to handle the errors present in the sensing information.

The work in this chapter has resulted in the following publication:

- **Rakesh Mundlamuri**, Rajeev Gangula, Christo Kurisummoottil Thomas, Florian Kaltenberger, and Walid Saad, "Sensing aided Channel Estimation in Wideband Millimeter-Wave MIMO Systems", *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2023.
- **Rakesh Mundlamuri**, Rajeev Gangula, Christo Kurisummoottil Thomas, Florian Kaltenberger, and Walid Saad, "Emulating Sensing aided Channel Estimation in Wideband MIMO Systems using OpenAirInterface", *to be submitted.*

Chapter 5 - Localization in a Digital Twin

In this chapter, we evaluate the performance of a signaling mechanism introduced in Chapter 3 in a digital twin platform known as the Colosseum. The goal is to demonstrate how the Colosseum can be utilized as a digital twin platform to evaluate the performance of localization algorithms, thereby eliminating the need to perform laborious outdoor measurement campaigns. We focus on addressing the performance gap between the results of the proposed signaling scheme obtained from an outdoor measurement campaign and those obtained from the digital twin representation of the same outdoor environment using the Colosseum.

The work in this chapter has resulted in the following publication:

- **Rakesh Mundlamuri**, Rajeev Gangula, Florian Kaltenberger, Raymond Knopp and Tommaso Melodia, "Colosseum as a Digital Twin platform for Round Trip Time Estimation in 5G NR and beyond", *to be submitted.*

Chapter 6 - Integrated Access and Backhaul

A wide range of localization and sensing applications arise from the mechanisms proposed in Chapter 3. One notable application is drone-based localization and sensing for SAR operations, where gNBs are installed on the drones. However, such applications require a backhaul connection to remain connected with the cellular network and to operate autonomously. In this chapter, we present the integrated access and backhaul systems in 5G NR and beyond that are crucial for enabling drone-based localization and sensing in SAR missions. Specifically, we demonstrate an open radio access network (O-RAN) based aerial integrated access and backhaul system and a terahertz (THz) backhaul system using OpenAirInterface.

The work in this chapter has resulted in the following publications:

- **Rakesh Mundlamuri**, Omid Esrafilian, Rajeev Gangula, Rohan Kharade, Cedric Roux, Florian Kaltenberger, Raymond Knopp, and David Gesbert, "Integrated Access and Backhaul in 5G with Aerial Distributed Unit using OpenAirInterface", demo, *17th ACM Workshop on Wireless Network Testbeds, Experimental evaluation and Characterization (WINTECH)*, 2023.
- **Rakesh Mundlamuri**, Sherif Badran, Rajeev Gangula, Florian Kaltenberger, Josep M. Jornet and Tommaso Melodia, "5G over Terahertz Using OpenAirInterface", *IEEE Wireless On-demand Network systems and Services Conference (WONS)*, 2024.

- Florian Kaltenberger, **Rakesh Mundlamuri**, Sherif Badran, Rajeev Gangula, Josep M. Jornet, and Tommaso Melodia, "In-lab experimental evaluation of 6G THz intersatellite communications", poster in, *ETSI Conference on Non-Terrestrial Networks, a Native Component of 6G*, 2024.

Chapter 7 - Conclusions

Finally, this chapter concludes the dissertation and discusses possible future research problems.

Other Research Contributions:

The other research contributions that I have made as a doctoral student but are not included in the dissertation are as follows:

Publications:

- Omid Esrafilian, **Rakesh Mundlamuri**, Florian Kaltenberger, Raymond Knopp and David Gesbert, "First Results on UAV-aided User Localization Using ToA and OpenAirInterface in 5G NR", *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2025.
- José A. del Peral-Rosado, Ali Yildirim, Auryn Soderin, **Rakesh Mundlamuri**, Florian Kaltenberger, et al, "Initial experimentation of a real-time 5G mmWave downlink positioning testbed", *European Navigation Conference (ENC)*, 2024.
- José A. del Peral-Rosado, Ali Yildirim, Susanne Schlötzer, Patric Nolle, Sara M. Razavi, Sagar Parsawar, **Rakesh Mundlamuri**, Florian Kaltenberger, et al, "First field trial results of hybrid positioning with dedicated 5G terrestrial and UAV-based non-terrestrial networks", *36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, 2023.
- José A. del Peral-Rosado, Ali Yildirim, Nils Klinger, Patric Nolle, Sara M. Razav, Sagar Parsawar, **Rakesh Mundlamuri**, Florian Kaltenberger and et al, "Preliminary field results of a dedicated 5G positioning network for enhanced hybrid positioning", *European Navigation Conference (ENC)*, 2023.
- José A. del Peral-Rosado, Patric Nolle, Fabian Rothmaier, Sara M. Razavi, Gustav Lindmark, Xiaolin Jiang, Deep Shrestha, Fredrik Gunnarsson, Sagar Parsawar, **Rakesh Mundlamuri**, Florian Kaltenberger and et al, "Proof-of-concept of dedicated aerial 5G and GNSS testbed for enhanced hybrid positioning", *35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, 2022.

Demonstrations:

- Autonomous UAV-aided User Localization Using ToA and OpenAirInterface in 5G NR Systems ↗, *ICC Workshops*, 2024
- Connected Robotics Part I: Control and monitor a UAV over 5G networks ↗, 2023
- Integrated Access and Backhaul in 5G with Aerial Distributed Unit using OpenAirInterface ↗, *ACM WINTECH*, 2023
- Autonomous Aerial 5G Relaying ↗, 2023

Chapter 2

5G New Radio using OpenAirInterface: Tools and Methodologies for Positioning

This chapter describes the tools and methodologies to prototype 5G NR positioning algorithms using OpenAirInterface (OAI).

2.1 Introduction

Despite the standardization of positioning methods in 5G NR, their performance evaluation is relatively limited to system-level simulations or a few proprietary real-world experimental evaluations [56, 57]. On the other hand, open-source 5G platforms such as OAI [58] and srsRAN [59] are playing a crucial role in experimental research. The ability to run the 5G protocol stack on general-purpose computing platforms paired with software-defined radios (SDRs) makes them an attractive tool for researchers and prototype developers.

Few works have demonstrated the timing-based positioning techniques in real-world experiments using the OAI platform [25, 27, 26, 30, 60, 61, 62, 63]. For instance, the works [25, 27, 26] demonstrated DL-TDOA-based positioning using PRS, and the works [30, 61] have demonstrated UL-TDoA-based positioning using SRS. E-CID-based positioning using a random access channel has also been demonstrated in [60]. Finally, a new RTT scheme has been proposed in [62, 63]. These methods are shown to be robust to clock drift and has reduced latency in estimating the RTT compared to the existing schemes in the standards.

All these works [25, 27, 26, 30, 60, 62, 63], however, lack a comprehensive documentation on the implementation details of the positioning methods within the OAI framework. The authors in [61] have attempted to address this issue by providing a detailed explanation of the positioning procedures implemented at the protocol level in OAI and a tutorial for performing positioning within the framework. However, detailed physical layer implementation aspects, such as fixed-point representation and device calibration, which are crucial for prototyping positioning schemes, are missing. For a researcher trying to develop positioning prototypes, navigating through a vast open-source codebase like OAI, understanding the reference signal implementation, calculating metrics such as signal-to-noise ratio (SNR), and calibrating the hardware might be daunting. Furthermore, tools to extract required data from OAI without affecting the system's performance are crucial in prototype development.

In this chapter, we provide a comprehensive guide on the physical layer implementation aspects and present the key functions related to the positioning in OAI. Specifically, our contributions in this chapter are as follows:

- Introduce OAI components and its operating modes.

- Present the essential functions specific to the reference signals relevant for positioning in OAI.
- Describe the physical layer implementation aspects in OAI.
- Present the `T_tracer` tool in OAI to extract the required data.

The rest of the chapter is organized as follows: Section 2.2 provides necessary background to OAI, detailing its components and various operating modes. This section also reviews the reference signals and concepts relevant to 5G positioning in OAI. In Section 2.3, we describe the physical layer implementation aspects in OAI. Section 2.4 introduces a data extraction tool in OAI. Finally, Section 2.5 concludes the chapter.

2.2 Background

This section provides an overview of the various components of OAI software, its operating modes, reference signals that are relevant to 5G positioning and radio resource control (RRC) connectivity states of a UE.

2.2.1 OpenAirInterface 5G NR Components

OpenAirInterface (OAI) is an open-source initiative that provides a reference implementation of a 5G gNB, user equipment (nrUE), and a 5GC network compliant with the 3GPP Release-15 and above. OAI operates on standard x86 computing hardware and utilizes commercial off-the-shelf (COTS) SDR cards, such as the universal software radio peripheral (USRP) and O-RAN radios. This setup allows the users to establish a end-to-end 3GPP compliant 5G network and interoperate with the commercial equipment. This strategy not only reduces implementation costs but also improves deployment flexibility. Detailed functionalities of each of the components in the OAI 5G stack are described as follows,

2.2.1.1 5G Core Network

The 5G core (5GC) network performs several essential functions, including authentication, mobility management, network slicing, and service orchestration. Each of these functions is managed by distinct network functions. The network functions supported by OAI 5GC are:

- Access and mobility management function (AMF)
- User plane function (UPF)
- Network repository function (NRF)
- Session management function (SMF)
- Unified data management (UDM)
- Unified data repository (UDR)
- Authentication server function (AUSF)
- Network slice selection function (NSSF)
- Location management function (LMF)

Furthermore, OAI offers container-based deployments of these network functions [64]. The 5GC component essential for positioning in 5G NR is the LMF. OAI supports the LMF with NRPPa support. A detailed implementation of the LMF and its tutorial can be found in [65].

2.2.1.2 5G NR Base-station

The 5G NR base-station (gNB) can be deployed in two ways: as a monolithic gNB or as a split architecture consisting of a centralized unit (CU) and a distributed unit (DU) connected via the F1 interface. The CU can be further divided into two components: CU control plane (CU-CP) and CU user plane (CU-UP) connected over the E1 interface. The CU-CP includes RRC and control plane packet data convergence protocol (PDCP-C), while CU-UP comprises service data adaption protocol (SDAP) and user plane packet data convergence protocol (PDCP-U). The DU implements the radio link control (RLC), medium access control (MAC), and physical (PHY) layers.

The PHY layer of the 5G NR utilizes OFDM waveform for transmission over the air, structured in a frame format. This frame structure, as defined by 3GPP, is presented in both the time and frequency domain as follows: A 5G NR frame in the time domain has a duration of 10 milliseconds (ms) and is divided into 10 subframes, each lasting 1 ms. Furthermore, each subframe is divided into $N_{Slot}^{Subframe}$ slots, depending on the subcarrier spacing (SCS) used. Each slot comprises of 14 OFDM symbols. The number of slots per subframe $N_{Slot}^{Subframe}$, for different SCS is detailed in Table 2.1.

In the frequency domain, the 5G NR frame structure offers various bandwidth configurations based on the SCS used. Each bandwidth configuration includes N_{RB} resource blocks (RBs), with each RB consisting of $N_{SC}^{RB} = 12$ subcarriers referred to as resource elements (REs). For a given frequency range (FR) and a specific SCS in kilohertz (KHz), the number of RBs N_{RB} of a possible bandwidth configuration from 5 MHz to 400 MHz is detailed in the Table 2.2. An illustration of time and frequency domain frame structure can be seen in Figure 2.1.

Table 2.1: Number of slots per subframe for a given SCS

SCS	$N_{Slot}^{Subframe}$
15 KHz	1
30 KHz	2
60 KHz	4
120 KHz	8
240 KHz	16

Table 2.2: Number of resource blocks (N_{RB}) for a bandwidth configuration in 5G NR

FR	SCS (KHz)	5	10	15	20	25	30	40	50	60	70	80	90	100	200	400
1	15	25	52	79	106	133	160	216	270							
1	30	11	24	38	51	65	78	106	133	162	189	217	245	273		
1	60		11	18	24	31	38	51	65	79	93	107	121	135		
2	60								66					132	264	
2	120								32					66	132	264

However, the support of SCS in OAI gNB is limited to 15 KHz, 30 KHz in FR1, and 120 KHz in FR2. The supported bandwidths in FR1 are 10, 20, 40, 50, 60, 80, and 100 MHz, while the supported bandwidths in FR2 are 50, 100 and 200 MHz. The OAI 5G NR PHY supports all physical channels and signals according to the 3GPP Release-15. Specifically for positioning purposes, it supports channel state information reference signal (CSI-RS), PRS in the downlink, and a SRS in the uplink.

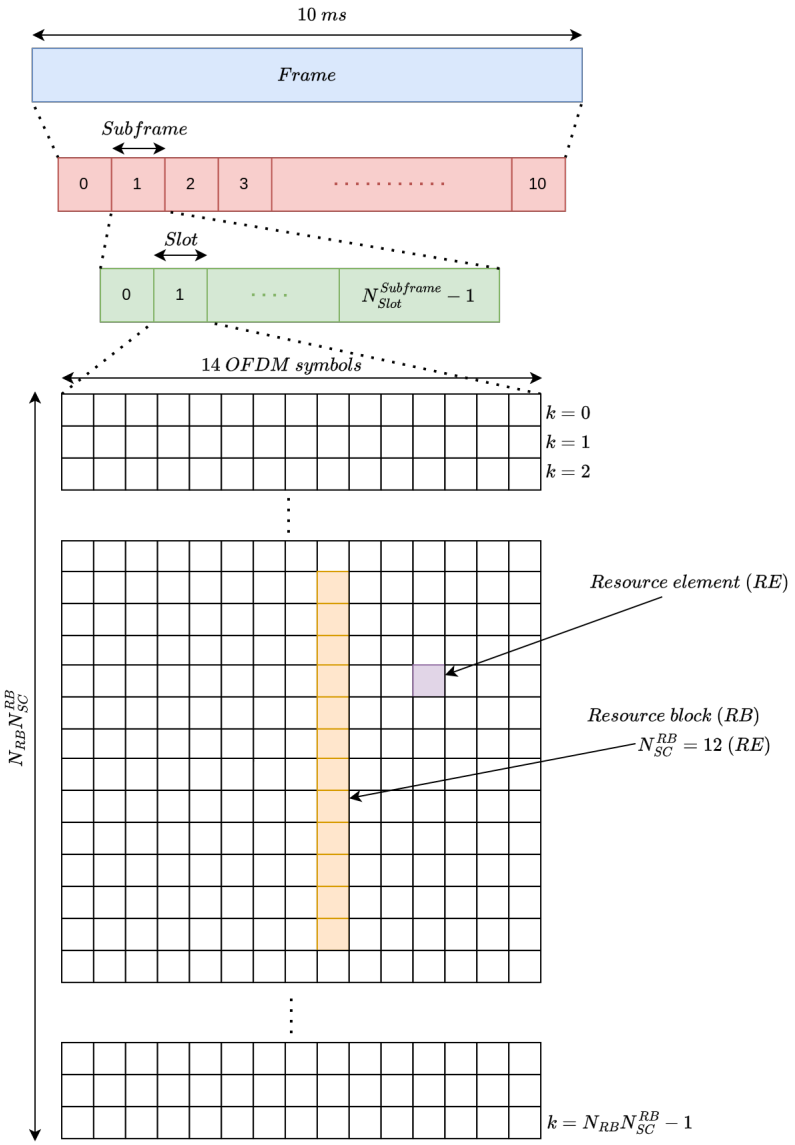


Figure 2.1: 5G OFDM resource grid.

Further, the fronthaul splits supported in OAI gNB are as follows: split 8 using COTS SDR cards, such as the USRP, as well as O-RAN split 7.2, which has been tested with different O-RAN compatible radio units (RUs). Moreover, OAI also supports the O-RAN E2 interface to the near real-time RAN intelligent controller (RIC) and the O1 interface to the service management and orchestration (SMO) framework. The interfaces supported by OAI 5G RAN are shown in Fig. 2.2.

2.2.1.3 User Equipment

The user equipment in OAI referred to as nrUE is a real-time experimentation platform that implements the functionalities of a 3GPP-compliant UE as open-source software running on standard x86 general computing hardware. It utilizes commercial software-defined radios, such as USRP, for transmission and reception. OAI nrUE works with OAI gNB and OAI 5GC, offering end-to-end functionality from the radio access network (RAN) to the Core. The availability of the source code enables developers and

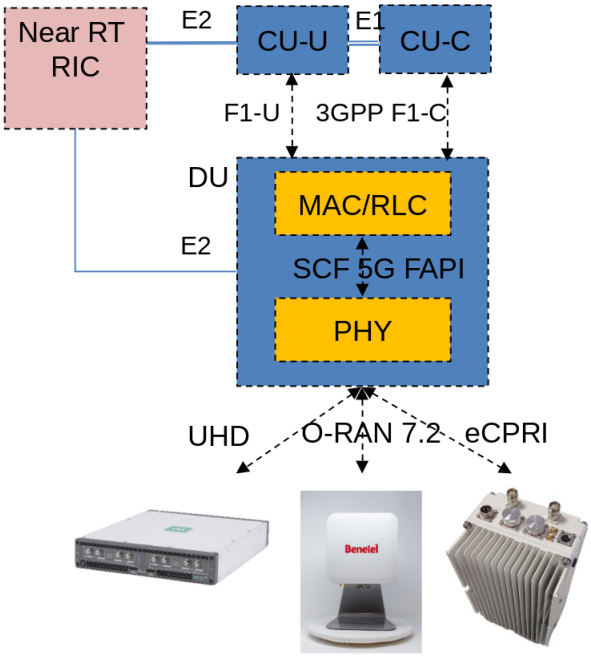


Figure 2.2: OAI 5G-NR Radio Access Network.

researchers to develop and verify various 5G NR features as well as non-compliant features in real time, including novel positioning algorithms.

2.2.1.4 Operating Modes

To support the development, debugging and real-time experimentation process, OAI supports several modes of operation. Specifically, the following two modes are widely used in over-the-air experiments and are illustrated in Figure 2.3.

- The `sa` mode enables the establishment of an end-to-end 5G network in standalone mode. Either a nrUE or a COTS UE can connect to the OAI 5G network.
- The `phy-test` mode, on the other hand, is designed specifically for testing the physical layer of the gNB and nrUE by abstracting the higher layers.

Using the `phy-test`, the developers and researchers can test and validate physical layer implementations and algorithms without worrying about the higher layer procedures. The upper layer abstraction is achieved by sharing a configuration file containing higher layer parameters between the gNB and nrUE. The instructions to setup these modes are described in [66].

Additionally, both the `sa` and `phy-test` modes can be run using `rfsim` mode. In this mode, the over-the-air transmission between the gNB and nrUE is simulated by sending the time-domain OFDM waveform through a socket, which abstracts the hardware for end-to-end testing. The instructions to operate in this modes is described in [67].

Further, the key reference signals utilized for positioning in 5G are discussed below.

2.2.2 Reference Signals

The widely used reference signals for positioning in 5G NR are as follows:

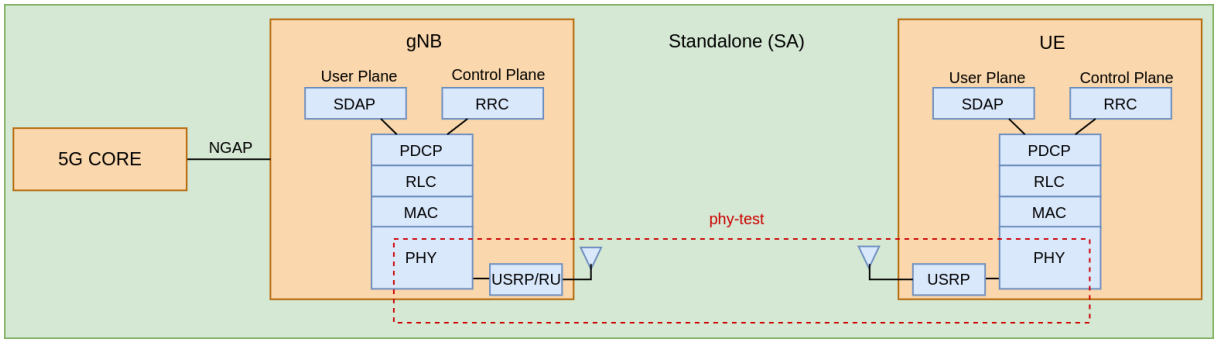


Figure 2.3: OAI Components and Operating modes.

2.2.2.1 Zadoff-chu Sequence

Zadoff-chu (ZC) sequences are widely used as a base sequence for many reference signals in 5G NR due to a number of desirable properties. A ZC sequence of length N_{ZC}, which must be an odd number, and root $q \in [1,2,\ldots,N_{ZC}-1]$ is defined as

$$x_q[n] = \exp\left(-j\frac{\pi q n(n+1)}{N_{ZC}}\right), 0 \le n \le N_{ZC}-1. \tag{2.1}$$

Some key properties of the ZC sequences are given below.

- All the elements in a ZC sequence have unit amplitude.
- Normalized cyclic auto-correlation: When the root q is relatively prime to N_{ZC},

$$\frac{1}{N_{ZC}}\sum_{n=0}^{N_{ZC}-1} x_q[n]x_q^*[(n+v)\mathrm{mod}N_{ZC}] = \delta[v], \tag{2.2}$$

  where mod represent the modulo operation and $\delta[v]$ represents the Kronecker delta function. There are N_{ZC} unique cyclic shifts of the sequence $x_q[n]$.
- Normalized cyclic cross-correlation: when $|q_1 - q_2|$ and N_{ZC} are relatively prime,

$$\frac{1}{N_{ZC}}\sum_{n=0}^{N_{ZC}-1} x_{q_1}[n]x_{q_2}^*[(n+v)\mathrm{mod}N_{ZC}] = \frac{1}{\sqrt{N_{ZC}}}. \tag{2.3}$$

- The discrete Fourier transform (DFT) (or its inverse) of a ZC sequence is also a ZC sequence.

2.2.2.2 Synchronization Signal Block

The synchronization signal block (SSB) is used for downlink time and frequency synchronization in a 5G network. The gNB periodically broadcasts the SSB, and when a 5G UE is switched on, it searches for SSB to synchronize its time and frequency in the downlink. The SSB consists of a primary synchronization signal (PSS), a secondary synchronization signal (SSS), and a physical broadcast channel (PBCH).

- The PSS helps the UE to identify the gNB.
- The SSS provides additional information that assists in precise timing and further gNB identification.
- The PBCH carries a master information block (MIB), which provides gNB information and is needed to decode the system information block (SIB) to initiate uplink synchronization.

The 5G SSB occupies in 4 OFDM symbols and 240 subcarriers. Multiple SSBs are transmitted periodically in a process known as the SSB burst. The number of SSBs and the periodicity of the SSBs in a SSB burst depend on specific options categorized as Case A, Case B, Case C, Case D, and Case E, which are determined by the subcarrier spacing and operating frequency. OAI supports all these options. Functions 1 and 2 in Table 2.3 provide implementation details related to SSB generation and reception.

2.2.2.3 Random Access Channel

The random access channel (RACH) is used for uplink synchronization. While the UE initiates the RA procedure for initial access, the gNB can order the UE to initiate an RA procedure in the event of loss of UL synchronization. By detecting the RACH preamble, the gNB can infer a coarse RTT between the gNB and UE. The RACH signal is generated using the ZC base sequence. Depending on the sequence length and repetitions, several formats are defined in 5G. The supported Formats in OAI are: 0, 1, 2, 3, A1, A2, A3, B1, B2, B3. The functions 3-6 in Table 2.3 provide the implementation details in OAI.

2.2.2.4 Positioning Reference Signal

3GPP has introduced the PRS specifically for localization purposes in the DL[68]. These reference signals were introduced in 4G and extended to 5G with better resolution and accuracy. PRS is generated using quadrature phase shift keying (QPSK) modulated 31-length gold sequence and can be flexibly arranged in any number of physical resource blocks in the frequency domain. In the time domain, the PRS resources can span {2,4,6,12} consecutive OFDM symbols. However, When it comes to OAI implementation, PRS feature is currently limited to `phy-test` mode usage as higher layer procedures supporting PRS are yet to be implemented. Functions 7 and 8 in Table 2.3 provide implementation details of the PRS. Detailed instructions for configuring and running the PRS can be found in [69].

2.2.2.5 Sounding Reference Signal

SRS is a wideband reference signal transmitted by the UE in the UL for channel estimation and positioning purposes. SRS is generated using the ZC sequence and has good auto and cross-correlation properties. Dedicated SRS for positioning is introduced in 3GPP Release-11. Although SRS for positioning and communication have a lot of commonalities, they can be configured separately [5]. SRS can be flexibly arranged in the frequency domain based on a few radio resource control parameters. In the time domain, the SRS resources can span {1,2,4} consecutive OFDM symbols. SRS can be configured to transmit periodically or aperiodically. Currently, OAI supports periodic SRS configuration and can be operated in both `sa` and `phy-test` mode. Functions 9-12 in Table 2.3 implements the SRS procedures in OAI.

2.2.3 5G Synchronization

Synchronization between gNB and UE is essential for reliable communication as well as positioning. The 5G synchronization process consists of DL and UL synchronization. The UE can detect symbol and frame boundary during the DL synchronization using SSB. Once DL is synchronized, the UE extracts configuration parameters by decoding the MIB) from the PBCH and later the SIB from the physical downlink shared channel (PDSCH). These parameters provide the necessary information to perform UL synchronization.

The UL synchronization enables UE to determine the exact time to send the UL data. Since a gNB serves multiple UEs located across the cell, the UL transmission times of the UEs need to be adjusted such that their reception is aligned with the gNB's UL reception. This is achieved with a RA procedure. The UL synchronization is as follows:

Table 2.3: Implementation details of the Reference signals in OAI

Function	Description
1. `nr_common_signal_procedures()`	SSB generation
2. `nr_initial_sync()`	Initiates SSB RX procedures
3. `nr_ue_prach_procedures()`	Initiates RACH TX procedures
4. `generate_nr_prach()`	Generates the RACH sequence
5. `L1_nr_prach_procedures()`	Initiates RACH RX procedures
6. `rx_nr_prach()`	RACH preamble detection
7. `nr_generate_prs()`	PRS sequence generation
8. `nr_prs_channel_estimation()`	PRS channel, RToA estimation
9. `ue_srs_procedures_nr()`	Initiates SRS TX procedures
10. `generate_srs_nr()`	Generates SRS sequence
11. `nr_srs_channel_estimation()`	SRS channel, RToA estimation
12. `configure_periodic_srs()`	Configure periodic SRS

- Either the UE initiates (in the case of initial access), or the gNB orders the UE (in case of loss of UL synchronization) to initiate the RA procedure through the physical random access channel (PRACH). While it is contention based RA in the former scenario, in the latter, it can be contention free, i.e., the gNB may configure the UE with a dedicated PRACH preamble.
- Based on the delay estimated from the PRACH, the gNB can measure a coarse/quantized RTT. This coarse/quantized version of RTT coined as timing advance (TA), is then sent to the UE via the random access response (RAR).
- Although the initial TA is sent via the RAR, gNB can periodically send updated UL timing corrections to the UE via TA commands. Through these TA commands, gNB can maintain the UL synchronization in case of UE mobility or clock drift.

The signaling procedure of RA and TA updates is depicted in Figures 2.4 and 2.5. An illustration of the UE timing correction using TA can be seen in Figure 2.6.

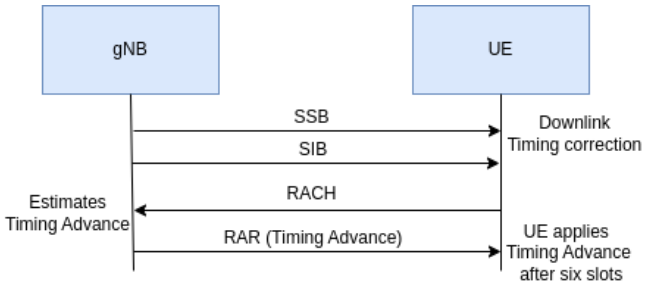


Figure 2.4: Synchronization procedure in 5G NR.

2.2.4 5G Radio Resource Control states

The RRC states represent the connectivity states of a UE. The three possible RRC states defined for a UE in 5G standalone mode are: NR_RRC_IDLE, NR_RRC_INACTIVE, and NR_RRC_CONNECTED. While the NR_RRC_CONNECTED indicates an active data transmission/reception, the UE in NR_RRC_IDLE and NR_RRC_INACTIVE stays asleep most of the time and periodically wakes up and looks for paging

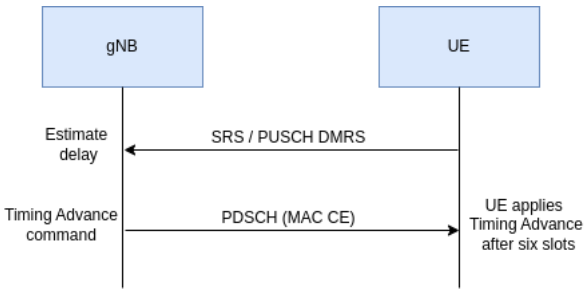


Figure 2.5: UE UL timing correction with Timing advance commands.

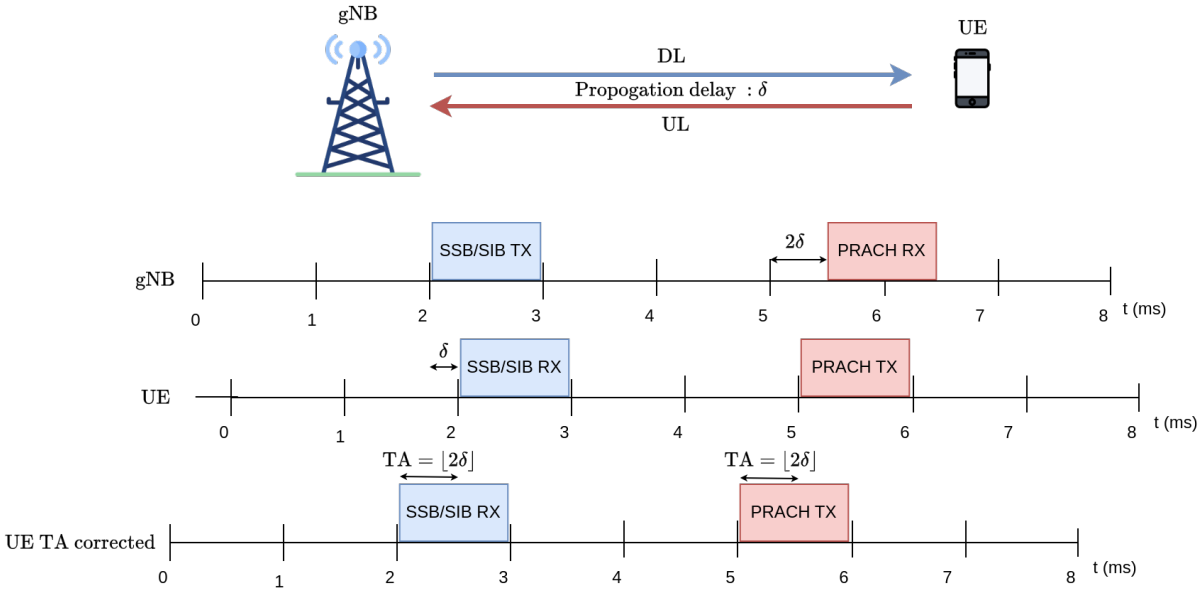


Figure 2.6: Illustration of a UE UL timing correction in 5G NR.

messages to look for active data (e.g., incoming voice call or data) and switches to NR_RRC_CONNECTED state. Contrary to the NR_RRC_IDLE mode, in NR_RRC_INACTIVE state, the gNB stores the UE context (e.g., RRC configuration) for periodic transmissions. It is to be noted that until 3GPP Release-16, majority of the current 5G positioning techniques that offer good accuracy work only when the UE is NR_RRC_CONNECTED. 3GPP Release-17 introduces NR_RRC_INACTIVE based positioning for low power high accuracy positioning (LPHAP) [70] for low power devices. The design requirements for the LPHAP include low power consumption, low complexity, low signaling overhead, and timing alignment to avoid interference with other UEs[71]. Further, in the next section, we describe the baseband representation of the reference signals in OAI.

2.3 OAI Physical Layer

Let us consider a scenario where a single antenna OAI transmitter (TX) communicating with a single antenna receiver (RX) using 5G NR protocol stack as shown in Figure 2.7. This models both the UL and DL communication scenarios. For example, when the TX is a gNB and the RX is a nrUE, it represents the

DL scenario. The received signal $y[k]$ at the RX on the k-th, $k \in [0, K-1]$, RE is represented as,

$$y[k] = h[k]x[k] + n[k], \tag{2.4}$$

where, K is the total number of REs, $h[k]$ represents the baseband propagation channel, $x[k]$ denotes the transmitted symbol and $n[k]$ is additive white Gaussian noise. We now present the fixed-point format used in OAI to represent these signals. This knowledge is crucial in OAI-based positioning experiments and system design.

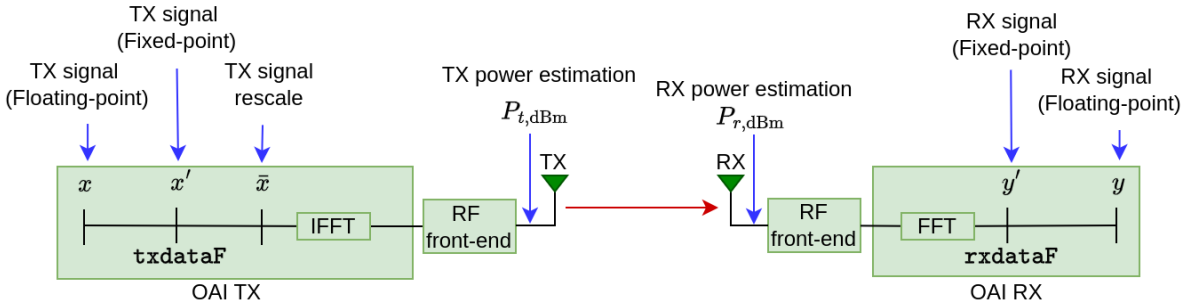


Figure 2.7: Transmission and Reception chain baseband representation in OAI.

2.3.1 Baseband Signal Representation

The frequency domain IQ samples at the TX are stored in a contiguous memory buffer `txdataF` as

$$\texttt{txdataF} = [\mathrm{I}_0\mathrm{Q}_0\mathrm{I}_1\mathrm{Q}_1 \ldots \mathrm{I}_{K-1}\mathrm{Q}_{K-1}], \tag{2.5}$$

where I_k and Q_k represent the in-phase and quadrature-phase components of the k-th RE, $k \in [0, K-1]$. Each I_k and Q_k are stored in 16 bits using signed Q1.15 format or in short Q15 format. The generated baseband signals are normalized such that their values lie between [-1,1) and then converted to fixed-point using Q15 format. The relation between $x[k]$ (floating-point) and $x'[k]$ (fixed-point) is given by

$$x'[k] = \left\lfloor x[k] \times 2^{15} \right\rfloor, \; x[k] = \frac{x'[k]}{2^{15}}, \tag{2.6}$$

where, $\lfloor . \rfloor$ represent the floor operation and $x'[k]$'s are stored in 2's complement form.

The signal $x'[k]$ is then rescaled before sending it to the inverse fast Fourier transform (IFFT) block to get the time-domain samples. The need for rescaling stems from two factors a) digital-to-analog conversion (DAC)/analog-to-digital conversion (ADC) resolution of the radio frequency (RF) fronted module b) the dynamic range of the IFFT block. Different RF front end modules such as USRP and various ORAN 7.2 split RUs (VVDN, LiteON, Benetel) are supported by the OAI gNB. The fixed-point baseband signal $x'[k]$ is scaled as

$$\bar{x}[k] = \left\lfloor \frac{\mathrm{A} \times x'[k]}{2^{15}} \right\rfloor, \tag{2.7}$$

where, A is a design parameter based on decibels relative to full scale (dBFS).

2.3.2 Decibels relative to Full Scale

Decibels relative to full scale (dBFS) is a unit of measure for the amplitude levels in digital systems [72]. In a Q15 fixed-point format, the maximum represented level $\mathrm{A}_{\max} = 2^{15}$. To convert a level A into dBFS

scale, we use the following formula

$$A_{dBFS} = 20\log_{10}\left(\frac{A}{A_{max}}\right). \tag{2.8}$$

The choice of A_{dBFS} depends on the device and signal characteristics and is configurable using the parameter `tx_amp_backoff_dB` in the configuration file in OAI. The value of A and A_{dBFS} for a USRP and an O-RAN 7.2 VVDN RU in OAI are mentioned in Table 2.4.

Table 2.4: Device specific IQ bit representation in OAI

Device	A_{dBFS}	A	Bits
USRP B210	-36	519	9
O-RAN 7.2 split VVDN RU	-12	8231	13

In the case of USRP B210, the choice of A_{dBFS} arises from two factors: 1. 12-bit ADC/DAC in USRP and 2. Input to the IFFT block is scaled down by 3 bits to guard against possible signal saturation during IFFT. On the other hand, the RU manufacturer mentions the A_{dBFS} in the device specifications.

We now shed light on estimating the transmit, receive powers per RE in digital and analog domains using the fixed-point tools. This is essential in calculating the link-budget, signal strength and SNR in OAI-based positioning experiments.

2.3.3 Transmit and Receive Power

Let the reference signal transmitted be denoted by $x'[k], k \in \mathcal{S}$, where $\mathcal{S}$ is the set of REs where the signal is mapped, and $|\mathcal{S}| = N$. The average power per RE is calculated as

$$P_t = \frac{1}{N}\sum_{k\in\mathcal{S}} |x'[k]|^2, \tag{2.9}$$

The power is then converted to dBm using

$$P_{t,\text{dBm}} = 10\log_{10}(P_t) - 10\log_{10}((2^{15})^2) + 30 + G_t + G_t^c, \tag{2.10}$$

where, the term $(2^{15})^2$ arises from the conversion from Q15, 30 appears due to the conversion of dBw to dBm, G_t and G_t^c are the transmit gain and calibration offset of a device respectively.

The received power per RE in Q15 can be estimated from the received signal as

$$P_r = \frac{1}{N}\sum_{k\in\mathcal{S}} |y'[k]|^2. \tag{2.11}$$

Further, P_r in dBm at the receiver antenna port can be obtained by,

$$P_{r,\text{dBm}} = 10\log_{10}(P_r) - 10\log_{10}((2^{15})^2) + 30 - G_r + G_r^c \tag{2.12}$$

where, G_r is the receive gain and G_r^c is the calibration offset. Note that the calibration values G_t^c, G_r^c are obtained by varying the gains G_t, G_r and measuring with a spectrum analyzer, and they vary from device to device.

2.3.4 SNR Estimation

In the computation of received SNR in an OFDM system, the received signal power P_r, a combination of both signal and noise power per RE is obtained from (2.11). The received SNR on a RE is obtained by,

$$\text{SNR} = \frac{P_r - P_n}{P_n}. \tag{2.13}$$

The noise power P_n is estimated similar to (2.11) from empty REs where no signal is present.

2.4 Data Extraction

This section presents the data collection procedure using the `T_tracer` tool in OAI. It provides an example of extracting the SRS channel estimates using the tool, but the procedure is similar for any signal.

The SRS frequency domain channel estimates of length K, estimated using least squares are stored in a variable named `srs_estimated_channel_freq[][][]` in the function `nr_srs_channel_estimation()`. The variable is a three dimensional array, with rx antenna index as a first dimension, tx antenna index as a second dimension and subcarrier index in the third dimension. Using the `T_tracer` tool, data from any variable can be stored over time in a file without effecting the real-time performance of the OAI gNB and UE. The use of `T_tracer` for data collection is as follows,

- Define an `ID` in the `T_messages.txt` file, for example, `GNB_PHY_UL_FREQ_CHANNEL_ESTIMATE` as shown in Listing 2.1.
- Use the `ID` in the code as `T_ID` and fill the function with appropriate variables as shown in Listing 2.2.
- Compile the `T_tracer` and gNB as described in [73].
- Run gNB using an additional argument `--T_stdout 2`.
- Parallel to running the gNB, in an another terminal, run `record` executable to record the data using the `ID` as shown in Listing 2.3.
- After recording the data, the channel estimates from the file `channel_frequency.raw` can be extracted using the variable `chest_f` as defined in Listing 2.1 and `extract` executable as as shown in Listing 2.4.

```
ID = GNB_PHY_UL_FREQ_CHANNEL_ESTIMATE
    DESC = gNodeB channel estimation in the frequency domain
    GROUP = ALL:PHY:GRAPHIC:HEAVY:GNB
    FORMAT = int,gNB_ID : int,rnti : int,frame : buffer,chest_f
```

Listing 2.1: Code snippet of a macro definition in T_messages.txt.

```
T(T_GNB_PHY_UL_FREQ_CHANNEL_ESTIMATE,
  T_INT(srs_pdu->rnti),
  T_INTframe_rx),
 T_BUFFER(srs_estimated_channel_freq[0][0], frame_parms->ofdm_symbol_size * sizeof(
    int32_t)));
```

Listing 2.2: T tracer based data extraction code snippet of SRS frequency domain channel estimation.

```
./record -d ../T_messages.txt -o channel_frequency.raw -on
    GNB_PHY_UL_FREQ_CHANNEL_ESTIMATE
```

Listing 2.3: Command to run T_tracer record.

```
./extract -d ../T_messages.txt channel_frequency.raw
    GNB_PHY_UL_FREQ_CHANNEL_ESTIMATE chest_f -o srschF.raw
```

Listing 2.4: Command to run T_tracer extract.

Now, the frequency domain SRS channel estimates will be stored in a binary file: `srschF.raw`. This binary file can be imported to MATLAB/OCTAVE for further offline analysis. The details of compiling `T_tracer` are available in [74]. A sample MATLAB/OCTAVE script that reads the binary file and plots the SRS channel estimates is provided in [75]. More details on the usage of `T_tracer` can be found in [73].

2.5 Conclusions

In this chapter, we introduced OAI, including its components and operating modes that are beneficial to developers and researchers in prototyping. We also delved into the essential functions of the reference signals related to positioning in OAI. Further, we provided a comprehensive overview of the baseband signal representation of these reference signals using fixed-point notation in OAI. Furthermore, we discussed important physical layer metrics such as TX, RX power, and SNR estimation in OAI. Finally, we presented the `T_tracer` tool, which facilitates data extraction within the OAI framework.

Chapter 3

Novel Round Trip Time Estimation in 5G NR and beyond

This chapter proposes two novel round-trip time estimation schemes at the cellular radio access network. The proposed schemes utilize DCI-based signaling and enable us to combine multiple CSI coherently, in contrast to traditional methods based on time-stamp. This coherent combination of multiple CSI measurements improves the system's performance, especially in low SNR scenarios.

3.1 Introduction

In 5G NR, there are mainly two approaches for obtaining RTT. Once the UE is synchronized in DL, the RTT in the form of TA can be estimated from a received RACH preamble during the RA procedure. Even though this appears to be a straightforward approach, it suffers from low accuracy due to the limited bandwidth of the RACH. Moreover, the UE performs the RA procedure only during initial access or when the UL synchronization is lost. In a more dedicated method, the PRS in the DL and SRS in the UL are used to estimate the Rx-Tx timing difference at the UE and gNB as described in Section 1.2.1.2. Typically, these measurements are based on a time-stamp and are then reported to the LMF located at the 5GC network to compute the RTT. However, reporting these measurements to the LMF introduces latency, and the accuracy of this method also depends on the bandwidth of the DL and UL resources and the SNR [5, 6].

Accurate RTT estimation is possible if the timing measurements from RACH can be augmented with wideband UL CSI measurements, for example, from SRS. Few works have considered the problem of estimating RTT based on UL CSI measurements at the gNB in real-world scenarios using open-source 4G/5G testbeds [76, 60]. The work in [76] is restricted to a scenario where there is no TA correction sent to the UE by the gNB after the initial random access, i.e., the UE is very close to the gNB. An improved scheme that overcomes this restriction has been proposed in [60]. However, both works ignore the effect of clock drift in the system. Indeed, large fluctuations in RTT estimates caused by these factors are reported in [60]. Moreover, RTT can only be obtained during initial access.

The inability to exploit multiple UL SRS measurements coherently in the RTT estimation stems from a) inherent timing control loops in 5G NR and b) clock drift. The timing control loops in 5G NR include UL and DL timing control. UL timing control is a continuous process in which gNB sends TA commands to the UE to adjust its UL transmission timing. This procedure is crucial for maintaining UL frame alignment with the gNB. On the other hand, in DL timing control, the UE experiences DL reception timing drift due to clock drift, and it corrects this drift based on DL reference signals and is implementation-specific. These timing control loops and the clock drift lead to the variability in delay estimated from SRS measurements obtained in different time slots. Therefore, even in a scenario where

the UE is static, and the gNB has access to multiple SRS measurements, they cannot be used jointly to estimate the RTT. The impact of clock drift and timing loops on the estimated distance using RTT from SRS measurements over time with a commercial UE (Quectel RM500-GL) at a fixed location is illustrated in Figure 3.1. However, it is well known that coherently combining multiple measurements improve the estimation performance in low SNR conditions.

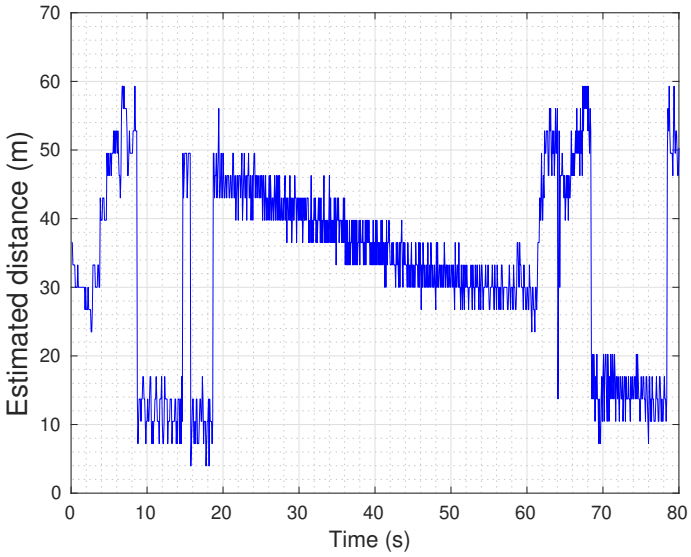


Figure 3.1: Effect of clock drift and timing loops on RTT in a commercial UE.

In this chapter, we propose a novel framework to estimate the RTT based on multiple coherent SRS measurements in 5G NR. This approach tremendously improves the RTT estimation accuracy in the low SNR regime. The main contributions of this chapter are:

- We propose two simple enhancements to the 5G NR signaling scheme capable of obtaining a sequence of similar UL SRS measurements.
- A matched-filter solution is proposed to estimate the RTT jointly from the collected measurements.
- The proposed method can obtain the RTT even when the 5G UE is in a RRC inactive state.
- The complete solution is experimentally validated with a real-word 5G testbed based on the OAI [58].

This chapter is organized as follows: Section 3.2 describe the proposed signaling enhancements for 3GPP. Section 3.3 presents the procedure for SRS channel estimation. Section 3.4 details the RTT estimation procedure and its associated algorithms. Section 3.5 outlines the experimental setup, while the evaluation results are presented in Section 3.6. Section 3.7 discusses the datasets collected during this experiment. Finally, Section 3.8 concludes this chapter.

3.2 Proposed Signaling Enhancements

The proposed signaling schemes aims to obtain multiple wide-band UL SRS measurements along with the RACH at the gNB. We leverage on the existing physical downlink control channel (PDCCH) order signaling mechanism in 5G NR to obtain these measurements. When an RTT request is made, the gNB sends an enhanced downlink control information (DCI) that includes information fields related to positioning to the UE as a DCI Format via PDCCH. Moreover, the DCI Format should consider both the NR_RRC_INACTIVE and NR_RRC_CONNECTED states of a UE.

It is possible to use an existing DCI Formats in the current 3GPP standard with minor modifications[77]. This can be achieved by adding an SRS request field to the DCI Format 1_0 for RAN paging in the NR_RRC_INACTIVE state and the DCI Format 1_0 for PDCCH order in the NR_RRC_CONNECTED state. However, the DCI Format 1_0 for RAN paging initiates a contention based RACH procedure, resulting in signaling overhead.

Furthermore, DL timing correction is crucial for positioning when a DCI is received. This can be observed from the behavior of a 3GPP Release-15 commercial UE (Quectel RM500-GL) as shown in Figure 3.2. The plot in Figure 3.2 indicates the distance estimated from RTT over time by combining TA from RACH and SRS measurements. An existing DCI (PDCCH order) is used to trigger the RACH, and the SRS is scheduled so that the UE transmits the SRS after applying the TA received from RAR. The sawtooth structure observed from the RTT measurements over time is shown in Figure 3.2. In this sawtooth behavior,

- The rise in the RTT estimates stems from the clock drift between the gNB and the UE because the UE does not correct its DL timing immediately after receiving the DCI.
- The fall occurs when the UE corrects its DL timing.

Currently, commercial UEs using 3GPP Release-15 have an implementation-specific timing correction that corrects the DL timing only based on the conformance requirement [78] but not when the DCI is received. Therefore, a new DCI Format is needed to reduce the signaling overhead, maintain DL and UL timing, and use a common DCI for both RRC states. This motivates us to propose two signaling mechanisms for positioning with a new DCI Format. The proposed signaling schemes are the SSB-SRS and PRS-SRS signaling schemes, described in the section below.

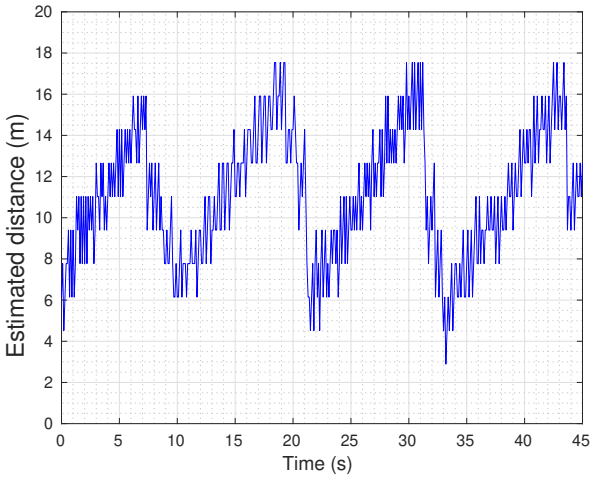


Figure 3.2: Effect of clock drift on RTT in a commercial UE using PDCCH order.

3.2.1 SSB-SRS signaling scheme

The proposed 3GPP like signaling scheme is depicted in Figure 3.3. A new DCI Format, termed as DCI Format X_Y, is used to signal the UE for positioning. Once the UE decodes the DCI Format X_Y, it adjusts or updates its DL synchronization based on the SSB[1]. The UE then triggers a contention free RACH using the dedicated preamble mentioned in the DCI Format X_Y. The gNB estimates the TA from the RACH preamble and sends it to the UE via RAR. The UE applies the TA after six slots (from current 3GPP standards) and then transmits the SRS, as shown in Figure 3.3. RTT can be calculated based on the TA and the SRS channel estimates as described in Section 3.4. This procedure is repeated several times to obtain multiple measurements. Note that the UE aligns its UL timing when sending the SRS using the TA value received in the RAR.

The DCI Format X_Y [77] includes the following fields: fullI-radio network temporary identifier (RNTI) or shortI-RNTI, Random Access Preamble index, UL/supplementary uplink (SUL) indicator, SS/PBCH index, PRACH Mask index, and SRS request as shown in Table. 3.1. In the proposed signaling mechanism,

- when UE is NR_RRC_INACTIVE state, the DCI Format X_Y is scrambled using P-RNTI,
- in NR_RRC_CONNECTED state, the DCI Format X_Y is scrambled using C-RNTI. In this case, the field fullI-RNTI or shortI-RNTI is set to 0.

Table 3.1: Contents of DCI Format X_Y : SSB-SRS signaling scheme

DCI Fields	Number of bits
fullI-RNTI or shortI-RNTI	40 or 24
Random Access Preamble index	6
UL/SUL indicator	1
SS/PBCH index	6
PRACH Mask index	4
SRS request	2 or 3

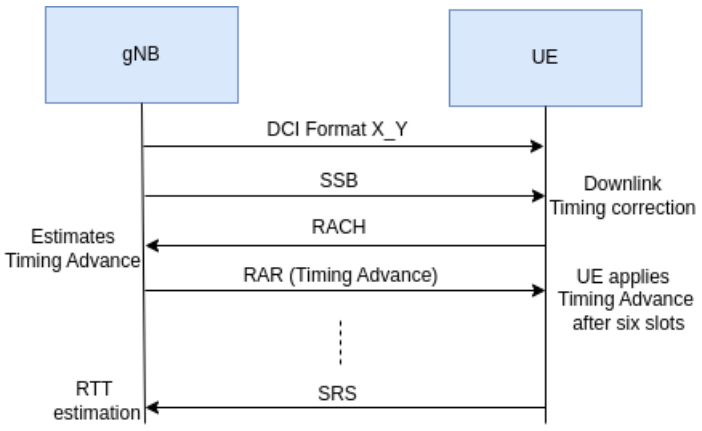


Figure 3.3: Proposed SSB-SRS signaling scheme for RTT estimation.

[1]Note that UE can update its DL synchronization by other means too

The description of the DCI fields are detailed as follows:

1. fullI-RNTI or shortI-RNTI : An identifier assigned to a UE in NR_RRC_INACTIVE state.
2. Random Access Preamble index : A dedicated random access preamble index to perform contention-free RA procedure.
3. UL/SUL indicator : Parameter to check if the UE is configured with SUL or not.
4. SS/PBCH index : Indicates the SS/PBCH that shall be used to determine the RACH occasion for the PRACH transmission.
5. SRS request : Parameter to check if the UE should send SRS or not.

3.2.2 PRS-SRS signaling scheme

The proposed PRS-SRS signaling scheme is similar to the proposed SSB-SRS signaling scheme, however it emphasis on improving the downlink timing synchronization at the UE using PRS. The proposed PRS-SRS signaling scheme is depicted in Figure 3.4.

Similar to SSB-SRS signaling scheme, a new DCI Format, termed as DCI Format X_Y, is introduced. Once the UE decodes the DCI Format X_Y, it adjusts or updates its DL synchronization based on the PRS. The UE then triggers a contention free RACH using the dedicated preamble mentioned in the DCI Format X_Y. The gNB estimates the TA from the RACH preamble and sends it to the UE via RAR. The UE applies the TA after six slots (from current 3GPP standards) and then transmits the SRS, as shown in Figure 3.4.

The DCI Format X_Y for PRS-SRS signaling scheme includes the following fields: fullI-RNTI or shortI-RNTI, Random Access Preamble index, UL/SUL indicator, SS/PBCH index, PRACH Mask index, SRS request and PRS decode request as shown in Table. 3.2. In the proposed signaling mechanism,

- when UE is NR_RRC_INACTIVE state, the DCI Format X_Y is scrambled using P-RNTI,
- in NR_RRC_CONNECTED state, the DCI Format X_Y is scrambled using C-RNTI. In this case, the field fullI-RNTI or shortI-RNTI is set to 0.

Table 3.2: Contents of DCI Format X_Y : PRS-SRS signaling scheme

DCI Fields	Number of bits
fullI-RNTI or shortI-RNTI	40 or 24
Random Access Preamble index	6
UL/SUL indicator	1
SS/PBCH index	6
PRACH Mask index	4
SRS request	2 or 3
PRS decode request	2 or 3

3.2.2.1 Cyclic-shift based signaling scheme

A more efficient signaling scheme for RTT estimation in NR_RRC_CONNECTED state using PRS in the DL and a new reference signal, namely uplink reference signal (URS), instead of SRS in the UL, has been proposed in [63]. This URS utilizes the cyclic shift property of the Zadoff-chu sequence as described in Section 2.2.2.1 to shift the signal by TA used by the UE and the downlink timing information

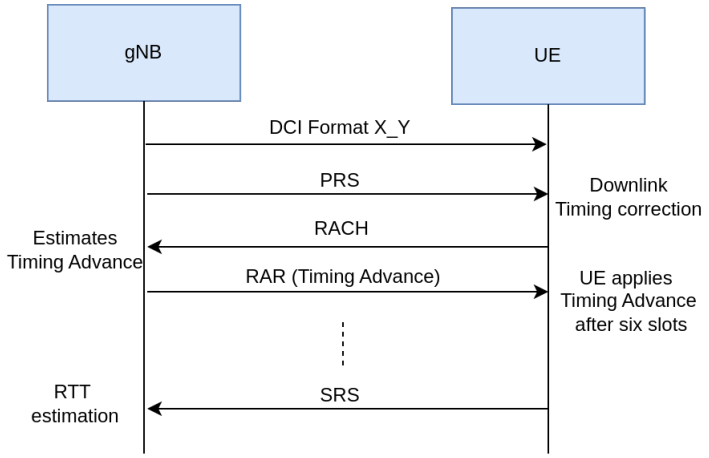


Figure 3.4: Proposed PRS-SRS signaling scheme for RTT estimation.

from the estimated PRS peak p_d as shown in Figure 3.5. This mechanism further reduces the latency by eliminating the need for RA procedure in the proposed SSB-SRS and PRS-SRS schemes, achieving the same accuracy performance. However, in this dissertation, we restrict our analysis to SSB-SRS and PRS-SRS signaling schemes.

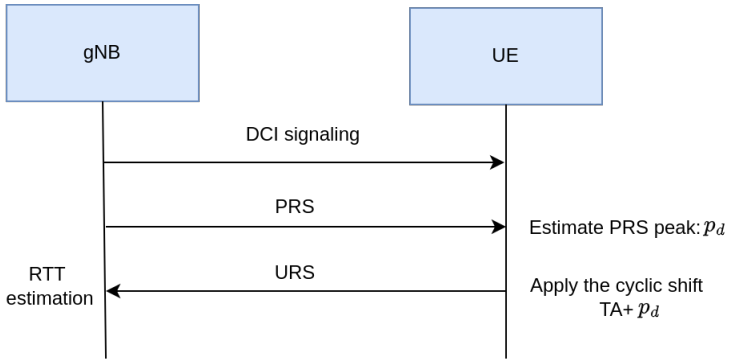


Figure 3.5: RTT estimation mechanism using Cyclic shift based URS.

Now, we describe the channel estimation procedure of the SRS obtained using both SSB-SRS and PRS-SRS signaling schemes.

3.3 SRS channel estimation

We consider a 5G NR system with a single antenna UE and gNB in our experiments. The received SRS at the gNB on the k-th, $k \in [0, K-1]$, subcarrier

$$y[k] = h[k]s[k] + n[k], \tag{3.1}$$

where, $k \in \{0, 1, \ldots, K-1\}$, K is the fast Fourier transform (FFT) size, $h[k]$ represents the baseband propagation channel, $s[k]$ represents the SRS pilot symbol and $n[k] \sim \mathcal{N}(0, \sigma^2)$ is additive white gaussian noise. We consider a LoS channel with L multi-path components. The UL channel at the d-th tap is modeled as,

$$h_d = \sum_{\ell=0}^{L-1} \alpha_\ell \rho(dT_s - \tau_\ell) \tag{3.2}$$

where, $\alpha_\ell = \alpha'_\ell e^{-j2\pi f_c \tau_\ell}$ is the complex channel gain of the ℓ-th path, α'_ℓ and τ_ℓ are the path-loss and delay of the ℓ-th path, f_c is the center frequency, T_s is the sampling period and $\rho(.)$ is the pulse-shaping filter. Further, the UL channel at a k-th subcarrier can be obtained by,

$$h[k] = \sum_{d=0}^{N_t-1} h_d e^{\frac{-j2\pi kd}{K}}, \tag{3.3}$$

where, N_t is the number taps. Furthermore, a least-square estimate of the channel is given by

$$\hat{h}[k] = s[k]^* y[k], \tag{3.4}$$

where, $(.)^*$ denotes the conjugate operator, and $s[k]$ is the known SRS symbol at the k-th subcarrier. The channel estimate $\hat{h}[k]$ is represented in the vector form as

$$\hat{\boldsymbol{h}} = \left[\hat{h}[0], \hat{h}[1], \ldots, \hat{h}[K-1]\right]^{\mathrm{T}}. \tag{3.5}$$

We further describe the RTT estimation procedure using TA obtained from RACH and the SRS channel estimates.

3.4 RTT Estimation

Based on the signal enhancements described in the previous section, the gNB can estimate a coarse RTT, i.e., TA value estimated from the RACH, and refine it further using SRS measurements. The coarse RTT τ^r can be obtained from the TA as

$$\tau^r = \frac{\mathrm{TA} \times 16 \times 64}{2^\mu} \mathrm{T}_c, \tag{3.6}$$

where, $\mu \in \{0,1,2,3,4,5\}$ is the numerology related to the subcarrier spacing $\Delta f = 15.2^\mu$ KHz, $\mathrm{T}_c = \frac{1}{(\Delta f_{max} \times K_{max})}$, $\Delta f_{max} = 480$ KHz is the maximum possible SCS and $K_{max} = 4096$ is the maximum possible FFT size in 5G NR [68].

By using the proposed signaling schemes in Section 3.2.1 and Section 3.2.2, we can obtain multiple coarse RTT's and SRS channel estimates. The m-th, $m \in [1, M]$ coarse RTT obtained from RACH using (3.6) and the channel estimate is denoted by τ^r_m and $\hat{\boldsymbol{h}}_m \in \mathbb{C}^{K\times 1}$ respectively. Each channel estimate $\hat{\boldsymbol{h}}_m$ is shifted by the respective coarse RTT τ^r_m to maintain the coherency among the channel estimates. A threshold based peak detector (PD) and threshold based matched filter (MF) estimate of the refined RTT $\hat{\tau}$ are discussed in the section below.

3.4.1 Threshold based Peak Detector

A refined RTT using a peak detector by detecting a first peak of the impulse response greater than a threshold T_h^{pd} can be obtained by,

$$\tilde{\boldsymbol{h}}_m = IDFT\left\{\mathbf{T}(\tau_m^r)\hat{\boldsymbol{h}}_m\right\} \tag{3.7}$$

$$\tilde{\boldsymbol{p}}_d^m = Ind\left(\left|\tilde{\boldsymbol{h}}_m\right| \geq T_h^{pd}\right) \text{ //Indices of } \left|\tilde{\boldsymbol{h}}_m\right| \geq T_h^{pd} \tag{3.8}$$

$$p_d^m = \begin{cases} \tilde{\boldsymbol{p}}_d^m(0), & \left|\tilde{\boldsymbol{h}}_m(\tilde{\boldsymbol{p}}_d^m(0))\right| \geq \left|\tilde{\boldsymbol{h}}_m(\tilde{\boldsymbol{p}}_d^m(1))\right| \\ \tilde{\boldsymbol{p}}_d^m(1), & \left|\tilde{\boldsymbol{h}}_m(\tilde{\boldsymbol{p}}_d^m(0))\right| < \left|\tilde{\boldsymbol{h}}_m(\tilde{\boldsymbol{p}}_d^m(1))\right| \end{cases} \tag{3.9}$$

$$\hat{\tau}\ (\text{PD}) = \frac{1}{f_s M}\sum_{m=1}^{M} p_d^m, \tag{3.10}$$

where, $\hat{\boldsymbol{h}}_m, m \in [1, M]$ is the m-th SRS channel estimate measurement, f_s is the sampling rate, $\mathbf{T}(\tau_m^r) = \text{diag}\left(1, e^{-j2\pi\Delta f\tau_m^r}, \ldots, e^{-j2\pi(K-1)\Delta f\tau_m^r}\right)$, $IDFT\{.\}$ denotes the inverse discrete Fourier transform and $\tilde{\boldsymbol{p}}_d^m(0), \tilde{\boldsymbol{p}}_d^m(1)$ are the first, second indices of the $\left|\tilde{\boldsymbol{h}}_m\right|$ that are $\geq T_h^{pd}$.

3.4.2 Threshold based Matched Filter

A refined RTT using a matched filter by detecting the first local maximum of the matched filter output greater than a threshold T_h^{mf} can be obtained by,

$$M_f(\tau_i) = \frac{1}{M}\sum_{m=1}^{M} |\boldsymbol{v}(\tau_i)^{\text{H}}\mathbf{T}(\tau_m^r)\hat{\boldsymbol{h}}_m|^2,\ i = \{1, \ldots, G\} \tag{3.11}$$

$$M_f = \left[M_f(\tau_1), M_f(\tau_2), \ldots, M_f(\tau_G)\right], \tag{3.12}$$

$$\bar{M}_f = \frac{M_f}{\max(M_f)} \tag{3.13}$$

$$\hat{\tau}(\text{MF}) = \underset{\tau_i}{\arg\min}\left(\texttt{find\_peaks}\left(\bar{M}_f, T_h^{mf}\right)\right) \tag{3.14}$$

where, $\boldsymbol{v}(\tau) = \left[1, e^{-j2\pi\Delta f\tau}, \ldots, e^{-j2\pi(K-1)\Delta f\tau}\right]^{\text{T}}$, and $\texttt{find\_peaks}\left(\bar{M}_f, T_h^{mf}\right)$ outputs all the local maxima in $\bar{M}_f$ that are $\geq T_h^{mf}$. The local maxima is a data value that is greater than its two neighboring data values and G is the grid size of the MF.

Further, the distance estimate ($\hat{d}$) between the gNB and the UE can be obtained from the estimated RTT ($\hat{\tau}$) as

$$\hat{d} = \frac{\hat{\tau}\, c}{2}, \tag{3.15}$$

where, c is the speed of light.

The performance of the proposed algorithm is evaluated using the following experimental setup.

3.5 Experimental Setup

We consider a scenario with a single antenna gNB and a UE having LoS condition. We leverage on the OAI 5G NR protocol stack [58] and USRP B210 SDR cards to build the gNB and UE. Additionally, SC2430 NR signal conditioning module is used as an external RF front-end at the gNB [79]. The measurements were taken in an anechoic chamber at the Northeastern University Burlington campus, as shown in Figure 3.6.

Since the signaling using the DCI Format X_Y is not implemented yet, we simplify the proposed SSB-SRS signaling scheme depicted in Figure 3.3 of Section 3.2.1 to the signaling scheme as shown in

Figure 3.7. Similarly, we simplify the proposed PRS-SRS signaling scheme depicted in Figure 3.4 of Section 3.2.2 to the signaling scheme as shown in Figure 3.8. Note that this simplification does not result in any loss in terms of the functional behavior of the proposed RTT estimation algorithm for the following reasons:

- The distance between the gNB and UE is always within the resolution of the RACH based TA during the experiment. For the used 5G NR configuration, the RACH TA resolution is 39.0625 meters.
- The delay between receiving the DCI Format X_Y and sending the SRS in the proposed framework (Figures 3.3 and 3.4) is emulated with a 20 slot offset between SSB/PRS reception and SRS transmission at the UE as shown in Figure 3.7 and Figure 3.8 respectively.
- The hardware delays are calibrated and compensated by applying a fixed timing advance at the UE throughout the experiment. For this, we have used the `phy-test` mode of the OAI [66] as described in Section 2.2.1.4. This mode operates only at the physical layer and abstracts the higher layers.

The 5G NR system parameters used in the experiment are listed in Table 3.3. Note that the proposed schemes applies to all the 3GPP bandwidth and numerology configurations.

During the experiment, the gNB is static, and the UE is moved in an increment of 1 meter from an initial gNB-UE distance of 7 to 11 meters, as shown in Figure 3.6. In all measurements, the LoS is maintained between the gNB and UE. Variation in uplink SNR is achieved by changing the USRP transmit (Tx) gain. Multiple SRS channel estimates were obtained at each distance, and the data was then stored for further offline analysis. The performance of both the proposed schemes based on the collected measurements are presented in the following section.

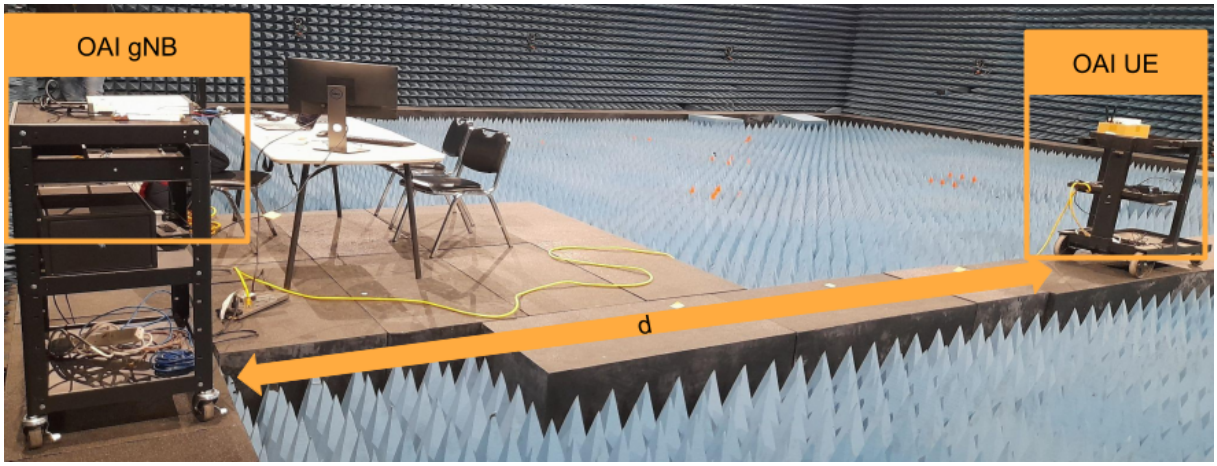


Figure 3.6: Experimental setup for evaluating the proposed schemes in an anechoic chamber.

3.6 Results

In this section, we will present the empirical results of both the proposed RTT estimation schemes at low and high uplink SNR scenarios. Furthermore, the impact of the number of measurements on the two algorithms, the PD and the MF is shown. The PD and the MF approaches are outlined in Section 3.4.

For both the schemes, in the high SNR scenario, we set the UE USRP Tx gain to 89.5 dB, resulting in an estimated uplink SNR of 25 dB. In the low SNR scenario, we have reduced the UE Tx gain by 50

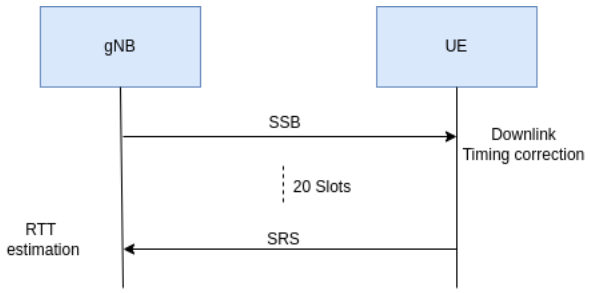


Figure 3.7: RTT implementation in OAI phy-test mode using SSB-SRS signaling scheme.

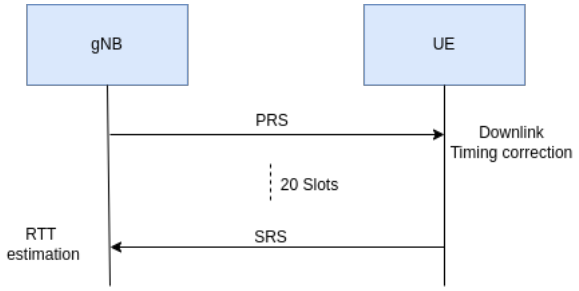


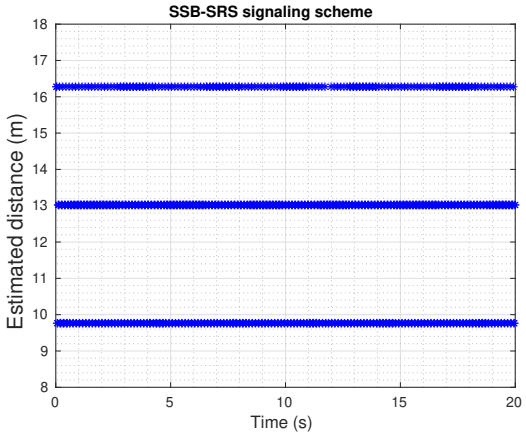
Figure 3.8: RTT implementation in OAI phy-test mode using PRS-SRS signaling scheme.

Table 3.3: System Parameters used for RTT estimation in OAI

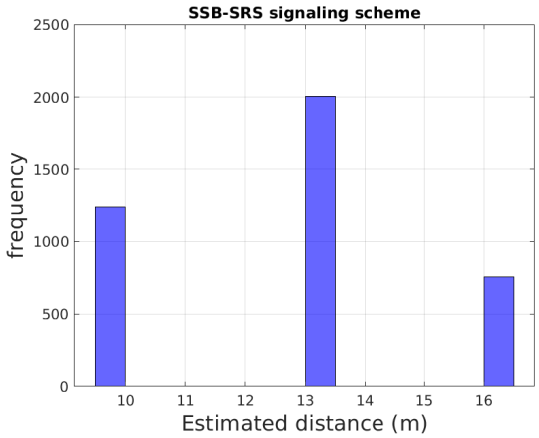
Parameters	Values
System bandwidth	38.16 MHz
Subcarrier Spacing (Δf)	30 KHz
Centre frequency (f_c)	3.69 GHz
Sampling rate (f_s)	46.08 MHz
Sampling Period (T_s)	21.70 ns
FFT size (K)	1536
Cyclic prefix (N_{cp})	132
SSB bandwidth	7.2 MHz
SRS bandwidth	37.44 MHz
SRS comb size (K_c)	2
PRS bandwidth	37.44 MHz
PRS comb size	2

dB to 39.5 dB. Finally, we used the `T_tracer` tool as described in Section 2.4 to extract the required data from OAI.

We can see that large variations shown in Figure 3.1 can be mitigated using the proposed SSB-SRS and PRS-SRS signaling schemes. As illustrated in Figures 3.9 and 3.10 at an actual gNB-UE distance of 11 m at high SNR using PD, the proposed signaling schemes mitigated the fluctuations in the estimated distance compared to the fluctuations in Figure 3.1. Note that the fluctuation of around 6.5 m in Figure 3.9 and around 3.25 m in Figure 3.10 is due to the accuracy of the distance estimation from single measurement depending on the bandwidth of the SSB and PRS respectively used for downlink correction.

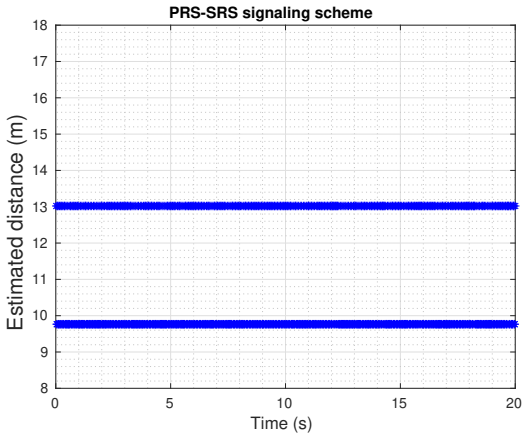


(a) Estimated distance over time.

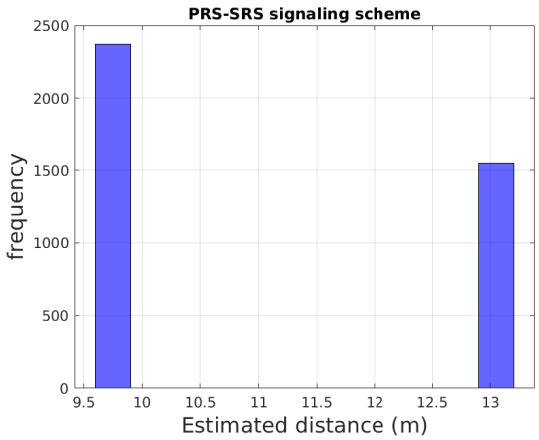


(b) Histogram of the estimated distance over time.

Figure 3.9: Estimated distance using proposed SSB-SRS signaling scheme over time.



(a) Estimated distance over time.



(b) Histogram of the estimated distance over time.

Figure 3.10: Estimated distance using proposed PRS-SRS signaling scheme over time.

Further, the RTT results in terms of distance/range estimation error for both the proposed schemes are discussed below.

3.6.1 SSB-SRS signaling scheme

The cumulative distribution Function (CDF) of the range estimation error for the MF and PD algorithms using the proposed SSB-SRS signaling scheme is shown in Figures 3.11 and 3.12, again for both high and low uplink SNRs. At each SNR, the empirical range CDF is obtained from a total of 25,000 SRS measurements, collected based on the signaling procedure depicted in Figure 3.7. As described in Section 3.5, these 25,000 measurements were obtained by fixing the gNB's position and moving the UE between 7 and 11 meters in 1-meter increments. At every SNR, 5,000 measurements were taken at each distance between 7 and 11 meters.

While the MF and PD schemes have similar performance when the SNR is high, in low SNR scenarios, the MF algorithm significantly outperforms the PD scheme. In a low SNR scenario, for M=20, the range estimation error of MF is below 3.25 meters for 90% of the time. Furthermore, by increasing the number of measurements from M=20 to M=60, we see an increase in the estimation performance for both methods.

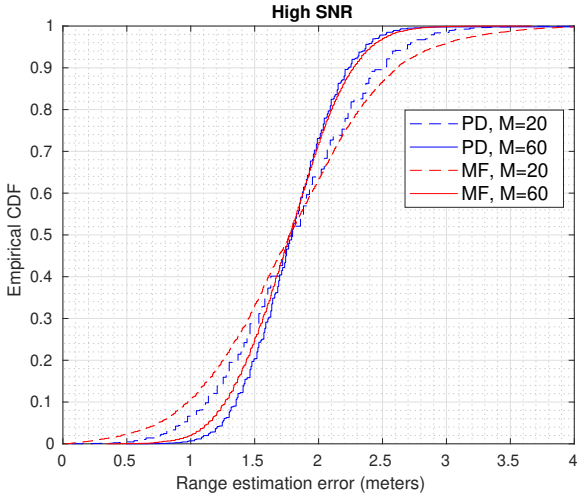


Figure 3.11: CDF of the range estimation error at High SNR using SSB-SRS signaling scheme.

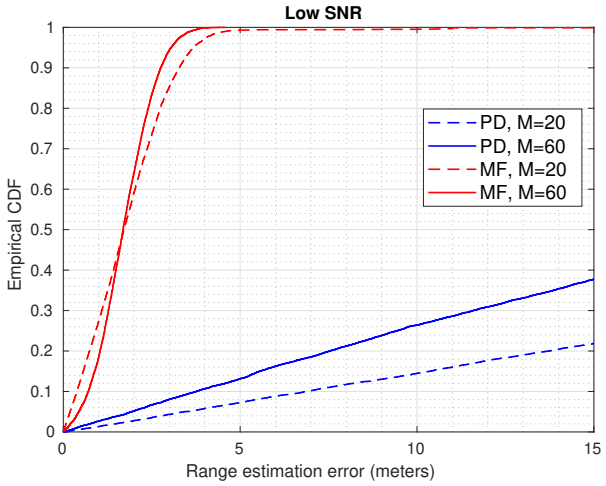


Figure 3.12: CDF of the range estimation error at Low SNR using SSB-SRS signaling scheme.

3.6.2 PRS-SRS signaling scheme

The CDF of the range estimation error for the MF and PD algorithms using the proposed PRS-SRS signaling scheme at both high and low uplink SNR is shown in Figures 3.13 and 3.14 respectively. At each SNR, the empirical range CDF is obtained from a total of 15,000 SRS measurements. These measurements are collected based on the signaling procedure depicted in Figure 3.8. As described in Section 3.5, these 15,000 measurements are obtained by keeping the gNB's position fixed and moving the UE between 9 to 11 meters with a 1 meter increment. At every SNR, 5,000 measurements are collected at each distance between 9 and 11 meters.

Similar to SSB-SRS signaling scheme, the MF and PD schemes perform comparably at high SNRs. However, in low SNR scenarios, the MF algorithm outperforms the PD scheme significantly. For low SNR and M=20, the range estimation error of the MF scheme is below 0.7 meters 90% of the time. Again, increasing the number of measurements from M=20 to M=60 results in improved estimation performance for both methods. Furthermore, using PRS for downlink correction in PRS-SRS signaling scheme results in improved range estimation error in both high and low SNR scenarios compared to SSB in SSB-SRS signaling scheme. This enhancement is due to the higher bandwidth of PRS compared to SSB. The measurements obtained using the proposed schemes are publicly available and discussed in the section below.

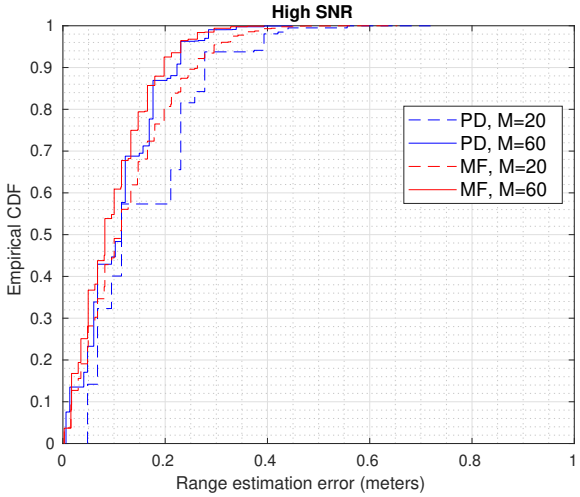


Figure 3.13: CDF of the range estimation error at High SNR using PRS-SRS signaling scheme.

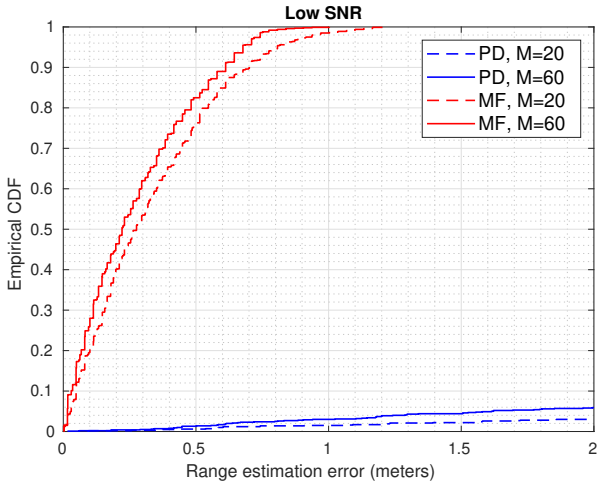


Figure 3.14: CDF of the range estimation error at Low SNR using PRS-SRS signaling scheme.

3.7 Dataset

The dataset collected using the RTT prototype mentioned above in an anechoic chamber is made public in [75]. The dataset includes multiple measurements at different distances varying from 7-11m in 1 m increments. At each distance, SNR is varied by changing the TX gain from 39.5 dB to 89.5 dB of the USRP in steps of 10 dB. The SNR corresponds to 89.5 is 25 dB. In the published dataset [75], the folder name contains the corresponding distance between gNB, UE, and the Tx gain used. The Tx gain can be inferred from the folder name as follows: the sub-string `ue_att_x` should be interpreted as x dB attenuation from the maximum gain of the USRP B210, which is 89.5 dB. For example, `ue_att_0` corresponds to the Tx gain 89.5 dB, and `ue_att_50` corresponds to the Tx gain 39.5 dB. Each folder contains the following recorded data files in Q15 format,

- `srs_chF.raw`: Frequency domain least square channel estimates of the SRS in comb fashion.
- `srs_chF_lin_interp.raw`: Frequency domain least square channel estimates of the SRS in comb fashion and the channel estimates of the subcarriers between the two SRS symbols in a comb are linearly interpolated.
- `srs_chT.raw`: Impulse response of the SRS.
- `noise.raw`: Noise measured in an empty OFDM symbol.

To read and analyze these files, a sample MATLAB script is provided in [75]. For example, an impulse response sample from the dataset at 10 m and a USRP Tx gain of 89.5 dB is shown in Figure 3.15. The x-axis in Figure 3.15 represents the IFFT index in samples. The RTT in samples between the gNB and UE can be estimated from the peak p of the impulse response. Finally, the range estimate $\hat{d}$ between the gNB and UE from peak p is obtained by,

$$\hat{d} = \frac{p \times c}{2 f_s}, \tag{3.16}$$

where, c is the speed of light and f_s is the sampling rate. Utilizing the system configuration mentioned in Table 3.3, the estimated range is 13.02 m. Note that in this example, the estimated range is based on the maximum peak of the channel impulse response (CIR) from a single measurement. However, better accuracy in terms of range estimation error can be achieved by combining multiple measurements as discussed in Section 3.6.

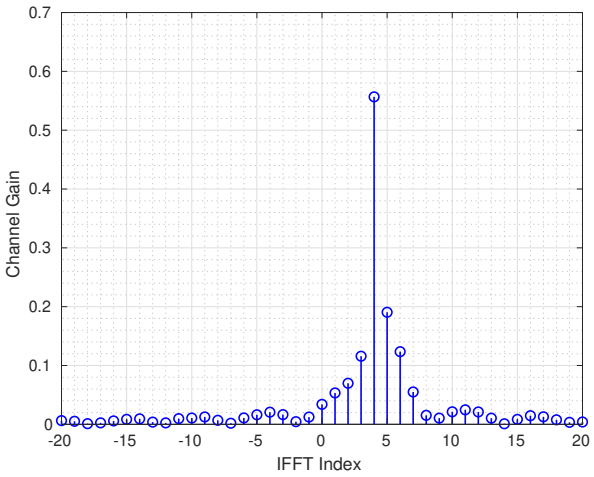


Figure 3.15: A sample impulse response from the dataset.

3.8 Conclusions

In this chapter, we proposed two RTT estimation schemes using DCI Format X_Y as a signaling mechanism for positioning. The proposed schemes are designed to work in both NR_RRC_INACTIVE and NR_RRC_CONNECTED states. It forces the UE to correct its timing after the reception of the DCI, which is currently not possible, as shown in our experiments with the COTS UEs. Furthermore, our framework enables the coherent combination of multiple uplink channel measurements and is robust to the clock drift and the inherent timing loops in the 5G system. We have validated the functionality of our proposed framework in real-time using OAI. Our results show that the proposed matched filter algorithm can achieve meter-level accuracy for bandwidth as low as 40MHz, even in low SNR scenarios.

Chapter 4

Sensing aided Channel Estimation in Wideband MIMO Systems

In this chapter, we present how to utilize the sensing information, such as the distance and angle information of a scatterer/reflector gathered from the environment, to enhance uplink channel estimation. We demonstrate that utilizing sensing information as side information can significantly reduce the number of pilots required for the channel estimation.

4.1 Introduction

Millimeter wave (mmWave) and THz frequencies are considered to be a key component of 5G and beyond cellular systems [80]. However, as the operating frequencies increase, path and absorption losses also increase. Despite these disadvantages, this approach will allow packing more antennas in a small area and, then, the network can leverage beamforming techniques to compensate for the losses operating in such frequencies. However, the gains stemming from these multiple antenna techniques hinge on the ability to accurately estimate the CSI.

Estimating channel coefficients over a wideband and across multiple antennas incurs significant resource overhead in terms of resources occupied for sending pilot symbols. However, it has been observed that the mmWave channel exhibits a sparse behavior with only a few resolvable multi-paths in angle and delay domain [81] and [82]. By leveraging such sparsity, several works have come with compressed sensing (CS) based approaches for channel estimation and precoder design in mmWave multi-input multi-output (MIMO) systems [83, 84, 85, 86, 87, 88]. However, while used in wideband massive MIMO systems, these approaches lead to higher complexity due to the requirement of inverting huge matrices (for every subcarrier) across such antenna arrays.

Since the sparse wireless channel is described by a few geometric multi-path propagation parameters, one might ask: Can the information on the physical propagation environment, for example, scatter or reflector locations, be useful in channel estimation? Indeed, one of the earlier works in [89] has utilized this key observation. The authors extract physical multi-path parameters from the CSI measurements in one frequency band and then use them to construct the CSI in another frequency band. However, no extra pilots are used in aiding the channel estimation, and they assume that the extracted multi-path parameters are perfect.

On the other hand, advances in radar and joint communication sensing made it possible to have real-time dynamic radio environment maps at the communicating devices providing situational awareness [10, 45, 46, 48, 49, 50, 51, 52]. The works in [45, 46, 48, 49, 50, 51] use such side information in multi-path angular domain for the beam prediction and channel estimation. A recent work in [47] tried to address the problem of channel estimation in massive MIMO systems by leveraging the sensing information obtained

from a co-located radar at the gNB. Both delays and angles of multi-path parameters are extracted from the radar information, and then used to initialize the dictionary in an orthogonal matching pursuit (OMP) based channel estimation algorithm. However, the extracted multi-path parameters from the radar are assumed to be error-free.

In practice, the presence of impairments such as clock drift and timing correction loops, as described in Section 1.2.3, makes it impossible to integrate the sensing information as side information for CSI estimation. This issue arises because such impairments in 5G NR introduce fluctuations in the estimated CSI. These fluctuations are clearly illustrated in Figure 3.1, where the estimated distance obtained from the RTT (LoS path) using SRS in a commercial UE. Despite the UE being static, the estimated distance shows significant fluctuations, indicating instability in the estimated CSI. Therefore, even with the available sensing information, we cannot use this sensing information as side information with such instabilities. To address these issues, the signaling schemes proposed in Section 3.2 aim to mitigate such fluctuations in the estimated CSI. Thus, such a system, as mentioned in Section 3.2, is necessary to provide CSI that is robust to these impairments, thereby enabling the integration of sensing information as side information. Furthermore, such signaling mechanisms not only provide CSI that is robust to impairments such as clock drift and timing correction loops but also enable the sensing capability in the uplink, which acts as an alternative to obtaining sensing information from radar.

In this chapter, we consider the problem of uplink channel estimation in a wideband MIMO system using radar sensing information as side information as shown in Figure 4.1. Contrary to state-of-the-art, we propose a sparse Bayesian learning (SBL) framework that efficiently incorporates erroneous delay and angular sensing information and improves their resolution with limited pilot overhead. The main contributions of the chapter are the following :

1. We present how the signaling schemes proposed in Section 3.2 can be utilized to obtain sensing information from the environment.
2. Unlike [47], we assume that the sensing information can be erroneous. We also consider cases in which scatterers detected in the sensing system might not be associated with the communication channel.
3. To address these issues, a novel simultaneous weighting orthogonal matching pursuit (SWOMP)-SBL based channel estimation is proposed that incorporates the imperfect sensing information.

4.2 Uplink Sensing

In this section, we discuss how environmental sensing information, such as the delay between the scatterer/reflector to the gNB in an environment, can be obtained in the uplink jointly from the communication signal utilizing the proposed signaling schemes in Section 3.2. We explain how uplink sensing can be enabled by the proposed signaling schemes by detailing the estimated uplink CIR within an example propagation environment.

An example propagation environment in Figure 4.2 consists of a gNB, UE, and two scatterers/reflectors. The transmitted signal in this environment is subjected to multiple propagation paths due to the scatterers/reflectors in the environment. Therefore, in the proposed signaling schemes, both the DL and UL transmitted signals are subjected to multiple propagation paths, which can be visualized as follows:

4.2.1 Downlink Scenario

In the DL scenario, as shown in Figure 4.2a, the transmitted signal (SSB/PRS) from the gNB reaches the UE via three different paths with delays denoted as τ_0, τ_1^d, and τ_2^d. Here, τ_0 represents the LoS path, and

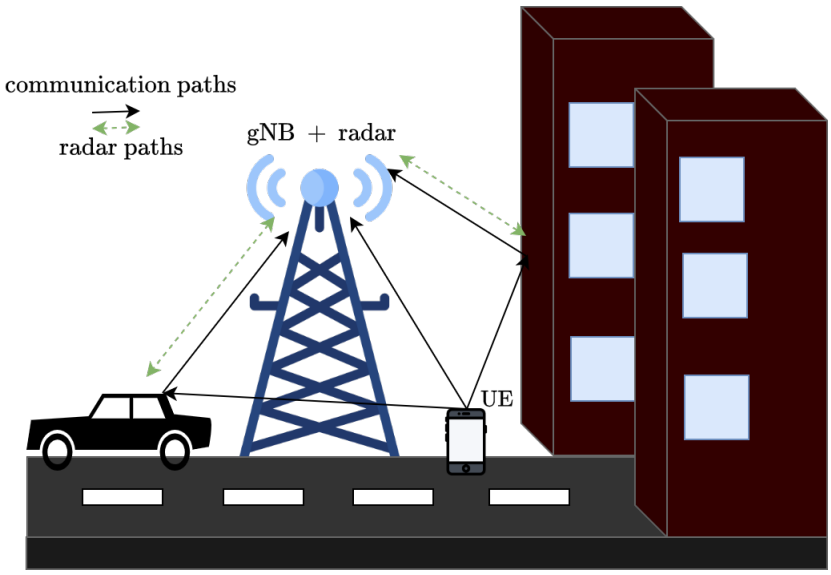


Figure 4.1: Uplink multi-path scenario along with the co-located radar.

the corresponding CIR can be seen in Figure 4.2c. The UE estimates these delays and synchronizes its timing with the LoS path (i.e., τ_0).

4.2.2 Uplink Scenario

After the UE has corrected its timing using the LoS path in the DL (i.e., τ_0), RACH procedure is initiated, where, RACH preamble is transmitted by the UE is received by the gNB to estimate TA (τ^r). After estimating the TA, the gNB sends the TA to the UE via RAR. The UE then decodes the RAR and then advances its UL timing by TA (τ^r) and transmits the SRS in the UL.

As illustrated in Figure 4.2b, the transmitted SRS also traverses in three different paths with the delays τ_0, τ_1^u, and τ_2^u. Since the UE transmits the SRS after aligning its DL timing with τ_0 and advancing it's UL timing with TA (τ^r), all the estimated delays from the SRS in the UL (τ_0, τ_1^u, and τ_2^u) are effectively shifted by $\tau_0 - \tau^r$ as shown in Figure 4.2d. Further, by compensating the TA from the SRS, referred to as TA compensated SRS (i.e., $\mathbf{T}(\tau^r)\hat{\boldsymbol{h}}$), all the estimated delays in the time domain, are effectively shifted by τ_0 as shown in Figure 4.3. Where, $\mathbf{T}(\tau^r) = \text{diag}\left(1, e^{-j2\pi\Delta f\tau^r}, \ldots, e^{-j2\pi(K-1)\Delta f\tau^r}\right)$, Δf is the SCS, K is the FFT size and $\hat{\boldsymbol{h}}$ is the SRS channel frequency response (CFR).

Note that the LoS path $2\tau_0$ as shown in Figure 4.3 is the delay of the first path of the TA compensated SRS, referred to as RTT. We estimate RTT by estimating the delay of the first path from the TA compensated SRS (i.e., $2\tau_0$). Furthermore, in the time division duplex (TDD) systems, $\tau_1^d = \tau_1^u = \tau_1$ and $\tau_2^d = \tau_2^u = \tau_2$ since the operating frequencies are the same. However, in frequency division duplex (FDD) systems, τ_1^d and τ_2^d may not be equal to τ_1^u and τ_2^u, respectively. Therefore, by estimating τ_0 and subtracting it from the estimated delays of the TA compensated SRS, we can determine the delays τ_1^u and τ_2^u caused by the scatterers/reflectors present in the environment.

Furthermore, considering TDD and a multiple antenna system, the delays and AoAs estimated from the TA compensated SRS as described above, can be used to determine the location of the scatterers/reflectors present in the environment. For example, in the scenario shown in Figure 4.4, let τ_0, θ_0 be the delay and AoA of the LoS path and $\tau_\ell = \tau'_\ell + \tau_\ell^{rad}, \theta_\ell$ be the delay and AoA estimated from the ℓ-th scatterer. The distance between the gNB and the ℓ-th scatterer $d_\ell^{rad} = \tau_\ell^{rad} c$ can be estimated using the triangle

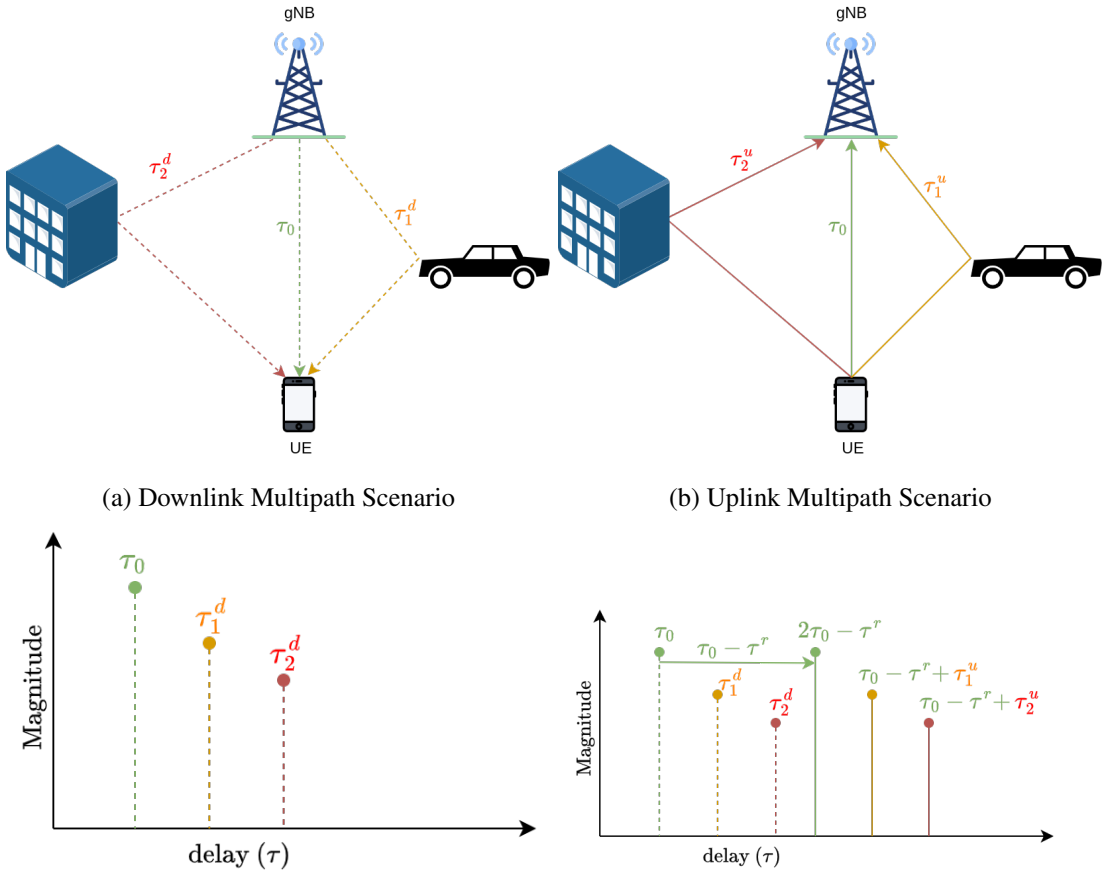
laws of cosines as follows,

$$(\tau'_\ell)^2 = \tau_0^2 + (\tau_\ell^{rad})^2 - 2\tau_0\tau_\ell^{rad} cos(\theta_\ell - \theta_0), \tag{4.1}$$

where c is the speed of light and solving for τ_ℓ^{rad} by substituting $\tau'_\ell = \tau_\ell - \tau_\ell^{rad}$ in (4.1),

$$\tau_\ell^{rad} = \frac{(\tau_\ell^2 - \tau_0^2)}{2(\tau_\ell - \tau_0 cos(\theta_\ell - \theta_0))}, \tag{4.2}$$

Thus, utilizing the known gNB location and the estimated delay (τ_ℓ^{rad}) and AoA (θ_ℓ) of the ℓ-th scatterer/reflector, the location of the ℓ-th scatterer/reflector in an environment can be determined using the proposed signaling schemes. Furthermore, the delay (τ_ℓ^{rad}) and AoA (θ_ℓ) information of the scatterers/reflectors, referred to as sensing information estimated using the proposed signaling schemes, can be further leveraged to enhance communication. This includes using the sensing information to aid in channel estimation to reduce the number of pilots required for the channel estimation, as discussed below.



(a) Downlink Multipath Scenario

(b) Uplink Multipath Scenario

(c) Downlink Multipath Channel

(d) Uplink Multipath Channel

Figure 4.2: Multipath Scenario of both Downlink and Uplink using Proposed Schemes.

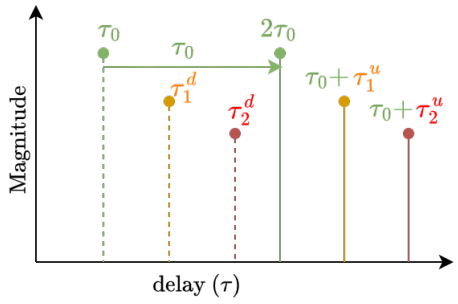


Figure 4.3: TA compensated SRS Channel Impulse Response.

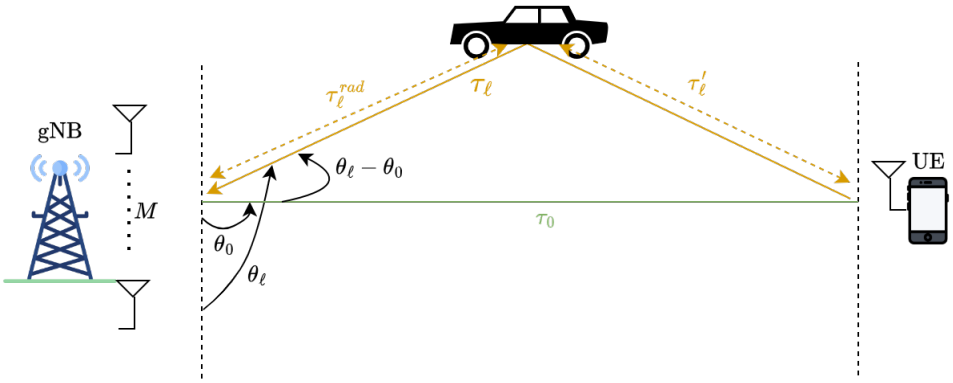


Figure 4.4: Estimation of the Scatterer Location using Uplink Sensing.

4.3 System Model

We consider a scenario where a UE communicates with gNB in an environment with the scatterers located between them. The scatterers are represented by $\mathcal{S}_r$, and $|\mathcal{S}_r| = L_r$. Only a subset of these scatterers, $\mathcal{S}_c \subseteq \mathcal{S}_r$, $|\mathcal{S}_c| = L_c$, are assumed to affect the UE-gNB communication channel. The set $\mathcal{S}_c$ is unknown, however, we assume that location estimates of scatterers in $\mathcal{S}_r$ are provided by a sensing system. This represents a scenario where the scatterers are present in the blind zone to UE but can be detected by a sensing system co-located at the gNB as shown in the Figure 4.5.

4.3.1 Sensing Information

We assume that the gNB obtains sensing information through either a radar [90] co-located with the gNB or a joint communication and sensing framework [Section 1.2.2, 4.2] , [40]. The sensing measurements available at the gNB are given by,

$$\tau_\ell^{rad} \sim \mathcal{N}(\bar{\tau}_\ell, \sigma_\tau^2),\ \ell = \{1,2,\ldots,L_r\} \tag{4.3}$$

$$\theta_\ell \sim \mathcal{N}(\bar{\theta}_\ell, \sigma_\theta^2),\ \ell = \{1,2,\ldots,L_r\} \tag{4.4}$$

where τ_ℓ^{rad} and θ_ℓ represent the delay and angle of the path from ℓ-th scatterer. They are assumed to be Gaussian distributed with means $\bar{\tau}_\ell$ and $\bar{\theta}_\ell$ representing the true delay and angle of the ℓ-th scatterer from the gNB, respectively. The error in the radar spatial information can appear due to noise and the inability of the radar to resolve delay and/or angles sufficiently.

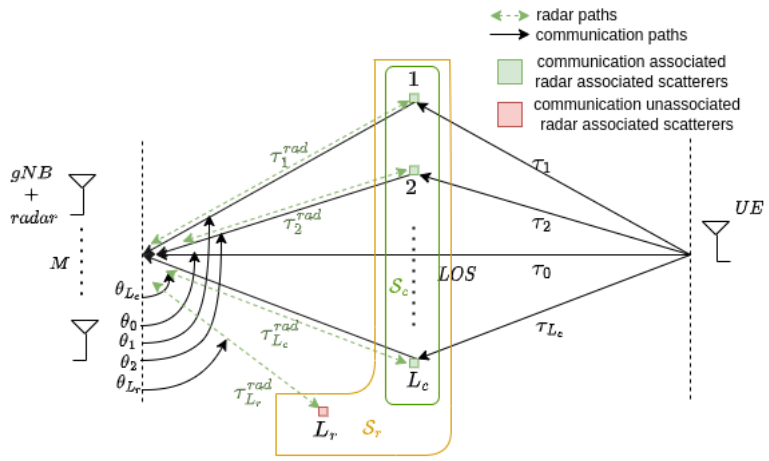


Figure 4.5: Uplink channel estimation in the presence of Scatterers along with the Sensing information.

4.3.2 Communication Model

We consider a mmWave OFDM) system with a single antenna UE and M antenna gNB. The gNB is equipped with a uniform linear array with half-wavelength spacing between consecutive antennas.

The UE sends $P \ll K$ (narrowband) pilots, where K is the total number of subcarriers used for communication. The pilot index $p \in \mathcal{P} \subset \{0,\ldots,K-1\}$ and $|\mathcal{P}| = P$. The received complex baseband signal at the p-th subcarrier after down-conversion, zero prefix removal, OFDM demodulation, and correlation with the pilots is given by

$$\boldsymbol{y}[p] = \boldsymbol{h}[p] + \boldsymbol{n}[p], \tag{4.5}$$

where $\boldsymbol{h}[p] \in \mathbb{C}^{M\times 1}$ represent the baseband channel, $\boldsymbol{n}[p] \sim \mathcal{CN}(0,\sigma^2\boldsymbol{I}_M)$ is a circularly symmetric complex Gaussian distributed additive noise vector. We define the received SNR at subcarrier p as $\|\boldsymbol{h}[p]\|^2/\sigma^2$. Next, we describe the mmWave channel model generation that is a parametric function of the multipath components.

4.3.3 Channel Model

A frequency-selective geometric channel model with N_c delay taps and L_c+1 paths [86] is considered. The channel consists of a LoS component, and L_c (yet unknown) reflections resulting from the scatterers as described earlier. The d-th delay tap is modeled as

$$\boldsymbol{h}_d = \sum_{\ell=0}^{L_c} \alpha_\ell\, p(dT_s - \tau_\ell)\boldsymbol{a}(\theta_\ell), \tag{4.6}$$

where $p(.)$ is the pulse-shaping filter, T_s is the sampling interval, α_ℓ, τ_ℓ, θ_ℓ represent the path gain, delay and the AoA of the ℓ-th path, respectively. The receiver array steering vector for the ℓ-th path is denoted by $\boldsymbol{a}(\theta_\ell) \in \mathbb{C}^{M\times 1}$. The index ℓ=0 is always associated with the LoS path. We can compactly represent the channel as $\boldsymbol{h}_d$=$\boldsymbol{A}\boldsymbol{\Delta}_d$, where $\boldsymbol{A}$=$[\boldsymbol{a}(\theta_0)\ \boldsymbol{a}(\theta_1)\ \ldots\ \boldsymbol{a}(\theta_{L_c})] \in \mathbb{C}^{M\times(L_c+1)}$ contains the receiver side steering vectors and

$$\boldsymbol{\Delta}_d = \left[\ \alpha_0 p(dT_s-\tau_0),\cdots,\alpha_{L_c} p(dT_s-\tau_{L_c})\ \right]^{\mathrm{T}}. \tag{4.7}$$

We obtain the frequency domain channel representation by taking a K-point DFT of the delay-domain channel, and the channel at subcarrier $k \in \{0,\ldots,K-1\}$ can be written as

$$\boldsymbol{h}[k] = \sum_{d=0}^{N_c-1} \boldsymbol{h}_d \exp\left(-\frac{j2\pi kd}{K}\right) = \boldsymbol{A}\boldsymbol{\Delta}[k], \tag{4.8}$$

and $\boldsymbol{\Delta}[k]$ is given by $\boldsymbol{\Delta}[k] = \sum_{d=0}^{N_c-1} \boldsymbol{\Delta}_d \exp\left(-\frac{j2\pi kd}{K}\right)$. Further substituting for $\boldsymbol{\Delta}_d$ from (4.7), we obtain

$$\boldsymbol{\Delta}[k] = \left[\beta_{k,0}\alpha_0, \beta_{k,1}\alpha_1, \ldots, \beta_{k,L_c}\alpha_{L_c}\right]^{\mathrm{T}}, \tag{4.9}$$

where,

$$\beta_{k,\ell} = \sum_{d=0}^{N_c-1} p(dT_s - \tau_\ell) \exp\left(-\frac{j2\pi kd}{K}\right). \tag{4.10}$$

Substituting $\boldsymbol{\Delta}[k]$ in (4.8), a compact form of the frequency domain channel $\boldsymbol{h}[k]$ can be obtained as

$$\boldsymbol{h}[k] = \boldsymbol{A}\boldsymbol{\beta}_k\boldsymbol{\alpha}, \tag{4.11}$$

where,

$$\boldsymbol{\beta}_k = \mathrm{diag}\left(\beta_{k,0},\ldots,\beta_{k,L_c}\right), \tag{4.12}$$

and $\boldsymbol{\alpha} = [\alpha_0,\ldots,\alpha_{L_c}]^{\mathrm{T}}$. Further substituting (4.11) in (4.5), the received frequency domain signal $\boldsymbol{y}[p]$ of the pilot index p can be written as

$$\boldsymbol{y}[p] = \boldsymbol{\Psi}_p\boldsymbol{\alpha} + \boldsymbol{n}[p], \tag{4.13}$$

where $\boldsymbol{\Psi}_p = \boldsymbol{A}\boldsymbol{\beta}_p \in \mathbb{C}^{M\times(L_c+1)}$.

4.4 Sensing Aided Channel Estimation

In this section, we provide a channel estimation framework that incorporates the sensing information available at the gNB. From (4.13), the received P pilots in vectorized form is given by

$$\boldsymbol{y} = \left[\boldsymbol{y}^{\mathrm{T}}[0]\,\boldsymbol{y}^{\mathrm{T}}[1]\ldots\boldsymbol{y}^{\mathrm{T}}[P-1]\right]^{\mathrm{T}}, \tag{4.14}$$

$$\boldsymbol{y} = \underbrace{\left[\boldsymbol{\Psi}_0^{\mathrm{T}}\boldsymbol{\Psi}_1^{\mathrm{T}}\cdots\boldsymbol{\Psi}_{P-1}^{\mathrm{T}}\right]^{\mathrm{T}}}_{\boldsymbol{\Omega}}\boldsymbol{\alpha} + \boldsymbol{n}, \tag{4.15}$$

where the matrix $\boldsymbol{\Omega} \in \mathbb{C}^{MP\times(L_c+1)}$ carries the delay-angle information of the multipath components and $\boldsymbol{n}$ is the vectorized noise $\boldsymbol{n} = [\boldsymbol{n}^{\mathrm{T}}[0]\boldsymbol{n}^{\mathrm{T}}[1]\cdots\boldsymbol{n}^{\mathrm{T}}[P-1]]^{\mathrm{T}}$.

Moreover, the sensing information can be used as an initial estimate of the multipath delays and angles. Let $\tilde{\boldsymbol{\theta}} = [\theta_0, \tilde{\theta}_1, \tilde{\theta}_2, \ldots, \tilde{\theta}_{L_r}]$, where θ_0 is the angle associated with the LoS path and $\tilde{\theta}_\ell$, $\ell \in [1, L_r]$ is the AoA of the ℓ-th path obtained from the sensing information. The propagation delay between the gNB and the ℓ-th, $\ell \in [1, L_r]$, scatterer is denoted by τ_ℓ^{rad}. Let us define $\tilde{\boldsymbol{\tau}} = [\tau_0, \tilde{\tau}_1, \tilde{\tau}_2, \ldots, \tilde{\tau}_{L_r}]$, where τ_0 is the delay between the UE and the gNB, and the delay of the ℓ-th communication path can be estimated using the radar delay τ_ℓ^{rad} as

$$\tilde{\tau}_\ell = \tau_\ell^{rad} + \tau'_\ell, \tag{4.16}$$

where τ'_ℓ is obtained using triangle laws of cosines as shown in Fig. 4.6,

$$\tau'_\ell = \sqrt{\tau_0^2 + \left(\tau_\ell^{rad}\right)^2 - 2\tau_0(\tau_\ell^{rad})cos(\tilde{\theta}_\ell - \theta_0)}. \tag{4.17}$$

Similar to the matrix $\boldsymbol{\Omega}$ in (4.15), using the sensing information $(\tilde{\boldsymbol{\tau}}, \tilde{\boldsymbol{\theta}})$, we can construct a matrix $\bar{\boldsymbol{\Omega}} \in \mathbb{C}^{MP\times(L_r+1)}$ that captures the delay-angle information of the L_r+1 paths. As we described earlier, only a subset of L_c among the L_r scatterers are included in the communication channel, and L_c is unknown. This can be mathematically represented as

$$\boldsymbol{\Omega} = \bar{\boldsymbol{\Omega}}\boldsymbol{B} + \boldsymbol{E}, \tag{4.18}$$

where $\boldsymbol{B} \in \mathbb{R}^{(L_r+1)\times(L_c+1)}$ is obtained by selecting L_c+1 columns of the identity matrix $\boldsymbol{I}_{L_r+1}$. The indices of the columns that are included in $\boldsymbol{B}$, correspond to the paths that are present both in the communication channel and sensing information. The unknown error term is denoted by $\boldsymbol{E}$.

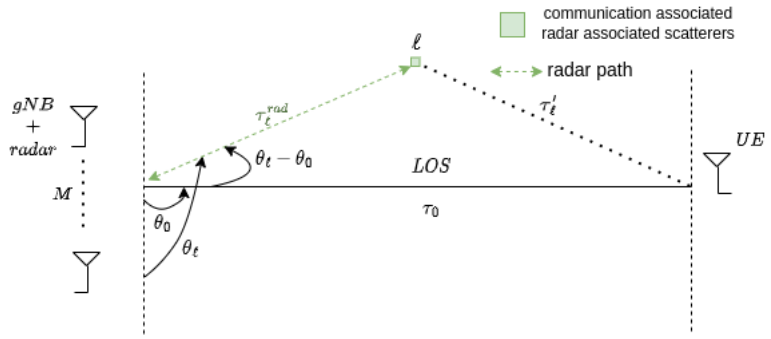


Figure 4.6: Communication delay estimation from the delay available in Sensing information.

4.4.1 Problem Formulation

Utilizing the received pilot signal (4.15) and the sensing information in the form of (4.18), the maximum a posteriori (MAP) based channel estimation problem is formulated as:

$$\left[\boldsymbol{\Omega}^*, \boldsymbol{\alpha}^*\right] = \arg\max_{\boldsymbol{\Omega},\boldsymbol{\alpha}} p(\boldsymbol{\Omega}, \boldsymbol{\alpha} \mid \boldsymbol{y}), \tag{4.19}$$

where $p(.)$ represents the probability distribution and $\boldsymbol{\alpha}$ is the channel gain vector.

The optimization problem at hand is difficult to solve in general as a) it is hard to obtain the distribution $p(\boldsymbol{\Omega}, \boldsymbol{\alpha} \mid \boldsymbol{y})$ b) the combinatorial nature of the path association matrix $\boldsymbol{B}$ and the unknown error. A conventional approach to relax this problem and solve it using compressed sensing schemes, such as SBL, by considering a joint dictionary matrix consisting of finely spaced angles and delays. However, such a solution results in cubic complexity with respect to the dictionary dimensions, which has to be finely spaced to alleviate the off-grid errors. Hence, a two-stage SWOMP-SBL algorithm is proposed to overcome such high complexity.

4.5 SWOMP-SBL Algorithm

The proposed algorithm works in two stages. In the first stage, based on the sensing information, a SWOMP algorithm is used to find the paths and their respective AoAs that are associated with the communication. Based on these selected paths, a SBL inference algorithm is used in the latter stage to

obtain a finer estimate of the delays and their corresponding channel gains $\widehat{\boldsymbol{\alpha}}$. A schematic describing this two-stage algorithm is shown in Fig 4.7.

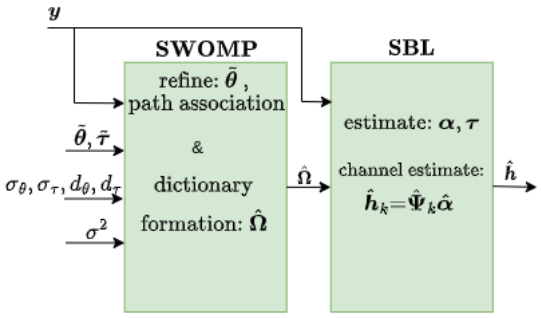


Figure 4.7: SWOMP-SBL algorithm.

4.5.1 SWOMP Stage

The algorithm is initialized with assuming that all the L_r+1 paths from the sensing information are present in the communication channel. The AoA's $\tilde{\boldsymbol{\theta}}$ are used to form the angle dictionary $\boldsymbol{A}'$ as described in steps 2 and 3 of the Algorithm 4.1. The SWOMP algorithm [91] outputs the maximum correlated paths $\hat{\boldsymbol{\theta}}$ corresponding to the angle dictionary $\boldsymbol{A}'$ with the received signal $\boldsymbol{y}$ as shown in Algorithm 4.2. The noise variance σ^2 is utilized as a stopping condition in SWOMP, where all the refined angles associated with the channel are estimated. The path index $p \in \boldsymbol{\chi}$ of a corresponding refined angle $\hat{\theta}_\ell$ is estimated using minimum absolute difference of $\hat{\theta}_\ell$ among the sensed angles $\tilde{\boldsymbol{\theta}}$. However, a dictionary matrix $\widehat{\boldsymbol{\Omega}}$ as defined in the step 18 of Algorithm 4.1 is needed to refine the delays further and estimate the channel gains. The path association matrix $\boldsymbol{B}$ can be obtained from the estimated $\boldsymbol{\chi}$, but it's avoided since the path indices are enough to create the dictionary matrix $\widehat{\boldsymbol{\Omega}}$. $\widehat{\boldsymbol{\Omega}}$ is constructed using the refined AoA $\hat{\boldsymbol{\theta}}$ obtained using SWOMP and a finely space dictionary matrix of the associated delays. The association of the path is given by the path indices $\boldsymbol{\chi}$ and maps the refined angles to their corresponding delays. The details of our algorithm are discussed in Algorithm 4.1. The refinement of the delays $\tilde{\boldsymbol{\tau}}$ and their corresponding channel gains $\boldsymbol{\alpha}$ are estimated using SBL with the obtained $\widehat{\boldsymbol{\Omega}}$ in the next stage. The computational complexity of SWOMP per iteration in the SWOMP stage is $MP(d_\theta L')^2 + MPd_\theta L_r + MPd_\theta L'$.

4.5.2 SBL Stage

Recalling the measurement equation with the obtained $\widehat{\boldsymbol{\Omega}}$, we write $\boldsymbol{y} = \widehat{\boldsymbol{\Omega}}\boldsymbol{\alpha} + \boldsymbol{n}$. We formulate the estimation method of $(\boldsymbol{\alpha}, \tilde{\boldsymbol{\tau}})$ using SBL as follows: SBL is a type-II maximum likelihood (MLH) estimation procedure to obtain the channel estimate [92, 93, 94]. In this method, we consider $\boldsymbol{\alpha}$ as a hidden variable, and obtain its posterior statistics given the observations. We impose a parameterized complex Gaussian prior on each column of the channel as $\mathcal{CN}(\boldsymbol{0}, \boldsymbol{\Gamma})$, where $\boldsymbol{\Gamma} = \text{diag}(\boldsymbol{\gamma})$. Using a common hyper-parameter $\boldsymbol{\gamma}$ across all the columns of $\boldsymbol{\alpha}$ aids in promoting common row sparsity in the solution. Now, we need to obtain the posterior distribution of $\boldsymbol{\alpha}$, and the hyper-parameter $\boldsymbol{\gamma}$. Since the prior and the noise are both Gaussian, obtaining the posterior statistics of $\boldsymbol{\alpha}$ is straightforward. But, computing $\boldsymbol{\gamma}$ requires computing the marginal probability distribution $p(\boldsymbol{y};\boldsymbol{\gamma})$ and maximizing it w.r.t. $\boldsymbol{\gamma}$, which is called evidence maximization or type-II maximum likelihood estimation.

To solve this, we use the expectation maximization (EM) algorithm, which works by lower bounding the logarithm of the evidence $p(\boldsymbol{y};\boldsymbol{\gamma})$, and maximizing it iteratively. We treat $\boldsymbol{\alpha}$ as a hidden variable. In the expectation (E) step, we compute the expectation of the log likelihood of $(\boldsymbol{y}, \boldsymbol{\alpha})$ w.r.t. $p(\boldsymbol{\alpha}|\boldsymbol{y}, \boldsymbol{\gamma})$. In the maximization (M) step, we compute the hyper-parameter $\boldsymbol{\gamma}$ by maximizing the function obtained in

Algorithm 4.1 SWOMP Stage

Require: $\boldsymbol{y}, \tilde{\boldsymbol{\theta}}, \tilde{\boldsymbol{\tau}}, d_\theta, d_\tau, \sigma_\theta, \sigma_\tau, \sigma^2$ //d_θ, d_τ - angle, delay dictionary size

1: Initialize: $\boldsymbol{\chi} = \{\}$

2: $\boldsymbol{\theta}'_l = \tilde{\theta}_l - 2\sigma_\theta : \frac{4\sigma_\theta}{d_\theta} : \tilde{\theta}_l + 2\sigma_\theta \in \mathbb{R}^{1\times d_\theta}$

3: $\boldsymbol{A}' = [a(\boldsymbol{\theta}'_0)\ a(\boldsymbol{\theta}'_1)\ \cdots\ a(\boldsymbol{\theta}'_{L_r})] \in \mathbb{C}^{M\times d_\theta(L_r+1)}$

4: $\hat{\boldsymbol{\theta}} = \mathbf{SWOMP}(\boldsymbol{y}, \boldsymbol{A}', \sigma^2)$ // **SWOMP**(.) defined in Algorithm 4.2

5: $\hat{\boldsymbol{\theta}} \in \mathbb{R}^{1\times L'}$ is $\{\hat{\theta}_\ell \mid \ell = 0, 1, \cdots, L'-1\}$

6: //**Path association:**

7: for $\ell = 0 : L'-1$

8: $\quad p = \arg\min\{|\hat{\theta}_\ell \mathbf{1} - \tilde{\boldsymbol{\theta}}|\}$ // $\mathbf{1} \in 1^{1\times(L_r+1)}$

9: $\quad \boldsymbol{\chi} = \boldsymbol{\chi} \cup p$ //p = path index

10: end

11: $\tilde{\boldsymbol{\tau}}(\boldsymbol{\chi}) \in \mathbb{R}^{1\times L'} = \{\tilde{\tau}_\ell(\boldsymbol{\chi}) \mid \ell = 0, 1, \cdots, L'-1\}$ //Delays of the corresponding path index obtained in step 9

12: $\hat{\boldsymbol{\tau}}_\ell = \tilde{\tau}_\ell(\boldsymbol{\chi}) - 2\sigma_\tau : \frac{4\sigma_\tau}{d_\tau} : \tilde{\tau}_\ell(\boldsymbol{\chi}) + 2\sigma_\tau \in \mathbb{R}^{1\times d_\tau}$

13: $\hat{\boldsymbol{\tau}} = [\hat{\boldsymbol{\tau}}_0\ \hat{\boldsymbol{\tau}}_1\ \cdots\ \hat{\boldsymbol{\tau}}_{L'-1}] \in \mathbb{R}^{1\times d_\tau L'}$

14: Compute $\boldsymbol{\beta}_k$ using $\hat{\boldsymbol{\tau}}$ as defined in (4.10), (4.12) and is denoted as $\hat{\boldsymbol{\beta}}_k \in \mathbb{C}^{d_\tau L'\times d_\tau L'}$

15: $\hat{\boldsymbol{A}}_\ell = [a(\hat{\theta}_\ell)a(\hat{\theta}_\ell)\cdots a(\hat{\theta}_\ell)] \in \mathbb{C}^{M\times d_\tau}$ //Repeat d_τ times

16: $\hat{\boldsymbol{A}} = [\hat{\boldsymbol{A}}_0\ \hat{\boldsymbol{A}}_1\ \cdots\ \hat{\boldsymbol{A}}_{L'-1}] \in \mathbb{C}^{M\times d_\tau L'}$

17: $\hat{\boldsymbol{\Psi}}_k = \hat{\boldsymbol{A}}\hat{\boldsymbol{\beta}}_k \in \mathbb{C}^{M\times d_\tau L'}$

18: $\hat{\boldsymbol{\Omega}} = [\hat{\boldsymbol{\Psi}}_0^{\mathrm{T}}\hat{\boldsymbol{\Psi}}_1^{\mathrm{T}}\cdots\hat{\boldsymbol{\Psi}}_{P-1}^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{C}^{MP\times d_\tau L'}$

Ensure: $\hat{\boldsymbol{\Omega}}$

the E step. More details of SBL and type-II MLH estimation can be found in [92, 95]. Detailed steps of multiple measurement vector SBL (MSBL) to compute the posterior mean and covariance of the channel gains, and the hyper-parameters are shown in Algorithm 4.3. Specifically, in Algorithm 4.3, the E-step of the EM algorithm corresponds to the computation of $\boldsymbol{\Sigma}_y^t$, $\boldsymbol{\Sigma}^t$ and $\widehat{\boldsymbol{\alpha}}$, and the M-step corresponds to the computation of $\boldsymbol{\Gamma}$. The SBL algorithm outputs the estimate of the channel gains $\widehat{\boldsymbol{\alpha}}$. Using step 17 in Algorithm 4.1, the channel estimate $\hat{\boldsymbol{h}}$ at the k-th subcarrier can be obtained for all the K subcarriers by

$$\hat{\boldsymbol{h}}_k = \hat{\boldsymbol{\Psi}}_k \widehat{\boldsymbol{\alpha}}, \tag{4.20}$$

The convergence properties of the SBL algorithm are well understood in the literature [92]. In short, using similar arguments in [92], we can show that the proposed SBL converges to the sparsest solution when the noise variance is zero and to a sparse local minimum, irrespective of the noise variance.

The computational complexity of each iteration of SBL is $(MP)^3 + 2(MP)^2 d_\tau L' + 2(d_\tau L')^2 MP + 2MPd_\tau L' + 2d_\tau L'$. Finally, the choice of the parameters $2\sigma_\tau$ and $2\sigma_\theta$ considered to refine both $\tilde{\boldsymbol{\tau}}$ and $\tilde{\boldsymbol{\theta}}$ in the Algorithm 4.1 is from the knowledge of the error distribution that most of the error lies within two standard deviations.

4.6 Simulation Results

In this section, we evaluate the performance of our proposed SWOMP-SBL algorithm in the uplink channel estimation utilizing the sensing information available at the gNB. We present the numerical

Algorithm 4.2 SWOMP

Require: $\boldsymbol{y}, \boldsymbol{A}', \sigma^2$

Initialize: $t = 0$, $w = \{\}$.
repeat
  $\boldsymbol{g} = \sum_{p=0}^{P-1} |(\boldsymbol{A}')^{\mathrm{H}} \boldsymbol{y}[p]]|$
  $q = \arg\max(\boldsymbol{g})$
  $w = w \cup q$
  MSE = 0
  for $p = 0 : P-1$
    $\boldsymbol{x}^t[p] = ((\boldsymbol{A}'_w)^{\mathrm{H}}(\boldsymbol{A}'_w))^{-1}(\boldsymbol{A}'_w)^{\mathrm{H}} \boldsymbol{y}[p]$ //$\boldsymbol{A}'_w = \boldsymbol{A}'(:, w)$
    $\boldsymbol{y}^t[p] = \boldsymbol{y}[p] - \boldsymbol{A}'_w \boldsymbol{x}^t[p]$
    MSE = MSE + $\boldsymbol{y}^t[p]^{\mathrm{H}} \boldsymbol{y}^t[p]$
  end
until MSE $< \sigma^2$

Ensure: w //Indices of the angles in the dictionary $\boldsymbol{A}'$

Algorithm 4.3 SBL Stage

Require: $\boldsymbol{y}$, $\widehat{\boldsymbol{\Omega}}$, $p_{\boldsymbol{y}}(\boldsymbol{y} \mid \widehat{\boldsymbol{\Omega}}, \boldsymbol{\alpha}), \sigma^2$

Initialize: $t = 0$, $\boldsymbol{\Gamma} = \boldsymbol{I}^{d_\tau L' \times d_\tau L'}$
repeat
  //Estimate $\boldsymbol{\alpha}$
  $\boldsymbol{\Sigma}_y^t = \sigma^2 \boldsymbol{I} + \widehat{\boldsymbol{\Omega}} \boldsymbol{\Gamma} \widehat{\boldsymbol{\Omega}}^{\mathrm{H}}$.
  $\widehat{\boldsymbol{\Sigma}}^t = \boldsymbol{\Gamma} - \boldsymbol{\Gamma} \widehat{\boldsymbol{\Omega}}^{\mathrm{H}} \left(\boldsymbol{\Sigma}_y^t\right)^{-1} \widehat{\boldsymbol{\Omega}} \boldsymbol{\Gamma}$.
  $\widehat{\boldsymbol{\alpha}}^t = \frac{1}{\sigma^2} \widehat{\boldsymbol{\Sigma}}^t \widehat{\boldsymbol{\Omega}}^{\mathrm{H}} \boldsymbol{y}$.
  //Hyper-parameters Update
  $\gamma_i^t = |\widehat{\boldsymbol{\alpha}}_i^t|^2 + \boldsymbol{\Sigma}_y^t[i, i]$
  $\Gamma = \mathrm{diag}(\gamma_1^t, \gamma_2^t, \ldots, \gamma_{d_\tau L'}^t)$
until Convergence

results obtained using MATLAB, considering a single transmit antenna UE in two scenarios based on the number of receive antennas at the gNB: one scenario with $M = 32$ receive antennas, and the other with $M = 1$ receive antenna. Additionally, we also present the numerical results obtained from the OAI using rfsimulator denoted as OAI RFSIM, as described in Section 2.2.1.4, specifically for the single antenna scenario, while considering the effects of fixed-point implementation.

Our simulation scenario involves a static gNB while the UE moves in 1 meter (m) increments, starting from an initial distance of 1 m from the gNB and continuing up to 40 m in a straight line, as illustrated in Figure 4.8. The multipath channel between the gNB and the UE, which includes multiple scatterers/reflectors, is simulated using the MATLAB raytracer with the locations of the gNB and UE. The locations of the gNB and UE are GPS coordinates derived from an OpenStreetMap, specifically corresponding to a drone cage located at Northeastern University in Burlington. An example of the multipath generated by the raytracer in the presence of multiple scatterers in a 3D scenario can be seen in Figure 4.9.

The ideal sensing information at a fixed location of gNB and UE is the actual delay information ($\bar{\tau}_\ell$) between the gNB and the scatterers and the angle information ($\bar{\theta}_\ell$) is obtained from the MATLAB

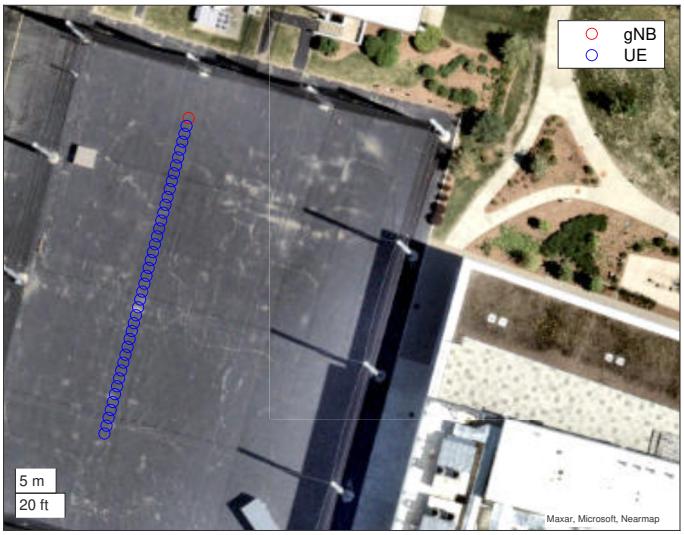


Figure 4.8: Matlab Raytracing Scenario for Sensing aided channel estimation.

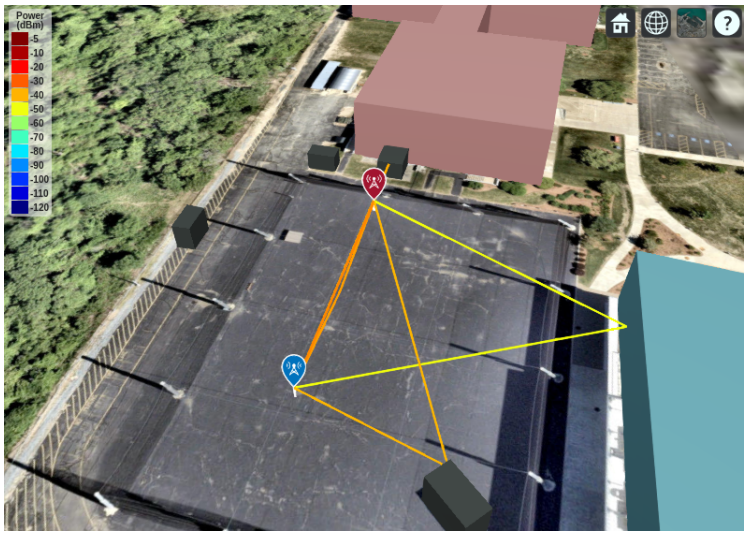


Figure 4.9: Matlab Raytracing multipath Scenario in 3D for Sensing aided channel estimation.

raytracer. In contrast, the sensing information with error incorporates an angular error with $\sigma_\theta = 3°$ and a timing error with $\sigma_\tau = T_s$ to the sensing information from MATLAB. Additionally, we consider that not all scatterers provided by the sensing information in $\mathcal{S}_r$ are not necessarily associated with the communication channel.

For each monte-carlo iteration, we randomly choose a UE position within a gNB-UE distance of 1 m to 40 m for the performance evaluation. Further, to simulate the scenario of unassociated scatterers, we introduce a random number of additional scatterers drawn from a uniform distribution $\mathcal{U}(1,4)$ into the sensing information for each position of the UE. The delay and angle information of each additional scatterer is drawn randomly from a uniform distribution $\frac{\mathcal{U}(1,40)}{c}$ and $\mathcal{U}(0,180)$, respectively, where c is the speed of light. In our simulations, SRS in the 5G standards [96] is utilized as the pilots in the uplink for the channel estimation. The arrangement of these pilots in the OFDM grid follows a comb structure as specified in the 3GPP standard [96]. Specifically, there is one pilot for every K_c subcarriers, as illustrated in Figure 4.10.

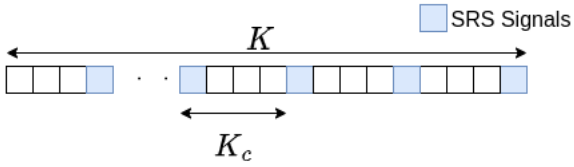


Figure 4.10: Uplink SRS comb structure in an OFDM symbol.

To evaluate the performance of our proposed algorithm, we consider a wideband scenario where the uplink channel is estimated using the classical algorithms with a standard number of pilots. We then compare the normalized mean square error (NMSE) of the estimated channel in the wideband scenario to the NMSE of the channel estimated using fewer pilots, known as a narrowband scenario. The NMSE between a true channel $\boldsymbol{h}$ and the estimated channel $\hat{\boldsymbol{h}}$ is defined as,

$$\text{NMSE} = \frac{||\boldsymbol{h} - \hat{\boldsymbol{h}}||^2}{||\boldsymbol{h}||^2}. \tag{4.21}$$

In the wideband scenario, we utilize classical algorithms like least squares (LS) and SWOMP for uplink channel estimation, referred to as **WB + LS** and **WB + SWOMP**, respectively, with $P = 624$ pilots and a comb size K_c^{WB}. In the case of a narrowband scenario, the performance of our proposed channel estimation procedure, which accounts for erroneous sensing information, is denoted as **NB + SWOMP-SBL + Sensing Info Error** in the plot. We compare this to channel estimation performance using LS with ideal sensing information, where the channel gains $\hat{\boldsymbol{\alpha}}$ are estimated using LS, assuming ideal sensing information is available at the gNB. This scenario is labeled as **NB + Ideal Sensing Info + LS** in the plot using $P = 16$ pilots and a comb size of K_c^{NB}. The system parameters utilized in these simulations are detailed in Table 4.1. Further, the NMSE performance of the uplink channel estimation for $M = 32$ and $M = 1$ receive antennas at the gNB is discussed in the section below.

Table 4.1: System Parameters used for Sensing aided channel estimation

Parameters	Values
System bandwidth	38.16 MHz
Subcarrier spacing	30 KHz
Sampling Period (T_s)	21.70 ns
Centre frequency	3.69 GHz
Sampling rate	46.08 MHz
FFT size (K)	1536
Cyclic prefix (N_{cp})	132
Wideband comb size (K_c^{WB})	2
Narrowband comb size (K_c^{NB})	78
Delay taps (N_c)	132
σ_θ	3°
σ_τ	T_s

4.6.1 Multiple Receive Antennas

In the case of a narrowband scenario with $M = 32$ receive antennas, the erroneous AoA from the sensing information is refined using SWOMP with a dictionary matrix considering d_θ=500 as described in the Algorithm 4.1. Further, the channel gains $\widehat{\alpha}$ are estimated using SBL considering d_τ=50. The channel is estimated using classical LS and SWOMP methods in a wideband scenario. Both algorithms utilize a dictionary that is discretized in the angular domain ranging from 0° to 180°, with a dictionary size of 500.

From Fig. 4.11, we can see that with sensing information, SWOMP-SBL based channel estimation algorithm has a significant gain in the NMSE compared to the wideband classical LS and greedy SWOMP algorithm with fewer pilots and robust to the errors in the sensing information. Hence, we reduce the pilot overhead from $P = 624$ to $P = 16$ by 97.43%.

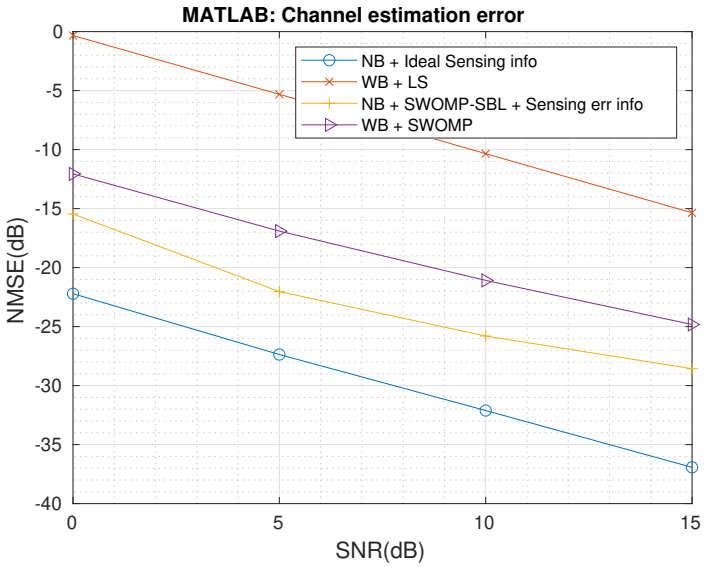


Figure 4.11: SNR vs NMSE of the channel estimates for M = 32 antennas.

Algorithm 4.4 Simplified SWOMP Stage

Require: $y, \tilde{\tau}, d_\tau, \sigma_\tau, \sigma^2$

1: $\hat{\tau}_\ell = \tilde{\tau}_\ell - 2\sigma_\tau : \frac{4\sigma_\tau}{d_\tau} : \tilde{\tau}_\ell + 2\sigma_\tau \in \mathbb{R}^{1\times d_\tau} \mid \ell = 0, 1, \cdots, L'-1\}$

2: $\hat{\tau} = [\hat{\tau}_0\ \hat{\tau}_1\ \cdots\ \hat{\tau}_{L'-1}] \in \mathbb{R}^{1\times d_\tau L'}$

3: Compute β_k using $\hat{\tau}$ as defined in (4.10), (4.12) and is denoted as $\hat{\beta}_k \in \mathbb{C}^{d_\tau L'\times d_\tau L'}$

4: $\hat{\Psi}_k = \text{diag}(\hat{\beta}_k) \in \mathbb{C}^{1\times d_\tau L'}$

5: $\widehat{\Omega} = [\hat{\Psi}_0^{\mathrm{T}} \hat{\Psi}_1^{\mathrm{T}} \cdots \hat{\Psi}_{P-1}^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{C}^{P\times d_\tau L'}$

Ensure: $\widehat{\Omega}$

4.6.2 Single Receive Antenna

In the case of a narrowband scenario with single receive antennas (i.e., $M = 1$), the SWOMP stage in Algorithm 4.1 is simplified to the Algorithm 4.4, since the angle refinement is not necessary. Further, the channel gains $\widehat{\alpha}$ are estimated using SBL considering d_τ=100. The classical LS method is utilized for channel estimation in a wideband scenario.

The numerical results from MATLAB are shown in Figure 4.12. These results indicate that, when utilizing sensing information, the SWOMP-SBL-based channel estimation algorithm significantly improves the NMSE compared to the classical wideband LS method, even when using fewer pilots. We successfully reduce the pilot overhead from $P = 624$ to $P = 16$, resulting in a pilot overhead reduction of 97.43%.

Furthermore, we also present the numerical results obtained using OAI in RFSIM mode alongside MATLAB results for a single receive antenna case. In this mode, the multipath information for each UE position, ranging from a gNB-UE distance of 1 m to 40 m, obtained from the MATLAB raytracer, is provided as input to the OAI RFSIM. The OAI RFSIM then generates a channel based on this multipath information and applies it to the transmitted SRS. The received SRS for each UE position is then stored for offline channel estimation. In this case, the channel generated by the OAI RFSIM is considered a ground truth. Note that this approach also considers the impairments caused by the fixed-point representation of a real-time system.

The numerical results from OAI RFSIM are presented in Figure 4.13. Here, we observe that, with the inclusion of sensing information, the SWOMP-SBL-based channel estimation algorithm again demonstrates a significant gain in NMSE compared to the wideband classical LS method, even with fewer pilots and robustness against errors in the sensing information. Moreover, we can observe that the channel estimation performance in OAI RFSIM degrades for all algorithms compared to that in MATLAB simulations. This degradation in the performance is caused by the fixed-point operations in OAI RFSIM.

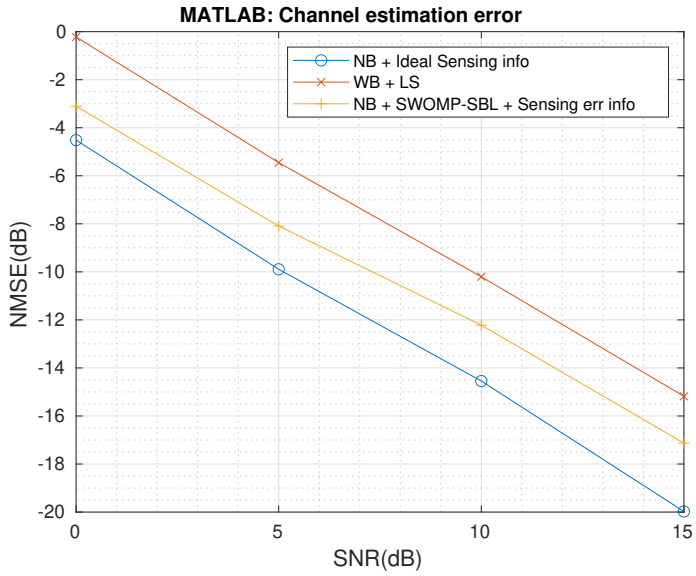


Figure 4.12: SNR vs NMSE of the channel estimates for M = 1 antenna.

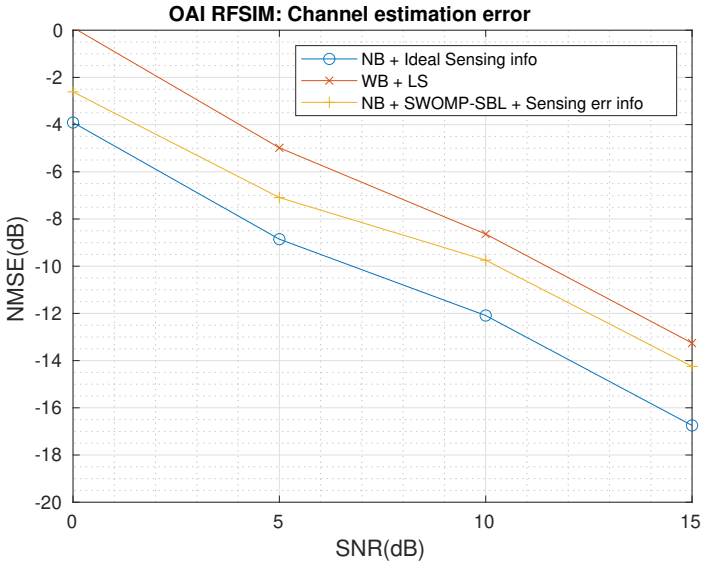


Figure 4.13: SNR vs NMSE of the channel estimates for M = 1 antenna.

4.7 Conclusions

In this chapter, we have studied the uplink channel estimation aided by sensing information available at the gNB. We proposed a framework utilizing the proposed signaling mechanisms in Chapter 3, making it robust to impairments such as clock drift and timing correction loops for fusing sensing information. We have also shown how the proposed signaling mechanisms in Chapter 3 enable uplink sensing. The proposed SWOMP-SBL algorithm uses fewer uplink pilots than traditional methods by incorporating sensing information. The proposed scheme is also robust to erroneous sensing information, including additional paths available in the sensing information but not associated with the communication. We presented the simulation results conducted in MATLAB for both multiple and single receive antennas at the gNB. Additionally, we evaluated the simulation results from OAI RFSIM, which account for the effects of fixed-point implementation in the case of a single receive antenna. Our simulation results have validated the superior performance of the proposed SWOMP-SBL scheme using fewer pilots compared to conventional state-of-the-art algorithms.

Chapter 5

Localization in a Digital Twin

So far, in this dissertation, we have discussed several localization and sensing techniques considered for 5G and beyond systems. However, validating these techniques using experimental prototypes is crucial for a successful real-world deployment. Conducting large-scale outdoor experiments can be challenging due to the need to transport heavy testing equipment and the potential impact of weather conditions such as rain and snow. To address these challenges, a digital twin platform that can emulate outdoor conditions is invaluable. In this chapter, we consider validating our proposed signaling scheme for localization in a digital twin platform called Colosseum.

5.1 Introduction

The Colosseum platform [97, 98, 99, 100, 101] at Northeastern University allows for the real-time emulation of the outdoor environments acting as a digital twin. Several works [102, 103, 104, 105, 106] have utilized the Colosseum as a digital twin to test and validate their algorithms in real-time by emulating an outdoor environment. The authors in [102] utilize the Colosseum as a digital twin to emulate a real-world scenario of a ship moving across Waikiki Beach in Honolulu, Hawaii, to test their spectrum sensing algorithm. In [103], the authors use Colosseum to create a digital twin that simulates a traffic generation scenario, classifying various types of traffic in 5G, including enhanced mobile broadband (eMBB), massive machine-type communications (MMTC), and ultra-reliable low-latency communications (URLLC). Additionally, the authors in [104] utilize Colosseum to deploy various nodes of integrated access and backhaul throughout different areas of Florence, Italy, emulating a real-world scenario. However, all the works mentioned above rely on a static scenario, where a scenario recorded offline is replayed using Colosseum. In contrast, the authors in [106] integrate the simulation of urban mobility (SUMO) simulator with the Colosseum to generate a real-time dynamic scenario. In this approach, the scenario in the Colosseum is updated dynamically using data obtained from the SUMO simulator in real-time.

Creating a real-world scenario in Colosseum begins with the development of a 3D model of the environment using tools like OpenStreetMap [107] or Blender [108]. This 3D model is then used to obtain multipath wireless propagation information such as number of paths, path loss, and path delays through ray-tracing software such as MATLAB [109], Nvidia Sionna [110], or Wireless InSite [111], based on the locations of the transmitter and receiver. With this multipath information from the raytracer, a wireless channel is generated, approximated, and converted into a specific format suitable for use with the Colosseum platform. It is important to note that the approximation of the wireless channel in the Colosseum is necessary due to its limitation of supporting only four taps. Consequently, a channel approximation mechanism that is close to reality, considering localization scenarios, is required. The Colosseum platform applies the wireless channel to transmitted signals via SDRs.

To address the challenge of channel approximation, the authors in [112] proposed using K-means clustering to represent the channel. They divided the available multipath information into K clusters (with K=4 for Colosseum) and calculated the centroids of these clusters. However, this approach is unrealistic because it alters the existing multipath information by rounding the centroids to the nearest tap to meet the requirements of the Colosseum. This rounding can introduce inaccuracies in distance estimation during localization scenarios. For example, consider a LoS path with a delay that lies between two taps; rounding it to the nearest tap would lead to errors in distance estimation. Therefore, we proposed a raised-cosine based channel approximation mechanism that is close to real-world scenarios considering localization scenarios. A realistic channel approximation utilizing sinc-based approximation and preserving the energy is proposed in [113].

In this chapter, we propose using the Colosseum as a digital twin to emulate a wireless channel in a real-world scenario for evaluating localization performance. Additionally, we will compare the localization performance achieved in the Colosseum with the results obtained from an outdoor measurement campaign. Specifically, our contributions are as follows:

- We conducted a measurement campaign to evaluate our proposed RTT estimation mechanism, as described in Section 3.2, in an outdoor environment located at Northeastern University's Burlington campus.
- We developed a 3D model replicating the same outdoor environment at Northeastern University's Burlington campus using OpenStreetMap and generated multipath information with the raytracer tool in MATLAB.
- We proposed a realistic channel approximation mechanism accounting for localization scenarios to be utilized with the Colosseum platform.
- Finally, we evaluated our proposed RTT estimation mechanism on the Colosseum platform and compared the results to the outdoor measurements.

5.2 Colosseum as a Digital Twin

In this section, we discuss using the Colosseum platform as a digital twin. We start by describing the architecture of the Colosseum platform in the section below.

5.2.1 Colosseum Architecture

Colosseum is the world's largest wireless network emulator with a hardware-in-the-loop platform that is publicly available to the research community. Originally built by the defense Advanced research projects agency (DARPA) and by the Johns Hopkins University Applied Physics Laboratory to support the Spectrum Collaboration Challenge [114, 115, 116], Colosseum is being expanded and operated by the Institute for the Wireless Internet of Things at Northeastern University through an national science foundation (NSF) grant, which also made it publicly available to the research community [98, 99, 100, 101]. With its 256 SDRs and 128 remotely-accessible compute nodes and graphics processing units (GPUs), Colosseum provides the capabilities to test full-protocol stack solutions at scale with real hardware devices and in emulated—yet realistic—environments with complex channel interactions (e.g., path loss, fading, multipath). The system comprises five primary components:

1. **Standard Radio Nodes** : The standard radio node (SRN) is a state-of-the-art server with 48-core Intel Xeon E5-2650 CPUs and an NVIDIA Tesla K40m GPU and drives an NI/Ettus USRP X310. Each X310 is equipped with two UBX-160 daughterboards that operate between 10 MHz and 6 GHz. The Colosseum platform enables multiple users to deploy softwarized containers,

implemented via linux containers (LXCs), on the bare-metal SRN. These containers can run a variety of protocol stacks (such as 4G, 5G, and Wi-Fi) while allowing users to control various parameters and configurations at different layers within those stacks.

2. **Massive Channel Emulator** : The massive channel emulator (MCHEM) performs the channel emulation in the Colosseum. It consists of four interconnected quadrants, each equipped with four NI ATCA 3671 field programmable gate array (FPGA) modules and 16 Virtex-7 690T FPGAs. These components drive an array of 128 USRPs, which are connected one-to-one with the USRPs of the SRNs, as illustrated in Figure 5.2.

   When an RF transmission occurs in the Colosseum, the signals generated by the USRPs at the SRN side (such as signal s_1 in Figure 5.2) are transmitted to the corresponding USRP X310 in the MCHEM, which performs the RF to baseband and ADC conversions. The resulting digital signals are then forwarded to the FPGAs within the MCHEM, where they are processed using finite impulse response (FIR) filters. These FIR filters are composed of 512 precomputed complex-valued taps that capture the characteristics of the channel in the time domain, i.e., the CIR, between any pair of SRNs [1].

   As shown in Figure 5.2, for a specific RF scenario involving N SRNs, the FIR filters in the MCHEM load the precomputed 512-tap CIR vectors $\boldsymbol{h_{i,j}}$, which represent the channel response between node i and node j, where $i, j \in \{1, \ldots, N\}$. These channel taps are then applied to the transmit signals through a convolution operation. Thus, the signal received at the node j is obtained by,

$$\boldsymbol{y_j} = \sum_{i=1}^{N} \boldsymbol{h_{i,j}} * \boldsymbol{s_i}, \tag{5.1}$$

   where, '*' denotes the convolution operation. In (5.1), all the transmit signals from N SRNs (i.e., $\boldsymbol{s_i}, i \in \{1, \ldots, N\}$) after applying their respective CIRs are aggregated to emulate the effects of real wireless channels, including node interference and the superimposition of signals from multiple nodes. Finally, this aggregated received signal is sent to SRN j.

   The RF scenario server, depicted in Figure 5.1 and Figure 5.2, maintains a catalog of the Colosseum RF scenarios and feeds their channel taps to the channel emulator at run time. The RF Scenarios make it possible to emulate the effects of the wireless channel, including path loss and fading over terrains of up to 1km^2 and within a bandwidth of up to 80 MHz. The modular architecture of MCHEM with independent USRPs allows Colosseum to emulate different scenarios across various experiments, enabling multiple users to operate the system simultaneously. Users can select the specific scenario to run through a specialized control interface.

3. **GPU Nodes** : The platform offers high-performance NVIDIA GPU nodes that support computationally intensive applications such as AI and machine learning (ML)-based wireless network optimizations.

4. **Traffic Generator** : The traffic generator (TGEN) is designed to emulate IP traffic flows between the SRNs, similar to how MCHEM simulates RF scenarios. It is based on the U.S. Naval Research Laboratory's multi-generator (MGEN) [117] and can generate traffic flows that adhere to a defined traffic scenario, which includes characteristics such as packet rate, size, and distribution. Once a traffic scenario is initiated, packets are delivered to the SRNs, which handle them through the user-defined protocol stack, such as by transmitting them through a cellular or Wi-Fi stack.

5. **Management Infrastructure** : The management infrastructure of the Colosseum includes a range of auxiliary services such as (i) a website that allows users to reserve resources and initiate

[1] Due to the high computational complexity required to generate scenarios and the large storage space needed, only four channel taps contain non-zero values.

experiments, (ii) a resource manager that allocates resources to users, (iii) gateways that provide user and management access to Colosseum; (iv) a 900 TB network attached storage (NAS) system for storing LXC images, experiment data, logs and (v) various network services, including those that ensure time synchronization across the entire testbed.

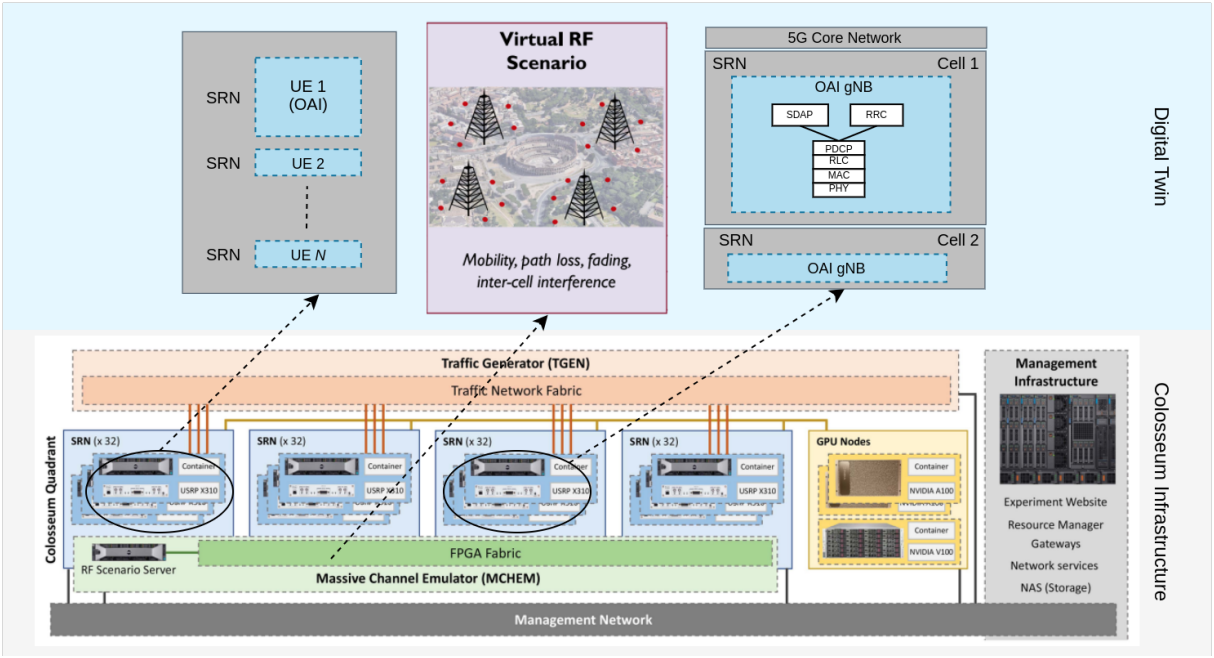


Figure 5.1: Colosseum Architecture.

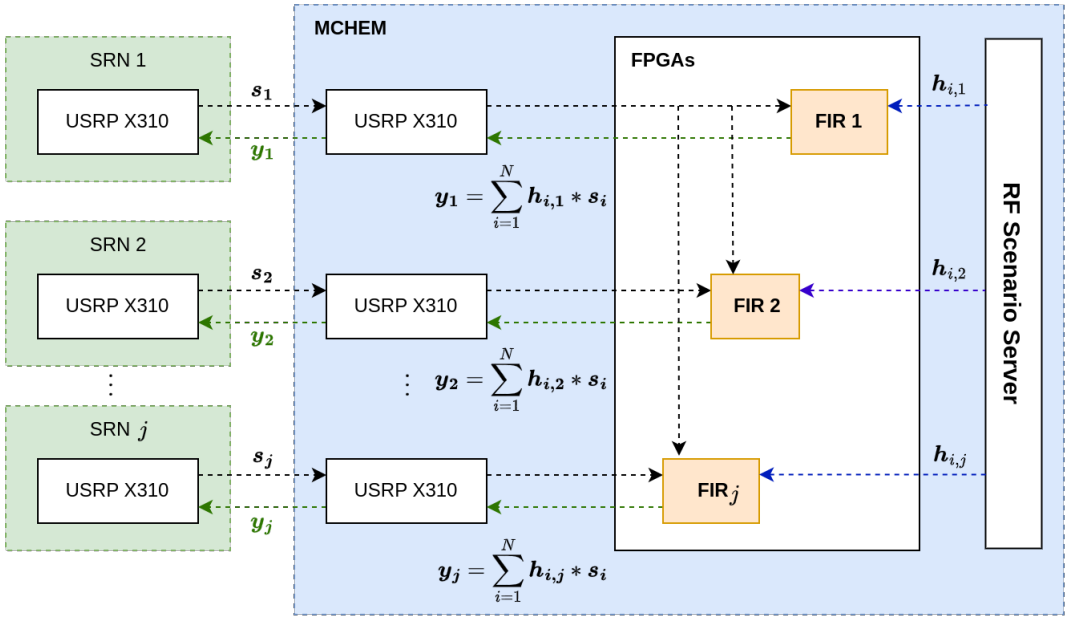


Figure 5.2: FPGA-based RF scenario emulation in Colosseum.

Thus, researchers can deploy, validate, and analyze full-protocol stack solutions across various wireless channel conditions utilizing the SRNs and MCHEM in the Colosseum, as per the user-defined RF

scenarios. This setup enables a hardware-in-the-loop digital twin for wireless networks. Also, it is crucial to generate RF scenarios that closely mimic real-world conditions to achieve realistic system performance. In the following sections, we will discuss the generation of RF scenarios in the Colosseum.

5.2.2 RF Scenario Generation Mechanism

The generation of RF scenarios in the Colosseum consists of 4 stages:

1. **3D Model Generation:** A 3D digital model of the physical environment is created, closely resembling the real world and accurately reflecting the material properties of various scatterers. Typically, tools like Blender or OpenStreetMap can be used to generate a 3D digital model.
2. **Raytracing:** The generated 3D model is then used to perform raytracing between the selected transmit location i and receive location j. This process yields multipath information, including the number of multipaths, path loss, phase shifts, and delays associated with each multipath. Typically, raytracing tools like MATLAB, NVIDIA Sionna, and Wireless Insite can be used to obtain this information.
3. **Channel Generation:** Based on the multipath information obtained from the raytracer, the wireless propagation channel at the d-th tap between the selected transmit location i and receive location j is modeled as,
$$h_d = \sum_{\ell=0}^{L-1} \alpha_\ell \rho(dT_s - \tau_\ell), \tag{5.2}$$
where, $\alpha_\ell = \alpha'_\ell e^{-j2\pi f_c \tau_\ell}$ is the complex channel gain of the ℓ-th path, α'_ℓ and τ_ℓ are the path-loss and delay of the ℓ-th path, f_c is the center frequency, T_s is the sampling period and $\rho(.)$ is the raised-cosine filter. Further, representing all the N_c taps as a vector, the CIR $\boldsymbol{h_{i,j}} \in \mathbb{C}^{N_c \times 1}$ between the transmit location i and receive location j is given by,
$$\boldsymbol{h_{i,j}} = \left[h_0, h_1, \ldots, h_{N_c-1}\right]^{\mathrm{T}}. \tag{5.3}$$
4. **Channel Approximation:** The generated channel $\boldsymbol{h_{i,j}}$ is approximated to contain non-zero values in only four channel taps. This simplification is essential due to the high computational complexity associated with FIR filter processing in the MCHEM of the Colosseum. The proposed channel approximation algorithm, which considers the localization use case, is detailed in the Algorithm 5.1. The four non-zero indices of the channel taps of a CIR $\boldsymbol{h_{i,j}}$ can be found in the set $\mathcal{W}$.

Algorithm 5.1 Raised-Cosine Channel Approximation

Require: $\boldsymbol{h_{i,j}}$, D

1: Initialize: $\mathcal{W} = \{q_1, q_2, q_3, q_4\}$

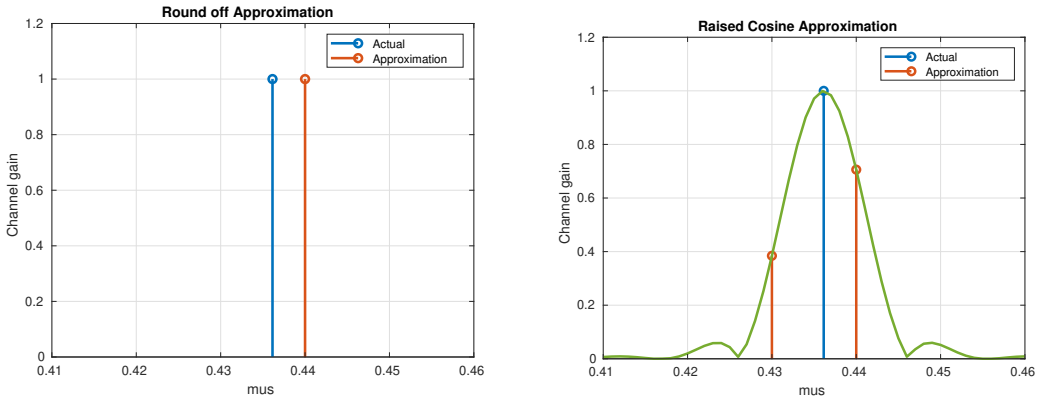
2: $q_1 = \left\lfloor \frac{f_s^m D}{c} \right\rfloor$, $q_2 = \left\lceil \frac{f_s^m D}{c} \right\rceil$

3: $q_3, q_4 = \underset{\neq\{q_1,q_2\}}{\arg\max} |\boldsymbol{h_{i,j}}|$ //Indices of the highest two peaks other than q_1, q_2

where, D is the distance between the nodes i and j, f_s^m is the sampling rate of the MCHEM and c is the speed of light.

Note that the channel generation and channel approximation proposed in this chapter considers the localization use cases compared to the one proposed by the authors in [112] currently used

in the Colosseum. The authors in [112] proposed utilizing K-means clustering to categorize the available multipath information into K clusters (set at K=4 for Colosseum) based on the delays associated with each multipath. They calculated the centroids of these clusters and rounded off to the nearest taps. However, this method is unrealistic because it alters the existing multipath information. Such rounding can introduce inaccuracies in distance estimation during localization scenarios. For instance, consider a LoS path with a delay that falls between two taps; rounding it to the nearest tap would result in errors in distance estimation, as illustrated in Figure 5.3a. In contrast, we propose a raised-cosine based channel approximation mechanism, which more accurately reflects real-world scenarios related to localization, as depicted in Figure 5.3b. Note that the sampling rate used in this case is $f_s^m = 100$ MHz (MCHEM sampling rate).



(a) Existing Channel Approximation

(b) Proposed Channel Approximation

Figure 5.3: Channel Approximation to fit in the MCHEM of the Colosseum.

Next, we describe the experimental scenarios to analyze the performance of the proposed PRS-SRS signaling scheme in outdoors and the Colosseum.

5.3 Experimental Scenario

In this section, we outline the experimental scenarios conducted outdoors using our proposed PRS-SRS signaling scheme, as discussed in Section 3.2.2. We also describe how we utilized OpenStreetMap to generate a 3D model replicating the same outdoor environment. Additionally, we describe how this 3D model is utilized in Colosseum to evaluate the localization performance of our PRS-SRS signaling scheme within a digital twin.

5.3.1 Outdoor Scenario

In the outdoor measurement campaign, we evaluate our proposed PRS-SRS signaling scheme as described in the Section 3.2.2. We consider a scenario with a single antenna gNB and a UE having LoS condition in a drone cage located at the Northeastern University, Burlington campus. We leverage on the OAI 5G NR protocol stack and USRP B210 SDRs to build the gNB and UE. Additionally, SC2430 NR signal conditioning module is used as an external RF front-end at the gNB. Both the gNB and UE are equipped with vertically polarized omni-directional antennas. The experimental setup outdoors using OAI gNB and UE can be seen in Figure 5.4. During the experiment, the gNB remains stationary while the UE is moved in 1 m increments, starting from an initial distance of 1 m and extending to 40 m, as shown in Figure 5.5. Throughout the measurement campaign, the LoS between the gNB and UE was maintained,

and the transmit and receive gains were kept constant. The estimated uplink SNR ranged from 25 dB to 30 dB. Multiple SRS channel estimates were collected at each distance, and the data was subsequently stored for further offline analysis.

Next, we describe how we used OpenStreetMap to generate a 3D model replicating this outdoor scenario.

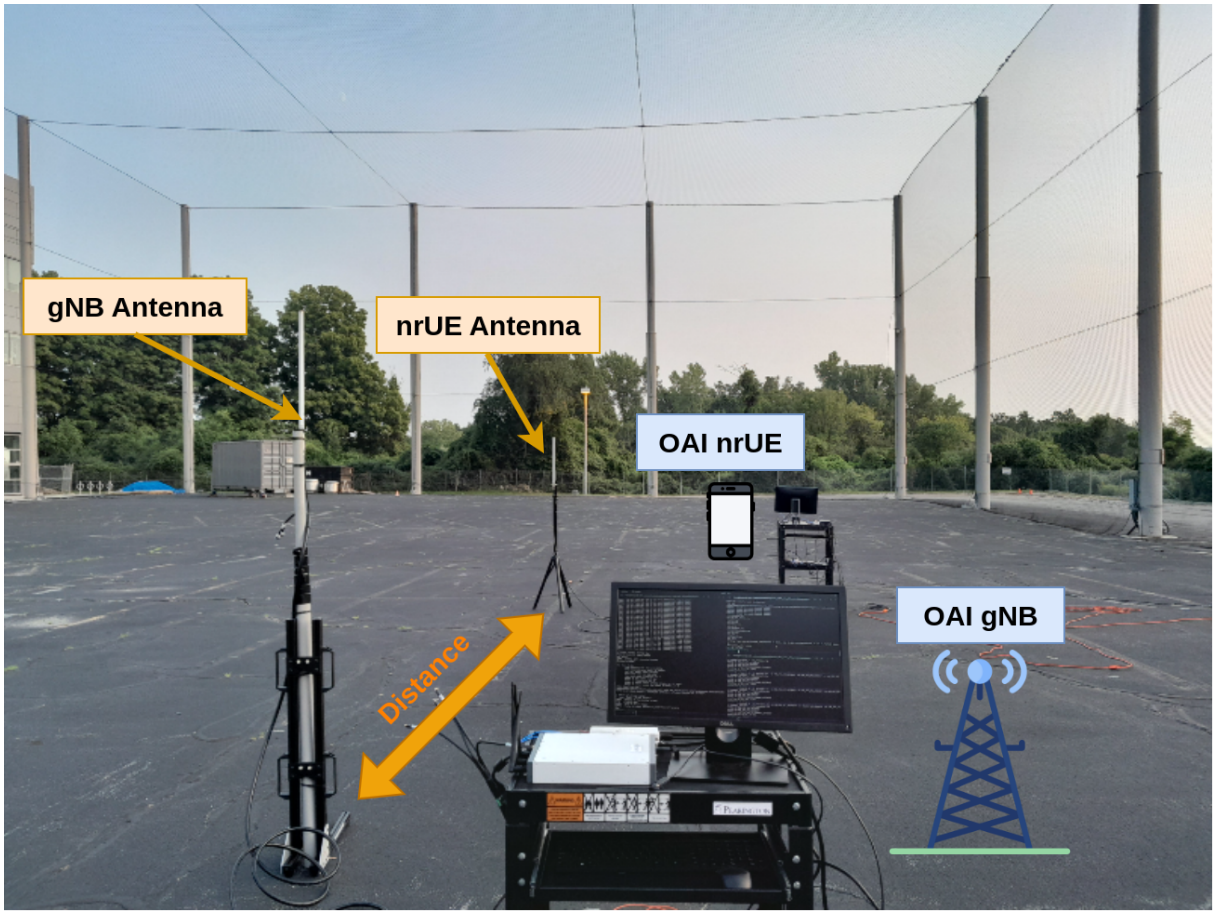


Figure 5.4: Outdoor measurement scenario in a Drone cage at Northeastern University.

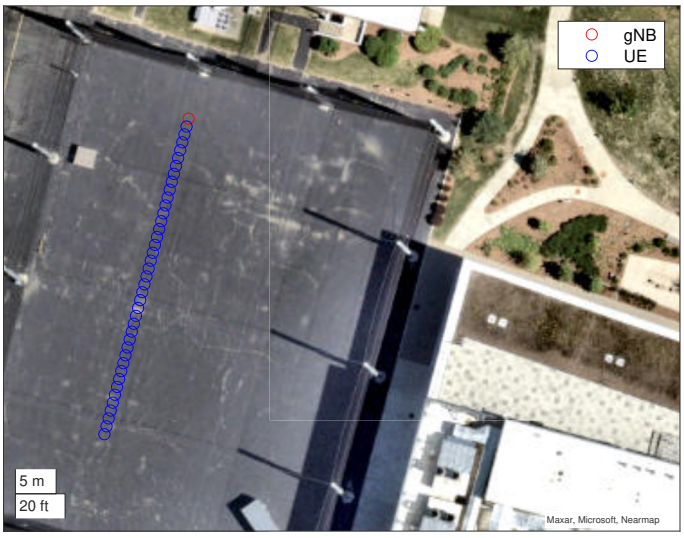


Figure 5.5: Various locations of gNB and UE in an outdoor measurement campaign scenario.

5.3.2 3D Model Generation

The outdoor measurement scenario mentioned in the Section 5.3.1, is replicated as a 3D model as follows:

1. The underlying 3D environment of the drone cage at Northeastern University, Burlington campus, is obtained from OpenStreetMap.
2. Additional scattering objects such as Container, Truck, and air-conditioner (AC) Container as shown in Figure 5.6 were added to the map to create an accurate 3D representation of the real world.
3. The properties of these scattering objects (e.g., brick, metal, and glass) have been appropriately set in MATLAB to ensure they closely match the actual materials.

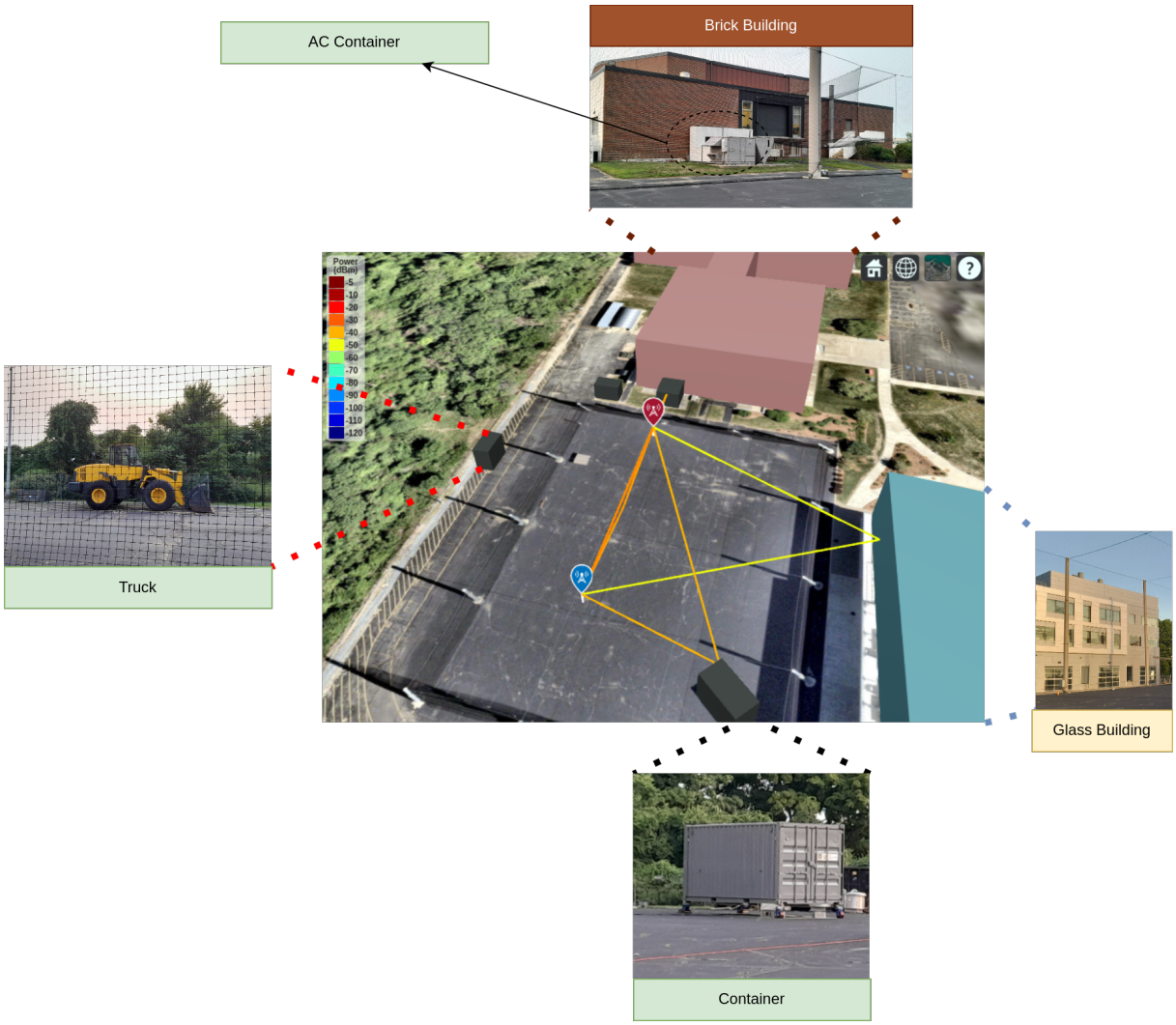


Figure 5.6: Matlab Raytracing multipath Scenario in 3D.

The locations of the gNB and UE in the outdoor measurement scenario, as described in Section 5.3.1 and illustrated in Figure 5.6, are replicated in the generated digital 3D model. Further, we describe how this 3D model is utilized in the Colosseum to emulate the wireless channel between the gNB and UE location in an outdoor environment.

5.3.3 Colosseum Scenario

The digital 3D model of an outdoor environment as described in Section 5.3.2 for a gNB, UE location is utilized in the Colosseum as follows:

1. Raytracing information such as the number of multipath, path delays, path loss, and phase shifts is obtained using the MATLAB raytracer for a transmit location i and receive location j.
2. The wireless channel $\boldsymbol{h_{i,j}}$ between the transmit location i and receive location j is determined using (5.2).
3. Due to limitations within the Colosseum, the wireless channel $\boldsymbol{h_{i,j}}$ is approximated to four delay taps, as described in Section 5.2.
4. The approximated wireless channel $\boldsymbol{h_{i,j}}$ is then fed into the RF scenario server in Colosseum.

The Colosseum scenario consists of the wireless channel emulated between various gNB and UE locations in the digital 3D model referred to as a digital twin, similar to the locations described in the outdoor measurement scenario described in Section 5.3.1. Furthermore, in the next section, we analyze the localization performance of the proposed PRS-SRS signaling scheme in the outdoors and compare it with the performance using Colosseum.

The system parameters used for Outdoor measurements, MATLAB raytracing and Colosseum are detailed in the Table 5.1.

Table 5.1: System Parameters used in Outdoor Measurements and Colosseum

Parameters	Values
System bandwidth	38.16 MHz
Subcarrier spacing	30 KHz
Sampling Period (T_s)	21.70 ns
Centre frequency	3.69 GHz
Sampling rate	46.08 MHz
MCHEM sampling rate (f_s^m)	100 MHz
FFT size (K)	1536
Cyclic prefix (N_{cp})	132
Delay taps (N_c)	132
SRS bandwidth	37.44 MHz
SRS comb size	2
PRS bandwidth	37.44 MHz
PRS comb size	2

5.4 Experimental Results

In this section, we analyze the multipath component (MPC) profile of the wireless channel measured outdoors using the proposed PRS-SRS signaling scheme and compare it with the wireless channel simulated using a digital 3D model in MATLAB with raytracing. Further, we will evaluate the localization performance of the PRS-SRS signaling scheme in the outdoors and a digital twin using the Colosseum.

We begin by comparing the CIR measured at a specific gNB-UE location during the outdoor measurement[2] campaign using the PRS-SRS signaling scheme to the CIR generated at that exact location in the

[2]The CIR plots from outdoor measurements are averaged over 200 measurements.

digital 3D model using the multipath information obtained from the MATLAB raytracer[3]. Specifically, we discuss the MPC profile derived from the CIRs recorded at distances of 18 m, 26 m, 31 m to 35 m, and 37 m between the gNB and UE, considering multipath effects from various scattering objects. It is important to note that the CIR obtained from the SRS, utilizing the PRS-SRS signaling scheme, follows the convention illustrated in Figure 4.3, where the actual uplink MPCs are shifted by the LoS delay.

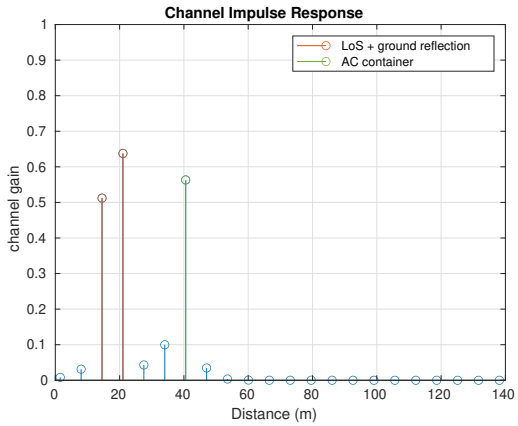
Starting with a distance of 18 m between the gNB and UE, we observe three multipath components: the LoS path, ground reflection, and reflection from the AC container, as depicted in Figure 5.7a. The corresponding taps in the CIR from both MATLAB and outdoor measurements are shown in Figure 5.7b and Figure 5.7c respectively. We can see that the LoS path and the ground reflection fall under the same tap, while the reflection from the AC container is represented in a different tap. Additionally, we can observe that the CIR from MATLAB and the outdoor measurements are comparable, with a shift in the distance of approximately 6.5 m (i.e., 1 sample) in the outdoor measurements, which is consistent with the performance of the proposed PRS-SRS signaling scheme as shown in Figure 3.10. Similarly, the multipath scenario at a gNB-UE distance of 26 m, shown in Figure 5.8a, reveals additional paths due to the Truck and the glass building. Here, the paths from the Truck and the AC container fall under a single tap, whereas the path from the glass building is represented in a different tap, as illustrated in Figure 5.8b and Figure 5.8c.

Further, an interesting observation arises at distances between 30 meters and 35 meters between the gNB and the UE. Here, constructive and destructive interference occurs due to the combination of the LoS and ground reflection. As seen in Figures 5.9, 5.10, and 5.11, both MATLAB and outdoor measurements show that the taps corresponding to the LoS and ground reflection undergo destructive interference. Consequently, the magnitude of the LoS and ground reflection tap is less than that of the other multipath components, primarily from the AC container and the glass building. This behavior aligns with the theoretical performance predicted by the two-ray interference model [118], as illustrated in Figure 5.13. Note that the gNB-UE distances ranging from 1 m to 40 m are within the breaking point (i.e., 193 m) of the two-ray interference model for the measurement scenario.

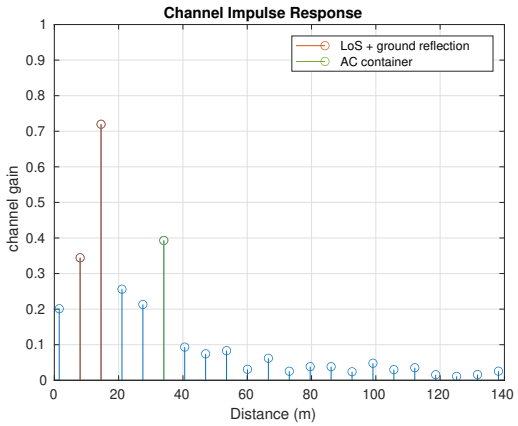
Furthermore, in the scenario at a distance of 37 meters, depicted in Figure 5.12a, an additional multipath component due to the container is observed. The corresponding taps from both MATLAB and outdoor measurements can be seen in Figures 5.12b and 5.12c, respectively. It is important to note that across all the scenarios discussed, the CIR obtained from the outdoor measurement campaign is consistent with the performance of the proposed PRS-SRS signaling scheme, staying within a 1 sample error margin.

[3]The path loss of the multipath components other than LoS and ground reflection obtained from the MATLAB raytracer is adjusted by 10 dB to be comparable with the multipath components from the outdoor measurements.

(a) gNB-UE distance: 18 m

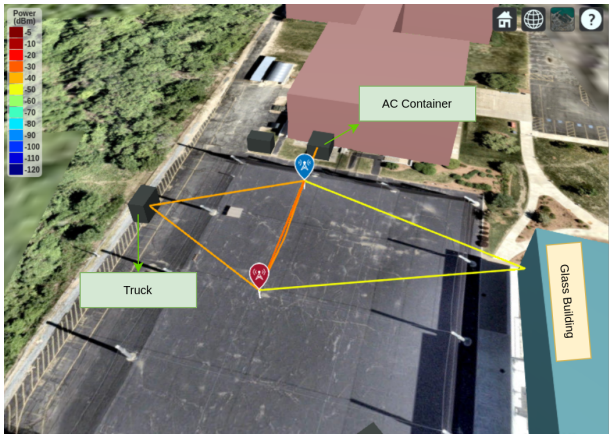


(b) MATLAB Raytracing, gNB-UE Distance: 18 m

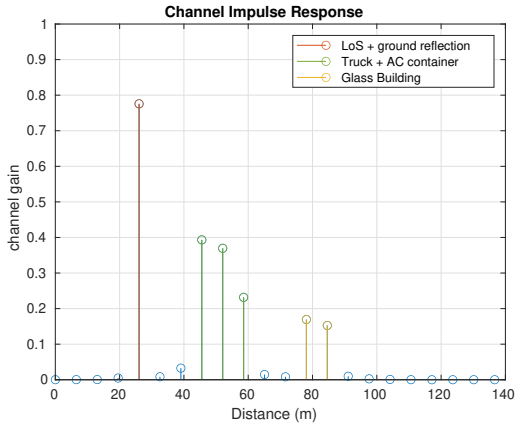


(c) Outdoor Measurement, gNB-UE Distance: 18 m

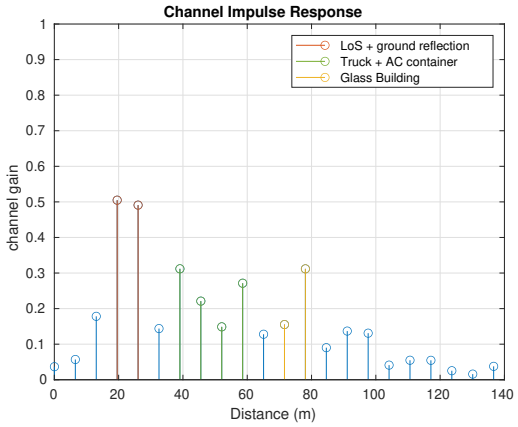
Figure 5.7: Uplink Multipath Scenario using proposed PRS-SRS signaling scheme at gNB-UE distance : 18 m.



(a) gNB-UE distance: 26 m

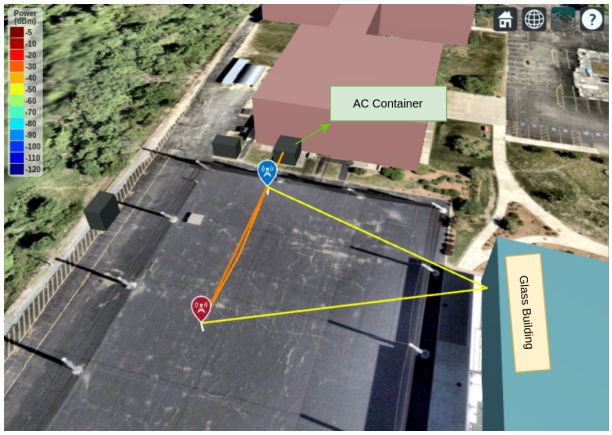


(b) MATLAB Raytracing, gNB-UE Distance: 26 m

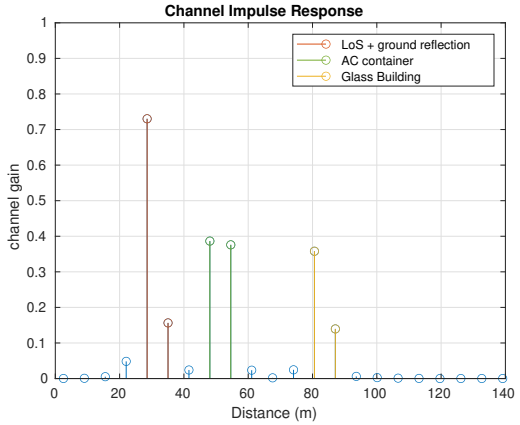


(c) Outdoor Measurement, gNB-UE Distance: 26 m

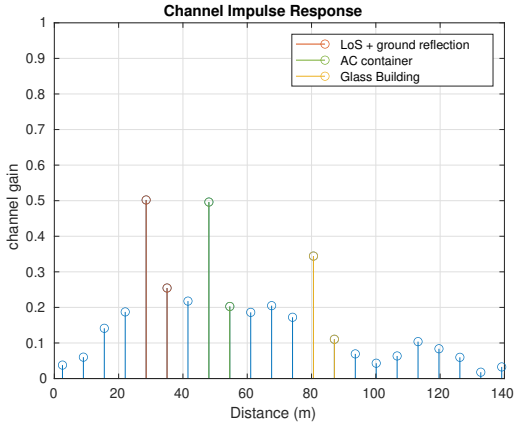
Figure 5.8: Uplink Multipath Scenario using proposed PRS-SRS signaling scheme at gNB-UE distance : 26 m.



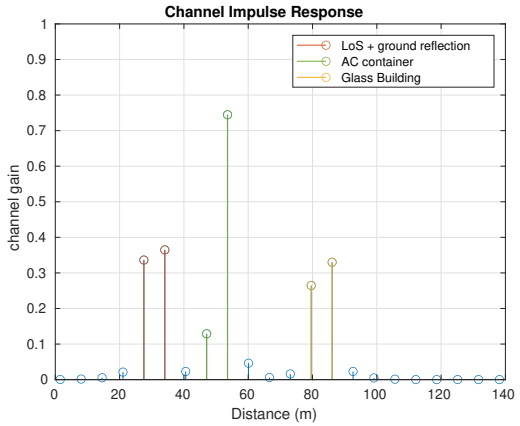
(a) gNB-UE distance: 30 m - 31 m



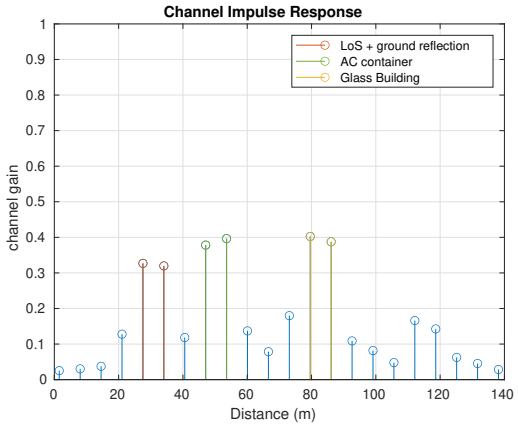
(b) MATLAB Raytracing, gNB-UE Distance: 30 m



(c) Outdoor Measurement, gNB-UE Distance: 30 m

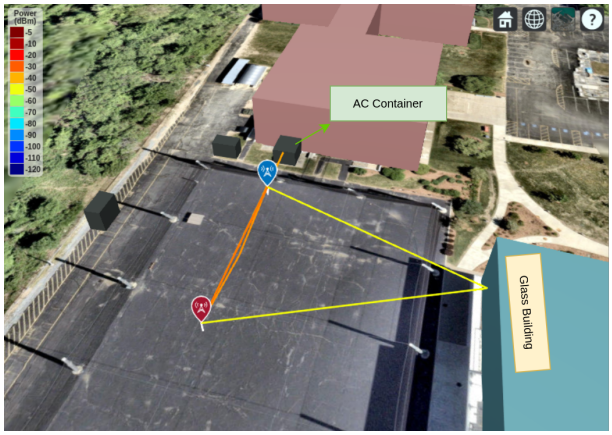


(d) MATLAB Raytracing, gNB-UE Distance: 31 m

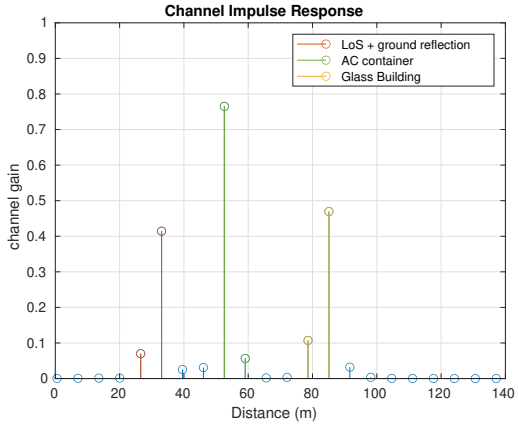


(e) Outdoor Measurement, gNB-UE Distance: 31 m

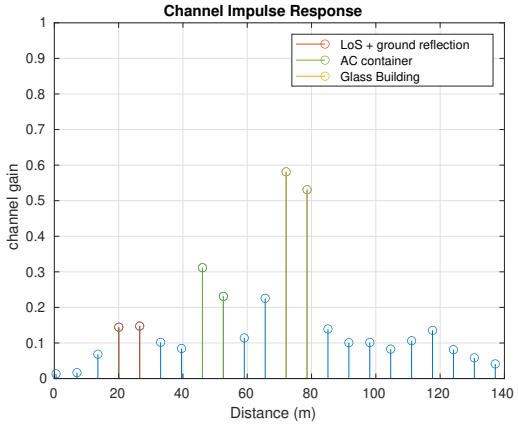
Figure 5.9: Uplink Multipath Scenario using proposed PRS-SRS signaling scheme at gNB-UE distance : 30 m to 31 m.



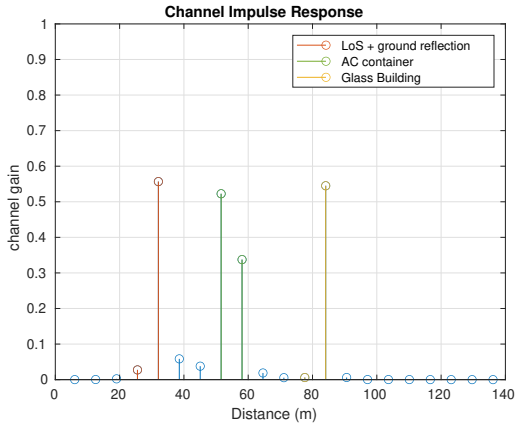
(a) gNB-UE distance: 32 m - 33 m



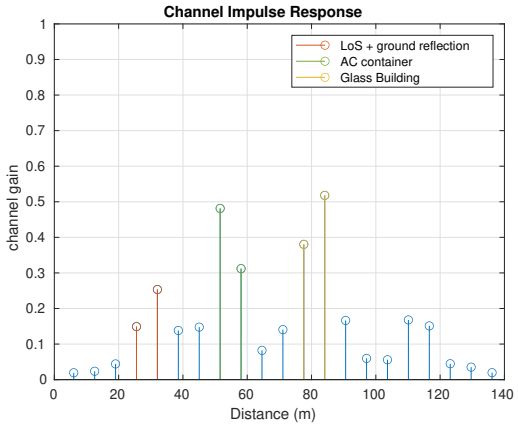
(b) MATLAB Raytracing, gNB-UE Distance: 32 m



(c) Outdoor Measurement, gNB-UE Distance: 32 m

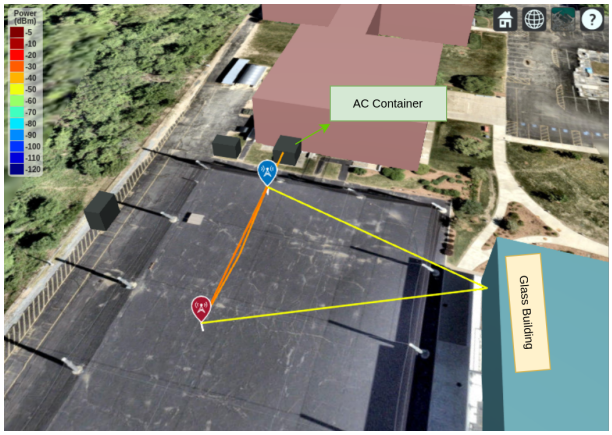


(d) MATLAB Raytracing, gNB-UE Distance: 33 m

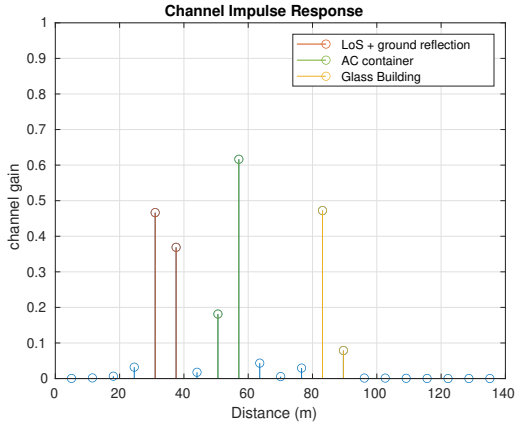


(e) Outdoor Measurement, gNB-UE Distance: 33 m

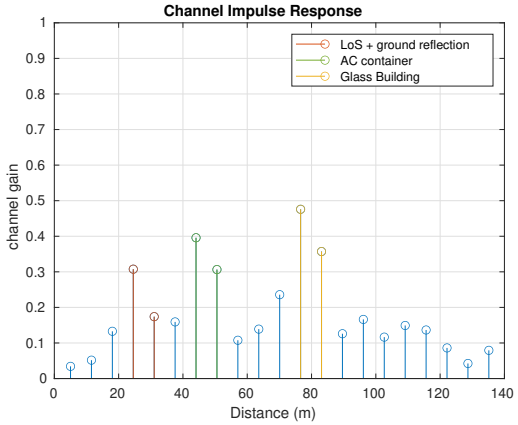
Figure 5.10: Uplink Multipath Scenario using proposed PRS-SRS signaling scheme at gNB-UE distance : 32 m to 33 m.



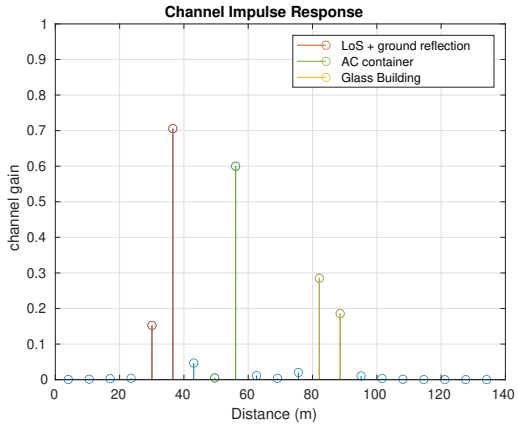
(a) gNB-UE distance: 34 m - 35 m



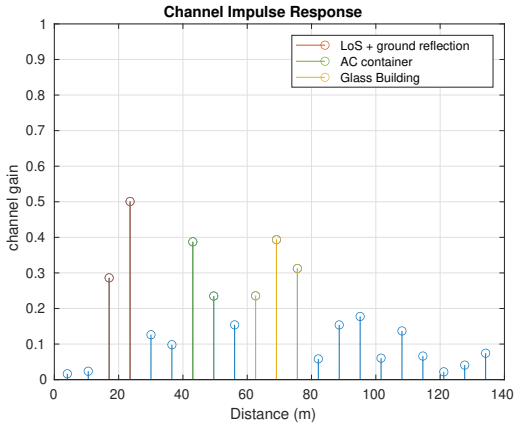
(b) MATLAB Raytracing, gNB-UE Distance: 34 m



(c) Outdoor Measurement, gNB-UE Distance: 34 m

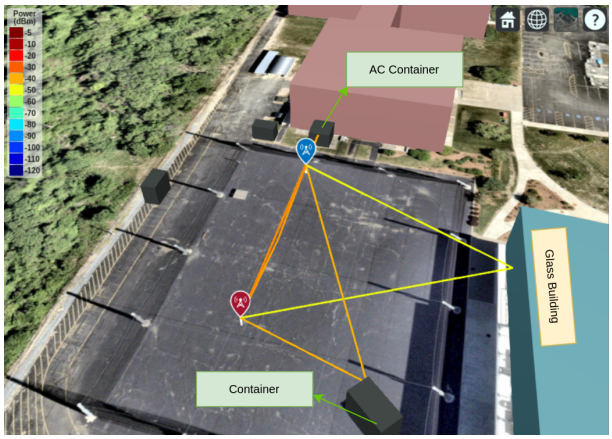


(d) MATLAB Raytracing, gNB-UE Distance: 35 m

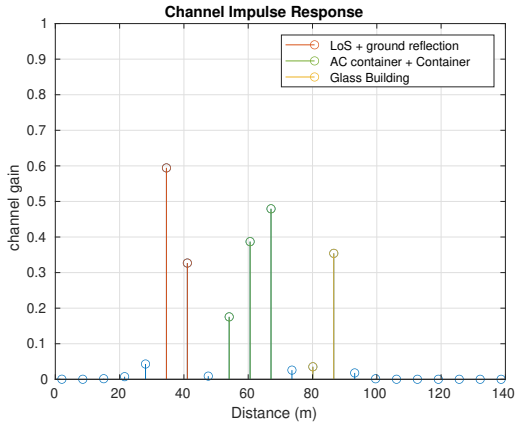


(e) Outdoor Measurement, gNB-UE Distance: 35 m

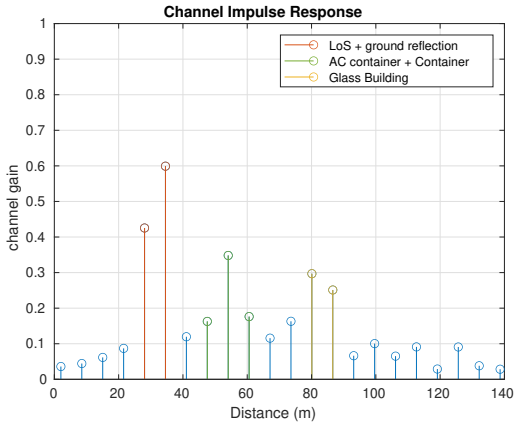
Figure 5.11: Uplink Multipath Scenario using proposed PRS-SRS signaling scheme at gNB-UE distance : 34 m to 35 m.



(a) gNB-UE distance: 37 m



(b) MATLAB Raytracing, gNB-UE Distance: 37 m



(c) Outdoor Measurement, gNB-UE Distance: 37 m

Figure 5.12: Uplink Multipath Scenario using Proposed Schemes at gNB-UE distance : 37 m.

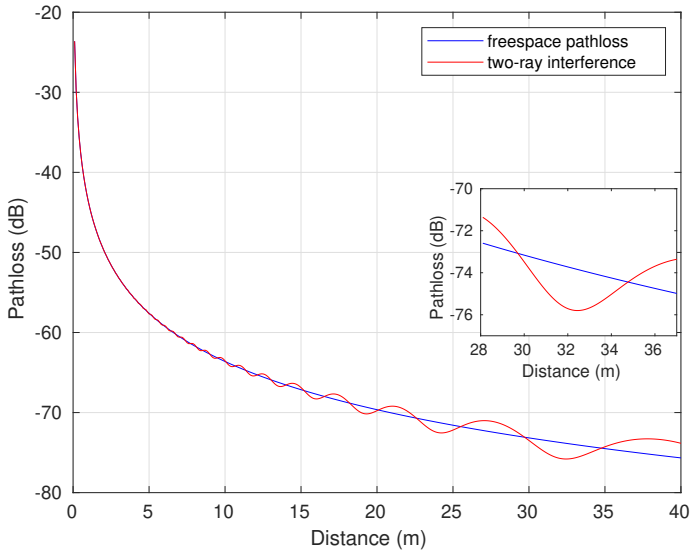


Figure 5.13: Theoretical two-ray interference pathloss model over a distance.

Finally, the localization performance of our proposed PRS-SRS signaling scheme is evaluated in an outdoor measurement campaign and a digital twin using Colosseum, based on the scenarios outlined in Section 5.3. To estimate the range between the gNB and the UE, we utilize a PD and a MF, as described in Section 3.4.

The CDF plot of the range estimation error at a high SNR of 25 dB, with multiple measurements (M = 60), is shown in Figure 5.14. At this high SNR with M=60, we can see that using the PD, the range estimation error is below 4.2 m for 90% of the time in the outdoor measurement campaign, whereas it is below 3.5 m for 90% of the time in the digital twin. Similarly, when using MF, the range estimation error is below 2.6 m for 90% of the time in the outdoor measurement campaign, whereas it is below 2.4 m for 90% of the time in the digital twin. The performance difference between the outdoor measurement campaign and the digital twin is 0.7 m when using the PD and 0.2 m when using the MF.

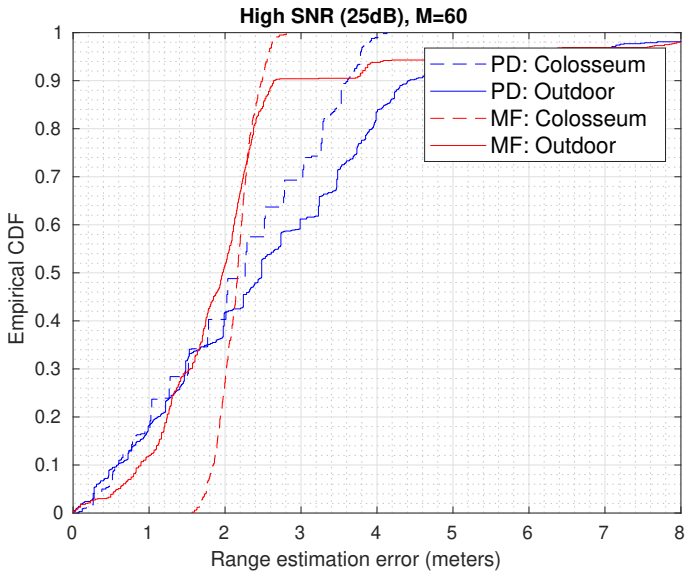


Figure 5.14: CDF of range estimation error in an Outdoor measurement campaign and the Colosseum.

5.5 Positioning with Multiple gNBs in Colosseum

In this section, we evaluate the localization performance of the proposed PRS-SRS signaling scheme in estimating the 2D position of the UE using multiple gNBs in a digital twin using the Colosseum. In this scenario, four gNBs are positioned on top of four buildings in a digital 3D model of the Northeastern University Burlington campus obtained from OpenStreetMap. Additionally, 48 UEs are randomly distributed throughout the environment in 2 dimensions, as illustrated in Figure 5.15. The positions of the four gNBs are known, and the height of the UEs is fixed. The range between each UE and its corresponding gNB is determined using PD and MF, as described in Section 3.4. Furthermore, the position of each UE is estimated using two methods: LS and non-least squares (NLS), as described in [35] utilizing the range estimates from PD and MF.

The CDF of the range estimation error and position estimation error at a high SNR of 25 dB, corresponding to M=60 measurements, is illustrated in Figure 5.16. At high SNR, both PD and MF exhibit similar performance, with the range estimation error falling below 1.5 m for 90% of the time, as shown in Figure 5.16a. Figure 5.16b presents the 2D positioning error for PD LS, MF LS, and MF NLS. The results indicate that the 2D positioning estimates using PD and MF with LS have comparable performance, maintaining an error below 2.6 m for 90% of the time. This consistency is attributed to the similar range estimation error performance of both methods at high SNR. However, when NLS is utilized, the positioning error improves by 1 m, achieving an error below 1.6 m for 90% of the time.

The CDF of the range estimation error and position estimation error at a low SNR of -25 dB, corresponding to both M=20 and M=60 measurements, is illustrated in Figure 5.17. At low SNR, it is evident that MF significantly outperforms PD, maintaining a range estimation error below 1.6 m for 90% of the time, as shown in Figure 5.17a. Additionally, as the number of measurements increases, the performance improves by 0.1 m, keeping the range estimation error below 1.5 m for 90% of the time. Figure 5.17b presents the 2D positioning error for PD LS, MF LS, and MF NLS with M=60 measurements. The results demonstrate that 2D positioning estimates using MF significantly outperform PD with LS, maintaining an error below 2.5 m for 90% of the time. This outcome aligns with the range estimation error performance observed at low SNR. Similarly, when using NLS, the positioning error improves by 0.5 m, achieving an error below 2 m for 90% of the time.

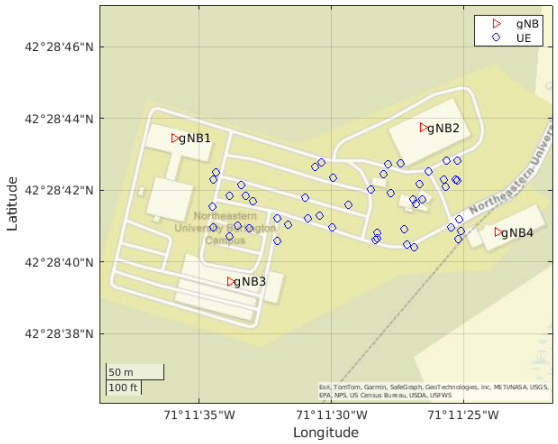
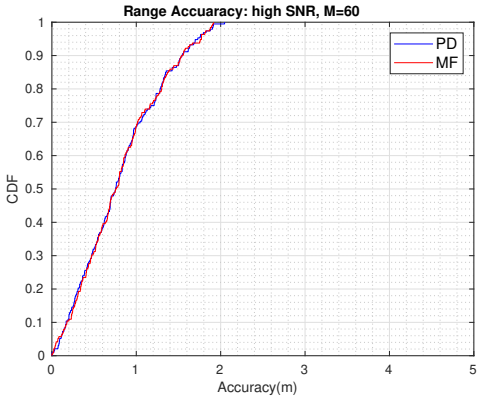
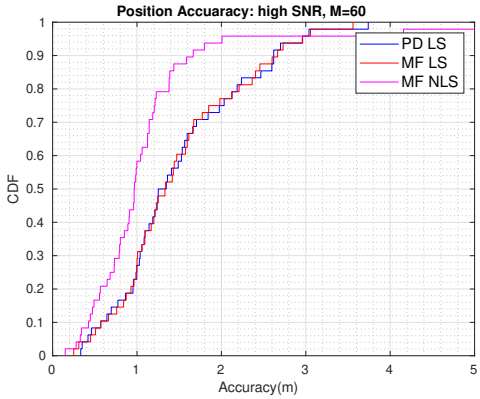


Figure 5.15: Northeastern university, Burlington campus with multiple gNBs scenario in Colosseum.

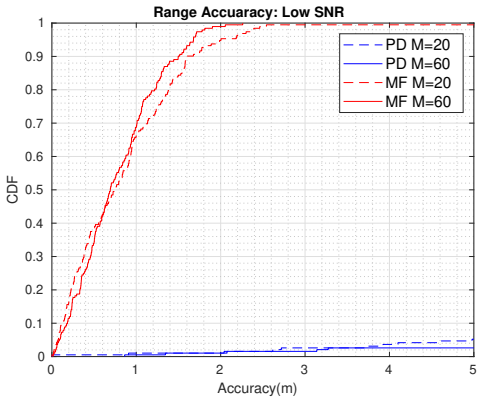


(a) CDF of Range estimation error.

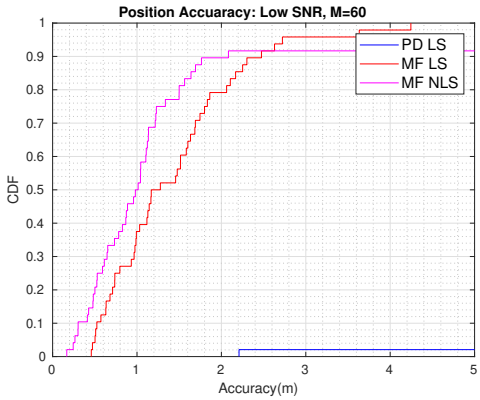


(b) CDF of Position estimation error.

Figure 5.16: Performance of the PRS-SRS signaling scheme in Colosseum at High SNR with M = 60 measurements.



(a) CDF of Range estimation error.



(b) CDF of Position estimation error.

Figure 5.17: Performance of the PRS-SRS signaling scheme in Colosseum at Low SNR with M measurements.

5.6 Mono-static Downlink Sensing using Colosseum

In this section, we discuss preliminary results of mono-static downlink sensing in 5G NR using the Colosseum as a digital twin.

Downlink sensing using full-duplex radios, as demonstrated in [119] to detect rogue drones in the restricted airspaces, can also be performed in a digital twin using the Colosseum platform, thereby eliminating the need for extensive outdoor measurement campaigns. Initial experiments on sensing multiple targets in full-duplex mode in the downlink are carried out using OAI and Colosseum, as illustrated in Figure 5.18. In this scenario, the PDSCH signal is transmitted from the gNB in the downlink operating in TDD using OAI `phy-test` mode. The transmitted PDSCH signal is reflected from the targets. The Colosseum can emulate this reflection from targets in full-duplex mode, emulating the channel between the transmitter and receiver at the gNB. The reflected signal from the targets received at the gNB in full-duplex mode is recorded in the same slot as the transmitted signal. Further, the received signal is used for channel estimation. Furthermore, the estimated channel is analyzed for target detection. As shown in Figure 5.19, we can successfully detect both targets from the estimated channel. The system parameters used are detailed in Table 5.1. The PDSCH bandwidth used for this experiment is 38.16 MHz.

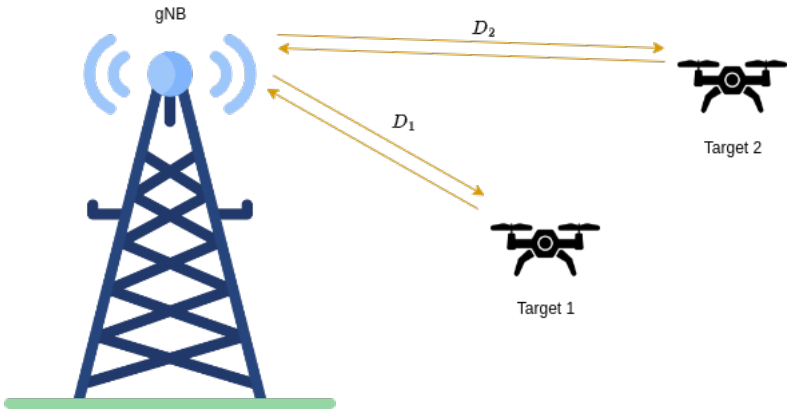


Figure 5.18: Full-Duplex Sensing Scenario in the Colosseum.

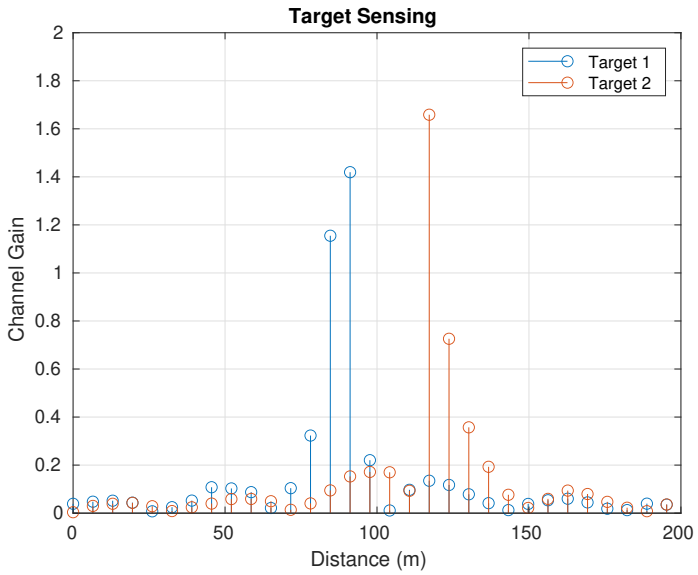


Figure 5.19: Target detection using Full-Duplex sensing in the Colosseum.

5.7 Conclusions

In this chapter, we demonstrated how the Colosseum can serve as a digital twin platform for evaluating the performance of localization algorithms, thus eliminating the need for laborious outdoor measurement campaigns. We explained the process of creating a digital twin of the actual outdoor environment and described how a wireless propagation channel is generated and approximated to fit within the Colosseum. Additionally, we evaluated the performance of a signaling mechanism introduced in Chapter 3 using the Colosseum platform as a digital twin. Specifically, we addressed the performance gap between the results of the proposed signaling scheme obtained from an outdoor measurement campaign and those obtained from the digital twin representation of the same outdoor environment using the Colosseum.

Chapter 6

Integrated Access and Backhaul

A wide range of localization and sensing applications arise from the mechanisms proposed in Chapter 3. One notable application is drone-based localization and sensing for SAR operations, where gNBs are installed on the drones. However, such applications require a backhaul connection to remain connected with the cellular network and to operate autonomously. In this chapter, we present the integrated access and backhaul systems in 5G NR and beyond that are crucial for enabling drone-based localization and sensing in SAR missions. Specifically, we demonstrate an O-RAN based aerial integrated access and backhaul system in Section 6.1 and a THz backhaul system in Section 6.2 using OpenAirInterface.

6.1 Aerial Integrated Access and Backhaul

6.1.1 Introduction

Unmanned aerial vehicle (UAV) mounted gNBs and access points have recently attracted significant attention [120]. Thanks to the 3D mobility offered by the UAV gNBs, they are instrumental in providing ultra-flexible radio network deployments in use cases such as tactical networks, disaster recovery, search and rescue scenarios.

Several prototypes of UAV gNBs and/or relays in 4G and 5G networks using open-source software are reported in the literature [121, 122, 123, 124]. While the UAV relay in [122, 123] has an on-board core network and relies on commercial backhaul links, authors in [121], demonstrated an UAV LTE relay with integrated access and backhaul (IAB) capability. The work is later extended to 5G scenario [125]. However, in all these works entire eNB or gNB application is running on the UAV.

On the other hand, disaggregated RAN with open interfaces and end-to-end programmability has become an essential element in 5G and beyond cellular networks. The traditional gNB unit in 5G can now be split into various physical entities such as CU, DU and RU. The CU has upper layer RAN protocol stack and can support multiple DUs running RLC layer and below network functionalities. With this architecture, lightweight DUs and RUs can be instantiated and programmed according to the needs of the network in a centralized manner [126].

In this chapter, we present a demonstration of a UAV with combined functionalities of DU and RU, serving ground users. The UAV is connected with a terrestrial CU using IAB. The CU-DU interface fully complies with the F1 application protocol (F1AP) protocol defined in 3GPP. The end-to-end network solution is based on OAI software. To the best of our knowledge, an autonomous and programmable aerial DU unit with IAB capabilities, built using open-source solutions, has never been demonstrated before.

6.1.2 System Design

To support open and disaggregated RAN, 3GPP TS 38.401 outlines the functional split of the gNB into CU, DU and RU. The CU comprises RRC and PDCP layer protocol stack in the control plane, and SDAP and PDCP in the user plane. The DU comprises RLC, MAC, and/or PHY layers. RU consisting of PHY layer is either a part of DU itself or can have separate interface with DU (for example, O-RAN 7.2 split). We consider the scenario where RU is a part of the DU. Each CU can be connected to one or more DUs. Communication between the CU and DU is carried out as a tunnel using the F1AP as illustrated in Figure 6.1. While the wired connection between CU and DU is straightforward, connecting the aerial DU with a terrestrial CU wirelessly over existing 5G RAN requires IAB.

An IAB system typically consists of an IAB Donor and IAB nodes [127]. The IAB donor, in our case, is a terrestrial CU wired to the DU, referred to as the IAB Donor. The IAB node (which is mounted on a drone) consists of an IAB-mobile terminal (MT), and a DU. The DU within the IAB node is called as a DU node. The DU node can wirelessly connect to the CU in the IAB Donor via IAB-MT, as depicted in Figure 6.2.

To achieve the over-the-air F1 interface, we implement F1 tunnel between the terrestrial CU and DU node as illustrated in Figure 6.3. This is achieved by using the general packet radio service tunneling protocol (GTP) via IAB-MT. The F1 tunnel is created within the PDU session of the IAB-MT. The F1 tunnel of the DU node starts via IAB-MT, passes over-the-air, tunnels through Donor DU, CU, and ends at 5GC UPF. The packets are further rerouted from 5GC UPF to the CU, completing the F1 tunnel for the IAB node. However, the path to 5GC UPF from CU and the rerouting from the 5GC UPF to CU can be bypassed by utilizing the backhaul adaptation protocol (BAP) in the IAB node tunnel as mentioned in 3GPP TS 38.340. Although the BAP protocol has not been implemented in the OAI, the functionality of an IAB system can be demonstrated using the proposed solution. We plan to incorporate the BAP protocol in future implementations, ultimately improving the overall functionality of the system.

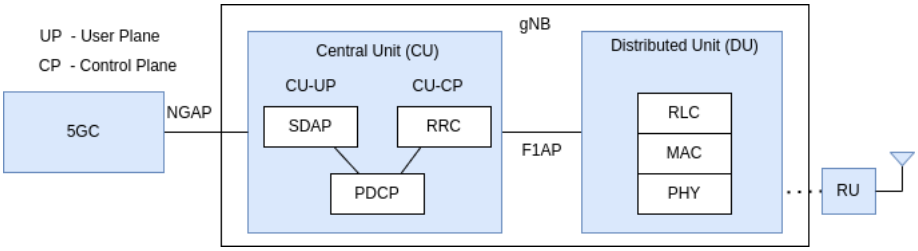


Figure 6.1: Illustration of the CU-DU split in 5G NR.

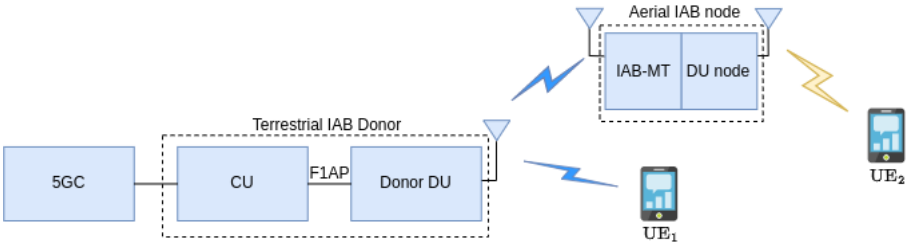


Figure 6.2: Aerial Integrated Access and Backhaul Demo Scenario.

6.1.3 Demo Description

We present an IAB scenario in 5G with an aerial DU node serving ground users. These aerial DUs can be deployed on-the-fly while being organized in a centralized manner. Such dynamic deployment has use cases in tactile networks and emergency scenarios. The proposed 5G IAB system comprises a Terrestrial IAB Donor and an Aerial IAB node that operate in different frequency bands. The Terrestrial IAB Donor is present on the ground and is made up of a CU and a Donor DU that are connected via Ethernet.

The Aerial IAB node which can be deployed as per the user demand is a custom-built box that includes a commercial Quectel RM500Q-GL user equipment and a DU node mounted on a UAV. The DU node uses USRP B200 mini as an RU and a custom-built power amplifier to improve its coverage. Entire end-to-end 5G network solution is based on the OAI software. An illustration of the demo setup is shown in Figure 6.4. The system parameters used are mentioned in Table 6.1.

In this demo [128], we have showcased a live video call between users UE_1 and UE_2, where the user locations are shown in Figure 6.4. The throughput results to the UE_2, i.e., from 5GC to UE_2 are shown in Figure 6.5.

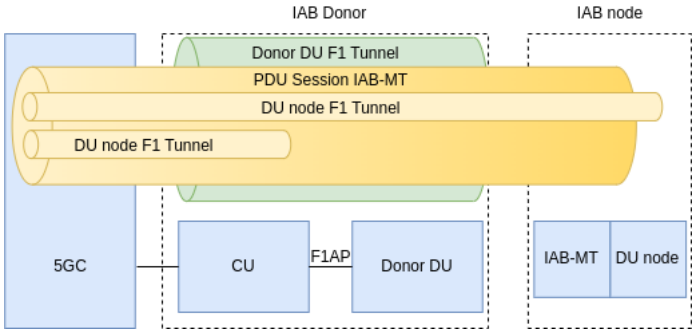


Figure 6.3: F1 tunneling used in the aerial IAB.

Table 6.1: System Parameters used for Aerial IAB demonstration

DU	Parameters	Values
Terrestrial Donor DU	Bandwidth	20 MHz
	Subcarrier Spacing	30 KHz
	Centre frequency	2.585 GHz (n41)
Aerial DU node	Bandwidth	30 MHz
	Subcarrier Spacing	30 KHz
	Centre frequency	3.47 GHz (n78)

6.1.4 Conclusions

We have successfully described and demonstrated the 5G Aerial IAB scenario prototype using a complete open-source solution OAI. The throughput results demonstrate the potential of the Aerial IAB system in extending coverage. Our prototype enables the researchers in the community to address a wide range of research problems related to IAB and implement and verify them in real-time.

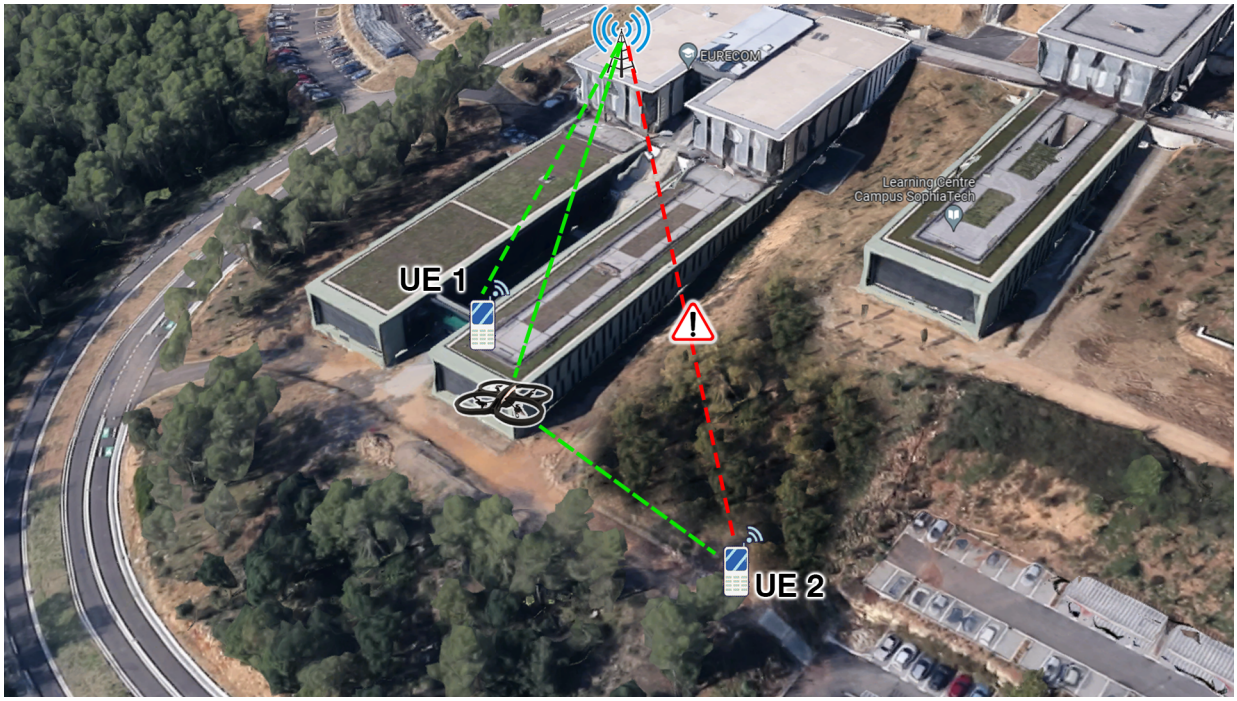


Figure 6.4: Aerial Integrated Access and Backhaul Demo Scenario.

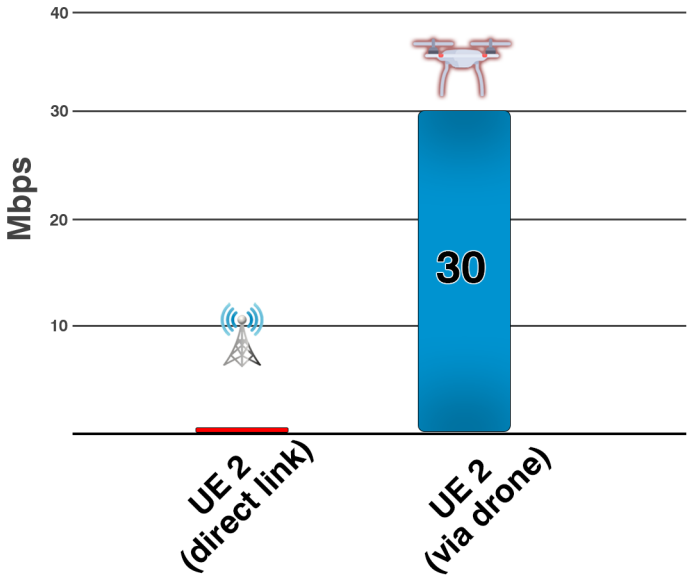


Figure 6.5: Throughput results of UE_2.

6.2 Terahertz Backhaul

6.2.1 Introduction

To satisfy the high data rate and low latency demands arising from augment reality (AR)/virtual reality (VR), digital twins and x-haul links in disaggregated O-RAN, it has become necessary to tap into the huge bandwidths available in THz frequency bands (100 GHz-10 THz). With this in mind, the federal communications commission (FCC) has created experimental licenses that span 21.2 GHz of spectrum in frequencies between 95 GHz and 3 THz. Particularly, multiple bands in the 110–160 GHz and 200–260 GHz have been allocated to fixed/mobile usage [129].

While the initial days of THz communication research is limited to channel modeling and numerical studies, recent advances in radio and photonic devices in THz frequencies have led to several experimental platforms demonstrating gigabit wireless links operating in the sub-terahertz and terahertz bands [130, 131]. To further advance the THz communication research and standardization activities, there is an urgent need to develop SDR based platforms and protocol stacks that can showcase real-time communication technologies at THz frequencies.

The majority of the current experimental platforms operating over 100 GHz have been either channel sounders or physical layer testbeds that rely on offline processing [131]. Recently the work in [132], has demonstrated a real-time programmable SDR platform that can support OFDM based physical layer with bandwidth on the order of several GHz, and operating at carrier frequencies 120-140 GHz. However, the platform is limited to the link level and no communication protocol stack that includes higher layers runs on the TX or the RX.

On the other hand, when it comes to 5G and beyond systems, open-source projects that implement 3GPP cellular standards on general-purpose computing hardware and COTS SDR cards are making a huge contribution to the experimental research, standardization, and testing of multi-vendor networks in O-RAN [133]. For example, the OAI [134] project is widely known for providing an end-to-end 3GPP standard-compliant 5G NR protocol stack that can run on various SDR platforms. It is possible to quickly build a 5G network using OAI with a combination of low cost with COTS SDRs and general-purpose x86 computers. Recently, it has been shown that OAI can operate in mmWave FR2 bands [135].

In this chapter, to facilitate the 6G communication system architecture and reproducible experimental research, we demonstrate an OAI-based real-time end-to-end 5G communication at THz frequencies. To the best of the our knowledge, no such platform exists as of today.

6.2.2 System Design and Implementation

We leverage on the OAI 5G NR protocol stack [134], USRP SDR cards, and TeraNova testbed [136] to build the OAI-THz platform. This platform is capable of delivering end-to-end real-time 5G over THz. The system architecture is depicted in Fig 6.6. The OAI stack, along with the USRP, is used at the gNB to generate the 5G NR signals at an intermediate frequency (IF) of 3.39 GHz, while a Quectel module (commercial 5G module) serves as a UE operating at the same intermediate frequency. Further, THz frontend modules from TeraNova testbed [136] are utilized to upconvert the IF signals into THz frequencies and downconvert the THz signals to IF frequencies.

As shown in Fig. 6.7, the gNB antenna ports from the USRP and the antenna ports of the UE are connected to the THz frontend modules that upconvert IF to THz frequencies and downconvert back to IF. Circulators, isolators, and attenuators are added, ensuring that the operating power levels do not exceed the damage limits of the transmitter IF port and prevent the reverse power/leakage into the receiver IF port.

We will first describe the OAI 5G architecture, and the description of THz frontend modules follows in Section 6.2.3.

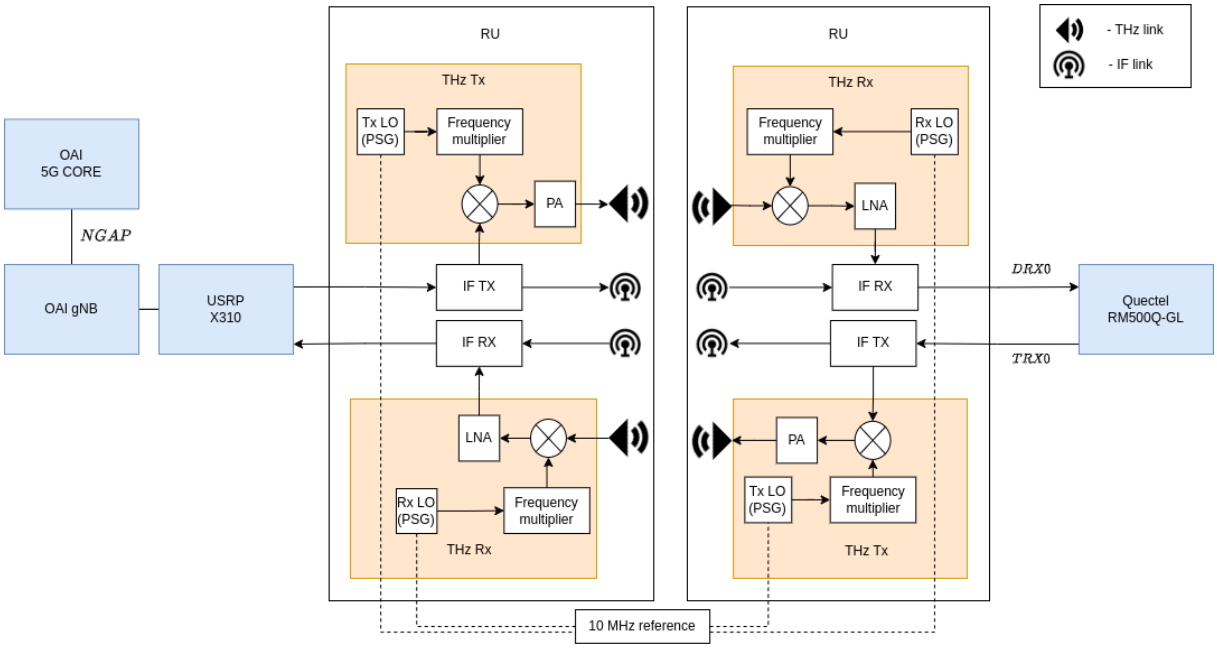


Figure 6.6: A block diagram depicting the OAI-THz system architecture.

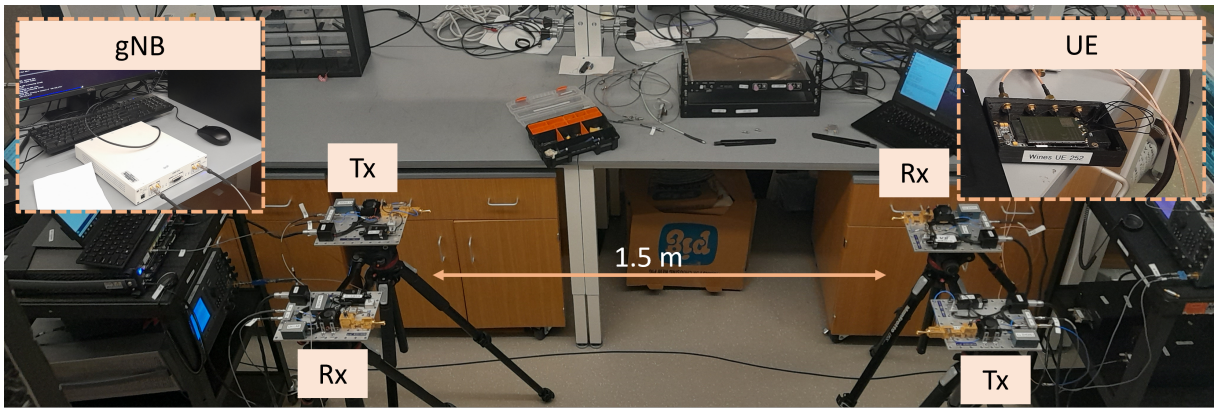


Figure 6.7: A picture of the OAI-THz experimental setup in the lab.

5G Base-station: In this work, we use a simple deployment as a monolithic gNB using the USRP as a radio frontend as described in Section. 2.2.1 and further connected to THz frontends. The transmit and receive paths of this system are detailed as follows: In the transmit path, the baseband signal generated by OAI gNB goes through a DAC, followed by up-conversion and amplification, and is transmitted at an IF. This IF signal is further up-converted to THz frequencies for over-the-air transmission using the THz radio frontends. In the receive path, the received signal at the THz frequencies by the THz frontend is down-converted to IF. At the IF stage, the signal is filtered, down-converted again, and sampled by an ADC, resulting in a baseband signal. The system parameters of the OAI-THz system are shown in Table 6.2.

User Equipment: In the OAI-THz setup, the Quectel RM500Q-GL module is used as UE, a commercial 5G modem with a Qualcomm chipset that supports 5G SA mode in real-time. The module has four antenna ports operating at 3.39 GHz frequency. Two of these ports are transmit/receive (TRX) antenna ports, while the other two are diversity receive antennas (DRXs). ANT0 and ANT3 correspond

to TRX1 and TRX0 antennas on the module, respectively, and ANT1 and ANT2 correspond to DRX0 and DRX1 antennas. The TRX0 antenna port is used as a transmitter, which is connected to the THz transmitter frontend, and DRX0 as a receiver connected to the frontend of the THz receiver. OAI nrUE, which can emulate the behavior of a real-time 5G UE using a programmable radio like USRP, has also been validated in the platform. However, only the results of the Quectel module are presented in this chapter.

Table 6.2: System Parameters used for OAI THz demonstration

Parameters	Values
Bandwidth	80 MHz
Subcarrier Spacing	30 KHz
Intermediate Frequency (IF)	3.39 GHz
Centre Frequency	130 GHz
Sampling Rate	92.16 MHz
FFT Size	3072

6.2.3 Terahertz Communication

The THz frontend modules used in the OAI-THz platform are a part of TeraNova testbed [137]. The TeraNova transmitter consists of an analog programmable signal generator (PSG) from Keysight Technologies and up-converter frontends, along with directional high-gain antennas encompassing frequency ranges in the terahertz band (0.095–1.05 THz) [138]. The PSG is used to generate the local oscillator (LO) signal and is capable of producing frequencies up to 50 GHz. The up-converter takes an IF signal, mixes it with the LO signal, and up-converts it to a higher RF signal. The up-converters manufactured by virginia diodes, Inc. (VDI) operate in the frequency range of 120–140 GHz. They consist of a frequency multiplier chain of $\times 4$, a frequency mixer with a double sideband (DSB) conversion loss of about 7 dB, and an RF power amplifier (PA) with a gain of 20 dB. The transmit power before feeding the antenna is about 13 dBm (20 mW).

The TeraNova receiver consists of a PSG of the same model as the transmitter, and down-converter frontends, along with similar high-gain antennas as the up-converters. The receiver PSG is used to generate the LO signal at the receiver side. The VDI down-converter frontends operate in the same frequency range of 120–140 GHz and have the same architecture as the up-converter frontends, but instead of an RF PA, an IF low-noise amplifier (LNA) is used to provide the required amplification. Fig. 6.6 depicts how the different transmitter and receiver components of the TeraNova testbed are interconnected. A 10 MHz reference cable is used to synchronize the transmitter and receiver PSGs and compensate for the carrier frequency and phase offsets. The testbed has multiple sets of broadband antennas with directivity gains ranging from 21 dBi to up to 40 dBi at the aforementioned frequencies.

6.2.4 Experimental Results

This section analyzes the CSI and throughput results at THz frequencies and compares them with those at the IF. The CSI, depicted in Fig. 6.8 and Fig. 6.9, is obtained in the uplink using wideband pilots known as SRS. The CFR in the wideband (80 MHz) is obtained using the least square estimates of the SRS, as shown in Fig. 6.8. Moreover, the CIR is obtained by taking the IFFT of the channel frequency response, as shown in Fig. 6.9.

From Fig. 6.8 and Fig. 6.9, we can infer that the CFR at THz frequencies is almost flat, whereas, at IF, it is frequency-selective and has a multi-path channel, as seen in Fig. 6.8. The peak at the center of

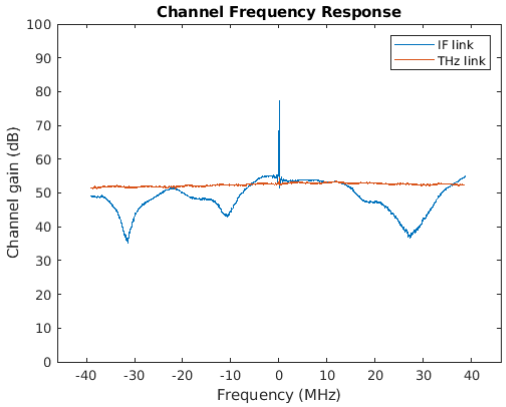


Figure 6.8: Channel Frequency Response at both IF and THz frequencies..

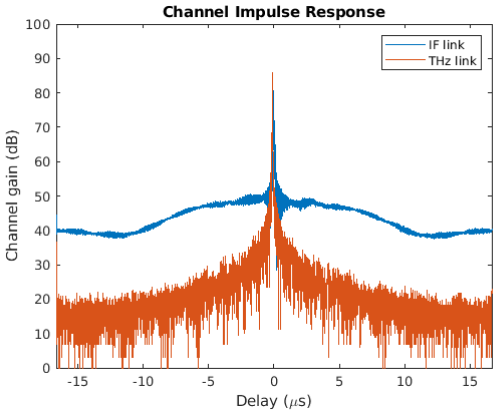


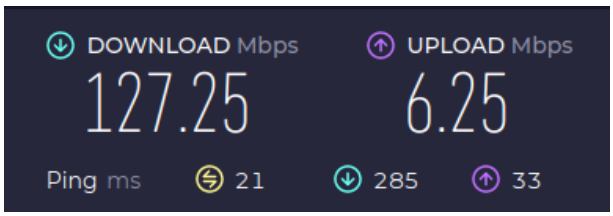
Figure 6.9: Channel Impulse Response at both IF and THz frequencies..

the CFR at IF frequency is due to the direct current (DC) leakage of the TX path into the RX path in the un-calibrated USRP X310 due to the usage of two individual dipole antennas for TX and RX (this could be avoided by using an external switch or circulator). This leakage is not present in the THz link is due to separation of UL and DL paths and the use of highly directive antennas. This DC leakage in the frequency domain is also the reason for the higher floor in the CIR of the IF link in Fig. 6.9.

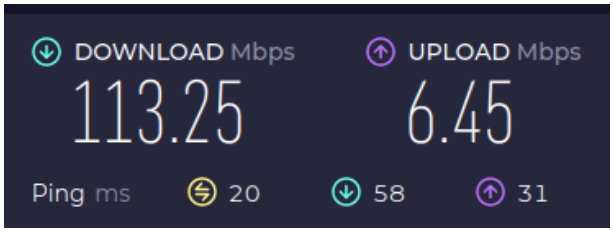
The throughput results, as depicted in Fig. 6.10, are obtained using a speed test web application by OOKLA[139] on the laptop connected to the internet via the Quectel module. The throughput results obtained at the THz frequencies are comparable to those obtained at the IF.

6.2.5 Conclusions

In this work, we have successfully demonstrated a first-of-a-kind real-time end-to-end 5G connectivity over THz frequencies using commercial user equipment with throughput results comparable to the throughput results of a 5G base-station operating at 3.39 GHz. The use of open-source software for the 5G stack and a THz platform allows researchers in academia and industry to facilitate the development of IAB solutions using THz links for 5G NR and beyond networks.



(a) Speed test at IF



(b) Speed test at THz

Figure 6.10: Speed test results at IF and THz frequencies.

Chapter 7

Conclusions and Future Perspectives

7.1 Conclusions

The focus of this dissertation was to design a system that enhances localization and sensing capabilities in 5G NR and beyond cellular networks. Localization and sensing capabilities of a system depend on the accurate estimation of the CSI. However, in practice, the CSI estimation is affected by the impairments such as clock drift caused by the asynchronous clocks between the gNB and the UE, making the estimated CSI unreliable for localization and sensing purposes. While cellular systems were traditionally designed to improve communication performance, they have introduced timing correction loops that periodically correct the clock drift. Although the influence of clock drift and timing correction loops on communication performance is minimal, their impact on localization and sensing performance is significant. The measurements obtained from a COTS UE in Section 1.2.3 have clearly demonstrated these detrimental effects.

In this dissertation, we designed a system and proposed signaling schemes that allow us to obtain CSI that is robust to clock drift and timing correction loops within a cellular system. Additionally, we proposed a system framework that overcomes the impairments caused by the clock drift and timing correction loops and leverages sensing information to improve the performance of the communication system. In specific, we reduced the pilots needed for channel estimation by utilizing sensing information available at the gNB. We also provided a framework to evaluate the performance of localization algorithms in a digital twin using the Colosseum platform. Furthermore, we highlighted a drone-based localization and sensing application for search and rescue missions, emphasizing the importance of backhaul connectivity to the cellular network in such scenarios. Finally, we prototyped and demonstrated most of our work using OpenAirInterface.

A summary of the contributions in each chapter is as follows:

- In Chapter 2, we introduced OAI, including its components and operating modes that are beneficial to developers and researchers in prototyping. We also delved into the essential functions of the reference signals related to positioning in OAI. Further, we provided a comprehensive overview of the baseband signal representation of these reference signals using fixed-point notation in OAI. Furthermore, we discussed important physical layer metrics such as TX, RX power, and SNR estimation in OAI. Finally, we presented the `T_tracer` tool, which facilitates data extraction within the OAI framework.
- In Chapter 3, we proposed two RTT estimation schemes using DCI Format X_Y as a signaling mechanism for positioning. The proposed schemes are designed to work in both NR_RRC_INACTIVE and NR_RRC_CONNECTED states. It forces the UE to correct its timing after the reception of the DCI, which is currently not possible, as shown in our experiments with the COTS UEs. Furthermore,

our framework enables the coherent combination of multiple uplink channel measurements and is robust to the clock drift and the inherent timing loops in the 5G system. We have validated the functionality of our proposed framework in real-time using OAI. Our results show that the proposed matched filter algorithm can achieve meter-level accuracy for bandwidth as low as 40 MHz, even in low SNR scenarios.

- In Chapter 4, we have studied the uplink channel estimation aided by sensing information available at the gNB. We proposed a framework utilizing the proposed signaling mechanisms in Chapter 3, making it robust to impairments such as clock drift and timing correction loops for fusing sensing information. We have also shown how the proposed signaling mechanisms in Chapter 3 enable uplink sensing. The proposed SWOMP-SBL algorithm uses fewer uplink pilots than traditional methods by incorporating sensing information. The proposed scheme is also robust to erroneous sensing information, including additional paths available in the sensing information but not associated with the communication. We presented the simulation results conducted in MATLAB for both multiple and single receive antennas at the gNB. Additionally, we evaluated the simulation results from OAI RFSIM, which account for the effects of fixed-point implementation in the case of a single receive antenna. Our simulation results have validated the superior performance of the proposed SWOMP-SBL scheme using fewer pilots compared to conventional state-of-the-art algorithms.
- In Chapter 5, we demonstrated how the Colosseum can serve as a digital twin platform for evaluating the performance of localization algorithms, thus eliminating the need for laborious outdoor measurement campaigns. We explained the process of creating a digital twin of the actual outdoor environment and described how a wireless propagation channel is generated and approximated to fit within the Colosseum. Additionally, we evaluated the performance of a signaling mechanism introduced in Chapter 3 using the Colosseum platform as a digital twin. Specifically, we addressed the performance gap between the results of the proposed signaling scheme obtained from an outdoor measurement campaign and those obtained from the digital twin representation of the same outdoor environment using the Colosseum.
- In Chapter 6, we have successfully described and demonstrated the 5G Aerial IAB scenario prototype using a complete open-source solution with OAI. The throughput results demonstrate the potential of the Aerial IAB system in maintaining backhaul connection and extending coverage. We have also successfully demonstrated a first-of-a-kind real-time end-to-end 5G connectivity over THz frequencies using commercial user equipment with throughput results comparable to the throughput results of a 5G base-station operating at 3.39 GHz. The use of open-source software for the 5G stack and a THz platform in our prototype enables the researchers in the community to address a wide range of research problems related to IAB and THz technologies. This allows the researchers to implement and verify these technologies in real-time for 5G NR and beyond networks.

7.2 Future Perspectives

The future prospects of our work in localization and sensing are as follows:

7.2.1 Localization

A wide range of localization applications arise from the mechanisms proposed in Chapter 3. One notable application is drone-based localization and sensing for search and rescue operations, where gNBs are installed on the drones to be used for locating individuals lost in remote areas, such as hikers in dense forests or skiers trapped in avalanche-prone zones. A preliminary demonstration of such a drone-based localization has been done in [140, 141] using a COTS UE (Quectel module) with the existing DCI as described in Section 3.2. However, due to the drawbacks of using the existing DCI, there is a variation in distance estimation even when the gNB and UE are static as shown in Figure 3.2. Consequently, the localization accuracy of the drone-based localization was limited to approximately 8 m. The localization performance can be improved using the signaling mechanisms proposed in Chapter 3. However, protocol changes in the UE need to be made, which leads to the use of UE restricted to OAI nrUE. In the future, our OAI UE can be used to demonstrate precise drone-based localization.

Furthermore, the signaling mechanisms proposed in Chapter 3 are currently being discussed to present in the sixth-generation (6G) cellular network standardization meetings by our team at EURECOM.

7.2.2 Sensing

The work on downlink sensing using full-duplex radios to detect rogue drones, as mentioned in Section 5.6, can be extended to perform in real-time using OAI. Moreover, as an alternative to using full-duplex radios at the gNB for downlink sensing, uplink sensing, enabled by the mechanisms proposed in Chapter 3, can achieve similar sensing performance while reducing the hardware complexity associated with full-duplex radios.

Additionally, the primary objective of sensing is to accurately identify the target, such as determining whether the detected object is a car, drone, human, etc. However, current research on inferring targets from channel state information is still in its early stages. This process of target inference can be significantly improved by integrating AI/ML algorithms.

Furthermore, the current validation of sensing-aided channel estimation has been carried out through simulations utilizing both floating-point and fixed-point representations, using MATLAB and OAI RFSIM, respectively. In the future, more practical validation can be achieved through real-time testing with over-the-air transmissions using OAI. Additionally, further analysis can be conducted to evaluate the impact of the number of pilots and errors present in the sensing information.

Bibliography

[1] Sampo Kuutti et al. “A Survey of the State-of-the-Art Localization Techniques and Their Potentials for Autonomous Vehicle Applications”. In: *IEEE Internet of Things Journal* 5.2 (2018), pp. 829–846.

[2] Azim Eskandarian, Chaoxian Wu, and Chuanyang Sun. “Research Advances and Challenges of Autonomous and Connected Ground Vehicles”. In: *IEEE Transactions on Intelligent Transportation Systems* 22.2 (2021), pp. 683–711.

[3] Hao Ran Chi et al. “A Survey of Network Automation for Industrial Internet-of-Things Toward Industry 5.0”. In: *IEEE Transactions on Industrial Informatics* 19.2 (2023), pp. 2065–2077.

[4] Andre Bourdoux et al. “6G white paper on localization and sensing”. In: *arXiv preprint arXiv:2006.01779* (2020).

[5] Satyam Dwivedi et al. “Positioning in 5G Networks”. In: *IEEE Communications Magazine* 59.11 (2021), pp. 38–44.

[6] Lorenzo Italiano et al. *A Tutorial on 5G Positioning*. 2024. arXiv: 2311.10551 [eess.SP]. URL: https://arxiv.org/abs/2311.10551.

[7] Ryan Keating et al. “Overview of Positioning in 5G New Radio”. In: *IEEE ISWCS*. 2019.

[8] Rocco Di Taranto et al. “Location-Aware Communications for 5G Networks: How location information can improve scalability, latency, and robustness of 5G”. In: *IEEE Signal Proc Magazine* 31.6 (2014), pp. 102–112.

[9] Peter Hammarberg et al. “Architecture, Protocols, and Algorithms for Location-Aware Services in Beyond 5G Networks”. In: *IEEE Communications Standards Magazine* 6.4 (2022), pp. 88–95.

[10] Christina Chaccour, Walid Saad, et al. “Joint Sensing and Communication for Situational Awareness in Wireless THz Systems”. In: *IEEE ICC*. 2022.

[11] 3GPP. “Functional stage 2 description of Location Services (LCS) in GERAN”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 43.059 v18.0.0* (2024).

[12] 3GPP. “Stage 2 functional specification of User Equipment (UE) positioning in UTRAN”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 25.305 v18.0.0* (2024).

[13] 3GPP. “Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 36.305 v18.0.0* (2023).

[14] Agassi Melikov. *Cellular Networks: Positioning, Performance Analysis, Reliability*. BoD–Books on Demand, 2011.

[15] Sara Modarres Razavi et al. “Positioning in cellular networks: Past, present, future”. In: *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE. 2018, pp. 1–6.

[16] Chao Yang, Shiwen Mao, and Xuyu Wang. “An overview of 3GPP positioning standards”. In: *GetMobile: Mobile Computing and Communications* 26.1 (2022), pp. 9–13.

[17] José A. del Peral-Rosado et al. “Survey of Cellular Mobile Radio Localization Methods: From 1G to 5G”. In: *IEEE Communications Surveys & Tutorials* 20.2 (2018), pp. 1124–1148. DOI: 10.1109/COMST.2017.2785181.

[18] 3GPP. “Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.305 v18.4.0* (2024).

[19] 3GPP. “Study on NR positioning support”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.855 v16.0.0* (2019).

[20] 3GPP. “NG-RAN; NR Positioning Protocol A (NRPPa)”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.455 v16.1.0* (2020).

[21] 3GPP. “study on NR positioning enhancements v17.0.0.(Rel-17),” in: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.455 v17.2.0* (2021).

[22] 3GPP. “NG-RAN; NR Positioning Protocol A (NRPPa)”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.455 v17.2.0* (2022).

[23] Yi Wang et al. “Recent Progress on 3GPP 5G Positioning”. In: *IEEE VTC-Spring*. 2023.

[24] Xinya Li et al. “Contributed Review: Source-localization algorithms and applications using time of arrival and time difference of arrival measurements”. In: *Review of Scientific Instruments* 87.4 (2016).

[25] José A del Peral-Rosado et al. “Proof-of-concept of dedicated aerial 5G and GNSS testbed for enhanced hybrid positioning”. In: *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*. 2022, pp. 2362–2376.

[26] José A del Peral-Rosado et al. “First field trial results of hybrid positioning with dedicated 5G terrestrial and UAV-based non-terrestrial networks”. In: *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*. 2023, pp. 1598–1605.

[27] José A. del Peral-Rosado et al. “Preliminary Field Results of a Dedicated 5G Positioning Network for Enhanced Hybrid Positioning”. In: *Engineering Proceedings* 54.1 (2023). ISSN: 2673-4591. DOI: 10.3390/ENC2023-15432. URL: https://www.mdpi.com/2673-4591/54/1/6.

[28] José A. del Peral-Rosado et al. “Initial Experimentation of a Real-Time 5G mmWave Downlink Positioning Testbed”. In: *European Navigation Conference (ENC 2024)*. to be published in Engineering Proceedings. Noordwijk, The Netherlands, May 2024.

[29] José A. del Peral-Rosado et al. “Sub-Meter Hybrid Positioning with Flying 5GNetworks and Synchronization Corrections”. In: *ION GNSS+, Technical meeting and showcase of GNSS technology, products and services*. Baltimore, MD, Sept. 2024.

[30] Mohsen Ahadi et al. “5G NR UL SRS TDoA Positioning by OpenAirInterface”. In: *2023 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN)- Work in Progress (WiP)*. 2023.

[31] Adeel Malik et al. “From Concept to Reality: 5G Positioning with Open-Source Implementation of UL-TDoA in OpenAirInterface”. In: *arXiv preprint arXiv:2409.05217* (2024).

[32] 3GPP. “NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.305 v16.2.0* (2020).

[33] 3GPP. “LTE Positioning Protocol (LPP)”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 37.355 V17.0.0* (2022).

[34] 3GPP. “NR; Requirements for support of radio resource management”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.133 V17.5.0* (2022).

[35] William Murphy and Willy Hereman. “Determination of a position in three dimensions using trilateration and approximate distances”. In: *Department of Mathematical and Computer Sciences, Colorado School of Mines, Golden, Colorado, MCS-95* 7 (1995), p. 19.

[36] Martin Braun et al. “Parametrization of joint OFDM-based radar and communication systems for vehicular applications”. In: *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*. 2009, pp. 3020–3024. DOI: 10.1109/PIMRC.2009.5449769.

[37] Klaus Martin Braun. “OFDM radar algorithms in mobile communication networks”. PhD thesis. Karlsruhe, Karlsruher Institut für Technologie (KIT), Diss., 2014, 2014.

[38] J Andrew Zhang et al. “Enabling Joint Communication and Radar Sensing in Mobile Networks-a Survey”. In: *IEEE Communications Surveys & Tutorials* (2021).

[39] Lorenzo Gaudio et al. “Performance Analysis of Joint Radar and Communication using OFDM and OTFS”. In: *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. 2019, pp. 1–6. DOI: 10.1109/ICCW.2019.8757044.

[40] J. Andrew Zhang et al. “An Overview of Signal Processing Techniques for Joint Communication and Radar Sensing”. In: *IEEE JSTSP* 15.6 (2021), pp. 1295–1315. DOI: 10.1109/JSTSP.2021.3113120.

[41] 3GPP. “Service requirements for Integrated Sensing and Communication; Stage 1”. In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 22.137 V19.1.0* (2024).

[42] ERICSSON. https://www.ericsson.com/en/blog/2024/6/integrated-sensing-and-communication.

[43] Nuria González-Prelcic et al. “Six Integration Avenues for ISAC in 6G and Beyond”. In: *IEEE Vehicular Technology Magazine* 20.1 (2025), pp. 18–39. DOI: 10.1109/MVT.2025.3529403.

[44] Dirk Slock. “Location aided wireless communications”. In: *IEEE ISCCSP*. 2012.

[45] Nil Garcia, Henk Wymeersch, et al. “Location-aided mm-wave channel estimation for vehicular communication”. In: *IEEE SPAWC*. 2016.

[46] Remun Koirala, Bernard Uguen, et al. “Direction Aided Multipath Channel Estimation for Millimeter Wave Systems”. In: *IEEE VTC-Spring*. 2021.

[47] Shuaifeng Jiang and Ahmed Alkhateeb. “Sensing Aided OTFS Channel Estimation for Massive MIMO Systems”. In: *arXiv preprint arXiv:2209.11321* (2022).

[48] Anum Ali, Nuria González-Prelcic, and Robert W. Heath. “Millimeter Wave Beam-Selection Using Out-of-Band Spatial Information”. In: *IEEE Trans on Comm* 17.2 (2018), pp. 1038–1052. DOI: 10.1109/TWC.2017.2773532.

[49] Anum Ali, Nuria González-Prelcic, and Amitava Ghosh. “Millimeter wave V2I beam-training using base-station mounted radar”. In: *IEEE RadarConf*. 2019.

[50] Fan Liu et al. “Radar-Assisted Predictive Beamforming for Vehicular Links: Communication Served by Sensing”. In: *IEEE Trans on Comm* 19.11 (2020), pp. 7704–7719. DOI: 10.1109/TWC.2020.3015735.

[51] Yuyang Wang, Murali Narasimha, et al. “MmWave Beam Prediction with Situational Awareness: A Machine Learning Approach”. In: *IEEE SPAWC*. 2018.

[52] Aldebaro Klautau, Nuria González-Prelcic, and Robert W. Heath. “LIDAR Data for Deep Learning-Based mmWave Beam-Selection”. In: *IEEE Wireless Communications Letters* 8.3 (2019), pp. 909–912. DOI: 10.1109/LWC.2019.2899571.

[53] Flavio Maschietti et al. “Robust location-aided beam alignment in millimeter wave massive MIMO”. In: *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE. 2017, pp. 1–6.

[54] Fernando Pedraza, Mari Kobayashi, and Giuseppe Caire. “Beam Refinement and User State Acquisition via Integrated Sensing and Communication with OFDM”. In: *2021 IEEE 22nd International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. 2021, pp. 476–480. DOI: 10.1109/SPAWC51858.2021.9593136.

[55] José Miguel Mateos-Ramos et al. “Model-Based End-to-End Learning for Multi-Target Integrated Sensing and Communication Under Hardware Impairments”. In: *IEEE Transactions on Wireless Communications* 24.3 (2025), pp. 2574–2589. DOI: 10.1109/TWC.2024.3522667.

[56] Qualcomm. https://www.youtube.com/watch?v=n51I3BBh8Mo.

[57] Qualcomm. https://www.youtube.com/watch?v=82zIWOa2PhI.

[58] Florian Kaltenberger et al. “OpenAirInterface: Democratizing innovation in the 5G Era”. In: *Computer Networks* 176 (2020), p. 107284.

[59] srsRAN. https://github.com/srsran.

[60] Dexin Li et al. “Performance Evaluation of E-CID based Positioning on OAI 5G-NR Testbed”. In: *IEEE/CIC ICCC*. 2022.

[61] Adeel Malik et al. *From Concept to Reality: 5G Positioning with Open-Source Implementation of UL-TDoA in OpenAirInterface*. 2024. arXiv: 2409.05217 [cs.IT]. URL: https://arxiv.org/abs/2409.05217.

[62] Rakesh Mundlamuri et al. "Novel Round Trip Time Estimation in 5G NR". In: *IEEE GLOBECOM*. 2024. URL: https://arxiv.org/abs/2404.19618v1.

[63] Rajeev Gangula et al. "Round Trip Time Estimation Utilizing Cyclic Shift of Uplink Reference Signal". In: *arXiv preprint arXiv:2410.04528* (2024).

[64] URL: https://gitlab.eurecom.fr/oai/cn5g/oai-cn5g-fed/-/blob/master/docs/DEPLOY_SA5G_BASIC_DEPLOYMENT.md.

[65] Adeel Malik et al. "From Concept to Reality: 5G Positioning with UL-TDoA in OpenAirInterface". In: *IEEE INFOCOM WKSHPS: NG-OPERA 2025: Next-generation Open and Programmable Radio Access Networks (INFOCOM NGOPERA 2025)*. London, United Kingdom (Great Britain), May 2025, p. 5.88.

[66] OpenAirInterface. https://gitlab.eurecom.fr/oai/openairinterface5g/-/blob/develop/doc/RUNMODEM.md.

[67] URL: https://gitlab.eurecom.fr/oai/openairinterface5g/-/blob/develop/doc/NR_SA_Tutorial_OAI_nrUE.md.

[68] 3GPP. "NR; Physical channels and modulation". In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.211 v16.0.0* (2020).

[69] OpenAirInterface. https://gitlab.eurecom.fr/oai/openairinterface5g/-/blob/develop/doc/RUN_NR_PRS.md.

[70] Yi Wang et al. "Enabling Low-Power High-Accuracy Positioning (LPHAP) in 3GPP NR Standards". In: *IEEE IPIN*. 2021.

[71] Mikko Säily et al. "Positioning Technology Trends and Solutions Toward 6G". In: *IEEE PIMRC*. 2021.

[72] Stanford. https://ccrma.stanford.edu/~jos/st/Specific_DB_Scales.html.

[73] OpenAirInterface. https://gitlab.eurecom.fr/oai/openairinterface5g/-/blob/develop/common/utils/T/DOC/T/howto_new_trace.md.

[74] OpenAirInterface. https://gitlab.eurecom.fr/oai/openairinterface5g/-/blob/develop/common/utils/T/DOC/T/basic.md.

[75] Round Trip Time Measurement Dataset. https://hdl.handle.net/2047/D20666241.

[76] Alejandro Blanco et al. "Performance Evaluation of Single Base Station ToA-AoA Localization in an LTE Testbed". In: *IEEE PIMRC*. 2019.

[77] Rakesh Mundlamuri et al. "System and a Method for Improved Round Trip Time Estimation". In: *EUROPEAN PATENT 23306847.7*. Oct. 2023.

[78] 3GPP. "NR; User Equipment (UE) conformance specification; Radio Resource Management (RRM)". In: *3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.533 V15.0.0* (2019).

[79] SignalCraft. https://www.signalcraft.com/products/test-measurement/microwave-systems/sc2430/.

[80] Walid Saad, Mehdi Bennis, and Mingzhe Chen. "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems". In: *IEEE Network* 34.3 (2020), pp. 134–142.

[81] Sundeep Rangan, Theodore S. Rappaport, and Elza Erkip. "Millimeter-Wave Cellular Wireless Networks: Potentials and Challenges". In: *Proceedings of the IEEE* 102.3 (2014), pp. 366–385.

[82] Akdeniz et al. "Millimeter Wave Channel Modeling and Cellular Capacity Evaluation". In: *IEEE JSAC* 32.6 (2014), pp. 1164–1179.

[83] Philip Schniter and Akbar Sayeed. "Channel estimation and precoder design for millimeter-wave communications: The sparse way". In: *IEEE Asilomar Conference on Signals, Systems and Computers*. 2014.

[84] Ahmed Alkhateeb et al. "Channel Estimation and Hybrid Precoding for Millimeter Wave Cellular Systems". In: *IEEE JSTSP* 8.5 (2014), pp. 831–846.

[85] Junho Lee et al. “Channel Estimation via Orthogonal Matching Pursuit for Hybrid MIMO Systems in Millimeter Wave Communications”. In: *IEEE Trans on Comm* 64.6 (2016), pp. 2370–2386.

[86] Kiran Venugopal et al. “Channel Estimation for Hybrid Architecture-Based Wideband Millimeter Wave Systems”. In: *IEEE JSAC* 35.9 (2017), pp. 1996–2009.

[87] Haoyue Tang, Jintao Wang, and Longzhuang He. “Off-Grid Sparse Bayesian Learning-Based Channel Estimation for MmWave Massive MIMO Uplink”. In: *IEEE Wireless Communications Letters* 8.1 (2019), pp. 45–48. DOI: 10.1109/LWC.2018.2850900.

[88] Amrita Mishra et al. “Sparse Bayesian learning-based channel estimation in millimeter wave hybrid MIMO systems”. In: *IEEE SPAWC*. 2017.

[89] Deepak Vasisht et al. “Eliminating channel feedback in next-generation cellular networks”. In: *Proceedings of the ACM SIGCOMM Conference*. 2016.

[90] Sandeep Rao. “Introduction to mmWave sensing: FMCW radars”. In: *Texas Instruments (TI) mmWave Training Series* (2017), pp. 1–11.

[91] Javier Rodríguez-Fernández et al. “Frequency-Domain Compressive Channel Estimation for Frequency-Selective Hybrid Millimeter Wave MIMO Systems”. In: *IEEE Trans on Comm* 17.5 (2018), pp. 2946–2960. DOI: 10.1109/TWC.2018.2804943.

[92] D.P. Wipf et al. “Sparse Bayesian learning for basis selection”. In: *IEEE Transactions on Signal Processing* 52.8 (2004), pp. 2153–2164. DOI: 10.1109/TSP.2004.831016.

[93] Zhilin Zhang and Bhaskar D. Rao. “Sparse Signal Recovery With Temporally Correlated Source Vectors Using Sparse Bayesian Learning”. In: *IEEE JSTSP* 5.5 (2011), pp. 912–926. DOI: 10.1109/JSTSP.2011.2159773.

[94] Sai Subramanyam Thoota et al. “Site-specific millimeter-wave compressive channel estimation algorithms with hybrid MIMO architectures”. In: *ITU Journal on Future and Evolving Technologies* 2.4 (2021).

[95] Michael E Tipping. “Sparse Bayesian learning and the relevance vector machine”. In: *J. Mach. Learn. Res.* 1.Jun (2001), pp. 211–244.

[96] “5G-NR; Physical Channels and Modulation”. In: *3GPP TS 38.211 version 15.2.0 Release 15* ().

[97] Colosseum. https://colosseum.sites.northeastern.edu/.

[98] Leonardo Bonati et al. “Colosseum: Large-Scale Wireless Experimentation Through Hardware-in-the-Loop Network Emulation”. In: *2021 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. 2021, pp. 105–113. DOI: 10.1109/DySPAN53946.2021.9677430.

[99] Davide Villa et al. “Colosseum as a Digital Twin: Bridging Real-World Experimentation and Wireless Network Emulation”. In: *IEEE Transactions on Mobile Computing* 23.10 (2024), pp. 9150–9166. DOI: 10.1109/TMC.2024.3359596.

[100] Michele Polese et al. “Colosseum: The Open RAN Digital Twin”. In: *IEEE Open Journal of the Communications Society* 5 (2024), pp. 5452–5466. DOI: 10.1109/OJCOMS.2024.3447472.

[101] Davide Villa et al. “CaST: A toolchain for creating and characterizing realistic wireless network emulation scenarios”. In: *Proceedings of the 16th ACM Workshop on Wireless Network Testbeds, Experimental evaluation & CHaracterization*. 2022, pp. 45–52.

[102] Davide Villa et al. “Twinning Commercial Radio Waveforms in the Colosseum Wireless Network Emulator”. In: *Proceedings of the 17th ACM Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*. WiNTECH ’23. Madrid, Spain: Association for Computing Machinery, 2023, pp. 33–40. ISBN: 9798400703409. DOI: 10.1145/3615453.3616519. URL: https://doi.org/10.1145/3615453.3616519.

[103] Mauro Belgiovine et al. “MEGATRON: Machine Learning in 5G with Analysis of Traffic in Open Radio Access Networks”. In: *2024 International Conference on Computing, Networking and Communications (ICNC)*. 2024, pp. 1054–1058. DOI: 10.1109/ICNC59896.2024.10556189.

[104] Eugenio Moro et al. “Toward Open Integrated Access and Backhaul with O-RAN”. In: *2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet)*. 2023, pp. 61–69. DOI: 10.1109/MedComNet58619.2023.10168870.

[105] Michele Polese et al. “ColO-RAN: Developing Machine Learning-Based xApps for Open RAN Closed-Loop Control on Programmable Experimental Platforms”. In: *IEEE Transactions on Mobile Computing* 22.10 (2023), pp. 5787–5800. DOI: 10.1109/TMC.2022.3188013.

[106] Gabriele Gemmi et al. “ColosSUMO: Evaluating Cooperative Driving Applications with Colosseum”. In: *2024 IEEE Vehicular Networking Conference (VNC)*. 2024, pp. 97–100. DOI: 10.1109/VNC61989.2024.10576000.

[107] OpenStreetMap. https://www.openstreetmap.org.

[108] Blender. https://www.blender.org/.

[109] MATLAB. https://fr.mathworks.com/products/matlab.html.

[110] Nvidia Sionna. https://developer.nvidia.com/sionna.

[111] Remcom. https://www.remcom.com/wireless-insite-propagation-software.

[112] Miead Tehrani-Moayyed et al. “Creating RF Scenarios for Large-scale, Real-time Wireless Channel Emulators”. In: *2021 19th Mediterranean Communication and Computer Networking Conference (MedComNet)*. 2021, pp. 1–8. DOI: 10.1109/MedComNet52149.2021.9501275.

[113] Christian Mehlführer et al. “Low-complexity MIMO channel simulation by reducing the number of paths”. In: *Proc. ITG/IEEE Workshop on Smart Antennas (WSA 2007), Vienna, Austria*. 2007.

[114] DARPA. Spectrum Collaboration Challenge : https://colosseum.sites.northeastern.edu/.

[115] Anthony T Plummer Jr and Kevin P Taylor. “Development and Operations on the Defense Advanced Research Project Agency’s Spectrum Collaboration Challenge”. In: *Johns Hopkins APL Technical Digest* 35.1 (2019), pp. 22–33.

[116] DM Coleman et al. “Overview of the colosseum: The world’s largest test bed for radio experiments”. In: *Johns Hopkins APL Technical Digest* 35.1 (2019), pp. 4–11.

[117] U.S. Naval Research Laboratory. MGEN Traffic Emulator. https://www.nrl.navy.mil/Our-Work/Areas-of-Research/Information-Technology/NCS/MGEN.

[118] Sommer Christoph and Dressler Falko. “Using the Right Two-Ray Model? A Measurement based Evaluation of PHY Models in VANETs”. In: *Proceedings of 17th ACM International Conference on Mobile Computing and Networking*. 2011.

[119] Qualcomm. https://www.youtube.com/watch?v=iGjPjz7CqbI.

[120] Mohammad Mozaffari et al. “A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems”. In: *IEEE Communications Surveys & Tutorials* 21.3 (2019), pp. 2334–2360.

[121] Rajeev Gangula et al. “Flying Rebots: First Results on an Autonomous UAV-Based LTE Relay Using Open Airinterface”. In: *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. 2018.

[122] Ayon Chakraborty et al. “SkyRAN: A Self-Organizing LTE RAN in the Sky”. In: *Proceedings of the 14th International Conference on Emerging Networking EXperiments and Technologies*. CoNEXT ’18. Heraklion, Greece, 2018.

[123] Ludovico Ferranti et al. “SkyCell: A Prototyping Platform for 5G Aerial Base Stations”. In: *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*. 2020.

[124] Eugenio Moro et al. “IABEST: An Integrated Access and Backhaul 5G Testbed for Large-Scale Experimentation”. In: *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*. MobiCom ’22. Sydney, NSW, Australia, 2022. ISBN: 9781450391818.

[125] Omid Esrafilian et al. *Aerial 5G relay*. 2023. URL: https://www.drone4wireless.com/projects/aerial-5g-relay.

[126] Michele Polese et al. *Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges*. 2022. arXiv: 2202.01032 [cs.NI].

[127] Henrik Ronkainen et al. “Integrated access and backhaul a New Type of Wireless Backhaul in 5G”. In: *Ericsson Technology Review* 2020.7 (2020), pp. 2–11.

[128] Rakesh Mundlamuri et al. *Integrated Access and Backhaul in 5G with Aerial Distributed Unit using OpenAirInterface*. 2023. URL: https://www.drone4wireless.com/projects/aerial-5g-integrated-access-and-backhaul.

[129] FCC. *FCC Opens Spectrum Horizons for New Services and Technologies*. URL: https://www.fcc.gov/document/fcc-opens-spectrum-horizons-new-services-technologies-0.

[130] Priyangshu Sen and Josep M. Jornet. “Experimental Demonstration of Ultra-broadband Wireless Communications at True Terahertz Frequencies”. In: *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. 2019.

[131] Theodore S. Rappaport et al. “Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond”. In: *IEEE Access* 7 (2019), pp. 78729–78757.

[132] Hussam Abdellatif et al. “A Real-Time Ultra-broadband Software-Defined Radio Platform for Terahertz Communications”. In: *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2022.

[133] Michele Polese et al. “Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges”. In: *IEEE Communications Surveys & Tutorials* 25.2 (2023), pp. 1376–1411. DOI: 10.1109/COMST.2023.3239220.

[134] Florian Kaltenberger et al. “OpenAirInterface: Democratizing innovation in the 5G Era”. In: *Computer Networks* 176 (2020), p. 107284. ISSN: 1389-1286.

[135] TMYTECH. *mmW-OAI - Establish a 5G FR2 End-to-End Test Network*. 2023. URL: https://tmytek.com/solutions/mmW-OAI.

[136] Priyangshu Sen et al. “A versatile experimental testbed for ultrabroadband communication networks above 100 GHz”. In: *Computer Networks* 193 (2021), p. 108092. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.108092. URL: https://www.sciencedirect.com/science/article/pii/S1389128621001778.

[137] Priyangshu Sen et al. “The TeraNova platform: An integrated testbed for ultra-broadband wireless communications at true Terahertz frequencies”. In: *Computer Networks* 179 (2020), p. 107370. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2020.107370. URL: https://www.sciencedirect.com/science/article/pii/S1389128620304473.

[138] Priyangshu Sen et al. “A versatile experimental testbed for ultrabroadband communication networks above 100 GHz”. In: *Computer Networks* 193 (July 2021), p. 108092. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.108092. URL: https://www.sciencedirect.com/science/article/pii/S1389128621001778.

[139] URL: https://www.speedtest.net/.

[140] Omid Esrafilian et al. “First Results on UAV-aided User Localization Using ToA and OpenAirInterface in 5G NR”. In: *arXiv preprint arXiv:2503.19529* (2025).

[141] Omid Esrafilian et al. https://youtu.be/jR4CiipPccQ.