UNIVERSITY OF CALIFORNIA,
IRVINE

Exploiting Cellular Signals for Navigation: 4G to 5G

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Electrical Engineering and Computer Science

by

Kimia Shamaei

Dissertation Committee:
Professor Zaher (Zak) M. Kassas, Chair
Professor Ender Ayanoglu
Professor Lee Swindlehurst

2020

DEDICATION

To my Parents and Mahdi

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

ACKNOWLEDGMENTS

I would like to thank my advisor Prof. Zak Kassas for giving me the opportunity to work at ASPIN lab, providing advice throughout my research, helping with my job and Green Card applications, and supporting me financially during my doctoral research. He introduced me to a new field of research, gave me the opportunity to follow all my ideas, and provided all the required equipments to evaluate them. He gave me the chance to attend numerous conferences and present my work to the community of Navigation.

I would like to thank my Ph.D. committee members Prof. Ender Ayanoglu and Prof. Lee Swindlehurst for taking time to serve in 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) and the National Institute of Standards and Technology (NIST) for supporting my research.

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 Prof. Todd Humphreys, Prof. Solamz Kia, and Prof. Demoz Gebre Egziabher for their help with my Green Card application so I can continue my research and work in the U.S.

I would like to thank my friends and colleagues: Joshua, Joe, and Ali for being always next to me throughout all ups and downs of my doctoral journey. I would also like to thank them for all the helpful discussions and their help with my experiments.

I would like to thank Marjan, Iman, Salma, Amirhosein, Laleh, and Arash for not only being my friends but also my family. Being with them helped me to overcome the hardship of living in a foreign country and being away from my family.

I would like to thank my family: Mom, Dad, Laleh, Alireza, Kamran, Coleene, Ladan, and Paul for all their supports. Even though I was not able to see most of them for more than four years throughout my doctoral studies due to the travel ban, they continuously encouraged me to pursue my dreams.

Finally, I would like to thank my husband Mahdi, who is my best friend, my greatest support, my biggest comfort, my strongest motivation, and my deepest love. He always believed in me and wanted the best for me. He sacrificed all his dreams so that I can reach mine. None of this would have been possible without his continuous support.

VITA

Kimia Shamaei

EDUCATION

Doctor of Philosophy in Electrical Engineering **2020**
University of California, Irvine *Irvine, California*

Master of Science in Electrical Engineering **2013**
University of Tehran *Tehran, Iran*

Bachelor of Science in Electrical Engineering **2010**
University of Tehran *Tehran, Iran*

RESEARCH EXPERIENCE

Graduate Research Assistant **2019–2020**
University of California, Irvine *Irvine, California*

Graduate Research Assistant **2015–2019**
University of California, Riverside *Riverside, California*

Graduate Research Assistant **2011–2013**
University of Tehran *Tehran, Iran*

TEACHING EXPERIENCE

Teaching Assistant **2019–2020**
University of California, Irvine *Irvine, California*

Teaching Assistant **2016–2019**
University of California, Riverside *Riverside, California*

Teaching Assistant **2012**
University of Tehran *Tehran, Iran*

HONORS & AWARDS

Session chair **2019**
ION GNSS+ Conference *Miami, Florida*

Samuel M. Burka Award **2012**
NAVIGATION, Journal of the Institute of Navigation

Best Presentation Award **2017**
ION GNSS+ Conference *Portland, Oregon*

Best Presentation Award **2016**
ION GNSS+ Conference *Portland, Oregon*

Best Student Paper Award **2016**
IEEE/ION Position, Location, and Navigation Symposium *Savannah, Georgia*

JOURNAL PUBLICATIONS

[J8] **Shamaei**, **K**., & Kassas, Z. (2020). Evaluating 5G signals for opportunistic navigation. *IEEE Transactions on Wireless Communications.* (in preparation)

[J7] **Shamaei**, **K**., & Kassas, Z. (2020). A joint TOA and DOA acquisition and tracking approach for positioning with LTE signals. *IEEE Transactions on Signal Processing.* (submitted)

[J6] **Shamaei**, **K**., & Kassas, Z. (2018, December). LTE receiver design and multipath analysis for navigation in urban environments. *NAVIGATION, Journal of the Institute of Navigation*, 65(4), 655–675. (ION Burka Award)

[J5] **Shamaei**, **K**., Khalife, J., & Kassas, Z. (2018, April). Exploiting LTE signals for navigation: Theory to implementation. *IEEE Transactions on Wireless Communications*, 17(4), 2173–2189.

[J4] Khalife, J., **Shamaei**, **K**., & Kassas, Z. (2018, April). Navigation with cellular CDMA signals – part I: Signal modeling and software-defined receiver design. *IEEE Transactions on Signal Processing*, 66(8), 2191–2203.

[J3] **Shamaei**, **K**., & Sabbaghian, M. (2015, November). Analytical performance evaluation of SC-FDMA systems in the presence of frequency and time offset. *IEEE Transactions on Wireless Communications*, 14(11), 6230–6239.

[J2] Maaref, M., Rezazadeh, A., **Shamaei**, **K**., & Tavakoli, M. (2016, August). A Gaussian mixture framework for cooperative rehabilitation therapy in assistive impedance-based tasks. *IEEE Transactions on Wireless Communications*, 10(5), 904–913.

[J1] Maaref, M., Rezazadeh, A., **Shamaei**, **K**., Ocampo, R., & Tavakoli, M. (2016, July). A bicycle cranking model for assist-as-needed robotic rehabilitation therapy using learning from demonstration. *IEEE Robotics and Automation Letters*, 1(2), 653–660.

MAGAZINE PUBLICATIONS

[M3] Kassas, Z., Maaref, M., Morales, J., Khalife, J., & **Shamaei**, **K**. (2018, September). Robust vehicular navigation and map-matching in urban environments with IMU, GNSS, and cellular signals. *IEEE Intelligent Transportation Systems Magazine*. (accepted)

[M2] Kassas, Z., Khalife, J., **Shamaei**, **K**., & Morales, J. (2017, September). I hear, therefore I know where I am: Compensating for GNSS limitations with cellular signals. *IEEE Signal Processing Magazine*, 111–124.

[M1] Kassas, Z., Morales, J., **Shamaei**, **K**., & Khalife, J. (2017, April). LTE steers UAV. *GPS World Magazine*, 28(4), 18–25.

CONFERENCE PUBLICATIONS

[C13] **Shamaei**, **K**., & Kassas, Z. (2019, September). Sub-meter accurate UAV navigation and cycle slip detection with LTE carrier phase. *In Proceedings of ION GNSS Conference* (pp. 2469–2479).

[C12] **Shamaei**, **K**., Morales, J., & Kassas, Z. (2019, April). A framework for navigation with LTE time-correlated pseudorange errors in multipath environments. *In Proceedings of IEEE Vehicular Technology Conference* (pp. 1–6).

[C11] **Shamaei**, **K**., Morales, J., & Kassas, Z. (2018, September). Positioning performance of LTE signals in Rician fading environments exploiting antenna motion. *In Proceedings of ION GNSS Conference* (pp. 3423–3432).

[C10] Abdallah, A., **Shamaei**, **K**., & Kassas, Z. (2018, September). Indoor positioning based on LTE carrier phase measurements and an inertial measurement unit. *In Proceedings of ION GNSS Conference* (pp. 3374–3384).

[C9] **Shamaei**, **K**., Khalife, J., & Kassas, Z. (2018, April). A joint TOA and DOA approach for positioning with LTE signals. *In Proceedings of IEEE/ION Position, Location, and Navigation Symposium* (pp. 81–91).

[C8] **Shamaei**, **K**., Khalife, J., & Kassas, Z. (2018, April). Pseudorange and multipath analysis of positioning with LTE secondary synchronization signals. *In Proceedings of Wireless Communications and Networking Conference* (pp. 286–291).

[C7] **Shamaei**, **K**., Khalife, J., Bhattacharya, S., & Kassas, Z. (2017, September). Computationally efficient receiver design for mitigating multipath for positioning with LTE signals. *In Proceedings of ION GNSS Conference* (pp. 3751–3760).

[C6] Khalife, J., Ragothaman, S., **Shamaei**, **K**., Morales, J., & Kassas, Z. (2017, April). Fusing lidar and cellular signals for robust ground and aerial autonomous navigation. *In Proceedings of Southern California Robotics Symposium.*

[C5] **Shamaei**, **K**., Khalife, J., & Kassas, Z. (2017, August). Ranging precision analysis of LTE signals. *In Proceedings of European signal processing Conference* (pp. 2788–2792).

[C4] **Shamaei**, **K**., Khalife, J., & Kassas, Z. (2017, January). Comparative results for positioning with secondary synchronization signal versus cell specific reference signal in LTE systems. *In Proceedings of ION International Technical Meeting Conference* (pp. 1256–1268).

[C3] **Shamaei**, **K**., Khalife, J., & Kassas, Z. (2016, September). Performance characterization of positioning in LTE systems. *In Proceedings of ION GNSS Conference* (pp. 2262–2270).

[C2] Khalife, J., **Shamaei**, **K**., & Kassas, Z. (2016, April). A software-defined receiver architecture for cellular CDMA-based navigation. *In Proceedings of IEEE/ION Position, Location, and Navigation Symposium* (pp. 816–826).

[C1] **Shamaei**, **K**., & Sabbaghian, M. (2012, November). Frequency offset estimation in SC-FDMA systems. *In Proceedings of IEEE International Symposium on Telecommunication* (pp. 216–220).

PATENTS

[P5] Kassas, Z., & **Shamaei**, **K**., "Sub-meter accurate navigation and cycle slip detection with LTE carrier phase measurements," U.S. Patent Application No. 62/930,298, Filed: November 4, 2019.

[P4] Kassas, Z., Abdallah, A., & **Shamaei**, **K**., "Indoor localization system with LTE code and carrier phase measurements and an IMU," U.S. Patent Application No. 62/913,078, Filed: October 9, 2019.

[P3] Kassas, Z., **Shamaei**, **K**., & Khalife, J., "A real-time, multipath-mitigating receiver design for navigation with LTE signals," U.S. Patent Application No. 62/561,023, Filed: September 20, 2017.

[P2] Kassas, Z., **Shamaei**, **K**., & Khalife, J., "SDR for navigation with LTE signals," U.S. Patent Application No. 62/398,403, Filed: September 22, 2016.

[P1] Kassas, Z., Khalife, J., & **Shamaei**, **K**., "SDR for navigation with cellular CDMA signals," U.S. Patent Application No. 62/294,758, Filed: February 12, 2016.

SOFTWARE

MATLAB, C++, LabVIEW

ABSTRACT OF THE DISSERTATION

Exploiting Cellular Signals for Navigation: 4G to 5G

By

Kimia Shamaei

Doctor of Philosophy in Electrical Engineering and Computer Science

University of California, Irvine, 2020

Professor Zaher (Zak) M. Kassas, Chair

Global navigation satellite systems (GNSS) have been the main technology used in aerial and ground vehicle navigation systems. As vehicles approach full autonomy, the requirements on the accuracy, reliability, and availability of their navigation systems become very stringent. Due to the limitations of GNSS, namely severe attenuation in deep urban canyons and susceptibility to interference, jamming, and spoofing, alternative sensors and signals are sought. The most common approach to address the limitations of GNSS-based navigation in urban environments is to fuse GNSS receivers with inertial navigation systems (INSs), lidars, cameras, and map matching algorithms. An alternative approach has emerged over the past decade, which is to exploit ambient signals of opportunity (SOPs), such as cellular, digital television, AM/FM, WiFi, and low Earth orbit (LEO) satellite signals.

Among SOPs, cellular signals have attracted significant attention due to their inherently desirable attributes, including: abundance, geometric diversity, high received power, and large transmission bandwidth. Cellular systems have gone through five generations. Long-term-evolution (LTE) and new radio (NR) are the standards of the last two generations of wireless technology, namely 4th generation (4G) and 5th generation (5G), respectively. LTE has been developed and standardized in most countries over the past few years and currently has more than four billion users. The structure of NR signals has been finalized in 2019 and since then cellular providers have started rolling 5G out in major cities around the world.

Cellular signals are not designed for navigation. In order to exploit cellular signals for navigation purposes, several challenges must be addressed: (1) specialized receivers are required to extract navigation observables from cellular signals, (2) cellular towers typically transmit from low elevation angles, causing multipath signals to be received alongside line-of-sight signals. Multipath can introduce error on the estimated navigation observables, which must be alleviated, (3) the achievable ranging accuracy in multipath-free and multipath-rich environments must be characterized, (4) navigation framework must be developed to localize the receiver using the derived navigation observables, and (5) cellular signals base stations' clock biases must be estimated, since they are not available to the receiver.

This dissertation aims to address all of the above challenges for cellular LTE and NR signals. In particular, for LTE, first, a software-defined receiver (SDR) is proposed that is capable of (1) extracting the essential parameters for navigation from received LTE signals, (2) acquiring and tracking LTE signals transmitted from multiple eNodeBs, and (3) producing navigation observables from LTE signals including code and carrier phase and Doppler frequency measurements. Second, the accuracy of the produced measurements are derived as a function of carrier-to-noise ratio and signal transmission bandwidth. It is shown that LTE cell-specific reference signal (CRS) can provide higher precision compared to the LTE secondary synchronization signal (SSS) due to its high transmission bandwidth. Third, standalone and non-standalone navigation frameworks are proposed to localize the receiver using the generated navigation observables. Fourth, it is proposed to exploit the received LTE signal's time-of-arrival (TOA) and direction-of-arrival (DOA) to produce a navigation solution in cold-start applications, where there is no estimate of the receiver's initial state. For this purpose, an SDR is designed to jointly acquire and track TOA and DOA of LTE signals.

For NR, first, an SDR is proposed that is capable of (1) acquiring synchronization signal

(SS), physical broadcast channel (PBCH) signal, and its associated demodulation reference signal (DM-RS), which are transmitted on a block called SS/PBCH block and (2) tracking SS/PBCH block to produce code and carrier phase and Doppler frequency measurements from NR signals. Second, the precision of the derived code and carrier phase measurements are analyzed as a function of carrier-to-noise ratio and NR numerology. Finally, the statistics of the NR position estimation error are derived for different propagation channels.

Throughout the dissertation, numerical and experimental results are provided to validate the theoretical contributions.

Chapter 1

Introduction

The inherently weak global navigation satellite system (GNSS) signals undergo severe attenuation in deep urban environments, making them unreliable for navigation [2]. Under these weak signal conditions, receivers cannot produce a navigation solution, since they cannot continuously track GNSS signals. Despite the inability to produce a navigation solution, some approaches utilized the received signal power, the periodicity of GPS satellites, and a power matching algorithm to estimate the receiver's state [3, 4]. Other approaches utilized three-dimensional (3-D) building maps to predict satellite visibility via shadow matching to aid conventional range-based GNSS positioning [5, 6]. The most common approach to address the limitations of GNSS-based navigation in urban environments is to fuse GNSS receivers with inertial navigation systems (INSs), lidars, cameras, and map matching algorithms [7–9]. Although fusing these systems with GNSS signals have improved the GNSS standalone navigation solution, they have failed to provide a reliable navigation solution in the absence of GNSS signals due to the dead reckoning characteristic of these sensors. Besides, the performance of some of these sensors such as camera and Lidar depends on the weather condition and availability of environmental features. Over the past decade, a new paradigm has emerged to address GNSS limitations, which is to exploit ambient signals of opportunity (SOPs). This approach is discussed in the next section.

1.1 Signals of Opportunity

SOPs are ambient radio frequency (RF) signals, which are not designed for navigation; however, they are freely available in the GNSS-challenged environments and can be exploited for navigation purposes. Cellular, digital television, AM/FM, Wi-Fi, and low-earth orbit (LEO) satellite signals are examples of SOPs [10–14].

The literature on SOPs answers theoretical questions on the observability and estimability of the SOPs landscape for various *a priori* knowledge scenarios [15] and prescribes receiver motion strategies for accurate receiver and SOP localization and timing estimation [16–18]. Moreover, a number of recent experimental results have demonstrated receiver localization and timing via different SOPs [19–23]. Among SOPs, cellular signals are particularly attractive for positioning due to their desirable attributes, which will be discussed next.

1.2 Cellular Signals

Cellular signals posses several desirable characteristics for opportunistic navigation, including [24]:

- **Abundance:** There are several towers from different cellular providers in each area that can be exploited for navigation. Note that these signals are used opportunistically and there is no need to be the subscriber of any of the networks.
- **Geometric diversity:** By construction of hexagonal cells in cellular networks, cellular towers possess a favorable geometry for positioning.

- **High received power:** Experimental results have shown that received cellular signals have more than 20 dB higher carrier-to-noise ratio compared to the GNSS signals even in deep indoor and urban environments.

- **Large bandwidth:** Cellular signals have significantly larger transmission bandwidth compared to the GNSS signals, which provides accurate time-of-arrival (TOA) estimation especially in GNSS-challenged environments.

- **Free to use:** In an opportunistic navigation, cellular downlink signals are exploited for navigation without the need to communicate back. Therefore, the receiver does not need to be a paying subscriber of the network.

- **Jamming and spoofing resistance:** Cellular signals are transmitted at different frequency bands and from different cellular providers. Therefore, jamming or spoofing all cellular signals at once requires sophisticated hardware and high power, which is impractical.

Over the past years, the potentials of cellular code division multiple access (CDMA), which is the transmission standard of the third generation (3G) of cellular signals, have been evaluated thoroughly and navigation frameworks and receiver architectures have been developed for these signals [25, 26]. Moreover, experimental results have demonstrated sub-meter-level accuracy for an unmanned aerial vehicle (UAV) navigating with cellular CDMA signals [22].

In recent years, the new generations of cellular signals namely long-term evolution (LTE) and new radio (NR) signals, which are the fourth and fifth generations (4G and 5G, respectively) of cellular transmission standards, respectively, have been developed and implemented. Exploiting cellular LTE and NR signals have received considerable attention due to their specific desirable characteristics, including: (1) higher transmission bandwidth compared to previous generations of wireless standards and (2) the ubiquity of their networks. Cellular LTE and NR signals use orthogonal frequency division multiple access (OFDMA) modulation for their transmission, which is significantly different than CDMA signals. Therefore, extending the receiver structure and navigation results of CDMA signals to LTE and NR signals is impractical. In order to exploit cellular LTE and NR signals for navigation, new receiver structure must be developed. Besides, the achievable ranging and localization accuracy of these signals must be derived accordingly. This dissertation tackles these challenges and makes several contributions that are discusses in the next section.

1.3 Dissertation Contributions

Over the past few years, literature have derived the Cramér-Rao lower bound (CRLB) of the achievable localization accuracy of cellular LTE signals [27, 28] and several software-defined receivers (SDRs) have been proposed for navigation using LTE signals [29–31]. However, there are several challenges associated with navigating with these SDRs, which rely on acquiring the primary synchronization signal (PSS) transmitted by the LTE base station (also known as evolved Node B or eNodeB). The first challenge results from the near-far effect created by the strongest PSS, which makes it impossible for the receiver to individually acquire the remaining ambient PSSs. A simple solution would be to track only the strongest PSSs (up to three). This raises a second challenge: the number of intra-frequency eNodeBs that the receiver can simultaneously use for positioning is limited [32]. To circumvent this problem, other cell-specific signals can be tracked, in which case the receiver must obtain high-level information of the surrounding eNodeBs, such as their cell IDs, signal bandwidths, and the number of transmitting antennas. The literature on LTE-based navigation assumes this information to be known *a priori*, which raises the third challenge associated with the published SDRs. In practice, it is desirable to have a receiver that is capable of obtaining this information on-the-fly in unknown environments, which is the first contribution of this dissertation.

After acquiring the received LTE signals of all the eNodeBs in the environment, the user equipment (UE) must estimate signal's TOA. Literature have proposed different methods to estimate TOA of LTE signals, including a joint channel and delay estimation method in [33], super resolution algorithm (SRA) in [31, 34], and a threshold-based approach in [30, 35]. These methods either have high computational complexity or low accuracy. The second contribution of this dissertation is developing three tracking methods to track TOA of the LTE signals, with low computational complexity and high accuracy. The achievable ranging accuracy of the proposed methods are derived analytically and compared with each other and the state-of-the-art experimentally.

In general, one of the main challenges of navigation with cellular signals is the unknown clock biases of the cellular base stations. To remove the effect of the eNodeBs' clock biases, some literature have considered synchronized eNodeBs, which can be obtained using lab emulated LTE signals [29]. This approach is not applicable to real-world scenarios since the eNodeBs' are not synchronized. The other approach could be estimating and removing the effect of the clock bias in a post-processing fashion using the known range measurements obtained by GNSS signals [30]. This approach is not practical for real-time applications. The third contribution of this dissertation is developing three navigation frameworks to estimate the location of the receiver on-the-fly. Experimental results are provided to evaluate the performance of the proposed navigation frameworks.

Although the aforementioned proposed navigation frameworks are able to provide a real-time estimate of the UE's position, they require *a priori* knowledge of the UE's state, e.g., using GNSS estimate before its cutoff. However, this is not available in cold-start applications. To overcome this challenge, it is proposed to exploit not only TOA measurements but also direction of arrival (DOA) measurements. The fourth contribution of this dissertation is developing an SDR to jointly acquire and track TOA and DOA of the LTE signals. The CRLBs of the achievable TOA and DOA precisions are derived and compared with the achievable precision of the proposed SDR. Then, the computational complexity of the proposed SDR is compared with the state-of-the-art. Finally, experimental results are provided to compare the performance of the proposed SDR with the state-of-the-art.

Over the past few years, the third generation partnership project (3GPP) has been developing the fifth generation of wireless access technology, which is known as NR. The structure of NR signals has been finalized in 2019 and since then cellular providers have started rolling 5G out in major cities around the world. Since NR signals are new to the field, literature lack a thorough study on the potentials of NR signals for opportunistic navigation. There are several challenges in an opportunistic navigation with NR signals: (1) low-level NR frame structure and signaling procedure are scattered in several technical reports, which makes it confusing and tiresome to follow for one without proper background, (2) potential reference signals for opportunistic navigation with NR signals have not been investigated, (3) specialized receiver to opportunistically extract navigation observables from NR signals has not been developed, and (4) achievable ranging and positioning accuracy with these signals have not been analyzed. This dissertation tackles these challenges by (1) providing the low-level NR signal structure and describing important parameters for opportunistic navigation, (2) presenting potential NR signals that can be exploited for navigation and their related coding and decoding procedure, (3) developing an SDR to extract navigation observables from NR signals, and (4) deriving ranging and positioning accuracy with NR signals. Moreover, this dissertation, for the first time, demonstrates pseudorange measurements extracted from real NR signals.

In the following, the refereed publications resulting from this dissertation are presented.

Journal Publications

[J1] 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.

[J2] 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.

[J3] 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.

[J4] K. Shamaei and Z. Kassas, “Evaluating 5G signals for opportunistic navigation,” *IEEE Transactions on Wireless Communications*, 2020, in preparation.

Conference Publications

[C1] K. Shamaei, J. Khalife, and Z. Kassas, “Performance characterization of positioning in LTE systems,” *in Proceedings of ION GNSS Conference*, September 2016, pp. 2262- 2270.

[C2] K. Shamaei, J. Khalife, and Z. Kassas, “Comparative results for positioning with secondary synchronization signal versus cell specific reference signal in LTE systems,” *in Proceedings of ION International Technical Meeting Conference*, January 2017, pp. 1256–1268.

[C3] K. Shamaei, J. Khalife, and Z. Kassas, “Ranging precision analysis of LTE signals,” *in Proceedings of European Signal Processing Conference*, August 2017, pp. 2788–2792.

[C4] K. Shamaei, J. Khalife, S. Bhattacharya, and Z. Kassas, “Computationally efficient receiver design for mitigating multipath for positioning with LTE signals,” *in Proceedings of ION GNSS Conference*, September 2017, pp. 3751–3760.

[C5] K. Shamaei, J. Khalife, and Z. Kassas, “A joint TOA and DOA approach for positioning with LTE signals,” *in Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2018, pp. 81–91.

[C6] 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.

[C7] K. Shamaei, J. Morales, and Z. Kassas, "Positioning performance of LTE signals in Rician fading environments exploiting antenna motion," *in Proceedings of ION GNSS Conference*, September 2018, pp. 3423–3432.

[C8] 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.

[C9] 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.

1.4 Dissertation Outline

This dissertation is organized as follow:

- **Chapter 2:** This chapter presents a summary of the LTE signal structure. Next, the LTE broadcast reference signals that can be exploited for navigation are presented and the advantages and challenges of each are discussed. Finally, the received signal model in the presence of symbol timing and frequency offset is presented.

- **Chapter 3:** This chapter presents the structure of the proposed SDR, which consists of four main stages: (1) coarse acquisition, (2) system information extraction and neighboring cell identification, (3) acquisition refinement, and (4) tracking. Three different tracking methods are discussed and the advantages and challenges of each are discussed.

- **Chapter 4:** This chapter analyzes the achievable ranging precision of the proposed SDR for the SSS and CRS signals.

- **Chapter 5:** This chapter presents three different navigation frameworks. The first one is an standalone framework, which uses only code phase measurements to estimate the position and velocity of the receiver and the difference between the clock bias and drift of the receiver and each of the eNodeBs'. The second one is an standalone navigation framework, which uses the single difference code and carrier phase and Doppler frequency measurements to estimate the position and velocity of the receiver. Finally, the third one is an IMU-aided SOP framework, where IMU measurements are used to propagate the states of the estimator and cellular code phase measurements are used to estimate the position and velocity of the receiver and the difference between the clock bias and drift of the receiver and each of the eNodeBs'. Simulation and experimental results are provided to evaluate each of the proposed navigation frameworks.

- **Chapter 6:** This chapter proposes a receiver to jointly estimate and track TOA and DOA of the received LTE signals. CRLBs of the TOA and DOA estimates are derived and computational complexity of the proposed approach is compared with the state-of-the-art methods. Finally, simulation and experimental results are provided to validate the theoretical results.

- **Chapter 7:** This chapter evaluates cellular NR signals for opportunistic navigation. First, the advantages and challenges of opportunistic navigation with NR signals are presented. Then, NR signals' structure and the reference signals that can be exploited for navigation are discussed. Next, an SDR is proposed to extract code and carrier phase and Doppler frequency measurements from cellular NR signals. Then, the achievable ranging and positioning accuracy and precision with cellular NR signals are analyzed. Finally, experimental results are provided to evaluate the proposed SDR.

- **Chapter 8:** This chapter summarizes the contributions of this dissertation and highlights the major discoveries.

Chapter 2

LTE Signal Model

In order to exploit cellular LTE signals for navigation, the low-level model of these signals must be known at the UE. Since the purpose of this dissertation is an opportunistic navigation, the UE cannot communicate with the eNodeB and must exploit the available broadcast reference signals to extract navigation observables. Note that these reference signals must be known at the UE, without being the subscriber of the network. Knowing the structure of the transmitted LTE reference signals, the received signal can be modeled and a proper receiver structure to navigate with these signals can be designed.

This chapter describes the transmitted and received LTE signal model. Section 2.1 presents the low-level model of LTE signals and their frame structure. Section 2.2 discusses the reference signals that can be exploited for positioning in an opportunistic navigation with LTE signals. Finally, Section 2.3 provides the received signal model.

2.1 Frame Structure

In LTE systems, OFDM modulation is used for data transmission. In OFDM, the transmitted symbols are mapped to different carrier frequencies called subcarriers, where a $\Delta f = 15$ kHz spacing is assigned between different subcarriers. Assuming that N_r subcarriers are allocated to data transmission, the transmitted serial data symbols must be first divided into groups of length N_r and mapped to each of these subcarriers. The mapping process depends on the LTE frame structure, where different data types are transmitted at different time and subcarriers. To reduce the interference on the neighboring frequency bands and on the transmitted data, a guard band is allocated to the OFDM signals, where no data is transmitted on the subcarriers at both sides of the N_r data subcarriers. This process is done by zero-padding the N_r data symbols to length N_c. Note that in LTE systems, no information is transmitted on direct current (DC) subcarrier. Next, an inverse fast Fourier transform (IFFT) is taken, resulting in an OFDM symbol in the time-domain, which has a duration of $T_{\text{symb}} = 1/\Delta f$. The last L_{CP} elements of the OFDM symbol are repeated at the beginning to provide the cyclic prefix (CP) and are used to suppress the inter-symbol interference (ISI) due to multipath. Fig. 2.1 summarizes the OFDM modulation scheme for a digital transmission.

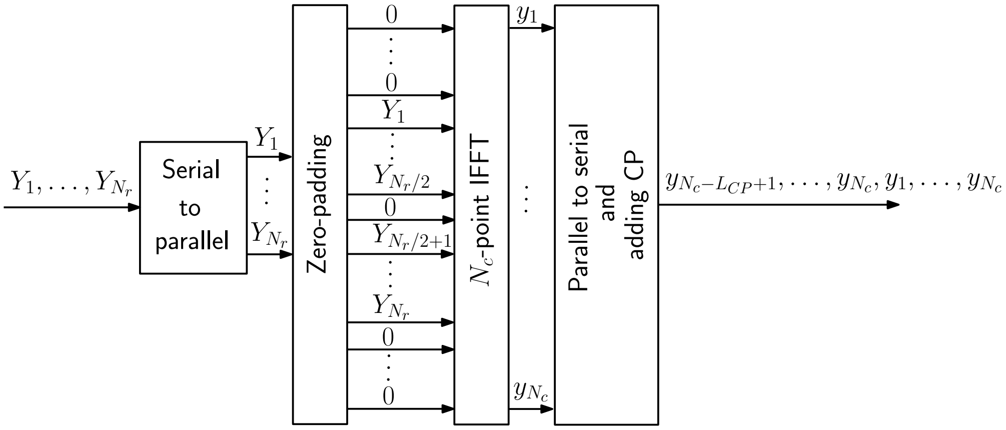


Figure 2.1: Block diagram of the OFDM modulation for a digital transmission

The transmitted symbols can be obtained at the receiver by executing the above steps in reverse order. Since the frequency reuse factor in LTE systems is one, all the eNodeBs of the same operator use the same frequency band. To reduce the interference caused by sharing the same frequency band, each signal is coded to be orthogonal to the transmitted signals from other eNodeBs. Using different frequency bands makes it possible to allocate the same cell IDs to the eNodeBs from different operators.

The number of subcarriers in an LTE frame, N_c, and the number of used subcarriers, N_r, are assigned by the network provider and can only take the values that are shown in Table 2.1. Hence, the occupied bandwidth can be calculated using $W = N_r \times \Delta f$, which is less than the assigned bandwidth shown in Table 2.1 to provide a guard band for LTE transmission [36].

Table 2.1: LTE System Bandwidths and Number of Subcarriers

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

The resulting OFDM symbols are grouped into frames with a duration of $T_f = 10$ ms. In an LTE system, the structure of the frame depends on the transmission type, which can be either frequency division duplexing (FDD) or time division duplexing (TDD). Due to the superior performance of FDD in terms of latency and transmission range, most network providers use FDD for LTE transmission. Hence, this dissertation only focuses on FDD transmission and for simplicity an FDD frame is simply called a frame.

A frame is composed of 10 ms data, which is divided into either 20 slots or 10 subframes with a duration of 0.5 ms or 1 ms, respectively. A slot can be decomposed into multiple resource grids (RGs) and each RG has numerous resource blocks (RBs). Then, an RB is broken down into the smallest elements of the frame, namely resource elements (REs). The frequency and time indices of an RE are called subcarrier and symbol, respectively. The structure of the LTE frame is illustrated in Fig. 2.2 [36]. Fig. 2.3 shows an example of the LTE frame structure with $N_r = 72$.

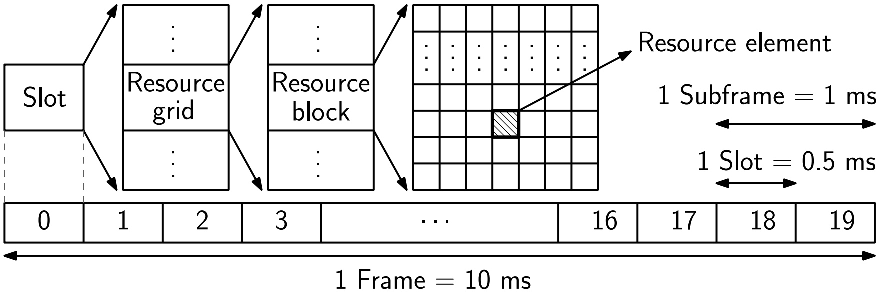


Figure 2.2: LTE FDD frame structure

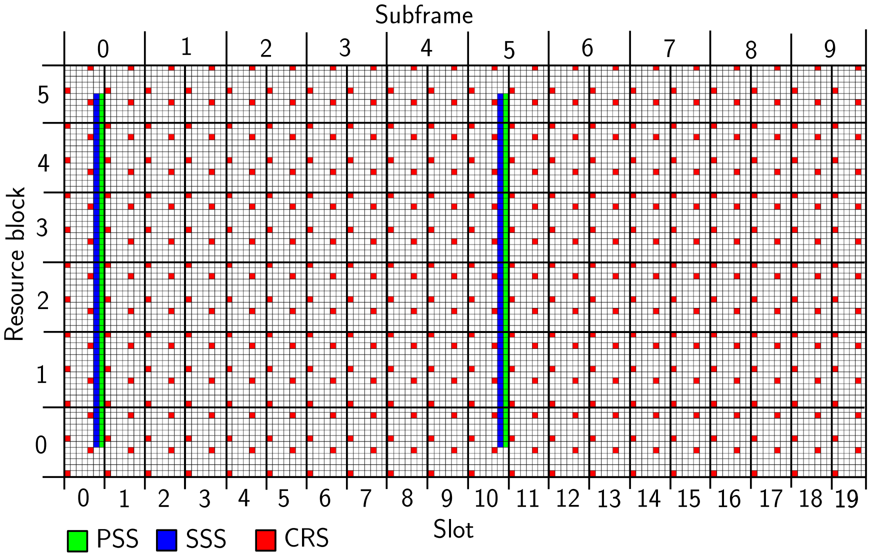


Figure 2.3: An example of the LTE frame structure with $N_r = 72$. PSS and SSS are transmitted on the middle 62 subcarriers. The last symbols of slots 0 and 10 are allocated to PSS. SSS is transmitted on the sixth symbol of slot 0 or 10. CRS is scattered in both frequency and time. CRS subcarriers are assigned based on the cell ID and symbol number.

Since each data type is mapped to a specific time and symbol, the UE needs to first convert the signal into the frame structure to be able to extract the transmitted information. This is achieved by first identifying the frame start time. To provide the frame start time to the UE, the PSS and secondary synchronization signal (SSS) are transmitted in each frame. The UE can estimate the frame start time by finding the peak of the correlation of the received signal with the locally generated PSS and SSS. Then, knowing the frame timing, the receiver can remove the CPs and take a fast Fourier transform (FFT) of each N_c symbols. The duration of a normal CP is 5.21 μs for the first symbol of each slot and 4.69 μs for the rest of the symbols [36].

2.2 Ranging Signals

There are five different sequences in the received LTE signal that can be used for positioning:

1. **CP:** A CP is transmitted to reduce ISI, which is caused by multipath. A CP of length L_{CP} repeats the last L_{CP} samples of each symbol at the beginning of the symbol. Therefore, by correlating the received samples with themselves, the time and frequency offsets can be estimated as discussed in [37].

2. **PSS:** To provide symbol timing, the PSS is transmitted on the last symbol of slot 0 and repeated on slot 10. The PSS is a length-62 Zadoff-Chu sequence, which is located in the 62 middle subcarriers of the bandwidth, excluding the DC subcarrier [38]. The PSS is transmitted in only three possible sequences which map to an integer value $N_{ID}^{(2)} \in \{0, 1, 2\}$, representing the sector number of the eNodeB.

3. **SSS:** The SSS is an orthogonal length-62 sequence, which is transmitted in either slot 0 or 10 in the symbol preceding the PSS and on the same subcarriers as the PSS. The SSS is obtained by concatenating two maximal-length sequences scrambled by a third

orthogonal sequence generated based on $N_{ID}^{(2)}$. There are 168 possible sequences for the SSS that are mapped to an integer number $N_{ID}^{(1)} \in \{0, \ldots, 167\}$, called the cell group identifier. After determining $N_{ID}^{(1)}$ and $N_{ID}^{(2)}$, the eNodeB's cell ID can be calculated as [36, 39]

$$N_{ID}^{Cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}. \tag{2.1}$$

The cell ID can be used for data association purposes.

4. **CRS:** The CRS is transmitted for channel estimation purposes and is scattered in time and bandwidth. The CRS sequence is defined based on the cell ID, allocated symbol, slot, and transmission antenna port number, such that different eNodeBs' CRS sequences are orthogonal to each other. The eNodeB's cell ID indicates the designated subcarriers to the CRS. In this dissertation, the transmitted CRS on the k-th subcarrier and i-th symbol is denoted by $S_i(k)$, where $k = m\Delta_{\text{CRS}} + \kappa$, $m = 0, \cdots, M-1$, $M = \lfloor N_r/\Delta_{\text{CRS}} \rfloor$, $\Delta_{\text{CRS}} = 6$, and κ is a constant shift depending on the cell ID and the symbol number i. In the sequel, for simplicity of notations, the subscript i is only used when it is required to indicate a specific symbol number. Fig. 2.3 shows the PSS, SSS, and CRS signals.

5. **PRS:** Similar to the CRS, the positioning reference signal (PRS) is a scattered pilot signal, which was introduced in LTE Release 9 for a network-based positioning. In positioning with the PRS, the dedicated resources to the PRS are free from interference since the neighboring eNodeBs do not transmit any signal on the subcarriers allocated to the PRS, when one eNodeB is transmitting its PRS sequence. The positioning accuracy of PRS is expected to be on the order of 50 m [40].

Note that all the above reference signals except PRS are broadcast in every LTE frame regardless of the presence of a UE in the environment. Therefore, it is always possible to use these reference signals for positioning. Besides, since the LTE reference signals are broadcast, the receiver does not need to be an authorized UE to be able to exploit these reference signals for navigation. This makes it possible to use the reference signals transmitted from eNodeBs of *different* network operators, simultaneously.

Although all the above signals can be exploited for extracting navigation observables, there are a few challenges associated with the CP, PSS, and PRS signals, which leaves the SSS and CRS signals more attractive for navigation. These challenges include:

- The estimated TOA with the CP signals may have high error in multipath environments. Besides, since the transmitted CPs for different eNodeBs are not orthogonal, it is not possible to estimate TOAs for different eNodeBs using the CPs.
- Since PSS signals can only accept three different orthogonal sequences, the number of intra-frequency eNodeBs that a UE can simultaneously use for positioning is limited to three [32].
- Network-based positioning using PRS suffers from a number of drawbacks: (1) the user's privacy is compromised since the user's location is revealed to the network [41], (2) localization services are limited only to paying subscribers and from a particular cellular provider, (3) ambient LTE signals transmitted by other cellular providers are not exploited, and (4) additional bandwidth is required to accommodate the PRS, which caused the majority of cellular providers to choose not to transmit the PRS in favor of dedicating more bandwidth to traffic channels. To circumvent these drawbacks, UE-based positioning approaches that exploit the CRS have been explored, where several advanced signal processing techniques were developed to achieve a performance similar to the PRS [29–31, 42, 43].

Due to the aforementioned challenges, this dissertation will focus only on the CRS and SSS signals.

2.3 Received Signal Model

In this section, the signal model for the received SSS and CRS are presented.

2.3.1 SSS Received Signal Model

The SSS is transmitted only once per frame. Denote the SSS sequence in frequency-domain by $S_{\text{SSS}}(f)$. Therefore, by taking an inverse Fourier transform (IFT) of $S_{\text{SSS}}(f)$, the SSS signal in time-domain can be obtained according to

$$s_{\text{SSS}}(t) = \begin{cases} \text{IFT}\{S_{\text{SSS}}(f)\}, & \text{for } t \in (0, T_{\text{symb}}), \\ 0, & \text{for } t \in (T_{\text{symb}}, T_f), \end{cases}$$

where $T_{\text{symb}} = 1/\Delta f$ is the duration of one symbol [36].

The received signal is processed in blocks, each of which spans the duration of a frame. Assuming that the transmitted signal is propagated in an additive white Gaussian noise (AWGN) channel, the received signal in time domain can be modeled as

$$\begin{aligned} &r(t) = \sqrt{C}e^{j(2\pi f_D t+\phi)} \cdot [s_{\text{code}}(t - t_{\text{TOA}_k} - kT_f) + d(t - t_{\text{TOA}_k} - kT_f)] + n(t), \\ &\text{for} \quad kT_f \leq t \leq (k+1)T_f, \quad k = 0, 1, 2, \cdots, \end{aligned}$$

where k is the frame number; $s_{\text{code}}(t) \triangleq \sqrt{\frac{T_f}{W_{\text{SSS}}}} s_{\text{SSS}}(t)$; $W_{\text{SSS}} = 945$ kHz is the SSS bandwidth; C is the received signal power including antenna gains and implementation loss; t_{TOA} is the TOA of the SSS signal; ϕ is the carrier phase; f_D is the total carrier frequency offset due to the Doppler frequency, clock drift, and oscillators' mismatch; $n(t)$ is an additive white noise with a constant power spectral density $N_0/2$ Watts/Hz; and $d(t)$ is some data transmitted by the eNodeB other than the SSS, where

$$d(t) = 0 \quad \text{for } t \notin (t_{\mathrm{TOA}}, t_{\mathrm{TOA}} + T_{\mathrm{symb}}).$$

2.3.2 CRS Received Signal Model

The transmitted OFDM symbol at the k-th subcarrier and on the i-th symbol, which contains CRS, can be expressed as

$$Y_i(k) = \begin{cases} S_i(k), & \text{if } k \in N_{CRS}, \\ D_i(k), & \text{otherwise,} \end{cases} \tag{2.2}$$

where N_{CRS} denotes the set of subcarriers containing the CRS and $D_i(k)$ represents some other data signals.

It is assumed that the OFDM symbol is transmitted in a multipath fading channel, which is assumed to stay constant over the duration of a symbol and has the CIR as

$$h_i(\tau) = \sum_{l=0}^{L-1} \alpha_{i,l}\, \delta(\tau - \tau_{i,l}),$$

where i is the symbol number; L is the number of multipath components; $\alpha_{i,l}$ and $\tau_{i,l}$ are the relative attenuation and delay components, respectively, of the l-th path with respect to the first path; $\alpha_{i,0} = 1$ and $\tau_{i,0} = 0$; and δ is the Dirac delta function. Therefore, the received symbol after removing the CP and taking an FFT in a perfect synchronization condition is modeled as

$$R_i(k) = \sqrt{C}\, Y_i(k) H_i(k) + W_i(k), \qquad \text{for } k = 0, \cdots, N_c - 1,$$

where $W_i(k) \sim \mathcal{CN}(0, \sigma^2)$, where $\mathcal{CN}(a, b)$ denotes the complex Gaussian distribution with mean a and variance b, and

$$H_i(k) = \sum_{l=0}^{L-1} \alpha_{i,l} e^{-j2\pi\tau_{i,l}k/T_{\text{symb}}} \tag{2.3}$$

is the channel frequency response (CFR).

In general, there is a mismatch between the estimated received symbol timing and the actual one, which can be due to imperfect synchronization, clock drift, Doppler frequency, and/or carrier frequency offset. Assuming that time mismatch is less than the CP duration, the received signal at the i-th symbol can be rewritten as [44, 45]

$$\begin{aligned} &R_i(k) = e^{j\pi e_f}\, e^{j2\pi(iN_t + L_{\text{CP}})e_f/N_c}\, e^{j2\pi e_\tau k/N_c} \sqrt{C}\, Y_i(k) H_i(k) + W_i(k), \\ &\text{for } k = 0, \cdots, N_c - 1, \end{aligned} \tag{2.4}$$

where $N_t = N_c + L_{\text{CP}}$, $e_f = \frac{f_D}{\Delta f}$, and $e_\tau = \frac{\hat{t}_{\text{TOA}} - t_{\text{TOA}}}{T_s}$ is the symbol timing error normalized by the sampling interval $T_s = T_{\text{symb}}/N_c$. Note that the first two exponentials in (2.4) model the effects of the carrier frequency offset and the third exponential models the effect of the symbol timing error. It is worth mentioning that Doppler frequency for each subcarrier is slightly different due to their different frequencies. In this dissertation, this difference is neglected and the Doppler frequency is defined with respect to the center frequency f_c.

Chapter 3

LTE Receiver Structure

LTE signals are not designed for navigation. Therefore, to exploit these signals for the navigation purpose, specialized receiver structure is required. This type of receiver must be able to extract navigation observables including code and carrier phase and Doppler frequency measurements, while maintaining low computational cost and high accuracy and precision. In this chapter, the structure of the proposed SDR is presented, which consists of four main stages. In the first stage, which is discussed in Section 3.1, a coarse estimate of the frame timing is obtained by correlating the received signal with the locally generated PSS and SSS sequences. In the second stage, which is provided in Section 3.2, the received samples are converted to the frame structure and some of the important parameters for navigation are decoded from the broadcast information on the physical channels. In the third stage, which is presented in Section 3.3, the received CRS signal is used to refine the frame timing estimate. In the last stage, which is discussed in Section 3.4, tracking loop is used to keep track of TOA changes.

The results of this chapter have been published in [46–49].

3.1 Coarse Acquisition

When a UE enters an unknown LTE environment, the first step it performs to establish communication with the network is synchronizing with the surrounding eNodeBs. This is achieved by acquiring the PSS and the SSS transmitted by the eNodeB, which is discussed in this section.

A UE initiates its connection by receiving the baseband samples of the OFDM symbols and their corresponding CPs as shown in Fig. 3.1. The UE may start receiving a signal at any time of any frame. The UE needs to obtain the symbol start time to be able to remove the CPs and take the FFT to convert the signal to the frame structure. For this purpose, the UE must first detect the location of the transmitted PSS in the frame. The UE exploits the orthogonality of the Zadoff-Chu sequences and correlates the received signal with all the possible choices of the PSS according to

$$\begin{aligned}\mathcal{R}(m) &\triangleq \sum_{n=0}^{N_f-1} r(n)s^*_{\text{PSS}}(n+m)_{N_f}\\ &= r(m) \circledast_{N_f} s^*_{\text{PSS}}(-m)_{N_f}, \end{aligned} \tag{3.1}$$

where $r(n)$ is the received signal, $s_{PSS}(n)$ is the receiver-generated PSS in time-domain, $N_f = T_f/T_s$ is the frame length, $(\cdot)^*$ denotes the complex conjugate, $(\cdot)_{N_f}$ denotes the circular shift operator, and $\circledast_N$ represents the circular convolution operation. Taking the FFT and IFFT of (3.1) yields

$$\mathcal{R}(m) = \text{IFFT}\left\{R(k)S^*_{\text{PSS}}(k)\right\}, \tag{3.2}$$

where $R(k) \triangleq \text{FFT}\{r(n)\}$ and $S_{\text{PSS}}(k) \triangleq \text{FFT}\{s_{\text{PSS}}(n)\}$. The PSS sequence corresponding to the highest correlation peak, represents $N_{ID}^{(2)}$.

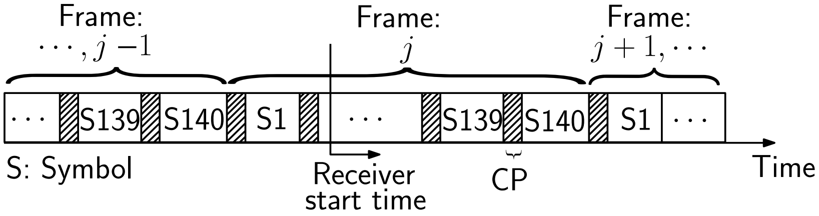


Figure 3.1: Received signal's samples structure. The receiver may start receiving the samples at any random time.

The FFT-based correlation in (3.2) is also used to detect the SSS signal. The SSS sequence corresponding to the highest correlation peak, represents $N_{ID}^{(1)}$. Once the PSS and SSS are detected, the UE can estimate the frame start time and the eNodeB's cell ID using (2.1). Fig. 3.2 summarizes the LTE signal coarse acquisition process.

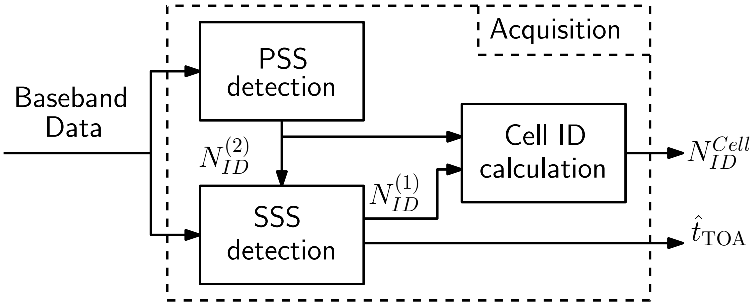


Figure 3.2: Signal acquisition block diagram.

The PSS is transmitted twice per frame. Hence, the correlation result has two peaks in the duration of one frame, which is 10 ms. Since the transmitted PSS sequences on slot 0 and 10 are the same, the UE cannot extract the symbol numbers from the correlation result and only the symbol start time can be obtained. Note that each type of signal is transmitted on a specific symbol and subcarrier of each frame. Therefore, knowing the symbol start time is not enough and the UE needs to exactly obtain the symbol numbers in each frame. Therefore, the signal is correlated with the locally generated time-domain SSS signal. The SSS correlation result has only one peak, since the SSS is transmitted only once per frame. Since the SSS sequence depends on the slot number, it is possible to obtain the symbol number using the SSS correlation results. Fig. 3.3 shows an example of the correlation of locally generated PSS and SSS signals with real LTE signals over 10 ms.

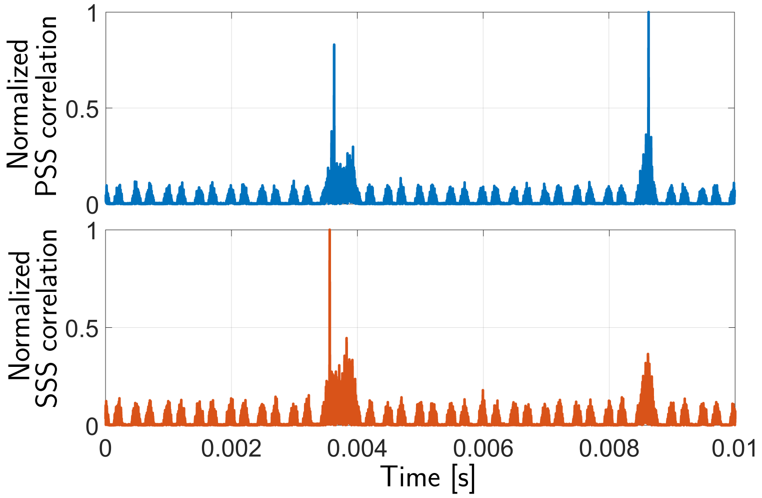


Figure 3.3: Normalized PSS and SSS correlation results with real LTE signals

The PSS and SSS have approximately 1 MHz bandwidth. Due to this low transmission bandwidth, the peak of the correlations may have a bias compared to the true frame timing in a multipath environment. This bias can be refined by estimating the timing error using the CRS signal, which has higher transmission bandwidth. This requires the knowledge of signal transmission bandwidth. However, when a UE enters an unknown LTE environment, it does not have any information about the signal transmission bandwidth. Therefore, it assumes that the signal is transmitted at the lowest transmission bandwidth. Then, it acquires the PSS and SSS and converts the signal to the frame, as discussed in this section. Next, the UE decodes the message that is broadcast in the frame to extract some of the signal parameters including the transmission bandwidth. Finally, it adjusts its received bandwidth to capture the whole transmission bandwidth of the signal. Important parameters for navigation and the process of decoding them from LTE frame are discussed in the next section.

3.2 System Information Extraction and Neighboring Cells Identification

After acquiring the LTE signal, the UE needs to determine several parameters of the LTE network in order to successfully communicate with the eNodeBs. Parameters relevant for navigation purposes include the system bandwidth, number of transmitting antennas, and neighboring cell IDs. These parameters are provided to the UE in two blocks, namely the master information block (MIB) and the system information block (SIB), which are transmitted on the physical broadcast channel (PBCH) and physical downlink shared channel (PDSCH), respectively. In this section, the steps to decode each block are discussed in details.

3.2.1 MIB Decoding

In order to exploit the high-bandwidth CRS signal, which improves the navigation performance in multipath environments, the UE must know the exact transmission bandwidth of the signal. This parameter along with the number of transmitting antennas are provided in the MIB, which must be decoded first. The MIB is transmitted on the PBCH and consists of 24 bits of data: 3 bits for downlink bandwidth, 3 bits for frame number, and 18 bits for other information and spare bits. The MIB is coded and transmitted on 4 consecutive symbols of the frame's second slot. However, it is not transmitted in REs reserved for the reference signals. Fig. 3.4 shows the steps that the MIB message goes through before transmission [36, 50].

In the first step, a cyclic redundancy check (CRC) of length $L = 16$ is obtained using the cyclic generator polynomial $g_{\text{CRC}}(D) = D^{16} + D^{12} + D^{5} + 1$. The number of transmitting antennas is not transmitted in the 24-bit MIB message. Instead, this information is provided in the CRC mask, which is a sequence used to scramble the CRC bits appended to the MIB.

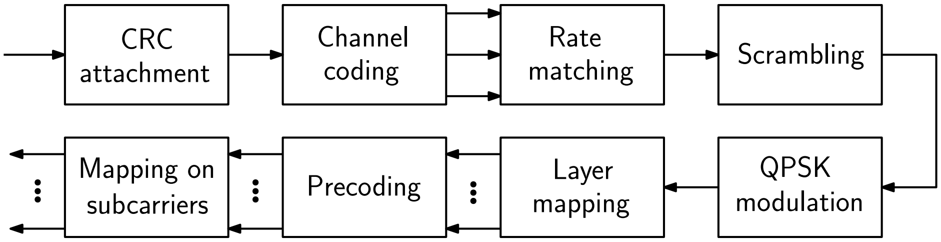


Figure 3.4: MIB coding process

The CRC mask is either all zeros, all ones, or $[0, 1, 0, \cdots, 0, 1]$ for 1, 2, or 4 transmitting antennas, respectively. In order to obtain the number of transmitting antennas from the received signal, the UE needs to perform a blind search over the number of all possible transmitting antennas. Then, by comparing the locally-generated CRC scrambled by the CRC mask to the received CRC, the right number of transmitting antennas may be identified.

In the second step, channel coding is performed using a convolutional encoder with constraint length 7 and coding rate 1/3. The configuration of the encoder is shown in Fig. 3.5. The initial value of the encoder is set to the value of the last 6 information bits in the input stream. The method illustrated in Fig. 3.6 is used to decode the received signal [51]. In this method, the received signal is repeated one time. Then, a Viterbi decoder is executed on the resulting sequence. Finally, the middle part of the sequence is selected and circularly shifted.

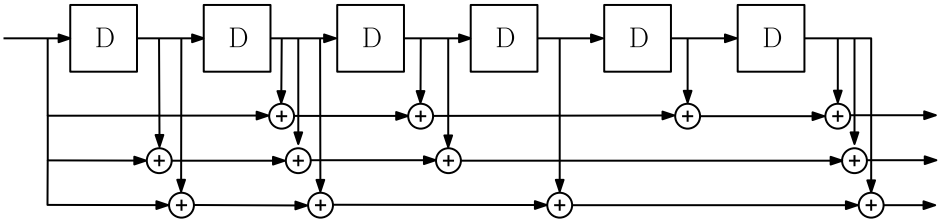


Figure 3.5: Tail biting convolutional encoder with constraint length 7 and coding rate 1/3

In the next step, the convolutional coded bits are rate-matched. In the rate matching step, the obtained data from channel coding is first interleaved. Then, the outcomes of interleaving each stream are repeated to obtain a 1920-bit long array [50]. Next, the output of the rate matching step is scrambled with a pseudo-random sequence, which is initialized with the

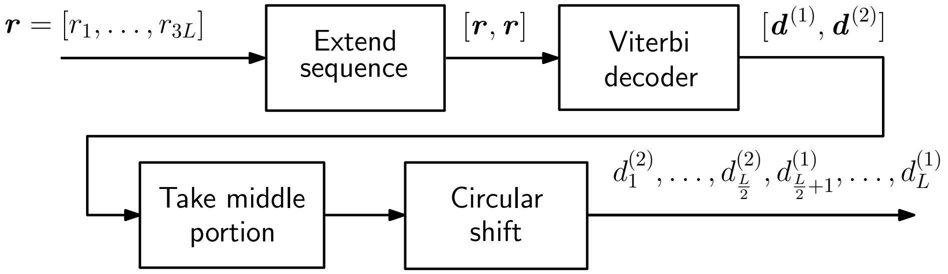

$\boldsymbol{r} = [r_1, \ldots, r_{3L}]$
Extend sequence
$[\boldsymbol{r}, \boldsymbol{r}]$
Viterbi decoder
$[\boldsymbol{d}^{(1)}, \boldsymbol{d}^{(2)}]$
Take middle portion
Circular shift
$d_1^{(2)}, \ldots, d_{\frac{L}{2}}^{(2)}, d_{\frac{L}{2}+1}^{(1)}, \ldots, d_L^{(1)}$

Figure 3.6: MIB channel decoding method

cell ID, yielding unique signal detection for all eNodeBs. Subsequently, quadrature phase shift keying (QPSK) is performed on the obtained data, resulting in 960 symbols which are mapped onto different layers to provide transmission diversity. To overcome channel fading and thermal noise, space-time coding is utilized. This process is performed in the precoding step. Finally, the resulting symbols are mapped onto the predetermined subcarriers for MIB transmission [50].

3.2.2 SIB Decoding

When a UE performs acquisition, it obtains the cell ID of the ambient eNodeB with the highest power, referred to as the main eNodeB in this dissertation. For navigation purposes, the UE needs access to multiple eNodeB signals to estimate its state. One solution is to perform the acquisition for all the possible values of N_{ID}^{Cell}. However, this method limits the number of eNodeBs that a UE can simultaneously use for positioning to only the intra-frequency eNodeBs. The other solution is to extract the neighboring cell IDs using the information provided in the SIB transmitted by the main eNodeB. Since other operators transmit on different carrier frequencies, the same approach can be exploited to extract the cell IDs of the neighboring eNodeBs from other operators. Knowing the eNodeBs' cell IDs, the receiver only needs to know the position of the eNodeBs using a database or pre-mapping approaches.

The SIB contains information on (1) the eNodeB to which it is connected, (2) inter- and intra-frequency neighboring cells from the same operator, (3) neighboring cells from other networks (UMTS, GSM, and CDMA2000), and (4) other information. The SIB has 17 different forms called SIB1 to SIB17, which are transmitted in different schedules. SIB1, which is transmitted in subframe 5 of every even frame, carries scheduling information of the other SIBs. This information can be used to extract the schedule of SIB4, which has the intra-frequency neighboring cell IDs. To decode SIB1, the UE has to go through several steps. In each step, the UE needs to decode a physical channel to extract a parameter required to perform other steps.

In general, all the downlink physical channels are coded in a similar fashion before transmission, as shown in Fig. 3.7. Although all the physical channels have the same general structure, each step in Fig. 3.7 differs from one channel to another. In the following, the steps to retrieve information from SIB4 are briefly discussed [36, 50].

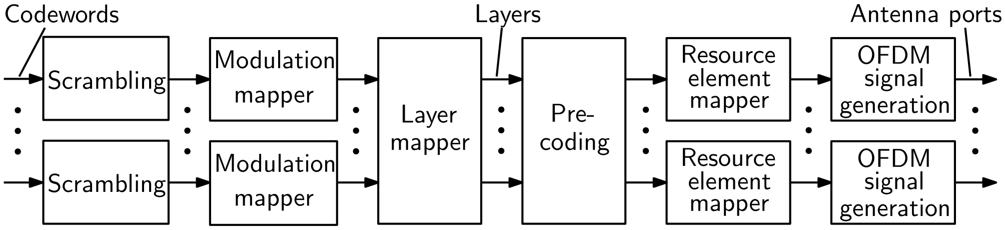


Figure 3.7: General structure of downlink physical channels

PCFICH Demodulation and CFI Decoding

The UE first obtains the control format information (CFI) from the physical control format indicator channel (PCFICH). The CFI indicates the number of REs dedicated to the downlink control channel and can take the values 1, 2, or 3. To decode the CFI, the UE first locates the 16 REs dedicated to the PCFICH. Then, it demodulates the obtained symbols by reverting the steps in Fig. 3.7, which results in a sequence of 32 bits. Finally, this sequence, which can be only one of three possible sequences, is mapped onto a CFI value.

PDCCH Demodulation and DCI Decoding

Knowing the CFI, the UE can identify the REs associated with the PDCCH and demodulate them, resulting in a block of bits corresponding to the DCI message. The packing of these bits can take one of several formats, and is not communicated with the UE. A blind search over the different formats must therefore be performed by the UE to unpack these bits. The "candidate" formats are either on the common search space, or on the UE-specific search space. Fortunately, for the SIBs, there are only two candidate formats and are both located on the common search space. A CRC is obtained to identify the right format.

PDSCH Demodulation and SIB Decoding

The parsed DCI provides the configuration of the corresponding PDSCH REs. The PDSCH, which carries the SIB, is then decoded, resulting in the SIB bits. Subsequently, these bits are decoded using an Abstract Syntax Notation One (ASN.1) decoder, which extracts the system information sent on SIBs by the eNodeB.

Fig. 3.8 summarizes all the aforementioned steps in this section.

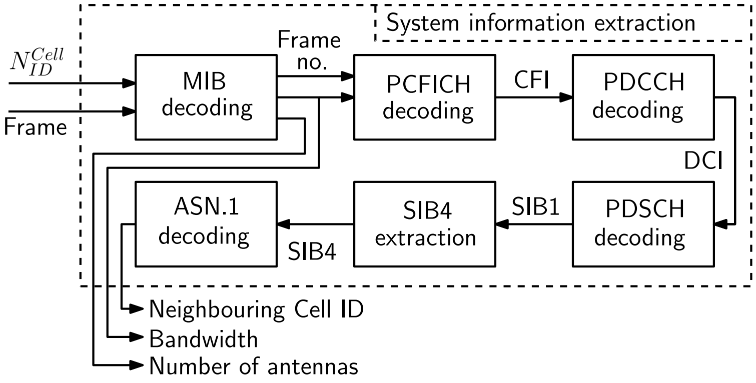


Figure 3.8: System information extraction block diagram

3.3 Acquisition Refinement

In this stage, the remaining symbol timing error is first estimated and removed from the received signal. Besides, due to the receiver's and transmitter's oscillator mismatches and Doppler frequency, a carrier frequency offset may remain in the received signal after carrier wipeoff. In this stage, this carrier frequency offset is initialized and removed from the received signal.

3.3.1 Symbol Timing Refinement

To refine the symbol timing, the CFR must be first estimated. In the i-th symbol and on the subcarriers that carry the CRS, the transmitted signal $Y_i(k)$ is equal to the CRS sequence $S_i(k)$. Since the CRS sequence is known at the receiver, it is possible to estimate the CFR as

$$\begin{aligned}\hat{H}_i(k) &= R_i(k)S_i^*(k), \\ &= \sqrt{C}\sum_{l=0}^{L-1}\alpha_{i,l}e^{j\pi e_f}\, e^{j\frac{2\pi(iN_t+L_{\text{CP}})e_f}{N_c}}\, e^{j\frac{2\pi\left(e_\tau-\tau_{i,l}/T_s\right)k}{N_c}} + W_i'(k), \\ &\text{for } k = m\Delta_{\text{CRS}}+\kappa, \quad m = 0,\cdots,M-1.\end{aligned} \tag{3.3}$$

where $W_i'(k) = W_i(k)S_i^*(k)$. The estimated CFR at the i-th symbol and subcarriers allocated to the CRS can be rewritten as

$$\begin{aligned}\hat{H}_i'(m) &\triangleq \hat{H}_i(m\Delta_{\mathrm{CRS}} + \kappa)\\ &= \sum_{l=0}^{L-1} \alpha_{i,l}' e^{-j\frac{2\pi m\Delta_{\mathrm{CRS}}\tau_{i,l}'}{T_{\mathrm{symb}}}} + W_i''(m)\\ &= \boldsymbol{a}_i^{\mathsf{T}}(m)\boldsymbol{\alpha}_i + W_i''(m), \end{aligned} \tag{3.4}$$

for $m = 0, \cdots, M-1$.

where

$$\begin{aligned}\boldsymbol{\alpha}_i &= \left[\alpha_{i,0}', \cdots, \alpha_{i,L-1}'\right]^{\mathsf{T}},\\ \boldsymbol{a}_i(m) &= \left[e^{-j\frac{2\pi m\Delta_{\mathrm{CRS}}\tau_{i,0}'}{T_{\mathrm{symb}}}}, \cdots, e^{-j\frac{2\pi m\Delta_{\mathrm{CRS}}\tau_{i,L-1}'}{T_{\mathrm{symb}}}}\right]^{\mathsf{T}},\\ \alpha_{i,l}' &= \sqrt{C}e^{j\pi e_f}\, e^{j\frac{2\pi(iN_t+L_{\mathrm{CP}})e_f}{N_c}}\, e^{-j\frac{2\pi\kappa\tau_{i,l}}{T_{\mathrm{symb}}}}\alpha_{i,l},\\ \tau_{i,l}' &= \tau_{i,l} - T_s e_\tau,\\ W_i''(m) &= W_i'(m\Delta_{\mathrm{CRS}} + \kappa).\end{aligned}$$

For simplicity of notation, the subscript i, which denotes the symbol number is dropped in the sequel, unless it is required. The set of estimated CFR over M different subcarriers can be written as

$$\begin{aligned}\hat{\boldsymbol{H}}' &= \left[\hat{H}'(0), \cdots, \hat{H}'(M-1)\right]^{\mathsf{T}}\\ &= \mathbf{A}\boldsymbol{\alpha} + \boldsymbol{W}''\end{aligned}$$

where

$$\begin{aligned}\mathbf{A} &= [\boldsymbol{a}(0), \cdots, \boldsymbol{a}(M-1)]^{\mathsf{T}},\\ \boldsymbol{W''} &= [W''(0), \cdots, W''(M-1)]^{\mathsf{T}}.\end{aligned}$$

The covariance matrix of the estimated channel $\hat{\boldsymbol{H}}'$ can be written as

$$\mathbf{R}_H = \mathbf{A}\mathbf{R}_\alpha\mathbf{A}^{\mathsf{H}} + \mathbf{R}_W,$$

where $\mathbf{R}_H$, $\mathbf{R}_\alpha$, and $\mathbf{R}_W$ are the covariance matrices of $\hat{\boldsymbol{H}}'$, $\boldsymbol{\alpha}$, and $\boldsymbol{W}''$, respectively. It can be shown that $\mathbf{A}$ has L linearly independent vectors, which span the L-dimensional signal subspace. The goal is to find L independent vectors that best fit the observed CFR. Several methods have been proposed to solve this problem including multiple signal classification (MUSIC) and estimation of signal parameters via rotational invariance techniques (ESPRIT). The ESPRIT method has lower complexity compared to other approaches. It uses the rotational invariance properties of the subarrays of the subcarriers with respect to each other to estimate τ' [52,53]. To be able to use the ESPRIT algorithm, the channel length L must be first estimated. The minimum descriptive length (MDL) criterion is one approach to estimate L [54]. In this subsection, the MDL criterion and the ESPRIT algorithm are summarized. The details of the proof of each approach are provided in [52,54].

Step 1: The data matrix $\mathbf{X}$ must be first constructed with snap shots of estimated CFR as

$$\mathbf{X} = \begin{bmatrix} \hat{H}'(0) & \hat{H}'(1) & \cdots & \hat{H}'(K-1) \\ \hat{H}'(1) & \hat{H}'(2) & \cdots & \hat{H}'(K) \\ \vdots & \vdots & \cdots & \vdots \\ \hat{H}'(P-1) & \hat{H}'(P) & \cdots & \hat{H}'(M-1) \end{bmatrix}$$

where P is the design parameter and $K = M - P + 1$.

Step 2: The channel length L can be estimated using the MDL metric. For this purpose the singular value decomposition (SVD) of $\mathbf{X} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{V}^{\mathsf{H}}$ must be calculated, where H represents the Hermitian operator, $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices, and $\boldsymbol{\Sigma}$ is a diagonal matrix with singular values $\sigma_1 \geq \cdots \geq \sigma_P$ on the diagonal. Next, calculate the MDL criterion as

$$MDL(\gamma) = -K(P-\gamma)\log\left(\frac{\prod_{l=\gamma}^{P-1}\lambda_l^{1/(P-\gamma)}}{\frac{1}{P-\gamma}\sum_{l=\gamma}^{P-1}\lambda_l}\right) + \frac{1}{2}\gamma(2P-\gamma)\log K,$$

for $\gamma = 0, \cdots, P-1$,

where $\lambda_l = \sigma_l^2$. The estimate of L is obtained as

$$\hat{L} = \arg\min_{\gamma} MDL(\gamma).$$

Step 3: By knowing the channel length, it is possible to organize the eigenvectors corresponding to the $\hat{L}$ largest eigenvalues as $\mathbf{U}_s = \mathbf{U}\left[\mathbf{I}_{\hat{L}}\ \mathbf{0}_{\hat{L}\times(P-\hat{L})}\right]^{\mathsf{T}}$, where $\mathbf{I}_l$ is an identity matrix of size l, $\mathbf{0}_{l\times p}$ is an l-by-p matrix whose elements are zeros. Then, construct

$$\mathbf{U}_1 \triangleq \left[\mathbf{I}_{P-1} \qquad \mathbf{0}_{(P-1)\times(P-1)}\right]\mathbf{U}_s,$$
$$\mathbf{U}_2 \triangleq \left[\mathbf{0}_{(P-1)\times(P-1)} \qquad \mathbf{I}_{P-1}\right]\mathbf{U}_s.$$

Step 4: Finally, the ESPRIT rotational matrix must be constructed as

$$\boldsymbol{\Psi} = \left(\mathbf{U}_1^{\mathsf{H}}\mathbf{U}_1\right)^{-1}\mathbf{U}_1^{\mathsf{H}}\mathbf{U}_2,$$

and compute its eigenvalues ψ_l, for $l = 0, \cdots, \hat{L}-1$. The values of τ_l' can be obtained as

$$\tau_l' = -\frac{1}{2\pi T_s \Delta f \Delta_{\text{CRS}}}\arg\{\psi_l\}.$$

Since it was assumed that $\tau_0 = 0$ and $\tau_l' = \tau_l - e_\tau$, the normalized estimated symbol timing error can be obtained as

$$\hat{e}_\tau = -\min_l \tau_l'.$$

Note that in some environments, the direct signal may be blocked and the minimum of the estimated channel delays may not correspond to the line-of-sight (LOS) signal. However, differentiating the LOS signal from non-LOS (NLOS) signals is out of the scope of this dissertation.

The normalized estimated symbol timing error $\hat{e}_\tau$ can be divided into two parts: integer, $\text{Int}\{\cdot\}$, and fractional, $\text{Frac}\{\cdot\}$, given by

$$\hat{e}_\tau = \text{Int}\{\hat{e}_\tau\} + \text{Frac}\{\hat{e}_\tau\},$$

where $-1 \leq \text{Frac}\{\hat{e}_\tau\} \leq 0$.

3.3.2 Frequency Offset Estimation

Next, the initial Doppler frequency can be estimated, by measuring the difference between the received signals' phases on the same symbols of two consecutive slots. For this purpose, define $z(m)$ as

$$\begin{aligned} z(m) &= R_{i+7}(k)R_i^*(k)S_{i+7}^*(k)S_i(k) \\ &= Ce^{j2\pi 7 N_t e_f/N_c}|H_i(k)|^2 + W_{i+7}'(k)W_i'(k), \end{aligned} \tag{3.5}$$

$$\text{for} \quad k = m\Delta_{\text{CRS}} + \kappa, \quad m = 0, \cdots, M-1.$$

Then, the initial carrier frequency offset is estimated as

$$\hat{f}_D = \frac{1}{2\pi T_{\text{slot}}} \Delta\varphi, \tag{3.6}$$

where $T_{\text{slot}} = 0.5$ ms and

$$\Delta\varphi \triangleq \arg \left[\sum_{m=0}^{M-1} z(m) \right]. \tag{3.7}$$

Note that $\Delta\varphi$ is a function of the difference between the phases of two received signals at two different symbols. Since in this dissertation the sampling clock frequency offset is assumed to be negligible, $\Delta\varphi$ is defined according to (3.7). As such, the Doppler frequency estimate (3.6) ignores the sampling clock frequency offset. To include the effect of this offset, an approach such as the one described in [55] could be adopted. The normalized estimated Doppler frequency is used to remove the initial phase estimate from the time-domain received signal as

$$r(n) \longleftarrow e^{-j\hat{\phi}(n)} r(n),$$

where $r(n)$ is the time-domain received signal, $\hat{\phi}(n) = 2\pi \hat{f}_D n T_s$.

After removing the total carrier frequency offset estimate from the received signal $r(n)$, the integer part of the symbol timing error is used to control the FFT window. Then, the FFT is taken from $r(n)$ to convert the signal to the frequency domain $R(k)$. Next, the fractional part of the estimated symbol timing error is removed from $R(k)$ as

$$R'(k) \triangleq e^{-j2\pi k \text{Frac}\{\hat{e}_\tau\}/N_c} R(k).$$

Therefore, the i-th received symbol on the subcarriers carrying the CRS after removing the symbol timing error estimate can be written as

$$R'_i(k) = e^{j\pi\tilde{e}_f}\, e^{j2\pi(iN_t+L_{\mathrm{CP}})\tilde{e}_f/N_c}\, e^{j2\pi\tilde{e}_\tau k/N_c}\sqrt{C}S_i(k)H_i(k) + W_i(k), \tag{3.8}$$
$$\text{for}\quad k = m\Delta_{\mathrm{CRS}} + \kappa, \quad m = 0, \cdots, M-1,$$

where $\tilde{e}_f = e_f - \hat{e}_f$ is the remaining carrier frequency offset and $\tilde{e}_\tau = e_\tau - \hat{e}_\tau$ is the remaining symbol timing error.

3.4 Tracking

After obtaining an initial estimate of the LTE frame timing, a tracking loop can be used to refine this estimate and keep track of any changes in TOA. In [33, 56], a method to jointly estimate the channel impulse response (CIR) and the time delay was proposed. The CIR was modeled statistically by a skew-t distribution in [57], which improves TOA estimation for low bandwidth signals. An SRA was exploited in [31] to obtain the TOA, which resulted in a root mean squared-error (RMSE) of 31.09 m. Although these methods yielded a relatively good positioning accuracy, they are computationally expensive. A first arriving path detection using maximum likelihood in a correlation-based approach was discussed in [35]. A threshold-based approach was used in [30, 58] to detect the first path. This method is computationally low-cost, but does not adapt to the environment, which causes significant errors when the noise level changes. In this section, three tracking loops are proposed, which answer the challenges of the above algorithms.

The SSS and CRS are two possible sequences that a UE can exploit to track the TOA and Doppler frequency. SSS is transmitted over contiguous subcarriers. Therefore, it is possible to obtain a time-equivalent form of the SSS signal and conventional tracking loop structures can be used to track the TOA of these signals. Subsection 3.4.1 presents the structure of the proposed SSS-based tracking loop [59]. The SSS is transmitted with the lowest possible bandwidth. Therefore, the SSS is extremely susceptible to multipath. To achieve a more precise localization using LTE signals, the CRS can be exploited. Since CRS signals are scattered in the subcarriers, conventional tracking loop structures cannot be used for extracting TOA of the CRS signals. Subsection 3.4.2 discusses the proposed threshold-based approach, where an adaptive threshold is calculated to detect the peaks of the CIR [48]. Finally, Subsection 3.4.3 presents a specialized tracking loop consisting a phase-locked loop (PLL) and a carrier-aided delay-locked loop (DLL) to track the CRS TOA and Doppler frequency [47, 49].

3.4.1 SSS-Based Tracking Loop

The proposed SSS-based tracking loop has a frequency-locked loop (FLL)-assisted PLL and a carrier-aided DLL. Fig. 3.9 shows the block diagram of the SSS-based tracking loop, where $\omega_c = 2\pi f_c$ and f_c is the carrier frequency. In this subsection, the structure of the SSS tracking loop is discussed in details.

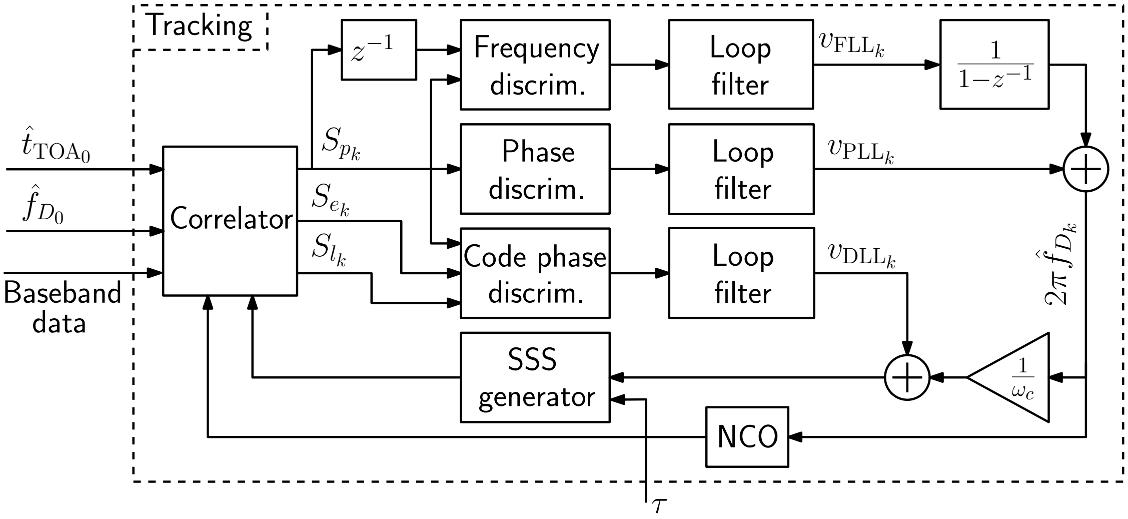


Figure 3.9: SSS-based tracking loop block diagram

FLL-Assisted PLL

The frequency reuse factor in LTE systems is set to be one, which results in high interference from neighboring cells. Under interference and dynamic stress, FLLs have better performance than PLLs. However, PLLs have significantly higher measurement accuracy compared to FLLs. An FLL-assisted PLL has both the dynamic and interference robustness of FLLs and the high accuracy of PLLs [60]. The main components of an FLL-assisted PLL are: a phase discriminator, a phase loop filter, a frequency discriminator, a frequency loop filter, and a numerically-controlled oscillator (NCO). The SSS is not modulated with other data. Therefore, an `atan2` discriminator could be used without the risk of introducing phase ambiguities. A third-order PLL was designed to track the carrier phase, with a loop filter transfer function given by

$$F_{\text{PLL}}(s) = 2.4\,\omega_{\text{PLL}} + \frac{1.1\omega_{\text{PLL}}^2}{s} + \frac{\omega_{\text{PLL}}^3}{s^2}, \tag{3.9}$$

where ω_{PLL} is the undamped natural frequency of the phase loop, which can be related to the PLL noise-equivalent bandwidth B_{PLL} by $B_{\text{PLL}} = 0.7845\,\omega_{\text{PLL}}$ [61]. The output of the phase loop filter is the rate of change of the carrier phase error $2\pi\hat{f}_{D_k}$, expressed in rad/s, where $\hat{f}_{D_k}$ is the Doppler frequency estimate at the k-th subaccumulation period. The phase loop filter transfer function in (3.9) is discretized and realized in state-space. The PLL is assisted by a second-order FLL with an `atan2` discriminator for the frequency as well. The frequency error at the k-th subaccumulation period is expressed as

$$e_{\text{FLL}_k} = \frac{\texttt{atan2}\left(Q_{p_k}I_{p_{k-1}} - I_{p_k}Q_{p_{k-1}}, I_{p_k}I_{p_{k-1}} + Q_{p_k}Q_{p_{k-1}}\right)}{T_{\text{sub}}},$$

where $S_{p_k} = I_{p_k} + jQ_{p_k}$ is the prompt correlation at the k-th subaccumalation period and $T_{\text{sub}} = 10$ ms is the subaccumulation period, which is chosen to be one frame length unless it is noted otherwise. The transfer function of the frequency loop filter is given by

$$F_{\text{FLL}}(s) = 1.414\,\omega_{\text{FLL}} + \frac{\omega_{\text{FLL}}^2}{s}, \tag{3.10}$$

where ω_{FLL} is the undamped natural frequency of the frequency loop, which can be related to the FLL noise-equivalent bandwidth B_{FLL} by $B_{\text{FLL}} = 0.53\,\omega_{\text{FLL}}$ [61]. The output of the frequency loop filter is the rate of change of the angular frequency $2\pi\hat{\dot{f}}_{D_k}(n)$, expressed in rad/s^2. It is therefore integrated and added to the output of the phase loop filter. The frequency loop filter transfer function in (3.10) is discretized and realized in state-space.

Carrier-Aided DLL

The carrier-aided DLL employs the non-coherent dot-product discriminator given by

$$e_{\text{DLL}_k} = c_{\text{DLL}}\left[(I_{e_k} - I_{l_k})\,I_{p_k} + (Q_{e_k} - Q_{l_k})\,Q_{p_k}\right],$$

where e_{DLL} is the code phase error and c_{DLL} is a normalization constant given by

$$c_{\text{DLL}} = \frac{T_c}{2(\mathbb{E}\{|S_{p_k}|^2\} - 2\sigma_{IQ}^2)},$$

where $S_{e_k} = I_{e_k} + jQ_{e_k}$ and $S_{l_k} = I_{l_k} + jQ_{l_k}$ are the early and late correlations, respectively, $T_c = \frac{1}{W_{\text{SSS}}}$ is the chip interval, $\mathbb{E}\{\cdot\}$ represents the expectation operator, and σ_{IQ}^2 is the interference-plus-noise variance.

The DLL loop filter was chosen to be similar to (3.10), with a noise-equivalent bandwidth B_{DLL} Hz. The output of the DLL loop filter v_{DLL} (in s/s) is the rate of change of the SSS code phase. Assuming low-side mixing, the TOA is updated according to

$$\hat{t}_{\text{TOA}_{k+1}} = \hat{t}_{\text{TOA}_k} - T_{\text{sub}}\left(v_{\text{DLL}_k} + \hat{f}_{D_k}/f_c\right).$$

The estimated TOA is used to reconstruct the received frame for the next loop iteration.

3.4.2 Threshold-Based Tracking

Threshold-based TOA estimation algorithm has been studied in different literature [35, 58]. One of the main challenges of a threshold-based approach is defining the proper value for threshold. In [58], a constant threshold is defined to detect the first peak. However, when the signal attenuation or the noise level is high, the performance of this approach is poor. In [35], the threshold is assigned with respect to the highest peak of the CIR. However, this approach can miss-detect the LOS signal, when it has much lower amplitude than the multipath signal with the highest peak. In this subsection, a first-peak estimation algorithm is proposed in which the threshold adapts to the environmental noise.

Multipath Detection

The estimated CIR is obtained by taking an IFFT from the estimated CFR given by

$$\hat{h}(n) = \text{IFFT}\left\{\hat{H}'(m)\right\} = h(n) + w''(n), \tag{3.11}$$

where $w''(n) \triangleq \text{IFFT}\{W''(k)\} \sim \mathcal{CN}(0, \sigma_h^2)$.

In general, a multipath CIR can be modeled as

$$\begin{aligned} h(n) &= \sum_{l=0}^{L-1} \alpha_l \delta[n - d_l], \\ \text{for} \quad n &= 0, \ldots, M-1, \end{aligned}$$

where d_l is the delay of the l-th path normalized by sampling time [62]. To simplify the derivation, it is assumed that the receiver's low-pass filter has infinite bandwidth. The goal is to estimate d_0, which represents the LOS TOA. In the absence of noise, L will be the number of non-zero components in the estimated CIR, and the position of the non-zero components will be d_l. In the presence of noise, the receiver must be able to distinguish between noise and multipath components at each specific n in the estimated CIR. This problem is similar to detecting the presence of a target in a noisy environment. Therefore, the problem can be modeled as a binary hypothesis test, with H_1 indicating the presence of a target (LOS or multipath signal) and noise, and H_0 indicating the presence of only noise. The hypotheses can be expressed as

$$\begin{cases} H_0 : & \hat{h}(n) = w''(n), & \text{for } n \neq d_l, \\ H_1 : & \hat{h}(n) = \alpha_l + w''(n), & \text{for } n = d_l, \end{cases}$$

where $l = 0, \ldots, L-1$. It is worth mentioning that the receiver does not have any knowledge of α_l, d_l, and L. Under H_0, $\hat{h}(n) = w''(n)$; therefore, $|\hat{h}(n)|$ has a Rayleigh distribution with a probability density function (pdf) given by

$$p\left(|\hat{h}(n)| = r \middle| H_0\right) = \frac{2r}{\sigma_h^2} e^{\left(-\frac{r^2}{\sigma_h^2}\right)}.$$

Under H_1, $\hat{h}(n) = \alpha_l + w''(n)$, where α_l is assumed to be a complex deterministic constant over a frame duration. Therefore, $|\hat{h}(n)|$ has a Rician distribution with the pdf

$$p\left(|\hat{h}(n)| = r \middle| H_1\right) = \frac{2r}{\sigma_h^2} e^{\left(-\frac{r^2+s^2}{\sigma_h^2}\right)} I_0\left(\frac{2rs}{\sigma_h^2}\right),$$

where $r \geq 0$, $I_0(\cdot)$ is the modified Bessel function of zeroth-order, and $s = |\alpha_l|$.

A Neyman-Pearson test is formulated to obtain the decision threshold, denoted η, where the probability of false alarm p_{FA} is set to a desired constant and is given by

$$p_{FA} = \int_{\eta}^{\infty} p\left(|\hat{h}(n)| = r \middle| H_0\right) dr = e^{-\frac{\eta^2}{\sigma_h^2}}. \tag{3.12}$$

The threshold is then calculated as

$$\eta = \sqrt{-\sigma_h^2 \ln(p_{FA})}. \tag{3.13}$$

After determining the threshold, the detection probability is obtained using

$$p_D = \int_{\eta}^{+\infty} \frac{2r}{\sigma_h^2} e^{\left(-\frac{r^2+|\alpha_l|^2}{\sigma_h^2}\right)} I_0\left(\frac{2r|\alpha_l|}{\sigma_h^2}\right) dr.$$

Although it is not possible to obtain a closed-form expression for the probability of detection, numerical solutions for p_D have been tabulated and can also be computed with software packages [63]. Fig. 3.10 demonstrates the receiver operating characteristics (ROC) for different $C/N_0 \triangleq |\alpha_l|^2/N_0$, where $N_0 \triangleq 2\sigma_h^2/\Delta f$.

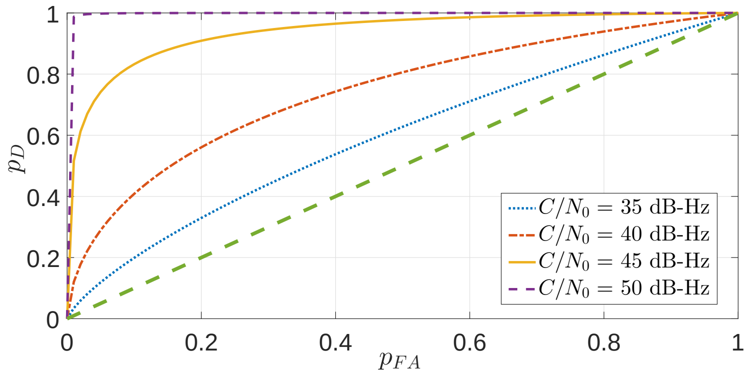


Figure 3.10: ROC for different C/N_0

CFAR for Adaptive Threshold Calculation

The derived threshold equation in (3.13) showed that the threshold depends on the noise variance, σ_h^2. However, the noise variance continuously changes in a dynamic environment, and the threshold must be updated accordingly. Changing the threshold to keep a constant p_{FA} is defined as constant false alarm rate (CFAR). Cell-averaging CFAR (CA-CFAR), shown in Fig. 3.11, is one of the CFAR techniques [64].

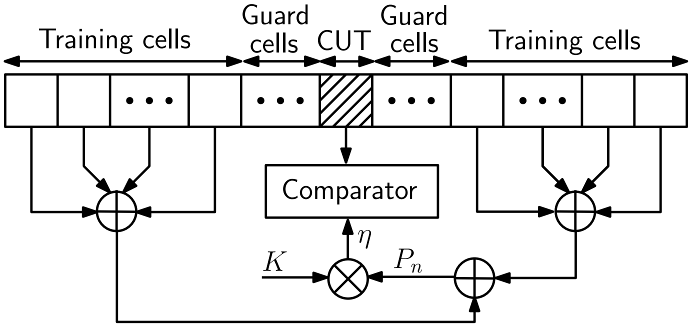


Figure 3.11: Block diagram of the CA-CFAR.

In CA-CFAR, each cell is tested for the presence of a signal. For a given cell under test (CUT), a function of N_t training cells separated from the CUT by N_g guard cells is computed. In a square-law detector, this functional will be the sum of $|\hat{h}(n)|^2$, which is proportional to the background noise level given by

$$P_n = \sum_{m=1}^{N_t} x_m,$$

where x_m is the functional evaluated at the m-th training cell. A threshold can be obtained by multiplying P_n by a constant K, hence $\eta = KP_n$, which can be shown to have a non-central chi-square distribution with $2N_t$ degrees of freedom. The probability of false alarm for a specified threshold was calculated in (3.12). The p_{FA} in CA-CFAR can be obtained by taking the average of (3.12) over all possible values of the decision threshold. This yields

$$\eta = \left(p_{FA}^{-1/N_t} - 1\right) P_n,$$

which is used to compare the desired cell's value to the noise floor.

To improve the probability of detection while maintaining a constant p_{FA}, a non-coherent integration can be used. For this purpose, it is proposed to integrate squared envelopes of $\hat{h}(n)$ at different slots and for different transmitting antennas (assuming that they have the same LOS path) in one frame duration. Defining n_i as the number of non-coherent integrations, the threshold will have a non-central chi-square distribution with $2\,n_i N_t$ degrees of freedom. By taking the average of the probability of false alarm given the threshold presented in (3.12) over the new pdf of this threshold, it can be shown that [64]

$$p_{FA} = \frac{1}{(1+K)^{n_i N_t}} \sum_{k=0}^{n_i-1} \frac{1}{k!} \frac{\Gamma(n_i N_t + k)}{\Gamma(n_i N_t)} \left(\frac{K}{K+1} \right)^k , \tag{3.14}$$

where $\Gamma(n) = (n-1)!$ is the gamma function. By knowing p_{FA} and its relation to K according to (3.14), the value of K can be solved numerically (e.g. using Newton algorithm) and the threshold will be determined from $\eta = K P_n$.

Using the proposed method for tracking the TOA, the probability of false alarm in detecting the first peak is equivalent to detecting the noise as a valid signal, which can cause significant errors and potentially loss of track. To resolve this problem, a low-pass filter is applied after the CFAR detector, which removes sudden changes in the estimated TOA. The localization error with the proposed method is acceptable for medium to high bandwidth LTE signals (e.g. above 10 MHz). For lower bandwidths, other methods could be exploited [57]. After detecting d_0, the residual TOA, $\tau = T_s\, d_0$, is fed-back to the tracking loops to improve the estimated frame start time $\hat{t}_{\text{TOA}}$.

3.4.3 CRS-Based Tracking Loop

Fig. 3.12 shows the structure of the proposed CRS-based tracking loop. The CRS-based tracking loop consists of a PLL and a carrier-aided DLL, which will be discussed in this subsection.

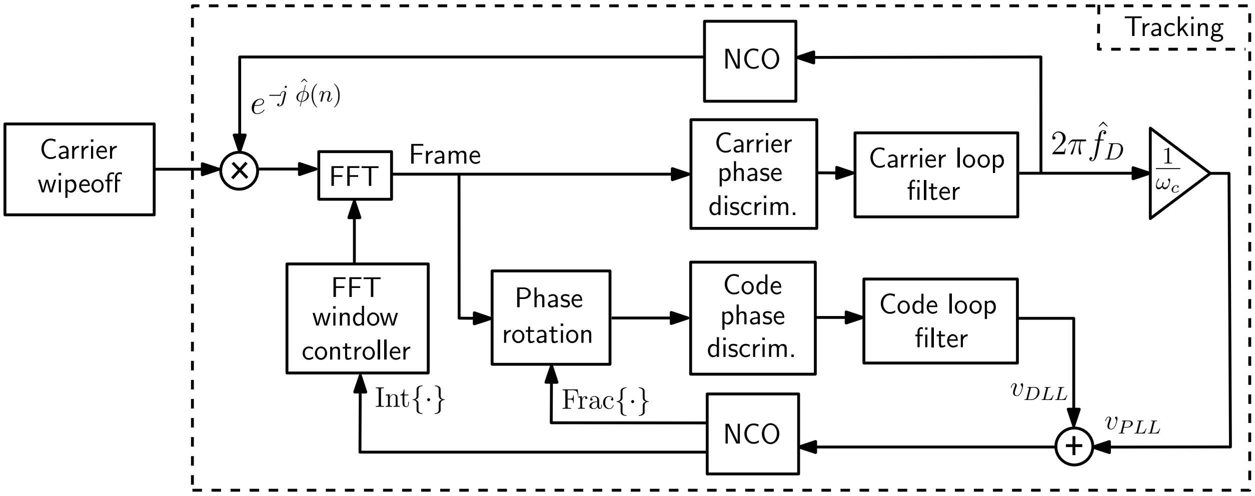


Figure 3.12: Block diagram of the proposed CRS-based tracking loop

PLL

A PLL has three main components: a carrier phase discriminator function, a carrier loop filter, and an NCO. The carrier phase discriminator function is defined as

$$D_{\text{PLL}} = \arg\left[\sum_{m=0}^{M-1} R'(k)S^*(k)\right],$$
$$\text{for}\quad k = m\Delta_{\text{CRS}} + \kappa, \quad m = 0, \cdots, M-1.$$

It can be shown that for $\tilde{e}_\tau \approx 0$ the PLL discriminator function for the i-th received signal and in a multipath-free environment can be written as

$$D_{\text{PLL}} = \Delta\phi + N_{\text{PLL}},$$

where $\Delta\phi = \pi\tilde{e}_f + 2\pi(iN_t + L_{\text{CP}})\tilde{e}_f/N_c$ and N_{PLL} is a zero-mean noise with variance

$$\text{var}\left[N_{\text{PLL}}\right] = \frac{\sigma^2}{2MC}\left(1 + \frac{\sigma^2}{2MC}\right). \tag{3.15}$$

A second-order PLL is used to track the carrier phase, with a loop filter transfer function similar to (3.10). The output of the filter is the rate of change of the carrier phase error $2\pi\hat{f}_D$ expressed in rad/s. The loop update rate was set to a frame duration of T_f. An NCO is used to integrate the phase as

$$\phi(n) \longleftarrow 2\pi\hat{f}_D nT_s + \phi(N_f),$$
$$\text{for } n = 0, \cdots, N_f,$$

where $N_f = T_f/T_s$ is the number of samples per frame. Then, the resulting phase is removed from the received signal as

$$r(n) \longleftarrow e^{-j\phi(n)}r(n).$$

DLL

In conventional DLLs (e.g., dot-product) the TOA error is obtained as a function of the early, late, and prompt correlations, which are the correlation of the received signals with locally generated early (advanced), late (delayed), and prompt versions of the code sequence, respectively. The CRS is scattered in the bandwidth, which makes obtaining its time-equivalent form infeasible. As a result, obtaining the time-domain correlation of the received signal and the code will not be possible and conventional DLLs cannot be used to track the CRS. In this dissertation, a specialized DLL, which is designed for OFDM signals, is used to track the CRS in LTE systems.

A DLL has three main components: a code phase discriminator function, a code loop filter, and an NCO. Fig. 3.13 shows the structure of the code phase discriminator function, which is an adaptation of [45] for LTE systems.

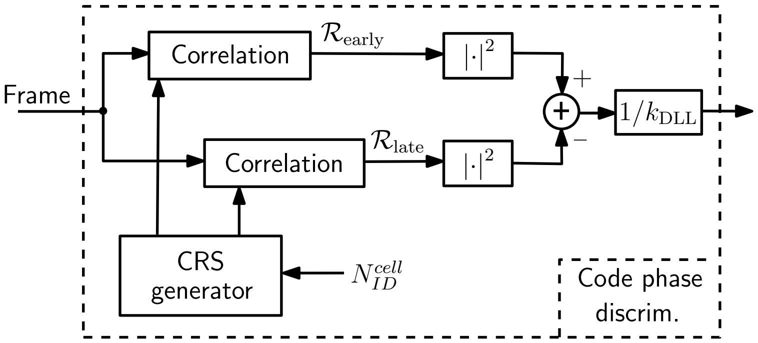


Figure 3.13: The structure of the code phase discriminator function for a CRS-based tracking loop

Since a shift in the time-domain is equivalent to a phase rotation in the frequency-domain, the locally generated early and late code signals for the OFDM symbol can be obtained respectively as

$$\begin{aligned} S_{\text{early}}(m) &= e^{-j2\pi m/M\xi}S(k), \\ S_{\text{late}}(m) &= e^{j2\pi m/M\xi}S(k), \\ &\text{for} \quad k = m\Delta_{\text{CRS}} + \kappa, \quad m = 0, \cdots, M-1. \end{aligned}$$

where $0 < \xi \leq 1/2$ is the normalized time shift. The early and late correlations in the frequency-domain can be expressed respectively as

$$\begin{aligned} \mathcal{R}_{\text{early}} &= \sum_{m=0}^{M-1} R'(m\Delta_{\text{CRS}} + \kappa)S^*_{\text{early}}(m), \\ \mathcal{R}_{\text{late}} &= \sum_{m=0}^{M-1} R'(m\Delta_{\text{CRS}} + \kappa)S^*_{\text{late}}(m). \end{aligned}$$

The discriminator function is defined as

$$D_{\mathrm{DLL}} \triangleq |\mathcal{R}_{\mathrm{early}}|^2 - |\mathcal{R}_{\mathrm{late}}|^2 \triangleq M^2 C \Lambda_{\mathrm{DLL}}(\tilde{e}_\tau, \xi) + N_{\mathrm{DLL}}, \tag{3.16}$$

where for a channel without multipath, $\Lambda_{\mathrm{DLL}}(\tilde{e}_\tau, \xi)$ is the normalized S-curve function, defined as

$$\Lambda_{\mathrm{DLL}}(\tilde{e}_\tau, \xi) \triangleq \left[\frac{\sin(\pi(\tilde{e}_\tau - \xi))}{M \sin(\pi(\tilde{e}_\tau - \xi)/M)}\right] - \left[\frac{\sin(\pi(\tilde{e}_\tau + \xi))}{M \sin(\pi(\tilde{e}_\tau + \xi)/M)}\right],$$

and N_{DLL} represents the noise with zero-mean and variance

$$\mathrm{var}[N_{\mathrm{DLL}}] \leq 2M^2\sigma^4 \left[1 + \frac{C}{M\sigma^2}\left(\frac{\sin(\pi(\tilde{e}_\tau - \xi))}{\sin(\pi(\tilde{e}_\tau - \xi)/M)}\right)^2 + \frac{C}{M\sigma^2}\left(\frac{\sin(\pi(\tilde{e}_\tau + \xi))}{\sin(\pi(\tilde{e}_\tau + \xi)/M)}\right)^2\right], \tag{3.17}$$

where equality holds for $\xi = 0.5$ [45]. In the following analysis, ξ is set to be 0.5. Fig. 3.14 shows the normalized S-curve.

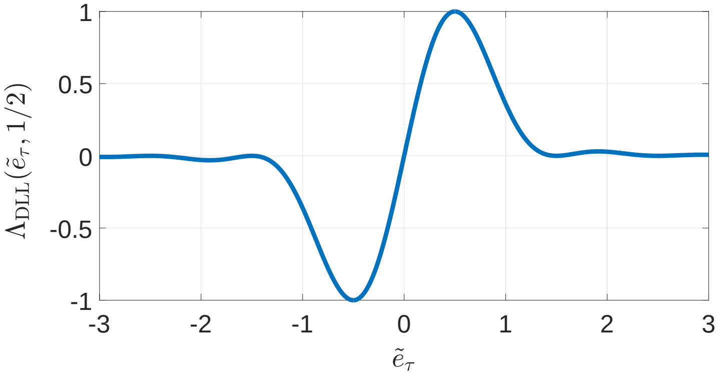


Figure 3.14: DLL discriminator function of the CRS signal

The output of the discriminator function is first normalized by the slope of the S-curve k_{DLL}, which represents the symbol timing error plus noise. Then, a DLL loop filter is used to achieve zero steady-state error. It can be assumed that the symbol timing error has linear variations, which can be due to the clock drift or receiver movement, and a second-order loop filter can provide zero steady-state error. Therefore, the normalized output of the discriminator function is first smoothed using a first-order low-pass filter (LPF) with a transfer function given by (3.10). The loop update rate was set to a frame duration of T_f.

Finally, the frame start time estimate is updated according to

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

where v_{DLL} is the output of the DLL filter, which is the rate of change of the symbol timing error expressed in s/s and $v_{PLL} = 2\pi \hat{f}_D/\omega_c$. The integer part of the frame start time estimate is used to control the FFT window and the fractional part is removed using the phase rotation in frequency domain.

Chapter 4

LTE Ranging Precision Analysis

LTE systems transmit using OFDMA, which is considerably different than CDMA – the transmission standard for GPS. The ranging precision for GPS signals has been extensively studied analytically and empirical error budgets have been established [65]. In this chapter, the ranging precision of LTE signals is analyzed. Section 4.1 derives analytical results for the ranging precision of the SSS-based receiver for both coherent and noncoherent discriminator functions. Section 4.2 presents the ranging precision of the PLL and DLL in a CRS-based receiver.

The results of this chapter have been published in [49, 66, 67].

4.1 SSS-Based Receiver

As discussed in Subsection 3.4.1, an SSS-based tracking loop includes a DLL to track the code phase measurements. There are two types of discriminator functions that can be considered for a DLL: (1) coherent and (2) noncoherent [65, 68]. Coherent discriminator function can be used when the carrier phase is known by the receiver. Noncoherent discriminator functions are independent of the carrier phase tracking accuracy (e.g., the dot-product or the early-power minus late-power discriminator functions). In this section, the ranging precision of each of these discriminator functions is evaluated.

4.1.1 Coherent Discriminator Function

Fig. 4.1 represents the general structure of the DLL. In this subsection, it is assumed that the residual carrier phase and Doppler frequency are negligible, i.e., $\Delta\phi \approx 0$ and $\Delta f_D \approx 0$. Therefore, a coherent baseband discriminator can be used in the DLL.

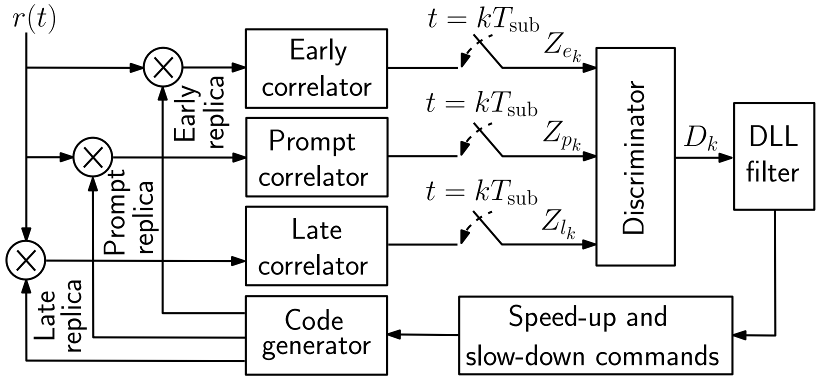


Figure 4.1: General structure of the DLL to track the code phase.

Correlation Signal Model

In the DLL, the received signal is first correlated with the early and late locally-generated replicas of the SSS. The resulting early and late correlations over the k-th subaccumulation period are given by

$$\begin{aligned}
Z_{e_k} &= \frac{1}{T_{\text{sub}}} \int_{kT_{\text{sub}}}^{(k+1)T_{\text{sub}}} r(t) s_{\text{code}}(t - \hat{t}_{\text{TOA}_k} + \frac{t_{\text{eml}}}{2} T_c - kT_{\text{sub}}) dt \\
&\triangleq S_{e_k} + N_{e_k}, \\
Z_{l_k} &= \frac{1}{T_{\text{sub}}} \int_{kT_{\text{sub}}}^{(k+1)T_{\text{sub}}} r(t) s_{\text{code}}(t - \hat{t}_{\text{TOA}_k} - \frac{t_{\text{eml}}}{2} T_c - kT_{\text{sub}}) dt \\
&\triangleq S_{l_k} + N_{l_k},
\end{aligned}$$

where t_{eml} is the correlator spacing (early-minus-late) and $\hat{t}_{\text{TOA}_k}$ is the estimated TOA. The signal components of the early and late correlations, S_{e_k} and S_{l_k}, respectively, are given by

$$\begin{aligned}
S_{e_k} &= \sqrt{C}\mathcal{R}\left(\Delta\tau_k - \frac{t_{\text{eml}}}{2} T_c\right), \\
S_{l_k} &= \sqrt{C}\mathcal{R}\left(\Delta\tau_k + \frac{t_{\text{eml}}}{2} T_c\right),
\end{aligned}$$

where $\Delta\tau_k \triangleq \hat{t}_{\text{TOA}_k} - t_{\text{TOA}_k}$ is the propagation time estimation error and $\mathcal{R}(\cdot)$ is the autocorrelation function of $s_{\text{code}}(t)$, given by

$$\begin{aligned}
\mathcal{R}(\Delta\tau) &= \frac{1}{T_{\text{sub}}} \int_0^{T_{\text{sub}}} s_{\text{code}}(t) s_{\text{code}}(t + \Delta\tau) dt \\
&= \text{sinc}(W_{\text{SSS}}\Delta\tau) - \frac{\Delta f}{W_{\text{SSS}}} \text{sinc}(\Delta f \Delta\tau) \\
&\approx \text{sinc}(W_{\text{SSS}}\Delta\tau).
\end{aligned}$$

It can be shown that the noise components of the early and late correlations, N_{e_k} and N_{l_k}, respectively, are zero mean with the following covariances [69]

$$\text{var}\{N_{e_k}\} = \text{var}\{N_{l_k}\} = \frac{N_0}{2T_{\text{sub}}}, \qquad \forall k$$

$$\mathbb{E}\{N_{e_k} N_{l_k}\} = \frac{N_0 \mathcal{R}(t_{\text{eml}} T_c)}{2T_{\text{sub}}}, \qquad \forall k$$

$$\mathbb{E}\{N_{e_k}N_{e_j}\} = \mathbb{E}\{N_{l_k}N_{l_j}\} = 0, \quad \forall k \neq j.$$

Open-Loop Statistics of the Code Phase Error for a Coherent Discriminator Function

The coherent baseband discriminator function is defined as

$$D_k \triangleq Z_{e_k} - Z_{l_k} = (S_{e_k} - S_{l_k}) + (N_{e_k} - N_{l_k}) \, .$$

The signal component of the discriminator function $S_{e_k} - S_{l_k}$ is shown in Fig. 4.2 for $t_{\mathrm{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$.

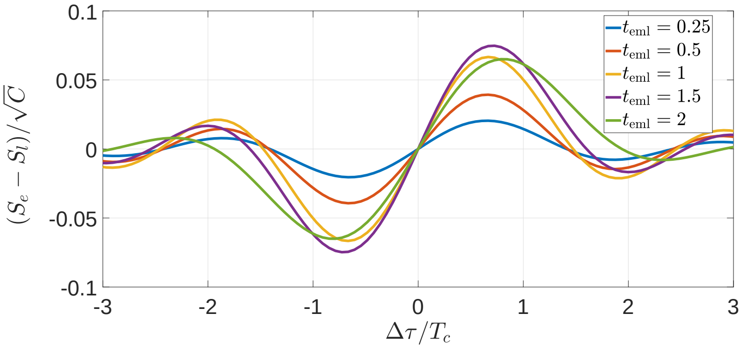


Figure 4.2: The signal component of the coherent baseband discriminator function for the SSS with different correlator spacing.

It can be seen from Fig. 4.2 that the discriminator function can be approximated by a linear function for small values of $\Delta\tau_k$, as given by

$$D_k = k_{\mathrm{SSS}}\Delta\tau_k + N_{e_k} - N_{l_k}, \tag{4.1}$$

where k_{SSS} is the slope of the discriminator function at $\Delta\tau_k = 0$, which is obtained by

$$\begin{aligned} k_{\text{SSS}} &= \left.\frac{\partial D_k}{\partial \Delta\tau_k}\right|_{\Delta\tau_k=0} \\ &= 4\sqrt{C}W_{\text{SSS}}\left(2\frac{\sin(\pi t_{\text{eml}}/2)}{\pi t_{\text{eml}}^2} - \frac{\cos(\pi t_{\text{eml}}/2)}{t_{\text{eml}}}\right). \end{aligned}$$

The mean and variance of D_k can be obtained from (4.1) as

$$\mathbb{E}\{D_k\} = k_{\text{SSS}}\Delta\tau_k, \tag{4.2}$$

$$\text{var}\{D_k\} = \frac{N_0}{T_{\text{sub}}}\big[1 - \mathcal{R}(t_{\text{eml}}T_c)\big]. \tag{4.3}$$

Closed-Loop Statistics of the Code Phase Error for a Coherent Discriminator Function

In a rate-aided DLL, the pseudorange rate estimated by the FLL-assisted PLL is added to the output of the DLL discriminator. In general, it is enough to use a first-order loop for the DLL loop filter since the FLL-assisted PLL's pseudrange rate estimate is accurate. The closed-loop error time-update for a first-order loop is shown to be [65]

$$\Delta\tau_{k+1} = (1 - 4B_L T_{\text{sub}})\Delta\tau_k + K_L D_k, \tag{4.4}$$

where B_L is the loop noise-equivalent bandwidth and K_L is the loop gain. To achieve the desired loop noise-equivalent bandwidth, K_L must be normalized according to

$$K_L = \left.\frac{4B_L T_{\text{sub}}\Delta\tau_k}{\mathbb{E}\{D_k\}}\right|_{\Delta\tau_k=0}. \tag{4.5}$$

Using (4.2), the loop noise gain for a coherent baseband discriminator becomes $K_L = \frac{4B_L T_{\text{sub}}}{k_{\text{SSS}}}$.

Assuming zero-mean tracking error, i.e., $\mathbb{E}\{\Delta\tau_k\} = 0$, the variance time-update is given by

$$\text{var}\{\Delta\tau_{k+1}\} \triangleq (1 - 4B_L T_{\text{sub}})^2 \text{var}\{\Delta\tau_k\} + K_L^2 \text{var}\{D_k\}. \tag{4.6}$$

At steady state, $\text{var}\{\Delta\tau\} = \text{var}\{\Delta\tau_{k+1}\} = \text{var}\{\Delta\tau_k\}$; hence,

$$\text{var}\{\Delta\tau\} = \frac{B_L\, g(t_{\text{eml}})}{8(1 - 2B_L T_{\text{sub}}) W_{\text{SSS}}^2 C/N_0}, \tag{4.7}$$

$$g(t_{\text{eml}}) \triangleq \frac{[1 - \text{sinc}(t_{\text{eml}})]}{\left[2\frac{\sin(\pi t_{\text{eml}}/2)}{\pi t_{\text{eml}}^2} - \frac{\cos(\pi t_{\text{eml}}/2)}{t_{\text{eml}}}\right]^2}. \tag{4.8}$$

From (4.7), it can be seen that the standard deviation of the ranging error is related to the correlator spacing through $g(t_{\text{eml}})$. Fig. 4.3 shows $g(t_{\text{eml}})$ for $0 \leq t_{\text{eml}} \leq 2$. It can be seen that $g(t_{\text{eml}})$ is not a linear function, and it increases significantly faster when $t_{\text{eml}} > 1$. Therefore, to achieve a relatively high ranging precision, t_{eml} must be set to be less than 1. It is worth mentioning that for the GPS C/A code with an infinite bandwidth, $g(t_{\text{eml}}) = t_{\text{eml}}$.

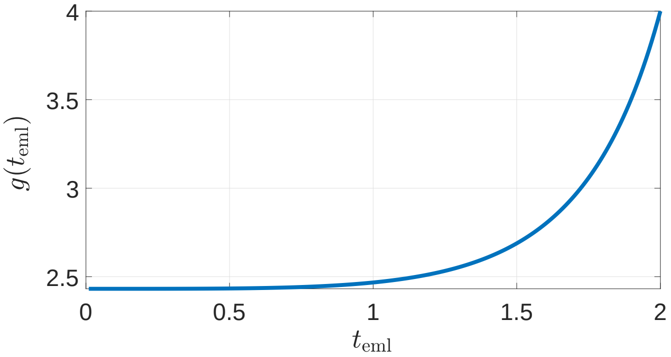


Figure 4.3: The standard deviation of the ranging error $\Delta\tau$ is related to the correlator spacing through $g(t_{\text{eml}})$, which is shown as a function of t_{eml}.

Fig. 4.4 shows the pseudorange error of a coherent DLL as a function of the carrier-to-noise ratio (C/N_0), with $B_L = \{0.005, 0.05\}$ Hz and $t_{\text{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$. It is worth mentioning that in Fig. 4.4, the bandwidth is chosen to be $B_L = \{0.005, 0.05\}$ Hz to enable the reader to compare the results with the standard GPS results provided in [69].

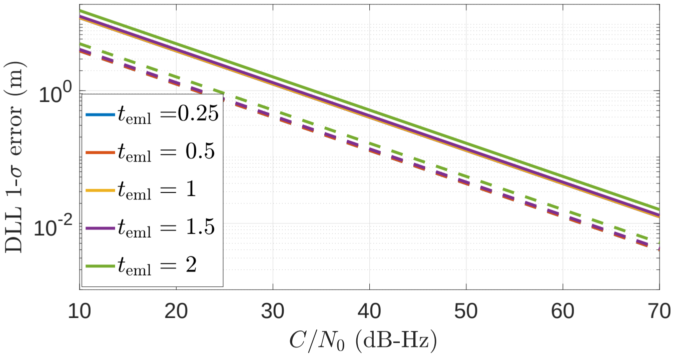


Figure 4.4: Coherent baseband discriminator noise performance as a function of C/N_0, for different t_{eml} values. Solid and dashed lines represent the results for $B_L = 0.05$ Hz and $B_L = 0.005$ Hz, respectively.

While the ranging accuracy of a coherent baseband DLL was evaluated in the presence of white noise, other sources of errors may affect the ranging accuracy. The effect of multipath, which is another significant source of error is discussed next.

Code Phase Error Analysis in Multipath Environments for a Coherent Discriminator Function

In general, the received signal in a multipath environment can be expressed as

$$r(t) = \sum_{l=0}^{L-1} \alpha_l(t) y(t - \tau_l(t)) + n(t), \tag{4.9}$$

where $y(t)$ is the transmitted data. Subsequently, the signal components of the early and late correlations are given by

$$\begin{aligned}
S_{e_k} &= \sqrt{C} \sum_{l=0}^{L-1} \alpha_l(t) \mathcal{R}\big[\Delta\tau_k - \frac{t_{\text{eml}}}{2} T_c - \tau_l(t)\big], \\
S_{l_k} &= \sqrt{C} \sum_{l=0}^{L-1} \alpha_l(t) \mathcal{R}\big[\Delta\tau_k + \frac{t_{\text{eml}}}{2} T_c - \tau_l(t)\big].
\end{aligned}$$

The discriminator function may be attenuated in a multipath channel, and the amount of attenuation depends on α_l and τ_l. In general, obtaining a closed-form expression for the pseudorange error from the DLL in a multipath environment is intractable. In this subsection, the performance of a DLL tracking the SSS code phase with a coherent discriminator function in a multipath environment is characterized numerically.

The considered scenario assumes a channel with only one multipath component with $\alpha_0 = 1$ and $\alpha_1 = 0.2512e^{j\phi}$ (i.e., the multipath amplitude is 6 dB lower than the LOS amplitude). The effect of the delay of the reflected signal (τ_1) on the pseudorange estimation performance is evaluated for $\phi = \{0, \pi\}$, i.e., for constructive and destructive interference, respectively. Moreover, since the goal is to assess the ranging performance in a multipath environment, no noise was added to the simulated signals. The zero-crossing point of the discriminator function was calculated using Newton's iterative method. The resulting pseudorange error is shown in Fig. 4.5 as a function of the relative path delay (in meters) and for different t_{eml} values.

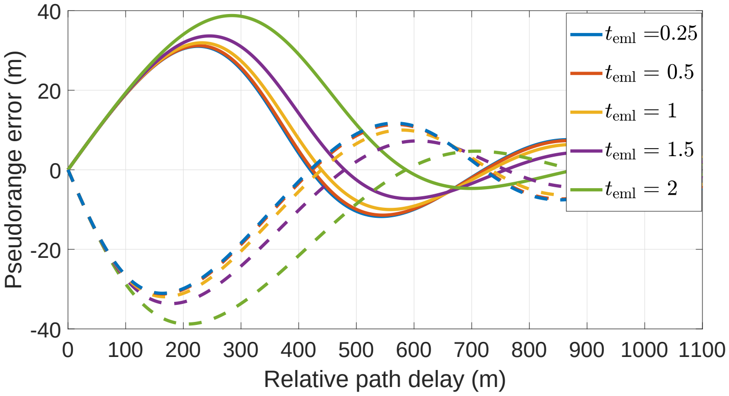


Figure 4.5: Pseudorange error for a channel with one multipath component with an amplitude that is 6 dB lower than the amplitude of the LOS signal. The error is plotted as a function of the path delay (in meters) and for different t_{eml} values. The solid and dashed lines represent constructive and destructive interferences, respectively.

4.1.2 Noncoherent Discriminator Function

This Section analyzes the ranging precision of LTE's SSS signals with noncoherent discriminator functions, which avoids the dependency on carrier phase tracking.

Correlation Signal Model

Denote the correlation of the received signal with the early, prompt, and late locally generated signals at time $t = kT_{\text{sub}}$ as

$$Z_{x_k} = I_{x_k} + jQ_{x_k},$$

where x can be either e, p, or l representing early, prompt, or late correlations, respectively. Assuming the receiver's signal acquisition stage to provide a reasonably accurate estimate of f_D, the in-phase and quadrature components of the early, prompt, and late correlations can be written as

$$\begin{aligned}
I_{x_k} &= \sqrt{C}\mathcal{R}\left(\Delta\tau_k + \kappa\frac{t_{\text{eml}}}{2}T_c\right)\cos(\Delta\phi_k) + \eta_{I,x_k},\\
Q_{x_k} &= \sqrt{C}\mathcal{R}\left(\Delta\tau_k + \kappa\frac{t_{\text{eml}}}{2}T_c\right)\sin(\Delta\phi_k) + \eta_{Q,x_k},
\end{aligned}$$

where x is e, p, or l and κ is -1, 0, or 1 for early, prompt, and late correlations, respectively. It can be shown that the noise components η_{I,x_k} and η_{Q,x_k} of the correlations have: (1) uncorrelated in-phase and quadrature samples, (2) uncorrelated samples at different time,

(3) zero-mean, and (4) the following variances and covariances

$$\mathrm{var}\{\eta_{I,x_k}\} = \mathrm{var}\{\eta_{Q,x_k}\} = \frac{N_0}{4T_{\mathrm{sub}}}, \tag{4.10}$$

$$\mathbb{E}\{\eta_{I,e_k}\eta_{I,l_k}\} = \mathbb{E}\{\eta_{Q,e_k}\eta_{Q,l_k}\} = \frac{N_0\mathcal{R}(t_{\mathrm{eml}}T_c)}{4T_{\mathrm{sub}}},$$

$$\mathbb{E}\{\eta_{I,x'_k}\eta_{I,p_k}\} = \mathbb{E}\{\eta_{Q,x'_k}\eta_{Q,p_k}\} = \frac{N_0\mathcal{R}(\frac{t_{\mathrm{eml}}}{2}T_c)}{4T_{\mathrm{sub}}}, \tag{4.11}$$

where x' is e or l.

Open-Loop Statistics of the Code Phase Error for a Dot-Product Discriminator Function

The dot-product discriminator function is defined as

$$D_k \triangleq (I_{e_k} - I_{l_k})I_{p_k} + (Q_{e_k} - Q_{l_k})Q_{p_k} \triangleq S_k + N_k,$$

where S_k is the signal component of the dot-product discriminator given by

$$S_k = C\mathcal{R}(\Delta\tau_k)\left\{\mathcal{R}\left(\Delta\tau_k - \frac{t_{\mathrm{eml}}}{2}T_c\right) - \mathcal{R}\left(\Delta\tau_k + \frac{t_{\mathrm{eml}}}{2}T_c\right)\right\},$$

and N_k is the noise component of the discriminator function, which has zero-mean. Fig. 4.6(a) shows S_k/C for $t_{\mathrm{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$. It can be seen that the signal component of the discriminator function is non-zero for $\Delta\tau_k/T_c > (1 + t_{\mathrm{eml}}/2)$; which is in contrast to being zero for GPS C/A code with infinite bandwidth. This is due to the sinc autocorrelation function of the SSS versus the triangular autocorrelation function of the GPS C/A code.

For small values of $\Delta\tau_k$, the discriminator function can be approximated by a linear function

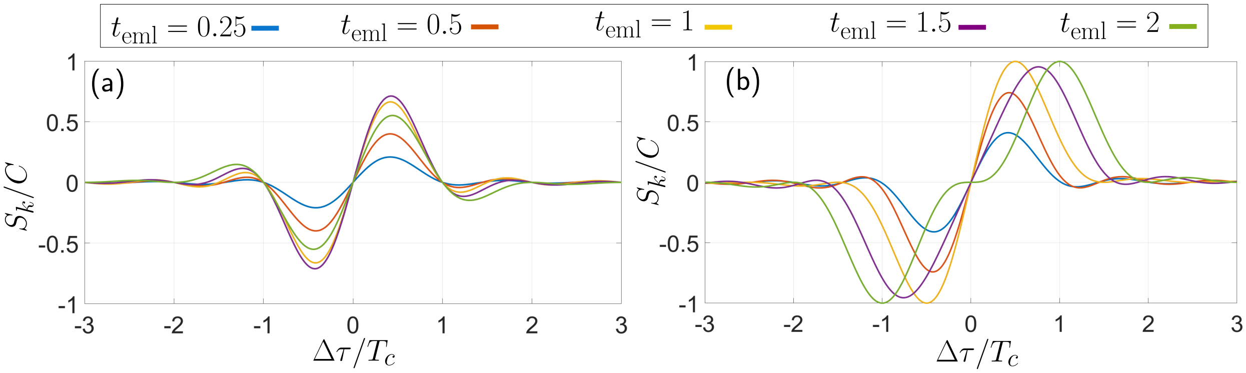


Figure 4.6: Signal component of (a) dot-product and (b) early-power-minus-late-power discriminator function for different correlator spacings.

according to

$$D_k \approx k_{\text{SSS}} \Delta\tau_k + N_k, \tag{4.12}$$

where $k_{\text{SSS}} \triangleq \frac{\partial D_k}{\partial \Delta\tau_k}\Big|_{\Delta\tau_k=0}$ and is given by

$$k_{\text{SSS}} = 4CW_{\text{SSS}} \left[\frac{\text{sinc}\left(\frac{t_{\text{eml}}}{2}\right) - \cos\left(\frac{\pi t_{\text{eml}}}{2}\right)}{t_{\text{eml}}} \right]. \tag{4.13}$$

The mean and variance of D_k are calculated to be

$$\mathbb{E}\{D_k\} = k_{\text{SSS}} \Delta\tau_k, \tag{4.14}$$

$$\begin{aligned} \text{var}\{D_k\} &= \text{var}\{N_k\}\Big|_{\Delta\tau_k=0} \\ &= \left(\frac{N_0^2}{4T_{\text{sub}}^2} + \frac{CN_0}{2T_{\text{sub}}} \right) [1 - \mathcal{R}(t_{\text{eml}} T_c)]\,. \end{aligned} \tag{4.15}$$

Open-Loop Statistics of the Code Phase Error for an Early-Power-Minus-Late-Power Discriminator Function

The early-power-minus-late-power discriminator function is defined as

$$D_k \triangleq I_{e_k}^2 + Q_{e_k}^2 - I_{l_k}^2 - Q_{l_k}^2 \triangleq S_k + N_k,$$

where S_k can be shown to be

$$S_k = C\left\{\mathcal{R}^2\left(\Delta\tau_k - \frac{t_{\text{eml}}}{2}T_c\right) - \mathcal{R}^2\left(\Delta\tau_k + \frac{t_{\text{eml}}}{2}T_c\right)\right\},$$

and N_k is the noise component of the discriminator function, which has zero-mean. Fig. 4.6(b) shows S_k/C of the early-power-minus-late-power discriminator function for $t_{\text{eml}} = \{0.25, 0.5, 1, 1.5, 2\}$.

The discriminator function can be approximated by a linear function for small values of $\Delta\tau_k$ (cf. (4.12)) with

$$k_{\text{SSS}} = 8CW_{\text{SSS}}\mathcal{R}\left(\frac{t_{\text{eml}}}{2}T_c\right)\left[\frac{\operatorname{sinc}\left(\frac{t_{\text{eml}}}{2}\right) - \cos\left(\frac{\pi t_{\text{eml}}}{2}\right)}{t_{\text{eml}}}\right]. \tag{4.16}$$

The mean and variance of D_k are calculated to be

$$\mathbb{E}\{D_k\} = k_{\text{SSS}}\Delta\tau_k, \tag{4.17}$$

$$\text{var}\{D_k\} = \frac{N_0^2}{2T_{\text{sub}}^2}\left[1 - \mathcal{R}^2\left(t_{\text{eml}}T_c\right)\right] + \frac{2CN_0}{T_{\text{sub}}}\mathcal{R}^2\left(\frac{t_{\text{eml}}}{2}T_c\right)\left[1 - \mathcal{R}\left(t_{\text{eml}}T_c\right)\right]. \tag{4.18}$$

Closed-Loop Statistics of the Code Phase Error for a Dot-Product Discriminator Function

Using a first-order DLL and at a steady-state, it can be shown that the closed-loop code phase error variance follows (4.6). The closed-loop code phase error in a dot-product discriminator can be obtained by substituting (4.13) and (4.15) into (4.6), yielding

$$\mathrm{var}\{\Delta\tau\} = \frac{B_L\, g_\alpha(t_{\mathrm{eml}}) \left(1 + \frac{1}{2T_{\mathrm{sub}}C/N_0}\right)}{16(1-2B_L T_{\mathrm{sub}})W_{\mathrm{SSS}}^2 C/N_0}, \tag{4.19}$$

where

$$g_\alpha(t_{\mathrm{eml}}) \triangleq \frac{t_{\mathrm{eml}}^2\,[1-\mathcal{R}(t_{\mathrm{eml}}T_c)]}{[\mathrm{sinc}\,(t_{\mathrm{eml}}/2) - \cos\,(\pi t_{\mathrm{eml}}/2)]^2}.$$

Fig. 4.7(a) shows $g_\alpha(t_{\mathrm{eml}})$ for $0 \leq t_{\mathrm{eml}} \leq 2$. It can be seen that $g_\alpha(t_{\mathrm{eml}})$ is a nonlinear function and increases significantly faster for $t_{\mathrm{eml}} > 1$. Fig. 4.8 shows the standard deviation of the pseudorange error for a dot-product DLL as a function of C/N_0 with $t_{\mathrm{eml}} = 1$ and $B_L = \{0.005, 0.05\}$ Hz, chosen as such in order to enable comparison with the GPS pseudorange error standard deviation provided in [66, 69].

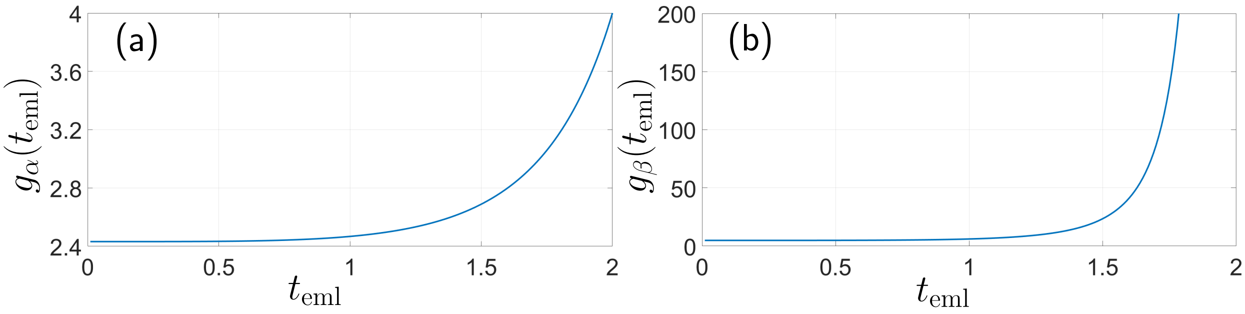


Figure 4.7: The variance of the ranging error in a dot-product discriminator is related to the correlator spacing through $g_\alpha(t_{\mathrm{eml}})$ shown in (a), while for an early-power-minus-late-power discriminator it is related through $g_\alpha(t_{\mathrm{eml}})$ and $g_\beta(t_{\mathrm{eml}})$ shown in (b).

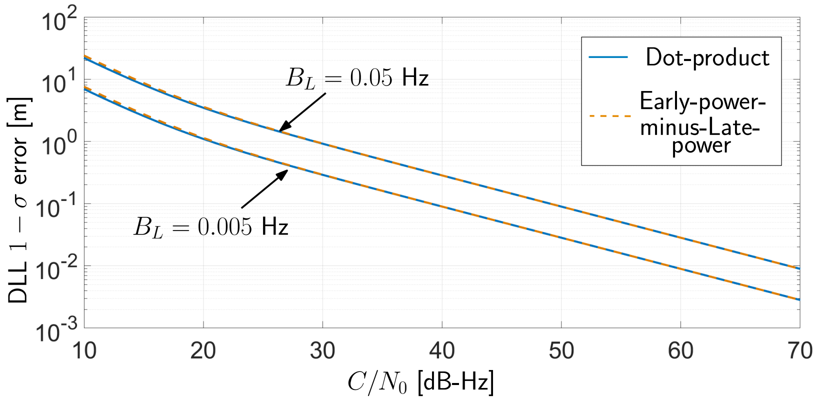


Figure 4.8: DLL performance as a function of C/N_0 for a dot-product discriminator (solid line) and an early-power-minus-late-power discriminator (dashed line), $B_L = \{0.05, 0.005\}$ Hz, and $t_{\text{eml}} = 1$.

Closed-Loop Statistics of the Code Phase Error for an Early-Power-Minus-Late-Power Discriminator Function

The variance of the ranging error in an early-power-minus-late-power discriminator can be obtained by substituting (4.16) and (4.18) into (4.6), yielding

$$\text{var}\{\Delta\tau\} = \frac{B_L\left[\frac{g_\beta(t_{\text{eml}})}{(C/N_0)} + 4T_{\text{sub}}g_\alpha(t_{\text{eml}})\right]}{64(1-2B_LT_{\text{sub}})T_{\text{sub}}W_{\text{SSS}}^2 C/N_0}, \tag{4.20}$$

where

$$g_\beta(t_{\text{eml}}) \triangleq \frac{1+\mathcal{R}\left(t_{\text{eml}}T_c\right)}{\mathcal{R}^2\left(\frac{t_{\text{eml}}}{2}T_c\right)} g_\alpha(t_{\text{eml}}).$$

Fig. 4.7(b) shows $g_\beta(t_{\text{eml}})$ for $0 \leq t_{\text{eml}} \leq 2$. It can be seen that $g_\beta(t_{\text{eml}})$ is significantly larger than $g_\alpha(t_{\text{eml}})$. To reduce the ranging error due to $g_\beta(t_{\text{eml}})$, t_{eml} must be chosen to be less than 1.5.

Fig. 4.8 shows the standard deviation of the pseudorange error for an early-power-minus-late-power discriminator DLL as a function of C/N_0 with $B_L = \{0.05, 0.005\}$ Hz and $t_{\text{eml}} = 1$.

It can be seen that decreasing the loop bandwidth decreases the standard deviation of the pseudorange error. However, very small values of B_L may cause the DLL to lose lock in a highly dynamic scenario.

Code Phase Error Analysis in Multipath Environments for a Noncoherent Discriminator Function

In order to evaluate the effect of multipath on the dot-product discriminator function performance, a multipath environment similar to the one in Subsection 4.1.1 is considered, where the channel consists of only one multipath component and one LOS component. The multipath signal amplitude is 6 dB lower than the LOS amplitude. Then, the effect of the delay of the reflected signal on the pseudorange estimation performance is evaluated for constructive and destructive interference. Since the goal is to assess the ranging performance in a multipath environment, no noise was added to the simulated signals. The zero crossing point of the discriminator function was calculated using Newton's method. The resulting pseudorange error for a dot-product discriminator is shown in Fig. 4.9 as a function of the relative path delay (in meters) for $t_{\text{eml}} = \{0.25, 0.5, 1, 1.5\}$. It was noted that the pseudorange errors for the early-power-minus-late-power discriminator were very close (within a few millimeters) to the plots in Fig. 4.9 for the same t_{teml} settings.

In what follows, some remarks outlining the major differences between a GPS and an LTE SSS-based receiver are presented.

Remark 1. The autocorrelation function of the GPS C/A code with an infinite bandwidth has a triangular shape, which is zero-valued for time delays greater than T_c. Therefore, for $\tau_l > (1 + t_{\text{eml}}/2)T_c$, multipath does not introduce any errors in the pseudorange. However, the autocorrelation function of the SSS is a sinc function, which has non-zero values for time delays higher than $(1 + t_{\text{eml}}/2)T_c$. Consequently, there will always be multipath-induced

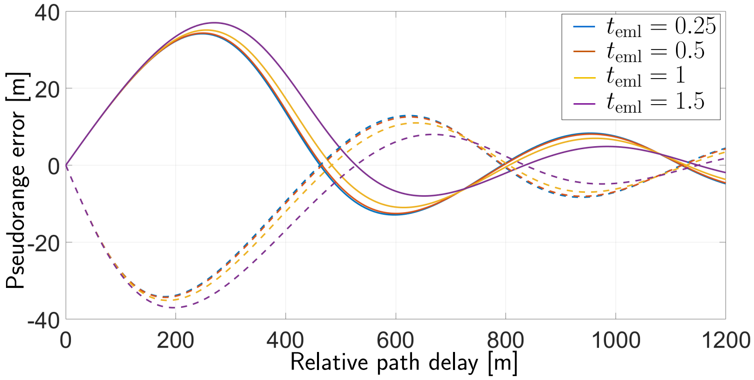


Figure 4.9: Pseudorange error for a dot-product discriminator for a channel with one multipath component with an amplitude that is 6 dB lower than the amplitude of the LOS signal. The error is plotted as a function of the path delay (in meters) and for different t_{eml} values. The solid and dashed lines represent constructive and destructive interferences, respectively. Pseudorange errors for an early-power-minus-late-power discriminator are almost identical.

pseudorange errors when tracking the SSS in multipath environments, even in the case of long-delay multipath (see Fig. 4.5).

Remark 2. In a GPS receiver with an infinite bandwidth in a noise-free environment, decreasing the correlator spacing, t_{eml}, always reduces the pseudorange error. In practice, due to the band-limiting effect of the receiver, the correlator spacing should be greater than the reciprocal of the receiver bandwidth. In an LTE receiver, on the other hand, decreasing the correlator spacing may either (1) reduce the pseudorange error if the signal is subject to channel noise only or if it is in a short-delay multipath environment or (2) increase the pseudorange error if the receiver is in a long-delay multipath environment.

4.2 CRS-Based Receiver

In this section, the open-loop statistics of the code and carrier phase errors are derived for LTE CRS signals. Using (4.6), the results can be simply extended to the closed-loop statistics, which are eliminated from this section.

4.2.1 Code Phase Statistics

Open-Loop Statistics of the Code Phase Error

In a multipath-free and noise-free environment, the point at which the discriminator function is zero represents the TOA. However, noise can move the zero crossing point as

$$\tilde{e}_\tau = \frac{N_{\text{DLL}}}{k_{\text{DLL}}}, \tag{4.21}$$

where

$$k_{\text{DLL}} = \left.\frac{\partial D_{\text{DLL}}(\tilde{e}_\tau, \xi)}{\partial \tilde{e}_\tau}\right|_{\substack{\tilde{e}_\tau \approx 0 \\ \xi = 1/2}} = \frac{4\pi C \cos(\frac{\pi}{2M})}{M\left(\sin(\frac{\pi}{2M})\right)^3}. \tag{4.22}$$

Therefore, the open-loop code phase error due to noise is a random variable with zero-mean and variance

$$\sigma^2_{\tilde{e}_\tau} = \frac{\text{var}[N_{\text{DLL}}]}{k^2_{\text{DLL}}} \approx \frac{\pi^2}{128MC/N_0}, \tag{4.23}$$

which is obtained by assuming $M \gg 1$ and carrier-to-noise ratio $C/N_0 \gg 1$ dB-Hz and defining the power spectral density of noise as $S_n(f) \triangleq N_0/2 = \sigma^2$. Fig. 4.10 plots the standard deviation of the pseudorange error as a function of C/N_0 for different values of N_c. The results show that the pseudorange error improves significantly as the number of subcarriers N_c in the LTE signal increases.

Time Integration

From (4.23), it can be seen that one of the parameters affecting the pseudorange error is the discriminator function's noise component. It can be shown that the average of I

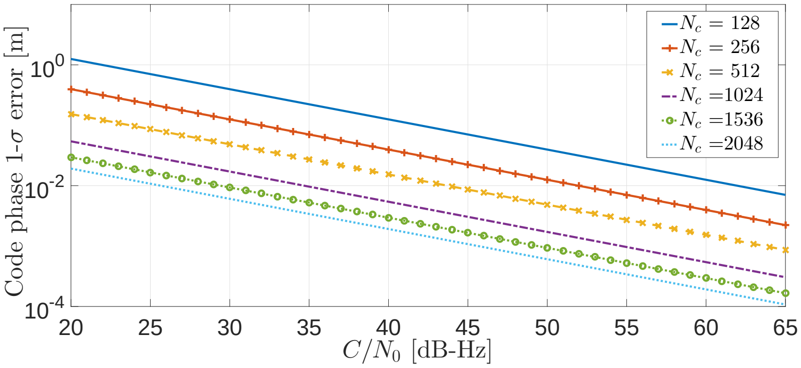


Figure 4.10: Standard deviation of the code phase error as a function of the C/N_0 for a different number of subcarriers N_c

independent and identically distributed (i.i.d.) random variables reduces the variance by a factor of I. This property can be used to reduce the code phase error variance. By averaging the discriminator functions over I different symbols, the overall DLL discriminator function is obtained as

$$D_{\text{tot}} \triangleq \frac{1}{I} \sum_{i \in I_{CRS}} D_{\text{DLL}_i} = M^2 C \Lambda_{\text{DLL}}(\tilde{e}_\tau, \xi) + N_{\text{tot}}, \tag{4.24}$$

where I_{CRS} is the set of symbols over which integration is performed and contains CRS, $I = \text{card}\,(I_{CRS})$, where card$\,(\cdot)$ is the cardinality of the set, and

$$N_{\text{tot}} = \frac{1}{I} \sum_{i \in I_{CRS}} N_{\text{DLL}_i}.$$

It can be shown that $\{N_{\text{DLL}_i}\}_{i \in I_{CRS}}$ is i.i.d. with zero-mean and variance given in (3.17). Therefore, N_{tot} is zero-mean with variance var$[N_{\text{tot}}] =$ var$[N_{\text{DLL}}]/I$. Using the discriminator function (4.24), it can be shown that the code phase error after averaging is a random variable with zero-mean and variance

$$\sigma^2_{\tilde{e}_\tau} \approx \frac{\pi^2}{128 M I C/N_0}, \tag{4.25}$$

which is decreased by a factor of I compared to (4.23). Since the CRS is transmitted on multiple symbols in a frame, it is possible to take the average over the symbols carrying the CRS in only one frame and keeping the DLL loop update time equal to a frame duration. However, increasing I too much may result in loss of coherence due to unknown receiver motion and clock drift. Consequently, a very long integration time may degrade the estimation performance. The use of a dead-reckoning (DR)-type sensor may help compensate for receiver motion. On the other hand, the magnitude of the clock drift is determined solely by the oscillator stability. While stable oscillators (e.g., oven-controlled crystal oscillators (OCXOs)) allow for longer integration time, they are expensive and large to install on cheap portable RF platforms. An integration time of 400 milliseconds may be achieved for a stationary receiver using cheap, small, but less stable oscillators (e.g., temperature-compensated crystal oscillators (TCXOs)) [70].

Code Phase Error Analysis in a Multipath Environment

In a multipath fading environment, the discriminator function can be expressed as [45]

$$D_{\text{DLL}} = M^2 C \Lambda_{\text{DLL}}(\tilde{e}_\tau, \xi) + N_{\text{DLL}} + \chi_1 + \chi_2 \tag{4.26}$$

where χ_1 and χ_2 represent the multipath channel effect on the discriminator function according to

$$\chi_1 = C \left| \sum_{m=0}^{M-1} \sum_{l=1}^{L-1} \alpha_l \, e^{-j2\pi(m/M)(\tau_l/T_s + \tilde{e}_\tau - \xi)} \right|^2 - C \left| \sum_{m=0}^{M-1} \sum_{l=1}^{L-1} \alpha_l \, e^{-j2\pi(m/M)(\tau_l/T_s + \tilde{e}_\tau + \xi)} \right|^2,$$

$$
\begin{aligned}
\chi_2 = 2\,C\,\Re\left\{\left[\sum_{m=0}^{M-1} e^{-j2\pi(m/M)(\tilde{e}_\tau-\xi)}\right]\cdot\left[\sum_{m'=0}^{M-1}\sum_{l=1}^{L-1}\alpha_l^* e^{j2\pi(m'/M)(\tau_l/T_s+\tilde{e}_\tau-\xi)}\right]\right\} \\
-\;2\,C\,\Re\left\{\left[\sum_{m=0}^{M-1} e^{-j2\pi(m/M)(\tilde{e}_\tau+\xi)}\right]\cdot\left[\sum_{m'=0}^{M-1}\sum_{l=1}^{L-1}\alpha_l^* e^{j2\pi(m'/M)(\tau_l/T_s+\tilde{e}_\tau+\xi)}\right]\right\},
\end{aligned}
$$

where $\Re\{\cdot\}$ represents the real part. It can be seen from (4.26) that multipath adds a bias to the discriminator function. Fig. 4.11 shows the code phase error in a multipath, but noise-free environment. The channel is assumed to have only two taps with the multipath amplitude 6 dB lower than the LOS' amplitude. The effect of the delay of the reflected signal, τ_1, on the pseudorange error is evaluated for constructive and destructive interferences, respectively. The results are obtained for different number of subcarriers. Fig. 4.11 shows that the pseudorange error reduces in both constructive and destructive channels when the bandwidth of the LTE signal increase. With $N_c = 2048$, the pseudorange error with constructive multipath interference is less than 50 cm.

4.2.2 Carrier Phase Statistics

Open-Loop Statistics of the Carrier Phase Error

In a noisy but multipath-free environment, noise can move the zero crossing point of the PLL discriminator function as

$$
\Delta_\phi = \frac{N_{\text{PLL}}}{k_{\text{PLL}}} \tag{4.27}
$$

where $k_{\text{PLL}} = 1$. Therefore, the open-loop carrier phase error due to noise is a random variable with zero-mean and variance

$$
\sigma^2_{\Delta\phi} = \frac{1}{4MC/N_0}\left(1+\frac{1}{4MC/N_0}\right).
$$

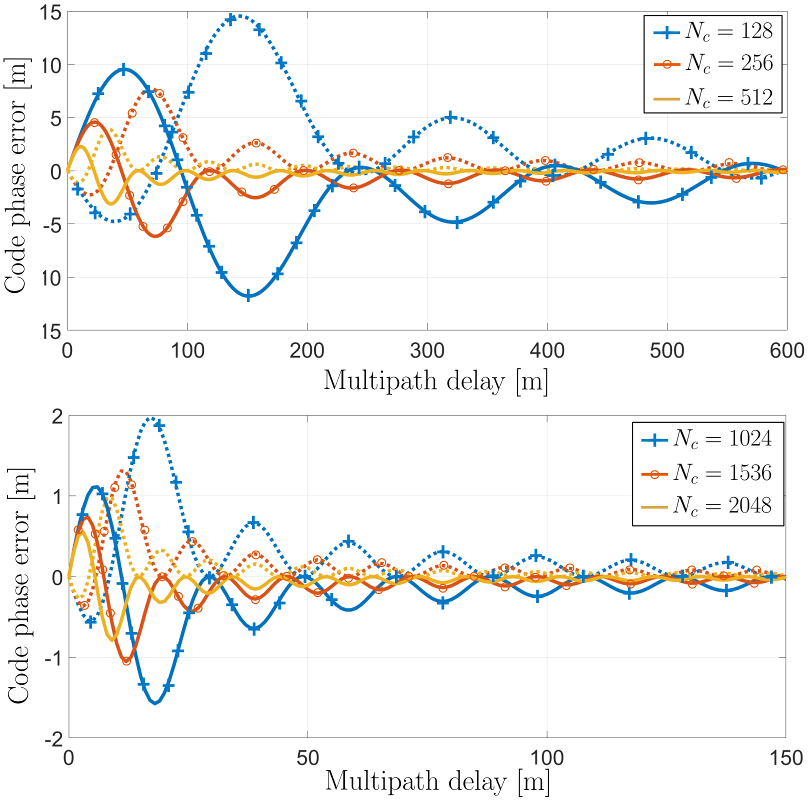


Figure 4.11: Code phase error for a multipath channel with $\alpha_0 = 1$ and $\alpha_1 = 0.2512$ and for different number of subcarriers. The solid and dashed lines represent constructive and destructive interferences, respectively.

Fig. 4.12 plots the standard deviation of the carrier phase error as a function of C/N_0 for different values of N_c. The results show that the carrier error improves significantly as the number of subcarriers N_c in the LTE signal increases.

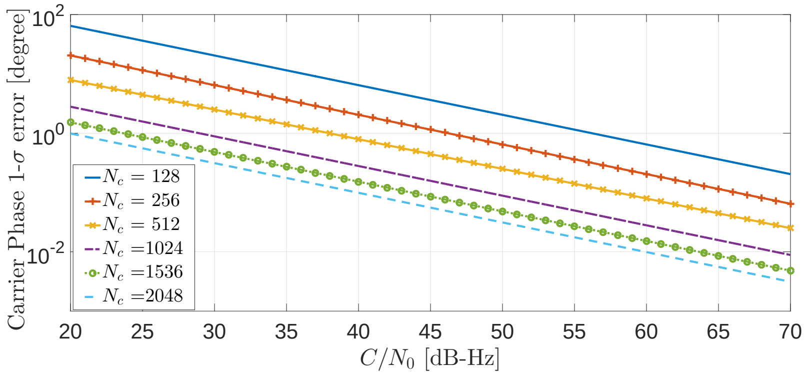


Figure 4.12: Standard deviation of the carrier phase error as a function of the C/N_0 for a different number of subcarriers N_c

Carrier Phase Error in a Multipath Environment

In a multipath fading environment, the PLL discriminator function can be expressed as

$$D_{\mathrm{PLL}} = \arg\left[M\sqrt{C}e^{j\Delta\phi} + \chi_{\mathrm{PLL}} + \text{noise}\right],$$

$$\text{for} \quad k = m\Delta_{\mathrm{CRS}} + \kappa, \quad m = 0, \cdots, M-1,$$

where

$$\chi_{\mathrm{PLL}} = \sum_{m=0}^{M-1}\sum_{l=1}^{L-1}\sqrt{C}e^{j\Delta\phi}\alpha_l\, e^{-j2\pi(m/M)(\tau_l/T_s)}$$

Fig. 4.13 shows the carrier phase error in a multipath, but noise-free environment. The channel is assumed to be similar to Section 4.2.1. The results are obtained for a different number of subcarriers. Fig. 4.13 shows that the maximum carrier phase error for a different number of subcarriers is the same. However, for higher N_c, the carrier phase error drops faster as the multipath delay increases.

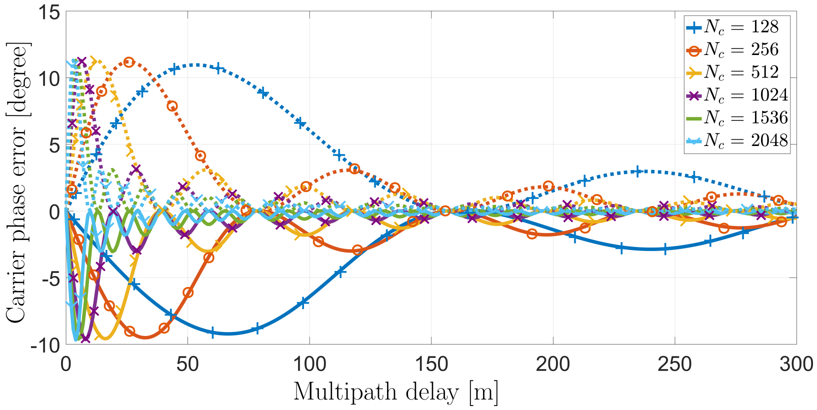


Figure 4.13: Carrier phase error for a multipath channel with $\alpha_0 = 1$ and $\alpha_1 = 0.2512$ and for a different number of subcarriers. The solid and dashed lines represent constructive and destructive interferences, respectively.

Chapter 5

Navigation Framework with LTE Signals

Chapter 3 presented the structure of the proposed SDR to extract navigation observables from cellular LTE SSS and CRS signals. This chapter proposes three frameworks to estimate the location of the UE using the derived navigation observables. Section 5.1 presents the navigation observables' models as functions of the UE's and eNodeBs' states. Section 5.2 and 5.3 propose two standalone navigation frameworks, where only statistical model is used to propagate the estimator's state. Section 5.4 uses IMU measurements to propagate the estimator's state between measurement updates from eNodeBs. The difference between Section 5.2 and 5.3 is that in Section 5.2, only code phase measurements are used to estimate the UE's position and velocity and the difference between the UE's clock bias and drift and those of the eNodeBs'. However, Section 5.3 uses single difference code and carrier phase and Doppler frequency measurements to estimate the UE's position and velocity. The advantages of each of these frameworks are discussed in details.

The results of this chapter have been published in [48, 49, 59, 71–73]

5.1 Navigation Observables Models

The LTE code phase measurement to the u-th eNodeB can be modeled as

$$\begin{aligned}&\rho^{(u)} = d^{(u)} + c\left(\delta t_\text{r} - \delta t_\text{s}^{(u)}\right) + \varepsilon_\rho^{(u)}, \qquad \text{[m]} \\ &\text{for} \quad u = 1, \cdots, U,\end{aligned} \tag{5.1}$$

where U is the total number of eNodeBs from which the receiver can extract measurements; $d^{(u)} \triangleq \left\|\boldsymbol{r}_\text{r} - \boldsymbol{r}_\text{s}^{(u)}\right\|$; $\boldsymbol{r}_\text{r} = [x_\text{r}, y_\text{r}, z_\text{r}]^\mathsf{T}$ and $\boldsymbol{r}_\text{s}^{(u)} = \left[x_\text{s}^{(u)}, y_\text{s}^{(u)}, z_\text{s}^{(u)}\right]^\mathsf{T}$ are the UE's and the u-th eNodeB's 3-D position, respectively; c is the speed of light; δt_r and $\delta t_\text{s}^{(u)}$ are the UE's and the u-th eNodeB's clock biases, respectively; and $\varepsilon_\rho^{(u)}$ is the code phase measurement noise, which is modeled as a zero-mean Gaussian random variable with a standard deviation of $\sigma_\rho^{(u)}$.

The LTE carrier phase measurement to the u-th eNodeB can be similarly modeled as

$$\begin{aligned}&\phi^{(u)} = d^{(u)} + c\left(\delta t_\text{r} - \delta t_\text{s}^{(u)}\right) + \lambda^{(u)} N^{(u)} + \varepsilon_\phi^{(u)}, \qquad \text{[m]} \\ &\text{for} \quad u = 1, \cdots, U,\end{aligned} \tag{5.2}$$

where $\lambda^{(u)} = \frac{c}{f_c^{(u)}}$ is the signal's wavelength; $N^{(u)}$ is the integer ambiguity representing the number of cycles from the u-th eNodeB to the UE; and $\varepsilon_\phi^{(u)}$ is the carrier phase measurement noise, which is modeled as a zero-mean Gaussian random variable with a standard deviation of $\sigma_\phi^{(u)}$.

The LTE Doppler frequency measurement to the u-th eNodeB can be modeled as

$$\begin{aligned}&f_\text{D}^{(u)} = -\frac{1}{\lambda^{(u)}} \frac{\dot{\boldsymbol{r}}_\text{r}^\mathsf{T}\left(\boldsymbol{r}_\text{r} - \boldsymbol{r}_\text{s}^{(u)}\right)}{d^{(u)}} + \frac{c}{\lambda^{(u)}}\left(\dot{\delta} t_\text{r} - \dot{\delta} t_\text{s}^{(u)}\right) + \varepsilon_f^{(u)}, \qquad \text{[Hz]} \\ &\text{for} \quad u = 1, \cdots, U,\end{aligned} \tag{5.3}$$

where $\dot{\boldsymbol{r}}_{\mathrm{r}} = [\dot{x}_{\mathrm{r}}, \dot{y}_{\mathrm{r}}, \dot{z}_{\mathrm{r}}]^{\mathsf{T}}$ is the velocity of UE; $\dot{\delta t}_{\mathrm{r}}$ and $\dot{\delta t}_{\mathrm{s}}^{(u)}$ are the UE's and the u-th eNodeB's clock drifts, respectively; and $\varepsilon_{f}^{(u)}$ is the Doppler frequency measurement noise, which is modeled as a zero-mean Gaussian random variable with a standard deviation of $\sigma_{f}^{(u)}$.

It can be seen from (5.1), (5.2), and (5.3) that the UE's and the eNodeBs' clock biases, which are unknown to the UE, affect all the measurements. The effect of the UE's clock bias and drift, which is common in all the measurements, can be removed by subtracting the l-th eNodeB's measurement from other eNodeBs' measurements, which results in single difference measurements defined as

$$\begin{aligned}\rho^{(ul)} &\triangleq \rho^{(u)} - \rho^{(l)} \\ &= d^{(ul)} - c\delta t_{\mathrm{s}}^{(ul)} + \varepsilon_{\rho}^{(ul)},\end{aligned} \tag{5.4}$$

$$\begin{aligned}\phi^{(ul)} &\triangleq \phi^{(u)} - \phi^{(l)} \\ &= d^{(ul)} - c\delta t_{\mathrm{s}}^{(ul)} + \lambda^{(u)} N^{(u)} - \lambda^{(l)} N^{(l)} + \varepsilon_{\phi}^{(ul)},\end{aligned} \tag{5.5}$$

$$\begin{aligned}\dot{\rho}^{(ul)} &\triangleq \dot{\rho}^{(u)} - \dot{\rho}^{(l)} \\ &= -\frac{\dot{\boldsymbol{r}}_{\mathrm{r}}^{\mathsf{T}} \left(\boldsymbol{r}_{\mathrm{r}} - \boldsymbol{r}_{\mathrm{s}}^{(u)}\right)}{d^{(u)}} + \frac{\dot{\boldsymbol{r}}_{\mathrm{r}}^{\mathsf{T}} \left(\boldsymbol{r}_{\mathrm{r}} - \boldsymbol{r}_{\mathrm{s}}^{(l)}\right)}{d^{(l)}} - c\dot{\delta t}_{\mathrm{s}}^{(ul)} + \varepsilon_{\dot{\rho}}^{(ul)},\end{aligned} \tag{5.6}$$

where $(\cdot)^{(ul)} \triangleq (\cdot)^{(u)} - (\cdot)^{(l)}$ and $\dot{\rho}^{(u)} \triangleq \lambda^{(u)} f_{\mathrm{D}}^{(u)}$. The l-th eNodeB will be called the reference eNodeB.

5.2 Standalone LTE Navigation Solution with Code Phase Measurements

In this section, a navigation framework based on an extended Kalman filter (EKF) is proposed, where the code phase measurements presented in (5.1) are used to estimate the UE's position and velocity and the difference between the UE's clock bias and drift and those of the eNodeBs'. This is due to the fact that the UE and eNodeBs' clock biases are unknown at the UE and must be estimated.

First, the state and dynamic models are discussed. Then, experimental hardware and software setup are presented. Next, two experimental results are demonstrated. In the first experiment, an SSS-based SDR is compared with a CRS-based SDR with a threshold-based tracking approach. The results show that the CRS-based SDR outperforms the SSS-based one significantly due to the higher transmission bandwidth of the CRS signals. In the second experiment, the performance of the CRS-based SDR with a tracking loop is compared to the state-of-the-art showing lower computational complexity and higher accuracy and precision of the proposed SDR. Finally, the concluded remarks from the presented experimental results are provided.

5.2.1 State and Dynamic Model

The UE is assumed to move in a two-dimensional (2-D) plane with known height, i.e., $z_{\mathrm{r}}(j) = z_0$ and $\dot{z}_{\mathrm{r}}(j) = 0$, where z_0 is a known constant. Moreover, the receiver's 2-D position is assumed to evolve according to a velocity random walk, with the continuous-time (CT) dynamics given by

$$\ddot{x}_{\mathrm{r}}(t) = \tilde{w}_x, \quad \ddot{y}_{\mathrm{r}}(t) = \tilde{w}_y, \tag{5.7}$$

where $\tilde{w}_x$ and $\tilde{w}_y$ are zero-mean white noise processes with power spectral densities $\tilde{q}_x$ and $\tilde{q}_y$, respectively. The receiver's discrete-time (DT) dynamics are hence given by

$$\boldsymbol{x}_{\text{pv}}(j+1) = \mathbf{F}_{\text{pv}}\boldsymbol{x}_{\text{pv}}(j) + \boldsymbol{w}_{\text{pv}}(j), \tag{5.8}$$

where

$$\boldsymbol{x}_{\text{pv}} \triangleq \begin{bmatrix} x_{\text{r}} \\ y_{\text{r}} \\ \dot{x}_{\text{r}} \\ \dot{y}_{\text{r}} \end{bmatrix}, \quad \mathbf{F}_{\text{pv}} = \begin{bmatrix} 1 & 0 & T & 0 \\ 0 & 1 & 0 & T \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

where $T \equiv T_f$ is the measurement's sampling time and $\boldsymbol{w}_{\text{pv}}$ is a DT zero-mean white sequence with covariance $\mathbf{Q}_{\text{pv}}$, where

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

The UE's clock bias and drift are assumed to evolve according to the following DT dynamics

$$\boldsymbol{x}_{\text{clk}_\text{r}}(j+1) = \mathbf{F}_{\text{clk}}\boldsymbol{x}_{\text{clk}_\text{r}}(j) + \boldsymbol{w}_{\text{clk}_\text{r}}(j), \tag{5.9}$$

where

$$\boldsymbol{x}_{\text{clk}_\text{r}} \triangleq \begin{bmatrix} c\delta t_{\text{r}} \\ c\dot{\delta} t_{\text{r}} \end{bmatrix}, \quad \mathbf{F}_{\text{clk}} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \quad \boldsymbol{w}_{\text{clk}_\text{r}} = \begin{bmatrix} w_{\delta t_{\text{r}}} \\ w_{\dot{\delta} t_{\text{r}}} \end{bmatrix},$$

where $\boldsymbol{w}_{\text{clk}_\text{r}}$ is the process noise, which is modeled as a DT zero-mean white sequence with covariance $\mathbf{Q}_{\text{clk}_{\text{r}}}$ with

$$\mathbf{Q}_{\text{clk}_r} = \left[\begin{array}{cc} S_{\tilde{w}_{\delta t_{\text{r}}}} T + S_{\tilde{w}_{\dot{\delta t}_{\text{r}}}} \frac{T^3}{3} & S_{\tilde{w}_{\dot{\delta t}_{\text{r}}}} \frac{T^2}{2} \\ S_{\tilde{w}_{\dot{\delta t}_{\text{r}}}} \frac{T^2}{2} & S_{\tilde{w}_{\dot{\delta t}_{\text{r}}}} T \end{array}\right].$$

The terms $S_{\tilde{w}_{\delta t_{\text{r}}}}$ and $S_{\tilde{w}_{\dot{\delta t}_{\text{r}}}}$ are the clock bias and drift process noise power spectra, respectively, which can be related to the power-law coefficients $\{h_\alpha\}_{\alpha=-2}^{2}$, which have been shown through laboratory experiments to characterize the power spectral density of the fractional frequency deviation $y(t)$ of an oscillator from nominal frequency according to $S_y(f) = \sum_{\alpha=-2}^{2} h_\alpha f^\alpha$. A common approximation involves only the h_0 and h_{-2} parameters, namely $S_{\tilde{w}_{\delta t_{\text{r}}}} \approx \frac{h_{0_{\text{r}}}}{2}$ and $S_{\tilde{w}_{\dot{\delta t}_{\text{r}}}} \approx 2\pi^2 h_{-2_{\text{r}}}$ [74].

The u-th eNodeBs' clock states $\boldsymbol{x}_{\text{clk}_{\text{s}}}^{(u)}$ evolve according to the same dynamic model as the UE's clock state (5.9), except that the process noise is replaced with $\boldsymbol{w}_{\text{clk}_{\text{s}}}^{(u)} \triangleq \left[w_{\delta t_{\text{s}}}^{(u)}, w_{\dot{\delta t}_{\text{s}}}^{(u)}\right]^{\mathsf{T}}$, which is modeled as a DT zero-mean sequence with covariance $\mathbf{Q}_{\text{clk}_{\text{s}}}^{(u)}$ [75].

One of the main challenges in navigation with LTE signals is the unavailability of the eNodeBs' positions and clock states. It has been previously shown that the SOP position can be mapped with a high degree of accuracy, whether collaboratively or non-collaboratively [75, 76]. In what follows, the eNodeBs' positions are assumed to be known, and an EKF will be utilized to estimate the vehicle's position $\boldsymbol{r}_{\text{r}}$ and velocity $\dot{\boldsymbol{r}}_{\text{r}}$ simultaneously with the difference between the receiver and each eNodeB's clock bias and drift states. The difference between the receiver's clock state vector and the u-th eNodeB's clock state vector $\Delta\boldsymbol{x}_{\text{clk}}^{(u)} \triangleq \boldsymbol{x}_{\text{clk}_{\text{r}}} - \boldsymbol{x}_{\text{clk}_{\text{s}}}^{(u)}$ evolves according to

$$\Delta\boldsymbol{x}_{\text{clk}}^{(u)}(j+1) = \mathbf{F}_{\text{clk}}\Delta\boldsymbol{x}_{\text{clk}}^{(u)}(j) + \boldsymbol{w}_{\text{clk}}^{(u)}(j),$$

where $\boldsymbol{w}_{\text{clk}}^{(u)} \triangleq \left(\boldsymbol{w}_{\text{clk}_{\text{r}}} - \boldsymbol{w}_{\text{clk}_{\text{s}}}^{(u)}\right)$ is a DT zero-mean white sequence with covariance $\mathbf{Q}_{\text{clk}}^{(u)}$, where $\mathbf{Q}_{\text{clk}}^{(u)} \triangleq \mathbf{Q}_{\text{clk}_{\text{r}}} + \mathbf{Q}_{\text{clk}_{\text{s}}}^{(u)}$.

The augmented state vector which will be estimated by the EKF is defined as

$$\boldsymbol{x} \triangleq \left[\boldsymbol{x}_{\text{pv}}^{\mathsf{T}}, \Delta\boldsymbol{x}_{\text{clk}}^{(1)^{\mathsf{T}}}, \ldots, \Delta\boldsymbol{x}_{\text{clk}}^{(U)^{\mathsf{T}}}\right]^{\mathsf{T}}.$$

This vector has the dynamics

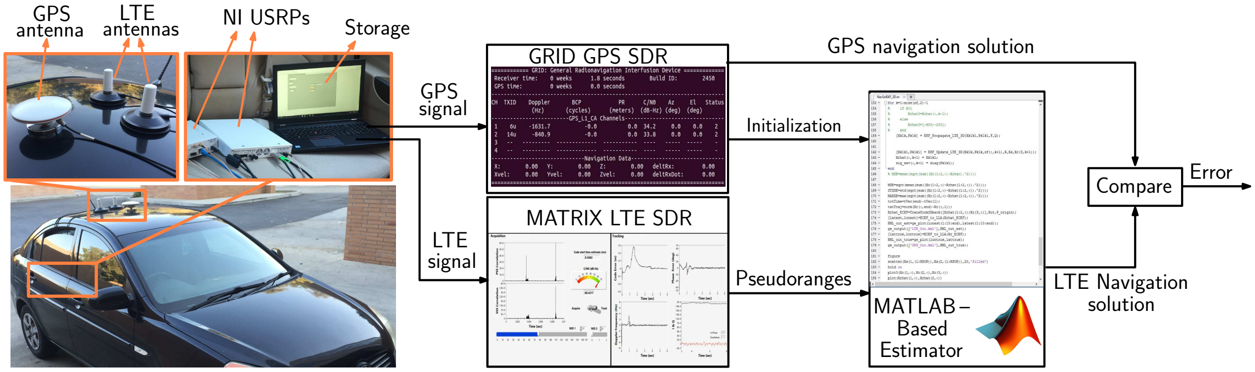
$$\boldsymbol{x}(j+1) = \mathbf{F}\boldsymbol{x}(j) + \boldsymbol{w}(j),$$

where $\mathbf{F} \triangleq \text{diag}\left[\mathbf{F}_{\text{pv}}, \mathbf{F}_{\text{clk}}, \ldots, \mathbf{F}_{\text{clk}}\right]$ and $\boldsymbol{w}$ is a DT zero-mean white sequence with covariance $\mathbf{Q} \triangleq \text{diag}\left[\mathbf{Q}_{\text{pv}}, \mathbf{Q}_{\text{clk}}\right]$ and

$$\mathbf{Q}_{\text{clk}} = \begin{bmatrix} \mathbf{Q}_{\text{clk}_\text{r}} + \mathbf{Q}_{\text{clk}_\text{s}}^{(1)} & \mathbf{Q}_{\text{clk}_\text{r}} & \cdots & \mathbf{Q}_{\text{clk}_\text{r}} \\ \mathbf{Q}_{\text{clk}_\text{r}} & \mathbf{Q}_{\text{clk}_\text{r}} + \mathbf{Q}_{\text{clk}_\text{s}}^{(2)} & \cdots & \mathbf{Q}_{\text{clk}_\text{r}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{Q}_{\text{clk}_\text{r}} & \mathbf{Q}_{\text{clk}_\text{r}} & \cdots & \mathbf{Q}_{\text{clk}_\text{r}} + \mathbf{Q}_{\text{clk}_\text{s}}^{(U)} \end{bmatrix}. \tag{5.10}$$

5.2.2 Experimental Hardware and Software Setup

To evaluate the performance of the navigation framework and the proposed SDRs, two field tests were conducted with real LTE signals in a suburban and urban environment. For this purpose, a mobile ground receiver was equipped with two types of antennas to acquire and track: (1) GPS signals and (2) LTE signals in different bands from nearby eNodeBs. The LTE antennas were consumer-grade 800/1900 MHz cellular omnidirectional antennas and the GPS antenna was a surveyor-grade Leica antenna. The LTE signals were simultaneously down-mixed and synchronously sampled via a dual-channel universal software radio peripheral (USRP)-2954R driven by a GPS-disciplined oscillator (GPSDO). LTE signals were sampled at a rate of 20 MSps. The GPS signals were collected on a separate NI single-channel USRP-2930 also driven by a GPSDO. It is worth mentioning that the GPSDO is only used to discipline the clock on the USRPs (which were not very stable without a GPSDO). Samples of the received signals were stored for off-line post-processing. The samples of the GPS signal were used to produce the vehicle's "ground truth" trajectory [77] and the LTE signals were processed by the proposed SSS- and CRS-based LTE SDRs. Fig. 5.1 shows the experimental hardware and software setup.



```
============ GRID: General Radionavigation Interfusion Device =============
 Receiver time:    0 weeks     1.8 seconds        Build ID:        2450
 GPS time:         0 weeks     0.0 seconds
---------------------------------------------------------------------------
CH  TXID   Doppler       BCP            PR     C/N0    Az     El   Status
            (Hz)       (cycles)      (meters) (dB-Hz) (deg)  (deg)
-------------------------GPS_L1_CA Channels--------------------------------
 1   6u   -1631.7          -0.0           0.0  34.2    0.0    0.0     2
 2  14u    -840.9          -0.0           0.0  33.8    0.0    0.0     2
 3  --   --------   -----------   ----------  ----   -----  -----     -
 4  --   --------   -----------   ----------  ----   -----  -----     -
-----------------------------Navigation Data-------------------------------
 X:        0.00   Y:        0.00   Z:        0.00   deltRx:          0.00
 Xvel:     0.00   Yvel:     0.00   Zvel:     0.00   deltRxDot:       0.00
===========================================================================
```

Figure 5.1: Experimental hardware and software setup

According to the LTE protocol, the modulated carrier frequency of LTE signals received from an eNodeB over 1 ms should be accurate to within ±50 parts per billion (ppb) with respect to a reference [78]. This reference is typically obtained by using OCXOs in the eNodeBs and the signals transmitted by GNSS. However, when GNSS signals are not available or reliable (e.g., in deep urban canyons), other standards (e.g., synchronous ethernet) could be used to transfer synchronization signals to the eNodeBs [78, 79].

The clock error dynamics modeled in (5.9) is only valid for a GPSDO over short periods of time. When the measurement rate is significantly higher than the GPSDO correction rate, it can be assumed that the clock follows the model presented in Section 5.2.1 between each GPSDO correction. In this dissertation, the measurements are obtained every 10 ms, while the GPSDO correction is performed usually less than once per second. Therefore, using the model in (5.9) is practical. The eNodeBs' clocks were modeled as OCXOs with $\{h_{0_{\text{s}}}\}_{i=1}^{N} = 2.6 \times 10^{-22}$ and $\{h_{-2_{\text{s}}}\}_{i=1}^{N} = 4 \times 10^{-26}$, while the UE's clock was modeled as a TCXO with $h_{0_{\text{r}}} = 9.4 \times 10^{-20}$ and $h_{-2_{\text{r}}} = 3.8 \times 10^{-21}$.

5.2.3 Experimental Results: SSS-Based vs. CRS-Based SDR

This experiment was performed in a suburban environment in Colton, CA, USA. Over the course of the experiment, the vehicle-mounted receiver traversed a total trajectory of 2 km while listening to 2 eNodeBs simultaneously. The LTE UE was tuned to 1955 and 2145 MHz carrier frequencies, which were allocated to USA providers AT&T and T-Mobile, respectively, and the transmission bandwidth was measured to be 20 MHz.

Pseudorange Measurements

In this subsection, the quality of the pseudoranges obtained by the SSS- and the CRS-based SDRs are evaluated. To this end, the change in the pseudorange between the receiver and eNodeB 1 and 2 was calculated using the SSS- and CRS-based SDRs. The result is plotted for each eNodeB in Fig. 5.2 and Fig. 5.4, respectively. The change in true range calculated from the GPS solution is also shown in these figures. The pseudorange error obtained from SSS-based SDR had a standard deviation of 32.72 m for eNodeB 1 and 37.49 m for eNodeB 2. The pseudorange error obtained from the CRS-based SDR had a standard deviation of 5.14 m for eNodeB 1 and 6.01 m for eNodeB 2. Fig. 5.3 and 5.5 show the pseudorange error and its cumulative distribution function (CDF) obtained by SSS- and CRS-based SDRs for eNodeB 1 and eNodeB 2, respectively.

Fig. 5.2 and Fig. 5.4 show that the main cause of error in the pseudorange obtained by tracking the SSS signal is due to multipath. The estimated CIR at $t = 13.04$ s for eNodeB 1 and $t = 8.89$ s for eNodeB 2 (Fig. 5.2 and Fig. 5.4, respectively) show several peaks resulting from multipath. These peaks are the main source of pseudorange error at $t = 13.04$ s for eNodeB 1 and $t = 8.89$ s for eNodeB 2, which are around 330 m and 130 m, respectively. Moreover, Fig. 5.2 and Fig. 5.4 show that the CRS-based receiver has a significantly lower pseudorange error compared to the SSS-based receiver in multipath environments. It is

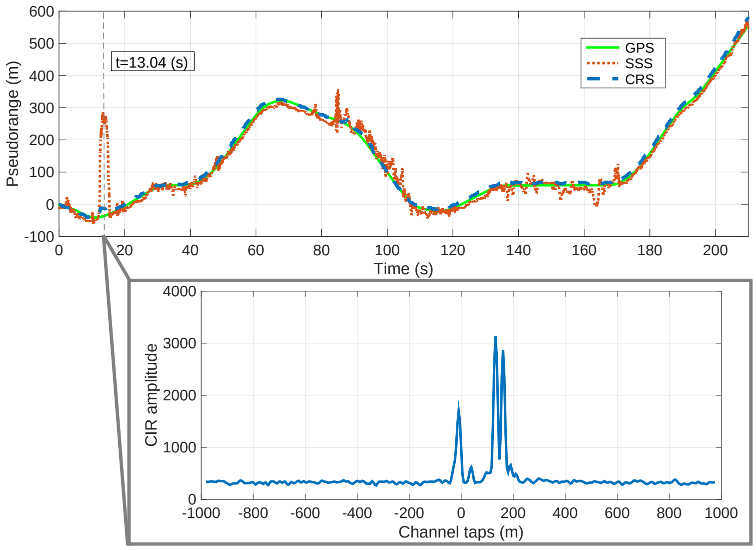


Figure 5.2: Estimated change in pseudorange and estimated CIR at $t = 13.04$ s for eNodeB 1. The change in the pseudorange was calculated using: (1) SSS pseudoranges, (2) CRS pseudoranges, and (3) true ranges obtained using GPS.

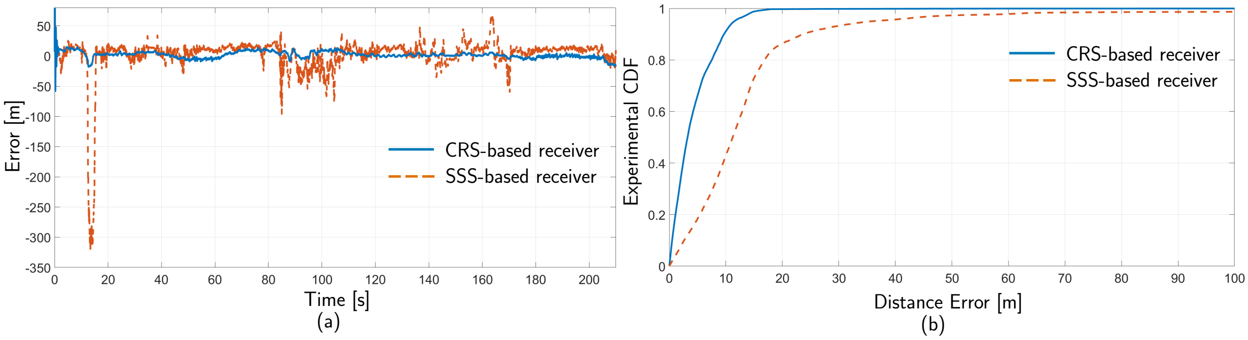


Figure 5.3: (a) Error in the change of the pseudorange obtained by LTE and GPS. (b) CDF of the distance error.

worth mentioning that in some environments with severe multipath, the LOS signal may have a significantly lower amplitude compared to the multipath signals. In this case, the CIR peak-detection threshold must be dynamically tuned in the receiver in order to detect the LOS peak. The pseudoranges shown in Fig. 5.2 and Fig. 5.4 are obtained by tuning the receiver threshold in post-processing. Fig. 5.6 shows the pseudorange obtained without dynamically adjusting the peak-detection threshold. An instance of having a LOS peak significantly lower than multipath peaks is shown in the estimated CIR at $t = 40.5$ s in Fig. 5.4. It can be seen from this estimated CIR that the LOS peak is at approximately -40 m,

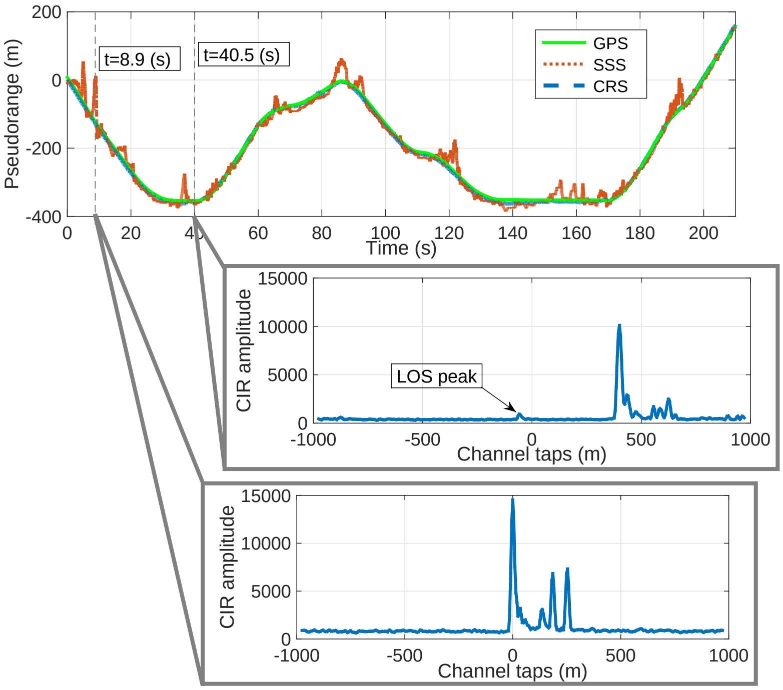


Figure 5.4: Estimated change in pseudorange and estimated CIR at $t = 8.89$ s and $t = 40.5$ s for eNodeB 2. The change in the pseudorange was calculated using: (1) SSS pseudoranges, (2) CRS pseudoranges, and (3) true ranges obtained using GPS.

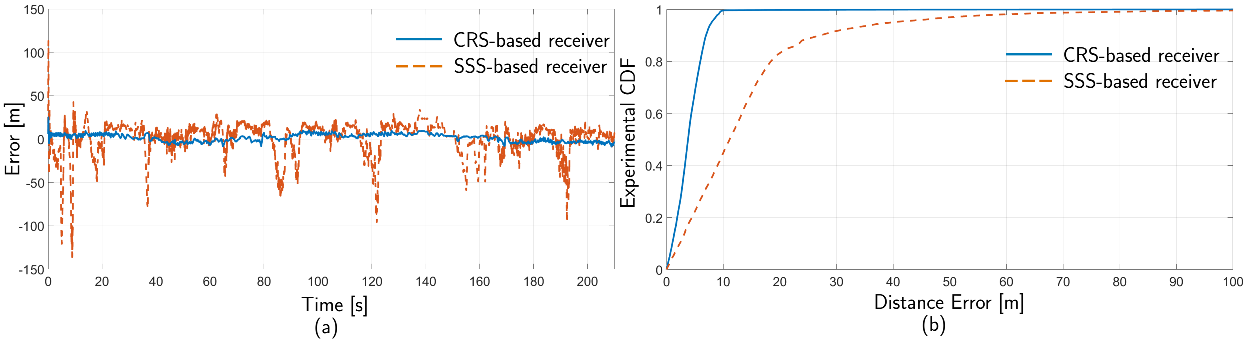


Figure 5.5: (a) Error in the change of the pseudorange obtained by LTE and GPS. (b) CDF of the distance error.

whereas the highest peak of the estimated CIR, which corresponds to a multipath signal, is at approximately 400 m. Consequently, an error of approximately 440 m due to multipath will be introduced into the pseudorange, as shown in 5.6.

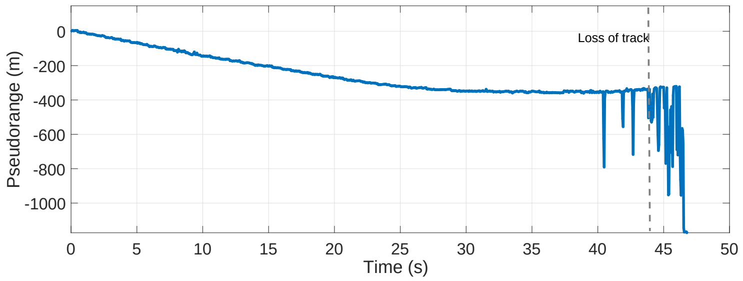


Figure 5.6: Tracking results for eNodeB 2: pseudorange obtained without dynamically tuning the peak-detection threshold

Navigation Solution

The second part of the experiment was to navigate using LTE signals exclusively and via the EKF framework discussed in the previous subsection. For this purpose, the receiver's position and velocity along with the difference of clock biases between the receiver and each eNodeB as well as the difference of clock drifts are estimated dynamically. To make the problem observable, it is assumed that the receiver has had access to GPS before navigating with LTE signals; hence, the receiver has full knowledge of its initial state [15].

The environment layout as well as the true and estimated receiver trajectories are shown in Fig. 5.7. The RMSE between the GPS and SSS-based navigation solutions along the traversed trajectory was calculated to be 50.46 m with a standard deviation of 41.07 m and a maximum error of 419.66 m. The RMSE between the GPS and CRS-based navigation solutions was calculated to be 9.32 m with a standard deviation of 4.36 m and a maximum error of 33.47 m. Theses results are summarized in Table 5.1.

Table 5.1: Experimental results [in meters] comparing navigation solutions obtained from SSS-based and CRS-based SDRs.

Receiver	**RMSE**	**Standard deviation**	**Maximum error**
SSS	50.46	41.07	419.66
CRS	9.32	4.36	33.47

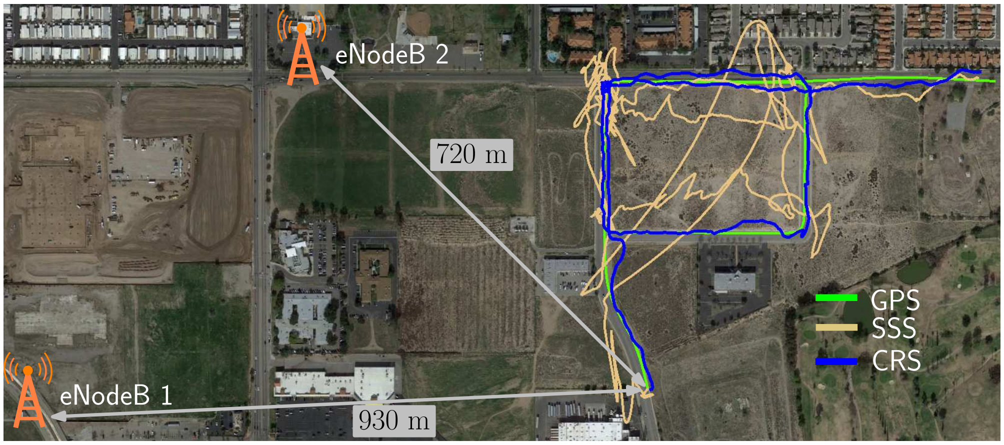


Figure 5.7: Receiver true and estimated trajectories and eNodeBs' locations.

5.2.4 Experimental Results: CRS-Based SDR vs. State-of-the-Art

In this experiment, the performance of the CRS-based SDR with tracking loop is evaluated and compared with the state-of-the-art apporaches. The experiment was conducted using a ground vehicle in an urban multipath environment: downtown Riverside, California. It is assumed that the receiver had access to GPS, and GPS was cut off at the start time of the experiment. Therefore, the EKF's states were initialized with the values obtained from the GPS navigation solution. The standard deviation of the initial uncertainty of position and velocity were set to be 5 m and 0.01 m/s, respectively [69]. The standard deviation of the initial uncertainty of the clock bias and drift were set to be 0.1 m and 0.01 m/s, respectively, which were obtained empirically. The process noise power spectral densities $\tilde{q}_x$ and $\tilde{q}_y$ were set to 0.1 (m^2/s^3) and the measurement noise standard deviation was set to 10 m^2, which were obtained empirically.

The DLL bandwidth was tuned between 0.05 and 0.2 Hz and the PLL bandwidth was tuned between 4 and 8 Hz. In order to choose the loop bandwidth, it is required to balance the performance in the presence of noise against the performance for a moving receiver. Low loop bandwidth improves the performance in the presence of noise by increasing the averaging time. However, a longer averaging time degrades the performance of a moving receiver. Experimental results revealed that the PLL with high loop bandwidth would fail to track signals with low C/N_0. Therefore, the PLL bandwidth has to be decreased for low C/N_0. To capture the dynamics of a moving receiver, the DLL loop bandwidth, on the other hand, must be increased. Typically, with high C/N_0, the PLL bandwidth can be increased and lower bandwidth for the DLL can be chosen.

The ESPRIT design parameter was set to $P = 0.5M$. The integration was performed over four consecutive OFDM symbols carrying CRS in four slots. The characteristics of the eNodeBs to which the receiver was listening during the experiment are presented in Table 5.2. The GPS navigation solution was produced from ten GPS satellites. Over the course of the experiment, the ground vehicle traversed a trajectory of 1.44 km in 90 s with an average speed of 16 m/s.

Table 5.2: ENodeBs' Characteristics

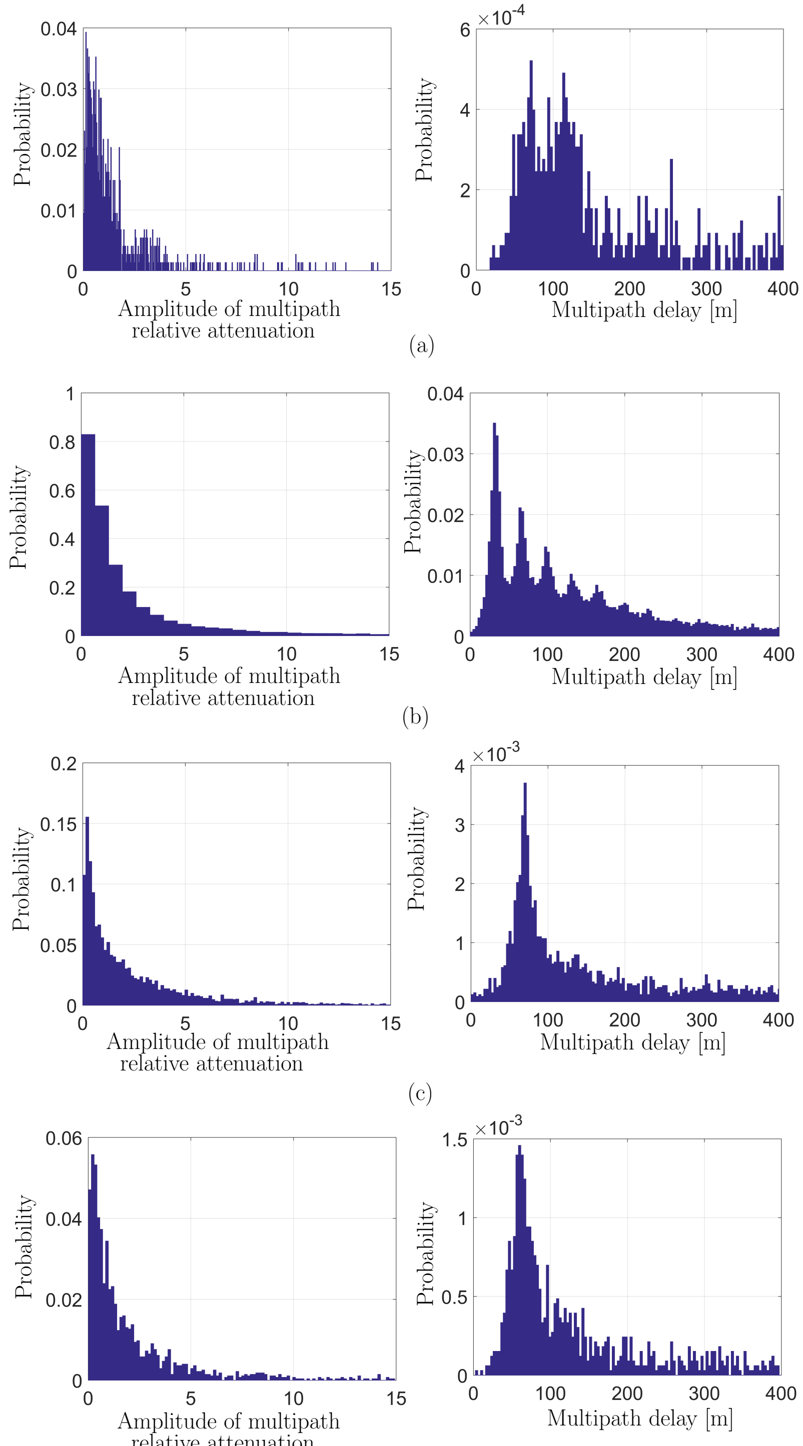
eNodeB	**Carrier frequency (MHz)**	$\boldsymbol{N_{ID}^{Cell}}$	**Bandwidth (MHz)**
1	739	152	10
2	1955	216	20
3	739	232	10
4	739	288	10

Pseudorange Measurements

In order to evaluate the channel condition, the ESPRIT algorithm was used to estimate the channel impulse response at each frame of the received LTE signal over the course of the experiment. Fig. 5.8 shows the probability of the relative (with respect to the first estimated path) attenuation and delay components of multipath for each eNodeB. The results showed that the average of the channel length L over the course of the experiment for eNodeBs 1–4 were 1.09, 4.29, 1.45, and 1.17, respectively, implying relatively less multipath compared to the extended typical urban (ETU) channel model with channel length of 9. In some environments, the received signal may be completely blocked resulting in a non-LOS signal. Differentiating the LOS signal from the NLOS signal is outside the scope of this dissertation, and the received signal with the lowest TOA is assumed to be the LOS signal.

The obtained pseudoranges with the proposed LTE SDR for each eNodeB are shown in Fig. 5.9(a) with dashed lines. The receiver had access to its actual position using the stored GPS signal. Therefore, the actual ranges of the receiver to each eNodeB was calculated and is shown in Fig. 5.9(a) with solid lines. To enable comparison, the initial values of the pseudoranges and actual ranges are removed in Fig. 5.9(a). It can be seen that the change in pseudoranges follows the actual ranges closely.

Fig. 5.9(b) shows the relative errors between the pseudoranges and their corresponding ranges. In this figure, it was assumed that the mean of each error is due to the difference of the clock biases between the receiver and the transmitter. Therefore, the mean of the obtained errors for each eNodeB was removed from the entire error, and the plotted errors have zero-mean. The results show that the standard deviation of the pseudorange errors for eNodeBs 1–4 are 4.55, 2.20, 1.96, and 2.04 m, respectively. The difference in the obtained standard deviations can be attributed to several factors, including: (1) different transmission bandwidth, (2) different multipath environment, and (3) different clock drifts. Fig. 5.9(c) shows the measured C/N_0 of the received signal from each eNodeB over the course of the experiment. It can be seen that eNodeB 1's C/N_0 drops to approximately 47 dB-Hz after 40 s. Fig. 5.9(d) shows the CIR of the received signal from eNodeB 1 at time instant 40 s. It can be seen that at this time instant, the noise level and multipath are significantly high



(a)

(b)

(c)

(d)

Figure 5.8: (a)–(d) The probability of the relative (with respect to the first estimated path) attenuation and delay components of the multipath over the course of experiment, for eNodeBs 1–4, respectively.

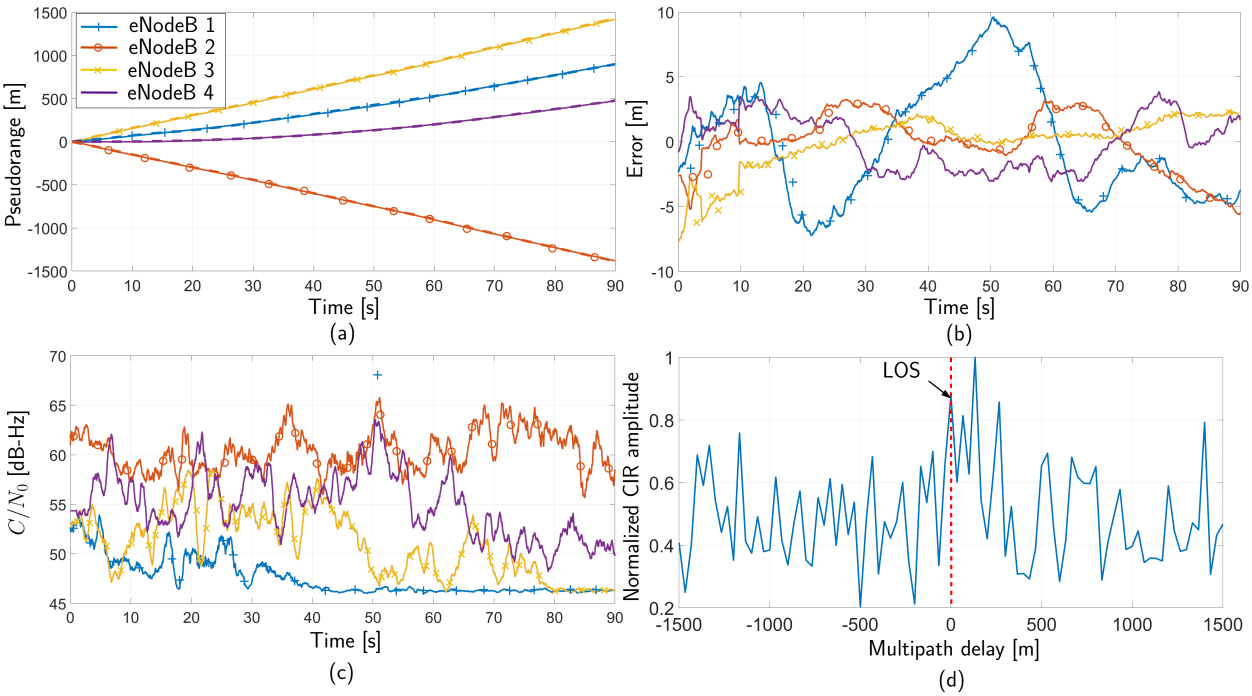


Figure 5.9: (a) Measured pseudoranges and actual ranges for each eNodeB, plotted with dashed and solid lines, respectively. The initial values were removed for comparison purposes. (b) The obtained error between the pseudoranges and the actual ranges, after removing the mean of the error. (c) Measured C/N_0 of the received signal from each eNodeB. (d) the normalized CIR of the received LTE signal from eNodeB 1 at time instant 40 s.

resulting in low C/N_0. Although multipath is severe for this received signal and the C/N_0 is low, the estimated pseudorange obtained by the proposed receiver still follows the actual range closely.

Fig. 5.10(a) and 5.10(b) show the tracking results for the carrier phase error and Doppler frequency, respectively, for eNodeB 3.

Navigation Solution

Fig. 5.11(a) shows the distance error between the navigation solution obtained by the LTE SDR and that of the GPS navigation solution over time. The experimental CDF of the error is shown in Fig. 5.11(b). The environment layout, the eNodeBs locations, and the entire trajectory are shown in Fig. 5.12. Table 5.3 summarizes the LTE navigation performance.

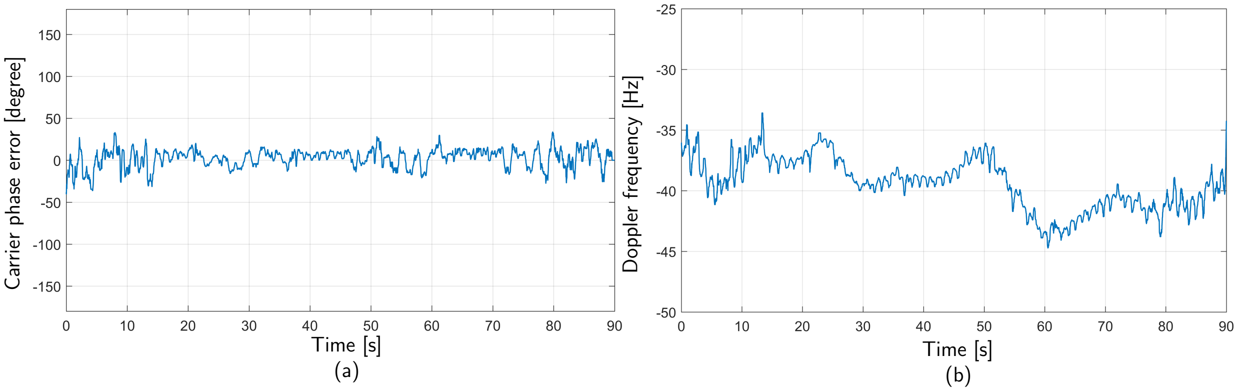


Figure 5.10: Tracking results for eNodeB 3: (a) carrier phase error and (b) Doppler frequency (Hz)

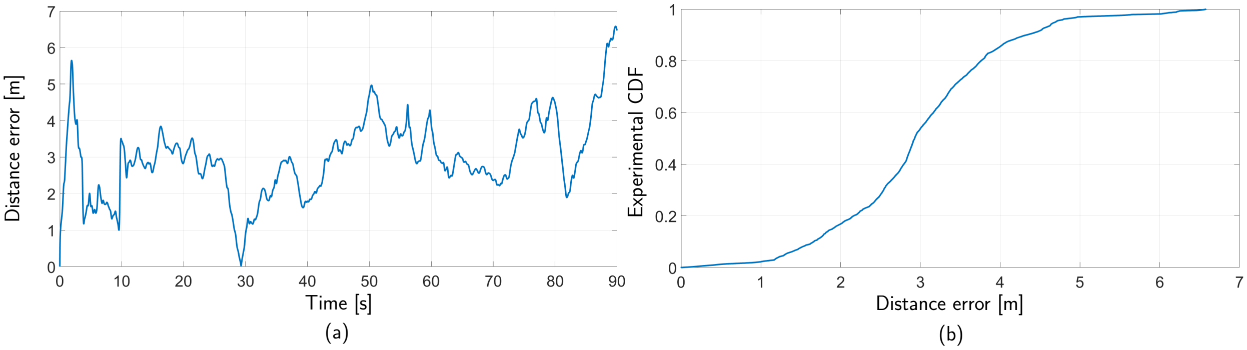


Figure 5.11: (a) Distance error between the navigation solution obtained by the LTE SDR and the GPS navigation solution over time. (b) The CDF of the error.

Table 5.3: LTE Navigation Performance with Proposed Method

Performance Measure	**Value**
RMSE	3.17 m
Standard deviation	1.06 m
Maximum error	6.58 m

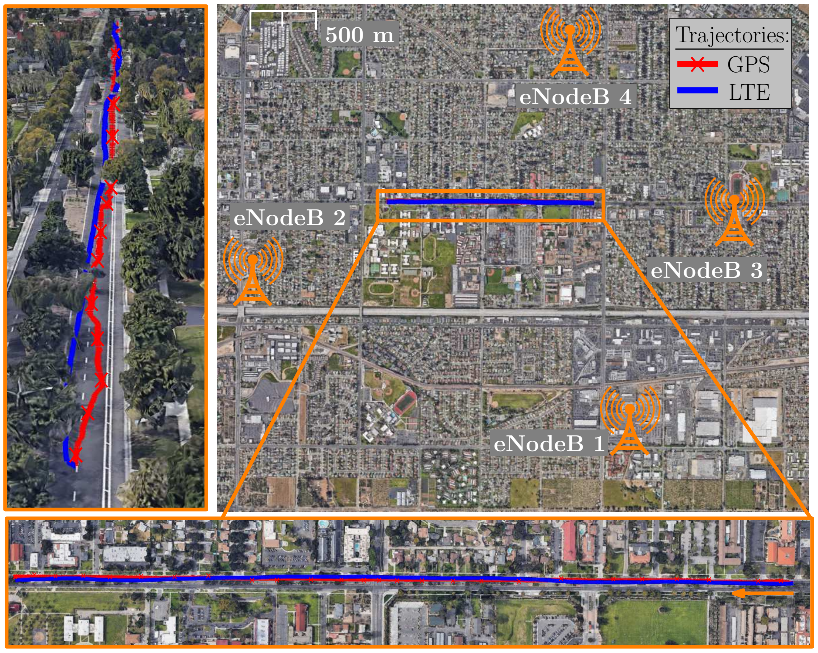


Figure 5.12: Environment layout, the eNodeBs' locations, and the traversed trajectory. The LTE navigation solution exhibited an RMSE of 3.17 m, standard deviation of 1.06 m, and maximum error of 6.58 m from the GPS navigation solution over a trajectory of 1.44 km. Image: Google Earth.

Comparison with Other Methods

With the threshold-based SDR proposed in Subsection 3.4.2, the signals from only 3 eNodeBs are trackable (i.e. eNodeBs 2–4) and the resulting RMSE over the same traversed trajectory is 11.96 m, with standard deviation of 6.83 m, and a maximum error of 40.42 m. The performance of the proposed receiver is also compared with the ESPRIT and EKAT algorithms discussed in [34]. The ESPRIT algorithm is known to provide highly accurate TOA estimation. However, this method needs perfect knowledge of the CIR length L to provide accurate results. The MDL method is an approach that can be used to estimate L; but, this method tends to overestimate the channel length. As a result, the ESPRIT TOA estimation has an outlier. The effect of this outlier can be reduced significantly using a Kalman filter and a predetermined threshold on the vehicle's speed, which is called EKAT in [34]. Fig. 5.13 shows the pseudoranges obtained by the ESPRIT, EKAT, and the proposed receiver for all eNodeBs. It can be seen that the pseudoranges obtained by ESPRIT have significant outliers, which is improved in EKAT. The pseudoranges shown in Fig. 5.13 are obtained using the same parameters as in [34]. It can be seen that the pseudoranges obtained by the proposed receiver are significantly more robust and accurate. For more explanation on the high error obtained using ESPRIT and EKAT algorithms, consider the results for eNodeB 1. As was discussed in Fig. 5.9, the noise level and multipath effect for eNodeB 1 increase after 40 s. Under this condition, the MDL algorithm tends to overestimate the channel length and as a result, the noise components are detected as the signal components in the ESPRIT algorithm. Although the EKAT algorithm could remove some of the outliers in the estimated CIR by ESPRIT, it could not eliminate a continuous error in the CIR estimates, obtained by the ESPRIT algorithm. Table 6.1 compares the pseudorange error statistics (standard deviation σ and maximum error) obtained with the proposed method versus the ESPRIT and EKAT algorithms.

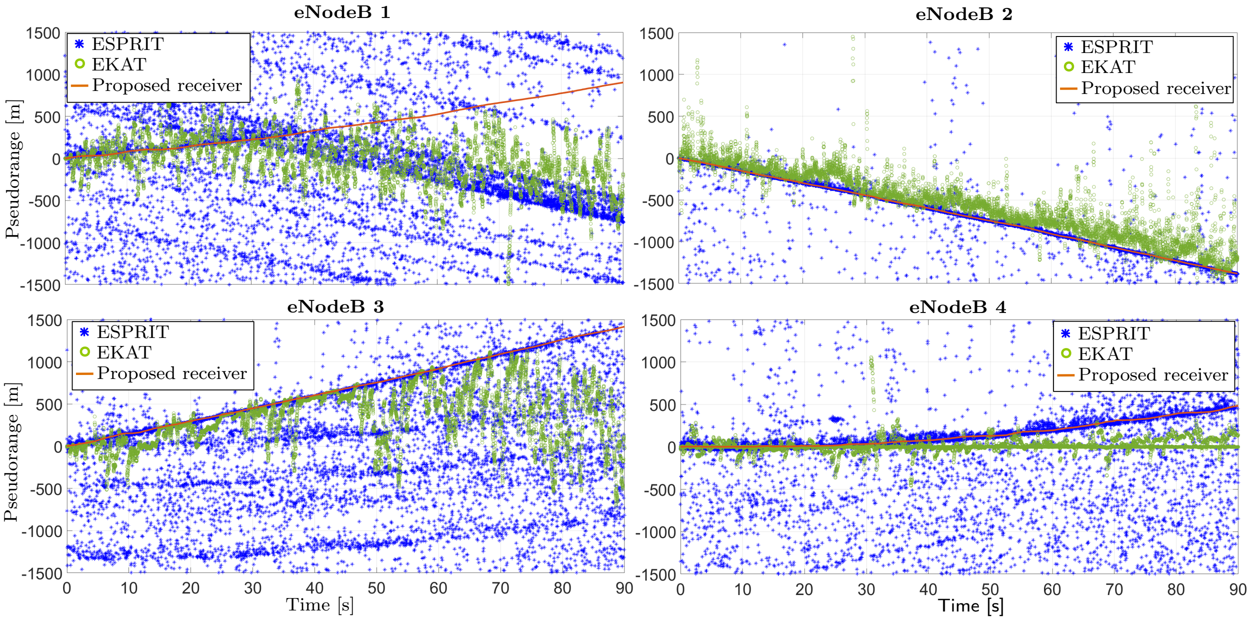


Figure 5.13: Estimated pseudoranges obtained by the proposed receiver, ESPRIT, and EKAT algorithms for all the eNodeBs

Table 5.4: Comparison of Pseudorange Errors Obtained by Each Method

	ESPRIT		**EKAT**		**Proposed Method**	
	σ **[m]**	**Max. Error [m]**	σ **[m]**	**Max. Error [m]**	σ **[m]**	**Max. Error [m]**
eNodeB 1	883.2	2102	495.6	1683	4.55	9.61
eNodeB 2	249.2	2981	176.6	2098	2.20	5.60
eNodeB 3	836.8	2431	422.1	1751	1.96	7.74
eNodeB 4	642.3	1884	148.4	1151	2.04	3.84

In terms of complexity, the ESPRIT and EKAT algorithms have complexity on the order of $\mathcal{O}(N_c^3)$, which is mainly due to the SVD operator. However, the complexity of the proposed receiver is on the order of $\mathcal{O}(N_c \log N_c)$, which is due to the FFT operator. Since acquisition is either performed once before tracking starts or after tracking is lost, and since the majority of the processing time is spent in the tracking stage, when evaluating the complexity, only the tracking stage is considered.

5.2.5 Remarks

This subsection summarizes key remarks concluded from the presented results.

- A GPSDO allows modeling the receiver's clock by a known clock model as discussed in Subsection 5.2.1. In an environment where GPS is not available and the receiver's clock model is unknown, other navigation frameworks could be used, e.g., collaboration via mapping and navigating receivers [22].

- The GPS navigation solution is only used (1) as ground truth to obtain the estimation error for navigating with LTE signals and (2) to initialize the EKF.

- The choice of hardware and software is not unique. Any hardware that can sample in cellular bands can be used to record LTE signals and any software that has the processing capabilities (e.g. LabVIEW, MATLAB, and C++) can be used to implement the receiver.

- The estimation performance depends on the geometric diversity of the eNodeBs, the number of eNodeBs in the environment, the dynamical model, and the measurement accuracy.

- There is a slight mismatch between the vehicle's true dynamical model and the assumed model in (5.8). In the assumed model, the EKF might allow the vehicle's position and velocity estimates to move freely, as opposed to constraining them to a road segment. This model mismatch will cause the estimation error to become larger. In order to minimize the mismatch between the true and assumed model, multiple models for the vehicle's dynamics may be used to accommodate the different behaviors of the vehicle in different segments of the trajectory. Alternatively, an inertial measurement unit (IMU), which is available in many practical systems (e.g., UAV, cars, and smart phones), can be used to propagate the state of the vehicle [23]. This will also aid in alleviating multipath-induced errors. Section 5.4 presents a navigation framework that uses IMU measurements to propagate the state of the filter between each measurement update.

5.3 Standalone LTE Navigation Solution with Code and Carrier Phase and Doppler Frequency Measurements

Section 5.2 discussed a navigation framework that uses code phase measurements to simultaneously estimate the position and velocity of the UE and the difference between the UE's clock bias and drift and those of the eNodeBs'. There are two main challenges in the proposed framework in Section 5.2: (1) the UE's and eNodeBs' clock models must be known at the UE and (2) code phase measurements have high error and accurate carrier phase and Doppler frequency measurements are not used. In this section, a navigation framework based on an EKF is proposed that resolves the aforementioned challenges. The proposed framework uses single difference code and carrier phase and range rate measurements, which do not have the effect of the UE's clock bias.

Although single difference measurements do not depend on the UE's clock model, they still have the effect of eNodeBs' clock biases. One approach to remove this dependency is to use a base-rover framework. In this framework, the navigation observables of a receiver with known location, which is called base receiver, is transmitted to the receiver with unknown location, which is called rover receiver. By subtracting the single difference measurements of the rover and base receiver, the common error terms (e.g., transmitters' clock biases) can be removed, resulting in highly accurate measurements. Note that the base receiver must be installed close to the rover receiver to be able to listen to the same transmitters and to experience similar errors (e.g., ionospheric error in GNSS measurements). A base-rover framework in GNSS systems requires a maximum distance of 10 to 20 km between the base and rover receivers. This distance ensures similarity between the base and rover common error sources, while listening to the same satellites. Therefore, GNSS systems require a relatively sparse base installation. However, this is not the case for navigation with cellular LTE signals. To reduce the interference of each eNodeB's signal with the neighboring eNodeBs, the signal coverage of each eNodeB is designed to be typically less than 4 km. Therefore, the base and rover distance must be less than 4 km in a base-rover framework for navigation with LTE signals. This necessitates a relatively dense network of base stations, which could be impractical. In this section, the high stability of LTE eNodeBs' clocks is used to eliminate the need for a base receiver. The details of the state and dynamic model are presented in Subsection 5.3.1

One of the main challenges in navigation with carrier phase measurements is the unknown number of integer cycles between the transmitter and the receiver, namely integer ambiguity. Different methods can be used to determine the values of integer ambiguities [69, 80]. As long as the carrier tracking loop maintains lock, integer cycles remain constant. However, several factors including high receiver's dynamics, momentary loss of phase lock (e.g., due to signal blockage), and multipath can cause a discontinuity in the integer cycles, while the fractional part of the phase is measured continuously. This discontinuity in the integer cycles is called a cycle slip. Several approaches have been proposed for cycle slip detection in GNSS signals, including: (1) phase-code comparison, (2) phase-phase ionospheric residual, (3) Doppler integration, and (4) differential phases [81]. Phase-code comparison can only be used for large cycle slip detection since the noise level of the code is high. The performance of phase-phase ionospheric residual depends on the ionospheric residuals and also requires multiple transmission frequencies (e.g., L1 and L2 in GPS). The receiver's high dynamics may be detected as cycle slip in Doppler integration and differential phases. Among the aforementioned algorithms for cycle slip detection, the second is geometry-free and has the highest accuracy for small ionospheric residuals due to precise phase measurements. Since the ionosphere does not affect terrestrial cellular signals, this approach seems promising for cycle slip detection of cellular signals. However, it requires phase measurements from multiple carrier frequencies for each transmitter, which is not usually available in cellular LTE systems since they are typically transmitted on one carrier frequency from each LTE eNodeB.

However, carrier phase measurements can be obtained from multiple transmission antennas, which are installed on each eNodeB. In Subsection 5.3.2, a new approach is proposed in which the carrier phase measurements of different LTE transmission antennas are used to detect cycle slips. The proposed navigation framework and cycle slip detection algorithm are evaluated experimentally with real LTE signals. Finally, Subsections 5.3.3 and 5.3.4 present the experimental setup and results, respectively.

5.3.1 State, Dynamic, and Measurement Model

Based on the LTE protocol, LTE eNodeBs are required to have sufficiently stable clocks [78]. Hence, it can be assumed that $\dot{\delta t}_{\mathrm{s}}^{(ul)}$ is zero over the UE's navigation course, resulting in the following model for the single difference range rate measurement

$$\dot{\rho}^{(ul)} \triangleq -\frac{\dot{\boldsymbol{r}}_{\mathrm{r}}^{\mathsf{T}}\left(\boldsymbol{r}_{\mathrm{r}}-\boldsymbol{r}_{\mathrm{s}}^{(u)}\right)}{d^{(u)}}+\frac{\dot{\boldsymbol{r}}_{\mathrm{r}}^{\mathsf{T}}\left(\boldsymbol{r}_{\mathrm{r}}-\boldsymbol{r}_{\mathrm{s}}^{(l)}\right)}{d^{(l)}}+\varepsilon_{\dot{\rho}}^{(ul)}. \tag{5.11}$$

The UE is assumed to have initial access to the GPS signals before starting to navigate with LTE signals. Therefore, the known initial position of the UE can be used to estimate $\delta t_{\mathrm{s}}^{(ul)}$. The estimated value of $\delta t_{\mathrm{s}}^{(ul)}$ is assumed to be constant during the UE's navigation course. The pseudorange and carrier phase measurements after removing the effect of eNodeBs' clock biases can be modeled as

$$\begin{aligned}\rho'^{(ul)} &\triangleq \rho^{(ul)}+c\hat{\delta t}_{\mathrm{s}}^{(ul)}\\ &= d^{(ul)}+\varepsilon_{\rho}^{(ul)},\end{aligned} \tag{5.12}$$

$$\begin{aligned}\phi'^{(ul)} &\triangleq \phi^{(ul)} + c\hat{\delta t}_{\mathrm{s}}^{(ul)} \\ &= d^{(ul)} + \underbrace{\lambda^{(u)}N^{(u)} - \lambda^{(l)}N^{(l)}}_{\triangleq N_{\text{float}}^{(ul)}} + \varepsilon_{\phi}^{(ul)}.\end{aligned} \tag{5.13}$$

By comparing (5.13) with GPS single difference carrier phase measurements, it can be seen that the effect of different eNodeBs' integer ambiguities cannot be modeled with one integer element. This is due to the fact that different LTE operators transmit at different carrier frequencies. Therefore, conventional algorithms to estimate integer ambiguities (e.g., Least-squares AMBiguity Decorrelation Adjustment (LAMBDA) algorithm [82]) cannot be used here. In this dissertation, the value of $N_{\text{float}}^{(ul)}$, which is not necessarily an integer, is estimated along with other states of the filter.

The EKF state consists of the UE's position and velocity, and the vector of ambiguities $\boldsymbol{N}$, given by

$$\boldsymbol{x} = \left[\boldsymbol{r}_{\mathrm{r}}^{\mathsf{T}}, \dot{\boldsymbol{r}}_{\mathrm{r}}^{\mathsf{T}}, \boldsymbol{N}\right]^{\mathsf{T}}, \tag{5.14}$$

where $\boldsymbol{N} \triangleq \left[N_{\text{float}}^{(21)}, \cdots, N_{\text{float}}^{(U1)}\right]^{\mathsf{T}}$. The state vector dynamics is modeled according to the following discretized model

$$\boldsymbol{x}(j+1) = \mathbf{F}\boldsymbol{x}(j) + \boldsymbol{w}(j), \tag{5.15}$$

where j is the discretized time sample; $\mathbf{F} = \text{blkdiag}\left[\mathbf{F}_{\text{pv}}, \mathbf{I}_{U-1}\right]$; blkdiag denotes a matrix block diagonal; $\mathbf{I}_m$ is the identity matrix of size m; $\boldsymbol{w}$ is a discrete-time zero-mean white noise with covariance matrix $\mathbf{Q} = \text{blkdiag}\left[\mathbf{Q}_{\text{pv}}, \epsilon\mathbf{I}_{U-1}\right]$; and $\epsilon > 0$ is set to be very small, e.g., 10^{-10}; The UE's dynamics is assumed to evolve according to a velocity random walk with the following dynamic model

$$\mathbf{F}_{\mathrm{pv}} = \begin{bmatrix} \mathbf{I}_3 & T\mathbf{I}_3 \\ \mathbf{0}_{3\times 3} & \mathbf{I}_3 \end{bmatrix}, \tag{5.16}$$

$$\mathbf{Q}_{\mathrm{pv}} = \begin{bmatrix} \tilde{q}_x\frac{T^3}{3} & 0 & 0 & \tilde{q}_x\frac{T^2}{2} & 0 & 0 \\ 0 & \tilde{q}_y\frac{T^3}{3} & 0 & 0 & \tilde{q}_y\frac{T^2}{2} & 0 \\ 0 & 0 & \tilde{q}_z\frac{T^3}{3} & 0 & 0 & \tilde{q}_z\frac{T^2}{2} \\ \tilde{q}_x\frac{T^2}{2} & 0 & 0 & \tilde{q}_x T & 0 & 0 \\ 0 & \tilde{q}_y\frac{T^2}{2} & 0 & 0 & \tilde{q}_y T & 0 \\ 0 & 0 & \tilde{q}_z\frac{T^2}{2} & 0 & 0 & \tilde{q}_z T \end{bmatrix}. \tag{5.17}$$

where T is the time interval between two measurements, and $\tilde{q}_x$, $\tilde{q}_y$, and $\tilde{q}_z$ are the power spectral densities of the acceleration in x, y, and z directions.

Due to the low vertical diversity of LTE eNodeBs, the UE's altitude estimate suffers from large error. An altimeter can be used to reduce the UE's altitude estimation uncertainty. The measurement vector is defined as $\boldsymbol{z} \triangleq \left[\boldsymbol{\rho}^{\mathsf{T}}, \boldsymbol{\phi}^{\mathsf{T}}, \dot{\boldsymbol{\rho}}^{\mathsf{T}}, a\right]^{\mathsf{T}}$, where $\boldsymbol{\rho} = \left[\rho'^{(21)}, \cdots, \rho'^{(U1)}\right]^{\mathsf{T}}$; $\boldsymbol{\phi} = \left[\phi'^{(21)}, \cdots, \phi'^{(U1)}\right]^{\mathsf{T}}$; $\dot{\boldsymbol{\rho}} = \left[\dot{\rho}^{(21)}, \cdots, \dot{\rho}^{(U1)}\right]^{\mathsf{T}}$; $a \triangleq z_{\mathrm{r}} + \varepsilon_a$ is the altitude estimate derived from an altimeter; and ε_a is the altitude measurement noise, which is modeled as a zero-mean Gaussian random variable with a standard deviation of σ_a.

The measurement noise covariance matrix is defined as $\mathbf{R} \triangleq \mathrm{blkdiag}\left[\mathbf{R}_\rho, \mathbf{R}_\phi, \mathbf{R}_{\dot{\rho}}, \sigma_a^2\right]$, where

$$\mathbf{R}_\rho = \begin{bmatrix} \mathrm{var}\left\{\varepsilon_\rho^{(21)}\right\} & \mathrm{var}\left\{\varepsilon_\rho^{(1)}\right\} & \cdots & \mathrm{var}\left\{\varepsilon_\rho^{(1)}\right\} \\ \mathrm{var}\left\{\varepsilon_\rho^{(1)}\right\} & \mathrm{var}\left\{\varepsilon_\rho^{(31)}\right\} & \ddots & \mathrm{var}\left\{\varepsilon_\rho^{(1)}\right\} \\ \vdots & \ddots & \ddots & \vdots \\ \mathrm{var}\left\{\varepsilon_\rho^{(1)}\right\} & \cdots & \mathrm{var}\left\{\varepsilon_\rho^{(1)}\right\} & \mathrm{var}\left\{\varepsilon_\rho^{(U1)}\right\} \end{bmatrix} \tag{5.18}$$

where var $\{\cdot\}$ represents the variance operator and var $\left\{\varepsilon_{\rho}^{(ul)}\right\} = {\sigma_{\rho}^{(u)}}^2 + {\sigma_{\rho}^{(l)}}^2$. The values of $\mathbf{R}_{\phi}$ and $\mathbf{R}_{\dot{\rho}}$ can be derived similar to (5.18).

5.3.2 Cycle Slip Detection

The LTE protocol considers 1, 2, or 4 transmission antennas for the eNodeBs in order to increase data throughput. Denote the u-th eNodeB's carrier phase measurement from antenna port i by

$$\begin{aligned}&\phi_i^{(u)} = \frac{1}{\lambda^{(u)}} d_i^{(u)} + \frac{c}{\lambda^{(u)}}\left(\delta t_{\mathrm{r}} - \delta t_{\mathrm{s}}^{(u)}\right) + N_i^{(u)} + \varepsilon_{\phi_i}^{(u)}, \quad \text{[cycle]}\\ &\text{for} \quad i = 1, \cdots, 4.\end{aligned}$$

Antenna ports 1 and 2 (and antenna ports 3 and 4 if available) only differ in the polarization and not the antennas positions [34]. Therefore, the received signals from antenna ports 1 and 2 have the same TOA at the receiver, which means $d_1^{(u)} = d_2^{(u)}$. Define $\phi_{12}^{(u)}$ and $\Delta\phi_{12}^{(u)}(n)$ at time-step n to be

$$\begin{aligned}\phi_{12}^{(u)}(n) &\triangleq \phi_1^{(u)}(n) - \phi_2^{(u)}(n)\\ &= \underbrace{N_1^{(u)}(n) - N_2^{(u)}(n)}_{\triangleq N_{12}^{(u)}(n)} + \varepsilon_{\phi_{12}}^{(u)}(n),\end{aligned}$$

$$\begin{aligned}\Delta\phi_{12}^{(u)}(n) &\triangleq \phi_{12}^{(u)}(n) - \phi_{12}^{(u)}(0)\\ &= N_{12}^{(u)}(n) - N_{12}^{(u)}(0) + \varepsilon_{\phi_{12}}^{(ul)}(n) - \varepsilon_{\phi_{12}}^{(ul)}(0).\end{aligned}$$

When there is no cycle slip, $N_{12}^{(u)}(n)$ remains constant over time. However, the value of $N_{12}^{(u)}(n)$ changes over time when a cycle slip with different values happen on the carrier phase measurements from two different eNodeB's antenna ports. Therefore, a threshold on

$\Delta\phi_{12}^{(u)}(n)$ can be used to detect cycle slips. Note that the proposed algorithm can miss-detect the presence of cycle slips when they are similar on the carrier phase measurements of both antenna ports.

5.3.3 Experimental Hardware and Software Setup

To evaluate the performance of the proposed method, an experiment was performed in Mission Viejo, CA, USA. This section presents the experimental hardware and software setup.

A DJI Matrice 600 UAV was equipped with a four-channel NI USRP-2955 to sample LTE signals at four different carrier frequencies. For this experiment, the LTE carrier frequencies 1955, 2145, 2125, and 739 MHz were used, which are allocated to the U.S. cellular operators AT&T, T-Mobile, and Verizon. The sampling rate was set to 10 MSps and the sampled LTE signals were recorded on a laptop.

A Septentrio AsteRx-i V, which was equipped with dual antenna multi-frequency GNSS receiver with RTK and a Vectornav VN-100 micro electromechanical systems (MEMS) IMU, was used to estimate the position and orientation of the drone, which was used as the ground truth. Fig. 5.14 shows the experimental hardware setup.

The values of the power spectral densities of the acceleration in x, y, and z directions were set to $\tilde{q}_x = 1$, $\tilde{q}_y = 1$, and $\tilde{q}_z = 0.1$ m^2/s^3, respectively. A random variable with a standard deviation of 1 m was added to the true altitude of the UAV over time and was used as an altimeter measurement. The true standard deviations of the measurements, which were obtained using the ground truth, were used to build the measurement covariance matrix $\mathbf{R}$.

Over the course of the experiment, the receiver traversed a trajectory of 605 m over 175 seconds, while listening to 11 eNodeBs. The locations of the eNodeBs in the environment

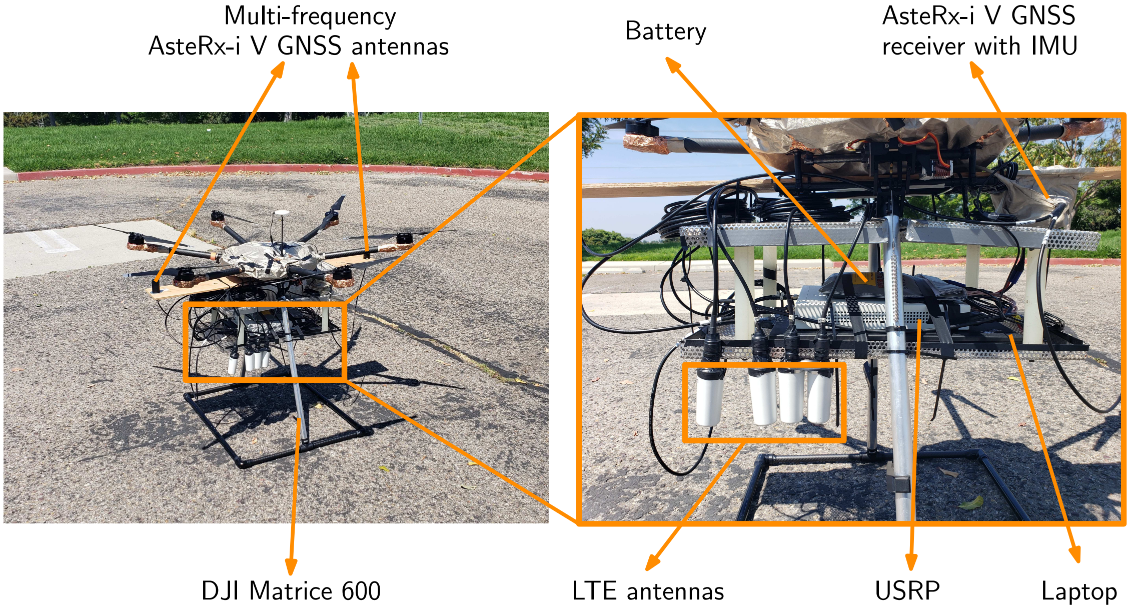


Figure 5.14: Experimental hardware setup

were mapped before the experiment. The eNodeBs' cell IDs and their corresponding carrier frequencies are presented in Table 5.5.

Table 5.5: eNodeBs' characteristics

Cell ID	**Carrier frequency (MHz)**
78	2145
104, 352	1955
308, 358, 224, 58, 354	2125
492, 5, 27	739

The sampled LTE signals were processed offline using the proposed LTE SDR in Section 3. The resulting measurements were used to estimate the location of the UAV using the proposed navigation framework in Subsection 5.3.1.

5.3.4 Experimental Results

This subsection presents the derived navigation observables and the achieved navigation solution over the course of the experiment.

Measurements

Fig. 5.15 presents the CDF of the single difference pseudorange and carrier phase measurement errors, i.e., $\rho^{(ul)} - d^{(ul)}$ and $\phi^{(ul)} - d^{(ul)}$. Note that $d^{(ul)}$ was obtained using the ground truth. To remove the effect of eNodeBs' clock biases and integer ambiguities from the plots, the means of $\rho^{(ul)} - d^{(ul)}$ and $\phi^{(ul)} - d^{(ul)}$ over time were subtracted from the results. Fig. 5.15 shows that the carrier phase measurements have higher precision compared to the pseudorange measurements.

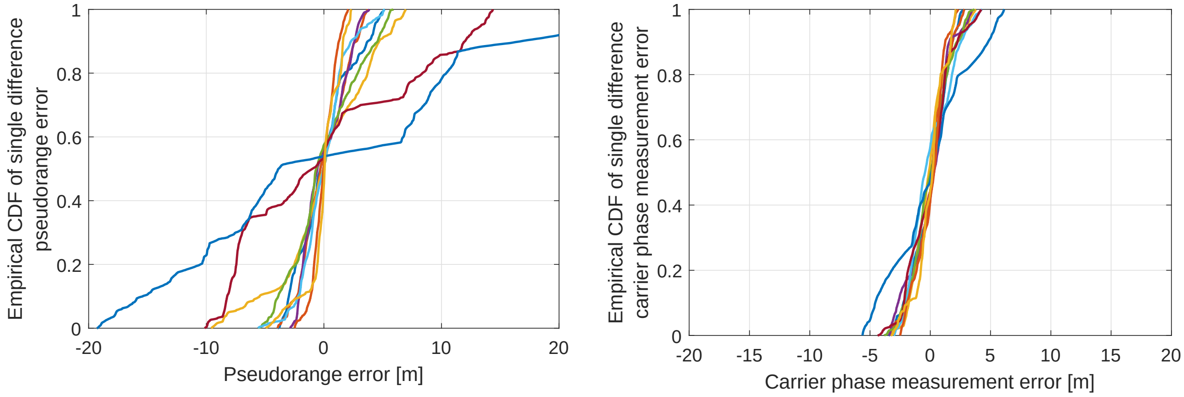


Figure 5.15: CDF of the single difference pseudorange and carrier phase measurement errors

Cycle Slip Detection

Fig. 5.16 shows $\Delta\phi_{12}^{(u)}(n)$ over time for all the cell IDs. It can be seen that only for eNodeB with cell ID 78, the value of $\Delta\phi_{12}^{(u)}(n)$ stays less than one cycle during the course of the experiment. This means that: (i) the carrier phase measurement from the cell ID 78 does not have any cycle slip or (ii) cycle slips on the carrier phase measurements from antenna ports 1 and 2 were equal. It can be concluded from Fig. 5.16 that all the carrier phase measurements except the one for cell ID 78 were affected by cycle slips. The cycle slips can be due to several factors including:

- High receiver's dynamics: The traversed path included several turns, which can cause receiver's loss of phase lock.
- Momentary signal loss: The UAV's altitude was relatively low compared to the surrounding buildings. Besides, the eNodeBs' have low altitudes and as a result, the signal can be blocked momentarily, which can cause cycle slips.
- Multipath: The buildings in the UAV's surrounding environment can cause significant multipath, which can result in a discontinuity in the integer cycles while the fractional part of the phase is measured continuously.

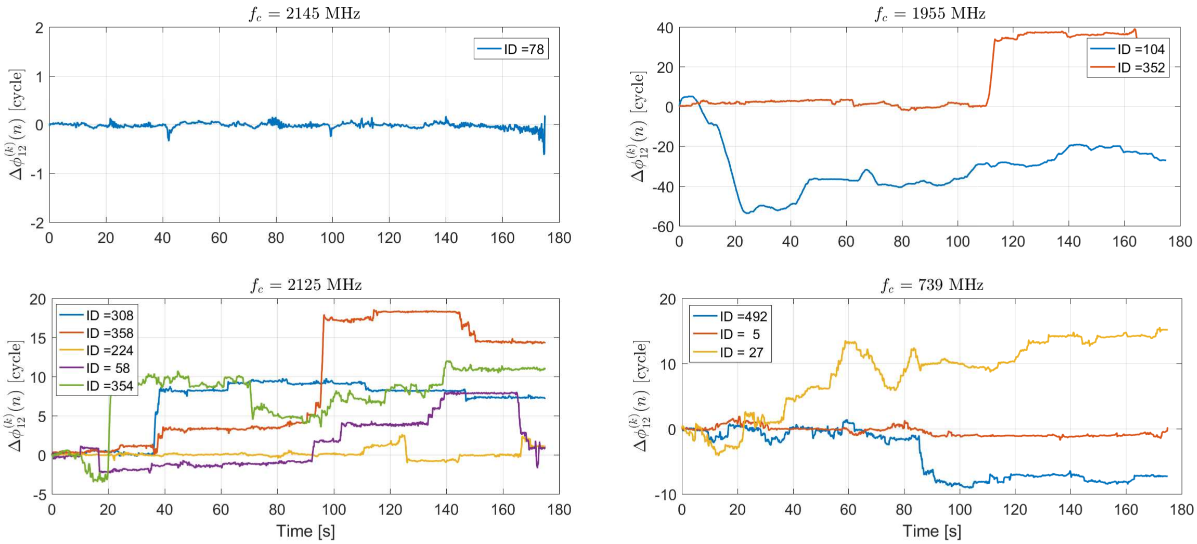


Figure 5.16: The values of $\Delta\phi_{12}^{(u)}(n)$ over time. This value can be used to detect cycle slips for each carrier phase measurement.

Navigation Solution

Fig. 5.17 presents the environmental layout of the experiment, the location of the eNodeBs, ground truth, and the LTE navigation solution. The result shows a 2-D RMSE of 81 cm over the course of the experiment. The results of the experiment are summarized in Table 5.6.

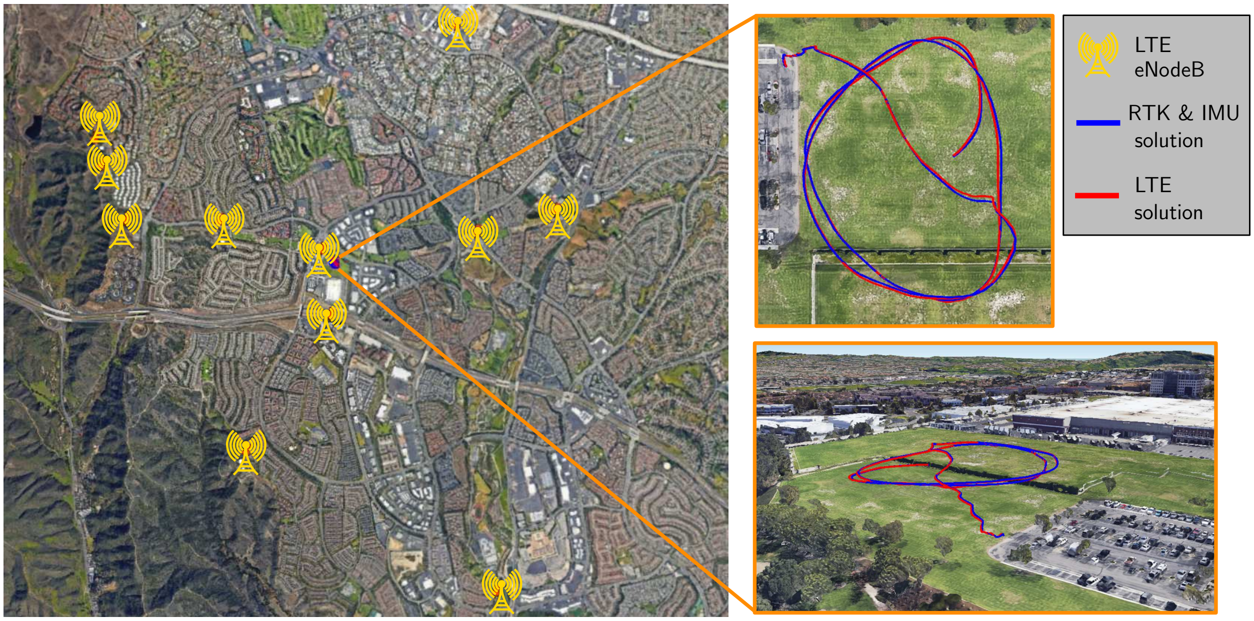


Figure 5.17: Environmental layout of the experiment, location of the eNodeBs, ground truth, and final navigation solution. The UAV traversed a trajectory of 605 m over 175 seconds. The results show a 2-D RMSE of 81 cm. Image: Google Earth.

Table 5.6: Navigation solution results

2-D RMSE [m]	**3-D RMSE [m]**	**Maximum error [m]**
0.81	0.86	2.49

Discussion

The difference between the LTE navigation solution and the ground truth is due to several sources of error, including:

- Cycle slip: As was shown in Fig. 5.16, the carrier phase measurements experienced significant cycle slips over the course of the experiment, which reduces the precision of carrier phase measurements.

- eNodeBs' clock biases: As was discussed in Section 5.3.1, the eNodeBs' clock biases were assumed to be constant over the course of the UAV's navigation. Small changes in the value of the eNodeBs' clock biases can introduce error in all the measurements. This can be resolved using a base receiver.

- Multipath: The UAV's altitude was relatively low compared to the surrounding buildings and trees. Therefore, the received signal suffered from multipath effects. The multipath error can be reduced by flying at higher altitudes.

- Uncertainty in eNodeBs' locations: The locations of the eNodeBs were mapped using Google Earth, which is not very accurate. Using a database can reduce the error due to this factor.

- Different carrier frequencies: Since different operators use different carrier frequencies, the effect of the number of cycles on single difference carrier phase measurements $N_{\text{float}}^{(ul)}$ is not an integer and its estimate can introduce error in the solution. This can be resolved using a base receiver.

- Model mismatch: A velocity random walk was used to model the UAV's dynamics. The mismatch between this model and the UAV's true dynamics causes error in the position estimate. This can be resolved by using an IMU to propagate the states.

5.4 IMU-Aided LTE Navigation Solution with Code Phase Measurements

Section 5.2 and 5.3 proposed two navigation frameworks based on an EKF, where a velocity random-walk was used to model the dynamics of the UE's position and velocity. However, there is a slight mismatch between the true vehicle's dynamic model and the velocity random-walk model. For example, a ground vehicle mostly moves on a road with straight segments. But, the velocity random-walk model does not take into consideration the trajectory constraints and allows the vehicle's position and velocity estimates to move freely. This mismatch will cause the estimation error to become larger. In order to minimize the mismatch between the true and assumed model, multiple models for the vehicle's dynamics may be used to accommodate the different behaviors of the vehicle in different segments of the trajectory. Alternatively, an IMU, which is available in many practical scenarios, can be used to propagate the state of the vehicle.

In addition to the model mismatch, multipath is among the most significant challenges that must be addressed for RF-based navigation. As discussed in Subsection 4.2.2, multipath introduces error in the estimated pseudoranges, where the magnitude of the error depends on the multipath condition, signal bandwidth, and sampling rate. The high transmission bandwidth of LTE signals (up to 20 MHz) could be used to resolve multipath. However, received LTE signals experience more multipath compared to GNSS signals, particularly for ground-based receivers in urban canyons, due to the low elevation angles at which signals are received. In a low dynamic environment, the multipath effect lasts over multiple epochs and the error due to multipath is time-correlated. Besides, the pseudorange error caused by multipath may affect multiple epochs due to the receiver's loop filter.

Several signal processing-based methods have been proposed to remove the effect of multipath in GNSS signals including a multipath-estimating delay-locked loop (MEDLL) [83], a batch filter to estimate the multipath using a known antenna motion [84], and a technique to correct multipath errors using signal-to-noise ratio [85]. These approaches have either high computational cost or they require prior knowledge of the multipath condition. Another approach to reduce the effect of multipath is based on beamforming. Beamforming can be performed using an antenna array, which has a bulky structure. Alternatively, one can synthesize an antenna array by moving the antenna. In synthetic aperture navigation (SAN), the antenna movement can be uniform or arbitrary. In a uniform movement, computationally low-cost approaches (e.g., MUSIC or ESPRIT) can be used to estimate the DOA [86, 87], whereas computationally expensive algorithms (e.g., space-alternating generalized expectation-maximization (SAGE)) must be used to estimate the DOA in an arbitrary movement [88]. Uniform structures require a bulky hardware platform, and the performance of arbitrary structures depends on the accuracy of the antenna location, which depends on the accuracy of the IMU. It has been shown that the antenna motion can also be used to decorrelate the error induced by multipath. Antenna motion was used in [89] to improve the detection performance and in [90] to reduce the carrier-phase error in carrier-phase differential GNSS (CDGNSS) positioning, where a first-order Gauss-Markov process was used to model the relative antenna position with respect to the reference antenna.

In a Kalman filter, the measurement noise is assumed to be time-uncorrelated. A time-correlated measurement noise will induce an error in the navigation solution estimate. Since the dynamics of the errors due to multipath is unknown, whitening approaches cannot be used to decorrelate the measurement noise. This section addresses this challenge by making two contributions. First, a navigation framework based on a multi-state constraint Kalman filter (MSCKF) is proposed. The MSCKF was first introduced in robotics literature [91]. In this framework, an IMU is used to capture the position of the antenna over a window of measurements. Unlike a traditional EKF, which uses a single measurement epoch to update the state estimate, this dissertation employs an MSCKF to use a sliding window of measurement epochs along with the antenna motion to decorrelate the measurement noise and provide constraints on the position estimate. Moreover, the difference of the clock bias of the receiver and each of the LTE eNodeBs are estimated along with the position of the antenna since the eNodeBs' clock biases are unknown to the receiver. Second, the results are evaluated with simulations and experiments.

5.4.1 State Model

The vehicle's state vector $\boldsymbol{x}$ is defined as

$$\boldsymbol{x} \triangleq \left[\, \boldsymbol{x}_{\text{IMU}}^{\mathsf{T}} \,,\ \boldsymbol{x}_{\text{clk}}^{\mathsf{T}} \,,\ \boldsymbol{\pi}_{1}^{\mathsf{T}} \,,\ \boldsymbol{\pi}_{2}^{\mathsf{T}} \,,\ \cdots, \boldsymbol{\pi}_{N}^{\mathsf{T}} \,\right]^{\mathsf{T}},$$

where $\boldsymbol{x}_{\text{IMU}}$ represents the IMU state vector, $\boldsymbol{x}_{\text{clk}}$ is the clock error state vector, and $\boldsymbol{\pi}_i$ is composed of the receiver's position and the difference between the clock bias of the receiver and each of the eNodeBs at the i-th pseudorange measurement.

The IMU state vector is given by

$$\boldsymbol{x}_{\text{IMU}} \triangleq \left[\, {}_{G}^{I}\bar{\boldsymbol{q}}^{\mathsf{T}} \,,\ {}^{G}\boldsymbol{r}_{\text{IMU}}^{\mathsf{T}} \,,\ {}^{G}\boldsymbol{v}_{\text{IMU}}^{\mathsf{T}} \,,\ \boldsymbol{b}_{g}^{\mathsf{T}} \,,\ \boldsymbol{b}_{a}^{\mathsf{T}} \,\right]^{\mathsf{T}},$$

where ${}_{G}^{I}\bar{\boldsymbol{q}}$ is the unit quaternion representing the rotation from a global frame G, such as an Earth-centered inertial (ECI) frame, to the IMU frame I; ${}^{G}\boldsymbol{r}_{\text{IMU}}$ and ${}^{G}\boldsymbol{v}_{\text{IMU}} = {}^{G}\dot{\boldsymbol{r}}_{\text{IMU}}$ are the 3-D position and velocity of the IMU in the global frame, respectively; and $\boldsymbol{b}_g$ and $\boldsymbol{b}_a$ are the gyroscope and accelerometer biases, respectively.

The clock error state vector is defined as

$$\boldsymbol{x}_{\text{clk}} \triangleq [\Delta\boldsymbol{x}_{\text{clk}}^{(1)^{\mathsf{T}}} \,,\ \cdots \,,\ \Delta\boldsymbol{x}_{\text{clk}}^{(U)^{\mathsf{T}}}]^{\mathsf{T}},$$

where $\Delta\boldsymbol{x}_{\text{clk}}^{(u)} \triangleq [c\Delta\delta t^{(u)}, c\Delta\dot{\delta}t^{(u)}]$, $\Delta\delta t^{(u)} = \delta t_{\text{r}} - \delta t_{\text{s}}^{(u)}$, and $\Delta\dot{\delta}t^{(u)} = \dot{\delta}t_{\text{r}} - \dot{\delta}t_{\text{s}}^{(u)}$.

The vector $\boldsymbol{\pi}_i$ is defined as

$$\boldsymbol{\pi}_i \triangleq \left[{}^G\boldsymbol{r}_{A_i}^{\mathsf{T}} \ , \ \boldsymbol{x}_{\text{clk,b}_i}^{\mathsf{T}} \right]^{\mathsf{T}},$$

where $\boldsymbol{x}_{\text{clk,b}_i} = \left[c\Delta\delta t_i^{(1)}, \cdots, c\Delta\delta t_i^{(U)} \right]^{\mathsf{T}}$ is the difference between the clock bias of the receiver and each of the eNodeBs and ${}^G\boldsymbol{r}_{A_i}$ is the antenna's position in the global frame at the i-th pseudorange measurement epoch.

5.4.2 State Propagation

The IMU produces measurements of the rotational velocity $\boldsymbol{\omega}_m$ and linear acceleration $\boldsymbol{a}_m$ every T seconds, which are modeled as

$$\boldsymbol{\omega}_m(k) = {}^I\boldsymbol{\omega}(k) + \boldsymbol{b}_g(k) + \boldsymbol{n}_g(k), \tag{5.19}$$

$$\boldsymbol{a}_m(k) = C\left({}^I_G\bar{\boldsymbol{q}}(k)\right)\left({}^G\boldsymbol{a}(k) - {}^G\boldsymbol{g}(k)\right) + \boldsymbol{b}_a(k) + \boldsymbol{n}_a(k), \tag{5.20}$$

where ${}^I\boldsymbol{\omega}$ is the true rotational velocity of the IMU; $\boldsymbol{n}_g$ and $\boldsymbol{n}_a$ are the gyroscope and accelerometer measurement noises with zero-mean and covariances $\sigma_g^2\mathbf{I}_{3\times3}$ and $\sigma_a^2\mathbf{I}_{3\times3}$, respectively; $\mathbf{I}_{m\times m}$ is an $m \times m$ identity matrix; ${}^G\boldsymbol{a}$ is the 3-D linear acceleration; ${}^G\boldsymbol{g}$ is the acceleration due to gravity; and $C\left({}^I_G\bar{\boldsymbol{q}}\right)$ is the equivalent rotation matrix of ${}^I_G\bar{\boldsymbol{q}}$.

The IMU measurements are used to propagate the IMU state estimate. The orientation estimate is propagated according to

$$^{I_{k+1|j}}_{G}\hat{\bar{\boldsymbol{q}}} = {}^{I_{k+1}}_{I_k}\hat{\bar{\boldsymbol{q}}} \otimes {}^{I_{k|j}}_{G}\hat{\bar{\boldsymbol{q}}}, \quad \text{for } k \geq j,$$

where $\otimes$ is the quaternion multiplication operator and ${}^{I_{k+1}}_{I_k}\hat{\bar{\boldsymbol{q}}}$ is the relative rotation of the IMU frame from time-step k to $k+1$, which is obtained using a fourth-order Runge-Kutta numerical solver [23].

The IMU position state estimate is propagated using trapezoidal integration according to

$$\begin{aligned}{}^{G}\hat{\boldsymbol{r}}_{\text{IMU}}(k+1|j) =& {}^{G}\hat{\boldsymbol{r}}_{\text{IMU}}(k|j)\\ &+\frac{T}{2}\left[{}^{G}\hat{\boldsymbol{v}}_{\text{IMU}}(k+1|j)+{}^{G}\hat{\boldsymbol{v}}_{\text{IMU}}(k|j)\right],\end{aligned}$$

where ${}^{G}\hat{\boldsymbol{v}}_{\text{IMU}}(k+1|j)$ is the propagated IMU velocity state estimate, which is obtained using trapezoidal integration according to

$$\begin{aligned}{}^{G}\hat{\boldsymbol{v}}_{\text{IMU}}(k+1|j) =& {}^{G}\hat{\boldsymbol{v}}_{\text{IMU}}(k|j)\\ &+\frac{T}{2}\left[\hat{\boldsymbol{s}}(k)+\hat{\boldsymbol{s}}(k+1)\right]+T\,{}^{G}\boldsymbol{g},\end{aligned}$$

where $\hat{\boldsymbol{s}}(k)=\mathbf{C}^{\mathsf{T}}\left({}^{I_{k|j}}_{G}\hat{\boldsymbol{q}}\right)\hat{\boldsymbol{a}}(k)$ and $\hat{\boldsymbol{a}}=\boldsymbol{a}_m-\hat{\boldsymbol{b}}_a$.

The gyroscope and accelerometer biases state estimates are propagated according to

$$\begin{aligned}\hat{\boldsymbol{b}}_g(k+1|j)&=\hat{\boldsymbol{b}}_g(k|j),\\ \hat{\boldsymbol{b}}_a(k+1|j)&=\hat{\boldsymbol{b}}_a(k|j).\end{aligned}$$

The clock state estimate is propagated according to

$$\hat{\boldsymbol{x}}_{\text{clk}}(k+1|j)=\mathbf{F}_{\text{clk}}\hat{\boldsymbol{x}}_{\text{clk}}(k|j), \tag{5.21}$$

where $\mathbf{F}_{\text{clk}}=\operatorname{diag}\left[\mathbf{F}_{\text{clk}}^{(1)},\ldots,\mathbf{F}_{\text{clk}}^{(U)}\right]$ and $\mathbf{F}_{\text{clk}}^{(u)}=\begin{bmatrix}1 & T\\ 0 & 1\end{bmatrix}$.

The one-step prediction error covariance matrix of the IMU and clock states is given by

$$\mathbf{P}(k+1|j) = \mathbf{F}(k)\mathbf{P}(k|j)\mathbf{F}(k)^{\mathsf{T}} + \mathbf{Q}, \tag{5.22}$$

where $\mathbf{F} \triangleq \text{diag}\left[\mathbf{F}_{\text{IMU}}, \mathbf{F}_{\text{clk}}\right]$ and $\mathbf{Q} = \text{diag}\left[\mathbf{Q}_{\text{IMU}}, \mathbf{Q}_{\text{clk}}\right]$; $\mathbf{F}_{\text{IMU}}$ is the linearized DT IMU state transition matrix and $\mathbf{Q}_{\text{IMU}}$ is the linearized DT IMU state process noise covariance matrix. The detailed derivations of $\mathbf{F}_{\text{IMU}}$ and $\mathbf{Q}_{\text{IMU}}$ are described in [92,93]. The clock process noise covariance matrix $\mathbf{Q}_{\text{clk}}$ is given by (5.10).

5.4.3 State Augmentation

The antenna position estimate is computed from the IMU pose estimate at every pseudorange measurement epoch according to

$$^{G}\hat{\boldsymbol{r}}_{A}(k|j) = {}^{G}\hat{\boldsymbol{r}}_{\text{IMU}}(k|j) + \mathbf{C}^{\mathsf{T}}\left({}^{I_{k|j}}_{G}\hat{\boldsymbol{q}}\right){}^{I}\hat{\boldsymbol{r}}_{A},$$

where ${}^{I}\hat{\boldsymbol{r}}_{A}$ is the position of the antenna in the IMU frame and is known *a priori*. The antenna position and the difference between the clock bias of the receiver and each of the eNodeBs are augmented to the state vector. The covariance matrix of the state estimate is augmented according to

$$\mathbf{P}_{\text{AUG}}(k|j) \longleftarrow \begin{bmatrix} \mathbf{I}_{L} \\ \mathbf{J} \end{bmatrix} \mathbf{P}_{\text{AUG}}(k|j) \begin{bmatrix} \mathbf{I}_{L} \\ \mathbf{J} \end{bmatrix}^{\mathsf{T}},$$

where $L = 15 + 2U + (3+U)n$, $n = 0, \cdots, N-1$ is the number of pseudorange measurements augmented to the measurement vector, $\mathbf{P}_{\text{AUG}}(k|j) \triangleq \mathbf{P}(k|j)$ for $n = 0$, and $\mathbf{J}$ is the Jacobian matrix given by

$$\mathbf{J} = \begin{bmatrix} \lfloor \mathbf{C}_{\hat{q}}^{\mathsf{T}}\, {}^{I}\boldsymbol{r}_A \times \rfloor & \mathbf{I}_3 & \mathbf{0}_{3\times 9} & \mathbf{0}_{3\times 2U} & \mathbf{0}_{3\times(3+U)n} \\ \mathbf{0}_{U\times 3} & \mathbf{0}_{U\times 3} & \mathbf{0}_{U\times 9} & \mathbf{K} & \mathbf{0}_{U\times(3+U)n} \end{bmatrix},$$

where $\mathbf{C}_{\hat{q}}^{\mathsf{T}} \triangleq \mathbf{C}^{\mathsf{T}}\left({}^{I_{k|j}}_{G}\hat{\boldsymbol{q}}\right)$; $\mathbf{K} = [\boldsymbol{e}_0, \cdots, \boldsymbol{e}_{U-1}]^{\mathsf{T}}$; $\boldsymbol{e}_i$ is a vector of length $2U$, where its $2i$-th element is one and the rest are zeros; $\mathbf{0}_{m\times n}$ is an $m \times n$ matrix of zeros; and $\lfloor \boldsymbol{\omega} \times \rfloor$ is the skew-symmetric matrix of vector $\boldsymbol{\omega}$ defined as

$$\lfloor \boldsymbol{\omega} \times \rfloor \triangleq \begin{bmatrix} 0 & -\omega_z & \omega_y \\ \omega_z & 0 & -\omega_x \\ -\omega_y & \omega_x & 0 \end{bmatrix}, \qquad \boldsymbol{\omega} = [\omega_x, \omega_y, \omega_z]^{\mathsf{T}}.$$

The augmented covariance matrix $\mathbf{P}_{\text{AUG}}$ can be partitioned as

$$\mathbf{P}_{\text{AUG}}(k|j) = \begin{bmatrix} \mathbf{P}(k|j) & \mathbf{P}_c(k|j) \\ \mathbf{P}_c^{\mathsf{T}}(k|j) & \mathbf{P}_A(k|j) \end{bmatrix},$$

where $\mathbf{P}_A$ is the covariance matrix of the estimate of (i) antenna's positions and (ii) difference between the clock biases of the receiver and each of the eNodeBs and $\mathbf{P}_c$ is the cross correlation of the evolving IMU and clock states with the estimate of the antenna's positions and the difference between the clock biases. When an IMU measurement is available, the IMU and clock state estimates and the covariance matrix $\mathbf{P}$ are propagated according to Subsection 5.4.2. The augmented covariance matrix is propagated according to

$$\mathbf{P}_{\text{AUG}}(k+1|j) = \begin{bmatrix} \mathbf{P}(k+1|j) & \mathbf{F}(k)\mathbf{P}_c(k|j) \\ \mathbf{P}_c^{\mathsf{T}}(k|j)\mathbf{F}^{\mathsf{T}}(k) & \mathbf{F}(k)\mathbf{P}_A(k|j)\mathbf{F}^{\mathsf{T}}(k) \end{bmatrix}.$$

5.4.4 Measurement Update

After $N+1$ pseudorange measurement epochs to all U eNodeBs, the vector $\boldsymbol{\rho}$ is formed as

$$\boldsymbol{\rho} = \left[\boldsymbol{\rho}^{(1)^{\mathsf{T}}}, \cdots, \boldsymbol{\rho}^{(U)^{\mathsf{T}}}\right]^{\mathsf{T}},$$

where $\boldsymbol{\rho}^{(u)} = \left[\rho^{(u)}(0), \cdots, \rho^{(u)}(N)\right]^{\mathsf{T}}$ and

$$\rho^{(u)}(i) = \begin{cases} h^{(u)}({}^{G}\boldsymbol{r}_A(i)) + c\Delta\delta t^{(u)}(i) + \varepsilon_{\rho}^{(u)}(i), & \text{if } i = 0, \cdots, N-1, \\ h^{(u)}({}^{G}\boldsymbol{r}_{\text{IMU}} + \mathbf{C}_{\hat{q}}^{\mathsf{T}}\,{}^{I}\boldsymbol{r}_A) + c\Delta\delta t^{(u)}(i) + \varepsilon_{\rho}^{(u)}(i), & \text{otherwise.} \end{cases}$$

where $h^{(u)}(\boldsymbol{r}) \triangleq ||\boldsymbol{r}_{\text{s}}^{(u)} - \boldsymbol{r}||$. Assuming the measurement noise to be independent for different eNodeBs, the measurement noise covariance matrix can be expressed as

$$\mathbf{R} = \text{diag}\left[\mathbf{R}^{(1)}, \cdots, \mathbf{R}^{(U)}\right],$$

where the (i,j)-th element of $\mathbf{R}^{(u)}$ is defined as

$$\mathbf{R}^{(u)}(i,j) = \begin{cases} \sigma_{\rho}^{(u)^2}(i), & \text{if } i = j \\ \varrho^{(u)}(i,j)\ \sigma_{\rho}^{(u)}(i)\sigma_{\rho}^{(u)}(j), & \text{otherwise.} \end{cases}$$

where $\sigma_{\rho}^{(u)}(i)$ is the standard deviation of $\varepsilon_{\rho}^{(u)}(i)$ and $\varrho^{(u)}(i,j)$ is the correlation coefficient of the measurement noise between time step i and j. The residual can be modeled as

$$\boldsymbol{r} = \boldsymbol{\rho} - \hat{\boldsymbol{\rho}} = \mathbf{H}\tilde{\boldsymbol{x}} + \boldsymbol{v},$$

where $\mathbf{H}$ is the Jacobian matrix defined as $\mathbf{H} = \begin{bmatrix} \mathbf{H}^{(1)} \\ \vdots \\ \mathbf{H}^{(U)} \end{bmatrix}$, with the i-th row of $\mathbf{H}^{(u)}$ given by

$$\mathbf{H}^{(u)}(i) = \begin{cases} \begin{bmatrix} \mathbf{0}_{1\times(15+2U)} & \mathbf{0}_{1\times(3+U)} & \cdots & \mathbf{A}^{(u)}(i) & \cdots & \mathbf{0}_{1\times(3+U)} \end{bmatrix}, & \text{if } i = 0, \cdots, N-1, \\ \begin{bmatrix} \mathbf{B}^{(u)}(i) & \mathbf{0}_{1\times(3+U)} & \cdots & \mathbf{0}_{1\times(3+U)} \end{bmatrix}, & \text{if } i = N. \end{cases}$$

where

$$\mathbf{A}^{(u)}(i) = \begin{bmatrix} \frac{\left(\boldsymbol{r}_{\mathrm{s}}^{(u)} - {}^{G}\hat{\boldsymbol{r}}_{A}(i)\right)^{\mathsf{T}}}{||\boldsymbol{r}_{\mathrm{s}}^{(u)} - {}^{G}\hat{\boldsymbol{r}}_{A}(i)||} & \underbrace{0 \ \cdots \ 0}_{u-1} & 1 & 0 & \cdots & 0 \end{bmatrix},$$

$$\mathbf{B}^{(u)}(i) = \begin{bmatrix} \lfloor \mathbf{C}_{\hat{q}}^{\mathsf{T}} \, {}^{I}\boldsymbol{r}_{A} \times \rfloor & \frac{\left(\boldsymbol{r}_{\mathrm{s}}^{(u)} - {}^{G}\hat{\boldsymbol{r}}_{\mathrm{IMU}}\right)^{\mathsf{T}}}{||\boldsymbol{r}_{\mathrm{s}}^{(u)} - {}^{G}\hat{\boldsymbol{r}}_{\mathrm{IMU}}||} & \underbrace{0 \cdots 0}_{2(u-1)} & 1 & 0 & \cdots & 0 \end{bmatrix}.$$

When an IMU measurement is available (i.e., every T), it is used to propagate the IMU pose estimate. When a pseudorange measurement is available (i.e., every LTE frame $T_{\mathrm{sub}} = 10$ ms), the antenna's position and the difference between the clock bias of the receiver and each of the eNodeBs are augmented to the state vector. Once $N + 1$ pseudorange measurement epochs are appended the measurement vector, an EKF update is performed. After each update, the states corresponding to the antenna's position and the difference between the clock bias of the receiver and each of the eNodeBs corresponding to N_{rem} epochs are removed from the state vector. The pseudorange measurements corresponding to these states are also removed from the measurement vector and the filter returns to the state propagation stage. Therefore, the update is performed every $N_{\mathrm{rem}}T_{\mathrm{sub}}$. By increasing N_{rem}, the time correlation between the measurement vectors of two consecutive updates decreases. However, increasing N_{rem} decreases the update rate. Therefore, the choice of N_{rem} depends on the level of time-correlation in the measurement noise and the application requirements for the update rate.

5.4.5 Simulation Results

To evaluate the proposed framework, a simulation environment was developed comprising a receiver navigating in an urban area (downtown Riverside, California) over a 6 km trajectory that includes straight segments and turns. The locations of the eNodeBs were simulated using real eNodeBs' locations in that environment. The simulation environment showing the receiver's trajectory and the eNodeBs' positions is shown in Fig. 5.18. The receiver's and eNodeBs' clocks were simulated with a TCXO and an OCXO, respectively.

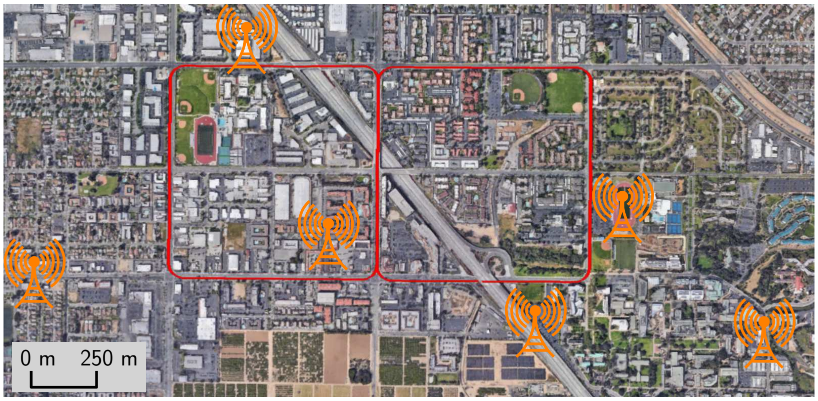


Figure 5.18: Simulated traversed trajectory and the positions of the LTE eNodeBs. Map data: Google Earth

The IMU's rotational velocity and linear acceleration measurements were generated at $T = 0.01$ s. The IMU's measurement noise and time evolution of the IMU's biases are determined by the grade of the IMU. In this simulation, data for a consumer-grade IMU was generated. It is assumed that the LTE pseudoranges were estimated every LTE frame duration, which is $T_{\text{sub}} = 10$ ms.

There are several factors that characterize the behavior of a wireless channel e.g., terrain features, relative speed of the transmitter and receiver, etc. Propagation mode including LOS, reflections, diffractions, and scattering is among these factors to characterize a wireless channel. Two channel models were introduced to capture these factors namely Rician and Rayleigh fading channels [94]. A channel with LOS can be modeled with a Rician fading, while a channel with no LOS can be modeled with a Rayleigh fading. The simulation environment assumes the receiver to have access to the LOS signal and the channel is modeled as a Rician fading channel. To characterize the LOS and multipath signal power and delay profile, the CIR was simulated based on an extended vehicular A (EVA) channel model [95] and the multipath error affecting the pseudorange was simulated based on the model presented in [45, 47]. The simulated CIRs were assumed to be correlated with two different correlation coefficients $\varrho = \{0.8, 0.98\}$. For comparison purposes, Fig. 5.19 shows the simulated multipath error for one of the eNodeBs over 10 s. The standard deviation of the generated multipath was 1.1 m. The measurement noise was assumed to be additive white Gaussian with a standard deviation obtained based on the carrier-to-noise ratio of the received signal for each eNodeB [69].

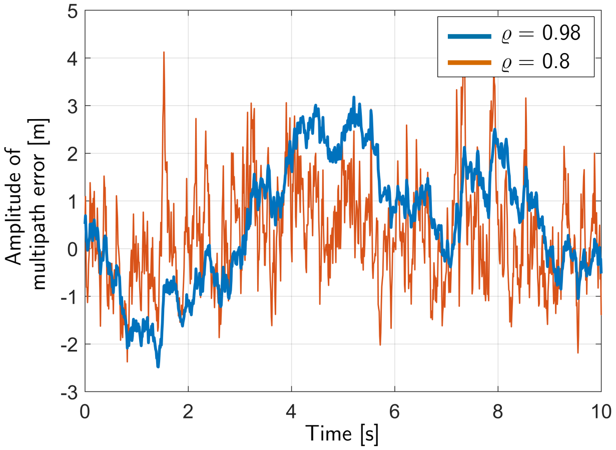


Figure 5.19: Example of the simulated multipath error for one eNodeB over 10 s.

The simulation was repeated for 20 different multipath and noise conditions. Fig. 5.20 shows the average of the 2-D and 3-D position RMSE over the entire simulated trajectory for each run using the proposed method. The values of the 2-D and 3-D position RMSEs were obtained for different update time (i.e., $N_{\text{rem}}T_{\text{sub}}$). The results were compared with an EKF, where the state update is done whenever a pseudorange measurement is available and no state augmentation is performed. For the sake of comparison, in the EKF approach, it is assumed that the pseudorange measurement is available every $N_{\text{rem}}T_{\text{sub}}$. The value of N

was set to 100.

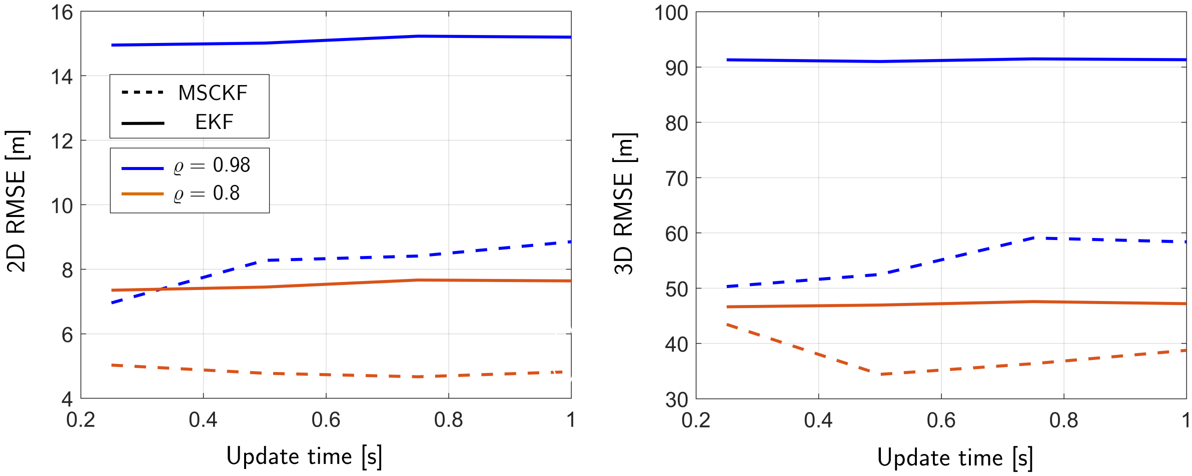


Figure 5.20: 2-D and 3-D position RMSE over the entire simulated trajectory for different update time.

The following conclusions can be drawn from the simulation results.

Remark 1 For both the MSCKF and EKF approaches, the 3-D position RMSE is worse than the 2-D RMSE, since the eNodeBs have approximately similar height and the geometric diversity in the vertical direction is poor.

Remark 2 The proposed MSCKF approach outperforms the EKF approach. The reduction in the RMSE for $\varrho = 0.98$ is higher compared to $\varrho = 0.8$, which means that when the measurement noise is highly time-correlated, the proposed approach can significantly reduce the position estimation error.

Remark 3 From several sets of simulations, it was concluded that a good rule of thumb for choosing N_{rem} is such that $N_{\text{rem}} \approx \lfloor N/2 \rfloor$. Such rule of thumb reduces the RMSE while maintaining a reasonable computational complexity (update time).

Next, the 2-D position RMSE was evaluated for different values of N. For this purpose, the value of N was selected from the set $\{0, 25, 50, 100\}$ and N_{rem} was set to $\lfloor N/2 \rfloor$. Note that when N is zero, the MSCKF approach is equivalent to an EKF since no augmentation is performed. Fig. 5.21 shows the results for this simulation, which was obtained by averaging the obtained 2-D position RMSE over 20 different simulated multipath and noise realizations. The results show that increasing N decreases the RMSE, especially for higher time-correlation in the measurement noise (i.e., $\varrho = 0.98$). However, increasing N increases the update time, which increases the computational burden.

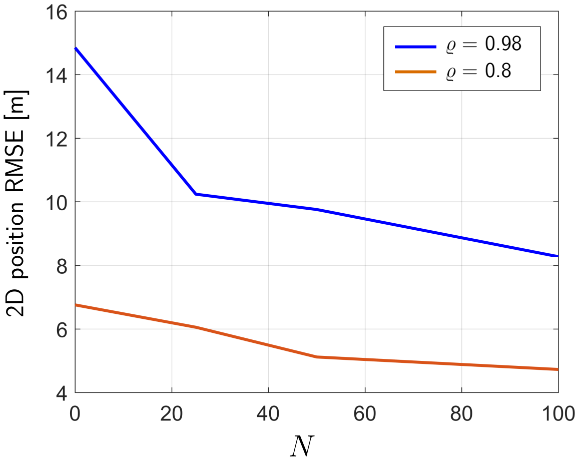


Figure 5.21: 2-D position RMSE over the entire simulated trajectory for different values of N and for $N_{\text{rem}} = \lfloor N/2 \rfloor$

5.4.6 Experimental Results

To evaluate the performance of the proposed framework, an experiment was performed in an urban area (downtown Riverside, California). In this experiment, a ground vehicle was equipped with two consumer-grade 800/1900 MHz cellular omnidirectional Laird antennas to receive LTE signals at 739 MHz and 1955 MHz carrier frequencies from the U.S. cellular provider AT&T. A dual-channel NI USRP-2954R, driven by a GPSDO was used to simultaneously down-mix and synchronously sample LTE signals with 10 MSps. A laptop was used to store LTE samples for post-processing. A Septentrio AsteRx-i V, which is equipped with dual antenna multi-frequency GNSS receiver with RTK and a Vectornav VN-100 MEMS IMU, was used to estimate the position and orientation of the ground vehicle, which was used as the ground truth. Fig. 5.22 shows the experimental hardware setup.

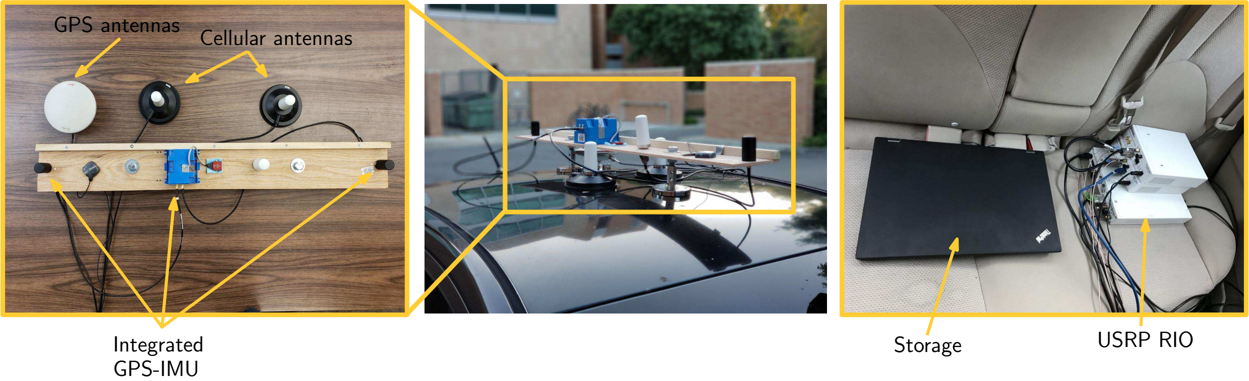


Figure 5.22: Experimental hardware setup

The receiver traversed a trajectory of 1380 m over 190 s while listening to 5 eNodeBs. The stored LTE samples were processed by the proposed SDR in Chapter 3, producing pseudoranges to LTE eNodeBs in the environment. The subaccumulation period was set to two LTE frames, which is $T_{\text{sub}} = 20$ ms.

The derived pseudoranges were used to estimate the receiver's position using the proposed MSCKF framework and the EKF framework. The receiver was assumed to have access to GPS signals at its initial position. Therefore, the receiver was able to estimate the initial values of its position and the difference of its clock bias with each of the eNodeBs, which makes the problem observable [15]. The AsteRx-i V's GNSS-INS provides orientation, position, velocity, and their covariances, which were used to initialize both the MSCKF and EKF frameworks. The gyroscope's and accelerometer's biases and their measurement noise covariances were initialized by taking the mean and variance of 5 seconds of stationary IMU data, respectively. The receiver and eNodeBs clocks were modeled as OCXO with $h_{0_\text{r}} = 8 \times 10^{-20}$, $h_{-2_\text{r}} = 4 \times 10^{-23}$, $h_{0_\text{s}}^{(u)} = 2.6 \times 10^{-22}$, and $h_{-2_\text{s}}^{(u)} = 4 \times 10^{-26}$, where $u = 1, \cdots, 5$. The initial values of the difference of the clock bias and drift of the receiver with each of the eNodeBs were set to 1 m and 0.01 m/s with initial covariance of 1 m^2 and 0.01 m^2/s^2, respectively. The measurement noise variance was determined empirically.

Fig. 5.23(a) shows the 2-D and 3-D position RMSE and maximum error for different values of N. In these results, it is assumed that $\varrho = 0.99$ and $N_{\text{rem}} = \lfloor N/2 \rfloor$. It can be seen that 2-D and 3-D position RMSE and maximum error are decreased by increasing N. The payoff due to increasing N from 50 to 100 diminishes. Fig. 5.23(b) shows the 2-D and 3-D position RMSE for different values of ϱ. In these results, $N = 50$ and $N_{\text{rem}} = \lfloor N/2 \rfloor$. It can be seen that higher ϱ decreases the position RMSE, which shows that the pseudorange measurements' errors were highly correlated. The results show that the proposed framework could reduce the 2-D and 3-D position RMSE by 29% and 64.7%, respectively, and the 2-D and 3-D maximum error by 19.6% and 86.7%, respectively, compared to the EKF approach.

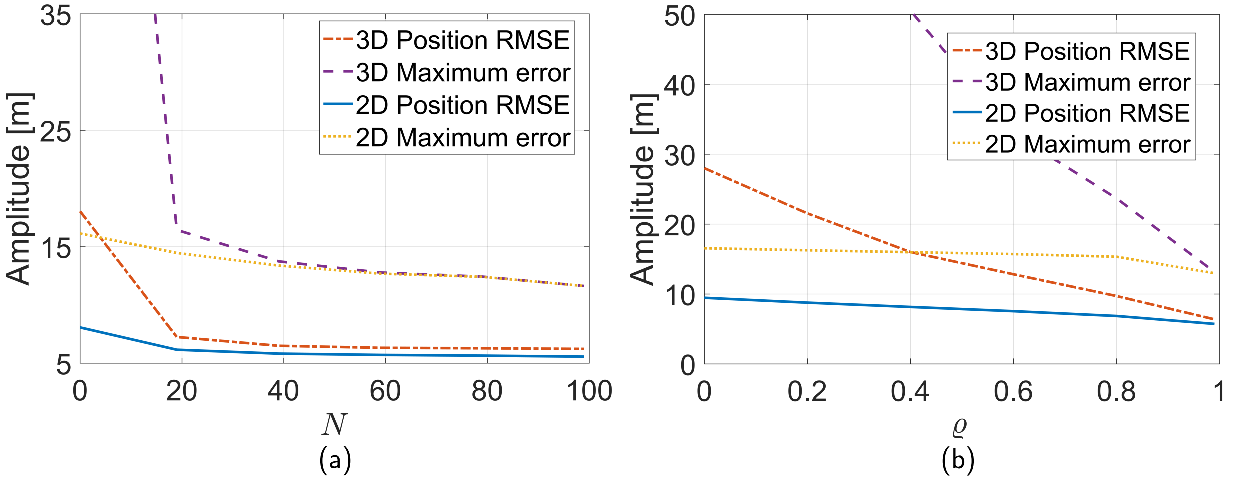


Figure 5.23: Experimental 2-D and 3-D position RMSE for (a) different numbers of states to augment and (b) different values of correlation coefficient

Fig. 5.24 shows the navigation solution errors in east-north-up (ENU) frame and their corresponding $\pm 3\sigma$ bounds for the EKF and proposed frameworks. It can be seen that the navigation solution error is lower for the proposed framework compared to an EKF. It can also be seen that the error in the proposed framework is within the estimated covariance bounds, which means that the filter is consistent. This is not the case for the results obtained by an EKF framework. Note that the growing vehicle's vertical estimation uncertainty is due to a lack of both vehicle's vertical motion and eNodeB's vertical geometric diversity. A calibrated altimeter would help reduce the vertical error and uncertainty.

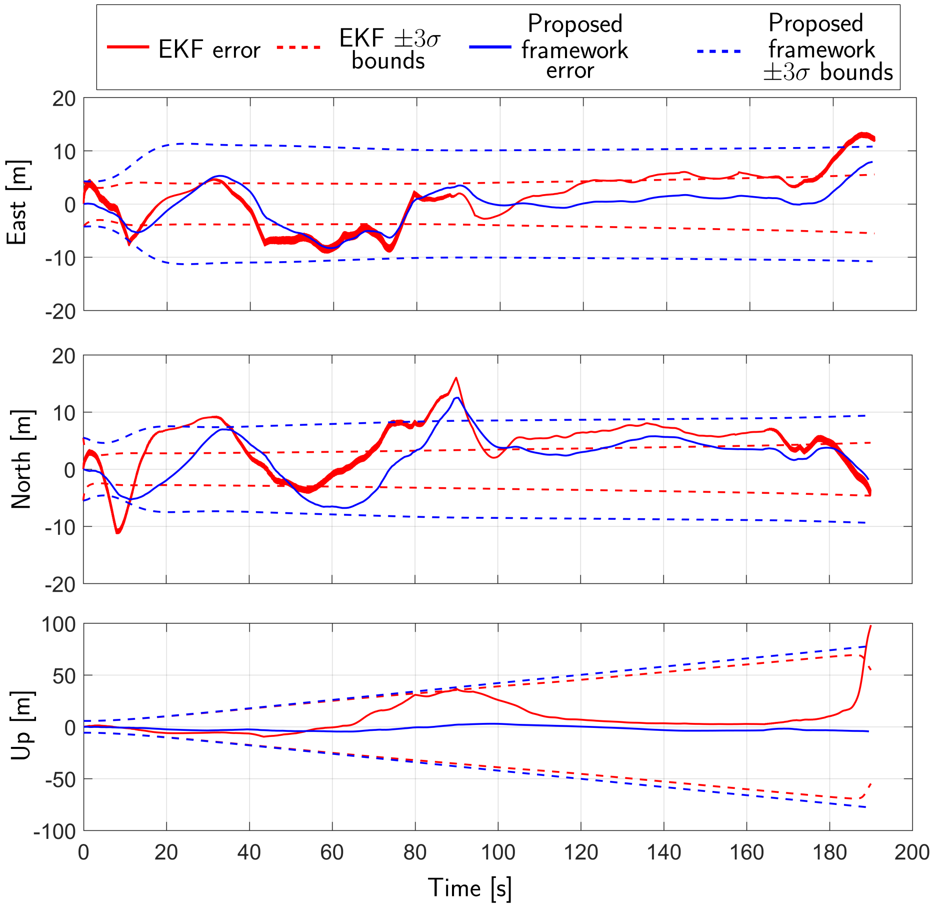


Figure 5.24: Navigation solution errors in ENU frame and their corresponding estimated ±3σ bounds for the EKF and proposed framework

Fig. 5.25 compares the navigation solutions obtained by the proposed MSCKF framework and the EKF framework versus the ground truth. Table 5.7 summarizes the resulting 2-D and 3-D position RMSE and maximum error.

Table 5.7: 2-D and 3-D position RMSE

Method	**2-D RMSE [m]**	**3-D RMSE [m]**	**2-D Maximum error [m]**	**3-D Maximum error [m]**
EKF	8.06	18.04	16.13	98.90
Proposed framework	5.72	6.37	12.97	13.15

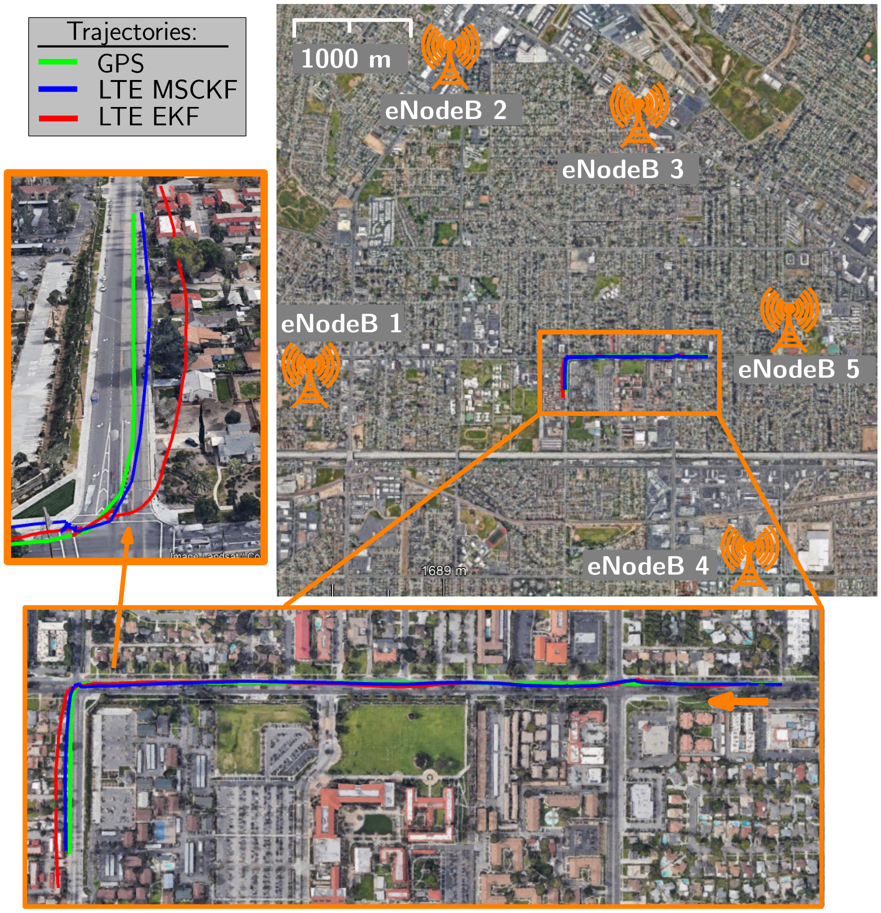


Figure 5.25: Experimental results showing the vehicle's ground truth trajectory (from a GNSS-IMU RTK system) and the estimated trajectory with the proposed MSCKF framework and an EKF. The total traversed trajectory was 1380 m. Image: Google Earth

Chapter 6

Joint TOA and DOA Acquisition and Tracking of LTE Signals

One of the main challenges in opportunistic navigation with LTE signals is the unknown clock biases of the UE and the eNodeBs. Current approaches to overcome this challenge include: (1) estimating and removing the clock bias in a post-processing fashion by using the known position of the UE [30,34], (2) using perfectly synchronized eNodeBs in laboratory-emulated LTE signals [29], or (3) estimating the difference of the clock biases of the UE and each eNodeB in an EKF framework [48]. The first approach does not provide an on-the-fly navigation solution. The second approach is not feasible with real LTE signals, whose eNodeBs are not perfectly synchronized. In the third approach, which was discussed in Chapter 5, certain *a priori* knowledge about the UE's and/or the eNodeBs' states must be assumed in order to make the estimation problem observable [15, 96]. For example, the eNodeBs' positions states were assumed to be known as well as the UE's initial states: position, velocity, clock bias, and clock drift. GPS signals were used to estimate the UE's initial states, and such estimates were used to initialize the EKF, which subsequently only used received LTE signals to estimate the UE's position and velocity and the difference between the UE's clock bias and drift and those of the eNodeBs'. However, such initial knowledge about the UE's states might not be available in many practical scenarios, e.g., cold-start applications in the absence of GNSS signals. To remove the required *a priori* knowledge about the UE's states, the temporal diversity of TOA measurements and spatial diversity of DOA measurements from LTE signals can be used to estimate the location of the receiver in a cold-start fashion.

The problem of joint angle and delay estimation (JADE) was first addressed in [97,98], where MUSIC and ESPRIT were used to jointly estimate the delay and angle [52, 99]. MUSIC and ESPRIT are two statistical techniques, which are based on the eigen-structure of the covariance matrix. These algorithms were obtained based on the assumption of noncoherent received signals. Therefore, in the presence of coherent multipath signals, additional signal processing must be performed [100]. In contrast to the MUSIC and ESPRIT algorithms, the matrix pencil (MP) approach works directly with data and does not need additional signal processing in the presence of coherent multipath signals [101, 102].

MP algorithm was first used in [101] to estimate the parameters of exponentially damped or undamped sinusoids. This idea was later extended to estimating 2-D frequencies in [102]. Later on, MP algorithm was used in different types of applications to estimate angles, TOA, or frequencies of the received signal [103–105]. In [103], a 3-D MP algorithm was used to estimate the frequency, elevation, and azimuth angles of the signal using a 3-D antenna array. In this approach, the TOA measurements, which are generally more accurate than angle measurements are not estimated. In [104, 105], a 2-D MP algorithm was used to estimate the DOA and TOA of the OFDM signals using a uniform linear array (ULA). Note that the estimated DOA using a ULA is always in the interval of $[0, \pi]$. This will introduce an ambiguity in the DOA estimates since signals received at angles $\theta \in [0, \pi]$ and $-\theta$ will be measured as θ. In this chapter, a uniform planar array (UPA) is used to overcome this ambiguity, where a 3-D MP algorithm is used to estimate the TOA, elevation, and azimuth angles of the LTE signals. Then, the performance of this algorithm in the presence of noise is derived using a first-order perturbation analysis.

One of the challenges of all JADE algorithms is their high computational cost. Therefore, they should be used only in the acquisition stage to provide initial estimates of the TOA and DOA and the tracking loops should be used to refine these estimates and track their changes. TOA tracking loops are well-established and are being used in navigation receivers [65]. The direction locked-loops (DiLL) with non-coherent/coherent discriminator functions were proposed for 1-D angle estimation using a ULA [106, 107]. The idea was then extended to a 2-D angle estimation of a mobile satellite communications using a UPA [108]. In the former DiLLs, the discriminator function contains a noticeable tracking bias when the angle is not zero. This bias was removed using a modification factor. In this chapter, a tracking loop to jointly track the TOA and 2-D DOA of LTE signals is proposed, where the estimates of the angles and TOA are first removed from the received signal. This removes the bias of the discriminator function and as a result, the need for modification factor is eliminated.

After discussing the acquisition and tracking stages of the TOA and DOA estimation, the CRLBs of the TOA and DOA estimates are derived to compare the performance of the proposed acquisition and tracking approaches with the best-case performance. The computational complexity of the proposed acquisition and tracking approaches are also compared. Finally, experimental results are provided with real LTE signals, which show higher stability of the proposed structure compared to MP algorithm.

The remainder of this chapter is organized as follows. Section 6.1 summarizes the transmitted and received LTE signal models. Section 6.2 presents the MP algorithm to acquire the TOA and DOA estimates of received LTE signals and analyzes its performance in the presence of noise. Section 6.3 presents the TOA and DOA tracking structure and analyzes its performance in the presence of noise and multipath. Section 6.4 derives the CRLB. Section 6.5 compares the computational complexity of the acquisition and tracking stages. Finally, Sections 6.6 and 6.7 present the simulation and experimental results, respectively.

The results of this chapter are presented in [109, 110].

6.1 Signal Model

At the receiver, a UPA can be used to estimate TOA and DOA (comprised of the azimuth and elevation angles) using the phase difference of the received signal at different antenna elements and different subcarriers. Fig. 6.1 shows a UPA with M antenna elements in the x-direction and N antenna elements in the y-direction. To provide directivity to the antenna array, the spacing between antenna elements should not be very small. However, large spacing causes multiple radiation lobes, which are not desirable. Therefore, the distance between adjacent antenna elements is typically assigned to be $d = \lambda/2$, where $\lambda = c/f_c$ is the received signal wavelength [111].

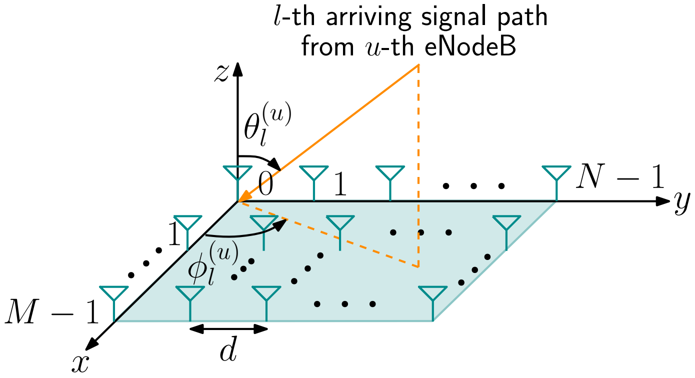


Figure 6.1: UPA structure and DOA representation

The transmitted signal from the u-th eNodeB propagates to the antenna array through $L^{(u)}$ different paths, where the l-th arriving path has an attenuation and delay of $\alpha_l^{(u)}$ and $\tau_l^{(u)}$, respectively, and impinges the antenna array at an azimuth angle $\phi_l^{(u)}$ and an elevation angle $\theta_l^{(u)}$, as shown in Fig. 6.1.

Denoting $\hat{\mathbf{H}}^{(u)} \in \mathbb{C}^{M\times N\times N_s}$ and $\mathbf{H}^{(u)} \in \mathbb{C}^{M\times N\times N_s}$ to be the estimated and true CFRs of the u-th eNodeB, it can be shown that $\hat{\mathbf{H}}^{(u)} = \mathbf{H}^{(u)} + \mathbf{W}$, where $W_{m,n,q} \sim \mathcal{CN}(0, \sigma^2)$ is the contribution of an AWGN channel at the (m, n)-th antenna element and the q-th CRS subcarrier; and

$$\begin{aligned}
H^{(u)}_{m,n,q} &= \sum_{l=0}^{L^{(u)}-1} \sqrt{C}\beta_l^{(u)}\, {x_l^{(u)}}^m {y_l^{(u)}}^n {z_l^{(u)}}^q, \qquad (6.1)\\
\beta_l^{(u)} &\triangleq \alpha_l^{(u)} e^{-j2\pi\nu_{N_{ID}^{Cell}} f_s \tau_l^{(u)}} e^{-j\omega_c \tau_l^{(u)}},\\
x_l^{(u)} &\triangleq e^{j\frac{\omega_c d}{c}\sin\theta_l^{(u)}\cos\phi_l^{(u)}},\\
y_l^{(u)} &\triangleq e^{j\frac{\omega_c d}{c}\sin\theta_l^{(u)}\sin\phi_l^{(u)}},\\
z_l^{(u)} &\triangleq e^{-j2\pi f_s N_{CRS}\tau_l^{(u)}},
\end{aligned}$$

where $f_s = 15$ kHz is the subcarrier spacing; $\nu_{N_{ID}^{Cell}}$ is a constant shift in the first CRS subcarrier number; $N_{CRS} = 6$; C is the carrier power; $\omega_c = 2\pi f_c$; and it is assumed that $\alpha_0^{(u)} = 1$. The objective is to estimate $\left(x_l^{(u)}, y_l^{(u)}, z_l^{(u)}\right)$ and obtain the relative TOA and DOA of each path as

$$\hat{\theta}_l^{(u)} = \sin^{-1}\left(\sqrt{\kappa^2 + \varsigma^2}\right), \tag{6.2}$$

$$\hat{\phi}_l^{(u)} = \operatorname{atan2}\left(\varsigma, \kappa\right), \tag{6.3}$$

$$\hat{\tau}_l^{(u)} = -\frac{1}{2\pi f_s N_{CRS}} \operatorname{atan2}\left(\Im\left\{\hat{z}_l^{(u)}\right\}, \Re\left\{\hat{z}_l^{(u)}\right\}\right), \tag{6.4}$$

where $\Re\{\cdot\}$ and $\Im\{\cdot\}$ represent real and imaginary parts, respectively; atan2 is the four-quadrant inverse tangent function and

$$\begin{aligned}
\kappa &\triangleq \frac{c}{\omega_c\, d} \operatorname{atan2}\left(\Im\left\{\hat{x}_l^{(u)}\right\}, \Re\left\{\hat{x}_l^{(u)}\right\}\right),\\
\varsigma &\triangleq \frac{c}{\omega_c\, d} \operatorname{atan2}\left(\Im\left\{\hat{y}_l^{(u)}\right\}, \Re\left\{\hat{y}_l^{(u)}\right\}\right).
\end{aligned}$$

The TOA and DOA estimation is performed in two stages, namely acquisition and tracking, which are discussed in the next two sections. For simplicity of notations, the superscript (u), which denotes the u-th eNodeB, will be dropped in the sequel, unless it is required.

6.2 Signal Acquisition

In the acquisition stage, the 3-D MP algorithm is used to jointly estimate the TOAs and DOAs of received LTE signals. This section discusses the process of estimating the TOA and DOA and characterizes the estimation performance in the presence of noise.

6.2.1 TOA and DOA Estimation

A 3-D MP algorithm can be divided into three 1-D MP algorithms to estimate x_l, y_l, and z_l individually [102,103]. There are five main steps in a 3-D MP algorithm, which are discussed next.

Step 1: Construct the estimated enhanced-matrix as

$$\hat{\mathbf{E}} \triangleq \begin{bmatrix} \hat{\mathbf{E}}_0 & \hat{\mathbf{E}}_1 & \cdots & \hat{\mathbf{E}}_{N_s-R} \\ \hat{\mathbf{E}}_1 & \hat{\mathbf{E}}_2 & \cdots & \hat{\mathbf{E}}_{N_s-R+1} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{\mathbf{E}}_{R-1} & \hat{\mathbf{E}}_R & \cdots & \hat{\mathbf{E}}_{N_s-1} \end{bmatrix}_{PKR\times[(M-P+1)(N-K+1)(N_s-R+1)]},$$

$$\hat{\mathbf{E}}_k \triangleq \begin{bmatrix} \hat{\mathbf{E}}_{0,k} & \hat{\mathbf{E}}_{1,k} & \cdots & \hat{\mathbf{E}}_{N-K,k} \\ \hat{\mathbf{E}}_{1,k} & \hat{\mathbf{E}}_{2,k} & \cdots & \hat{\mathbf{E}}_{N-K+1,k} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{\mathbf{E}}_{K-1,k} & \hat{\mathbf{E}}_{K,k} & \cdots & \hat{\mathbf{E}}_{N-1,k} \end{bmatrix},$$

$$\hat{\mathbf{E}}_{j,k} \triangleq \begin{bmatrix} \hat{H}_{0,j,k} & \hat{H}_{1,j,k} & \cdots & \hat{H}_{M-P,j,k} \\ \hat{H}_{1,j,k} & \hat{H}_{2,j,k} & \cdots & \hat{H}_{M-P+1,j,k} \\ \vdots & \vdots & \ddots & \vdots \\ \hat{H}_{P-1,j,k} & \hat{H}_{P,j,k} & \cdots & \hat{H}_{M-1,j,k} \end{bmatrix},$$

$$\text{for} \quad j = 0, 1, \ldots, N-1, \quad \text{and} \quad k = 0, 1, \ldots, N_s - 1,$$

where P, K, and R are pencil parameters. The pencil parameters are tuning parameters that are used to improve the estimation accuracy and must satisfy the following necessary conditions

$$\begin{aligned} &(P-1)RK \geq L, \qquad (K-1)PK \geq L, \qquad (R-1)PK \geq L, \\ &(M-P+1)(N-K+1)(N_s-R+1) \geq L. \end{aligned}$$

For efficient noise filtering, it has been shown that the pencil parameters should be selected between one third and two third of their corresponding parameters [101].

Step 2: Decompose $\hat{\mathbf{E}}$ using an SVD operation as $\hat{\mathbf{E}} = \hat{\mathbf{U}}\hat{\mathbf{\Sigma}}\hat{\mathbf{V}}^{\mathsf{H}}$, where $\hat{\mathbf{U}}$ and $\hat{\mathbf{V}}$ are unitary matrices of singular vectors, and $\hat{\mathbf{\Sigma}}$ is the matrix of singular values $\sigma_1 \geq \cdots \geq \sigma_{KPR}$. Next, use the MDL criterion to estimate the multipath channel length [54].

Step 3: Knowing the length of the channel impulse response, the enhanced matrix $\hat{\mathbf{E}}$ can be decomposed into the signal and noise subspaces as $\hat{\mathbf{E}} = \hat{\mathbf{U}}_s\hat{\mathbf{\Sigma}}_s\hat{\mathbf{V}}_s^{\mathsf{H}} + \hat{\mathbf{U}}_n\hat{\mathbf{\Sigma}}_n\hat{\mathbf{V}}_n^{\mathsf{H}}$, where $\hat{\mathbf{U}}_s$ and $\hat{\mathbf{V}}_s$ are composed of the singular vectors corresponding to the $\hat{L}$ largest singular values of $\hat{\mathbf{E}}$ and span the signal subspace of $\hat{\mathbf{E}}$; and $\hat{\mathbf{U}}_n$ and $\hat{\mathbf{V}}_n$ span the noise subspace of $\hat{\mathbf{E}}$. Remove the last and first PK rows of $\mathbf{U}_s$ to build the matrices $\hat{\mathbf{U}}_{s_1}$ and $\hat{\mathbf{U}}_{s_2}$, respectively, as

$$\begin{aligned} &\hat{\mathbf{U}}_{s_1} = \mathbf{C}_1\mathbf{U}_s, \qquad \mathbf{C}_1 = \left[\mathbf{I}_{PK(R-1)}, \mathbf{0}_{PK(R-1)\times PK}\right], \\ &\hat{\mathbf{U}}_{s_2} = \mathbf{C}_2\mathbf{U}_s, \qquad \mathbf{C}_2 = \left[\mathbf{0}_{PK(R-1)\times PK}, \mathbf{I}_{PK(R-1)}\right]. \end{aligned} \tag{6.5}$$

Derive the generalized eigenvalues of the pencil pair $(\hat{\mathbf{U}}_{s_2}, \hat{\mathbf{U}}_{s_1})$, which are equal to the eigenvalues of $\hat{\mathbf{\Psi}}_z = \hat{\mathbf{U}}_{s_1}^{\dagger}\hat{\mathbf{U}}_{s_2}$, where † is the Moore-Penrose pseudo-inverse. The resulting eigenvalues are permutation of $\left\{\hat{z}_0, \cdots, \hat{z}_{\hat{L}-1}\right\}$.

Step 4: Form the matrix $\hat{\mathbf{U}}_j = \mathbf{J}\hat{\mathbf{U}}_s$, where $\mathbf{J}$ is the permutation matrix given by

$$\mathbf{J} \triangleq [\mathbf{J}_0, \mathbf{J}_1, \cdots, \mathbf{J}_{K-1}]^{\mathsf{T}},$$

where $\mathbf{J}_i$ is defined as

$$\begin{aligned}\mathbf{J}_i \triangleq [&\boldsymbol{p}(1+iP), \cdots, \boldsymbol{p}(P+iP),\\ &\boldsymbol{p}(1+iP+PK), \cdots, \boldsymbol{p}(P+iP+PK), \cdots\cdots,\\ &\boldsymbol{p}(1+iP+(R-1)PK), \cdots, \boldsymbol{p}(P+iP+(R-1)PK)],\end{aligned}$$

where $\boldsymbol{p}(\ell)$ is a column vector of size KPR with one in the (ℓ)-th element and zero elsewhere. Similar to (6.5), build $\hat{\mathbf{U}}_{j_1}$ and $\hat{\mathbf{U}}_{j_2}$ from $\hat{\mathbf{U}}_j$ by removing the last and first PR rows, respectively. The eigenvalues of $\hat{\mathbf{\Psi}}_y = \hat{\mathbf{U}}_{j_1}^{\dagger}\hat{\mathbf{U}}_{j_2}$ are permutation of $\left\{\hat{y}_0, \cdots, \hat{y}_{\hat{L}-1}\right\}$.

Step 5: Form the matrix $\hat{\mathbf{U}}_p = \mathbf{P}\hat{\mathbf{U}}_s$, where $\mathbf{P}$ is the permutation matrix defined as

$$\begin{aligned}\mathbf{P} \triangleq [&\boldsymbol{p}(1), \boldsymbol{p}(1+P), \cdots, \boldsymbol{p}(1+(KR-1)P),\\ &\boldsymbol{p}(2), \boldsymbol{p}(2+P), \cdots, \boldsymbol{p}(2+(KR-1)P), \cdots\cdots,\\ &\boldsymbol{p}(P), \boldsymbol{p}(P+P), \cdots, \boldsymbol{p}(P+(KR-1)P)]^{\mathsf{T}}.\end{aligned}$$

Similar to (6.5), build $\hat{\mathbf{U}}_{p_1}$ and $\hat{\mathbf{U}}_{p_2}$ from $\hat{\mathbf{U}}_p$ by removing the last and first KR rows, respectively. The eigenvalues of $\hat{\mathbf{\Psi}}_x = \hat{\mathbf{U}}_{p_1}^{\dagger}\hat{\mathbf{U}}_{p_2}$ are permutation of $\left\{\hat{x}_0, \cdots, \hat{x}_{\hat{L}-1}\right\}$.

The estimated values of $\{x_l\}_{l=0}^{\hat{L}-1}$, $\{y_l\}_{l=0}^{\hat{L}-1}$, and $\{z_l\}_{l=0}^{\hat{L}-1}$ are not necessarily in the same order. Therefore, they must be paired together correctly before calculating the TOA and DOA of the LOS signal. It can be shown that $\mathbf{\Psi}_x$, $\mathbf{\Psi}_y$, and $\mathbf{\Psi}_z$ have the same eigenvectors, which implies

$$\mathbf{\Psi}_x = \mathbf{A}\mathbf{X}\mathbf{A}^{-1},$$
$$\mathbf{\Psi}_y = \mathbf{A}\mathbf{Y}\mathbf{A}^{-1},$$
$$\mathbf{\Psi}_z = \mathbf{A}\mathbf{Z}\mathbf{A}^{-1},$$

where $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$ are diagonal matrices consisting the permutation of estimation of $\{x_l\}_{l=0}^{\hat{L}-1}$, $\{y_l\}_{l=0}^{\hat{L}-1}$, and $\{z_l\}_{l=0}^{\hat{L}-1}$, respectively. Next, the eigenvalues of $\mathbf{\Psi}_z$ are used to calculate the TOA of each multipath and the TOA estimates are sorted in ascending order. The eigenvectors of $\mathbf{\Psi}_z$, which are the column vectors of matrix $\mathbf{A}$, must be also sorted according to the TOA estimates, yielding the matrix $\mathbf{A}'$. Then, define the matrices $\mathbf{X}'$ and $\mathbf{Y}'$ according to

$$\mathbf{X}' = \mathbf{A}'^{-1}\mathbf{\Psi}_x\mathbf{A}',$$
$$\mathbf{Y}' = \mathbf{A}'^{-1}\mathbf{\Psi}_y\mathbf{A}'.$$

The diagonal elements of $\mathbf{X}'$ and $\mathbf{Y}'$ are $\{\hat{x}_1, \cdots, \hat{x}_{\hat{L}}\}$ and $\{\hat{y}_1, \cdots, \hat{y}_{\hat{L}}\}$, respectively, and are in the right order.

After estimating the TOA and DOA of the LOS and multipath signals, the LOS DOA and TOA estimates will be tracked in the tracking loop to refine the estimates and track the changes over time. In this dissertation, in order to remove the tracking bias, which were discussed in [106, 107], from the tracking loops discriminator functions, the LOS DOA and TOA estimates are removed from the CFR resulting in

$$H'_{m,n,q} \triangleq \hat{H}_{m,n,q}\hat{x}_0^{-m}\hat{y}_0^{-n}\hat{z}_0^{-q}. \tag{6.6}$$

Denoting the LOS TOA and DOA estimation error by $e_\tau \triangleq \hat{\tau}_0 - \tau_0$, $e_\phi \triangleq \hat{\phi}_0 - \phi_0$, and

$e_\theta \triangleq \hat{\theta}_0 - \theta_0$, and assuming small TOA and DOA estimation errors, it can be shown that $H'(m,n,q)$ can be rewritten as

$$\begin{aligned} {H'}_{m,n,q} =& \sqrt{C}\beta_0 e^{-j\frac{\omega_c d}{c}(m\cos\theta_0\cos\phi_0 + n\cos\theta_0\sin\phi_0)e_\theta} \\ & e^{j\frac{\omega_c d}{c}(m\sin\theta_0\sin\phi_0 - n\sin\theta_0\cos\phi_0)e_\phi} \\ & e^{j2\pi q f_s N_{CRS} e_\tau} + I_{m,n,q} + W'_{m,n,q}, \end{aligned} \tag{6.7}$$

where $I_{m,n,q}$ is the effect of multipath and is defined as

$$I_{m,n,q} \triangleq \sqrt{C}\sum_{l=1}^{L-1}\beta_l \ (x_l/\hat{x}_0)^m (y_l/\hat{y}_0)^n (z_l/\hat{z}_0)^q,$$

and $W'_{m,n,q}$ is the noise component defined as $W'_{m,n,q} \triangleq W_{m,n,q}\hat{x}_0^{-m}\hat{y}_0^{-n}\hat{z}_0^{-q}$, where $W'_{m,n,q} \sim \mathcal{CN}(0,\sigma^2)$. The derivation of (6.7) ia detailed in Appendix A.1.

6.2.2 Noise Performance Analysis

In the presence of noise, the estimated DOA and TOA are slightly different than their actual values. The statistics of this discrepancy will be derived in this subsection.

In Subsection 6.2.1, it was shown that the values of $\{\hat{z}_l\}_{i=0}^{\hat{L}}$ are the eigenvalues of $\hat{\mathbf{U}}_{s_1}^\dagger \hat{\mathbf{U}}_{s_2}$. Using first-order perturbation theory, it can be shown that the perturbation of the eigenvalue $\hat{z}_i$, which is denoted by Δz_i, is obtained as

$$\Delta z_i = \frac{\boldsymbol{s}_i^{\mathsf{H}} \Delta\left(\mathbf{U}_{s_1}^\dagger \mathbf{U}_{s_2}\right)\boldsymbol{r}_i}{\boldsymbol{s}_i^{\mathsf{H}}\boldsymbol{r}_i}, \tag{6.8}$$

where $\boldsymbol{s}_i$ and $\boldsymbol{r}_i$ are the left and right eigenvectors of $\mathbf{U}_{s_1}^\dagger \mathbf{U}_{s_2}$, respectively, corresponding to $\hat{z}_i$ [112]. Using the equalities $\Delta\left(\mathbf{U}_{s_1}^\dagger \mathbf{U}_{s_2}\right) = \Delta\mathbf{U}_{s_1}^\dagger \mathbf{U}_{s_2} + \mathbf{U}_{s_1}^\dagger \Delta\mathbf{U}_{s_2}$, $\Delta\mathbf{U}_{s_1}^\dagger = -\mathbf{U}_{s_1}^\dagger \Delta\mathbf{U}_{s_1}\mathbf{U}_{s_1}^\dagger$, and the facts that $\mathbf{U}_s^\dagger = \mathbf{U}_s^{\mathsf{H}}$, $\mathbf{C}_1^\dagger = \mathbf{C}_1^{\mathsf{H}}$, and $\mathbf{U}_{s_1}^\dagger \mathbf{U}_{s_2}\boldsymbol{r}_i = z_i\boldsymbol{r}_i$, equation (6.8) can be simplified to

$$\Delta z_i = \frac{\boldsymbol{s}_i^{\mathsf{H}} \mathbf{U}_s^{\mathsf{H}} \mathbf{C}_1^{\mathsf{H}} \left(\mathbf{C}_2 - z_i \mathbf{C}_1\right) \Delta \mathbf{U}_s \boldsymbol{r}_i}{\boldsymbol{s}_i^{\mathsf{H}} \boldsymbol{r}_i}. \tag{6.9}$$

It has been shown that $\Delta \mathbf{U}_s = \mathbf{U}_n \mathbf{U}_n^{\mathsf{H}} \Delta \mathbf{E} \mathbf{V}_s \boldsymbol{\Sigma}_s^{-1}$ [113]. Therefore, equation (6.9) can be simplified to

$$\Delta z_i = \boldsymbol{a}_i^{\mathsf{H}} \Delta \mathbf{E} \boldsymbol{q}_i, \tag{6.10}$$

where $\boldsymbol{a}_i^{\mathsf{H}} = \frac{\boldsymbol{s}_i^{\mathsf{H}} \mathbf{U}_s^{\mathsf{H}} \mathbf{C}_1^{\mathsf{H}} (\mathbf{C}_2 - z_i \mathbf{C}_1) \mathbf{U}_n \mathbf{U}_n^{\mathsf{H}}}{\boldsymbol{s}_i^{\mathsf{H}} \boldsymbol{r}_i}$ and $\boldsymbol{q}_i = \mathbf{V}_s \boldsymbol{\Sigma}_s^{-1} \boldsymbol{r}_i$. After some algebraic manipulation and using the fact that $\Delta \mathbf{H} = \mathbf{W}$, equation (6.10) can be rewritten as

$$\Delta z_i = \boldsymbol{a}_i^{\mathsf{H}} \mathbf{Q} \text{vec} \left\{ \mathbf{W} \right\}, \tag{6.11}$$

where

$$\mathbf{Q} = \begin{bmatrix} \mathbf{Q}_0 \cdots \mathbf{Q}_{N_s-R} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} \;\; \mathbf{Q}_0 \quad \cdots & \mathbf{Q}_{N_s-R} & \ddots & \vdots \\ \vdots \quad \ddots \quad \ddots & \vdots & \ddots & \mathbf{0} \\ \mathbf{0} \;\; \cdots \quad \mathbf{0} & \mathbf{Q}_0 & \cdots & \mathbf{Q}_{N_s-R} \end{bmatrix}_{PKR \times MNN_s},$$

$$\mathbf{Q}_k = \begin{bmatrix} \mathbf{Q}_{0,k} & \cdots & \mathbf{Q}_{N-K,k} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{Q}_{0,k} & \cdots & \mathbf{Q}_{N-K,k} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \mathbf{Q}_{0,k} & \cdots & \mathbf{Q}_{N-K,k} \end{bmatrix}_{PK \times MN},$$

$$\mathbf{Q}_{l,k} = \begin{bmatrix} q_{il'} & \cdots & q_{il'+M-P} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & q_{il'} & \cdots & q_{il'+M-P} \end{bmatrix}_{P\times M},$$

$$\text{for} \quad l' = (k(N-K+1)+l)(M-P+1).$$

Using (6.11), variance of Δz_i can be obtained as

$$\mathrm{var}\{\Delta z_i\} = \sigma^2 \boldsymbol{a}_i^{\mathsf{H}} \mathbf{Q}\mathbf{Q}^{\mathsf{H}} \boldsymbol{a}_i. \tag{6.12}$$

Therefore, the variance of τ_i estimation error can be obtained as

$$\mathrm{var}\{\Delta \tau_i\} = \frac{1}{2\left(2\pi f_s N_{CRS}\right)^2} \mathrm{var}\{\Delta z_i\}. \tag{6.13}$$

A similar approach can be used to derive $\mathrm{var}\{\Delta x_i\}$ and $\mathrm{var}\{\Delta y_i\}$, resulting in a similar structure to (6.12). Note that $\boldsymbol{a}_i^{\mathsf{H}}$ is replaced by $\boldsymbol{a}_i^{\mathsf{H}} = \frac{\boldsymbol{s}_i^{\mathsf{H}}\mathbf{U}_s^{\mathsf{H}}\mathbf{J}^{\dagger}\mathbf{C}_1^{\mathsf{H}}(\mathbf{C}_2 - y_i\mathbf{C}_1)\mathbf{J}\mathbf{U}_n\mathbf{U}_n^{\mathsf{H}}}{\boldsymbol{s}_i^{\mathsf{H}}\boldsymbol{r}_i}$ for Δy_i and $\boldsymbol{a}_i^{\mathsf{H}} = \frac{\boldsymbol{s}_i^{\mathsf{H}}\mathbf{U}_s^{\mathsf{H}}\mathbf{P}^{\dagger}\mathbf{C}_1^{\mathsf{H}}(\mathbf{C}_2 - x_i\mathbf{C}_1)\mathbf{P}\mathbf{U}_n\mathbf{U}_n^{\mathsf{H}}}{\boldsymbol{s}_i^{\mathsf{H}}\boldsymbol{r}_i}$ for Δx_i. Also, note that $\boldsymbol{s}_i$ and $\boldsymbol{r}_i$ are the left and right eigenvectors of $\mathbf{U}_{j_1}^{\dagger}\mathbf{U}_{j_2}$ and $\mathbf{U}_{p_1}^{\dagger}\mathbf{U}_{p_2}$ for Δy_i and Δx_i, respectively, and matrices $\mathbf{C}_1$ and $\mathbf{C}_2$ are used to remove the first and last few rows of $\mathbf{U}_p$ and $\mathbf{U}_j$ as discussed in the last subsection. The variance of the estimation of θ and ϕ can be obtained as

$$\begin{aligned} \mathrm{var}\{\Delta\theta_i\} = & \frac{c^2}{2\omega_c^2 d^2 \cos^2\theta_i} \left[\cos^2\phi_i \mathrm{var}\{\Delta x_i\} + \sin^2\phi_i \mathrm{var}\{\Delta y_i\} \right. \\ & \left. + 2\sin\phi_i\cos\phi_i \Re\left\{\mathrm{cov}\{\Delta x_i, \Delta y_i\}\right\}\right], \end{aligned} \tag{6.14}$$

$$\begin{aligned} \mathrm{var}\{\Delta\phi_i\} = & \frac{c^2}{2\omega_c^2 d^2 \sin^2\theta_i} \left[\sin^2\phi_i \mathrm{var}\{\Delta x_i\} + \cos^2\phi_i \mathrm{var}\{\Delta y_i\} \right. \\ & \left. - 2\sin\phi_i\cos\phi_i \Re\left\{\mathrm{cov}\{\Delta x_i, \Delta y_i\}\right\}\right]. \end{aligned} \tag{6.15}$$

6.3 Signal Tracking

In the tracking stage, the receiver refines the TOA and DOA estimates and keeps track of their changes. Fig. 6.2 shows the structure of the proposed tracking stage, where azimuth, elevation, and delay locked-loops (ALL, ELL, and DLL, respectively) are used to estimate and remove the TOA and DOA errors. For this purpose, an estimate of the TOA and DOA errors, $\hat{e}_\tau$, $\hat{e}_\theta$, and $\hat{e}_\phi$, are first removed from ${H'}_{m,n,q}$ resulting in

$$\begin{aligned}{H''}_{m,n,q} =&\sqrt{C}\beta_0 e^{j\frac{\omega_c d}{c}(m\cos\theta_0\cos\phi_0+n\cos\theta_0\sin\phi_0)\Delta e_\theta}\\ &e^{-j\frac{\omega_c d}{c}(m\sin\theta_0\sin\phi_0-n\sin\theta_0\cos\phi_0)\Delta e_\phi}\\ &e^{-j2\pi q f_s N_{CRS}\Delta e_\tau}+I'_{m,n,q}+W''_{m,n,q},\end{aligned} \tag{6.16}$$

where $I'_{m,n,q}$ and $W''_{m,n,q}$ are the interference and noise components, respectively, after removing the TOA and DOA errors; and $\Delta e_\tau \triangleq \hat{e}_\tau - e_\tau$, $\Delta e_\phi \triangleq \hat{e}_\phi - e_\phi$, and $\Delta e_\theta \triangleq \hat{e}_\theta - e_\theta$ are TOA and DOA tracking loop errors. Next, a noncoherent discriminator function is used in each loop to obtain the tracking error signals. Finally, low pass filters and accumulators are used to smooth and accumulate the error signals.

In the next subsections, the structure of these loops and their performance in the presence of noise and multipath are discussed in details.

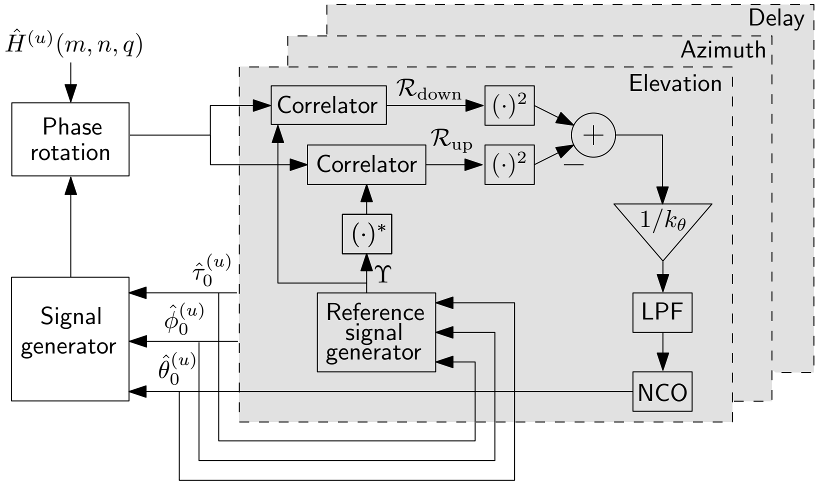


Figure 6.2: ELL, ALL, and DLL tracking loop structure. The ALL and DLL are identical to the ELL shown above with appropriate modifications to their respective discriminators, scaling, and reference signal generators.

6.3.1 ELL

Discriminator Function

The elevation angle discriminator function is defined as

$$D_\theta \triangleq \begin{cases} \sum_{q=0}^{N_s-1}\sum_{n=0}^{N-1}\left[|\mathcal{R}_{\text{down}}|^2 - |\mathcal{R}_{\text{up}}|^2\right], & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \sum_{q=0}^{N_s-1}\sum_{m=0}^{M-1}\left[|\mathcal{R}_{\text{down}}|^2 - |\mathcal{R}_{\text{up}}|^2\right], & \text{otherwise,} \end{cases}$$

where two different conditions are used to keep the tracking error bounded; $\eta_{\text{thr}} = \frac{\sqrt{2}}{2}$; and $\mathcal{R}_{\text{down}}$ and $\mathcal{R}_{\text{up}}$ are the down and up cross-correlation functions of $H''_{m,n,q}$ with the up-down locally generated signal Υ and its conjugate, respectively, which are defined according to

$$\mathcal{R}_{\text{down}} \triangleq \begin{cases} \sum_{m=0}^{M-1} H''_{m,n,q}\Upsilon_m, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \sum_{n=0}^{N-1} H''_{m,n,q}\Upsilon_n, & \text{otherwise,} \end{cases}$$

$$\mathcal{R}_{\text{up}} \triangleq \begin{cases} \sum_{m=0}^{M-1} H''_{m,n,q} \Upsilon_m^*, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \sum_{n=0}^{N-1} H''_{m,n,q} \Upsilon_n^*, & \text{otherwise}, \end{cases}$$

$$\Upsilon_m \triangleq \begin{cases} e^{j\frac{\omega_c d}{c}\left(m\cos\hat{\theta}_0\cos\hat{\phi}_0\xi_\theta\right)}, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ e^{j\frac{\omega_c d}{c}\left(m\cos\hat{\theta}_0\sin\hat{\phi}_0\xi_\theta\right)}, & \text{otherwise}, \end{cases}$$

where ξ_θ is the up-down correlator spacing. It can be shown that

$$\mathcal{R}_{\text{down}} = S_{\text{down}} + I_{\text{down}} + n_{\text{down}},$$
$$\mathcal{R}_{\text{up}} = S_{\text{up}} + I_{\text{up}} + n_{\text{up}},$$

where S, I, and n are the overall signal, interference, and noise components of the correlation functions, respectively, which are defined according to

$$\begin{aligned} S_{\text{down}} &\triangleq \begin{cases} \sqrt{C}e^{j\vartheta}\frac{\sin(MA_\theta(\Delta e_\theta+\xi_\theta))}{\sin(A_\theta(\Delta e_\theta+\xi_\theta))}, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \sqrt{C}e^{j\vartheta}\frac{\sin(NB_\theta(\Delta e_\theta+\xi_\theta))}{\sin(B_\theta(\Delta e_\theta+\xi_\theta))}, & \text{otherwise}, \end{cases} \\ I_{\text{down}} &\triangleq \begin{cases} \sum_{m=0}^{M-1} I'_{m,n,q} \Upsilon_m, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \sum_{n=0}^{N-1} I'_{m,n,q} \Upsilon_n, & \text{otherwise}, \end{cases} \\ n_{\text{down}} &\triangleq \begin{cases} \sum_{m=0}^{M-1} V'_{m,n,q} \Upsilon_m, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \sum_{n=0}^{N-1} V'_{m,n,q} \Upsilon_n, & \text{otherwise}, \end{cases} \end{aligned} \tag{6.17}$$

where ϑ is the overall phase; $A_\theta \triangleq \frac{\omega_c d}{2c}\cos\hat{\theta}_0\cos\hat{\phi}_0$, $B_\theta \triangleq \frac{\omega_c d}{2c}\cos\hat{\theta}_0\sin\hat{\phi}_0$; S_{up} has similar structure to S_{down} except for a negative sign before ξ_θ; and I_{up} and n_{up} have similar structure to I_{down} and n_{down} except for Υ^* instead of Υ.

To evaluate the performance of the ELL discriminator function in the presence of noise, an AWGN channel is first considered, where $I_{\text{down}} = I_{\text{up}} = 0$. In an AWGN channel, the elevation angle discriminator function can be rewritten as

$$D_\theta = S_\theta + n_\theta,$$

where S_θ is the S-curve, representing the signal part of the discriminator function given by

$$S_\theta = \begin{cases} CNN_s\left[\left(\frac{\sin(MA_\theta(\Delta e_\theta+\xi_\theta))}{\sin(A_\theta(\Delta e_\theta+\xi_\theta))}\right)^2 - \left(\frac{\sin(MA_\theta(\Delta e_\theta-\xi_\theta))}{\sin(A_\theta(\Delta e_\theta-\xi_\theta))}\right)^2\right], & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ CMN_s\left[\left(\frac{\sin(NB_\theta(\Delta e_\theta+\xi_\theta))}{\sin(B_\theta(\Delta e_\theta+\xi_\theta))}\right)^2 - \left(\frac{\sin(NB_\theta(\Delta e_\theta-\xi_\theta))}{\sin(B_\theta(\Delta e_\theta-\xi_\theta))}\right)^2\right], & \text{otherwise,} \end{cases} \tag{6.18}$$

and n_θ is the noise part of the discriminator function. It can be shown that n_θ is zero-mean with the following variance

$$\text{var}\{n_\theta\} = \begin{cases} 2N_sNM^2\sigma^4\left(1 + \frac{2C}{M\sigma^2\sin^2(\frac{\pi}{2M})}\right), \\ \qquad \text{if } |\sin\phi_0| < \eta_{\text{thr}} \text{ and } \xi_\theta = \frac{\pi}{2MA_\theta}, \\ 2N_sMN^2\sigma^4\left(1 + \frac{2C}{N\sigma^2\sin^2(\frac{\pi}{2N})}\right), \\ \qquad \text{if } |\sin\phi_0| \geq \eta_{\text{thr}} \text{ and } \xi_\theta = \frac{\pi}{2NB_\theta}. \end{cases} \tag{6.19}$$

In the sequel, the ELL correlator spacing is assumed to be $\xi_\theta = \frac{\pi}{2MA_\theta}$ for $|\sin\phi_0| < \eta_{\text{thr}}$ and $\xi_\theta = \frac{\pi}{2NB_\theta}$ otherwise.

It can be seen from (6.18) that the ELL S-curve depends on the elevation and azimuth angles and the correlator spacings. Fig. 6.3 shows the ELL S-curve for $C = 1$, $N_s = 1$, $M = N = 8$, $\phi_0 = \pi/6$, and different values of θ_0.

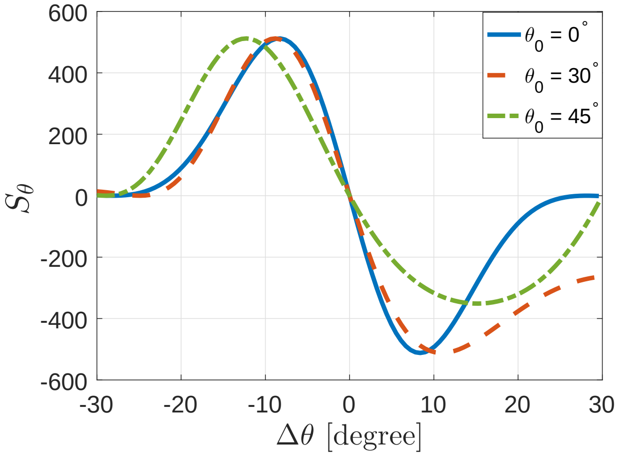


Figure 6.3: ELL S-curve for $C = 1$, $N_s = 1$, $M = N = 8$, $\phi_0 = \pi/6$, and different values of θ_0

Closed-Loop Statistics of the Elevation Angle Error

For small values of Δe_θ, the discriminator function can be approximated by a linear function given by

$$D_\theta = k_\theta \Delta e_\theta + n_\theta,$$

where k_θ is the slope of the S-curve at $\Delta e_\theta = 0$, which is obtained by

$$\begin{aligned} k_\theta &= \frac{\partial S_\theta}{\partial \Delta e_\theta}\Big|_{\Delta e_\theta = 0} \\ &= \begin{cases} -4CNN_s A_\theta \frac{\cos(\frac{\pi}{2M})}{\sin^3(\frac{\pi}{2M})}, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ -4CMN_s B_\theta \frac{\cos(\frac{\pi}{2N})}{\sin^3(\frac{\pi}{2N})}, & \text{otherwise.} \end{cases} \end{aligned}$$

A second-order loop filter can be used to track the linear changes in the elevation angle, with the following transfer function

$$H(s) = \frac{4\pi\zeta f_N s + (2\pi f_N)^2}{s^2 + 4\pi\zeta f_N s + (2\pi f_N)^2}, \tag{6.20}$$

where ζ is the damping ratio and can be set to $\zeta = 1/\sqrt{2}$ to have a step response that rises sufficiently fast with a small overshoot; and f_N is the undamped natural frequency, which is related to the noise equivalent bandwidth of the loop according to $B_L = 1.06\pi f_N$ [69]. Using the derived noise variance in (6.19), the variance of the closed-loop elevation angle estimation error can be obtained as [69]

$$\begin{aligned} \sigma_\theta^2 &= \frac{2B_L T_{\text{sub}} \text{var}\{n_\theta\}}{k_\theta^2} \\ &\approx \begin{cases} \frac{B_L T_{\text{sub}} M}{2NN_s A_\theta^2 C/\sigma^2} \frac{\sin^4(\frac{\pi}{2M})}{\cos^2(\frac{\pi}{2M})}, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \frac{B_L T_{\text{sub}} N}{2MN_s B_\theta^2 C/\sigma^2} \frac{\sin^4(\frac{\pi}{2N})}{\cos^2(\frac{\pi}{2N})}, & \text{otherwise,} \end{cases} \end{aligned} \tag{6.21}$$

where the approximation is valid for large C/σ^2 and T_{sub} is the time interval between two samples, which can be set to one LTE frame length, i.e., 10 ms.

The following remarks can be made from (6.21):

- The variance of the elevation angle estimation error depends on the elevation and azimuth angles values at each time.
- The variance of the error has its highest value at $\cos\theta \approx 0$.
- The variance of the elevation angle estimation error is inversely proportional to (C/σ^2).

Elevation Angle Error Analysis in a Multipath Environment

In the presence of multipath, the ELL discriminator function can be rewritten as

$$D_\theta = S_\theta + I_\theta + n_\theta,$$

where I_θ is the effect of multipath on the discriminator function, and is given by

$$I_\theta = \sum_{q=0}^{N_s-1} \left[2\Re\left\{S^*_{\text{down}} \cdot I_{\text{down}_q}\right\} + |I_{\text{down}_q}|^2\right] - \left[2\Re\left\{S^*_{\text{up}} \cdot I_{\text{up}_q}\right\} + |I_{\text{up}_q}|^2\right].$$

Fig. 6.4(a) shows the elevation angle estimation error for an environment with $L = 2$, $\alpha_1 = 0.2512$, $c(\tau_1 - \tau_0) = 100$ m, and $\theta_0 = \phi_0 = \pi/4$. The receiver is assumed to have $M = N = 16$ and $N_s = 200$. The results, which are presented for different multipath azimuth and elevation angles, show that the error depends on the relative azimuth and elevation angles of the multipath signal with respect to the LOS signal. Fig. 6.4(b) shows the amplitude of the maximum elevation angle estimation error for the same multipath settings as Fig. 6.4(a), but for different number of antenna elements $M = N$.

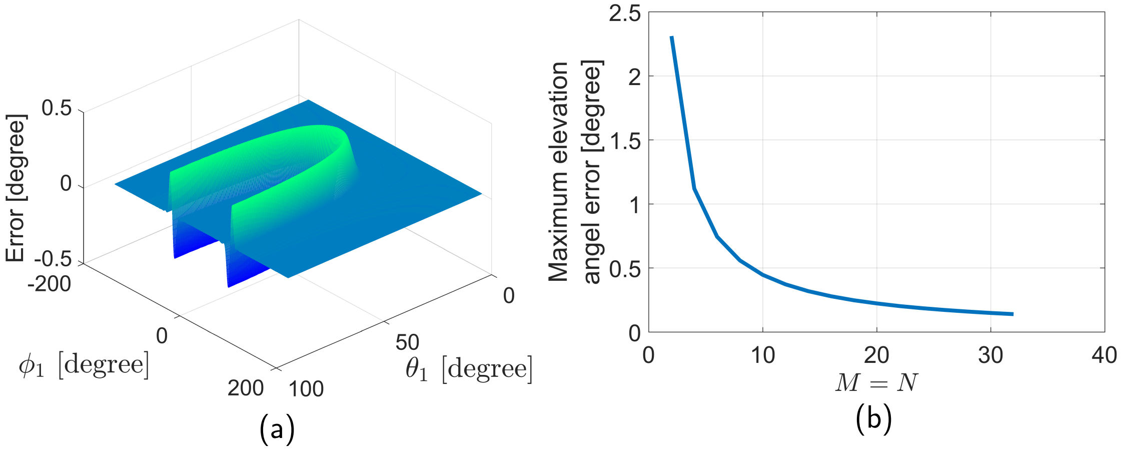


Figure 6.4: Evaluating the effect of the multipath signal on elevation angle estimation for an environment with $L = 2$, $\alpha_1 = 0.2512$, $c(\tau_1 - \tau_0) = 100$ m, $\theta_0 = \phi_0 = \pi/4$, and $N_s = 200$. (a) Elevation angle estimation error for different azimuth and elevation angles of multipath, assuming $M = N = 16$ and (b) amplitude of the maximum elevation angle estimation error for different number of antenna elements.

The following remarks can be made from the results presented in this subsection:

- The elevation angle estimation error due to multipath depends on the relative azimuth and elevation angles of multipath with respect to the LOS signal.
- The elevation angle estimation error due to multipath depends on the LOS azimuth

and elevation angles.

- Increasing the number of antennas reduces the elevation angle estimation error caused by multipath.

6.3.2 ALL

Discriminator Function

Similar to an ELL, the ALL discriminator function is defined to be

$$D_\phi \triangleq \begin{cases} \sum_{q=0}^{N_s-1}\sum_{m=0}^{M-1}\left[|\mathcal{R}_{\text{left}}|^2 - |\mathcal{R}_{\text{right}}|^2\right], & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \sum_{q=0}^{N_s-1}\sum_{n=0}^{N-1}\left[|\mathcal{R}_{\text{left}}|^2 - |\mathcal{R}_{\text{right}}|^2\right], & \text{otherwise.} \end{cases}$$

where $\mathcal{R}_{\text{left}}$ and $\mathcal{R}_{\text{right}}$ are the left and right correlation functions defined as

$$\mathcal{R}_{\text{left}} \triangleq \begin{cases} |\sum_{n=0}^{N-1} H''_{m,n,q}\Upsilon_n|, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ |\sum_{m=0}^{M-1} H''_{m,n,q}\Upsilon_m|, & \text{otherwise,} \end{cases}$$

$$\mathcal{R}_{\text{right}} \triangleq \begin{cases} \sum_{n=0}^{N-1} H''_{m,n,q}\Upsilon_n^*, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \sum_{m=0}^{M-1} H''_{m,n,q}\Upsilon_m^*, & \text{otherwise.} \end{cases}$$

Note that Υ in an ALL is the left-right locally generated signal, defined as

$$\Upsilon_m \triangleq \begin{cases} e^{j\frac{\omega_c d}{c}\left(m\sin\hat{\theta}_0\cos\hat{\phi}_0\xi_\phi\right)}, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ e^{-j\frac{\omega_c d}{c}\left(m\sin\hat{\theta}_0\sin\hat{\phi}_0\xi_\phi\right)}, & \text{otherwise,} \end{cases}$$

where ξ_ϕ is the left-right correlator spacing.

In an AWGN channel, the ALL discriminator function can be rewritten according to $D_\phi =$

$S_\phi + n_\phi$, where S_ϕ is the azimuth angle S-curve, representing the signal part of the discriminator function given by

$$S_\phi = \begin{cases} CMN_s \left[\left(\frac{\sin\left(NB_\phi(\Delta e_\phi + \xi_\phi)\right)}{\sin\left(B_\phi(\Delta e_\phi + \xi_\phi)\right)} \right)^2 - \left(\frac{\sin\left(NB_\phi(\Delta e_\phi - \xi_\phi)\right)}{\sin\left(B_\phi(\Delta e_\phi - \xi_\phi)\right)} \right)^2 \right], & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ CNN_s \left[\left(\frac{\sin\left(MA_\phi(\Delta e_\phi + \xi_\phi)\right)}{\sin\left(A_\phi(\Delta e_\phi + \xi_\phi)\right)} \right)^2 - \left(\frac{\sin\left(MA_\phi(\Delta e_\phi - \xi_\phi)\right)}{\sin\left(A_\phi(\Delta e_\phi - \xi_\phi)\right)} \right)^2 \right], & \text{otherwise,} \end{cases} \tag{6.22}$$

where $A_\phi \triangleq \frac{\omega_c d}{2c} \sin\hat{\theta}_0 \sin\hat{\phi}_0$ and $B_\phi \triangleq \frac{\omega_c d}{2c} \sin\hat{\theta}_0 \cos\hat{\phi}_0$. It can be shown that the noise part of the ALL discriminator function n_ϕ is zero-mean with the following variance

$$\text{var}\{n_\phi\} = \begin{cases} 2N_s MN^2\sigma^4 \left(1 + \frac{2C}{N\sigma^2 \sin^2(\frac{\pi}{2N})}\right), \\ \qquad \text{if } \xi_\phi = \frac{\pi}{2NB_\phi} \text{ and } |\sin\phi_0| < \eta_{\text{thr}}, \\ 2N_s NM^2\sigma^4 \left(1 + \frac{2C}{M\sigma^2 \sin^2(\frac{\pi}{2M})}\right), \\ \qquad \text{if } \xi_\phi = \frac{\pi}{2MA_\phi} \text{ and } |\sin\phi_0| \geq \eta_{\text{thr}}. \end{cases}$$

In the sequel, the left-right correlator spacing is assumed to be $\xi_\phi = \frac{\pi}{2NB_\phi}$ for $|\sin\phi_0| < \eta_{\text{thr}}$ and $\xi_\phi = \frac{\pi}{2MA_\phi}$ otherwise.

It can be seen from (6.22) that the shape of the ALL S-curve depends on the elevation and azimuth angles. Fig. 6.5 shows the ALL S-curve for $C = 1$, $N_s = 1$, $M = N = 8$, $\eta_{\text{thr}} = \frac{\sqrt{2}}{2}$, $\theta_0 = \pi/4$, and different values of ϕ_0.

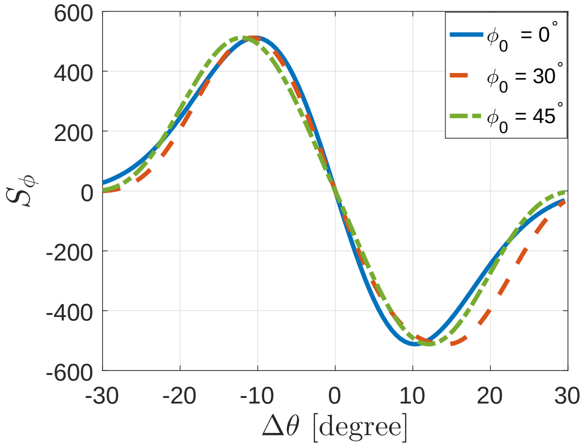


Figure 6.5: ALL S-curve for $C = 1$, $N_s = 1$, $M = N = 8$, $\eta_{\text{thr}} = \frac{\sqrt{2}}{2}$, $\theta_0 = \pi/4$, and different values of ϕ_0

Closed-Loop Statistics of the Azimuth Angle Error

For small values of Δe_ϕ, the discriminator function can be approximated by a linear function given by $D_\phi = k_\phi \Delta e_\phi + n_\phi$, where k_ϕ is the slope of the S-curve at $\Delta e_\phi = 0$ given by

$$k_\phi = \begin{cases} -4CMN_sB_\phi \frac{\cos\left(\frac{\pi}{2N}\right)}{\sin^3\left(\frac{\pi}{2N}\right)}, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ -4CNN_sA_\phi \frac{\cos\left(\frac{\pi}{2M}\right)}{\sin^3\left(\frac{\pi}{2M}\right)}, & \text{otherwise.} \end{cases}$$

Using a second-order loop filter with the transfer function presented in (6.20), it can be shown that the variance of the steady-state tracking error follows

$$\sigma_\phi^2 \approx \begin{cases} \frac{B_LT_{\text{sub}}N}{2MN_sB_\phi^2C/\sigma^2} \frac{\sin^4(\frac{\pi}{2N})}{\cos^2(\frac{\pi}{2N})}, & \text{if } |\sin\phi_0| < \eta_{\text{thr}}, \\ \frac{B_LT_{\text{sub}}M}{2NN_sA_\phi^2C/\sigma^2} \frac{\sin^4(\frac{\pi}{2M})}{\cos^2(\frac{\pi}{2M})}, & \text{otherwise,} \end{cases} \tag{6.23}$$

where the approximation is valid for large C/σ^2.

The following remarks can be made based on (6.23):

- The variance of the azimuth angle estimation error depends on the elevation and azimuth angles values.

- The variance of the azimuth angle estimation error has its highest value at $\sin\theta_0 \approx 0$.

- The variance of the azimuth angle estimation error is inversely proportional to (C/σ^2).

Azimuth Angle Error Analysis in a Multipath Environment

In the presence of multipath, the ALL discriminator function can be rewritten as $D_\phi = S_\phi + I_\phi + n_\phi$, where I_ϕ is the effect of multipath on the discriminator output given by

$$\begin{aligned} I_\phi = \sum_{q=0}^{N_s-1} & \left[2\Re\left\{S^*_{\text{left}} \cdot I_{\text{left}}\right\} + |I_{\text{left}}|^2\right] \\ & - \left[2\Re\left\{S^*_{\text{right}} \cdot I_{\text{right}}\right\} + |I_{\text{right}}|^2\right]. \end{aligned}$$

where S_{left}, S_{right}, I_{left}, I_{right} can be defined similar to (6.17).

Fig. 6.6(a) shows the azimuth angle estimation error for a an environment with $L = 2$, $\alpha_1 = 0.2512$, $\theta_0 = \phi_0 = \pi/4$. The receiver is assumed to have $M = N = 16$ and $N_s = 200$. The results, which are presented for different multipath azimuth and elevation angles, show that the error depends on the relative azimuth and elevation angles of the multipath signal with respect to the LOS signal. Fig. 6.6(b) shows the amplitude of the maximum azimuth angle estimation error for the same multipath settings as Fig. 6.6(a), but for different number of antenna elements. Similar remarks as the ELL can be made from these results.

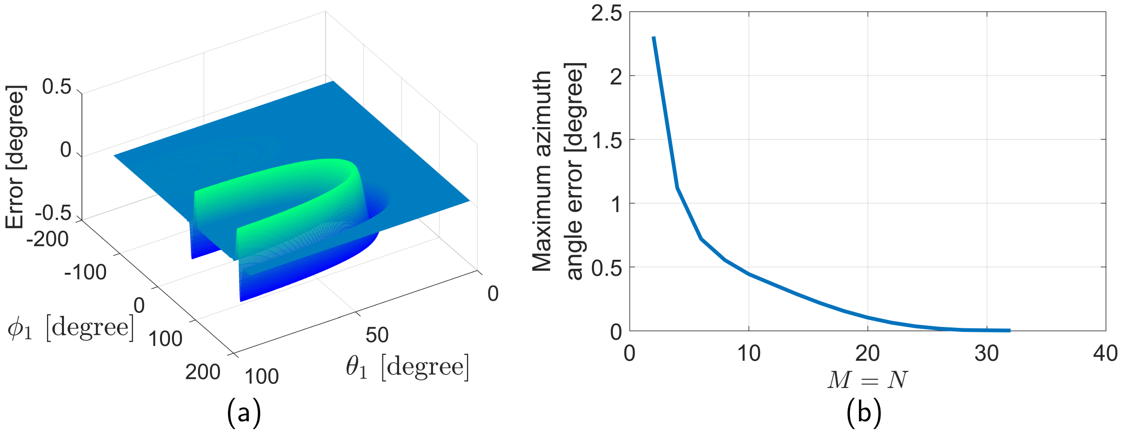


Figure 6.6: Evaluating the effect of multipath signal on the azimuth angle estimation for $\theta_0^{(u)} = \phi_0^{(u)} = \pi/4$, $L = 2$, $\alpha_1 = 0.2512$, and $N_s = 200$. (a) Azimuth angle estimation error for different azimuth and elevation angles of multipath, assuming $M = N = 16$ and (b) amplitude of the maximum azimuth angle estimation error for different number of antenna elements.

6.3.3 DLL

The structure of the DLL was discussed in details in [45] and [49]. In this section, the presented results in [45] and [49] are adapted to the UPA antenna array.

Discriminator Function

The DLL discriminator function is defined as

$$D_\tau \triangleq \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \left[|\mathcal{R}_{\text{late}}|^2 - |\mathcal{R}_{\text{early}}|^2 \right],$$

where $\mathcal{R}_{\text{early}}$ and $\mathcal{R}_{\text{late}}$ are early and late correlation functions, which are obtained by the cross-correlation of $H''_{m,n,q}$ with the early-late locally generated signal and its conjugate, respectively. An early-late locally generated signal is defined to be $\Upsilon_q \triangleq e^{j2\pi q f_s N_{CRS} \xi_\tau}$, where ξ_τ is the early-late correlator spacing.

For an AWGN channel, the DLL discriminator function can be rewritten as $D_\tau = S_\tau + n_\tau$, where S_τ is the DLL S-curve, representing the signal part of the DLL discriminator function given by

$$S_\tau = CMN \left[\left(\frac{\sin\left(\pi f_s N_{CRS} N_s (\Delta e_\tau + \xi_\tau)\right)}{\sin\left(\pi f_s N_{CRS} (\Delta e_\tau + \xi_\tau)\right)} \right)^2 - \left(\frac{\sin\left(\pi f_s N_{CRS} N_s (\Delta e_\tau - \xi_\tau)\right)}{\sin\left(\pi f_s N_{CRS} (\Delta e_\tau - \xi_\tau)\right)} \right)^2 \right]. \tag{6.24}$$

and n_τ is the noise component with zero-mean and the following variance

$$\mathrm{var}\{n_\tau\} \leq 2MNN_s^2\sigma^4 \left[1 + \frac{2C \sin\left(\pi f_s N_{CRS} N_s \xi_\tau\right)}{N_s \sigma^2 \sin^2(\pi f_s N_{CRS} \xi_\tau)} \right].$$

where the equality holds for $\xi_\tau = \frac{1}{2f_s N_{CRS} N_s}$, which is used in the rest of the chapter [45]. Fig. 6.7 shows S_τ for $C = 1$, $M = N = 1$ and $N_s = 200$. It can be seen from (6.24) that, in contrast to S_θ and S_ϕ, which depend on θ_0 and ϕ_0, the DLL S-curve S_τ does not depend on τ_0.

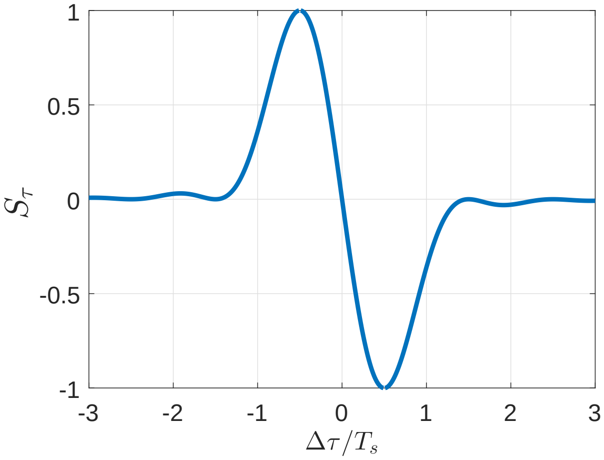


Figure 6.7: DLL S-curve for $C = 1$, $M = N = 1$ and $N_s = 200$

Closed-Loop Statistics of the Delay Error

For small values of Δe_τ, the DLL discriminator function can be approximated by a linear function, according to $D_\tau = k_\tau \Delta e_\tau + n_\tau$, where k_τ is the slope of S_τ for $\Delta e_\tau = 0$, given by

$$k_\tau = -4\pi C M N f_s N_{CRS} \frac{\cos(\frac{\pi}{2N_s})}{\sin^3(\frac{\pi}{2N_s})}.$$

Using a second-order loop filter with transfer function presented in (6.20), the closed-loop delay estimation error can be obtained as

$$\sigma_\tau^2 \approx \frac{B_L T_{\text{sub}} N_s}{2\pi^2 M N f_s^2 N_{CRS}^2 C/\sigma^2} \frac{\sin^4(\frac{\pi}{2N_s})}{\cos^2(\frac{\pi}{2N_s})}. \tag{6.25}$$

Delay Error Analysis in a Multipath Environment

In the presence of multipath, the DLL discriminator function can be rewritten as $D_\tau = S_\tau + I_\tau + n_\tau$, where I_τ is the effect of multipath on the DLL output given by

$$I_\tau = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \left[2\Re\left\{S_{\text{late}}^* I_{\text{late}}\right\} + |I_{\text{late}}|^2\right] - \left[2\Re\left\{S_{\text{early}}^* I_{\text{early}}\right\} + |I_{\text{early}}|^2\right].$$

Fig. 6.8(a) shows the error caused by multipath on the TOA estimation for $L = 2$, $\alpha_1 = 0.2512$, $M = N = 16$, and $N_s = 200$. It can be seen that multipath delay changes the error in TOA estimation. Fig. 6.8(b) shows amplitude of the maximum delay estimation error due to multipath for different N_s values. It can be seen that increasing N_s reduces the TOA estimation error. In contrast to the ELL and ALL, the TOA estimation error due to the multipath only depends on the relative multipath delay with respect to the LOS TOA.

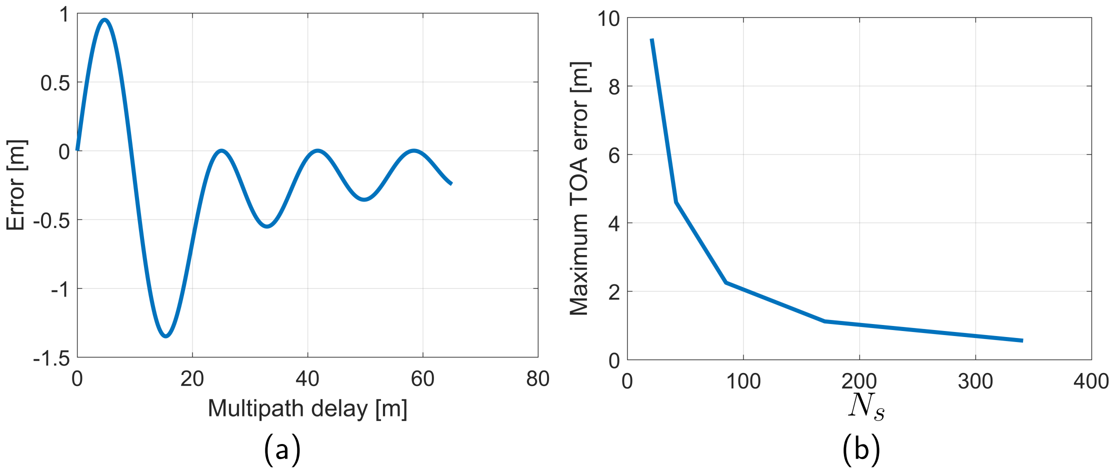


Figure 6.8: Evaluating the effect of multipath on the TOA estimation for $L = 2$, $\alpha_1 = 0.2512$, $M = N = 1$, and $N_s = 200$. (a) TOA estimation error for different multipath delays and (b) amplitude of the maximum TOA estimation error for different N_s

6.4 Cramér-Rao Lower Bound

The measurements are considered to be the CFRs of all UPA antenna elements and at different CRS subcarriers. It can be shown that the matrix of CFRs at all antenna elements and on the q-th CRS subcarrier $\mathbf{H}_q$ can be written as

$$\mathbf{H}_q = \mathbf{X}\text{diag}\left\{\boldsymbol{b} \circ \boldsymbol{z}'_q\right\}\mathbf{Y}^{\mathsf{T}},$$

where $\circ$ is the Hadamard product and

$$\begin{aligned}
\mathbf{X} &\triangleq [\boldsymbol{x}_0, \cdots, \boldsymbol{x}_{L-1}],\\
\boldsymbol{x}_i &\triangleq \left[1, x_i, \cdots, x_i^{M-1}\right]^{\mathsf{T}},\\
\mathbf{Y} &\triangleq [\boldsymbol{y}_0, \cdots, \boldsymbol{y}_{L-1}],\\
\boldsymbol{y}_i &\triangleq \left[1, y_i, \cdots, y_i^{N-1}\right]^{\mathsf{T}},\\
\boldsymbol{b} &\triangleq \sqrt{C}[\beta_0, \cdots, \beta_{L-1}]^{\mathsf{T}},\\
\boldsymbol{z}'_q &\triangleq \left[z_0^q, \cdots, z_{L-1}^q\right]^{\mathsf{T}}.
\end{aligned}$$

Using the equality of $\text{vec}\left\{\mathbf{A}_1\text{diag}\left\{\boldsymbol{a}\right\}\mathbf{A}_2^{\mathsf{T}}\right\} = (\mathbf{A}_2 \odot \mathbf{A}_1)\,\boldsymbol{a}$ for any vector $\boldsymbol{a}$ and matrices $\mathbf{A}_1$ and $\mathbf{A}_2$ of the proper size [98, 105], the vector $\text{vec}\left[\mathbf{H}_q\right]$ can be obtained as

$$\begin{aligned}\text{vec}\left[\mathbf{H}_q\right] &= \left[\mathbf{Y} \odot \mathbf{X}\right]\left(\boldsymbol{b} \circ \boldsymbol{z}_q'\right)\\ &= \left[\mathbf{Y} \odot \mathbf{X}\right]\text{diag}\left\{\boldsymbol{b}\right\}\boldsymbol{z}_q'.\end{aligned} \tag{6.26}$$

where $\text{vec}\left\{\mathbf{X}\right\}$ stacks columns of matrix $\mathbf{X}$ one under another and $\odot$ is a Khatri-Rao product. Define $\mathbf{G} \triangleq \left[\text{vec}\left\{\mathbf{H}_0\right\}, \cdots, \text{vec}\left\{\mathbf{H}_{N_s-1}\right\}\right]$. Using (6.26), $\mathbf{G}$ can be rewritten as

$$\mathbf{G} = \left[\mathbf{Y} \odot \mathbf{X}\right]\text{diag}\left\{\boldsymbol{b}\right\}\mathbf{Z}^{\mathsf{T}},$$

where $\mathbf{Z} \triangleq \left[\boldsymbol{z}_0, \cdots, \boldsymbol{z}_{L-1}\right]$ and $\boldsymbol{z}_i \triangleq \left[1, z_i, \cdots, z_i^{N_s-1}\right]^{\mathsf{T}}$. Therefore, $\boldsymbol{g} = \text{vec}\left[\mathbf{G}\right]$ can be obtained as $\boldsymbol{g} = \mathbf{S}\boldsymbol{b}$, where $\mathbf{S} \triangleq \mathbf{Z} \odot \left[\mathbf{Y} \odot \mathbf{X}\right]$. The same approach can be used for the estimated CFRs, resulting in $\hat{\boldsymbol{g}} = \mathbf{S}\boldsymbol{b} + \boldsymbol{w}$, where $\boldsymbol{w} = \text{vec}\left[\mathbf{W}\right]$ represents the noise effect. It can be seen that, $\hat{\boldsymbol{g}}$ has a similar form as equation (13) in [105]. Therefore, one can use the results in [105] to derive the CRLB of the relevant parameters $\boldsymbol{\eta} = [\boldsymbol{\theta}, \boldsymbol{\phi}, \boldsymbol{\tau}]$ for a UPA-LTE system, yielding

$$\text{CRLB}(\boldsymbol{\eta}) = \frac{\sigma^2}{2}\left\{\Re\left[\mathbf{B}_e^{\mathsf{H}}\mathbf{D}^{\mathsf{H}}\left(\mathbf{I} - \mathbf{S}\mathbf{S}^{\dagger}\right)\mathbf{D}\mathbf{B}_e\right]\right\}^{-1}, \tag{6.27}$$

where $\mathbf{B}_e = \mathbf{I}_3 \otimes \text{diag}\left\{\boldsymbol{b}\right\}$; $\mathbf{D} = [\partial\mathbf{S}/\partial\boldsymbol{\theta}, \partial\mathbf{S}/\partial\boldsymbol{\phi}, \partial\mathbf{S}/\partial\boldsymbol{\tau}]$; and

$$\begin{aligned}\partial\mathbf{S}/\partial\boldsymbol{\theta} &= \left[\boldsymbol{d}_{\theta_0}, \cdots, \boldsymbol{d}_{\theta_{L-1}}\right],\\ \partial\mathbf{S}/\partial\boldsymbol{\phi} &= \left[\boldsymbol{d}_{\phi_0}, \cdots, \boldsymbol{d}_{\phi_{L-1}}\right],\\ \partial\mathbf{S}/\partial\boldsymbol{\tau} &= \left[\boldsymbol{d}_{\tau_0}, \cdots, \boldsymbol{d}_{\tau_{L-1}}\right],\end{aligned}$$

$$
\begin{aligned}
&\boldsymbol{d}_{\theta_i} = \boldsymbol{z}_i \otimes \left(\partial \boldsymbol{y}_i/\partial\theta_i \otimes \boldsymbol{x}_i + \boldsymbol{y}_i \otimes \partial \boldsymbol{x}_i/\partial\theta_i\right), \\
&\boldsymbol{d}_{\phi_i} = \boldsymbol{z}_i \otimes \left(\partial \boldsymbol{y}_i/\partial\phi_i \otimes \boldsymbol{x}_i + \boldsymbol{y}_i \otimes \partial \boldsymbol{x}_i/\partial\phi_i\right), \\
&\boldsymbol{d}_{\tau_i} = \partial \boldsymbol{z}_i/\partial\tau_i \otimes \left(\boldsymbol{y}_i \otimes \boldsymbol{x}_i\right), \\
&\text{for} \quad i = 0, \cdots, L-1.
\end{aligned}
$$

where $\otimes$ represents the Kronecker product.

The above results can be simplified to the following (see Appendix A.2) for a channel with only a LOS signal.

$$
\sigma^2_{\theta_0,CRLB} = \frac{6}{C/\sigma^2 MNN_s(\omega_c d/c)^2 \cos^2\theta_0 \left[(N^2-1)\sin^2\phi_0 + (M^2-1)\cos^2\phi_0\right]}, \tag{6.28}
$$

$$
\sigma^2_{\phi_0,CRLB} = \frac{6}{C/\sigma^2 MNN_s(\omega_c d/c)^2 \sin^2\theta_0 \left[(N^2-1)\cos^2\phi_0 + (M^2-1)\sin^2\phi_0\right]}, \tag{6.29}
$$

$$
\sigma^2_{\tau_0,CRLB} = \frac{6}{C/\sigma^2 MNN_s(N_s^2-1)(2\pi f_s N_{CRS})^2}. \tag{6.30}
$$

The following remarks can be made from (6.28)–(6.30):

- For $M = N$, both azimuth and elevation angles' CRLBs are independent of the actual azimuth angle.
- The azimuth and elevation angles' CRLBs tend to infinity for $\sin\theta_0 = 0$ and $\cos\theta_0 = 0$, respectively.
- The TOA CRLB does not depend on the DOA and TOA values.

6.5 Computational Complexity

In the 3-D MP algorithm, the most computationally intensive step is to estimate the signal subspace using the SVD decomposition, which requires $17P^3K^3R^3/3 + 2P^2K^2R^2(M - P +$

$1)(N-K+1)(N_s-R+1)$ real multiplications [114]. The discriminator functions are the most computationally intensive steps in the tracking stage, which require $8(MN+N_s)$ real multiplications.

6.6 Simulation Results

This section presents simulation results to evaluate the performance of the proposed acquisition and tracking stages and demonstrate the analytical results derived in Sections 6.2 to 6.4.

6.6.1 Acquisition Stage Noise Performance

To evaluate the acquisition stage performance, a CFR was modeled based on (6.1) and for $M = N = N_s = 32$, $P = K = R = \lceil M/3 \rceil$, $L = 1$, $\tau_0 = 0$, $\phi_0 = \theta_0 = \pi/4$. Then, for each C/σ^2, 300 different noise realizations with the proper σ^2 were added to the CFRs. The MP algorithm presented in Subsection 6.2.1 was used to estimate TOAs and DOAs for each generated CFR and the standard deviation of the estimation errors were obtained, which represents the noise performance of the acquisition stage. Fig. 6.9 shows the simulation results with blue '+' markers. The derived analytical results in (6.13), (6.14), and (6.15) are plotted with the solid blue lines, which show the simulation results follow the analytical results closely.

The CRLBs of the TOA and DOA, which were derived in (6.28), (6.29), and (6.30), can be used to evaluate the performance of the acquisition stage. Fig. 6.9 shows the TOA and DOA CRLBs with dashed orange lines. It can be seen that the acquisition stage noise performance is very close to the CRLB.

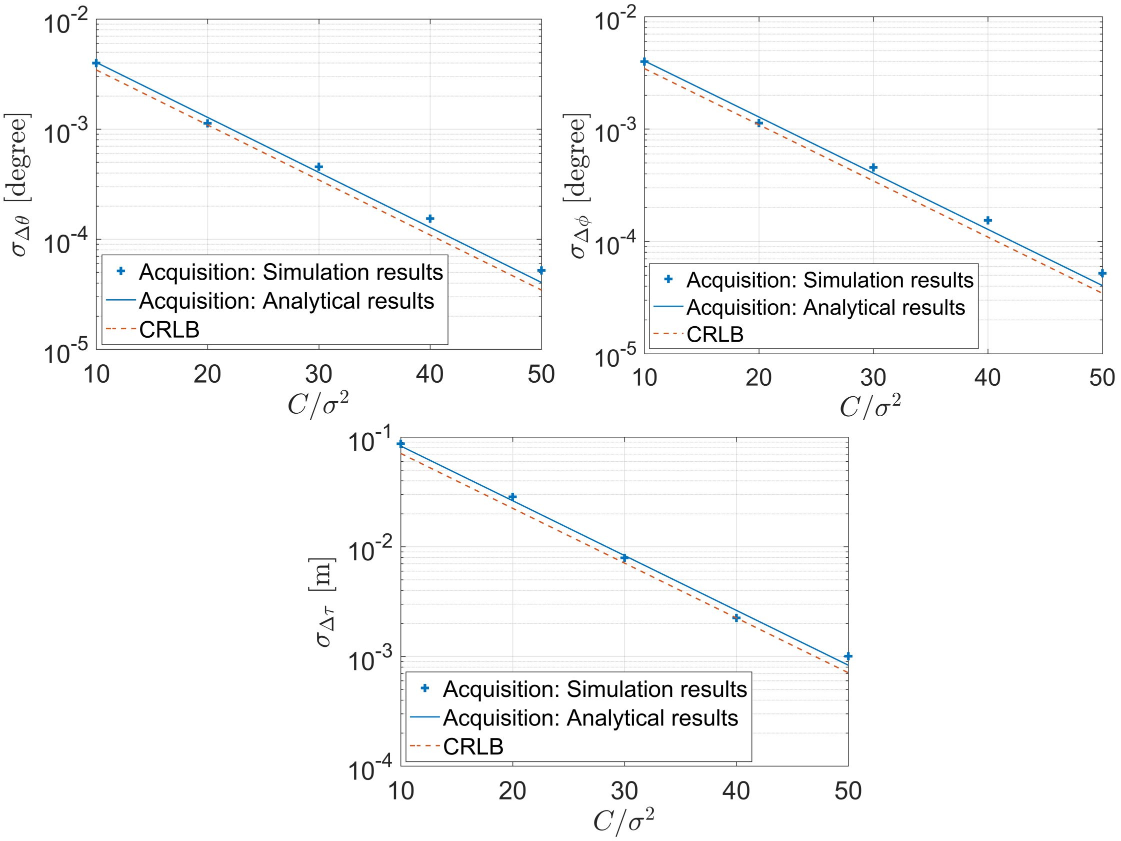


Figure 6.9: CRLB and acquisition stage standard deviation of elevation and azimuth angles and delay estimation errors for different C/σ^2. The results are presented for $M = N = N_s = 32$, $P = K = R = \lceil M/3 \rceil$, $L = 1$, $\tau_0 = 0$, $\phi_0 = \theta_0 = \pi/4$.

6.6.2 Tracking Stage Noise Performance

To evaluate the performance of the tracking stage, a similar approach to Subsection 6.6.1 was used to generate CFRs for $L = 1$, $\tau_0 = 0$, $\phi_0 = \theta_0 = \pi/4$. Then, the tracking stage noise performance was obtained for different $M = N = N_s$, B_L, and C/σ^2, and was compared to the analytical results presented in (6.21), (6.23), and (6.25). It can be seen that the simulation results ('o' markers) follow the analytical results (solid lines) closely.

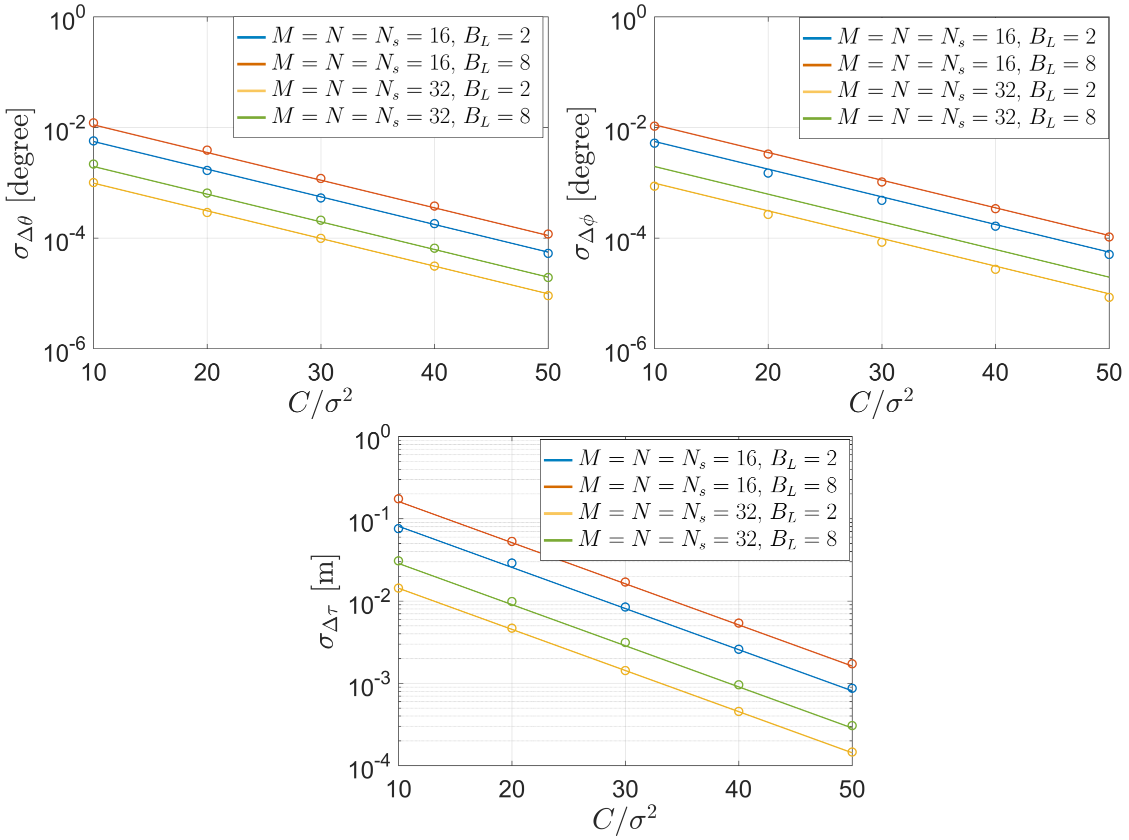


Figure 6.10: Tracking stage standard deviation of elevation and azimuth angles and delay estimation errors for different C/σ^2. The results are presented for $L = 1$, $\tau_0 = 0$, $\phi_0 = \theta_0 = \pi/4$.

6.7 Experimental Results

To evaluate the performance of the proposed framework, a field test was conducted with real LTE signals in the Anteater parking structure at the University of California, Irvine, USA. This section presents the experimental setup and obtained results.

6.7.1 Hardware and Software Setup

To perform the experiment, a cart was equipped with

- Four consumer-grade 800/1900 MHz Laird cellular omnidirectional antennas to record

LTE signals. The antennas were arranged in a 2×2 UPA array structure with $d = 7$ cm.

- An NI four-channel USRPs-2955 to simultaneously down-mix and synchronously sample the LTE signals received by the four antennas at a sampling rate of 10 MSps and a carrier frequency of 1955 MHz.
- A host laptop computer to store the samples for post-processing.
- An NI USRP 2930 and a consumer-grade 800/1900 MHz LTE antenna to transmit a tone signal before performing the experiment to remove the initial phase offsets between different elements of the antenna array.
- A GPS antenna to discipline the USRP's oscillator.
- A Septentrio AsteRx-i V, which was equipped with a dual antenna multi-frequency GNSS receiver with RTK and a Vectornav VN-100 MEMS IMU to estimate the position and orientation of the ground vehicle, which was used as the "ground truth".

Fig. 7.12(a) shows the experimental hardware setup. The location of the LTE eNodeB, the traversed trajectory, and the environmental layout of the experiment is shown in Fig. 7.12(b).

The receiver traversed a trajectory of 153 m over 180 s, while listening to 1 LTE eNodeBs. The true orientation of the receiver was obtained using the Septentrio device described above.

6.7.2 Calibration

The USRP's filters, mixers, amplifiers, and phase locked-loops may contribute to a phase error on the received signals from different antennas. This phase error may vary with time, temperature, and mechanical conditions. To remove these errors, an initial and periodic

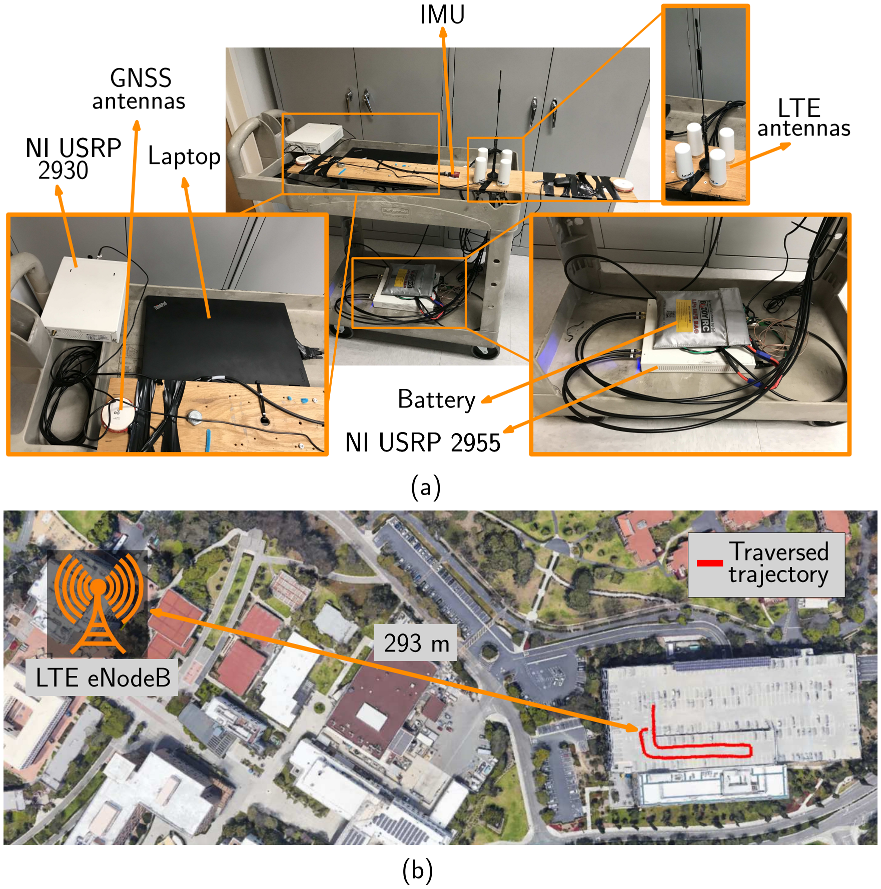


Figure 6.11: (a) Experimental hardware setup and (b) location of the LTE eNodeB, the traversed trajectory, and the environmental layout of the experiment

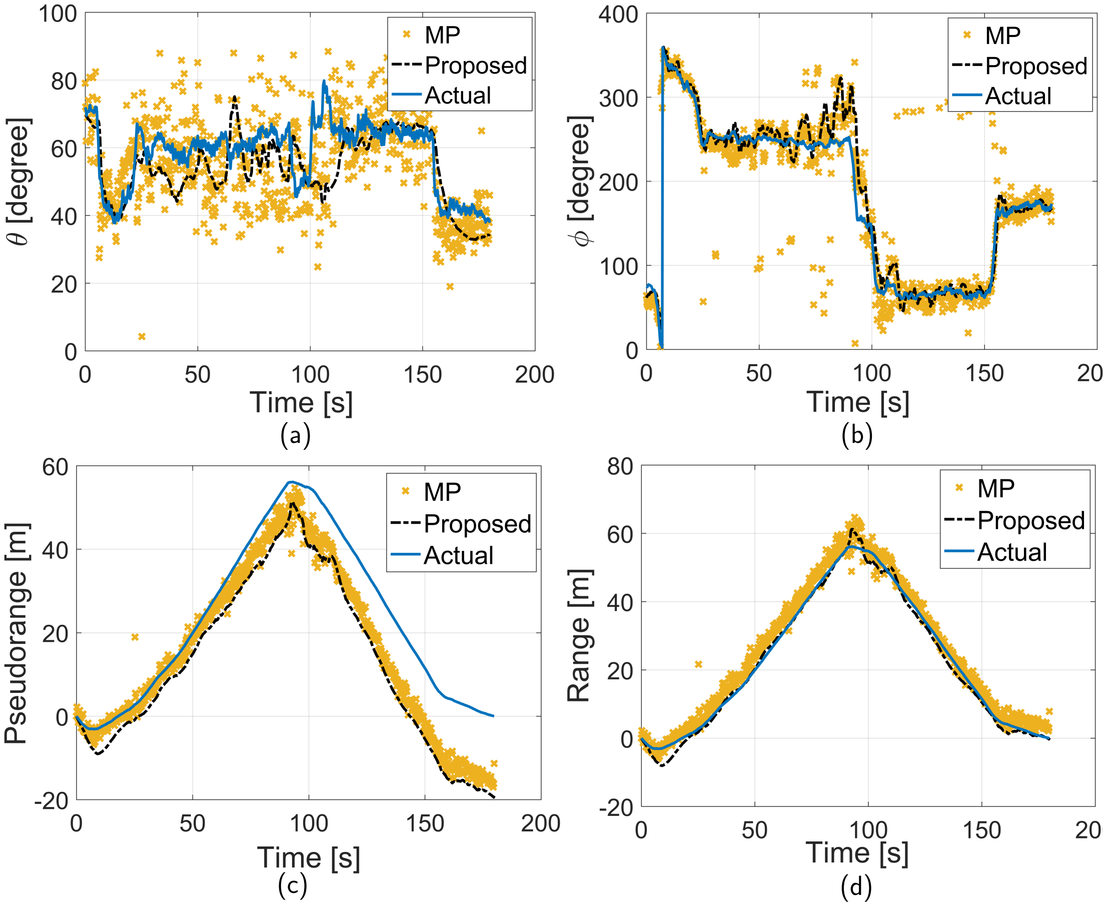
calibration is required [115]. For this purpose, a calibration tone was transmitted to all the USRP's channels and the phase and amplitude differences between all the channels with the first channel was measured. Then, the phase and amplitude difference was removed from the received signals over the course of the experiment. Since the phase differences may vary with time and temperature, it is important to perform the calibration routine before each experiment.

6.7.3 Results

The stored LTE samples were used to jointly estimate the TOA and DOA of the received LTE signals using (1) only MP algorithm and (2) the proposed receiver structure. Then, the results were compared against the true value, which are shown in Fig. 6.12. Fig. 6.12(c) compares the estimated pseudoranges with the true range. Note that the initial bias is removed from the range and pseudoranges for comparison purposes. The difference between the true range and the estimated pseudoranges are due to noise, multipath, and clock drift. In order to remove the effect of the clock, a linear function was mapped to the error, which represents a constant clock drift model. The estimated drift was -0.11 m/s. Then, this function was used to remove the effect of clock drift from the pseudoranges. Fig. 6.12(d) shows the estimated ranges after removing the effect of the clock. Table 6.1 compares the standard deviation of the TOA and DOA errors. It can be seen that a reduction of 93%, 57%, and 31% in the standard deviation of the estimated TOA, azimuth, and elevation angles errors, respectively, was achieved using the proposed receiver structure compared to the MP algorithm. Note that the MDL method tends to overestimate the channel length. As a result, the MP algorithm has an outlier. Since pseudorange estimates are obtained by multiplying TOA estimates with the speed of light, this outlier tends to have large numbers, which results in large estimation error standard deviation. Note that the y-axis in Fig. 6.12 is limited for better visualization and does not show the outlier completely.

Table 6.1: Standard deviation of the estimated TOA and DOA errors

	MP algorithm	**Proposed algorithm**
Azimuth [degrees]	43.21	18.62
Elevation [degrees]	11.49	7.89
TOA [m]	21.86	1.60



(a)

(b)

(c)

(d)

Figure 6.12: Estimated TOA and DOA obtained by MP algorithm and the proposed receiver structure

Chapter 7

NR: Signal Model, Receiver Design, and Ranging/Positioning Error Statistics

Autonomous ground vehicles (AGVs), also known as self-driving cars, already navigate the streets todays in several cities around the world. Companies such as Waymo, GM Cruise, and Apple have reported more than 1.5 million miles with their self-driving cars in 2018 [116]. AGVs promise higher quality of life by reducing the number accidents and reducing countless hours of wasted time. However, this is only achievable with reliable autonomy. One important factor to evaluate the reliability of an AGV is called disengagement rate, which is defined based on the California Department of Motor Vehicles (DMV) as the number of times the AGV's test driver has to disengage the autonomous mode and to take immediate manual control of the vehicle [117]. Although Waymo's, GM Cruise's, and Apple's AGVs are among the top tier performing AGVs, they have reported disengagement rates of 0.09, 0.19, and 0.5 per 1,000 miles, respectively, in 2018. At this point, AGVs are a long way from reliable, full autonomy.

Situational awareness is key to achieving reliable, full autonomy. One of the key enablers is vehicle-to-everything (V2X) communication, which includes vehicle's communication with other vehicles, pedestrians, infrastructure, and network. In 2009, the United States assigned an IEEE 802.11p-based dedicated short range communication (DSRC) technology to vehicle-to-vehicle (V2V) communication over a pre-specified transmission band to ensure low interference. Although DSRC has been tested over large-scale trials over the past years for V2V transmissions, it has failed to answer the demands for vehicle-to-network (V2N) and vehicle-to-infrastructure (V2I) due to its low transmission bandwidth and lack of proper roadside units. To overcome the limitations of DSRC, the third generation partnership project (3GPP) has developed a cellular-based V2X communication in Release 15 and 16 for the 5th generation (5G) of wireless access technology (also known as new radio (NR)) [118].

Low latency and high data rate are among the main characteristics of NR signals. To achieve these characteristics, higher transmission bandwidth is essential. However, unlicensed spectrum in lower frequencies is scarce. Due to this limitation, using millimeter waves (mmWaves) for NR signal transmission has been considered. But, mmWaves suffer from high signal path loss, which can be compensated by beamforming techniques and massive multiple-input multiple-output (mMIMO) antenna structure. Beamforming requires the knowledge of the user's location. Therefore, 5G-based positioning is not only a service that is provided to users, but also a key enabler to high data rates via proactive resource allocation and beamforming [119].

The 3GPP has evaluated different types of positioning techniques including timing, angle, carrier phase, and received reference signal power-based techniques for NR downlink and uplink signals in Release 15 and 16 [120]. Positioning performance evaluation of 5G signals is not only limited to 3GPP reports. For example, mmWaves signals' characteristics were evaluated for positioning in [121]. Position and orientation error bounds were derived in [122, 123] as a function of the Cramér-Rao lower bounds (CRLBs) of the direction-of-departure

(DOD), direction-of-arrival (DOA), and time-of-arrival (TOA) for both uplink and downlink communications. A methodology to design 5G networks for precise positioning was proposed in [124] and was evaluated with simulation results. Several channel estimation algorithms were proposed in [125–127] to estimate DOD, DOA, and TOA of the user equipment (UE) by means of compressed sensing tools, which exploit the sparsity of mmWaves' channels. The received reference signal strength from multiple base stations was used in [128] to estimate the DOD and position of the UE in a two-stage Kalman filter. In [129], a method was proposed to jointly estimate the position and orientation of the UE, as well as the location of reflectors or scatterers in the absence of the line-of-sight (LOS) path. To remove the effect of the clock bias, a two-way localization approach was proposed in [130] and its position and orientation error bounds were derived.

All the proposed approaches in the literature require a pre-specified reference signal transmission, namely positioning reference signal (PRS), where cellular providers must allocate additional bandwidth to the PRS transmission. Besides, the aforementioned algorithms require prior knowledge of the systems' parameters (e.g., number of transmission antennas and beamforming matrix), which are not available at the UE in practical applications. Therefore, a network-based positioning approach must be used, which compromises the privacy of the UEs. This chapter presents an opportunistic navigation with NR signals, where NR reference signals that are broadcast to the UE are *exploited* for navigation purposes.

Over the past decade, opportunistic navigation has been demonstrated in the literature with different types of radio frequency (RF) signals, also known as signals of opportunity (SOPs). Cellular, digital television, AM/FM, Wi-Fi, and low-earth orbit (LEO) satellite signals are examples of SOPs [10–14]. Among SOPs, cellular signals have attracted considerable attentions due to their desirable attributes, including: (1) large transmission bandwidth, (2) high carrier-to-noise ratio (C/N_0), and (3) favorable geometric diversity. The potential of cellular code-division multiple access (CDMA) and long-term evolution (LTE) signals for navigation have been thoroughly studied in the literature [25, 30, 31, 49, 131]. CDMA and LTE are the standards of the 3rd and 4th generations (3G and 4G) of wireless communication systems, respectively. The structure of NR signals has finalized in 2019, and since then, only a few operators have started implementing this standard mainly in major cities around the world. Since NR signals are new to the field, the literature lacks a thorough study on the potential of NR signals for opportunistic navigation.

There are several challenges for an opportunistic navigation with NR signals: (1) low-level NR frame structure and signaling processing are scattered in several technical reports, which makes them confusing and tiresome to follow for one without proper background, (2) potential reference signals for opportunistic navigation with NR signals have not been investigated, (3) specialized receivers to opportunistically extract navigation observables from NR signals have not been developed, and (4) achievable ranging and positioning accuracy with these signals have not been analyzed. This chapter tackles these challenges by

- providing the low-level NR signal structure and describing important parameters for opportunistic navigation,
- presenting potential signals for opportunistic navigation and their related coding and decoding procedure,
- developing a software-defined receiver (SDR) to extract navigation observables from NR signals, and
- deriving ranging and positioning accuracy with NR signals.

In addition to the above contributions, experimental results with real NR signals are provided showing a standard deviation of 1.19 m for the estimated range with the proposed SDR. To the authors' knowledge, this is the first time that navigation observables are extracted from real NR signals.

The structure of this chapter is organized as follows. Section 7.1 discusses the advantages and challenges of navigation with NR signals. Section 7.2 presents NR frame structure and the potential reference signals for opportunistic navigation. Section 7.3 shows the structure of the proposed SDR to extract navigation observables from NR signals. Section 7.4 derives the ranging precision of the NR signals. Section 7.5 analyzes the statistics of the position estimation error. Finally, Section 7.6 demonstrates the experimental results.

7.1 Opportunistic Navigation with NR Signals: Opportunities and Challenges

This section discusses the opportunities and challenges associated with exploiting NR signals for navigation.

7.1.1 Opportunities

NR signals possess multiple desirable characteristics for opportunistic navigation, which are summarized next.

- **Operating at high frequency bands:** NR is designed to support transmission at different frequency ranges (FRs). According to the NR specifications, these FRs can be divided into two main ranges: (1) FR1, which is also known as sub-6 GHz, corresponds to 450 MHz to 6 GHz and (2) FR2, which is also known as mmWaves, corresponds to 24.25 GHz to 52.6 GHz [132]. Due to the high path loss in mmWaves, the received signal will contain an LOS signal with a few dominant multipath components. Therefore, multipath effect on the navigation observables is lower for mmWaves compared to low frequency signals. This will yield a more accurate TOA estimation [121]. Moreover, due to high path loss, 5G networks have higher density to provide a reliable coverage, which results in a desirable geometric diversity for navigation purposes.

- **mMIMO structure:** mMIMO structure in NR is advantageous for navigation purposes, since (1) the large number of antennas increases the received signal's carrier-to-noise ratio (C/N_0), which has direct relationship with ranging precision and (2) highly directional signals reduce the interference of other NR base stations (also known as next generation NodeBs or gNBs), which increases the ranging accuracy.
- **Large transmission bandwidth:** A single NR can have a maximum of 100 MHz and 400 MHz bandwidth in sub-6 and mmWaves, respectively. The large transmission bandwidth of NR signals enables differentiating multipath from LOS, which improves the accuracy of TOA estimation.

7.1.2 Challenges

To exploit NR signals for navigation, the following challenges must be tackled.

- **Ultra-lean transmission:** In opportunist navigation, a broadcast reference signal is used to derive navigation observables such as TOA and DOA. This signal is known at the UE and is independent of the network operator. Therefore, the UE can exploit it opportunistically for navigation without being a network subscriber. In cellular LTE signals, several reference signals, such as cell-specific reference signal (CRS), are broadcast at regular time intervals even when there is no UE in the environment. This reduces the network energy efficiency and increases the network operational expenses and interference. One of the main features of NR is its ultra-lean transmission, which minimizes the transmission of these "always-on" signals. NR has four main reference signals: demodulation reference signals, phase tracking reference signals, sounding reference signals, and channel state information reference signals. These signals are only transmitted when necessary, making previously developed opportunistic navigation approaches with these signals impossible [133]. This limits opportunist navigation with NR signals to only synchronization signal and physical broadcast channel (SS/PBCH) block, which is always-on. As will be discussed in the next section, SS/PBCH block is not transmitted on the whole signal's bandwidth. Therefore, one cannot exploit the full ranging accuracy that can be achieved by NR signals.

- **Unknown mMIMO structure:** As discussed in the introduction of this chapter, mMIMO is a requirement for NR transmission to overcome high path loss, increase throughput, and reduce interference. In a conventional MIMO structure, all signal processing is performed in baseband and each antenna has a separate RF chain. In mmWaves, antenna elements must be placed close to each other to avoid granting lobes. Therefore, allocating one RF chain to each antenna element is impossible for mmWave mMIMO due to space limitations. Moreover, large number of RF chains increases the power consumption, which is a limiting factor [134]. Due to these limitations, hybrid analog-digital precoding and combining has been proposed for NR transmission. As a result, the channel measured in the digital baseband is intertwined with the choice of analog precoding and combining vectors and the entries of the channel matrix are not directly accessible. Therefore, existing approaches to estimate angles and TOA are not straightforwardly applicable, since the choice of hybrid-digital precoding structure, the number of antennas at the gNB, and the structure of array depend on the network provider and is unknown at the UE.

- **Need for specialized receiver structure:** A specialized receiver is required to extract navigation observables from NR signals, since these signals are not designed for navigation purposes.

- **Unknown gNBs' clock biases:** NR signals are designed for communication purposes. Therefore, a stringent level of synchronization between gNBs is not required.

In order to achieve an accurate navigation solution with NR signals, the gNBs' clock biases must be known and removed from the pseudorange measurements. However, these clock biases are unknown at the UE and must be estimated.

7.2 NR Signal Structure

This section presents the low-level models of NR signals and frame structure.

7.2.1 NR Frame Structure

NR downlink transmission is based on orthogonal frequency division multiplexing (OFDM) modulation with cyclic prefix (CP). An NR frame has a duration of 10 ms and consists of 10 subframes with durations of 1 ms. A frame can also be decomposed into two half-frames, where subframes 0 to 4 form half-frame 0 and subframes 5 to 9 form half-frame 1. This structure enables the coexistence of LTE and NR systems.

In the time-domain, each subframe breaks down into numerous slots, each of which contains 14 OFDM symbols for a normal CP length. The number of slots per subframe depends on the subcarrier spacing. In contrast to LTE, which has a constant subcarrier spacing of 15 kHz, NR defines different numerologies $\mu \in \{0, \cdots, 4\}$ to support flexible subcarrier spacing $\Delta f = 2^{\mu} \cdot 15$ [kHz]. As a result, there are 2^{μ} slots in each subframe and the CP is down-scaled by a factor of 2^{μ} compared to the LTE signal's CP length [1]. Subcarrier spacings of 15 and 30 kHz are more suitable for FR1 since the signal's attenuation is lower and the cell size can be larger, while higher subcarrier spacings are more applicable to FR2.

In the frequency-domain, each subframe is divided into numerous resource grids, each of which has multiple resource blocks with 12 subcarriers. The number of resource grids in the frame is provided to the UE from higher level signallings. A resource element is the smallest element of a resource grid that is defined by its symbol and subcarrier number. Fig. 7.1 summarizes the NR frame structure.

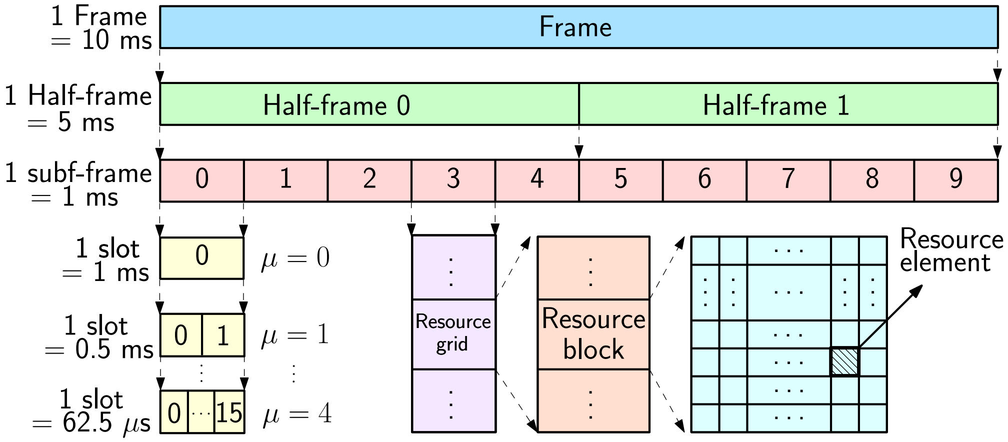


Figure 7.1: NR frame structure

7.2.2 NR SS/PBCH Block

When a UE receives an NR signal, it must first convert the signal into the frame structure to be able to extract the transmitted information. This is achieved by first identifying the frame start time. Then, knowing the frame start time, the UE can remove the CPs and take a fast Fourier transform (FFT) to construct all the OFDM symbols in the frame.

To provide frame timing to the UE, a gNB broadcast synchronization signals (SS) on pre-specified symbol numbers, which are known at the UE. The UE can obtain frame start time by acquiring the SS. An SS includes a primary synchronization signal (PSS) and a secondary synchronization signal (SSS), which provide symbol and frame timing, respectively.

The PSS and SSS are transmitted along with the physical broadcast channel (PBCH) signal and its associated demodulation reference signal (DM-RS) on a block called SS/PBCH block. The SS/PBCH block consists of four consecutive OFDM symbols and 240 consecutive subcarriers. Fig. 7.2 demonstrates an SS/PBCH block structure and Table 7.1 shows the subcarriers and symbols allocated to each symbol in the SS/PBCH block.

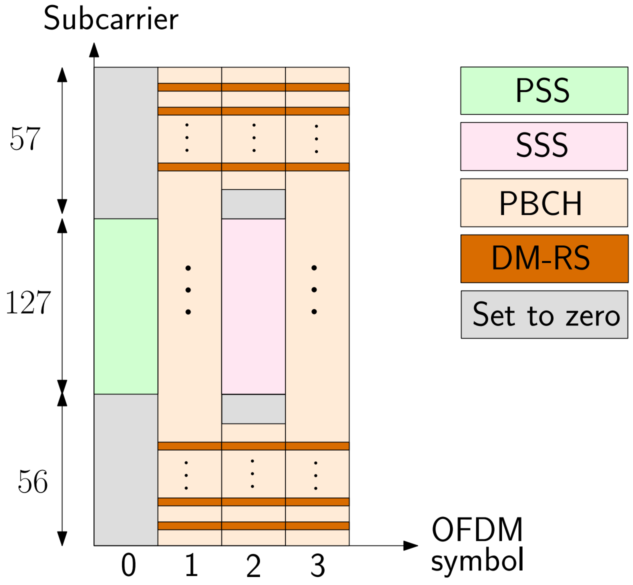


Figure 7.2: SS/PBCH block structure

The frequency location of the SS/PBCH block depends on the NR high-level signallings. The SS/PBCH block has a periodicity of 20 ms and is transmitted numerous times on one of the half frames, which is also known as SS/PBCH burst. Each SS/PBCH block is transmitted in a different direction using beamforming techniques. The OFDM symbol numbers on which the SS/PBCH block starts and the number of SS/PBCH blocks per frame depend on the numerology and transmission frequency f_c of the signal. Table 7.2 summarizes these values based on Section 4.1 of [135]. Index 0 in this table represents the first symbol of the half frame containing SS/PBCH blocks. Note that in the 5G protocol, SS/PBCH is not transmitted on subcarrier spacing of 60 kHz.

7.2.3 PSS and SSS Sequence Generation

The PSS and SSS are two orthogonal maximum-length sequences (m-sequences) of length $N_{\text{SS}} = 127$, which are transmitted on contiguous subcarriers. The PSS is transmitted in one form of three possible sequences, each of which maps to an integer representing the sector ID of the gNB, i.e., $N_{ID}^{(2)} \in \{0, 1, 2\}$.

Table 7.1: Symbol and subcarrier numbers in an SS/PBCH block based on Table 7.4.3.1-1 in [1]

Signal type	**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, $\cdots$, 191
PBCH	1, 3	0, 1, $\cdots$, 239
	2	0, 1, $\cdots$ 47, 192, 193, $\cdots$, 239
DMRS	1, 3	$0 + v$, $4 + v$, $\cdots$, 236+ v
	2	$0 + v$, $4 + v$, $\cdots$, 44+ v $192 + v$, $196 + v$, $\cdots$, $236 + v$

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

Table 7.2: 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	$\{2, 8\} + 14n$	$\{0, 1\}$
	$3 < f_c \leq 6$ GHz		$\{0, \cdots, 3\}$
Case B: 30	$f_c \leq 3$ GHz	$\{4, 8, 16, 20\} + 28n$	$\{0\}$
	$3 < f_c \leq 6$ GHz		$\{0, 1\}$
Case C: 30	$f_c \leq 3$ GHz	$\{2, 8\} + 14n$	$\{0, 1\}$
	$3 < f_c \leq 6$ GHz		$\{0, \cdots, 3\}$
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	$\{8, 12, 16, 20, 32,$ $36, 40, 44\} + 56n$	$\{0, \cdots, 8\}$

The SSS is transmitted in one of 336 possible forms, each of which maps to an integer representing the gNB's group identifier, i.e., $N_{ID}^{(1)} \in \{0, \cdots, 335\}$. The values of $N_{ID}^{(2)}$ and $N_{ID}^{(1)}$ define the physical cell identity of the gNB according to

$$N_{ID}^{Cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}.$$

The instructions to generate the PSS and SSS sequences are provided in Section 7.4.2 of [1].

7.2.4 PBCH Sequence Generation

PBCH is a physical channel to transmit essential system information for establishing a connection between the gNB and UE. These parameters are sent in a block called master information block (MIB). An MIB is a 23 bits message containing: (1) frame number (6 bits), (2) subcarrier spacing (1 bit) (this bit shows subcarrier spacing of 15 or 30 kHz for FR1 and subcarrier spacing of 60 or 120 kHZ for FR2), (3) subcarrier offset between the first subcarrier of SS/PBCH block and the first subcarrier of the resource grid containing the SS/PBCH block k_{SSB} (4 bits), (4) position of the DM-RS corresponding to physical downlink shared channel (PDSCH) (1 bit), (5) parameters related to the physical downlink control channel (PDCCH) and system information block (SIB) (8 bits), (6) a flag showing if the cell is barred or not (a UE may not use a barred cell for cell selection/reselection) (1 bit), (7) a flag to allow intra frequency reselection (1 bit), and (8) a spare bit (1 bit) [136]. PBCH also contains 1 bit message representing the type of message in PBCH, which can be either MIB or a messageClassExtension. Therefore, the size of PBCH message is 24 bits [136]. Once the PBCH message is generated at the higher layers, it is encoded and transmitted on physical channel. Fig. 7.3 shows the block diagram of PBCH coding stages, in which PBCH message is denoted by vector $\bar{\boldsymbol{a}}$ of length $\bar{A} = 24$ [1, 137].

In the payload generation stage, PBCH message $\bar{\boldsymbol{a}}$ is first extended to length $A = \bar{A} + 8$

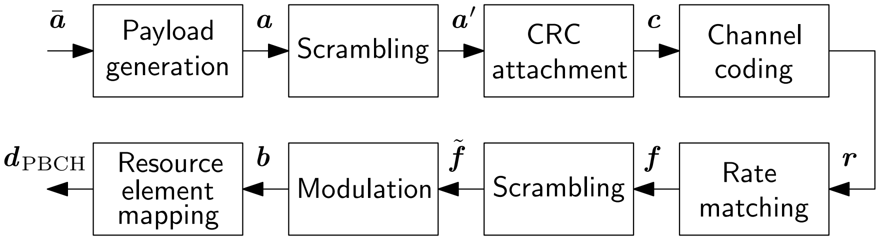


Figure 7.3: PBCH coding block diagram

and then interleaved according to Section 7.1.1 in [137]. Next, the resulting vector $\boldsymbol{a}$ is scrambled to $\boldsymbol{a}'$ of size 32 based on Section 7.1.2 of [137]. Then, the entire vector is used to generate cyclic redundancy check (CRC) parity bits of length 32 according to Section 7.1.3 of [137]. The resulting CRC is attached to vector $\boldsymbol{a}'$, resulting in vector $\boldsymbol{c}$ of length 64. The vector $\boldsymbol{c}$ is then passed to the channel coding block, where a polar coding is used to code the message according to Section 7.1.4 of [137]. The output of channel coding block is passed to the rate matching block, resulting in vector $\boldsymbol{f}$ of length 864 as discussed in Section 7.1.5 in [137]. Then, the vector $\boldsymbol{f}$ is scrambled, modulated to quadrature phase-shift keying (QPSK) symbols, and mapped to physical resources according to Section 7.3.3 in [1]. The scrambling code at this stage depends on the SS/PBCH block index. Therefore, by decoding PBCH message, the exact symbol number can be obtained. The final PBCH sequence $\boldsymbol{d}_{\text{PBCH}}$ with length of 432 is transmitted on the symbols allocated to this message, which are shown in Fig. 7.2.

7.2.5 DM-RS for PBCH Sequence Generation

A DM-RS is a reference signal, which is transmitted to the UE to provide an estimate of the channel frequency response. In NR, each physical channel has a DM-RS signal, which is used for decoding that specific physical channel, and also providing some system parameters. The DM-RS is transmitted on only specific symbols and subcarriers (not the whole transmission band). A DM-RS for PBCH depends on the half frame containing the SS/PBCH block n_{hf}, the number of SS/PBCH block transmission per frame, and the SS/PBCH block index i_{SSB}. The structure of DM-RS sequence is shown in Section 7.4.1.4 of [1].

7.3 Receiver Structure

This section presents the structure of the proposed SDR to opportunistically extract TOA from NR signals. The proposed SDR consists of three main stages: (1) carrier frequency extraction, (2) acquisition, and (3) tracking. Each of these stages are discussed in details next.

7.3.1 Carrier Frequency Extraction

When a UE is activated, it first needs to perform a blind search over all possible frequencies in order to find any available SS/PBCH block. In NR, only specified channel raster can carry SS/PBCH blocks, which is called synchronization raster. The center frequency of the synchronization channel raster, which is equivalent to the frequency of the 121th subcarrier of the SS/PBCH block, is denoted by SS_{ref}. The value of SS_{ref} is a function of a parameter called global synchronization channel number (GSCN). This function depends on the frequency band of the signal and is presented in Section 5.4.3.1 of [132].

It is worth mentioning that if a UE knows SS_{ref} *a priori*, it can skip this stage.

7.3.2 Acquisition

Once the UE determines the SS/PBCH block center frequency SS_{ref}, it starts sampling at a minimum rate equal to the SS/PBCH transmission bandwidth. Next, it wipes off the carrier frequency to convert the samples into the baseband domain. The resulting samples are correlated with all the possible PSS sequences and the PSS sequence corresponding to the highest correlation peak determines the $N_{ID}^{(2)}$. The location of the peak of the correlation represents the SS/PBCH symbol start time and can be used to control the FFT window. Then, the cyclic prefix is removed from the signal and by taking the FFT from the received samples, the signal is converted into the frame structure. At this stage, the UE can extract the SS/PBCH block. Next, the received SSS signal is correlated with all possible SSS sequences, and the one corresponding to the highest correlation peak determines the value of $N_{ID}^{(1)}$. Knowing $N_{ID}^{(1)}$ and $N_{ID}^{(2)}$, the UE is able to calculate the cell ID N_{ID}^{Cell}. The cell ID is used to map the subcarriers allocated to the DM-RS. An exhaustive search must be performed over all possible DM-RS sequences and the one with the highest peak is selected. Once the DM-RS sequence is detected, it can be used to estimate the channel frequency response (CFR). The next stage is to decode the PBCH message. For this purpose, the effect of CFR on the received PBCH message is removed using a channel equalizer. Then, the resulting PBCH message is decoded by following the steps in Fig. 7.3 in reverse order.

After obtaining the PBCH message, the UE can reconstruct the SS/PBCH block locally. Then, the resulting code on the second or fourth symbol of the SS/PBCH block is used to estimate the CFR and refine the frame start time, which is called TOA in this paper. The TOA refinement can be performed using a super resolution algorithm such as estimation of signal parameters via rotational invariant techniques (ESPRIT) [52]. The phase difference between the CFR on the second and fourth symbols of the PBCH is used to provide a coarse estimate of Doppler frequency $\hat{f}_D$. Fig. 7.4 summarizes the structure of the acquisition stage.

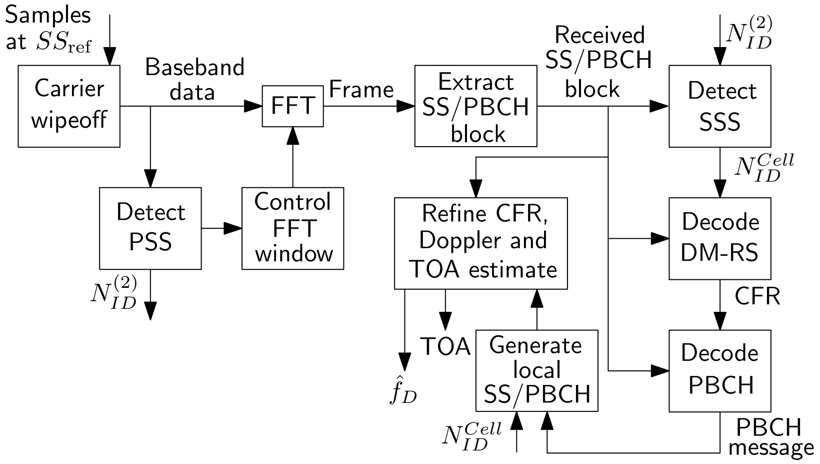


Figure 7.4: Block diagram of the acquisition stage

7.3.3 Tracking

After obtaining a coarse estimate of the TOA, a tracking loop can be used to refine the TOA estimate and keep track of any changes. The tracking loop is composed of a phase-locked loop (PLL)-aided delay-locked loop (DLL). The main components of the PLL and DLL are: a discriminator function, a low-pass filter (LPF), and a numerically-controlled oscillator (NCO). Fig. 7.5 shows the structure of the proposed tracking loop.

At each tracking loop iteration, the estimated phase, which is obtained by integrating the Doppler frequency $\hat{f}_D$ over time, is removed from the baseband signal. Then, the estimated TOA, which is normalized by the sampling time T_s, is divided into a fractional part $0 \leq \text{Frac}\{\cdot\} < 1$ and an integer part $\text{Int}\{\cdot\}$. The integer part is used to control the FFT window, while the fractional part is removed from the signal in the frequency domain using a phase rotation. Then, the DLL and PLL are used to estimate the remaining code and carrier phase errors, respectively.

It has been shown that the PLL discriminator function can be the phase of the integrated CFRs over the entire subcarriers [49]. An early-power-minus-late-power discriminator function can be used for the DLL discriminator function to derive the normalized timing error

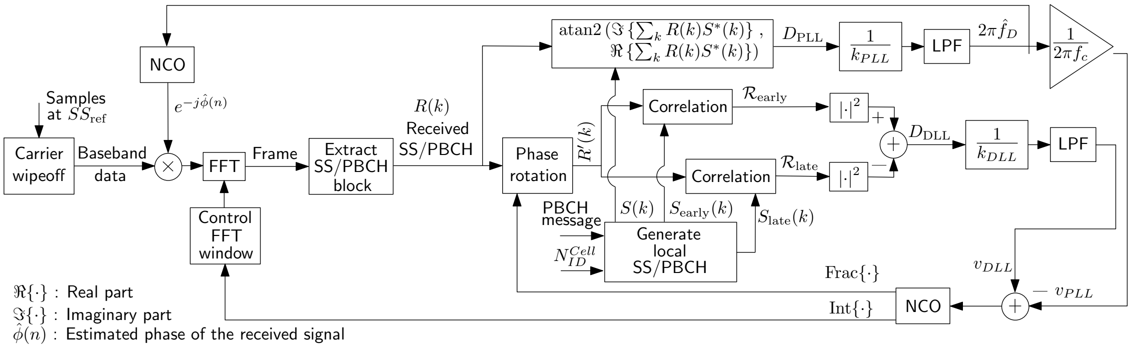


Figure 7.5: Block diagram of the tracking stage

$\tilde{e}_\tau$ [45]. Since a shift in the time-domain is equivalent to a phase rotation in the frequency-domain, the locally generated early and late code signals for the OFDM symbol can be obtained respectively as

$$
\begin{aligned}
S_{\text{early}}(k) &= e^{-j2\pi\xi k/K}S(k),\\
S_{\text{late}}(k) &= e^{j2\pi\xi k/K}S(k),\\
\text{for}\quad k &= 0,\cdots,K-1.
\end{aligned}
$$

where $S(k)$ is the locally generated SS/PBCH symbol at the k-th subcarrier, $K = 240$ is the number of subcarriers allocated to the SS/PBCH block at each symbol, and $0 < \xi \leq 1/2$ is the normalized time shift. The early and late correlations in the frequency-domain can be expressed respectively as

$$
\begin{aligned}
\mathcal{R}_{\text{early}} &= \sum_{k=0}^{K-1} R'(k)S^*_{\text{early}}(k),\\
\mathcal{R}_{\text{late}} &= \sum_{k=0}^{K-1} R'(k)S^*_{\text{late}}(k),
\end{aligned}
$$

where $R'(k)$ is the received signal at the k-th subcarrier after phase shift. The DLL discriminator function is defined as

$$D_{\mathrm{DLL}} \triangleq |\mathcal{R}_{\mathrm{early}}|^2 - |\mathcal{R}_{\mathrm{late}}|^2 \triangleq K^2 C \Lambda_{\mathrm{DLL}}(\tilde{e}_\tau, \xi) + N_{\mathrm{DLL}}, \tag{7.1}$$

where C is the received signal power, $\Lambda_{\mathrm{DLL}}(\tilde{e}_\tau, \xi)$ is the normalized S-curve function, defined as

$$\begin{aligned}\Lambda_{\mathrm{DLL}}(\tilde{e}_\tau, \xi) \triangleq & \left[\frac{\sin(\pi(\tilde{e}_\tau - \xi))}{K \sin(\pi(\tilde{e}_\tau - \xi)/K)}\right]^2 \\ & - \left[\frac{\sin(\pi(\tilde{e}_\tau + \xi))}{K \sin(\pi(\tilde{e}_\tau + \xi)/K)}\right]^2,\end{aligned}$$

and N_{DLL} represents the noise with zero-mean and variance

$$\begin{aligned}\mathrm{var}[N_{\mathrm{DLL}}] \leq 2K^2\sigma^4 & \left[1 + \frac{C}{K\sigma^2}\left(\frac{\sin(\pi(\tilde{e}_\tau - \xi))}{\sin(\pi(\tilde{e}_\tau - \xi)/K)}\right)^2\right. \\ & \left. + \frac{C}{K\sigma^2}\left(\frac{\sin(\pi(\tilde{e}_\tau + \xi))}{\sin(\pi(\tilde{e}_\tau + \xi)/K)}\right)^2\right],\end{aligned} \tag{7.2}$$

where equality holds for $\xi = 0.5$ and σ^2 is the variance of the received signal's noise [45]. In the following analysis, ξ is set to be 0.5.

The output of the discriminator functions are first normalized by the slope of the discriminator functions at zero error. Then, a loop filter is used to achieve zero steady-state error. It can be assumed that the symbol timing error has linear variations and a second-order loop filter can be used to achieve zero steady-state error. Therefore, a first-order LPF can be used with a transfer function given by

$$F(s) = 2\zeta\,\omega_L + \frac{\omega_L^2}{s}, \tag{7.3}$$

where ω_L is the undamped natural frequency of the delay loop and ζ is the damping ratio. The damping ratio was set to $1/\sqrt{2}$ to have a step response that rises fast enough with little overshoot [69]. Therefore, the noise-equivalent bandwidth is $B_L = 0.53\,\omega_L$ [61]. The loop filter transfer function in (7.3) is discretized and realized in state-space. The loop update rate was set to two frame duration, i.e., $T_f = 20$ ms since SS/PBCH block has periodicity of 20 ms.

Finally, the TOA estimate $\hat{e}_\tau$ is updated according to

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

where v_{DLL} and v_{PLL} are the outputs of the DLL and PLL filters, respectively.

7.4 Code Phase Error Statistics

In this section, the SS/PBCH block open-loop code phase error in the absence and presence of multipath is evaluated. Since the derivation of the results are similar to the ones in [49] and [45], only the final expressions are presented.

7.4.1 Code Phase Error in Multipath-Free Environment

It can be shown that the open-loop code phase error due to noise is a random variable with zero-mean and variance

$$\sigma^2_{\tilde{\varepsilon}} \approx \frac{c^2\pi^2}{128\Delta f^2 K^3 C/N_0}, \qquad [\mathrm{m}^2] \tag{7.4}$$

where c is the speed of light. Fig. 7.6 compares the standard deviation of the code phase error for different values of C/N_0 and for different numerologies. It can be seen that due to the large transmission bandwidth of higher numerologies, the standard deviation of code phase error is an order of magnitude lower compared to lower numerologies.

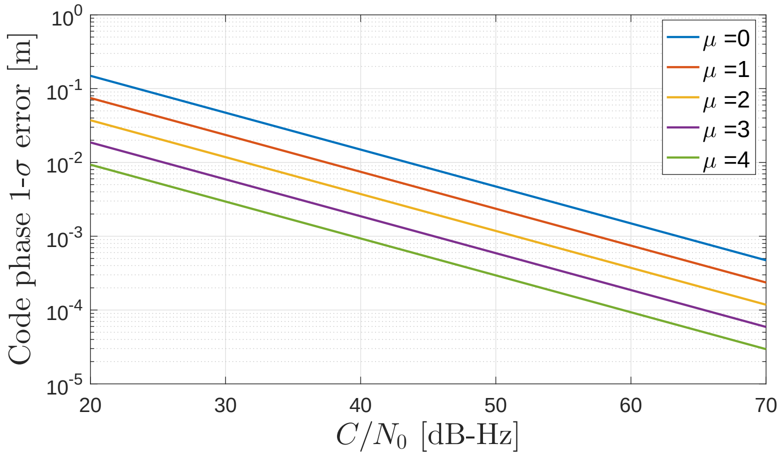


Figure 7.6: Standard deviation of the code phase error for different values of C/N_0 and for different numerologies

7.4.2 Code Phase Error in a Multipath Environment

Multipath environments introduce a bias in the DLL discriminator function given by [45]

$$b = \frac{c\left(\sin\left(\frac{\pi}{2K}\right)\right)^3}{4\pi\Delta f\cos\left(\frac{\pi}{2K}\right)}\left(\chi_1+\chi_2\right), \qquad [\mathrm{m}] \tag{7.5}$$

where

$$\begin{aligned}\chi_1 = &\left|\sum_{k=0}^{K-1}\sum_{l=1}^{L-1}\alpha_l\, e^{-j2\pi(k/K)(\tau_l/T_s-\xi)}\right|^2\\ &-\left|\sum_{k=0}^{K-1}\sum_{l=1}^{L-1}\alpha_l\, e^{-j2\pi(k/K)(\tau_l/T_s+\xi)}\right|^2,\end{aligned}$$

$$
\begin{aligned}
\chi_2 = 2\, \Re \Bigg\{ & \left[\sum_{k=0}^{K-1} e^{j2\pi(k/K)\xi} \right] \\
& \cdot \left[\sum_{k'=0}^{K-1} \sum_{l=1}^{L-1} \alpha^*(l) e^{j2\pi(k'/K)(\tau_l/T_s-\xi)} \right] \Bigg\} \\
& - 2\, \Re \Bigg\{ \left[\sum_{k=0}^{K-1} e^{-j2\pi(k/K)\xi} \right] \\
& \cdot \left[\sum_{k'=0}^{K-1} \sum_{l=1}^{L-1} \alpha^*(l) e^{j2\pi(k'/K)(\tau_l/T_s+\xi)} \right] \Bigg\},
\end{aligned}
$$

where $\Re\{\cdot\}$ denotes the real part; L is the number of multipath components; α_l and τ_l are the relative attenuation and delay components, respectively, of the channel impulse response's l-th path; $\alpha_0 = 1$ and $\tau_0 = 0$; and $\xi = 0.5$. To evaluate the effect of multipath delay on the SS/PBCH block ranging error, a channel with only one LOS and one multipath component is considered, where the multipath component has 6 dB lower amplitude than the LOS signal. Fig. 7.7 shows the results. The solid and dashed lines represent the results for constructive and destructive multipath, respectively. It can be seen that although multipath can cause high error on low numerologies, higher numerologies are more robust to multipath.

A proper channel model is essential for evaluating the effect of multipath on the SS/PBCH ranging performance. The existing channel models must be modified to be adopted for mmWaves, since they have different radio propagation characteristics than sub-6 GHz signals. Over the past years, several channel models have been proposed to model radio propagation characteristics of different frequency bands [138]. In this paper, tapped delay line (TDL) 3GPP channel model is used, which is a proper model for simplified evaluations, e.g., non-MIMO evaluations, and is valid for a frequency range between 0.5 GHz and 100 GHz [139]. More specifically, TDL-D and TDL-E channel models are considered to model a LOS propagation environment, where the first tap follows a Rician fading distribution and the rest of the taps follow Rayleigh distribution. Channel delay's taps can have different delay spreads from very short to very long. For each channel model, 10^5 channel taps are

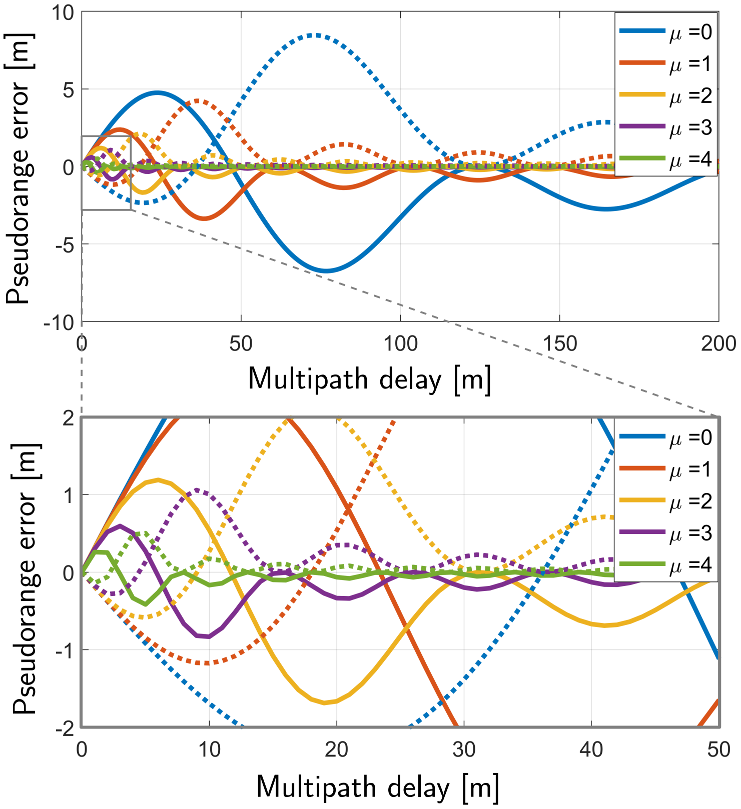


Figure 7.7: Code phase error for a multipath channel with $\alpha_0 = 1$ and $\alpha_1 = 0.2512$ and for different numerologies. The solid and dashed lines represent constructive and destructive interferences, respectively. The bottom figure is a zoomed version of the top figure.

generated according to the specified distributions in Section 7.7.2 of [139]. Then, multipath error is calculated according to (7.5). Fig. 7.8 shows the histogram of the code phase error for different numerologies and for (a) TDL-D and (b) TDL-E channel models with nominal delay spread. Similar figures can be plotted for the rest of the delay spreads. It can be seen that the distribution has slightly heavier tail for positive multipath errors, which is due to the fact that multipath delays are always larger than the LOS delay.

The mean and standard deviation of the error for each channel model are obtained, which are presented in Fig. 7.9 and 7.10. It can be seen that for each channel model, e.g., a TDL-D with short delay spread, increasing subcarrier spacing (i.e., increasing numerologies) reduces the mean and standard deviation of the error. This is due to the fact that for larger subcarrier spacing, the SS/PBCH signal bandwidth is larger, which provides higher

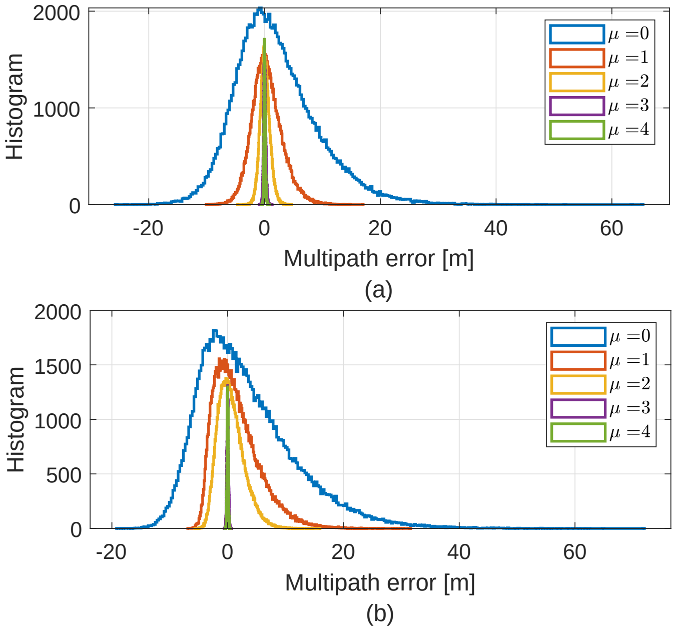
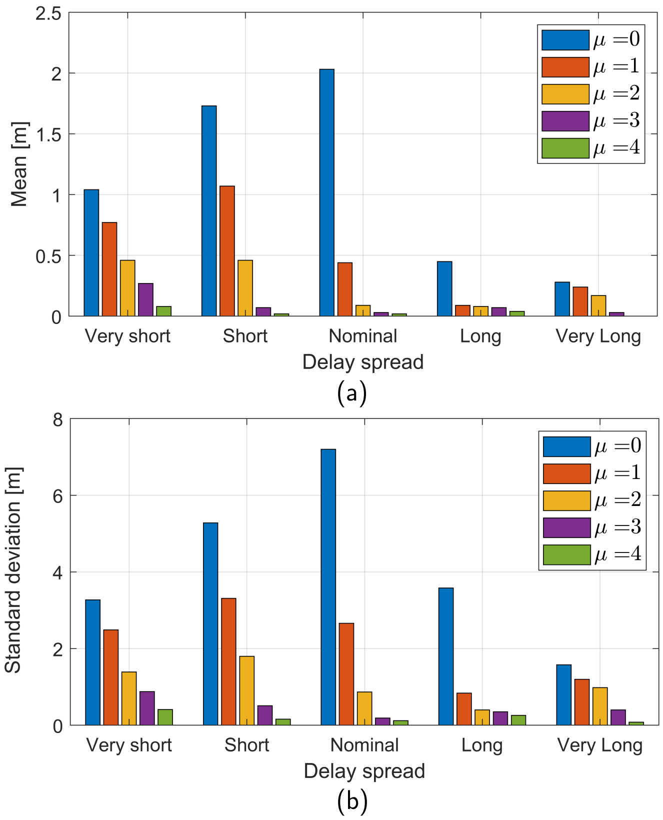


Figure 7.8: Histogram of the code phase error for different numerologies and for (a) TDL-D and (b) TDL-E channel models with nominal delay spread

resolution to differentiate the LOS from multipath. Fig. 7.7, 7.9, and 7.10 also show that pseudorange error does not decrease monotonically with the multipath delay. This is due to the limited band of the received signal, which causes a sinc autocorrelation function in the time domain.

7.5 Position Estimation Error Statistics

The structure of the proposed SDR to extract navigation observables from NR signals was discussed in Section 7.3. Then, the achievable ranging precision and the model of multipath error were derived in Section 7.4. In this section, these results are used to derive the statistics of the position estimation error.



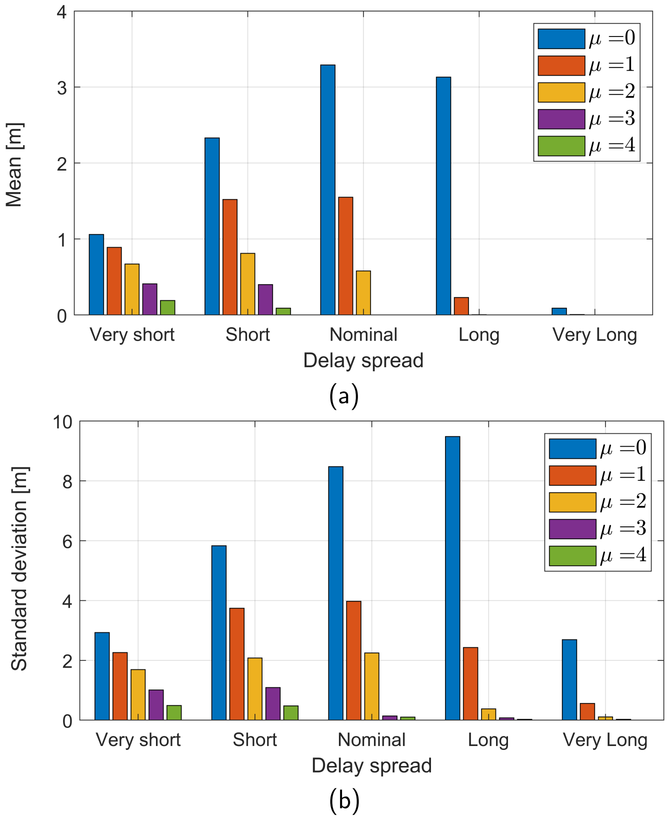
(a)

(b)

Figure 7.9: Mean and standard deviation of the code phase error for different values of delay spread for a TDL-D channel model

7.5.1 TOA Measurement Model

Consider a 2-dimensional (2D) network of $U \geq 3$ gNBs, which are distributed independently and uniformly around the UE with a binomial point process (BPP) model [140]. The minimum distance between the UE and the gNBs for far-field assumption to hold is assumed to be $d_{\min}$. The maximum distance for which ranging signals can be detected by the UE is assumed to be $d_{\max}$. The location of the u-th gNB can be presented by $(d^{(u)}, \phi^{(u)})$, where $d^{(u)} = \left\| \boldsymbol{r}_{\mathrm{r}} - \boldsymbol{r}_{\mathrm{s}}^{(u)} \right\|$ is the distance between the u-th gNB and the UE and $\phi^{(u)} = \arctan\left(\frac{y_{\mathrm{s}}^{(u)} - y_{\mathrm{r}}}{x_{\mathrm{s}}^{(u)} - x_{\mathrm{r}}}\right)$, where $\boldsymbol{r}_{\mathrm{r}} = [x_{\mathrm{r}}, y_{\mathrm{r}}]^{\mathsf{T}}$ and $\boldsymbol{r}_{\mathrm{s}}^{(u)} = \left[x_{\mathrm{s}}^{(u)}, y_{\mathrm{s}}^{(u)}\right]^{\mathsf{T}}$ are the locations of the UE and the u-th gNB, respectively. For simplicity, it is assumed that the gNBs and UE are synchronized.



(a)

(b)

Figure 7.10: Mean and standard deviation of the code phase error for different values of delay spread for a TDL-E channel model

The UE makes TOA measurements to all gNBs according to

$$\boldsymbol{\rho} = \boldsymbol{d} + \boldsymbol{b} + \boldsymbol{\varepsilon}, \tag{7.6}$$

where $\boldsymbol{\rho} \triangleq \left[\rho^{(1)}, \cdots, \rho^{(U)}\right]^{\mathsf{T}}$ is the vector of TOA measurements; $\boldsymbol{d} \triangleq \left[d^{(1)}, \cdots, d^{(U)}\right]^{\mathsf{T}}$ is the vector of ranges; $\boldsymbol{b} \triangleq \left[b^{(1)}, \cdots, b^{(U)}\right]^{\mathsf{T}}$ is the vector of biases caused by multipath according to (7.5), with mean $\boldsymbol{\mu}_b$ and covariance matrix $\boldsymbol{\Sigma}_b$; and $\boldsymbol{\varepsilon} \triangleq \left[\varepsilon^{(1)}, \cdots, \varepsilon^{(U)}\right]^{\mathsf{T}}$, where $\varepsilon^{(u)}$ is the measurement noise, which is modeled as zero-mean Gaussian random variable with standard deviation of $\sigma_\varepsilon^{(u)}$. Since the effect of multipath and noise on TOA measurements are independent, the covariance matrix of $\boldsymbol{\rho}$ can be obtained according to

$$\boldsymbol{\Sigma}_\rho \triangleq \operatorname{cov}\left\{\boldsymbol{\rho}\right\} = \boldsymbol{\Sigma}_\varepsilon + \boldsymbol{\Sigma}_b,$$

where $\mathbf{\Sigma}_{\varepsilon} \triangleq \operatorname{cov}\{\boldsymbol{\varepsilon}\} = \operatorname{diag}\left[\sigma_{\varepsilon}^{(1)^2}, \cdots, \sigma_{\varepsilon}^{(U)^2}\right]$ and diag represents diagonal matrix.

Denoting the received carrier-to-noise ratio from the gNB located at distance $d_{\min}$ to the UE by C/N_0, and using the path-loss model, it can be shown that the carrier-to-noise ratio of the u-th gNB follows

$$(C/N_0)^{(u)} = \left(\frac{d_{\min}}{d^{(u)}}\right)^a C/N_0, \tag{7.7}$$

where a is the path-loss exponent, which depends on the propagation environment [141]. Therefore, using the results of (7.4), the u-th gNB's TOA measurement noise variance can be modeled according to

$$\sigma_{\varepsilon}^{(u)^2} = \frac{c^2\pi^2}{128\Delta f^2 K^3 C/N_0}\left(\frac{d^{(u)}}{d_{\min}}\right)^a \qquad [\mathrm{m}^2]. \tag{7.8}$$

7.5.2 Position Estimation Error Statistics

The UE can obtain an estimate of $\mathbf{\Sigma}_{\varepsilon}$ using the correlation function. However, the UE does not have any information about the multipath bias on its estimated TOA, since the channel impulse response parameters are not estimated in the DLL. Therefore, $\boldsymbol{b}$ is unknown at the UE and is assumed to be zero.

It is assumed that the UE employs a weighted nonlinear least squares (WNLS) estimator. Therefore, if $\boldsymbol{b}$ is nonzero, it can be shown that the UE's position estimation error $\tilde{\boldsymbol{r}}_r$ has the following mean and covariance matrix

$$\mathbb{E}\{\tilde{\boldsymbol{r}}_r\} = \left(\mathbf{G}^{\mathsf{T}}\mathbf{\Sigma}_{\varepsilon}^{-1}\mathbf{G}\right)^{-1}\mathbf{G}^{\mathsf{T}}\mathbf{\Sigma}_{\varepsilon}^{-1}\boldsymbol{b}, \tag{7.9}$$

$$\begin{aligned}\operatorname{cov}\{\tilde{\boldsymbol{r}}_r\} = &\left(\mathbf{G}^{\mathsf{T}}\mathbf{\Sigma}_{\varepsilon}^{-1}\mathbf{G}\right)^{-1} \\ &+\left(\mathbf{G}^{\mathsf{T}}\mathbf{\Sigma}_{\varepsilon}^{-1}\mathbf{G}\right)^{-1}\mathbf{G}^{\mathsf{T}}\mathbf{\Sigma}_{\varepsilon}^{-1}\mathbf{\Sigma}_b\mathbf{\Sigma}_{\varepsilon}^{-1}\mathbf{G}\left(\mathbf{G}^{\mathsf{T}}\mathbf{\Sigma}_{\varepsilon}^{-1}\mathbf{G}\right)^{-1},\end{aligned} \tag{7.10}$$

Table 7.3: Monte Carlo simulation parameters

Parameter	**Values**
C/N_0	60 [dB-Hz]
a	3.7
$d_{\min}$	10
$d_{\max}$	200
U	$\{5, 10, 15\}$

where

$$\mathbf{G} \triangleq \begin{bmatrix} \cos\phi^{(1)}, & \cdots, & \cos\phi^{(U)} \\ \sin\phi^{(1)}, & \cdots, & \sin\phi^{(U)} \end{bmatrix}^{\mathsf{T}}.$$

Next, the effect of gNBs' locations and multipath error on the statistics of the position estimation error is evaluated. Since deriving a closed-form equation for the statistics of the position estimation error is intractable, the results will be limited to Monte Carlo simulations.

7.5.3 Numerical Results

In this section, Monte Carlo simulations are used to numerically analyze the statistics of the position estimation error for TDL-D and TDL-E channel propagation environments. As it was shown in Subsection 7.4.2, nominal delay spread has the highest ranging error. Therefore, the results of this subsection will be only limited to this worst-case scenario. For each multipath environment, 10^4 realizations of the channel impulse response and the location of the gNBs are generated and a WNLS is used to solve for the position of the UE. Table 7.3 summarizes the values of the Monte Carlo simulation parameters.

Fig. 7.11 shows the resulting cumulative distribution function (CDF) of the position estimation error. Table 7.4 shows the 95% probability position estimation error bounds for

$U = 5$ and $\mu = 0, \cdots, 4$. It can also be seen that increasing the numerologies has the highest effect on the position estimation error, while the effect of the number of gNBs on the error is insignificant.

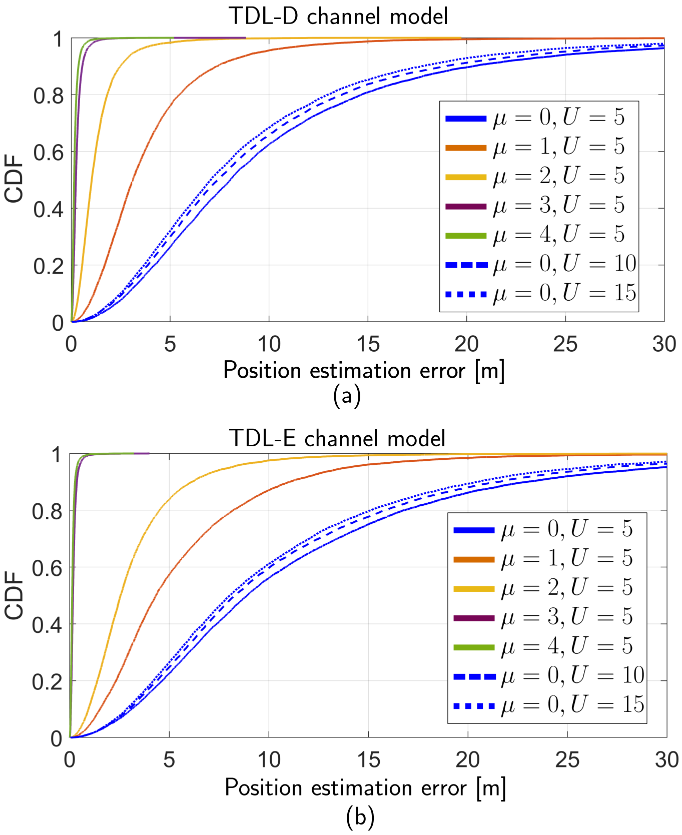


Figure 7.11: CDF of the position estimation error for TDL-D and TDL-E channel models with nominal delay spreads

7.6 Experimental Results

In order to evaluate the proposed receiver, an experiment was performed with real 5G signals in the Anteater parking structure at the University of California, Irvine, USA. In this section, the experimental hardware and software setup are first presented. Then, the experimental results are presented.

Table 7.4: Position estimation error $< \eta$ [m] with 95% probability

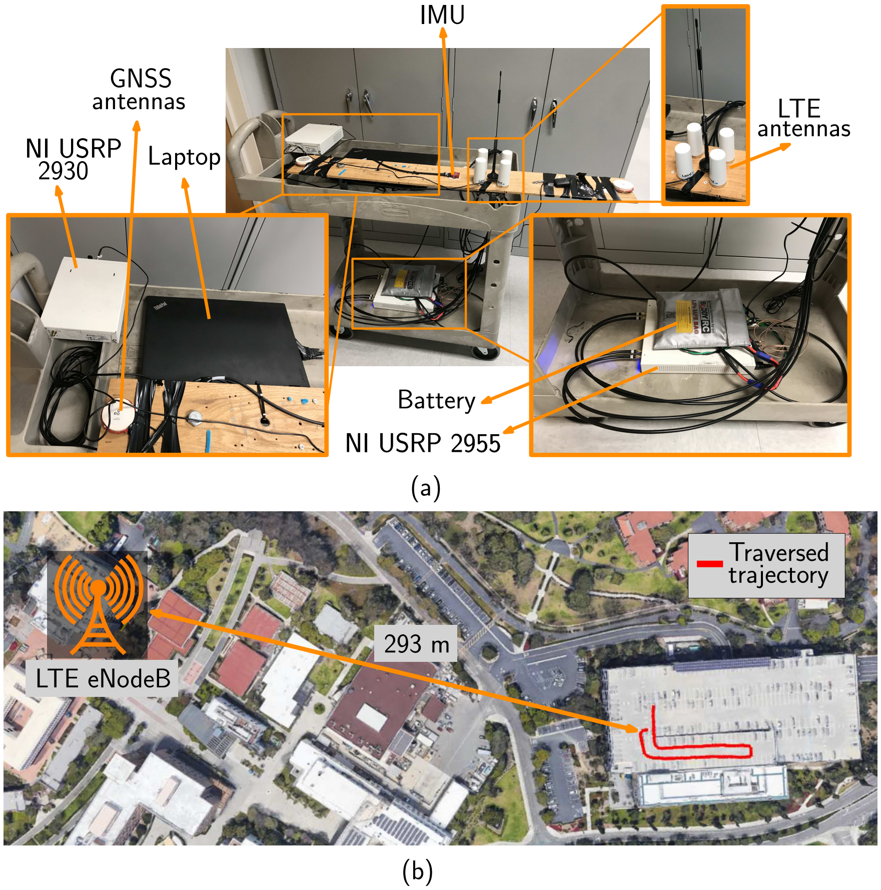
μ	$\eta_{\text{TDL-D}}$	$\eta_{\text{TDL-E}}$
0	26.85	29.74
1	9.75	13.98
2	3.24	8.06
3	0.74	0.46
4	0.48	0.36

7.6.1 Experimental Hardware and Software Setup

Since 5G protocol has been finalized very recently, it has not been fully implemented by all operators. The U.S. operators AT&T, Verizon, and Sprint have partially implemented their 5G networks in some areas of a few major cities. On December 6th, 2019, T-Mobile announced a nationwide 5G implementation on its band 71 (i.e., frequency range of 600 MHz). At the time and location of this paper's experiment, only T-Mobile was transmitting 5G signals and the available gNBs were limited to only this operator. Over the course of the experiment, the 5G signal to only one gNB was available. Therefore, extracting a position estimate from one pseudorange measurement was infeasible. Hence, the experimental results were confined to evaluating the pseudorange measurements.

In order to perform the experiment, a ground vehicle was equipped with 1 cellular Laird antenna to receive 5G signals at a center frequency of 630.05 MHz, which was obtained by searching over all possible frequency candidates as discussed in Section 7.3.1. Using Table 5.4.3.3-1 of [132], it can be seen that the SS/PBCH block can only accept Case A on band 71, which has 15 kHz subcarrier spacing. Therefore, the SS/PBCH block at this band has 3.6 MHz bandwidth. The cellular antenna was connected to a national instrument (NI) universal software radio peripheral (USRP)-2955, driven by a GPS-disciplined oscillator (GPSDO) to down-mix and sample 5G signals at 5 MSps. A laptop was used to record the samples using LabVIEW. The recorded samples were processed with MATLAB offline. A Septentrio

AsteRx-i V, which was equipped with dual antenna multi-frequency GNSS receiver with real-time kinematic (RTK) and a Vectornav VN-100 micro electromechanical systems (MEMS) inertial measurement unit (IMU), was used to estimate the position of the ground vehicle, which was used as the "ground truth." The ground vehicle traversed a loop path four times over 135 seconds. The code and carrier loop bandwidth were set to 0.1 and 4 Hz, respectively. Fig. 7.12 shows the experimental hardware setup, the location of the gNB, and the traversed trajectory.



(a)

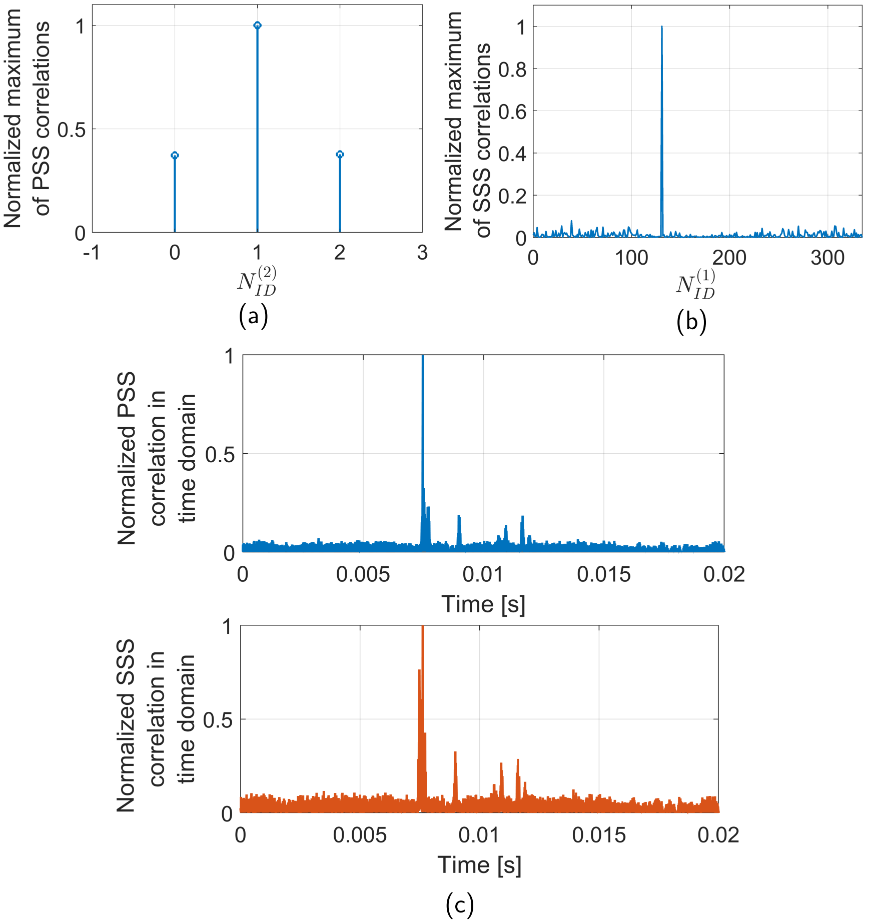
(b)

Figure 7.12: (a) Experimental hardware setup and (b) location of the gNBs and the traversed trajectory

7.6.2 Experimental Results

First, the received signal was correlated with all the possible PSS sequences and the one with the highest peak was selected resulting in $N_{ID}^{(2)} = 1$. Fig. 7.13(a) shows the maximum of the PSS correlations, which is normalized by the highest value. Next, the signal was converted to the frame structure and the SS/PBCH block was extracted. Then, the received SSS signal was correlated with all possible SSS sequences and the one with the highest peak was selected resulting in $N_{ID}^{(1)} = 131$. Fig. 7.13(b) shows the maximum of the SSS correlations, which is normalized by the highest value. Fig. 7.13(c) shows the normalized correlation of the received signal with the selected PSS and SSS sequences in time-domain. Note that as Table 7.2 shows, case A contains four SS/PBCH block for carrier frequency below 3 GHz. The small peaks on Fig. 7.13(c) show the position of the rest of the SS/PBCH blocks.

Fig. 7.14(a) shows the estimated pseudorange using the proposed receiver. In order to compare the results visually, the entire value of pseudorange is shifted to have similar initial value as the true range. The difference of these two curves is plotted in Fig. 7.14(b) with the blue line. It can be seen that this difference decreases over time. This is due to the clock drift. To remove the effect of the clock bias and drift, the measured pseudorange ρ over time t is modeled as $\rho(t) = d + \left(\dot{\delta} t + \delta\right) + \varepsilon$, where d is the actual range, δ and $\dot{\delta}$ are the clock bias and drift, respectively, and ε is the measurement noise. In this model, it is assumed that the clock has a constant drift over time and a first-order polynomial was fitted to estimate this drift. The resulting polynomial was used to remove the effect of the clock bias and drift from the estimated pseudorange. The red line in Fig. 7.14(b) shows the resulting first-order polynomial and the yellow line shows the difference of the pseudorange and range after removing the effect of the clock. The results showed that the estimated range has a standard deviation of 1.19 m. Since the experimental environment was a relatively open area, the received signal had less multipath than the TDL-D and TDL-E channel models. Therefore, the resulting standard deviation was less than the results presented in Fig. 7.9



(a)

(b)

(c)

Figure 7.13: (a) Maximum of correlation of the received signal with all possible PSS sequences, (2) maximum of correlation of the received signal with all possible SSS sequences, and (3) correlation of the received signal with the selected PSS and SSS sequence in time domain

and 7.10.

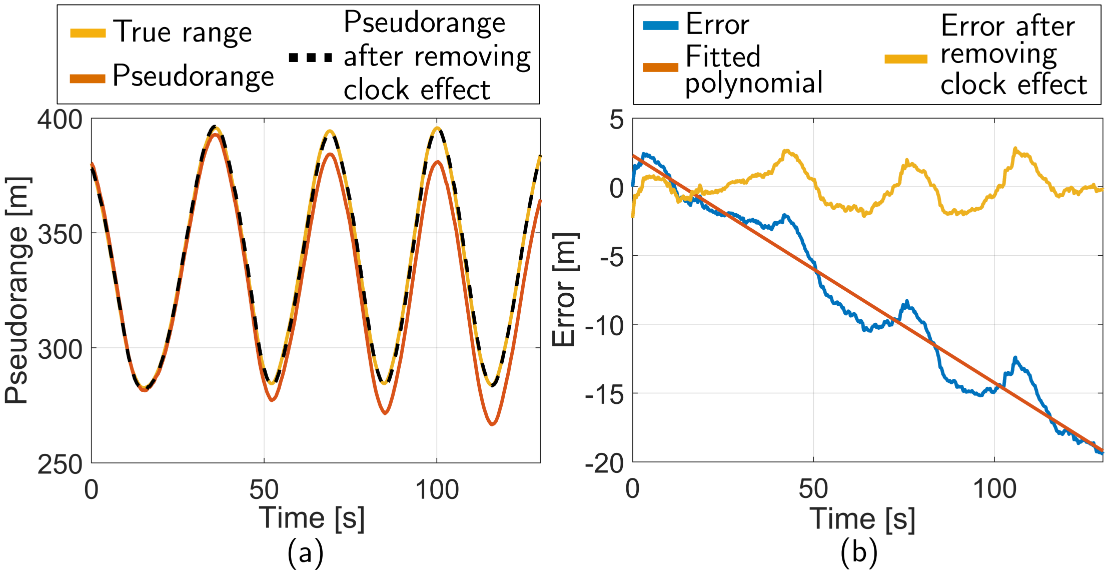


Figure 7.14: (a) Actual range, estimated pseudorange, and pseudorange after removing clock bias, (b) the difference between pseudorange and true range, fitted polynomial to this difference to model clock bias and drift, and remaining error after removing the clock effect

Chapter 8

Conclusions

In this dissertation, exploiting cellular LTE and NR signals for navigation was evaluated. The structure of cellular LTE signals was first presented and possible reference signals that can be exploited for navigation were discussed. Considering the advantages and disadvantages of these signals, the SSS and CRS were selected as two possible candidates for navigation and their received signal models were presented. Next, an SDR to extract navigation observables from these signals was presented, which consists of four main stages: (1) coarse acquisition, (2) system information extraction and neighboring cell identification, (3) acquisition refinement, and (4) tracking. Three different tracking methods were developed to extract navigation observables from the SSS and CRS signals. The first approach uses an FLL-assisted PLL and a carrier-aided DLL to track the code and carrier phase of the received SSS signal. The second approach uses an adaptive threshold-based approach to detect and track the first peak of the estimated CIR using the received CRS signals. The third approach uses a carrier-aided DLL to track the code and carrier phase of the received CRS signal. The achievable ranging accuracy of each of these methods were analyzed in multipath-free and multipath-rich environments. The results showed that the CRS can achieve higher ranging accuracy compared to the SSS, especially in multipath-rich environments due to the high transmission bandwidth of the CRS.

Next, three different navigation frameworks were presented to estimate the location of the UE. The first framework, which is an standalone navigation framework based on an EKF, uses the produced code phase measurements by the proposed SDR to estimate the location and velocity of the UE and the difference between the UE's clock bias and drift and those of the eNodeBs'. Experimental results validated that the CRS-based SDR has higher accuracy compared to the SSS-based one in multipath-rich environments. Moreover, experimental results demonstrated that the proposed SDR has higher precision and accuracy compared to the state-of-the-art. To remove the effect of the clock bias from the measurements, the second navigation framework was proposed, which is an standalone framework based on an EKF and uses the single difference code and carrier phase and Doppler frequency measurements to estimate the location and velocity of the UE. In this framework, the eNodeBs' clock biases are initialized and assumed constant over the course of the navigation. A method to detect cycle slip in LTE carrier phase measurements was presented and validated with experimental results. The proposed framework demonstrated a sub-meter level position estimation accuracy for a UAV navigating with LTE signals. In order to reduce the effect of the time-correlated multipath errors and the model mismatch between the true dynamics of the UE and the statistical model, the third navigation framework was proposed. This framework is based on an MSCKF and uses the IMU measurements to propagate the state of the estimator. Code phase measurements were used to estimate the location and velocity of the UE and the difference between the UE's clock bias and drift and those of the eNodeBs'. The presented simulation and experimental results showed that the MSCKF estimator can significantly reduce the RMSE compared to an EKF estimator in the presence of time-correlated multipath errors.

All the presented navigation frameworks required initial knowledge of the estimator's states, which was obtained by a GNSS navigation solution before the GNSS cutoff. In order to remove this assumption and produce navigation solution in cold-start applications, it was proposed to exploit both TOA and DOA of the received signal. For this purpose, an SDR to jointly estimate and track TOA and DOA of the received LTE signals was proposed. In the proposed SDR, a 3-D MP algorithm is first used in the acquisition stage to provide an initial estimate of the TOA and DOA. Then, three different tracking loops are used in parallel to jointly track delay, azimuth and elevation of the received signal. The discriminator functions of the tracking loops were derived and their accuracy in multipath-free and multipath-rich environments was analyzed. The CRLBs of the TOA and DOA were derived and compared to the performance of the proposed SDR. It was shown that the proposed SDR has lower computational complexity and higher precision compared to the state-of-the-art JADE algorithms. Simulation and experimental results were provided validating theoretical results.

After evaluating cellular LTE signals for opportunistic navigation and developing an SDR to extract navigation observables from LTE signals, exploiting NR signals for navigation was analyzed. The advantages and challenges of NR signals for navigation were discussed. Then, possible reference signals that can be exploited for opportunistic navigation were presented. It was shown that since NR signals have ultra-lean transmission, the only signal that is broadcast in every NR frame and can be used for opportunistic navigation is SS/PBCH block. Then, an SDR was proposed to extract code and carrier phase and Doppler frequency measurements from NR SS/PBCH block. The ranging and positioning precision of the proposed SDR were analyzed. Finally, for the first time, experimental results were provided showing pseudorange measurement derived from real NR signals.

Bibliography

[1] 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.

[2] S. Ji, W. Chen, X. Ding, Y. Chen, C. Zhao, and C. Hu, "Potential benefits of GPS/GLONASS/GALILEO integration in an urban canyon – Hong Kong," *Journal of Navigation*, vol. 63, no. 4, pp. 681–693, October 2010.

[3] S. Saab and Z. Kassas, "Map-based land vehicle navigation system with DGPS," in *Proceedings of IEEE Intelligent Vehicle Symposium*, vol. 1, June 2002, pp. 209–214.

[4] 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.

[5] L. Wang, P. Groves, and M. Ziebart, "GNSS shadow matching: improving urban positioning accuracy using a 3D city model with optimized visibility scoring scheme," *NAVIGATION, Journal of the Institute of Navigation*, vol. 60, no. 3, pp. 195–207, 2013.

[6] R. Yozevitch and B. Moshe, "A robust shadow matching algorithm for GNSS positioning," *NAVIGATION, Journal of the Institute of Navigation*, vol. 62, no. 2, pp. 95–109, Summer 2015.

[7] M. Tsakiri, A. Kealy, and M. Stewart, "Urban canyon vehicle navigation with integrated GPS/GLONASS/DR systems," *NAVIGATION, Journal of the Institute of Navigation*, vol. 46, no. 3, pp. 161–174, Fall 1999.

[8] R. Toledo-Moreo, D. Betaille, and F. Peyret, "Lane-level integrity provision for navigation and map matching with GNSS, dead reckoning, and enhanced maps," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 1, pp. 100–112, March 2010.

[9] K. Kozak and M. Alban, "Ranger: A ground-facing camera-based localization system for ground vehicles," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2016, pp. 170–178.

[10] 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.

[11] 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.

[12] 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.

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

[14] J. Morales, J. Khalife, U. S. 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.

[15] Z. Kassas and T. Humphreys, “Observability analysis of collaborative opportunistic navigation with pseudorange measurements,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 260–273, February 2014.

[16] Z. Kassas and T. Humphreys, “Motion planning for optimal information gathering in opportunistic navigation systems,” in *Proceedings of AIAA Guidance, Navigation, and Control Conference*, August 2013, pp. 4551–4565.

[17] Z. Kassas, A. Arapostathis, and T. Humphreys, “Greedy motion planning for simultaneous signal landscape mapping and receiver localization,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 2, pp. 247–258, March 2015.

[18] Z. Kassas and T. Humphreys, “Receding horizon trajectory optimization in opportunistic navigation environments,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 51, no. 2, pp. 866–877, April 2015.

[19] F. Benedetto, G. Giunta, and S. Bucci, “A unified approach for time-delay estimators in spread spectrum communications,” *IEEE Transactions on Communications*, vol. 59, no. 12, pp. 3421–3429, December 2011.

[20] 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.

[21] C. Yang and T. Nguyen, “Tracking and relative positioning with mixed signals of opportunity,” *NAVIGATION, Journal of the Institute of Navigation*, vol. 62, no. 4, pp. 291–311, December 2015.

[22] 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.

[23] J. Morales, P. Roysdon, and Z. Kassas, “Signals of opportunity aided inertial navigation,” in *Proceedings of ION GNSS Conference*, September 2016, pp. 1492–1501.

[24] 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.

[25] J. Khalife, K. Shamaei, and Z. Kassas, “Navigation with cellular CDMA signals – part I: Signal modeling and software-defined receiver design,” *IEEE Transactions on Signal Processing*, vol. 66, no. 8, pp. 2191–2203, April 2018.

[26] J. Khalife and Z. Kassas, “Navigation with cellular CDMA signals – part II: Performance analysis and experimental results,” *IEEE Transactions on Signal Processing*, vol. 66, no. 8, pp. 2204–2218, April 2018.

[27] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, “Achievable localization accuracy of the positioning reference signal of 3GPP LTE,” in *Proceedings of International Conference on Localization and GNSS*, June 2012, pp. 1–6.

[28] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, “Analysis of positioning capabilities of 3GPP LTE,” in *Proceedings of ION GNSS Conference*, September 2012, pp. 139–146.

[29] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, P. Crosta, R. Ioannides, and M. Crisci, “Software-defined radio LTE positioning receiver towards future hybrid localization systems,” in *Proceedings of International Communication Satellite Systems Conference*, October 2013, pp. 14–17.

[30] F. Knutti, M. Sabathy, M. Driusso, H. Mathis, and C. Marshall, “Positioning using LTE signals,” in *Proceedings of Navigation Conference in Europe*, April 2015, pp. 1–8.

[31] 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.

[32] Y. Shen, T. Luo, and M. Win, “Neighboring cell search for LTE systems,” *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 908–919, March 2012.

[33] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, “Joint channel and time delay estimation for LTE positioning reference signals,” in *Proceedings of Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*, December 2012, pp. 1–8.

[34] M. Driusso, F. Babich, F. Knutti, M. Sabathy, and C. Marshall, "Estimation and tracking of LTE signals time of arrival in a mobile multipath environment," in *Proceedings of International Symposium on Image and Signal Processing and Analysis*, September 2015, pp. 276–281.

[35] 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.

[36] 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

[37] J. van de Beek, M. Sandell, and P. Borjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE Transactions on Signal Processing*, vol. 45, no. 7, pp. 1800–1805, July 1997.

[38] F. Benedetto, G. Giunta, and E. Guzzon, "Initial code acquisition in lte systems," *Recent Patents on Computer Science*, vol. 6, pp. 2–13, April 2013.

[39] S. Sesia, I. Toufik, and M. Baker, *LTE, The UMTS Long Term Evolution: From Theory to Practice.* Wiley Publishing, 2009.

[40] S. Fischer, "Observed time difference of arrival (OTDOA) positioning in 3GPP LTE," Qualcomm Technologies, Inc., Tech. Rep., June 2014.

[41] M. Hofer, J. McEachen, and M. Tummala, "Vulnerability analysis of LTE location services," in *Proceedings of Hawaii International Conference on System Sciences*, January 2014, pp. 5162–5166.

[42] J. del Peral-Rosado, J. Parro-Jimenez, J. Lopez-Salcedo, G. Seco-Granados, P. Crosta, F. Zanier, and M. Crisci, "Comparative results analysis on positioning with real LTE signals and low-cost hardware platforms," in *Proceedings of Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*, December 2014, pp. 1–8.

[43] M. Ulmschneider and C. Gentner, "Multipath assisted positioning for pedestrians using LTE signals," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2016, pp. 386–392.

[44] M. Speth, S. Fechtel, G. Fock, and H. Meyr, "Optimum receiver design for wireless broad-band systems using OFDM. I," *IEEE Transactions on Communications*, vol. 47, no. 11, pp. 1668–1677, November 1999.

[45] 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.

[46] K. Shamaei, J. Khalife, and Z. Kassas, "Performance characterization of positioning in LTE systems," in *Proceedings of ION GNSS Conference*, September 2016, pp. 2262–2270.

[47] K. Shamaei, J. Khalife, S. Bhattacharya, and Z. Kassas, "Computationally efficient receiver design for mitigating multipath for positioning with LTE signals," in *Proceedings of ION GNSS Conference*, September 2017, pp. 3751–3760.

[48] 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.

[49] 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.

[50] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); multiplexing and channel coding," 3rd Generation Partnership Project (3GPP), TS 36.212, January 2010. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36212.htm

[51] Y. Wang and R. Ramesh, "To bite or not to bite-a study of tail bits versus tail-biting," in *Proceedings of Personal, Indoor and Mobile Radio Communications*, vol. 2, October 1996, pp. 317–321.

[52] R. Roy and T. Kailath, "ESPRIT-estimation of signal parameters via rotational invariance techniques," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 37, no. 7, pp. 984–995, July 1989.

[53] B. Yang, K. Letaief, R. Cheng, and Z. Cao, "Channel estimation for OFDM transmission in multipath fading channels based on parametric channel modeling," *IEEE Transactions on Communications*, vol. 49, no. 3, pp. 467–479, 2001.

[54] M. Wax and T. Kailath, "Detection of signals by information theoretic criteria," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 33, no. 2, pp. 387–392, April 1985.

[55] M. Speth, S. Fechtel, G. Fock, and H. Meyr, "Optimum receiver design for OFDM-based broadband transmission–part II: A case study," *IEEE Transactions on Communications*, vol. 49, no. 4, pp. 571–578, April 2001.

[56] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, "Joint maximum likelihood time-delay estimation for LTE positioning in multipath channels," in *Proceedings of EURASIP Journal on Advances in Signal Processing, special issue on Signal Processing Techniques for Anywhere, Anytime Positioning*, September 2014, pp. 1–13.

[57] P. Muller, J. del Peral-Rosado, R. Piche, and G. Seco-Granados, "Statistical trilateration with skew-t distributed errors in LTE networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 7114–7127, October 2016.

[58] 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.

[59] K. Shamaei, J. Morales, and Z. Kassas, "Positioning performance of LTE signals in Rician fading environments exploiting antenna motion," in *Proceedings of ION GNSS Conference*, September 2018, pp. 3423–3432.

[60] W. Ward, "Performance comparisons between FLL, PLL and a novel FLL-assisted-PLL carrier tracking loop under RF interference conditions," in *Proceedings of ION GNSS Conference*, September 1998, pp. 783–795.

[61] E. Kaplan and C. Hegarty, *Understanding* GPS*: Principles and Applications*, 2nd ed. Artech House, 2005.

[62] X. Li and K. Pahlavan, "Super-resolution TOA estimation with diversity for indoor geolocation," *IEEE Transactions on Wireless Communications*, vol. 3, no. 1, pp. 224–234, 2004.

[63] N. Nechval, *Adaptive CFAR Tests for Detection of a Signal in Noise and Deflection Criterion*, T. Wysocki, H. Razavi, and B. Honary, Eds. Boston, MA: Springer US, 1997.

[64] B. Mahafza, *Radar Systems Analysis and Design Using MATLAB*, 1st ed. Boca Raton, FL, USA: CRC Press, 2000.

[65] A. van Dierendonck, P. Fenton, and T. Ford, "Theory and performance of narrow correlator spacing in a GPS receiver," *NAVIGATION, Journal of the Institute of Navigation*, vol. 39, no. 3, pp. 265–283, September 1992.

[66] K. Shamaei, J. Khalife, and Z. Kassas, "Ranging precision analysis of LTE signals," in *Proceedings of European Signal Processing Conference*, August 2017, pp. 2788–2792.

[67] 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.

[68] M. Braasch and A. van Dierendonck, "GPS receiver architectures and measurements," *Proceedings of the IEEE*, vol. 87, no. 1, pp. 48–64, January 1999.

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

[70] K. Wesson, K. Pesyna, J. Bhatti, and T. Humphreys, "Opportunistic frequency stability transfer for extending the coherence time of GNSS receiver clocks," in *Proceedings of ION GNSS Conference*, September 2010, pp. 2959–2968.

[71] K. Shamaei, J. Khalife, and Z. Kassas, "Comparative results for positioning with secondary synchronization signal versus cell specific reference signal in LTE systems," in *Proceedings of ION International Technical Meeting Conference*, January 2017, pp. 1256–1268.

[72] 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.

[73] 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.

[74] Y. Bar-Shalom, X. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation.* New York, NY: John Wiley & Sons, 2002.

[75] Z. Kassas, V. Ghadiok, and T. Humphreys, "Adaptive estimation of signals of opportunity," in *Proceedings of ION GNSS Conference*, September 2014, pp. 1679–1689.

[76] 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.

[77] T. Humphreys, J. Bhatti, T. Pany, B. Ledvina, and B. O'Hanlon, "Exploiting multicore technology in software-defined GNSS receivers," in *Proceedings of ION GNSS Conference*, September 2009, pp. 326–338.

[78] D. Bladsjo, M. Hogan, and S. Ruffini, "Synchronization aspects in LTE small cells," *IEEE Communications Magazine*, vol. 51, no. 9, pp. 70–77, September 2013.

[79] O. Mancini, "Tutorial precision frequency generation utilizing OCXO and rubidium atomic standards with applications for commercial, space, military, and challenging environments," IEEE Long Island, Tech. Rep., March.

[80] P. Teunissen, *GPS Carrier Phase Ambiguity Fixing Concepts.* Springer Berlin Heidelberg, 1998, pp. 319–388.

[81] G. Xu, *GPS Theory, Algorithms and Applications*, 2nd ed. Springer-Verlag Berlin Heidelberg, 2007.

[82] P. J. G. Teunissen, "The least-squares ambiguity decorrelation adjustment: a method for fast gps integer ambiguity estimation," *Journal of Geodesy*, vol. 70, no. 1, pp. 65–82, November 1995.

[83] R. van Nee, "The multipath estimating delay lock loop," in *Proceedings of Spread Spectrum Techniques and Applications Symposium*, November 1992, pp. 39–42.

[84] M. Psiaki, T. Ertan, B. O'Hanlon, and S. Powell, "GNSS multipath mitigation using antenna motion," *NAVIGATION, Journal of the Institute of Navigation*, vol. 62, no. 1, pp. 1–22, Spring 2015.

[85] P. Axelrad, C. Comp, and P. Macdoran, "SNR-based multipath error correction for GPS differential phase," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 32, no. 2, pp. 650–660, April 1996.

[86] Y. D. Jong and M. Herben, "High-resolution angle-of-arrival measurement of the mobile radio channel," *IEEE Transactions on Antennas and Propagation*, vol. 47, no. 11, pp. 1677–1687, November 1999.

[87] T. Pany, N. Falk, B. Riedl, C. Stober, J. Winkel, and H. Ranner, "GNSS synthetic aperture processing with artificial antenna motion," in *Proceedings of ION GNSS Conference*, September 2013, pp. 3163–3171.

[88] M. Yaqoob, F. Tufvesson, A. Mannesson, and B. Bernhardsson, "Direction of arrival estimation with arbitrary virtual antenna arrays using low cost inertial measurement units," in *Proceedings of International Conference on Communications Workshops*, June 2013, pp. 79–83.

[89] A. Broumandan, J. Nielsen, and G. Lachapelle, "Narrowband signal detection in correlated Rayleigh fading with a moving antenna," in *Proceedings of Antenna Technology and Applied Electromagnetics and the Canadian Radio Science Meeting*, February 2009, pp. 1–4.

[90] K. Pesyna, T. Humphreys, R. Heath, T. Novlan, and J. Zhang, "Exploiting antenna motion for faster initialization of centimeter-accurate GNSS positioning with low-cost antennas," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 4, pp. 1597–1613, August 2017.

[91] A. Mourikis and S. Roumeliotis, "A multi-state constraint Kalman filter for vision-aided inertial navigation," in *Proceedings IEEE International Conference on Robotics and Automation*, April 2007, pp. 3565–3572.

[92] J. Farrell and M. Barth, *The Global Positioning System and Inertial Navigation.* New York: McGraw-Hill, 1998.

[93] P. Groves, *Principles of* GNSS*, Inertial, and Multisensor Integrated Navigation Systems*, 2nd ed. Artech House, 2013.

[94] S. Kumar, P. Gupta, G. Singh, and D. Chauhan, "Performance analysis of Rayleigh and Rician fading channel models using MATLAB simulation," *International Journal of Intelligent Systems and Applications*, vol. 5, no. 9, pp. 94–102, August 2013.

[95] 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

[96] J. Morales and Z. Kassas, "Stochastic observability and uncertainty characterization in simultaneous receiver and transmitter localization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 2, pp. 1021–1031, April 2019.

[97] M. Vanderveen, C. Papadias, and A. Paulraj, “Joint angle and delay estimation (JADE) for multipath signals arriving at an antenna array,” *IEEE Communications Letters*, vol. 1, no. 1, pp. 12–14, January 1997.

[98] M. Vanderveen, A. V. der Veen, and Paulraj, “Estimation of multipath parameters in wireless communications,” *IEEE Transactions on Signal Processing*, vol. 46, no. 3, pp. 682–690, March 1998.

[99] R. Schmidt, “Multiple emitter location and signal parameter estimation,” *IEEE Transactions on Antennas and Propagation*, vol. 34, no. 3, pp. 276–280, March 1986.

[100] T. Shan, M. Wax, and T. Kailath, “On spatial smoothing for direction-of-arrival estimation of coherent signals,” *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 33, no. 4, pp. 806–811, August 1985.

[101] Y. Hua and T. Sarkar, “Matrix pencil method for estimating parameters of exponentially damped/undamped sinusoids in noise,” *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 38, no. 5, pp. 814–824, May 1990.

[102] Y. Hua, “Estimating two-dimensional frequencies by matrix enhancement and matrix pencil,” *IEEE Transactions on Signal Processing*, vol. 40, no. 9, pp. 2267–2280, September 1992.

[103] N. Yilmazer, R. Fernandez-Recio, and T. Sarkar, “Matrix pencil method for simultaneously estimating azimuth and elevation angles of arrival along with the frequency of the incoming signals,” *Digital Signal Processing*, vol. 16, no. 6, pp. 796–816, November 2006.

[104] A. Gaber and A. Omar, “A study of wireless indoor positioning based on joint TDOA and DOA estimation using 2-D matrix pencil algorithms and IEEE 802.11ac,” *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2440–2454, May 2015.

[105] A. Gaber and A. Omar, “Utilization of multiple-antenna multicarrier systems and NLOS mitigation for accurate wireless indoor positioning,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6570–6584, October 2016.

[106] W. Hou and H. Kwon, “Interference suppression receiver with adaptive antenna array for code division multiple access communications systems,” in *Proceedings of IEEE Vehicular Technology Conference*, vol. 3, September 2000, pp. 1249–1254.

[107] S. Min, D. Seo, K. Lee, H. Kwon, and Y. Lee, “Direction-of-arrival tracking scheme for DS/CDMA systems: direction lock loop,” *IEEE Transactions on Wireless Communications*, vol. 3, no. 1, pp. 191–202, January 2004.

[108] R. Gieron and P. Siatchoua, “Application of 2D-direction locked loop tracking algorithm to mobile satellite communications,” in *Proceedings of IEEE Workshop on Sensor Array and Multichannel Processing*, July 2006, pp. 546–550.

[109] K. Shamaei, J. Khalife, and Z. Kassas, “A joint TOA and DOA approach for positioning with LTE signals,” in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2018, pp. 81–91.

[110] 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.

[111] B. Clerckx and C. Oestges, *MIMO Wireless Networks: Channels, Techniques and Standards for Multi-Antenna, Multi-User and Multi-Cell Systems*, 2nd ed. Orlando, FL, USA: Academic Press, Inc., 2013.

[112] G. Stewart, “Stochastic perturbation theory,” *SIAM Review*, vol. 32, no. 4, pp. 579–610, December 1990.

[113] F. Li, H. Liu, and R. Vaccaro, “Performance analysis for DOA estimation algorithms: unification, simplification, and observations,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 29, no. 4, pp. 1170–1184, October 1993.

[114] G. Golub, V. Loan, and F. Charles, *Matrix Computations*, 3rd ed. Baltimore, MD, USA: Johns Hopkins University Press, 1996.

[115] Synchronization and MIMO capability with USRP devices. [Online]. Available: https://kb.ettus.com/SynchronizationandMIMOCapabilitywithUSRPDevices

[116] A. Madrigal, “Waymo’s robots drove more miles than everyone else combined,” https://www.theatlantic.com/technology/archive/2019/02/the-latest-self-driving-car-statistics-from-california/582763/, February 2019.

[117] A. Hawkins, “California’s self-driving car reports are imperfect, but they’re better than nothing,” https://www.theverge.com/2019/2/13/18223356/california-dmv-self-driving-car-disengagement-report-2018, February 2019.

[118] G. Americas, “Cellular V2X communications towards 5G,” 5G Americas, Tech. Rep., March 2018. [Online]. Available: https://www.5gamericas.org/cellular-v2x-communications-towards-5g/

[119] A. Kakkavas, M. Castaneda Garcia, R. Stirling-Gallacher, and J. Nossek, “Multi-array 5G V2V relative positioning: Performance bounds,” in *IEEE Global Communications Conference*, December 2018, pp. 206–212.

[120] 3GPP, “Study on NR positioning support,” 3rd Generation Partnership Project (3GPP), TR 38.855, March 2019. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.855/

[121] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, “5G mmwave positioning for vehicular networks,” *IEEE Wireless Communications*, vol. 24, no. 6, pp. 80–86, December 2017.

[122] Z. Abu-Shaban, X. Zhou, T. Abhayapala, G. Seco-Granados, and H. Wymeersch, “Error bounds for uplink and downlink 3D localization in 5G millimeter wave systems,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 4939–4954, August 2018.

[123] Z. Abu-Shaban, X. Zhou, T. Abhayapala, G. Seco-Granados, and H. Wymeersch, “Performance of location and orientation estimation in 5G mmwave systems: Uplink vs downlink,” in *Proceedings of IEEE Wireless Communications and Networking Conference*, April 2018, pp. 1–6.

[124] J. Peral-Rosado, J. Lopez-Salcedo, S. Kim, and G. Seco-Granados, “Feasibility study of 5G-based localization for assisted driving,” in *Proceedings of International Conference on Localization and GNSS*, June 2016, pp. 1–6.

[125] J. Lee, G. Gil, and Y. H. Lee, “Exploiting spatial sparsity for estimating channels of hybrid MIMO systems in millimeter wave communications,” in *Proceedings of IEEE GLOBECOM*, December 2014, pp. 3326–3331.

[126] A. Shahmansoori, G. Garcia, G. Destino, G. Seco-Granados, and H. Wymeersch, “Position and orientation estimation through millimeter-wave MIMO in 5G systems,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, March 2018.

[127] D. Yacong, “Channel estimation for massive MIMO systems based on sparse representation and sparse signal recovery,” Ph.D. dissertation, University of California, San Diego, 2018.

[128] E. Rastorgueva-Foi, M. Costa, M. Koivisto, K. Leppanen, and M. Valkama, “User positioning in mmw 5G networks using beam-RSRP measurements and Kalman filtering,” in *Proceedings of International Conference on Information Fusion*, July 2018, pp. 1–7.

[129] R. Mendrzik, H. Wymeersch, and G. Bauch, “Joint localization and mapping through millimeter wave MIMO in 5G systems,” in *Proceedings of IEEE Global Communications Conference*, December 2018, pp. 1–6.

[130] Z. Abu-Shaban, H. Wymeersch, T. Abhayapala, and G. Seco-Granados, “Distributed two-way localization bounds for 5G mmwave systems,” in *Proceedings of IEEE Globecom Workshops*, December 2018, pp. 1–6.

[131] J. del Peral-Rosado, J. Lopez-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, “Evaluation of the LTE positioning capabilities under typical multipath channels,” in *Proceedings of Advanced Satellite Multimedia Systems Conference and Signal Processing for Space Communications Workshop*, September 2012, pp. 139–146.

[132] 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

[133] A. Zaidi, "Three design principles of 5G new radio," https://www.ericsson.com/en/blog/2017/8/three-design-principles-of-5g-new-radio, August 2017.

[134] R. Heath, N. Gonzalez-Prelcic, S. Rangan, W. Roh, and A. Sayeed, "An overview of signal processing techniques for millimeter wave MIMO systems," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 3, pp. 436–453, April 2016.

[135] 3GPP, "Physical layer procedures for control," 3rd Generation Partnership Project (3GPP), TS 38.213, July 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/138200_138299/138213/15.02.00_60/ts_138213v150200p.pdf

[136] 3GPP, "5g; nr; radio resource control (rrc); protocol specification," 3rd Generation Partnership Project (3GPP), TS 38.331, October 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/138300_138399/138331/15.03.00_60/ts_138331v150300p.pdf

[137] 3GPP, "Multiplexing and channel coding," 3rd Generation Partnership Project (3GPP), TS 38.212, October 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/138200_138299/138212/15.03.00_60/ts_138212v150300p.pdf

[138] I. Hemadeh, K. Satyanarayana, M. El-Hajjar, and L. Hanzo, "Millimeter-wave communications: Physical channel models, design considerations, antenna constructions, and link-budget," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 870–913, Second Quarter 2018.

[139] 3GPP, "Study on channel model for frequency spectrum above 6 ghz," 3rd Generation Partnership Project (3GPP), TS 38.900, June 2017. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/138900_138999/138900/14.02.00_60/tr_138900v140200p.pdf

[140] J. Schloemann, H. Dhillon, and R. Buehrer, "Toward a tractable analysis of localization fundamentals in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1768–1782, March 2016.

[141] S. Aditya, H. Dhillon, A. Molisch, R. Buehrer, and H. Behairy, "Characterizing the impact of SNR heterogeneity on time-of-arrival-based localization outage probability," *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 637–649, January 2019.

Appendix A

Appendix for Chapter 6

A.1 Derivation of Equation (6.7)

In order to prove (6.7), first (6.6) is rewritten as

$$\begin{aligned} {H'}_{m,n,q} =& \sqrt{C}\beta_0 e^{j\frac{m\omega_c d}{c}\left(\sin\theta_0\cos\phi_0-\sin\hat{\theta}_0\cos\hat{\phi}_0\right)} e^{j\frac{n\omega_c d}{c}\left(\sin\theta_0\sin\phi_0-\sin\hat{\theta}_0\sin\hat{\phi}_0\right)} \\ & e^{-j2\pi q f_s N_{CRS}(\tau_0-\hat{\tau}_0)} + I_{m,n}(q) + V'_{m,n}(k), \end{aligned} \tag{A.1}$$

It can be shown that for small values of e_θ and e_ϕ the following equalities hold.

$$\begin{aligned} \sin\left(\hat{\theta}_0\right) &= \sin\left(\theta_0 + e_\theta\right) \\ &\approx \sin\left(\theta_0\right) + \cos\left(\theta_0\right) e_\theta \end{aligned} \tag{A.2}$$

$$\begin{aligned} \sin\left(\hat{\phi}_0\right) &= \sin\left(\phi_0 + e_\phi\right) \\ &\approx \sin\left(\phi_0\right) + \cos\left(\phi_0\right) e_\phi \end{aligned} \tag{A.3}$$

$$\cos\left(\hat{\phi}_0\right) = \cos\left(\phi_0 + e_\phi\right)$$
$$\approx \cos\left(\phi_0\right) - \sin\left(\phi_0\right) e_\phi \tag{A.4}$$

Using (A.2), (A.3), and (A.4), it can be shown that

$$\sin\hat{\theta}_0 \cos\hat{\phi}_0 = \sin\theta_0 \cos\phi_0 - \sin\theta_0 \sin\phi_0 e_\phi$$
$$+ \cos\theta_0 \cos\phi_0 e_\theta - \cos\theta_0 \sin\phi_0 e_\theta e_\phi \tag{A.5}$$

$$\sin\hat{\theta}_0 \sin\hat{\phi}_0 = \sin\theta_0 \sin\phi_0 + \sin\theta_0 \cos\phi_0 e_\phi$$
$$+ \cos\theta_0 \sin\phi_0 e_\theta + \cos\theta_0 \cos\phi_0 e_\theta e_\phi \tag{A.6}$$

where for small values of e_θ and e_ϕ, the last terms in (A.5) and (A.6) can be neglected. After replacing (A.5) and (A.6) into (A.1), it can be shown that (6.7) holds.

A.2 Derivation of CRLB (6.27)

The diagonal elements of the CRLB($\boldsymbol{\eta}$) in (6.27) represent the CRLB of $\boldsymbol{\theta}$, $\boldsymbol{\phi}$, and $\boldsymbol{\tau}$ error variances. For $L = 1$, $\mathbf{D} = [\boldsymbol{d}_{\theta_0}, \boldsymbol{d}_{\phi_0}, \boldsymbol{d}_{\tau_0}]$ and $\mathbf{S} = \boldsymbol{z}_0 \otimes (\boldsymbol{y}_0 \otimes \boldsymbol{x}_0)$ is a vector, which is replaced by $\boldsymbol{s}$ to follow the notations. Therefore, the DOA and TOA CRLB error variances can be simplified to

$$\sigma^2_{\theta_0,CRLB} = \frac{\sigma^2}{2} \left\{ \Re\left[C \left(\boldsymbol{d}^{\mathsf{H}}_{\theta_0} \boldsymbol{d}_{\theta_0} - \boldsymbol{d}^{\mathsf{H}}_{\theta_0} \boldsymbol{s} (\boldsymbol{s}^{\mathsf{H}} \boldsymbol{s})^{-1} \boldsymbol{s}^{\mathsf{H}} \boldsymbol{d}_{\theta_0} \right) \right] \right\}^{-1},$$

$$\sigma^2_{\phi_0,CRLB} = \frac{\sigma^2}{2}\left\{\Re\left[C\left(\boldsymbol{d}^{\mathsf{H}}_{\phi_0}\boldsymbol{d}_{\phi_0} - \boldsymbol{d}^{\mathsf{H}}_{\phi_0}\boldsymbol{s}(\boldsymbol{s}^{\mathsf{H}}\boldsymbol{s})^{-1}\boldsymbol{s}^{\mathsf{H}}\boldsymbol{d}_{\phi_0}\right)\right]\right\}^{-1},$$

$$\sigma^2_{\tau_0,CRLB} = \frac{\sigma^2}{2}\left\{\Re\left[C\left(\boldsymbol{d}^{\mathsf{H}}_{\tau_0}\boldsymbol{d}_{\tau_0} - \boldsymbol{d}^{\mathsf{H}}_{\tau_0}\boldsymbol{s}(\boldsymbol{s}^{\mathsf{H}}\boldsymbol{s})^{-1}\boldsymbol{s}^{\mathsf{H}}\boldsymbol{d}_{\tau_0}\right)\right]\right\}^{-1},$$

For any matrices $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, and $\mathbf{A}_4$ of proper size, the general relations $(\mathbf{A}_1 \otimes \mathbf{A}_2)(\mathbf{A}_3 \otimes \mathbf{A_3}) = (\mathbf{A}_1\mathbf{A}_3)\otimes(\mathbf{A}_2\mathbf{A}_4)$ and $(\mathbf{A}_1 \otimes \mathbf{A}_2)^{\mathsf{H}} = \left(\mathbf{A}_1^{\mathsf{H}} \otimes \mathbf{A}_2^{\mathsf{H}}\right)$ hold. Using these relations, it can be shown that the following equalities hold, which can be used to obtain (6.28), (6.29), and (6.30).

$$\begin{aligned}
\boldsymbol{s}^{\mathsf{H}}\boldsymbol{s} &= MNN_s,\\
\boldsymbol{d}^{\mathsf{H}}_{\theta_0}\boldsymbol{s} &= -j\frac{\omega_c d N_s MN \cos\theta_0}{2c}\left[(N-1)\sin\phi_0 + (M-1)\cos\phi_0\right],\\
\boldsymbol{d}^{\mathsf{H}}_{\phi_0}\boldsymbol{s} &= -j\frac{\omega_c d N_s MN \sin\theta_0}{2c}\left[(N-1)\cos\phi_0 - (M-1)\sin\phi_0\right],\\
\boldsymbol{d}^{\mathsf{H}}_{\tau_0}\boldsymbol{s} &= j\pi f_s N_{CRS} MNN_s(N_s-1),
\end{aligned}$$

$$\begin{aligned}
\boldsymbol{d}^{\mathsf{H}}_{\theta_0}\boldsymbol{d}_{\theta_0} &= \frac{MNN_s}{2}\left(\frac{\omega_c d\cos\theta_0}{c}\right)^2\left[\frac{(N-1)(2N-1)}{3}\sin^2\phi_0\right.\\
&\quad + \frac{(M-1)(2M-1)}{3}\cos^2\phi_0\\
&\quad \left. + (N-1)(M-1)\sin\phi_0\cos\phi_0\right],\\
\boldsymbol{d}^{\mathsf{H}}_{\phi_0}\boldsymbol{d}_{\phi_0} &= \frac{MNN_s}{2}\left(\frac{\omega_c d\sin\theta_0}{c}\right)^2\left[\frac{(N-1)(2N-1)}{3}\cos^2\phi_0\right.\\
&\quad + \frac{(M-1)(2M-1)}{3}\sin^2\phi_0\\
&\quad \left. - (N-1)(M-1)\sin\phi_0\cos\phi_0\right],\\
\boldsymbol{d}^{\mathsf{H}}_{\tau_0}\boldsymbol{d}_{\tau_0} &= \frac{MNN_s(N_s-1)(2N_s-1)}{6}(2\pi f_s N_{CRS})^2,
\end{aligned}$$