UC Irvine

UC Irvine Electronic Theses and Dissertations

Title

Cellular Signals for Navigation: 4G, 5G, and Beyond

Permalink

https://escholarship.org/uc/item/94r6r9tn

Author

Abdallah, Ali A.

Publication Date

2023

Peer reviewed|Thesis/dissertation

eScholarship.org Powered by the California Digital Library
University of California

UNIVERSITY OF CALIFORNIA,
IRVINE

Cellular Signals for Navigation: 4G, 5G, and Beyond

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Electrical Engineering and Computer Science

by

Ali A. Abdallah

Dissertation Committee:
Professor A. Lee Swindlehurst, Chair
Professor Ender Ayanoglu
Professor Hamid Jafarkhani

2023

© 2023 Ali A. Abdallah

DEDICATION

To my parents Ahmad and Ghazwa; my siblings: Houda, Tarek, Shadia, Mai, Safa, Fatima, and Mohamad; and to the love of my life, Fatima. You are all with me every second.

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

LIST OF ALGORITHMS

ACKNOWLEDGMENTS

I extend my deepest gratitude to my advisor, Prof. A. Lee Swindlehurst, for his steadfast guidance, unwavering support, boundless positivity, and empathetic understanding throughout my doctoral journey in his lab. Prof. Swindlehurst's profound expertise and insightful perspectives have been instrumental in shaping not only the trajectory of my research but also my development as a scholar. I would also like to thank Prof. Swindlehirst for giving me the opportunity to attend and present at many conferences in the field. If I were to encapsulate my gratitude in a few words, they would be these: Prof. Swindlehurst, you are a real inspiration. Your mentorship has left an indelible mark on my career, and I will always hold the utmost respect and admiration for you.

I am grateful to my advisor during the initial phase of my doctoral journey, Prof. Zak Kassas, for his guidance and support. Prof. Kassas was pivotal in challenging me to explore the furthest reaches of my potential, instilling in me a profound understanding of my capabilities. His generosity in providing opportunities to attend and present at numerous conferences, along with ensuring access to essential research equipment and materials, has been invaluable. The unique scientific experiences I gained at the ASPIN lab have not only enriched my doctoral studies but also set a solid foundation for my future career.

My heartfelt thanks go to Prof. Samer Saab, whose belief in my potential and inspiring encouragement were the driving forces behind my decision to pursue doctoral studies. His guidance has been a beacon both academically and personally, shaping my journey in profound ways.

I extend my deepest appreciation to Dr. Joe Khalife, an exemplary mentor whose guidance has been invaluable. The time spent under his tutelage, absorbing not only academic wisdom but also personal insights, has been a cornerstone of my growth. Conversations with Dr. Khalife, ranging from research to music, philosophy, and the nuances of life, are moments I will forever treasure and draw inspiration from.

I would like to thank my Ph.D. committee members Prof. Ender Ayanoglu and Prof. Hamid Jafarkhani for taking the time to serve on the committee and for all their helpful advice throughout my Qualifying exam and Ph.D. Defense.

I would like to thank the Office of Naval Research (ONR), the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), the Department of Transportation (DOT), the U.S. Air Force, the Sandia National Laboratories, and the University of California, Irvine (UCI) for supporting my research. DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited. 412TW-PA-20146.

I would like to thank Institute of Electrical and Electronics Engineers (IEEE) and Institute of Navigation (ION) for giving me the chance to present my work to the rest of the community by publishing my conference and journal papers.

I would like to thank my friends and colleagues: Joe, Joshua, Samer, Kimia, Ceren, and

Shady for their support throughout the Ph.D. journey and for all the helpful discussions and help with experiments.

My deepest gratitude goes to my parents, Ahmad and Ghazwa, and my siblings - Houda, Tarek, Shadia, Mai, Safa, Fatima, and Mohamad - for being the most wonderful family one could ever hope for. Words fall short in expressing my immense love and longing for them. Their unconditional support has been the cornerstone of my journey, propelling me to heights I never imagined possible. It is my earnest hope that they take pride in my achievements, just as I take pride in being part of our incredible family.

Finally, my profound thanks to the love of my life, Fatima, whose unwavering support and love shone brightly across any distance. Her selfless sacrifices were a beacon of strength and resilience, helping me navigate through this challenging journey. I am eternally grateful and deeply committed to bringing as much joy and happiness into her life as she has brought into mine.

VITA

Ali A. Abdallah

EDUCATION

Doctor of Philosophy in Electrical Engineering **2023**
University of California, Irvine *Irvine, Califronia*

Master of Science in Electrical Engineering **2022**
University of California, Irvine *Irvine, Califronia*

Bachelor of Engineering in Electrical Engineering **2017**
Lebanese American University *Byblos, Lebanon*

RESEARCH EXPERIENCE

Research Scientist **January 2022 – Present**
Google LLC via Magnit *Irvine, California, USA*

Graduate Research Assistant **2019–2023**
University of California, Irvine *Irvine, California, USA*

Ph.D. Research Intern **June 2022 – September 2022**
Google LLC *Mountain View, California, USA*

Graduate Research Assistant **2018–2019**
University of California, Riverside *Riverside, California, USA*

REFEREED JOURNAL PUBLICATIONS

[J10] **A. Abdallah** and A. L. Swindlehurst (2023) "A Passive EKF-Based Reconfigurable Intelligent Surface (RIS)-Aided Cellular Navigation System," *IEEE Transactions on Aerospace and Electronic Systems*, in progress.

[J9] Z. Kassas, **A. Abdallah**, S. Shahcheraghi, A. Kaiss, J. Khalife, C. Lee, J. Jurado, S. Wachtel, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, and R. Tay (2023) "I can hear you loud and clear: GNSS-less high altitude aircraft navigation with terrestrial cellular signals of opportunity," *IEEE Transactions on Aerospace and Electronic Systems*, submitted.

[J8] Z. Kassas and **A. Abdallah** (2023) "No GPS no problem: exploiting cellular OFDM-based signals for accurate navigation," *IEEE Transactions on Aerospace and Electronic Systems*, accepted.

[J7] Z. Kassas, J. Khalife, **A. Abdallah**, C. Lee, J. Jurado, S. Wachtel, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, and R. Tay (2023) "Flight demonstration of high altitude aircraft navigation with cellular signals," *IEEE Intelligent Transportation Systems Magazine*, Vol. 15, no. 4, pp. 150–165.

[J6] **A. Abdallah**, J. Khalife, and Z. Kassas (2023) "Exploiting on-demand 5G downlink signals for opportunistic navigation," *IEEE Signal Processing Letters*, Vol. 30, pp. 389-393.

[J5] C. Jao, **A. Abdallah**, C. Chen, M. Seo, S. Kia, Z. Kassas, and A. Shkel (2022) "PINDOC: pedestrian indoor navigation system integrating deterministic, opportunistic, and cooperative functionalities," *IEEE Sensors Journal*, Vol. 22, no. 14, pp. 14424-14435.

[J4] Z. Kassas, J. Khalife, **A. Abdallah**, C. Lee, J. Jurado, S. Wachtel, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, and R. Tay (2022) "Assessment of cellular signals of opportunity for high altitude aircraft navigation," *IEEE Aerospace and Electronic Systems Magazine*, Vol. 37, no. 10, pp. 4-19.

[J3] Z. Kassas, J. Khalife, **A. Abdallah**, and C. Lee (2022) "I am not afraid of the GPS jammer: resilient navigation via signals of opportunity in GPS-denied environments," *IEEE Aerospace and Electronic Systems Magazine*, Vol. 37, no. 7, pp. 4-19.

[J2] **A. Abdallah**, C. Jao, Z. Kassas, and A. Shkel (2022) "A pedestrian indoor navigation system using deep-learning-aided cellular signals and ZUPT-aided foot-mounted IMUs," *IEEE Sensors Journal*, Vol. 22, no. 6, pp. 5188-5198.

[J1] **A. Abdallah** and Z. Kassas (2021) "Multipath mitigation via synthetic aperture beamforming for indoor and deep urban navigation," *IEEE Transactions on Vehicular Technology*, Vol. 70, Issue 9, pp. 8838–8853.

REFEREED CONFERENCE PUBLICATIONS

[C24] **A. Abdallah** and A. L. Swindlehurst (2023) "A Passive EKF-Based RIS-Aided Cellular Navigation System," *IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing*, Dec. 10-13, 2023, Los Sueño, Costa Rica, accepted.

[C23] **A. Abdallah** and A. L. Swindlehurst (2023) "5G and Beyond: An EKF-Based Reconfigurable Intelligent Surface (RIS)-Aided Navigation Approach," *ION Global Navigation Satellite Systems Conference*, Sep. 11-15, 2023, Denver, CO, pp. 2348-2360.

[C22] Z. Kassas, **A. Abdallah**, C. Lee, J. Jurado, S. Wachtel, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, and R. Tay (2022) "Protecting the skies: GNSS-less aircraft navigation with terrestrial cellular signals of opportunity," *ION Global Navigation Satellite Systems*

Conference, Sep. 19-23, 2022, Denver, CO, pp. 1014-1025.
[C21] C. Jao, **A. Abdallah**, C. Chen, M. Seo, S. Kia, Z. Kassas, and A. Shkel (2022) "Submeter accurate pedestrian indoor navigation system with dual ZUPT-aided INS, machine learning-aided LTE, and UWB signals," *ION Global Navigation Satellite Systems Conference*, Sep. 19-23, 2022, Denver, CO, pp. 1108-1126.
[C20] **A. Abdallah**, M. Orabi, and Z. Kassas (2022) "Multipath mitigation of 5G signals via reinforcement learning for navigation in urban environments," *IEEE Vehicular Technology Conference*, Jun. 19-22, 2022, Helsinki, Finland, pp. 1-5.
[C19] **A. Abdallah**, Z. Kassas, and C. Lee (2022) "Demo: I am not afraid of the GPS jammer: exploiting cellular signals for accurate ground vehicle navigation in a GPS-denied environment," *ACM Workshop on Automotive and Autonomous Vehicle Security*, Apr. 24, 2022, San Diego, CA, pp. 1-1.
[C18] **A. Abdallah** and Z. Kassas (2022) "Opportunistic navigation using sub-6 GHz 5G downlink signals: a case study on a ground vehicle," *European Conference on Antennas and Propagation*, Mar. 27 - Apr. 1, 2022, Madrid, Spain, pp. 1-5 (special session).
[C17] Z. Kassas, **A. Abdallah**, J. Khalife, C. Lee, J. Jurado, S. Wachtel, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, and R. Tay (2022) "Received power characterization of terrestrial cellular signals on high altitude aircraft," *IEEE Aerospace Conference*, Mar. 5-12, 2022, Big Sky, MT, pp. 1-8.
[C16] S. Kozhaya, J. Haidar-Ahmad, **A. Abdallah**, Z. Kassas, and S. Saab (2021) "Comparison of neural network architectures for simultaneous tracking and navigation with LEO satellites," *ION Global Navigation Satellite Systems Conference*, Sep. 20-24, 2021, St. Louis, MO, pp. 2507–2520.
[C15] **A. Abdallah** and Z. Kassas (2021) "UAV navigation with 5G carrier phase measurements," *ION Global Navigation Satellite Systems Conference*, Sep. 20-24, 2021, St. Louis, MO, pp. 3294-3306.
[C14] M. Orabi, **A. Abdallah**, J. Khalife, and Z. Kassas (2021) "A machine learning multipath mitigation approach for opportunistic navigation with 5G signals," *ION Global Navigation Satellite Systems Conference*, Sep. 20-24, 2021, St. Louis, MO, pp. 2895-2909.
[C13] **A. Abdallah**, J. Khalife, and Z. Kassas (2021) "Experimental characterization of received 5G signals carrier-to-noise ratio in indoor and urban environments," *IEEE Vehicular Technology Conference*, Apr. 25-28, 2021, Helsinki, Finland, pp. 1-5.
[C12] H. Lee, **A. Abdallah**, J. Park, J. Seo, and Z. Kassas (2020) "Neural network-based ranging with LTE channel impulse response for localization in indoor environments," *International Conference on Control, Automation, and Systems*, Oct. 13-16, 2020, Busan, South Korea, pp. 939–944.
[C11] Z. Kassas, J. Khalife, **A. Abdallah**, and C. Lee (2020) "I am not afraid of the jammer: navigating with signals of opportunity in GPS-denied environments," *ION Global Navigation Satellite Systems Conference*, Sep. 21-25, 2020, St. Louis, MO, pp. 1566–1585.
[C10] **A. Abdallah**, K. Shamaei, and Z. Kassas (2020) "Assessing real 5G signals for opportunistic navigation," *ION Global Navigation Satellite Systems Conference*, Sep. 21-25, 2020, St. Louis, MO, pp. 2548–2559.
[C9] **A. Abdallah** and Z. Kassas (2020) "Deep learning-aided spatial discrimination for multipath mitigation," *IEEE/ION Position, Location, and Navigation Symposium*, Apr. 22-24, 2020, Portland, OR, pp. 1324–1335.

[C8] M. Orabi, J. Khalife, **A. Abdallah**, Z. Kassas, and S. Saab (2020) "A machine learning approach for GPS code phase estimation in multipath environments," *IEEE/ION Position, Location, and Navigation Symposium*, Apr. 22-24, 2020, Portland, OR, pp. 1224–1229.
[C7] **A. Abdallah**, K. Shamaei, and Z. Kassas (2019) "Performance characterization of an indoor localization system with LTE code and carrier phase measurements and an IMU," *International Conference on Indoor Positioning and Indoor Navigation*, Sep. 30 - Oct. 3, 2019, Pisa, Italy, pp. 1-8.
[C6] **A. Abdallah** and Z. Kassas (2019) "Evaluation of feedback and feedforward coupling of synthetic aperture navigation with LTE signals," *IEEE Vehicular Technology Conference*, Sep. 22-25, 2019, Honolulu, HI, pp. 1-6.
[C5] **A. Abdallah**, K. Shamaei, and Z. Kassas (2019) "Indoor localization with LTE carrier phase measurements and synthetic aperture antenna array," *ION Global Navigation Satellite Systems Conference*, Sep. 16-20, 2019, Miami, FL, pp. 2670-2679.
[C4] C. Ardito, J. Morales, J. Khalife, **A. Abdallah**, and Z. Kassas (2019) "Performance evaluation of navigation using LEO satellite signals with periodically transmitted satellite positions," *ION International Technical Meeting*, Jan. 28-31, 2019, Reston, VA, pp. 306-318.
[C3] J. Morales, J. Khalife, **A. Abdallah**, C. Ardito, and Z. Kassas (2018) "Inertial navigation system aiding with Orbcomm LEO satellite Doppler measurements," *ION Global Navigation Satellite Systems Conference*, Sep. 24-28, 2018, Miami, FL, pp. 2718-2725.
[C2] **A. Abdallah**, K. Shamaei, and Z. Kassas (2018) "Indoor positioning based on LTE carrier phase measurements and an inertial measurement unit," *ION Global Navigation Satellite Systems Conference*, Sep. 24-28, 2018, Miami, FL, pp. 3374-3384.
[C1] **A. Abdallah**, S. Saab, and Z. Kassas (2018) "A machine learning approach for localization in cellular environments," *IEEE/ION Position, Location, and Navigation Symposium*, Apr. 23-26, 2018, Monterey, CA, pp. 1223-1227.

SOFTWARE

LabVIEW, MATLAB, Wireless InSight, C++; LaTeX; MS: Word, Excel. "

PATENTS

Z. Kassas and **A. Abdallah** (2022) "Receiver design for Doppler positioning with low Earth orbit satellites and differential carrier phase measurements," U.S. Patent Application No. 63/355,890.

Z. Kassas and **A. Abdallah** (2022) "Systems and methods for user equipment based 5G navigation and downlink bandwidth operations," U.S. Patent Application No. 63/315,719.

Z. Kassas, **A. Abdallah**, and K. Shamaei (2019) "Indoor localization system with LTE code and carrier phase measurements and an IMU," U.S. Patent Application No. 62/913,078.

Z. Kassas and **A. Abdallah** (2019) "Synthetic aperture navigation with LTE signals," U.S. Patent Application No. 62/913,074.

Z. Kassas, J. Khalife, and **A. Abdallah** (2019) "Receiver design for Doppler positioning with low Earth orbit satellites and differential carrier phase measurements," U.S. Patent Application No. 62/834,317.

AWARDS

Best Demo Award Runner-Up, "I am not afraid of the GPS jammer: exploiting cellular signals for accurate ground vehicle navigation in a GPS-denied environment," ACM Workshop on Automotive and Autonomous Vehicle Security (AutoSec), San Diego, CA, 2022.

Best Presentation Award, "Protecting the Skies: GNSS-Less Aircraft Navigation with Terrestrial Cellular Signals of Opportunity," *ION GNSS+ Conference*, Denver, CO, 2022.

Best Presentation Award, "A Machine Learning Multipath Mitigation Approach for Opportunistic Navigation with 5G Signals," *ION GNSS+ Conference*, St. Louis, MO, 2021.

Grand Prize at the IEEE Signal Processing Society Contest for Beamforming Research (5-MICC), 2020.

Best Presentation Award, "I am Not Afraid of the Jammer: Navigating with Signals of Opportunity in GPS-Denied Environments," *ION GNSS+ Conference*, Virtual, 2020.

Best Presentation Award, "Assessing Real 5G Signals for Opportunistic Navigation," *ION GNSS+ Conference*, Virtual, 2020.

Best Student Paper Award, "Deep learning-aided spatial discrimination for multipath mitigation," *IEEE/ION Position, Location, and Navigation Symposium*, Portland, OR, 2020.

Best Presentation Award, "Indoor Localization with LTE Carrier Phase Measurements and Synthetic Aperture Antenna Array," *ION GNSS+ Conference*, Miami, FL, 2019.

Paul and Beverly Holmes Endowed Fellowship, *University of California, Irvine*, Irvine, CA, 2020.

Bachelor of Engineering Full Scholarship, *Lebanese American University*, Byblos, Lebanon, 2013-2017.

ABSTRACT OF THE DISSERTATION

Cellular Signals for Navigation: 4G, 5G, and Beyond

By

Ali A. Abdallah

Doctor of Philosophy in Electrical Engineering and Computer Science

University of California, Irvine, 2023

Professor A. Lee Swindlehurst, Chair

Global Navigation Satellite Systems (GNSSs) have long been the cornerstone for positioning, navigation, and timing. Despite their widespread use, GNSS signals face vulnerabilities such as jamming, spoofing, and unreliable coverage in various environments like urban canyons, indoors, tunnels, and parking structures. These limitations make exclusive reliance on GNSS inadequate for the rigorous demands of future applications, including autonomous vehicles (AVs), intelligent transportation systems, and location-based services.

To enhance GNSS performance in challenging settings, traditional methods have typically incorporated dead-reckoning sensors like inertial measurement units, lidars, or cameras. These sensors, however, accumulate errors over time and only offer navigation solutions within a local frame, relative to the user equipment's (UE) initial position. In contrast, alternative signal-based approaches, known as signals of opportunity (SOPs) – encompassing AM/FM radio, satellite communication signals, digital television signals, Wi-Fi, and cellular – hold considerable promise as global navigation sources in GNSS-challenged environments.

Among SOPs, cellular signals, particularly from third-generation (3G, code-division multiple access (CDMA)), fourth-generation (4G, long-term evolution (LTE)), and fifth-generation (5G, new radio (NR)) networks, stand out as potential navigation aids. Their navigation-friendly characteristics include ubiquity, geometric diversity, high carrier frequencies, spectral

diversity, spatial diversity, broad bandwidth, strong signal strength, and free accessibility.

Nevertheless, as SOPs are primarily designed for communication rather than navigation, utilizing cellular signals for navigational purposes presents several challenges. These include (1) the lack of specific low-level signal and error models for optimal state and parameter extraction for positioning and timing, (2) the absence of published robust, efficient, and reliable receiver architectures to generate navigation observables, (3) continual updates and changes in cellular protocols, and (4) the scarcity of frameworks for high-accuracy navigation using such signals.

This dissertation addresses these challenges, focusing on cellular signals from 4G and 5G networks, with potential extensions to future cellular systems. The foundational contributions of this work are empirically validated on various platforms including ground vehicles (GVs), unmanned aerial vehicles (UAVs), and high-altitude aircraft, demonstrating GNSS-level navigation accuracy.

Chapter 1

Introduction

1.1 Background

Global Navigation Satellite Systems (GNSSs) have been a dominant technology in positioning, navigation, and timing for several decades. Despite their widespread use, GNSS signals encounter notable limitations:

1. Weakness in signal strength makes them ineffective in certain environments like indoor spaces or deep urban canyons [2].
2. Vulnerability to both unintentional interference and deliberate jamming [3, 4].
3. Civilian signals are not encrypted nor authenticated and are detailed in publicly accessible documents, leading to potential spoofing risks [4].
4. Imprecise vertical position estimates due to limited angle diversity of GNSS space vehicles, posing challenges, especially for aerial vehicles [5].

Given these limitations, relying solely on GNSSs falls short of meeting the stringent require-

ments of future applications, including autonomous vehicles (AVs), intelligent transportation systems, and location-based services. To augment GNSS performance in challenging environments, conventional methods typically involve dead-reckoning sensors such as inertial measurement units [6], lidars [7], or cameras [8]. These sensors, however, accumulate errors over time and provide navigation solutions only within a local frame, relative to the AV's initial position.

An alternative approach is utilizing Signals of Opportunity (SOPs) for global navigation in environments where GNSS is compromised. SOPs are ambient signals not originally intended for positioning, navigation, and timing; they include cellular, AM/FM radio [9], satellite communication [10], digital television [11], and Wi-Fi signals [12, 13]. Among these, cellular signals, particularly the following systems:

- The third-generation (3G), also known as the code-division multiple access (CDMA).
- The fourth-generation (4G), also known as the long-term evolution (LTE).
- The fifth-generation (5G), also known as the new radio (NR)

The cellular signals show significant promise as navigation aids due to their:

1. Ubiquity: The widespread presence of cellular base stations (BSs) due to the prevalence of cellular networks and smartphones.
2. Geometric diversity: Cellular BSs are strategically positioned to provide favorable geometry, unlike certain terrestrial transmitters which are often co-located.
3. High carrier frequency: Ranging from 600 MHz to 3,500 MHz and extending to millimeter-wave (mmWave) bands (28 to 52 GHz), enabling precise carrier phase navigation observations.

4. Broad bandwidth: Cellular signals boast bandwidths up to 100 MHz in 4G (LTE) Advanced, and potentially 1 GHz in mmWave 5G, facilitating accurate time-of-arrival estimates.

5. Strong signal strength: Cellular signals maintain high usability in GNSS-challenged environments, with a carrier-to-noise ratio (CNR) significantly exceeding that of GNSS signals.

Furthermore, cellular signals offer the advantage of zero deployment costs for positioning and navigation as they are already in place and free to use. Specifically, the receiver, or user equipment (UE), can passively receive cellular transmissions without active communication with the BS, extracting crucial positioning and timing data from the signals and computing the navigation solution locally. While network-based navigation methods requiring two-way communication exist, this dissertation concentrates on elucidating the precision of UE-based navigation using cellular signals, particularly focusing on 4G (LTE) and 5G (NR) technologies, with potential extensions to future orthogonal frequency division multiplexing (OFDM)-based cellular systems. The core contributions of this dissertation are showcased across various scenarios, including pedestrians, ground vehicles, unmanned aerial vehicles (UAVs), and high-altitude aircraft, demonstrating meter-level accuracy in navigation solely through the use of cellular 4/5G signals.

1.2 Related Work

Research aimed at enabling effective navigation in environments where GNSS faces challenges is broadly categorized into two distinct approaches: sensor-based and signal-based [14–16]. The sensor-based approach leverages various types of sensors, such as inertial measurement units (IMUs) [17–20], lidars [21, 22], cameras [23, 24], or a combination of sensors [8, 25, 26],

to gather data about the vehicle's or device's surroundings and movement. These sensors, often used in a complementary manner, provide vital information about orientation, speed, and environmental features, allowing for the calculation of position and navigation solutions independent of satellite signals. These approaches, however, tend to accumulate errors over time, requiring occasional re-calibration or reference to a known position.

On the other hand, the signal-based approach to navigation in GNSS-challenged environments employs two main strategies. First, it involves the development and application of advanced signal processing algorithms, as discussed in various studies [27–30]. Second, this approach increasingly utilizes ambient SOPs, which are signals not originally intended for navigation purposes. These signals encompass a range of sources, including cellular networks [31–37], AM/FM radio [38, 39], low Earth orbit (LEO) communication satellites [10, 40–44], digital television (DTV) [45, 46], and Wi-Fi [47–49]. By analyzing signal characteristics such as time-of-arrival (TOA), signal strength, carrier phase, and angle of direction, these SOPs provide alternative means to deduce location and movement.

Each navigation approach has its distinct advantages and limitations, and the selection typically depends on the navigation task's specific requirements and environmental factors. Studies have shown that AM radio and DTV signals can achieve positioning accuracies of approximately 20 meters and 5 meters, respectively [38, 45]. However, these signals often suffer from poor geometric diversity due to transmitters being co-located by design. In contrast, Wi-Fi-based localization, as explored in [50], has demonstrated a positioning accuracy within the 80th percentile of about 5.6 meters. This method, however, requires accurate and current information about Wi-Fi access point locations and is limited by the availability of Wi-Fi signals in certain environments like tunnels or parking structures, and their potential unavailability during emergencies.

Moreover, leveraging LEO communication satellites for navigation has emerged as a promising approach in recent years [44, 51]. This is particularly relevant considering the increasing

number of LEO satellites. Nevertheless, challenges remain due to the directivity of these signals and the typically unknown signal structure for the public, which complicates their utilization for navigation purposes.

This dissertation delves into cellular SOPs, with a particular emphasis on cellular 4/5G signals and future advancements. The exploration into 4G signal-based navigation has been significantly shaped by the development of specialized 4G navigation receivers. Foundational research in this area, as illustrated in [52–54], laid the cornerstone for advanced receiver design. These efforts have yielded promising results, achieving meter- and sub-meter level accuracy in outdoor environments using 4G signals for both ground [1, 52, 54–58] and aerial vehicles [59].

A particularly desirable reference signal (RS), known as the cell-specific RS (CRS), has been leveraged in conventional 4G navigation receivers due to its high bandwidth. Owing to the spectral nature of OFDM, the CRS is transmitted on distinct OFDM symbols and subcarriers, also referred to as logical ports. Studies like [60] proposed a maximum likelihood-based method for first path estimation using one antenna port. The positioning challenges in multipath environments were addressed in [61] and [62], focusing on single antenna port utilization. Moreover, a recent study [63] developed a tracking algorithm that adaptively mitigated multipath in 4G positioning receivers while utilizing CRS from one antenna port. The impact of different antenna ports on TOA estimation using CRS was investigated in [64], revealing that varied channel responses for different antenna ports can diversify incoming signals and enhance positioning accuracy. The utility of signal diversity provided by multiple antenna ports for cycle slip detection in 4G carrier phase measurements was demonstrated in [59]. Additionally, [65] considered exploiting two antenna ports, treating signals from each as separate measurements, while [66] independently tracked signals from each port.

The navigation capabilities of 5G have been the focus of extensive research in recent years [67, 68], employing various methods such as direction-of-arrival (DOA) [69], direction-of-

departure (DOD) [70], TOA [71], or their combinations [72] for precise positioning. However, these studies were largely confined to simulations and laboratory-emulated 5G signals or relied on restrictive assumptions, including the need for network-based localization. Such approaches can compromise user privacy and restrict users to 5G base stations (also known as the Next Generation Node B (gNB)) within their subscribed network. In contrast, downlink 5G signals can be opportunistically exploited for navigation without network communication, as explored in [73]. This approach, which extracts navigation observables from "always-on" transmitted synchronization signals (SSs), has been validated experimentally with promising results.

In signal-based navigation systems, a comprehensive understanding of the radio environment is crucial to extract useful information from the sensed signals. A significant challenge in such environments is signal attenuation, which is particularly pronounced for 5G-and-beyond cellular signals. These signals typically operate at higher carrier frequencies with wavelengths in the millimeter range. The inherent physical characteristics of millimeter wave (mm-wave) signals limit their ability to travel long distances or penetrate through objects. While this limitation reduces the multipath phenomenon—a potentially beneficial attribute for navigation—it poses challenges for communication purposes. In scenarios where line-of-sight (LOS) signals are absent, multipath propagation can ensure a more robust and diverse communication link between the BS and the UE. To address these propagation challenges and enhance the efficiency and reliability of mm-wave cellular systems, the concept of reconfigurable intelligent surfaces (RISs) has emerged as a transformative solution. RISs are essentially passive devices consisting of a large array of electronically tunable unit cells. These cells can be adjusted to control and direct RF propagation favorably, offering a new means to manipulate the radio environment [74–76].

The benefits of RIS for positioning and navigation have been the subject of extensive research in recent years. Various methodologies and localization frameworks have been proposed, uti-

lizing TOA, angle-of-arrival (AOA) / angle-of-departure (AOD), or a combination of these measurements in conjunction with RIS for precise localization. An RIS is utilized for indoor positioning in [77], leveraging ultra-wideband (UWB) signals. This study, both analytical and simulation-based, indicates that RIS can replace traditional active APs and suggests a preference for TOA measurements for position estimation. The work in [78] explores RIS capabilities in multi-user passive localization. By dividing the RIS phase profile into constant and time-varying components and selecting time-varying elements based on orthogonal sequences, it avoids interference between reflected non-line-of-sight (NLOS) signals and the LOS paths, achieving sub-meter accuracy. In [79], a new approach is proposed to exploit wavefront curvature in geometric near-field (NF) conditions, focusing on a downlink scenario. The study suggests that proximity to the RIS or a sufficiently large RIS can enable UE's position inference directly from the RIS-reflected multipath component in NF, without requiring a direct path. However, in far-field (FF) scenarios, both LOS and NLOS paths are needed for effective localization. The concept of partially-connected receiving RISs (R-RISs) is introduced in [80]. This design, comprising several co-located single-RX-RF RIS subarrays, facilitates three-dimensional (3-D) localization in a computationally efficient manner, independent of any BS or AP. A two-stage RIS-aided localization algorithm, named PAssive PosItioning with RIS (PAPIR), is presented in [81]. PAPIR retrieves the TOA and the DOA of RSs sent by the UE to estimate its position.

1.3 Challenges

Despite the advancements, current state-of-the-art 4/5G receiver designs encounter several challenges:

- They exhibit limited robustness and accuracy in environments with significant signal attenuation and short-delay multipath, such as indoor settings. This limitation poses

a critical barrier to their practical applicability in various scenarios.

- The receivers' ability to estimate the initial Doppler in the acquisition stage is limited due to the small duty factor of the synchronization signals utilized for acquiring the signal's Doppler shift, namely 1.43%. This limitation becomes more pronounced in high dynamics applications, where wider Doppler shift ranges require a reliable coarse estimate for effective lock-in in tracking loops.

- They are burdened with a high computational cost, primarily due to their reliance on a communication-influenced frequency-based design that necessitates processing every received OFDM frame. This design feature, while standard in 4G communication receivers for demodulating received data, introduces additional complexity and processing overhead in navigation applications.

To this end, developing an efficient, robust, and accurate 4G navigation receiver that is adaptable to different environments and applications is imperative.

Also, none of the conventional 4G receiver designs have concurrently exploited all antenna ports as a single navigation source, identifying a potential research area. Generally, the extraction of navigation observables from 4G signals in existing methods has been approached predominantly from a communication systems perspective [62], suggesting the need for a 4G navigation receiver that fully exploits the signal's antenna ports.

In addition to the technical intricacies of receiver design, a comprehensive understanding and detailed characterization of the signal are essential for creating a robust navigation receiver. Although theoretical studies have made strides in addressing various challenges associated with cellular 4/5G signals, the practical understanding of these signals is intricately linked to the real-world dynamics of cellular network infrastructure and the influence of the physical environment. Key aspects such as the received signal power and the stability of the signals from BSs are critical for an effective navigation system. However, these elements have not

been extensively explored in practical scenarios. The characterization of received power, which directly impacts signal detectability and accuracy, and the analysis of signal stability from BSs, crucial for consistent and reliable navigation, are areas that require further empirical investigation. This exploration is vital to develop a navigation framework that is not only theoretically sound but also practically robust and reliable in diverse real-world conditions. Such practical insights into signal behavior will significantly enhance the design and implementation of navigation systems that leverage cellular 4/5G signals.

In the realm of cellular navigation, utilizing 5G signals for user-based opportunistic navigation presents unique challenges when compared to 4G. The core of these challenges lies in the ultra-lean transmission policy of 5G networks, which significantly minimizes the transmission of "always-on" signals such as synchronization signals. This policy inherently limits the scope of UE-based opportunistic navigation to these synchronization signals only. When considering the potential downlink bandwidth B_{p} available in 5G networks and comparing it to the bandwidth B_{s} allocated for synchronization signals, it becomes evident that only a small portion of the available spectrum is being used for opportunistic navigation purposes. This limited utilization of the bandwidth is a substantial impediment, as signals with a wider bandwidth are known to provide more precise TOA estimates. These estimates are crucial for effectively differentiating the LOS signals from the multipath components, a key factor in enhancing the accuracy and reliability of navigation solutions. Consequently, harnessing the full potential of 5G signals for user-based navigation, particularly in the context of maximizing bandwidth utilization, remains a significant and unexplored area of research. Overcoming this challenge could unlock new possibilities in navigation accuracy and robustness, especially in complex urban environments where multipath effects are prevalent.

Previous studies have effectively demonstrated the potential of RISs in enhancing positioning and navigation within various scenarios, setting a foundational path for their future incorporation into wireless navigation systems. Nonetheless, a common limitation in these studies,

as highlighted in [80], is the focus on stationary UE. To address this gap, this dissertation presents a novel RIS-based localization approach for mobile UEs in an uplink millimeter-wave cellular environment. This proposed approach synergizes the latest cellular 5G navigation receivers and develops passive AOA estimators, enabling the estimation of both TOA and AOA measurements from RIS-reflected paths for navigation purposes.

1.4 Contributions and Dissertation Outline

The dissertation is structured around the following contributions:

Chapter 2: Model Description

This chapter presents an in-depth analysis of OFDM within 4G and 5G cellular networks, highlighting the desirable characteristics in the signal design that can be exploited for navigation purposes. It explores the transition from 4G to 5G, specifically focusing on the advanced numerologies of 5G, which are vital for designing an effective 4/5G navigation receiver that optimally utilizes OFDM signals. Moreover, the chapter presents a model for received 4/5G signals and introduces two dynamic models for UE motion: the white noise acceleration model for low-dynamic scenarios and the continuous Wiener process acceleration model for high-dynamic contexts. These models form a comprehensive framework for evaluating navigational performance using cellular signals. Additionally, it investigates the dynamics of clock errors in cellular BSs and UE, crucial for precise signal transmission and reception. The chapter concludes by presenting mathematical models for various navigation observables derived from 4/5G signals.

Chapter 3: Accurate, Robust, and Efficient 4/5G Opportunistic Cellular Navigation Receiver

This chapter proposes a novel design for a 4/5G opportunistic cellular navigation receiver, aiming to enhance accuracy, robustness, and efficiency. It evaluates the architecture of conventional frequency-domain-based receivers for 4G and 5G cellular navigation, highlighting their limitations such as weak signal power in challenging environments and a restricted pool of resources for navigation in 5G's ultra-lean transmission approach. To overcome these constraints, the chapter proposes the Ultimate Reference Signal (URS) for 4G and the Ultimate Synchronization Signal (USS) for 5G, designed to utilize a wider bandwidth and improve signal power, thereby facilitating better navigation in demanding conditions.

The chapter presents a time-domain-based navigation receiver that exploits the 4G-URS and 5G-USS for more effective extraction of navigation observables from received 4/5G OFDM signals. This approach differs from conventional SDRs by aggregating all accessible resource elements (REs) to form a composite signal, enhancing the signal's frequency and time resources. The dissertation provides a detailed methodology for generating these signals and outlines the acquisition and tracking stages of the proposed SDR. Tracking results from various scenarios, including high-altitude aircraft and ground vehicle applications, are presented to demonstrate the efficacy of the proposed receiver design.

Chapter 4: Experimental Characterization of 4/5G Signals

This chapter explores the practicality of using 4/5G signals for navigation by assessing their frequency stability and carrier-to-noise ratio (C/N_0) under various conditions. Experiments conducted in different environments reveal the reliable frequency stability of 4/5G networks, with 5G showing particularly more consistent frequency stability. The chapter also assesses the impact of environmental factors, antenna quality, and receiver clock accuracy on 4/5G

signal strength. Results indicate that both 4G and 5G signals maintain similar C/N_0 levels in diverse scenarios, including indoor settings with varying structural barriers, and outdoors with different antenna grades and receiver clocks. Additionally, a mobile outdoor experiment highlights that 5G signals remain robust over considerable distances, suggesting strong potential for reliable navigation solutions even in semi-urban environments. This comprehensive analysis underscores the viability of 4/5G signals for precise and dependable navigation applications.

Chapter 5: Navigation Performance

This comprehensive chapter demonstrates the navigation performance of the proposed 4/5G opportunistic navigation receiver in various scenarios, including ground vehicles, high-altitude aircraft, and UAVs. A ground vehicle equipped with a 4G receiver demonstrated robust navigation in Global Positioning System (GPS)-denied conditions. The vehicle successfully navigated through a challenging course at Edwards Air Force Base, California, showcasing the efficacy of 4G signals for navigation during GPS jamming exercises. Furthermore, in a groundbreaking experiment, 4G signals were harnessed for navigation in high-altitude aircraft scenarios. The study, conducted with a Beechcraft C-12 Huron over Southern California, demonstrated the potential of 4G signals for robust navigation solutions in high-altitude and high-speed environments. This study included characterizing signal strength, the 4G's BSs availability (also known as the evolved Node B (eNodeB)) availability, and the impact of aircraft maneuvers on signal reception. Finally, Experiments in urban settings revealed the capability of 5G signals for precise navigation. Both ground vehicle and UAV scenarios were tested, with the latter showing a remarkable position root mean-squared error (RMSE) of 3.35 meters. This indicates the growing feasibility of using 5G signals for accurate and reliable navigation in various urban applications.

Chapter 6: Exploiting On-Demand 5G Downlink Signals for Opportunistic Navigation

This chapter presents the first UE-based 5G navigation framework that exploits the "on-demand" 5G downlink signals. In this framework, the entire system bandwidth of incoming 5G signals is utilized in an opportunistic fashion. The proposed framework involves a cognitive approach to acquire the so-called URS for 5G, which includes the "on-demand" as well as "always-on" RSs. Experimental results are presented showing that the acquired URS: (i) spans the entire 5G downlink bandwidth, (ii) increases the CNR by 10 dB compared to state-of-the-art 5G UE-based opportunistic navigation receiver, and (iii) reduces significantly the carrier and code phase errors. A ranging error standard deviation of 2.75 m was achieved with the proposed framework with a stationary receiver placed 290 m away from a 5G gNB in a clear line-of-sight environment, which is lower than the 5.05 m achieved when using the "always-on" 5G downlink signals.

Chapter 7: A Passive EKF-Based Reconfigurable Intelligent Surface (RIS)-Aided Cellular Navigation System

This chapter presents a novel localization approach in a millimeter-wave uplink cellular environment, utilizing an RIS and focusing on mobile UE. The approach encompasses a sophisticated measurement engine that integrates a state-of-the-art carrier-aided code-phase-based 5G navigation receiver. This integration is enhanced by a passive, correlation-based angle-locked loop (ALL) for accurate TOA and AOA estimations. In addition, we have implemented an extended Kalman filter (EKF)-based navigation framework, leveraging the RIS to accurately estimate the 3-D position and velocity of mobile UEs. This framework takes into account the relative clock biases and drifts between the BS and UEs. It processes TOA and AOA measurements corresponding to both LOS and virtual LOS (VLOS) signals.

The performance of the proposed system was rigorously evaluated through Monte Carlo (MC) simulations across diverse scenarios, including pedestrian movement, ground vehicles, and UAVs. These simulations were conducted under various conditions: synchronous and asynchronous clock settings between the BS and UE, and environments with and without multipath effects. The results from these simulations highlight the proficiency of the proposed navigation system, demonstrating its capability to achieve sub-meter to meter-level positioning accuracy in a range of scenarios.

Chapter 8: Conclusions

This chapter summarizes the contributions of this dissertation.

The scholarly output of my Ph.D. journey culminated in contributions to 10 journal articles and 24 conference papers. This dissertation, however, selectively presents only the following publications in which I was the main contributor.

Journal Publications

[J1] **A. Abdallah**, J. Khalife, and Z. Kassas (2023) "Exploiting on-demand 5G downlink signals for opportunistic navigation," *IEEE Signal Processing Letters*, Vol. 30, pp. 389-393.
[J2] Z. Kassas and **A. Abdallah** (2023) "No GPS no problem: exploiting cellular OFDM-based signals for accurate navigation," *IEEE Transactions on Aerospace and Electronic Systems*, accepted.
[J3] Z. Kassas, **A. Abdallah**, S. Shahcheraghi, A. Kaiss, J. Khalife, C. Lee, J. Jurado, S. Wachtel, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, and R. Tay (2023) "I can hear you loud and clear: GNSS-less high altitude aircraft navigation with terrestrial cellular signals of opportunity," *IEEE Transactions on Aerospace and Electronic Systems*, accepted.
[J4] **A. Abdallah** and A. L. Swindlehurst (2023) "A Passive EKF-Based Reconfigurable In-

telligent Surface (RIS)-Aided Cellular Navigation System," *IEEE Transactions on Aerospace and Electronic Systems*, in progress.

Conference Publications

[C1] **A. Abdallah**, K. Shamaei, and Z. Kassas (2020) "Assessing real 5G signals for opportunistic navigation," *ION Global Navigation Satellite Systems Conference*, Sep. 21-25, 2020, St. Louis, MO, pp. 2548–2559.

[C2] **A. Abdallah**, J. Khalife, and Z. Kassas (2021) "Experimental characterization of received 5G signals carrier-to-noise ratio in indoor and urban environments," *IEEE Vehicular Technology Conference*, Apr. 25-28, 2021, Helsinki, Finland, pp. 1-5.

[C3] **A. Abdallah** and Z. Kassas (2021) "UAV navigation with 5G carrier phase measurements," *ION Global Navigation Satellite Systems Conference*, Sep. 20-24, 2021, St. Louis, MO, pp. 3294-3306.

[C4] **A. Abdallah** and Z. Kassas (2022) "Opportunistic navigation using sub-6 GHz 5G downlink signals: a case study on a ground vehicle," *European Conference on Antennas and Propagation*, Mar. 27 - Apr. 1, 2022, Madrid, Spain, pp. 1-5 (special session).

[C5] **A. Abdallah**, Z. Kassas, and C. Lee (2022) "Demo: I am not afraid of the GPS jammer: exploiting cellular signals for accurate ground vehicle navigation in a GPS-denied environment," *ACM Workshop on Automotive and Autonomous Vehicle Security*, Apr. 24, 2022, San Diego, CA, pp. 1-1.

[C6] Z. Kassas, **A. Abdallah**, C. Lee, J. Jurado, S. Wachtel, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, and R. Tay (2022) "Protecting the skies: GNSS-less aircraft navigation with terrestrial cellular signals of opportunity," *ION Global Navigation Satellite Systems Conference*, Sep. 19-23, 2022, Denver, CO, pp. 1014-1025.

[C7] **A. Abdallah** and A. L. Swindlehurst (2023) "5G and Beyond: An EKF-Based Reconfigurable Intelligent Surface (RIS)-Aided Navigation Approach," *ION Global Navigation*

Satellite Systems Conference, Sep. 11-15, 2023, Denver, CO, pp. 2348-2360.

[C8] **A. Abdallah** and A. L. Swindlehurst (2023) "A Passive EKF-Based RIS-Aided Cellular Navigation System," *IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing*, Dec. 10-13, 2023, Los Sueño, Costa Rica, accepted.

Chapter 2

Model Description

This chapter is organized as follows. Section 2.1 offers an in-depth look at the frame structures of 4/5G OFDM and identifies potential navigation RSs. Section 2.2 is dedicated to modeling the received 4/5G signal. In Section 2.3, we discuss two dynamic models relevant for 4/5G-based navigation: the white noise acceleration model and the continuous Wiener process acceleration model. Section 2.4 introduces a two-state model to capture the clock error dynamics in both UE and BS. Finally, Section 2.5 elaborates on the modeling of various navigation measurements derived from the received 4/5G signal.

2.1 OFDM Cellular Signals

Cellular signals, since 4G, deploy a multi-carrier modulation technique known as OFDM, where all subcarrier signals within a communication channel are orthogonal to one another. The orthogonality allows for efficient modulation and demodulation implementation using the fast Fourier transform (FFT) algorithm on the receiver's side, and inverse FFT (IFFT) on the transmitter's side. OFDM is more resistant to intersymbol interference, which is often

caused by multipath propagation, due to two primary reasons: (i) the use of low symbol rate modulation schemes, involving parallel low-rate streams instead of a single high-rate stream, and (ii) the insertion of guard intervals between OFDM symbols. In the guard interval, a partial copy of the OFDM symbol, known as the cyclic prefix (CP), is transmitted so that the receiver integrates over an integer number of sinusoid cycles for each multipath signal. Intersymbol interference can be avoided if the multipath time-spreading is shorter than the CP, which varies according to the configuration of the transmitted OFDM signal.

In the realm of OFDM cellular transmission, two primary duplexing methods, TDD (Time Division Duplexing) and FDD (Frequency Division Duplexing), distinguish how frequency resources are allocated for uplink and downlink communications. TDD utilizes the same frequency band for both uplink and downlink but allocates different time intervals for each, making it particularly suitable for scenarios with asymmetrical traffic. However, its range can be shorter due to the necessary guard period to prevent interference. In contrast, FDD allocates distinct frequency bands for uplink and downlink transmissions, allowing simultaneous communication without interference. While FDD generally requires a broader spectrum, it often boasts a wider operational range and consistent performance. In this study, we focus on sub-6 GHz 4/5G signals, also known as frequency range 1 (FR1). Most cellular providers prefer using FDD in this range due to its advantages in coverage and reduced latency. Therefore, FDD is primarily considered in the presentation of 4/5G frame structures. However, the proposed system is capable of utilizing TDD signals as well by simply taking into consideration the corresponding changes in the frame structure due to changing the duplexing mode.

The remainder of this section details the 4G and 5G cellular signal models. This includes (i) the 4/5G frame structures and (ii) potential 4/5G RSs that are suitable for navigation purposes.

2.1.1 4/5G Frame Structure

OFDM uses a multi-carrier transmission scheme: transmitted data symbols are mapped into multiple narrowband subcarriers in the frequency-domain, which reduces the frequency selective fading effect caused by multipath. The serial data symbols $\{S_1, \cdots, S_N\}$ are parallelized in group symbols, each of length N_R, where N_R is the number of subcarriers carrying the data. Then, a guard band in the frequency-domain is applied by zero-padding both sides of the signal and extending the N_R subcarriers into N_c subcarriers. At this step, an inverse fast Fourier transform (IFFT) is taken, and the last LCP elements are repeated at the beginning, which serves as a guard band in the time-domain to protect the OFDM signals from intersymbol interference (ISI). At the receiver, the transmitted symbols are demodulated by executing these steps in reverse order. The obtained OFDM signals are arranged in a 2-D frame. The structure of this frame depends on the transmission duplexing mode as discussed earlier.

When configuring an OFDM system, two main design parameters have to be chosen, i.e., the subcarrier spacing and the corresponding CP length. Compared with the 4G system that had one configuration, 5G introduced different configurations for various reasons:

- **Diverse Service Requirements**: 5G is designed to support a variety of use cases such as enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC), and Massive Machine Type Communications (mMTC). Each use case has distinct performance needs. For instance, URLLC demands low latency, while mMTC may prioritize coverage. Different numerologies allow the system to meet these varied requirements.

- **Varied Frequency Bands**: 5G is designed to operate across a wide range of frequency bands, from sub-1 GHz to mmWave frequencies. Different frequency bands

have different propagation characteristics, interference scenarios, and deployment use cases. Varied numerologies help in optimizing system performance across these bands.

- **Flexible Deployment Scenarios**: 5G supports diverse deployment scenarios, including macro cells, small cells, indoor cells, and more. Different numerologies can cater to the specific needs of each deployment type, such as managing interference in dense urban areas or enhancing coverage in rural areas.

- **Interference Management**: By using different subcarrier spacings, 5G can better manage interference. For instance, larger subcarrier spacings can be used for scenarios where faster time domain scheduling is required, thereby reducing latency.

- **Backward Compatibility and Coexistence**: Different numerologies facilitate the coexistence of 5G with legacy systems like 4G in the same frequency band. It aids in ensuring that the new system doesn't adversely affect the performance of the existing one.

In summary, the introduction of different numerologies in 5G is a strategic design decision to ensure the system's flexibility, scalability, and capability to address a vast spectrum of requirements, frequency bands, and deployment challenges.

In 5G networks, a range of subcarrier spacing (SCS) configurations are possible, in contrast to the fixed 15 kHz SCS of 4G systems. These configurations in 5G are identified by a numerology μ, which can take values from the set $\{0, \cdots, 4\}$. The corresponding SCS for a given numerology μ is calculated as $\Delta f = 2^{\mu} \cdot 15$ kHz. It is evident that the 4G SCS is a specific case within the 5G framework. Therefore, throughout this section, we will employ the 5G terminologies to describe the frame structure.

The temporal structure of the FDD 5G frame is uniform across different configurations,

defined by the equation

$$T_f = \frac{\Delta f_{\max} \cdot N_f}{100} \cdot T_c = 10\,\text{ms}, \tag{2.1}$$

where $\Delta f_{\max} = 480\,\text{kHz}$ represents the maximum subcarrier spacing, $N_f = 4096$ is the number of subcarriers, and $T_c = \frac{1}{\Delta f_{\max} \cdot N_f} = 0.509$ ns is the basic time unit in 5G. This frame is composed of ten 1 ms subframes. Further division yields two half-frames, each spanning 5 ms and comprising five subframes: half-frame 0 includes subframes 0-4, and half-frame 1 consists of subframes 5-9.

In the time domain, each subframe is partitioned into several slots. The number of slots in a subframe, and the number of OFDM symbols within each slot, depend on the chosen numerology μ. The relationship for the number of OFDM symbols in a subframe is expressed as

$$N_{\text{symb}}^{\text{subframe},\mu} = N_{\text{symb}}^{\text{slot},\mu} \times N_{\text{slot}}^{\text{subframe},\mu}, \tag{2.2}$$

where $N_{\text{symb}}^{\text{slot},\mu}$ denotes the number of OFDM symbols per slot, which is either 14 for a normal CP or 12 for an extended CP, and $N_{\text{slot}}^{\text{subframe},\mu}$ is the number of slots in each subframe for a given μ. To this end, the number of slots is denoted by $n_s^\mu \in \{0, 1, \cdots, N_{\text{slot}}^{\text{subframe},\mu}\}$ or $n_s'^\mu \in \{0, 1, \cdots, N_{\text{slot}}^{\text{frame},\mu}\}$ in an increasing order within a subframe or a frame respectively. Figure 2.1 shows the different numerologies of 5G and the corresponding: single OFDM carrier; the timing of two consecutive OFDM symbols guarded by CP; and the SCS, CP type, number of OFDM symbols per slot, number of slots per frame, OFDM symbol duration, and CP duration for different numerologies.

Depending on the numerology, a resource grid with $N_{\text{grid}}^{\text{size},\mu} N_{\text{sc}}^{\text{RB}}$ subcarriers and $N_{\text{symb}}^{\text{subframe},\mu}$ OFDM symbols are defined, starting at a common RB $N_{\text{grid}}^{\text{start},\mu}$, which is indicated by higher-layer signaling [82]. The carrier bandwidth $N_{\text{grid}}^{\text{size},\mu}$ and the starting position $N_{\text{grid}}^{\text{start},\mu}$ for

μ	Δf [kHz]	CP	$N_{\text{symb}}^{\text{slot}}$	$N_{\text{slot}}^{\text{frame},\mu}$	Symbol duration [μs]	CP duration [μs]
0	15	N	14	10	66.67	4.69
1	30	N	14	20	33.33	2.34
2	60	N/E	14/12	40	16.67	1.17
3	120	N	14	80	8.33	0.57
4	240	N	14	160	4.17	0.29

N: normal; E: extended; CP: cyclic prefix

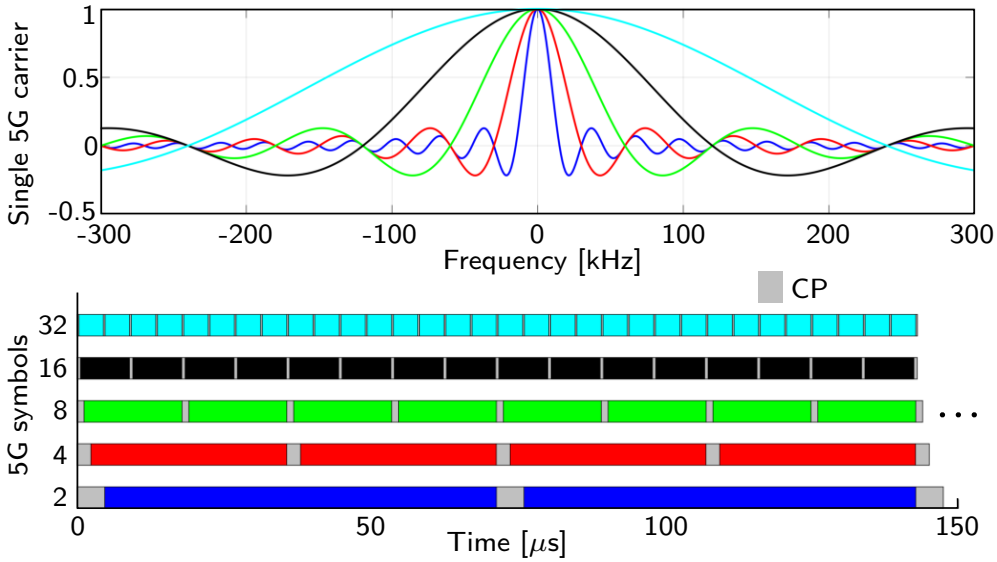


Figure 2.1: Different numerologies of 5G and the corresponding: single OFDM carrier; the timing of two consecutive OFDM symbols guarded by CP; and the SCS, CP type, number of OFDM symbols per slot, number of slots per frame, OFDM symbol duration, and CP duration for different numerologies.

a specific numerology μ are given by the higher-layering signaling *carrierBandwidth* and *offsetToCarrier* in the *SCS-SpecificCarrier* IE, respectively.

A RB is defined as $N_{\text{sc}}^{\text{RB}} = 12$ subcarriers in the frequency domain and has the time length of a resource grid $N_{\text{symb}}^{\text{subframe},\mu}$. A RB consists of resource elements (REs). The minimum and maximum number of RBss in 5G along with the corresponding bandwidth for different numerologies is summarized in Table 2.1. However, for 4G, the number of subcarriers in a 4G frame, N_c, and the number of used subcarriers, N_r, are not unique and are assigned by the network provided according to the system bandwidth as tabulated in Table

Each element in the 5G frame is uniquely identified for a specific antenna port p and subcarrier configuration μ by $(k, l)_{p,\mu}$, where k is the index in frequency domain l is the symbol position in the time domain relative to some reference point. In 5G protocol, "Point A" serves as a common reference point and can be obtained as reported in [82]. Figure 2.2 summarizes the 4/5G frame structure.

Table 2.1: The minimum and maximum number of RBs and the corresponding bandwidths for different numerologies.

μ	$N_{\text{RB}}^{\text{min}}$	$N_{\text{RB}}^{\text{max}}$	**Minimum bandwidth [Mhz]**	**Maximum bandwidth [Mhz]**
0	24	275	4.32	49.5
1	24	275	8.64	99
2	24	275	17.28	198
3	24	275	34.56	396
4	24	138	69.12	397.44

2.1.2 4/5G Potential Reference Signal

In 4G and 5G systems, there are specific RSs known as pilot signals. These are dataless, predetermined sequences that are interspersed within the transmission at regular intervals.

Table 2.2: 4G system bandwidths and number of subcarriers.

Bandwidth [MHz]	**Total number of subcarrier (N_c)**	**Number of used subcarriers (N_r)**
1.4	128	72
3	256	180
5	512	300
10	1024	600
15	1536	900
20	2048	1200

They can be used by the receiver to perform various communication-essential tasks, such as:

- **Channel Estimation**: To determine the effect of the channel on the transmitted signal, which is necessary for correct demodulation and decoding.
- **Frequency and Time Synchronization**: To synchronize the receiver's frequency and time to that of the transmitter.
- **Signal Strength Measurement**: To measure the received signal strength indicator (RSSI), RS received power (RSRP), and RS received quality (RSRQ).
- **Beamforming Feedback**: Especially in 5G, where directional transmission is a key feature, pilot signals help in determining the best beamforming vectors.

These signals, owing to their predefined structure and scheduling, can be leveraged for an opportunistic user-based navigation approach. The following section will outline the potential 4G and 5G RSs that are suitable for such applications. It is also worth noting that there are specific RSs in these systems dedicated to positioning, which will be discussed as well.

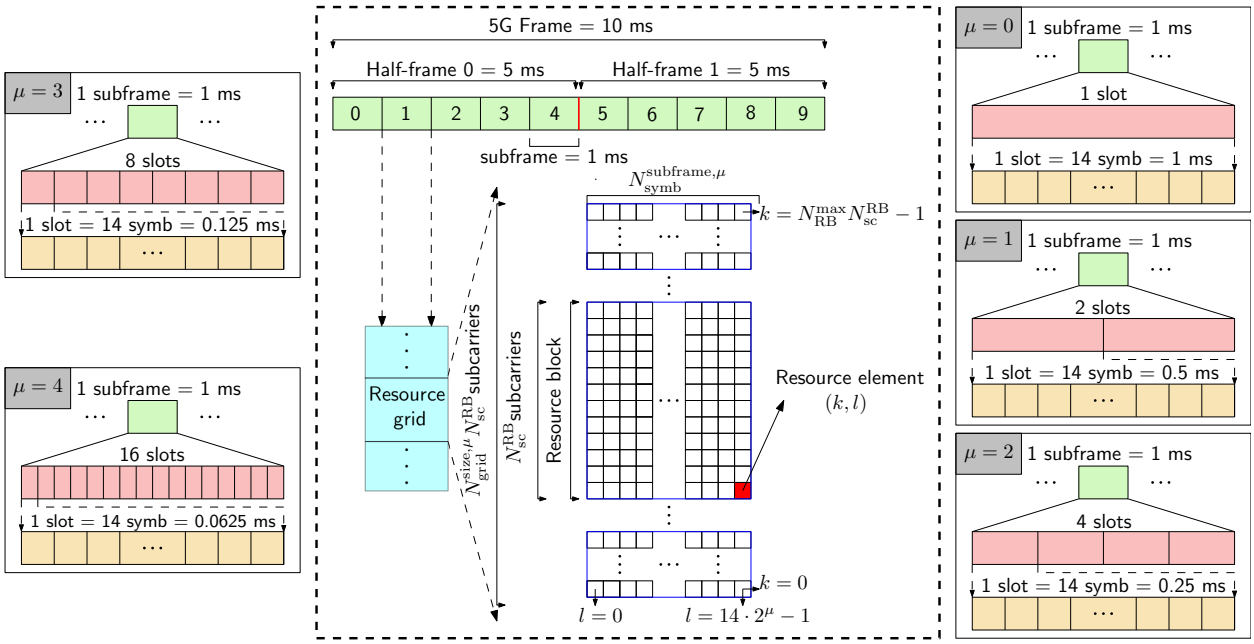


Figure 2.2: 4/5G frame structure.

2.1.2.1 4G Potential Reference Signal

The 4G system has multiple candidates for downlink RSs that can be exploited for an opportunistic navigation approach such

1. Initial cell search and SSs
   (a) Primary Synchronization Signal (PSS)
   (b) Secondary Synchronization Signal (SSS)
2. Channel estimation RSs
   (a) Cell-Specific Reference Signals (CRS)
3. Dedicated positioning RSs
   (a) Positioning Reference Signals (PRS)

Figure 2.3 shows the RE allocation of the various 4G potential RSs that can be leveraged for positioning.

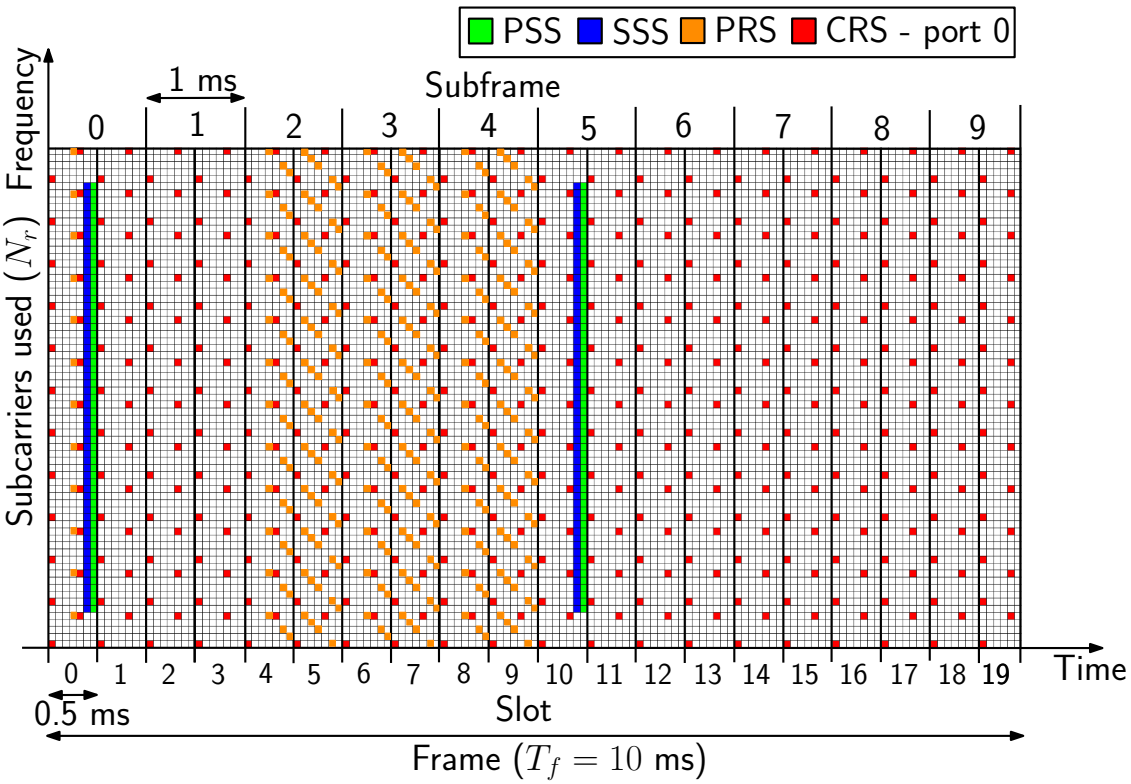


Figure 2.3: Resource element (RE) allocation of potential 4G RSs.

2.1.2.1.1 PSS and SSS

The PSS and SSS are vital components for the initial cell search procedure in 4G networks. They enable the UE to deduce the frame start time and the specific cell identity (ID) of the eNodeB. The PSS utilizes a Zadoff-Chu sequence of length 62, centrally positioned across the 63 middle subcarriers—except for the direct current (DC) carrier—occupying approximately 0.93 MHz of the total system bandwidth. This signal is transmitted on the final symbol of the 0th slot and again in the 10th slot. Each PSS can assume one of three distinct sequences, which are distinguished by an integer $N_{\text{ID}}^{(2)} \in \{0, 1, 2\}$. This integer is an identifier for the eNodeB's sector.

Conversely, the SSS, a length-62 orthogonal sequence, is broadcast immediately prior to the PSS in either the 0th or 10th slot and shares the same subcarriers. The formation of the SSS involves the amalgamation of two maximal-length sequences, which are further scrambled by

a unique orthogonal sequence that corresponds to the sector ID, $N_{\text{ID}}^{(2)}$. A total of 168 distinct SSS permutations are possible, corresponding to a group identifier, $N_{\text{ID}}^{(1)}$, with a range of $\{0, \ldots, 167\}$. Together, these values formulate the physical cell ID of the eNodeB, defined as

$$N_{\text{ID}}^{\text{Cell}} = 3N_{\text{ID}}^{(1)} + N_{\text{ID}}^{(2)}. \tag{2.3}$$

Reference to the standard can be made for further details on the synchronization signals structure [83].

2.1.2.1.2 Cell-specific Reference Signals

The CRSs serve as orthogonal sequences distributed across time and frequency, primarily aiding in channel estimation. The allocation pattern of CRS REs is inherently linked to several parameters, including the cell ID, symbol number, slot number, and transmission antenna port, as detailed in [84]. The REs for the u-th eNodeB on the k-th subcarrier within the l-th symbol are allocated according to

$$Y_l^{(u)}(k) = \begin{cases} S_l^{(u)}(k), & \text{if } k = m\Delta_{CRS} + \nu_{l,N_{\text{ID}}^{\text{Cell}}}, \\ D_l^{(u)}(k), & \text{otherwise,} \end{cases} \tag{2.4}$$

where $S_l^{(u)}(k)$ denotes the CRS sequence, and $D_l^{(u)}(k)$ signifies all other data signals. Here, m ranges from 0 to $M-1$, with $M = \lfloor N_r/\Delta_{CRS} \rfloor$ signifying the number of REs available for CRS, given a subcarrier spacing $\Delta_{CRS} = 6$. The term $\nu_{l,N_{\text{ID}}^{\text{Cell}}}$ denotes a cell-specific shift determined by the cell ID and the symbol index l. This representation caters to a single antenna port scenario, $p = 0$, consistent with existing 4G literature. The complex mapping of REs for various antenna ports, pertinent to more advanced configurations, will be expounded in the subsequent chapter.

2.1.2.1.3 Positioning Reference Signal

The PRS is intended for location-based services in 4G networks and was initially proposed for enhancing positioning capabilities. Despite their intended purpose, an examination of the current 4G infrastructure—specifically within the United States—revealed that these signals are not actively transmitted by cellular operators. Consequently, the PRS has not been incorporated into the design of the navigation method proposed herein. It is noteworthy to acknowledge that due to the substantial similarity between the PRS and CRS, the omission of PRS is unlikely to detract from the system's overall positioning performance. The probable redundancy of PRS, along with a preference for optimizing bandwidth for data traffic, may account for its non-utilization in the operational networks.

2.1.2.2 5G Potential Reference Signal

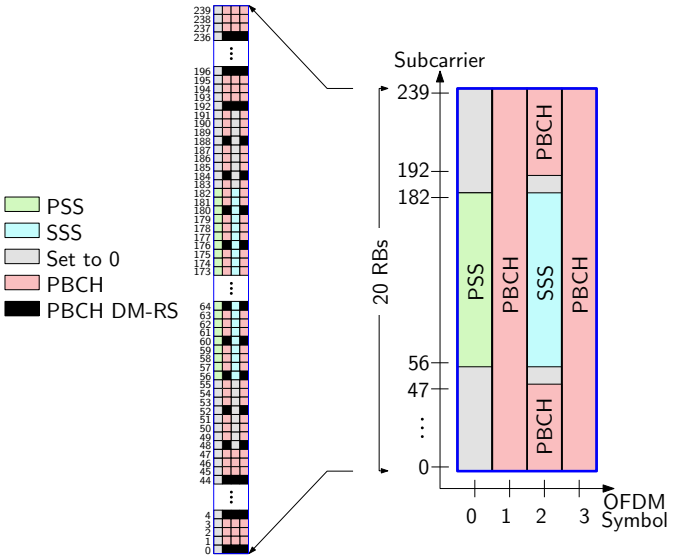
The 5G system has multiple candidates for downlink RSs that can be exploited for an opportunistic navigation approach such

1. Initial cell search and synchronization signals
    (a) Primary Synchronization Signal (PSS)
    (b) Secondary Synchronization Signal (SSS)
    (c) Physical Broadcast Channel (PBCH) and its demodulation reference signal (PBCH-DMRS)
2. Channel estimation RSs
    (a) Channel State Information Reference Signal (CSI-RS)

2.1.2.2.1 SS/PBCH

In 5G cellular networks, the gNodeB (gNB) transmits SS to facilitate the determination of the frame start time. These SS encompass both the PSS and the SSS, which are pivotal for acquiring symbol and frame timing, respectively. The identification of the frame start time enables the CPs to be stripped away and allows for the execution of an FFT, which is instrumental in constructing OFDM symbols that make up the frame.

The SS, along with the PBCH and the corresponding DM-RS, are encapsulated within a four-symbol block known as the SS/PBCH block. This block comprises 240 contiguous subcarriers, equivalent to 20 resource blocks (RBs), and spans across four consecutive OFDM symbols. Within the SS/PBCH block, subcarriers are sequentially numbered from 0 to 239. The structural composition of the SS/PBCH block, including the mapping of OFDM symbols and subcarriers to the various signals, is depicted in Figure 2.4.



Signal	Symbol number	Subcarrier number
PSS	0	$56, 57, \cdots, 182$
SSS	0	$56, 57, \cdots, 182$
Set to zero	0	$0, 1, \cdots, 55$ $183, 184, \cdots, 239$
	2	$48, 49, \cdots, 55$ $183, 184, \cdots, 239$
PBCH	1, 3	$0, 1, \cdots, 239$
	2	$0, 1, \cdots, 47$ $192, 193, \cdots, 239$
DM-RS	1, 3	$0 + v, 4 + v, 236 + v$
	2	$0 + v, 4 + v, 44 + v$ $192 + v, 196 + v, 236 + v$

$v = N_{ID}^{Cell} \bmod 4$

Figure 2.4: The structure of the SS/PBCH block and the associated mapping of OFDM symbols and subcarriers to different signals within the block.

It is important to note that the positioning of the PBCH DM-RS is variable and dependent on the parameter v, which itself varies with the physical cell ID $N_{\mathrm{ID}}^{\mathrm{Cell}}$. The SS/PBCH

Table 2.3: Symbol numbers containing SS/PBCH block for different numerologies and frequency bands.

subcarrier spacing (kHz)	**Carrier frequency**	**Symbol number**	**Slot number n**
Case A: 15	$f_c \leq 3$ GHz $3 < f_c \leq 6$ GHz	$\{2, 8\} + 14n$	$\{0, 1\}$ $\{0, \cdots, 3\}$
Case B: 30	$f_c \leq 3$ GHz $3 < f_c \leq 6$ GHz	$\{4, 8, 16, 20\} + 28n$	$\{0\}$ $\{0, 1\}$
Case C: 30	$f_c \leq 3$ GHz $3 < f_c \leq 6$ GHz	$\{2, 8\} + 14n$	$\{0, 1\}$ $\{0, \cdots, 3\}$
Case D: 120	$f_c > 6$ GHz	$\{4, 8, 16, 20\} + 28n$	$\{0, \cdots, 3,$ $5, \cdots, 8,$ $10, \cdots, 13,$ $15, \cdots, 18\}$
Case E: 240	$f_c > 6$ GHz	$\{8, 12, 16, 20, 32,$ $36, 40, 44\} + 56n$	$\{0, \cdots, 8\}$

block is periodically transmitted every two frames and is disseminated multiple times as an SS/PBCH burst, which is constrained to a half-frame window (5 ms) for transmission. Each instance of the block within the burst is subject to beamforming in differing directions.

The placement of the SS/PBCH block within the 5G frame is contingent upon the overarching 5G signaling. Furthermore, both the temporal allocation of the SS/PBCH block and the dimension of the SS/PBCH burst within the frame are dictated by the transmission frequency f_c and the numerology μ, as outlined in Table 2.3, with the index 0 denoting the initial OFDM symbol of the first slot in a half-frame.

The PSS and SSS are two orthogonal maximum-length sequences (m-sequences), each with a length of 127 symbols. These sequences are transmitted over adjacent subcarriers, with their occupied bandwidth being a function of the subcarrier spacing. The subcarrier spacing is determined by the numerology, denoted by μ, which leads to a varying bandwidth for the PSS and SSS. Specifically, the bandwidth can be as narrow as 1.905 MHz when $\mu = 0$, and

can increase to as much as 30.48 MHz for $\mu = 4$. Similar to 4G, there are three potential variations of the PSS, denoted by $N_{\mathrm{ID}}^{(2)} \in \{0, 1, 2\}$, each correlating to an integer representing the sector ID of the gNB. In contrast, there exist 336 permutations for the SSS, indicated by $N_{\mathrm{ID}}^{(1)} \in \{0, \ldots, 335\}$, which correspond to a group identifier of the gNB. The physical cell identity of the gNB is thus determined by the following expression:

$$N_{\mathrm{ID}}^{\mathrm{Cell}} = 3N_{\mathrm{ID}}^{(1)} + N_{\mathrm{ID}}^{(2)}. \tag{2.5}$$

The PBCH serves as the conduit for transmitting system information that is essential for establishing a connection between the gNB and the UE. The demodulation of the PBCH parameters is elaborately discussed in [82]. Moreover, the DM-RS associated with the PBCH facilitates decoding and aids in the estimation of the channel's frequency response, with the generation of the PBCH DM-RS sequence detailed in Section 7.4.1.4 of [85]. The bandwidth of the PBCH message and its corresponding scattered DM-RS can be as narrow as 3.6 MHz when $\mu = 0$, and can increase to as much as 57.6 MHz for $\mu = 4$.

2.2 Received Signal Model

The received cellular 4/5G baseband signal model can be expressed as

$$\begin{aligned} r[n] = \sum_{u=1}^{N} & \left(\alpha_u c_u[\tau_n - t_{s_u}[n]] \exp\left(j\theta_u[\tau_n]\right)\right. \\ & \left. + d_u[\tau_n - t_{s_u}[n]] \exp\left(j\theta_u[\tau_n]\right)\right) + w[n], \end{aligned} \tag{2.6}$$

where $r[n]$ is the received signal at the nth time instant; α_u is the complex channel gain between the UE and the u-th BS (eNodeB/gNB); τ_n is the sample time expressed in the

receiver time; N is the number of BSs; $c_u[n]$ is the periodic RS with a period of L samples; $t_{s_u}[n]$ is the code-delay corresponding to the UE and the u-th BS at the nth time instant; $\theta_u[\tau_n] = 2\pi f_{D_u}[n]T_s n$ is the carrier phase in radians, with $f_{D_u}[n]$ being the Doppler frequency at the nth time instant and T_s is the sampling time; $d_u[\tau_n]$ represents the samples of some data transmitted from the u-th BS; and $w[n]$ is a zero-mean independent and identically distributed noise with $\mathbb{E}\{w[m]w^*[n]\} = \sigma_w^2\delta[m-n]$, where $\delta[n]$ is the Kronecker delta function, and X^* denotes the complex conjugate of random variable X.

2.3 UE Dynamics Model

The primary objective of this study is to evaluate the baseline navigational performance achievable using only cellular signals for UE-based navigation. To capture the range of motion characteristics pertinent to various navigation scenarios—including pedestrian, ground vehicle, UAV, and high-altitude aircraft applications—two distinct dynamic models are utilized: the white noise acceleration model and the continuous Wiener process acceleration model. Subsequent sections are dedicated to the detailed mathematical exposition of these two models.

2.3.1 White Noise Acceleration Model

Despite its simplicity, the white noise acceleration model is effectively used for UEs exhibiting low dynamics. It captures the essential dynamics that occur between updates of the navigation filter. This model is described by the following continuous-time (CT) state equation:

$$\dot{\boldsymbol{x}}_{\text{pv}}(t) = \mathbf{A}_{\text{pv}}\boldsymbol{x}_{\text{pv}}(t) + \mathbf{D}_{\text{pv}}\tilde{\boldsymbol{w}}_{\text{pv}}(t), \tag{2.7}$$

where the matrices $\mathbf{A}_{\text{pv}}$ and $\mathbf{D}_{\text{pv}}$ are defined as:

$$\mathbf{A}_{\text{pv}} = \begin{bmatrix} \mathbf{0}_{3\times3} & \mathbf{I}_{3\times3} \\ \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} \end{bmatrix}, \quad \mathbf{D}_{\text{pv}} = \begin{bmatrix} \mathbf{0}_{3\times3} \\ \mathbf{I}_{3\times3} \end{bmatrix}, \tag{2.8}$$

In the above equations, $\boldsymbol{x}_{\text{pv}} \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}\right]^{\mathsf{T}}$, with $\boldsymbol{r}_r \triangleq [x_r, y_r, z_r]^{\mathsf{T}}$, represents the state vector consisting of position and velocity. The process noise vector $\tilde{\boldsymbol{w}}_{\text{pv}} = [\tilde{w}_x, \tilde{w}_y, \tilde{w}_z]^{\mathsf{T}}$ comprises elements modeled as zero-mean, mutually independent white noise processes with respective power spectral densities $\tilde{q}_x$, $\tilde{q}_y$, and $\tilde{q}_z$.

When discretized with a uniform sampling interval T, the UE's dynamics expressed in (2.7) are transformed into a discrete-time (DT) model:

$$\boldsymbol{x}_{\text{pv}}(k+1) = \mathbf{F}_{\text{pv}}\boldsymbol{x}_{\text{pv}}(k) + \boldsymbol{w}_{\text{pv}}(k), \quad k \in \mathbb{N}, \tag{2.9}$$

$$\mathbf{F}_{\text{pv}} = \begin{bmatrix} \mathbf{I}_{3\times3} & T\mathbf{I}_{3\times3} \\ \mathbf{0}_{3\times3} & \mathbf{I}_{3\times3} \end{bmatrix}, \tag{2.10}$$

with $\boldsymbol{w}_{\text{pv}}$, the DT process noise, assumed to be a zero-mean white noise sequence with covariance matrix $\mathbf{Q}_{\text{pv}}$, which is specified as:

$$\mathbf{Q}_{\text{pv}} = \begin{bmatrix} \tilde{q}_x\frac{T^3}{3} & 0 & 0 & \tilde{q}_x\frac{T^2}{2} & 0 & 0 \\ 0 & \tilde{q}_y\frac{T^3}{3} & 0 & 0 & \tilde{q}_y\frac{T^2}{2} & 0 \\ 0 & 0 & \tilde{q}_z\frac{T^3}{3} & 0 & 0 & \tilde{q}_z\frac{T^2}{2} \\ \tilde{q}_x\frac{T^2}{2} & 0 & 0 & \tilde{q}_xT & 0 & 0 \\ 0 & \tilde{q}_y\frac{T^2}{2} & 0 & 0 & \tilde{q}_yT & 0 \\ 0 & 0 & \tilde{q}_z\frac{T^2}{2} & 0 & 0 & \tilde{q}_zT \end{bmatrix}. \tag{2.11}$$

2.3.2 Continuous Wiener Process Acceleration Model

In scenarios involving higher dynamic movements, such as high-altitude aircraft navigation, the continuous Wiener process acceleration model is often more appropriate. Upon discretization of this model over a uniform time interval T, the resulting equations are expressed as follows:

$$\boldsymbol{x}_{\text{pva}}(k+1) = \mathbf{F}_{\text{pva}}\boldsymbol{x}_{\text{pva}}(k) + \boldsymbol{w}_{\text{pva}}(k), \quad \text{for} \quad k \in \{0, 1, 2, \ldots\}, \tag{2.12}$$

$$\mathbf{F}_{\text{pva}} = \begin{bmatrix} \mathbf{I}_{3\times3} & T\mathbf{I}_{3\times3} & \frac{T^2}{2}\mathbf{I}_{3\times3} \\ \mathbf{0}_{3\times3} & \mathbf{I}_{3\times3} & T\mathbf{I}_{3\times3} \\ \mathbf{0}_{3\times3} & \mathbf{0}_{3\times3} & \mathbf{I}_{3\times3} \end{bmatrix}, \tag{2.13}$$

where $\boldsymbol{x}_{\text{pva}} \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, \ddot{\boldsymbol{r}}_r^{\mathsf{T}}\right]^{\mathsf{T}}$ encapsulates the 3-D position, velocity, and acceleration states. The noise sequence $\boldsymbol{w}_{\text{pva}}$ is characterized as a zero-mean white noise with a covariance matrix $\mathbf{Q}_{\text{pva}}$:

$$\mathbf{Q}_{\text{pva}} = \begin{bmatrix} \frac{T^5}{20} & \frac{T^4}{8} & \frac{T^3}{6} \\ \frac{T^4}{8} & \frac{T^3}{3} & \frac{T^2}{2} \\ \frac{T^3}{6} & \frac{T^2}{2} & T \end{bmatrix} \otimes \tilde{\boldsymbol{S}}_{xyz}, \tag{2.14}$$

The Kronecker product, denoted by $\otimes$, combines the matrix with $\tilde{\boldsymbol{S}}_{xyz} = \text{diag}\left[\tilde{q}_x', \tilde{q}_y', \tilde{q}_z'\right]$, which defines the power spectra of jerk noise in the x, y, and z axes as $\tilde{q}_x'$, $\tilde{q}_y'$, and $\tilde{q}_z'$, respectively.

While this work focuses on two models for UE dynamics to study the navigation performance of cellular signals exclusively, other more complex models exist that can better represent specific types of motion. These include but are not limited to the Singer acceleration model, mean-adaptive acceleration, circular and curvilinear motion, and the coordinated turn, as

detailed by Li and Jilkov in their survey [86]. Additionally, when an inertial navigation system (INS) is accessible, it can provide motion information, which is further refined by integrating cellular signal data.

2.4 Clock Error Dynamics Model

Synchronization among transmitters is critical in radio navigation systems such as the GNSS. GNSS satellites, equipped with atomic clocks, transmit their timing errors within the navigation message, along with their positions. This protocol ensures that, for GNSS-based navigation, only the UE's clock bias needs to be estimated.

In contrast, cellular BSs utilize oscillators that, despite being synchronized with GNSS, exhibit less stability. As a result, the clock error states for cellular BSs, including both bias and drift, typically remain undetermined and require simultaneous estimation. To address this, it is necessary to explicitly define the dynamics of the clock error states. The two-state model is widely accepted for this purpose. It accounts for the clock bias, represented by δt, and the clock drift, denoted by $\dot{\delta} t$, as shown in Figure 2.5.

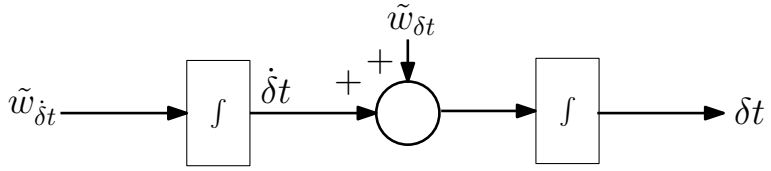


Figure 2.5: Clock error states dynamics model.

The evolution of the clock error states is governed by

$$\dot{\boldsymbol{x}}_{\mathrm{clk},\kappa}(t) = \mathbf{A}_{\mathrm{clk}} \boldsymbol{x}_{\mathrm{clk}_\kappa}(t) + \tilde{\boldsymbol{w}}_{\mathrm{clk}_\kappa}(t), \tag{2.15}$$

$$\boldsymbol{x}_{\mathrm{clk}_\kappa} = \begin{bmatrix} \delta t_\kappa \\ \dot{\delta} t_\kappa \end{bmatrix}, \quad \tilde{\boldsymbol{w}}_{\mathrm{clk}_\kappa} = \begin{bmatrix} \tilde{w}_\delta t_\kappa \\ \tilde{w}_{\dot{\delta} t_\kappa} \end{bmatrix}, \quad \mathbf{A}_{\mathrm{clk}} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \tag{2.16}$$

where $\kappa \in \left\{ \{\mathrm{UE}\}_{i=1}^{i=I}, \{\mathrm{BS}\}_{u=1}^{u=U} \right\}$. The variables $\tilde{\boldsymbol{w}}_{\mathrm{clk}_\kappa}$ are modeled as zero-mean, mutually independent white noise processes. The power spectral density (PSD) of these processes is expressed by $\tilde{\mathbf{Q}}_{\mathrm{clk}_\kappa} = \mathrm{diag}\left[S_{\tilde{w}_{\delta t_\kappa}}, S_{\tilde{w}_{\dot{\delta} t_\kappa}} \right]$.

Upon discretizing the continuous-time dynamics given in Equations (2.15) and (2.16) at a sampling interval T, we obtain the discrete-time equivalent model

$$\boldsymbol{x}_{\mathrm{clk}_\kappa}(k+1) = \mathbf{F}_{\mathrm{clk}} \boldsymbol{x}_{\mathrm{clk}_\kappa}(k) + \boldsymbol{w}_{\mathrm{clk}_\kappa}(k), \tag{2.17}$$

where $\boldsymbol{w}_{\mathrm{clk}_\kappa}$ represents a discrete-time white noise sequence with zero mean and covariance matrix $\mathbf{Q}_{\mathrm{clk}_\kappa}$ with

$$\mathbf{F}_{\mathrm{clk}} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \quad \mathbf{Q}_{\mathrm{clk}_\kappa} = \begin{bmatrix} S_{\tilde{w}_{\delta t_\kappa}} T + S_{\tilde{w}_{\dot{\delta} t_\kappa}} \frac{T^3}{3} & S_{\tilde{w}_{\dot{\delta} t_\kappa}} \frac{T^2}{2} \\ S_{\tilde{w}_{\dot{\delta} t_\kappa}} \frac{T^2}{2} & S_{\tilde{w}_{\dot{\delta} t_\kappa}} T \end{bmatrix}. \tag{2.18}$$

Cellular BSs typically utilize oven-controlled crystal oscillators (OCXOs), whereas many UEs are equipped with temperature-compensated crystal oscillators (TCXOs), which are less stable. The clock error dynamics are commonly approximated by considering only the frequency random walk coefficient h_{-2} and the white frequency coefficient h_0. This leads to the approximations $S_{\tilde{w}_{\delta t}} \approx \frac{h_0}{2}$ and $S_{\tilde{w}_{\dot{\delta} t}} \approx 2\pi^2 h_{-2}$ [87]. Typical values for h_0 and h_{-2} in TCXOs and OCXOs are presented in Table 2.4.

Table 2.4: Typical values of h_0 and h_{-2} for TCXOs and OCXOs.

Oscillator	h_0	h_{-2}
Typical TCXO	2.0×10^{-19}	2.0×10^{-20}
Best TCXO	9.4×10^{-20}	3.8×10^{-21}
Typical OCXO	2.6×10^{-22}	4.0×10^{-26}
Best OCXO	8.0×10^{-20}	4.0×10^{-23}

2.5 Cellular Measurements Models

Various measurements can be obtained from the received 4/5G OFDM signals. This section discusses four different types of measurements that are pertinent to location estimation. These measurements are categorized based on their underlying principles: TOA and AOA. The TOA-based measurements encompass: the LOS measurement derived from the direct path between the BS and UE, and a reflected measurement from a particular surface in the environment. The latter, which involves an RIS, is pivotal to a cellular navigation approach elaborated in a subsequent chapter. This measurement is associated with a VLOS, as recognized in existing literature.

The pseudorange measurements for LOS and VLOS between the i-th UE and the u-th BS, denoted by $\rho_i^{(u)}$ and $\rho_i^{'(u)}$, respectively, are modeled in meters as follows

$$\rho_i^{(u)}(k) = \|\boldsymbol{r}_{r,i}(k) - \boldsymbol{r}_{\text{ris}}\|_2 + c \cdot [\delta t_{r,i}(k) - \delta t_{s,u}(k)] + \nu_{\rho,i,u}(k), \tag{2.19}$$

$$\rho_i^{'(u)}(k) = \|\boldsymbol{r}_{r,i}(k) - \boldsymbol{r}_{s,u}\|_2 + \|\boldsymbol{r}_{s,u} - \boldsymbol{r}_{\text{ris}}\|_2 + c \cdot [\delta t_{r,i}(k) - \delta t_{s,u}(k)] + \nu_{\rho,i,u}^{'}(k), \tag{2.20}$$

where $\boldsymbol{r}_{r,i} = [x_{r,i}, y_{r,i}, z_{r,i}]^T$ represents the 3-D position of the i-th UE, $\boldsymbol{r}_{s,u} = [x_{s,u}, y_{s,u}, z_{s,u}]^T$ denotes the 3-D position of the u-th BS, and $\boldsymbol{r}_{\text{ris}} = [x_{\text{ris}}, y_{\text{ris}}, z_{\text{ris}}]^T$ is the RIS's 3-D position. Here, c signifies the speed of light, $\delta t_{r,i}$ and $\delta t_{s,u}$ are the clock biases of the UE and BS, respectively, and $\nu_{\rho,i,u}$ and $\nu_{\rho,i,u}^{'}$ represent the measurement noise, modeled as zero-mean

white Gaussian noise with respective variances $\sigma^2_{\rho,i,u}$ and $\sigma'^2_{\rho,i,u}$.

In a network-based localization framework that will discussed in a later chapter, the positions of the BSs $\{\boldsymbol{r}_{s,u}\}_{u=1}^{U}$ and the RIS are assumed to be known parameters. This assumption is practical, as the fixed infrastructure locations are typically predetermined and available for use in location computation. This prior knowledge facilitates the simplification of the RIS-reflected pseudorange measurement $\rho_i^{'(u)}(k)$. The measurement reflects the sum of the known distance from the u-th BS to the RIS and the unknown distance from the RIS to the i-th UE. Thus, one can deduce the latter by subtracting the former from the overall pseudorange measurement, leaving the distance between the i-th UE and the RIS as the remaining unknown component to be determined and expressed as

$$\rho_i^{''(u)}(k) = \rho_i^{'(u)}(k) - \left\|\boldsymbol{r}_{s,u} - \boldsymbol{r}_{\text{ris}}\right\|_2 . \tag{2.21}$$

For ease of notation, we will henceforth refer to the updated measurement simply as $\rho_i^{'(u)}(k)$, omitting the double prime.

The azimuth measurement of the LOS path and both the azimuth and elevation measurements of the VLOS path can be defined mathematically as

$$\psi_i(k) = \arctan\left(\frac{y_{r,i}(k) - y_{s,u}}{x_{r,i}(k) - x_{s,u}}\right) + \nu_{\psi,i,u}(k), \tag{2.22}$$

$$\phi_i(k) = \arctan\left(\frac{y_{r,i}(k) - y_{\text{ris}}}{x_{r,i}(k) - x_{\text{ris}}}\right) + \nu_{\phi,i,u}(k), \tag{2.23}$$

$$\theta_i(k) = \arctan\left(\frac{z_{r,i}(k) - z_{\text{ris}}}{\sqrt{(x_{r,i}(k) - x_{\text{ris}})^2 + (y_{r,i}(k) - y_{\text{ris}})^2}}\right) + \nu_{\theta,i,u}(k), \tag{2.24}$$

$$\text{for} \quad i = 1, 2, ..., I,$$

where $\nu_{\psi,i,u}$, $\nu_{\phi,i,u}$, $\nu_{\theta,i,u}$ are the measurement noises, which are modeled as zero-mean white Gaussian random sequences with variances $\sigma^2_{\psi,i,u}$, $\sigma^2_{\phi,i,u}$, and $\sigma^2_{\theta,i,u}$, respectively.

Chapter 3

Accurate, Robust, and Efficient 4/5G Opportunistic Cellular Navigation Receiver

This chapter is organized as follows. Section 3.1 evaluates the architecture of traditional frequency-domain-based receivers for 4G and 5G cellular navigation, focusing on their inherent limitations. Section 3.2 introduces the URS for 4G and the USS for 5G, both engineered to leverage a broader bandwidth for improved signal power. Section 3.3 presents a novel time-domain-based navigation receiver designed for optimizing the use of 4G-URS and 5G-USS. This section further elaborates on the generation of 4G-URS and 5G-USS, signal acquisition, and tracking loops.

3.1 Conventional Frequency-Domain-Based 4/5G Cellular Navigation Receivers

The design of the 4G (LTE) or 5G communication receivers excels at its intended communication tasks. This successful foundation has naturally prompted the conceptualization of cellular 4/5G navigation receivers as supplementary enhancements, built incrementally upon the pre-existing communication receiver infrastructure. Such designs have demonstrated the capability of achieving meter-level and submeter-level positioning accuracies for pedestrians, ground vehicles, and UAVs [1, 52–54, 59, 61, 68, 73, 88–98].

This section delves into the architecture of contemporary frequency-domain-based receivers employed in 4/5G cellular navigation systems. The design principles underlying these receivers are outlined and provided with a critical examination of their inherent limitations. The discussion aims to lay the groundwork for understanding the operational framework and the challenges faced by these advanced navigation technologies.

3.1.1 Conventional 4G Navigation Receiver

The conventional 4G receiver, a state-of-the-art frequency-domain-based system, has been detailed in collective works such as [1, 54, 93]. Its architecture is delineated in the software-defined receiver (SDR) format, with the structural diagram provided in Figure 3.2. This receiver comprises three primary stages: initial acquisition, acquisition refinement, and tracking.

During the initial acquisition, the receiver, by connecting nodes A, B, and C to node 1, carries out carrier removal and retrieves the baseband samples of OFDM symbols along with their CPs at the UE. As the UE could commence signal reception at any frame instance,

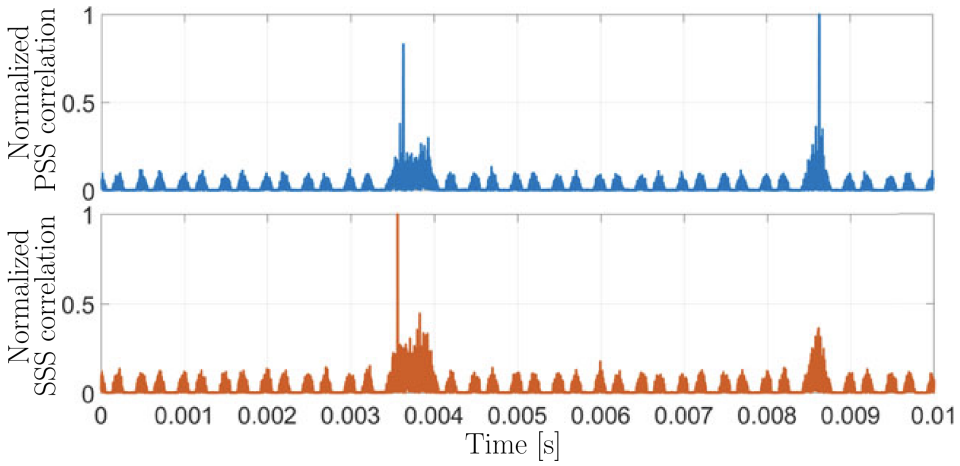


Figure 3.1: Primary synchronization signal (PSS) and secondary synchronization signal (SSS) normalized correlation results with real 4G signals [1].

it must pinpoint the symbol's commencement to discard the CPs and employ the FFT for frame structuring. This process begins with PSS correlation in the time domain, exploiting its bi-frame transmission for peak identification over a frame's 10-millisecond span. The UE, however, cannot discern symbol numbers solely from PSS peaks due to identical sequences at slots 0 and 10. Consequently, SSS correlation is necessary for acquiring precise symbol numbers, with the SSS's unique frame transmission yielding a singular correlation peak. Figure 3.1 exemplifies PSS and SSS correlations with actual 4G signals, showcasing their 1 MHz bandwidth. Multipath conditions may induce biases in correlation peaks, addressed as symbol timing errors in the signal model. Post carrier wipeoff, residual carrier frequency offsets may persist, attributable to oscillator discrepancies and Doppler shifts, characterized as the total carrier frequency offset.

In the acquisition refinement phase, by interfacing nodes A, B, and C with node 2, the receiver estimates and corrects symbol timing errors and carrier frequency offsets in the signal. This necessitates an initial channel frequency response (CFR) estimation. When processing CRS sequences at port $p = 0$, the known CRS facilitates CFR estimation via the estimation of signal parameters via rotational invariance techniques (ESPRIT) algorithm.

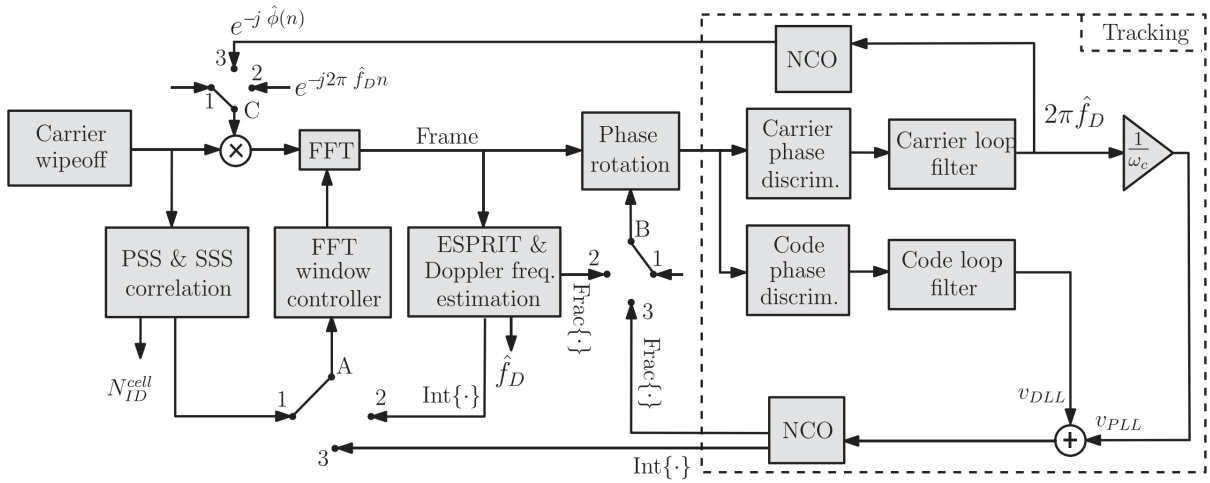


Figure 3.2: Block diagram of the conventional 4G receiver architecture. Abbreviations include ESPRIT (Estimation of Signal Parameters via Rotational Invariance Techniques), FFT (Fast Fourier Transform), NCO (Numerically Controlled Oscillator), PSS (Primary Synchronization Signal), and SSS (Secondary Synchronization Signal).

The final tracking phase involves a specialized delay-locked loop (DLL), supported by a phase-locked loop (PLL), to maintain symbol timing by connecting nodes A, B, and C to node 3. Given that the CRS is distributed across the bandwidth, traditional DLL approaches are unviable for CRS tracking due to the difficulty in obtaining time-domain correlations. Therefore, this receiver employs a specifically tailored DLL for the CRS in 4G systems.

For an exhaustive discussion on the receiver's design stages, refer to [1, 54, 93].

3.1.2 Conventional 5G Navigation Receiver

In parallel with 4G technologies, the conventional 5G communication receiver architecture, which similarly utilizes frequency-domain processes, has been adapted to extract navigation observables. The design of this receiver, as well as its function in extracting navigation data, has been elaborated in collective studies [73, 92]. Notably, a segment of this design is attributed to the author's research efforts and represents a substantive contribution to the dissertation presented herein.

The carrier-aided code SDR aims at opportunistically extracting the TOA measurements from received 5G signals and it has three main stages: (i) 5G carrier frequency extraction, (ii) acquisition, and (iii) tracking. The rest of this section discusses each of these stages.

3.1.2.1 5G Carrier Frequency Extraction

This stage is required if the carrier frequency of the transmitted 5G signal is unknown for the UE. Otherwise, if this information is known, this stage can be skipped, and the UE can start at the acquisition stage. At this stage, a blind search is performed over all candidate 5G frequency bands in order to find the carrier frequency of the transmitted 5G signals. To do so, the UE searches for available SS/PBCH block, which is carried by the synchronization raster. The synchronization raster indicates the frequency positions of the synchronization block that can be used by the UE for system acquisition when explicit signaling of the synchronization block position is not present. The center frequency of the synchronization raster is the center subcarrier of the SS/PBCH block, i.e., the 121-th subcarrier denoted by SS_{REF}. The frequency position of SS_{REF} is defined with corresponding to global synchronization channel number (GSCN) [99]. The parameters defining the SS_{REF} and GSCN for all frequency ranges are presented in Table 3.1. More details can be found in Section 5.4.3 in [99].

3.1.2.2 Acquisition

Knowing the frequency position of SS_{REF}, the UE starts sampling the 5G signals with at least a sufficient sampling rate to capture the entire SS/PBCH bandwidth. Then, the received signal is converted to the baseband domain by wiping out the carrier frequency. At this level, a coarse estimate of the frame start time and $N_{ID}^{(2)}$ are obtained by acquiring the PSS signal. The frame start time is used to control the FFT window timing. The CP elements are removed and an FFT is taken to convert the signal into the 5G frame structure. Then,

Table 3.1: GSCN parameters for the global frequency raster.

Frequency range [MHz]	SS_{REF} **frequency position**	**GSCN**	**Range of GSCN**
0 – 3000	$N \cdot 1200$ kHz $+M \cdot 50$ kHz $N = 1:1:2499,\ M \in \{1,3,5\}^*$	$3N + (M-3)/2$	2 – 7498
3000 – 24250	3000 MHz $+N \cdot 1.44$ MHz $N = 1:1:14756$	$7499 + N$	7499 – 22255
24250 – 100000	24250.08 MHz $+N \cdot 17.28$ MHz $N = 1:1:4383$	$22256 + N$	22256 – 26639

* The default value for operating bands with SCS spaced channel raster is $M = 3$

the SS/PBCH block is extracted, and the received SSS signal is correlated with the possible locally generated sequences to determine $N_{ID}^{(1)}$, and calculate N_{ID}^{Cell} of the gNB. Note that the frequency reuse of 5G is 1, i.e., the received signal may have 5G signal from multiple gNBs with different N_{ID}^{Cell}, In this case, multiple PSS and SSS peaks can be observed corresponding to more than one gNB. Once the UE determines the N_{ID}^{Cell} of the acquired signal, it maps the DM-RS subcarriers and extracts it from the SS/PBCH block. The extracted DM-RS is correlated with all possible sequences, and the one with the highest peak is used to estimate the channel frequency response (CFR). Knowing the CFR, the estimated channel distortion is reversed using a channel equalizer. Then, the PBCH message is decoded and the second and fourth symbols of the SS/PBCH block are used to refine the frame start time estimate using ESPRIT algorithm, where in this paper, the frame start time represents the TOA of the received 5G signal. A coarse estimate of Doppler frequency $\hat{f}_D$ is obtained by looking at the phase difference between the CFR estimated from two distinct symbols in the SS/PBCH block.

3.1.2.3 Tracking

In this stage, a PLL-aided DLL is used to track the TOA of the received signal. At each tracking loop iteration, the phase effect is wiped off from the received signal, which is assumed constant over a duration of two frames and calculated by integrating $\hat{f}_D$ over time. Then, the TOA is normalized by the sampling time T_s, where the integer part of samples Int$\{.\}$ is used to control the FFT window timing and the fractional part of samples $0 \leq \text{Frac}\{\cdot\} < 1$ is removed from the signal using a phase rotation in the frequency domain. The remaining code and carrier phase errors are estimated using a DLL and PLL, respectively.

The carrier phase discriminator can be defined as the phase of the integrated CFRs over the entire subcarrier as shown in [1]. Then, a second-order loop filter at the output of the discriminator can be used to estimate the rate of change of the carrier phase error $2\pi\hat{f}_D$ expressed in rad/s. For code tracking, an early-power-minus-late-power discriminator is used to derive the normalized timing error $\tilde{e}_\tau$ [100]. Assuming that the symbol timing error has linear variations, a second-order loop is used to achieve zero steady-state error. Finally, the TOA estimate $\tilde{e}_\tau$ is updated according to

$$\hat{e}_\tau \longleftarrow \hat{e}_\tau + \frac{T_f}{T_s}\left(v_{DLL} - v_{PLL}\right),$$

where $T_f = 20$ ms and v_{DLL} and v_{PLL} are the outputs of the DLL and PLL filters, respectively. Figure 3.3 presents the block diagram of the acquisition and tracking stages.

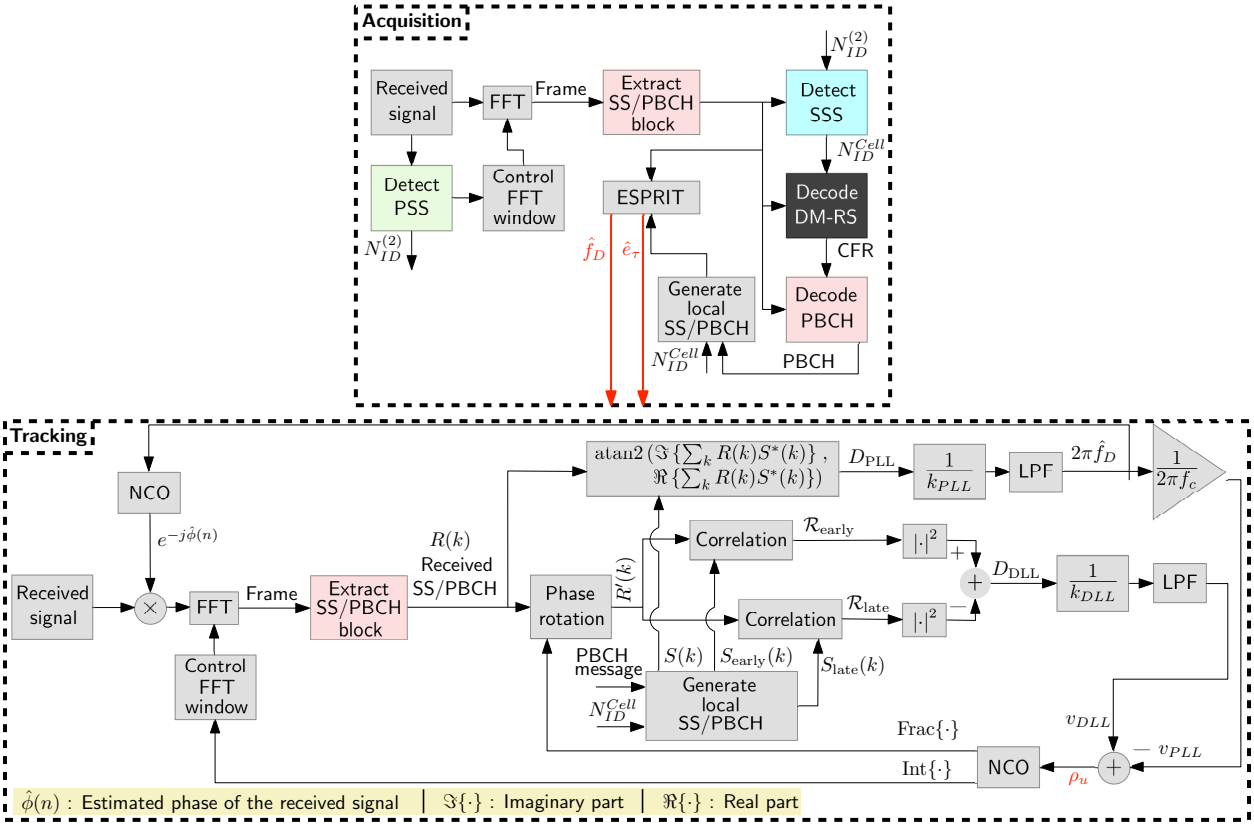


Figure 3.3: Block diagram of the frequency-domain-based carrier-aided code 5G navigation receiver.

3.1.3 Challenges and Limitations of Existing 4/5G Navigation Receivers

The designs of the aforementioned 4/5G navigation receivers are not without their limitations. This section will discuss these limitations in detail and will also explore the untapped potential of these signals for navigation purposes. To facilitate this discussion, we introduce two metrics. Firstly, r_{B,RS_i} represents the ratio of the bandwidth occupied by the RS RS_i to the entire downlink bandwidth of the system. For instance, a $r_{B,\mathrm{RS}_i} = 100\%$ indicates that RS_i is using the full bandwidth. Secondly, r_{T,RS_i} denotes the duty factor of the RSs RS_i, which is the proportion of OFDM symbols that are active in a 4/5G OFDM frame. An OFDM symbol is deemed active if at least 1% of its subcarriers are active. For example, a $r_{T,\mathrm{RS}_i} = 50\%$ means that in a 4G system, half of the OFDM symbols, or 70 out of 140, are active.

3.1.3.1 Coverage

In demanding environments such as deep urban canyons, the interiors of buildings, and at high altitudes, cellular 4/5G terrestrial signals experience significant path losses. These losses stem from environmental structures that cause attenuation, as well as from the extended distances of wireless propagation. Consequently, such conditions can impede 4/5G navigation receivers from successfully acquiring signals and extracting the requisite navigation observables.

In the realm of 4G technology, conventional receivers capitalize on the CRS primarily from a single antenna port, specifically $p = 0$. Better design may allow for the allocation of additional resources, thereby amplifying the power of the signals received. Conceptually, the acquisition of 4G signals can be framed as a detection challenge, where an increase in

signal power directly translates to an elevated CNR. A higher CNR, in turn, augments the likelihood of signal detection, offering a clear advantage in the receiver's performance.

In the case of 5G signals, the adoption of ultra-lean transmission strategies restricts the pool of available resources predominantly to the SS/PBCH block. A standalone reliance on these signals constrains the cumulative power that could otherwise be harnessed if the design ingeniously amalgamated all available signals concurrently. Such an integrated approach promises to significantly amplify the signal power, which is critical for robust signal detection.

3.1.3.2 Initial Doppler Estimation

A pivotal challenge in OFDM-based navigation systems is the precise estimation of initial Doppler shifts during the acquisition stage. This estimation is inherently constrained by the SSs having a small duty cycle, quantified as $r_{\mathrm{T,SS}} = \frac{\text{SSs symbols}}{\text{Total symbols}} \cdot 100$, which amounts to 1.43% for 4G and 0.71% for 5G. The impact of this limitation is particularly pronounced in high-dynamic environments where the Doppler shifts exhibit broader variations, necessitating a robust initial estimate to ensure successful lock-in by tracking loops. Additionally, significant clock drift mismatches between the UE and the BS exacerbate this issue by inducing large Doppler shifts, further complicating the acquisition process.

3.1.3.3 Ultra-Lean Transmission

Unlike previous cellular systems, 5G applies an ultra-lean transmission policy, which minimizes the transmission of "always-on" signals; hence, limiting UE-based opportunistic navigation to only SSs. To demonstrate the impact of this limitation, consider the possible 5G downlink bandwidth B_{5G}, which ranges between 4.32 to 397.44 MHz, with SSs spanning a bandwidth B_{SS} that ranges between 3.6 to 57.6 MHz. As such, for $B_{\mathrm{5G}} = 397.44$ and $B_{\mathrm{SS}} = 57.6$, only $r_{B,\mathrm{RS}_{\mathrm{5G,SS}}} = 14.5\%$ of the bandwidth is being exploited opportunistically

with SSs alone. Higher bandwidth signals yield more precise time-of-arrival estimates and facilitate differentiating the LOS signal from multipath components.

3.2 Ultimate Reference/Synchronization Signal

In the pursuit of enhancing navigation capabilities within cellular networks, this section introduces an innovative concept: the Ultimate Reference Signal (URS) for 4G and the Ultimate Synchronization Signal (USS) for 5G. These signals are designed to overcome the limitations of weak signal power and limited resource utilization inherent in standard receiver designs.

3.2.1 4G Ultimate Reference Signal

This section introduces the URS concept for 4G to tackle the issue of weak signal power in OFDM-based navigation. The 3GPP standards define antenna ports for the 4G/LTE cellular system as logical entities identified by their unique reference sequences, rather than by physical antennas. An antenna port may cover multiple RSs associated with a single physical antenna or be distributed across multiple transmit antennas. The formal definition from the 3GPP standards is: An antenna port is such that the channel through which an OFDM symbol is transmitted can be inferred from the channel of another symbol on the same port [101]. Each antenna port has its own resource grid, and the transmission of a physical channel or signal may involve several antenna ports depending on their configuration.

With the proposed approach, the CRS that spans the entire bandwidth of the 4G system—previously described in Chapter 2.1.1 and known to the UE—is fully exploited. For CRS, the relevant antenna ports p could be a single port $p = 0$, a pair $p \in \{0, 1\}$, or a set $p \in \{0, 1, 2, 3\}$. Prior research has focused on using only $p = 0$ [54]. Although different

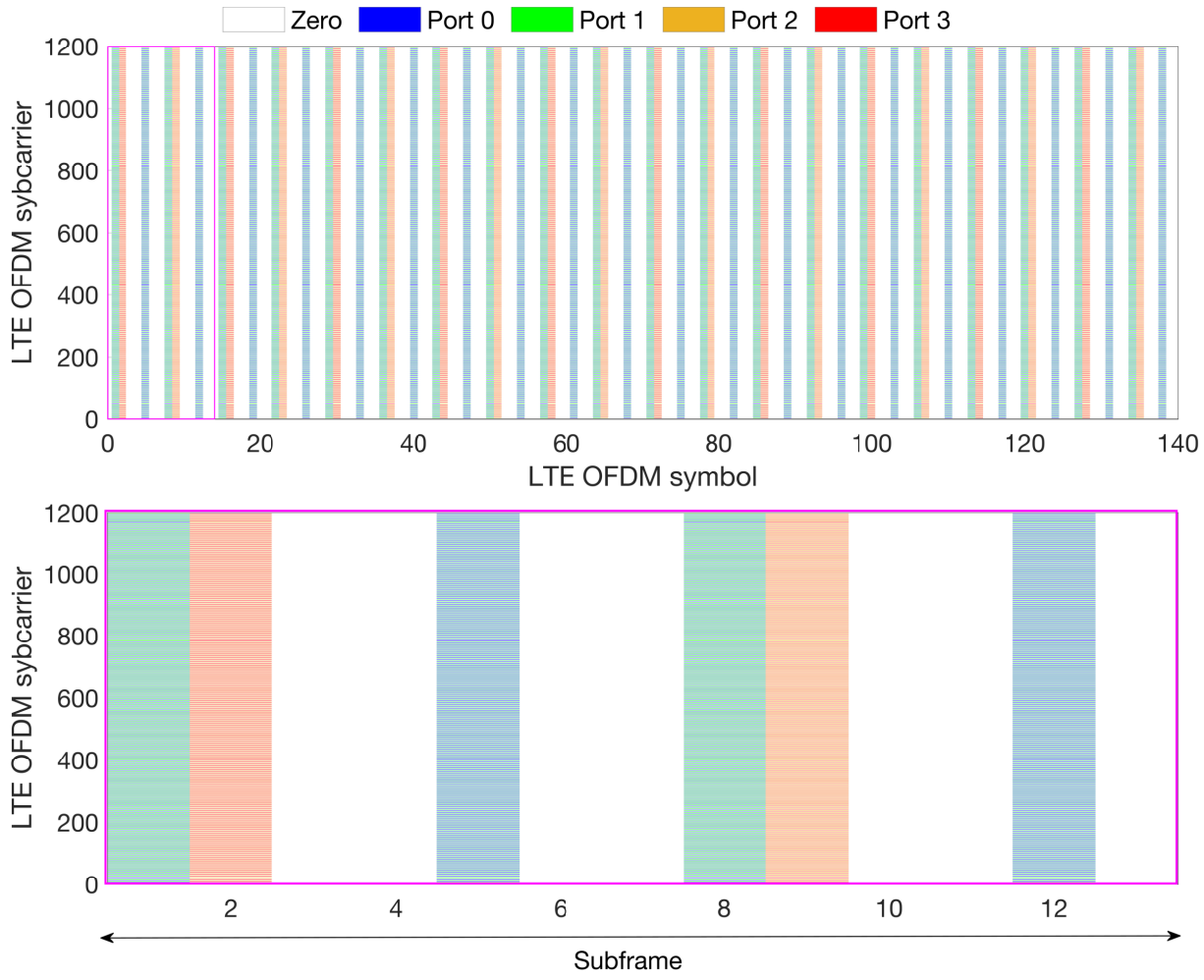


Figure 3.4: 4G frame representation CRS REs allocation for all antenna ports.

antenna ports do not necessarily correlate to distinct physical antennas for all RSs, CRS uniquely maintains a direct mapping. Figure 3.4 illustrates the 4G OFDM frame, highlighting the CRS resources for all antenna ports. The frame shown represents a simulated 4G downlink with a 20 MHz system bandwidth, the maximum possible, translating to 1200 subcarriers with a spacing of 15 kHz each [102].

Previously, 4G SDRs utilized only CRS resources corresponding to $p = 0$, marked in blue in Figure 3.4, which resulted in a duty factor $r_{\mathrm{T,CRS_{con}}} = 0.71$ %. For brevity, $\mathrm{CRS_{con}}$ will henceforth be denoted simply as CRS, referring to the CRS resources used in the last generation of 4G SDRs. The proposed approach, by employing various available ports,

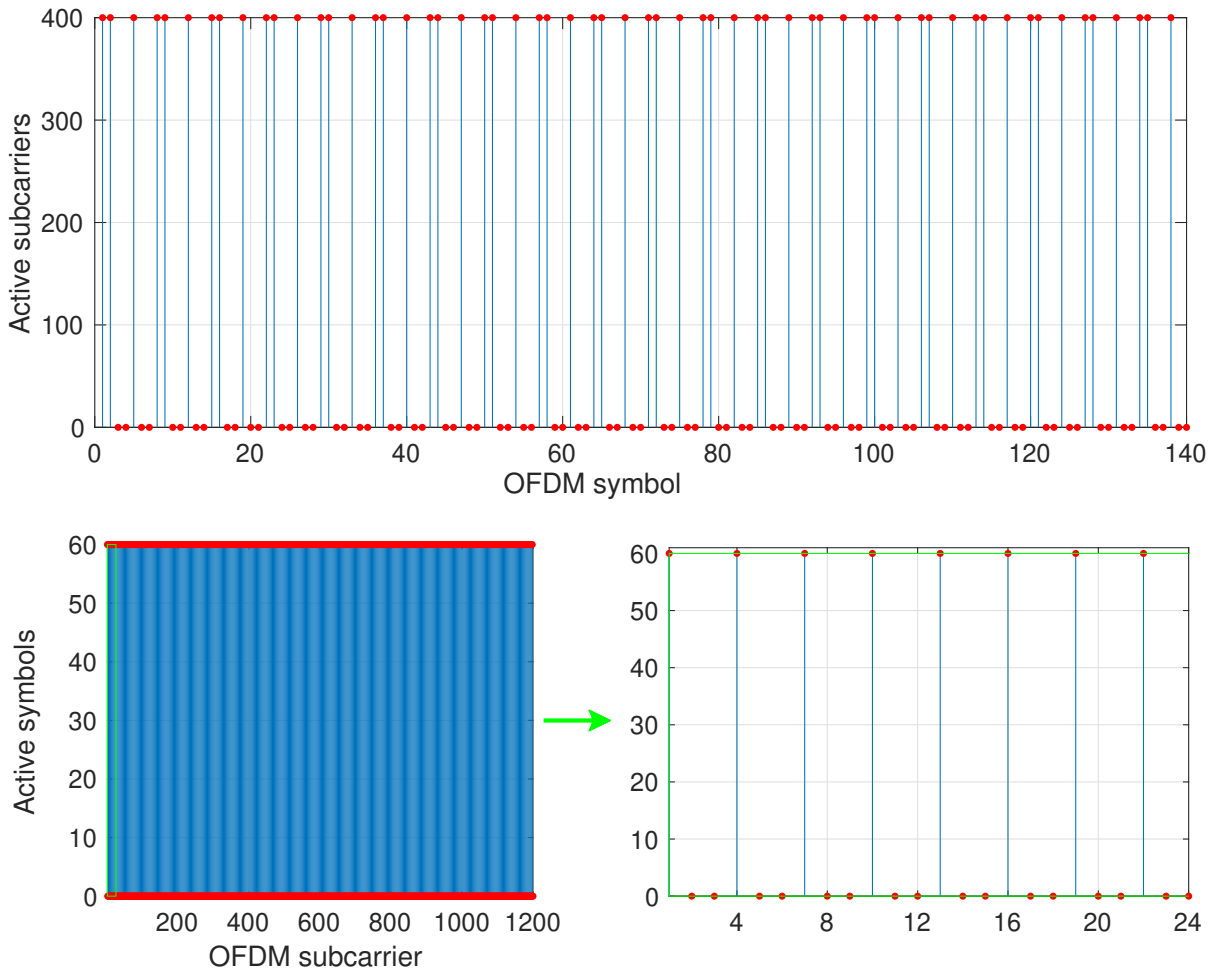


Figure 3.5: (a) The number of active subcarriers for each URS symbol and (b) the number of active symbols for each URS subcarrier.

amalgamates CRSs from different antenna ports to form the 4G-URS. Consequently, the combined OFDM REs, as depicted in Figure 3.4, constitute the 4G-URS. An analysis of the 4G-URS's spectral efficiency $r_{\mathrm{B,4G-URS}}$ and duty factor $r_{\mathrm{T,4G-URS}}$, based on the number of active subcarriers and symbols, is visualized in Figure 3.5. The duty factor of $r_{\mathrm{T,4G-URS}} = 42.86\%$, a significant increase from $r_{\mathrm{T,SS}} = 1.43\%$. For the bandwidth ratio, it is noted that $r_{\mathrm{B,4G-URS}} = r_{\mathrm{B,CRS}} = 100\%$.

The URS approach offers distinct advantages. It leverages 24,000 REs compared to the 200 REs used by previous SDRs, thereby amplifying the 4G signal power by a factor of 120.

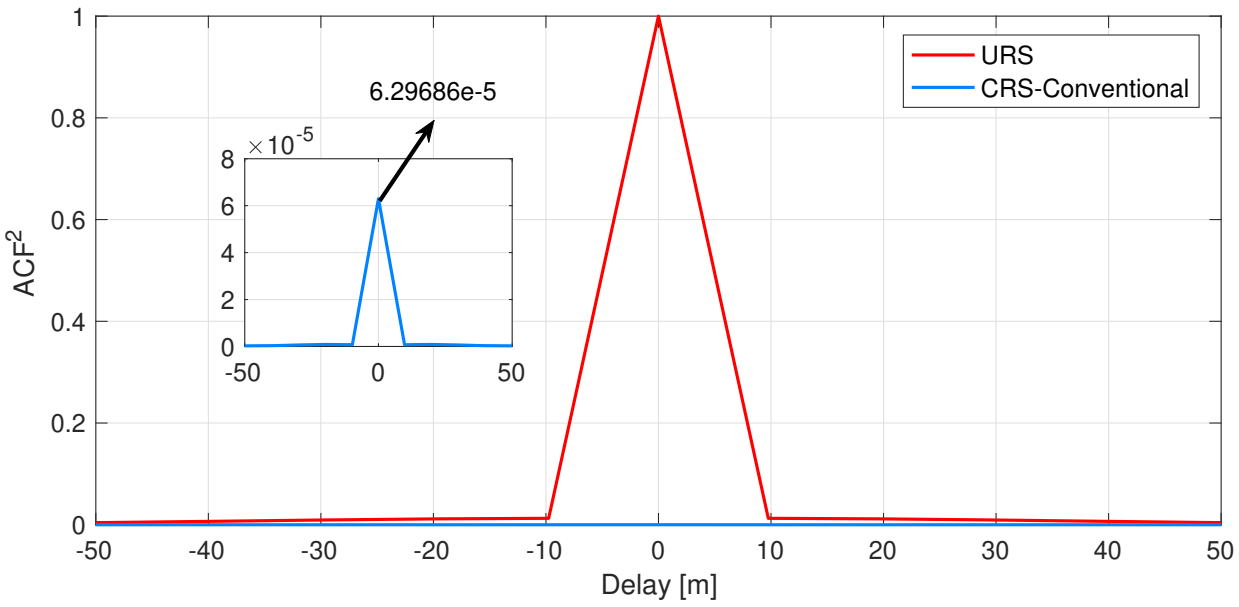


Figure 3.6: A comparison of the CRS-based autocorrelation function (ACF) and the proposed URS.

This amplification is crucial for addressing weak signals in challenging scenarios such as high-altitude aircraft navigation. Figure 3.6 demonstrates the gain in the squared autocorrelation function (ACF) magnitude when comparing CRS-based and URS-based approaches, assuming equal power among all REs. The gain factor, calculated as $r_{\text{gain}} \approx \sqrt{\frac{1}{6.29687 \times 10^{-5}}} = 126.02$, exceeds the anticipated factor of 120, attributed to the inclusion of CP REs before the IFFT of each OFDM symbol—a process that will be further explained when discussing URS replica generation. Moreover, the URS significantly improves the duty cycle, which directly enhances the accuracy of carrier phase estimation, notably in estimating the initial Doppler shift.

3.2.2 5G Ultimate Synchronization Signal

In the context of 5G, the available resources are confined to the SS/PBCH block, as dictated by the ultra-lean transmission approach previously discussed. Nevertheless, a method akin to the 4G URS can be adopted for 5G to formulate an USS. This USS amalgamates all user-known RSs, specifically the PSS, SSS, and PBCH DM-RS, to maximize resource utilization.

To evaluate the USS's correlation characteristics, a 5G OFDM frame was constructed adhering to the parameters specified in Table 3.2. An image plot of this frame is depicted in Figure 3.7. The USS in the time domain was derived by converting the frame into samples, as delineated in Subsection 2.1.1. Subsequently, the USS's ACF was computed, as illustrated in Figure 3.8(a). For comparative analysis, separate OFDM frames for each standalone SS—namely the PSS, SSS, and PBCH DM-RS—were also constructed. Their respective time-domain sequences were generated, and the ACFs were calculated accordingly, as demonstrated in Figure 3.8(a).

The DM-RS exhibits a sharper autocorrelation peak compared to the PSS and SSS, which is anticipated given its wider bandwidth of approximately 3.6 MHz versus 1.905 MHz for the PSS and SSS. Conversely, the USS correlation shows a considerably stronger peak. However, its first zero-crossing lies between the PSS/SSS and the PBCH DM-RS. This variation arises because the USS correlation is no longer a singular sinc function but now contains two distinct sinc components derived from the PSS/SSS and PBCH DM-RS. The distinct characteristics of these components are visible upon examining the PSD of the ACFs, presented in Figure 3.8(b). The PSDs for the PSS and SSS are represented as

$$S_{\text{PSS/SSS}}(f) = a\,\text{rect}(f/1.905), \tag{3.1}$$

with f denoting frequency in MHz and a symbolizing an amplitude contingent on the sequence's power. The PBCH DM-RS's PSD is approximated by

$$S_{\text{DMRS}}(f) \approx b\,\text{rect}(f/3.6), \tag{3.2}$$

where b is another amplitude parameter. This approximation is necessitated by the scattered allocation of PBCH DM-RS REs in the 5G frequency domain, unlike the contiguous PSS and SSS, as visualized in Figure 3.7. Therefore, an approximate PSD for the USS can be

formulated as

$$S_{\mathrm{USS}}(f) \approx 2a\,\mathrm{rect}(f/1.905) + b\,\mathrm{rect}(f/3.6), \tag{3.3}$$

leading to an inferred USS ACF

$$R_{\mathrm{USS}}(\tau) \approx \mathcal{F}^{-1}\left\{S_{\mathrm{USS}}(f)\right\} = 3.81a\,\mathrm{sinc}(1.905\tau) + 3.6b\,\mathrm{sinc}(3.6\tau), \tag{3.4}$$

where τ is the time delay in microseconds. This estimated $R_{\mathrm{USS}}(\tau)$, plotted with a red dashed line in Figure 3.8(a), closely aligns with the empirically determined autocorrelation, depicted by the solid purple line. From this analysis, we can deduce the spectral efficiency, denoted as $r_{\mathrm{B,USS}}$, and the duty factor, denoted as $r_{\mathrm{T,USS}}$, for the USS. Notably, the duty factor for the USS is $r_{\mathrm{T,USS}} = 1.43\%$. This represents a marked improvement over the $r_{\mathrm{T,SRS}} = 0.36\%$, which refers to the duty factor when a single reference signal (SRS) is used in isolation, as is typical in standard 4/5G navigation receivers. Regarding the bandwidth utilization, the USS achieves a bandwidth ratio of $r_{\mathrm{B,USS}} = r_{\mathrm{B,DMRS}} = 14\%$, which reflects the proportion of the total available bandwidth that the USS occupies.

Table 3.2: The 5G USS simulation settings.

Parameter	**Value**
μ	0
N_{ID}^{Cell}	0
$\bar{i}_{\mathrm{ssb}}$	0
SS/PBCH subcarrier spacing	0
System bandwidth	20 MHz
N^{RB}	100

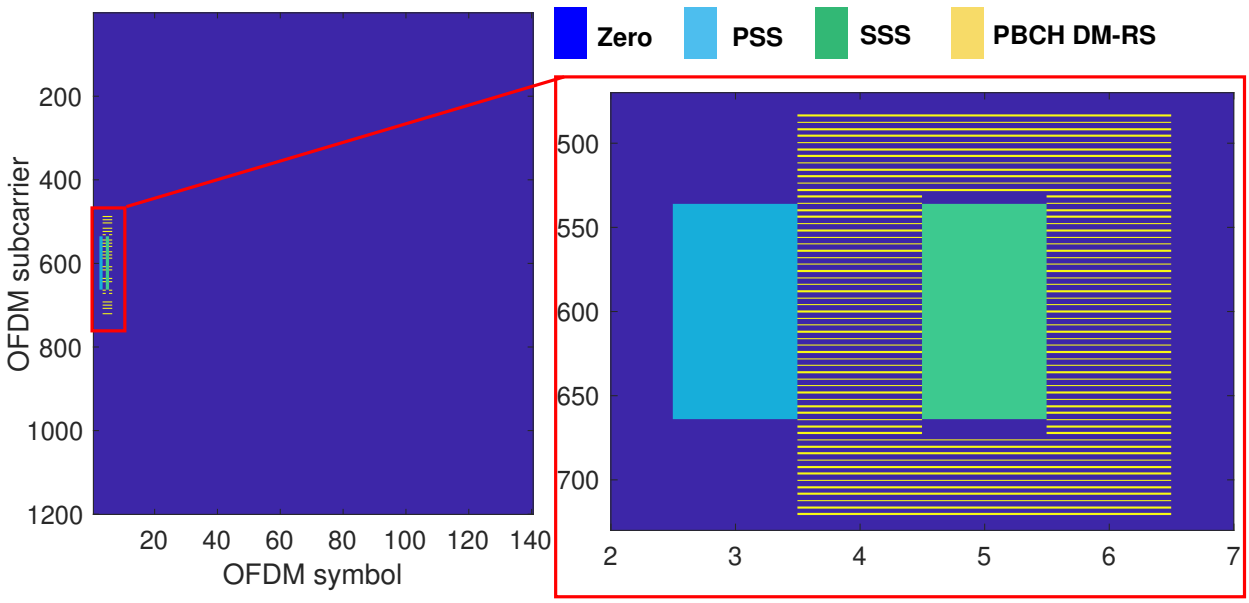


Figure 3.7: A 5G USS simulated frame.

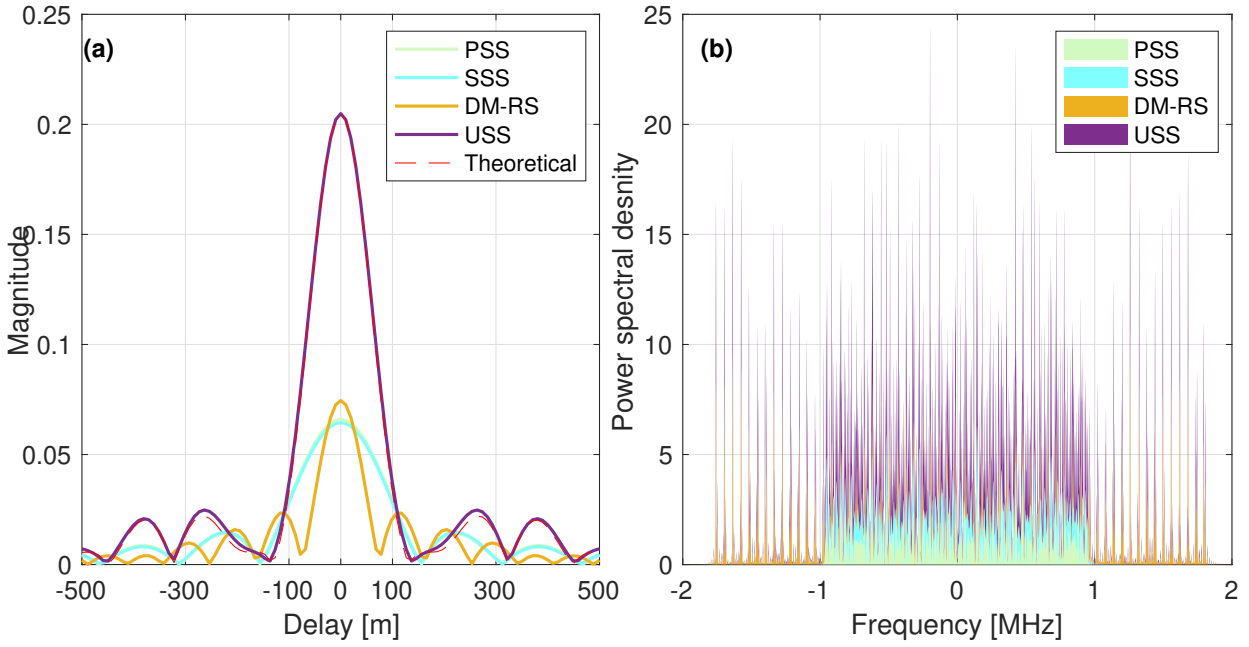


Figure 3.8: The (a) Autocorrelation and (b) power spectral density (PSD) of the USS compared to standalone PSS, SSS, and PBCH DM-RS synchronization sequences for gNB with $\mu = 0$,$N_{ID}^{Cell} = 0$, $\bar{i}_{\text{ssb}} = 0$, and 20 MHz system bandwidth.

3.3 Time-Domain-Based 4/5G Cellular Navigation Receiver

In this section, a time-domain-based SDR that utilizes the 4G-URS and 5G-USS. These 4G-URS and 5G-USS are designed to harness time orthogonality and thereby extract navigation observables from received 4/5G OFDM signals more effectively. Unlike the conventional 4/5G SDRs that rely on frequency-domain orthogonality of synchronization and channel estimation RSs—where the OFDM frame is reconstructed from the received time-domain serial data—the proposed SDR takes a novel approach. While previous systems estimate navigation observables using the RS with the largest bandwidth, which stems from communication-focused applications that require OFDM frame reconstruction for two-way communication, the proposed method pivots towards opportunistic navigation. Here, the primary objective is to capitalize on the most extensive frequency (bandwidth) and time (duty factor) resources available in the received signal for navigation observables extraction.

Leveraging the inherent orthogonality of OFDM signals across both frequency and time dimensions, the proposed SDR aggregates all accessible REs (REs) to form a composite 4G-URS/5G-USS. The subsequent subsections detail the generation process of the UXS and delineate the two fundamental stages of the proposed time-domain SDR: acquisition and tracking. Figure 3.9 depicts the block diagram of the proposed SDR.

3.3.1 Generation of 4G-URS and 5G-USS Sequences

The generation and mapping procedures for the 4G-URS and the 5G-USS are comprehensively detailed in Appendices A.1 and A.2, respectively. The culmination of these procedures results in the creation of OFDM frames that represent the frequency-domain versions of the

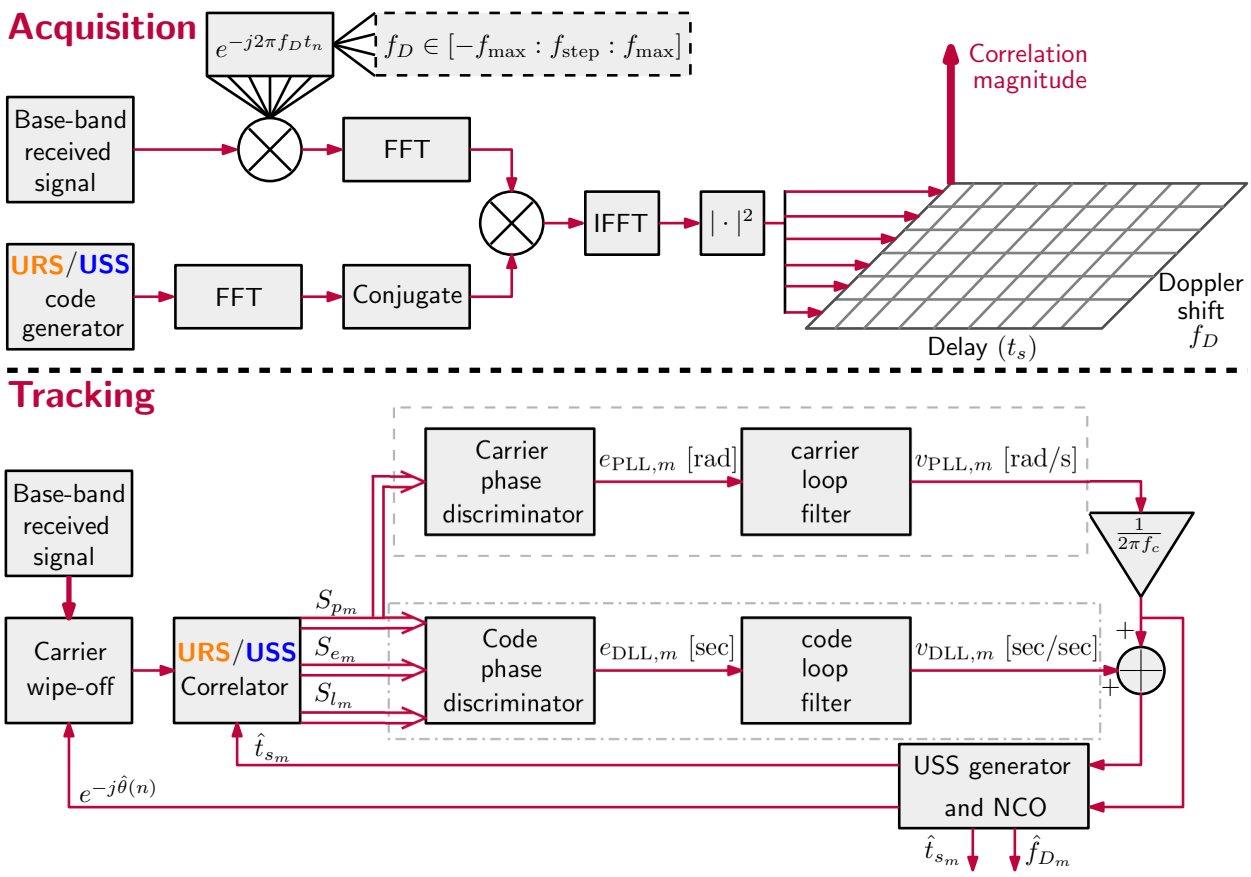


Figure 3.9: Block diagram of the proposed time-domain carrier-aided code-based 4/5G cellular navigation receiver. Thick lines represent complex quantities.

4G-URS and 5G-USS, symbolically represented as $\mathbf{UXS}^{f}_{\text{sig,ID}}$. Here, sig $\in \{4\text{G}, 5\text{G}\}$ specifies the signal type, and ID denotes the physical Cell ID of the cellular node.

To transform these frames into a practical form for transmission, $\mathbf{UXS}^{f}_{\text{sig,ID}}$ is first converted into a time-domain sequence, designated as $\mathbf{UXS}^{t}_{\text{sig,ID}}$. This conversion involves zero-padding by $\frac{1}{2}N_{\text{RB}}^{\text{max,DL}} - N_{\text{RB}}^{\text{DL}}$ REs on both sides of the signal in the frequency domain. An IFFT is then applied. Subsequently, CP elements are added to each OFDM symbol to mitigate ISI. This CP addition essentially involves appending a copy of the end portion of the OFDM symbol to its beginning.

This entire procedure mirrors the signal processing that occurs at the eNodeB/gNB, with the key difference being the replacement of data in the data-allocated REs with zeros in our case. This substitution is critical to avoid interference and maintain the orthogonality of $\mathbf{UXS}^{t}_{\text{sig,ID}}$. For the sake of simplicity and clarity in the following discussions, the superscript ^{t} will be omitted, and $\mathbf{UXS}^{t}_{\text{sig,ID}}$ will henceforth be referred to simply as $\mathbf{UXS}_{\text{sig,ID}}$.

3.3.2 Acquisition

The primary goal of the acquisition stage is to identify nearby eNodeBs/gNBs and obtain coarse estimates of their corresponding code start times and Doppler frequencies. Assuming that the UE knows the carrier frequencies of surrounding eNodeBs/gNBs, it begins by sampling the 4/5G cellular signals at a rate sufficient to cover the entire system bandwidth. These signals are then converted to the baseband domain by eliminating the carrier frequency. The resulting discrete-time signal is represented as $x[n]$, where n signifies a discrete-time instance. A search is then conducted over the code start time and Doppler frequency to detect the presence of a signal at $n = 0$ within $x[n]$.

For identification, there are 504 potential URS sequences for 4G, arising from CRS combi-

nations, and 1008 potential USS sequences for 5G, derived from PBCH-DMRS. These are denoted as $\{\mathbf{UXS}_{\text{4G,ID}}\}_{\text{ID}=0}^{503}$ and $\{\mathbf{UXS}_{\text{5G,ID}}\}_{\text{ID}=0}^{1008}$, respectively. Each $\mathbf{UXS}_{\text{sig,ID}}$ serves as a pseudo-random number (PRN) for the SDR, similar to GPS.

The enhanced duty factor offered by the UXS allows for a GPS-like frequency acquisition search, aiding in the initial Doppler shift estimation. This search yields coarse estimates of the initial Doppler frequency $\hat{f}_{D_0}$ and the code start time $\hat{t}_{s_0}$, which are then input into the tracking loops. It is important to note that the SSs are deliberately excluded from the proposed UXS due to their non-uniqueness for every eNodeB/gNB, which could lead to interference in scenarios where multiple eNodeBs/gNBs are detectable, such as in aviation with a clear line of sight from multiple cellular nodes.

3.3.2.1 Acquisition Optimization

The computational burden of the acquisition stage, particularly due to the Doppler search for all possible IDs, is a significant challenge. For context, the number of potential PRNs is about 16/32 times greater than that of GPS L1, depending on the signal type. To address this, the proposed SDR incorporates two optimization strategies:

Firstly, the SDR combines different sectors of the same cellular node, meaning Cell IDs with varying PSS but identical SSS. This is feasible because (i) the UXS exhibits excellent cross-correlation properties and (ii) SSs are not used in the UXS. Therefore, the three sectors of an eNodeB/gNB can be represented by a single PRN:

$$\begin{aligned}\mathbf{UXS}_{\text{sig,ID}'} &= \mathbf{UXS}_{\text{sig,ID=ID}'} + \mathbf{UXS}_{\text{sig,ID=ID}'+1} + \mathbf{UXS}_{\text{sig,ID=ID}'+2}, \\ &\text{for ID}' = \{0, 3, 6, \cdots, 502\},\end{aligned}$$

where each term represents one of the three sectors. This approach effectively reduces the

number of potential UXSs by a factor of three.

Secondly, the SDR optimizes the Doppler search by considering Doppler values with integer differences of the UXS-frame frequency spacing ($\frac{1}{t_{\text{frame}}} = 100$ Hz for 4G-URS and 50 Hz for 5G-USS). The Doppler search range is thus defined as:

$$f_{D,\text{search}} \in [-f_{\max}, f_{\text{step}}, f_{\max}] ,$$

where $f_{\max}$ is the maximum search value, and f_{step} is the search step. If $f_{\max} > \frac{1}{t_{\text{frame}}} = f_{\text{frame}}$ Hz, a new search range f_0 is defined as:

$$f_0 \equiv [-f_{\text{frame}}, f_{\text{step}}, f_{\text{frame}}] .$$

Thus, higher search ranges are effectively circularly-shifted versions of f_0 of the locally-generated UXSs.

3.3.2.2 Acquisition Sample Outputs

Figures 3.10 and 3.11 present the two-dimensional acquisition output samples from experimental data, showcasing results from a stationary 4G receiver and a UAV-based 5G receiver, respectively. The output from the 4G receiver demonstrates superior detection capabilities, which can be attributed to the more extensive resources available in the 4G-URS, in contrast to those in the 5G-USS. It shall be noted that the acquisition illustrated in Figure 3.10 was conducted over the span of a single frame. In comparison, for the 5G acquisition shown in Figure 3.11, a subaccumulation technique encompassing three frames was employed. This approach was necessary to compensate for the relatively low duty cycle of the 5G-USS signal, even after its enhancement from the utilization of a single reference signal at a time.

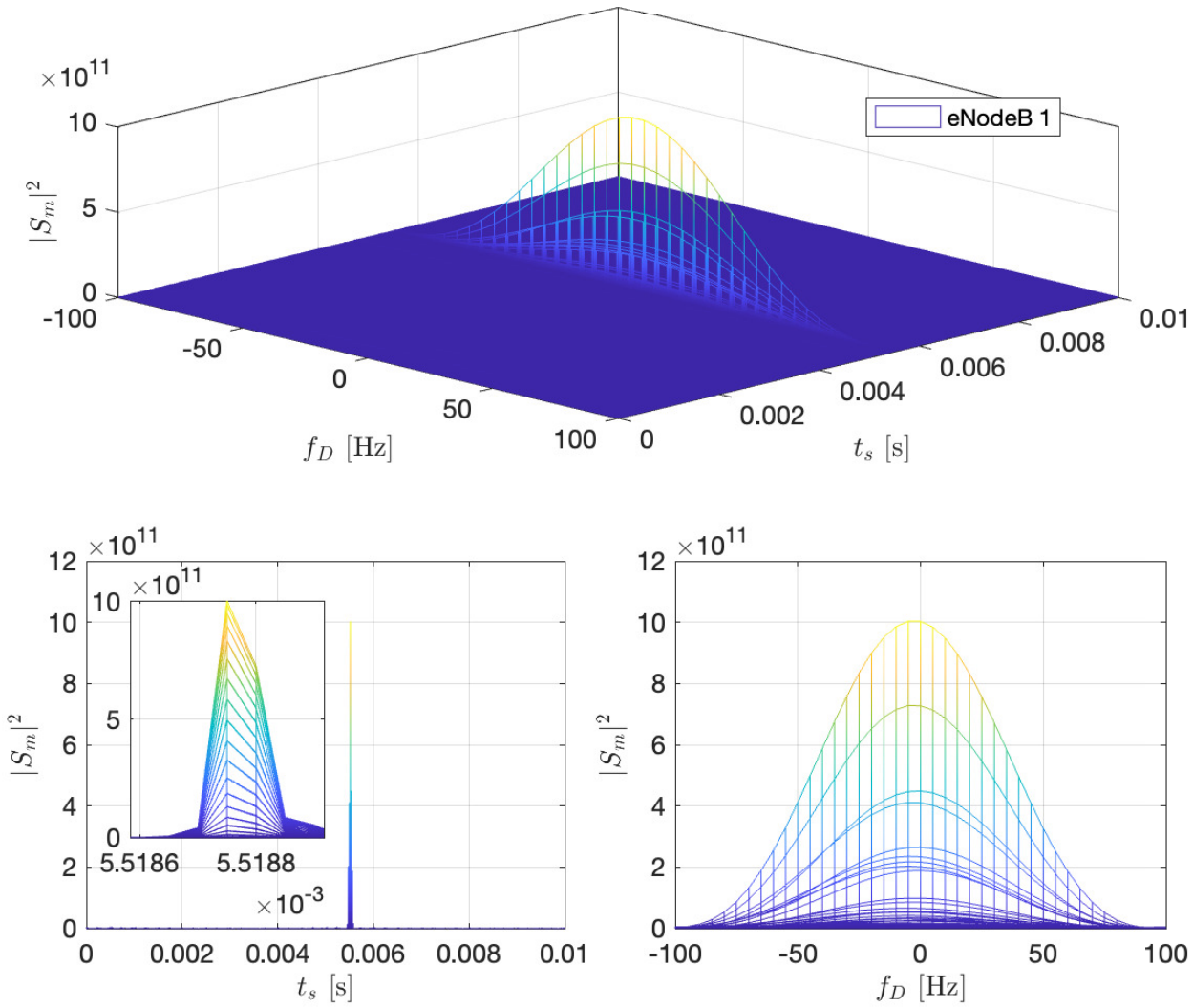


Figure 3.10: Cellular 4G signal acquisition results showing $|S_m|^2$ versus $\hat{t}_{s_0}$ $\hat{f}_{D_0}$ for one detected eNodeB from a stationary 4G experiment, along with the cross-sectional view of the 2D search in time- and frequency- domains.

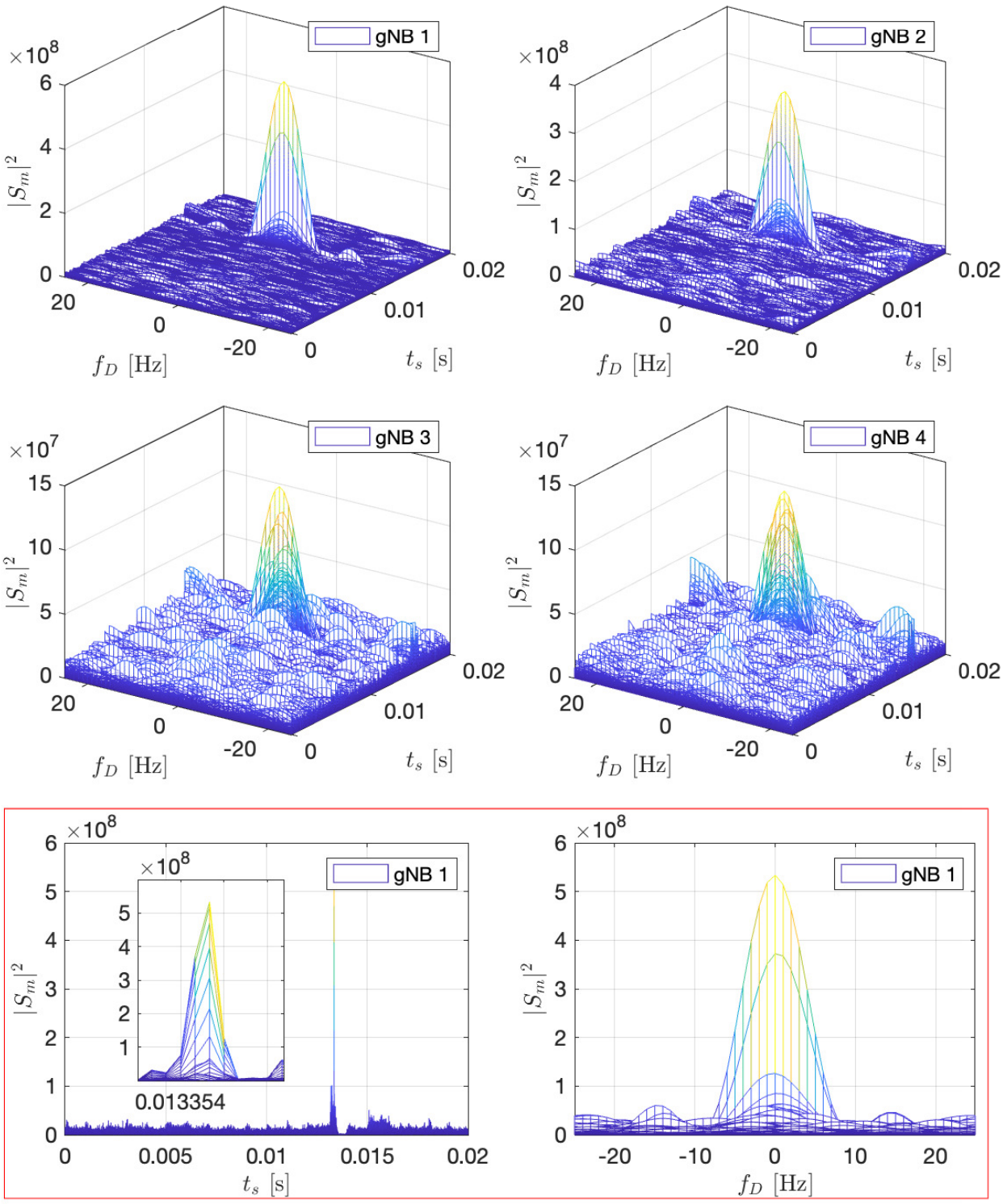


Figure 3.11: Cellular 5G signal acquisition results showing $|S_m|^2$ versus $\hat{t}_{s_0}$ $\hat{f}_{D_0}$ for four detected gNBs from a UAV-based 5G experiment, along with the cross-sectional view of the 2D search in time- and frequency- domains of gNB 1.

3.3.3 Tracking

After obtaining coarse estimates of the initial Doppler frequency $\hat{f}_{D_0}$ and the initial code start time $\hat{t}_{s_0}$, the receiver refines and maintains these estimates via tracking loops. In the proposed design, a PLL is employed to track the carrier phase and a carrier-aided DLL is used to track the code phase.

The PLL consists of a phase discriminator, a loop filter, and a numerically-controlled oscillator (NCO). Since URS is a data-less pilot channel, an atan2 discriminator, which remains linear over the full input error range of $\pm\pi$, could be used without the risk of having phase ambiguities. It was found that a second-order PLL is sufficient to maintain track of the carrier phase for different dynamical scenarios. The loop filter transfer function is given by

$$F_{\text{PLL}}(s) = \frac{2\zeta w_n s + w_n^2}{s}, \tag{3.5}$$

where $\zeta \equiv \frac{1}{\sqrt{2}}$ is the damping ratio and w_n is the undamped natural frequency, which can be related to the PLL's noise-equivalent bandwidth $B_{n,\text{PLL}}$ by $B_{n,\text{PLL}} = \frac{w_n}{8\zeta}\left(4\zeta^2 + 1\right)$ [5]. The output of the loop filter at the m-th subaccumulation $v_{\text{PLL},m}$ is the rate of change of the carrier phase error, expressed in rad/s. Then, the Doppler frequency estimate is obtained as $\hat{f}_{D_m} = \frac{v_{\text{PLL},m}}{2\pi}$. The carrier phase estimate is modeled as

$$\hat{\theta}(t_n) = 2\pi \hat{f}_{D_m} t_n + \theta_0, \tag{3.6}$$

where $t_n = nT_s$ is the sample time expressed in receiver time, T_s is the sampling time, and θ_0 is the initial beat carrier phase of the received signal.

The carrier-aided DLL employs the non-coherent dot product discriminator, in which the prompt, early, and late correlations, denoted by S_{p_m}, S_{e_m}, and S_{l_m}, respectively. The DLL loop filter is a simple gain K, with a noise-equivalent bandwidth $B_{n,\text{DLL}} = \frac{K}{4} \equiv 0.05$ Hz.

The output of the DLL loop filter $v_{\mathrm{DLL},m}$ is the rate of change of the code phase, expresses in s/s. Assuming low-side mixing, the code start time is updated according to

$$\hat{t}_{s_{m+1}} = \hat{t}_{s_m} - (v_{\mathrm{DLL},m} + \hat{f}_{D_m}/f_c) \cdot N_s T_s, \tag{3.7}$$

where f_c is the carrier frequency of the received signal and N_s is the number of samples per subaccumulation.

3.3.3.1 Tracking Sample Outputs

Experimental results from a high-altitude aircraft employing a 4G receiver and a ground vehicle utilizing a 5G receiver are presented in Figures 3.12 and 3.13, respectively. These figures display the tracking outputs of the receivers, providing a comprehensive view of various metrics. The data includes (i) the in-phase and quadrature components of the prompt correlation, (ii) the carrier-to-noise ratio (C/N_0), (iii) the code phase error in samples, (iv) the carrier phase error in degrees, (v) the measured pseudorange in meters, and (vi) the measured Doppler shift in Hz.

These figures and their accompanying metrics provide valuable insights into the tracking capabilities and performance of 4G and 5G receivers in different operational environments.

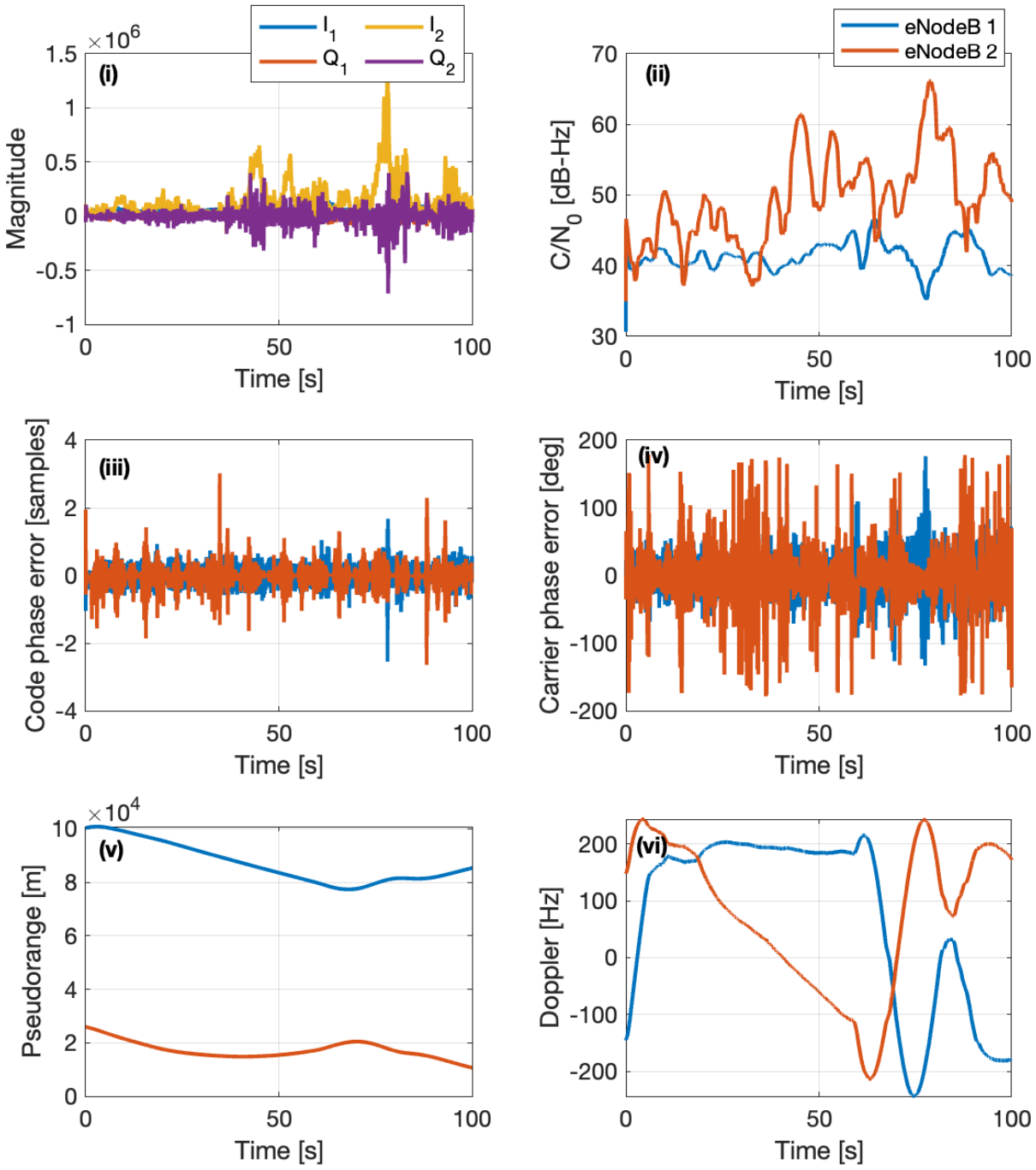


Figure 3.12: 4G signal tracking results from a high-altitude aircraft-based receiver, illustrating (i) in-phase and quadrature components of the prompt correlation, (ii) C/N_0, (iii) code phase error in samples, (iv) carrier phase error in degrees, (v) measured pseudorange, and (vi) Doppler shift.

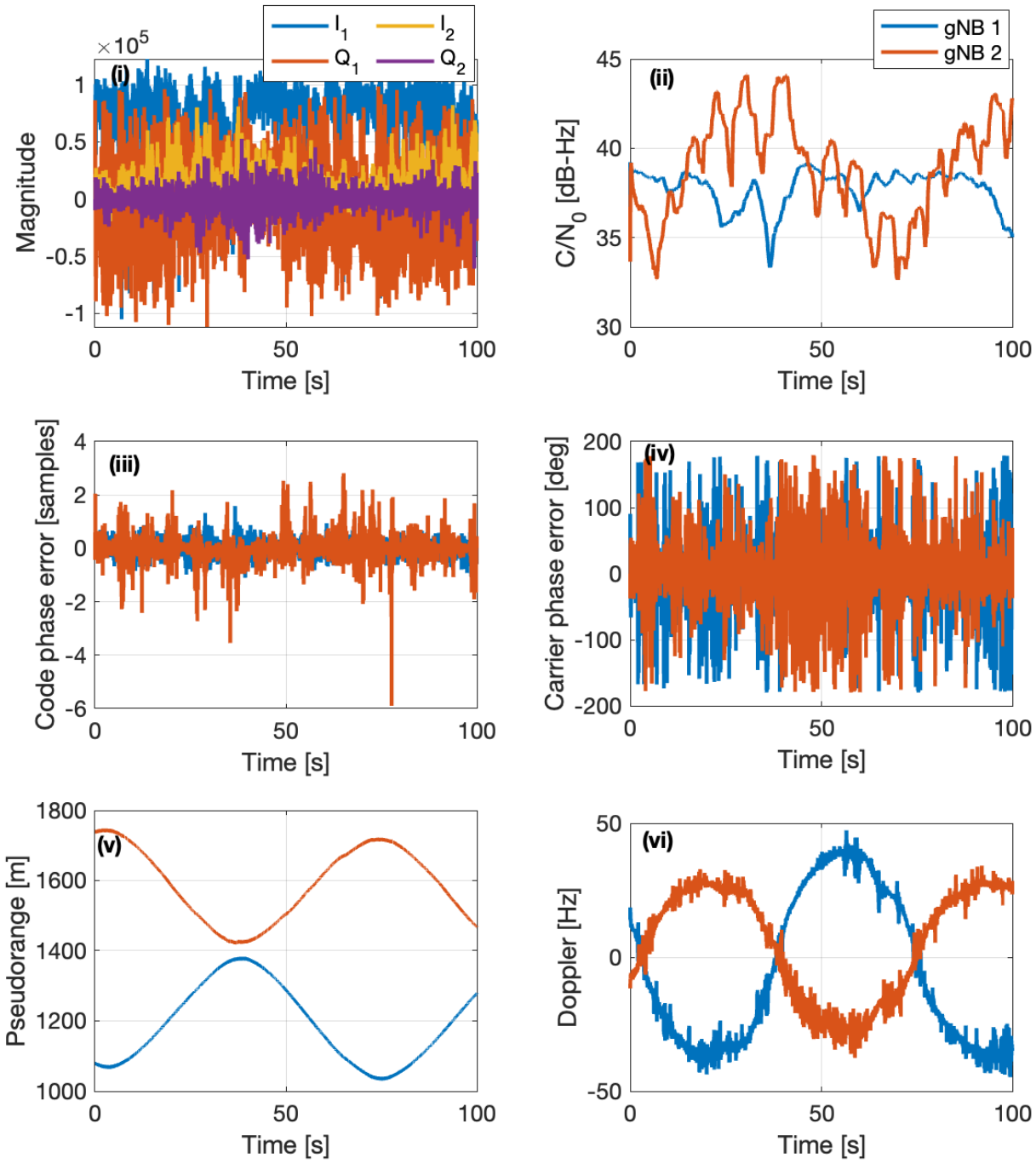


Figure 3.13: 5G signal tracking results from a ground vehicle-based receiver, showing (i) in-phase and quadrature components of the prompt correlation, (ii) C/N_0, (iii) code phase error in samples, (iv) carrier phase error in degrees, (v) measured pseudorange, and (vi) Doppler shift.

Chapter 4

Experimental Characterization of 4/5G Signals

This chapter is organized as follows. Section 4.1 details an experimental analysis focused on the frequency stability characteristics of 4/5G networks. In Section 4.2, we investigate the influence of environmental variables, antenna performance, and receiver clock precision on the strength of 4/5G signals. This section also includes a mobile outdoor experiment aimed at modeling the relationship between 5G signal reception and distance in a semi-urban setting.

4.1 Frequency Stability of Cellular 4/5G Signal

4.1.1 Carrier Frequency Search

As detailed in Subsection 3.1.2.1, determining the frequency position of SS_{REF} is essential when unknown to the UE. To address this, an extensive search across the 5G frequency bands in FR1 was conducted in three Californian cities: Irvine, Costa Mesa, and Santa Ana.

Following the guidelines in Table 3.1, the search primarily found 5G signals in the sub-3 GHz range, particularly in the n5 and n71 bands, linked to AT&T and T-Mobile. Interestingly, during these searches, a new smartphone with AT&T service indicated a 5G signal on the n5 band, but initial searches in the expected frequency positions yielded no results. It was only after an expanded search that a 5G signal at 872 MHz, outside the listed frequency positions, was discovered. Another detected signal at 632.55 MHz corresponded to a frequency position for $N = 527$ and $M = 3$ (GSCN = 1581), as per the search parameters.

4.1.2 Stationary Experiment: Frequency Stability in Cellular 5G System

4.1.2.1 Experimental Setup and Environmental Layout

A stationary experiment was conducted at the University of California, Irvine (UCI), USA, using a quad-channel National Instrument (NI) universal software radio peripheral (USRP)-2955 connected to a UE receiver. This setup utilized two consumer-grade cellular omnidirectional Laird antennas, with the USRP sampling signals at 10 mega samples per second (Msps). The USRP was tuned to two different carrier frequencies to receive signals from one eNodeB and one gNB, belonging to two different U.S. cellular providers. The characteristics of these BSs are outlined in Table 4.1. The collected 4G and 5G signals were transferred from the USRP-2955 to a laptop via a PCI Express cable for subsequent post-processing. Figure 4.1 displays the experiment's environmental layout, including the positions of the eNodeB and gNB, and the hardware and software setup used.

Table 4.1: Frequency Stability Experiment: eNodeB's and gNB's Characteristics.

Base station	Carrier frequency [MHz]	N_{ID}^{Cell}	Cellular provider
eNodeB	751	223	Verizon
gNB	872	872	AT&T

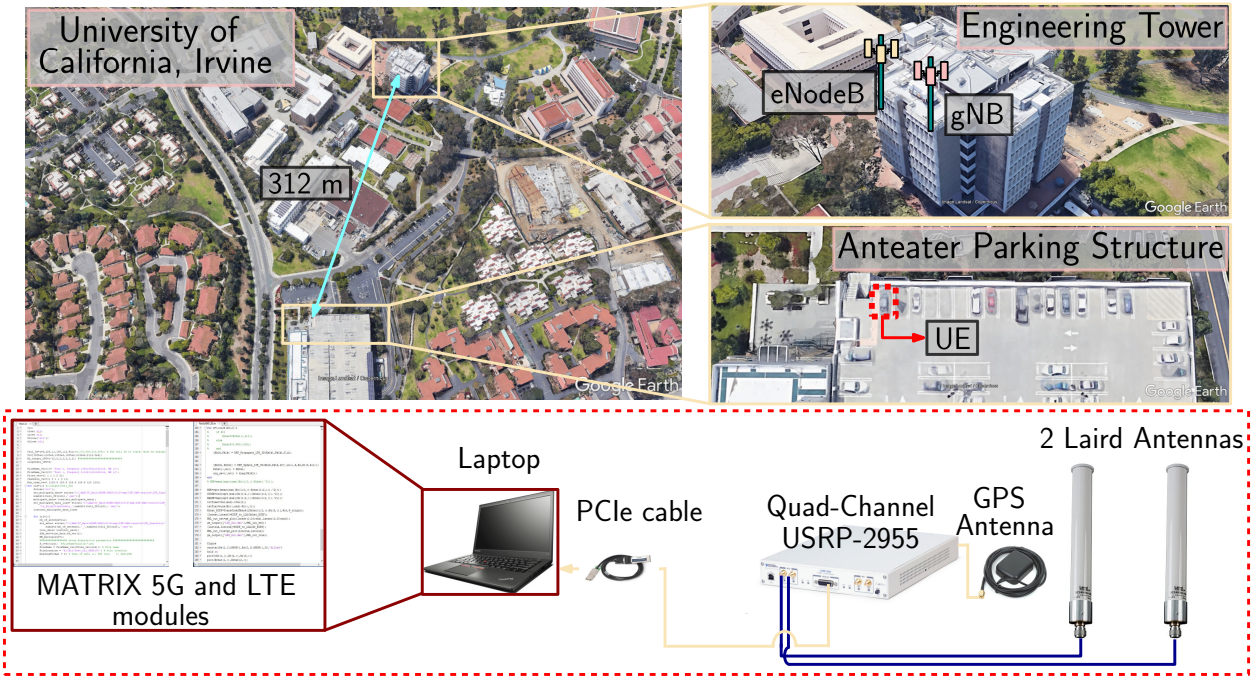


Figure 4.1: Environmental layout and experimental setup.

4.1.2.2 Results

The collected data over approximately 7970 seconds (around 2 hours and 13 minutes) encompassed 4G and 5G signals. These signals were analyzed post-processing using the SDR methodologies from [1] and this paper. The USRP-2955's clock was synchronized by a GPS-disciplined oscillator (GPSDO), meaning the observed Doppler frequencies mainly reflected the clock drifts in the eNodeB and gNB. The Allan deviation $\hat{\sigma}_A(\tau)$ and the corresponding

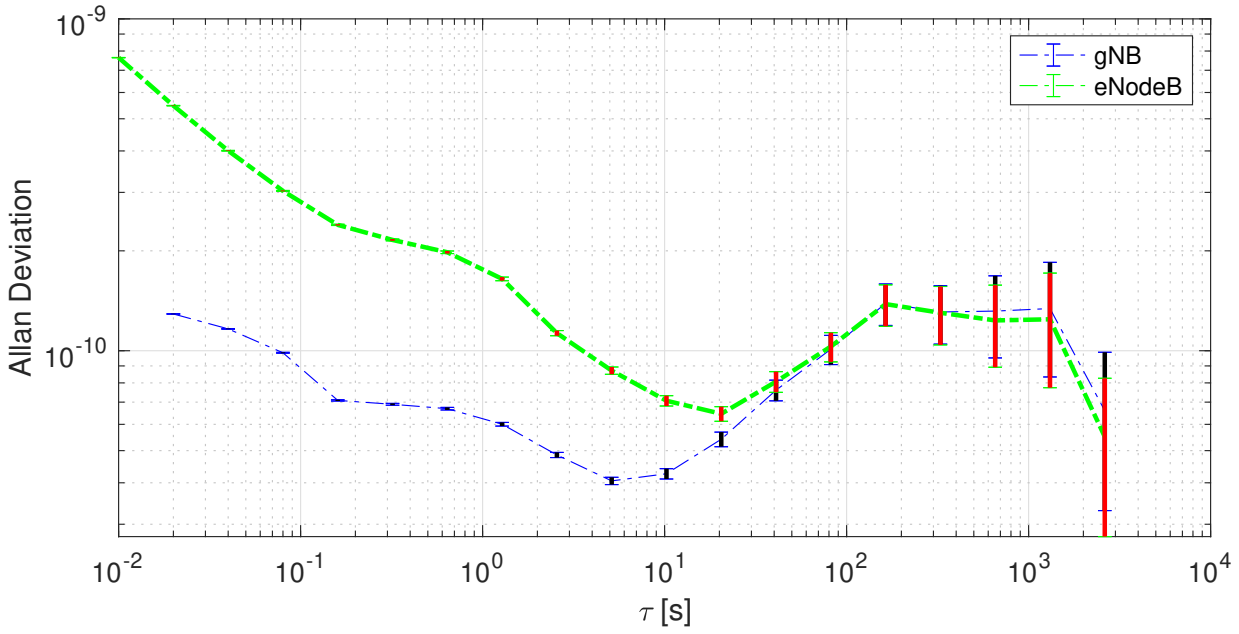


Figure 4.2: Allan deviations for collocated eNodeB and gNB at UCI.

error bound $\hat{e}_b$ were estimated as follows:

$$\hat{\sigma}_A(\tau) = \sqrt{\frac{0.5}{M_T - m} \sum_{i=0}^{M_T - m - 1} \left(f_{D_n}[(i+1)m] - f_{D_n}[(im)]\right)^2},$$

$$\hat{e}_b = \frac{\hat{\sigma}_A(\tau)}{M_T + 1},$$

where $m = \tau \cdot f_s$, $f_{D_n} = f_D / f_c$ is the normalized Doppler frequency, M_T is the total number of samples, m is the averaging factor in samples, τ is the averaging time, and f_s is the data rate. Figures 4.2 and 4.3 illustrate the Allan deviations and the normalized Doppler frequencies for both eNodeB and gNB. Notably, the gNB frequencies were more tightly confined within the bounds compared to the eNodeB, which had higher mean absolute deviation (MAD) magnitudes and more variations. This suggests greater stability in the gNB's clock. However, the Allan deviations for both systems' clocks still fell within the nominal range for an OCXO. Given past research showing promising positioning accuracies with 4G, these results indicate the potential of 5G for navigation, especially as mmWave infrastructure will likely employ more stable clocks, enhancing reliability for navigational use.

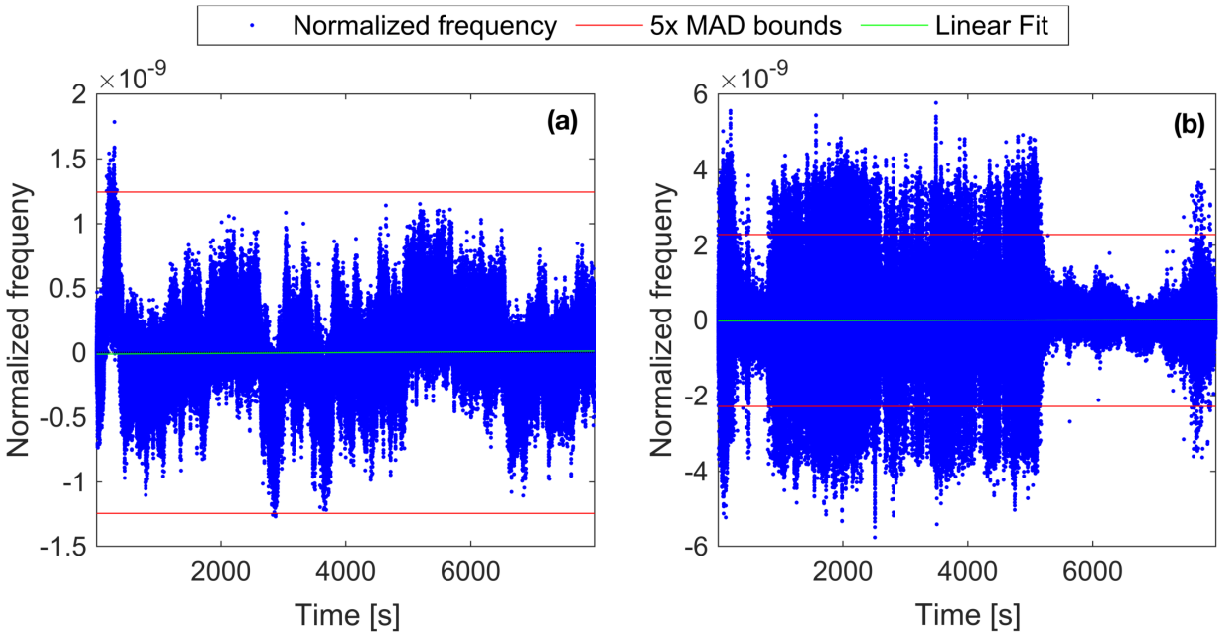


Figure 4.3: Normalized Doppler frequencies for gNB and eNodeB with MAD bounds.

4.2 Performance Evaluation of 4/5G Signal Reception in Varied Environments

This section evaluates a key metric for opportunistic navigation using 4/5G signals: the received C/N_0. The study focuses on several aspects: (i) the influence of various indoor structures and floor levels on the C/N_0 of 5G signals, (ii) the impact of receiver antenna quality, receiver's clock accuracy, and sampling rate on the C/N_0, and (iii) the relationship between the receiver's distance from the cellular node and the C/N_0.

4.2.1 Methodology

The assessment encompasses both 4G signals and 5G signals within FR1, where FDD is predominantly utilized by cellular providers for its advantages in coverage and latency. The C/N_0 of these signals is determined by tracking the 4G-URS and the 5G-USS using the SDR

described in Section 3.3. The C/N_0 is calculated as follows:

$$
\begin{aligned}
C/N_0 &= 10\log_{10}\left[\frac{\Delta f(C-\sigma_n^2)}{\sigma_n^2}\right], \\
C &= \max_t \{|\boldsymbol{h}(t)|\}, \\
\sigma_n^2 &= \frac{1}{\lceil \frac{3}{4}M\rceil - \lceil \frac{1}{4}M\rceil} \sum_{t_i=\lceil \frac{1}{4}M\rceil}^{\lceil \frac{3}{4}M\rceil} |\boldsymbol{h}(t_i)|^2,
\end{aligned}
$$

where Δf is the subcarrier frequency, C represents the carrier power, σ_n^2 is the noise power, $\boldsymbol{h}(t)$ is the estimated impulse response within the tracking loop of the navigation SDR, and M is the length of $\boldsymbol{h}(t)$. The symbol $\lceil\cdot\rceil$ denotes integer rounding towards $+\infty$.

4.2.2 Experimental Results

This section evaluates the signal power of sub-6 GHz 4/5G signals and their potential for opportunistic navigation in diverse environments. Three distinct scenarios are examined to compare the C/N_0 of 5G and 4G signals: (1) a stationary indoor scenario assessing the impact of walls and floors, (2) a stationary outdoor scenario examining the influence of sampling rate, antenna quality, and receiver clock accuracy, and (3) a mobile outdoor experiment to analyze the C/N_0 relative to the receiver's distance from cellular nodes.

4.2.2.1 Scenario 1: Stationary Indoors

This scenario investigates the C/N_0 of 4G and 5G signals within indoor environments.

4.2.2.1.1 Experimental Setup

In the first scenario, the C/N_0 of FR1-5G and 4G signals are characterized indoors, where the effect of wall and floor partitions are studied. To this end, 5G and 4G signals were collected over durations of five minutes at 14 different locations in the Engineering Gateway building at the University of California, Irvine (UCI), USA. Out of the 14 locations, 12 are labeled with a number and a letter according to "ij", where $i \in \{1, 2, 3, 4\}$ corresponds to the floor number and $j \in \{a, b, c, d, e, f\}$ corresponds to a building area. The remaining two locations are labeled "bridge" (an indoor bridge with glass walls on the 3-rd floor connecting the two buildings) and "elevator" (an elevator in the middle of the building which was going up and down between floors 1 and 4 during data collection). At each location, signals from two U.S. cellular providers were received: T-Mobile and AT&T, transmitting at four different frequencies in total, as summarized in Table 4.2. Both gNB1 and eNodeB1 were located on top of the Engineering Tower building on the UCI campus. In addition to being from the same operator, gNB2 and eNodeB2 have the same cell ID. As a result, they are most likely co-located; however, their exact locations are not known. The receiver was equipped with four omnidirectional, low-grade (LG), magnetic mount antennas connected to a quad-channel NI USRP-2955R to simultaneously down-mix and synchronously sample signals at the four carrier frequencies with a sampling rate of 10 Msps. The signals were processed in a post-processing fashion using the proposed 4/5G SDR in Section 3.3. Figure 4.4 shows the environment layout in which the experiment was performed, the eNodeBs' and gNBs' positions from which signals were collected, and the experimental hardware and software setup.

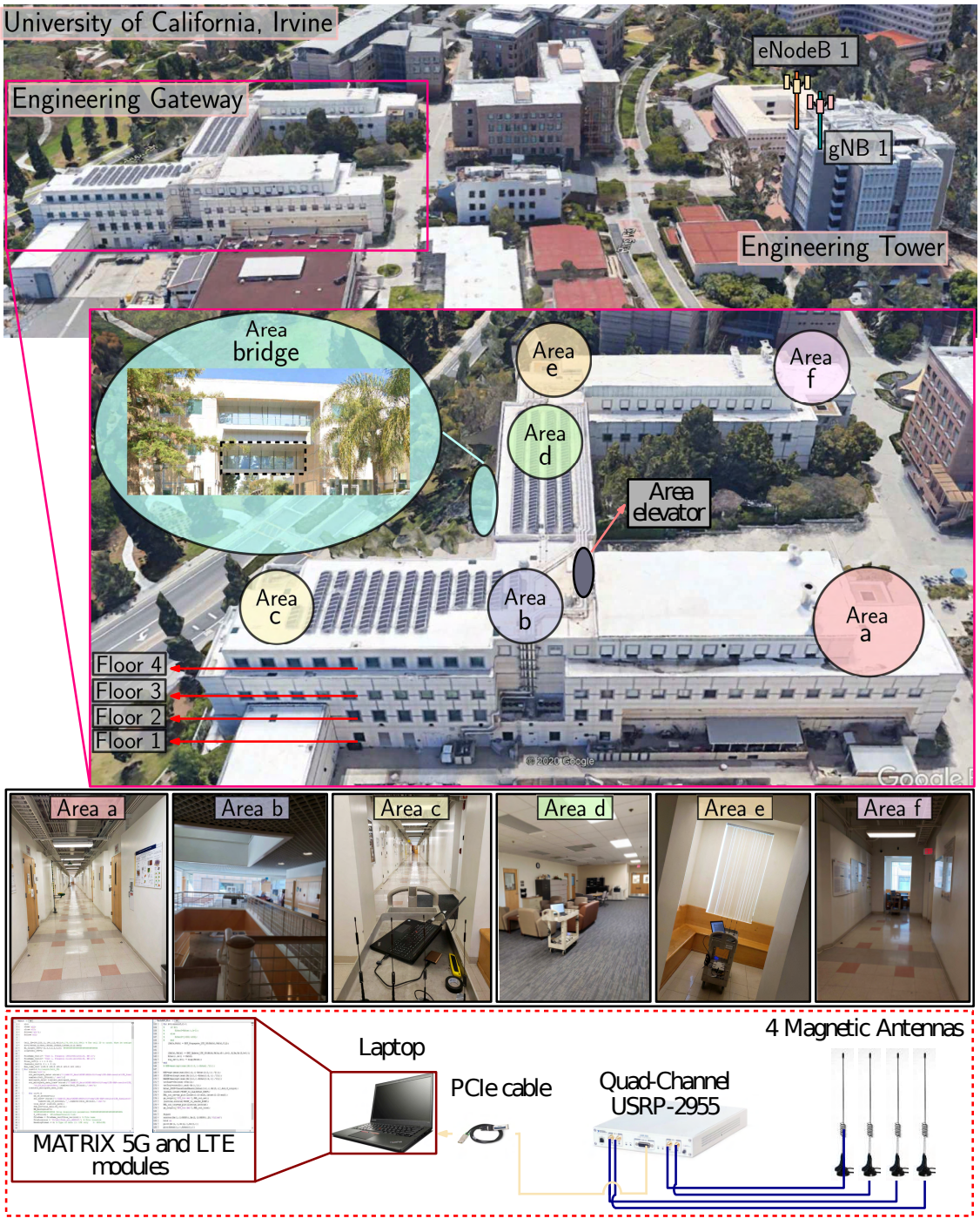


Figure 4.4: Environment layout and hardware and software setup of scenario 1. Map data: Google Earth.

Table 4.2: Indoor C/N_0 Assessment: eNodeB's and gNB's Characteristics.

Base station	**Carrier frequency [MHz]**	N_{ID}^{Cell}	**Cellular provider**
gNB 1	872	872	AT&T
gNB 2	632.55	394	T-Mobile
eNodeB 1	739	93	AT&T
eNodeB 2	731.5	394	T-Mobile
eNodeB 3	751/2125	221	T-Mobile

4.2.2.1.2 Experimental Results

The measured C/N_0 at each location for the BSs listed in Table 4.2 is shown in Figure 4.5. A summary of the minimum, maximum, average, and standard deviation of C/N_0 values at each site is presented in Figure 4.6. Key observations include:

1. Both 4G and 5G signals from the providers exhibited similar C/N_0 across different locations, indicating comparable navigational accuracy.

2. No clear trend in C/N_0 was observed across floors or areas. This conclusion is surprising and implies that a uniform navigation performance is expected throughout the entire building.

3. Despite metal elevator walls, signal strength inside the elevator was unexpectedly high, indicating that receivers in motion within the building can maintain signal tracking without the need to perform re-acquisition.

4.2.2.2 Scenario 2: Stationary Outdoors

In this scenario, the effect of sampling rate, antenna grade, and receiver clock quality on the C/N_0 is studied.

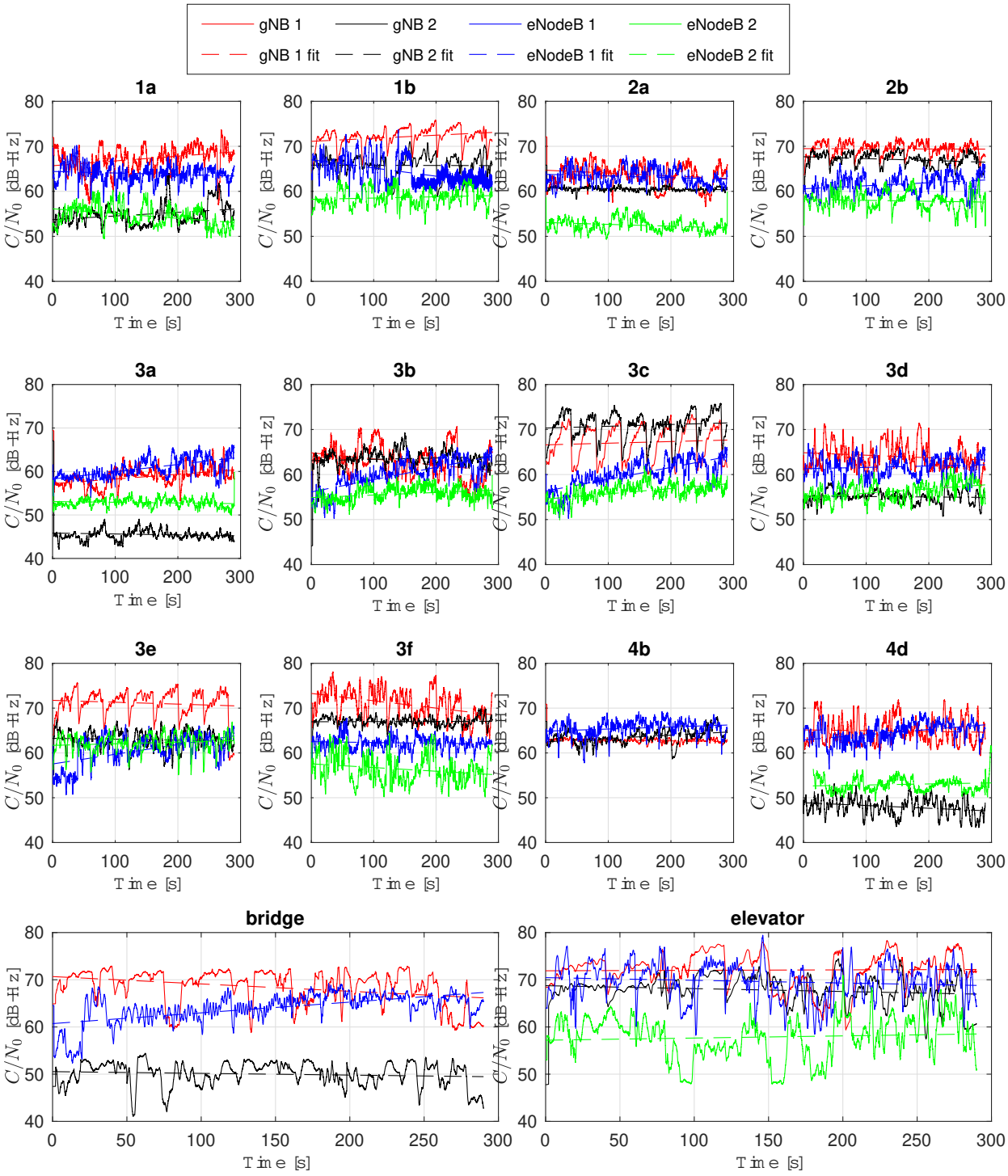


Figure 4.5: Experimental results of scenario 1 showing the C/N_0 values of the 2 gNBs and eNodeBs 1 & 2 from Table 4.2 in different locations in the Engineering Gateway building on UCI campus.

Area	gNB 1				gNB 2				eNodeB 1				eNodeB 2			
	Min	Max	Avg	Std	Min	Max	Avg	Std	Min	Max	Avg	Std	Min	Max	Avg	Std
1a	57.0	73.7	67.2	2.8	50.3	67.9	54.9	2.6	57.0	70.2	63.9	2.0	49.4	60.3	54.6	2.3
1b	64.6	75.8	72.1	2.0	54.8	71.0	65.8	2.6	58.1	73.7	64.4	3.0	52.7	63.1	58.6	1.9
2a	56.6	72.1	63.8	2.6	58.3	65.8	60.6	0.6	57.7	68.0	63.2	1.8	49.3	59.8	52.5	1.4
2b	63.7	72.2	69.4	1.5	60.5	69.8	67.1	1.6	56.2	66.3	61.5	2.0	51.9	62.9	57.9	2.0
3a	53.2	69.4	58.8	2.2	42.1	67.1	45.5	2.1	54.0	66.2	60.7	2.2	49.9	59.8	52.8	1.0
3b	54.2	70.7	62.9	3.6	44.1	69.3	63.5	2.3	50.2	66.2	60.1	3.1	51.1	59.8	55.7	1.6
3c	59.9	73.3	67.1	3.8	61.9	75.8	70.9	2.9	50.7	66.4	60.4	3.2	49.9	61.9	56.2	1.8
3d	57.1	71.4	64.0	2.7	50.7	58.5	55.1	1.3	54.0	66.9	61.7	2.3	51.2	61.7	56.3	2.0
3e	58.4	75.7	71.1	3.0	55.1	67.6	63.0	2.0	50.7	66.4	60.7	3.3	55.1	66.9	62.2	2.0
3f	62.3	78.1	70.9	3.2	61.0	69.9	67.0	1.1	57.8	67.8	62.2	1.5	50.1	64.5	56.4	3.1
4b	61.3	70.9	62.8	0.8	58.7	68.1	63.6	1.6	57.8	69.2	65.5	1.8	NA	NA	NA	NA
4d	59.4	71.9	64.9	2.8	43.4	53.1	48.0	2.0	56.4	69.2	64.6	2.1	49.2	61.9	53.0	1.8
Bridge	58.8	72.9	68.4	3.7	41.0	54.5	50.0	2.5	52.3	69.2	64.0	3.1	NA	NA	NA	NA
Elevator	59.4	78.2	72.0	3.6	47.8	74.5	67.9	3.3	58.2	79.5	69.6	3.8	49.9	71.0	57.9	4.4

Figure 4.6: Summarized tabulated results of the C/N_0 values of the eNodeBs and gNBs indoors.

4.2.2.2.1 Experimental Setup

The receiver was placed on the roof of the Anteater parking structure on UCI campus, 300 m away from gNB1 and eNodeB1 with direct LOS. The hardware setup is similar to that of the stationary indoors setup in scenario 1, except that two of the omnidirectional LG antennas were replaced by two high-grade (HG) 10 Watts, omnidirectional Laird antennas with a gain of 1.5 dBi. The antennas were connected to the same USRP mentioned in the previous setup to simultaneously down-mix and synchronously sample signals at the four carrier frequencies, which are then post-processed by the proposed SDR in Section 3.3. The USRP's oscillator was operated in two modes: (i) a GPSDO (precise frequency standard) and (ii) free running internal oscillator (typical OCXO). Moreover, the signals were sampled at (i) 10 Msps and (ii) 20 Msps to study the effect of the sampling rate on the C/N_0. Figure 4.7 shows the experimental hardware and software setup.

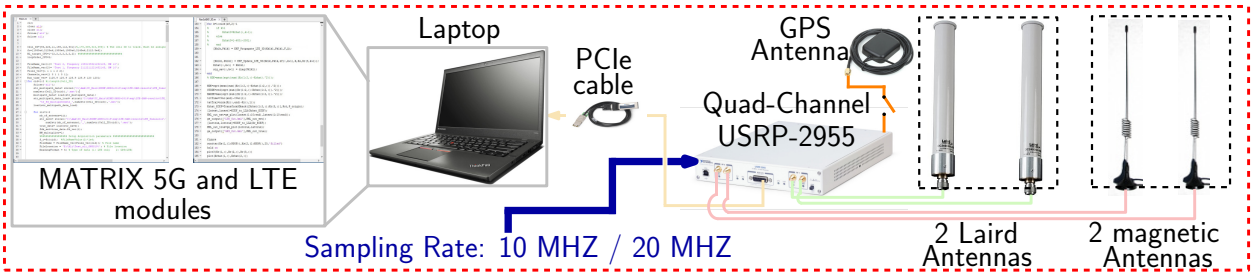


Figure 4.7: Hardware and software setup of scenario 2.

4.2.2.2.2 Experimental Results

The C/N_0 values of the 4G and 5G signals for different antenna grades, clock qualities, and sampling rates are shown in Figure 4.8. The following can be concluded from these plots:

- As expected, the C/N_0 values with the HG antenna are consistently 3–6 dB higher than that with the LG antenna. While these results imply that investing in a HG antenna (around $40 USD price difference) yields a 3–6dB gain in the C/N_0, which goes a long way in low signal-to-noise ratio (SNR) applications, it is also important to notice that the C/N_0 values with the LG antenna are mainly above 50 dB-Hz. Such C/N_0 is high enough to produce a reliable navigation solution. Similar values were obtained indoors with the LG antenna, as indicated in Figure 4.8.

- When operating with the GPSDO, the receiver produces stable values of C/N_0. When operating with the USRP's internal OCXO, the C/N_0 values are less stable initially but appear to stabilize around high enough C/N_0 values as time progresses. This implies that such signals are useful in GNSS-challenged environments (e.g., scenario 1 and in deep urban canyons) or in environments under spoofing or jamming attacks.

- There does not seem to be any noticeable gain in increasing the sampling rate from 10 Msps to 20 Msps, as the bandwidth of the 4G and 5G signals under study was 10 MHz.

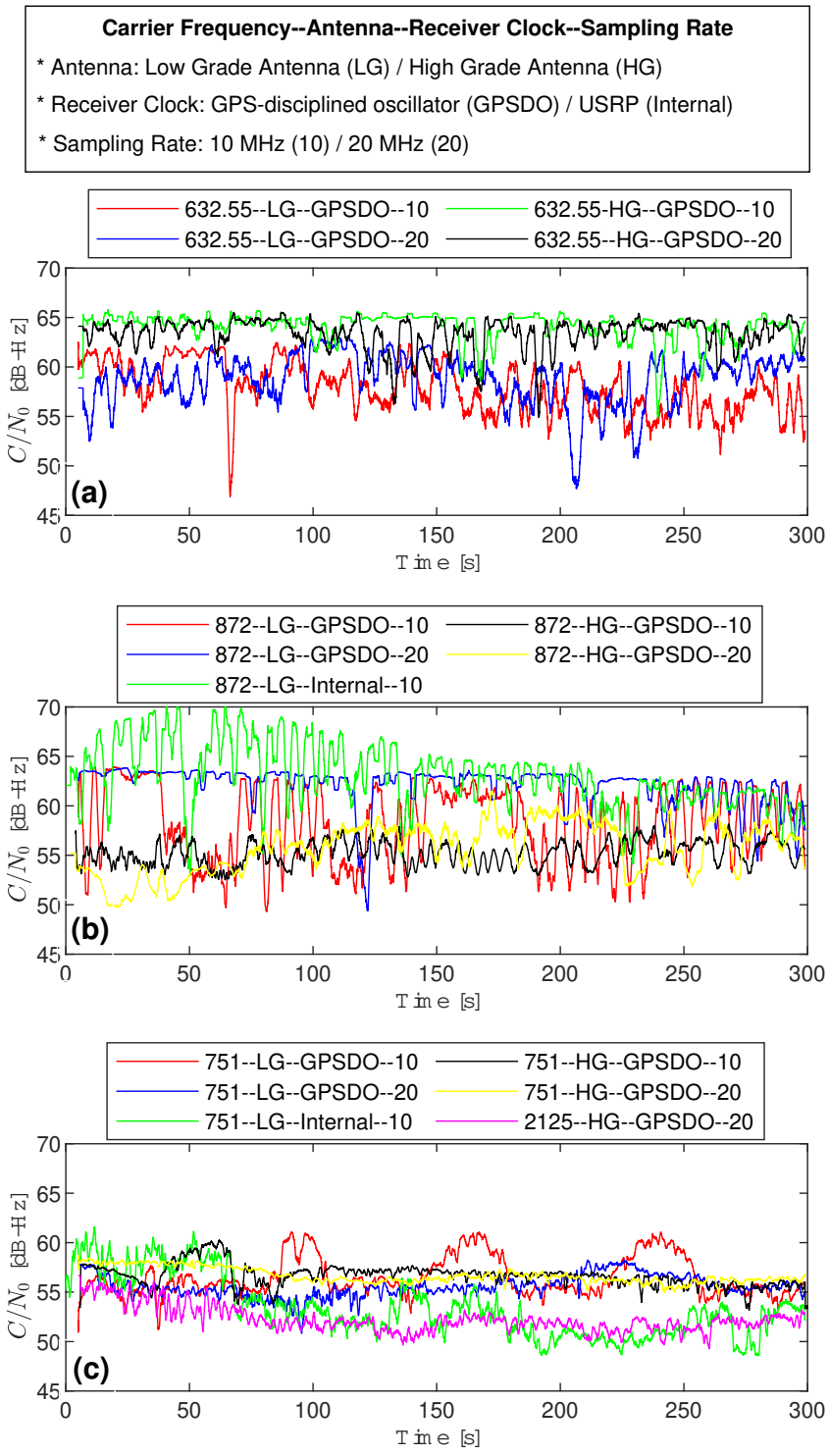


Figure 4.8: Experimental results of scenario 2 showing the C/N_0 values of gNBs 1 & 2 and eNodeB3 from Table 4.2 for a stationary outdoor receiver and for different antenna grade, receiver clock quality, and sampling rate.

4.2.2.3 Scenario 3: Mobile Outdoors

This scenario characterizes the C/N_0 as a function of the range r between the receiver and the gNB.

4.2.2.3.1 Experimental Setup

In this third scenario, the experiment was conducted on Fairview Road in Costa Mesa, California, USA. One of the HG Laird antennas was connected to the USRP, which was in turn mounted on a vehicle and tuned to listen to FR1-5G signals at an 872 MHz carrier frequency, which corresponds to the U.S. cellular provider AT&T. The gNB cell ID was 608 and its location was surveyed prior to the experiment. The USRP's GPSDO was used throughout this experiment. The vehicle was equipped with a Septentrio AsteRx-i V integrated GNSS-IMU whose x-axis pointed toward the front of the vehicle, y-axis pointed to the right side of the vehicle, and z-axis pointed upward. AsteRx-i V is equipped with a dual-antenna multi-frequency GNSS receiver and a VectorNav VN-100 micro-electromechanical system (MEMS) IMU. The loosely-coupled GNSS-IMU with satellite-based augmentation system (SBAS) navigation solution produced by AsteRx-i V was used as ground truth in this experiment. Figure 4.9 shows the environment layout and the experimental hardware and software setup.

4.2.2.3.2 Experimental Results

The C/N_0 was computed along the trajectory and plotted as a function of the range between the gNB and the receiver and is shown in Figure 4.10 along with a linear fit. The following can be concluded from this plot. While simple, the linear model seems to fit well the behavior of the C/N_0 in this semi-urban environment. Such models can be particularly

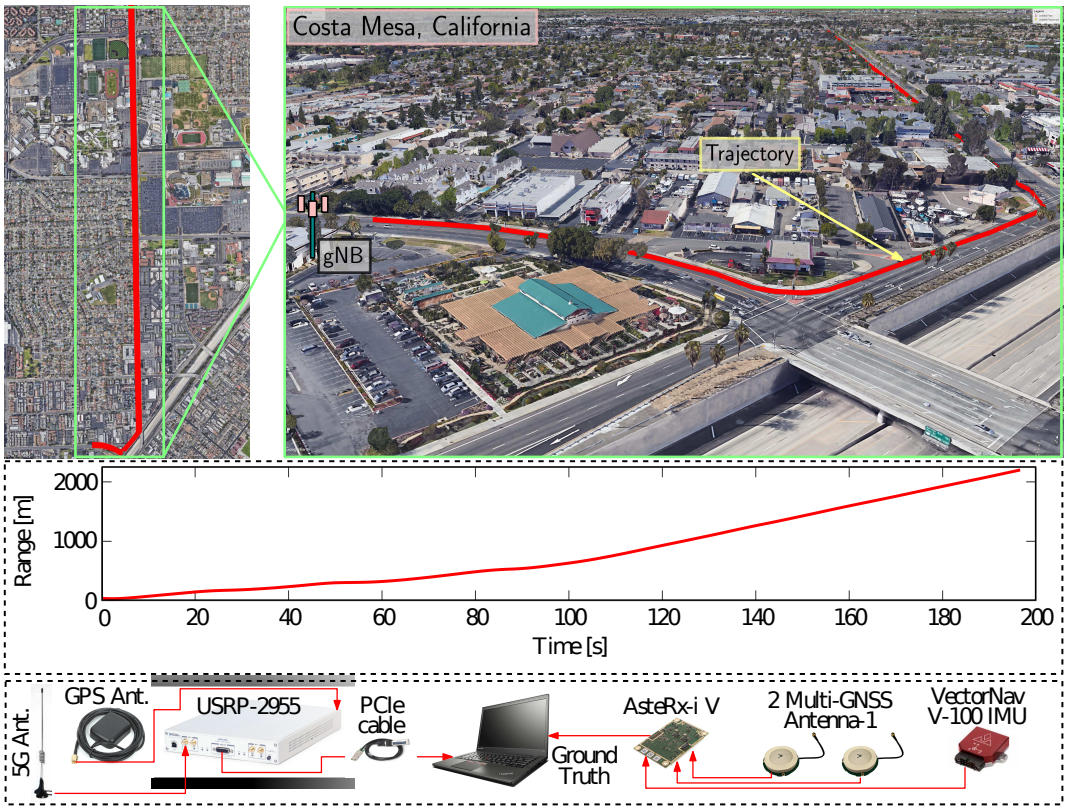


Figure 4.9: Scenario 3: environment layout, hardware and software setup, and the range between the ground vehicle-mounted receiver and the gNB over the entire experiment. Map data: Google Earth.

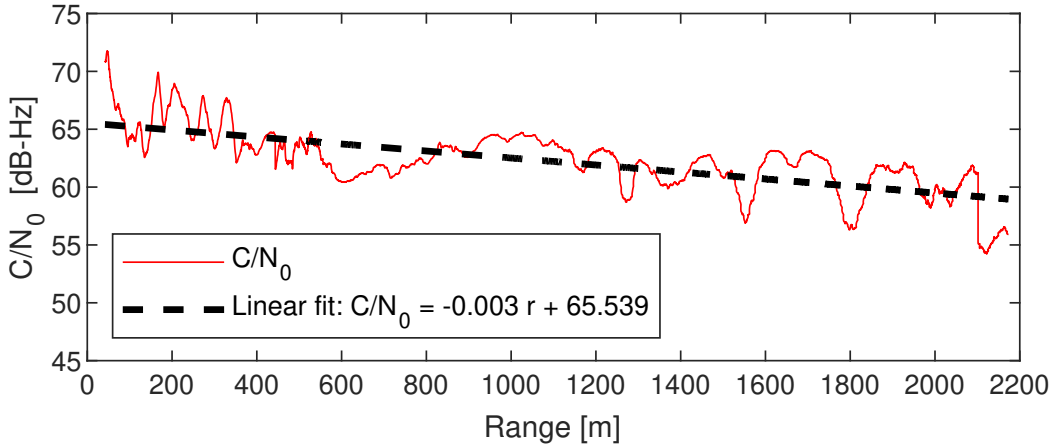


Figure 4.10: Experimental results of scenario 3 showing the C/N_0 values of a gNB in a semi-urban environment as a function of the range between the gNB and an outdoor mobile receiver mounted on a vehicle.

useful for navigation framework design and analyses. Moreover, the received 5G signals are surprisingly powerful at more than 55 dB-Hz beyond 2 km, which is a typical cell size in semi-urban environments. This result implies that the receiver could reliably track signals from numerous 5G gNBs, which directly improves the navigation performance.

Chapter 5

Navigation Performance

This chapter is structured to provide a detailed exploration of various navigation scenarios. Section 5.1 demonstrates the navigation capabilities of a ground vehicle using the proposed 4G receiver under a real-world GPS-denied environment. Section 5.2 details a pioneering experiment where 4G signals are utilized for navigation in high-altitude aircraft environments, covering aspects such as signal strength, eNodeB availability, the influence of aircraft maneuvers on signal reception, and overall navigation performance. Section 5.3 showcases an experimental validation of the proposed 5G receiver in a ground vehicle, navigating a suburban area using sub-6 GHz 5G signals from two gNBs. Lastly, Section 5.4 describes an experiment featuring the proposed 5G receiver on a UAV, assessing its navigation capabilities in an urban setting.

5.1 4G – Ground Vehicle Scenario in a Real GPS-Jamming Experiment

This section presents an experimental demonstration of the proposed 4G receiver mounted on a ground vehicle navigating in a real-world GPS-denied environment. A mapping campaign was conducted before the experiment to locate 4G eNodeBs in the environment. The vehicle was driven in the Mojave Desert at Edwards Air Force Base (AFB), California, USA, during the intentional GPS jamming exercises, known as NAVFEST. The vehicle's trajectory was composed of three segments: (A) GPS signals were available (0–40 seconds; 1.1 km), (B) GPS signals were intermittent (40–50 seconds; 0.4 km), and (C) GPS signals were not available (50–180 seconds; 3.5 km).

5.1.1 Environmental Layout and Hardware Setup

Six high-power jammers and one portable box jammer were spread over an area of approximately 50 miles north of Edwards AFB. Figure 5.1 shows the jamming-to-signal ratio J/S heatmap; which actually extends outside the depicted rectangle; however, this was the only data provided by Edwards AFB.

The ground vehicle, shown in Figure 5.1, was equipped with an NI-USRP-2955, two consumer-grade Laird cellular antennas, PCIe cable, laptop, and a Septentrio GNSS-IMU system, comprising a multi-frequency GNSS AsteRx-i V receiver, an industrial-grade Vectornav VN-100 MEMS IMU, and a dual-GNSS antenna system. The vehicle-mounted GNSS-IMU was used to obtain the vehicle's ground truth trajectory, utilizing signals from non-jammed GNSS constellations (Galileo and GLONASS). The USRP utilized a GNSS-disciplined oscillator (GNSSDO) and was tuned to listen to two carrier frequencies corresponding to the U.S.

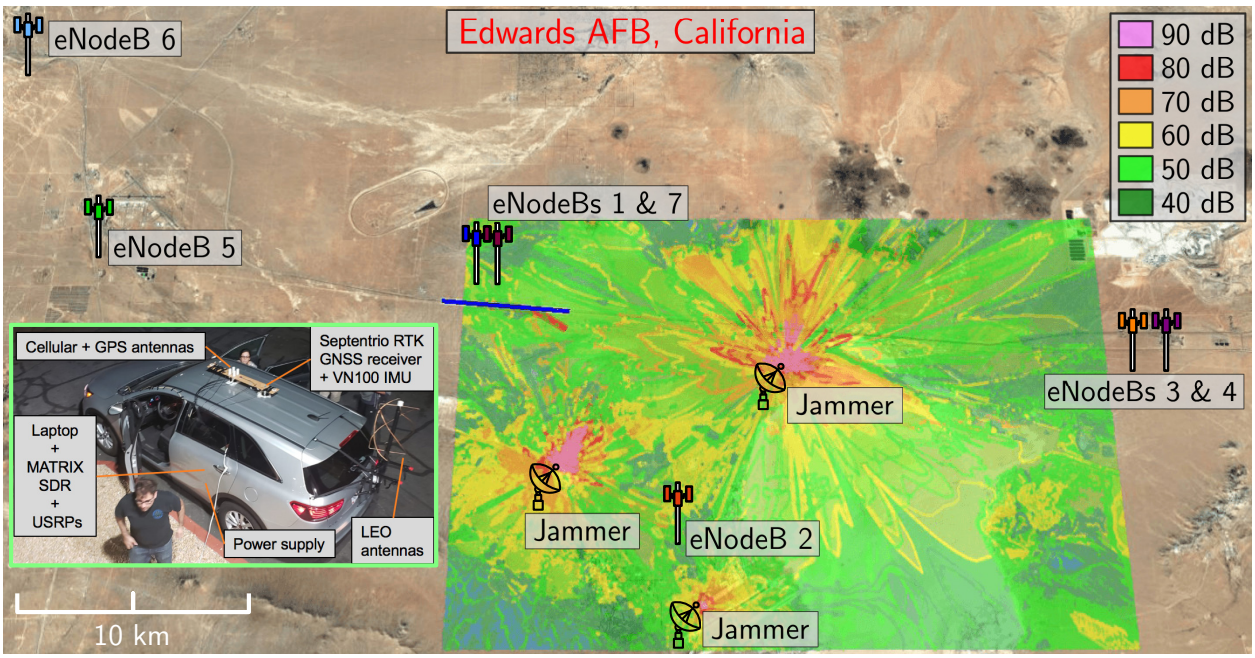


Figure 5.1: Environment layout and jamming-to-signal ratio J/S heatmap. The ground vehicle's trajectory is within the dashed white rectangle.

Table 5.1: Ground Vehicle Navigation in a Jamming Experiment: eNodeBs' Characteristics.

eNodeB	Carrier frequency	Cell ID	Cellular provider
1	751 MHz	417	Verizon
2	751 MHz	399	Verizon
3	751 MHz	393	Verizon
4	751 MHz	402	Verizon
5	2145 MHz	186	T-Mobile
6	2145 MHz	195	T-Mobile
7	2145 MHz	489	T-Mobile

cellular providers: Verizon Wireless and T-Mobile, as tabulated in Table 5.1.

5.1.2 Receiver Output: Tracking Results

The receiver discussed in Section 3.3 was used to acquire and track signals from 7 4G eNodeBs (see Figure 5.1). A second-order PLL with a noise-equivalent bandwidth of 6 Hz was employed to track the carrier phase, and a carrier-aided DLL whose loop filter is a simple

gain $K = 0.2$ was used to track the code phase.

Figure 5.2 shows the code phase tracking error. From Table 5.1 and Figure 5.2, it can be inferred that the receiver was able to track 4G signals at 751 MHz and 2145 MHz, with the tracking loops failing to track as the receiver drove further away from the eNodeBs. It is worth noting that not all seven eNodeBs were continuously tracked along the entire trajectory. In particular, while eNodeBs 1, 2, and 7 were continuously tracked along the receiver's trajectory, eNodeBs 5 and 6 were tracked during the earlier part of the trajectory, while eNodeBs 3 and 4 were tracked during the latter part of the trajectory.

Figure 5.3 shows the tracking results: (i) CNR, (ii) pseudorange estimates versus expected ranges (the latter calculated from the receiver's ground truth trajectory and eNodeBs' positions), and (iii) range error (i.e., the difference between pseudorange and range). The CNR is calculated from CNR $= \frac{P_r - N0}{N_0 T}$, where P_r, N_0, and T denote the received signal power, noise power, and subaccumulation time interval, which is set to the 4G frame duration.

From Figure 5.3(a), it can be seen that the CNR for tracked eNodeBs is about 50 dB-Hz, with some of the closer eNodeBs having a CNR exceeding 75 dB-Hz. The intermittency in tracking is due to the receiver tracking loops failing to acquire/track all eNodeBs along the entire trajectory. From Figure 5.3(b), it can be seen that eNodeBs 3 and 6 were tracked, while being 25.5 km and 23.6 km, respectively, away from the vehicle. The drift in the range error in Figure 5.3(c) is due to the combined receiver–eNodeB's clock error, which is dominated by the eNodeB's clock error, since the receiver possessed a GNSSDO. These drifts are indicative of the eNodeBs being equipped with high-quality OCXOs. The correlation observed among some of the eNodeBs could be due to the "loose" network synchronization: eNodeBs need to be synchronized, as per the 3GPP standards, with certain eNodeBs tend to exhibit tighter synchronization, forming so-called "clusters" [103]. It is worth noting in Figure 5.3(c) starting segment (C), which is when GPS signals become completely unavailable, there seems to be an "inflection" point impacting the range error. It is speculated that this is due to the

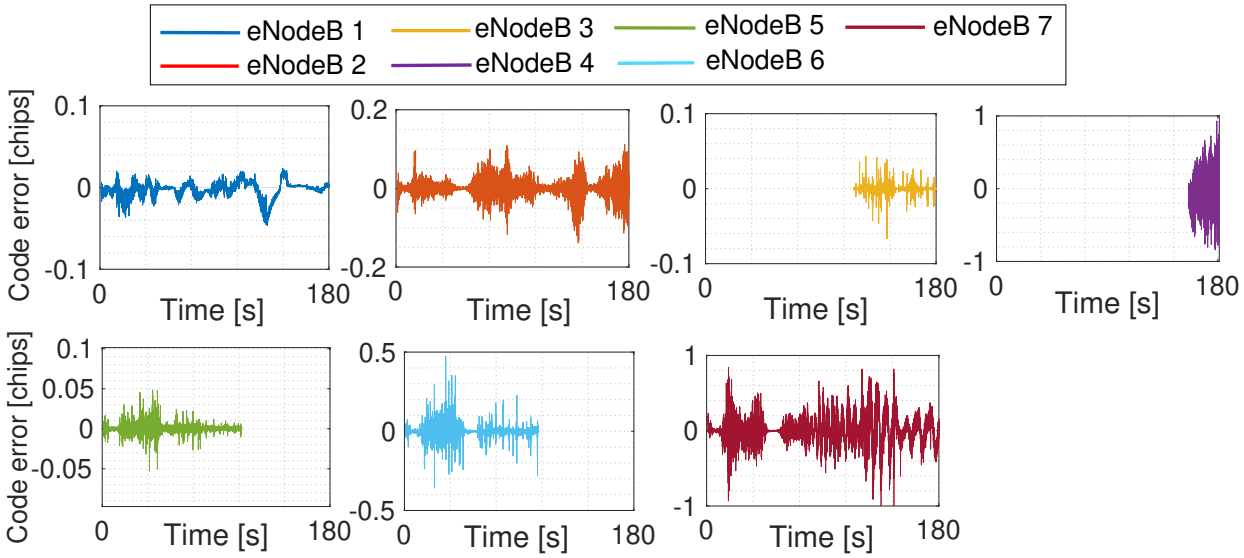


Figure 5.2: Cellular 4G code phase tracking error results.

jamming impact on eNodeBs' clocks; however, it is difficult to assert such a statement.

5.1.3 Navigation Solution

The extracted carrier-aided code-phase pseudorange measurements were fused in an EKF to estimate the receiver's 3-D position $\boldsymbol{r}_r$ and velocity $\dot{\boldsymbol{r}}_r$, and relative clock bias and drift between the receiver's and eNodeBs' clocks denoted by $\{\delta t_r - \delta t_{s,u}\}_{u=1}^{7}$ and $\left\{\dot{\delta t}_r - \dot{\delta t}_{s,u}\right\}_{u=1}^{7}$, respectively. The EKF state vector can be expressed as

$$\boldsymbol{x} \triangleq \left[\boldsymbol{x}_r^{\mathsf{T}}, \boldsymbol{x}_{\text{clk}}^{\mathsf{T}}\right]^{\mathsf{T}}, \tag{5.1}$$

where $\boldsymbol{x}_r = \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}\right]$ and $\boldsymbol{x}_{\text{clk}}$ is the clock state vector. As observed in [104], and due to high vertical dilution of precision when using terrestrial eNodeBs alone, the vertical estimation error was much higher than horizontal errors. As such, 2-D navigation errors are reported and compared with those achieved in [104], in which the conventional state-of-the-art frequency-domain 4G receiver discussed in Subsection 3.1.1 was deployed. For this purpose, the receiver is assumed to move in a 2-D plane with a constant known height

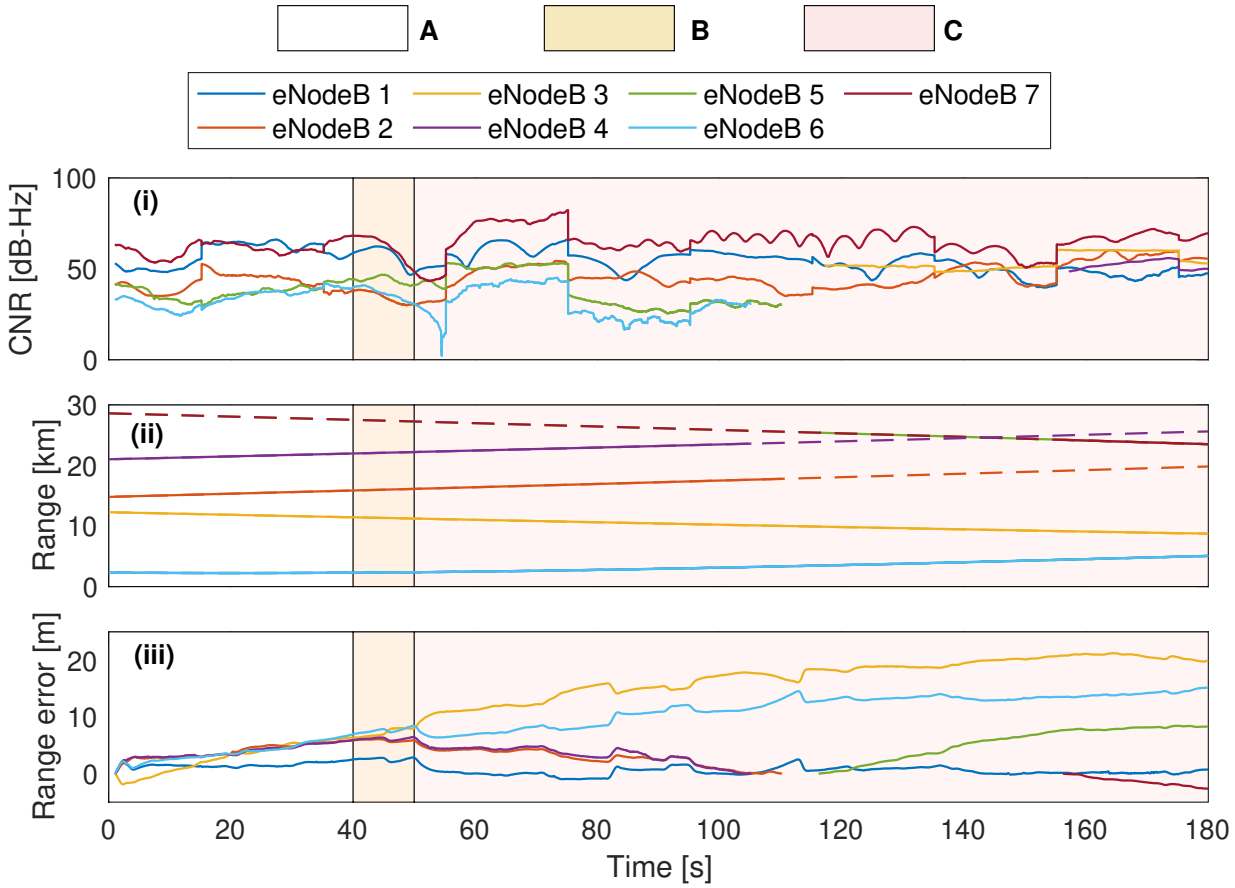


Figure 5.3: Cellular 4G tracking results: (i) CNR, (ii) pseudorange estimates in solid lines versus expected ranges in dashed lines (after removing the initial biases), and (iii) range error.

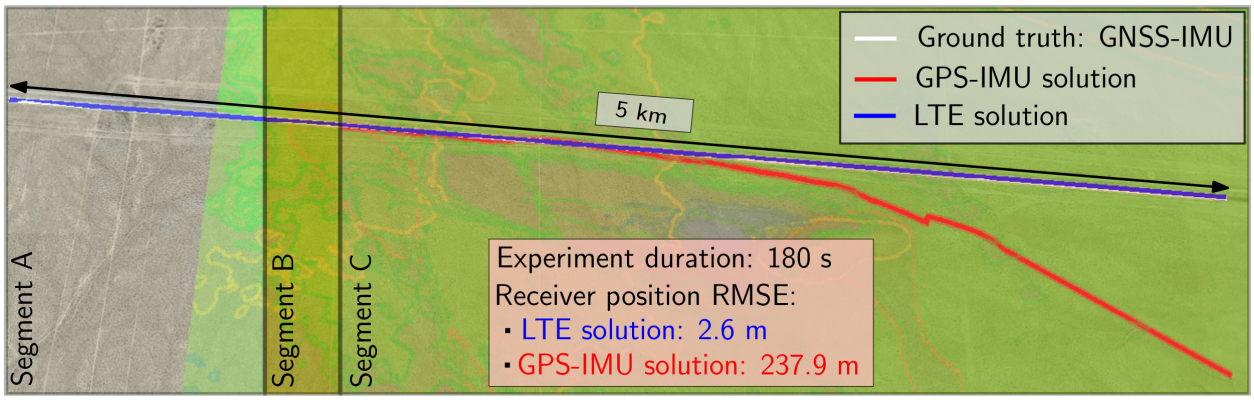


Figure 5.4: Navigation solutions of GNSS-IMU, GPS-IMU, and cellular 4G. Map data: Google Earth.

$z_r \equiv z_0$. The receiver's motion is assumed to evolve according to the white noise acceleration model discussed in Subsection 2.3.1. The clock state vector $\boldsymbol{x}_{\text{clk}}$ is defined as $\boldsymbol{x}_{\text{clk}} \triangleq \left[c\Delta\delta t_1, c\Delta\dot{\delta} t_1, \cdots, c\Delta\delta t_U, c\Delta\dot{\delta} t_U\right]^{\mathsf{T}}$. The clock error dynamics are assumed to evolve according to the discrete-time dynamics discussed in Section 2.4. In this experiment, the receiver was assumed to be equipped with a typical TCXO, while the eNodeBs are assumed to be equipped with a typical OCXO for the experimental values as depicted in Table 2.4. The measurements noise variances were chosen according to the models described in [104], which when using the expressions relating CNR to measurement noise variances [1], the variances were found to vary between 0.2 – 22 m^2.

After traversing a trajectory of 5 km in 180 seconds, a 2-D position RMSE of 2.6 m and a 2-D maximum error of 4.5 m were achieved using only 4G signals, without using other sensors (see Figure 5.4). This unprecedented accuracy is an order of magnitude lower than previously published results in the same environment and the same collected raw 4G in-phase and quadrature samples, in which a 2-D position RMSE of 29.4 m was achieved [104]. While the state-of-the-art receiver in [104] was only able to acquire and track the 5 km-away eNodeB 1, the proposed receiver acquired and tracked weaker signals from eNodeBs 2–6. The GPS-IMU navigation solution exhibited a position RMSE of 237.9 m.

5.2 4G – High-Altitude Aircraft Scenario

This section delves into evaluating the availability, signal strength, and navigation performance of cellular 4G signals at high altitudes, marking the first exploration of cellular signals for navigation in high-altitude aircraft environments. The research was propelled by an innovative aerial campaign in March 2020, a collaborative endeavor between the Autonomous Systems, Perception, Intelligence, and Navigation (ASPIN) laboratory and the United States Air Force (USAF) at Edwards AFB in California, USA. Dubbed "SNIFFER: Signals of opportunity for Navigation In Frequency-Forbidden EnviRonments," this week-long flight campaign aimed to capture ambient cellular 4G signals across the Southern California region using a USAF Beechcraft C-12 Huron, a fixed-wing aircraft.

The campaign sought to address several critical questions:

1. The feasibility of receiving and utilizing cellular 4G signals at aircraft altitudes and speeds for robust navigation solutions.
2. The impact of cellular BS antenna tilt on reliable signal reception at high altitudes.
3. The availability of a sufficient number of detectable cellular BSs for sustained navigation over extensive high-altitude trajectories.
4. The potential navigation accuracy achievable exclusively with cellular 4G signals in high-altitude aircraft scenarios.

To answer these questions, the following aspects are thoroughly examined: (i) the hardware setup for signal collection, (ii) specific flight regions and aircraft maneuvers during the campaign, (iii) data processing methodologies, (iv) characterization of 4G signals at high altitudes, (v) performance of the proposed receiver's, and (vi) overall navigation performance.

5.2.1 Hardware Setup

The equipment, prepared at the ASPIN Laboratory, was meticulously assembled on a specialized rack provided by the USAF and then shipped for installation on the C-12 aircraft. The rack's configuration included:

1. A quad-channel NI-USRP-2955 for signal reception and processing.
2. A desktop computer outfitted with a 1 terabyte (TB) solid-state drive, designated for data storage.
3. A laptop computer set up for real-time 4G signal acquisition. During flights, a flight engineer operated this system to actively monitor and identify available cellular 4G channels. This information was crucial to appropriately adjust the USRP-2955's tuning. The laptop was interfaced with the USRP-2955 through a PCIe cable.
4. A GPS antenna that served dual purposes: firstly, to provide GPS measurements for the aircraft's navigation system, and secondly, to discipline the onboard GPSDO of the USRP.

Additionally, three consumer-grade 800/1900 MHz Laird cellular antennas were affixed to the underside of the C-12, establishing a direct connection to the USRP-2955. This setup enabled the USRP to tune into three distinct carrier frequencies, each corresponding to major U.S. cellular providers: T-Mobile, AT&T, and Verizon. The experiment was conducted with each cellular channel being sampled at a rate of 10 Msps. Subsequently, the collected data was processed using the proposed 4G SDR. Figure 5.5 shows the hardware setup with which the C-12 aircraft was equipped

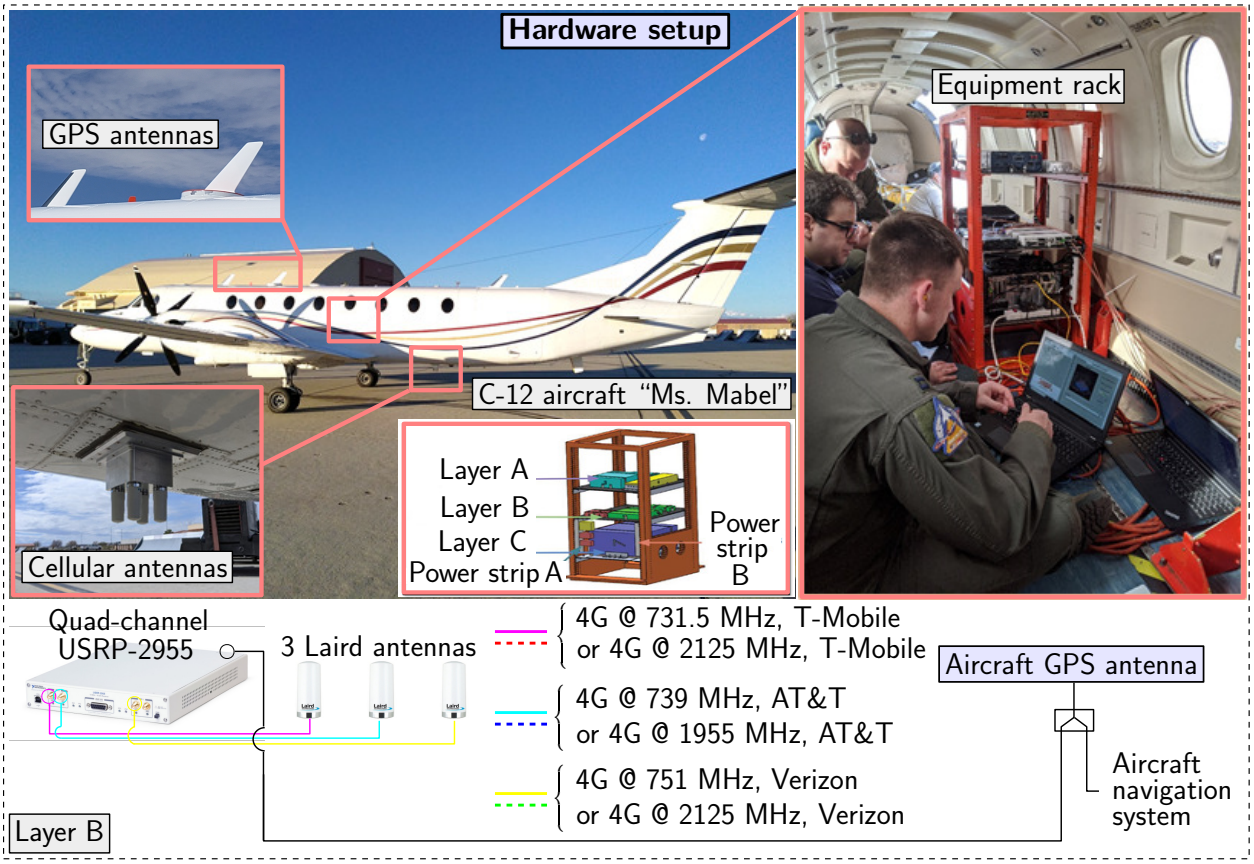


Figure 5.5: Hardware setup with which the C-12 aircraft was equipped.

5.2.2 Flight Regions and Aircraft Maneuvers

A comprehensive flight campaign was executed over four consecutive days, focusing on the collection of 4G signal samples for subsequent post-processing. This extensive campaign resulted in the accumulation of terabytes (TBs) of data across 65 individual flight runs, creating a unique dataset. This dataset predominantly features signal samples from 55 flight runs conducted over two distinct regions: (i) Region A, characterized as a rural area within Edwards AFB in California, and (ii) Region B, a semi-urban region in Palmdale, California. Figure 5.6 illustrates these specific regions where the experimental flights took place.

In the course of this campaign, more than 200 4G eNodeBs were methodically mapped using the procedure outlined in [105]. To ensure accuracy and completeness, the identified eNodeB locations were cross-verified using Google Earth and relevant online databases. These verified eNodeB positions are depicted as orange pins in Figure 5.6, providing a visual representation of the extensive coverage and distribution of the cellular towers encountered during the experimental flights.

The C-12 flew with altitudes up to 23,000 ft above ground level (AGL) and performed two types of maneuvers to test several aspects of aircraft navigation with cellular SOPs. The first type was a climbing/descending teardrop-like pattern. These patterns were used to characterize eNodeBs availability versus altitude, C/N_0, and multipath interference. The second was a grid-like pattern with many turns and straight elements. These patterns were used to stress-test the proposed 4G navigation receiver's tracking loops. Figure 5.7 illustrates the maneuvers, where the "geographic point of interest" refers to the "center" of the climbing/descending teardrop, which the aircraft flew through as it ascended/descended vertically in order to assess the received signals as a function of altitude.

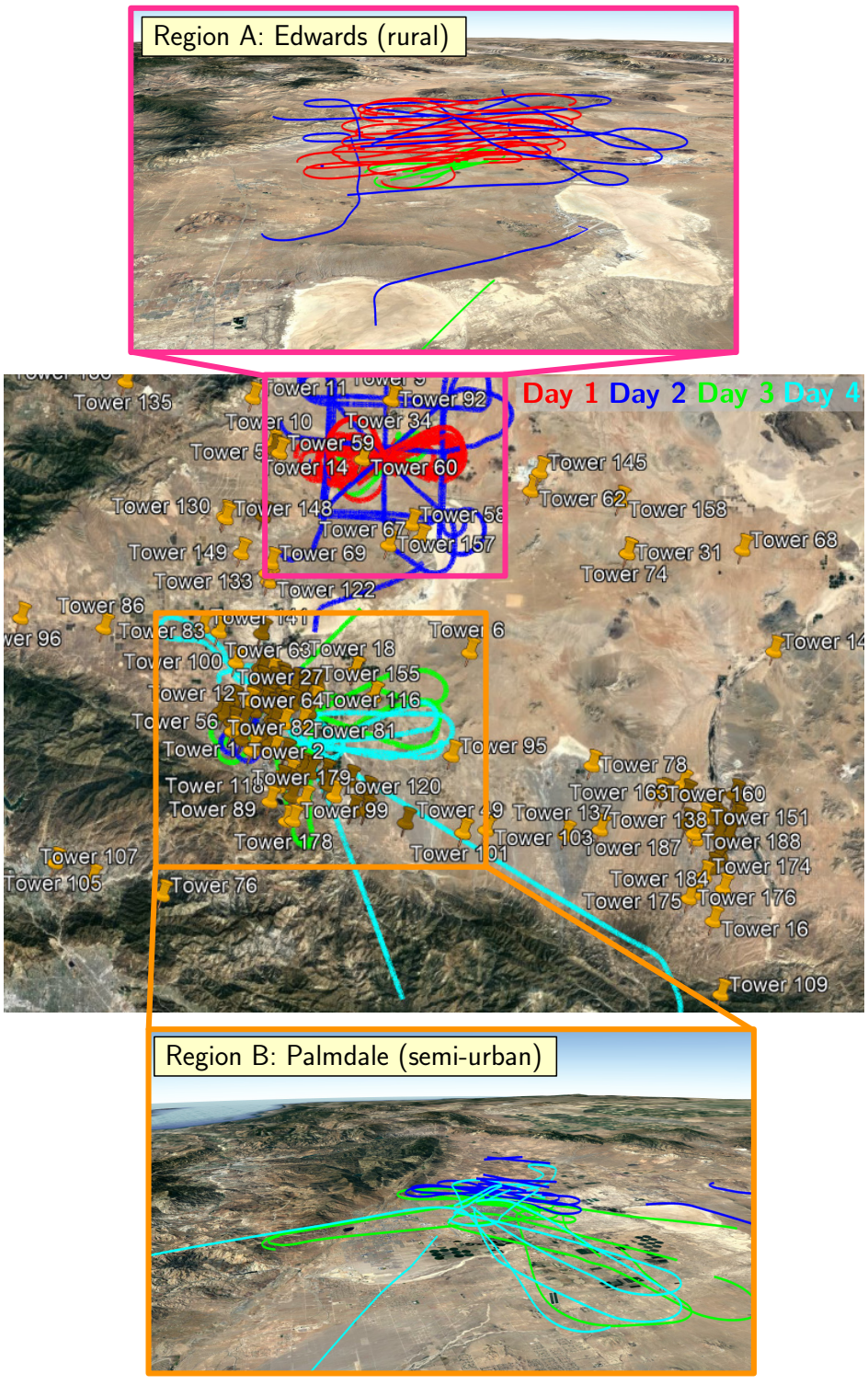


Figure 5.6: Regions A and B in Southern California, USA, over which the flight campaign took place. The orange pins represent cellular 4G towers. The flight trajectories over the four days are shown in different colors.

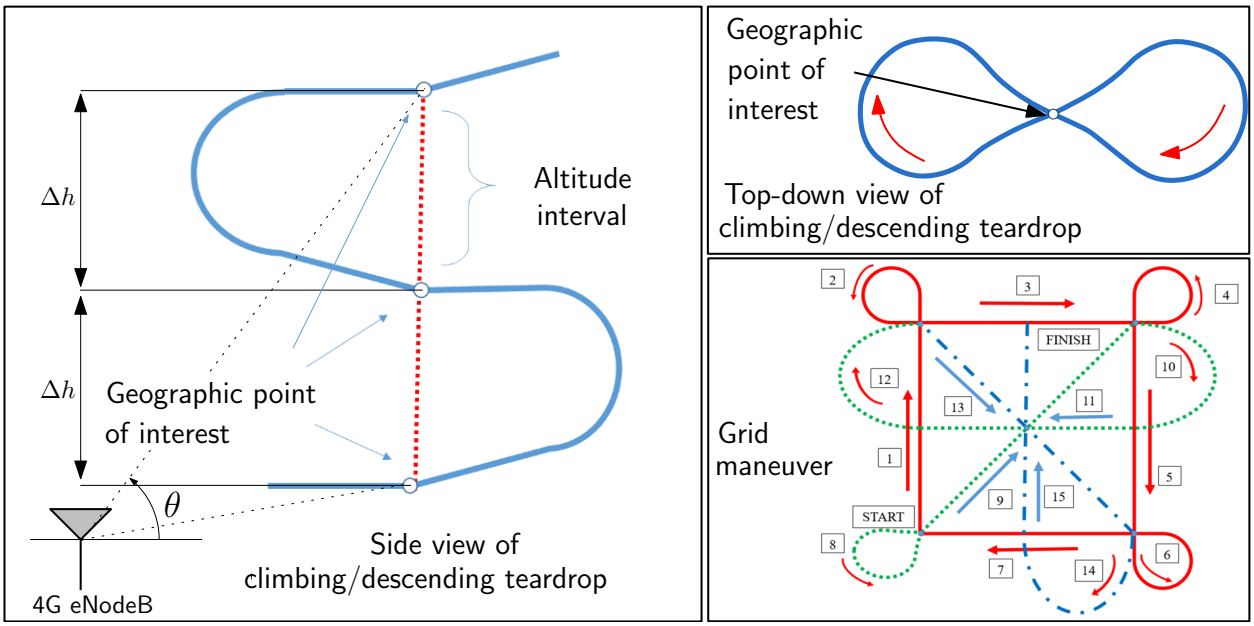


Figure 5.7: Maneuvers performed by the C-12 aircraft. The altitude step is denoted by Δh and θ denotes the elevation angle.

5.2.3 Data Processing

To efficiently process terabytes (TBs) of 4G signal data, an autonomous version of the proposed SDR was developed. This autonomous SDR is designed to automatically process the collected data and produce key metrics, including Doppler frequency, carrier phase, pseudorange, C/N_0, carrier phase error $e_{\mathrm{PLL,m}}$, and code phase error $e_{\mathrm{DLL,m}}$. The workflow of this autonomous SDR is illustrated in Figure 5.8.

The first step involves down-sampling the 4G data, followed by an acquisition process. This process correlates the received data with locally generated 4G-URSs as discussed in 3.3.2, yielding a coarse estimate of the code start time, Doppler frequency, and the corresponding C/N_0 for the received signal. Detected eNodeBs' acquisition parameters are then fed into the tracking loops to continuously monitor code and carrier phases.

A key feature of this autonomous SDR is its dynamic tracking adjustment. It periodically performs a re-acquisition every $t_{\mathrm{re-ac}}$ seconds, a user-defined parameter, to add new eN-

odeBs to the tracking loop. Additionally, every t_{as} seconds, another user-defined interval, it evaluates the tracking performance of the eNodeBs. This assessment involves analyzing the variance of the carrier phase error, denoted as $\sigma^2_{e_{\text{PLL,n}'}}$, where $n' = t_{\text{as}}/t_{\text{frame}}$ represents the window size for calculating $\sigma^2_{e_{\text{PLL,n}'}}$. If this variance exceeds a predefined threshold $\sigma^2_{\text{PLL,Th}}$, the tracking of the corresponding eNodeB is discontinued. For the SNIFFER 4G campaign, these parameters were set to $t_{\text{re-ac}} = 20$ seconds, $t_{\text{as}} = 5$ seconds, and $\sigma^2_{\text{PLL,Th}} = 6 \times 10^3\,\text{deg}^2$. The noise-equivalent bandwidth of the PLL, $B_{n,\text{PLL}}$, was configured to 12 Hz.

The data processing from each flight run yields crucial tracking information for all detectable eNodeBs, which is then archived for comprehensive analysis. This dissertation's subsequent sections focus on utilizing this data to evaluate the receiver's performance, explore the reception characteristics of 4G signals, and assess the potential of these signals for high-altitude aircraft navigation. To support these assessments, the USAF team provided time-stamped data on the position, orientation, and other vital ground truth parameters of the C-12 aircraft at the end of each flight day. This information was captured using the aircraft's onboard Honeywell H764-ACE EGI INS/GPS system. A meticulous examination and synchronization of this ground truth data with the cellular data from each flight were conducted. This synchronization process was instrumental in organizing the cellular data by key metrics such as altitude and roll angle. Furthermore, aligning these datasets is pivotal for the ensuing analysis of navigational performance using 4G signals, providing a foundation for comprehensive evaluations.

5.2.4 Receiver Performance

The data collected from the campaign profoundly influenced the development of a novel time-domain-based 4/5G receiver, as elaborated in Section 3.3. Initially, the experiment aimed to analyze the data using a state-of-the-art frequency-based 4G receiver, detailed in

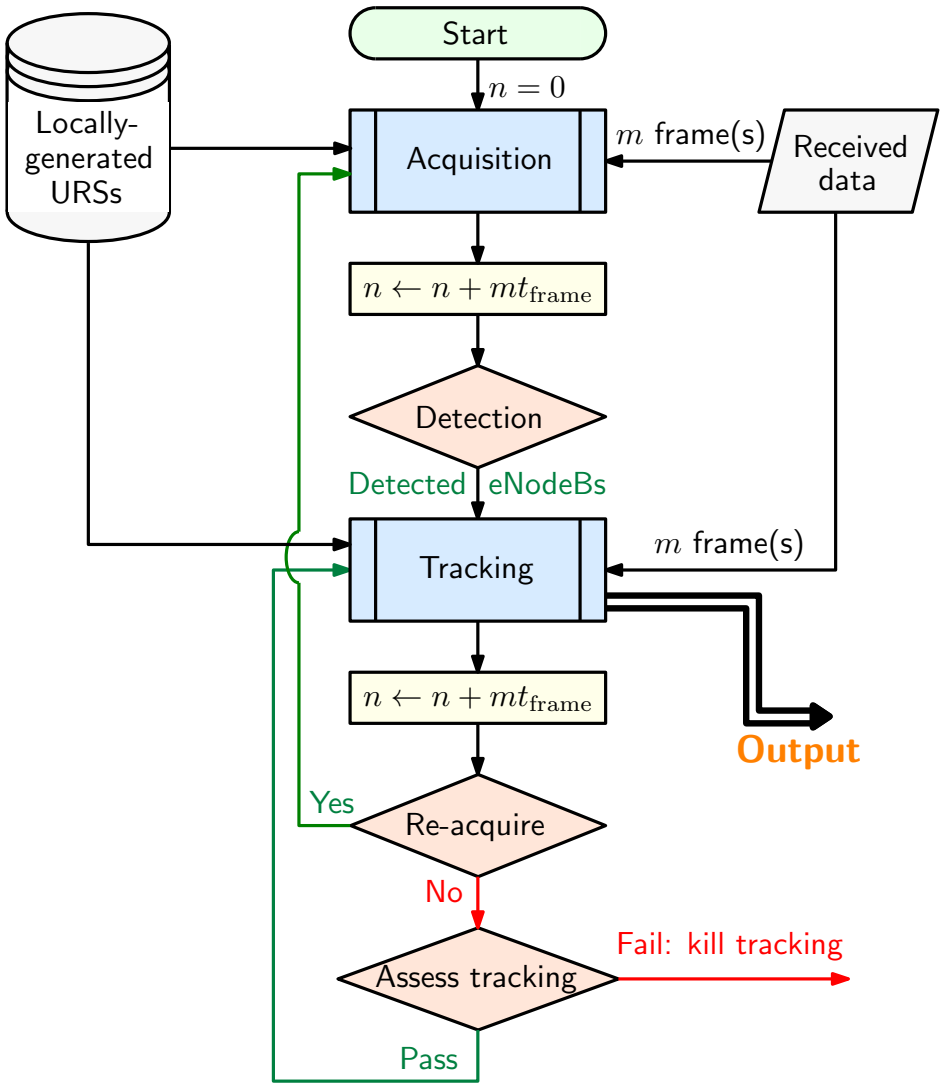


Figure 5.8: Flowchart of the developed autonomous SDR.

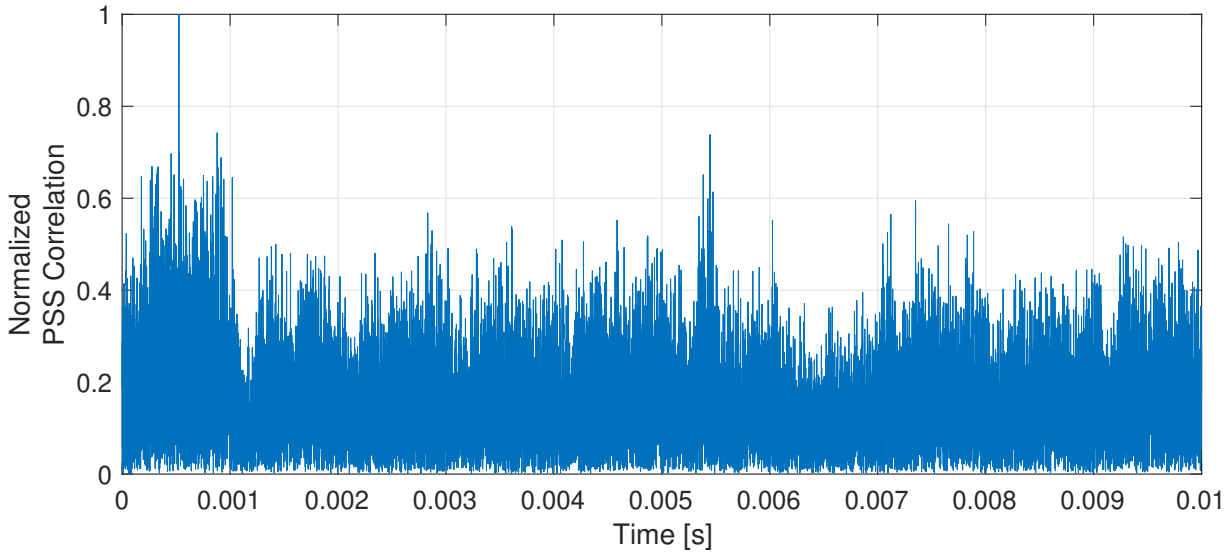


Figure 5.9: Acquisition output of the state-of-the-art frequency-domain-based 4G SDR at 5,500 ft AGL.

Subsection 3.1.1. However, this receiver faced significant challenges in acquiring and tracking terrestrial cellular signals when deployed on high-altitude aircraft, particularly with eNodeBs displaying low SNR or experiencing high Doppler shifts.

The acquisition outcomes of the PSS using the frequency-based 4G receiver, demonstrated in Figure 5.9, were obtained over a region with a dense 4G eNodeB network. These results starkly reveal the receiver's inability to acquire any 4G signal, contrasting sharply with its successful acquisitions under different conditions, as shown in Figure 3.1. This discrepancy underscored the necessity to develop a new time-domain-based 4/5G receiver capable of overcoming these challenges, leading to the proposed receiver in Section 3.3.

Employing the new 4G SDR, as per the process outlined in Subsection 5.2.3, across more than 55 flight runs yielded surprising results. The SDR detected over 100 eNodeBs simultaneously, far exceeding the typical 10-15 eNodeBs detected in other scenarios like pedestrian, ground vehicle, or UAV contexts. Remarkably, some eNodeBs were detected at distances up to 100 km, with the SDR still effectively tracking their signals and generating reliable navigation observables. Figures 5.10 to 5.13 present sample outputs from Region A's climbing flight

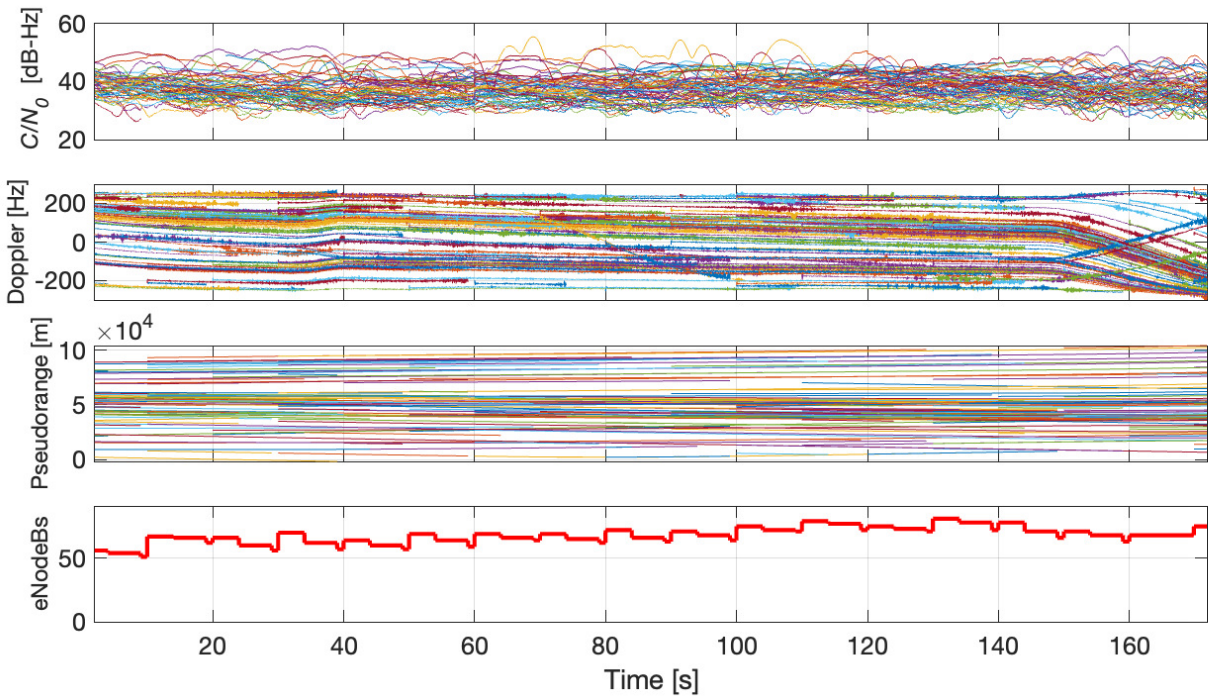


Figure 5.10: Receiver Output: Region A, climb, altitude range = [1.76 2] km AGL.

mode for various flight runs. Notably, Figure 5.13 illustrates the takeoff phase, where a significant increase in detectable eNodeBs is observed as the C-12 aircraft ascends.

The receiver outputs for flight runs 24 and 28, showcased in Figures 5.14 and 5.15, respectively, correspond to grid maneuvers conducted in Region A at altitudes of around 5.46 and 1.4 km. Similarly, Figures 5.16 and 5.17 depict outputs from flight runs 44 and 49, involving teardrop maneuvers.

For Region B, Figures 5.18 through 5.21 display sample outputs from various climbing flight runs, while Figures 5.22 and 5.23 show outputs for grid maneuvers at altitudes around 1.7 and 1.68 km. Additionally, Figure 5.24 presents the output from flight 54's teardrop maneuver.

These exhaustive results serve as the foundation for further mining and characterization of 4G signals at high altitudes, and for assessing their navigation performance.

Table 5.2: Summary of the data processed from the 55 flight runs conducted by the USAF.

Flight Number	**Region**	**Flight Mode**	**Altitude Range AGL [km]**		**Total Number of eNodeBs**	**Average C/N_0 [dB-Hz]**
1	Region A	Climb	1.76	2	113	37.48
2	Region A	Climb	2	2.28	118	37.08
3	Region A	Climb	2.28	2.58	145	36.78
4	Region A	Climb	2.59	2.94	141	36.61
5	Region A	Climb	2.98	3.19	155	36.03
6	Region A	Climb	3.2	3.44	155	36
7	Region A	Climb	3.44	3.87	165	36.07
8	Region A	Climb	3.91	4.2	144	35.84
9	Region A	Climb	4.23	4.54	150	35.58
10	Region A	Climb	4.54	4.85	127	35.48
11	Region A	Climb	4.86	5.14	143	35.13
12	Region A	Climb	5.16	5.45	124	35.51
13	Region A	Climb	5.47	5.77	131	34.72
14	Region A	Climb	5.78	5.88	102	35.5
15	Region A	Climb	5.99	6.37	122	34.51
16	Region A	Climb	6.4	6.71	103	34.89
17	Region A	Climb	6.72	6.96	119	34.33
18	Region A	Climb	7	7.03	91	34.41
19	Region A	Climb	1.15	1.31	126	36.81
20	Region A	Climb	1.35	1.58	134	36.56
21	Region A	Climb	1.59	1.78	129	37.08
22	Region A	Climb	0.69	0.76	66	37.23
23	Region A	Climb	0	1.34	91	38.22
24	Region A	Grid	5.45	5.47	144	34.66
25	Region A	Grid	5.45	5.48	155	34.5
26	Region A	Grid	5.45	5.47	132	34.49
27	Region A	Grid	5.46	5.47	145	34.55
28	Region A	Grid	1.26	1.61	161	36.85
29	Region A	Grid	1.61	1.61	116	36.06
30	Region A	Grid	1.6	1.62	164	36.09
31	Region B	Climb	3.06	3.13	112	35.51
32	Region B	Climb	3.38	3.53	104	35.54
33	Region B	Climb	3.69	3.7	99	34.64
34	Region B	Climb	4	4.1	90	34.29
35	Region B	Climb	4.31	4.32	97	33.68
36	Region B	Climb	4.62	4.62	76	33.24
37	Region B	Climb	4.93	4.94	102	33.42
38	Region B	Climb	5.24	5.25	62	33.27
39	Region B	Climb	5.39	5.4	82	33.94
40	Region B	Climb	1.7	2.32	127	37.22
41	Region B	Climb	2.46	2.64	132	36.62
42	Region B	Climb	2.76	2.77	50	36.11
43	Region B	Climb	2.92	2.92	93	35.72
44	Region A	TearDrop	1.08	1.1	85	37.07
45	Region A	TearDrop	1.1	1.24	94	37.79
46	Region A	TearDrop	1.27	1.4	82	37.32
47	Region A	TearDrop	1.51	1.57	109	37.28
48	Region A	TearDrop	1.55	1.71	103	36.79
49	Region A	TearDrop	1.7	1.86	93	37.18
50	Region B	Grid	1.7	1.71	120	37.56
51	Region B	Grid	1.69	1.72	132	37.08
52	Region B	Grid	1.69	1.72	142	37.27
53	Region B	Grid	1.66	1.71	118	37.82
54	Region B	TearDrop	1.08	1.86	84	37.84
55	Region B	Climb	1.45	1.93	100	36.7

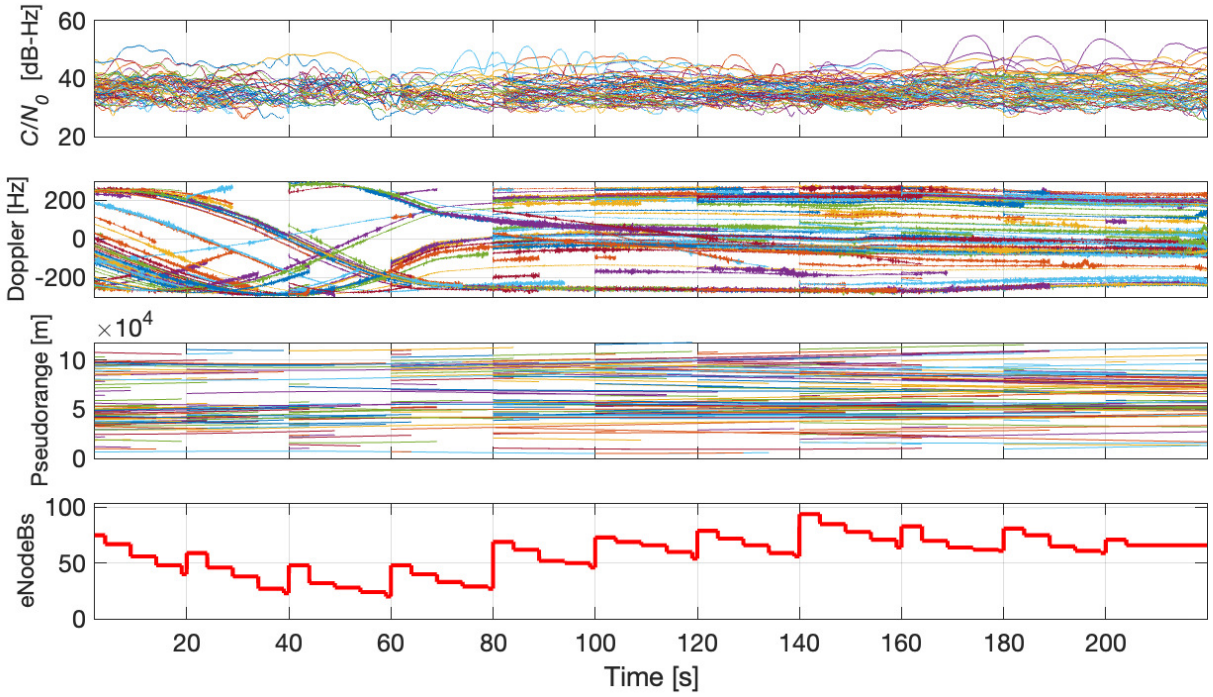


Figure 5.11: Receiver Output: Region A, climb, altitude range = [3.91 4.2] km AGL.

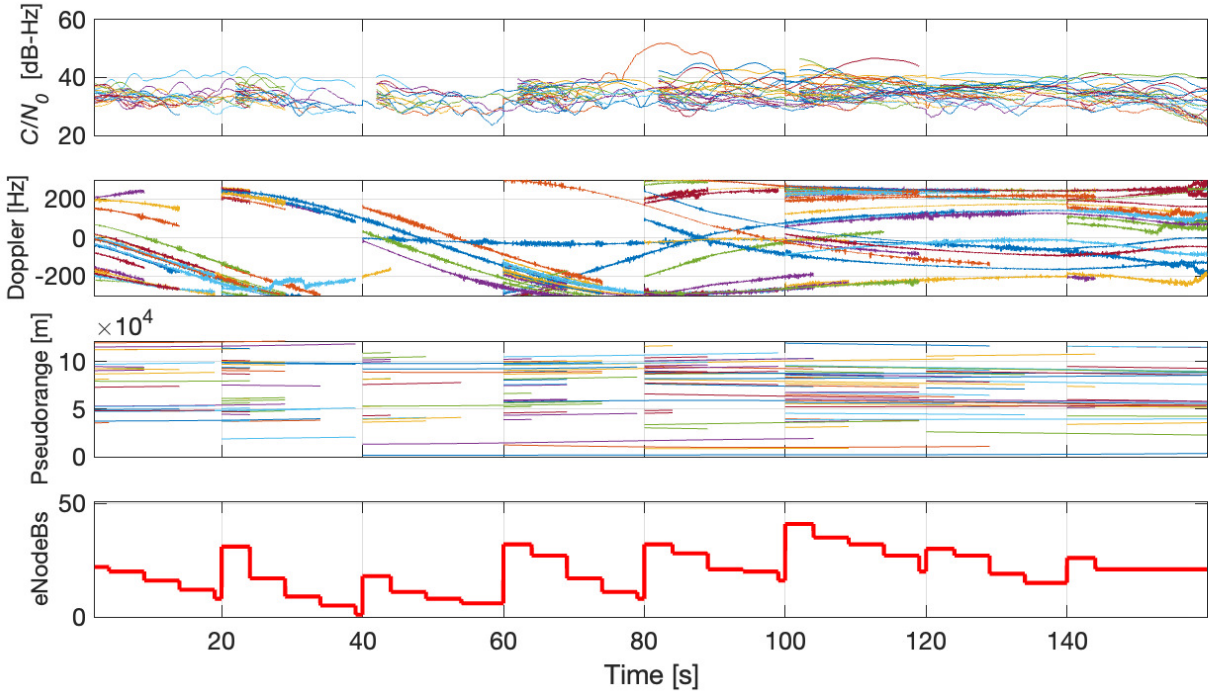


Figure 5.12: Receiver Output: Region A, climb, altitude range = [7 7.03] km AGL.

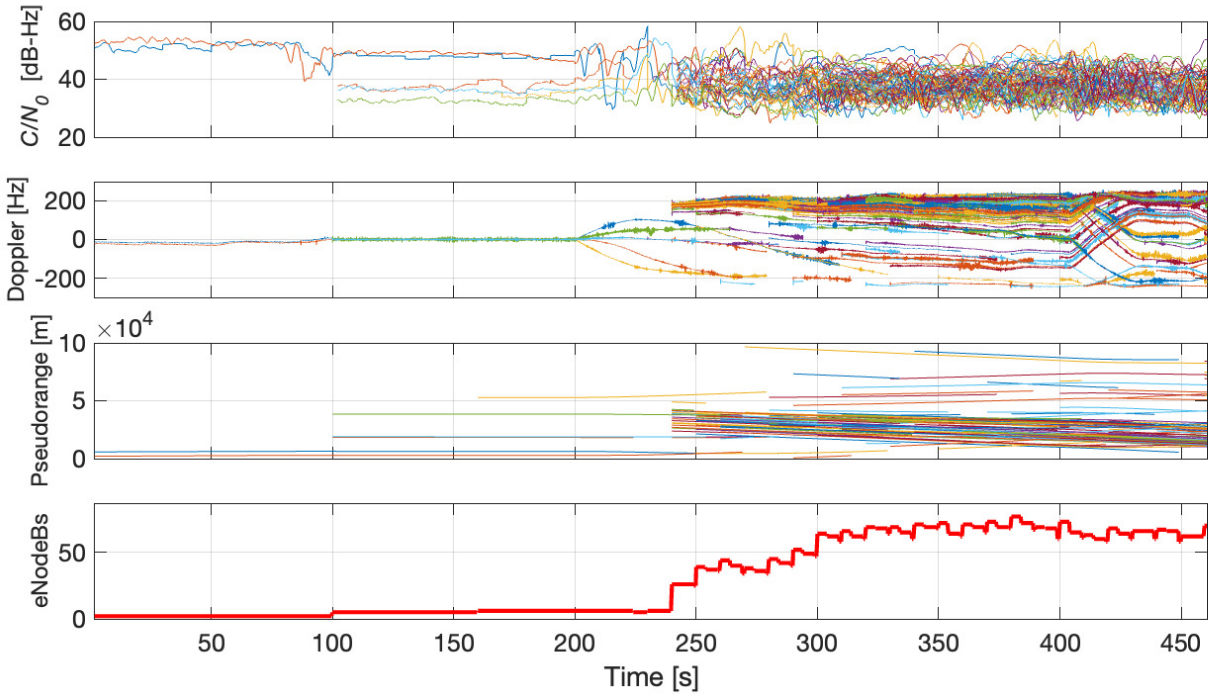


Figure 5.13: Receiver Output: Region A, takeoff, altitude range = [0 1.34] km AGL.

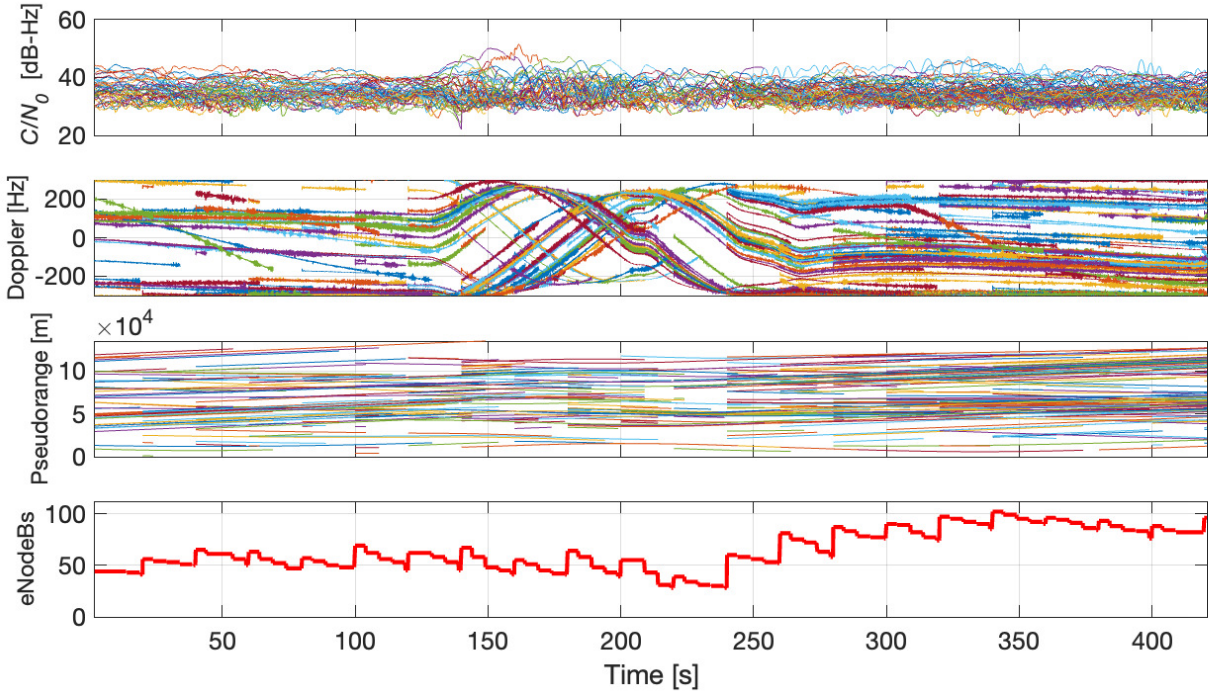


Figure 5.14: Receiver Output: Region A, grid, altitude range = [5.45 5.47] km AGL.

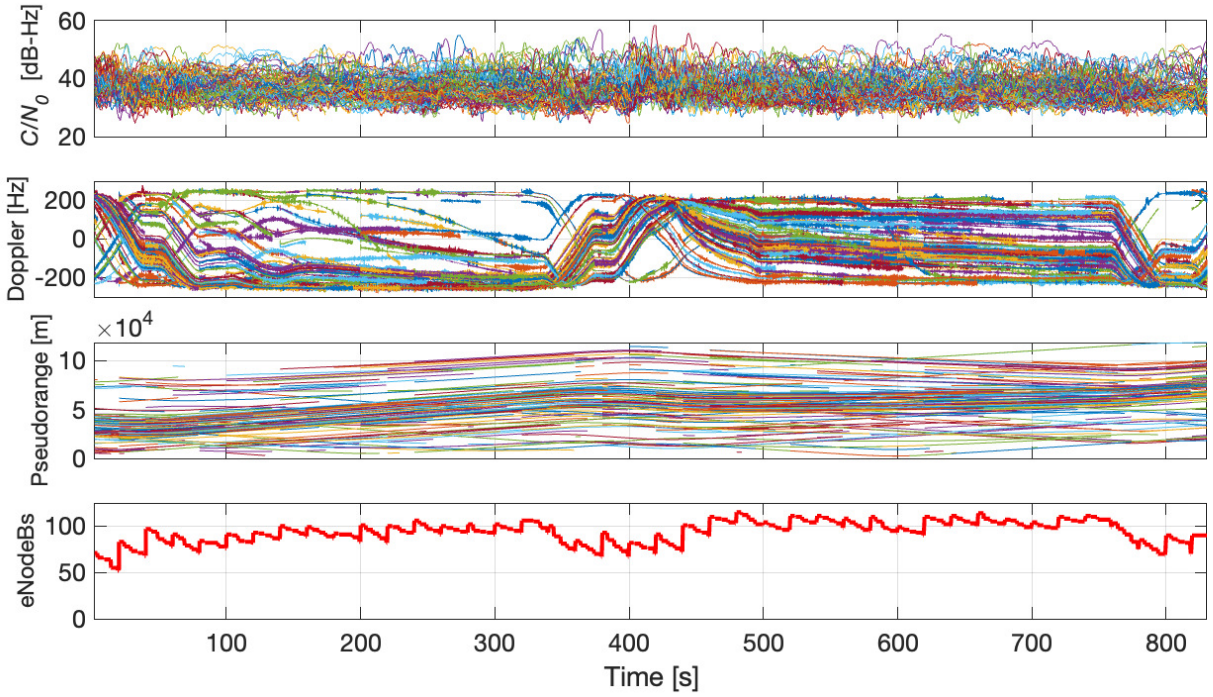


Figure 5.15: Receiver Output: Region A, grid, altitude range = [1.26 1.61] km AGL.

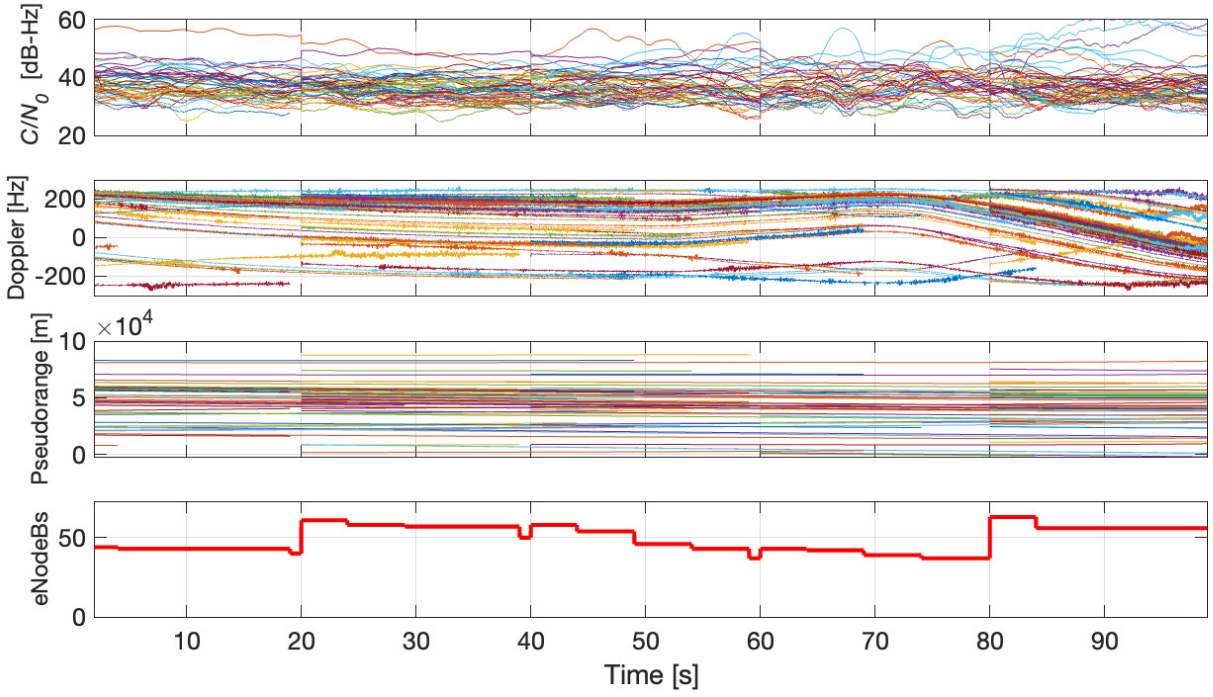


Figure 5.16: Receiver Output: Region A, teardrop, altitude range = [1.08 1.1] km AGL.

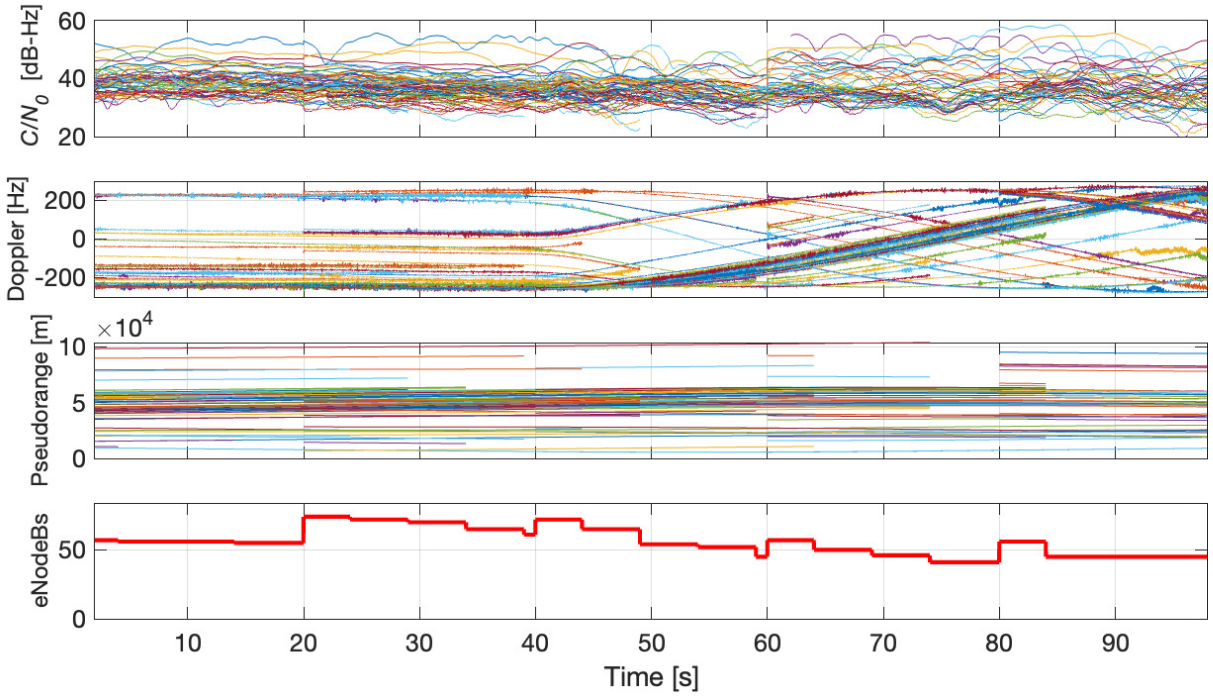


Figure 5.17: Receiver Output: Region A, teardrop, altitude range = [1.7 1.86] km AGL.

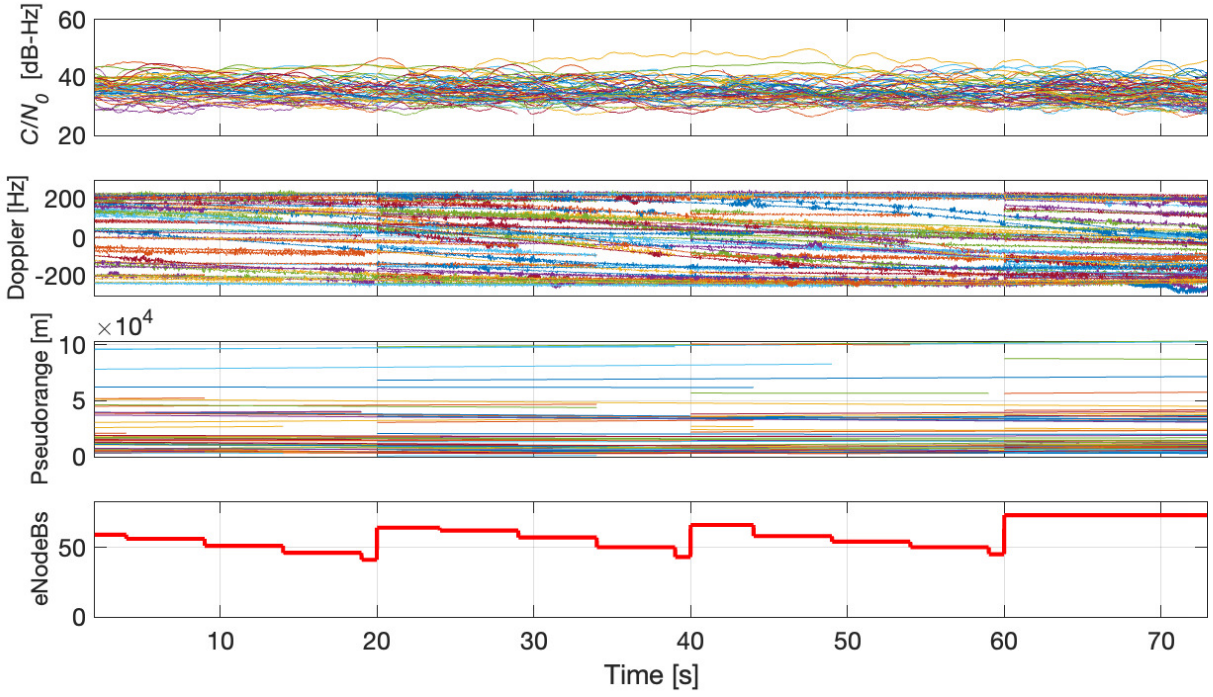


Figure 5.18: Receiver Output: Region B, climb, altitude range = [3.06 3.13] km AGL.

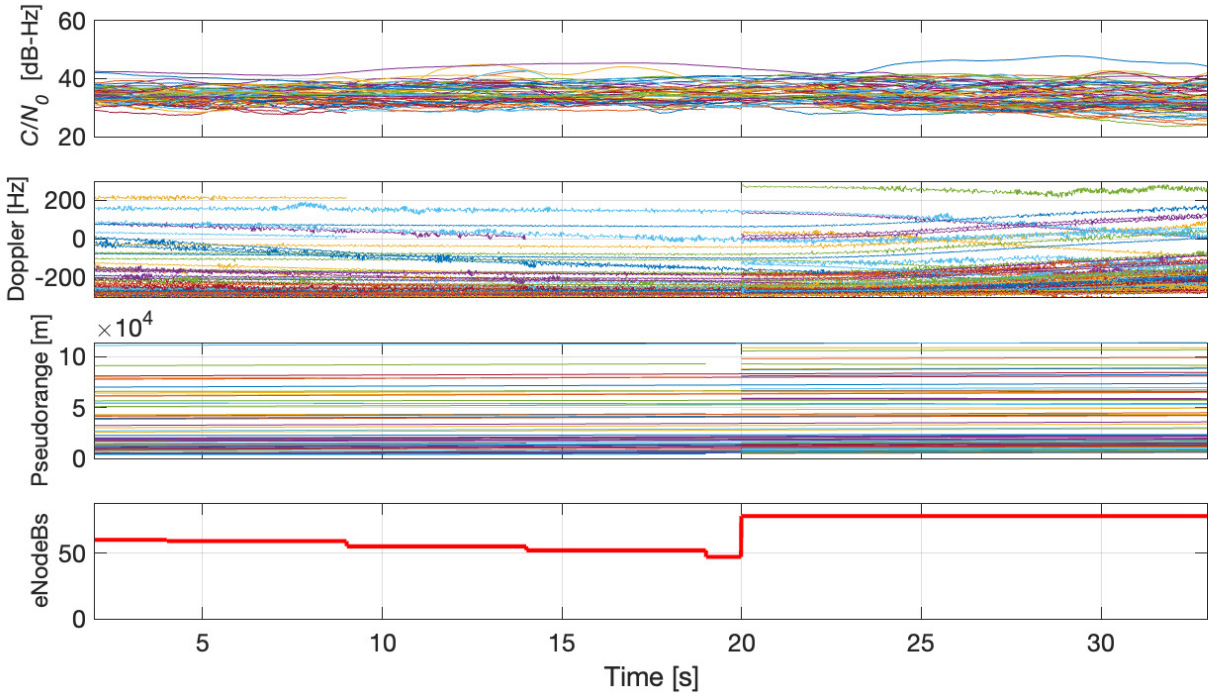


Figure 5.19: Receiver Output: Region B, climb, altitude range = [4 4.1] km AGL.

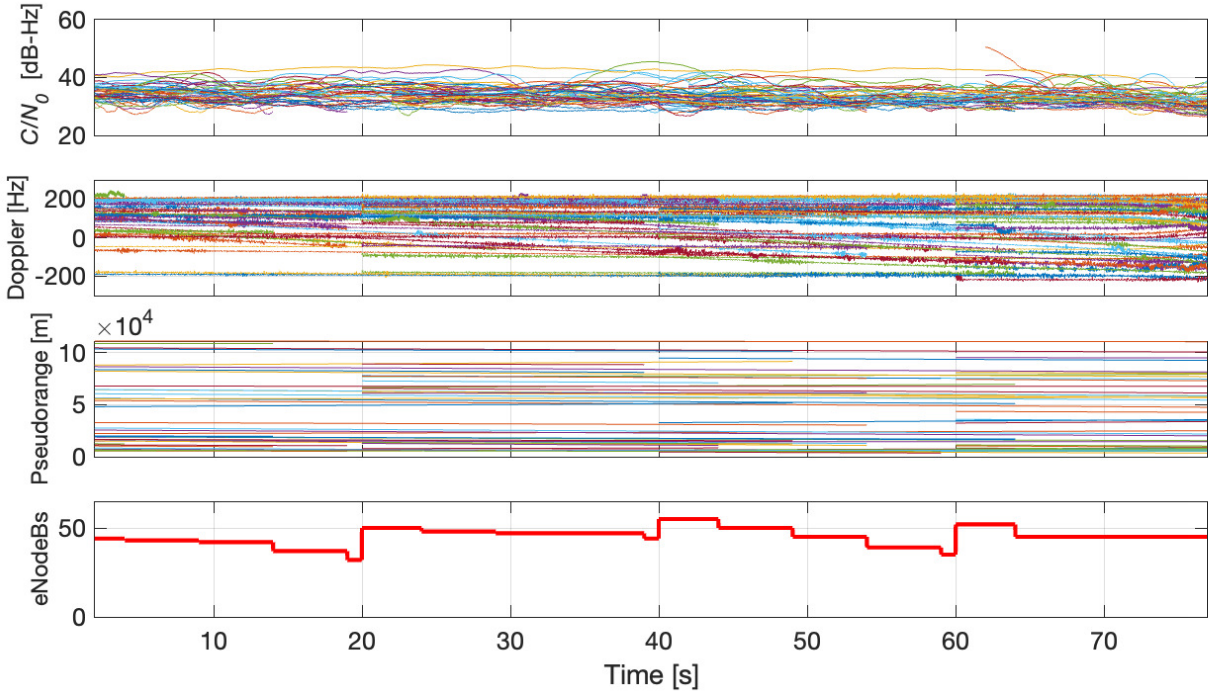


Figure 5.20: Receiver Output: Region B, climb, altitude range = [5.39 5.4] km AGL.

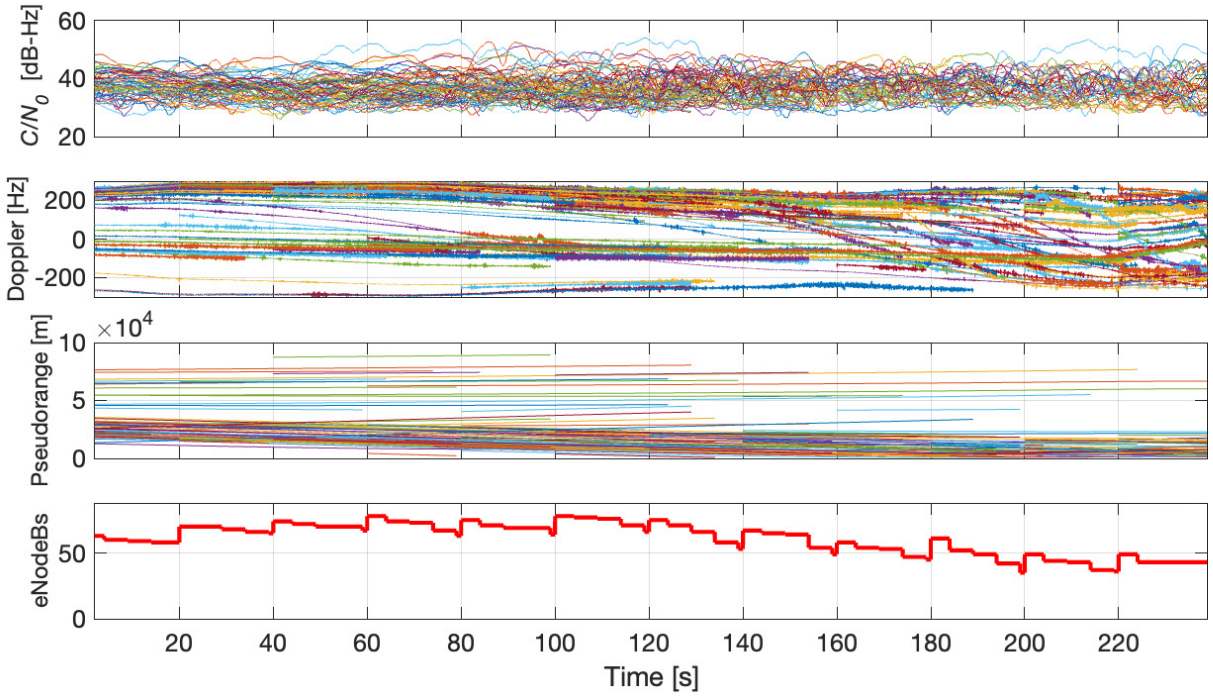


Figure 5.21: Receiver Output: Region B, climb, altitude range = [1.45 1.93] km AGL.

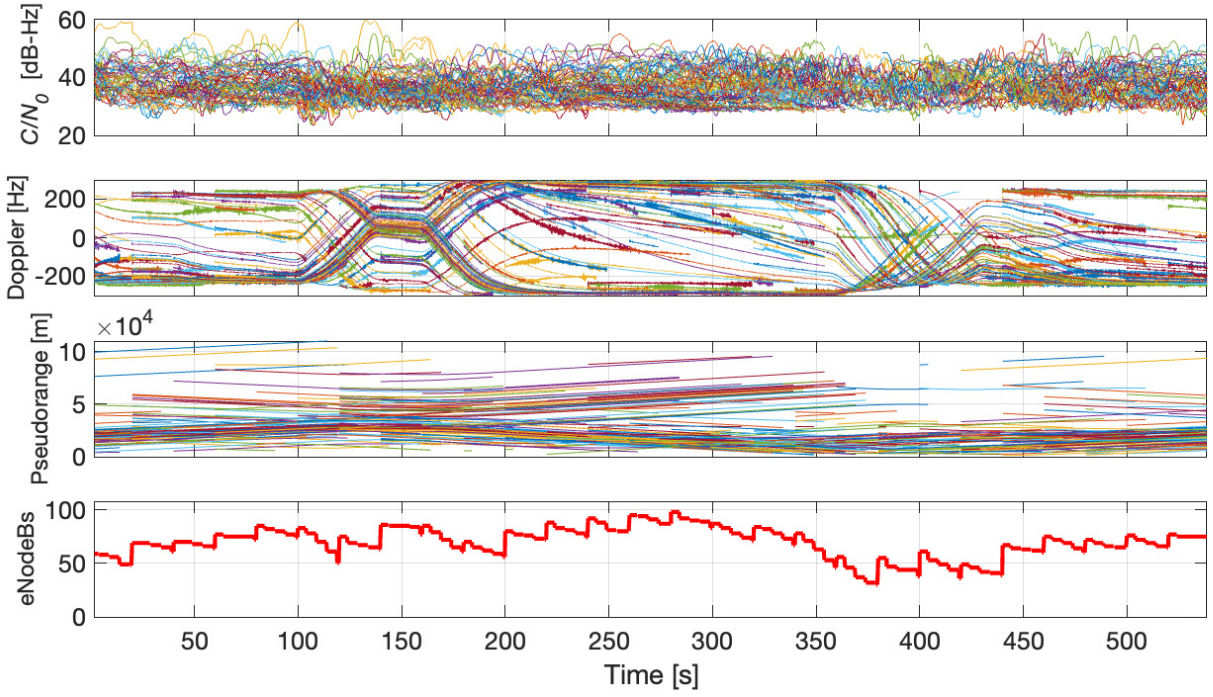


Figure 5.22: Receiver Output: Region B, grid, altitude range = [1.69 1.72] km AGL.

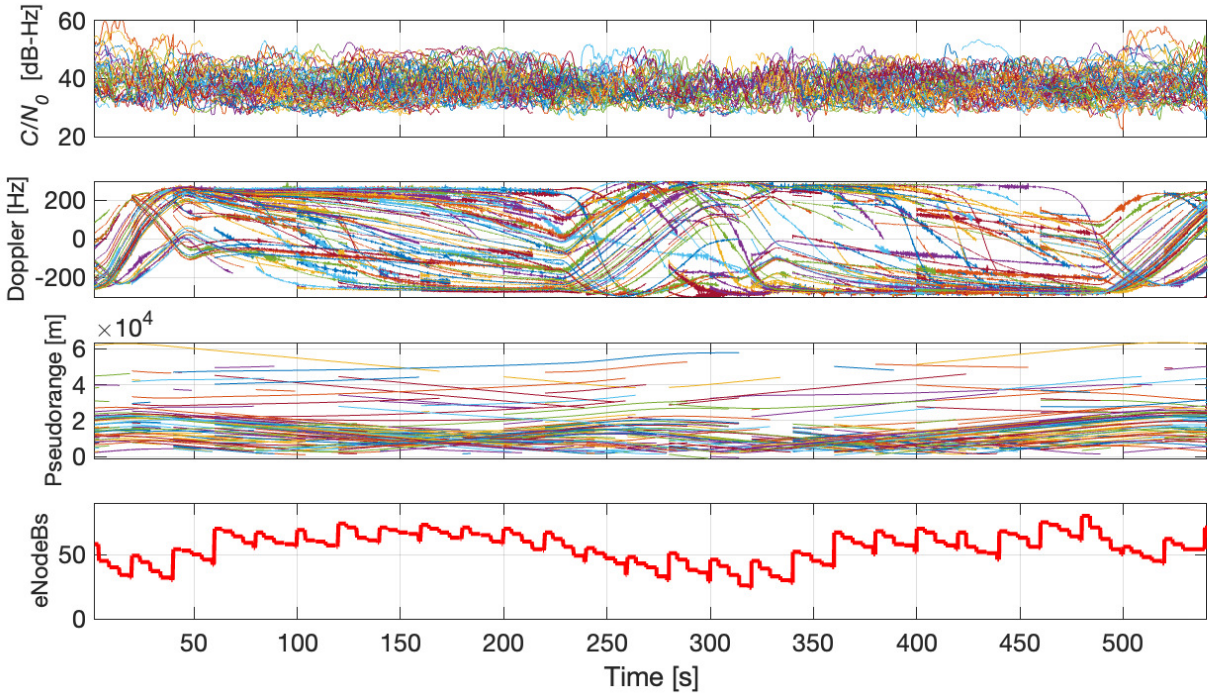


Figure 5.23: Receiver Output: Region B, grid, altitude range = [1.66 1.71] km AGL.

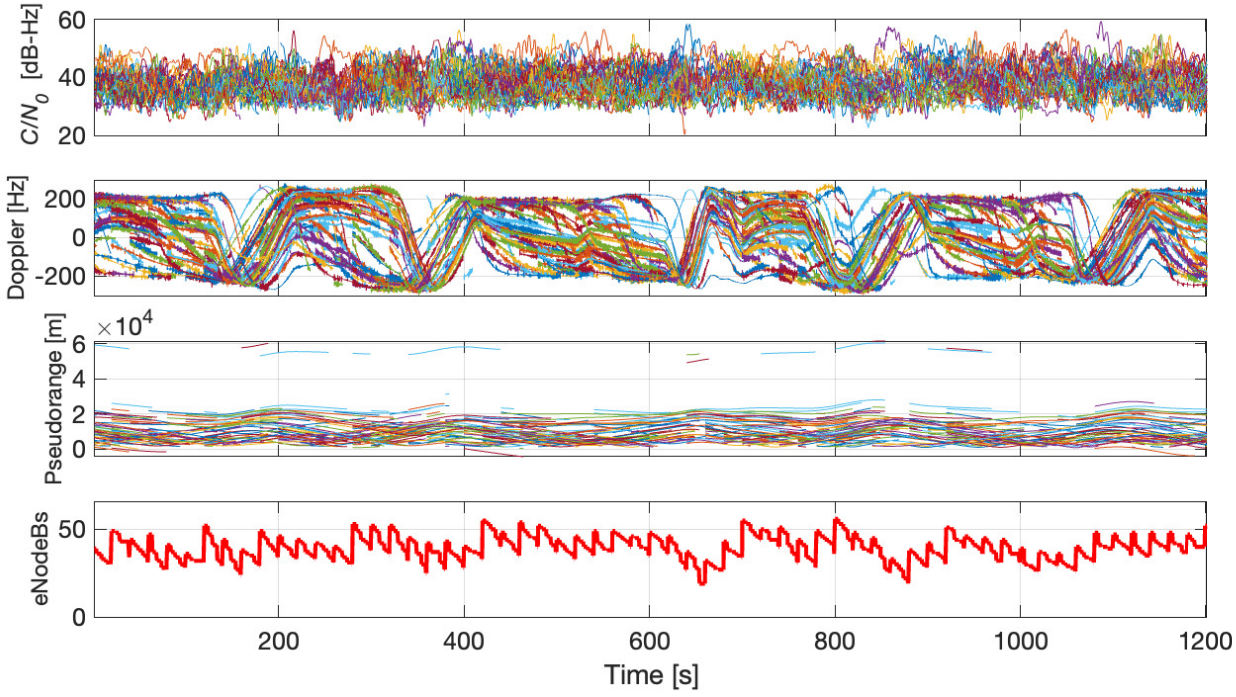


Figure 5.24: Receiver Output: Region B, teardrop, altitude range = [1.08 1.86] km AGL.

5.2.5 Characterization of 4G Signals at High Altitudes

5.2.5.1 Receiver Output Preliminary Takeaways

The preliminary analysis of the flight run data, as summarized in Table 5.2, has led to several important observations:

Regional Variations: The data reveals significant differences between Region A and Region B. In Region A, there is a higher count of detectable eNodeBs along with a marginally better average CNR. This may suggest that Region A presents less challenging terrain for signal propagation compared to Region B.

Flight Mode Impact: Analysis of different flight modes, such as Climb, Grid, and Teardrop, highlights variations in eNodeB detection capabilities and CNR values. The Climb mode, in particular, tends to demonstrate a broader range of altitude fluctuations and a higher number of detectable eNodeBs. This indicates that increased altitudes could enhance line-of-sight access to multiple eNodeBs.

Altitude Influence: The altitude AGL exhibits a nuanced impact on the count of detectable eNodeBs and CNR. While ascending typically boosts visibility and line-of-sight, it also presents challenges due to the extended distance from the eNodeBs. The data points towards an optimal altitude range where the interplay between visibility and distance maximizes both eNodeB detection and CNR.

eNodeB Density and CNR Correlation: A notable correlation is observed between the count of detected eNodeBs and the average CNR. Regions and flight modes recording higher eNodeB numbers usually exhibit improved CNR values, likely due to an enhanced probability of line-of-sight connections.

These findings emphasize the criticality of considering geographic, altitudinal, and operational variables in signal characterization. The subsequent sections delve deeper into the correlation between eNodeB detection and altitude across various flight modes, as well as the influence of multipath effects.

5.2.5.2 Comparative Analysis of eNodeB Detection vs. Altitude in Different Flight Modes

This section is dedicated to evaluating the availability of 4G signals at various altitudes, with a particular focus on quantifying the number of eNodeBs that are detectable at different heights and with different flight modes. The analysis is grounded in the processed data derived from 55 distinct flight runs over regions A and B. This data has been methodically categorized based on two pivotal metrics: (i) the altitude AGL, symbolized as h, and its equivalent in ft, and (ii) the roll angle of the C-12 aircraft during its flight operations. A significant aspect of this categorization is the inclusion of the roll angle. This metric is crucial as it facilitates an understanding of how the aircraft's banking maneuvers might influence the detectability of eNodeBs, particularly in scenarios where the aircraft body could obstruct signal reception.

Figure 5.25 illustrates the relationship between the average number of detectable eNodeBs and altitude, up to a height of 7 kilometers (approximately 23,000 ft) AGL, under steady flight conditions, defined as having a roll angle $\leq 10°$. Data from Region A is comprehensive, covering the full altitude range from ground level to 7 km (0 to 23,000 ft), as take-offs and landings occurred at Edwards AFB, located within this region. Conversely, the dataset for Region B encompasses altitudes ranging from 400 meters (0.4 km or approximately 1,312 ft) to 4.6 kilometers (approximately 15,091 ft).

An empirical analysis aimed at modeling the number of eNodeBs relative to altitude h

reveals two distinct intervals: (i) altitudes below 300 meters (approximately 984 ft), and (ii) altitudes above 300 meters. In the first interval, which only includes data from Region A, a linear increase in the number of eNodeBs with altitude is observed, ranging from an estimated 5.82 eNodeBs at ground level in rural areas to 45.96 eNodeBs at 300 meters AGL. For altitudes above 300 meters, the data fits a parabolic curve more precisely, with the peak number of eNodeBs observed at altitudes of 3.15 km (approximately 10,335 ft) and 2.28 km (approximately 7,480 ft) for Regions A and B, respectively. Beyond these peak altitudes, there is a noticeable decrease in the number of eNodeBs with increasing altitude; however, even at the upper limit of 7 km AGL (approximately 23,000 ft), at least 20 eNodeBs remained detectable. This observation is particularly notable and underscores the significant potential of using cellular signals for navigation at high altitudes.

The observed discrepancy in the number of detectable eNodeBs between Regions A and B can be explained by differences in transmission power. eNodeBs in rural areas like Region A typically have higher transmission powers to ensure sufficient coverage over expansive areas and open spaces. This is in contrast to urban/semi-urban eNodeBs, like those in Region B, which are generally calibrated for high-density usage and are characterized by lower transmission powers to manage interference and optimize energy efficiency.

Figure 5.26 illustrates the relationship between the number of detectable eNodeBs and altitude for scenarios where the aircraft was in a banking mode, defined by a roll angle greater than 10°. In this context, the data from Region A is again more exhaustive, encompassing altitudes ranging from 0.43 kilometers (approximately 1,411 feet) to 7 kilometers (approximately 23,000 feet). In contrast, the data from Region B covers a narrower altitude range, from 0.59 kilometers (approximately 1,936 feet) to 2.29 kilometers (approximately 7,513 feet).

Analysis of the number of eNodeBs detectable within these altitude ranges suggests that a parabolic curve effectively characterizes the observed behavior. The apex of this parabola,

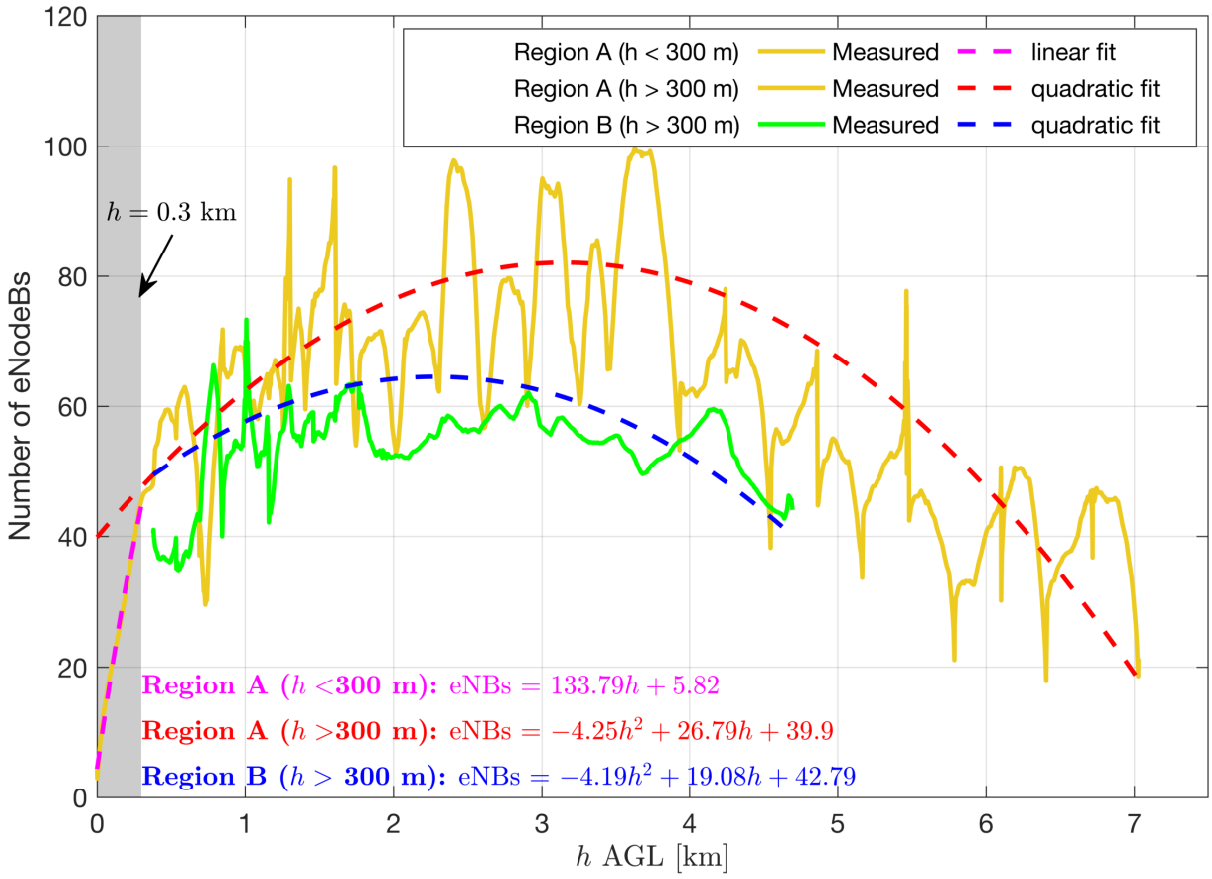


Figure 5.25: Measured number of eNodeBs vs AGL altitude h [km] in regions A and B along with the quadratic fit of the measured data in airplane steady mode (roll angle $\leq 10°$). The shaded region represents $h < 0.3$ km.

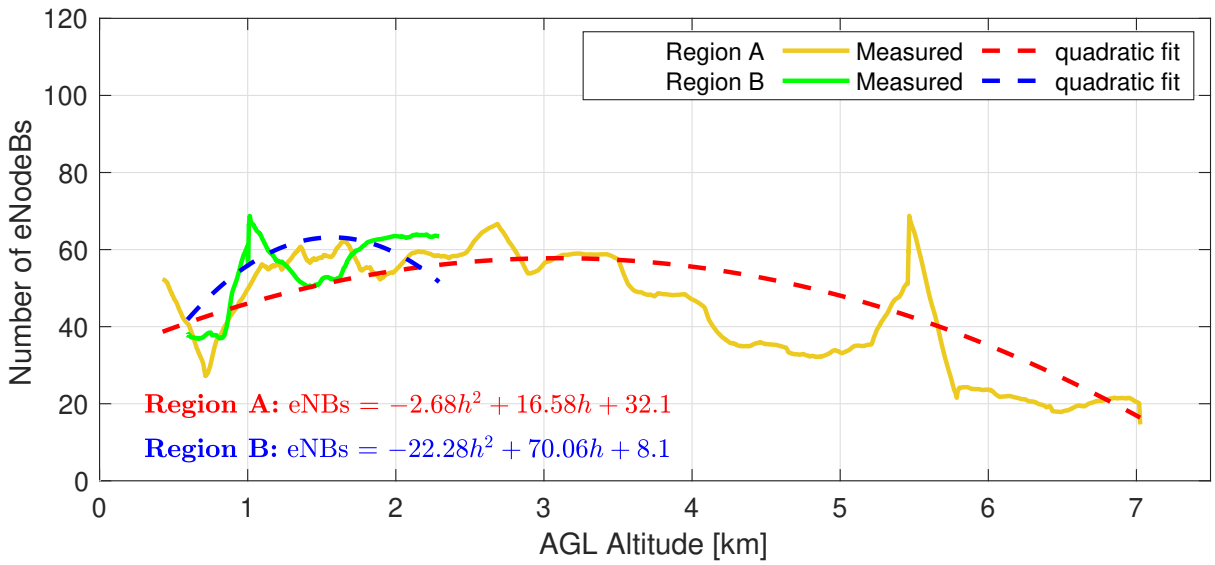


Figure 5.26: Measured number of eNodeBs vs AGL altitude h [km] in regions A and B along with the quadratic fit of the measured data in airplane banking mode (roll angle $> 10°$).

indicating the maximum number of eNodeBs, occurs at altitudes of 3.09 kilometers (approximately 10,138 feet) in Region A and 1.57 kilometers (approximately 5,151 feet) in Region B. Following these peak altitudes, a discernible decline in the number of detectable eNodeBs is observed with increasing altitude in both regions. This pattern indicates that despite the changes in altitude and aircraft banking angles, there is a consistent trend in the detectability of eNodeBs, with a peak followed by a gradual decrease as altitude continues to rise.

5.2.5.2.1 Discussion

In order to comprehensively understand how the number of detected eNodeBs varies with altitude in different flight modes, Figure 5.27 presents the obtained empirical models over the altitude range from 0 to 7 km (0 to approximately 23,000 feet) for Regions A and B. The analysis reveals distinct patterns in eNodeB detectability across different flight conditions:

1. **Region A:**

   (a) **Steady Mode:** Observations indicate an increase in the number of detected

eNodeBs with altitude, reaching a peak at approximately 3.15 km (approximately 10,335 feet). Beyond this peak, a gradual decrease in detectability is observed.

(b) **Banking Mode:** A similar trend is noted, with the peak detectability occurring around 3.09 km (approximately 10,138 feet). It is noteworthy that the peak number of detectable eNodeBs in banking mode is marginally lower compared to steady mode.

2. **Region B:**

(a) **Steady Mode:** The pattern mirrors that of Region A, with a detectability peak at around 2.28 km (approximately 7,480 feet). However, the decrease in eNodeB detection beyond the peak is less pronounced compared to Region A.

(b) **Banking Mode:** A markedly different behavior is observed, characterized by a rapid increase in eNodeB detection up to about 1.57 km (approximately 5,151 feet), followed by a precipitous decline.

In Region A, the altitude yielding the highest eNodeB detectability appears to be consistently around 3 km (approximately 10,138 to 10,335 feet) for both flight modes, suggesting a more uniform eNodeB distribution or different geographic characteristics compared to Region B. Conversely, Region B exhibits significant discrepancies between steady and banking modes, with the optimal altitude for eNodeB detection in banking mode being notably lower than in steady mode. This disparity may be attributable to the influence of aircraft banking on the visibility of eNodeBs, which are potentially more scattered or located in varied terrains.

Furthermore, steady mode in Region A consistently outperforms banking mode in terms of eNodeB detectability across most altitudes, particularly at higher altitudes. In Region B, while steady mode generally detects more eNodeBs at lower altitudes, banking mode temporarily surpasses steady mode around 1.5 km (approximately 5,151 feet) before rapidly decreasing.

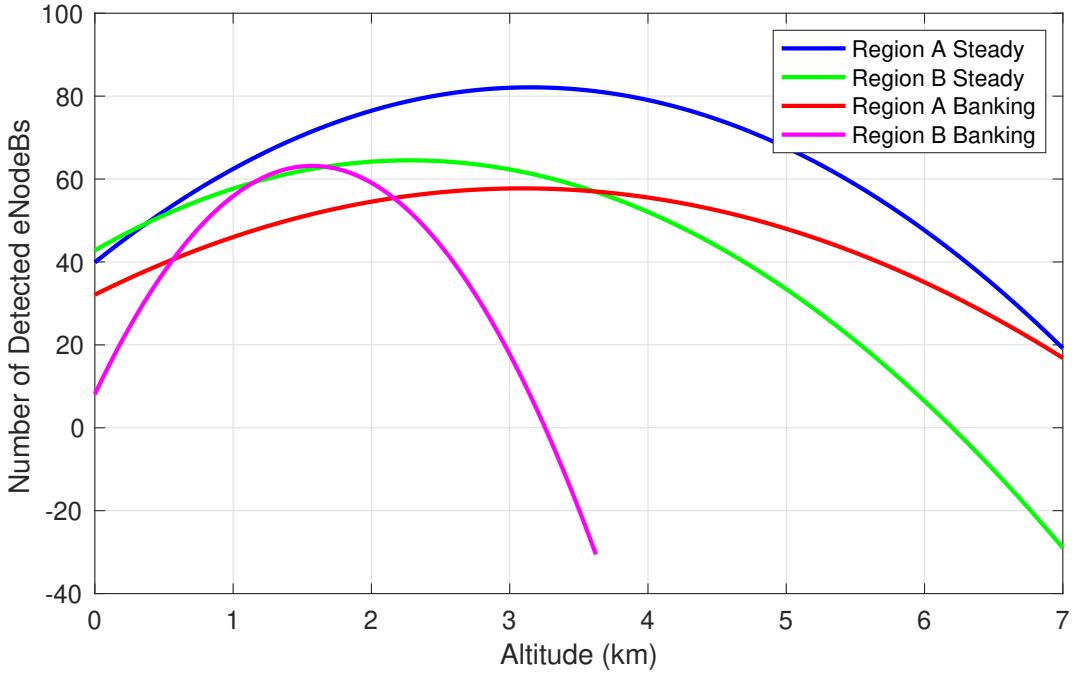


Figure 5.27: The obtained empirical models of the detected eNodeBs vs altitude for different Regions and flight modes.

These findings provide valuable insights into the relationship between flight mode, altitude, and cellular network coverage, which is pivotal for the development of cellular-based navigation systems for aircraft.

5.2.5.3 Multipath Characterization

This section focuses on characterizing the accuracy of 4G navigation observables at high altitudes, particularly in the context of multipath channel effects. Both severe- and short-delay multipath can introduce significant biases in pseudorange measurements, adversely affecting the navigation solution. A key method for assessing the multipath channel involves estimating the channel impulse response (CIR) using the receiver proposed in Section 3.3. The CIR is evaluated at various altitudes within Regions A and B to understand its impact.

Representative results for each region are depicted in Figure 5.28, with a focus on a 4G signal

bandwidth of 10 MHz. The data presented in Figure 5.28 illustrates that the LOS signal is predominant in the CIR up to altitudes of 23,000 ft AGL. Interestingly, the results indicate that multipath effects are more pronounced at lower altitudes. This trend is attributed to the increased presence of reflective surfaces near the ground, which contribute to multipath. Consequently, the CIRs at lower altitudes are either relatively free of multipath or exhibit low multipath levels, suggesting higher accuracy in pseudorange measurements.

It is noteworthy that the CIRs appear to deteriorate slightly at altitudes around 15,000 ft (AGL) and above. However, this degradation is primarily attributed to channel noise rather than multipath. Such insights into the CIR at various altitudes are crucial for understanding and enhancing the accuracy of high-altitude 4G navigation solutions.

5.2.6 Navigation Performance

This section focuses on assessing the navigation performance of the proposed 4G-based high-altitude aircraft navigation system. Specifically, it examines two flight runs, namely flight runs 28 and 54. Flight run 28 involves a grid maneuver over Region A, while flight run 54 encompasses a teardrop maneuver over Region B. These maneuvers are detailed in Table 5.2. Subsequent discussions in this section will delve into the design and settings of the navigation filter and explore the navigation performance observed in both flight runs.

5.2.6.1 Navigation Filter

The extracted carrier-aided code-phase pseudorange measurements were fused in an EKF to estimate the receiver's 3-D position $\boldsymbol{r}_r$, velocity $\dot{\boldsymbol{r}}_r$, and acceleration $\ddot{\boldsymbol{r}}_r$ expressed in North-East-Down (NED) frame, and relative clock bias and drift between the receiver's and

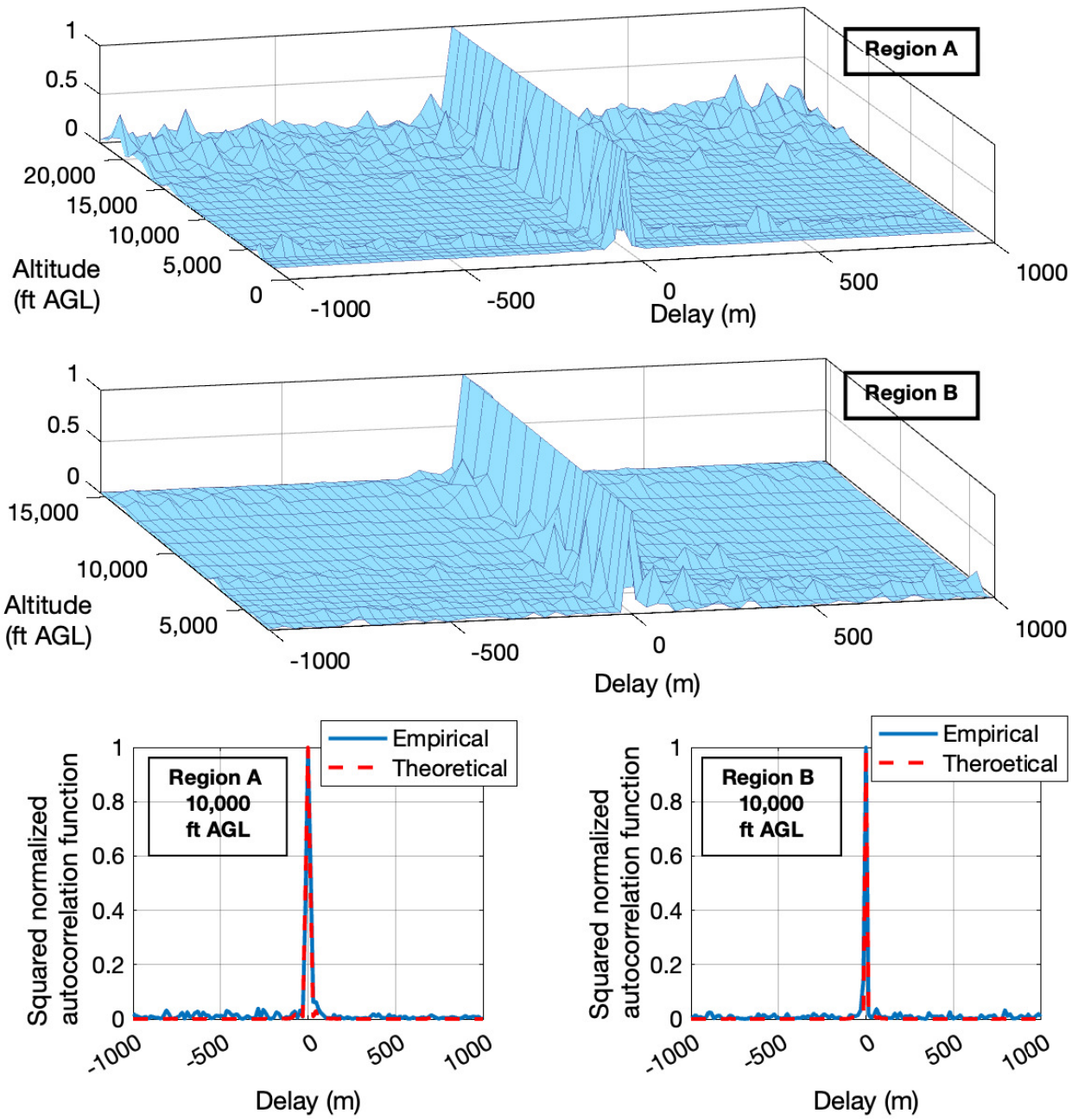


Figure 5.28: Top: Surface plots of the CIR as a function of altitude for representative eNodeBs in Regions A nad B. Bottom: Snapshots of empirical CIR in Regions A and B at 10,000 ft AGL along with the theoretical CIR.

eNodeBs' clocks. The EKF state vector is expressed as

$$\boldsymbol{x} \triangleq \left[\boldsymbol{x}_{\text{pva}}^{\mathsf{T}}, \boldsymbol{x}_{\text{clk}_1}^{\mathsf{T}}, \cdots, \boldsymbol{x}_{\text{clk}_U}^{\mathsf{T}}\right]^{\mathsf{T}}, \tag{5.2}$$

where $\boldsymbol{x}_{pva} \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, \ddot{\boldsymbol{r}}_r^{\mathsf{T}}\right]^{\mathsf{T}}$, $\boldsymbol{x}_{\text{clk}_u} \triangleq \left[c\Delta\delta t_{s,u}, c\Delta\dot{\delta} t_{s,u}\right]^{\mathsf{T}}$, $\Delta\delta t_{s,u} \triangleq \delta t_r - \delta t_{s,u}$, $\Delta\dot{\delta} t_{s,u} \triangleq \dot{\delta} t_r - \dot{\delta} t_{s,u}$, and U is the total number of eNodeBs. The dynamics of $\boldsymbol{x}$ can be expressed as

$$\boldsymbol{x}(k+1) = \mathbf{F}\boldsymbol{x}(k) + \boldsymbol{w}(k), \tag{5.3}$$

where $\mathbf{F} \triangleq \text{diag}\left[\mathbf{F}_{\text{pva}}, \mathbf{F}_{\text{clk}}, \cdots, \mathbf{F}_{\text{clk}}\right]$, with $\mathbf{F}_{\text{pva}}$ and $\mathbf{F}_{\text{clk}}$ defined in (2.12) and (2.18), respectively; and $\boldsymbol{w}(k)$ is the overall process noise vector, which is modeled as a zero-mean white sequence with covariance $\mathbf{Q} \triangleq \text{diag}\left[\mathbf{Q}_{\text{pva}}, \mathbf{Q}_{\text{clk}}\right]$. The dynamics covariance $\mathbf{Q}_{\text{pva}}$ is defined in (2.14) except for $\tilde{\boldsymbol{S}}_{xyz} \equiv \tilde{\boldsymbol{S}}_{\text{NED}}$, where $\tilde{\boldsymbol{S}}_{\text{NED}} = \text{diag}\left[\tilde{q}_{\text{N}}^{'}, \tilde{q}_{\text{E}}^{'}, \tilde{q}_{\text{D}}^{'}\right]$, with $\tilde{q}_x^{'}$, $\tilde{q}_y^{'}$, and $\tilde{q}_z^{'}$ being the NED jerk continuous-time noise spectra, respectively. The clock error covariance $\mathbf{Q}_{\text{clk}}$ is defined as

$$\mathbf{Q}_{\text{clk}} = \Gamma\mathbf{Q}_{\text{clk}_r}\Gamma^{\mathsf{T}} + \mathbf{Q}_{\text{clk}_s}, \tag{5.4}$$

$$\Gamma \triangleq \left[\mathbf{I}_{2\times 2}, \cdots, \mathbf{I}_{2\times 2}\right]^{\mathsf{T}}, \tag{5.5}$$

$$\mathbf{Q}_{\text{clk}_s} \triangleq \text{diag}\left[\mathbf{Q}_{\text{clk}_{s,u=1}}, \cdots, \mathbf{Q}_{\text{clk}_{s,u=U}}\right], \tag{5.6}$$

where $\mathbf{Q}_{\text{clk}_r}$ and $\mathbf{Q}_{\text{clk}_{s,u}}$ are the receiver's and the u-th eNodeB's clock process noise covariance matrices, with $\mathbf{Q}_{\text{clk}_\kappa}$ as defined in (2.18).

5.2.6.2 Navigation Solution

5.2.6.2.1 EKF Settings

The EKF was configured with a measurement rate of $T = 0.01s$, aligning with the duration of the 4G-URS replica. The jerk process noise spectra were set to $\tilde{q}'_{\mathrm{N}} = \tilde{q}'_{\mathrm{E}} = 5\ \mathrm{m}^2/\mathrm{s}^5$ and $\tilde{q}'_{\mathrm{D}} = 1\ \mathrm{m}^2/\mathrm{s}^5$. The covariance matrices for the receiver's and eNodeBs' clock process noise were defined as

$$\mathbf{Q}_{\mathrm{clk}_r} = \begin{bmatrix} 4.22 \times 10^{-5} & 3.37 \times 10^{-7} \\ 3.37 \times 10^{-7} & 6.74 \times 10^{-5} \end{bmatrix}, \tag{5.7}$$

$$\mathbf{Q}_{\mathrm{clk}_{s,u}} = \begin{bmatrix} 3.59 \times 10^{-5} & 3.54 \times 10^{-9} \\ 3.54 \times 10^{-9} & 7.09 \times 10^{-7} \end{bmatrix}. \tag{5.8}$$

Considering the similar altitudes of terrestrial cellular transmitters as viewed from a high-flying aircraft, a large vertical dilution of precision (VDOP) is expected. To address this, the EKF's measurement-update step integrates altimeter data z_{alt} from the aircraft's navigation system with cellular carrier-aided code-phase pseudorange measurements. The altimeter measurement error variance $\sigma^2_{\mathrm{alt}}(k)$ was set to 5 m^2. The cellular measurement noise variances, based on CNR and receiver parameters as discussed in [106], varied between $0.3 - 11.7$ m^2 in Region A and $3.1 - 29.0$ m^2 in Region B.

5.2.6.2.2 Results

Figure 5.29 presents the navigation solution for a flight run featuring a 90°-turn maneuver over Edwards, California, USA (Region A). During this 450-second run covering 42.23 km, navigation observables from 32 out of 144 tracked eNodeBs, coupled with altimeter

measurements, yielded a 4G-based navigation solution with a position RMSE of 9.86 m.

Figure 5.32 illustrates the solution for a flight run with a teardrop maneuver over Palmdale, California, USA (Region B). Over 600 seconds and 56.56 km, observables from 18 out of 84 eNodeBs, alongside altimeter data, produced a navigation solution with a position RMSE of 10.37 m.

Figures 5.30 and 5.33 display CNR, pseudoranges, and errors in clock bias ($\Delta\tilde{\delta}t_{s,u} = \Delta\hat{\delta}t_{s,u} - \Delta\delta t_{s,u}$) and drift ($\Delta\dot{\tilde{\delta}}t_{s,u} = \Delta\dot{\hat{\delta}}t_{s,u} - \Delta\dot{\delta}t_{s,u}$) for the mapped eNodeBs in each flight.

Figures 5.31 and 5.34 exhibit the EKF error plots with $\pm 3\sigma$ bounds for position and velocity in the East and North directions. Variations in σ-bounds are attributed to the relative geometry between the aircraft and eNodeBs, the number of tracked eNodeBs, and model mismatches, particularly during banking maneuvers. Table 5.3 summarizes the navigation performance for Regions A and B.

While the findings presented in this paper offer encouraging prospects for aircraft navigation using cellular terrestrial signals, it is crucial to differentiate between the specific requirements of military operations and civil aviation for practical implementation. This study primarily concentrated on demonstrating the aspects of ranging and accuracy. However, critical factors such as integrity, availability, and continuity have not been addressed and thus merit further investigation. Moreover, the paper raises pertinent questions regarding the alignment of civil aviation's long operational timeline with the rapidly evolving cellular technology. This situation leads to key inquiries: How can we reconcile these potentially conflicting timelines? What kind of commitments should be expected from regulatory bodies, such as the 3GPP, or local cellular service providers, to ensure the viability and reliability of using cellular signals for aviation purposes? These questions underscore the necessity for a collaborative approach involving various stakeholders to successfully integrate cellular technology into aviation systems.

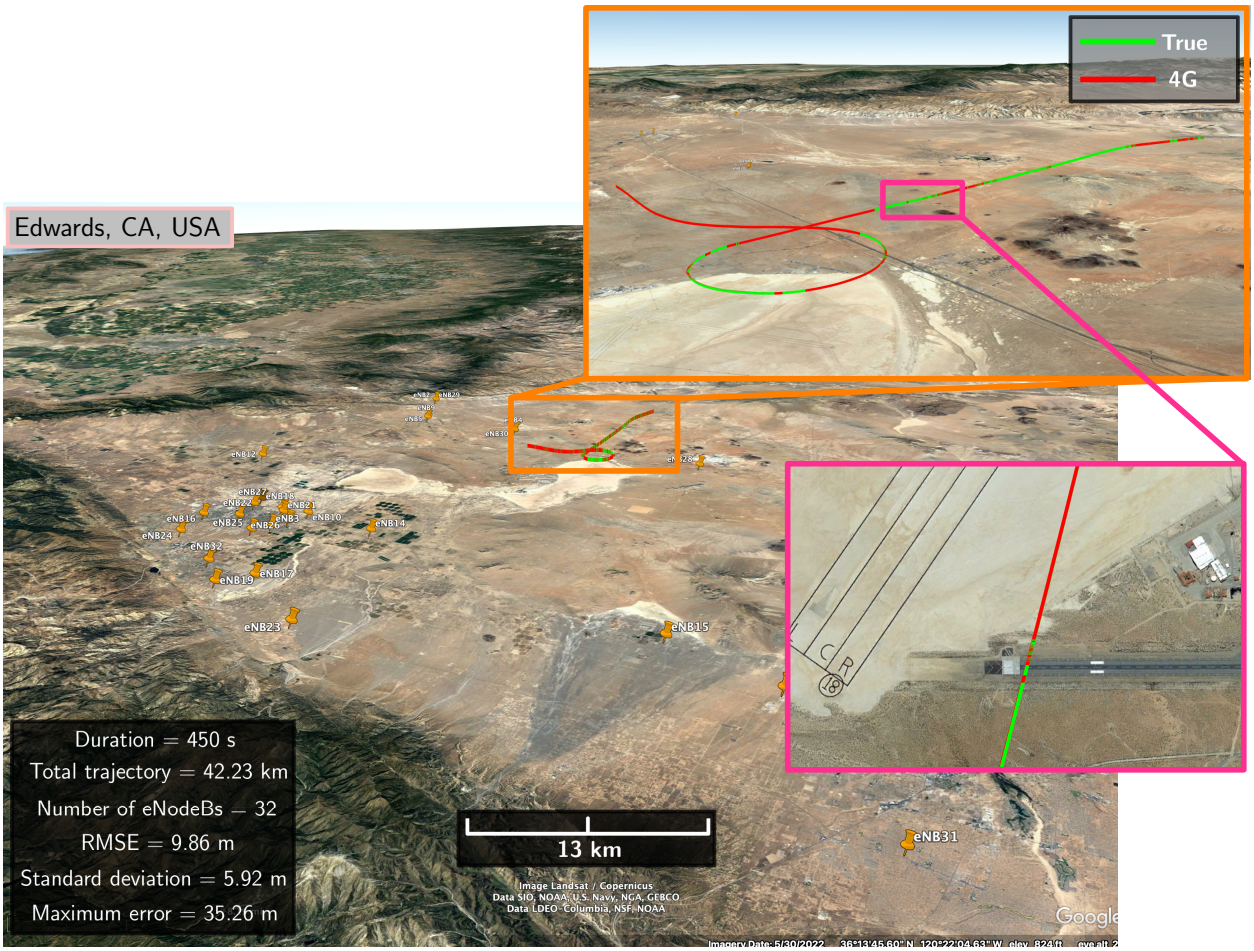


Figure 5.29: High-altitude aircraft navigation – Region A: Edwards, CA, USA – Experimental environment and aircraft navigation results showing: eNodeB positions, true aircraft trajectory, and aircraft trajectory estimated exclusively using cellular 4G signals. The aircraft traversed a total distance of 42.23 km traversed in 450 s during the experiment. The position RMSE over the entire trajectory was 9.86 m.

5.3 5G – Ground Vehicle Scenario

This section presents an experimental demonstration of the proposed 5G receiver mounted on a ground vehicle navigating in a suburban environment while utilizing sub-6 GHz 5G signals from two gNBs. It is shown that while a state-of-the-art frequency-domain-based 5G opportunistic navigation receiver can only reliably track the gNBs' signals over a trajectory of 1.02 km traversed in 100 seconds, producing a position RMSE of 14.93 m; the proposed time-domain-based receiver was able to track over a trajectory of 2.17 km traversed in 230

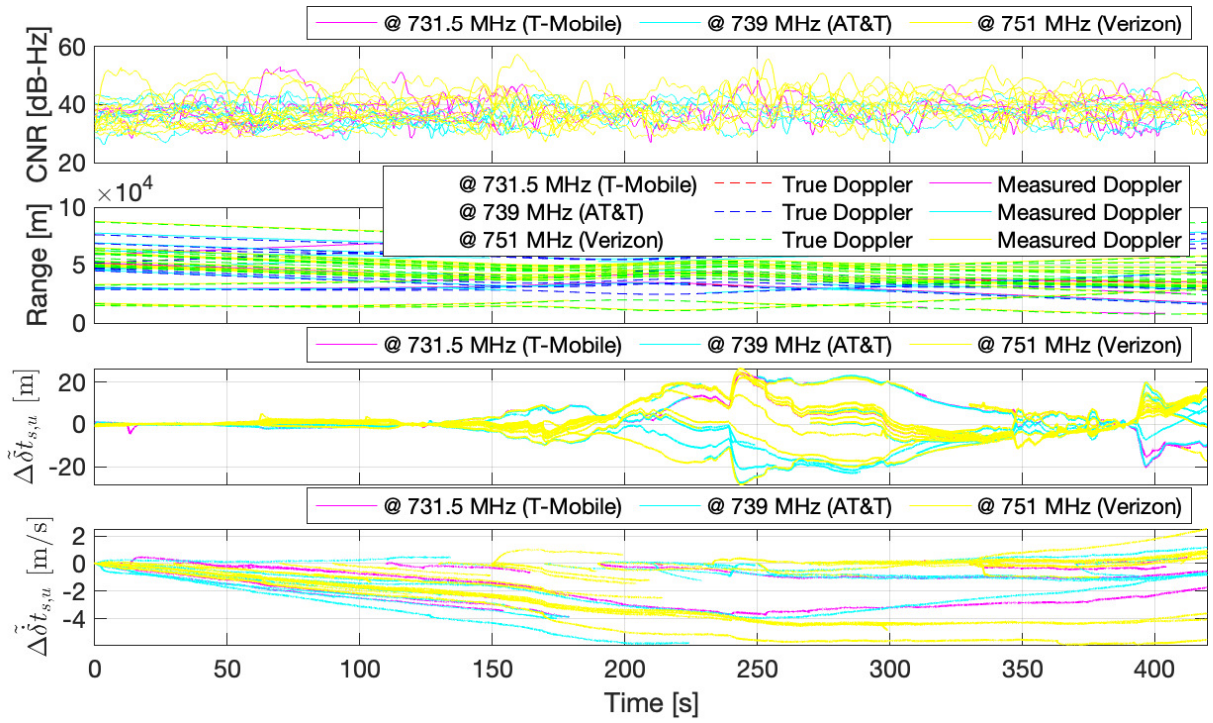


Figure 5.30: High-altitude aircraft navigation – Region A: Edwards, CA, USA – Top to bottom: (a) Time history of CNRs for all eNodeBs used to compute the navigation solution in Region A. (b) Time history of pseudoranges estimated by the proposed receiver and corresponding true range. The initial values of the pseudoranges and ranges were subtracted out for ease of comparison. (c) Time history of the clock bias error (pseudorange plus the estimated bias minus the true range). (d) Time history of the clock drift error (pseudorange rate plus the estimated drift minus the true range rate).

seconds, achieving a position RMSE of 9.71 m.

5.3.1 Experimental Setup and Environmental Layout

The experiment was performed on the Fairview Road in Costa Mesa, California, USA. In this experiment, a quad-channel NI USRP-2955 was mounted on a vehicle, where only two channels were used to sample 5G signals with a sampling ratio of 10 MSps. The receiver was equipped with two consumer-grade cellular omnidirectional Laird antennas. The USRP was tuned to listen to 5G signals from AT&T and T-Mobile U.S. cellular providers as summarized in Table 5.4. The vehicle was equipped with a Septentrio AsteRx-i V integrated GNSS-IMU

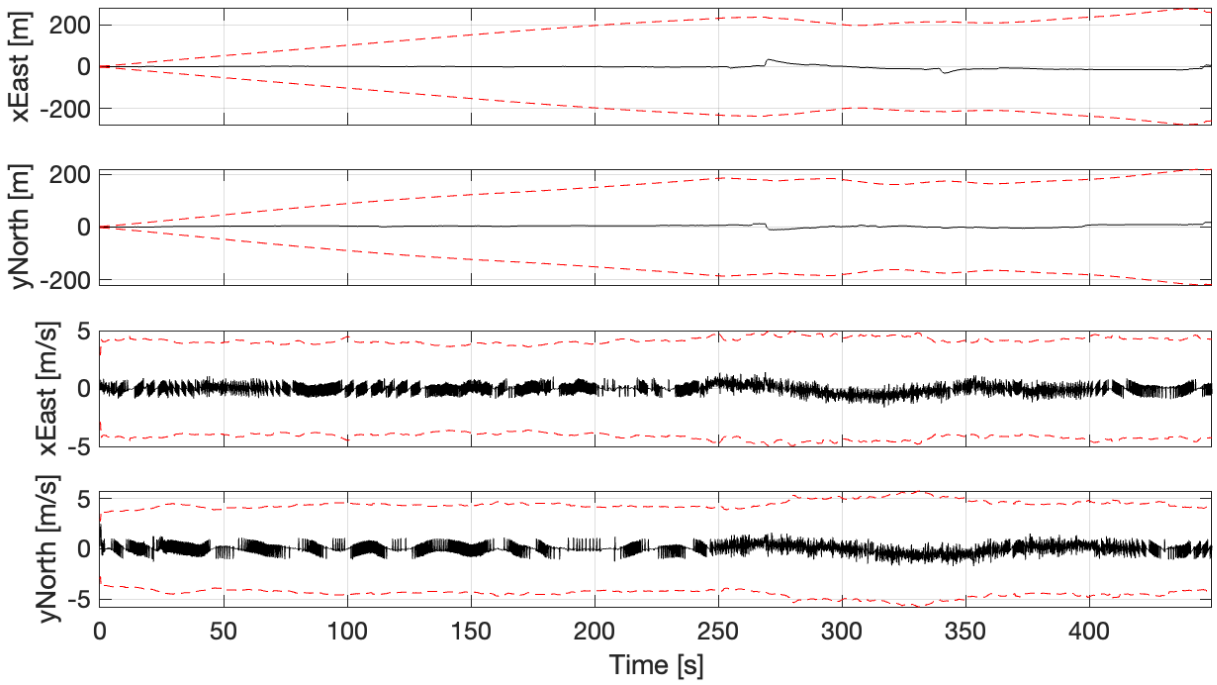


Figure 5.31: High-altitude aircraft navigation – Region A: Edwards, CA, USA – EKF plots showing the time history of the position and velocity errors as well as the $\pm 3\sigma$ bounds.

to be used as a ground truth in this experiment. Figure 5.35 shows the experimental hardware and software setup.

5.3.2 Signal Acquisition and Tracking Performance

The signal acquisition was performed to detect the hearable gNBs. Two gNBs were detected as shown in Figure 5.36. The gNBs' positions were mapped prior to the experiment. In the tracking stage, the 5G signals from both gNBs were tracked for 230 seconds. Figure 5.37 shows the tracking results of the two gNBs including: (i) CNR, (ii) Doppler frequency estimate versus expected Doppler obtained using the ground vehicle's ground truth reference, (iii) pseudorange estimate versus expected range after removing the initial bias, and (iv) range errors.

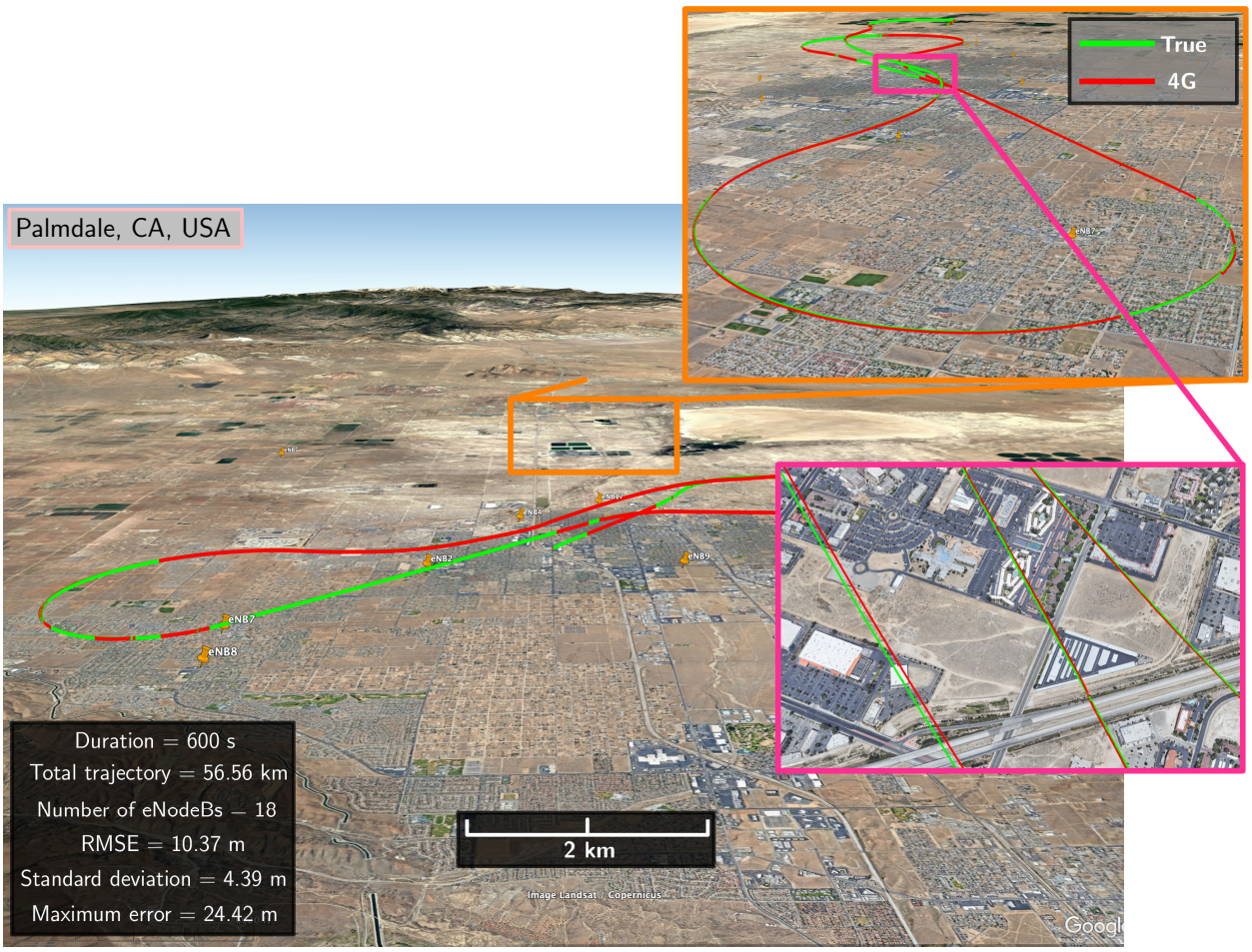


Figure 5.32: High-altitude aircraft navigation – Region B: Palmdale, CA, USA – Experimental environment and aircraft navigation results showing: eNodeB positions, true aircraft trajectory, and aircraft trajectory estimated exclusively using cellular 4G signals. The aircraft traversed a total distance of 56.56 km traversed in 600 s during the experiment. The position RMSE over the entire trajectory was 10.37 m.

5.3.3 Navigation Filter

The 5G pseudorange measurements are fed to an EFK to estimate the state vector $\boldsymbol{x}$ defined as

$$\boldsymbol{x} \triangleq \left[\boldsymbol{x}_r^{\mathsf{T}}, \boldsymbol{x}_{\text{clk}}^{\mathsf{T}}\right]^{\mathsf{T}}, \tag{5.9}$$

$$\boldsymbol{x}_r \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}\right]^{\mathsf{T}}, \tag{5.10}$$

$$\boldsymbol{x}_{\text{clk}} \triangleq \left[c\Delta\delta t_1, c\Delta\dot{\delta} t_1, \cdots, c\Delta\delta t_U, c\Delta\dot{\delta} t_U\right]^{\mathsf{T}} \tag{5.11}$$

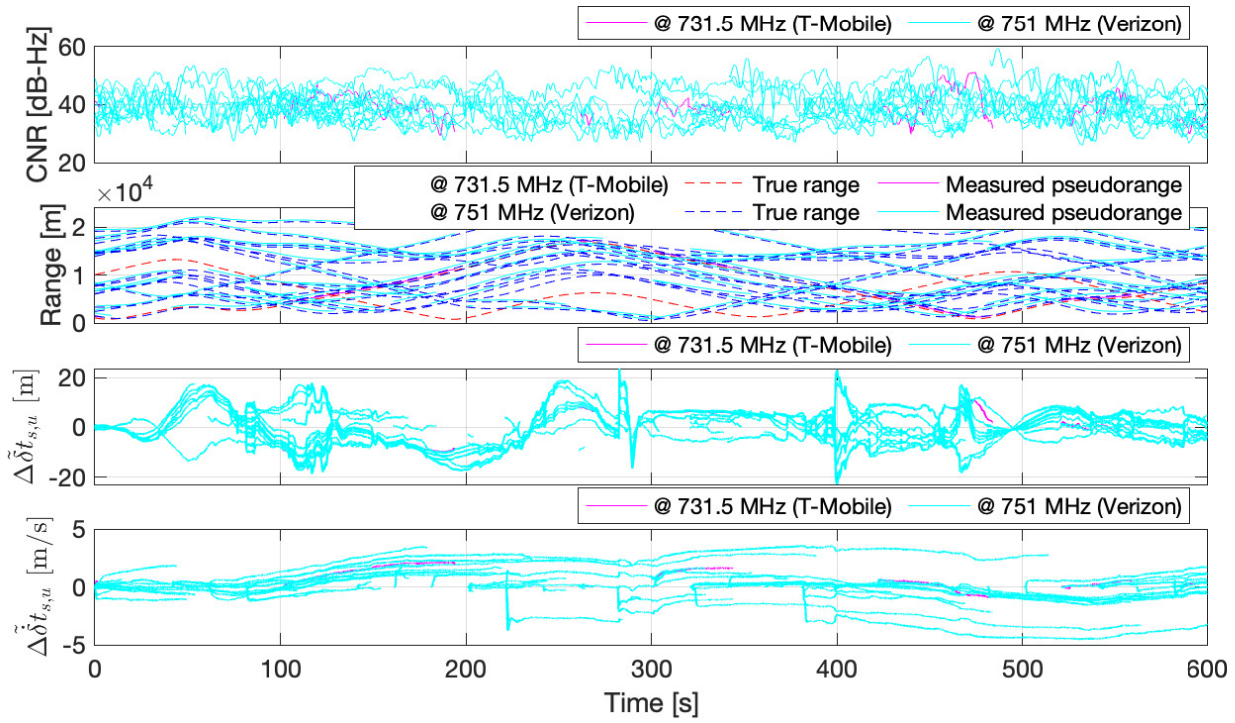


Figure 5.33: High-altitude aircraft navigation – Region B: Palmdale, CA, USA – Top to bottom: (a) Time history of CNRs for all eNodeBs used to compute the navigation solution in Region A. (b) Time history of pseudoranges estimated by the proposed receiver and corresponding true range. The initial values of the pseudoranges and ranges were subtracted out for ease of comparison. (c) Time history of the clock bias error (pseudorange plus the estimated bias minus the true range). (d) Time history of the clock drift error (pseudorange rate plus the estimated drift minus the true range rate).

where and $\boldsymbol{x}_{\text{clk}}$ is the clock error state vector, $\{\Delta\delta t_u \triangleq \delta t_r - \delta t_{s,u}\}_{u=1}^{U}$ and $\{\Delta\dot{\delta} t_u \triangleq \dot{\delta} t_r - \dot{\delta} t_{s,u}\}_{u=1}^{U}$ are the relative clock bias and drift between the receiver and the u-th gNB. The temporal evolution of $\boldsymbol{x}_r$ used in the EKF is assumed to follow the white noise acceleration model, as discussed in Subsection 2.3.1, and the clock error dynamics is assumed to follow a double integrator driven by process noise model, as discussed in Subsection 2.4.

5.3.4 Navigation Solution

The vehicle traversed a trajectory of 2.17 km in 230 seconds. The receiver's position and velocity state vectors and their corresponding covariances were initialized from the GNSS-

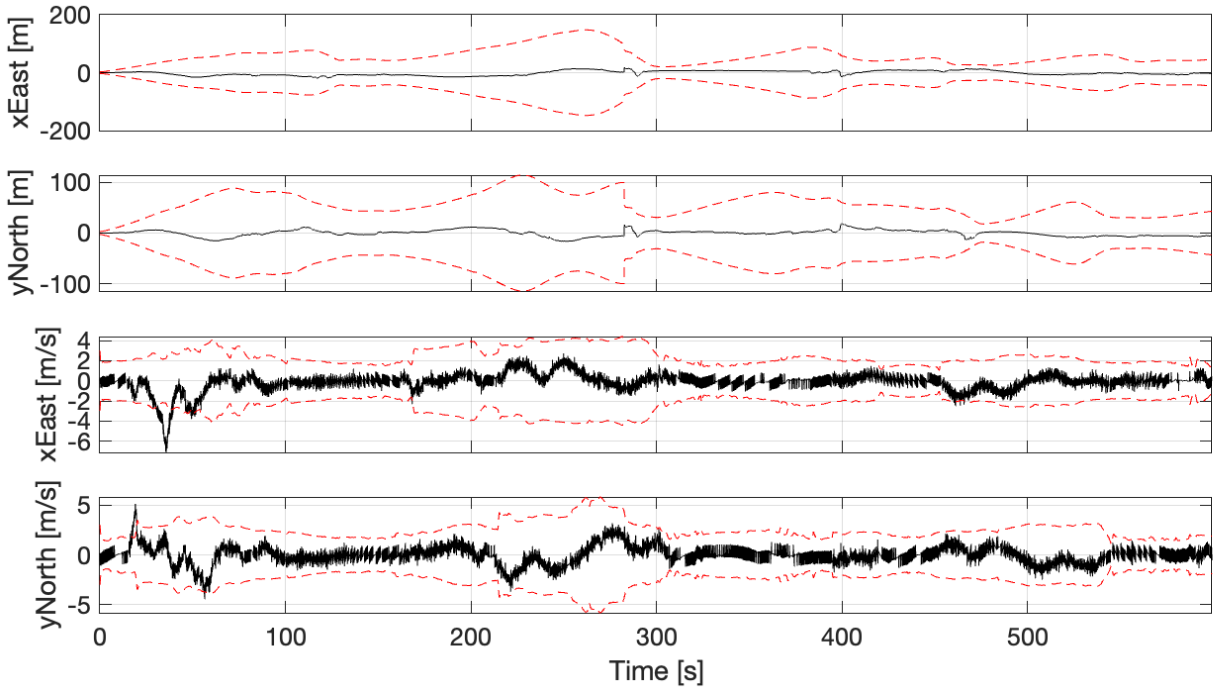


Figure 5.34: High-altitude aircraft navigation – Region B: Palmdale, CA, USA – EKF plots showing the time history of the position and velocity errors as well as the $\pm 3\sigma$ bounds.

IMU system. Using the expressions of measurement noise variances as a function of the CNR and receiver parameters in [107], the variances were found to vary between 0.67 to 12.78 m^2. Figure 5.38 shows the environmental layout, 5G gNBs location, and the navigation solution of the proposed 5G framework versus ground truth. The proposed 5G opportunistic navigation framework tracked the 5G signals, achieving a position RMSE of 9.71 m. In contrast, the previous generation 5G SDR, presented in Subsection 3.1.2, was only able to track over a shorter segment of 1.02 km, achieving a position RMSE of 14.93 m as shown in Figure 5.39. It is worth noting that due to bad gNB geometric diversity, the majority of errors are in the east direction. Figure 5.40 shows the EKF errors of the ground vehicle's (a) east-position, (b) north-position, along with the associated $\pm 1\sigma$ bounds, and (c) position errors along the east and the north directions.

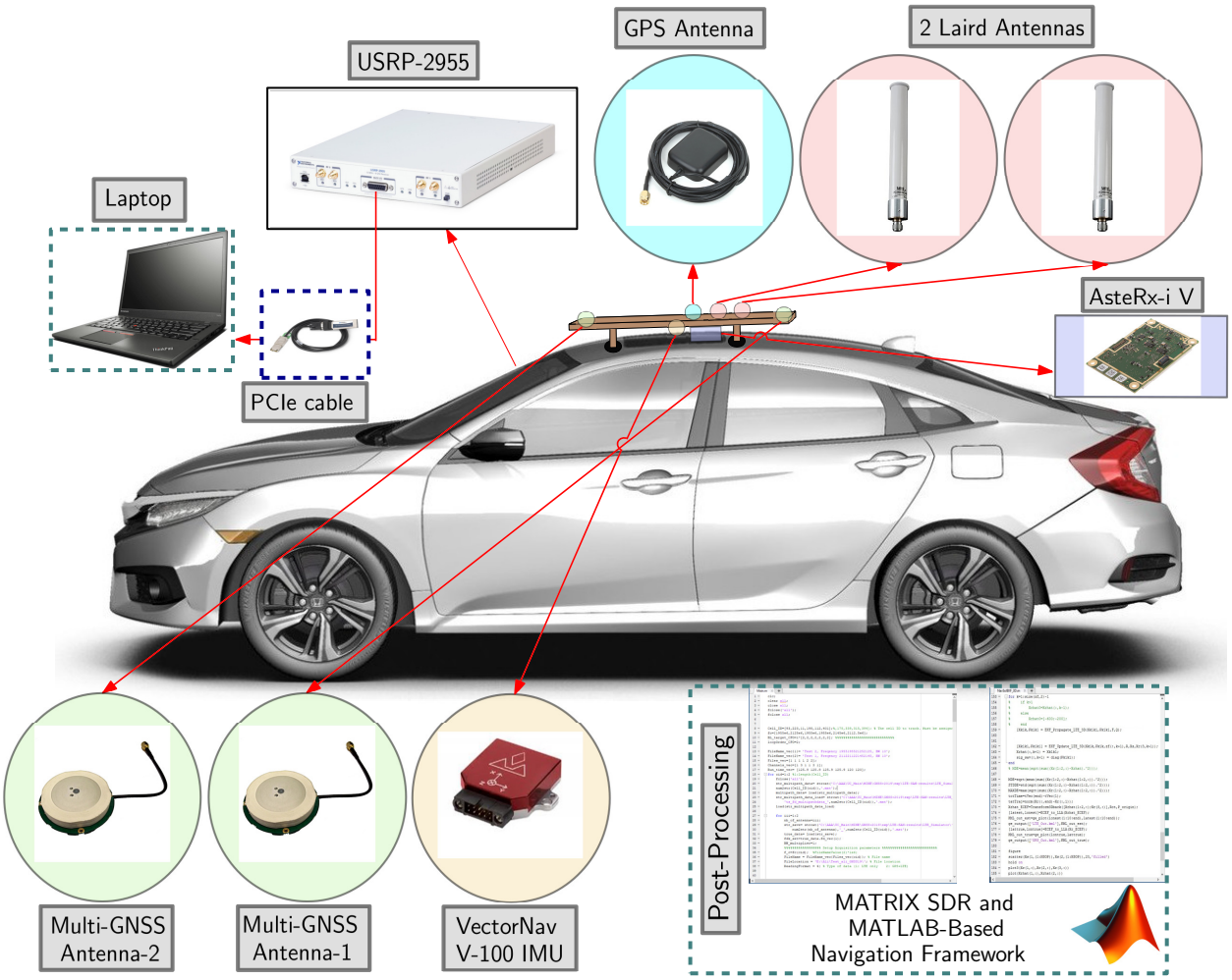


Figure 5.35: Experimental hardware and software setup.

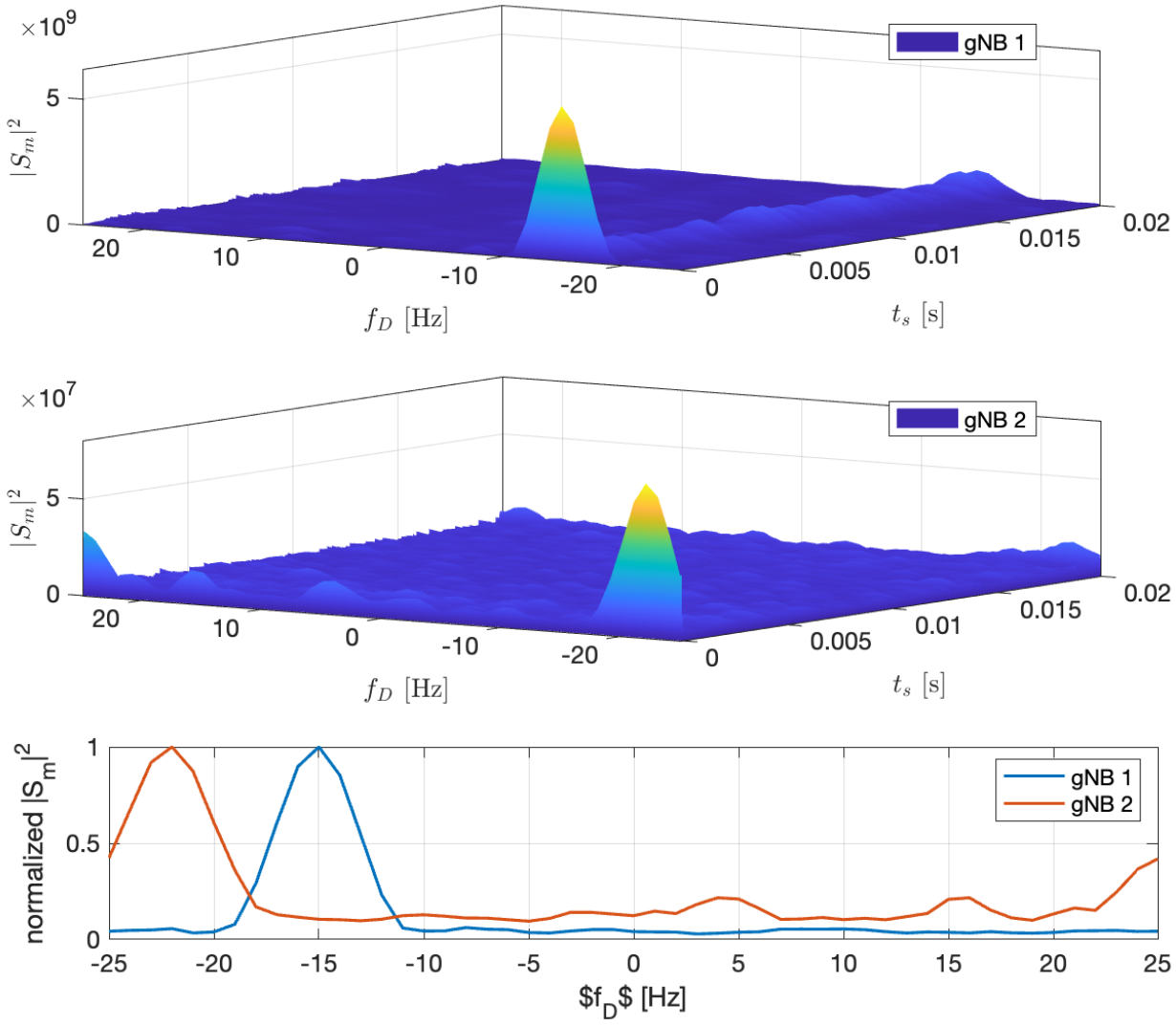


Figure 5.36: Cellular 5G signal acquisition results showing squared correlation magnitude $|S_m|^2$ versus initial estimates of the code start time $\hat{t}_{s_0}$ and Doppler frequency $\hat{f}_{D_0}$ for the two detected gNBs.

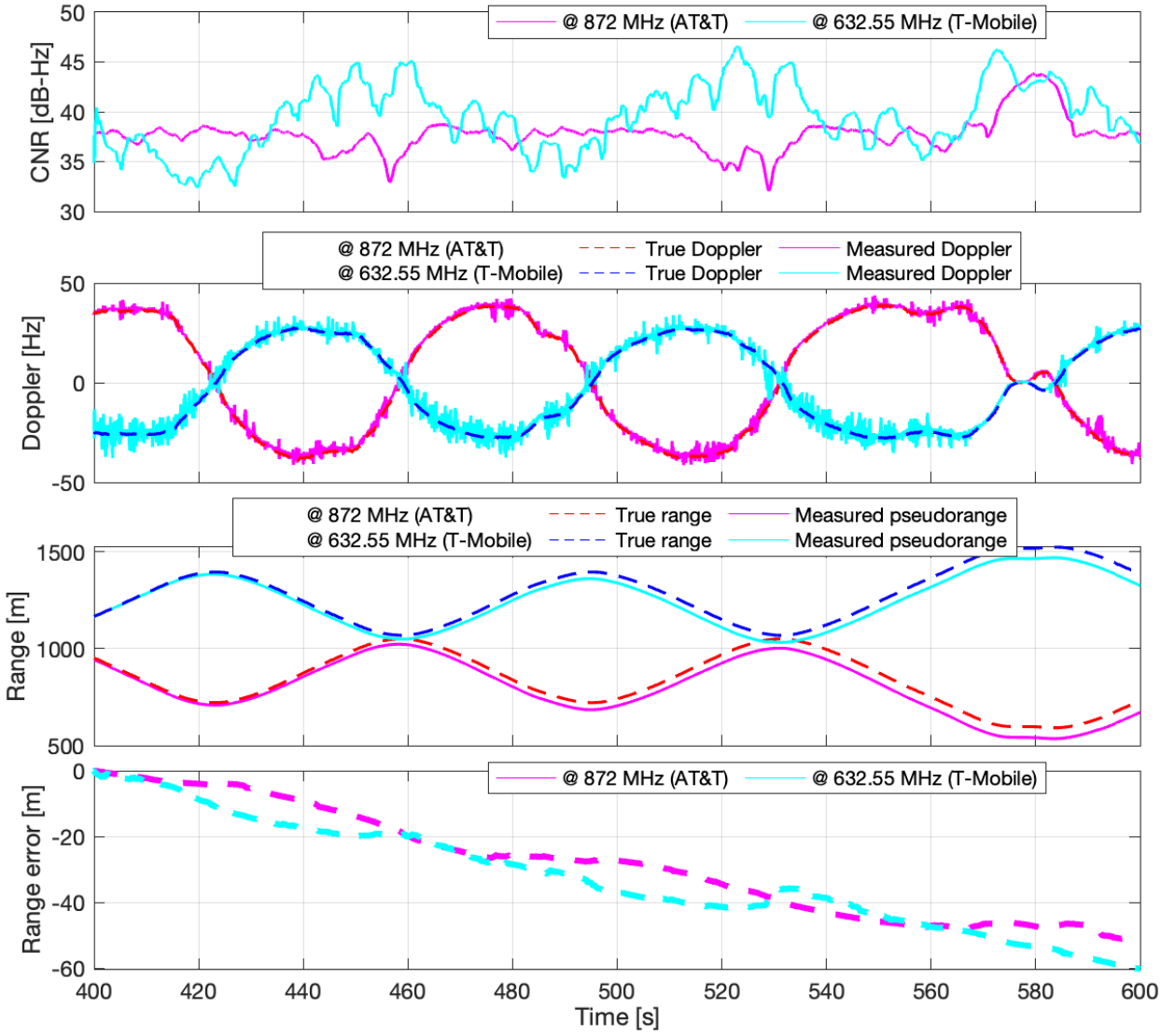


Figure 5.37: Cellular 5G signal tracking results of the two gNBs showing: (i) CNR, (ii) Doppler frequency estimate in solid lines versus expected Doppler obtained using the vehicle's ground-truth reference in dashed lines, (iii) pseudorange estimate in solid lines versus expected range in dashed lines after removing the initial bias, and (iv) range errors.

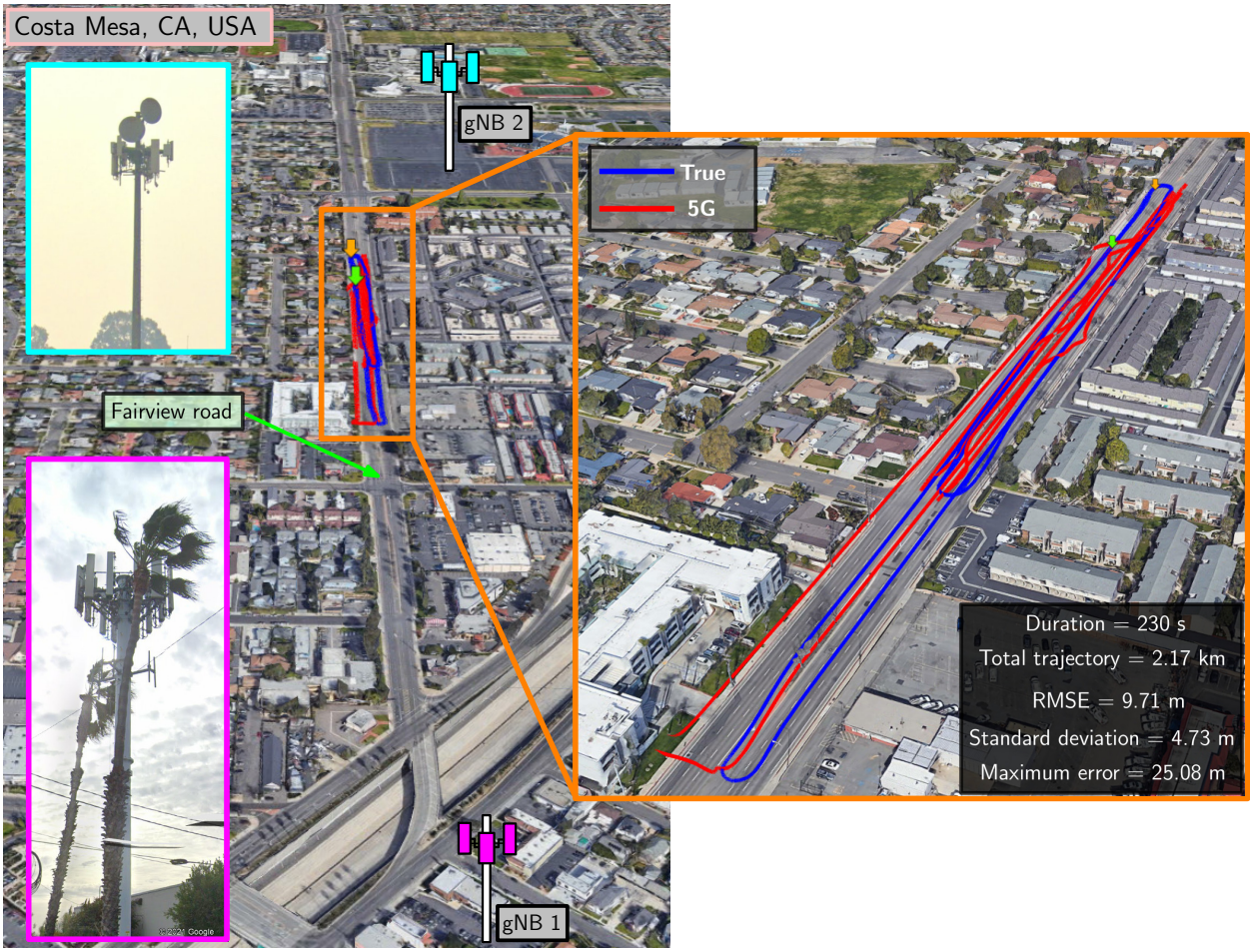


Figure 5.38: Environmental layout with 5G gNBs and the traversed trajectory (ground truth versus estimated with 5G signals). Image: Google Earth.

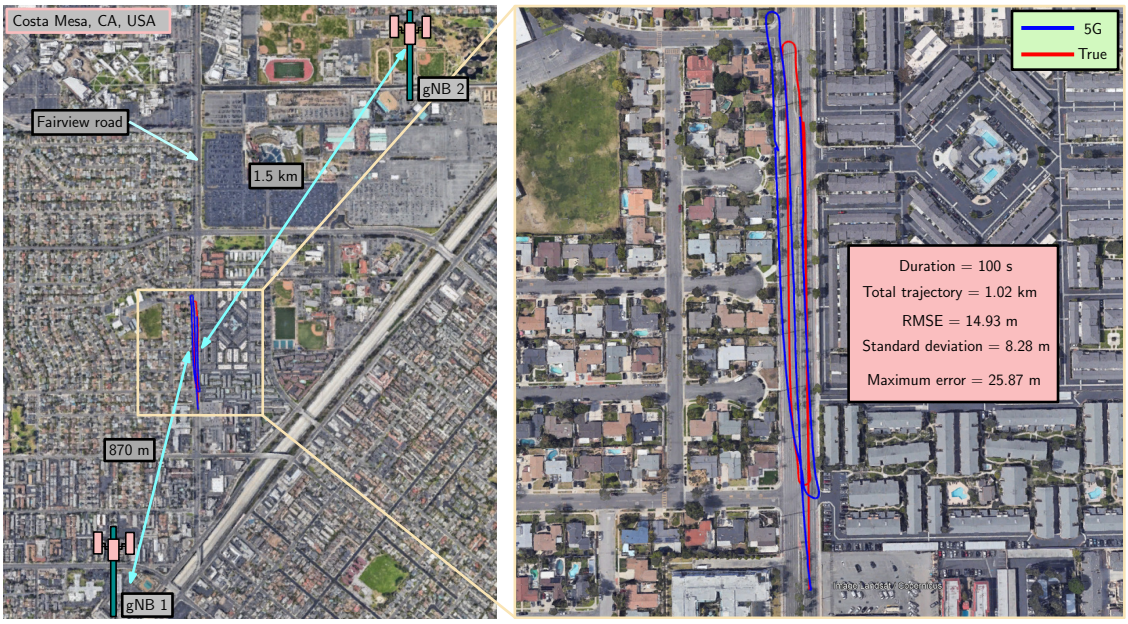


Figure 5.39: Environmental layout with 5G gNBs and the traversed trajectory (ground truth versus estimated with 5G signals) when using the conventional 5G receiver. Image: Google Earth.

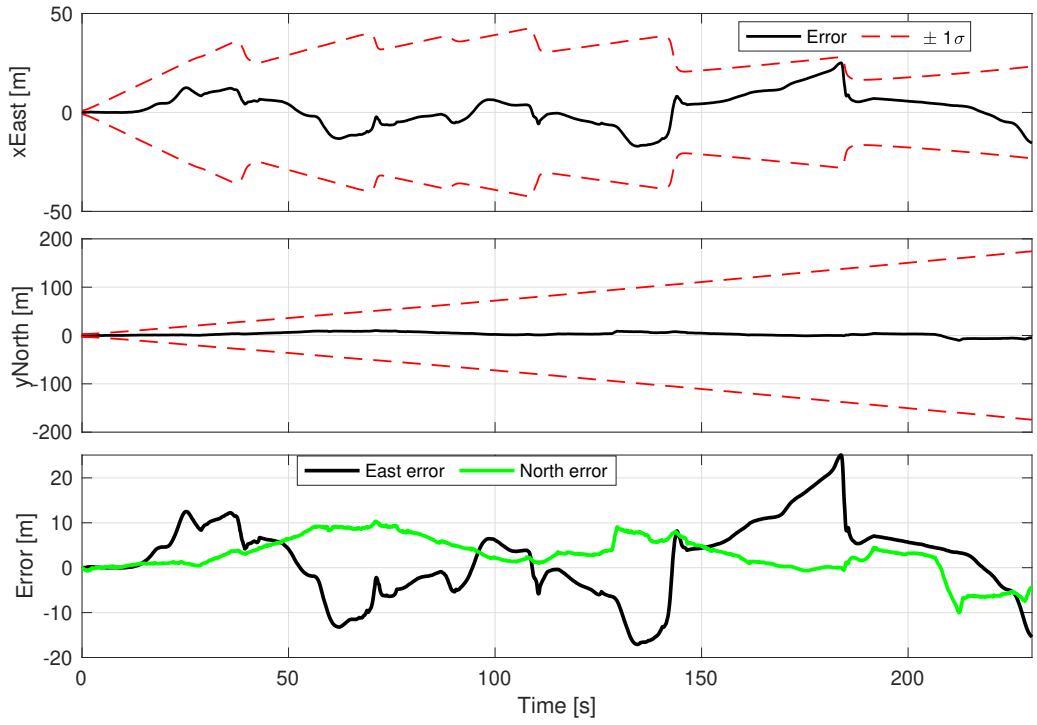


Figure 5.40: The EKF estimation of the ground vehicle's (a) east-position and (b) north-position along with the associated $\pm 3\sigma$ bounds. (c) A comparison of the position errors along the east and the north directions.

Table 5.3: Navigation Performance with Cellular 4G Signal on High Altitudes.

Metric	Region A	Region B
Total number of tracked eNodeBs	144	84
Total number of unique eNodeBs used (mapped)	32	18
Number of {min, max} eNodeBs used	17-27	5-17
Cellular frequency [MHz]	731.5. 739, 751	731.5, 739
Flight duration [sec]	450	600
Flight length [km]	42.23	56.56
Altitude range AGL [ft] [MHz]	7,530-7,598	3,540-4,573
Position RMSE [m]	9.86	10.37
Velocity RMSE [m/s]	0.34	0.39
Position error standard deviation [m]	5.92	4.39
Velocity error standard deviation [m/s]	0.19	0.22
Maximum position error [m]	35.26	24.42
Maximum velocity error [m/s]	3.62	3.14

Table 5.4: gNBs's Characteristics.

gNB	Carrier frequency [MHz]	N_{ID}^{Cell}	Cellular provider
1	872	608	AT&T
2	632.55	398	T-Mobile

5.4 5G – Unmanned Aerial Vehicle Scenario

This section presents an experimental demonstration of the proposed 5G receiver mounted on a UAV over an urban environment. The experimental results of a UAV navigating with the proposed 5G SDR, while receiving signals from four 5G gNBs, are demonstrated. It is shown that over a trajectory of 500 m traversed in 145 seconds, the position RMSE was 3.35 m.

Figure 5.41: Experimental setup.

5.4.1 Experimental Setup and Environmental Layout

An experiment was conducted in Santa Ana, California, USA. In the experiment, the navigator was an Autel Robotics X-Star Premium UAV equipped with a single-channel Ettus 312 USRP connected to a consumer-grade 800/1900 MHz cellular antenna and a small consumer-grade GPS antenna to discipline the on-board oscillator. The cellular receivers were tuned to the cellular carrier frequency 632.55 MHz, which is a 5G frequency allocated to the U.S. cellular provider T-Mobile. The Samples of the received signals were stored for off-line postprocessing with a sampling ratio of 10 MSps. The ground-truth reference trajectory was taken from the on-board Ettus 312 USRP GPS solution. The UAV traversed a trajectory of 500 m in 145 seconds. Figures 5.41 and 5.42 show the experimental setup and the environment layout, respectively.

5.4.2 Receiver Output

The signal acquisition process was applied to detect the ambient 5G signals from the collected data. Based on experimental data, the Doppler frequency search window was chosen to be between -25 and 25 Hz. The code start time search window was chosen to be one code interval with a delay spacing of one sample. Four gNBs were detected, three of which were hearable starting at $t_n = 0$ seconds, and a fourth gNB was hearable at $t_n = 25$ seconds. The gNBs' positions were mapped prior to the experiment. Figure 5.43 shows $|S_m|^2$ versus $\hat{t}_{s_0}$

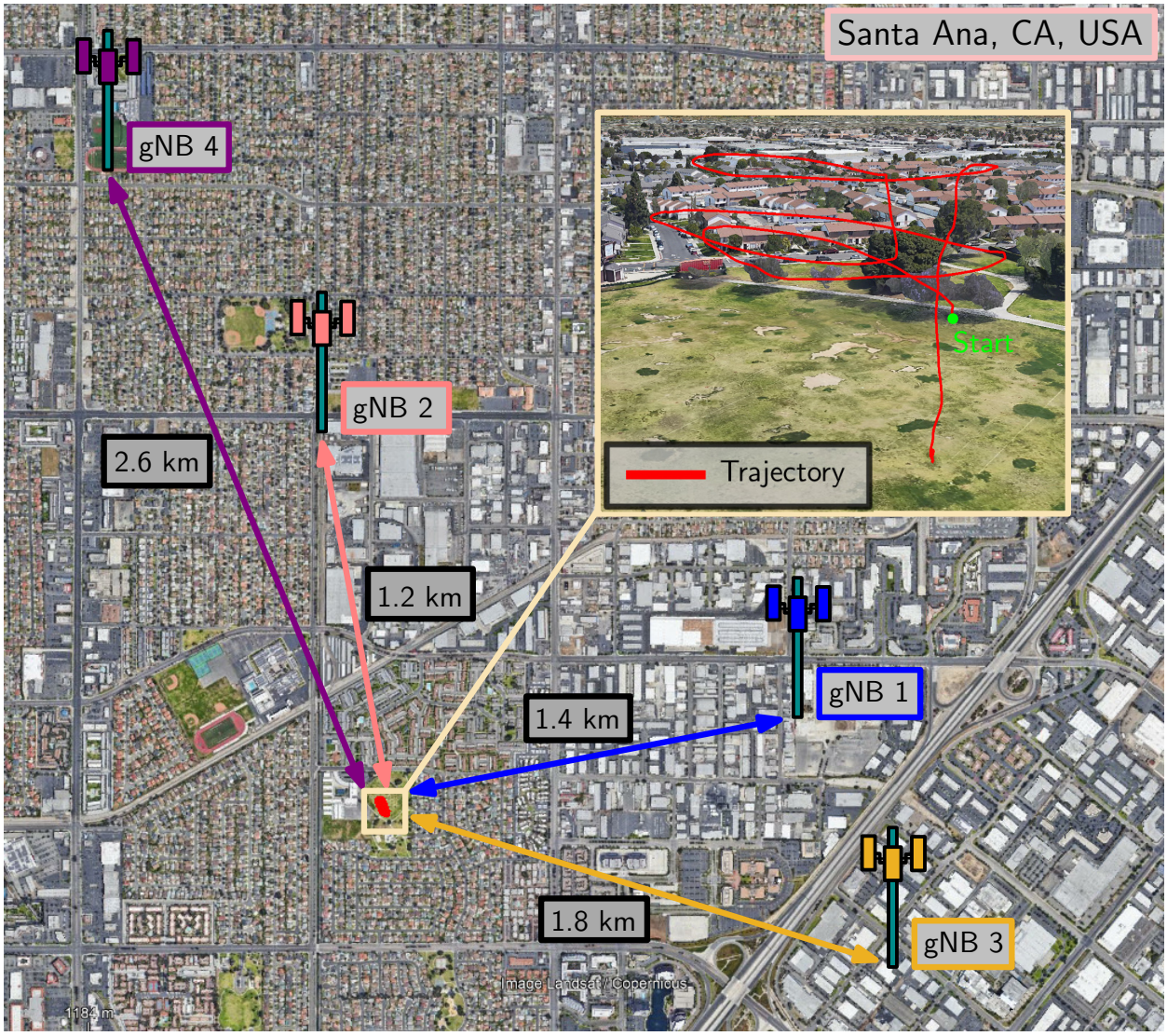


Figure 5.42: Environmental layout and UAV trajectory.

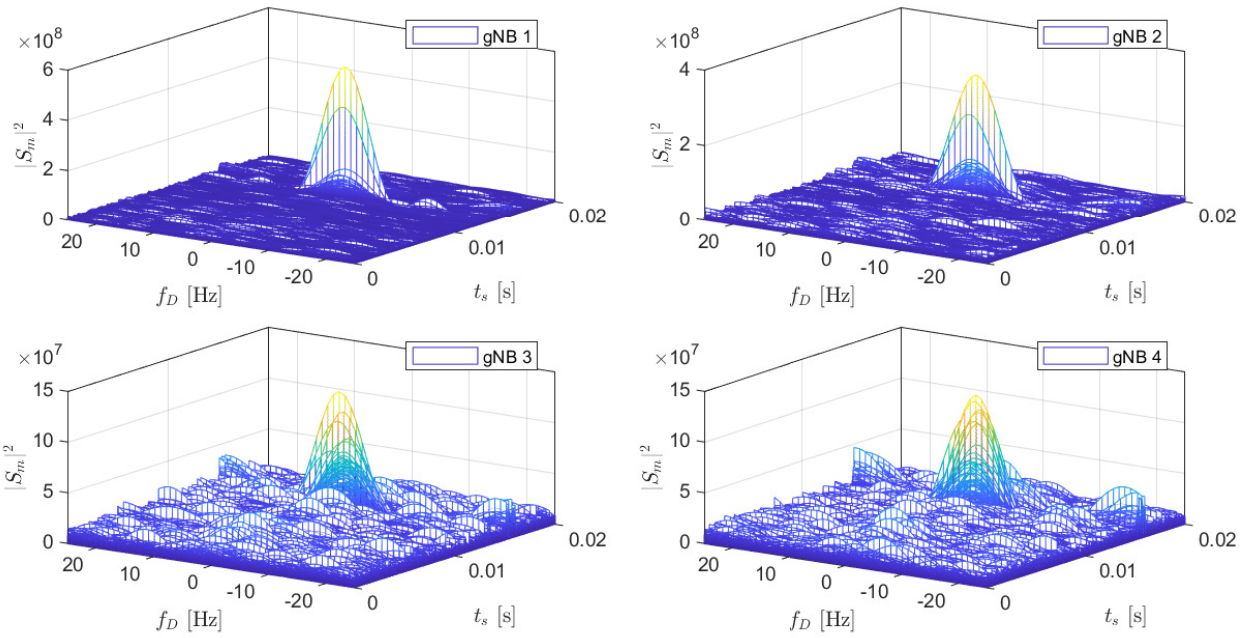


Figure 5.43: Cellular 5G signal acquisition results showing $|S_m|^2$ versus $\hat{t}_{s_0}$ $\hat{f}_{D_0}$ for the four detected gNBs.

$\hat{f}_{D_0}$ for the four detected gNBs.

In the tracking stage, the noise-equivalent bandwidths $B_{n,\text{PLL}}$ and $B_{n,\text{DLL}}$ were chosen to be 6 Hz and 0.05 Hz, respectively. Figure 5.44 shows cellular 5G signal tracking results of the four gNBs including: (i) CNR, (ii) Doppler frequency estimate in solid lines versus expected Doppler obtained using the UAV's ground-truth reference in dashed lines, (iii) Pseudorange estimate in solid lines versus expected range in dashed lines after removing the initial bias, and (iv) range error estimate in solid lines versus measured error in dashed lines.

5.4.3 Navigation Solution

The 5G measurements are fed into an EKF similar to the one deployed in Subsection 5.3.3 to produce the position estimates. The UAV traversed a distance of 500 m in 145 seconds. The receiver's position and velocity state vectors and their corresponding covariances were initialized using the output of the Ettus 312 USRP GPS solution. The initial relative clock

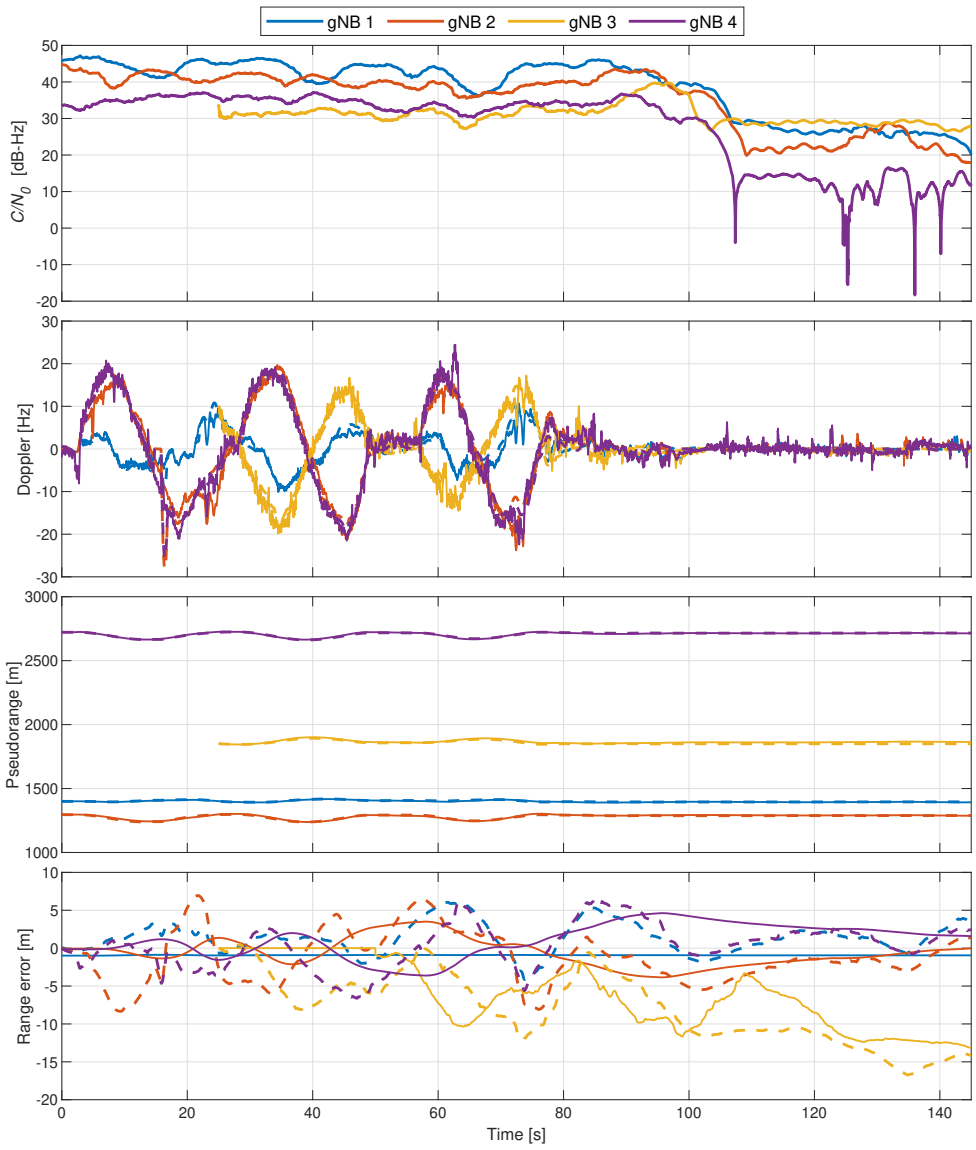


Figure 5.44: Cellular 5G signal tracking results of the four gNBs showing: (i) CNR, (ii) Doppler frequency estimate in solid lines versus expected Doppler obtained using the UAV's ground-truth reference in dashed lines, (iii) Pseudorange estimate in solid lines versus expected range in dashed lines after removing the initial bias, and (iv) range error estimate in solid lines versus measured error in dashed lines.

Figure 5.45: The 5G navigation solution exhibited a position RMSE of 3.35 m versus the ground-truth reference navigation solution. Image: Google Earth.

biases were eliminated, i.e., the EKF's relative clock biases were initialized to zero. The first two 5G measurements were dropped, where the first two positions from the Ettus 312 GPS solution were used to initialize the relative clock drifts. The receiver's and gNBs' clocks were modeled as OCXO with $S_{\tilde{w}_{\delta t_j}} = 1.3 \times 10^{-22}$ and $S_{\tilde{w}_{\dot{\delta} t_j}} = 7.9 \times 10^{-25}$ [108]. The process noise power spectral densities $\tilde{q}_x$ and $\tilde{q}_y$ were set to 0.1 ($\mathrm{m}^2/\mathrm{s}^3$).

Figure 5.45 shows the navigation solution of the USS-based 5G receiver versus the Ettus 312 GPS solution. The proposed receiver yielded a UAV position RMSE of 3.35 m.

Chapter 6

Exploiting On-Demand 5G Downlink Signals for Opportunistic Navigation

This chapter is organized as follows. Section 6.1 establishes the foundation by motivating the problem under study. In Section 6.2, we introduce the pioneering UE-based 5G navigation framework that capitalizes on the 'on-demand' 5G downlink signals. This section elaborates on the various phases involved in the framework, including the acquisition of 5G-URS, its preprocessing, and the development of tracking loops. Section 6.3 details the innovative implementation of UE-based carrier and code phase tracking, leveraging the full bandwidth of the sampled 5G downlink. It also presents and evaluates the results of 5G-URS acquisition, preprocessing, and tracking using real 5G data from the existing sub-6 GHz 5G infrastructure in the US.

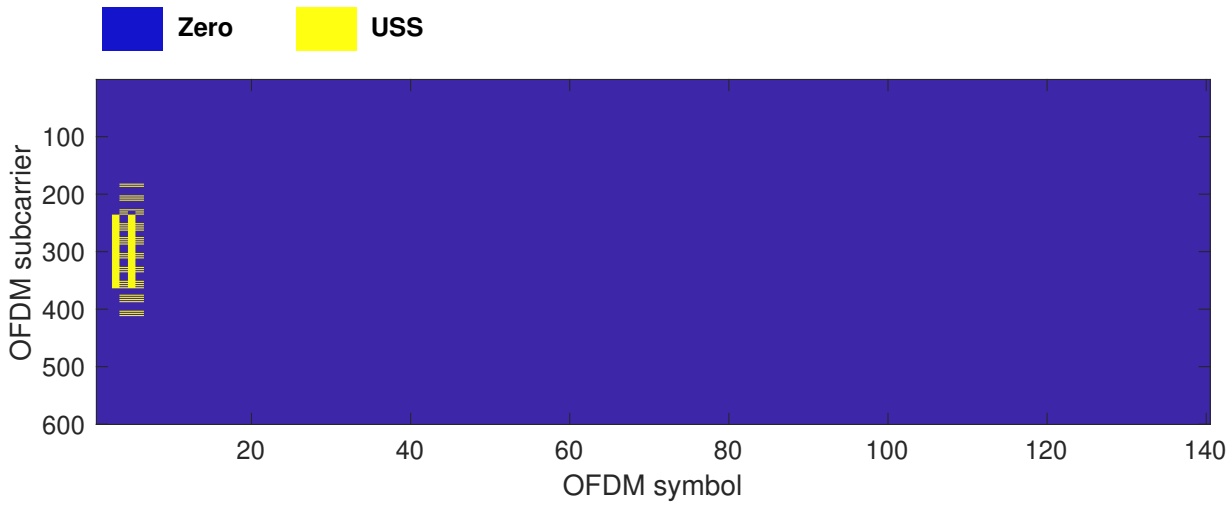


Figure 6.1: The 5G-USS OFDM locally-generated frame.

6.1 Motivation

The carrier-aided code phase-based 5G receiver that was proposed in Section 3.3, demonstrated its superior performance compared to the conventional frequency-based state-of-the-art SDR discussed in Subsection 3.1.2, and claimed the state-of-the-art status. However, the proposed SDR extracts navigation observables only from the known "always-on" 5G downlink denoted by 5G-USS while utilizing the time-domain orthogonality of downlink signals. The 5G-USS is essentially the 5G frame with a normalized SS/PBCH and zeros elsewhere. Aside from the improvement that this approach achieved, it is still limited by the ratio of USS bandwidth versus the entire downlink bandwidth $r_{\mathrm{B,5G-USS}}$ and the duty factor $r_{\mathrm{T,5G-USS}}$, which limits the accuracy of the delay and carrier phase estimates, respectively [109]. For different configurations, $r_{\mathrm{B,USS}}$ and $r_{\mathrm{T,USS}}$ range between 14.5%–36% and 0.0104%–5.33%, respectively. Figure 6.1 shows the USS locally-generated 5G frame in the frequency-domain, where only the yellow REs are known to the UE, and the rest is set to zero. The depicted frame represents a 5G downlink signal with $\mu = 0$, 10 MHz bandwidth, $r_{\mathrm{B,5G-USS}} = 36\%$, and $r_{\mathrm{T,5G-USS}} = 1.33\%$.

The "always-on" approach requires knowing the signal structure, specifically the RSs. To alleviate this, a cognitive opportunistic navigation (CON) framework was proposed in [110] to exploit all available RSs, including ones unknown to the UE. The CON framework successfully estimated a periodic 5G RS, which was subsequently tracked, and exploited for navigation. However, the following question arises: How much of the available resources does the cognitively-acquired RS capture compared to the "always-on" (i.e., 5G-USS)? Given that the OFDM frame start time is unknown in the CON framework, the only way to assess the acquired signal is to look at the narrowness of the normalized ACF of both RSs, which gives an estimate of the bandwidth that is being exploited (i.e., $r_{\mathrm{B,RS}}$). The results in [110] showed $r_{\mathrm{B,5G-CON}} = 25\%$ versus $r_{\mathrm{B,5G-USS}} = 36\%$.

The CON framework suffers from the following limitations

- The acquisition in the CON framework is challenged by the propagation channel fading and stationarity, which limits the coherent processing interval (CPI), i.e., the time interval in which the Doppler, delay, and channel gains are considered constant. Short CPI means fewer resources to be captured in the cognitively-acquired signal.

- The CON framework requires the UE to be in motion to exploit multiple gNBs transmitting on the same channel. Yet, to do so, the CON framework uses Doppler subspace to differentiate between gNBs; thus, the framework acquires only the most powerful gNB among different gNBs with similar Doppler profiles. This results in acquiring fewer gNBs than the "always-on" approach.

- The 5G frame start time remains unknown in the CON framework; hence, it is not possible to construct the frame structure of the acquired signal. As such, pre-filtering and power allocation of different RSs cannot be performed, which affects the fidelity of the acquired signal.

6.2 Proposed Framework

This section presents the proposed framework in which the on-demand 5G signals are exploited. The framework aims to maximize $r_{\mathrm{B,5G-URS}}$ and $r_{\mathrm{T,5G-URS}}$ by exploiting other periodic RSs in the 5G downlink signals that are unknown to the UE, such as: channel state information RS (CSI-RS); other DM-RSs for the physical downlink control channel (PDCCH) and physical data shared channel (PDSCH); and phase tracking RS (PTRS).

6.2.1 Signal Model

The received baseband signal model can be expressed as

$$\begin{aligned} r[n] = \sum_{u=1}^{N} & \left(\alpha_u c_u[\tau_n - t_{s_u}[n]] \exp\left(j\theta_u[\tau_n]\right)\right. \\ & \left. + d_u[\tau_n - t_{s_u}[n]] \exp\left(j\theta_u[\tau_n]\right)\right) + w[n], \end{aligned} \tag{6.1}$$

where $r[n]$ is the received signal at the nth time instant; α_u is the complex channel gain between the UE and the u-th gNB; τ_n is the sample time expressed in the receiver time; N is the number of gNBs; $c_u[n]$ is the periodic RS with a period of L samples; $t_{s_u}[n]$ is the code-delay corresponding to the UE and the u-th gNB at the nth time instant; $\theta_u[\tau_n] = 2\pi f_{D_u}[n] T_s n$ is the carrier phase in radians, with $f_{D_u}[n]$ being the Doppler frequency at the nth time instant and T_s is the sampling time; $d_u[\tau_n]$ represents the samples of some data transmitted from the u-th gNB; and $w[n]$ is a zero-mean independent and identically distributed noise with $\mathbb{E}\{w[m]w^*[n]\} = \sigma_w^2 \delta[m-n]$, where $\delta[n]$ is the Kronecker delta function, and X^* denotes the complex conjugate of random variable X.

6.2.2 Proposed Approach

The structure of the proposed framework is shown in Figure 6.2. This framework utilizes a so-called URS for 5G opportunistic navigation, which takes advantage of both "always-on" and "on-demand" 5G downlink RSs. Since the USS is always transmitted in the 5G downlink signal, it is used as a prior to acquire OFDM resources, which (i) extends the CPI, (ii) uses the USS subspace to exploit all available gNBs (even gNBs with similar Doppler profiles), and (iii) allows preprocessing of the acquired replica to suppress noise and interference and maintain equally-distributed power among different RSs.

6.2.2.1 5G-USS-Based Acquisition and Tracking

In the acquisition stage, the USS is used to determine which gNBs are in the UE's proximity and obtain a coarse estimate of their corresponding code start times $\left\{\hat{t}_{s_{u,0}}\right\}_{u=1}^{U}$ and Doppler frequencies $\left\{\hat{f}_{D_{u,0}}\right\}_{u=1}^{U}$, where U is the total number of gNBs.

In the tracking stage, the receiver refines these coarse estimates via a PLL and a carrier-aided DLL. At first, node A in Figure 6.2 is connected to 1 and the tracking loops use the USS as the local replica. These two steps are discussed in detail in Subsections 3.3.2 and 3.3.3.

6.2.2.2 5G-URS Acquisition

After the tracking loop achieves lock, the acquisition of the 5G-URS is performed as

$$\mathbf{URS}_{5\mathrm{G},u} \triangleq \frac{1}{K}\sum_{k=1}^{K}\hat{\boldsymbol{y}}_{u,k}, \tag{6.2}$$

where K is the total number of 5G frames used to capture the 5G-URS and $\hat{\boldsymbol{y}}_{u,k}$ is the received k-th 5G frame, defined as

$$\hat{\boldsymbol{y}}_{u,k} \triangleq \exp(-j2\pi \hat{f}_{D_{u,k}}[\boldsymbol{\tau}_k]) \odot \boldsymbol{r}_k[(n - \lfloor \hat{t}_{s_{u,k}} \cdot f_s \rceil)_L], \tag{6.3}$$

where $\boldsymbol{a} \odot \boldsymbol{b}$ is the element-wise product, $\lfloor \cdot \rceil$ rounds the argument to the nearest integer, $(\cdot)_L$ denotes modulo-L operation, f_s is the sampling frequency, and $\boldsymbol{r}_k$ and $\boldsymbol{\tau}_k$ are defined as

$$\boldsymbol{r}_k \triangleq [r[(k-1)L+1], r[(k-1)L+2], \cdots, r[kL]]^{\mathsf{T}},$$
$$\boldsymbol{\tau}_k \triangleq \left[\tau_{(k-1)L+1}, \tau_{(k-1)L+2}, \cdots, \tau_{kL}\right]^{\mathsf{T}}.$$

6.2.2.3 5G-URS Preprocessing

A main advantage of the proposed framework is its ability to estimate the 5G OFDM frame start time. This allows converting the captured time-domain 5G-URS into 5G frame structure (i.e., frequency-domain) where the transmitted symbols are generated, which gives access to each received 5G RE separately. This capability can be utilized to pre-filter the acquired URS and minimize interference. The preprocessing is summarized in Algorithm 1, where γ is a predefined threshold chosen empirically between 0 and 1, which depends on the fading channel between the gNB and UE. The preprocessing stage outputs a modified version of the URS signal denoted by $\mathbf{URS}'_{5\mathrm{G},u}$.

6.2.2.4 5G-URS Tracking

After acquiring and preprocessing the 5G-URS, node A switches to 2 and uses the 5G-URS as the local replica in standard tracking loops (e.g., as in [111]).

Algorithm 1 5G-URS Pre-processing.

Input: $\mathbf{URS}_{5\mathrm{G},u}$

Output: $\mathbf{URS}'_{5\mathrm{G},u}$

1: Convert $\mathbf{URS}_{5\mathrm{G},u}$ to frame structure $\mathbf{URS}^{f}_{5\mathrm{G},u}$ (i.e., time-domain serial array to matrix)

2: Normalize by maximum magnitude of REs

$$\mathbf{URS}^{f}_{5\mathrm{G},u} = \mathbf{URS}^{f}_{5\mathrm{G},u}/\mathrm{URS}_{\mathrm{m}}, \quad \mathrm{URS}_{\mathrm{m}} \triangleq \max\left\{\left|\mathbf{URS}^{f}_{5\mathrm{G},u}\right|\right\}$$

3: **for** $x = 0$, $x{+}{+}$, while $x <$ Number of symbols **do**

4: **for** $y = 0$, $y{+}{+}$, while $y <$ Number of subcarriers **do**

5: **if** $\left|\mathbf{URS}^{f}_{5\mathrm{G},u}(x,y)\right| < \gamma$ **then**

6: $\mathbf{URS}^{f}_{5\mathrm{G},u}(x,y) \leftarrow 0$

7: **end if**

8: **end for**

9: **end for**

10: Normalize element-wise: $\mathbf{URS}^{f}_{5\mathrm{G},u} = \mathbf{URS}^{f}_{5\mathrm{G},u}./\left|\mathbf{URS}^{f}_{5\mathrm{G},u}\right|$

11: Convert $\mathbf{URS}^{f}_{5\mathrm{G},u}$ into time-domain $\mathbf{URS}'_{5\mathrm{G},u}$

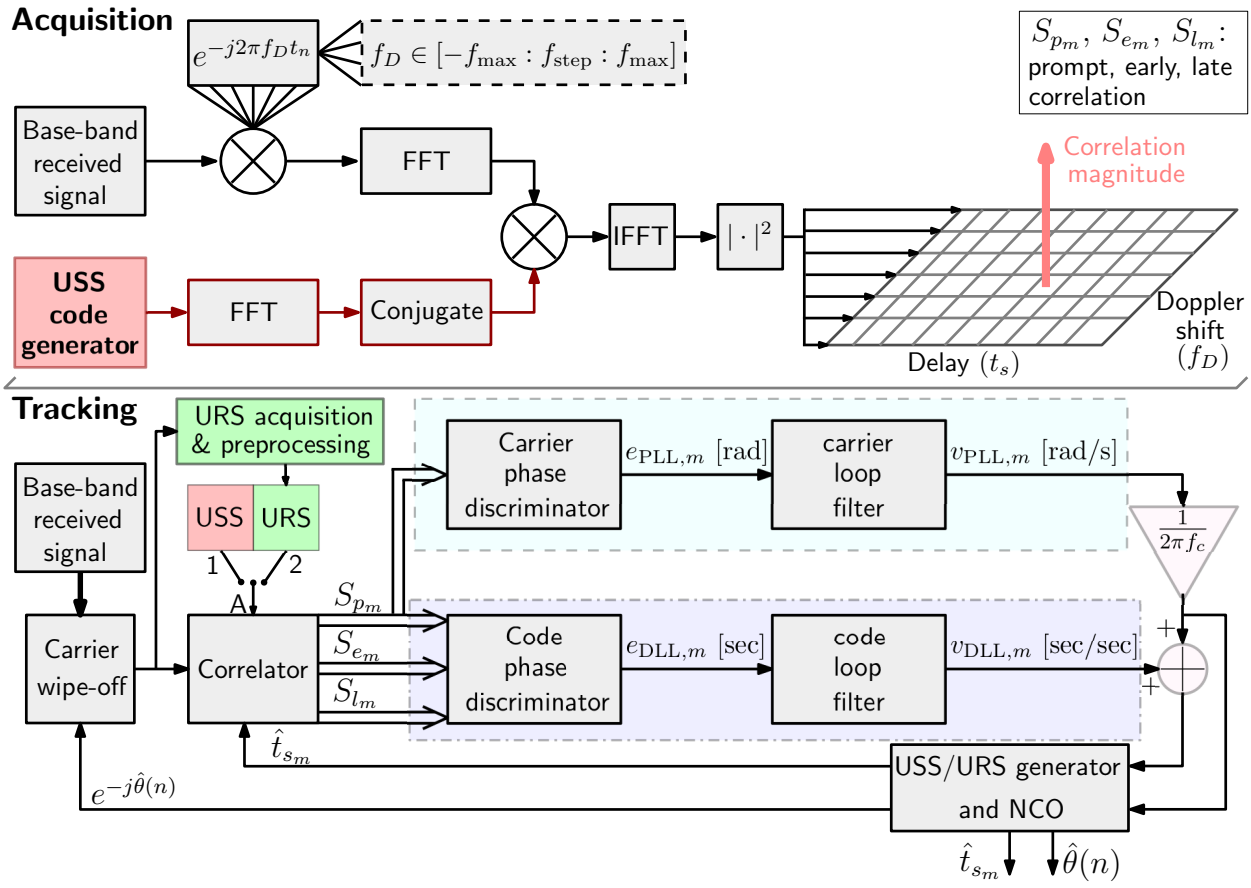


Figure 6.2: Block diagram of the proposed framework.

6.3 Experimental Results

This section presents the first UE-based carrier and code phase tracking, exploiting the entire sampled 5G downlink bandwidth. To this end, a stationary NI-USRP-2955 was equipped with a consumer-grade omnidirectional Laird antenna to receive 5G downlink signals. The bandwidth was set to 10 MHz and the carrier frequency was set to 632.55 MHz, which corresponds to the U.S. cellular provider T-Mobile. The collected data was stored on a laptop for off-line processing. 5G-URS acquisition, preprocessing, and tracking results are presented next.

6.3.1 5G-URS Acquisition and Preprocessing

The USRP recorded 5G signals for 300 seconds. The 5G-USS was used to detect a nearby gNB as in [94]. The gNB was mapped prior to the experiment and its location was known to the receiver. The receiver determined the gNB cell ID, Doppler, and code start time through the correlation approach detailed in Subsection 3.3.2. A gNB with $N_{ID}^{\text{Cell}} = 394$ was detected. The processing needed to track the Doppler and code start time followed the steps outlined in Subsection 3.3.3.

After the tracking loops achieved lock, the proposed framework acquired the 5G-URS signal for 4 seconds. Then, the acquired signal was preprocessed as discussed in Algorithm 1 with $\gamma = 0.2$. Figure 6.3 shows the frame structure of acquired 5G-URS before and after preprocessing.

To study 5G-URS's spectral efficiency $r_{\text{B,5G-URS}}$ and duty factor $r_{\text{T,5G-URS}}$, the number of active subcarriers and symbols was obtained from the preprocessed 5G-URS as shown in Figure 6.4. Assuming that a 5G-URS symbol is active if 10 or more subcarriers are active

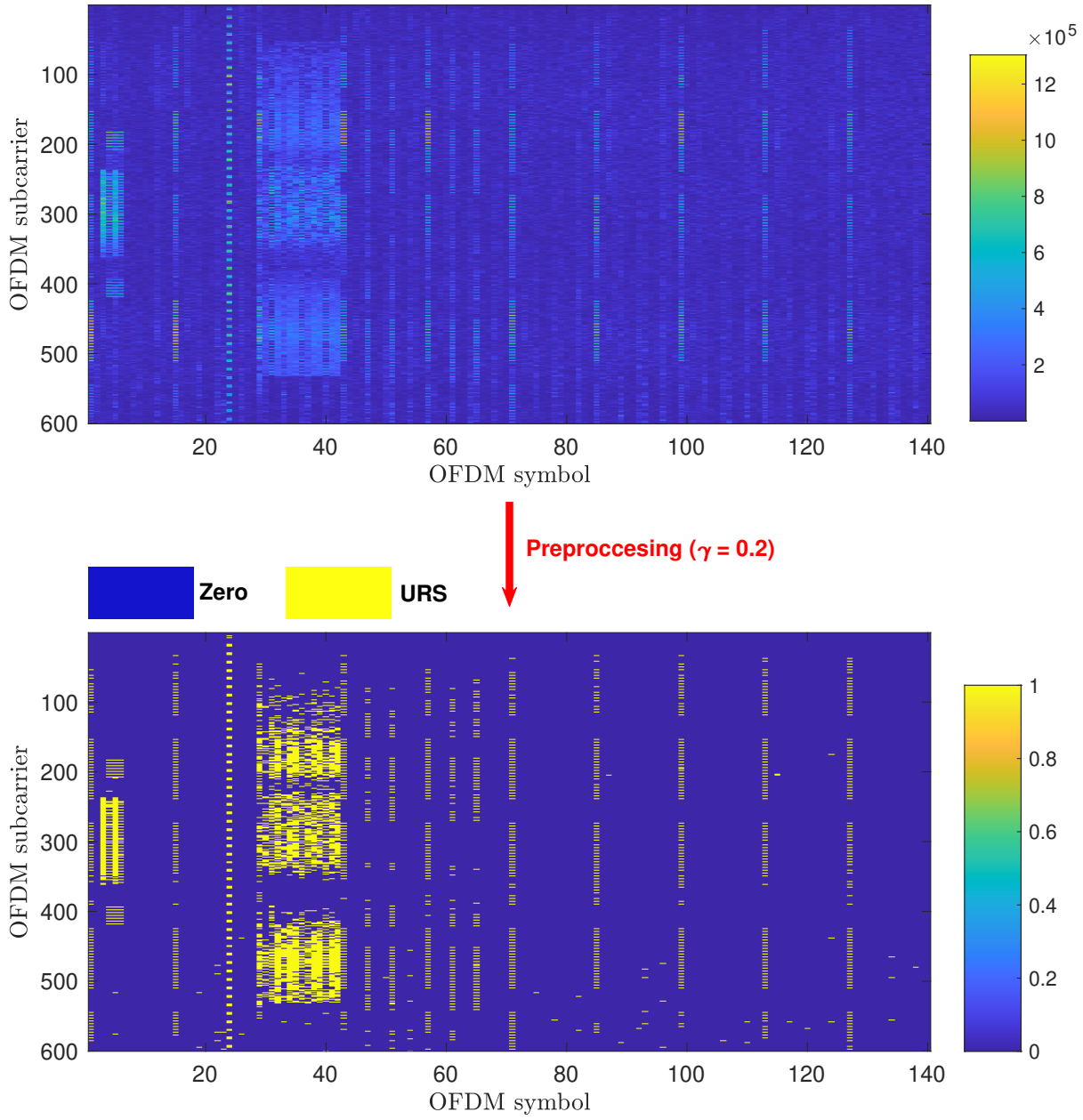


Figure 6.3: Frame structure of the 5G-URS before and after preprocessing.

within that symbol results in having 32 active symbols; hence, $r_{\mathrm{T,5G-URS}} = 22.86\%$ compared to $r_{\mathrm{T,5G-USS}} = 2.86\%$. For the bandwidth ratio, Figure 6.4 shows that $r_{\mathrm{B,5G-URS}} = 100\%$ compared to $r_{\mathrm{B,5G-USS}} = 36\%$ and $r_{\mathrm{B,5G-CON}} = 25\%$. The advantage of this increase in bandwidth ratio can be seen in the narrowness of the 5G-URS-ACF as shown in Figure 6.5, which gives higher resolution in the time-domain to discriminate the LOS from multipath components.

6.3.2 5G-URS Tracking Results

Next, the receiver switched to using the URS for tracking the signal parameters. Figure 6.6 shows the tracking results of the proposed framework utilizing the entire sampled 5G bandwidth compared to the USS-based approach. It can be seen how the CNR significantly increased by approximately 10 dB when using the acquired 5G-URS. This is due to the fact that in typical time-of-arrival-based ranging, the variance of the ranging error is a decreasing function of (i) the signal bandwidth and (ii) the signal-to-noise ratio. In the proposed approach, the bandwidth of the SS was increased by learning more synchronization sequences in higher subcarriers. Moreover, synchronization sequences were learned in different symbols of the frame. This resulted in a 10 dB increase in CNR as shown in Figure 6.6. Consequently, the standard deviation of the 5G-URS-based method is significantly decreased compared to that of the 5G-USS-based method. Also, smaller carrier and code phase errors were obtained by the proposed approach, which translates to better-ranging performance. It is worth noting that the CNR increase comes with an additional computational complexity on the order of $O(K \cdot n)$, from (6.2) and (6.3). Also, the 5G-URS cannot be used until after K time-steps. However, this delay is reasonably short. For example, in the presented results, the duration was only 4 seconds.

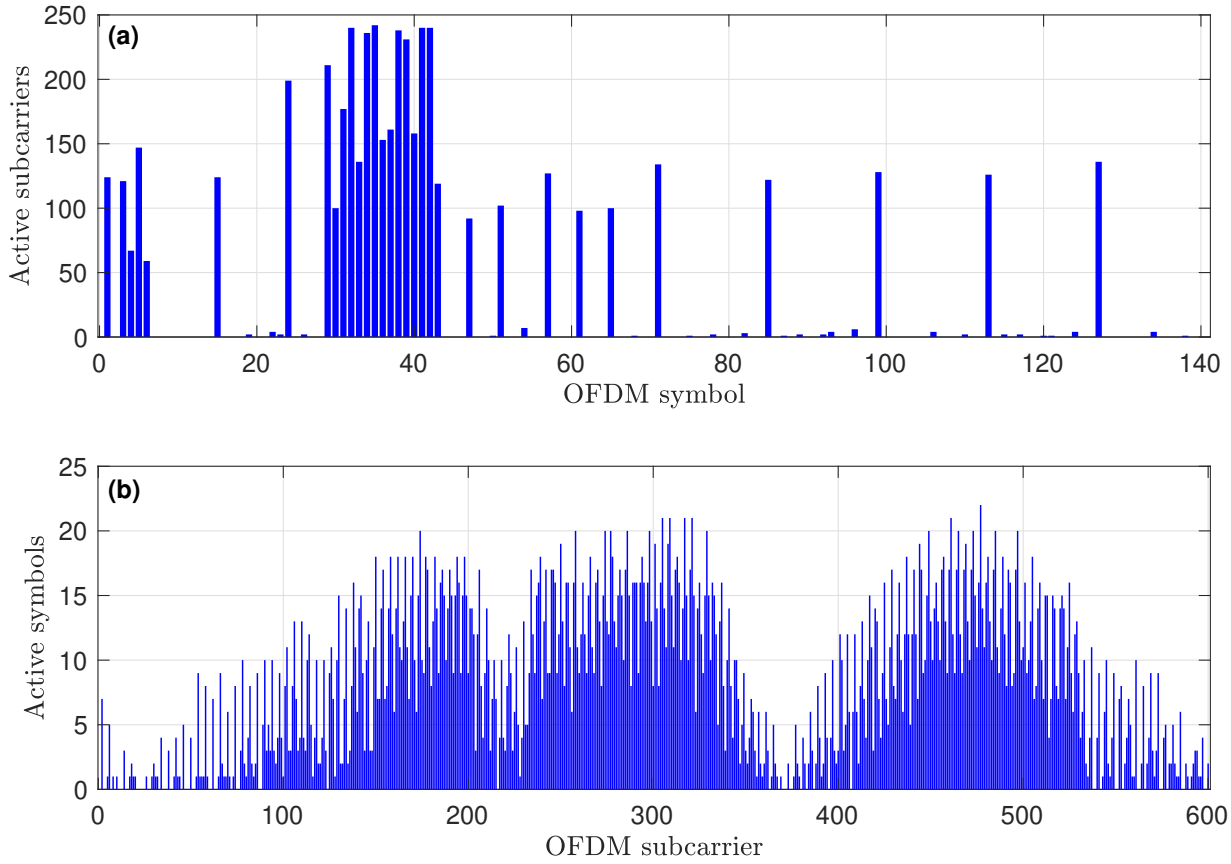


Figure 6.4: (a) Number of active subcarriers for each 5G-URS symbol and (b) number of active symbols for each 5G-URS subcarrier.

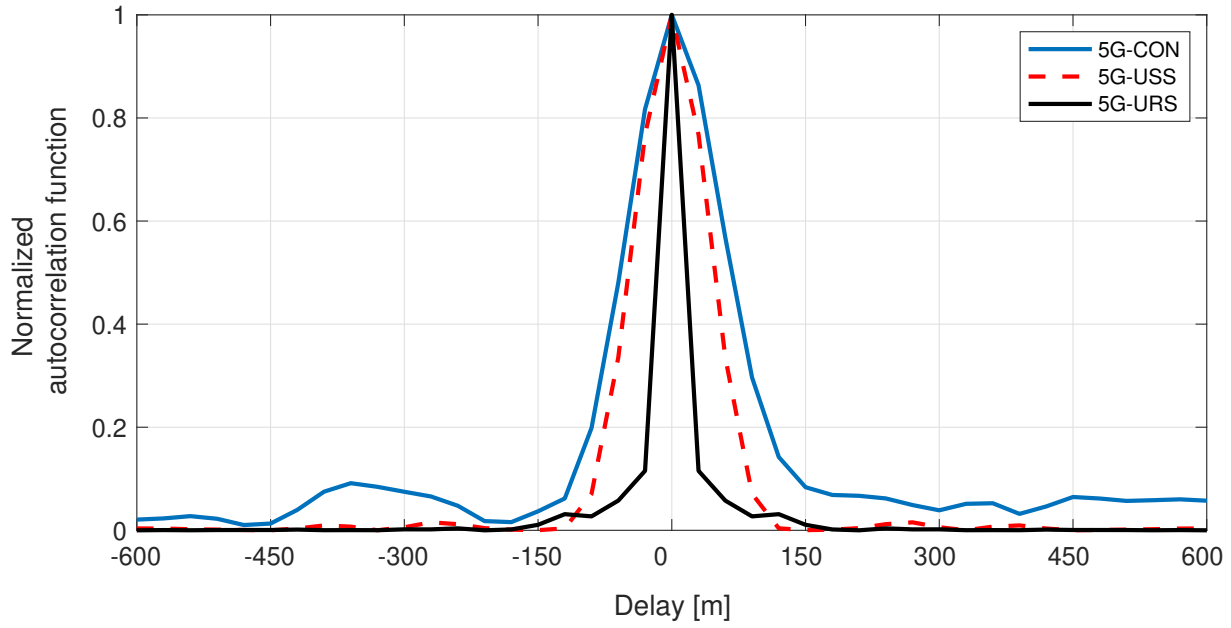


Figure 6.5: Normalized autocorrelation function of the 5G-URS compared with the ones estimated with the CON receiver and to the 5G-USS.

6.3.3 Ranging Results

This subsection assesses the ranging performance of the proposed framework. In this stationary scenario, the true range is fixed (290 m); hence, after removing the initial range error, the remaining range error over time can be observed in Figure 6.7. Note that the range error of the proposed 5G-URS-based framework drifts slower than that of the 5G-USS-based framework. The range error's standard deviation of the 5G-USS and 5G-URS frameworks were 5.05 m and 2.75 m, respectively.

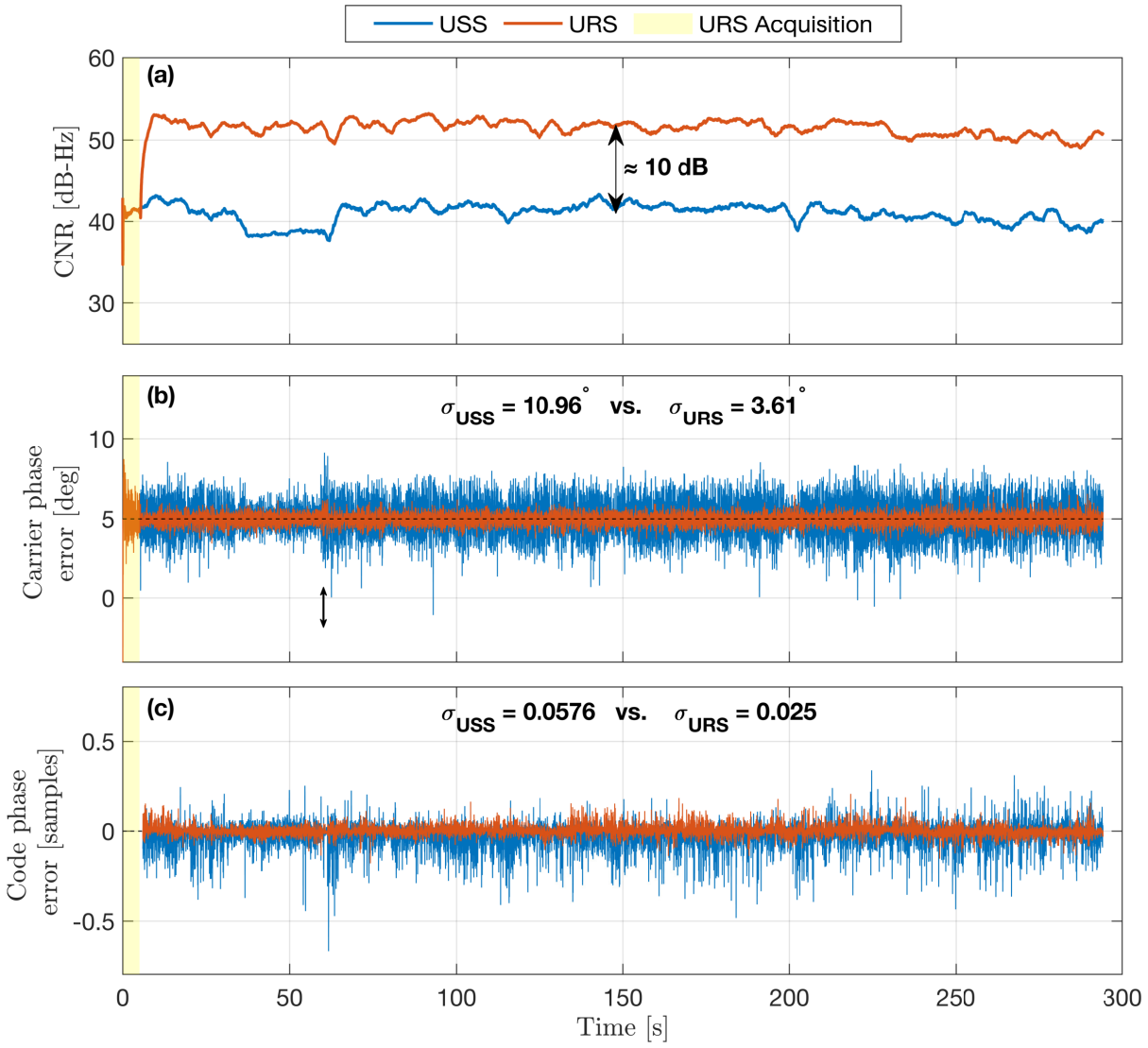


Figure 6.6: Cellular 5G tracking results of the proposed 5G-URS versus USS: (a) C/N_0, (b) carrier phase error, and (c) code phase error.

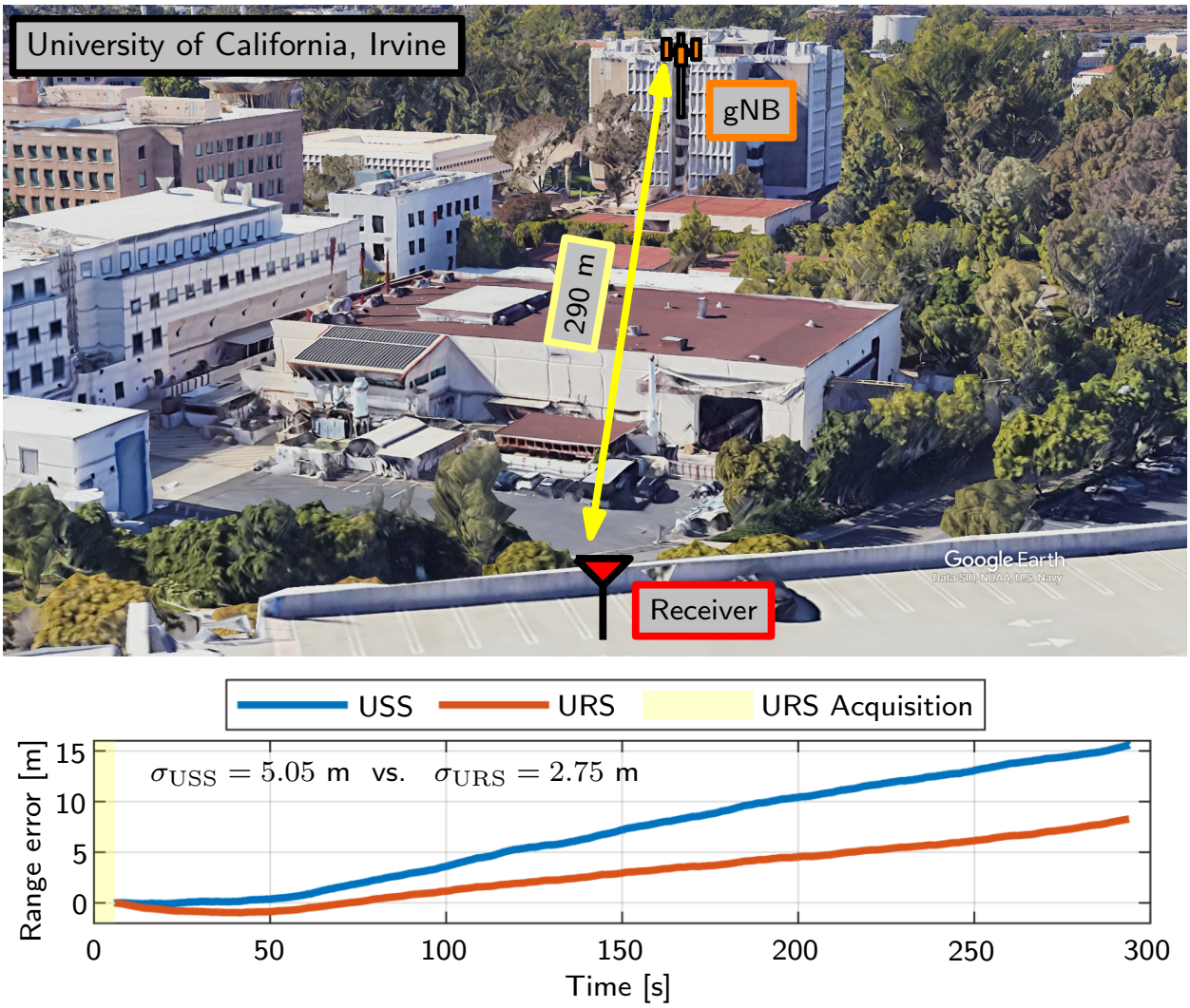


Figure 6.7: Environment layout and ranging error of 5G-USS and 5G-URS frameworks.

Chapter 7

A Passive EKF-Based Reconfigurable Intelligent Surface (RIS)-Aided Cellular Navigation System

This chapter is organized as follows. Section 7.1 describes the system model including the location scheme and the signal and channel models. Section 7.2 presents the measurement engine to estimate the TOA and AOA from the uplink LOS and VLOS received signals. Section 7.3 discusses the RIS phase profile optimization. Section 7.4 implements an EKF as a navigation filter for the proposed system. Section 7.5 presents a cellular-5G-OFDM simulator to evaluate the performance of the proposed approach through Monte Carlo (MC) simulations across diverse scenarios, including pedestrian movement, ground vehicles, and UAVs. These simulations were conducted under various conditions: synchronous and asynchronous clock settings between the BS and UE, and environments with and without multipath effects. The results from these simulations highlight the proficiency of the proposed navigation system, demonstrating its capability to achieve sub-meter to meter-level positioning accuracy in a range of scenarios.

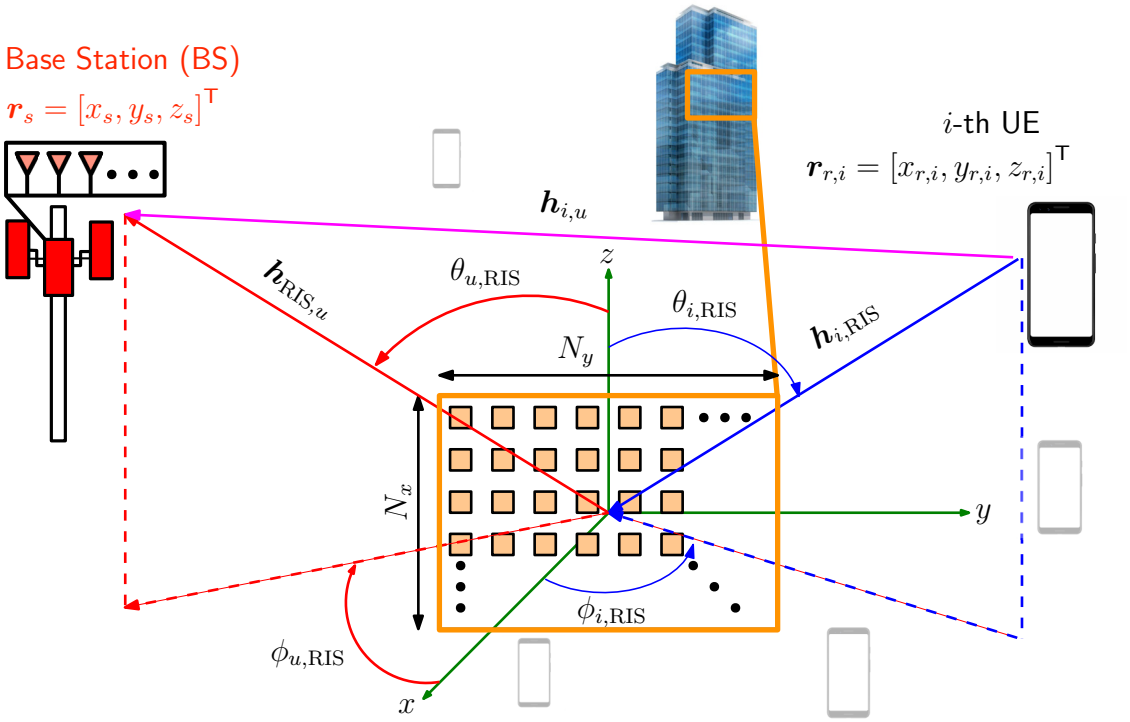


Figure 7.1: Location scheme.

7.1 Model Description

7.1.1 Location Scheme

We consider a 3-D localization scenario with I single-antenna UEs, a BS each equipped with a N_u-length uniform linear antenna array whose elements are regularly spaced with inter-element spacing $d = \lambda/2$, and an $N = N_x \times N_y$ element rectangular RIS. The i-th UE is located at $\boldsymbol{r}_{r,i} = [x_{r,i}, y_{r,i}, z_{r,i}]^\mathsf{T}$. Each BS is equipped with a uniform linear antenna array consisting of M elements. The array at the BS is centered at $\boldsymbol{r}_s = [x_s, y_s, z_s]^\mathsf{T}$ with the elements spaced at $\lambda/2$ apart. The RIS is assumed to lie in the yz-plane with a reference point $\mathbf{0}_3$, where the location of the n-th element is denoted by $\boldsymbol{r}_{\text{ris},n} = [0, y_{\text{ris},n}, z_{\text{ris},n}]^\mathsf{T}$. The RIS elements are regularly spaced with inter-element spacing $d = \lambda/2$ in both dimensions. Figure 7.1 depicts the localization scenario.

7.1.2 Signal and Channel Model

We consider a mmWave uplink transmission that employs OFDM as its modulation technique. In this revised scenario, the complex baseband signal received by the antenna array at the u-th BS from the i-th UE comprises several components: (i) A direct LOS signal, (ii) a signal reflected by the RIS, often referred to as the VLOS in literature, and (iii) L multipath signals. The received signal at the multiple antenna elements of the BS from the i-th UE can be expressed as

$$\mathbf{R}_i(t) = \left[\boldsymbol{r}_i^{(1)}(t), \cdots, \boldsymbol{r}_i^{(N_u)}(t)\right]^{\mathsf{T}}, \tag{7.1}$$

where $\boldsymbol{r}_i^{(n_u)}(t) \in \mathbb{C}^{N_{s,i}\times 1}$, with $N_{s,i}$ being the number of OFDM samples, is the received signal at the n_u-th antenna element of uth BS and can be expressed as

$$\boldsymbol{r}_i^{(n_u)}(t) = \sqrt{P}\sum_{l=0}^{l=L+1} \gamma_{i,l}^{(n_u)} \boldsymbol{s}_i(t-\tau_{i,l}) + \boldsymbol{w}_i^{(n_u)}(t), \tag{7.2}$$

$$\gamma_{i,l}^{(n_u)} \triangleq a(\psi_{i,l}^{(n_u)})\alpha_{i,l}^{(n_u)}, \tag{7.3}$$

where P is the transmit power; $\boldsymbol{s}(t) \in \mathbb{C}^{N_{s,i}\times 1}$ denotes the known OFDM signal vector; $\boldsymbol{w}_i^{(n_u)}(t)$ represents zero-mean white Gaussian noise vector with a PSD of $N_0/2$; $\tau_{0,i} = \frac{\|\boldsymbol{r}_{r,i}-\boldsymbol{r}_s\|_2}{c}$ and $\tau_{1,i} = \frac{\|\boldsymbol{r}_{r,i}\|_2+\|\boldsymbol{r}_s\|_2}{c}$ correspond to the LOS and VLOS delays, respectively; signals for which $l > 1$ are identified as multipath components; $a(\psi_{i,l}^{(n_u)}) = e^{j(n_u-1)\mu_{i,l}}$ is the n_u-th response element of the l-th path between the i-th UE and the BS, with $\mu_{i,l} = -\frac{2\pi}{\lambda}d\sin(\psi_{i,l})$ being the the spatial frequency associated with that path, and $\psi_{i,l}$ is the corresponding azimuth AOA; and c is the speed of light. The channel complex gains $\alpha_{i,l}^{(n_u)}$, $l \in \{0,1\}$ are

modeled geometrically in the mmWave regime [112] as

$$\alpha_{i,0}^{(n_u)} = e^{-j2\pi f_c \tau_{i,0}} \frac{\lambda}{4\pi \left\| \boldsymbol{r}_{r,i} - \boldsymbol{r}_s \right\|_2}, \tag{7.4}$$

$$\alpha_{i,1}^{(n_u)} = e^{-j2\pi f_c \tau_{i,1}} \frac{\lambda^2}{16\pi^2 \left\| \boldsymbol{r}_{r,i} \right\|_2 \left\| \boldsymbol{r}_s \right\|_2} \boldsymbol{h}_{\mathrm{RIS},u}^{\mathsf{T}} \boldsymbol{\Omega} \boldsymbol{h}_{i,\mathrm{RIS}}, \tag{7.5}$$

where f_c is the carrier frequency, $\boldsymbol{h}_{\mathrm{RIS},u} \in \mathbb{C}^{N\times 1}$ is the RIS to BS response vector, $\boldsymbol{h}_{i,\mathrm{RIS}} \in \mathbb{C}^{N\times 1}$ is the i-th UE to RIS response vector, and $\boldsymbol{\Omega}$ is an $N \times N$ diagonal matrix, which is assumed to be electronically controlled and optimized depending on the current estimates of the UE locations. The response vector $\boldsymbol{h}_{\mathrm{RIS},u}$ can be expressed as

$$\left[\boldsymbol{h}_{\mathrm{RIS},u}\right]_n = e^{-j\boldsymbol{r}_{\mathrm{ris},n}^{\mathsf{T}} \boldsymbol{k}(\phi_{\mathrm{RIS},u}, \theta_{\mathrm{RIS},u})}, \ n \in \{0, 1, \cdots, N-1\}, \tag{7.6}$$

where $\phi_{\mathrm{RIS},u}$ and $\theta_{\mathrm{RIS},u}$ are the azimuth and elevation corresponding to the angle of departure of the signal from the RIS to the BS, and $\boldsymbol{k}(\phi, \theta)$ is the wavevector expressed as

$$\boldsymbol{k}(\phi, \theta) = -\frac{2\pi}{\lambda} \begin{bmatrix} \sin(\theta)\cos(\phi) \\ \sin(\theta)\sin(\phi) \\ \cos(\theta) \end{bmatrix}. \tag{7.7}$$

The response vector $\boldsymbol{h}_{i,\mathrm{RIS}}$ can be expressed as

$$\left[\boldsymbol{h}_{i,\mathrm{RIS}}\right]_n = e^{-j\boldsymbol{r}_{\mathrm{ris},n}^{\mathsf{T}} \boldsymbol{k}(\phi_{i,\mathrm{RIS}}, \theta_{i,\mathrm{RIS}})}, \ n \in \{0, 1, \cdots, N-1\}. \tag{7.8}$$

The RIS phase profile matrix $\boldsymbol{\Omega}$ can be expressed as

$$\boldsymbol{w}_{\mathrm{RIS}} = \mathrm{diag}(\boldsymbol{\Omega}), \tag{7.9}$$

where $\boldsymbol{w}_{\mathrm{RIS}} = [e^{jw_{\mathrm{RIS},0}}, e^{jw_{\mathrm{RIS},1}}, \cdots, e^{jw_{\mathrm{RIS},N-1}}]^{\mathsf{T}}$.

7.2 Measurement Engine

The received signal from the lth path of the i-th UE to the BS, which is operated upon by the measurement engine, is formulated as the beamformed signal from that specific direction. This can be mathematically expressed as

$$\boldsymbol{r}_i^{'}(t) = \boldsymbol{w}_{i,l}\mathbf{R}_i(t), \tag{7.10}$$

$$\boldsymbol{w}_{i,l} = \boldsymbol{a}_{i,l}^{*}, \tag{7.11}$$

$$\boldsymbol{a}_{i,l} = \left[1, e^{j\mu_{i,l}}, e^{j2\mu_{i,l}}, \cdots, e^{j(N_u-1)\mu_{i,l}}\right]^{\mathsf{T}}, \tag{7.12}$$

$$\mu_{i,l} = -\frac{2\pi}{\lambda} d \sin(\hat{\psi}_{i,l}), \quad \text{for } l \in \{0, 1\}, \tag{7.13}$$

where $\hat{\psi}_{i,l}$ represents the current estimate of the azimuth AOA of the LOS path for $l = 0$, or the known azimuth AOA of the VLOS for $l = 1$.

7.2.1 TOA Estimation

For TOA estimation, the proposed time-domain-based SDR in Section 3.3 is adopted and modified in the next parts of this chapter to develop a passive AOA estimator for an RIS-aided cellular navigation framework.

7.2.2 AOA Estimation

In this section, we introduce a passive AOA estimator designed to determine the azimuth and elevation angles between the UE and the RIS. This estimator capitalizes on the correlation properties of the OFDM uplink signals as received by the BS.

An illustration of the exhaustive UE-RIS AOA search can be found in Figure 7.2. This

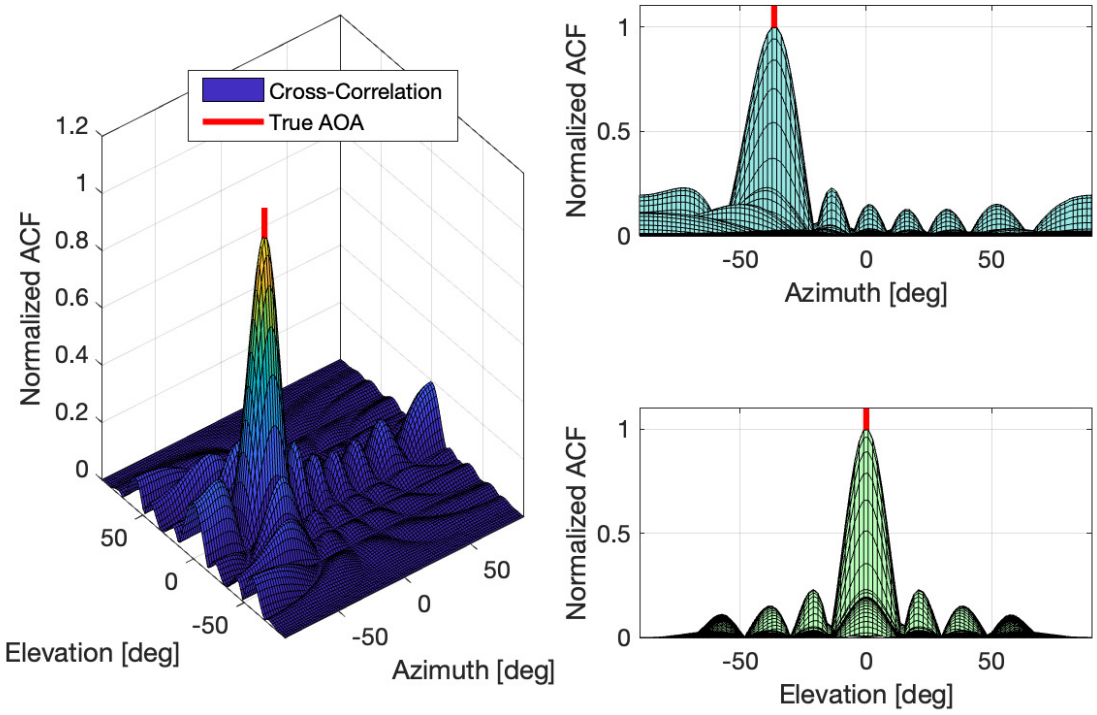


Figure 7.2: Sample output of the initial UE-RIS AOA search.

representation assumes that the BS is privy to knowledge of the channel coefficients $\boldsymbol{h}_{\mathrm{RIS},u}^{\mathsf{T}}$ and the RIS phase profile $\boldsymbol{\Omega}$. Given that in uplink scenarios the position of the BS is known, this assumption holds. Observing the figure, it's evident that the normalized ACF exhibits a peak aligned with the true AOA. Interestingly, the ACF's magnitude diminishes when the generated replica deviates from the desired AOA, indicating that AOA data can be extracted from the ACF. Yet, it's imperative to recognize that the efficacy of such a comprehensive search is intertwined with the AOA search resolution. A heightened search resolution inevitably amplifies the computational expense associated with the estimation process. Consequently, this section delves into the exploration of an AOA estimator that strikes a balance between accuracy and computational efficiency.

7.2.2.1 AOA Discriminator Design

The quest for an optimal AOA estimator that addresses prevailing challenges leads us to derive inspiration from the DLL architecture. While the DLL encompasses standard loop features like integrations, filters, and NCOs, its uniqueness emerges from the specialized discriminator it employs. This discriminator gauges the error of the current delay estimate. Facilitating this, the DLL incorporates two auxiliary correlations—*early* and *late*. These can be conceptualized as delayed and advanced replicas of the *prompt* code, respectively. The rationale behind this is the generation of the S-curve, a product of the differential between the early and late correlators. It is the zero-crossing of this S-curve that the DLL monitors keenly. By doing so, it ascertains the current error, which is subsequently directed back to the local code generation block. This feedback mechanism adjusts and refines the preceding estimate of the incoming code delay.

To visually encapsulate this mechanism, one can refer to Figure 7.3. This figure vividly depicts both the early and late correlations, alongside the resultant S-curve birthed from their interplay. Operational nuances of the DLL emphasize its functioning within the linear domain of the discriminator, specifically between -0.5 and $+0.5$ chips. Such an operating window ensures a direct linear relationship between the discriminator output and the actual offset.

To design the AOA discriminator, it's imperative to first understand the AOA error in relation to the ACF. To achieve this, we performed a MC analysis. This simulation mirrored a wireless environment comprising a singular BS, an RIS, and one UE. Notably, we focused exclusively on evaluating the reflected path, i.e., the VLOS. Specific details regarding this simulation setting can be accessed in Table 7.1.

Upon analyzing the outcomes of over 1000 iterations, the relation between AOA errors and the normalized ACF was obtained, as shown in Figure 7.4. Based on these insights, we

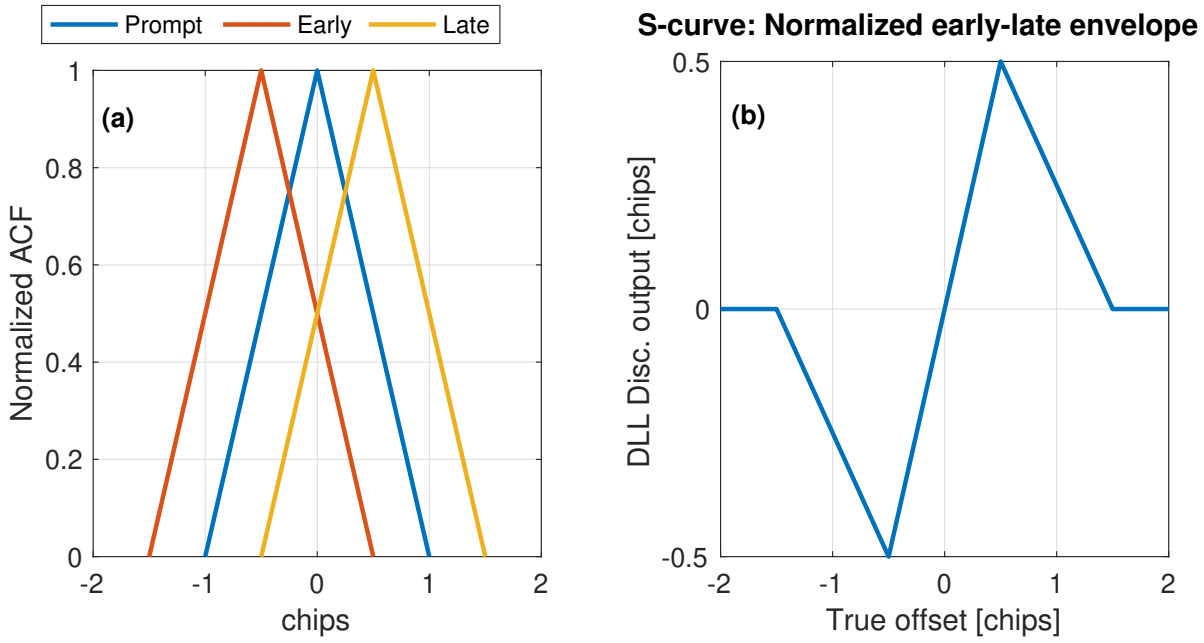


Figure 7.3: (a) Normalized early, prompt, and late ACF for GPS L1 signal. (b) S-curve for the normalized early minus late discriminator.

engineered a normalized early-minus-late (eml) angle discriminator. This involved extracting S-curves for both azimuth and elevation corresponding to various eml angles, symbolized as a_{eml}.

For the purpose of AOA estimation, we defined our region of interest within a range of $-5°$ to $5°$. This span effectively encapsulates the variance in AOAs across two sequential measurements. The ensuing step involved evaluating the linearity of each S-curve, followed by the computation of a linear RMSE fit. Our analyses determined that an a_{eml} value approximating $1°$ yielded the most precise open-loop estimates. For a more detailed visual representation of the azimuth and elevation eml discriminator's performance, readers are directed to Figures 7.5 and 7.6, respectively.

The comparison between the extensive search and the open-loop discriminator approaches is depicted in Figure 7.7. It can be seen how the discriminator approach outperforms the extensive search; however, it struggles to converge to a zero-error steady state. To achieve

Table 7.1: AOA Discriminators Monte-Carlo Settings.

Parameter	Value	Description
x_{range}	[-2.5, 2.5] km	The geometric range in the x direction. A typical cell size
y_{range}	[-2.5, 2.5] km	The geometric range in the y direction
z_{range}	[-50, 50] m	The geometric range in the z direction. Represents the relative height between BS, RIS, and UE
f_c	28 GHz	Carrier frequency
B	100 MHz	OFDM Signal Bandwidth
t_{frame}	10 ms	Typical 4/5G frame duration
sc	15 kHz	OFDM subcarrier spacing
N	64	Number of RIS elements

this, a closed-loop ALL is designed next.

7.2.2.2 AOA-Locked Loop

Besides the developed early-minus-late AOA discriminator, the ALL loop filter is a simple gain $B_{n,\text{ALL}} = \frac{K}{4} \equiv 1$ Hz. The output of the ALL loop filters $v_{\text{ALL},m}$ is the rate of change of the azimuth and elevation angles, respectively, expressed in °/s. The block diagram of the overall measurement engine is depicted in Figure 7.8.

7.3 RIS Optimization

In signal-based localization techniques, estimation error has an inverse relationship with the received SNR [5]. For a specific scenario, consider the SNR of the i-th UE received at the u-th BS antenna, which is represented as two separate SNRs corresponding to the LOS and

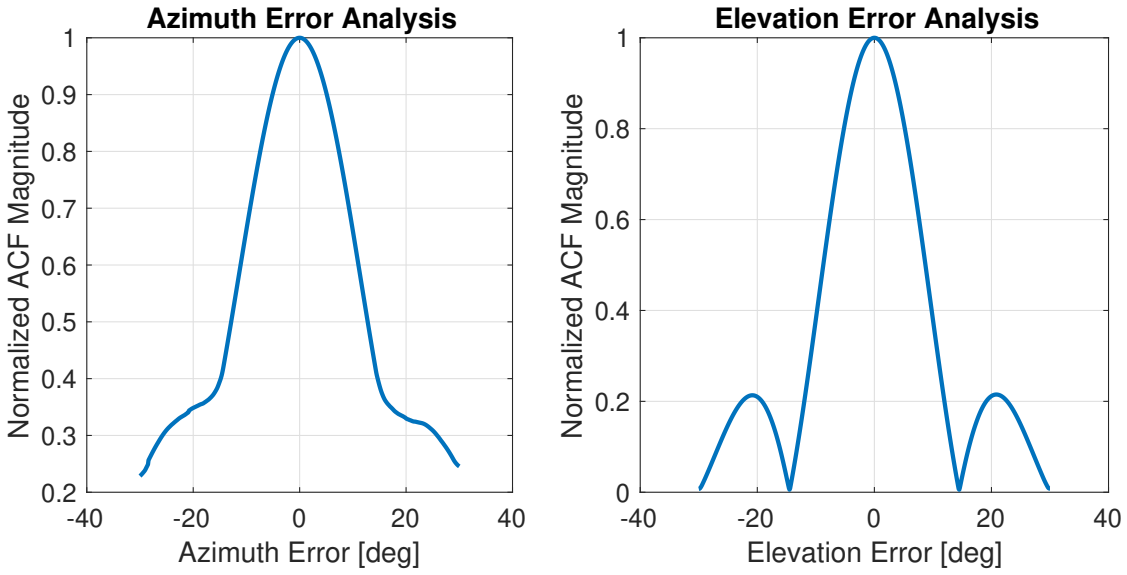


Figure 7.4: AOA errors vs ACF in Monte Carlo fashion.

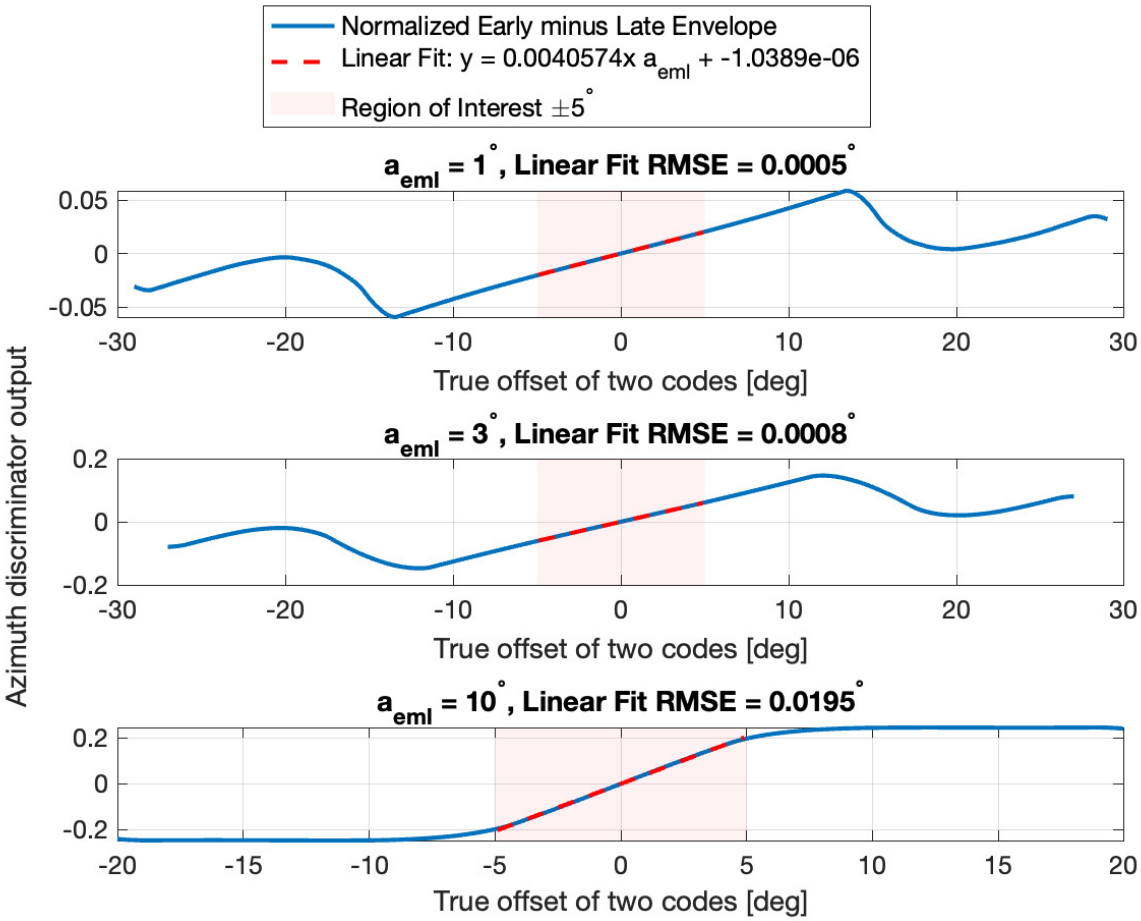


Figure 7.5: Azimuth early-late discriminator.

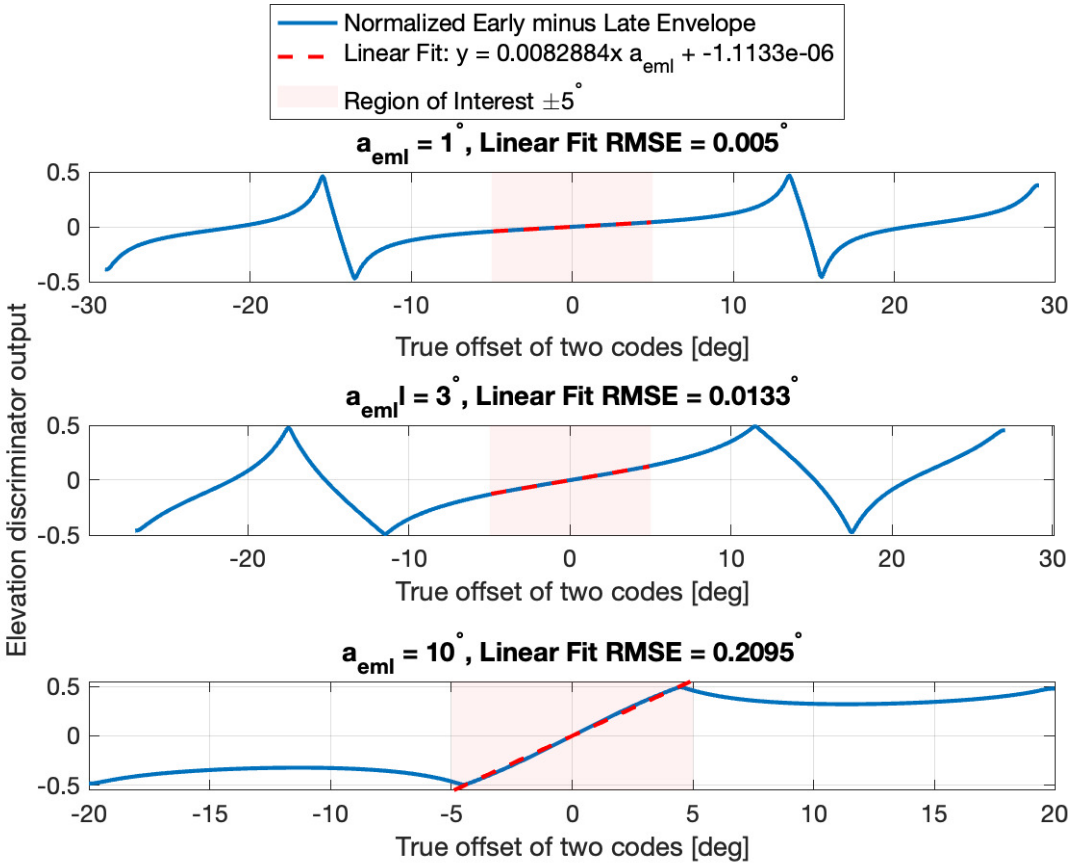


Figure 7.6: Elevation early-late discriminator.

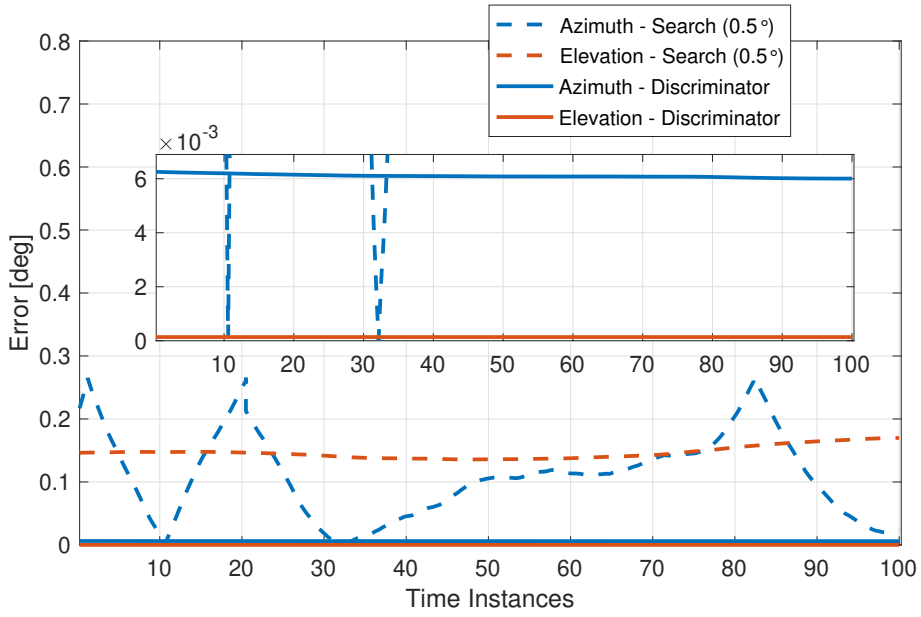


Figure 7.7: AOA estimation comparison between extensive search with resolution 5° and the proposed discriminators with 1° early-minus-late offset.

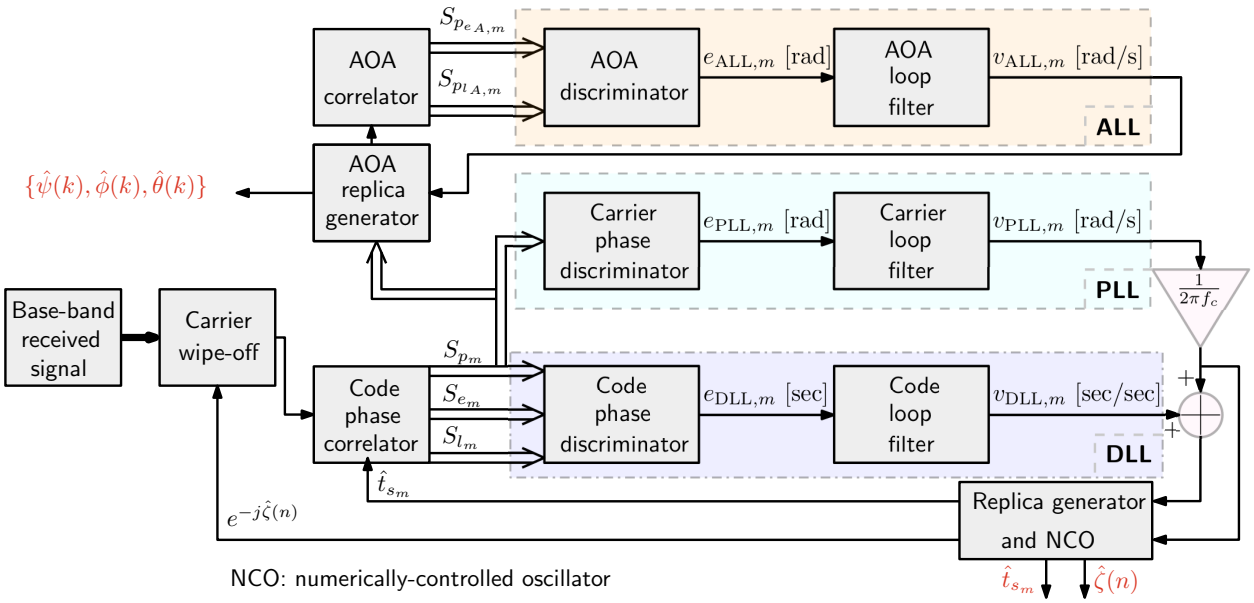


Figure 7.8: Measurement engine diagram.

the VLOS as

$$\mathrm{SNR}_{i,l} \triangleq P \frac{\sum_{n_u=1}^{n_u} \left|\alpha_{i,l}^{(n_u)}\right|^2}{N_u \sigma_n^2}, \quad \text{for } l \in 0, 1, \tag{7.14}$$

where $l = 0$ and $l = 1$ denote the LOS and VLOS signals, respectively.

Assuming a single BS that is controlling the RIS phase profile, and in the presence of multiple UEs, the optimization of the RIS phase profile, $\boldsymbol{\Omega}$, is formulated to maximize the minimum SNR among the VLOS of all UEs, which can be formulated as

$$\underset{\Omega}{\text{maximize}} \quad \min\{\mathrm{SNR}_{i,1}\}_{i=1}^{i=I} \tag{7.15}$$

$$\text{subject to} \quad |w_j| = 1, \quad \text{for} \quad j = 1, \cdots, N. \tag{7.16}$$

7.4 EKF Implementation

Separate EKFs are deployed to estimate the UEs' 3D positions and velocities along with relative clock bias and drift using the TOA and AOA measurements. The EKF state vector for the i-th UE is expressed as

$$\boldsymbol{x}_i \triangleq \left[\boldsymbol{x}_{r,i}^{\mathsf{T}}, \boldsymbol{x}_{\text{clk}}^{\mathsf{T}}\right]^{\mathsf{T}}, \tag{7.17}$$

$$= \left[\boldsymbol{r}_{r,i}^{\mathsf{T}}, \dot{\boldsymbol{r}}_{r,i}^{\mathsf{T}}, c\Delta\delta t, c\Delta\dot{\delta}t\right]^{\mathsf{T}} \tag{7.18}$$

where $\Delta\delta t \triangleq \delta t_{\mathbf{i}} - \delta t_{\mathbf{s}}$; $\delta t_{\mathbf{i}}$ and $\delta t_{\mathbf{s}}$ are the clock biases of the i-th UE and the BS, respectively; $\Delta\dot{\delta}t \triangleq \dot{\delta}t_{\mathbf{i}} - \dot{\delta}t_{\mathbf{s}}$; and $\dot{\delta}t_{\mathbf{i}}$ and $\dot{\delta}t_{\mathbf{s}}$ are the clock drifts of the i-th UE and the BS, respectively.

7.4.1 EKF Time Update

The receiver's motion is assumed to evolve according to the white noise acceleration model as discussed in Subsection 2.3.1. The receiver's discrete-time dynamics are hence given by

$$\hat{\boldsymbol{x}}_i(k+1|j) = \mathbf{F}_i \boldsymbol{x}_i(k|j) + \boldsymbol{w}_i(k), \tag{7.19}$$

$$\mathbf{F}_i \triangleq \text{diag}\left[\mathbf{F}_r, \mathbf{F}_{\text{clk}}, \right], \quad \mathbf{F}_{\text{clk}} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \tag{7.20}$$

where where T is the measurement update period, and k and j are two discrete-time indices such as $k \geq j$. The prediction error covariance matrix is given by

$$\mathbf{P}_i(k+1|j) = \mathbf{P}_i(k|j)\mathbf{F}_i^{\mathsf{T}} + \mathbf{Q}_i, \tag{7.21}$$

$$\mathbf{Q}_i \triangleq \text{diag}\left[\mathbf{Q}_r, c^2\mathbf{Q}_{\text{clk}}\right], \tag{7.22}$$

$$\mathbf{Q}_{\text{clk}} = \mathbf{Q}_{\text{clk},i} + \mathbf{Q}_{\text{clk,BS}}, \tag{7.23}$$

$$\mathbf{Q}_{\text{clk},\kappa} = \begin{bmatrix} S_{\tilde{w}_{\delta t_\kappa}} T + S_{\tilde{w}_{\dot{\delta} t_\kappa}} \frac{T^3}{3} & S_{\tilde{w}_{\dot{\delta} t_\kappa}} \frac{T^2}{2} \\ S_{\tilde{w}_{\dot{\delta} t_\kappa}} \frac{T^2}{2} & S_{\tilde{w}_{\dot{\delta} t_\kappa}} T \end{bmatrix}, \tag{7.24}$$

where $\kappa \in \left\{\{\text{UE}\}_{i=1}^{i=I}, \text{BS}\right\}$.

7.4.2 EKF Measurement Update

Once the EKF receives the measurement vector $\boldsymbol{z}_i$, it performs a measurement update according to

$$\hat{\boldsymbol{x}}_i(k+1|k+1) = \hat{\boldsymbol{x}}_i(k+1|j) + \mathbf{K}_i(k+1)\boldsymbol{\nu}_i(k+1)$$

where $\boldsymbol{\nu}$ and $\mathbf{K}$ are the innovation vector and Kalman gain, respectively, given by

$$\begin{aligned}
&\boldsymbol{\nu}_i(k+1) \triangleq \boldsymbol{z}_i(k+1) - \hat{\boldsymbol{z}}_i(k+1), \\
&\boldsymbol{z}_i(k+1) = \left[\rho_i(k+1), \rho_i^{'}(k+1), \psi_i(k+1), \phi_i(k+1), \theta_i(k+1)\right]^{\mathsf{T}}, \\
&\mathbf{K}_i(k+1) \triangleq \mathbf{P}_i(k+1|j)\mathbf{H}_i^{\mathsf{T}}(k+1)\mathbf{S}_i^{-1}(k+1), \\
&\mathbf{S}_i(k+1) \triangleq \mathbf{H}_i(k+1)\mathbf{P}(k+1|j)\mathbf{H}_i^{\mathsf{T}}(k+1) + \mathbf{R}_i(k+1),
\end{aligned}$$

where $\mathbf{R}_i$ is the measurement noise covariance matrix the $i$ith receiver given by

$$\mathbf{R}_i \triangleq \left[\sigma^2_{\rho,i}, \sigma'^2_{\rho,i}, \sigma^2_{\psi,i}, \sigma^2_{\phi,i}, \sigma^2_{\theta,i}\right], \tag{7.25}$$

and $\mathbf{H}_i$ is the Jacobian matrix defined as

$$\mathbf{H}_i = \begin{bmatrix} \mathbf{H}_i^{(1)} \\ \vdots \\ \mathbf{H}_i \end{bmatrix}, \tag{7.26}$$

where

$$\mathbf{H}_i(k+1) = \begin{bmatrix} H_{1,1}(\cdot) & H_{1,2}(\cdot) & H_{1,3}(\cdot) & \mathbf{0}_{1\times 3} & 1 & 0 \\ H_{2,1}(\cdot) & H_{2,2}(\cdot) & H_{2,3}(\cdot) & \mathbf{0}_{1\times 3} & 1 & 0 \\ H_{3,1}(\cdot) & H_{3,2}(\cdot) & H_{3,3}(\cdot) & \mathbf{0}_{1\times 3} & 0 & 0 \\ H_{4,1}(\cdot) & H_{4,2}(\cdot) & H_{4,3}(\cdot) & \mathbf{0}_{1\times 3} & 0 & 0 \\ H_{5,1}(\cdot) & H_{5,2}(\cdot) & H_{5,3}(\cdot) & \mathbf{0}_{1\times 3} & 0 & 0 \end{bmatrix}, \tag{7.27}$$

$$H_{1,1} = \frac{x_{r,i} - x_s}{\left\|\boldsymbol{r}_{r,i} - \boldsymbol{r}_{s,u}\right\|_2}, \tag{7.28}$$

$$H_{1,2} = \frac{y_{r,i} - y_s}{\left\|\boldsymbol{r}_{r,i} - \boldsymbol{r}_{s,u}\right\|_2}, \tag{7.29}$$

$$H_{1,3} = \frac{z_{r,i} - z_s}{\left\|\boldsymbol{r}_{r,i} - \boldsymbol{r}_{s,u}\right\|_2}, \tag{7.30}$$

$$H_{2,1} = \frac{x_{r,i} - x_{\text{ris}}}{\left\|\boldsymbol{r}_{r,i} - \boldsymbol{r}_{\text{ris}}\right\|_2}, \tag{7.31}$$

$$H_{2,2} = \frac{y_{r,i} - y_{\text{ris}}}{\left\|\boldsymbol{r}_{r,i} - \boldsymbol{r}_{\text{ris}}\right\|_2}, \tag{7.32}$$

$$H_{2,3} = \frac{z_{r,i} - z_{\text{ris}}}{\left\|\boldsymbol{r}_{r,i} - \boldsymbol{r}_{\text{ris}}\right\|_2}, \tag{7.33}$$

$$H_{3,1} = -\frac{y_{r,i} - y_s}{(x_{r,i} - x_s)^2 \left[1 + \frac{(y_{r,i} - y_s)^2}{(x_{r,i} - x_s)^2}\right]}, \tag{7.34}$$

$$H_{3,2} = \frac{x_{r,i} - x_s}{(x_{r,i} - x_s)^2 \left[1 + \frac{(y_{r,i} - y_s)^2}{(x_{r,i} - x_s)^2}\right]}, \tag{7.35}$$

$$H_{3,3} = 0, \tag{7.36}$$

$$H_{4,1} = -\frac{y_{r,i} - y_{\text{ris}}}{(x_{r,i} - x_{\text{ris}})^2 \left[1 + \frac{(y_{r,i} - y_{\text{ris}})^2}{(x_{r,i} - x_{\text{ris}})^2}\right]}, \tag{7.37}$$

$$H_{4,2} = \frac{x_{r,i} - x_{\text{ris}}}{(x_{r,i} - x_{\text{ris}})^2 \left[1 + \frac{(y_{r,i} - y_{\text{ris}})^2}{(x_{r,i} - x_{\text{ris}})^2}\right]}, \tag{7.38}$$

$$H_{4,3} = 0, \tag{7.39}$$

$$H_{5,1} = \frac{(z_{r,i} - z_{\text{ris}})(x_{r,i} - x_{\text{ris}})}{\left\|\boldsymbol{r}_{r,i} - \boldsymbol{r}_{\text{ris}}\right\|_2^2 \sqrt{(x_{r,i} - x_{\text{ris}})^2 + (y_{r,i} - y_{\text{ris}})^2}}, \tag{7.40}$$

$$H_{5,2} = \frac{(z_{r,i} - z_{\text{ris}})(y_{r,i} - y_{\text{ris}})}{\left\|\boldsymbol{r}_{r,i} - \boldsymbol{r}_{\text{ris}}\right\|_2^2 \sqrt{(x_{r,i} - x_{\text{ris}})^2 + (y_{r,i} - y_{\text{ris}})^2}}, \tag{7.41}$$

$$H_{5,3} = \frac{\sqrt{(x_{r,i} - x_{\text{ris}})^2 + (y_{r,i} - y_{\text{ris}})^2}}{\left\|\boldsymbol{r}_{r,i} - \boldsymbol{r}_{\text{ris}}\right\|_2^2}. \tag{7.42}$$

Please note that for simplicity of notation, $(k+1)$ was dropped from the above equations. The estimation error covariance matrix is updated according to

$$\mathbf{P}_i(k+1|k+1) = \left[\mathbf{I} - \mathbf{K})i(k+1)\mathbf{H}_i(k+1)\right] \mathbf{P}_i(k+1|j). \tag{7.43}$$

7.5 Results

The efficacy of the proposed approach is demonstrated through its application to three distinct scenarios: pedestrians, ground vehicles, and UAVs. This section is structured as follows: First, we present the configuration of the simulator used for the performance evaluation. This is followed by an analysis of the accuracy of the measurement engine, comparing its performance with and without the presence of multipath effects across the different scenarios. Finally, we assess the overall navigation performance of the proposed approach, delineating its effectiveness in each of the aforementioned scenarios.

7.5.1 Simulator

A 5G OFDM simulator was developed to evaluate the proposed method, ensuring the realistic emulation of received 5G signals. The block diagram of the simulator is illustrated in Figure 7.9. The simulator operates in two primary stages: the user interface and the 5G simulation process.

In the user interface stage, parameters such as the dynamic range of the receiver, local map generation, cell size, carrier frequency denoted by f_c, signal bandwidth, multipath characteristics, and RIS configurations are specified by the user. The dynamic parameters for the simulation are selected at random within the bounds of the user-defined dynamic range for the scenarios considered.

During the 5G simulation process, several key steps are carried out:

1. Random generation of UEs' trajectories within the constraints of the cell size defined by the user.

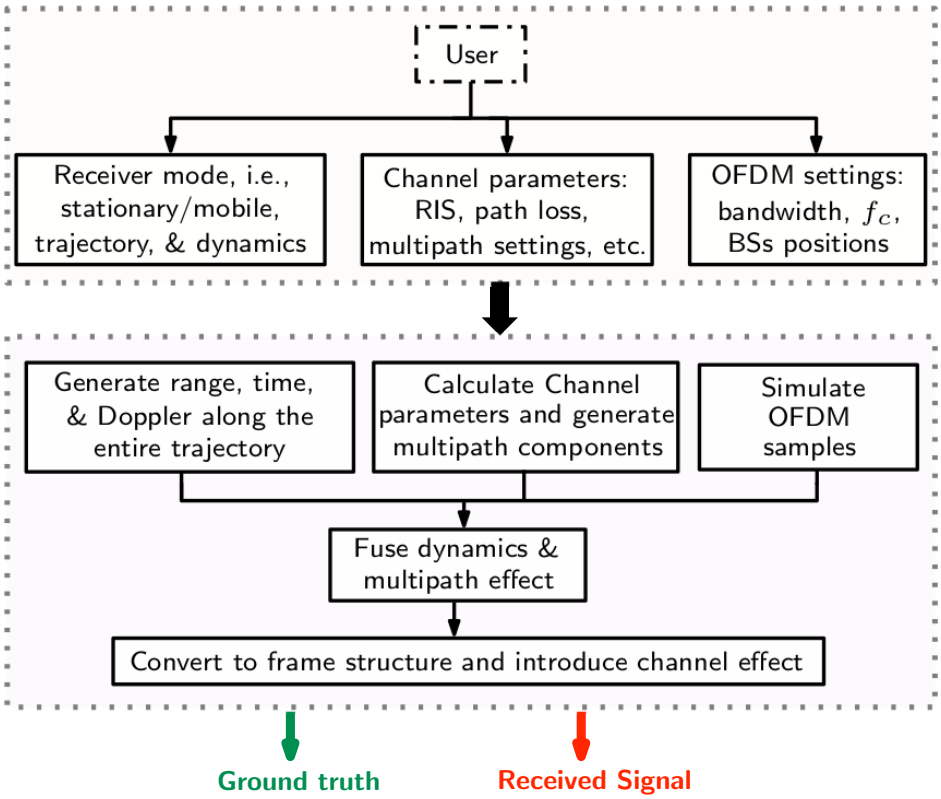


Figure 7.9: Simulator block diagram.

2. Determination of the BSs' positions and virtual multipath reflectors, distributed randomly based on the user's cell size preferences and the specified multipath delay spread.

3. Creation of time histories for range and Doppler shifts associated with LOS, VLOS, and multipath signal components.

4. Synthesis of the benchmark 5G OFDM signal for each UE, with the allocation of a unique 5G physical cell ID and signal configuration adhering to 3GPP standards [85].

5. Computation of channel parameters as detailed in Subsection 7.1.2.

6. Integration of dynamic parameters with the channel effects.

7. Compilation of the received signal for each user, coupled with ground truth data to facilitate performance assessment.

Table 7.2: Simulation Settings.

Parameter	Value	Description
x_{range}	[-1, 1] km	The geometric range in the x direction. A typical cell size
y_{range}	[-1, 1] km	The geometric range in the y direction
z_{range}	[-10, 10] m	The geometric range in the z direction. Represents the relative height between BS, RIS, and UE
N	64	Number of RIS elements
v_{init}	[0, 2.5] m/s	speed range of a pedestrian
q_x & q_y	[0, 1.44] m/s^2	range of pedestrian acceleration in the x and y directions
q_z	[0, 1] m/s^2	range of pedestrian acceleration in the z direction
$\mathbf{P}(0\|0)$	$\text{diag}([\mathbf{10}_{1\times3}^{\mathsf{T}}, \mathbf{5}_{1\times3}^{\mathsf{T}}]^{\mathsf{T}})$	Initial covariance matrix
$\mathbf{R}$	$\text{diag}([1, 5, 5]^{\mathsf{T}})$	measurement noise covariance matrix

7.5.2 Sample Iteration

In the rest of this chapter, the measurement engine and the proposed RIS-enabled navigation framework are assessed. To do so, MC simulations are conducted. This section presents a simplified single-realization sample, i.e., an iteration in the MC simulations. In this realization, a single UE and walking pedestrian dynamics are considered. The simulation settings are summarized in Table 7.2. The OFDM settings used are the same in Table 7.1. The duration of the simulation was set to be 300 seconds, in which the UE traversed a distance of 1.5 km. The proposed approach exhibited a position RMSE of 0.78 m and 1.2 m in 2D and 3D, respectively. The simulation scenario and the navigation solution are shown in Figure 7.10. the empirical cumulative distribution function (CDF) of the positioning error is shown in Figure 7.12, where the depicted 50-th and 80-th percentile are 0.14 and 0.35 m, respectively. Finally, the EKF estimation errors along with the $\pm 3\sigma$ bounds are presented in Figure 7.11.

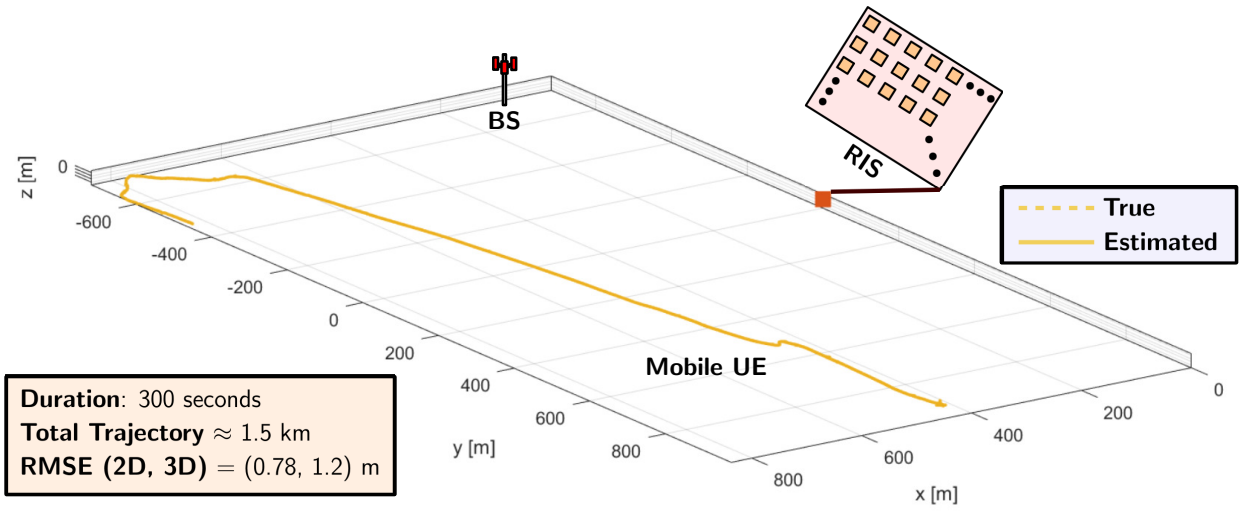


Figure 7.10: Sample iteration - Simulation scenario and navigation solution:

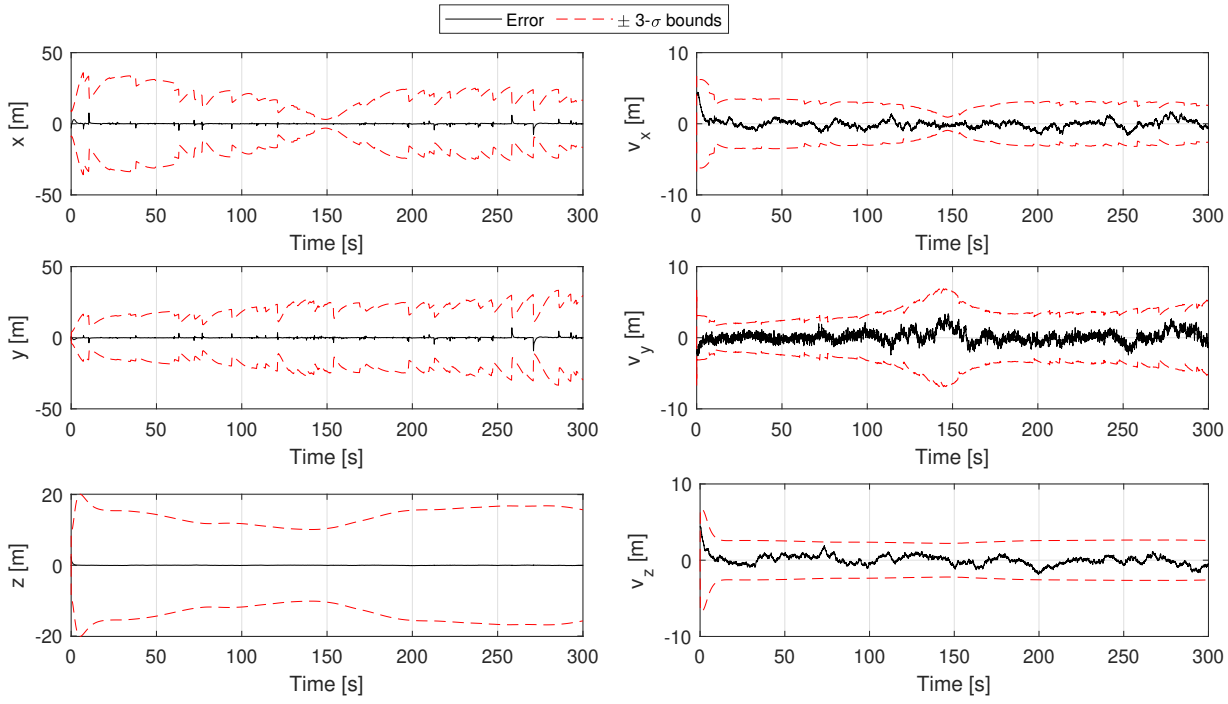


Figure 7.11: Sample iteration - EKF estimation errors along with the $\pm 3\sigma$ bounds.

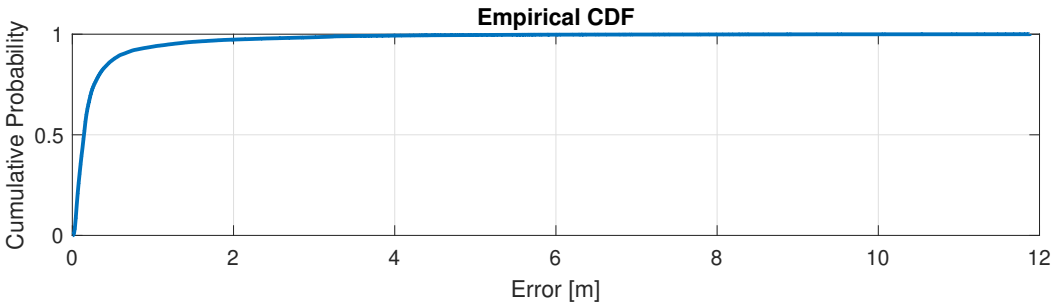


Figure 7.12: Sample iteration - Positioning error empirical CDF.

Table 7.3: Dynamics parameters for different platforms.

Platform	Parameter	Value
Pedestrian	v_{init}	[0, 2.5] m/s
	q_x & q_y	[0, 1.44] m/s^2
	q_z	[0, 1] m/s^2
Ground Vehicle	v_{init}	[0, 50] m/s
	q_x & q_y	[0, 5] m/s^2
	q_z	[0, 2] m/s^2
UAV	v_{init}	[0, 25] m/s
	q_x & q_y	[0, 3] m/s^2
	q_z	[0, 4] m/s^2

7.5.3 Performance Evaluation

7.5.3.1 Multipath-Free with Only VLOS Available

This section presents an MC simulation that assesses the navigation accuracy of the proposed system under different dynamic scenarios, assuming only the VLOS path is accessible and that UE and BS clocks are synchronized. Three platforms are considered: pedestrian, ground vehicle, and UAV. The simulation parameters align with those in Table 7.2, with adjustments in the ranges for v_{init} and $[q_x, q_y, q_z]$ to suit each platform according to Table 7.3.

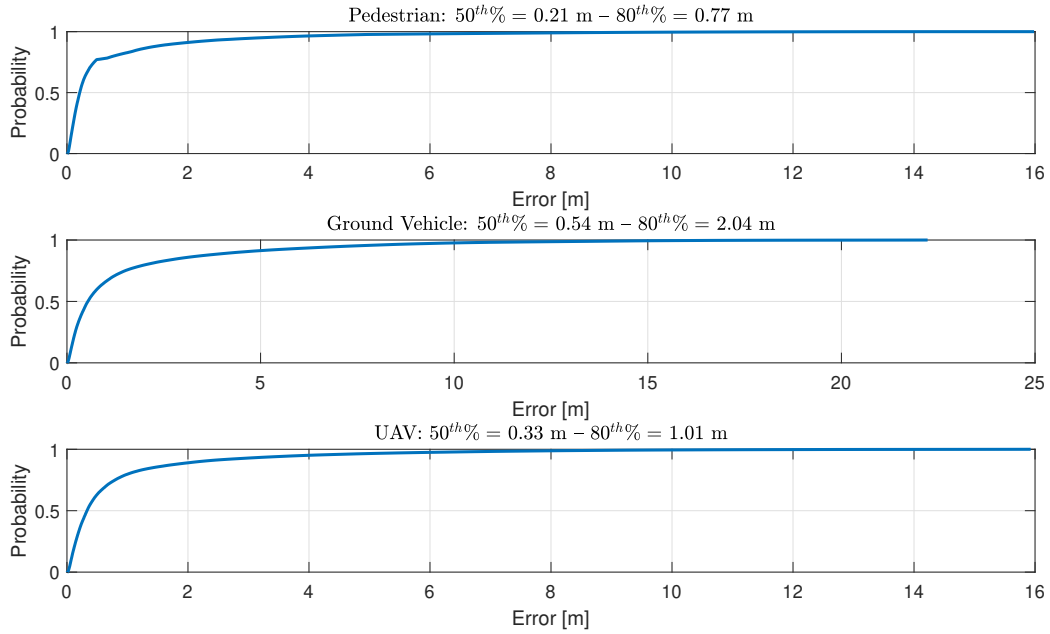


Figure 7.13: Scenario: VLOS Only with Synchronized Clocks – Empirical CDF of Positioning Error for Different Platforms.

The simulation, executed for 100 iterations, examines the positioning error. Figure 7.13 displays the empirical CDFs of these errors. Results indicate that pedestrian dynamics yield the highest accuracy, while ground vehicles show slightly lower accuracy, attributable to their more complex dynamics introducing greater noise in both processes and measurements.

7.5.3.2 Multipath-Free with Both LOS and VLOS Available

This section extends the MC simulations to consider scenarios where both LOS and VLOS paths are available, with synchronized UE and BS clocks. The three platforms - pedestrian, ground vehicle, and UAV - are again evaluated, using simulation parameters from Table 7.2 but tailored for each platform type according to Table 7.3.

Conducted over 500 iterations, the simulation investigates the combined effect of LOS and VLOS paths on positioning accuracy. Figure 7.14 presents the average empirical CDFs of positioning errors across all iterations and user scenarios. Consistent with the VLOS-only

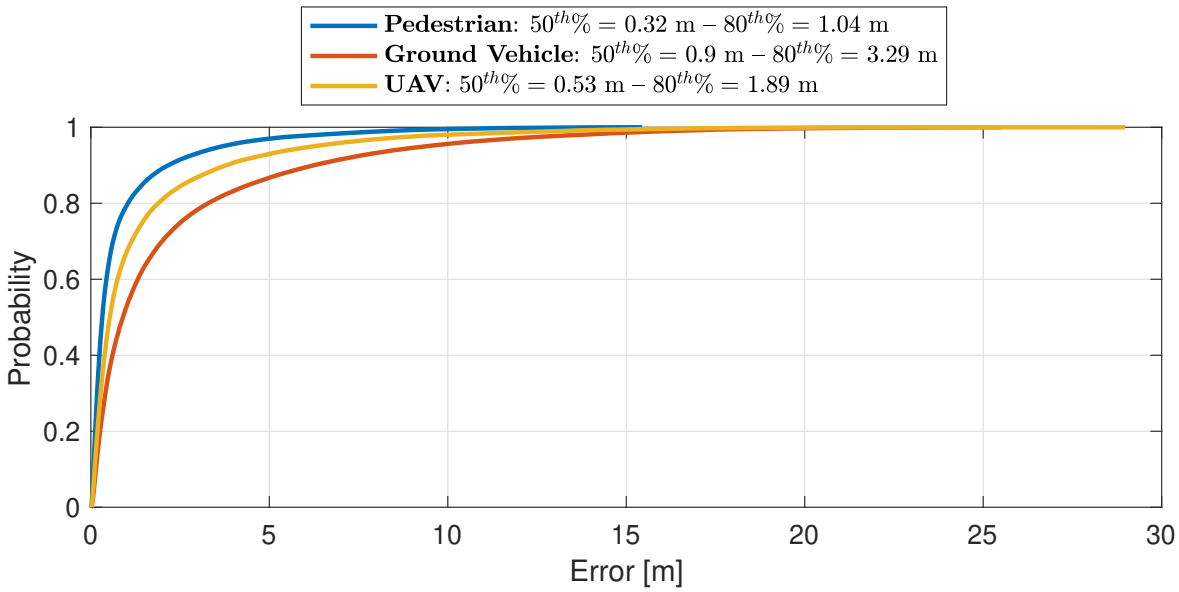


Figure 7.14: Scenario: LOS and VLOS with Synchronized Clocks – Empirical CDF of Positioning Error for Different Platforms.

scenario, pedestrians exhibit the highest accuracy, with ground vehicles showing slightly lower accuracy. Notably, including LOS measurements significantly enhances navigation precision compared to relying solely on VLOS measurements.

7.5.3.3 Mutlipath Analysis

In this section, the accuracy of the measurement engine is analyzed in a closed-loop fashion where both LOS and VLOS paths are available, with synchronized UE and BS clocks, and a single-antenna BS. To do so, an MC simulation is conducted. The simulation settings are summarized in Tables 7.4 and 7.3. The MC simulation was run for 500 iterations per scenario, each with a random set of parameters selected according to the ranges provided in the aforementioned tables.

In analyzing the performance of the proposed approach under various scenarios, including pedestrians with short-delay and long-delay multipath (SDM and LDM), ground vehicles with SDM and LDM, and UAVs with SDM and LDM, several trends are observed as depicted

Table 7.4: Monte Carlo Simulation Settings.

Parameter	**Value**	**Description**
x_{range}	[-2.5, 2.5] km	The geometric range in the x direction. A typical cell size
y_{range}	[-2.5, 2.5] km	The geometric range in the y direction
z_{range}	[-50, 50] m	The geometric range in the z direction. Represents the relative height between BS, RIS, and UE
f_c	28 GHz	Carrier frequency
B	20 MHz	OFDM Signal Bandwidth
t_{frame}	10 ms	Typical 5G frame duration
sc	15 kHz	OFDM subcarrier spacing
N	64	Number of RIS elements
N_u	{1, 2, 4, 6, 8, 12, 16, 24}	Number of BS antennas
L	$\{1, \cdots, 15\}$	Number of multipath signals
$\sigma_{\tau,l}$	$\{0.1, 1\}^*$ km	Multipath delay spread
$\mathbf{P}(0\|0)$	$\text{diag}(\boldsymbol{p}_{\text{init}})$	Initial covariance matrix
$\mathbf{R}(0\|0)$	$\text{diag}(\boldsymbol{r}_{\text{init}})$	Measurement noise covariance matrix
v_{init}	[Table 7.3]	Initial speed range
q_x, q_y, & q_z	[Table 7.3]	Range of acceleration in the x, y, and z directions
t_{iter}	20 sec	Duration of each iteration
I	[1, 15]	Number of UEs

$\boldsymbol{p}_{\text{init}} \triangleq \left[\mathbf{10}_{1\times3}^{\mathsf{T}}, \mathbf{5}_{1\times3}^{\mathsf{T}}, \mathbf{10}_{1\times2}^{\mathsf{T}}, \cdots\right]^{\mathsf{T}}$
$\boldsymbol{r}_{\text{init}} \triangleq [1, 1, 5, 1]^{\mathsf{T}}$
* Considered short-delay and long-delay multipath.

in Figure 7.15. It is worth mentioning that this study assumed a single-antenna BS to study the effect of multipath. The observed trends are influenced by the increasing number of multipath signals, as reflected in the azimuth and elevation AOA accuracies, positioning accuracies, and signal tracking success rates.

For pedestrians in SDM conditions, there is a noticeable increase in azimuth and elevation AOA accuracies with the number of multipath signals, peaking at four signals before a slight decrease, likely attributed to the imperfections in the MC simulation rather than an actual deterioration in system performance. The positioning accuracy worsens with an increase in multipath signals, while the signal tracking success rate shows a substantial decline.

In the scenario of pedestrians in LDM, both azimuth and elevation AOA accuracies increase slightly with more multipath signals, but the positioning accuracy worsens marginally. The signal tracking success rate remains consistently high, only showing a slight drop at higher signal numbers, which again might be due to simulation imperfections.

Ground vehicles in SDM exhibit a significant increase in both azimuth and elevation AOA accuracies with an increasing number of multipath signals. However, similar to pedestrians, the positioning accuracy deteriorates, and the signal tracking success rate decreases notably after three signals, a pattern possibly exaggerated by the simulation's limitations.

For ground vehicles in LDM, there is a moderate increase in azimuth AOA accuracy with more multipath signals, and the elevation AOA accuracy follows a similar trend. The positioning accuracy slightly deteriorates with increasing multipath signals. The signal-tracking success rate remains high, indicating robustness in these conditions.

In the case of UAVs with SDM, both azimuth and elevation AOA accuracies increase significantly, particularly up to four signals, and then stabilize. The positioning accuracy worsens with more multipath signals, and the signal-tracking success rate decreases significantly, which might be partly due to the imperfections in the simulation process.

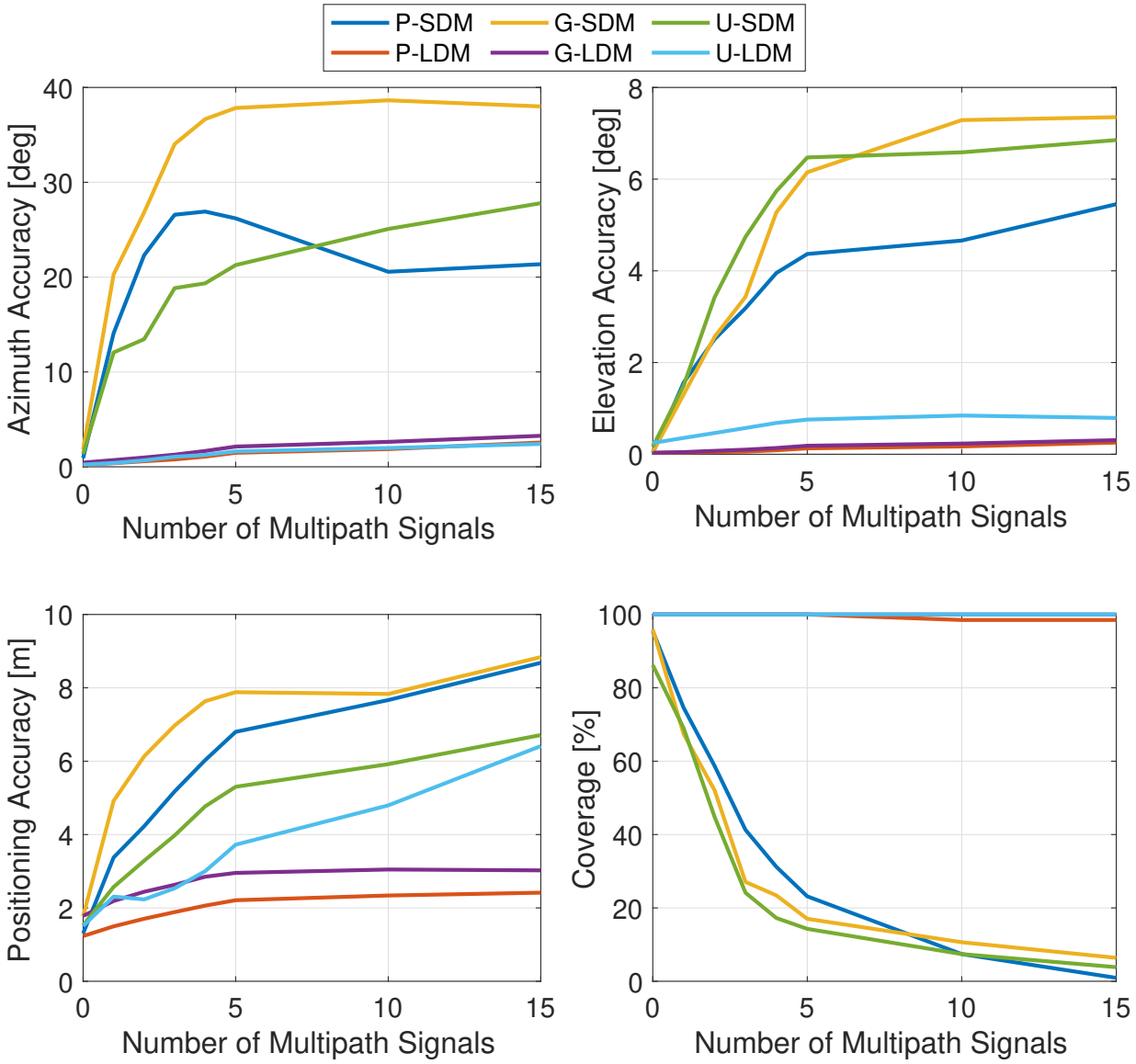


Figure 7.15: Performance evaluation of the proposed approach vs multipath under various scenarios, including pedestrians with short-delay and long-delay multipath (SDM and LDM), ground vehicles with SDM and LDM, and UAVs with SDM and LDM.

Lastly, UAVs in LDM conditions show a gradual increase in azimuth AOA accuracy with more multipath signals, and the elevation AOA accuracy increases slightly then stabilizes. The positioning accuracy worsens with an increasing number of multipath signals, but the signal tracking success rate remains consistently high across all signal numbers, suggesting a potential overestimation in the simulation's accuracy at higher multipath conditions.

Overall, these trends suggest that the increase in multipath signals generally leads to a deterioration in positioning accuracy and signal tracking success rate, with some variations in azimuth and elevation AOA accuracies. However, it is important to note that the slight decreases observed after certain peaks in the data are likely anomalies resulting from the imperfections inherent in the MC simulation process, rather than true reflections of system performance.

7.5.3.4 Effect of the BS's Antennas Design

In this section, the effect of the number of the BS's antenna elements on the performance of the proposed approach is studied. The simulation settings are similar to the ones in Tables 7.4 and 7.3 except for assuming no multipath signals to exclusively assess the impact of the BS infrastructure for different dynamical scenarios. The MC simulation was run for 200 iterations per scenario. The results of the simulation are depicted in Figure 7.16.

The data from the three scenarios - pedestrians, ground vehicles, and UAVs - reveal insightful trends concerning the number of antenna elements of the BS and its influence on azimuth and elevation AOA accuracies, positioning accuracy, and signal tracking success rate.

For pedestrians, as the number of antenna elements increases from 1 to 24, there is a clear improvement in the azimuth AOA accuracy, decreasing from 0.4369 degrees to 0.0493 degrees. The elevation AOA accuracy remains consistently low, with a minimal variation, suggesting high precision. Positioning accuracy improves significantly, decreasing from 0.7636 meters

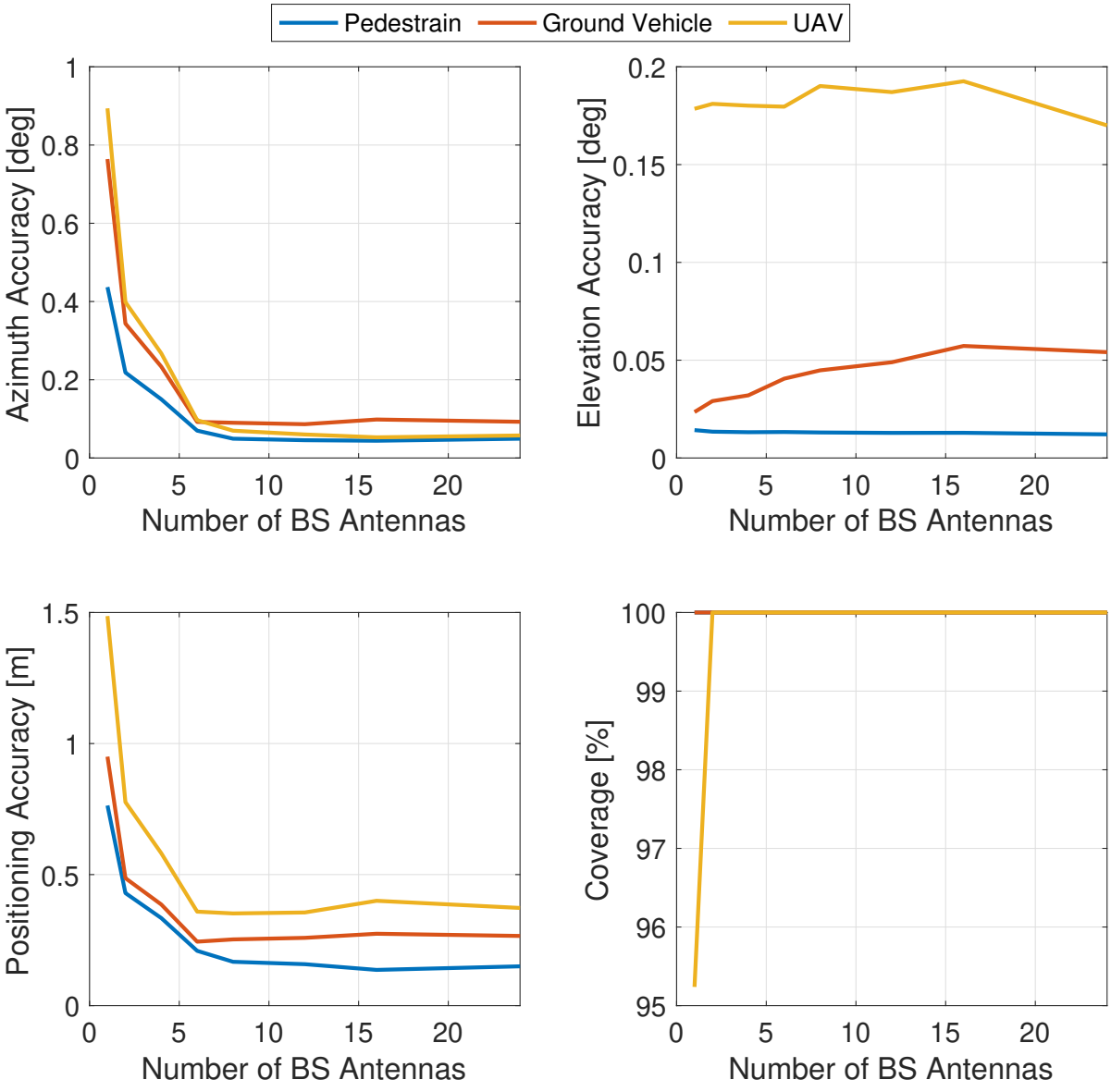


Figure 7.16: Performance evaluation of the proposed approach vs the number of the BS's antenna elements under various scenarios including pedestrians, ground vehicles, and UAVs

to 0.1500 meters, while the signal tracking success rate remains consistently high at 100

In the case of ground vehicles, a similar trend is observed. The azimuth AOA accuracy improves markedly with an increase in antenna elements, dropping from 0.7641 degrees to 0.0926 degrees. Elevation AOA accuracy also shows improvement, although with slightly more variation compared to the pedestrian scenario. Positioning accuracy exhibits significant enhancement, reducing from 0.9500 meters to 0.2659 meters, with a constant signal tracking success rate of 100

For UAVs, the data shows an initial high azimuth AOA accuracy at 1 antenna element (0.8939 degrees), which then improves consistently as the number of antenna elements increases, reaching 0.0575 degrees at 24 elements. Elevation AOA accuracy demonstrates a relatively stable trend with slight fluctuations. Positioning accuracy improves from 1.4864 meters to 0.3727 meters as the number of antenna elements increases. Notably, the signal tracking success rate starts at 95.2381% with one antenna element and reaches 100% with two or more elements, indicating a rapid improvement in tracking capabilities with additional antenna elements.

These trends collectively suggest that increasing the number of antenna elements in a BS significantly enhances the accuracy of azimuth and elevation AOAs and improves overall positioning accuracy. The consistent 100% success rate in tracking signals for ground vehicles and UAVs, and the rapid achievement of this rate in the UAV scenario, further underscores the effectiveness of increasing antenna elements in navigation systems. This improvement is particularly notable in scenarios with higher complexity, such as UAV operations, where precise navigation is crucial.

Chapter 8

Conclusion

This dissertation represents a significant foray into the realm of 4G and 5G cellular signals, exploring their potential and developing innovative applications in navigation. The journey embarked upon in this research has yielded insights and technological advancements that redefine the boundaries of cellular navigation technology.

The initial phase of this work entailed a deep analysis of the evolution from 4G to 5G, focusing on advanced numerologies and dynamic models for UE motion. This exploration was instrumental in understanding the potential of these signals for navigation, laying the groundwork for subsequent innovations.

Building upon this foundational knowledge, a novel design for an opportunistic cellular navigation receiver was introduced, targeting enhancements in accuracy, robustness, and efficiency. The development of the Ultimate Reference Signal for 4G and the Ultimate Synchronization Signal for 5G marked a significant step forward, enabling improved navigation capabilities, especially in challenging conditions.

Practical evaluation followed, with the experimental characterization of 4/5G signals. As-

sessing their stability and carrier-to-noise density ratio in various conditions underscored the feasibility of these signals for precise and dependable navigation.

The performance of the proposed receiver was then demonstrated through experiments in diverse scenarios such as ground vehicles, high-altitude aircraft, and UAVs. These tests showcased the effectiveness of 4G and 5G signals in providing robust and accurate navigation across different platforms and environments.

Further innovation was presented through the development of a UE-based 5G navigation framework that efficiently utilizes 'on-demand' 5G downlink signals. This novel approach led to marked improvements in signal quality and a significant reduction in ranging errors, highlighting the advanced capabilities of 5G in navigational applications.

Lastly, a novel approach involving a RIS-aided cellular navigation system was developed for millimeter-wave uplink environments. This approach, integrating a sophisticated measurement engine and an EKF-based framework, demonstrated the potential to achieve impressive positioning accuracy in a variety of scenarios for future cellular systems.

In summary, this dissertation contributes significantly to the field of cellular navigation, not only by enhancing the understanding of 4G and 5G signals but also by introducing practical, robust, and efficient solutions for their use in navigation. This work opens new avenues for the application of cellular signals in real-world navigation and sets a foundation for future research and development in this promising domain.

Bibliography

[1] K. Shamaei and Z. Kassas, "LTE receiver design and multipath analysis for navigation in urban environments," *NAVIGATION, Journal of the Institute of Navigation*, vol. 65, no. 4, pp. 655–675, December 2018.

[2] G. Seco-Granados, J. Lopez-Salcedo, D. Jiménez-Baños, and G. Lopez-Risueño, "Challenges in indoor global navigation satellite systems: Unveiling its core features in signal processing," *IEEE Signal Processing Magazine*, vol. 29, no. 2, pp. 108–131, March 2012.

[3] J. Grabowski, "Personal privacy jammers: locating Jersey PPDs jamming GBAS safety-of-life signals," *GPS World Magazine*, pp. 28–37, April 2012.

[4] C. Günther, "A survey of spoofing and counter-measures," *NAVIGATION, Journal of the Institute of Navigation*, vol. 61, no. 3, pp. 159–177, 2014.

[5] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Ganga-Jamuna Press, 2010.

[6] J. Farrell and M. Barth, *Aided Navigation: GPS with High Rate Sensors*. New York: McGraw-Hill, 2008.

[7] W. Wen and L. Hsu, "3D LiDAR aided GNSS NLOS mitigation in urban canyons," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 18 224–18 236, 2022.

[8] L. Fusini, T. Fossen, and T. Johansen, "Nonlinear observers for GNSS-and camera-aided inertial navigation of a fixed-wing UAV," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 5, pp. 1884–1891, 2017.

[9] M. Psiaki and B. Slosman, "Tracking of digital FM OFDM signals for the determination of navigation observables," in *Proceedings of ION GNSS Conference*, September 2019, pp. 2325–2348.

[10] M. Orabi, J. Khalife, and Z. Kassas, "Opportunistic navigation with Doppler measurements from Iridium Next and Orbcomm LEO satellites," in *Proceedings of IEEE Aerospace Conference*, March 2021, accepted.

[11] C. Yan and H. Fan, "Asynchronous differential TDOA for non-GPS navigation using signals of opportunity," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, 2008, pp. 5312–5315.

[12] Y. Zhuang and N. El-Sheimy, "Tightly-coupled integration of WiFi and MEMS sensors on handheld devices for indoor pedestrian navigations," *IEEE Sensors Journal*, vol. 16, no. 1, pp. 224–234, 2016.

[13] Z. Zhang, S. He, Y. Shu, and Z. Shi, "A self-evolving WiFi-based indoor navigation system using smartphones," *IEEE Transactions on Mobile Computing*, vol. 19, no. 8, pp. 1760–1774, 2020.

[14] J. Seo, Y. Chen, D. De Lorenzo, S. Lo, P. Enge, D. Akos, and J. Lee, "A real-time capable software-defined receiver using GPU for adaptive anti-jam GPS sensors," *Sensors*, vol. 11, no. 9, pp. 8966–8991, September 2011.

[15] A. Kerns, D. Shepard, J. Bhatti, and T. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[16] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 134–139, August 2017.

[17] Y. Wu, J. Wang, and D. Hu, "A new technique for INS/GNSS attitude and parameter estimation using online optimization," *IEEE Transactions on Signal Processing*, vol. 62, no. 10, pp. 2642–2655, May 2014.

[18] S. Zhao, Y. Chen, and J. Farrell, "High-precision vehicle navigation in urban environments using an MEM's IMU and single-frequency GPS receiver," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 10, pp. 2854–2867, October 2016.

[19] M. Atia, A. Hilal, C. Stellings, E. Hartwell, J. Toonstra, W. Miners, and O. Basir, "A low-cost lane-determination system using GNSS/IMU fusion and HMM-based multistage map matching," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 3027–3037, November 2017.

[20] E. Hinüber, C. Reimer, T. Schneider, and M. Stock, "INS/GNSS integration for aerobatic flight applications and aircraft motion surveying," *Sensors*, vol. 17, no. 5, pp. 941–956, 2017.

[21] A. Garcia-Moreno and J. Gonzalez-Barbosa, "GPS precision time stamping for the HDL-64E Lidar sensor and data fusion," in *Proceedings of IEEE Electronics, Robotics and Automotive Mechanics Conference*, November 2012, pp. 48–53.

[22] J. Khalife, S. Ragothaman, and Z. Kassas, "Pose estimation with lidar odometry and cellular pseudoranges," in *Proceedings of IEEE Intelligent Vehicles Symposium*, June 2017, pp. 1722–1727.

[23] J. Meguro, T. Murata, J. Takiguchi, Y. Amano, and T. Hashizume, "GPS multipath mitigation for urban area using omnidirectional infrared camera," *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 1, pp. 22–30, March 2009.

[24] A. Mulloni, D. Wagner, I. Barakonyi, and D. Schmalstieg, "Indoor positioning and navigation with camera phones," *IEEE Pervasive Computing*, vol. 8, no. 2, pp. 22–31, April 2009.

[25] A. Hassani, N. Morris, M. Spenko, and M. Joerger, "Experimental integrity evaluation of tightly-integrated IMU/LiDAR including return-light intensity data," in *Proceedings of ION GNSS Conference*, September 2019, pp. 2637–2658.

[26] L. Chang, X. Niu, T. Liu, J. Tang, and C. Qian, "GNSS/INS/LiDAR-SLAM integrated navigation system based on graph optimization," *Remote Sensing*, vol. 11, no. 9, p. 1009, 2019.

[27] S. Saab and Z. Kassas, "Power matching approach for GPS coverage extension," *IEEE Transactions on Intelligent Transportation Systems*, vol. 7, no. 2, pp. 156–166, June 2006.

[28] F. Caron, M. Davy, E. Duflos, and P. Vanheeghe, "Particle filtering for multisensor data fusion with switching observation models: application to land vehicle positioning," *IEEE Transactions on Signal Processing*, vol. 55, no. 6, pp. 2703–2719, June 2007.

[29] B. Xu, Q. Jia, and L. Hsu, "Vector tracking loop-based GNSS NLOS detection and correction: Algorithm design and performance analysis," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 7, pp. 4604–4619, 2019.

[30] C. Jiang, S. Chen, Y. Chen, D. Liu, and Y. Bo, "GNSS vector tracking method using graph optimization," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 4, pp. 1313–1317, 2020.

[31] R. Martin, C. Yan, H. Fan, and C. Rondeau, "Algorithms and bounds for distributed TDOA-based positioning using OFDM signals," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1255–1268, March 2011.

[32] I. Bilik, K. Adhikari, and J. R. Buck, "Shannon capacity bound on mobile station localization accuracy in urban environments," *IEEE Transactions on Signal Processing*, vol. 59, no. 12, pp. 6206–6216, December 2011.

[33] C. Yang, T. Nguyen, and E. Blasch, "Mobile positioning via fusion of mixed signals of opportunity," *IEEE Aerospace and Electronic Systems Magazine*, vol. 29, no. 4, pp. 34–46, April 2014.

[34] J. Khalife, K. Shamaei, and Z. Kassas, "A software-defined receiver architecture for cellular CDMA-based navigation," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2016, pp. 816–826.

[35] Z. Kassas, J. Khalife, K. Shamaei, and J. Morales, "I hear, therefore I know where I am: Compensating for GNSS limitations with cellular signals," *IEEE Signal Processing Magazine*, pp. 111–124, September 2017.

[36] A. Abdallah, S. Saab, and Z. Kassas, "A machine learning approach for localization in cellular environments," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2018, pp. 1223–1227.

[37] Z. Kassas, "Position, navigation, and timing technologies in the 21st century," J. Morton, F. van Diggelen, J. Spilker, Jr., and B. Parkinson, Eds. Wiley-IEEE, 2021, vol. 2, ch. 43: Navigation from low Earth orbit – Part 2: models, implementation, and performance, pp. 1381–1412.

[38] J. McEllroy, "Navigation using signals of opportunity in the AM transmission band," Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA, 2006.

[39] S. Fang, J. Chen, H. Huang, and T. Lin, "Is FM a RF-based positioning solution in a metropolitan-scale environment? A probabilistic approach with radio measurements analysis," *IEEE Transactions on Broadcasting*, vol. 55, no. 3, pp. 577–588, September 2009.

[40] M. Joerger, L. Gratton, B. Pervan, and C. Cohen, "Analysis of Iridium-augmented GPS for floating carrier phase positioning," *NAVIGATION, Journal of the Institute of Navigation*, vol. 57, no. 2, pp. 137–160, 2010.

[41] K. Pesyna, Z. Kassas, and T. Humphreys, "Constructing a continuous phase time history from TDMA signals for opportunistic navigation," in *Proceedings of IEEE/ION Position Location and Navigation Symposium*, April 2012, pp. 1209–1220.

[42] J. Morales, J. Khalife, U. Santa Cruz, and Z. Kassas, "Orbit modeling for simultaneous tracking and navigation using LEO satellite signals," in *Proceedings of ION GNSS Conference*, September 2019, pp. 2090–2099.

[43] J. Khalife and Z. Kassas, "Receiver design for Doppler positioning with LEO satellites," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, May 2019, pp. 5506–5510.

[44] Z. Kassas, J. Khalife, M. Neinavaie, and T. Mortlock, "Opportunity comes knocking: overcoming GPS vulnerabilities with other satellites' signals," *Inside Unmanned Systems Magazine*, pp. 30–35, June/July 2020.

[45] M. Rabinowitz and J. Spilker, Jr., "A new positioning system using television synchronization signals," *IEEE Transactions on Broadcasting*, vol. 51, no. 1, pp. 51–61, March 2005.

[46] P. Thevenon, S. Damien, O. Julien, C. Macabiau, M. Bousquet, L. Ries, and S. Corazza, "Positioning using mobile TV based on the DVB-SH standard," *NAVIGATION, Journal of the Institute of Navigation*, vol. 58, no. 2, pp. 71–90, 2011.

[47] R. Faragher, C. Sarno, and M. Newman, "Opportunistic radio SLAM for indoor navigation using smartphone sensors," in *Proceedings of IEEE/ION Position Location and Navigation Symposium*, April 2012, pp. 120–128.

[48] J. Prieto, S. Mazuelas, A. Bahillo, P. Fernandez, R. Lorenzo, and E. Abril, "Adaptive data fusion for wireless localization in harsh environments," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1585–1596, April 2012.

[49] J. Khalife, Z. Kassas, and S. Saab, "Indoor localization based on floor plans and power maps: Non-line of sight to virtual line of sight," in *Proceedings of ION GNSS Conference*, September 2015, pp. 2291–2300.

[50] Y. Shu, Y. Huang, J. Zhang, P. Coue, P. Cheng, J. Chen, and K. Shin, "Gradient-based fingerprinting for indoor localization and tracking," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 4, pp. 2424–2433, 2016.

[51] T. Reid, A. Neish, T. Walter, and P. Enge, "Leveraging commercial broadband LEO constellations for navigating," in *Proceedings of ION GNSS Conference*, September 2016, pp. 2300–2314.

[52] C. Gentner, E. Munoz, M. Khider, E. Staudinger, S. Sand, and A. Dammann, "Particle filter based positioning with 3GPP-LTE in indoor environments," in *Proceedings of IEEE/ION Position, Location and Navigation Symposium*, April 2012, pp. 301–308.

[53] M. Driusso, C. Marshall, M. Sabathy, F. Knutti, H. Mathis, and F. Babich, "Indoor positioning using LTE signals," in *Proceedings of International Conference on Indoor Positioning and Indoor Navigation*, October 2016, pp. 1–8.

[54] K. Shamaei, J. Khalife, and Z. Kassas, "Exploiting LTE signals for navigation: Theory to implementation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2173–2189, April 2018.

[55] F. Pittino, M. Driusso, A. Torre, and C. Marshall, "Outdoor and indoor experiments with localization using LTE signals," in *Proceedings of European Navigation Conference*, May 2017, pp. 311–321.

[56] Z. Kassas, J. Morales, K. Shamaei, and J. Khalife, "LTE steers UAV," *GPS World Magazine*, vol. 28, no. 4, pp. 18–25, April 2017.

[57] K. Shamaei, J. Khalife, and Z. Kassas, "Pseudorange and multipath analysis of positioning with LTE secondary synchronization signals," in *Proceedings of Wireless Communications and Networking Conference*, April 2018, pp. 286–291.

[58] K. Shamaei, J. Morales, and Z. Kassas, "A framework for navigation with LTE time-correlated pseudorange errors in multipath environments," in *Proceedings of IEEE Vehicular Technology Conference*, April 2019, pp. 1–6.

[59] K. Shamaei and Z. Kassas, "Sub-meter accurate UAV navigation and cycle slip detection with LTE carrier phase," in *Proceedings of ION GNSS Conference*, September 2019, pp. 2469–2479.

[60] W. Xu, M. Huang, C. Zhu, and A. Dammann, "Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 3, pp. 339–356, 2016.

[61] P. Wang and Y. Morton, "Multipath estimating delay lock loop for LTE signal TOA estimation in indoor and urban environments," *IEEE Transactions on Wireless Communications*, vol. 19, no. 8, pp. 5518–5530, 2020.

[62] H. Dun, C. Tiberius, and G. Janssen, "Positioning in a multipath channel using OFDM signals with carrier phase tracking," *IEEE Access*, vol. 8, pp. 13 011–13 028, 2020.

[63] P. Wang, Y. Wang, and J. Morton, "Signal tracking algorithm with adaptive multipath mitigation and experimental results for LTE positioning receivers in urban environments," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 4, pp. 2779–2795, August 2022.

[64] C. Yang, T. Pany, and P. Weitkemper, "Effect of antenna ports on TOA estimation with 4G LTE signals in urban mobile environments," in *Proceedings of ION GNSS+ Conference*, January 2020, pp. 2166–2181.

[65] M. Driusso, C. Marshall, M. Sabathy, F. Knutti, H. Mathis, and F. Babich, "Vehicular position tracking using LTE signals," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3376–3391, April 2017.

[66] I. Lapin, G. Granados, J. Samson, O. Renaudin, F. Zanier, and L. Ries, "STARE: Real-time software receiver for LTE and 5G NR positioning and signal monitoring," in *Proceedings of Workshop on Satellite Navigation Technology*, April 2022, pp. 1–11.

[67] J. Gante, L. Sousa, and G. Falcao, "Dethroning GPS: Low-power accurate 5G positioning systems using machine learning," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 10, no. 2, pp. 240–252, 2020.

[68] I. Lapin, G. Seco-Granados, O. Renaudin, F. Zanier, and L. Ries, "Joint delay and phase discriminator based on ESPRIT for 5G NR positioning," *IEEE Access*, vol. 9, pp. 126 550–126 563, 2021.

[69] N. Garcia, H. Wymeersch, E. Larsson, A. Haimovich, and M. Coulon, "Direct localization for massive MIMO," *IEEE Transactions on Signal Processing*, vol. 65, no. 10, pp. 2475–2487, May 2017.

[70] C. Guo, J. Yu, W. Guo, Y. Deng, and J. Liu, "Intelligent and ubiquitous positioning framework in 5G edge computing scenarios," *IEEE Access*, vol. 8, pp. 83 276–83 289, 2020.

[71] X. Cui, T. Gulliver, J. Li, and H. Zhang, "Vehicle positioning using 5G millimeter-wave systems," *IEEE Access*, vol. 4, pp. 6964–6973, 2016.

[72] M. Koivisto, M. Costa, J. Werner, K. Heiska, J. Talvitie, K. Leppanen, V. Koivunen, and M. Valkama, "Joint device positioning and clock synchronization in 5G ultra-dense networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 2866–2881, May 2017.

[73] K. Shamaei and Z. Kassas, "Receiver design and time of arrival estimation for opportunistic localization with 5G signals," *IEEE Transactions on Wireless Communications*, 2021, accepted.

[74] E. Basar, M. D. Renzo, J. D. Rosny, M. Debbah, M. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, 2019.

[75] M. D. Renzo, A. Zappone, M. Debbah, M. Alouini, C. Yuen, J. D. Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE journal on selected areas in communications*, vol. 38, no. 11, pp. 2450–2525, 2020.

[76] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. D. Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE communications surveys & tutorials*, vol. 23, no. 3, pp. 1546–1577, 2021.

[77] T. Ma, Y. Xiao, X. Lei, W. Xiong, and Y. Ding, "Indoor localization with reconfigurable intelligent surface," *IEEE Communications Letters*, vol. 25, no. 1, pp. 161–165, 2020.

[78] K. Keykhosravi, M. Keskin, S. Dwivedi, G. Seco-Granados, and H. Wymeersch, "Semi-passive 3D positioning of multiple RIS-enabled users," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 11 073–11 077, 2021.

[79] M. Rahal, B. Denis, K. Keykhosravi, B. Uguen, and H. Wymeersch, "RIS-enabled localization continuity under near-field conditions," in *IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2021, pp. 436–440.

[80] J. He, A. Fakhreddine, C. Vanwynsberghe, H. Wymeersch, and G. Alexandropoulos, "3D localization with a single partially-connected receiving RIS: Positioning error analysis and algorithmic design," *arXiv preprint arXiv:2212.02088*, 2022.

[81] A. Albanese, P. Mursia, V. Sciancalepore, and X. Costa-Pérez, "PAPIR: Practical RIS-aided localization via statistical user information," in *International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2021, pp. 531–535.

[82] 3GPP, "Physical channels and modulation," https://www.etsi.org/deliver/etsi_ts/138200_138299/138211/17.06.00_60/ts_138211v170600p.pdf, 5G; NR; 3rd Generation Partnership Project (3GPP), TS 38.211, October 2023.

[83] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); physical channels and modulation," 3rd Generation Partnership Project (3GPP), TS 36.211, January 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36211.htm

[84] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); requirements for support of radio resource management," 3rd Generation Partnership Project (3GPP), TS 36.133, April.

[85] 3GPP, "Physical channels and modulation," https://www.etsi.org/deliver/etsi-ts/138200-138299/138211/15.02.00-60/ts-138211v150200p.pdf, 5G; NR; 3rd Generation Partnership Project (3GPP), TS 38.211, July 2018.

[86] X. Li and V. Jilkov, "Survey of maneuvering target tracking. Part I: Dynamic models," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 39, no. 4, pp. 1333–1364, 2003.

[87] Y. Bar-Shalom, X. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*. New York, NY: John Wiley & Sons, 2002.

[88] A. Abdallah, K. Shamaei, and Z. Kassas, "Performance characterization of an indoor localization system with LTE code and carrier phase measurements and an IMU," in *Proceedings of International Conference on Indoor Positioning and Indoor Navigation*, September 2019, pp. 1–8.

[89] A. Abdallah, K. Shamaei, and Z. Kassas, "Indoor localization with LTE carrier phase measurements and synthetic aperture antenna array," in *Proceedings of ION GNSS Conference*, September 2019, pp. 2670–2679.

[90] K. Shamaei and Z. Kassas, "A joint TOA and DOA acquisition and tracking approach for positioning with LTE signals," *IEEE Transactions on Signal Processing*, 2020, submitted.

[91] A. Soderini, P. Thevenon, C. Macabiau, L. Borgagni, and J. Fischer, "Pseudorange measurements with LTE physical channels," in *Proceedings of ION International Technical Meeting*, January 2020, pp. 817–829.

[92] A. Abdallah, K. Shamaei, and Z. Kassas, "Assessing real 5G signals for opportunistic navigation," in *Proceedings of ION GNSS Conference*, 2020, pp. 2548–2559.

[93] A. Abdallah and Z. Kassas, "Multipath mitigation via synthetic aperture beamforming for indoor and deep urban navigation," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 8838–8853, 2021.

[94] A. Abdallah, , and Z. Kassas, "UAV navigation with 5G carrier phase measurements," in *Proceedings of ION GNSS Conference*, 2021, pp. 3294–3306.

[95] P. Wang, Y. Wang, , and J. Morton, "Signal tracking algorithm with adaptive multipath mitigation and experimental results for LTE positioning receivers in urban environments," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 4, pp. 2779–2795, August 2022.

[96] R. Whiton, J. Chen, T. Johansson, and F. Tufvesson, "Urban navigation with LTE using a large antenna array and machine learning," in *Proceedings of IEEE Vehicular Technology Conference*, September 2022, pp. 1–5.

[97] L. Chen, X. Zhou, F. Chen, L. Yang, and R. Chen, "Carrier phase ranging for indoor positioning with 5G NR signals," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10 908–10 919, 2022.

[98] J. Tian, L. Fangchi, T. Yafei, and L. Dongmei, "Utilization of non-coherent accumulation for LTE TOA estimation in weak LOS signal environments," *EURASIP Journal on Wireless Communications and Networking*, vol. 2023, no. 1, pp. 1–31, 2023.

[99] 3GPP, "Base station (BS) radio transmission and reception," 3rd Generation Partnership Project (3GPP), TS 38.104, July 2018. [Online]. Available: https://www.etsi.org/deliver/etsi-ts/138100-138199/138104/15.02.00-60/ts-138104v150200p.pdf

[100] B. Yang, K. Letaief, R. Cheng, and Z. Cao, "Timing recovery for OFDM transmission," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 11, pp. 2278–2291, November 2000.

[101] 3GPP2, "Physical layer standard for cdma2000 spread spectrum systems (C.S0002-E)," 3rd Generation Partnership Project 2 (3GPP2), TS C.S0002-E, June 2011.

[102] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); user equipment (UE) radio transmission and reception," 3rd Generation Partnership Project (3GPP), TS 136.101, June 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36212.htm

[103] J. Khalife and Z. Kassas, "On the achievability of submeter-accurate UAV navigation with cellular signals exploiting loose network synchronization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 5, pp. 4261–4278, October 2022.

[104] Z. Kassas, J. Khalife, A. Abdallah, and C. Lee, "I am not afraid of the GPS jammer: resilient navigation via signals of opportunity in GPS-denied environments," *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, no. 7, pp. 4–19, July 2022.

[105] J. Morales and Z. Kassas, "Optimal collaborative mapping of terrestrial transmitters: receiver placement and performance characterization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 2, pp. 992–1007, April 2018.

[106] Z. Kassas, J. Khalife, A. Abdallah, C. Lee, J. Jurado, S. Wachtel, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte *et al.*, "Assessment of cellular signals of opportunity for high-altitude aircraft navigation," *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, no. 10, pp. 4–19, 2022.

[107] Z. Kassas, "Position, navigation, and timing technologies in the 21st century," J. Morton, F. van Diggelen, J. Spilker, Jr., and B. Parkinson, Eds. Wiley-IEEE, 2021, vol. 2, ch. 37: Navigation with cellular signals.

[108] Z. Kassas, V. Ghadiok, and T. Humphreys, "Adaptive estimation of signals of opportunity," in *Proceedings of ION GNSS Conference*, September 2014, pp. 1679–1689.

[109] A. Graff, W. Blount, P. Iannucci, J. Andrews, and T. Humphreys, "Analysis of OFDM signals for ranging and communications," in *Proceedings of ION GNSS Conference*, 2021, pp. 2910–2924.

[110] M. Neinavaie, J. Khalife, and Z. Kassas, "Cognitive opportunistic navigation in private networks with 5G signals and beyond," *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no. 1, pp. 129–143, 2022.

[111] M. Braasch and A. Dempster, "Tutorial: GPS receiver architectures, front-end and baseband signal processing," *IEEE Aerospace and Electronic Systems Magazine*, vol. 34, no. 2, pp. 20–37, February 2019.

[112] A. Shahmansoori, G. Seco-Granados, and H. Wymeersch, "Power allocation for OFDM wireless network localization under expectation and robustness constraints," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 2027–2038, 2017.

Appendix A

4G-URS and 5G-USS: Sequence Generation and Mapping

A.1 4G-URS

A.1.1 Sequence Generation

In the frame structure, the CRS sequence can be $d_{\mathrm{CRS}}(k)$ is defined as

$$d_{\mathrm{CRS}}(m) = \frac{1}{\sqrt{2}}\left(1 - 2 \cdot c(2m)\right) + j\frac{1}{\sqrt{2}}\left(1 - 2 \cdot c(2m+1)\right),$$
$$m = 0, 1, \cdots, 2N_{\mathrm{RB}}^{\max,\mathrm{DL}} - 1, \tag{A.1}$$

where n_s is the slot number within the frame, $N_{\mathrm{RB}}^{\mathrm{max,DL}}$ is the largest downlink bandwidth configuration. The pseudo-random sequence $c(i)$ is defined as

$$c(n) = (x_1(n + N_c) + x_2(n + N_c)) \mod 2 \tag{A.2}$$

$$x_1(n + 31) = (x_1(n + 3) + x_1(n)) \mod 2 \tag{A.3}$$

$$x_2(n + 31) = (x_2(n + 3) + x_2(n + 2) + x_2(n + 1) + x_2(n)) \mod 2 \tag{A.4}$$

where $N_c = 1600$ and the first maximal length sequence (m-sequence) shall be initialized with $x_1(0) = 1$, $x_1(n) = 0$, $n = 1, 2, \cdots, 30$. The initialization of the second m-sequence is denoted by

$$c_{\mathrm{init}} = 2^{10} \cdot \Big(7 \cdot (n_s^{'} + 1) + l + 1\Big) \cdot (2 \cdot i + 1) + 2 \cdot i + N_{\mathrm{CP}}, \tag{A.5}$$

where it is initialized at the start of each OFDM symbol such as

$$n_s^{'} = \begin{cases} 10\lfloor n_s/10 \rfloor + n_s \mod 2, & \text{if frame structure type 3} \\ n_s, & \text{otherwise.} \end{cases}$$

$$N_{\mathrm{CP}} = \begin{cases} 1, & \text{for normal CP} \\ 0, & \text{for extended CP.} \end{cases}$$

A.1.2 Sequence Mapping

The CRS sequence $d_{\mathrm{CRS}}(m)$ shall be mapped to complex-valued modulation symbols $Y_{k,l}^{(p)}$ used as reference symbols for antenna port p in slot n_s according to

$$Y_{k,l}^{(p)} = d_{\mathrm{CRS}}(m^{'}), \tag{A.6}$$

where

$$k = 6m + (v + v_{\text{shift}}) \bmod 6$$

$$l = \begin{cases} 0, N_{\text{symb}}^{\text{DL}} - 3 & \text{if } p \in \{0, 1\} \\ 1, & \text{if } p \in \{2, 3\}. \end{cases}$$

$$m = 0, 1, \cdots, 2.N_{\text{RB}}^{\text{DL}} - 1$$

$$m^{'} = m + N_{\text{RB}}^{\text{max,DL}} - N_{\text{RB}}^{\text{DL}},$$

where $N_{\text{RB}}^{\text{DL}}$ is the downlink bandwidth configuration of the received 4G signals, and the variables v and v_{shift} define the position in the frequency domain for different RSs for v given as

$$v = \begin{cases} 0, & \text{if } p = 0 \ \& \ l = 0 \\ 3, & \text{if } p = 0 \ \& \ l \neg 0 \\ 3, & \text{if } p = 1 \ \& \ l = 0 \\ 0 & \text{if } p = 1 \ \& \ l \neg 0 \\ 3(n_s \bmod 2), & \text{if } p = 2 \\ 3 + 3(n_s \bmod 2), & \text{if } p = 3, \end{cases}$$

and $v_{\text{shift}} = N_{\text{ID}}^{\text{Cell}} \bmod 6$ for CRS.

A.2 5G-USS

A.2.1 Sequence Generation

A.2.1.1 PSS

The PSS sequence $d_{\text{PSS}}(n)$ is a 127-length m-sequence defined as

$$d_{\text{PSS}}(n) = 1 - 2x(m), \tag{A.7}$$

$$m = (n + 43N_{\text{ID}}^{(2)}) \bmod 127, \tag{A.8}$$

$$0 \leq n < 127, \tag{A.9}$$

where

$$x(i+7) = (x(i+4) + x(i)) \bmod 2, \tag{A.10}$$

and

$$\begin{bmatrix} x(6) & x(5) & x(4) & x(3) & x(2) & x(1) & x(0) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}. \tag{A.11}$$

A.2.1.2 SSS

The SSS sequence $d_{\mathrm{SSS}}(n)$ is another 127-length m-sequence defined as

$$d_{\mathrm{SSS}}(n) = \left[1 - 2x_0((n + m_0) \bmod 127)\right]\left[1 - 2x_1((n + m_1) \bmod 127)\right], \tag{A.12}$$

$$m_0 = 15\lfloor \frac{N_{\mathrm{ID}}^{(1)}}{112} \rfloor + 5N_{\mathrm{ID}}^{(2)}, \tag{A.13}$$

$$m_1 = N_{\mathrm{ID}}^{(1)} \bmod 112, \tag{A.14}$$

$$0 \leq n < 127, \tag{A.15}$$

where

$$x_0(i + 7) = (x_0(i + 4) + x_0(i)) \bmod 2, \tag{A.16}$$

$$x_1(i + 7) = (x_1(i + 4) + x_1(i)) \bmod 2, \tag{A.17}$$

and

$$\begin{bmatrix} x_0(6) & x_0(5) & x_0(4) & x_0(3) & x_0(2) & x_0(1) & x_0(0) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \tag{A.18}$$

$$\begin{bmatrix} x_1(6) & x_1(5) & x_1(4) & x_1(3) & x_1(2) & x_1(1) & x_1(0) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{A.19}$$

A.2.1.3 PBCH-DMRS

The PBCH-DMRS is a special type of physical layer signal that functions as a reference signal for decoding PBCH. In 4G, this kind of special DMRS for PBCH is not needed because the CRS can be used for PBCH decoding. However, in 5G/NR there is no CRS. That's why the DMRS is dedicated for PBCH decoding. The PBCH-DMRS sequence $d_{\mathrm{DMRS}}(m)$ is a pseudo-random sequence that is dependent on the initialization value that is made up of

various components like physical cell ID, SSB index, and half frame number. That is, by decoding this DMRS, UE can figure out SSB Index and Half Frame. The UE shall assume the reference sequence $d_{\mathrm{DMRS}}(m)$ for an SS/PBCH block is defined by

$$d_{\mathrm{DMRS}}(m) = \frac{1}{\sqrt{2}}\left(1 - 2 \cdot c(2m)\right) + j\frac{1}{\sqrt{2}}\left(1 - 2 \cdot c(2m+1)\right), \tag{A.20}$$

where $c(n)$ is given by is given by clause 5.2 in [82]. The scrambling sequence generator shall be initialized at the start of each SS/PBCH block occasion with

$$c_{\mathrm{init}} = 2^{11}\left(\bar{i}_{\mathrm{SSB}} + 1\right)\left(\lfloor N_{\mathrm{ID}}^{\mathrm{Cell}}/4 \rfloor + 1\right) + 2^{6}\left(\bar{i}_{\mathrm{SSB}} + 1\right) + \left(N_{\mathrm{ID}}^{\mathrm{Cell}} \bmod 4\right), \tag{A.21}$$

where

- For $\bar{L}_{\max} = 4$, $\bar{i}_{\mathrm{SSB}} = i_{\mathrm{SSB}} + 4n_{\mathrm{hf}}$, where n_{hf} is the number of half-frame in which the PBCH is transmitted in a frame with $n_{\mathrm{hf}} = 0$ for the first half-frame in the frame and $n_{\mathrm{hf}} = 1$ for the second half-frame in the frame, and i_{SSB} is the two least significant bits of the candidate SS/PBCH block index.
- For $\bar{L}_{\max} > 4$, $\bar{i}_{\mathrm{SSB}} = i_{\mathrm{SSB}}$ where i_{SSB} i is the three least significant bits of the candidate SS/PBCH block index.

A.2.2 Sequence Mapping

The PSS, SSS, and PBCH DMRS are allocated specific resource elements (REs) within the 5G frame structure. The exact locations depend on the frequency range (FR1 or FR2), subcarrier spacing, and bandwidth. The mapping of these RSs is depicted in Figure 2.4.