Cognitive Sensing and Navigation with Unknown Terrestrial and LEO Satellite Signals

Dissertation

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of The Ohio State University

By

Mohammad Neinavaie, MS

Graduate Program in Electrical and Computer Engineering

The Ohio State University

2023

Dissertation Committee:

Professor Zaher M. Kassas, Advisor

Professor Lee Potter

Professor Philip Schniter

Professor Parinaz Naghizadeh

Abstract

Due to significant advancements in cellular technologies and dense deployment of cellular infrastructure, fifth-generation (5G) cellular and low Earth orbit (LEO)-based communication networks will be adopted by intelligent transportation systems to enable reliable and safe autonomous operations. Several features in 5G and LEO-based networks depend on the ability to localize the user equipment (UE) to a high degree of accuracy. Estimation of time-of-arrival (TOA), direction-of-arrival (DOA), and/or frequency-of-arrival (FOA) of multiple users/targets is an inseparable block of some 5G and LEO-based technologies, such as joint sensing and communication. While the third generation (3G) cellular uses code division multiple access (CDMA) technique, the fourth generation (4G) long-term evolution (LTE) and 5G new radio (NR) adopt orthogonal frequency division multiplexing (OFDM) technique. In addition, new constellations of broadband LEO space vehicles (SVs) will transmit OFDM-type signals. In both CDMA and OFDM-based systems, a part of the transmitted power is dedicated to periodic synchronization signals, referred to as reference signals (RSs), which are transmitted for synchronization purposes. RSs are designed (or selected) based on their distinctive bandwidth and correlation properties and the physical channel type. While the RSs allocated to a single LTE channel have a *predetermined* bandwidth of up to 20 MHz, the allocated bandwidth for the RSs in a single 5G channel is *dynamic*, i.e., it adaptively changes based on the transmission mode, and can go up to

100 MHz and 400 MHz for frequency ranges 1 and 2 (FR1 and FR2), respectively. On the other hand, Starlink downlink signals occupy 250 MHz bandwidth of the Ku-band to provide high-rate broadband connectivity, but the allocated bandwidth (and other signal characteristics) of the RSs are *unknown*. Navigation receivers typically rely on known RSs transmitted by the sources to draw TOA, DOA, and FOA measurements. Conventional opportunistic navigation receivers (i.e., those only utilizing the downlink signals) will either fail to operate or will be unable to exploit the entire available bandwidth in situations where RSs are unknown and/or dynamic, which is the case in 5G NR and private networks, such as broadband LEO.

This dissertation addresses the following challenges of navigation with signals of unknown and dynamic nature. First, unlike public networks where the broadcast RSs are known at the UE and are universal across network operators, in private networks, the signal specifications of some RSs may not be available to the public or are subject to change. Second, in cellular LTE networks, several RSs (e.g., cell-specific reference signal (CRS)) are broadcast at regular and known time intervals, regardless of the number of UEs in the environments. *Ultra-lean* design refers to minimizing these *always-on* transmissions. 5G NR and modern communication systems transmit some of the RSs only when necessary or *on-demand*.

In this dissertation, a receiver architecture is proposed to cognitively extract navigation observables from 3G, 4G, 5G, and LEO-based signals. Unlike conventional opportunistic receivers which require knowledge of the signal structure, particularly the RSs, the proposed receiver only relies on the periodicity of the RSs and requires knowledge of only the carrier frequency of the signal. To exploit the full available bandwidth and improve

ranging accuracy, the proposed receiver is designed to estimate all the RSs contained in the transmitted signals corresponding to multiple sources. Navigation observables (pseudorange and carrier phase) are subsequently derived from the estimated RSs. The proposed receiver operates in two stages: (i) acquisition and (ii) tracking. The acquisition stage of the proposed receiver is modeled as a sequential detection problem where the number of gNBs and their corresponding RSs and Doppler frequencies are unknown. The generalized likelihood ratio (GLR) test for sequentially detecting active sources is derived and used to estimate the number of unknown sources and their RSs. In order for the receiver to refine and maintain the Doppler and RS estimates provided by the acquisition stage, tracking loops are designed. A sufficient condition on the Doppler estimation error to ensure that the proposed GLR asymptotically achieves a constant false alarm rate (CFAR) is derived. The output of the tracking loops, namely carrier phase and code phase, are then used to estimate the receiver's position.

Extensive experimental results are presented demonstrating the capabilities of the proposed receiver with real 3G, 4G, 5G, and LEO SV signals on ground and aerial platforms.

To my parents

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. Lee Potter, Prof. Philip Schniter, and Prof. Parinaz Naghizadeh for taking time to serve in the committee and for all their helpful advice throughout my Candidacy exam and Ph.D. Defense. I would like to thank the Office of Naval Research (ONR) and US Department of Transportation (USDOT) 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. Thomas Pany, and Prof. Tryphon Georgiou 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: Joe, Mu, and Sharbel 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

Pouria Haghi for not only being my friend 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 Maral for supporting me and being there for me though out this journey. I would like to thank my family: Mom, Dad, and Maryam 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.

Vita

Jun 2023 ..... Ph.D.,
Electrical and Computer Engineering,
The Ohio State University, USA.

August 2009 ..... M.Sc.,
Electrical Engineering,
Shiraz University, Iran.

August 2007 ..... B.Sc.,
Electrical Engineering,
Boushehr Univeristy, Iran.

Publications

Journal Publications:

1. M. Neinavaie and Z. Kassas “Unveiling Starlink LEO Satellite OFDM-Like Signal Structure Enabling Precise Positioning", *in IEEE Transactions on Aerospace and Electronic Systems,* Accepted. 2023.
2. M. Neinavaie, J. Khalife, and Z. Kassas “Cognitive Detection of Unknown Beacons of Terrestrial Signals of Opportunity for Localization", *in IEEE Transactions of Wireless Communications,* Accepted. 2022.
3. M. Neinavaie, J. Khalife, and Z. Kassas “Cognitive Opportunistic Navigation in Private Networks with 5G Signals and Beyond", *in IEEE Journal of Selected Topics in Signal Processing,* vol. 16, no. 1, pp. 129-143, Jan. 2022.

4. M. Neinavaie, J. Khalife, and Z. Kassas “Acquisition, Doppler Tracking, and Positioning with Starlink LEO Satellites: First Results", *in IEEE Transactions on Aerospace and Electronic Systems,* vol. 58, no. 3, pp. 2606-2610, June 2022.

5. J. Khalife, M. Neinavaie, and Z. Kassas “The First Carrier Phase Tracking and Positioning Results with Starlink LEO Satellites", *in IEEE Transactions on Aerospace and Electronic Systems,* vol. 58, no. 2, pp. 1487-1491, April 2022.

Conference Papers and Workshops

1. M. Neinavaie, J. Khalife, and Z. Kassas, "Exploiting Starlink Signals for Navigation: First Results*:* ION Global Navigation Satellite Systems Conference, Sep. 20-24, 2021, St. Louis, MO, pp. 2266-2773

2. J. Khalife, M. Neinavaie, and Z. Kassas, "Universal Receiver Architecture for Blind Navigation with Partially Known Terrestrial and Extraterrestrial Signals of Opportunity*:* ION Global Navigation Satellite Systems Conference, Sep. 20-24, 2021, St. Louis, MO, pp. 2201-2211

3. M. Neinavaie, J. Khalife, and Z. Kassas, Blind Opportunistic Navigation with LEO Satellites ION GNSS 2020

4. M. Neinavaie, J. Khalife, and Z. Kassas,“Blind Doppler Tracking from OFDM Signals Transmitted by Broadband LEO Satellites"*I*EEE Vehicular Technology Conference, Apr. 25-28, 2021, Helsinki, Finland, pp. 1-5

5. M. Neinavaie, J. Khalife, and Z. Kassas,“Blind Doppler Tracking and Beacon Detection for Opportunistic Navigation with LEO Satellite Signals"*I*EEE Aerospace Conference, Mar. 6-13, 2021, Big Sky, MT, pp. 1-8

6. M. Neinavaie, J. Khalife, and Z. Kassas, "Blind Opportunistic Navigation: Cognitive Deciphering of Partially Known Signals of Opportunity*:* ION Global Navigation Satellite Systems Conference, Sep. 21-25, 2020, St. Louis, MO, pp. 2748-2757

7. J. Khalife, M. Neinavaie, and Z. Kassas. "Navigation With Differential Carrier Phase Measurements From Megaconstellation LEO Satellites." In 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 1393-1404. IEEE, 2020.

8. J. Khalife, M. Neinavaie, and Z. Kassas, "Blind Doppler Estimation from LEO Satellite Signals: A Case Study with Real 5G Signals." ION Global Navigation Satellite Systems Conference, Sep. 21-25, 2020, St. Louis, MO, pp. 3046-3054

US Patent

1. Z. Kassas and M. Neinavaie, M. (2023). Cognitive opportunistic navigation with Starlink LEO satellites: on-demand and always-on OFDM reference signals. U.S. Patent Application No. 63/457,372

2. Z. Kassas and M. Neinavaie (2022). Systems and methods for positioning and navigation with low Earth orbit satellite signals. U.S. Patent Application No. 63/393,501.

3. Z. Kassas, J. Khalife, and M. Neinavaie (2021). Systems and methods for acquisition and tracking of unknown LEO satellite signals. U.S. Patent Application No. 63/210,595.

4. Z. Kassas, M. Neinavaie, and J. Khalife (2020). Systems and methods for blind opportunistic navigation, cognitive deciphering of partially known signals of opportunity, and blind Doppler estimation from LEO satellite signals. U.S. Patent Application No. 63/087,591.

5. Z. Kassas, J. Khalife, and M. Neinavaie (2020). Navigation with differential carrier phase measurement from low Earth orbit satellites. U.S. Patent Application No. 63/047,796.

Fields of Study

Major Field: Computer Science and Engineering

Studies in:

Cognitive Sensing and Navigation with Terrestrial and Low Earth orbit (LEO) Satellite Signals	Prof. Kassas

Table of Contents

Page

List of Tables

Table **Page**

List of Figures

Figure **Page**

Chapter 1: Introduction

Due to significant advancements in cellular and low earth orbit (LEO) satellite technologies and dense deployment of cellular and LEO infrastructure, cellular networks will be adopted by intelligent transportation systems to enable reliable and safe autonomous operations [179, 224, 226]. Several features in cellular and LEO satellite networks depend on the ability to localize the user equipment (UE) to a high degree of accuracy [232]. Estimation of time-of-arrival (TOA), direction-of-arrival (DOA), and/or frequency-of-arrival (FOA) of multiple users/targets is an inseparable block of modern cellular and LEO satellite-based technologies, such as joint sensing and communication [169].

Cellular and LEO-based communication systems employ a synchronization *beacon* for receiver timing and/or carrier recovery. The beacon signals for the currently active networks, either *public*, e.g., the third generation (3G), fourth generation (4G), and fifth generation (5G) of cellular networks, or *private*, e.g., SpaceX and Oneweb, networks can be categorized into two classes:

- Beacons with integer constraint (IC): The samples of the beacon with IC are drawn from a finite alphabet set, e.g., M phase shif keying (PSK) modulation. One example of a beacon with IC is pseudorandom noise (PRN) sequence. This type of beacon

is currently used in code-division multiple access (CDMA)-based networks such as 3G network and Globalstar LEO satellite signals [181]. Orbcomm and Iridium LEO satellites also use beacons with IC [145, 199].

- Beacons with no integer constraint (NIC): The samples of beacons with NIC can be any arbitrary number in the time domain. For instance, the primary synchronization signal (PSS) and secondary synchronization signal (SSS) in orthogonal frequency-division multiplexing (OFDM)-based systems such as 4G long-term evolution (LTE) and 5G new radio (NR) [37, 54, 198]. While these signals are originally drawn from a finite alphabet, at the transmitter, they are input to the inverse discrete Fourier transform (IDFT). Therefore, in the time domain, the equivalent beacon's elements are arbitrary complex numbers. Most of the modern communication systems including 5G NR and Starlink LEO satellite signals are currently using this type of beacons [38, 198].

In the navigation literature, *navigation observables* are ranges or angles which are deduced from parameters such as TOA, DOA, or phase differences based on a comparison between received signals and receiver-generated beacons. Generating a replica of the beacon signal at the receiver side is not a straightforward task in the following scenarios:

1)Private Networks: For public networks, one can refer to the publicly available protocols to design a receiver capable of extracting navigation observables from the received signals by acquiring and tracking the timing and phase of these synchronization beacons. However, these receivers would not work when the beacon signals are unknown, such as in communication systems with closed protocols. This applies particularly to LEO broadband satellites [150], as private companies such as OneWeb, SpaceX, Boeing, and others are planning to launch thousands of them, yet very little is known about their transmitted signal

structure [97, 161]. A natural question then arises: Can one still exploit the unknown signals transmitted by cellular emitters or LEO satellites for navigation?

2)Ultra-lean Transmission: In the previous generations of cellular networks, several beacon signals, such as the cell-specific reference signal (CRS), are broadcast at regular and known time intervals, regardless of the number of UEs in the environments. *Ultra-lean* design refers to minimizing these *always-on* transmissions. Modern communication systems such as 5G NR, transmit some of the beacon signals only when necessary or *on-demand* [158]. Therefore, a navigation receiver should be able to detect and exploit the on-demand beacons cognitively to draw the navigation observables more effectively.

In this dissertation *Cognitive sensing and navigation (CSN)* is defined as a system which is capable of learning the beacon signals blindly* and exploit them for sensing and navigation purposes. Endowed with CSN, software receivers may sense and localize unknown and/or on-demand ambient signals and exploit them for navigation. Building blocks of a CSN framework are introduced by the authors of the dissertation in [104, 144, 145, 149].

The signal specifications of private networks are either unknown or partially known. Moreover, the beacon signal specifications of private networks follow some standards which can be modified frequently. Deciphering and tracking these signals cognitively is *a must* to exploit the beacon signals of these networks. The main objective of this dissertation is to develop a CSN framework. The main tasks of the CSN framework are listed as follows:

*For some private networks, limited information about the signal structure might be publicly available. For instance, the carrier frequency of the transmitted signals, the bandwidth, and the type and the length of the beacon sequences might be publicly available. Hence, a cognitive navigation framework may use this *partial information* to exploit the unknown parameters. However, these known parameters may change due to design updates in private companies. Therefore, in the following dissertation, *a pure blind scenario* is considered.

- **Blind signal acquisition:** The signal acquisition includes (i) signal activity detection and spectrum sensing, (ii) blind beacon estimation (iii) initial Doppler and Doppler rate estimation, and (iv) blind source enumeration.

- **Blind signal tracking and refinement:** The initial estimates of the Doppler frequencies corresponding to each source are fed to the tracking stage along with the estimated beacons. By employing a phase-locked loop (PLL) and a delay-locked loop (DLL) the delay and the Doppler are tracked over time. The estimated beacon is also refined in the blind signal tracking and refinement stage.

- **Interference and multipath classification:** A blindly detected source in the acquisition can be either: (i) a valid source (a cellular tower or a LEO satellite downlink signal), (ii) a false alarm due to interfering signals and/or non-line of sight or multipath components. Valid source and false alarm signal classification is a task of the CSN framework.

- **Sensing and Navigation:** The final stage of the CSN is the blind localization of the valid sources (sensing) and/or blind navigation of the UE by feeding the obtained navigation observables into a navigation filter.

The beacon signals in LTE and 5G signals are not considered to be taking integer values and can assume any arbitrary complex-valued numbers. Therefore, they can be considered as beacons with NIC. The detection problem of an unknown source in the presence of other interfering signals falls into the paradigm of *matched subspace detectors*, which has been widely studied in the classic detection theory literature [113, 180]. Matched subspace detectors are used frequently in radar signal processing, e.g., in source positioning

in multiple-input multiple-output (MIMO) radars [109] and passive bistatic radar [233]. In [16], the design of subspace-matched filters in the presence of a mismatch in the steering vector was addressed. In [31], adaptive vector subspace detection in partially homogeneous Gaussian disturbance was addressed. In [32], the performance of low-rank adaptive normalized matched subspace detectors was studied. In [219], the structure of the noise covariance matrix was exploited to enhance the matched subspace detection performance. In [221], the idea of subspace matching was used to present a solution to the problem of detecting the number of signals in both white and colored noise. Recently, machine learning approaches have been proposed for unknown transmitter detection, identification, and classification [18,176]. In the navigation literature, the detection of unknown signals has been studied to design frameworks that are capable of navigating with unknown or partially known signals. The problem of detecting Galileo and Compass satellites signals was studied in [49], which revealed the spread spectrum codes for these satellites.

Fundamental challenges of detection of beacons with IC are: (i) the presence of multiple interfering unknown sources, (ii) the effect of Doppler estimation error on the performance of the matched subspace detector, (iii) selection of the detection threshold. The proposed approach in this dissertation is developing a sequential detection algorithm to detect multiple unknown sources. The proposed detector in this dissertation is a generalized version of the matched subspace detector with successive interference cancellation. The signal subspace was defined by the Doppler frequencies of unknown sources. Signal activity detection of unknown sources relies on the Doppler subspace. A hypothesis testing problem was solved sequentially in multiple stages to detect the active sources in the environment. At each stage, a test was performed to detect the most powerful source by comparing a likelihood with a predetermined threshold, while the *Doppler subspace* of the previously detected sources

were nulled. The so-called *general linear detector* [90] was modified based on the signal model and used at each stage of the sequential detection algorithm.

In the detection problem with IC, the integer constraint of the beacon symbols in the matched subspace detectors leads to a class of integer least square problems [70, 127]. One example of beacons with IC is the PRN sequence in CDMA-based communication systems. A low computational complexity approach to estimate the beacon symbols is the *symbol by symbol* estimation which suffers from a poor performance in low signal to noise ratio (SNR) regimes. In [49], a symbol by symbol (SBS) estimation scheme was considered to blindly estimate the symbols of the PRN sequences of Galileo and Compass satellites, and a 1.8 m high-gain antenna was used to accumulate enough signal power. The optimal algorithm proposed in [70] and [127] can be used to solve the integer least squares problem with a polynomial computational complexity.

A fundamental challenge of the detection methods with IC is the computational and hardware complexity of the integer least squares problem. Integer least squares problems usually contain a search over a discrete space which depends on the modulation order and beacon length. The length of beacon sequences is usually a large number in practical scenarios. For instance, the length of the beacon for GPS PRNs is $2^{10} - 1$. Therefore, the search space of the integer least square problem is large. The proposed approach in this dissertation is designing a near-optimal beacon detector with linear computational complexity to reduce the computational complexity of the detection problem of terrestrial signals with IC. The matched subspace detector for beacons with IC is derived and simplified to reduce the computational complexity. It is shown that the proposed detection algorithm

has a computational complexity that is linear with problem size and achieves a near-optimal performance.

The beacon signal detection method in the CSN framework relies on a knowledge of the beacon period. In public networks, the beacon period is typically mentioned in the protocol description. For instance, the period of 5G NR beacons 10 ms [198]. However, the beacon period for private networks is unknown and subject to change. The period estimation problem is extensively studied in the literature [33, 40, 53, 203, 207, 212]. An ML-based method for period estimation is presented in [33]. In [207] time-domain based method is proposed to estimate the period using the autocorrelation function.

In [40, 53] a Fourier transform-based technique is presented for periodicity analysis. The problem of detecting multiple hidden periodicities is studied in [203]. A hierarchical approach to finding all periodicities is presented in [93]. A fundamental challenge that should be addressed is the effect of the Doppler rate on the period estimation. Non-stationary transmitter and/or maneuvering UE result in significant values of the Doppler rate in the processing time. Unlike the Doppler effect which does not change the magnitude of the autocorrelation function, the Doppler rate has a destructive effect on the autocorrelation function. None of the period estimation methods in the literature take the effect of the Doppler rate into account. Therefore, the mentioned methods are not capable of estimating the beacon period in scenarios where the Doppler rate is high, e.g., LEO satellites. The autocorrelation of a large enough time segment of the received signal will result in a train of an impulse-like function whose shape depends on the autocorrelation properties of the synchronization signals. The distance between two consecutive impulses is equal to the beacon period. In conventional tracking algorithms, in order to track the time-variations of

the code- and carrier-phase, a traditional DLL and PLL is composed of three basic constituent blocks: (i) a code and carrier-phase discriminator, which is in charge of providing output measurements that, on average, are proportional to the code-phase and carrier-phase error to be compensated; (ii) a loop filter, which is nothing but a very narrow low-pass filter that smoothes the variability caused by thermal noise at the phase detector output; and (iii) a numerically-controlled oscillator (NCO) for generating the local carrier replica based on the corrections imposed by the loop filter output [122, 195, 220].

In 5G and beyond networks, the ultra-lean transmission allows the network to transmit some of the beacons only when it is necessary and the transmitted beacons are subject to change. Therefore, the CSN framework should be able to update the estimated beacon dynamically in the tracking process to be able to exploit all the available beacon power. The proposed approach in this dissertation is designing a tracking loop that is capable of refining the beacon estimate along with refined code- and carrier-phase. The core blocks of the proposed tracking loop are similar to the traditional carrier and code-phase tracking architectures [122]. The major difference between the proposed tracking loops and the conventional tracking loops is the RS-locked loop (RSLL). The task of the RSLL is to update the beacon signal in the tracking process. The received signal is used to update the beacon estimate. Adaptive gains are designed weigh the received signal samples based on the signal power.

The detected sources at the acquisition stage can be either a valid source (such as a 5G gNB or a LEO satellite signal) or a false alarm. A false alarm might be due to interfering signals and/or multipath components. The CSN framework should be able to classify the detected signal. Feature extraction is the main component of interference classification

algorithms [213, 214, 216, 217]. A single-tone, multi-tone, and narrow-band interference model is presented in [214] to perform interference cancellation. A convolutional neural network-based feature extraction algorithm is used in [216]. The sparsity of some forms of interference in the time or frequency domain was exploited in [213] to perform interference classification.

The CSN framework should be able to cognitively classify the false alarm and the valid signals in cellular and LEO satellite-based networks. Due to the limited information about the unknown environment in that the UE is operating, the interference classification should be performed in a blind fashion. The features which are considered in the interference classification algorithm are either specifically designed based on the signal model, or require a training phase that is not available in a blind scenario. A valid signal for the CSN framework is the line-of-sight component of the transmitted signal from a cellular tower or a LEO satellite. In the presence of line-of-sight component, the amplitude gain is characterized by a Rician distribution [206]. The carrier phase error in the tracking loops directly depends on the line-of-sight signal power [131]. The proposed approach distinguishes between a valid source and a false alarm based on the carrier phase error. If the detected source in the acquisition stage is a false alarm, the carrier phase error variance will be a large number. The proposed CSN framework considers the variance of carrier phase error in the tracking loops as the classification feature of false alarm and valid signals.

1.1 Other Related Work

1.1.0.1 Opportunistic Navigation

Over the past decade, opportunistic navigation [71] has been demonstrated in the literature with different types of signals [83], also known as signals of opportunity (SOPs). SOP examples include cellular [37, 72], digital television [28, 58, 66, 191, 192, 231], AM/FM [29, 128, 164, 167, 168], Wi-Fi [43, 188–190, 230, 237, 238], cellular [4, 17, 35, 41, 47, 48, 56, 68, 69, 84, 92, 95, 194, 218], low-earth orbit (LEO) satellite signals [15, 42, 44, 55, 87, 94, 105, 110, 112, 118, 139, 155, 160, 178, 199, 200, 222], and geostationary Earth orbit (GEO) satellites [50]. Among terrestrial SOPs, cellular signals have attracted considerable attention recently [3,46,67,98,114,121,162,186,202,228] due to their desirable attributes [27], including: (i) large transmission bandwidth, (ii) high carrier-to-noise ratio [7], and (iii) desirable geometric diversity [38]. Meter-level accuracy was achieved outdoors using cellular signals on ground and aerial vehicles [6,13,34,74,81,82,86,88,124,125,134,136,138,163,205,225], the potential of achieving of sub-meter level accuracy on aerial vehicles with LTE signals was demonstrated [36, 96, 99, 100, 106, 183], and the viability of navigating exclusively in with LTE signals in GPS-jammed environments was established [80]. Among extraterrestrial SOPs, LEO signals have attracted considerable attention over the past few years [26, 57, 59, 63–65, 85, 89, 111, 137, 140, 165, 166, 187, 193, 204, 210, 234] due to their desirable attributes [79]: (i) proximity to Earth compared to GNSS, (ii) high dynamics, (iii) spectral and geometric diversity, and (iv) projected abundance, with plans to launch tens of thousands of satellites into LEO over the current decade.

1.1.0.2 Positioning with 5G Signals

The characteristics of mmWave signals were evaluated for positioning in [227]. Cramér-Rao lower bounds (CRLBs) of the direction-of-departure (DOD), DOA, and TOA for both uplink and downlink mmWave signals were derived in [11, 12], showing sub-meter positioning error, and sub-degree orientation error. To exploit the sparsity of mmWave channels, tools relying on compressed sensing were proposed in [116], [229] to estimate DOD, DOA, and TOA of the UE, showing sub-meter level position error via simulation results. The DOD and UE's position were estimated in a two-stage Kalman filter using the signal strength from multiple base stations in [171], which yielded sub-meter-level three-dimensional (3-D) position accuracy. The joint estimation of 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, were considered in [129], showing less than 15 m position root mean-squared error (RMSE) and less than 7 degree orientation RMSE. A two-way distributed localization protocol was proposed in [10] to remove the effect of the clock bias in TOA estimates. In [45], a positioning method for multiple-output single-input systems was proposed, where the DOD and TOA of the received signal were used to localize a UE. In [123], estimation of signal parameters via rotational invariant techniques (ESPRIT) was used to estimate the DOA and DOD of the signal. Experimental results in [185] and [9] showed meter-level navigation using TOA estimates from 5G signals. The results presented therein rely only on the PSS and SSS for TOA estimation. It is shown that the proposed receiver yields a narrower RS autocorrelation function, which translates to more accurate TOA estimates. Moreover, the proposed receiver architecture can be readily adapted to any type of signal containing periodic RSs.

1.1.1 Resulting Publications

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

Journal Publications:

1. M. Neinavaie, J. Khalife, and Z. Kassas,“Cognitive Opportunistic Navigation in Private Networks with 5G Signals and Beyond", *in IEEE Journal of Selected Topics in Signal Processing,* vol. 16, no. 1, pp. 129-143, Jan. 2022.

2. M. Neinavaie, J. Khalife, and Z. Kassas, “Acquisition, Doppler Tracking, and Positioning with Starlink LEO Satellites: First Results", *in IEEE Transactions on Aerospace and Electronic Systems,*vol. 58, no. 3, pp. 2606-2610, June 2022.

3. M. Neinavaie, J. Khalife, and Z. Kassas,“Cognitive Detection of Unknown Beacons of Terrestrial Signals of Opportunity for Localization", *in IEEE Transactions of Wireless Communications,* Accepted. 2022.

4. M. Neinavaie and Z. Kassas,“Unveiling Starlink LEO Satellite OFDM-Like Signal Structure Enabling Precise Positioning", *in IEEE Transactions on Aerospace and Electronic Systems,* Accepted. 2023.

5. M. Neinavaie, and Z. Kassas,“Cognitive Sensing and Navigation with Unknown OFDM Signals with Application to Terrestrial 5G and Starlink LEO Satellites", *in IEEE Journal of Selected Areas in Communications,* Under Revision.

6. M. Neinavaie, J. Saroufim, S. Shahcheraghi, and Z. Kassas “Exploiting Unknown LEO Satellite Signals for Navigation: Acquisition Tracking, and Differential Navigation", Under Preparation.

7. M. Neinavaie and Z. Kassas,“Now You Are Beaming, Now You Are Not: Cognitive Opportunistic Navigation with Always-On and On-Demand Starlink OFDM Signals", Under Preparation,

Conference Papers and Workshops

1. M. Neinavaie and Z. Kassas, “Signal mode transition detection in Starlink LEO satellite downlink signals", IEEE/ION Position, Location, and Navigation Symposium, Apr. 25-27, 2023, Monterey, accepted.

2. M. Neinavaie, J. Khalife, and Z. Kassas, “Detection of constrained unknown beacon signals of terrestrial transmitters and LEO satellites with application to navigation," IEEE Vehicular Technology Conference, Sep. 26-29, 2022, London, England, pp. 1-5.

3. M. Neinavaie and Z. Kassas, “Joint detection and tracking of unknown beacons for navigation with 5G signals and beyond," ION Global Navigation Satellite Systems Conference, Sep. 19-23, 2022, Denver, CO, pp. 921-932.

4. M. Neinavaie and Z. Kassas, “Unveiling beamforming strategies of Starlink LEO satellites," ION Global Navigation Satellite Systems Conference, Sep. 19-23, 2022, Denver, CO, pp. 2525-2531.

5. M. Neinavaie, Z. Shadram, S. Kozhaya, and Z. Kassas, “First results of differential Doppler positioning with unknown Starlink satellite signals," IEEE Aerospace Conference, Mar. 5-12, 2022, Big Sky, MT, pp. 1-14.

6. M. Neinavaie, J. Khalife, and Z. Kassas, “Doppler stretch estimation with application to tracking Globalstar satellite signals," IEEE Military Communications Conference, Nov. 28 - Dec. 1, 2021, San Diego, CA, pp. 647-651 (special session)

7. M. Neinavaie, J. Khalife, and Z. Kassas, "Exploiting Starlink Signals for Navigation: First Results*:* ION Global Navigation Satellite Systems Conference, Sep. 20-24, 2021, St. Louis, MO, pp. 2266-2773.

8. M. Neinavaie, J. Khalife, and Z. Kassas,“Blind Doppler Tracking and Beacon Detection for Opportunistic Navigation with LEO Satellite Signals"*I*EEE Aerospace Conference, Mar. 6-13, 2021, Big Sky, MT, pp. 1-8.

9. M. Neinavaie, J. Khalife, and Z. Kassas, “Blind Opportunistic Navigation: Cognitive Deciphering of Partially Known Signals of Opportunity" ION Global Navigation Satellite Systems Conference, Sep. 21-25, 2020, St. Louis, MO, pp. 2748-2757.

1.1.2 Dissertation Outline

This dissertation is organized as follow:

- **Chapter 2:** In this chapter a receiver architecture is proposed to cognitively extract navigation observables from fifth generation 5G NR signals of opportunity. Unlike conventional opportunistic receivers which require knowledge of the signal structure, particularly the RSs, the proposed cognitive opportunistic navigation (CON) receiver requires knowledge of only the frame duration and carrier frequency of the signal. To exploit the full available bandwidth and improve ranging accuracy, the proposed CON receiver is designed to estimate all the RSs contained in the transmitted signals

corresponding to multiple 5G base stations, (i.e., gNBs). Navigation observables (pseudorange and carrier phase) are subsequently derived from the estimated RSs. The proposed receiver operates in two stages: (i) acquisition and (ii) tracking. The acquisition stage of the CON receiver is modeled as a sequential detection problem where the number of gNBs and their corresponding RSs and Doppler frequencies are unknown. The generalized likelihood ratio (GLR) test for sequentially detecting active gNBs is derived and used to estimate the number of gNBs and their RSs. In order for the receiver to refine and maintain the Doppler and RS estimates provided by the acquisition stage, tracking loops are designed. A sufficient condition on the Doppler estimation error to ensure that the proposed GLR asymptotically achieves a constant false alarm rate (CFAR) is derived. The output of the tracking loops, namely carrier phase and code phase, are then used to estimate the receiver's position. Extensive experimental results are presented demonstrating the capabilities of the proposed CON receiver with real 5G signals on ground and aerial platforms, with an experiment showing the first navigation results with real 5G signals on an unmanned aerial vehicle (UAV) navigating using the CON receiver over a 416 m trajectory with a position RMSE of 4.35 m.

- **Chapter 3:** A cognitive approach is proposed to detect unknown beacons of terrestrial SOPs. Two scenarios are considered in the chapter: (i) detection of unknown beacons with IC and (ii) detection of unknown beacons with NIC. Matched subspace detectors are proposed for both scenarios, and it is shown experimentally that the proposed matched subspace detectors are capable of detecting cellular 3G cdma2000 signals and 5G OFDM signals. A low complexity method is derived to simplify the matched subspace detector with IC for M-ary MPSK modulation. The effect of symbol errors

in the estimated beacon signal on the carrier to noise ratio (CNR) is characterized analytically. Closed-form expressions for the asymptotic probability of detection and false alarm are derived. Experimental results are presented showing an application of the proposed cognitive approach by enabling a UAV to detect and exploit terrestrial cellular signals for navigation purposes. The UAV achieved submeter-level accurate navigation over a trajectory of 1.72 km, by exploiting signals from four 3G cdma2000 transmitters.

- **Chapter 4:** A receiver architecture for cognitive sensing and navigation with OFDM-based systems is proposed. Similar to conventional navigation receivers the proposed architecture involves acquisition and tracking stages. However, both acquisition and tracking stages are supplemented by the unorthodox capability of estimating and updating the RS signals. The acquisition stage instructs the tracking stage by reporting the performance metrics to the tracking stage. The tracking stage adjusts the loop gains based on the reported information to update the RS accordingly. A chirp model is considered at the acquisition stage to capture the high dynamics of Doppler frequency in *intensive Doppler scenarios*, where the navigating vehicle is maneuvering or the transmitting source is not static. The effect of Doppler rate estimation error on the frame length estimation is analyzed. Using the proposed algorithm, the OFDM signal tracking results with Starlink downlink signals are presented. Experimental results are presented demonstrating the performance of the proposed receiver by: (i) enabling an unmanned aerial vehicle (UAV) to detect and exploit terrestrial 5G NR cellular signals for navigation purposes showing an RMSE which is bounded between 4.2m and 5.8 m in a total trajectory of 416 m, and (ii) enabling a ground vehicle to cognitively sense (detect blindly, exploit all the information, and track) an unknown gNB in a traversed

trajectory of 1.79 km, and estimating the position of the gNB with a two-dimensional error of 5.83 m in a blind fashion.

- **Chapter 5** In this chapter, it is shown that despite the dynamic nature of Starlink RSs, the proposed matched subspace detector senses the *transition between the transmission modes* of Starlink RSs, and detects all the accessible RSs with a predetermined probability of false alarm. To demonstrate the performance of the proposed receiver experimentally, a base with a known position and a stationary rover with an unknown position was equipped with the proposed receiver. Two baselines between the base and rover receivers were considered: 1.004 km and 8.6 m. Despite the fact that the satellites' ephemerides were poorly known (with errors on the order of several kilometers, as they are predicted from two-line element (TLE) files and an SGP4 propagator), the differential framework estimated the rover's two-dimensional (2D) position with an error of 3.9 m and 83 cm, respectively.

- **Chapter 6:** This chapter starts with exploiting the RSs of the Starlink downlink signals. The frame length of the downlink OFDM-like signals is estimated. The whole available bandwidth of multiple Starlink SVs is exploited and the corresponding RSs are estimated and used to obtain the code and carrier phase observables. The experimental results show a horizontal positioning error of 6.5 m with known receiver altitude. Several experiments are provided to show the capability of the proposed method in exploiting downlink signals of multi-constellations.

- **Chapter 7:** This chapter summarizes the contributions of this dissertation and highlights the major discoveries.

Chapter 2: Cognitive Opportunistic Navigation in Private Networks With 5G Signals and Beyond

2.1 Introduction

Current capabilities offered by fourth generation (4G) mobile communications will not meet the demands of emerging applications such as internet of things (IOT) and autonomous vehicles [14, 23]. To address such demands, fifith generation (5G) has been developed, with a focus on features such as enhanced mobile broadband, ultra-reliable low-latency communications, and massive machine type communications [158]. Based on the performance requirements set by the international telecommunication union (ITU), the third generation partnership project (3GPP) began 5G standardization in 2015 and released its first specifications on a 5G system in June 2018, which included both the new air interface, known as new radio (NR), and 5G core network (5GC) [198]. One main characteristic of 5G signals is high data rate, which necessitates a higher transmission bandwidth and more sophisticated multiplexing techniques. The scarcity of unlicensed spectrum in lower frequencies called for using millimeter waves (mmWaves) for NR signal transmission [19]. The high path loss of propagated mmWave signals can be compensated for by beamforming techniques and massive multiple-input multiple-output (mMIMO) antenna structures [52]. Beamforming in

5G requires the knowledge of the user's location, which means that 5G-based positioning is not only an auxiliary service, but is essential for resource allocation and beamforming for high data rate transmission [45]. Different types of positioning techniques have been evaluated by the 3GPP in Release 15 and 16 [1].

Cellular positioning techniques in the literature can be classified into *network-based* and *opportunistic* approaches [37, 72]. Network-based approaches require two-way communication with the network and the transmission of a pre-specified positioning reference signal (PRS) and some system parameters such as the number of transmission antennas and the beamforming matrix. Network-based positioning capabilities in wireless communication systems have been defined since 4G systems [35]. In a contrast to network-based approaches, in opportunistic approaches, the user equipment (UE) estimates its position from downlink signals, without communicating back with the network. As such, opportunistic approaches are more attractive than network-based approaches since: they (i) do not require additional overhead or bandwidth, (ii) preserve the UE's privacy, (iii) do not require paying subscription to the network, and (iv) enable the UE to exploit signals from multiple cellular providers simultaneously, which improves the positioning accuracy.

Opportunistic navigation frameworks usually rely on the broadcast reference signals (RSs), which are used to derive direction-of-arrival (DOA) and time-of-arrival (TOA) [184]. These signals are known at the UE and are universal across network operators. Hence, they can be exploited for positioning without the need for the UE to be a network subscriber. In cellular long-term evolution (LTE) networks, several RSs, such as the cell-specific reference signal (CRS), are broadcast at regular and known time intervals, regardless of the number of UEs in the environments. This *always-on* type of transmitted RSs reduces the network's

energy efficiency and increases operational expenses and interference. One of the main features of 5G signals is *ultra-lean* transmission, which minimizes the transmission of always-on signals. For instance, CRS which used to be an always-on RS in LTE, is not necessarily being continuously transmitted in 5G signals. Up until now, 5G opportunistic navigation methods relied on the always-on signals, e.g., the primary and secondary synchronization signals (PSS and SSS, respectively) and the physical broadcast channel (SB/PBCH) block, none of which use the entire signal bandwidth [9, 75, 185].

This chapter presents a cognitive opportunistic navigation framework (CON) by developing a 5G receiver architecture to simultaneously detect the active gNBs in the environment, estimate the number of gNBs and their unknown RSs which are not necessarily *always-on*, and exploit them to derive navigation observables in a cognitive fashion. There are four main RSs in 5G signals: demodulation RSs, phase tracking RSs, sounding RSs, and channel state information (CSI) RSs. These RSs are only transmitted on demand, which limits the efficacy of conventional opportunistic navigation frameworks which rely on always-on RSs. For instance, while the receiver proposed in [185] was the first 5G-based opportunistic navigation receiver, it relies on the always-on SB/PBCH block. The downside of relying only on the SB/PBCH block is the limited bandwidth. Higher signal bandwidth translates to more accurate TOA estimates. In order to exploit the full ranging accuracy achievable with 5G signals, the proposed CON receiver is designed to cognitively estimate the RSs present in the entire bandwidth and exploit them to obtain navigation observables (pseudoranges and carrier phase). Not only the proposed receiver is capable of exploiting RSs which are not always-on, but the cognitive nature of the proposed receiver enables opportunistic navigation with future communication standards with unknown or partially known signal specifications. The proposed receiver architecture relies solely on the periodicity of the

RSs and requires very limited information about the 5G signal, namely it only assumes knowledge of the frame duration and the carrier frequency. It should be pointed out that an energy detector can be used to provide an estimate of the carrier frequency and using the current literature, e.g., the period estimator in [33], the frame duration can also be estimated in a pre-processing stage. One main challenge faced by the CON receiver is the problem of distinguishing signals from multiple 5G base stations, i.e., gNBs, multiplexed over the same channel. This task is relatively simple when the RSs are known, as RSs are usually designed to have desirable autocorrelation and cross-correlation properties. Since this chapter does not assume knowledge of the RSs, it is desirable for the CON receiver to be able to detect multiple gNBs and distinguish their signals. To this end, a subspace-based detection scheme leveraging the Doppler frequency subspace is proposed to estimate the number of available gNBs and estimate their RSs.

Specifically, the contributions of this chapter are as follows:

- A CON receiver design is presented, which could estimate the unknown RSs of a gNB. The cognitive nature of the proposed receiver enables estimating both always-on and on demand RSs which are not necessarily always-on. Using extensive experiments, it is shown that the estimated RSs posses higher bandwidth compared to conventional 5G opportunistic navigation receivers, which allows for producing more precise navigation observables.
- A sequential generalized likelihood ratio (GLR) detector is derived to detect the presence of multiple gNBs on the same channel and provide an estimate of the number of active gNBs. The detector relies on matched subspace detection, where the signal subspace is defined by the Doppler frequencies of the gNBs. The sequential GLR

detector estimates the number of gNBs, and their Doppler frequencies, and it provides an initial estimate of their unknown RSs, which are then used and refined in the tracking loops.

- A sufficient condition on the Doppler estimation error to ensure that the proposed GLR asymptotically achieves a constant false alarm rate (CFAR) is derived.

- Extensive experimental results are presented demonstrating the capabilities of the proposed CON receiver with real 5G signals on ground and aerial platforms. On a ground vehicle, it is demonstrated that the CON receiver yields a reduction of 10% and 37.7% in the estimated delay and Doppler root mean squared error (RMSE), respectively, over that achieved with a conventional opportunistic navigation 5G receiver that has complete knowledge of the transmitted RSs but only relies on always-on RSs. On an unmanned aerial vehicle (UAV), it is demonstrated that the proposed CON receiver enables the UAV to navigate over a 416 m trajectory with two 5G NR gNBs achieving a position RMSE of 4.35 m. To evaluate the performance of the CON receiver in a scenario where the RSs are always-on, another experiment is conducted in which a UAV navigates with long-term evolution (LTE) eNodeBs, achieving a position RMSE of 2.07 m, which is identical to the performance achieved with a conventional opportunistic navigation 4G receiver that has complete knowledge of the transmitted RSs.

The rest of the chapter is organized as follows. Section 4.2 surveys related research on navigation with 4G and 5G signals. Section 2.2 describes the received baseband signal model. Section 6.3 presents the proposed CON receiver architecture. Section 2.4 presents the experimental results.

2.2 Received Baseband Signal Model

This section provides a brief review of the NR RSs, and presents the signal model.

2.2.1 Brief Review of NR RSs

NR adopts orthogonal frequency division multiplexing (OFDM) scheme, as was the case in 4G. In OFDM-based transmission, the symbols are mapped onto multiple carrier frequencies, referred to as subcarriers, with a particular spacing known as subcarrier spacing. Unlike the 4G signal standard, which considers a fixed subcarrier spacing of 15 kHz, subcarrier spacing values of $15 \times 2^{\mu}$, with $\mu \in \{0, 1, 2, 3\}$ are supported by NR. The system selects subcarrier spacing values based on carrier frequency, and/or other requirements and scenarios. Once the subcarrier spacing is configured, the frame structure is identified. An NR frame has a duration of 10 ms and consists of 10 subframes with durations of 1 ms [198]. In the proposed receiver, only the frame duration and carrier frequency are assumed to be known. 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 [198].

To provide frame timing to the UE, a gNB broadcasts synchronization signals (SS) on pre-specified symbol numbers. An SS includes PSS and SSS, which provide symbol and frame timing, respectively. The PSS and SSS are transmitted along with the 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. The SS/PBCH block has a periodicity of 20 ms and is transmitted numerous times on one of the half frames, also known as SS/PBCH burst.

2.2.2 Signal Model

As it was mentioned previously, the SS/PBCH block is not transmitted on the whole signal's bandwidth. Therefore, methods which only rely on SS/PBCH block, cannot exploit the full ranging accuracy that can be achieved by 5G signals. Other periodic RSs are not necessarily *always-on* and the cognitive receiver should be able to exploit them to be able to achieve the available ranging accuracy. In this chapter, with a focus on exploiting navigation observables using the RSs in the entire 5G bandwidth, the 5G NR signal is modeled as an unknown periodic signal in the presence of interference and noise. If an RS is being periodically transmitted, it will be detected by the receiver, estimated, and used to derive navigation observables. The estimated RS will involve an estimation of always-on signals such as the SSs and any other active reference signal that is being periodically transmitted. It will be shown experimentally in section 2.4 that the exploited bandwidth by the proposed cognitive method is larger than that of the method which only relies on always-on signals. Denoting a continues-time signal at time t by $c(t)$, and a discrete-time signal at time instant n by $c[n]$, the received baseband signal model can be expressed as

$$\begin{aligned} r[n] = \sum_{i=1}^{N} & \left(\alpha_i c_i(\tau_n - t_{s_i}[n]) \exp\left(j\theta_i(\tau_n)\right)\right. \\ & \left. + d_i(\tau_n - t_{s_i}[n]) \exp\left(j\theta_i(\tau_n)\right)\right) + w[n], \end{aligned} \tag{2.1}$$

where $r[n]$ is the received signal at the nth time instant; α_i is the complex channel gain between the UE and the ith gNB; τ_n is the sample time expressed in the receiver time; N is the number of gNBs; $c_i[n] \triangleq c_i(\tau_n)$ is the periodic RS with a period of L samples; $t_{s_i}[n]$ is the code-delay corresponding to the UE and the ith gNB at the nth time instant;

$\theta_i(\tau_n) = 2\pi f_{D_i}[n]T_s n$ is the carrier phase in radians, where $f_{D_i}[n]$ is the Doppler frequency at the nth time instant and T_s is the sampling time; $d_i(\tau_n)$ represents the samples of some data transmitted from the ith gNB; and $w[n]$ is a zero-mean independent and identically distributed noise with $\mathbb{E}\{w[m]w^*[n]\} = \sigma_w^2\delta[m-n]$, where $\delta[n]$ is the the Kronecker delta function, and X^* denotes the complex conjugate of random variable X.

According to (4.1), the channel between the ith gNB and the UE is considered to have a single tap with the complex channel gain α_i. The desired RS from the ith gNB is defined as

$$s_i[n] \triangleq \alpha_i c_i(\tau_n - t_{s_i}[n]) \exp\left(j\theta_i(\tau_n)\right), \tag{2.2}$$

and the equivalent noise is

$$w_{\text{eq}_i}[n] = d_i(\tau_n - t_{s_i}[n]) \exp\left(j\theta_i(\tau_n)\right) + w[n]. \tag{2.3}$$

Hence, the signal model can be rewritten as

$$r[n] = \sum_{i=1}^{N} \left(s_i[n] + w_{\text{eq}_i}[n]\right). \tag{2.4}$$

It should be noted that due to the periodicity of the RS, assuming a constant Doppler in the processing time, i.e., $f_{D_i}[n] = f_{D_i}$, the desired RS has the following property

$$s_i[n+mL] = s[n] \exp\left(j\omega_i mL\right) \quad 0 \leq n \leq L-1, \tag{2.5}$$

where $\omega_i = 2\pi f_{D_i} T_s$ is the normalized Doppler, and $-\pi \leq \omega_i \leq \pi$. The acquisition stage will estimate $s_i[n]$ and the estimation of $s_i[n]$ will be used at the receiver to obtain the navigation observables.

Definition: The coherent processing interval (CPI) is defined as the time interval during which the Doppler, delay, and channel gains are considered to be constant.

One can form a vector of L observation samples corresponding to the kth period of the signal as

$$\mathbf{y}_k \triangleq [r[(k-1)L+1], r[(k-1)L+2], \ldots, r[kL]]^{\mathsf{T}}. \tag{2.6}$$

Considering a CPI of length $K \times L$ samples, the observation vector is constructed as $\mathbf{y} = [\mathbf{y}_1^{\mathsf{T}}, \mathbf{y}_2^{\mathsf{T}}, \ldots, \mathbf{y}_K^{\mathsf{T}}]^{\mathsf{T}}$. Therefore,

$$\mathbf{y} = \sum_{i=1}^{N} \mathbf{H}_i \mathbf{s}_i + \mathbf{w}_{\mathrm{eq}_i}, \tag{2.7}$$

where $\mathbf{s}_i = [s_i[1], s_i[2], \ldots, s_i[L]]^{\mathsf{T}}$, $\mathbf{w}_{\mathrm{eq}_i}$ is the equivalent noise vector corresponding to the ith source, and the $KL \times L$ Doppler matrix corresponding to the ith source is defined as

$$\mathbf{H}_i \triangleq [\mathbf{I}_L, \exp(j\omega_i L)\mathbf{I}_L, \ldots, \exp(j\omega_i (K-1)L)\mathbf{I}_L]^{\mathsf{T}}, \tag{2.8}$$

where $\mathbf{I}_L$ is an $L \times L$ identity matrix.

2.3 CON Receiver Structure

This section presents the structure of the proposed receiver. The proposed receiver consists of two main stages: (i) acquisition and (ii) tracking. Each of these stages are discussed in details next.

2.3.1 Acquisition

In this chapter, the acquisition stage is modeled as a sequential matched subspace detection problem. The acquisition stage comprises estimating the number of gNBs, an initial estimate of normalized Doppler, and the RSs, i.e., N, ω_i, and $\mathbf{s}_i$, respectively. At each step of the acquisition, a test is performed to detect the most powerful gNB when the subspace of the previously detected gNBs are nulled. In the following subsection, matched

subspace detection is overviewed and the hypothesis test for detection of multiple gNBs is formulated.

2.3.1.1 Matched Subspace Detector

As it was mentioned previously, in the first step of the proposed sequential algorithm, the presence of a single gNB is tested and if the null hypothesis is accepted, then $\hat{N} \equiv 0$, which means that no gNB is detected to be present in the environment under the test. If the test rejects the null hypothesis, the algorithm verifies the presence of at least one source and performs the test to detect the presence of other gNBs in the presence of the previously detected gNBs. The unknown Doppler and the RS of each gNBs are estimated at each step. In general, if the null hypothesis at the ith level of the sequential algorithm is accepted, the algorithm is terminated and the estimated number of gNBs will be $\hat{N} = i - 1$.

In order to test the presence of $\mathbf{s}_i$, at the ith stage of the acquisition algorithm, the observation vector can be written as

$$\mathbf{y} = \mathbf{H}_i \mathbf{s}_i + \mathbf{B}_{i-1} \boldsymbol{\theta}_{i-1} + \mathbf{w}_{\mathrm{eq}_i}, \tag{2.9}$$

$$\mathbf{B}_{i-1} \triangleq [\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_{i-1}],\ \boldsymbol{\theta}_{i-1} \triangleq [\mathbf{s}_1^{\mathsf{T}}, \mathbf{s}_2^{\mathsf{T}}, \ldots, \mathbf{s}_{i-1}^{\mathsf{T}}]^{\mathsf{T}}. \tag{2.10}$$

The following binary hypothesis test is used to detect the ith gNB:

$$\begin{cases} \mathscr{H}_0^i : & \mathbf{y} = \mathbf{B}_{i-1} \boldsymbol{\theta}_{i-1} + \mathbf{w}_{\mathrm{eq}_i} \\ \mathscr{H}_1^i : & \mathbf{y} = \mathbf{H}_i \mathbf{s}_i + \mathbf{B}_{i-1} \boldsymbol{\theta}_{i-1} + \mathbf{w}_{\mathrm{eq}_i}. \end{cases} \tag{2.11}$$

For a given set of Doppler frequencies, $\mathscr{W}_i = \{\omega_1, \omega_2, \ldots, \omega_i\}$, the GLR at the ith stage is derived as (see Appendix .1)

$$\mathscr{L}_i(\mathbf{y}|\mathscr{W}_i) = \frac{\mathbf{y}^{\mathsf{H}} \mathbf{P}_{\mathbf{S_i}} \mathbf{y}}{\mathbf{y}^{\mathsf{H}} \mathbf{P}^{\perp}_{\mathbf{B_{i-1}}} \mathbf{P}^{\perp}_{\mathbf{S_i}} \mathbf{P}^{\perp}_{\mathbf{B_{i-1}}} \mathbf{y}}, \tag{2.12}$$

where $\mathbf{y}^{\mathsf{H}}$ is the Hermitian transpose of $\mathbf{y}$, $\mathbf{P}_{\mathbf{X}} \triangleq \mathbf{X}(\mathbf{X}^{\mathsf{H}}\mathbf{X})^{-1}\mathbf{X}^{\mathsf{H}}$, denotes the projection matrix to the column space of $\mathbf{X}$, and

$$\mathbf{P}_{\mathbf{X}}^{\perp} \triangleq \mathbf{I} - \mathbf{X}\left(\mathbf{X}^{\mathsf{H}}\mathbf{X}\right)^{-1}\mathbf{X}^{\mathsf{H}}, \tag{2.13}$$

denotes the projection matrix onto the space orthogonal to the column space of $\mathbf{X}$, and $\mathbf{S}_i = \mathbf{P}_{\mathbf{B}_{i-1}}^{\perp}\mathbf{H}_i$. Intuitively, in (5.10) the subspace of previously detected gNBs, i.e., $\mathbf{B}_{i-1}$, is nulled to detect the ith gNB.

Remark 1: (*Vector space interpretation of (5.10)*): If the subspace spanned by the columns of $\mathbf{S}_i = \mathbf{P}_{\mathbf{B}_{i-1}}^{\perp}\mathbf{H}_i$, is viewed as the *ith gNB's signal subspace*, and the orthogonal subspace as the *noise subspace*, then the likelihood (5.10) can be interpreted as an estimated signal to noise ratio (SNR). The reader is referred to [180] for further interpretations of matched subspace detectors.

Remark 2: At the ith stage of the proposed sequential algorithm, the GLR requires an estimate of the set $\mathscr{W}_i$. The sequential nature of the algorithm enables a single variable estimation of the Doppler frequency at each step. For instance, at the first step of the algorithm, a single dimensional search is required to obtain the maximum likelihood (ML) estimate of ω_1, denoted by $\hat{\omega}_1$. In the second stage of the algorithm, $\hat{\omega}_1$ is used to construct the projection matrix to null the subspace of the first gNB. Consequently, at the ith step of the algorithm, invoking the previously estimated Dopplers, a single dimensional search is required to estimate ω_i, and construct the estimated projection matrix and the estimated Doppler matrix for the corresponding stage, denoted by $\hat{\mathbf{P}}_{\mathbf{S}_i}$ and $\hat{\mathbf{H}}_i$, respectively.

The following lemma simplifies the likelihood function (5.10).

Lemma 1: In the likelihood function (5.10), the following equality holds

$$\mathbf{H}_i^{\mathsf{H}} \mathbf{P}_{\mathbf{B}_{i-1}}^{\perp} \mathbf{H}_i = \lambda_i \mathbf{I}, \tag{2.14}$$

where the scalar λ_i is the Schur complement of block $\mathbf{C}_{i-1}$, i.e., the upper $(i-1)\times(i-1)$ block of the matrix $\mathbf{C}_i$[††], where

$$\mathbf{C}_i = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1i} \\ c_{21} & c_{22} & \dots & c_{2i} \\ \vdots & \ddots & \ddots & \vdots \\ c_{i1} & c_{i2} & \dots & c_{ii} \end{bmatrix}, \tag{2.15}$$

and $c_{ij} \triangleq \sum_{k=0}^{K-1} \exp\big(j(\omega_j - \omega_i)Lk\big)$.

Proof: See Appendix .2.

According to Lemma 1, the likelihood (5.10) at the ith stage can be simplified as

$$\mathscr{L}_i(\mathbf{y}) = \frac{\|\hat{\lambda}_i^{-1} \hat{\mathbf{H}}_i^{\mathsf{H}} \hat{\mathbf{P}}_{\mathbf{B}_{i-1}}^{\perp} \mathbf{y}\|^2}{\|\hat{\mathbf{P}}_{\mathbf{B}_{i-1}}^{\perp} \mathbf{y}\|^2 - \|\hat{\lambda}_i^{-1} \hat{\mathbf{H}}_i^{\mathsf{H}} \hat{\mathbf{P}}_{\hat{\mathbf{B}}_{i-1}}^{\perp} \mathbf{y}\|^2} \underset{\mathscr{H}_0^i}{\overset{\mathscr{H}_1^i}{\gtrless}} \eta_i. \tag{2.16}$$

where η_i is a predetermined threshold at the ith stage. The ML estimate of $\hat{\omega}_i$, is obtained by maximizing the likelihood function under $\mathscr{H}_1^i$ which yields

$$\hat{\omega}_i = \arg\max_{\omega_i} \|\mathbf{H}_i^{\mathsf{H}} \mathbf{P}_{\mathbf{B}_{i-1}}^{\perp} \mathbf{y}\|^2, \tag{2.17}$$

and is used to construct $\hat{\mathbf{P}}_{\mathbf{B}_{i-1}}$, $\hat{\mathbf{H}}_i$, and $\hat{\lambda}_i$.

For a known ω_i, the least squares (LS) estimate of the ith source, i.e., $\mathbf{s}_i$, is given by

$$\hat{\mathbf{s}}_i = \frac{1}{\lambda_i} \mathbf{H}_i^{\mathsf{H}} \mathbf{P}_{\mathbf{B}_{i-1}}^{\perp} \mathbf{y}, \tag{2.18}$$

It should be noted that the estimated RS, i.e., $\hat{\mathbf{s}}_i$, contains the effect of the channel between the gNB and the UE. Small values of $|\alpha_i|$ degrades the estimation quality of the desired

[††]Consider $p \times p$ matrix $\mathbf{A}$, $p \times 1$ vectors $\mathbf{b}$ and $\mathbf{c}$ and scalar d. For the matrix $\begin{bmatrix} \mathbf{A} & \mathbf{b} \\ \mathbf{c}^{\mathsf{T}} & d \end{bmatrix}$, the Schur complement of block $\mathbf{A}$ is defined as $d - \mathbf{c}^{\mathsf{T}} \mathbf{A}^{-1} \mathbf{b}$.

RS and, consequently, affects the acquisition and tracking performance. It should also be pointed out that $\frac{1}{\lambda_i}\mathbf{H}_i^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{y} = \mathbf{s}_i + \mathbf{w}_{\text{acq}_i}$, where $\mathbf{w}_{\text{acq}_i} = \frac{1}{\lambda_i}\mathbf{H}_i^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{w}_{\text{eq}_i}$. In other words, for a known Doppler frequency, the LS estimator of the *i*th source is an unbiased estimator, i.e., $\mathbb{E}\{\hat{\mathbf{s}}_i\} = \mathbf{s}_i$. However, since the true Doppler is not known to the CON receiver, the ML estimate of the Doppler is used to compute the LS estimate of the *i*th RS instead. Moreover, it can be shown that

$$\frac{1}{\hat{\lambda}_i}\hat{\mathbf{H}}_i^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{B}_{i-1}}\mathbf{H}_i = \beta_{\text{acq}_i}\mathbf{I}, \tag{2.19}$$

where β_{acq_i} is some complex scalar. As such, the LS estimate of the RS using the ML estimate of the Doppler becomes

$$\hat{\mathbf{s}}_i = \frac{1}{\hat{\lambda}_i}\hat{\mathbf{H}}_i^{\mathsf{H}}\hat{\mathbf{P}}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{y} = \beta_{\text{acq}_i}\mathbf{s}_i + \hat{\mathbf{w}}_{\text{acq}_i}, \tag{2.20}$$

where $\hat{\mathbf{w}}_{\text{acq}_i} \triangleq \frac{1}{\hat{\lambda}_i}\hat{\mathbf{H}}_i^{\mathsf{H}}\hat{\mathbf{P}}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{w}_{\text{eq}_i}$. Furthermore, the asymptotically efficient property of the ML estimator results in $|\beta_{\text{acq}_i}| \to 1$ as $K \to \infty$ [236].

2.3.1.2 Asymptotic CFAR property

The Doppler estimation error affects the probability of detection and the probability of false alarm. For known subspaces and the corresponding projection matrices, using Theorem 7.1 in [90], one can show that the probability of false alarm for the *i*th stage of the likelihood in (5.10) asymptotically tends to

$$P_{\text{fa}_i} = \exp(-L\eta_i)\sum_{n=0}^{L-1}\frac{(L\eta_i)^n}{n!}, \tag{2.21}$$

for a large number of observation samples. In other words, the detector is not a function of unknown parameters for known Doppler frequencies, which means that it ensures CFAR property. Next, the effect of Doppler estimation error on the probability of false alarm is

assessed. The following theorem gives a sufficient condition to ensure the CFAR property for a scenario with two gNBs for a large enough CPI.

Theorem 1: Consider two gNBs with Doppler frequencies ω_1 and ω_2 and corresponding estimates $\hat{\omega}_1$ and $\hat{\omega}_2$, respectively. Define the Doppler estimation error of ω_1 as $\Delta\omega_1 \triangleq \omega_1 - \hat{\omega}_1$. As $K \to \infty$, sufficient conditions for the matched subspace detector in (5.10) to be a CFAR detector in the second stage are (i) $|\Delta\omega_1 L| \ll \frac{1}{K}$ and (ii) $|\hat{\omega}_2 L - \hat{\omega}_1 L| > \frac{1}{K}$.

Proof: See Appendix .3.

Numerical simulations were conducted in order to visualize the results of Theorem 1. To this end, 5G-like signals were simulated for two different sources at: (i) $\omega_1 L = 0$ and (ii) $\omega_2 L = 0.2$. Then, the CPI length was varied from $K = 5$ to $K = 30$ and $(\hat{\omega}_1 L - \hat{\omega}_2 L)$ was varied from -0.5 to 0.5. For each $(K, \hat{\omega}_1 L - \hat{\omega}_2 L)$ pair, 10^5 realizations of the noise $\mathbf{w}_{\text{eq}_i}$ were used to numerically calculate P_{fa}. The detection threshold was selected such that $P_{\text{fa}} = 0.001$ in the absence of the second source. The results are shown in Fig. 2.1 indicating that P_{fa} for $|\hat{\omega}_i L - \hat{\omega}_j L| > \frac{1}{K}$ is almost constant at 0.001, and approaches 1 otherwise, which demonstrates Theorem 1.

It should be pointed out that in the experiments, (4.20) is used to select the threshold for a given probability of false alarm. According to Theorem 7.1 in [90], (4.20) holds for a large number of observation samples and for known subspaces. Due to the asymptotic efficiency property of the ML estimator, it is assumed that the subpsapce estimation error tends to zero for a large number of observation samples. In the experiments, the number of samples in a CPI is selected to be large and (4.20) holds asymptotically. The acquisition algorithm is summarized in Algorithm 1.

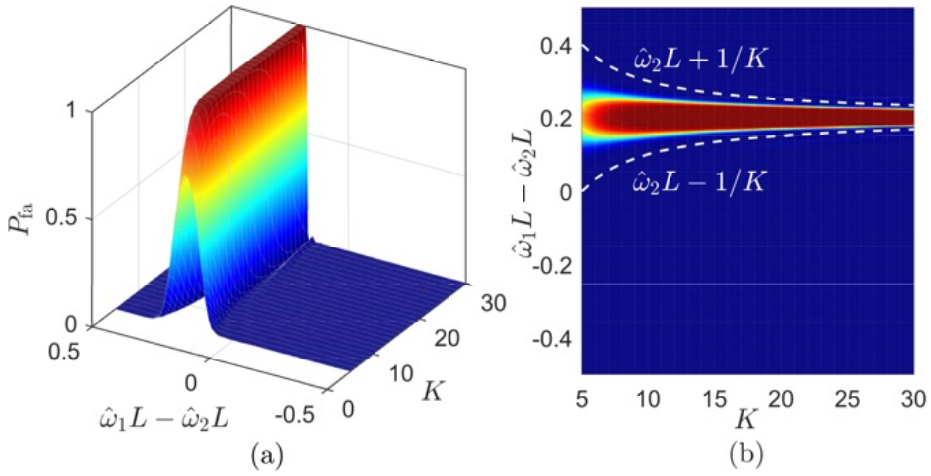


Figure 2.1: Simulation results demonstrating Theorem 1. (a) A surface plot of P_{fa} for varying values of K and $\hat{\omega}_1 L - \hat{\omega}_2 L$. (b) A heat map of P_{fa} along with the CFAR convergence boundaries in dashed white lines, as determined by Theorem 1.

2.3.2 Tracking

After obtaining coarse estimates of the Doppler frequencies and estimates of the RSs in the acquisition step, the receiver refines and maintains these estimates. Specifically, phase-locked loops (PLLs) are employed to track the carrier phases of the detected RSs and carrier-aided delay-locked loops (DLLs) are used to track the RSs' code phases. Each detected source has its own dedicated tracking loop. Therefore, for compactness of notation, the source index i is dropped in the subsequent analysis. The tracking loops are discussed next.

2.3.2.1 RS Estimate Update

The acquisition step provides a coarse initial estimate of the RS, denoted by $\hat{\mathbf{s}}_{\text{acq}_i}[n]$. From (2.20), the nth symbol of the estimated RS can be expressed as $\hat{s}_{\text{acq}}[n] = \beta_{\text{acq}} s[n] + \hat{w}_{\text{acq}}[n]$, where β_{acq} is obtained according to (2.19) and $x[n]$ is the nth element of vector $\mathbf{x}$. Recall

Algorithm 1 Sequential Matched Subspace Detector

Input: $\mathbf{y}$, P_{fa}
Output: $\hat{N}$, $\hat{\omega}_i$, and $\hat{\mathbf{s}}_i$ for $i = 1, \ldots, \hat{N}$

1: Initialization: $i = 1$, $\mathbf{P}^{\perp}_{\mathbf{B}_0} = \mathbf{I}$
2: Calculate $\mathscr{L}_i(\mathbf{y})$ according to (4.19) and the threshold using (4.20).
3: **if** $\mathscr{L}_i(\mathbf{y}) < \eta_i$ **then**
4: $\quad \hat{N} = i - 1$.
5: $\quad$ Break
6: **end if**
7: Estimate ω_i according to (6.5), and construct $\hat{\mathbf{H}}_i$, $\hat{\mathbf{P}}^{\perp}_{\mathbf{B}_{i-1}}$, and $\hat{\lambda}_i$
8: $\hat{\mathbf{s}}_i = \frac{1}{\hat{\lambda}_i} \hat{\mathbf{H}}_i^{\mathsf{H}} \hat{\mathbf{P}}^{\perp}_{\mathbf{B}_{i-1}} \mathbf{y}$
9: $i \leftarrow i+1$, update $\hat{\mathbf{P}}^{\perp}_{\mathbf{B}_{i-1}}$ using $\hat{\omega}_i$, and go to step 2.

that β_{acq_i} depends on the Doppler estimation error in the acquisition stage. Let $\hat{t}_{s_k}$ and $\hat{f}_{D_k}$ be the code phase and the Doppler estimates at time-step k in the tracking loop, respectively. In this step of the tracking loop, the RS estimate is updated by coherently integrating the observations after delay compensation and Doppler wipe-off. As such, the RS estimate at the kth iteration of the tracking loops is given by

$$\begin{aligned} \hat{s}_k[n] &= \frac{k}{k+1} \hat{s}_{k-1}[n] + \frac{1}{k+1} y_k[n + \hat{n}_{d_k}] \exp\left(-j2\pi \hat{f}_{D_k} n\right) \\ &= \frac{1}{k+1} \left[\hat{s}_{\text{acq}_i}[n] + \sum_{m=1}^{k} y_m[n + \hat{n}_{d_m}] \exp\left(-j2\pi \hat{f}_{D_m} n\right) \right], \end{aligned} \tag{2.22}$$

where $\hat{n}_{d_m} \triangleq \left\lfloor \frac{\hat{t}_{s_m}}{T_s} \right\rceil$ and $\lfloor \cdot \rceil$ denotes rounding to the closest integer.

2.3.2.2 PLL

The PLL consists of a phase discriminator, a loop filter, and a numerically-controlled oscillator (NCO). It was found that the receiver could easily track the carrier phase with a second-order PLL with a loop filter transfer function

$$F_{\text{PLL}}(s) = \frac{2\kappa\omega_n s + \omega_n^2}{s}, \tag{2.23}$$

where $\kappa \equiv \frac{1}{\sqrt{2}}$ is the damping ratio and ω_n is the undamped natural frequency, which can be related to the PLL noise-equivalent bandwidth $B_{n,\text{PLL}}$ by $B_{n,\text{PLL}} = \frac{\omega_n}{8\zeta}(4\zeta^2+1)$ [131]. The loop filter transfer function in (6.35) is discretized at a sampling period $T_{\text{sub}} \triangleq LT_s$, which is the time interval at which the loop filters are updated and is typically known as the subaccumulation interval. The discretized transfer function is realized in state-space. The output of the loop filter at time-step k, denoted by $v_{\text{PLL},k}$, is the rate of change of the carrier phase error, expressed in rad/s. The Doppler frequency estimate at time-step k is deduced by dividing $v_{\text{PLL},k}$ by 2π. The loop filter transfer function in (6.35) is discretized and realized in state-space. The noise-equivalent bandwidth is chosen to range between 4 and 8 Hz. The carrier phase estimate at time-step k is updated according to

$$\hat{\theta}_k = \hat{\theta}_{k-1} + v_{\text{PLL}} \cdot T_{\text{sub}}, \tag{2.24}$$

where $\hat{\theta}_0 \equiv 0$. A measure of the change in distance between the transmitter and receiver can be formed from the carrier phase as $z(k) = -\frac{c}{2\pi f_c}\hat{\theta}_k$, where c is the speed-of-light and f_c is the carrier frequency. The term z is typically referred to as the carrier phase expressed in meters. The model relating z to the receiver's position is discussed in Subsection 2.4.2.

2.3.2.3 DLL

The carrier-aided DLL employs an early-minus-late discriminator. The early and late correlations at time-step k used in the discriminator are denoted by Z_{e_k} and Z_{l_k}, respectively, which are calculated by correlating the received signal with an early and a delayed version of the estimated RS, respectively. The time shift between Z_{e_k} and Z_{l_k} is defined as the early-minus-late time, denoted by ξ. The DLL loop filter is a simple gain K_{DLL}, with a noise-equivalent bandwidth $B_{n,\text{DLL}} = \frac{K_{\text{DLL}}}{4} \equiv 0.5$ Hz. The output of the DLL loop filter

v_{DLL} is the rate of change of the code phase, expressed in s/s. Assuming low-side mixing at the radio frequency front-end, the code phase estimate is updated according to

$$\hat{t}_{s_{k+1}} = \hat{t}_{s_k} - \left(v_{\mathrm{DLL},k} + \frac{v_{\mathrm{PLL},k}}{2\pi f_c} \right) \cdot T_{\mathrm{sub}}. \tag{2.25}$$

The code phase estimate can be used to readily deduce the pseudorange observables.

2.4 Experimental Results

This section validates the proposed CON receiver experimentally. To this end, three experiments are conducted: (i) an experiment on a ground vehicle with real 5G NR signals, (ii) an experiment on UAV with real 5G NR signals, and (iii) an experiment on UAV with real 4G LTE signals. The objective of these experiments are to: (i) validate the signal model, (ii) evaluate the acquisition and tracking performance of the CON receiver, (iii) demonstrate the capability of detecting multiple sources, i.e., gNBs in 5G and eNodeBs in LTE, transmitting on the same carrier frequency, (iv) showcase the navigation solution obtained via the CON receiver, (iv) and evaluate the navigation performance of the CON receiver in a scenario where the RSs are always-on and compare it to the navigation solution obtained with a conventional opportunistic navigation receiver which has complete knowledge of the RSs. The parameters considered in the experiments are listed in Table 2.1.

2.4.1 CON with Real 5G Signals: Comparison with a Conventional 5G Receiver on a Ground Vehicle

The first experiment aims to compare the acquisition and tracking performance of the CON receiver with the conventional 5G receiver [185] which only relies on the always-on

Table 2.1: Receiver parameters

Parameter	LTE	5G
Carrier frequency	1955, 2145, 2125, and 739 MHz [184]	632.55, and 872 MHz [9]
Sampling rate	10 MHz	10 MHz
η	1.012 for $P_{fa} = 10^{-4}$ (21)	1.007 for $P_{fa} = 10^{-4}$ (21)
$B_{n,\text{PLL}}$	4-8 Hz (empirically)	4-8 Hz (empirically)
$B_{n,\text{DLL}}$	0.5 Hz (empirically)	0.5 Hz (empirically)
T_{sub}	10 ms [184]	20 ms [9]
K	40 (empirically)	40 (empirically)

RSs. The experimental setup and results for the experiment with real 5G NR signals are discussed next.

2.4.1.1 Experimental Setup and Environmental Layout

In this experiment, a ground vehicle was equipped with a quad-channel National Instrument (NI) universal software radio peripheral (USRP)-2955 and four consumer grade 800/1900 MHz cellular antennas to sample 5G signals near Fairview Road in Costa Mesa, California, USA. Only one channel from the USRP was used and was tuned to a 872 MHz carrier frequency, which is a 5G NR frequency allocated to the U.S. cellular provider AT&T. The sampling rate was set to 10 Mega-samples per second (MSps) and the sampled 5G signals were stored on a laptop for post-processing. In order to obtain ground-truth, the vehicle was equipped with a Septentrio AsteRx-i V GNSS-aided inertial navigation system (INS), which is a dual antenna, multi-frequency GNSS receiver with real-time kinematics (RTK) capabilities. The GNSS receiver is coupled with a Vectornav VN-100 micro electromechanical systems (MEMS) inertial measurement unit (IMU) to estimate the position

and orientation of the ground vehicle at a rated horizontal accuracy of 0.6 cm in clear sky conditions (RTK performance). The vehicle traversed a trajectory of 4.1 km in 315 seconds. Fig. 2.2 shows the environment layout and the vehicle trajectory. The acquisition results are presented next.

Figure 2.2: Experimental setup and vehicle trajectory for the 5G NR experiment with ground vehicle.

2.4.1.2 Signal Model Validation

The signal model (4.1) considers a channel with a single tap, which corresponds to the LOS path with an arbitrary complex channel gain α_i. In other words, the channel is modeled as $h_i[n] = \alpha_i \delta[n - \lfloor t_{s_i}[n] \rceil]$, where α_i is the complex channel gain between the ith gNB and the UE, $t_{s_i}[n]$ is the code-delay corresponding to the UE and the ith gNB, and $\lfloor \cdot \rceil$ is the rounding operation to the closest integer. Note that this channel models flat fading, where multiple received "close" signal paths are combined into a single α_i. To justify the signal

model in the tested scenario, two test points are considered for the ground vehicle (see Fig. 2.3(a)). In this figure, the term *clear LOS* refers to a scenario where the signal is not blocked by an obstacle, e.g., a building. The two test points, i.e., receiver location 1 and receiver location 2, are considered based on the existence of the clear LOS with respect to the 5G gNB. Receiver location 1 has a clear LOS and is also closer to the gNB. On the other hand, receiver location 2 is blocked by a building and does not have a clear LOS. The magnitude of the channel impulse response for both locations are plotted in Fig. 2.3(b). The magnitudes of the channel impulse responses are estimated by reconstructing the frame as described in [9]. As it can be seen in this figure, the channel impulse response for receiver location 2 is weaker than that of receiver location 1 which is due to blockage of the signal by an obstacle. The complex channel gain in (4.1) captures this effect by attenuating the LOS signal. If the acquisition of a gNB is performed when the receiver does not have a clear LOS, e.g., receiver location 2, the detection performance will be degraded, which in turn affects the tracking performance. Fig. 2.4 demonstrates the likelihood at the first stage of acquisition for receiver location 1 and 2. As can be seen in Fig. 2.4, the likelihood is degraded at receiver location 2 due to signal blockage. Note that in both receiver locations, $|h(\tau)|$ does not exhibit multiple taps (i.e., $h_i[n] = \sum_{j=1}^{M} \alpha_{i,j}\delta[n - \lfloor t_{s_{i,j}}[n] \rceil]$, where M is the number of paths), which corresponds to the impulse response of a frequency selective channel. While the considered signal model is simple, yet valid for the conducted experiments, more sophisticated channel models, e.g., frequency selective channels, can be considered in future work [206].

2.4.1.3 Acquisition Results

The recorded 5G signals were processed in two ways for comparison: (i) using the proposed CON receiver and (ii) using the conventional 5G receiver proposed in [185]. The

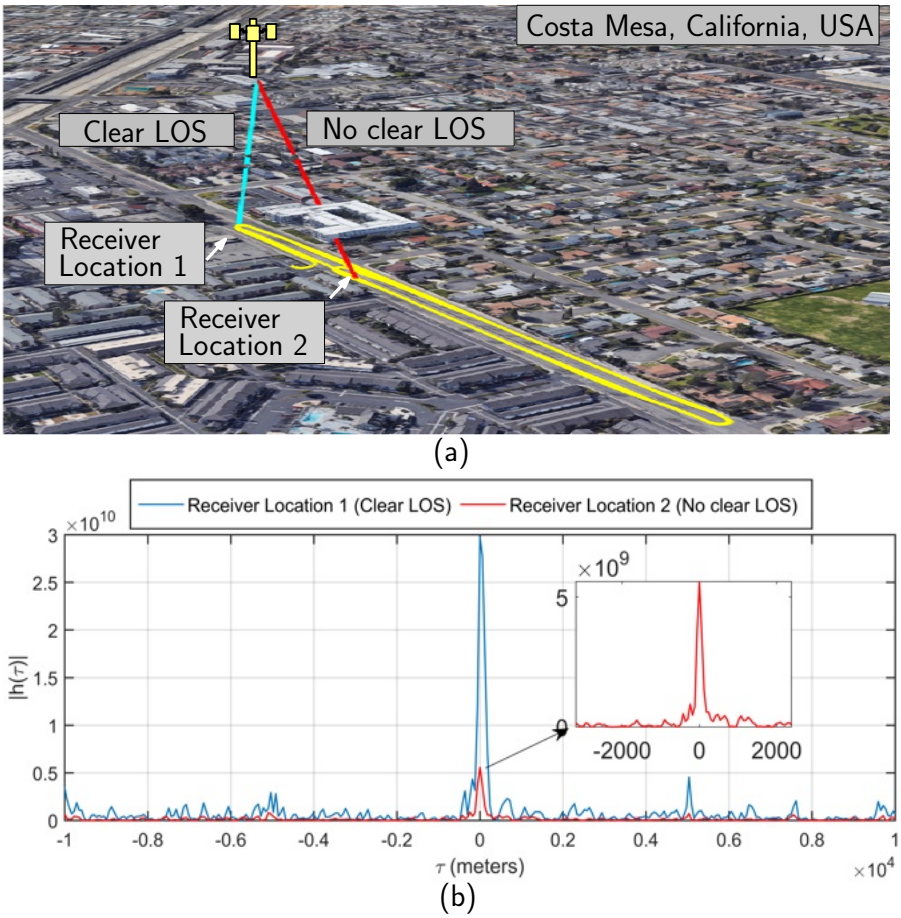


Figure 2.3: (a) Receiver locations for two cases: with and without clear LOS. (b) Channel impulse response at the two receiver locations.

conventional 5G receiver detected 1 gNB with an initial Doppler frequency of -7.2 Hz. Note that the limited number of gNBs was expected as 5G gNBs are sparsely deployed at the present time. The location of the gNB was mapped prior to the experiment. Next, the signal acquisition stage was applied to detect the ambient 5G gNB. The detection threshold was set such that $P_{\text{fa}} = 10^{-4}$, which yielded $\eta = 1.008$, K was set to 40, and T_{sub} was set to 20 ms. Doppler estimation was performed by searching for the maximizer of the likelihood function according to (6.5) with a step size of 1 Hz. The acquisition stages in the CON receiver is shown in Fig. 2.5. As it can be seen in this figure, in the first stage of the acquisition, one

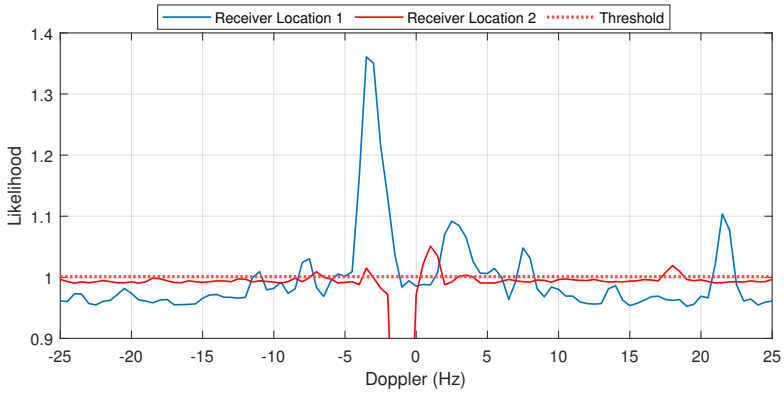


Figure 2.4: The likelihood (5.10) calculated at receiver location 1 and 2 for $i = 1$ demonstrates that no clear line of sight dramatically degrades the likelihood function.

gNB is detected at frequency -7 Hz. In the second stage, the Doppler subspace of this gNB is nulled and the resulting likelihood is less than the threshold for all Doppler frequencies. This implies that, no other gNBs are detected in the second stage of the acquisition or equivalently $\hat{N} = 1$.

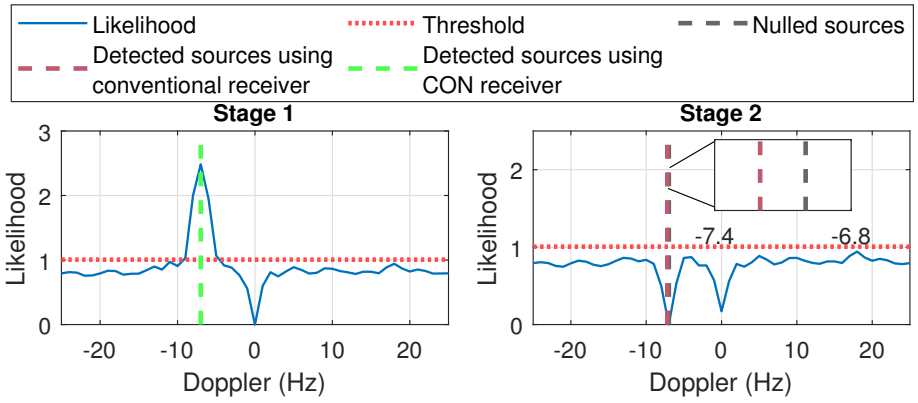


Figure 2.5: Acquisition stages in the CON receiver for 5G NR signals on a ground vehicle showing the likelihood function at each stage and the detected and nulled sources. The DC component, i.e., at zero Doppler frequency, was nulled as it was saturating the detector.

2.4.1.4 Tracking Results

After acquiring the Doppler and RSs, the tracking loops are initialized and the signal is tracked. Fig. 2.6 show the resulting Doppler frequency and delay, expressed in meters, obtained using the CON and conventional receivers. As it can be seen in Fig. 2.6(b) the estimated delays for the CON and the conventional receivers are slightly drifting away from the ground-truth which is due to the clock drifts. The effect of clock drift is considered in the carrier phase model (see equation (2.26)). Note that the initial value of the delays were subtracted out to facilitate comparison. The Doppler and delay RMSE values were calculated from ground-truth for both receivers and are summarized in Table 2.2, which shows that the CON receiver outperforms the conventional one.

A main reason behind the CON receiver performing better than a conventional 5G receiver is that the former exploits the RSs in the entire bandwidth, making the bandwidth of estimated RS higher than the RSs used in the conventional receiver (mainly, PSS and SSS). Fig. 2.7 shows this: the normalized autocorrelation function of the RS estimated with the CON receiver is narrower than that of a 5G PSS.

Table 2.2: Delay and Doppler RMSE for the CON and conventional receivers.

	Delay RMSE (m)	Doppler RMSE (Hz)
Conventional	24.33	3.66
CON	21.88	2.28

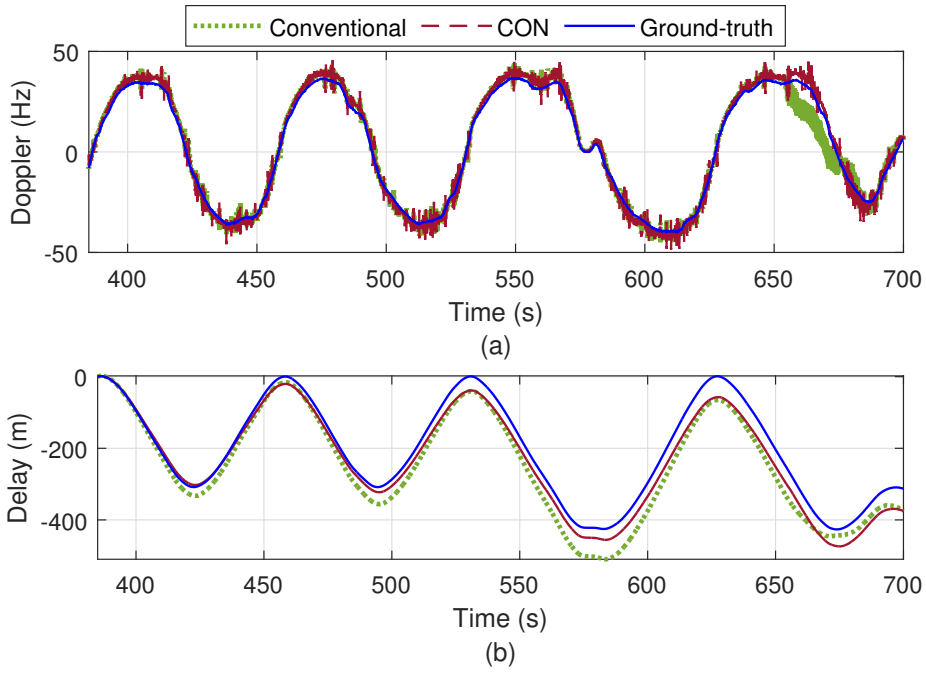


Figure 2.6: (a) Doppler tracking and (b) delay tracking results for the 5G NR ground vehicle experiment. The ground-truth is calculated according to the true position of the vehicle and the gNBs.

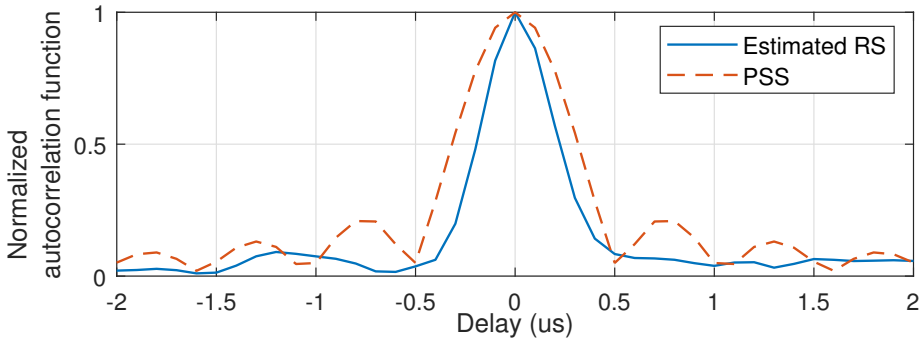


Figure 2.7: Normalized autocorrelation function of the RS estimated with the CON receiver compared to that of a 5G PSS.

Remark 3: The conventional and the proposed cognitive methods use tracking loops which involve the same computational complexity. The main difference between the computational complexity of the proposed cognitive receiver and a conventional receiver stems

from the acquisition stage. The number of complex operations is considered as a metric for computational complexity. In the likelihood function (5.10), the size of the projection matrices increases with the detection stage, i.e., i. However, in [91] (Appendix 8B), a recursive formula is provided to calculate the projection matrix at the ith stage based on the already calculated projection matrix at $(i-1)$th stage. Using the recursive formula presented in this appendix, the complexity of the projection matrix is $\mathcal{O}(K^2)$ where $\mathcal{O}(\cdot)$ denotes the rate of growth of a function, i.e., its order. Consequently, the number of complex operations to calculate the matched subspace detector is $\mathcal{O}((5(KL)^2+KL)N)$.

2.4.2 CON with real 5G signals: The First Navigation Results on a UAV

The second experiment aims to find a navigation solution on a UAV using the CON receiver. To the best of author's knowledge this is the first navigation results with real 5G signals on a UAV.

2.4.2.1 Experimental Setup and Environment Layout

In this experiment, the navigator was an Autel Robotics X-Star Premium UAV equipped with a single-channel Ettus 312 USRP connected to a consumer-grade 800/1900 MHz cellular antenna and a small consumer-grade GPS antenna to discipline the on-board oscillator. The cellular receivers were tuned to the cellular carrier frequency 632.55 MHz, which is a 5G NR frequency allocated to the U.S. cellular provider T-Mobile. Samples of the received signals were stored for off-line post-processing. The ground-truth reference trajectory was taken from the on-board Ettus 312 USRP GPS solution. The UAV traversed a trajectory of

416 m. Fig. 3.9 shows the environment layout and the vehicle trajectory. The acquisition results are presented next.

Figure 2.8: Environment layout and UAV trajectory for the 5G NR UAV experiment.

2.4.2.2 Acquisition Results

Next, the signal acquisition stage was applied to detect the ambient 5G gNBs. The CON 5G receiver detected 2 gNBs with initial Doppler frequencies of 3.5 Hz and 11.5 Hz. The location of the gNBs was mapped prior to the experiment. The acquisition stages in the CON receiver are shown in Fig. 2.9.

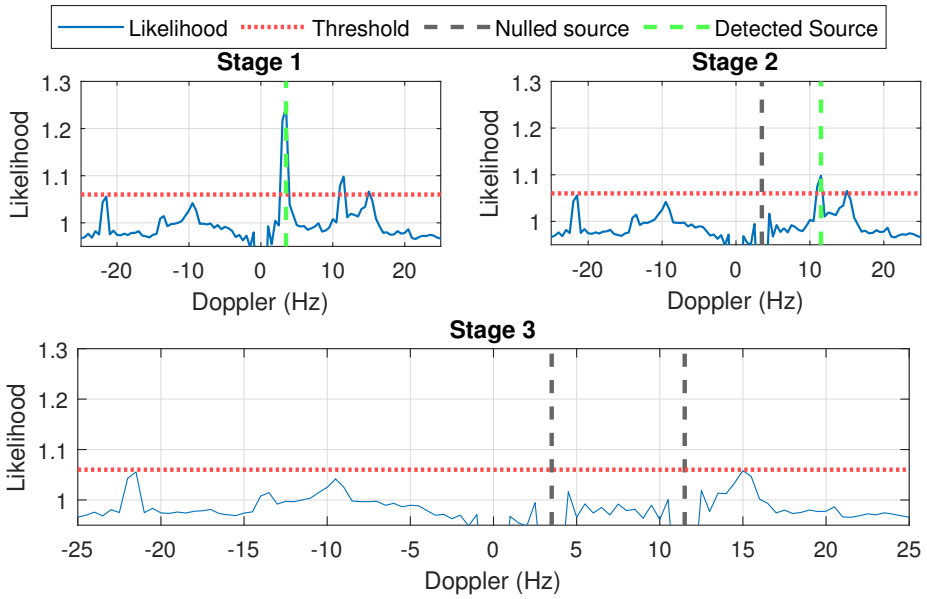


Figure 2.9: Acquisition stages in the CON receiver for 5G NR signals on a UAV showing the likelihood function at each stage and the detected and nulled sources. The DC component, i.e., at zero Doppler frequency, was nulled as it was saturating the detector.

2.4.2.3 Tracking Results

After acquiring the Doppler and the RSs, the tracking loops are initialized and the signal is tracked. Fig. 2.10 shows the resulting Doppler frequencies and delays, expressed in meters, obtained using the CON receiver.

2.4.2.4 Navigation Solution

In the following, it is assumed that (i) the UAV's altitude is known at all time and (ii) the UAV has an estimate of its position at time-step k_0, prior to navigating with 5G signals. The carrier phase to the i-th gNB $z_i(k)$ at time-step k expressed in meters can be modeled as

$$z_i(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_i}\| + c\delta t_r(k) - c\delta t_{s_i} + v_i(k), \tag{2.26}$$

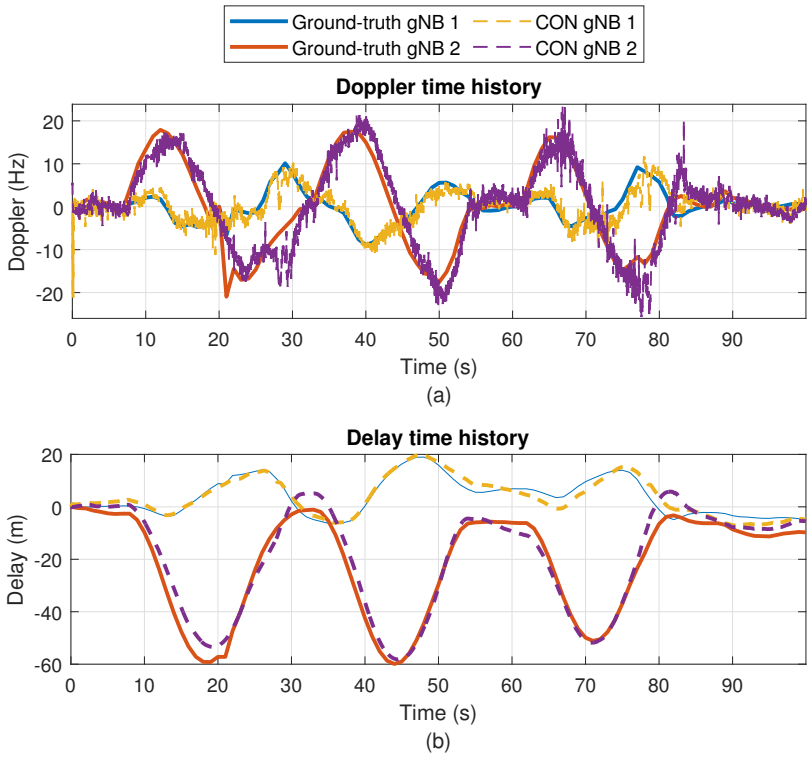


Figure 2.10: (a) Doppler tracking and (b) delay tracking results for the UAV 5G experiment. The ground-truth is calculated according to the true position of the vehicle and the gNBs.

where $\boldsymbol{r}_r$ and $\boldsymbol{r}_{s_i}$ are the three-dimensional (3–D) position vectors of the UAV-mounted receiver and the i-th gNB, respectively; c is the speed of light; δt_r is the UAV-mounted receiver's clock bias; δt_{s_i} models the i-th gNB's clock bias and carrier phase ambiguity; and $v_i(k)$ is the measurement noise, which is modeled as a zero-mean Gaussian random variable with variance σ_i^2 [183]. Note that since the UAV's altitude is known, e.g., using an altimeter, only its two-dimensional (2–D) position is estimated. The time reference for the transmitter and receiver clocks is chosen such that $\delta t_r(k_0) = 0$. Using the position estimate at k_0 and the fact that $\delta t_r(k_0) = 0$, the gNBs clock biases can be estimated from $z_i(k_0)$ resulting in the estimate $\hat{\delta} t_{s_i}$. Next, define the corrected carrier phase measurement $\bar{z}_i(k) \triangleq z_i(k) + \hat{\delta} t_{s_i}$

which can be approximated as

$$\bar{z}_i(k) \approx \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_i}\| + c\delta t_r(k) + v_i(k), \quad \forall k > k_0. \tag{2.27}$$

Subsequently, the corrected carrier phase measurements were fed to an extended Kalman filter (EKF) to solve the state vector $\boldsymbol{x}(k) \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}(k), \dot{\boldsymbol{r}}_r^{\mathsf{T}}(k), c\delta t_r(k), c\dot{\delta} t_r(k)\right]^{\mathsf{T}}$, where $\dot{\boldsymbol{r}}_r(k)$ is the UAV's 2–D velocity vector and $\dot{\delta} t_r(k)$ is the receiver's clock drift. A nearly constant velocity model was used for the UAV's position and velocity dynamics, and a standard double integrator driven by process noise was used to model the clock bias and drift dynamics [77]. As such, the discrete-time dynamics model of $\boldsymbol{x}$ are given by

$$\boldsymbol{x}(k+1) = \mathbf{F}\boldsymbol{x}(k) + \boldsymbol{w}(k), \tag{2.28}$$

where $\mathbf{F}$ is the state transition matrix obtained according to [77] and $\boldsymbol{w}(k)$ is the process noise vector, which is modeled as a zero-mean Gaussian random vector with covariance matrix $\mathbf{Q}$ obtained according to [77]. The UAV's x, y acceleration process noise spectra in the nearly constant velocity model were set to $q_x = q_y = 10$ m^2/s^5, and the receiver's clock process noise was chosen to be that of a typical temperature-compensated crystal oscillator (TCXO) [76, 159]. Note that $\boldsymbol{r}_r(k)$ is expressed in an East-North-Up (ENU) frame centered at the UAV's true initial position. The EKF state estimate was initialized at $\hat{\boldsymbol{x}} = \boldsymbol{R}_{6\times 1}$ with an initial covariance of $4 \cdot \mathbf{I}_{6\times 6}$. The measurement noise covariance was set to $\mathbf{R} = 2 \cdot \mathbf{I}_{2\times 2}$. The position RMSE of the UAV was calculated to be 4.35 m with the aforementioned parameters. The true and estimated UAV trajectories are shown in Fig. 2.11.

2.4.2.5 Effect of False Alarm

The effect of a false alarm on the performance of the tracking loops is assessed next. It will be demonstrated that if at the acquisition stage a false alarm happens and a gNB

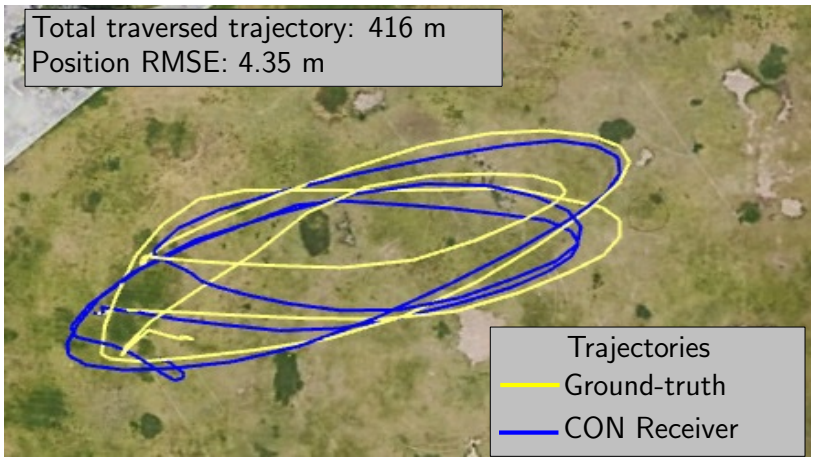


Figure 2.11: Ground-truth and estimated trajectories using CON receiver for 5G NR signals on a UAV. The CON receiver yielded a UAV position RMSE of 4.35 m. Map data: Google Earth.

is mistakenly detected, the carrier phase error will not converge in the tracking loops. In this case, the proposed method should neglect the detected source. To demonstrate this experimentally, Fig. 2.12 plots the likelihood function. In this experiment, the acquisition stage is forced to detect a false alarm, i.e., the acquisition stage is confirming the existence of a source which does not exist. Fig. 2.13 demonstrates the carrier phase error for the valid gNB and the false alarm gNB. As it can be seen in Fig. 2.13, the carrier phase error for the valid gNB converges whereas the carrier phase error for the false alarm is not. It should also be noted that P_{fa} can be selected based on the operating environments.

2.4.3 CON with LTE Signals: Comparing with a Conventional Receiver when the RSs are always-on

This experiment was conducted with real LTE signals on a UAV to (i) compare the navigation performance with a receiver which exploits all the available RSs in a scenario where the RSs are always-on, and (ii) to evaluate the performance of the CON receiver in

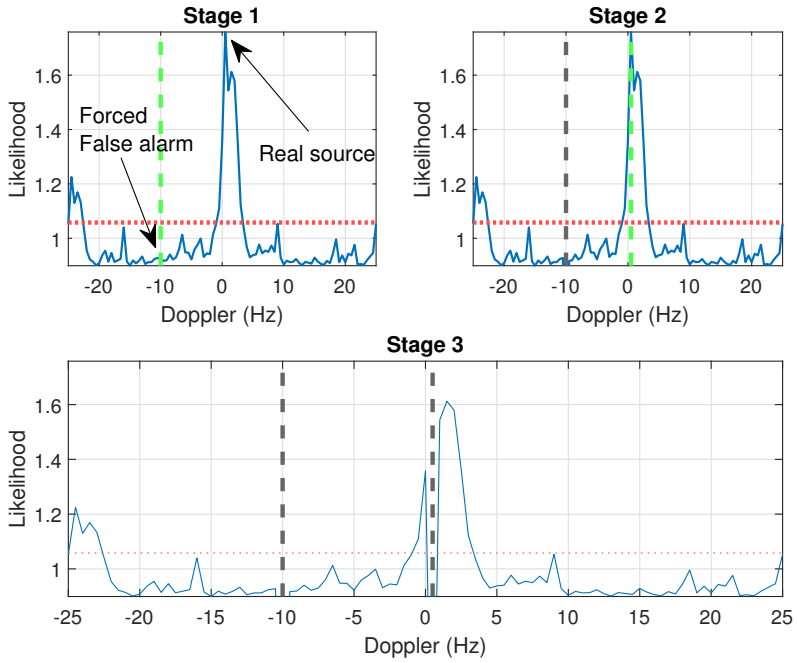


Figure 2.12: Likelihood function for the UAV 5G experiment: In stage 1, a non-existent source at a corresponding Doppler of -10 Hz was fictitiously induced to pass the threshold (i.e., forced false alarm). In stage 2, this fictitious source is nulled and a valid source of 0 Hz is detected.

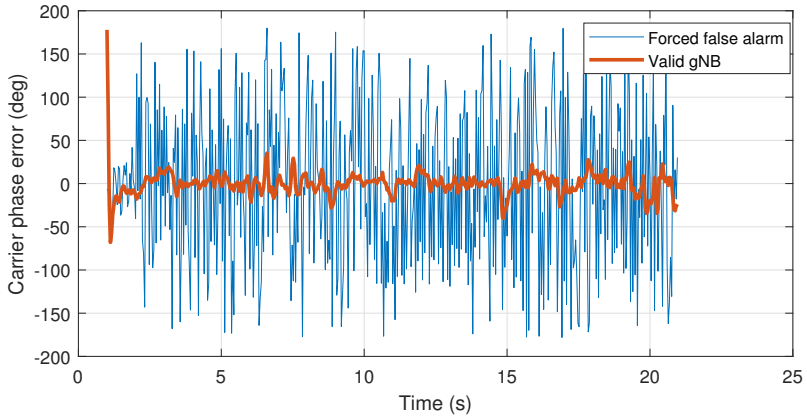


Figure 2.13: Carrier phase error for a valid gNB (at 0 Hz) and a forced false alarm gNB (at -10 Hz) shown in Fig 2.12.

an environment with multiple LTE eNodeBs operating in the same carrier frequency. The experimental setup and results are discussed next.

2.4.3.1 Experimental Setup

In this experiment, a DJI Matrice 600 UAV was equipped with the NI USRP-2955 and four consumer grade 800/1900 MHz cellular antennas to sample LTE signals near Aliso Viejo, California, USA. The channels of the USRP were tuned to 1955, 2145, 2125, and 739 MHz carrier frequencies, respectively, which are 4G LTE frequencies allocated to the U.S. cellular providers AT&T, T-Mobile, and Verizon. The sampling rate for each channel was set to 10 MSps and the sampled LTE signals were stored on a laptop for post-processing. The UAV was equipped with the same Septentrio GNSS-aided INS described in Subsection 2.4.1 for ground-truth.

2.4.3.2 Acquisition Results

The recorded LTE signals were processed in two ways for comparison: (i) using the proposed CON receiver and (ii) using the conventional LTE receiver developed in [182]. The conventional LTE receiver detected 11 eNodeBs over the 4 channels. The locations of the eNodeBs were mapped prior to the experiment and are shown in Fig. 2.14.

Next, the signal acquisition stage was applied to detect the ambient LTE eNodeBs. The detection threshold was set such that $P_{\text{fa}_i} = 10^{-4}$, which yielded $\eta_i = 1.012$, K was set to 40, and T_{sub} was set to 10 ms for all i. Doppler estimation was performed in a similar as the previous experiment. The acquisition stages for the 1955 MHz carrier frequency are shown in Fig. 2.15. In particular, Fig. 2.15 shows how the likelihood function changes as sources

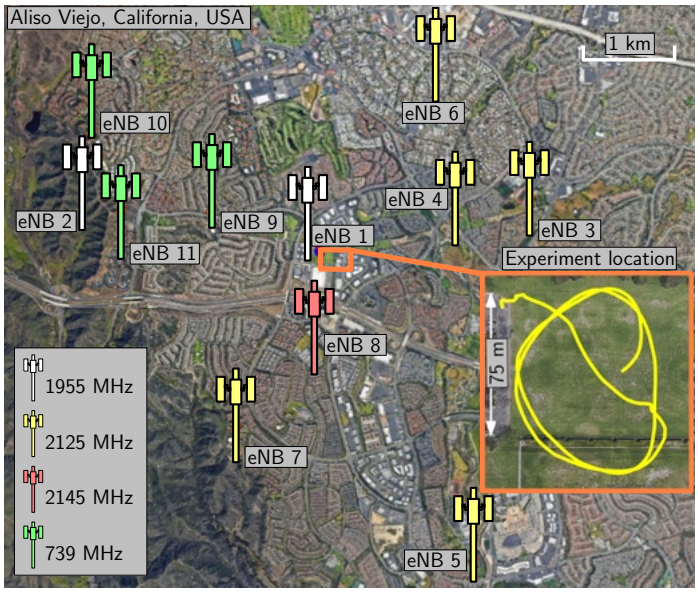


Figure 2.14: Layout of eNodeBs and UAV trajectory for the 4G LTE experiment.

are detected and nulled by the CON receiver. The conventional LTE receiver detected two eNodeBs at the 1955 MHz carrier frequency, denoted by eNodeB 1 and eNodeB 2 in Fig. 2.14, with eNodeB 1 having a Doppler frequency of -18.5 Hz and eNodeB 2 having a Doppler frequency of -17.5 Hz. The CON receiver detected 3 eNodeBs at the 1955 MHz carrier frequency with Doppler frequencies -22 Hz, -18, and 18 Hz. The eNodeBs detected by the CON receiver were manually associated with the ones detected by the conventional receiver by matching the Doppler and delay profiles. Sophisticated data association techniques could be employed to perform this step; however, it is out of the scope of the current chapter. After performing data association, it was found that only one of the Doppler frequencies detected by the CON receiver pertains to the ones detected by the conventional LTE receiver. Specifically, the CON receiver detected eNodeB 1 at a -18 Hz Doppler frequency, which is 0.5 Hz off from the one estimated by the conventional receiver. This error is due to the 1 Hz step size used in the Doppler search. For $K = 40$, the

condition from Theorem 1 for the CON receiver to be able to distinguish between eNodeB 1 and eNodeB 2 at the specified $P_{\text{fa}_i} = 10^{-4}$ is that the difference between their Doppler frequencies must be greater than 1.25 Hz. However, the Doppler frequency difference between eNodeB 1 and 2 measured by the conventional receiver is 1 Hz which violates the aforementioned condition. This direct consequence of Theorem 1 explains why the CON receiver could not detect eNodeB 2. Similar acquisition results are obtained with the remaining carrier frequencies. A total of 11 eNodeBs were acquired by the CON receiver. After manual data association, it is found that only 6 of them pertain to the ones detected by the conventional receiver (eNodeBs 1, 4, 5, 7, 8, and 10) and the rest pertain to unknown eNodeBs that were not detected by the conventional receiver.

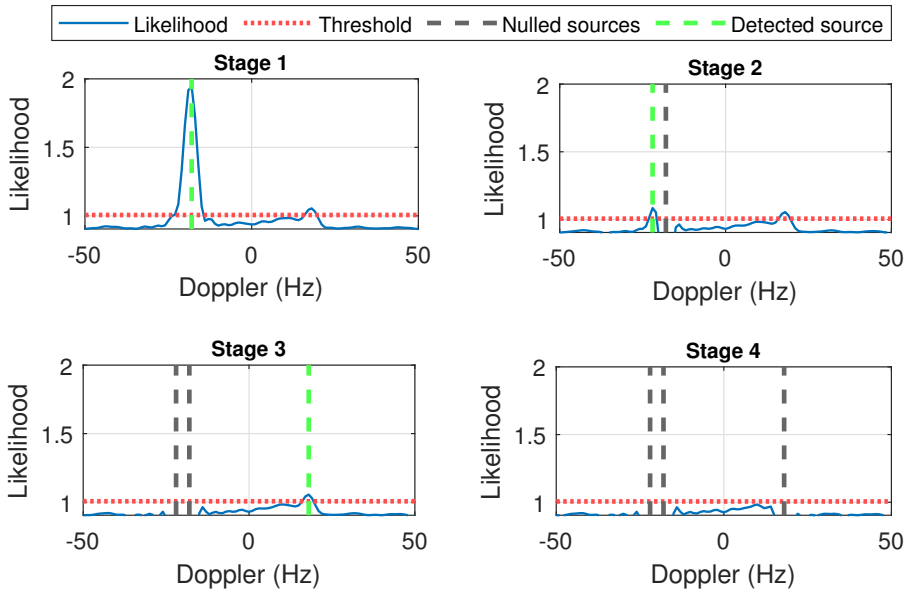


Figure 2.15: Acquisition stages for the 1955 MHz carrier frequency showing the likelihood function at each stage and the detected and nulled sources.

2.4.3.3 Tracking Results

After acquiring the Doppler frequencies and the RSs, the tracking loops are initialized and the signals are tracked. Fig. 2.16 shows the resulting carrier phases, expressed in meters, obtained using the CON and conventional receivers for the eNodeBs acquired on the 1955 MHz carrier frequency. The carrier phase expressed in meters is a smoother estimate of the true range than the RS delays. The subsequent analyses focus on carrier phase measurements since they will be used to compute the navigation solution. The carrier phase RMSE values are summarized in Table 2.3. Note that eNodeBs 2, 3, 6, 9, and 11 are not included in Table 2.3 since they were not detected by the CON receiver; however, as mentioned previously, the CON receiver acquired and tracked 5 unknown eNodeBs that were not detected by the conventional LTE receiver. One example is shown in Fig. 2.16. For fair comparison, only the common eNodeBs will be used to compute a navigation solution.

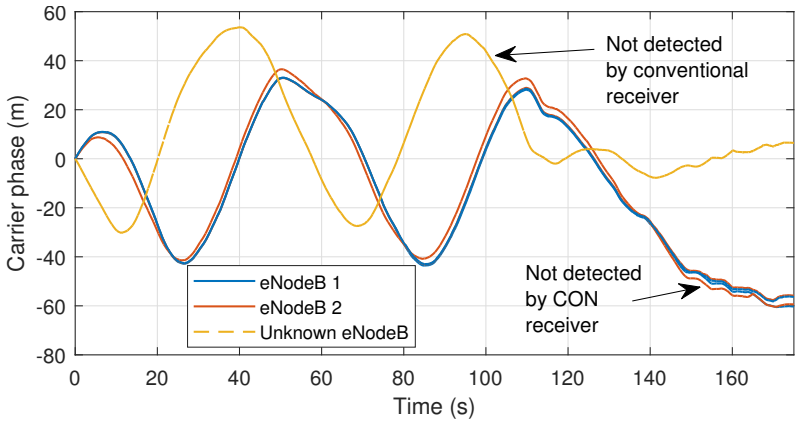


Figure 2.16: Tracking results showing the carrier phase, expressed in meters, obtained from the CON and conventional receivers for the 1955 MHz carrier frequency. Solid lines represent the carrier phases tracked by the conventional receiver while the dashed lines represent the ones tracked by the CON receiver.

Table 2.3: Carrier phase RMSE between the CON and conventional LTE receivers and ground-truth.

eNodeB	1	4	5	7	8	10
CON RMSE (m)	3.34	3.00	2.80	2.37	2.85	5.13
Conventional RMSE (m)	3.39	2.52	2.70	2.92	2.84	3.40

2.4.3.4 Navigation Solution

The navigation framework discussed in Subsection 2.4.1 is employed to compute the UAV's 2–D position from the navigation observables produced by the CON and conventional receivers. Two position estimates were calculated using six carrier phase measurements from the eNodeBs in Table 2.3: (i) for the conventional receiver and (ii) for the CON receiver. The position RMSE of the conventional and CON receivers were both calculated to be 2.07 m. The true and estimated UAV trajectories are shown in Fig. 2.17.

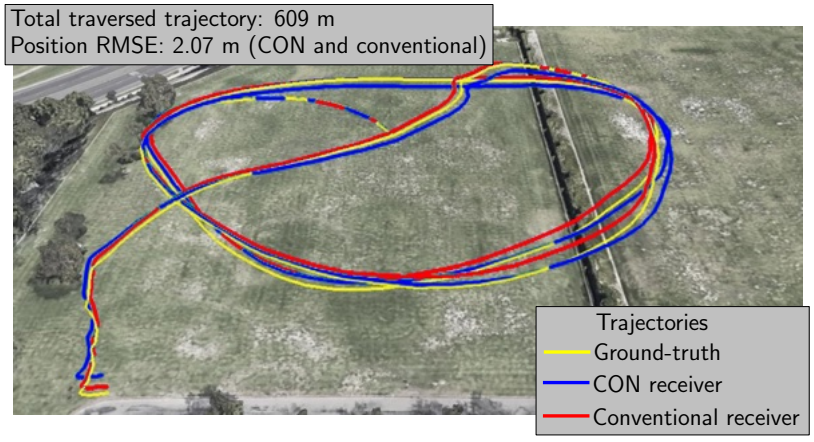


Figure 2.17: Ground-truth and estimated trajectories using CON and a conventional LTE receivers. Both approaches yielded a UAV position RMSE of 2.07 m. Map data: Google Earth.

Chapter 3: Cognitive Detection of Unknown Beacons of Terrestrial Signals of Opportunity for Localization

3.1 Introduction

Global navigation satellite system (GNSS) signals suffer from constraining limitations in deep urban environments and are prone to jamming and spoofing. In spite of these limitations, we live in a world rich with man-made signals of opportunity (SOPs), which have been demonstrated as feasible complements or alternatives to GNSS in challenging environments [80]. SOP navigation receivers typically rely on known synchronization sequences or beacons transmitted by SOP sources to draw time-of-arrival (TOA), direction-of-arrival (DOA), and frequency-of-arrival (FOA) measurements [47, 156, 184, 228].

Cognitive opportunistic navigation [149] has been recently introduced to addresses the following challenges of navigation with SOPs:

Unknown reference signals in private networks: Opportunistic navigation frameworks usually rely on the broadcast reference signals (RSs), which are used to derive DOA and TOA [184]. For public networks, these signals are known at the user equipment (UE) and are universal across network operators. Hence, they can be exploited for positioning

without the need for the UE to be a network subscriber. However, in *private networks*, the signal specifications of some SOP sources may not be available to the public, which makes acquiring and tracking these signals impossible for conventional opportunistic navigation receivers [149]. Private networks and broadband providers do not usually disclose the transmitted signal structure to protect their intellectual property. For instance, very limited information is available about Starlink satellite signals.

Dynamic nature and ultra-lean transmission of the fifth-generation (5G) new radio (NR) and beyond networks: In cellular long-term evolution (LTE) networks, several RSs, such as the cell-specific reference signal (CRS), are broadcast at regular and known time intervals, regardless of the number of UEs in the environments. This *always-on* type of transmitted RSs reduces the network's energy efficiency and increases operational expenses and interference. One of the main features of 5G NR, is ultra-lean transmission, which minimizes the transmission of always-on signals. For instance, CRS which used to be an always-on RS in LTE, is not necessarily being continuously transmitted in 5G signals. On the other hand, the RSs in 5G networks and beyond can be dynamic and may continuously change [158]. As such, designing cognitive receivers that can cognitively acquire *partially known*, *unknown*, or *dynamic* beacon signals is an emerging need for the future of cognitive navigation [104, 144, 145, 149] [†].

This dissertation considers a cognitive opportunistic approach to detect the unknown beacon of terrestrial SOPs to enable exploitation of these signals for positioning and navigation purposes. Two scenarios are considered: (i) unknown beacon signals with integer

[†]In this dissertation, only the length of the beacon signals is assumed to be known at the receiver. It should be pointed out that period estimation techniques, e.g., [33], can be used to estimate the length of the beacon sequence in a preprocessing stage.

constraints (IC) on the symbols of the beacon, and (ii) unknown beacon signals with no integer constraints (NIC). An example of beacons with IC is pseudo-noise (PN) sequences in cellular code division multiple access (CDMA), while an example of beacons with NIC are the RSs in orthogonal frequency-division multiplexing (OFDM)-based systems. Since the symbols of PN sequences in CDMA signals are drawn from a set with a finite alphabet size, e.g., phase shift keying (PSK) set, they can be categorized as beacons with IC. On the other hand, the RSs in OFDM-based systems, e.g., secondary synchronization signal (SSS) in cellular LTE and 5G NR, are arbitrary complex numbers in the time domain and, therefore, can be categorized as beacon signals with NIC.

The main contributions of this dissertation are as follows:

- A cognitive opportunistic navigation method is proposed, whereby unknown beacons of terrestrial SOPs are detected, enabling exploitation of these signals for navigation purposes. To this end, matched subspace detectors are implemented practically for two different scenarios: (i) beacons with IC, e.g., the symbols of the beacon are drawn from M-ary PSK (MPSK) modulation set, and (ii) beacon with NIC, i.e., the beacon signal are not constrained to take integer values and can assume any arbitrary complex-valued number.

- A near-optimal algorithm which has a lower computational complexity compared to the traditional detectors with IC is proposed. The effect of the symbol errors in the detected beacon signal on the carrier-to-noise ratio (CNR) is characterized analytically. The proposed matched subspace detectors are shown to be capable of detecting multiple unknown real 5G NR and 3G signals with a relatively low computational complexity.

- For the NIC scenario, closed-form expressions for the probability of detection and false alarm are derived. The effective signal to noise ratio (SNR) is calculated and the effect of Doppler estimation error on the performance of the detector is analyzed. It is shown that the coherence processing interval (CPI) can be selected optimally in the sense that it maximizes the probability of detection. The estimated CPI is shown to provide better estimation of the beacon signal in a practical scenario. To the best of the authors' knowledge, the estimation of CPI has not been previously studied in the literature.

- Experimental results are presented showing an application of the proposed cognitive approach by enabling an unmanned aerial vehicle (UAV) to detect and exploit terrestrial cellular signals for navigation purposes. In one experiment, the UAV achieved submeter-level accurate navigation over a trajectory of 1.72 km, by exploiting signals from four 3G cdma2000 transmitters. In another experiment, the UAV achieves a position root mean-squared error (RMSE) of 4.63 m over a trajectory of 416 m, by exploiting signals from two 5G transmitters. It should be pointed out that the number of currently active 5G transmitters are relatively lower than that of the previous generations. The 5G NR navigation results will be improved dramatically with more active 5G transmitters.

- The OFDM frame of 5G signals are reconstructed in a blind fashion. On-demand and always-on beacons are demonstrated in the OFDM signal structure of real 5G signals. To the best of the authors' knowledge, the blind reconstruction of the OFDM frame of 5G signals has not been done in any other work in the current literature.

The rest of this dissertation is organized as follows. Section 4.2 surveys relevant related work. Section 5.5 presents the received baseband signal model. Section 3.4 derives the generalized likelihood ratio (GLR) detector for beacons of terrestrial SOPs, when the elements of the beacons are drawn from MPSK modulation, while Section 3.5 analyzes the performance of the derived detector. Section 3.6 derives the GLR detector for beacons of terrestrial SOPs when the elements of the beacons are arbitrary complex numbers. Section 3.7 presents experimental results for cognitive detection of both beacons with IC and without NIC as well as an application of the proposed approach in the context of UAV navigation.

3.2 Related Work

3.3 Received Baseband Signal Model

Let $c(t)$ denote the beacon signal consisting of L consecutive symbols with symbol duration T_s. The beacon signal is continuously transmitted at a period of LT_s. After channel propagation and baseband sampling, the received signal can be modeled as

$$y[n] = \alpha \exp(j2\pi\Delta f n) \sum_{i=-\infty}^{\infty} c[n - iL - n_d] + w[n], \tag{3.1}$$

where $y[n]$ is the complex baseband sample at the nth time slot, $\Delta f \triangleq f_D T_s$ is the normalized Doppler frequency, f_D is the true Doppler frequency in Hz, $w[n]$ models noise and interference, n_d is the unknown delay of the received beacon signal, and α is an unknown complex amplitude. The periodic discrete-time beacon signal is defined as $s[n] = \sum_{i=-\infty}^{\infty} c[n - iL - n_d]$.

For convenience of notation, define the kth truncated vector of received samples of length L as

$$\mathbf{y}_k \triangleq [y[kL], y[kL+1], \ldots, y[(k+1)L-1]]^{\mathsf{T}}.$$

The analysis herein applies for a CPI of K consecutive beacon periods, in which Δf and α are assumed to be constant. Therefore, without loss of generality, k is limited to the set $\{0,1,\ldots,K-1\}$.

Considering a CPI of length KL samples, the observation vector can be constructed as $\mathbf{y} \triangleq [\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_K]^{\mathsf{T}}$. Consequently, the system model can be written as

$$\mathbf{y} = \alpha \mathbf{H}\mathbf{s} + \mathbf{w}_{\text{eq}}, \tag{3.2}$$

where, $\mathbf{s} = [s[1], \ldots, s[L]]^{\mathsf{T}}$, $\mathbf{w}_{\text{eq}}$ is the equivalent noise vector, and the $KL \times L$ Doppler matrix is defined as

$$\mathbf{H} \triangleq [\mathbf{D}, \exp(j2\pi\Delta f L)\mathbf{D}, \ldots, \exp(j2\pi\Delta f (K-1)L)\,\mathbf{D})]^{\mathsf{T}}, \tag{3.3}$$

where $\mathbf{D} \triangleq \text{diag}\{1, \exp(j2\pi\Delta f), \ldots, \exp(j2\pi(L-1)\Delta f)\}$ and $\text{diag}\{a, b, \ldots, c\}$ is a diagonal matrix with $a, b, \ldots, c$ on its diagonal elements.

Remark 1: In the signal model (6.38), the channel between the transmitter and the receiver is modeled as $h[n] = \alpha\delta[n - n_d]$, where α is the complex channel gain between the transmitter and the receiver and n_d is the corresponding code-delay. In other words, it is assumed that the channel has a single tap. This model assumes a scenario that a strong enough LOS component exists between the transmitter and the receiver. It will be shown in Section 3.7 that the considered signal model is valid for the conducted experiments in this dissertation. A frequency selective channel scenario (i.e., $h[n] = \sum_{j=1}^{M} \alpha_j \delta[n - n_{d_j}]$, where M is the number of paths) can be considered in future work.

3.4 Terresterial Signal Activity Detection with IC

In this section, GLR detector is derived to detect the beacon signals of terrestrial SOPs when the elements of the beacon $\mathbf{s}$ are drawn from MPSK modulation. One example of this type of beacons is the PN sequences in CDMA-based systems. Globalstar LEO satellites employ a 4PSK CDMA system. The spreading sequence structure is comprised of an inner PN sequence pair and an outer PN sequence which are drawn from 4PSK modulation scheme. Another example of this type of beacons is transmitted by Orbcomm satellites. The Orbcomm communication system utilizes the classic symmetric differential phase shift keying (SDPSK) as the modulation scheme for the downlink signals. The following Remark explains how (6.3) is descriptive of a CDMA-based system scenario.

Remark 2: In CDMA systems, several logical channels are multiplexed on the same physical channel. For example, there is a total of 128 logical channels multiplexed onto the cdma2000 physical forward channel: (i) one pilot channel, (ii) one sync channel, (iii) up to seven paging channels, and (iv) traffic on the remaining channels. Each of these logical channels is spread orthogonally by a 128-Walsh code, multiplexed with the rest of the channels, and the resulting signal is multiplied by a complex PN sequence which consists of a pair of maximal-length sequences. In such a system, and CDMA systems in general, the signal on the pilot channel simplifies to the complex PN sequence, which is the beacon of interest. Therefore, one can look at the CDMA signal as the sum of (i) the signal on the pilot channel, or the beacon signal and (ii) the sum of the remaining channels. Due to the properties of Walsh codes and assuming the symbols on the sync, paging, and traffic channels are uncorrelated, one can model the aforementioned second term as noise. In fact, for a large number of logical channels such as in cdma2000 and Globalstar, the *central limit*

theorem practically applies and the resulting noise can be modeled as a zero-mean Gaussian random sequence with a determined variance [206]. Consequently, the CDMA signal can be modeled according to (6.38), where $s[n]$ is the beacon on the pilot channel, and $w[n]$ captures channel noise and the effect of the rest of the logical channels.

The following binary hypothesis test is considered

$$\begin{cases} \mathscr{H}_0: & \mathbf{y} = \mathbf{w}_{\text{eq}} \\ \mathscr{H}_1: & \mathbf{y} = \alpha \mathbf{H}\mathbf{s} + \mathbf{w}_{\text{eq}}, \end{cases} \tag{3.4}$$

where $\mathbf{w}_{\text{eq}}$ is an independent and identically distributed (i.i.d.) Gaussian noise vector whose elements are zero-mean with variance σ^2. Also, consider the set $\mathscr{S}$ consisting all M^L vector combinations whose elements are the integers between 0 to $M-1$. For MPSK, a beacon sequence is $\mathbf{s} = \exp\left(\frac{j2\pi}{M}\mathbf{q}\right)$ where $\mathbf{q} \in \mathscr{S}$. The GLR detector for (3.4) is derived as (see Appendix .4)

$$\mathscr{L}_{\text{IC}} = \frac{\max_{\mathbf{q}\in\mathscr{S},\Delta f} |\exp\left(-\frac{j2\pi}{M}\mathbf{q}^{\mathsf{H}}\right)\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2}{K^2\|\mathbf{y}\|^2} \underset{\mathscr{H}_0}{\overset{\mathscr{H}_1}{\gtrless}} \eta_{\text{IC}}, \tag{3.5}$$

where the superscript H denotes Hermitian transpose, and η_{IC} is selected such that the probability of false alarm equals desired value.

3.4.1 Integer Least Squares Problem

To derive the constrained GLR detector in (3.5), the following integer least squares problem should be solved

$$\underset{\mathbf{q}\in\mathscr{S},\Delta f}{\text{argmax}} \left|\mathbf{z}^{\mathsf{H}} \exp\left(\frac{j2\pi}{M}\mathbf{q}\right)\right|, \tag{3.6}$$

where, $\mathbf{z} \triangleq \frac{1}{K}\mathbf{H}^{\mathsf{H}}\mathbf{y}$. A solution to the optimization problem (6.45) consists of a linear search over Doppler candidates and an exponential exhaustive search over all possible values of $\mathbf{q}$. Denoting the number of Doppler search candidates by D, the order of the overall search is

DM^L. The detection algorithm presented in [70] can be used to solve (6.45), optimally, with a complexity of order $O(DL\log L)$. However, due to the large size of the beacon signals in practice, the resulting computational complexity of existing methods is still significant. The following Lemma establishes a reduced number of search candidates.

Lemma 1: The optimal solution of the optimization problem (6.45) can be obtained by searching over DL candidates.

Proof: See Appendix .5.

In what follows, a low-complexity beacon signal detection (LCBSD) algorithm of complexity $O(DL)$ to solve (6.45) is presented. Next, using numerical analysis it is shown that the proposed LCBSD algorithm performs almost similarly as the maximum likelihood (ML) estimator.

3.4.2 LCBSD Algorithm

Under $\mathscr{H}_1$, the ML estimate of α for *known* beacon $\mathbf{q}$ is given by

$$\hat{\alpha}_{\mathrm{ML}} = \frac{1}{L}\left[\exp\left(\frac{j2\pi}{M}\mathbf{q}\right)\right]^{\mathsf{T}}\mathbf{z}. \tag{3.7}$$

Let $\mathbf{q}_l$ and $\mathbf{z}_l$ denote the vectors containing the first l elements of $\mathbf{q}$ and of $\mathbf{z}$, respectively, and let $\hat{\mathbf{q}}_l$ denote the corresponding estimate. From (3.7), the estimate of α obtained from $\hat{\mathbf{q}}_l$ is

$$\hat{\alpha}_l = \frac{1}{l}\left[\exp\left(\frac{j2\pi}{M}\hat{\mathbf{q}}_l\right)\right]^{\mathsf{T}}\mathbf{z}_l. \tag{3.8}$$

Note that $\mathbf{q}_l$ and $\hat{\mathbf{q}}_l$ correspond to symbols 0 to $l-1$ and their estimates, respectively. To estimate the lth symbol, $\hat{\alpha}_l$ is used to wipe-off the effect of α in the lth observation, then an

SBS estimator is used according to

$$\hat{q}_l \triangleq \underset{q_l \in \{0,1,\ldots,M-1\}}{\operatorname{argmax}} \Re\left\{ \alpha_l z_l^{\mathsf{H}} \exp\left(\frac{j2\pi}{M} q_l \right) \right\}, \tag{3.9}$$

where $\Re\{\cdot\}$ denotes the real part, z_l is the lth observation, and q_l is the lth element of $\mathbf{q}$ and $\hat{q}_l$ its corresponding estimate. Solving (3.9) yields

$$\hat{q}_l = \text{round}\left[\frac{(\angle z_l - \angle \hat{\alpha}_l) M}{2\pi} \right] \mod M. \tag{3.10}$$

Next, l is set to $l+1$ and the recursion continues. Let $\hat{\mathbf{q}}$ be the final estimate of the beacon. For the case $l = 0$, an initial estimate of q_0 is needed. It is important to note from Appendix .5 that the ML estimate of $\mathbf{q}$ will have an ambiguity of M. This ambiguity results in a constant phase rotation in the estimated beacon, which does not affect the absolute value of the correlation function and the TOA estimation performance. To this end, $\hat{q}_0$ is chosen arbitrarily from $\{0, 1, \ldots, M-1\}$.

3.5 Performance Analysis

This section defines the performance metrics of interest in a cognitive opportunistic navigation scenario and presents theoretical and numerical analyses of these metrics.

3.5.1 Carrier-to-Noise Ratio and TOA Measurements Error Variance

The navigation performance in TOA-based navigation depends on two main factors: (i) the DOP and (ii) the TOA estimation error variance. The DOP is strictly a function of the geometry between the transmitters and receiver. However, the TOA estimation error variance is a function of the CNR. From (6.38), it can be seen that the carrier power is

given by $C = |\alpha|^2$. SOP receivers correlate the received signal with known, local replicas of the beacons to draw TOA measurements. The correlation function peaks at the TOA. Consequently, the TOA estimation performance is determined by the peak-to-noise ratio, which, in the case of fully known beacon, is the CNR. In cognitive opportunistic navigation, this peak-to-noise ratio, or apparent CNR, is less than the actual CNR since the magnitude of the correlation function peak is reduced due to errors in the detected beacon symbols. It was mentioned in the previous section that the LCBSD algorithm yields an ambiguity of M in the SOP receiver's local beacon symbols. This ambiguity translates to an initial phase rotation in the correlation function; therefore, it does not affect its amplitude. As a result, the magnitude of the correlation peak will be preserved, which in turn preserves the CNR.

3.5.2 Probability of Error Definition

As mentioned above, the ambiguity in the detected beacons does not affect the TOA estimation performance. Hence, unlike the classic definition of the probability of error in symbol demodulation, the number of errors in the detected symbols of the beacon is not a suitable definition for the probability of error. Consequently, the probability of error P_e is defined as

$$P_e \triangleq \min_{m\in\{0,1,\ldots,M-1\}} \frac{1}{L}\sum_{l=0}^{L-1} \Pr\left[((\hat{q}_l - m) \mod M) \neq q_l\right]. \tag{3.11}$$

Let $m^\star$ denote the minimizer. The above expression cannot be computed straightforwardly since $\Pr\left[((\hat{q}_l - m^\star) \mod M) \neq q_l\right]$ varies with l. To see this, the symbol error probability curves were computed numerically from 10^6 Monte Carlo noise $\mathbf{w}_{\text{eq}}$ realizations for $L = 2^{11}$, $M = 4$, and SNR of 4 and 10 dBs, and are shown Fig. 3.1.

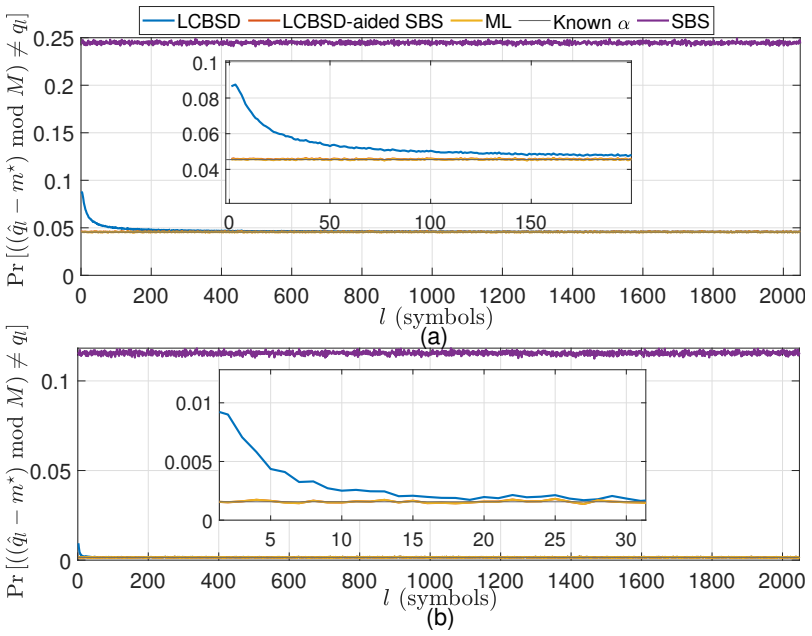


Figure 3.1: Error probability $\Pr[((\hat{q}_l - m^\star) \mod M) \neq q_l]$ for (i) SBS detector (ii) the ML estimator, (iii) the proposed LCBSD algorithm, and (iv) the LCBSD-aided SBS detector versus l, for $L = 2^{10}$, $M = 4$: for (a) SNR $= 4$ dB, and (b) SNR = 10 dB.

Fig. 3.1 shows that the LCBSD performance converges to that of the ML as l increases. Comparing 3.1(a) and 3.1(b) shows that the rate of convergence is faster for larger values of SNR. It can be also seen that the ML and the proposed LCBSD algorithm outperform the SBS estimation dramatically. While SBS is adopted in [49, 130] for beacon symbol recovery, it yields a poor probability of error. LCBSD-aided SBS performs SBS estimation for all the beacon symbols after convergence of $\hat{\alpha}_l$. This step eliminates the transient of the LCBSD symbol error probability. It should be pointed out that in Fig. 3.1, the LCBSD-aided SBS, the ML method, and the method with known α are achieving *almost equal* probability of error in the considered SNR values. Moreover, Fig. 3.1 shows that both the ML in [70] and the LCBSD error probabilities converge to the case that α is known. To this end, in the CNR analysis in Section 3.5.3, the probability of error is assumed constant over l and is equal to that of SBS estimation when α is known.

3.5.3 Apparent Carrier-to-Noise Ratio

The apparent CNR is calculated from the correlation function of s with its estimate $\hat{s}$. Let s_l and $\hat{s}_l$ denote the l-th symbol and its estimate, respectively. Note that $\hat{s}_l$ is a random variable whose support is the MPSK constellation, and the probability of each symbol is computed from the observation probability density function (pdf). Subsequently, the apparent carrier power $\bar{C}$ can be derived according to

$$\bar{C} = |\alpha|^2 \left| \mathbb{E}\left[\frac{1}{L} \sum_{l=0}^{L-1} s_l^* \hat{s}_l \right] \right|^2 = |\alpha|^2 \left| \frac{1}{L} \sum_{l=0}^{L-1} s_l^* \mathbb{E}[\hat{s}_l] \right|^2 . \tag{3.12}$$

Due to the symmetry of MPSK systems, it can be readily shown that $\mathbb{E}[\hat{s}_l] = \beta s_l$, where it can be further shown that $\beta = 1 - 2Q(\sqrt{2\text{SNR}})$ for BPSK systems and $\beta = 1 - 2Q(\sqrt{\text{SNR}})$ for QPSK systems. Subsequently, the apparent carrier-to-noise ratio is computed according to

$$\bar{C}/N_0 = |\alpha|^2 \beta^2 / N_0 = \beta^2 C/N_0, \tag{3.13}$$

and it simplifies to $\bar{C}/N_0 = [1 - 2Q(\sqrt{2\text{SNR}})]^2 C/N_0$ for BPSK and $\bar{C}/N_0 = [1 - 2Q(\sqrt{\text{SNR}})]^2 C/N_0$ for QPSK.

3.5.4 Numerical Analysis

A numerical analysis is conducted to assess the effect of the proposed LCBSD algorithm in comparison to the ML algorithm on the apparent CNR. To this end, 10^6 Monte Carlo noise $\mathbf{w}_{\text{eq}}$ realizations were generated for a beacon signal of length $L = 2^{11}$ with $M = \{2, 4\}$. The apparent CNR of the simplified GLR (SGLR) method in [197] is also compared with that of the proposed algorithm and the ML algorithm. The ratio β^2 is calculated and plotted as a function of the SNR, which is given by $\text{SNR} = \frac{1}{\sigma^2}$. Fig. 3.2 shows that the proposed

LCBSD algorithm is near optimal and obtains equal apparent CNR with the SGLR algorithm in [197] for BPSK and QPSK modulation schemes.

Remark 3: The method in [70] requires L divisions and the sorting operation, which can be accomplished by $L\log L$ complex operations. A total number of $L\log L+4L-3$ complex operations per Doppler bin is required for [70]. The total number of complex operations for the proposed method is $4L-3$ per Doppler bin. It should be pointed out that the proposed method is as complex as the SBS algorithm after the convergence of $\hat{\alpha}_l$. In many practical scenarios, the coherence time of the channel might be of the order of tens to thousands of symbols [206]. During the channel coherence time, the algorithm does not need to keep updating $\hat{\alpha}_l$ after it converges. According to Fig. 3.1, the convergence rate of $\hat{\alpha}_l$ depends on the operating SNR and is relatively high.

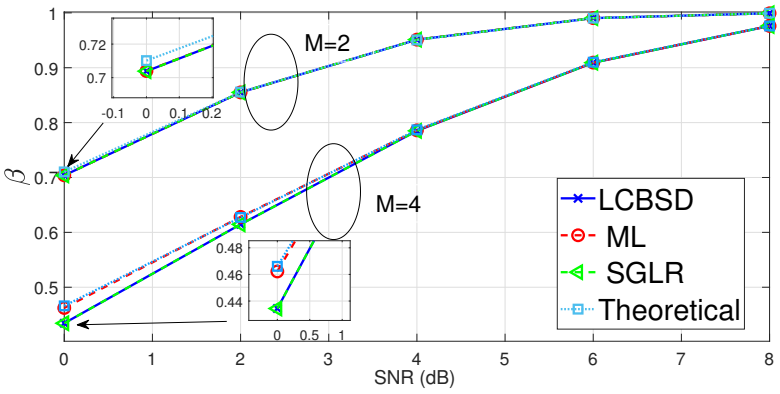


Figure 3.2: Monte Carlo results for β^2 of (1) the ML estimator, (2) the proposed LCBSD algorithm, (3) the SGLR algorithm, and (4) the theoretical value (3.13) versus the SNR for $L=2^{11}$ and $M=\{2,4\}$.

3.6 Terrestrial Signal Activity Detection with NIC

In this subsection, a GLR detector is proposed to detect the beacon signals when the elements of the beacon $\mathbf{s}$ are arbitrary complex numbers. In OFDM-based systems such as LTE and 5G NR, the beacon sequences such as primary synchronization signal (PSS) and secondary synchronization signal (SSS) still have integer constraints. However, at the transmitter, the symbols are input to the inverse discrete Fourier transform (IDFT). Therefore, in the time domain, the equivalent beacon's elements are arbitrary complex numbers. The following Remark explains how (6.3) can be descriptive of an OFDM-based system.

Remark 4: NR adopts an OFDM scheme, as was the case in 4G LTE. In OFDM-based transmission, the symbols are mapped onto multiple carrier frequencies, referred to as subcarriers, with a particular spacing known as subcarrier spacing. Once the subcarrier spacing is configured, using a higher level signaling, the frame structure is identified. In LTE and 5G, a frame has a duration of 10 ms and consists of 10 subframes with durations of 1 ms [198]. To provide frame timing to the user, an OFDM-based system such as 5G NR, broadcasts synchronization signals (SS) on pre-specified symbol numbers. An SS includes a PSS and SSS, which provide symbol and frame timing, respectively. The SS and the data symbols are input to the IDFT. In [153], it is shown that the complex envelope of the OFDM signals can be considered to be asymptotically white and Gaussian. Therefore, in (6.3), $\mathbf{s}$ contains the complex elements of the IDFT of the SS and $\mathbf{w}_{\text{eq}}$ captures the effect of receiver noise and data symbols which can be considered to be white Gaussian with variance σ^2.

Since there is no integer constraint on $\mathbf{s}$, the effect of α and matrix $\mathbf{D}$ can be lumped into $\mathbf{s}$. It should be pointed out that $|\alpha|^2\mathbf{D}^{\mathsf{H}}\mathbf{D} = |\alpha|^2\mathbf{I}$. Therefore, the correlation properties of

$\alpha\mathbf{s}$ and $\alpha\mathbf{D}\mathbf{s}$ are identical. Hence, the system model (6.3) can be rewritten as

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{w}_{\text{eq}}, \tag{3.14}$$

where $\mathbf{w}_{\text{eq}}$ is the equivalent noise vector, and the $KL \times L$ Doppler matrix is defined as

$$\mathbf{H} \triangleq [\mathbf{I}_L, \exp(j2\pi\Delta f L)\mathbf{I}_L, \ldots, \exp(j2\pi\Delta f (K-1)L)\,\mathbf{I}_L)]^{\mathsf{T}}, \tag{3.15}$$

where $\mathbf{I}_L$ is an $L \times L$ identity matrix. The following binary hypothesis test is considered

$$\begin{cases} \mathscr{H}_0: & \mathbf{y} = \mathbf{w}_{\text{eq}} \\ \mathscr{H}_1: & \mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{w}_{\text{eq}}. \end{cases} \tag{3.16}$$

The GLR detector for the testing hypothesis (3.4) is known as matched subspace detector, and is derived as [180]

$$\mathscr{L}_{\text{NIC}} = \max_{\Delta f} \frac{\mathbf{y}^{\mathsf{H}}\mathbf{P}_{\mathbf{H}}\mathbf{y}}{\mathbf{y}^{\mathsf{H}}\mathbf{P}_{\mathbf{H}}^{\perp}\mathbf{y}}, \tag{3.17}$$

where $\mathbf{P}_{\mathbf{H}} \triangleq \mathbf{H}(\mathbf{H}^{\mathsf{H}}\mathbf{H})^{-1}\mathbf{H}^{\mathsf{H}}$ denotes the projection matrix to the column space of $\mathbf{H}$, $\mathbf{P}_{\mathbf{H}}^{\perp} \triangleq \mathbf{I}_L - \mathbf{P}_{\mathbf{H}}$ denotes the projection matrix onto the space orthogonal to the column space of $\mathbf{H}$. Since $\mathbf{H}^{\mathsf{H}}\mathbf{H} = K\mathbf{I}_L$,

$$\frac{\mathbf{y}^{\mathsf{H}}\mathbf{P}_{\mathbf{H}}\mathbf{y}}{\mathbf{y}^{\mathsf{H}}\mathbf{P}_{\mathbf{H}}^{\perp}\mathbf{y}} = \frac{1}{\frac{\|\mathbf{y}\|^2}{\frac{1}{K^2}\|\mathbf{H}^{\mathsf{H}}\mathbf{y}\|^2} - 1}, \tag{3.18}$$

which is a monotonically increasing function of $\frac{\|\mathbf{H}^{\mathsf{H}}\mathbf{y}\|^2}{\|\mathbf{y}\|^2}$. Hence, the GLR detector (5.10) is equivalent to

$$\max_{\Delta f} \frac{\|\mathbf{H}^{\mathsf{H}}\mathbf{y}\|^2}{\|\mathbf{y}\|^2} \underset{\mathscr{H}_0}{\overset{\mathscr{H}_1}{\gtrless}} \eta_{\text{NIC}}, \tag{3.19}$$

where η_{NIC} is determined according to the desired probability of false alarm.

3.6.1 Derivation of Probability of Detection and False Alarm

In this subsection, closed-form expressions for the asymptotic probability of detection and false alarm are derived in the presence of Doppler estimation error and for a large CPI

K. To this end, the pdfs of the numerator and the denominator of the likelihood function (5.10) are derived. Next, it is shown that the numerator and the denominator are statistically independent. Finally, for large values of K, the pdf of the ratio of the numerator and denominator is derived. The likelihood function (5.10) can be rewritten as

$$\frac{N(\mathbf{y})}{D(\mathbf{y})} = \frac{K(L-1)}{L} \frac{\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{H}}\mathbf{y}}{\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{H}}^{\perp}\mathbf{y}}, \tag{3.20}$$

where $\hat{\mathbf{P}}_{\mathbf{H}}$ and $\hat{\mathbf{P}}_{\mathbf{H}}^{\perp}$ are the estimated projection matrices when the estimate of Doppler is replaced in $\mathbf{P}_{\mathbf{H}}$ and $\mathbf{P}_{\mathbf{H}}^{\perp}$, respectively. The numerator of the likelihood can be written as $N(\mathbf{y}) = \frac{K(L-1)}{\sigma^2}\hat{\mathbf{s}}^{\mathsf{H}}\mathbf{C}^{-1}\hat{\mathbf{s}}$, where $\mathbf{C} \triangleq \frac{1}{\sigma^2}\hat{\mathbf{H}}^{\mathsf{H}}\hat{\mathbf{H}}$ and

$$\hat{\mathbf{s}} = (\hat{\mathbf{H}}^{\mathsf{H}}\hat{\mathbf{H}})^{-1}\hat{\mathbf{H}}^{\mathsf{H}}\mathbf{y} = \frac{1}{K}\hat{\mathbf{H}}\mathbf{H}\mathbf{s} + \frac{1}{K}\hat{\mathbf{H}}^{\mathsf{H}}\mathbf{w}_{\text{eq}}. \tag{3.21}$$

The following lemma gives the distribution of $N(\mathbf{y})$.

Lemma 2: *Assuming that the $r \times 1$ vector $\mathbf{v}$ is a complex Gaussian random vector distributed as $\mathbf{v} \sim \mathscr{CN}(\boldsymbol{\mu}, \mathbf{C})$, where $\boldsymbol{\mu}$ is the $r \times 1$ mean vector and $\mathbf{C}$ is the $r \times r$ covariance matrix, the scalar $\mathbf{v}^{\mathsf{H}}\mathbf{C}^{-1}\mathbf{v}$ is distributed as*

$$\mathbf{v}^{\mathsf{H}}\mathbf{C}^{-1}\mathbf{v} \sim \begin{cases} \chi^2_{2r}, & \boldsymbol{\mu} = 0 \\ \chi'^2_{2r}(\lambda), & \boldsymbol{\mu} \neq 0, \end{cases} \tag{3.22}$$

where χ^2_{2r} denotes a chi-squared random variable with $2r$ degrees of freedom, $\chi'^2_{2r}(\lambda)$ denotes a noncentral chi-squared random variable with $2r$ degrees of freedom and non-centrality parameter λ, and $\lambda = \boldsymbol{\mu}^{\mathsf{H}}\mathbf{C}^{-1}\boldsymbol{\mu}$ [90].

According to Lemma 2, for the numerator of the likelihood function, one obtains

$$\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}_{H}\mathbf{y} \sim \begin{cases} \chi^2_{2L} & \mathscr{H}_0 \\ \chi'^2_{2L}(\lambda) & \mathscr{H}_1, \end{cases} \tag{3.23}$$

where $\lambda = \frac{\mathbf{s}^{\mathsf{H}}(\hat{\mathbf{H}}^{\mathsf{H}}\mathbf{H})\mathbf{s}}{\sigma^2}$. According to the definition of the Doppler matrix, one has

$$\hat{\mathbf{H}}^{\mathsf{H}}\mathbf{H} = \rho\mathbf{I}, \tag{3.24}$$

where

$$\rho = \left| \frac{\sin\left(K\pi\Delta f_{\mathrm{e}} L\right)}{\sin\left(\pi\Delta f_{\mathrm{e}} L\right)} \right|, \tag{3.25}$$

and $\Delta f_{\mathrm{e}} = \Delta f - \widehat{\Delta f}$ is the Doppler estimation error. Hence, the non-centrality parameter of the numerator under $\mathscr{H}_0$ can be written as $\lambda = \frac{\rho \|\mathbf{s}\|^2}{\sigma^2}$. It should be pointed out that $0 \leq \rho \leq K$. The maximum value of ρ is obtained when $\Delta f_{\mathrm{e}} \to 0$. It will be shown that the probability of detection is characterized by λ. In other words, λ is the equivalent SNR for the GLR detector (5.10). Thus, when the Doppler estimation error Δf_{e} tends to zero, the equivalent SNR, i.e., λ, is maximized. It should be noted; however, that ρ, and in turn λ, may decay as the CPI increases in the case where Δf_{e} is not *small enough*. One can show that a sufficient condition for ρ to approach K as the latter increases is that

$$\Delta f_{\mathrm{e}} \ll \frac{1}{2KL}. \tag{3.26}$$

For the denominator of the likelihood function, one has

$$\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}_H^{\perp}\mathbf{y} = \left(\frac{\mathbf{Hs}}{\sigma} + \frac{\mathbf{w}}{\sigma}\right)^{\mathsf{H}} \hat{\mathbf{P}}_H^{\perp} \left(\frac{\mathbf{Hs}}{\sigma} + \frac{\mathbf{w}}{\sigma}\right) \tag{3.27}$$

The following Lemma is used to derive the pdf of (21).

Lemma 3: *If the* $r \times 1$ *vector* $\mathbf{v}$ *is distributed as* $\mathbf{v} \sim \mathscr{CN}(\boldsymbol{\mu}, \mathbf{I})$*, and* $\mathbf{A}$ *is an* $r \times r$ *Hermitian matrxi,* $\mathbf{v}^{\mathsf{H}}\mathbf{A}\mathbf{v}$ *has non-central complex chi-squared distribution with* $\mathrm{rank}(\mathbf{A})$ *degrees of freedom and non-centrality parameter* $\boldsymbol{\mu}^{\mathsf{H}}\mathbf{A}\boldsymbol{\mu}$*, if and only if* $\mathbf{A}$ *is an idempotent matrix* [90].

According to Lemma 3, and since $\mathbf{P}_H^{\perp}$ is an idempotent matrix of rank $K(L-1)$, one has

$$\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\mathbf{P}_H^{\perp}\mathbf{y} \sim \begin{cases} \chi^2_{2K(L-1)}, & \mathscr{H}_0 \\ \chi'^2_{2K(L-1)}(\lambda'), & \mathscr{H}_1, \end{cases} \tag{3.28}$$

where $\lambda' = \frac{1}{\sigma^2}\left(K - \frac{\rho}{K}\right)\|\mathbf{s}\|^2$, and ρ is defined in (4.18).

The pdf of numerator and denominator can be obtained using (3.23) and (3.28). Now, the independence of the numerator and the denominator of the likelihood function (5.10) is assessed using the following lemma.

Lemma 4: *Let the vector* $\mathbf{v}$ *be an* $r \times 1$ *complex Gaussian vector with mean* $\boldsymbol{\mu}$ *and covariance matrix* $\mathbf{C}$*, and let* $\mathbf{A}$ *and* $\mathbf{B}$ *be* $r \times r$ *Hermitian matrices. If* $\mathbf{ACB} = \mathbf{0}$ *then* $\mathbf{v}^{\mathsf{H}}\mathbf{Av}$ *and* $\mathbf{v}^{\mathsf{H}}\mathbf{Bv}$ *are statistically independent* [90].

Since $\hat{\mathbf{P}}_{\mathbf{H}}^{\perp}$ and $\hat{\mathbf{P}}_{\mathbf{H}}$ are orthogonal matrices, according to Lemma 4, $\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{H}}\mathbf{y}$ and $\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{H}}^{\perp}\mathbf{y}$ are statistically independent.

If (3.26) is satisfied, then

$$\lim_{K\to\infty} \frac{\sin\left(K 2\pi\Delta f_{\mathrm{e}} L\right)}{\sin\left(2\pi\Delta f_{\mathrm{e}} L\right)} = K,$$

hence, according to (4.18), $\lim\limits_{K\to\infty} \lambda' = 0$. A non-central chi-squared random variable with a non-centrality parameter of zero equals a central chi-square with the same parameters, under $\mathscr{H}_1$. Therefore, for a large number of K, one has $\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\mathbf{P}_H^{\perp}\mathbf{y} \sim \chi'^2_{2K(L-1)}(0) \equiv \chi^2_{2K(L-1)}$, Finally, using the following lemma, the pdf of the likelihood function can be obtained under both hypotheses.

Lemma 5: If $x_1 \sim \chi'^2_{r_1}(\lambda')$ and $x_2 \sim \chi^2_{r_2}$ are independent, then $\frac{x_1/r_1}{x_2/r_2} \sim F'_{r_1,r_2}(\lambda)$, where $F'_{r_1,r_2}(\lambda)$ denotes a non-central F-distribution with pdf

$$f(x) = \exp\left(-\frac{\lambda}{2}\right) \sum_{k=1}^{\infty} \frac{(\lambda/2)^k}{k!} \frac{(r_1/r_2)^{\frac{1}{2}r_1+k}}{B\left(\frac{r_1+2k}{2}, \frac{r2}{2}\right)}$$
$$x^{\frac{r_1}{2}+k-1}\left(1+\frac{r_1}{r_2}x\right)^{-\frac{1}{2}(r_1+r_2)-k}, \tag{3.29}$$

with r_1 and r_2 degrees of freedom, where λ is the noncentrality parameter, and $B\left(\frac{r_1+2k}{2}, \frac{r2}{2}\right)$ is the beta function defined as $B(x,y) \triangleq \int_0^1 t^{x-1}(1-t)^{y-1}dt$ [90].

According to Lemma 4 and Lemma 5, under $\mathscr{H}_1$, if $\Delta f_e \ll \frac{1}{2KL}$, it follows that $\frac{K(L-1)}{L}\frac{\frac{1}{\sigma^2}\mathbf{y}^H\hat{\mathbf{P}}_\mathbf{H}\mathbf{y}}{\frac{1}{\sigma^2}\mathbf{y}^H\hat{\mathbf{P}}^\perp_\mathbf{H}\mathbf{y}} \sim F'_{2KL,2K(L-1)}(\lambda)$, and under $\mathscr{H}_0$, $\frac{K(L-1)}{L}\frac{\frac{1}{\sigma^2}\mathbf{y}^H\hat{\mathbf{P}}_\mathbf{H}\mathbf{y}}{\frac{1}{\sigma^2}\mathbf{y}^H\hat{\mathbf{P}}^\perp_\mathbf{H}\mathbf{y}} \sim F_{2KL,2K(L-1)}$. Hence, the probability of detection and false alarm are

$$P_\mathrm{D} = \mathscr{Q}_{F'_{2KL,2K(L-1)}(\lambda)}\left(\eta_\mathrm{NIC}\right), \tag{3.30}$$

and

$$P_\mathrm{Fa} = \mathscr{Q}_{F_{2KL,2K(L-1)}}\left(\eta_\mathrm{NIC}\right), \tag{3.31}$$

receptively, where $Q_{F'_{2KL,2K(L-1)}(\lambda)}(x)$ is the right tail probability of noncentral F-distribution defined as $Q_{F'_{2KL,2K(L-1)}(\lambda)}(x) \triangleq \int_x^\infty f(x)dx$, and $f(x)$ is defined in (3.29).

Remark 5: It can be observed from (3.30) that the probability of detection is characterized by λ. On one hand, if (3.26) is satisfied, then λ will tend to ∞ as K increases, in which case P_D tends to one. On the other hand, λ may approach zero as K increases if (3.26) is not satisfied, in which case P_D tends to zero. It should be pointed out that the prabability of false alarm is not a function of unknown parameters. Therefore, if (3.26) is satisfied then the detector is a constant false alarm rate (CFAR) detector.

3.6.2 Numerical Versus Theoretical Probability of Detection

Numerical simulations were conducted in order to compare the derived probability of detection with simulations. To this end, 5G signals were simulated and the CPI length was varied from $K = 10$ to $K = 50$ for a set of Doppler estimation errors of

$\Delta f_e \in \{0, 1.6\times10^{-5}, 2\times10^{-5}, 2.4\times10^{-5}\text{Hz}\}$. It should be pointed out that these values are close to the typical Doppler estimation error values which are observed in the experiments. The SNR was considered to be 20 dB. A total of 10^6 Monte Carlo noise $\mathbf{w}_{\text{eq}}$ realizations were used to numerically calculate P_{D}. The results are shown in Fig. 3.3. It can be seen from the figure that as the Doppler estimation error increases, the probability of detection decreases. It can be also seen that if the condition in (3.26) is violated, the probability of detection decays with the CPI. This is a direct consequence of Remark 5 which shows that the obtained theoretical analysis is corroborated with the numerical simulations.

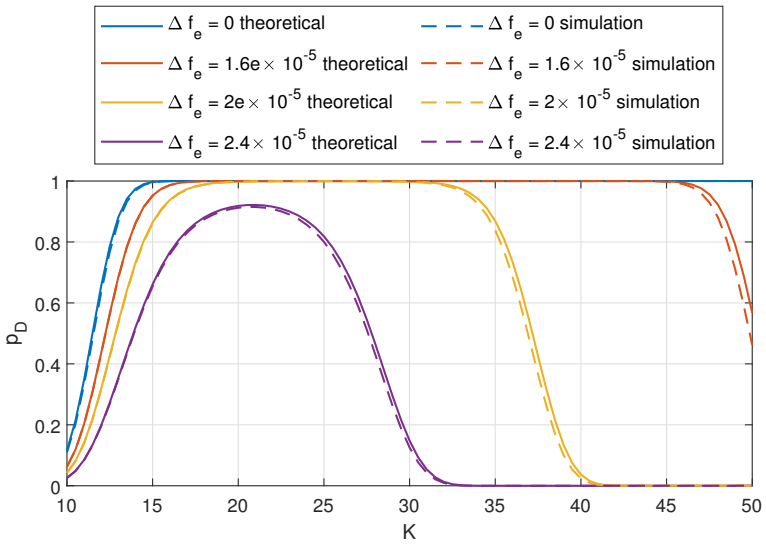


Figure 3.3: Monte Carlo simulation results comparing theoretical (3.30) and simulated probability of detection. It can be seen that increasing the CPI improves the probability of detection if the Doppler estimation error satisfies (21).

Remark 6: The detection performance curves in Fig. 3.3 demonstrate an *optimal regime of CPIs* for a given Doppler estimation error. Assuming that the Doppler is estimated

perfectly, increasing the CPI results in a higher probability of detection, which leads to a more reliable estimation of the beacon. Due to the Doppler estimation error in practice, an optimal regime of CPIs exists in which the probability of detection is maximized. If one thinks of the subspace spanned by the columns of $\mathbf{H}$ as the “signal subspace" and the orthogonal subspace as the “noise subspace," then the test statistic (5.10) is an estimated SNR for the proposed method. The ML estimation of the CPI can be obtained by maximizing (5.10) over different values of the CPI. It will be shown in Section 3.7 that the ML estimation of the CPI can be obtained using the likelihood (5.10). It will be also shown that the estimated beacon using the ML estimate of the CPI is *cleaner* than the estimated beacon using an arbitrarily chosen CPI.

After obtaining coarse estimates of the Doppler frequencies and estimates of the beacons, the receiver refines and maintains these estimates. Specifically, conventional phase-locked loops (PLLs) are employed to track the carrier phases of the detected RSs and carrier-aided delay-locked loops (DLLs) are used to track the RSs' code phases [107].

3.7 Experimental Results

This section presents experimental results demonstrating the proposed cognitive approach to detect unknown beacons of terrestrial SOPs with IC and NIC to enable cognitive opportunistic navigation of a UAV with real cdma2000 and 5G NR signals. In the detection algorithms, the thresholds are selected according to (4.20) for $P_{\text{FA}} = .001$.

3.7.1 Experiment 1: Cognitive Detection and Navigation with Unknown Beacons with IC–cdma2000 signals

The first experiment aims to show the performance of the proposed cognitive framework with unknown beacons with IC, corresponding to terrestrial cellular 3G cdma2000 signals.

3.7.1.1 Experimental Setup

A UAV was equipped with an Ettus E312 universal software radio peripheral (USRP) to sample cdma2000 signals, a consumer-grade 800/1900 MHz cellular antenna, and a small consumer-grade GPS antenna to discipline the on-board oscillator. The receiver was tuned to a 882.75 MHz carrier frequency, which is a cdma2000 channel allocated for the U.S. cellular provider Verizon Wireless. All the 3G base transceiver stations (BTSs) in this experiment transmit at 882.75 MHz. Samples of the received signals were stored for off-line post-processing. The ground-truth reference for the UAV trajectory was taken from its on-board navigation system, which uses a GNSS receiver, an inertial measurement unit (IMU), and other sensors. The UAV's total traversed trajectory was 1.72 km, which was completed in 3 minutes. Over the course of the experiment, the receiver on-board the UAV was listening to four BTSs, whose positions were mapped prior to the experiment [132]. The experimental setup and environment is shown in Fig. 3.4.

3.7.1.2 Detection Results

The cdma2000 PN sequence was estimated from the forward link signal, using the LCBSD algorithm. Fig. 3.5 shows the likelihood function (3.5) in terms of Doppler frequency. As it can be seen, four BTSs are detected in this experiment. Fig. 3.6(a) shows a

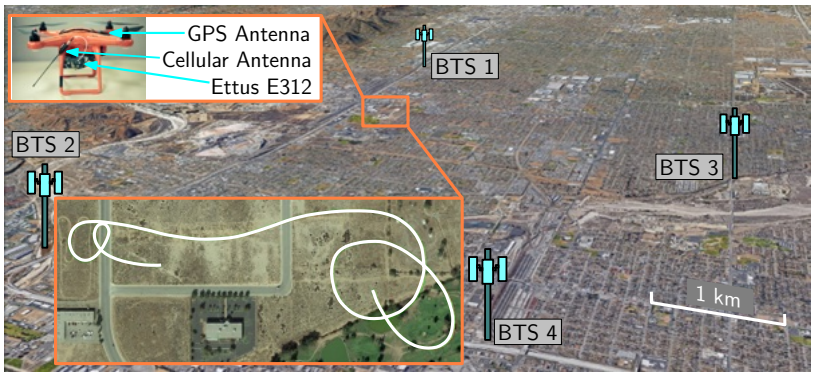


Figure 3.4: Environment layout and UAV trajectory for the cdma2000 experiment.

scatter plot of $\mathbf{z}$ in (6.45) which resembles the scatter plot of a rotated noisy 4PSK modulated signal. Fig. 3.6(b) shows the correlation function between the estimated and true cdma2000 forward channel PN sequence using the LCBSD algorithm, whose clean peak indicates that the estimated sequence can be reliably used to despread the cdma2000 signal. The value of β was found to be 0.486, which from Fig. 3.2, indicates that the receiver was operating in less than unity SNR regime.

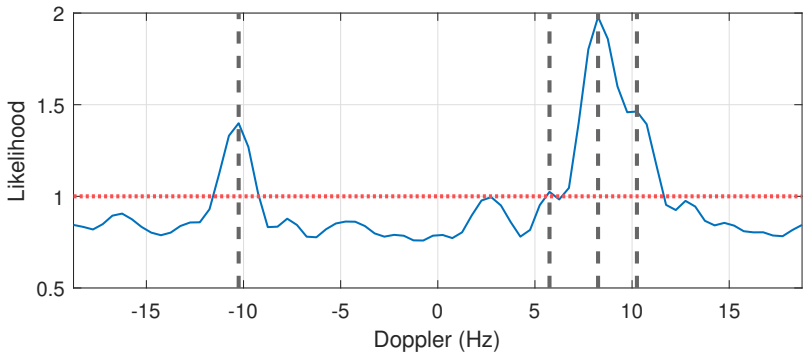


Figure 3.5: The likelihood (3.5) in terms of Doppler frequency (solid blue) and the threshold (dotted red). Four BTSs are detected in this experiment.

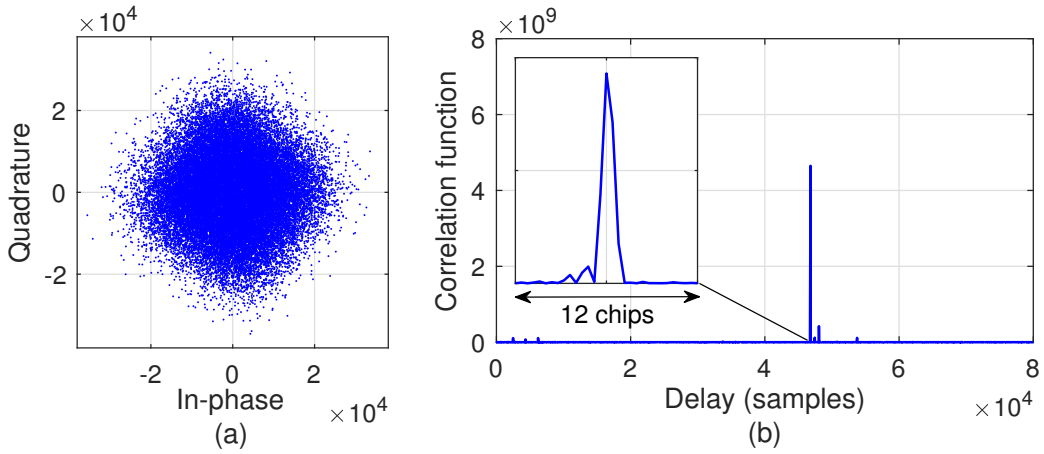


Figure 3.6: (a) Scatter plot of **z** from real cdma2000 forward channel signals. (b) Correlation function between the detected and true cdma2000 PN sequence.

3.7.1.3 Navigation Results

The detected PN sequence was used to acquire and track the received cdma2000 signals and produce TOA-like measurements using the receiver implementation discussed in [107]. It is worth noting that a carrier-aided delay-locked loop (DLL) was used to estimate the TOA, which yields smoother and more precise estimates than a standalone DLL. Next, the estimation of the position of the UAV-mounted receiver, denoted $\boldsymbol{r}_r$, from TOA measurements from the four BTSs is discussed. The UAV's altitude was assume to be known, e.g., using an altimeter, and only its two-dimensional (2–D) position was estimated. The TOA, expressed in meters, from the n-th BTS, where $n \in \{1,2,3,4\}$, can be modeled as

$$z_n(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_n}\| + c \cdot [\delta t_r(k) - \delta t_{s_n}(k)] + v_n(k), \tag{3.32}$$

where $\boldsymbol{r}_{s_n}$ is the 2–D position of the n-th BTS, c is the speed of light, δt_r and δt_{s_n} are the receiver and n-th BTS's clock biases, respectively, and v_n is the measurement noise, which is modeled as a zero-mean white Gaussian sequence with variance σ_n^2. The terms

$c \cdot [\delta t_r(k) - \delta t_{s_n}(k)]$ are combined into one term as they do not need to be estimated separately, yielding $c\delta t_n(k) \triangleq c \cdot [\delta t_r(k) - \delta t_{s_n}(k)]$, [78, 133]. The cellular BTSs possess tighter carrier frequency synchronization than time (code phase) synchronization (the code phase synchronization requirement as per the cellular protocol is reported to be within 10 μs in [2], and was experimentally observed to be within 3 μs in [96]). Therefore, the resulting clock biases in the TOA estimates will be very similar, up to an initial bias, as shown in Fig. 3.7. Consequently, one may leverage this relative frequency stability to eliminate parameters that need to be estimated.

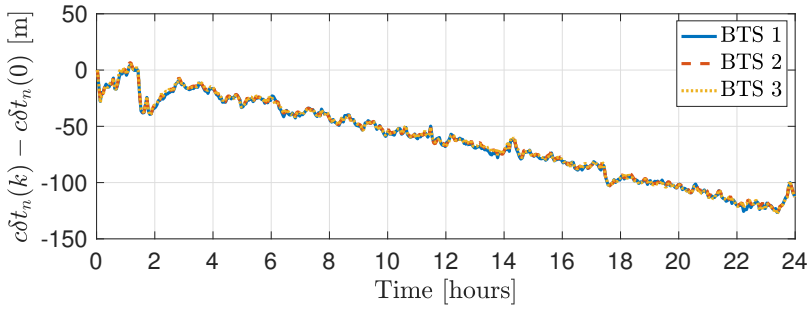


Figure 3.7: Experimental data showing $c\delta t_n(k) - c\delta t_n(0)$ obtained from carrier phase measurements over 24 hours for three neighboring BTSs. It can be seen that the clock biases $c\delta t_n(k)$ in the carrier phase measurement are very similar, up to an initial bias $c\delta t_n(0)$ which has been removed.

Motivated by Fig. 3.7, the following re-parametrization is proposed

$$c\bar{\delta} t_n(k) \triangleq c\delta t_n(k) - c\delta t_n(0) \equiv c\delta t(k) + \varepsilon_n(k), \quad \forall n \tag{3.33}$$

where $c\delta t$ is a time-varying common bias term independent of the nth BTS, and ε_n is the deviation of $c\bar{\delta} t_n$ from this common bias and is treated as measurement noise. Using (4.26), the TOA measurement (5.20) can be re-parameterized as $z_n(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_n}\| + c\delta t(k) +$

$c\delta t_{0_n} + \eta_n(k)$, where $c\delta t_{0_n} \triangleq c\delta t_n(0)$ and $\eta_n(k) \triangleq \varepsilon_n(k) + v_n(k)$ is the overall measurement noise. Note that $c\delta t_{0_n}$ can be obtained by knowing the initial receiver's position and from the initial measurement $z_n(0)$, according to $c\delta t_{0_n} \approx z_n(0) - \|\boldsymbol{r}_r(0) - \boldsymbol{r}_{s_n}\|$. This approximation ignores the contribution of the initial measurement noise.

The TOA measurements were fed to an extended Kalman filter (EKF) to estimate the state vector $\boldsymbol{x} \triangleq \left[\boldsymbol{r}_r^\mathsf{T}, \dot{\boldsymbol{r}}_r^\mathsf{T}, c\delta t, c\dot{\delta} t\right]^\mathsf{T}$, where $\dot{\boldsymbol{r}}_r$ is the UAV's 2–D velocity vector and $\dot{\delta} t$ is the clock drift. A white noise acceleration model was used for the UAV's dynamics, and a standard double integrator driven by process noise was used to model the clock bias and drift dynamics [72]. As such, the discrete-time dynamics model of $\boldsymbol{x}$ is given by

$$\boldsymbol{x}(k+1) = \mathbf{F}\boldsymbol{x}(k) + \boldsymbol{w}(k), \tag{3.34}$$

where $\mathbf{F} = \text{diag}\left[\mathbf{F}_{\text{pv}}, \mathbf{F}_{\text{clk}}\right]$ with $\mathbf{F}_{\text{pv}} = \begin{bmatrix} \mathbf{I}_2 & T\mathbf{I}_2 \\ \mathbf{0}_{2\times 2} & \mathbf{I}_2 \end{bmatrix}$, $\mathbf{F}_{\text{clk}} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}$, and T is the time interval between two measurements; $\boldsymbol{w}(k)$ is the process noise, which is modeled as a zero-mean white random sequence with covariance matrix $\mathbf{Q} = \text{diag}\left[\mathbf{Q}_{\text{pv}}, \mathbf{Q}_{\text{clk}}\right]$ where

$$\begin{aligned} \mathbf{Q}_{\text{pv}} &= \begin{bmatrix} \tilde{q}_x \frac{T^3}{3} & 0 & \tilde{q}_x \frac{T^2}{2} & 0 \\ 0 & \tilde{q}_y \frac{T^3}{3} & 0 & \tilde{q}_y \frac{T^2}{2} \\ \tilde{q}_x \frac{T^2}{2} & 0 & \tilde{q}_x T & 0 \\ 0 & \tilde{q}_y \frac{T^2}{2} & 0 & \tilde{q}_y T \end{bmatrix}, \\ \mathbf{Q}_{\text{clk}} &= c^2 \begin{bmatrix} S_{\tilde{w}_{\delta t}} T + S_{\tilde{w}_{\dot{\delta} t}} \frac{T^3}{3} & S_{\tilde{w}_{\dot{\delta} t}} \frac{T^2}{2} \\ S_{\tilde{w}_{\dot{\delta} t}} \frac{T^2}{2} & S_{\tilde{w}_{\dot{\delta} t}} T \end{bmatrix}, \end{aligned} \tag{3.35}$$

where the x, y acceleration process noise spectra of the white noise acceleration model were set to $\tilde{q}_x = \tilde{q}_y = 5\ \text{m}^2/\text{s}^3$, the time interval between two measurements was $T = 0.0267$ s, and the receiver's clock process noise spectra were chosen to be $S_{\tilde{w}_{\delta t}} = 1.3 \times 10^{-22}$ and $S_{\tilde{w}_{\dot{\delta} t}} = 7.9 \times 10^{-25}$ which are that of a typical temperature-compensated crystal oscillator (TCXO) [72]. Note that $\boldsymbol{r}_r$ is expressed in an ENU frame centered at the UAV's true initial position. The EKF state estimate was initialized at $\hat{\boldsymbol{x}}(0) = \mathbf{0}_{6\times 1}$ with an initial covariance

of $\mathbf{P}(0) = \text{diag}[3 \cdot \mathbf{I}_{2\times2}, \mathbf{I}_{2\times2}, 10^{-2}, 10^{-4}]$. The measurement noise covariance was set to $\mathbf{R} = \mathbf{I}_{2\times2}$.

The UAV's position was estimated using the aforementioned EKF and the total position RMSE was found to be 77.1 cm over the entire trajectory. The true and estimated trajectories are shown in Fig. 3.8.

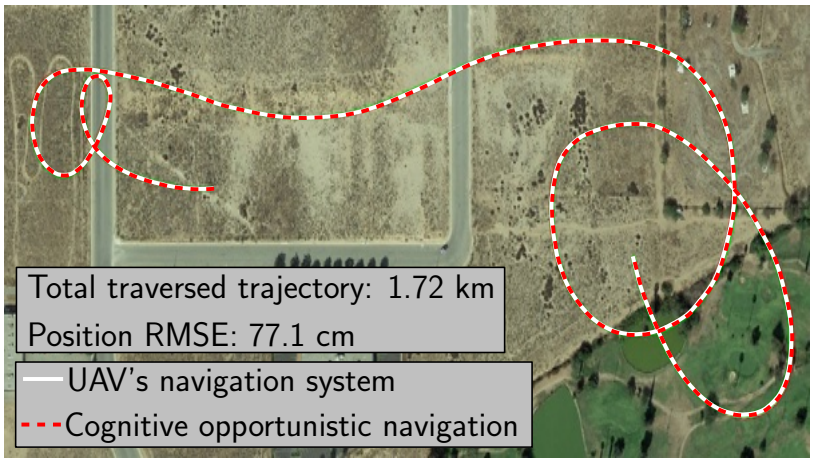


Figure 3.8: True UAV trajectory and the estimated trajectory using the proposed cognitive opportunistic navigation framework.

3.7.2 Experiment 2: Cognitive Detection and Navigation with Unknown Beacons with NIC–5G Signals

In the second experiment, the GLR detector with no integer constraint (3.19) is used to detect 5G NR downlink signals. The location of the gNBs was mapped prior to the experiment.

3.7.2.1 Experimental Setup

In this experiment, the navigator was an Autel Robotics X-Star Premium UAV equipped with a single-channel Ettus 312 USRP connected to a consumer-grade 800/1900 MHz cellular antenna and a small consumer-grade GPS antenna to discipline the on-board oscillator. The cellular receivers were tuned to the cellular carrier frequency 632.55 MHz, which is a 5G NR frequency allocated to the U.S. cellular provider T-Mobile. All the 5G gNBs in this experiment use 632.55 MHz carrier frequency. Samples of the received signals were stored for off-line post-processing. The UAV traversed a trajectory of 416 m. Fig. 3.9 shows the environment layout and the vehicle trajectory. The acquisition results are presented next.

Figure 3.9: Environment layout and UAV trajectory for the 5G NR UAV experiment.

3.7.2.2 Detection of 5G gNBs and the Corresponding RSs

Fig. 3.10 demonstrates the likelihood function (3.19) in terms of Doppler frequency. It can be seen that three different sources are detected at Doppler frequencies of 4 Hz, 12 Hz, and 15 Hz using the GLR test. In 5G NR, the always-on synchronization signal includes PSS and 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 [185]. Fig. 5.9, demonstrates the reconstructed OFDM frame of the estimated RS at 4 Hz. The always-on synchronization signals, i.e., SS/PBCH block, can be seen in the estimated OFDM frame (the block of symbols and subcarriers with the highest power in the red box). It can be seen that other than the always-on beacons, on-demand beacons are also estimated which are spread periodically in different OFDM symbols and subcarries.

In 5G NR, 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 [185]. In order to assess the performance of the detector, the estimated RS of the source at 4 Hz is correlated with the three possible 5G NR PSSs, as shown in Fig. 3.12. A strong correlation between the estimated RS and the third PSS is observed, while the correlations with the first two are negligible. This implies that the gNB at 4 Hz was actually transmitting the third PSS in the sector within which the UAV was flying.

False alarm: A detected source can be either a valid transmitter or a *false alarm*. A false alarm may occur due to multipath or an unwanted interfering source. The estimated

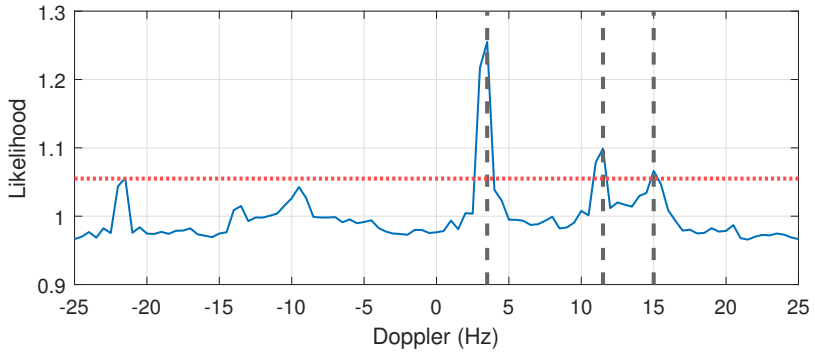


Figure 3.10: The likelihood (3.19) in terms of Doppler frequency (solid blue) and the threshold (dotted red). Three gNBs are detected in this experiment.

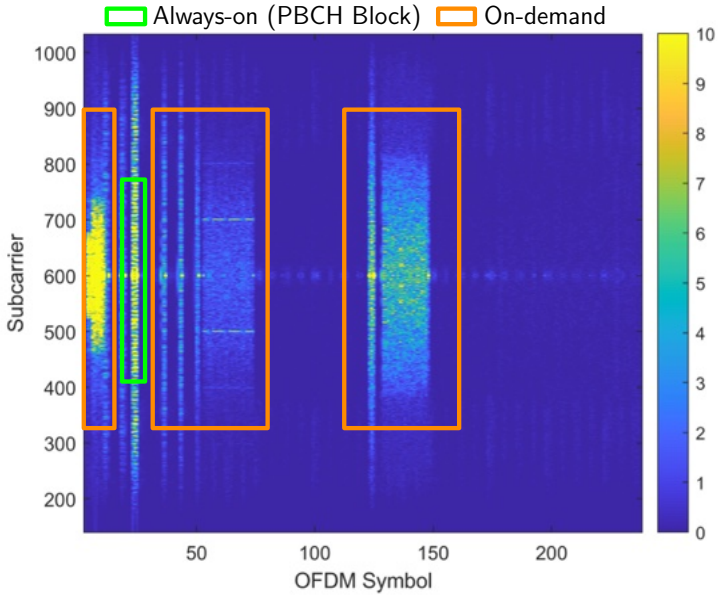


Figure 3.11: The OFDM frame structure of the estimated RS. The always-on synchronization signals, i.e., SS/PBCH block, can be seen in the estimated OFDM frame (the block of symbols and subcarriers with the highest power located in the red box).

RSs are fed to tracking loops to get carrier phase and code phase observables. If a source is mistakenly detected, the tracking loops will fail to track the signal. Fig. 3.13 demonstrates the carrier phase error for the three detected sources at 4 Hz, 12 Hz, and 15 Hz. It can be

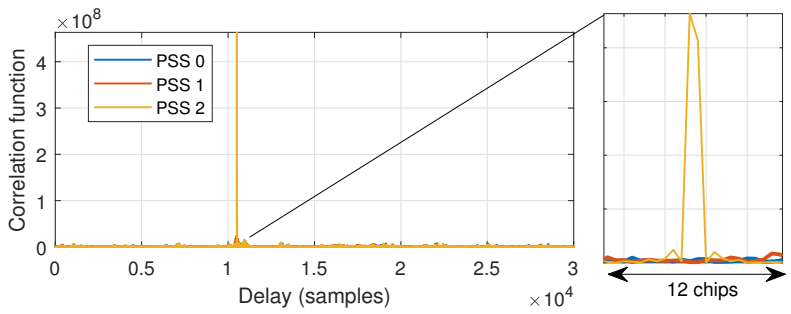


Figure 3.12: Correlation of the detected RS with three different PSSs of 5G NR.

seen that the carrier phase error of the two sources at 4 Hz and 12 Hz are converging, while the carrier phase error of the source at 15 Hz is not converging. Hence, the method identifies this source as a false alarm.

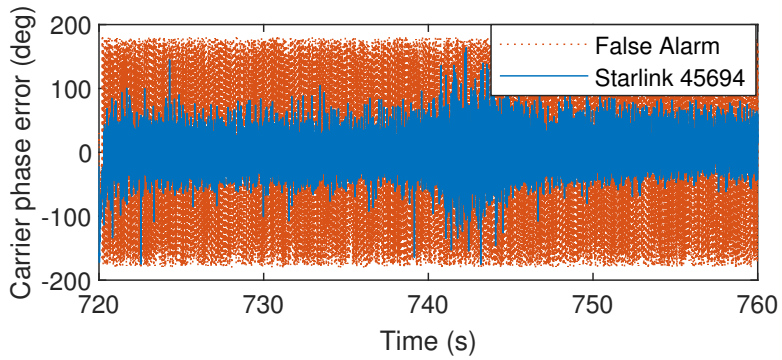


Figure 3.13: Carrier phase error for the three detected RS at 4 Hz, 12 Hz, and 15 Hz. The carrier phase error of the detected source at 15 Hz is not converging.

ML estimation of the CPI: Fig. 3.14 demonstrates the likelihood function for different values of CPI. As discussed in Remark 6, the ML estimation of the CPI can be obtained by maximizing the likelihood function (5.10). A CPI of $K = 60$ maximizes the likelihood for the first gNB and a CPI of $K = 36$ maximizes the likelihood corresponding to the second

gNB. It should be pointed out that the optimal choice of the CPI depends on the channel statistics and the dynamics of the UAV. In a scenario where the Doppler is changing rapidly, the ML estimate of the CPI becomes smaller. On the other hand, in a static scenario, the receiver will have more time to coherently accumulate the received samples and obtain a better estimate of the RS. Fig. 3.15 demonstrates the estimated PRNs for the first gNB for two different values of CPI: (i) an arbitrary CPI of $K = 20$, and (ii) the ML estimate of a CPI of $K = 60$. It can be seen that the estimated RS for $K = 60$ is cleaner than that of the arbitrarily chosen CPI.

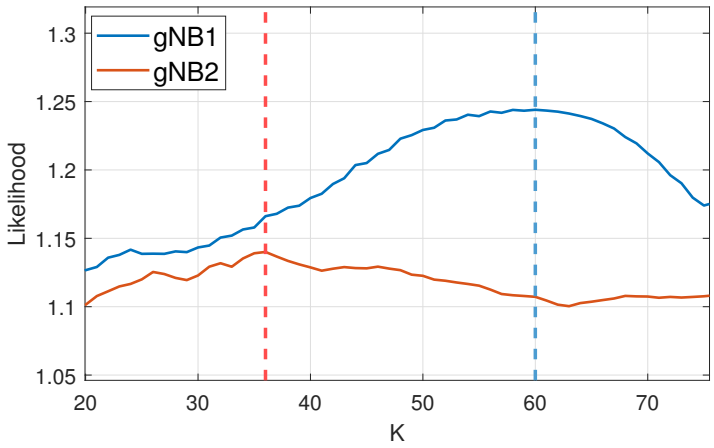


Figure 3.14: The likelihood (3.19) in terms of different values of CPI.

3.7.2.3 Navigation Results

The estimated beacon is used to produce TOA measurements using the receiver implementation discussed in [149]. Note that since the UAV's altitude is known using an altimeter, only its two-dimensional position is estimated. Similar measurement models as in Section

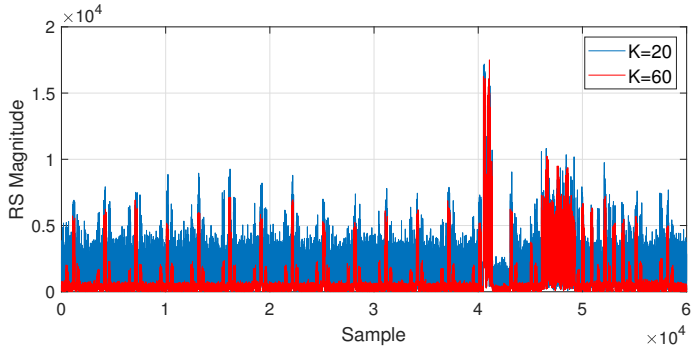


Figure 3.15: The estimated RS at 4Hz for $K = 20$ and $K = 60$. The estimated RS for the optimal CPI ($K = 60$) is less noisy than the estimated RS for the arbitrarily chosen CPI ($K = 20$).

6.13.3 are considered. The TOA measurements were fed to an extended Kalman filter (EKF) to estimate the state vector $\boldsymbol{x} \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, c\delta t, c\dot{\delta} t\right]^{\mathsf{T}}$, where $\dot{\boldsymbol{r}}_r$ is the UAV's 2–D velocity vector and $\dot{\delta} t$ is the clock drift as discussed in Section 6.13.3. The x, y acceleration process noise spectra in the nearly constant velocity model were set to $\tilde{q}_x = \tilde{q}_y = 5$ m^2/s^3, the time interval between two measurements was $T = 1$ s, and the receiver's clock process noise spectra were chosen to be $S_{\tilde{w}_{\delta t}} = 1.3 \times 10^{-22}$ and $S_{\tilde{w}_{\dot{\delta} t}} = 7.9 \times 10^{-25}$. The EKF state estimate was initialized at $\hat{\boldsymbol{x}}(0) = \mathbf{0}_{6\times 1}$ with an initial covariance of $\mathbf{P}(0) = \text{diag}[3{\cdot}\mathbf{I}_{2\times 2}, \mathbf{I}_{2\times 2}, 10^{-2}, 10^{-4}]$. The measurement noise covariance was set to $\mathbf{R} = \mathbf{I}_{2\times 2}$. The position RMSE of the UAV was calculated to be 4.63 m with the aforementioned parameters. The true and estimated UAV trajectories with the proposed method versus the receiver in [5] which uses the *known* beacon are shown in Fig. 3.16. It can be seen that the proposed cognitive opportunistic framework achieves lower position RMSE compared to the method presented in [5]. This is due to the fact that the method in [5] only relies on always-on signals, whereas the cognitive opportunistic navigation framework exploits all the available bandwidth of the received signal, which in turn results in a more accurate TOA estimation and, consequently, less positioning RMSE [149].

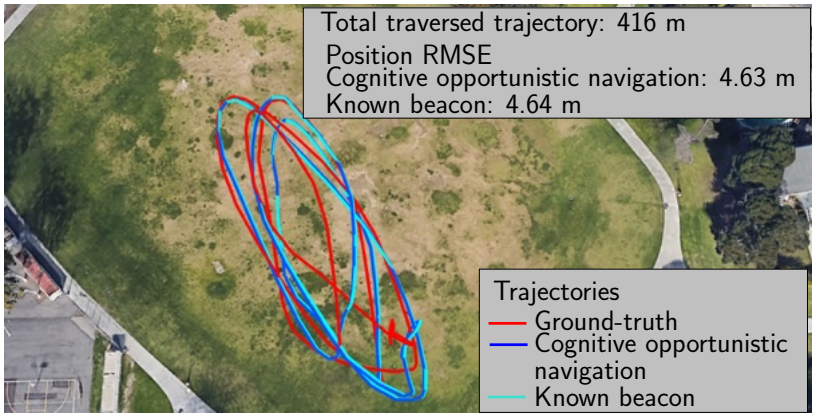


Figure 3.16: UAV's ground-truth and estimated trajectories using the proposed cognitive opportunistic navigation framework versus the method in [5], which uses the known always-on beacons for 5G NR signals. Map data: Google Earth.

3.7.3 Signal Model Validation

In the signal model (6.38), a single tap channel which corresponds to the LOS path with arbitrary channel gain α is considered. More precisely, the channel impulse response is modeled as $h[n] = \alpha\delta[n-n_d]$, where α is the complex channel gain between the transmitter and the receiver, and n_d is the code-delay corresponding to the transmitter and the receiver. This channel model considers a *flat fading* scenario, where the effect of multiple "close" paths is considered in a single path gain α. Based on the underlying distribution of α, the considered $h[n]$ can model a *Rayleigh* or *Rician* flat fading channel [206]. To justify the single tap flat fading channel model for the UAV scenario, the channel impulse response between the UAV and one of the gNBs is assessed. The physical environment between the gNB and the UAV is demonstrated in Fig. 3.17. In this figure, the term clear LOS refers to a scenario where the signal is not blocked by an obstacle, e.g., a building. It can be seen that there is a clear LOS between the gNB and the UAV. The magnitude of the channel impulse response is plotted in Fig. 3.18(a). The magnitudes of the channel

impulse responses are estimated by reconstructing the frame as described in [9]. Fig. 3.18(b) demonstrates the true and estimated code delay between the gNB and the UAV. It can be observed from Fig. 3.18 that the channel impulse response $|h(\tau)|$ does not exhibit multiple taps (i.e., $h[n] = \sum_{i=1}^{M} \alpha_i \delta[n - n_{d_i}]$, where M is the number of paths). Hence, considering a single tap flat fading model is valid for the conducted experiments. Frequency selective channels can be considered in future work.

Figure 3.17: The environment layout and the physical channel between the gNB and the UAV.

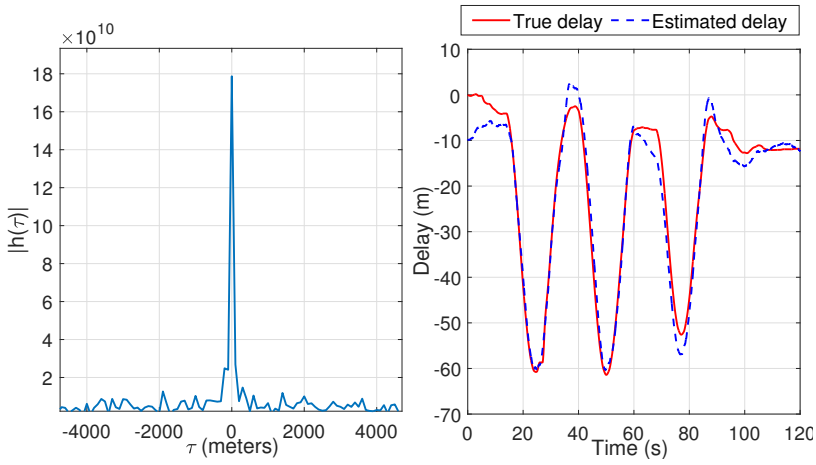


Figure 3.18: (a) The channel impulse response magnitude between the gNB and the UAV at $t = 0$. (b) The code-delay corresponding to the corresponding between the gNB and the UAV during the course of the experiment.

Chapter 4: Cognitive Sensing and Navigation with Unknown OFDM Signals with Application to Terrestrial 5G and Starlink LEO Satellites

4.1 Introduction

Due to significant advancements in cellular technologies and dense deployment of cellular infrastructure, fifth-generation (5G) and beyond cellular networks will be adopted by intelligent transportation systems to enable reliable and safe autonomous operations [226]. Several features in 5G and beyond cellular networks depend on the ability to localize the user equipment (UE) to a high degree of accuracy [232]. Estimation of time-of-arrival (TOA), direction-of-arrival (DOA), and/or frequency-of-arrival (FOA) of multiple users/targets is an inseparable block of some 5G and beyond technologies, such as joint sensing and communication [169].

Similar to 4G long-term evolution (LTE), 5G new radio (NR) adopts orthogonal frequency division multiplexing (OFDM) [37]. In addition, new constellations of broadband low Earth orbit (LEO) space vehicles (SVs) will transmit OFDM-type signals [143]. In OFDM-based systems, a part of the transmitted power is dedicated to periodic synchronization signals, referred to as reference signals (RSs), which are transmitted for synchronization

purposes. RSs are designed (or selected) based on their distinctive bandwidth and correlation properties and the physical channel type [22]. While the RSs allocated to a single LTE channel have a *predetermined* bandwidth of up to 20 MHz, the allocated bandwidth for the RSs in a single 5G channel is *dynamic*, i.e., it adaptively changes based on the transmission mode, and can go up to 100 MHz and 400 MHz for frequency ranges 1 and 2 (FR1 and FR2), respectively [198]. On the other hand, Starlink downlink signals occupy 250 MHz bandwidth of the Ku-band to provide high-rate broadband connectivity, but the allocated bandwidth (and other signal characteristics) of the RSs are *unknown* [38].

Navigation receivers typically rely on known RSs transmitted by the sources to draw TOA, DOA, and FOA measurements [184]. Conventional opportunistic navigation receivers (i.e., those only utilizing the downlink signals) will either fail to operate or will be unable to exploit the entire available bandwidth in situations where RSs are unknown and/or dynamic, which is the case in 5G NR and private networks, such as broadband LEO. Cognitive opportunistic navigation [149] has been recently introduced to address the following challenges of navigation with signals of unknown and dynamic nature. First, unlike public networks where the broadcast RSs are known at the UE and are universal across network operators, in private networks, the signal specifications of some RSs may not be available to the public or are subject to change. Second, in cellular LTE networks, several RSs (e.g., cell-specific reference signal (CRS)) are broadcast at regular and known time intervals, regardless of the number of UEs in the environments. *Ultra-lean* design refers to minimizing these *always-on* transmissions. 5G NR transmit some of the RSs only when necessary or *on-demand* [158]. As such, designing cognitive receivers that can cognitively acquire *partially known*, *unknown*, or *dynamic* beacon signals (periodic synchronization signals) is an emerging need for the future of navigation receivers [104, 145].

The problem of cognitively exploiting on-demand and always-on 5G NR signals has been previously studied in [8, 148, 149]. These methods rely on the difference between the Doppler frequencies of the SOPs to acquire and track the unknown sources. However, the acquisition and tracking of unknown sources may fail in the following extreme scenarios: (i) an almost static scenario that may lead to a *Doppler subspace overlap* and (ii) a high dynamic scenario where the receiver or the transmitter are moving with high dynamics which results in an *intensive Doppler rate*. These two extreme scenarios introduce the following challenges in the acquisition and tracking of the unknown sources:

The almost static scenario: In a scenario where the receiver and the transmitter are almost static, the Doppler frequencies of the transmitting sources will be very close to each other. This event is referred to as the Doppler subspace overlap. Distinguishing between the sources with Doppler subspace overlap becomes very challenging for the cognitive navigation framework.

Intensive Doppler rate scenario: In cognitive navigation frameworks, the unknown and dynamic parameters of the RSs are estimated via a coherent accumulation of the received samples over time. High values of Doppler rate limits the coherence time, i.e., the time interval that the channel between the transmitter and the receiver is static. A limited coherence time affects the unknown source acquisition and tracking performance. Therefore, considering the effect of the Doppler rate in the signal model and selecting a proper coherent processing interval (CPI) play a key role in intensive Doppler rate scenarios.

This chapter addresses the two challenges by: (i) presenting a maximum likelihood (ML)-based detection method to estimate the CPI jointly with the Doppler and the Doppler rate, (ii) presenting a sequential matched subspace detector based on a chirp Doppler model

to distinguish between the sources with Doppler subspace overlap, and (iii) designing tracking loops with adaptive loop gains which enable RS tracking in challenging scenarios. The contributions of this work are:

- A full receiver architecture is presented which could jointly estimate the unknown RSs of multiple SOPs in almost static and intensive Doppler rate scenarios. The cognitive nature of the proposed receiver enables estimating both always-on and on-demand RSs, the latter of which are not necessarily always-on. Both components were shown to be detected and refined in post-acquisition and tracking stages. The roles of providing a fine estimate of the RS, and tracking the code and carrier phases are played by the tracking loops via properly designed adaptive gains. The adaptive gains are provided by the acquisition stage and are designed based on the source detection performance. Feeding this information to the tracking loops, establishes a link between the acquisition and tracking loops which is necessary in challenging scenarios and distinguishes the proposed architecture from conventional navigation algorithms. To the best of the author's knowledge, this link between the acquisition and tracking stages is not considered in both classic GNSS receivers, e.g., [25, 209], and the state-of-the-art joint detection and tracking techniques, e.g., [149]. One of the contributions of this chapter is demonstration of the importance of reporting the detection performance to the tracking loops by experimentally showing that the state-of-the-art receiver architectures will fail to track the signals in challenging scenarios without the proposed link between the acquisition and tracking loops.

- The effect of Doppler rate estimation error on the autocorrelation function is presented analytically. A closed-form solution for the autocorrelation attenuation is presented

which matches the experimental results. The analysis of the effect of Doppler rate estimation error on the autocorrelation function is crucial in navigation with LEO satellites. This analysis, enables a novel blind Doppler rate estimation technique for LEO satellite signals.

- Experimental results are presented showing an application of the proposed receiver architecture by (i) enabling an unmanned aerial vehicle (UAV) to detect and exploit terrestrial 5G NR cellular signals for navigation purposes, achieving a position root mean-squared error (RMSE) of 4.2 m over a total trajectory of 416 m; (ii) enabling a ground vehicle to cognitively sense (detect and track) an unknown 5G gNB in the environment, estimating the position of the gNB with a two-dimensional (2D) error of 5.83 m in a blind fashion; and (iii) exploiting Starlink downlink OFDM signals to localize a stationary receiver, showing that starting from an initial estimate of 200 km away, the final 2D error converges to 6.5 m.

4.2 Related Work

This section overviews related work in positioning with 5G NR, unknown signals, and LEO SV signals.

4.2.0.1 Positioning with 5G NR

Positioning with 5G signals has been studied in the literature [46, 108, 115, 154, 223]. High data rate in 5G signals necessitates a higher transmission bandwidth and more advanced spatial and time-domain-based multiplexing techniques. However, since the unlicensed spectrum in lower frequencies is scarce, millimeter waves (mmWaves) have been adopted

for 5G FR2 [19]. To mitigate the high pathloss of propagated mmWave signals different beamforming techniques and massive multiple-input, multiple-output (mMIMO) antenna structures are proposed for the 5G protocol [52]. Since beamforming in 5G requires the knowledge of the user's location, 5G-based positioning is essential for resource allocation [45]. The signal characteristics of mmWave for positioning were studied in [227]. [232] focuses on the integrated positioning methodology of GNSS and device-to-device (D2D) measurements in 5G communication networks. In [223], a tensor-based method for channel estimation in mmWave systems was presented, which enables positioning and mapping using diffuse multipath in 5G mmWave communication systems. Experimental results in [5] showed meter-level navigation using TOA estimates from 5G signals. All the aforementioned methods relied on the knowledge of the beacon signals. The proposed cognitive framework in this chapter is capable of detecting and tracking unknown on-demand and always-on beacons. This feature of the proposed receiver architecture enables navigation with systems with ultra-lean design, where dynamic and on-demand beacons are adopted.

4.2.0.2 Positioning with Unknown Signals

The detection problem of an unknown source in the presence of other interfering signals falls into the paradigm of *matched subspace detectors*, which has been widely studied in the classic detection theory literature [61, 113, 180, 233]. In the navigation literature, detection of unknown signals has been studied to design frameworks, which are capable of navigating with unknown or partially known signals [49, 130]. Preliminary results for navigation with partially known signals from low and medium Earth orbit satellites were conducted in [104, 144, 145]. In particular, a chirp parameter estimator was used in [144] to blindly estimate the GPS pseudorandom noise (PRN) codes. In [148, 149], a cognitive opportunistic

navigation framework was developed to navigate with LTE and 5G NR signals. None of the aforementioned methods have considered the optimal selection of CPI, which dramatically affects the performance. Such selection is addressed in the proposed receiver in this chapter, which is capable of jointly detecting and tracking both always-on and on-demand RSs in a challenging acquisition scenarios. Moreover, unlike conventional signal acquisition and tracking methods, the proposed receiver utilizes information about acquisition performance into the tracking loops, which enables tracking weak signals in challenging environments. Such a connection between the acquisition and tracking stages is crucial for navigation with unknown signals (whether terrestrial 5G NR or Starlink LEO SV) in challenging scenarios, such as intensive Doppler.

4.2.0.3 Navigation with Starlink LEO SV Signals

The first positioning results with Starlink SV signals were presented in [105, 147, 151]. These chapters exploited a train of pure tones in the downlink of Starlink SV signals to obtain carrier-phase and Doppler measurements. Starlink downlink signals occupy 250 MHz bandwidth of the Ku-band to provide a high-rate broadband connectivity [38]. In this chapter, the Starlink OFDM-based RSs are detected cognitively. It is shown that the RSs of Starlink downlink signals have an ultra-lean-like behavior, in which some of the RSs are not always-on. The RSs of multiple Starlink SVs are estimated and the whole available signal bandwidth is exploited and employed in tracking loops to provide code-phase and carrier-phase observables.

4.3 Signal Model

4.3.1 Overview of OFDM Frame

In OFDM-based transmission, the symbols are mapped onto multiple carrier frequencies, referred to as subcarriers, with a particular spacing known as subcarrier spacing. The subcarrier spacing is either fixed, e.g., LTE standard, or selected based on the carrier frequency, and/or other requirements and scenarios, e.g., 5G NR. Once the subcarrier spacing is configured, using a higher-level signalling, the frame structure is identified. One of the challenges that should be addressed in the proposed receiver design is the estimation of the frame length of the OFDM signals. 5G NR frame has a duration of 10 ms and consists of 10 subframes with durations of 1 ms [198]. Due to the high Doppler dynamics in LEO satellites, a smaller frame length should be selected to avoid Doppler spread [206]. It should be pointed out that the frame length is equal to the period of the synchronization signals. The autocorrelation of a large enough time segment of the received signal will result in a train of an impulse-like function whose shape depends on the autocorrelation properties of the synchronization signals. The distance between two consecutive impulses is equal to the OFDM frame length. Fig. 4.1(a) demonstrates the autocorrelation of a 100 ms time segment of the Starlink downlink signal after Doppler rate wipe-off. The details of the Doppler rate wipe-off process will be discussed later. It can be seen that the distance between the impulses of the resulting train is estimated to be 1.33331 ms. Also, as a reference, Fig. 4.1(b) shows the same processing on a 40 ms time segment of a 5G NR signal which results in a frame length estimation of 10 ms which corroborates the standard frame length of 5G NR downlink signals. More details about frame length estimation and the effect of Doppler rate on the autocorrelation function will be discussed in Section 5.6.1. In the frequency

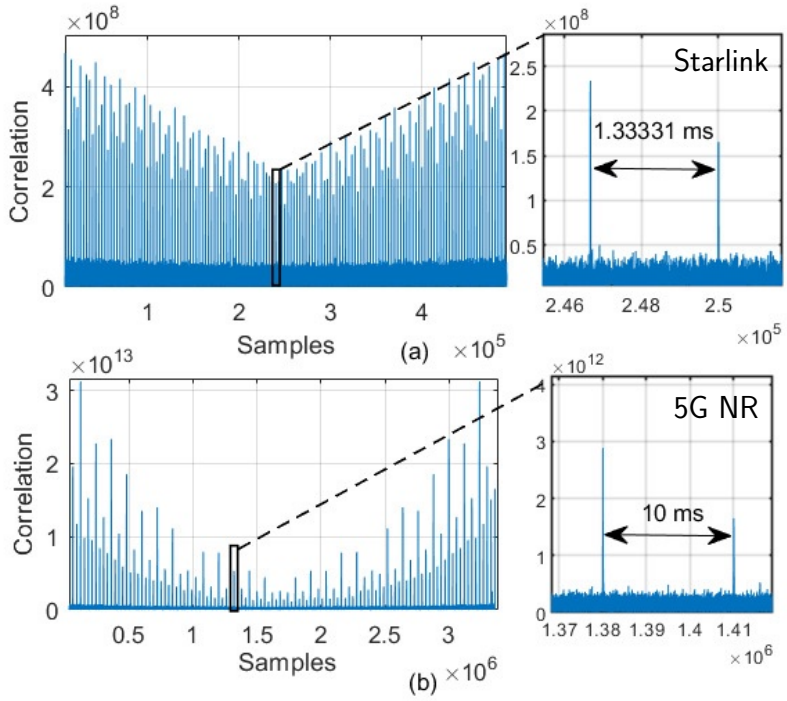


Figure 4.1: Autocorrelation of the recorded signal after Doppler wipe-off: (a) Autocorrelation of the 100 ms of Starlink Downlink signal shows a frame length of 1.33331 ms. (b) Autocorrelation of 40 ms of 5G NR downlink signal which shows the frame length of 10 ms (5G NR standard frame length).

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 [198]. To provide frame timing to the UE, a gNB broadcasts synchronization signals (SS) on pre-specified symbol numbers. 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 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. The SS/PBCH block

is transmitted numerous times on one of the half frames, which is also known as SS/PBCH burst. Fig. 4.2 demonstrates the SS/PBCH subcarriers and non-active subcarriers which are color-coded by dark-blue. A non-active subcarrier can be a subcarrier that is allocated to data or on-demand RSs.

4.3.2 baseband Signal Model

The common feature of always-on and on-demand RSs is periodicity. If a subcarrier is being periodically transmitted, it will be detected by the receiver, estimated, and used to derive navigation observables. The channel between the ith source and the UE is considered

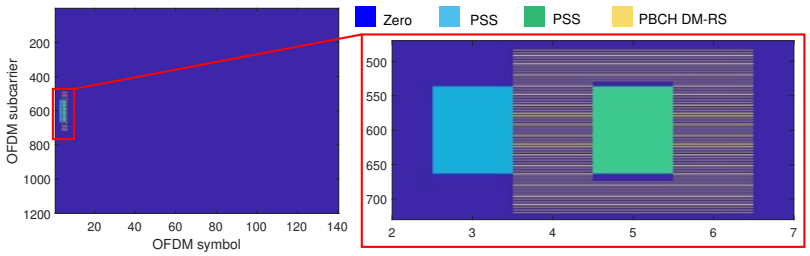


Figure 4.2: OFDM frame structure (always-on subcarriers): SS/PBCH block and the corresponding OFDM symbols and subcarriers are indicated in the red box.

to have a single tap with the complex channel gain α_i. The received baseband signal samples can be modeled as

$$r[n] = \sum_{i=1}^{N} \alpha_i \left(c_i \left(\tau_r[n] \right) + d_i \left(\tau_r[n] \right) \right) \exp \left(j\theta_i[n] \right) + w[n], \tag{4.1}$$

where $r[n]$ is the received signal at the nth time instant; $\alpha_i[n]$ is the complex channel gain between the UE and the ith source at the nth time instant; and $\tau_r[n] \triangleq \tau_n - t_{s_i}[n]$, where $t_{s_i}[n]$ is the code-delay corresponding to the UE and the ith source at the nth time instant,

and τ_n is the sample time expressed in the receiver time. Moreover, N is the number of unknown sources; $c_i[n]$ represents the samples of the continuous-time waveform $c_i(t)$ of the periodic RS corresponding to the ith source with a period of L samples; $\theta_i[n] = 2\pi f_{D_i}[n]T_s n$ is the carrier-phase in radians, where $f_{D_i}[n]$ is the Doppler frequency at the nth time instant and T_s is the sampling time; $d_i[n]$ represents the samples of some data transmitted from the ith source; and $w[n]$ is a zero-mean independent and identically distributed noise with $\mathbb{E}\{w[m]w^*[n]\} = \sigma_w^2\delta[m-n]$, where $\delta[n]$ is the Kronecker delta function, and $w^*[n]$ denotes the complex conjugate of random variable $w[n]$. The received signals can be expressed in terms of equivalent RS from the ith source, denoted by $s_i[n]$, and the equivalent noise, denoted by w_{eq_i}, which are defined as

$$s_i[n] \triangleq \alpha_i c_i[\tau_n - t_{s_i}[n]] \exp\left(j\theta_i[\tau_n]\right), \tag{4.2}$$

$$w_{\text{eq}_i}[n] = d_i[\tau_n - t_{s_i}[n]] \exp\left(j\theta_i[\tau_n]\right) + w[n]. \tag{4.3}$$

Hence, the baseband samples can be rewritten as

$$r[n] = \sum_{i=1}^{N} \left(s_i[n] + w_{\text{eq}_i}[n]\right). \tag{4.4}$$

Remark 1: In this chapter, the Doppler frequency is modeled as a linear chirp, i.e., $f_{D_i}[n] = f_{D_{i_0}}[n] + \beta_i[n]T_s n$, where $f_{D_{i_0}}[n]$ is the initial Doppler frequency, and $\beta_i[n]$ is the Doppler rate.

Definition 1: The CPI is defined as the number of periods of an RS in a time interval during which the Doppler $f_{D_{i_0}}[n]$, Doppler rate $\beta_i[n]$, delay $t_{s_i}[n]$, and channel gains α_i are considered to be constant.

4.4 Receiver Architecture

This section describes the proposed receiver.

4.4.1 Frame Length Estimation

Detection and tracking of unknown sources rely on two fundamental features of the RS: (i) periodicity and (ii) correlation properties in the time- and frequency-domains. In broadband communication systems, the RS waveform is designed based on the correlation properties of the so-called synchronization sequences. Different sequences have distinct correlation behaviors and can be adopted in a particular system based on the physical considerations. For instance, Zadoff-Chu sequences are known for their low autocorrelation sidelobes at zero Doppler shift, and Bjorck sequences can more effectively decouple the effect of time and frequency shifts [22].

The correlation properties of a sequence are usually characterized using the so-called *ambiguity function*.

Definition 2: Let $p[n]$ be a sequence of numbers of length L, where $n = 0, \ldots, L-1$. Define the periodic sequence $c[n]$ as the periodic extension of $p[n]$, i.e., $c[m] = p[k]$, for $m \in \mathbb{Z}$, where $0 \leq k \leq L-1$ and $k \equiv (m \mod L)$. The discrete ambiguity function of periodic code $c[m]$ is defined as [22]

$$\mathscr{A}_c(m,n) = \frac{1}{L} \sum_{k=0}^{L-1} c[m+k] c^{\star}[k] \exp\left(-\frac{j2\pi kn}{L}\right). \tag{4.5}$$

In order for the acquisition stage to be able to detect always-on and on-demand RSs, having an estimate (or the exact value) of the RS period is necessary. While the frame length is

known for public networks (e.g., 5G NR), in private networks, the frame length might be unknown or dynamically change based on the transmission mode [198]. The first stage of the proposed receiver involves frame length estimation. The autocorrelation of a large enough time segment of the received signal results in a periodic train of ambiguity functions in the time-domain. If the transmitted sequences have *good correlation properties*, the ambiguity functions will have an impulse-like shape. Good autocorrelation means that the RS waveform of the RS is nearly uncorrelated with its own time-shifted versions, while good crosscorrelation indicates that the RSs of different satellites' waveforms are nearly uncorrelated.

The following Lemma provides a closed-form solution for the autocorrelation function in the presence of the Doppler rate.

Lemma 1: Denoting the autocorrelation function of a large enough and arbitrary time segment of length L' of the received signal by $R_{rr}[m] \triangleq \frac{1}{L'}\sum_{k=0}^{L'} r[m+k]r^{\star}[k]$, where $L' \gg L$, the following equality holds

$$R_{rr}[m] = \bar{\alpha}_i \bar{\mathscr{A}_{c_i}}(m,0)\frac{\sin\left(2\pi\beta T_s^2 mL'\right)}{\sin\left(2\pi\beta T_s^2 m\right)} + R_{ww}[m], \tag{4.6}$$

where $|\bar{\alpha}_i| = 1$, $\bar{\mathscr{A}_{c_i}}(m,0) = \mathrm{E}\{\mathscr{A}_{c_i}(m,0)\}$ is the expected value of the periodic ambiguity function of the RS corresponding to the ith satellite and $R_{ww}[m]$ is the autocorrelation function of noise.

Proof: See Appendix .6.

Note that the term $\frac{\sin\left(2\pi\beta T_s^2 mL'\right)}{\sin\left(2\pi\beta T_s^2 m\right)}$ in (4.6) has a sinc function-like behavior in terms of m for a nonzero Doppler rate. Assuming that the RS has good correlation properties, the term $\mathscr{A}_{c_i}(m,0)$ contains a periodic train of impulse-like functions with a period of L samples (the

RS period). For a non-zero Doppler rate, due to sinc-like behavior of the term $\frac{\sin\left(2\pi\beta T_s^2 mL'\right)}{\sin\left(2\pi\beta T_s^2 m\right)}$, the autocorrelation function $R_{rr}[m]$ is not periodic as the periodic impulse-like functions are attenuated by the effect of the the sinc.

To validate Lemma 1 practically, real Starlink LEO SV signals are analyzed to demonstrate the effect of the Doppler rate on the autocorrelation function. The details of the hardware setup which is used to record Starlink LEO SV signals is presented in Section 4.5.3. Fig. 4.3 demonstrates the autocorrelation function of 150 ms of real Starlink downlink signal for different values of the Doppler rate: (a) $\beta = 1323$, (b) $\beta = 523$, (c) $\beta = 323$, and (d) $\beta = 0$ Hz/s. To achieve these Doppler rate values in Fig. 4.3, the actual Doppler rates of the Starlink LEO SV was estimated using the receiver that will be described in Section 5.6. The estimated Doppler rate is partially wiped-off to obtain the different β values in Fig. 4.3. The large impulse in the center of the autocorrelation function contains the summation of the autocorrelation function, the RS ambiguity function, and noise autocorrelation at $m = 0$, i.e.,

$$R_{rr}[0] = \bar{\alpha}_i L' \bar{\mathscr{A}}_{c_i}(0,0) + R_{ww}[0]. \tag{4.7}$$

Assuming white Gaussian noise, i.e., $R_{ww}[m] = 0$ for $m \neq 0$, (4.7) can be used to estimate the carrier-to-noise ratio (CNR) of the received signal. For the white Gaussian noise case, the amplitude of the impulses for $m \neq 0$ correspond to the term $\left|\bar{\mathscr{A}}_{c_i}(m,0)\frac{\sin\left(2\pi\beta T_s^2 mL'\right)}{\sin\left(2\pi\beta T_s^2 m\right)}\right|$ in (4.6). The train of the impulse-like functions, i.e., $|\bar{\mathscr{A}}_{c_i}(m,0)|$, is associated with the ambiguity function of the always-on and on-demand RSs which have good correlation properties. The period of $|\bar{\mathscr{A}}_{c_i}(m,0)|$ is approximately 1.33 ms. It can be seen in Fig. 4.3 that the amplitude of the impulse train follow the sinc function-like behavior of $\left|\frac{\sin\left(2\pi\beta T_s^2 mL'\right)}{\sin\left(2\pi\beta T_s^2 m\right)}\right|$ which matches the results of Lemma 1.

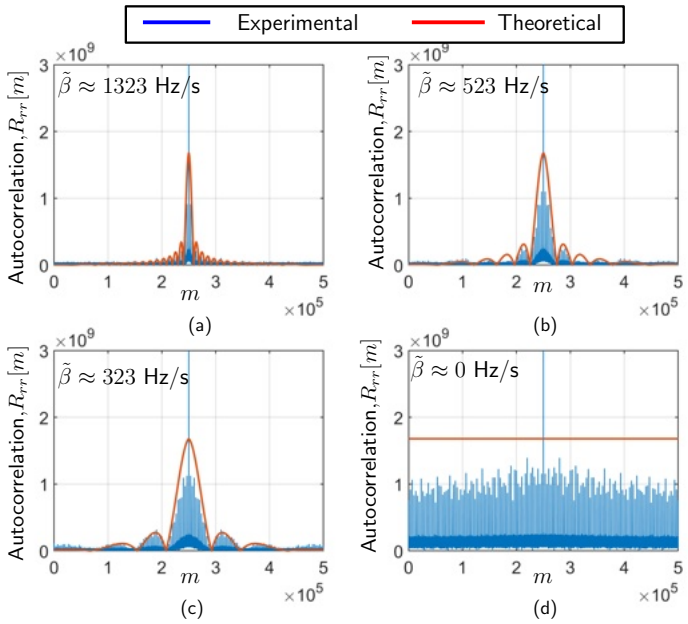


Figure 4.3: Theoretical and experimental autocorrelation function of a time segment of 150 ms for different values of β.

It should be pointed out that for large Doppler rate values, the term $\left|\frac{\sin\left(2\pi\beta T_s^2 mL'\right)}{\sin\left(2\pi\beta T_s^2 m\right)}\right|$ approaches a Kronecker delta. Therefore, large values of Doppler rate will attenuate the impulses. On the other hand,

$$\lim_{\beta\to 0}\left|\frac{\sin\left(2\pi\beta T_s^2 mL'\right)}{\sin\left(2\pi\beta T_s^2 m\right)}\right| = L' \quad \forall m, \tag{4.8}$$

which is the case in Fig. 4.3(d).

Remark 2: Lemma 1 shows that when the Doppler rate is perfectly wiped-off, the autocorrelation function is almost constant as the impulses will have equal amplitudes. Therefore, Lemma 1 can be used to obtain a rough estimate of the Doppler rate by searching over different values of the Doppler rate to find the one that results in a constant autocorrelation function. Assume that the estimated Doppler rate is denoted by $\hat{\beta} = \beta + e_\beta$, where β is the actual Doppler rate of the satellite and e_β is the estimation error for the Doppler rate. β^*

denotes an arbitrarily guessed Doppler rate value. The received signal at the nth time instant when the Doppler rate is wiped off by β^* is denoted by $r'[n]$

$$r'[n] \triangleq \exp(-j2\pi\beta^\star T_s^2 n^2) r[n]. \tag{4.9}$$

The $r'[n]$ contains a residual Doppler rate denoted by $\tilde{\beta} = \beta - \beta^\star$. Note that if $\beta^* = \beta$, the Doppler rate is wiped off perfectly and, since $\lim_{\beta\to 0} \frac{\sin\left(2\pi\beta T_s^2 mL'\right)}{\sin\left(2\pi\beta T_s^2 m\right)} = L'$, it is expected from Lemma 2 that

$$R_{r'r'}[m] = \bar{\alpha}_i \bar{\mathscr{A}}_{c_i}(m,0)L' + R_{ww}[m], \tag{4.10}$$

for $\beta^* = \beta$.

4.4.2 Acquisition

The received signal at the nth time instant when the Doppler rate is wiped-off according to $r'[n] \triangleq \exp(-j2\pi\beta_i T_s^2 n^2) r[n]$. Due to the periodicity of $c(\tau_n)$, $s_i[n]$ has the following property

$$s_i[n+mL] = s_i[n]\exp(j\omega_i mL) \quad 0 \le n \le L-1, \tag{4.11}$$

where $\omega_i = 2\pi f_{D_{i_0}} T_s$ is the normalized Doppler corresponding to the ith transmitting source, and $-\pi \le \omega_i \le \pi$. A vector of L observation samples corresponding to the mth period of the signal is formed as $\mathbf{z}_m \triangleq [r'[mL], r'[mL+1], \ldots, r'[(m+1)L-1]]^\mathsf{T}$. The CPI vector is constructed by concatenating K aggregates of $\mathbf{z}_m$ vectors to form the $KL \times 1$ vector

$$\mathbf{y} = \sum_{i=1}^{N} \mathbf{H}_i \mathbf{s}_i + \mathbf{w}, \tag{4.12}$$

where $\mathbf{s}_i = [s_i[1], \ldots, s_i[L]]^\mathsf{T}$; the $KL \times L$ Doppler matrix is defined as

$$\mathbf{H}_i \triangleq [\mathbf{I}_L, \exp(j\omega_i L)\mathbf{I}_L, \ldots, \exp(j\omega_i (M-1)L)\mathbf{I}_L]^\mathsf{T},$$

where $\mathbf{I}_L$ denotes an $L \times L$ identity matrix; and $\mathbf{w}$ is the noise vector. Similar to [149], the concept of *sequential matched subspace detection* is used to provide an initial estimate for the unknown parameters which are: (i) number of unknown sources, (ii) corresponding RSs, (iii) chirp parameters, and (iv) CPI. A hypothesis testing problem is solved sequentially in multiple stages to detect the active sources in the environment. Unlike [149], where a constant Doppler subspace was used to distinguish between different sources. In this, chapter the matched subspace is defined based on the chirp parameters of each source. At each stage, a test is performed to detect the most powerful source, while the *chirp subspace* of the previously detected sources are nulled. The so-called *general linear detector* [90] is used at each stage of the sequential detection algorithm. In the first stage of the sequential algorithm, the presence of a single source is tested, and if the null hypothesis is accepted, then $\hat{N} \equiv 0$, which means that no source is detected to be present in the environment. If the test rejects the null hypothesis, the algorithm asserts the presence of at least one source and performs the test to detect the presence of other sources in the presence of the previously detected source. The unknown chirp parameters, the RSs of each sources, and the corresponding CPIs are estimated at each stage. In general, if the null hypothesis at the ith level of the sequential algorithm is accepted, the algorithm is terminated and the estimated number of sources will be $\hat{N} \equiv i-1$.

The detection problem of ith RS is defined as a binary hypothesis test

$$\begin{cases} \mathscr{H}_0^i: & i\text{th source is absent} \\ \mathscr{H}_1^i: & i\text{th source is present.} \end{cases} \tag{4.13}$$

Under $\mathscr{H}_1^i$, the signal model can be modeled as

$$\mathbf{y} = \mathbf{H}_i \mathbf{s}_i + \mathbf{B}_{i-1} \boldsymbol{\theta}_{i-1} + \mathbf{w}_{\mathrm{eq}_i}, \tag{4.14}$$

where $\mathbf{B}_{i-1} \triangleq [\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_{i-1}]$ and $\boldsymbol{\theta}_{i-1} \triangleq [\mathbf{s}_1^{\mathsf{T}}, \mathbf{s}_2^{\mathsf{T}}, \ldots, \mathbf{s}_{i-1}^{\mathsf{T}}]^{\mathsf{T}}$ stores the chirp parameters and estimated RS in the previous steps. The decision criteria for the source detection is developed based on the generalize likelihood ratio (GLR). A matched subspace detector for a generic form of (4.13) is derived in [180]. Based on the specific characteristics of the Doppler subspace matrix in (6.3), an alternative derivation of the matched subspace detector is presented in Appendix .1. The likelihood of the GLR detector is

$$\mathscr{L}_i(\mathbf{y}|\omega_i, \beta_i, K_i) = \frac{\mathbf{y}^{\mathsf{H}} \mathbf{P}_{\mathbf{S_i}} \mathbf{y}}{\mathbf{y}^{\mathsf{H}} \mathbf{P}^{\perp}_{\mathbf{B_{i-1}}} \mathbf{P}^{\perp}_{\mathbf{S_i}} \mathbf{P}^{\perp}_{\mathbf{B_{i-1}}} \mathbf{y}}, \tag{4.15}$$

for a given normalized Doppler frequency ω_i, Doppler rate β_i, and CPI K_i. Vector $\mathbf{y}^{\mathsf{H}}$ is the Hermitian transpose of $\mathbf{y}$, $\mathbf{P}_{\mathbf{X}} \triangleq \mathbf{X}(\mathbf{X}^{\mathsf{H}}\mathbf{X})^{-1}\mathbf{X}^{\mathsf{H}}$ denotes the projection matrix to the column space of $\mathbf{X}$, and $\mathbf{P}^{\perp}_{\mathbf{X}} \triangleq \mathbf{I} - \mathbf{P}_{\mathbf{X}}$ denotes the projection matrix onto the space orthogonal to the column space of $\mathbf{X}$. Also, $\mathbf{S}_i \triangleq \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} \mathbf{H}_i$. It should be pointed out that $\mathbf{H}_i^{\mathsf{H}} \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} \mathbf{H}_i = \lambda_i \mathbf{I}$, where the scalar λ_i is the Schur complement of block $\mathbf{C}_{i-1}$, i.e., the upper $(i-1) \times (i-1)$ block of the matrix $\mathbf{C}_i$, whose ijth element is (see Appendix .1)

$$c_{ij} \triangleq \sum_{k=0}^{K-1} \exp\left(j(\omega_j - \omega_i)Lk\right). \tag{4.16}$$

It can be seen from (4.16) that the elements of the matrix $\mathbf{C}_i$, and consequently the scalar λ_i, are scalar functions of the Doppler frequency difference between ith source and the previously detected sources.

Remark 3: Similar calculation to Theorem 9.1 in [90] to derive the probability of detection results in

$$P_{\mathrm{d_i}} = \exp\left(-\rho_i + L\eta_i\right) \sum_{k=0}^{\infty} \frac{\rho_i^k}{k!} \sum_{n=0}^{L+k-1} \frac{(L\eta_i)^n}{n!}, \tag{4.17}$$

where $P_{\mathrm{d_i}}$ is the probability of detection of the ith source and

$$\rho_i = \beta_{\mathrm{acq}} \lambda_i \frac{\|\mathbf{s}_i\|^2}{\sigma_w^2}, \tag{4.18}$$

is the effective SNR of ith source. The probability of detection is a monotonically increasing function of the scalar λ_i. In other words, λ_i provides a measure for the reliability of detection of the ith source. When the Doppler frequencies of the ith source and other sources are very close, λ_i the becomes small which result in a poor detection performance, i.e., $\lim_{\lambda_i \to 0} P_{\mathrm{d_i}} = 0$.

The simplified likelihood can be written as (Appendix .1)

$$\mathscr{L}_i^*(\mathbf{y}) = \arg \max_{\omega_i, \beta_i, K_i} \frac{\|\lambda_i^{-1} \hat{\mathbf{H}}_i^{\mathsf{H}} \hat{\mathbf{P}}_{\mathbf{B}_{i-1}}^{\perp} \mathbf{y}\|^2}{\|\hat{\mathbf{P}}_{\mathbf{B}_{i-1}}^{\perp} \mathbf{y}\|^2 - \|\lambda_i^{-1} \hat{\mathbf{H}}_i^{\mathsf{H}} \hat{\mathbf{P}}_{\hat{\mathbf{B}}_{i-1}}^{\perp} \mathbf{y}\|^2}. \tag{4.19}$$

The likelihood should be compared with predetermined threshold η_i which is designed based on a particular probability of false alarm. For known subspaces and the corresponding projection matrices, the probability of false alarm for the ith stage of the likelihood in (5.10) asymptotically tends to (cf. Theorem 7.1 in [90])

$$P_{\mathrm{fa}_i} = \exp(-L\eta_i) \sum_{n=0}^{L-1} \frac{(L\eta_i)^n}{n!}, \tag{4.20}$$

for a large number of observation samples. In the experimental results presented in Section 5.8, (4.20) is used to determine the threshold.

The ML estimates of the CPI, denoted by $\hat{K}_i$, and the chirp parameters, $(\hat{f}_{D_i}, \hat{\beta}_i)$ can be obtained by maximizing $\mathscr{L}_i(\mathbf{y})$. Accordingly, the least squares (LS) estimate of the ith source, i.e., $\mathbf{s}_i$, is given by

$$\hat{\mathbf{s}}_{\mathrm{acq}_i} = \lambda_i^{-1} \mathbf{H}_i^{\mathsf{H}} \mathbf{P}_{\mathbf{B}_{i-1}}^{\perp} \mathbf{y}. \tag{4.21}$$

The conventional and the proposed cognitive methods use tracking loops which involve the same computational complexity. The main difference between the computational complexity of the proposed cognitive receiver and a conventional receiver stems from the acquisition stage. The number of complex operations is considered as a metric for computational complexity. In the likelihood function (5.10), the size of the projection matrices

increases with the detection stage, i.e., i. However, in [91] (Appendix 8B), a recursive formula is provided to calculate the projection matrix at the ith stage based on the already calculated projection matrix at $(i-1)$th stage. Using the recursive formula presented in this appendix, the complexity of the projection matrix is $\mathscr{O}(K^2)$ where $\mathscr{O}(\cdot)$ denotes the rate of growth of a function, i.e., its order. Consequently, the number of complex operations to calculate the matched subspace detector is $\mathscr{O}((5(KL)^2+KL)N)$.

4.4.3 Tracking

The initial estimate of the chirp parameters $\hat{f}_{D_i}$ and $\hat{\beta}_i$, the estimated CPI $\hat{K}_i$, and the associated likelihood functions $\mathscr{L}_i^*$s are fed to the tracking stage along with the estimated RS. By employing the a phase-locked loop (PLL) and a delay-locked loop (DLL) the delay and the Doppler are tracked over time. The major difference between the proposed tracking loops and the conventional tracking loops is the RS-locked loop (RSLL). The tracked Doppler and the delay are used to lock the estimated RS signal along with the code and carrier-phase. The details of the tracking loops are discussed next.

4.4.3.1 RS-locked loop (RSLL)

The RS in the tracking loop for the ith source is initialized with the RS estimated in the acquisition stage $\hat{\mathbf{s}}_{\text{acq}_i}$. Therefore, $\hat{\mathbf{s}}_{0_i} = \hat{\mathbf{s}}_{\text{acq}_i}$. Assuming that the ith source is being tracked, in this subsection the subscript i is dropped for convenience of notation. Let $\hat{t}_{s_k}$ and $\hat{f}_{D_k}$ be the code-phase and the Doppler estimates at time-step k in the tracking loop, respectively. In the kth time-step of the tracking loop, the estimated RS is updated by coherently accumulating

the measurement at the kth step of the tracking loop when the delay and Doppler are wiped-off. If the subspace spanned by the columns of $\mathbf{S}_i = \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{H}_i$ is viewed as the *ith source's signal subspace*, and the orthogonal subspace as the *noise subspace*, then the likelihood $\mathscr{L}_i^*$ in (4.19) can be interpreted as an estimated SNR corresponding to the ith gNB. The reader is referred to [180] for further interpretations of matched subspace detectors. The gain loop of the RSLL is designed based on the performance of the acquisition. If the estimated SNR of the ith source, i.e. , $\mathscr{L}_i^*$, is large, the tracking loop relies more on the acquisition by diluting the contribution of the new measurements in the estimation of the RS. Hence, the metric $\mathscr{L}_i^*$ informs the performance of the detection of the ith source to the tracking loops. It will be shown that this link between the acquisition and the tracking results in a dramatic effect on the navigation performance.

The nth sample of the updated RS at kth time-step of tracking loop is calculated as

$$\begin{aligned}\hat{s}_k[n] = &\frac{k}{k+1}\cdot\frac{\hat{s}_{k-1}}{||\hat{s}_{k-1}||}[n] \\ &+\frac{G_i}{k+1}\cdot\frac{y_k[n+\hat{n}_{d_k}]\exp\big(-j2\pi\hat{f}_{D_k}n\big)}{||y_k[n+\hat{n}_{d_k}]||},\end{aligned} \tag{4.22}$$

where $\hat{n}_{d_k} \triangleq \left\lfloor \frac{\hat{t}_{s_k}}{T_s} \right\rceil$ and $\lfloor\cdot\rceil$ denotes rounding to the closest integer, and $G_i = \frac{1}{\hat{K}_i}\cdot\frac{1}{\mathscr{L}_i^*}$, denotes the loop-gain for the RSLL.

4.4.3.2 PLL and DLL

To track the phase of the received signals, a PLL, consisting of a phase discriminator, a loop filter, and a numerically-controlled oscillator (NCO) with a second-order PLL with a loop filter transfer function is employed. The estimate of the Doppler frequency at each time-step k is deduced by dividing the rate of change of the carrier-phase error $v_{\mathrm{PLL},k}$ in

rad/s by 2π. Assuming a zero initial carrier-phase, the estimate of the carrier-phase estimate at time-step k is updated according to $\hat{\theta}_k = \hat{\theta}_{k-1} + v_{\text{PLL}} \cdot T_{\text{sub}}$, where T_{sub} is the time length of coherent accumulation in the tracking loop.

Subsequently, a carrier-aided DLL, consisting of an early-minus-late discriminator and a simple gain loop filter is used to follow the delay of each T_{sub} of the measured signals. The rate of change of the code-phase v_{DLL} is used to update code-phase of the received signals, assuming low-side mixing at the radio frequency front-end, according to

$$\hat{t}_{s_{k+1}} = \hat{t}_{s_k} - \left(v_{\text{DLL},k} + \frac{v_{\text{PLL},k}}{2\pi f_c} \right) \cdot T_{\text{sub}}. \tag{4.23}$$

Fig. 4.4 illustrates the proposed tracking loops. The difference between the proposed tracking loop and conventional tracking loops is highlighted in red color. The core blocks of the proposed tracking loop are similar to the traditional carrier and code-phase tracking architectures [122]. In order to track the time-variations of the carrier-phase, a traditional PLL is composed of three basic constituent blocks: (i) a code and carrier-phase discriminator, which is in charge of providing output measurements that, on average, are proportional to the code-phase and carrier-phase error to be compensated; (ii) a loop filter, which is nothing but a very narrow low-pass filter that smoothes the variability caused by thermal noise at the phase detector output; and (iii) a numerically-controlled oscillator (NCO) for generating the local carrier replica based on the corrections imposed by the loop filter output. The main difference between the proposed tracking loop and conventional tracking loops is the local RS generator with adaptive gains as described in Section 4.4.3.1.

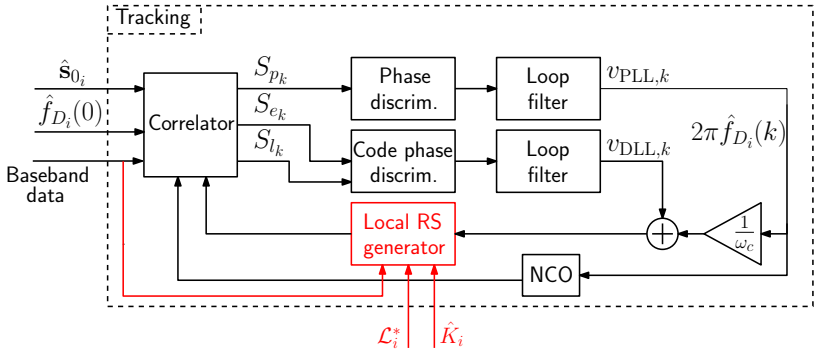


Figure 4.4: Tracking loops: The main difference between the proposed tracking loop and conventional tracking loops [122] is the local RS generator with adaptive gains which is highlighted in red color as described in Section 4.4.3.1.

Figure 4.5: Experimental environment for the 5G NR scenario showing UAV trajectory and the two gNBs.

4.5 Experimental Results

The performance of the proposed receiver is assessed in three different scenarios: (i) to navigate a UAV with terrestrial 5G NR signals, (ii) to localize an unknown 5G gNB in the environment from measurements made by a mobile ground vehicle, and (iii) to localize a stationary receiver with Starlink LEO SV downlink signals. The objectives of the experiments are to: (i) demonstrate the performance of the acquisition of unknown signals in the *almost static* and *intensive Doppler rate* scenarios, (ii) assess the effect of CPI estimation on the navigation performance, (iii) examine the effect of the proposed RSLL tracking loop on the quality of RS estimation, and (iv) analyze the transmission of Starlink unknown signals to detect the always-on and on-demand modes of Starlink LEO SVs. In the following experiments, (4.20) is used to calculate the threshold η_i for a probability of false alarm of 10^{-4} for all the stages.

4.5.1 Experiment 1: UAV Navigation with 5G NR Signals

An Autel Robotics X-Star Premium UAV equipped with a single-channel Ettus 312 universal software radio peripheral (USRP) connected to a consumer-grade 800/1900 MHz cellular antenna. The cellular receivers were tuned to the cellular carrier frequency 632.55 MHz, which is a 5G NR frequency allocated to the U.S. cellular provider T-Mobile. Samples of the received signals were stored for off-line post-processing. The experimetnal layout is presented in Fig. 4.5. During the course of the experiment, the receiver was listening to two gNBs referred to as gNB1 and gNB2 in Fig. 4.5. The ground-truth reference trajectory was taken from the on-board Ettus 312 USRP GPS solution.

The main limitations of the algorithm are: (i) the proposed receiver, requires periodic RSs in the downlink signal, and (ii) in the signal model, a single tap channel which corresponds to the LOS path with arbitrary channel gain α is considered. More precisely, the channel impulse response is modeled as $h[n] = \alpha\delta[n - n_d]$, where α is the complex channel gain between the transmitter and the receiver, and n_d is the code-delay corresponding to the transmitter and the receiver. This channel model considers a *flat fading* scenario, where the effect of multiple "close" paths is considered in a single path gain α. Based on the underlying distribution of α, the considered $h[n]$ can model a *Rayleigh* or *Rician* flat fading channel.

Recall from (4.16) and (4.17) that when the apparent Doppler frequencies of the unknown sources are close to each other, the effective SNR, i.e., ρ_i defined in (4.18), will have a small value which in turn results in a poor detection/acquisition performance. Therefore, in order for the unknown sources to have enough separation in the Doppler subspace, it is practically preferred to perform the acquisition stage when the UAV is moving. However, to challenge the proposed receiver, the acquisition is performed in the starting phase of the flight when the UAV is almost stationary. The Doppler frequency depends on the LOS velocity between the UAV and the gNBs. When the UAV is almost stationary, the Doppler subspaces of the two gNBs will overlap which results in a small ρ_i. It will be seen that in the starting phase of the flight, there is only going to be a very slight separation in the Doppler subspace (on the order of 1 Hz) which is due to very small movements of the UAV.

4.5.1.1 Detection and Tracking

The ML estimate of the CPI was obtained to be 100 for both gNBs. The likelihoods in the two different stages of the acquisition are plotted in Fig. 4.6(a). The blue curve demonstrates the likelihood in the first stage. It can be seen that the only one peak at -1 Hz is observed in the blue curve which corresponds to the first detected gNB. Due to the mentioned Doppler subspace overlap, the two sources are masking each other in the Doppler subspace. In the second stage the first gNB is nulled (red curve in 4.6(a)). After nulling the first gNB, a second peak appears in the likelihood function which is located at 0 Hz and corresponds to the second gNB. Fig. 4.6(b) demonstrates the carrier-phase errors corresponding to the two gNBs, showing that the two gNBs are being tracked.

4.5.1.2 Post-Acquisition and Post-Tracking Reconstructed Frame

After the detection of each gNB, (4.21) is used to estimate the corresponding RS. In this subsection, the reconstructed RS frame structure is presented for the post-acquisition stage where the estimate of the RS is given in (4.21), and after the estimated RS is refined in the tracking loops using (4.22). Fig. 4.7 demonstrates the frame structure of the estimated RS for gNB1. Fig. 4.7(a) shows the resulting RS frame structure after acquisition, and Fig. 4.7(b) shows the refined estimated RS after tracking. Comparing the reconstructed frame in 4.7 with Fig. 4.2 shows that other than the broad cast signals (SS/PBCH blcok), several on-demand active subcarriers are also detected. As discussed in Section 5.5, the subcarriers indicated with dark blue color code in the OFDM frame are the subcarrier that do not correspond to the RSs. Ideally, in the estimated RS, the energy of these subcarriers should be zero (darker blue). However, due to the effect of noise, these subcarriers may not

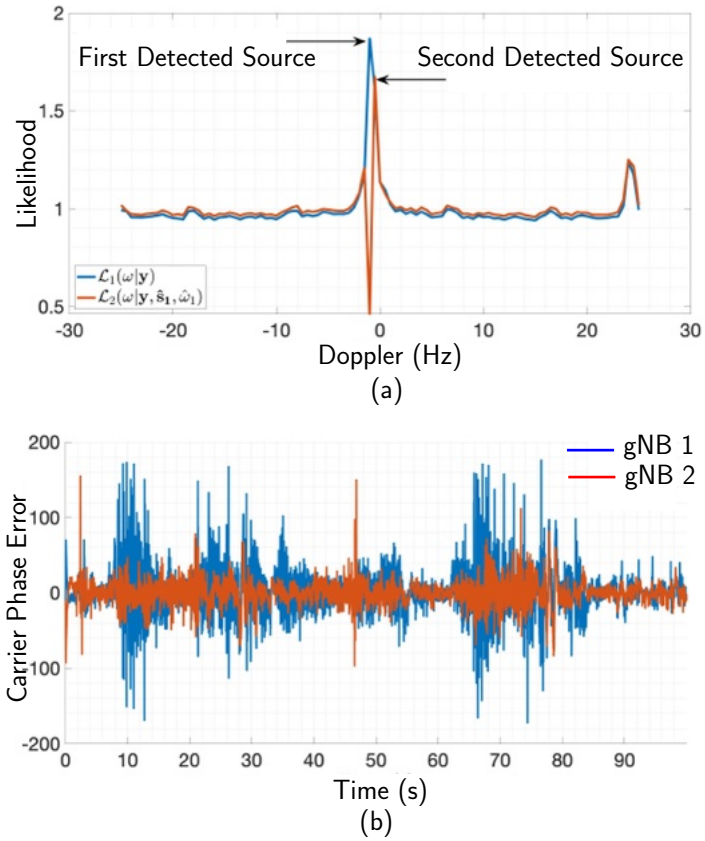


Figure 4.6: Acquisition and tracking 5G gNBs: (a) The two gNBs are detected although their Doppler frequencies are almost right on the top of each other. The likelihood in the first stage (blue curve) exceeds the threshold which means that the first gNB is detected. In the likelihood of the second stage (the red curve) the first gNB is nulled, and the second gNB is detected. (b) The carrier-phase error in the tracking loops for the two gNBs. The carrier-phase errors of both detected sources are converging which means that the tracking loops are locked for both detected sources.

appear in dark blue color. It can also be observed that the post-tracking estimated RS is less noisy (darker) than the RS obtained by (4.21) in the acquisition.

4.5.1.3 Navigation Framework

Next, the pseudorange observables from the two gNBs will be used to estimate the 2D position of the UAV-mounted receiver, denoted by $\boldsymbol{r}_r$. The code-phase in (4.23) can be used

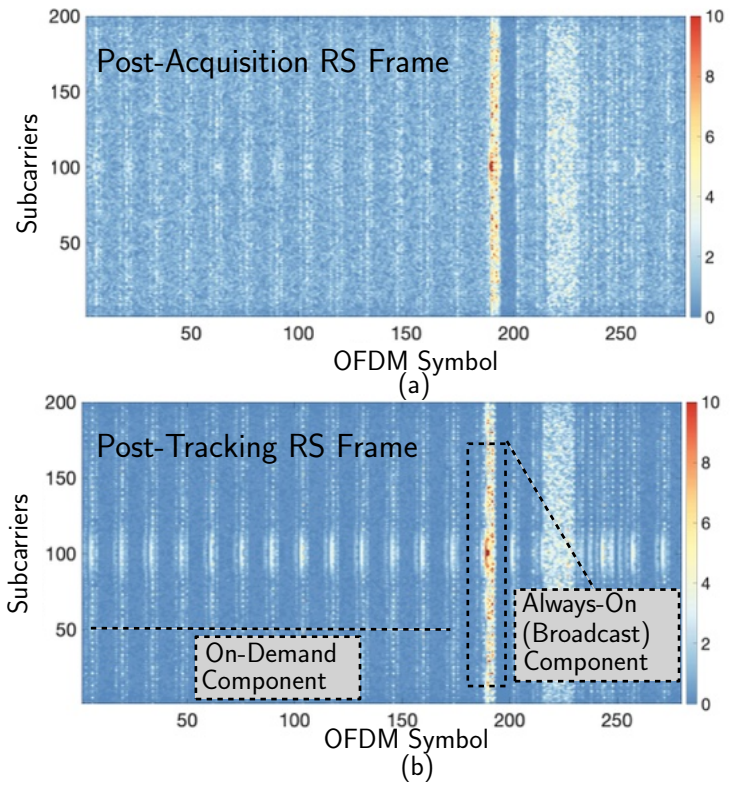


Figure 4.7: The reconstructed frame structure: (a) post-acquisition stage, and (b) post-tracking stage. The blue subcarriers correspond to non-active subcarriers or the subcarriers which do not correspond to the RS. Ideally these subcarriers should have zero energy in the detected RS. The non-active subcarriers in (b) have less energy in the detected RS which means that the post-tracking version of the estimated RS is less noisy.

to readily deduce the pseudorange observables. The pseudorange, expressed in meters, from the n-th gNB can be modeled as

$$z_n(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_n}\| + c \cdot [\delta t_r(k) - \delta t_{s_n}(k)] + v_n(k), \tag{4.24}$$

where $\boldsymbol{r}_{s_n}$ is the 2D position of the n-th gNB, c is the speed of light, δt_r and δt_{s_n} are the receiver 'sand n-th gNB's clock biases, respectively, and v_n is the measurement noise, which is modeled as a zero-mean white Gaussian sequence with variance σ_n^2. The location of the gNBs were mapped prior to the experiment, therefore, $\boldsymbol{r}_{s_n}$ is known. The terms $c \cdot [\delta t_r(k) - \delta t_{s_n}(k)]$ are combined into one term as they do not need to be estimated separately,

yielding

$$c\delta t_n(k) \triangleq c \cdot [\delta t_r(k) - \delta t_{s_n}(k)]. \tag{4.25}$$

Cellular gNBs possess tighter carrier frequency synchronization than time (code-phase) synchronization– the code-phase synchronization requirement as per the cellular protocol is typically within 1.1 μs [177]. It is assumed that the resulting clock biases in the TOA estimates will be very similar, up to an initial bias. Consequently, one may leverage this relative frequency stability to eliminate parameters that need to be estimated. The following re-parametrization is proposed

$$c\bar{\delta} t_n(k) \triangleq c\delta t_n(k) - c\delta t_n(0) \equiv c\delta t(k) + \varepsilon_n(k), \ \ \forall n \tag{4.26}$$

where $c\delta t$ is a time-varying common bias term independent of the nth gNB, and ε_n is the deviation of $c\bar{\delta} t_n$ from this common bias and is treated as measurement noise. Using (4.26), the TOA measurement (5.20) can be re-parameterized as

$$z_n(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_n}\| + c\delta t(k) + c\delta t_{0_n} + \eta_n(k), \tag{4.27}$$

where $c\delta t_{0_n} \triangleq c\delta t_n(0)$ and $\eta_n(k) \triangleq \varepsilon_n(k) + v_n(k)$ is the overall measurement noise. Note that $c\delta t_{0_n}$ can be obtained by knowing the initial receiver's position and from the initial measurement $z_n(0)$, according to $c\delta t_{0_n} \approx z_n(0) - \|\boldsymbol{r}_r(0) - \boldsymbol{r}_{s_n}\|$.

The TOA measurements were fed to an extended Kalman filter (EKF) to estimate the state vector $\boldsymbol{x} \triangleq \left[\boldsymbol{r}_r^\mathsf{T}, \dot{\boldsymbol{r}}_r^\mathsf{T}, c\delta t, c\dot{\delta} t\right]^\mathsf{T}$, where $\dot{\boldsymbol{r}}_r$ is the UAV's 2–D velocity vector and $\dot{\delta} t$ is the clock drift. A white noise acceleration model was used for the UAV's dynamics, and a standard double integrator driven by process noise was used to model the clock bias and drift dynamics [20]. As such, the discrete-time dynamics model of $\boldsymbol{x}$ is given by

$$\boldsymbol{x}(k+1) = \mathbf{F}\boldsymbol{x}(k) + \boldsymbol{w}(k), \tag{4.28}$$

where $\mathbf{F} = \text{diag}\left[\mathbf{F}_{\text{pv}}, \mathbf{F}_{\text{clk}}\right]$,

$$\mathbf{F}_{\text{pv}} = \begin{bmatrix} \mathbf{I}_2 & T\mathbf{I}_2 \\ \mathbf{0}_{2\times 2} & \mathbf{I}_2 \end{bmatrix}, \quad \mathbf{F}_{\text{clk}} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \tag{4.29}$$

and T is the time interval between two measurements; and $\boldsymbol{w}(k)$ is the process noise, which is modeled as a zero-mean white random sequence with covariance matrix $\mathbf{Q} = \text{diag}\left[\mathbf{Q}_{\text{pv}}, \mathbf{Q}_{\text{clk}}\right]$ where

$$\mathbf{Q}_{\text{pv}} = \begin{bmatrix} \frac{T^3}{3}\tilde{\mathbf{Q}}_{xy} & \frac{T^2}{2}\tilde{\mathbf{Q}}_{xy} \\ \frac{T^2}{2}\tilde{\mathbf{Q}}_{xy} & T\tilde{\mathbf{Q}}_{xy} \end{bmatrix}, \tag{4.30}$$

$$\mathbf{Q}_{\text{clk}} = c^2 \begin{bmatrix} S_{\tilde{w}_{\delta t}} T + S_{\tilde{w}_{\dot{\delta} t}} \frac{T^3}{3} & S_{\tilde{w}_{\dot{\delta} t}} \frac{T^2}{2} \\ S_{\tilde{w}_{\dot{\delta} t}} \frac{T^2}{2} & S_{\tilde{w}_{\dot{\delta} t}} T \end{bmatrix}, \tag{4.31}$$

$\tilde{\mathbf{Q}}_{xy} \triangleq \text{diag}\left[\tilde{q}_x, \tilde{q}_y\right]$, and the x, y acceleration process noise spectra of the white noise acceleration model were set to $\tilde{q}_x = \tilde{q}_y = 5\ \text{m}^2/\text{s}^3$, the time interval between two measurements was $T = 0.0267$ s, and the receiver's clock process noise spectra were chosen to be $S_{\tilde{w}_{\delta t}} = 1.3 \times 10^{-22}$ and $S_{\tilde{w}_{\dot{\delta} t}} = 7.9 \times 10^{-25}$ which are that of a typical temperature-compensated crystal oscillator (TCXO) [239]. Note that $\boldsymbol{r}_r$ is expressed in an east-north-up (ENU) frame centered at the UAV's true initial position. The EKF state estimate was initialized at $\hat{\boldsymbol{x}}(0) = \mathbf{0}_{6\times 1}$ with an initial covariance of $\mathbf{P}(0) = \text{diag}[3{\cdot}\mathbf{I}_{2\times 2}, \mathbf{I}_{2\times 2}, 10^{-2}, 10^{-4}]$. The measurement noise covariance was set to $\mathbf{R} = \mathbf{I}_{2\times 2}$.

Effect of RSLL loop gain on the navigation results: Next, the effect of the RSLL loop gain on the navigation results is assessed. The RSLL loop gain is set to be $G_i = \frac{1}{\hat{K}_i} \cdot \frac{1}{\mathscr{L}_i^*}$, where $\mathscr{L}_i^*$ is the likelihood of the ith Rs, and the $\hat{K}_i$ is the estimated CPI corresponding to the ith RS. Fig. 4.8 demonstrates the position RMSE in terms of the RSLL loop gain.

According to the obtained values of $\hat{K}_i$, and $\mathscr{L}_i^*$ in this experiment, the designed RSLL loop gains are $G_1 = \frac{1}{\hat{K}_1} \cdot \frac{1}{\mathscr{L}_1^*} = 0.002$ and $G_2 = \frac{1}{\hat{K}_2} \cdot \frac{1}{\mathscr{L}_2^*} = 0.005$. To assess the effect of

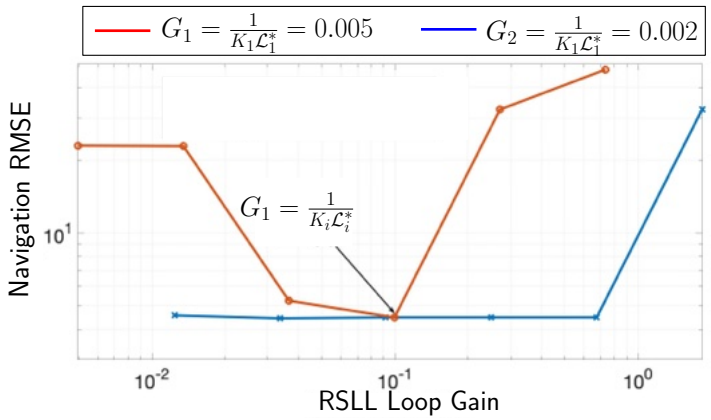


Figure 4.8: The effect of the loop gain on the navigation RMSE. The minimum RMSE is obtained when $G_1 = \frac{1}{\hat{K}_1} \cdot \frac{1}{\mathscr{L}_1^*}$ and $G_2 = \frac{1}{\hat{K}_2} \cdot \frac{1}{\mathscr{L}_2^*}$.

the loop gain on the navigation RMSE, the loop gain for the second RS is set to 0.002, and the loop gain for the first RS is swept between different orders of magnitude as $5 \times [10^{-6}, 10^{-5}, \ldots, 10^{-1}]$ (blue curve). Similarly, the loop gain for the first RS is set to be 0.005, and sweeping the loop gain for the second RS different orders of magnitude as $2 \times [10^{-6}, 10^{-5}, \ldots, 10^{-1}]$. It can be seen that the least navigation RMSE is obtained by selecting $G_1 = \frac{1}{\hat{K}_1} \cdot \frac{1}{\mathscr{L}_1^*}$, and $G_2 = \frac{1}{\hat{K}_2} \cdot \frac{1}{\mathscr{L}_2^*}$ as the loop gains corresponding to the first and the second sources, respectively.

Effect of CPI on the navigation solution: Next, the effect of CPI selection on the navigation results is assessed. Fig. 4.9(a) compares the RMSE for different values of CPI. It can be seen that if one selects a CPI which is less than a particular value, the navigation solution does not converge. It can also be observed that for a range of CPIs the error would be bounded between 4.2 to 5.8 m in the 416 m of flight trajectory. Fig. 4.9(b) shows the estimated trajectories via the proposed receiver and the receiver in [185] which only uses the SS/PBCH block, and the ground truth trajectory.

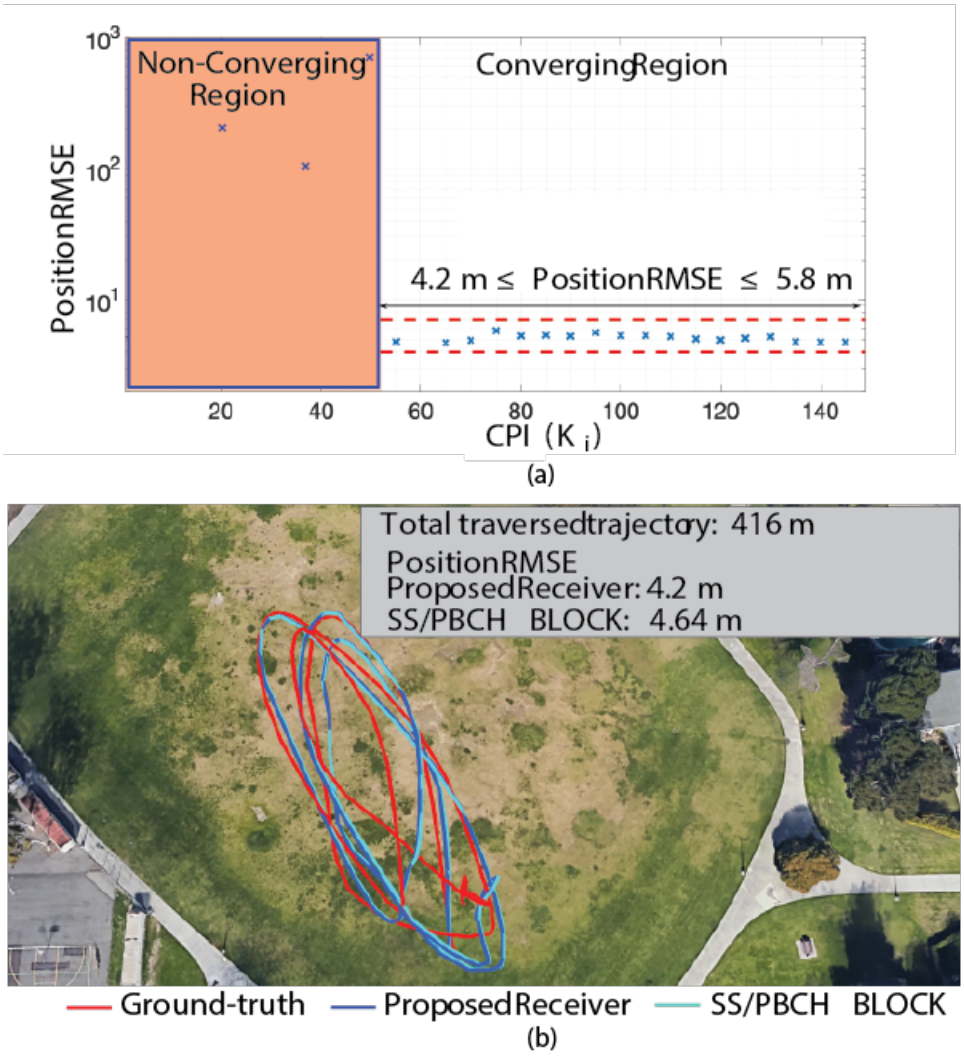


Figure 4.9: (a) The navigation solution for different values of CPIs demonstrates a region where the solution does not converge. (b) The estimated trajectories via the proposed receiver and the receiver in [185] which only uses the SS/PBCH block, and the ground truth trajectory.

4.5.2 Experiment 2: Cognitive Sensing a 5G NR gNB on a Ground Vehicle

A ground vehicle was equipped with a quad-channel National Instrument (NI) USRP-2955 and two consumer-grade 800/1900 MHz cellular antennas to sample 5G signals near Ohio Stadium in Columbus, Ohio, USA. One channel from the USRP was tuned to a 632.55

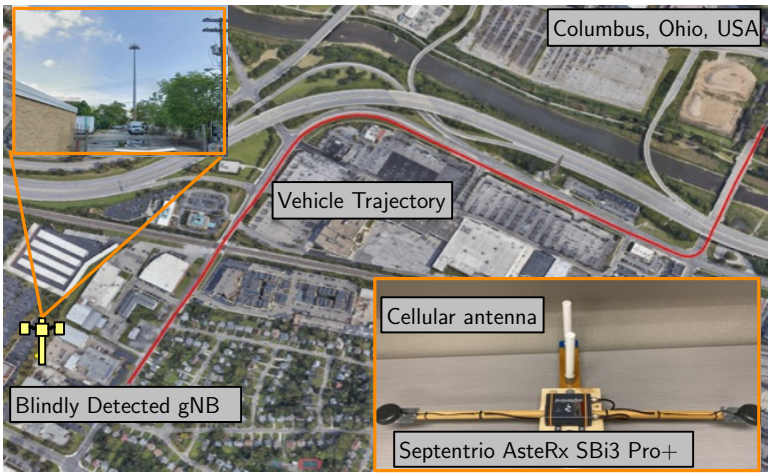


Figure 4.10: The environment layout, vehicle trajectory, and experiment setup. The true location and a photo of the site of the blindly detected gNB are shown.

MHz carrier frequency, which is a 5G NR frequency allocated to the U.S. cellular provider T-Mobile. The sampling rate was set to 20 Mega-samples per second (MSps) and the sampled 5G signals were stored on a laptop for post-processing. In order to obtain the vehicle's trajectory, the vehicle was equipped with a Septentrio AsteRx SBi3 Pro+ with a dual antenna multi-frequency GNSS receiver with real-time kinematic (RTK) and an industrial-grade inertial measurement unit (IMU). The vehicle's traversed a trajectory of 1.79 km. Fig. 5.7 shows the environment layout, the vehicle trajectory, and the experiment setup.

The location of the gNB and the transmitted RS from the gNB were unknown to the receiver. The goal of this experiment was to cognitively sense the location of the gNB via the proposed receiver. Only the carrier frequency of the transmitted signal was known to the receiver. Fig. 5.8 demonstrates the acquisition results. It can be seen that five sources were detected by the receiver. The detected sources could correspond to either gNBs or false

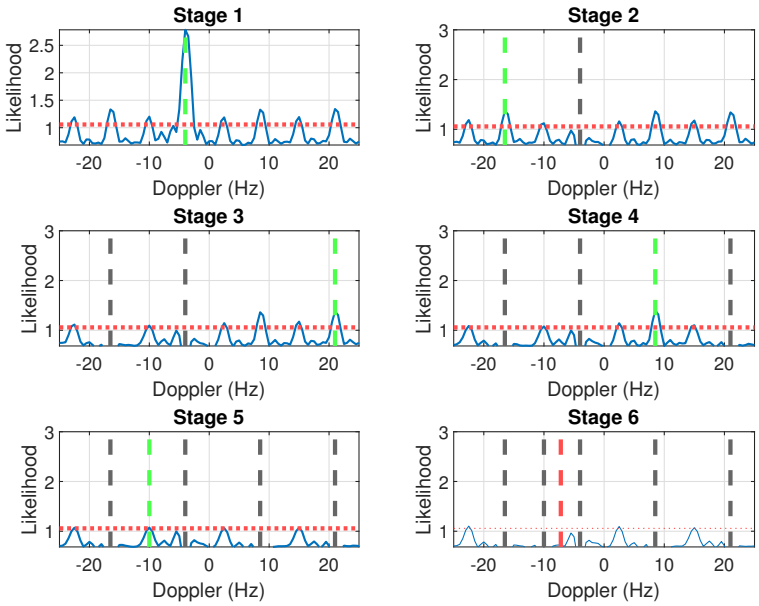


Figure 4.11: The acquisition results: Five sources are detected in the acquisition stage. The red dashed horizontal line is the threshold and the green vertical line corresponds to the detected source at each stage. The gray vertical lines are the previously detected sources at each stage.

alarm due to multipath. The first detected source in Stage 1 of the acquisition algorithm has the largest likelihood, therefore, it corresponds to the strongest path.

The transmitter and receiver clock terms, i.e., $\delta t_r(k)$ and $\delta t_{s_n}(k)$ in (5.20), are both unknown to the receiver. Assuming a first-order clock model for both the gNB and the receiver, the combined clock term in (5.20) can be written as $c\delta t_n(k) = c \cdot [\delta t_r(k) - \delta t_{s_n}(k)] \triangleq \xi + \psi k$ where ξ is the clock bias and ψ is the clock drift [21]. Note that $\boldsymbol{r}_r(k)$ is known and the receiver uses pseudorange observables to estimate the gNB's position $\boldsymbol{r}_s$. Next, define the parameter vector $\boldsymbol{x} \triangleq [\boldsymbol{r}_s^\mathsf{T}, \xi, \psi]^\mathsf{T}$. Let $\boldsymbol{z}$ denote the vector of all the pseudorange observables stacked together. Then, one can write the measurement equation given by $\boldsymbol{z} = \boldsymbol{g}(\boldsymbol{x}) + \boldsymbol{v}_z$, where $g(\boldsymbol{x})$ is a vector-valued function that maps the parameter vector $\boldsymbol{x}$ to the pseudorange observables according to (5.20), and $\boldsymbol{v}_z$ denotes the vector of all measurement noises stacked together. Next, a nonlinear least-squares (NLS) estimator was used to estimate $\boldsymbol{x}$ denoted by $\hat{\boldsymbol{x}}$. The estimated position was validated by on-site verification. The 2D position error of the estimated gNB found to be 5.83 m. The true location of the gNB and the estimated location of the gNB are shown in Fig. 5.11.

Fig. 4.12 demonstrates the delay tracking results for each source versus the true delay which was obtained according to the true location of the gNB and the ground truth trajectory of the receiver. The estimated Doppler is plotted in Fig. 5.10. It can be seen that the tracked Doppler using the method in [185] which only relies on always-on signals has a larger estimation variance compared to the proposed method.

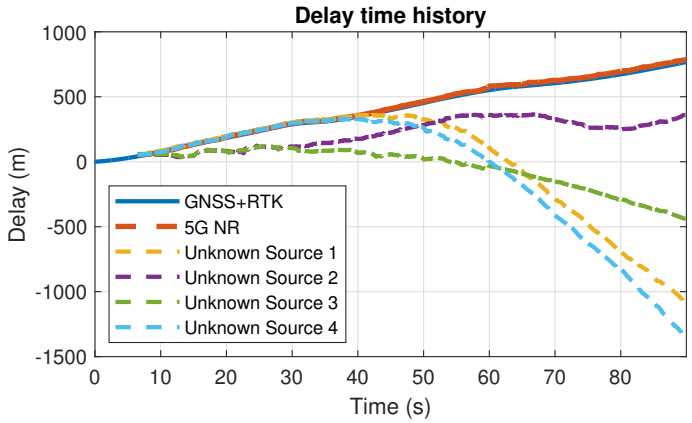


Figure 4.12: Delay tracking results of the detected sources versus the true delay corresponding to the gNB. The delay of one of the sources matches the true delay. In this chapter, the cognitive sensing of the gNB is considered. The cognitive sensing of multipath and other interfering components can be considered in future work.

4.5.3 Experiment 3: Stationary Positioning with Starlink LEO SV Signals

A stationary National Instrument (NI) universal software radio peripheral (USRP) 2945R was equipped with a consumergrade Ku antenna and low-noise block (LNB) downconverter to receive Starlink signals in the Ku-band. The sampling rate was set to 2.5 MHz and the carrier frequency was set to 11.325 GHz to record Ku signals over a period of 800 s. Six SVs were detected this period. To avoid redundancy, the acquisition and tracking results of one of the Starlink SVs are presented next.

4.5.3.1 Acquisition

The acquisition stages in the proposed receiver is shown in Fig. 4.15. As it can be seen in this figure, in the first stage of the acquisition, one source is detected at the normalized Dopplre frequency of 199 Hz. Finally, In the second stage, the Doppler subspace of the first source is nulled and the resulting likelihood is less than the threshold or equivalently $\hat{N} = 1$.

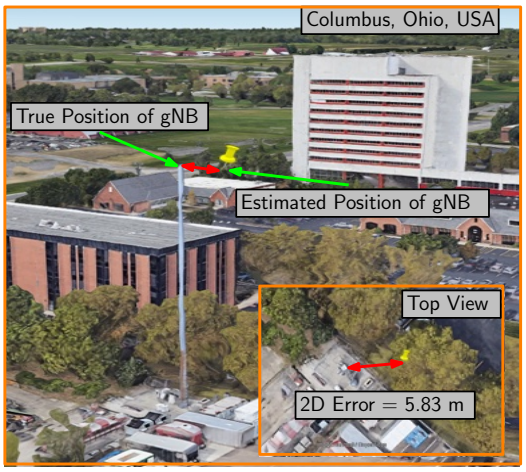


Figure 4.13: The cognitive sensing results: The True position of the gNB and the blindly estimated position are plotted. The 2D error was found to be 5.83 m.

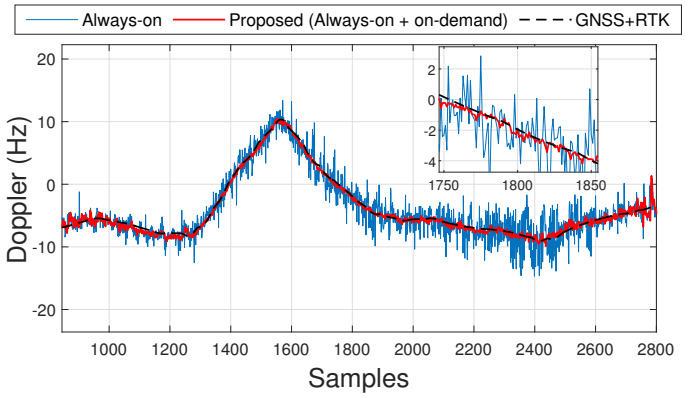


Figure 4.14: The estimated Doppler using the proposed method which exploits the always-on and on-demand components versus the method in [185].

4.5.3.2 The effect of CPI on Tracking Performance

Fig. 5.15 demonstrates the carrier-phase error for the different values of K_1= 40 and the K_1=300 which was the ML estimate of the CPI obtained by maximizing (5.10) over different

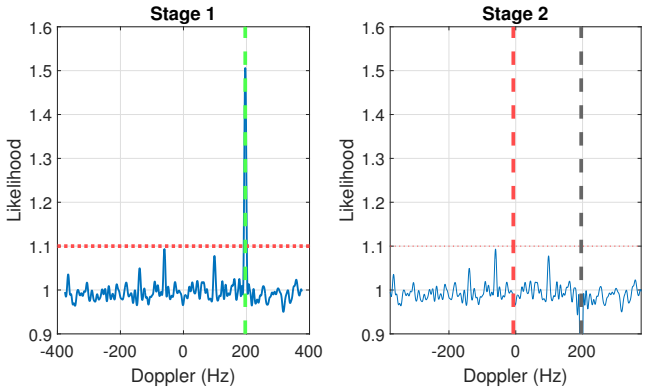


Figure 4.15: Acquisition stages in the proposed receiver for Starlink downlink signals showing the likelihood function (33) at each stage and the detected and nulled source. In the first stage, a source is detected at 200 Hz (dashed green line). In the second stage the first detected source is nulled.

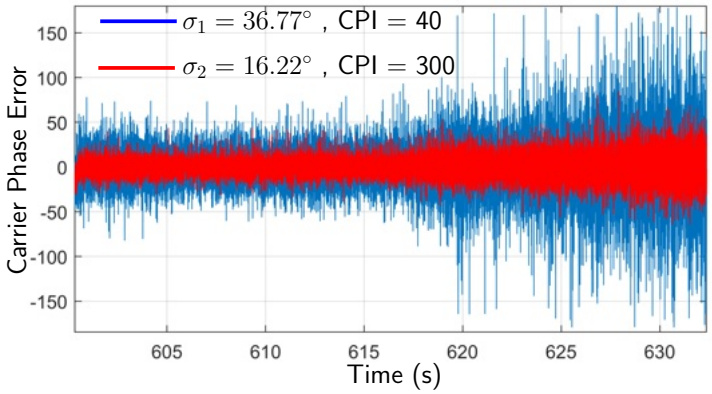


Figure 4.16: Carrier-phase error for arbitrary selected CPI of 40, and the ML estimated CPI of 300.

Table 4.1: Positioning Results Comparison between values of CPI

	CPI (K_1) = 300	**CPI (K_1) = 40**	**CPI (K_1) = 30**
2D Error	6.5 m	22.1 m	Not-converging

values of CPI. As it can be seen in Fig. 5.15, the standard deviation of the carrier-phase error for For K_1=300 is smaller than that of the case where CPI is arbitrary selected to be K_1=40.

4.5.3.3 Navigation results

The navigation results can be seen in Fig. 6.6. The experimental setup and the navigation framework is similar to the setup in [147]. Six starlink satellite was tracked using the proposed receiver. The receiver position was initialized as the centroid of all SV positions, projected onto the surface of the earth, yielding an initial position error of 200 km. The final two dimensional error was 6.5 m using the six Starlink LEO SVs. Table I compares the 2D positioning results for different values of CPI. It can be seen that if one select CPI = 30, the 2D navigation solution does not converge. The skyplot of the satellites and the navigation results are shown in Fig. 6.6.

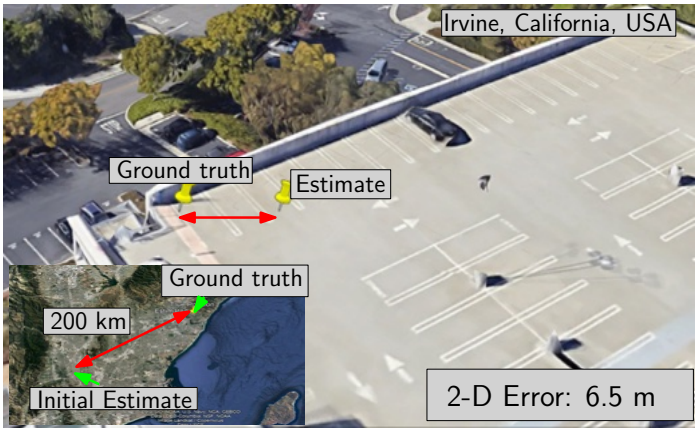


Figure 4.17: Environment layout, Skyplot, and positioning results.

Chapter 5: Acquisition, Doppler Tracking, and Positioning With Starlink LEO Satellites: First Results

5.1 Introduction

Theoretical and experimental studies have demonstrated the potential of low Earth orbit (LEO) broadband communication satellites as promising reliable sources for navigation [73, 119, 141, 174]. Companies like Amazon, Telesat, and SpaceX are deploying so-called *megaconstellations* to provide global broadband internet [173]. In particular, launching thousands of space vehicles (SVs) into LEO by SpaceX can be considered as a turning-point in the future of LEO-based navigation technologies. Although they suffer from higher Doppler effect, signals received from LEO SVs can be about 30 dB stronger than signals received from medium Earth orbit (MEO) SVs, where global navigation satellite systems (GNSS) SVs reside [141].

Research has shown that one could exploit LEO SV broadband communication signals opportunistically for navigation purposes [73]. Three of the main challenges of navigation with Starlink SV signals are (i) limited information about the signal structure, (ii) very-high dynamics of Starlink LEO SVs, and (iii) poorly known ephemerides. Assuming that Starlink LEO SV downlink signals contains a periodic reference signal (RS), this dissertation tackles

the first challenge by formulating a *matched subspace detection* problem to (i) detect the unknown RS of Starlink SVs and (ii) estimate the unknown period and Doppler frequency. The second challenge is addressed by adopting a second-order model to capture the dynamics of the Doppler frequency, and designing a Kalman filter (KF)-based algorithm which is capable of tracking the unknown parameters of the Doppler model. A blind approach was presented in [144, 145] to exploit partially known signals for navigation purposes. However, these approaches were designed for M-ary phase-shift keying (MPSK) signaling and are incapable of deciphering sophisticated signals, such as Starlink's orthogonal frequency-division multiple access (OFDMA) signals.

This letter makes the following contributions. First, a model for the Starlink LEO SV's downlink signals is presented. Second, an algorithm is proposed to (i) acquire the Starlink LEO SV signals and (ii) track the Doppler frequency of each detected SV. Third, next to [105], the first experimental positioning results with Starlink downlink signals are presented in this dissertation. In [105], an adaptive Kalman filter is used to track the carrier phase of Starlink LEO SVs. However, the method presented in [105] relies on tracking the phase of a single carrier. When a more complicated signal structure is used in the downlink signal, e.g., OFDMA, a more sophisticated method should be developed to exploit the entire signal bandwidth for navigation purposes. Indeed, the method in [105] is not capable of exploiting the entire signal bandwidth, and it only relies on tracking a single frequency component. In this dissertation, by considering a general model for the Starlink downlink signals, the unknown parameters of the signal are estimated for the first time for Starlink LEO SVs, and are subsequently used to detect the Starlink LEO SVs and track their corresponding Doppler frequencies. The proposed method enables one to estimate the synchronization signals of the Starlink LEO SVs.

5.2 Received Signal Model

5.2.1 Starlink Downlink Signals

Except for the carrier frequencies and the bandwidths, more detailed signal specifications of Starlink downlink signals are unavailable to the public. SpaceX uses the Ku-band spectrum for the satellite-to-user links (both uplink and downlink) and the satellite-to-ground contacts are carried out in Ka-band [38]. Software-defined radios (SDRs) allow one to sample bands of the radio frequency spectrum. However, Ku/Ka-bands are beyond the carrier frequency of most commercial SDRs. Hence, in the experiments carried out in this letter, a 10 GHz mixer is employed between the antenna and the SDR to downconvert Starlink LEO SV signals from the Ku-band, namely 11.325 GHz to 1.325 GHz.

In order to formulate a detection problem to detect the activity of Starlink downlink signals, a signal model is proposed which solely relies on the periodicity of the transmitted signals. The logic behind the proposed signal model is that in most commercial communication systems, a periodic RS is transmitted for synchronization purposes, e.g., primary synchronization signals (PSS) in long-term evolution (LTE) and the fifth generation (5G) signals. The following subsection presents a model for the Starlink LEO SV's downlink signals.

5.2.2 Baseband Signal Model

As mentioned previously, in most commercial communication systems, a periodic RS is transmitted, e.g., PSS in OFDMA-based and spreading codes in code division multiple access (CDMA)-based signals. In this dissertation, the Starlink LEO SV downlink signal is

modeled as an unknown periodic signal in the presence of interference and noise. If an RS, such as PSS in OFDMA-based signals, is being periodically transmitted, it will be detected and estimated by the proposed method. By denoting the continues-time signal at time instant t by $c(t)$, and the discrete time signal at time instant n by $c[n]$, the received baseband signal is modeled as

$$\begin{aligned} r[n] = \alpha(c(\tau_n - t_s[n])\exp(j\theta(\tau_n)) \\ + d(\tau_n - t_s[n])\exp(j\theta(\tau_n))) + w[n], \end{aligned} \tag{5.1}$$

where $r[n]$ is the received signal at the nth time instant; α is the complex channel gain between the receiver and the Starlink LEO SV; τ_n is the sample time expressed in the receiver time; $c(\tau_n)$ represents the samples of the complex periodic RS with a period of L samples; $t_s[n]$ is the code-delay between the receiver and the Starlink LEO SV at the nth time instant; $\theta(\tau_n) = 2\pi f_D[n]T_s n$ is the carrier phase in radians, where $f_D[n]$ is the instantaneous Doppler frequency at the nth time instant and T_s is the sampling time; $d_i(\tau_n)$ represents the complex samples of some data transmitted from the Starlink LEO SV; and $w[n]$ is measurement noise, which is modeled as a complex, zero-mean, independent, and identically distributed random sequence with variance σ_w^2.

Starlink LEO SV's signals suffer from very high Doppler shifts. Higher lengths of processing intervals require higher order Doppler models. In order for a Doppler estimation algorithm to provide an accurate estimate of the Doppler frequency, the processing interval should be large enough to accumulate enough power. According to the considered processing interval length in the experiments, it was observed that during the kth processing interval, the instantaneous Doppler frequency is nearly a linear function of time, i.e., $f_D[n] = f_{D_k} + \beta_k n$, where f_{D_k} is referred to as constant Doppler, and β_k is the Doppler rate at the kth processing

interval. The coherent processing interval (CPI) is defined as the time interval in which the constant Doppler, f_{D_k}, and the Doppler rate, β_k, are constant.

The received signal at the nth time instant when the Doppler rate is wiped-off is denoted by $r'[n] \triangleq \exp(-j2\pi\beta_k n^2) r[n]$. One can define *the desired RS* which is going to be detected in the acquisition stage as

$$s[n] \triangleq \alpha c(\tau_n - t_s[n]) \exp\left(j2\pi f_{D_k} T_s n\right), \tag{5.2}$$

and the equivalent noise as

$$\begin{aligned} w_{\text{eq}}[n] &= d(\tau_n - t_s[n]) \exp\left(j2\pi f_{D_k} T_s n\right) \\ &\quad + \exp\left(-j2\pi\beta n^2\right) w[n]. \end{aligned} \tag{5.3}$$

Hence, $r'[n] = s[n] + w_{\text{eq}}[n]$. Due to the periodicity of the RS, $s[n]$ has the following property

$$s[n+mL] = s[n] \exp\left(j\omega_k mL\right) \quad 0 \le n \le L-1, \tag{5.4}$$

where $\omega_k \triangleq 2\pi f_{D_k} T_s$ is the normalized Doppler at the kth CPI, and $-\frac{1}{2} \le \omega_k \le \frac{1}{2}$. A vector of L observation samples corresponding to the mth period of the signal is formed as

$$\mathbf{z}_m \triangleq [r'[mL], r'[mL+1], \ldots, r'[(m+1)L-1]]^{\mathsf{T}}. \tag{5.5}$$

The kth CPI vector is constructed by concatenating M vectors of length L to form the $ML \times 1$ vector

$$\mathbf{y}_k = [\mathbf{z}_{kM}^{\mathsf{T}}, \mathbf{z}_{kM+1}^{\mathsf{T}}, \ldots, \mathbf{z}_{(k+1)M-1}^{\mathsf{T}}]^{\mathsf{T}}. \tag{5.6}$$

Therefore,

$$\mathbf{y}_k = \mathbf{H}_k \mathbf{s} + \mathbf{w}_{\text{eq}_k}, \tag{5.7}$$

where $\mathbf{s} = [s[1], s[2], \ldots, s[L]]^{\mathsf{T}}$, and the $ML \times L$ Doppler matrix is defined as

$$\mathbf{H}_k \triangleq [\mathbf{I}_L, \exp\left(j\omega_k L\right) \mathbf{I}_L, \ldots, \exp\left(j\omega_k (M-1)L\right) \mathbf{I}_L]^{\mathsf{T}}, \tag{5.8}$$

where $\mathbf{I}_L$ is an $L \times L$ identity matrix and $\mathbf{w}_{\text{eq}_k}$ is the equivalent noise vector.

5.3 Proposed Framework

This section, presents the structure of the proposed framework. The proposed receiver consists of two main stages: (i) acquisition and (ii) tracking. In the acquisition stage, an estimate of the period of the RS in the Downlink signal of Starlink SV, and an initial estimate for the Doppler parameters are provided at $k = 0$, which is discussed in the following subsection. In order for the receiver to refine and maintain the Doppler estimate, a tracking stage is also presented.

5.3.1 Acquisition

In this section, a detection scheme is proposed to detect the existence of Starlink LEO SVs in the carrier frequency of 11.325 GHz within a bandwidth of 2.5 MHz, at $k = 0$. The following binary hypothesis test is used to detect the Starlink LEO SV signal

$$\begin{cases} \mathscr{H}_0: & \mathbf{y}_0 = \mathbf{w}_{\text{eq}_0} \\ \mathscr{H}_1: & \mathbf{y}_0 = \mathbf{H}_0\mathbf{s} + \mathbf{w}_{\text{eq}_0}. \end{cases} \tag{5.9}$$

For a given set of unknown variables $\mathscr{W}_0 = \{L, \omega_0, \beta_0\}$, the generalized likelihood ratio (GLR) detector for the testing hypothesis (19) is known as matched subspace detector [51, 180], and is derived as (see Theorem 9.1 in [90])

$$\mathscr{L}(\mathbf{y}_0|\mathscr{W}_0) = \frac{\mathbf{y}_0^{\mathsf{H}}\mathbf{P}_{\mathbf{H_0}}\mathbf{y}_0}{\mathbf{y}_0^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{H_0}}\mathbf{y}_0} \underset{\mathscr{H}_0}{\overset{\mathscr{H}_1}{\gtrless}} \eta, \tag{5.10}$$

where $\mathbf{y}_0^{\mathsf{H}}$ is the Hermitian transpose of $\mathbf{y}_0$, $\mathbf{P}_{\mathbf{H}_0} \triangleq \mathbf{H}_0(\mathbf{H}_0^{\mathsf{H}}\mathbf{H}_0)^{-1}\mathbf{H}_0^{\mathsf{H}}$ denotes the projection matrix to the column space of $\mathbf{H}_0$, $\mathbf{P}^{\perp}_{\mathbf{H}_0} \triangleq \mathbf{I} - \mathbf{P}_{\mathbf{H}_0}$ denotes the projection matrix onto the space

orthogonal to the column space of $\mathbf{H}_0$, and η is the threshold which is predetermined according to the probability of false alarm. Since, $\mathbf{H}_k^{\mathsf{H}}\mathbf{H}_k = M\mathbf{I}_L$ for all k, the likelihood $\mathscr{L}(\mathbf{y}_0|\mathscr{W}_0)$ can be rewritten as $\mathscr{L}(\mathbf{y}_0|\mathscr{W}_0) = \frac{1}{\frac{\|\mathbf{y}_0\|^2}{\frac{1}{M^2}\|\mathbf{H}_0^{\mathsf{H}}\mathbf{y}_0\|^2}-1}$, which is a monotonically increasing function of $\frac{\|\mathbf{H}_0^{\mathsf{H}}\mathbf{y}_0\|^2}{\|\mathbf{y}_0\|^2}$. Hence, the GLR detector (5.10) is equivalent to

$$\frac{\|\mathbf{H}_0^{\mathsf{H}}\mathbf{y}_0\|^2}{\|\mathbf{y}_0\|^2} \underset{\mathscr{H}_0}{\overset{\mathscr{H}_1}{\gtrless}} \eta', \tag{5.11}$$

where η' is determined according to a desired probability of false alarm. The maximum likelihood estimate of $\mathscr{W}_0$ is

$$\hat{\mathscr{W}}_0 = \text{argmax}_{L,\omega_0,\beta_0}\|\mathbf{H}_0^{\mathsf{H}}\mathbf{y}_0\|^2. \tag{5.12}$$

It should be pointed out that the estimated Doppler using (5.12) results in a constant ambiguity denoted by $\omega_a = 2\pi f_a$. This constant ambiguity is accounted for in the navigation filter.

Fig. 5.1 demonstrates the likelihood in terms of Doppler frequency and the period for real Starlink downlink signals. The CPI was set to be 200 times the period. As it can be seen in Fig. 5.1, a Starlink LEO SV downlink signal is detected with a period of 32 μs and at a Doppler frequency of -2745 Hz.

5.3.2 Doppler Tracking Algorithm

It is important to note that the receiver does not have knowledge of the Doppler ambiguity f_a. The Doppler frequency that will be tracked by the receiver contains this constant ambiguity. In order to track the Doppler, a KF-based tracking loop is developed. The KF formulation allows for arbitrary Doppler model order selection, which is crucial due to the LEO SVs' high-dynamics. The KF-based Doppler tracking algorithm is described below.

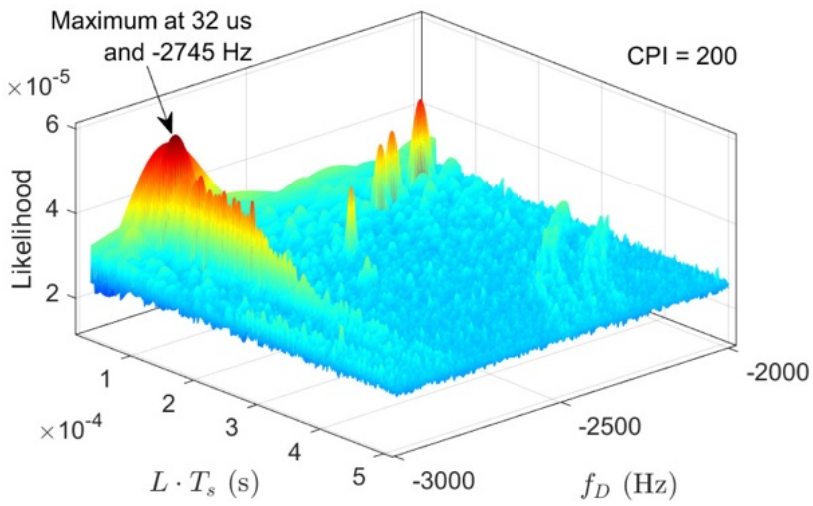


Figure 5.1: Acquisition: The likelihood function versus Doppler frequency and the period at Starlink downlink carrier frequency of 11.325 GHz.

5.3.2.1 Doppler Dynamics Model

The time-varying component of the continuous-time true Doppler, denoted by $f(t)$, is a function of (i) the true range rate between the LEO SV and the receiver, denoted by $\dot{d}(t)$, and (ii) the time-varying difference between the receiver's and LEO SV's clock bias rate, denoted by $\dot{b}(t)$, expressed in meters per second. Hence, $\omega(t) = 2\pi\left[-\frac{\dot{d}(t)}{\lambda} + \frac{\dot{b}(t)}{\lambda} + f_a\right]$, where, $\omega(t) = 2\pi f(t)$, and λ is the carrier wavelength. The clock bias is assumed to have a constant drift, i.e., $b(t) = a \cdot (t - t_0) + b_0$, where a is the clock drift, b is the constant bias, and t_0 is the initial time. Moreover, simulations with Starlink LEO SVs show that the kinematic model $\dddot{d}(t) = \tilde{w}(t)$, where $\tilde{w}$ is a zero-mean white noise process with power spectral density $q_{\tilde{w}}$ holds for short periods of time. Let k denote the time index corresponding to $t_k = kT + t_0$, where $T = MLT_s$ is the sampling interval also known as subaccumulation period, and ML is the number of subaccumulated samples. The vector $\boldsymbol{\omega}_k \triangleq [\omega_k, \dot{\omega}_k]^{\mathsf{T}}$ is considered as

the Doppler state vector for the proposed tracking algorithm. The initial state is given by $\boldsymbol{\omega}_0 = \left[2\pi f_a + \frac{2\pi}{\lambda}(a - \dot{d}(t_0)), -\frac{2\pi}{\lambda}\ddot{d}(t_0)\right]^{\mathsf{T}}$.

5.3.2.2 KF-Based Doppler Tracking

Let $\hat{\boldsymbol{\omega}}_{k|l}$ and $\mathbf{P}_{k|l}$ denote the KF estimate of $\boldsymbol{\omega}_k$ and corresponding estimation error covariance, respectively, given all measurements up to time-step $l \leq k$. The initial estimate $\hat{\boldsymbol{\omega}}_{0|0}$ with a corresponding $\mathbf{P}_{0|0}$ are provided from the acquisition stage. The KF-based tracking algorithm follows a regular KF for the time-update. The measurement update is discussed next. The KF measurement update equations are carried out based on the maximum likelihood estimate of the Doppler. The Doppler wipe-off is performed as $\tilde{r}_k[i] = r[i + kML]\exp\left[-j\hat{\theta}_{k+i|k}\right]$, where $\hat{\theta}_{k+i|k}$ is obtained according to $\hat{\theta}_{k+i|k} = \hat{\omega}_{k|k} iT_s + \hat{\dot{\omega}}_{k|k}\frac{i^2}{2}T_s^2$, for $i = 0, \ldots, ML-1$. The vector $\tilde{\mathbf{y}}_{k+1}$ is constructed as $\tilde{\mathbf{y}}_{k+1} = [\tilde{r}_k[0], \ldots, \tilde{r}_k[ML-1]]^{\mathsf{T}}$. One can show that (cf. (6.3))

$$\tilde{\mathbf{y}}_{k+1} = \tilde{\mathbf{H}}_{k+1}\mathbf{s} + \tilde{\mathbf{w}}_{\mathrm{eq}_{k+1}}, \tag{5.13}$$

where the residual Doppler matrix is

$$\begin{aligned} &\tilde{\mathbf{H}}_{k+1} \\ &\triangleq [\mathbf{I}_L, \exp(j\Delta\omega_k L)\,\mathbf{I}_L, \ldots, \exp(j\Delta\omega_{k+1}(M-1)L)\,\mathbf{I}_L]^{\mathsf{T}}, \end{aligned} \tag{5.14}$$

and $\Delta\omega_{k+1} = \omega_{k+1} - \hat{\omega}_{k+1|k}$. The proposed KF innovation is given by

$$\nu_{k+1} = \mathrm{argmax}_{\Delta\omega_{k+1}} \frac{1}{M}\|\tilde{\mathbf{H}}_{k+1}^{\mathsf{H}}\tilde{\mathbf{y}}_{k+1}\|^2, \tag{5.15}$$

which is a direct measure of the Doppler error. The measurement noise is chosen proportional to the Doppler search step size. The initial estimates of the Doppler $\hat{\omega}_{0|0}$ and the Doppler rate $\hat{\dot{\omega}}_{0|0}$ are obtained from the acquisition stage.

5.4 Experimental Results

This section provides the first results for blind Doppler tracking and positioning with Starlink signals of opportunity. A stationary National Instrument (NI) universal software radio peripheral (USRP) 2945R was equipped with a consumer-grade Ku antenna and low-noise block (LNB) downconverter to receive Starlink signals in the Ku-band. The sampling rate was set to 2.5 MHz and the carrier frequency was set to 11.325 GHz, which is one of the Starlink downlink frequencies. The samples of the Ku signal were stored for off-line processing. The tracking results are presented next.

5.4.1 Blind Doppler Tracking Results

The USRP was set to record Ku signals over a period of 800 seconds. During this period, a total of six Starlink SVs transmitting at 11.325 GHz passed over the receiver, one at a time. The framework discussed in Section 5.3 was used to acquire the downlink signals and track the Doppler frequencies and rates from these LEO SVs, which are shown in Fig. 5.2 along with the ones predicted from two-line element (TLE) files [73]. It can be seen that the proposed algorithm is tracking the Doppler and the Doppler rate of six Starlink LEO SVs. It can also be seen that the estimated Doppler frequencies have a constant bias compared to the predicted ones from the TLEs.

5.4.2 Position Estimation

Next, pseudorange rate observables are formed from the tracked Doppler frequencies by (i) downsampling by a factor D to avoid large time-correlations in the pseudorange observables and (ii) multiplying by the wavelength to express the Doppler frequencies in

meters per second. Let $i \in \{1,2,3,4,5,6\}$ denote the SV index. The pseudorange rate observable to the ith SV at time-step $\kappa = k \cdot D$, expressed in meters, is modeled as

$$z_i(\kappa) = \frac{\dot{\boldsymbol{r}}_{\mathrm{SV}_i}^{\mathsf{T}}(\kappa)\left[\boldsymbol{r}_r - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\right]}{\|\boldsymbol{r}_r - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\|} + a_i + v_{z_i}(\kappa), \tag{5.16}$$

where $\boldsymbol{r}_r$ and $\boldsymbol{r}_{\mathrm{SV}_i}(\kappa)$ are the receiver's and ith Starlink SV three-dimensional (3–D) position vectors, $\dot{\boldsymbol{r}}_{\mathrm{SV}_i}(\kappa)$ is the ith Starlink SV 2–D velocity vector, a_i is the constant bias due to the unknown Doppler frequency ambiguity f_a, and $v_{z_i}(\kappa)$ is the measurement noise, which is modeled as a zero-mean, white Gaussian random variable with variance $\sigma_i^2(\kappa)$. The value of $\sigma_i^2(\kappa)$ is the first diagonal element of $\mathbf{P}_{\kappa|\kappa}$, expressed in $\mathrm{m}^2/\mathrm{s}^2$. Next, define the parameter vector $\boldsymbol{x} \triangleq \left[\boldsymbol{r}_r{}^{\mathsf{T}}, a_1, \ldots, a_6\right]^{\mathsf{T}}$. Let $\boldsymbol{z}$ denote the vector of all the pseudorange observables stacked together, and let $\boldsymbol{v}_z$ denote the vector of all measurement noises stacked together, which is a zero-mean Gaussian random vector with a diagonal covariance $\mathbf{R}$ whose diagonal elements are given by $\sigma_i^2(\kappa)$. Then, one can readily write the measurement equation given by $\boldsymbol{z} = \boldsymbol{g}(\boldsymbol{x}) + \boldsymbol{v}_z$, where $\boldsymbol{g}(\boldsymbol{x})$ is a vector-valued function that maps the parameter $\boldsymbol{x}$ to the pseudorange rate observables according to (5.16). Next, a weighted nonlinear least-squares (WNLS) estimator with weight matrix $\mathbf{R}^{-1}$ is solved to obtain an estimate of $\boldsymbol{x}$ given by $\hat{\boldsymbol{x}} = \left[\hat{\boldsymbol{r}}_r^{\mathsf{T}}, \hat{a}_1, \ldots, \hat{a}_6\right]^{\mathsf{T}}$. The SV positions were obtained from TLE files and SGP4 software. It is important to note that the TLE epoch time was adjusted for each SV to account for ephemeris errors. This was achieved by minimizing the pseudorange rate residuals for each SV.

Subsequently, the receiver position was estimated using the aforementioned WNLS. The 3–D position error was found to be 22.9 m, while the 2–D position error was 10 m. A skyplot of the Starlink SVs and the environment layout summarizing the positioning results are shown in Fig. 5.3.

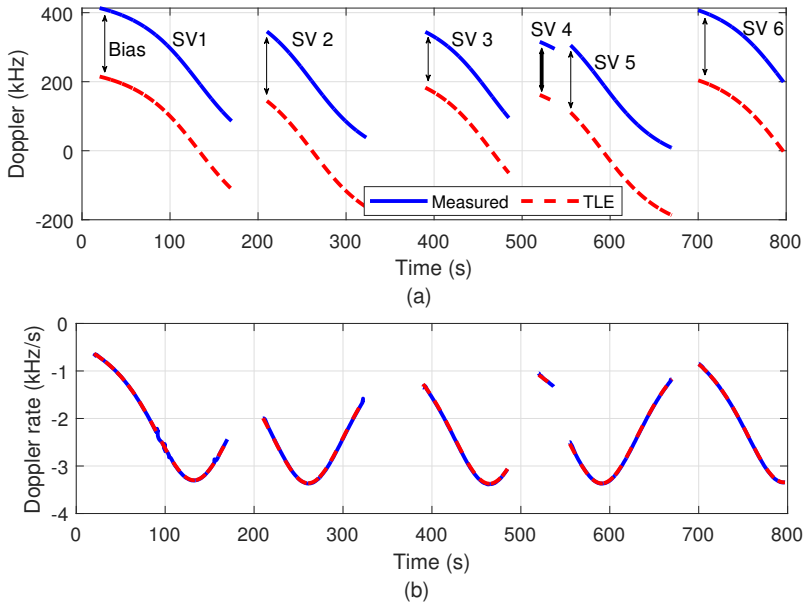


Figure 5.2: Experimental results showing measured and predicted (a) Doppler frequencies and (b) Doppler frequency rates from 6 Starlink LEO SVs.

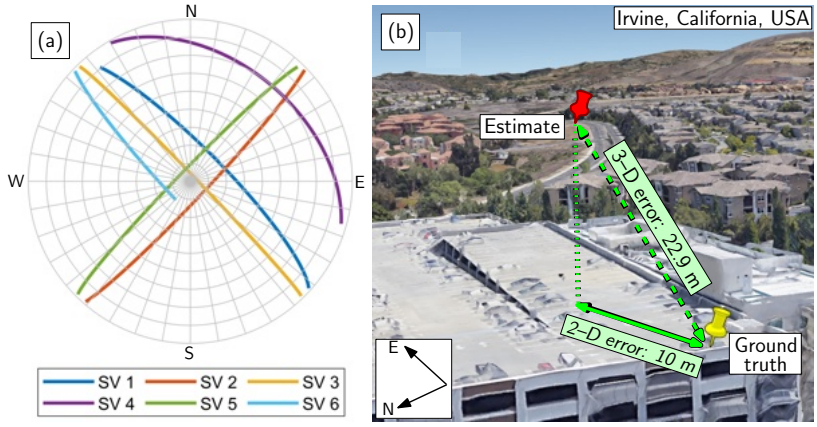


Figure 5.3: (a) Skyplot showing the Starlink SVs' trajectories during the experiment. (b) Environment layout and positioning results.

In this chapter, a matched subspace detector is generalized to sequentially detect real OFDM RSs of multiple Starlink LEO SVs. The always-on and on-demand RSs are detected cognitively, with a predetermined probability of false alarm, and exploited for navigation.

The method is shown to be capable of sensing the transition between the RSs in the received signals. The detected RSs are used in the tracking loops which exploit the time and frequency correlation properties of the detected RSs to provide carrier and code phase observables. The main contributions of this chapter are:

- For a class of sequences that are widely used in modern RSs in OFDM-based signals, it is theoretically shown that the Fourier transform of the sequence preserves the correlation properties. Based on this property of autocorrelation function: (i) the Starlink downlink OFDM-based signal model is formulated, and (ii) the RS type of Starlink downlink signals are classified.

- A closed-form solution for the autocorrelation function in the presence of the Doppler rate is derived. To demonstrate the validity of the closed-form solution, it is compared with the experimentally obtained autocorrelation function of Starlink signals for different values of Doppler rate.

- To demonstrate the performance of the proposed receiver, a base with a known position and a stationary rover with an unknown position were equipped with the proposed receiver. Two baselines between the base and rover receivers were considered: 1.004 km and 8.6 m. Despite the fact that the satellites' ephemerides were poorly known (with errors on the order of several kilometers, as they are predicted from two-line element (TLE) files and an SGP4 propagator), the proposed differential framework estimated the rover's two-dimensional (2D) position with an error of 3.9 m and 83 cm, respectively.

- To further demonstrate the capability of the proposed receiver in detecting new types of RSs, it is fictitiously assumed that the Starlink satellites *multiplex* the 5G NR RSs as a new component in their downlink signals. It is shown that the proposed method is capable of detecting and tracking the new signals simultaneously with the real Starlink RSs.

The rest of this chapter is organized as follows. Section 5.5 presents the received baseband signal model. Section 5.6 presents different stages of the proposed receiver. Section 5.8 presents experimental results.

5.5 Signal Model

Fig. 5.4 demonstrates the spectrum of Starlink downlink signal recorded at 200 MHz sampling rate. The downlink signal of Starlink contains two components: (i) nine pure tones located at the center of the frequency spectrum, and (ii) OFDM subcarriers. The frame structure in OFDM-based transmission is either fixed or identified based on the physical requirements [198]. Each OFDM frame contains always-on and on-demand RSs which are transmitted for synchronization and channel estimation purposes. The period of the RSs is usually equal to the frame length of the OFDM signals. Acquisition and tracking OFDM RSs require knowledge of the frame length. While the frame length is known in public networks, such as 5G NR, it can be unknown (and subject to change) in private networks, e.g., Starlink LEO SV broadband system. For private networks, the frame length should be estimated and updated cognitively. This chapter, provides a thorough analysis of frame length estimation of OFDM signals taking into account the high dynamics of the Starlink LEO SVs. In order to have an intuition about the frame length estimation process, one can consider a simple

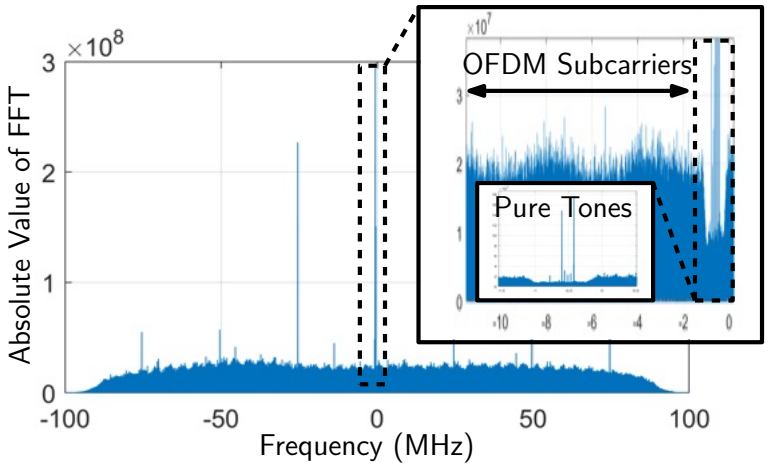


Figure 5.4: Starlink downlink signals recorded at 200 MHz sampling rate. OFDM subcarriers and a group of pure tones are observed in the spectrum of Starlink downlink signals.

autocorrelation-based technique. Assuming that the RSs have good correlation properties, the autocorrelation of a large enough time segment of the received signal will result in a train of an impulse-like function whose shape depends on the correlation properties of the synchronization signals. The distance between two consecutive impulses is equal to the OFDM frame length. Fig. 5.5(a) demonstrates the autocorrelation of a 100 ms time segment of the Starlink downlink signal. It can be seen that the distance between the impulses of the resulting train is estimated to be approximately 1.33 ms. Also, for comparative purpose, Fig. 5.5(b) shows the same processing on a 40 ms time segment of a 5G NR signal which results in a frame length estimation of 10 ms, which corroborates the standard frame length of 5G NR downlink signals [198].

Two factors may affect the frame length estimation process: (i) high dynamics of Starlink LEO SVs which result in a high Doppler rate that attenuates the impulses in the autocorrelation function and (ii) correlation properties of the RS. The effect of the Doppler rate on the autocorrelation is analyzed in Subsection 5.6.1. The following subsections,

provide some background about the correlation properties of the RSs. Then the received baseband signal model is also described.

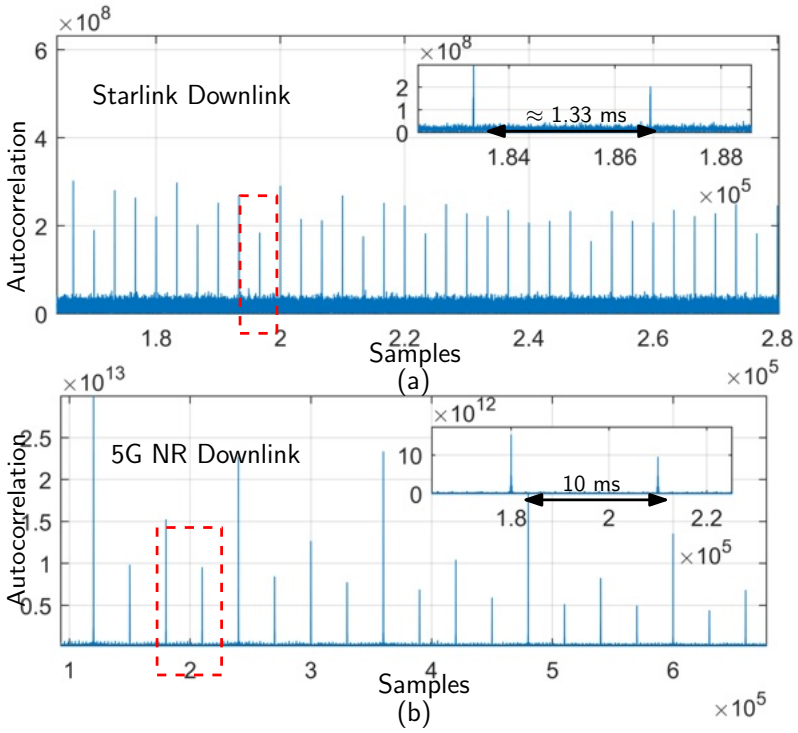


Figure 5.5: Autocorrelation of recorded signal after Doppler wipe-off: (a) Autocorrelation of a 100 ms of Starlink Downlink signal shows a frame length of approximately 1.33 ms. (b) Autocorrelation of a 40 ms of 5G NR downlink signal which shows the frame length of 10 ms (5G NR standard frame length).

5.5.1 Dual Correlation Properties

Detection and tracking of unknown sources rely on two fundamental features of the RS: (i) periodicity and (ii) correlation properties in the time- and frequency-domains. In broadband communication systems, the RS waveform is designed based on the correlation

properties of the so-called synchronization sequences. Different sequences have distinct correlation behaviors and can be adopted in a particular system based on physical considerations. For instance, Zadoff-Chu sequences are known for their low autocorrelation sidelobes at zero Doppler shift. In this subsection, the concept of dual correlation property is explained, which motivates the proposed OFDM-based signal model.

The correlation properties of a sequence are usually characterized using the *ambiguity function*.

Definition 1: Let $p[n]$ be a sequence of numbers of length L, where $n = 0, \ldots, L-1$. Define the periodic sequence $c[n]$ as the periodic extension of $p[n]$, i.e., $c[m] = p[k]$, for $m \in \mathbb{Z}$, where $0 \leq k \leq L-1$ and $k \equiv (m \mod L)$. The discrete ambiguity function of periodic code $c[m]$ is defined as [22]

$$\mathscr{A}_c(m,n) = \frac{1}{L} \sum_{k=0}^{L-1} c[m+k] c^{\star}[k] \exp\left(-\frac{j2\pi kn}{L}\right), \tag{5.17}$$

where $c^{\star}[k]$ denotes the complex conjugate of complex number $c[k]$. In order to explain the correlation duality and make the proofs tractable in this subsection, the class of constant amplitude zero autocorrelation (CAZAC) sequences are considered. CAZAC sequences have been widely used in different communication systems due to their optimal transmission efficiency and tight time localization properties. Two examples of CAZAC sequences are the Zadoff-Chu and the Wiener sequences [22].

Definition 2: The sequence $p[n]$ for $n = 0, \ldots, L-1$ is a CAZAC sequence if $|p[n]| = 1$ for all n, and the ambiguity function of the periodic extension of $p[n]$, i.e, $c[n]$ in Definition 1, has the following property

$$\mathscr{A}_c(m,0) = 0, \tag{5.18}$$

for $1 \leq m \leq L-1$.

The property of CAZAC sequences presented in (5.18) simply means that the ambiguity function of a CAZAC sequence is a periodic train of impulses with period L when the Doppler frequency is zero.

Lemma 1: Assume that the sequence $c[n]$ is CAZAC. Denoting the discrete Fourier transform (DFT) of $c[n]$ by $c_{\mathrm{F}}[k]$, where

$$c_{\mathrm{F}}[k] = \frac{1}{L}\sum_{n=0}^{L-1} c[n]\exp\left(\frac{j2\pi nk}{L}\right), \tag{5.19}$$

for $0 \leq k \leq L-1$, the sequence $c_{\mathrm{F}}[k]\exp\left(\frac{j2\pi f_D k}{L}\right)$ is also CAZAC [22].

Lemma 1 plays an important role in formulating the signal model of OFDM-based systems, which will be discussed later in this section. In OFDM-based transmission, the symbols are mapped onto multiple carrier frequencies via the inverse fast Fourier transform (IFFT) [206]. Therefore, the samples of the received signal in the time-domain contain the IFFT of the samples of the transmitted sequence. The acquisition and tracking stages of the proposed receiver adopt a phase-rotated time-domain version of the RS as the *beacon*. Lemma 1 guarantees that for the class of CAZAC sequences such as Zadoff-Chu sequence, the considered beacon has good correlation properties. Fig. 5.6 demonstrates the autocorrelation of a Zadoff-Chu sequence in the time and frequency-domain, which demonstrates that the Fourier operation preserves the correlation properties.

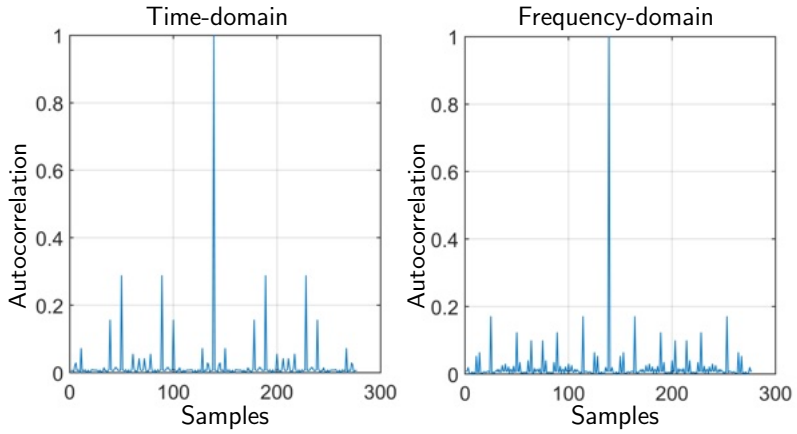


Figure 5.6: Autocorrelation of Zadoff-Chu sequence in (a) time- and (b) frequency-domains (25th root with a length of 139): It can be seen that the Fourier transform preserves the autocorrelation properties of the sequence.

5.6 Receiver Architecture

This section describes the architecture of the proposed received in details.

5.6.1 Frame Length Estimation

In order for the acquisition stage to be able to detect always-on and on-demand RSs, having a knowledge of the RS period is necessary. While the frame length is known for public networks such as 5G NR, in private companies, the frame length might be unknown or dynamically change based on the transmission mode [198]. The first stage of the proposed receiver involves frame length estimation. The autocorrelation of a large enough time segment of the received signal results in a periodic train of ambiguity functions in the time-domain. If the transmitted sequences have *good correlation properties*, the ambiguity functions will have an impulse-like shape. As discussed in Section 5.5, good autocorrelation means that the waveform of the RS is nearly uncorrelated with its own time-shifted versions,

while good crosscorrelation indicates that the RSs of different satellites' waveforms are nearly uncorrelated.

The following Lemma provides a closed-form solution for the autocorrelation function in the presence of the Doppler rate.

Acquisition and tracking stages are similar to the previous chapter.

5.7 The Impact of Cognitive Estimation of Always-on and On-demand Signals

In this section, the impact of cognitive estimation of always-on and on-demand signals is evaluated experimentally. Communication systems transmit always-on RSs at regular intervals even when there is no data to transmit to any user. Ultra-lean design refers to minimizing the always-on transmissions by transmitting on-demand RSs when necessary. The proposed receiver, cognitively detects both always-on and on-demand components. An experiment is conducted to test the receiver with real 5G signals. The receiver estimates the always-on and on-demand components of the transmitted signal. To see the impact of exploiting the whole bandwidth of the received signal, i.e., estimating all the available periodic components which are always-on and/or on-demand, the receiver in [5] that only relies on always-signals is used for comparison. Moreover, and emulation of Starlink LEO SVs transmitting 5G signals is provided to evaluate the performance of the receiver in a scenario that Starlink LEO SVs are fictitiously transmitting 5G-like signals.

5.7.1 Experimental Demonstration of Estimation of Always-on and On-demand signals

A ground vehicle was equipped with a quad-channel National Instrument (NI) USRP-2955 and two consumer-grade 800/1900 MHz cellular antennas to sample 5G signals near Ohio Stadium in Columbus, Ohio, USA. One channel from the USRP was tuned to a 632.55 MHz carrier frequency, which is a 5G NR frequency allocated to the U.S. cellular provider T-Mobile. The sampling rate was set to 20 Mega-samples per second (MSps) and the sampled 5G signals were stored on a laptop for post-processing. In order to obtain the vehicle's trajectory, the vehicle was equipped with a Septentrio AsteRx SBi3 Pro+ with a dual antenna multi-frequency GNSS receiver with real-time kinematic (RTK) and an industrial-grade inertial measurement unit (IMU). The vehicle's traversed a trajectory of 1.79 km. Fig. 5.7 shows the environment layout, the vehicle trajectory, and the experiment setup.

Figure 5.7: The environment layout, vehicle trajectory, and experiment setup. The true location and a photo of the site of the blindly detected gNB are shown.

The location of the gNB and the transmitted RS from the gNB were unknown to the receiver. The goal of this experiment was to cognitively sense the location of the gNB via the proposed receiver and a receiver in [5] which only uses always-on signals. Fig. 5.8 demonstrates the acquisition results. It can be seen that five sources were detected by the receiver. The first detected source in Stage 1 of the acquisition algorithm has the largest likelihood, therefore, it corresponds to the strongest path. Fig. 5.9 demonstrates the

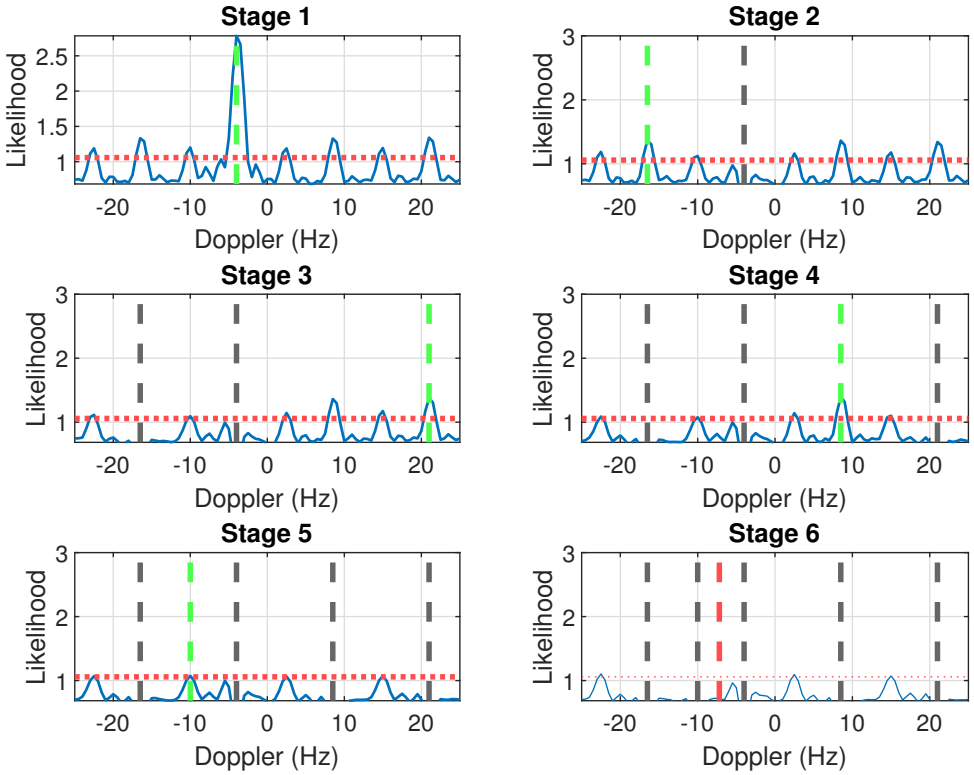


Figure 5.8: The acquisition results: Five sources are detected in the acquisition stage. The red dashed horizontal line is the threshold and the green vertical line corresponds to the detected source at each stage. The gray vertical lines are the previously detected sources at each stage.

reconstructed OFDM frame structure of the estimated RS from the 5G gNB. It can be seen that the detected subcarriers are spread across the whole recorded bandwidth which is 20 MHz in this experiment. The estimated Doppler is plotted in Fig. 5.10. It can be seen that the tracked Doppler using the method in [185] which only relies on always-on signals has a larger estimation variance compared to the proposed method.

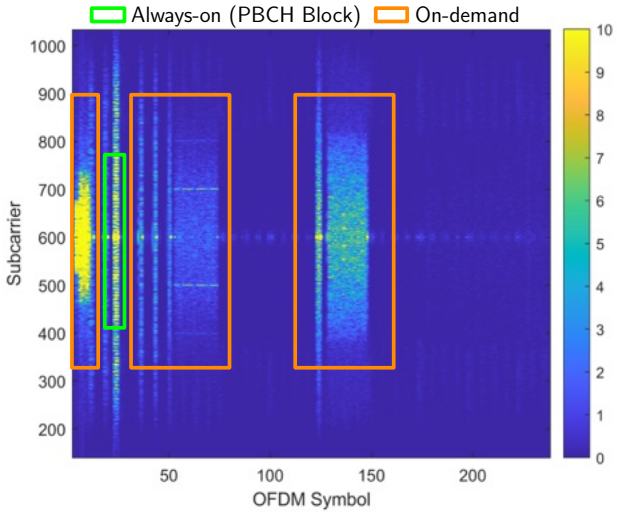


Figure 5.9: Reconstructed frame structure of the estimated RS: While the always-on subcarriers (subcarriers in the green box) only cover a small portion of the available bandwidth, the on-demand components (subcarriers in the orange box) are spread across the whole recorded bandwidth which is 10 MHz in this experiment.

Next, the pseudorange observables from the gNB will be used to estimate the 2D position of the UAV-mounted receiver, denoted by $\boldsymbol{r}_s$. The code-phase in (4.23) can be used to readily deduce the pseudorange observables. The pseudorange, expressed in meters, from the gNB can be modeled as

$$z(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_s\| + c \cdot [\delta t_r(k) - \delta t_s(k)] + v(k), \tag{5.20}$$

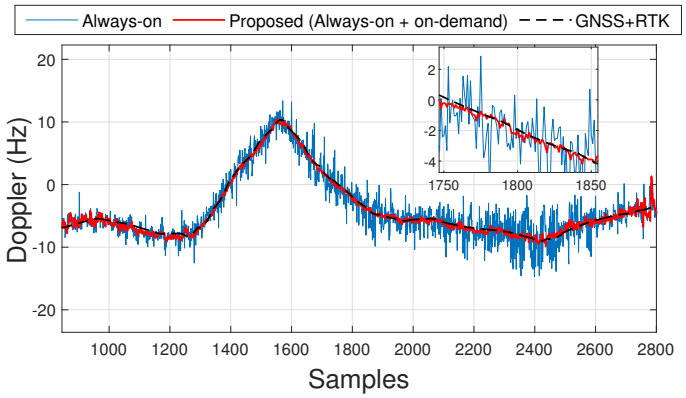


Figure 5.10: The estimated Doppler using the proposed method which exploits the always-on and on-demand components versus the method in [185].

where $\boldsymbol{r}_s$ is the 2D position of the gNB, c is the speed of light, δt_r and δt_s are the receiver's and gNB's clock biases, respectively, and $v(k)$ is the measurement noise, which is modeled as a zero-mean white Gaussian sequence with variance σ^2. The transmitter and receiver clock terms, i.e., $\delta t_r(k)$ and $\delta t_{s_n}(k)$ in (5.20), are both unknown to the receiver. Assuming a first-order clock model for both the gNB and the receiver, the combined clock term in (5.20) can be written as $c\delta t_n(k) = c \cdot [\delta t_r(k) - \delta t_{s_n}(k)] \triangleq \xi + \psi k$ where ξ is the clock bias and ψ is the clock drift [21]. Note that $\boldsymbol{r}_r(k)$ is known and the receiver uses pseudorange observables to estimate the gNB's position $\boldsymbol{r}_s$. Next, define the parameter vector $\boldsymbol{x} \triangleq [\boldsymbol{r}_s^\mathsf{T}, \xi, \psi]^\mathsf{T}$. Let $\boldsymbol{z}$ denote the vector of all the pseudorange observables stacked together. Then, one can write the measurement equation given by $\boldsymbol{z} = \boldsymbol{g}(\boldsymbol{x}) + \boldsymbol{v}_z$, where $g(\boldsymbol{x})$ is a vector-valued function that maps the parameter vector $\boldsymbol{x}$ to the pseudorange observables according to (5.20), and $\boldsymbol{v}_z$ denotes the vector of all measurement noises stacked together. Next, a nonlinear least-squares (NLS) estimator was used to estimate $\boldsymbol{x}$ denoted by $\hat{\boldsymbol{x}}$. The estimated position was validated by on-site verification. The 2D position error of the estimated gNB found to be

5.83 m whereas the estimated position using only always-on signals did not converge. The true location of the gNB and the estimated location of the gNB are shown in Fig. 5.11.

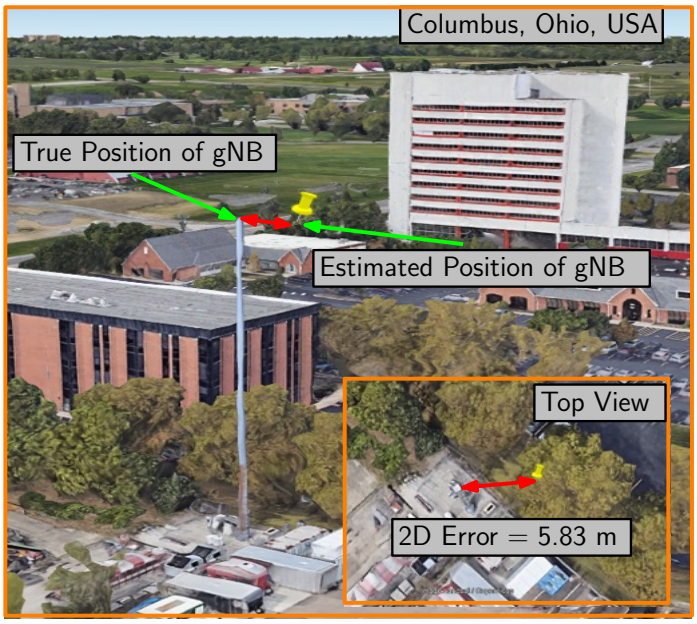


Figure 5.11: The cognitive sensing results: The True position of the gNB and the blindly estimated position are plotted. The 2D error was found to be 5.83 m.

5.7.2 Emulating Simultaneous 5G NR and Broadband OFDM Signals in Starlink LEO SV Downlink

To further examine the performance of the proposed receiver, it is fictitiously assumed that the Starlink satellites *multiplex* the 5G NR RSs as a new component in their downlink signals. In particular, real 5G NR RSs are modulated into real Starlink satellite signals [102]. The 5G NR RSs were reconstructed based on [149]. The Delay and the Doppler of the Starlink satellite were added to the 5G Rs to emulate the transmission from the Starlink LEO SV. The resulting RS were added in time domain with real Starlink downlink signals. It

should be pointed out that, in order to add the delay and Doppler to the 5G RS, the delay and the Doppler of the Starlink satellite were obtained from the TLE files propagated through SGP4 to modulate the 5G RS. The period of the 5G NR component is denoted by L_1, and the period of the Starlink satellite signals is denoted by L_2. As was mentioned previously, the period of Starlink broadband OFDM signals is approximately 1.33 ms while the period of terrestrial 5G NR RSs is 10 ms [198]. In this emulation, the frame length of 5G NR component of Starlink LEO SV signals is assumed to be 1 ms. This small OFDM frame length choice is considered to: (i) avoid the *Doppler spread* effect [206] and (ii) choosing a period which is not necessarily equal to the Starlink broadband OFDM component. Due to the high Doppler rate of Starlink satellites, a long frame length, e.g., a frame length similar to terrestrial 5G NR, leads to a dramatic Doppler change during one period of the RS. The 5G NR signal is modulated with the Doppler frequency of Starlink-45694. Fig. 5.12 demonstrates the acquisition and tracking results. Since two separate periods are considered, two different likelihood functions should be constructed for each L to detect the satellites corresponding to each period. Fig. 5.12(a) demonstrates the likelihood function considering the period is $L_1 = 1$ ms which is the period of emulated 5G NR. The peak of the likelihood at -232. Fig. 5.12(b) demonstrates the likelihood function of the received signal assuming that the period is $L_2 \approx 0.33$. It can be seen that both components of Starlink RSs are detected. Fig. 5.12(c) shows the Doppler tracking results, and Fig. (d) demonstrates the amplitude of the estimated 5G NR RS. The PSS and SSS of 5G NR signals are detected along with other periodic components.

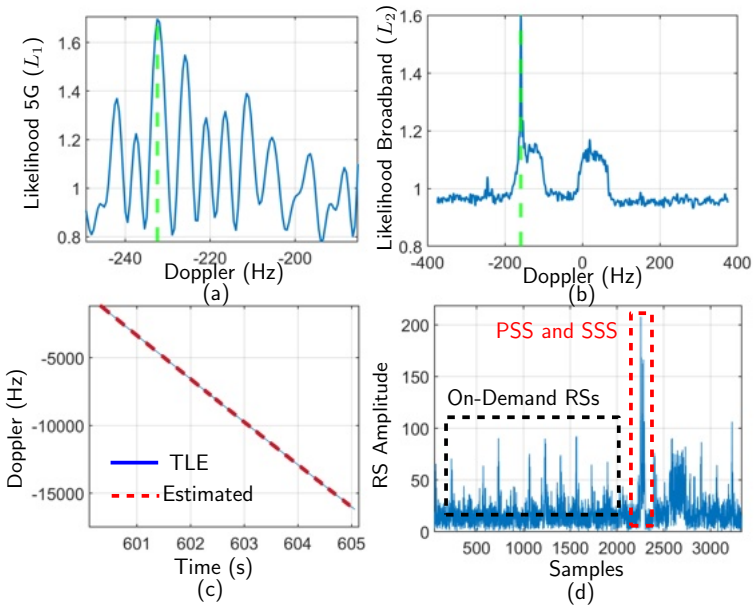


Figure 5.12: Emulated 5G NR signals modulated on real Starlink signals.

5.8 Experimental Results

This section validates the performance of the proposed receiver experimentally. The objectives of the experiments in this section are to: (i) analyze Starlink LEO SV transmission modes and RS correlation properties, (ii) show the potential of the proposed receive in achieving meter-level accuracy in a differential Doppler positioning scenario.

5.8.1 Now You Are Beaming, Now You are Not: Detection of Always-on and On-demand Starlink Downlink Signals

As it was mentioned previously, Starlink LEO SVs transmit nine pure tones located in a, roughly, 1 MHz gap at the center of the transmission bandwidth at the Ku band. The pure tones were exploited for Doppler positioning in [105, 147, 151]. In this subsection, more details about the RSs of Starlink LEO SVs and their corresponding properties are assessed.

In particular, it will be shown that two types of RSs with two different correlation properties are being transmitted.

In the first experiment, a stationary National Instrument (NI) universal software radio peripheral (USRP) 2945R equipped with a consumergrade Ku antenna and low-noise block (LNB) downconverter to receive Starlink signals in the Ku-band. The sampling rate was set to 2.5 MHz and the carrier frequency was set to 11.325.

5.8.1.1 Always-on and On-demand RSs

Fig. 5.13 concentrates on the time epochs in which a transmission mode change has occurred. The autocorrelation and the likelihood functions at time epochs of $t = 606$ s and $t = 607$ s are plotted in Fig. 5.13. It will be shown that the RS structure and the correlation properties will change in the transition between these two time epochs for Starlink-45694, at the time of the experiment. Fig. 5.13(a) and (b) demonstrate the autocorrelation function at $t = 606$ s and $t = 607$ s. In the autocorrelation function at $t = 606$ s, the previously discussed ambiguity function impulses in (4.6) are observed. The amplitude of the impulses follows the sinc-function behavior, which is due to the Doppler rate effect as explained in Lemma 2. Recall that these impulses are approximately 1.33 ms apart. However, at $t = 607$ s the ambiguity function impulses disappeared. While the autocorrelation function is suggesting that the periodic RSs are not being transmitted at $t = 607$ s, the likelihood function shows a surprising behavior. At $t = 606$ s the likelihood includes two different components which are shown in a black and a red box in Fig. 5.13(c). The probability of false alarm is set to be 10^{-4} to obtain the threshold (the horizontal dotted line). Recall that when the likelihood passes the threshold, the existence of an RS with period a of approximately 1.33 ms is

guaranteed by the detector with a certain probability of detection. The likelihood at $t = 607$ s shows that the component in the black box is not being transmitted anymore while the component in the red box is *still on*. The signal in the red box is periodic with period 1.33 ms which is associated with the OFDM RSs. However, as it can be seen in Fig. 5.13(b), the signal in the red box does is not have good *time correlation* properties. The signal in the red box is continuously transmitted when the boradband OFDM signal is active and is referred to as always-on RS in this chapter. As discussed in 5.7, always-on signals are broadcast and on-demand signals are transmitted when the transmitter is beaming at the receiver. The behavior of the signal in the black box is similar to 5G NR on-demand RSs which are not always active and, therefore, are referred to as on-demand RSs in this chapter. The same behavior in the autocorrelation and likelihood functions are observed in the recorded signals from Starlink satellites in all the experiments conducted in this chapter.

Next, the tracking results in the mentioned time interval are presented. The tracking results give a better understanding of correlation properties of the two detected RSs in the tracking feedback loops. The bandwidith of the PLL is set to be 65 Hz and the bandwidth of the DLL is set to be 20 Hz. Fig. 5.14(a) demonstrates delay tracking and Fig. 5.14(b) demonstrates carrier phase tracking results for Starlink-45694. As it was expected, at a time epoch between $t = 606$ s and $t = 607$ s the code phase tracking is lost. This is due to the fact that the on-demand signal which has suitable time autocorrelation properties is not active anymore at this time epoch. However, Fig. 5.14(b) shows that the carrier phase tracking loop is still locked. This is due to the fact that the always-on signal (the signal in the red box in Fig. 5.13(c)) is showing good frequency correlation properties. The frequency-domain correlation property of the always-on signal guarantees carrier phase tracking even if the on-demand signal is not active.

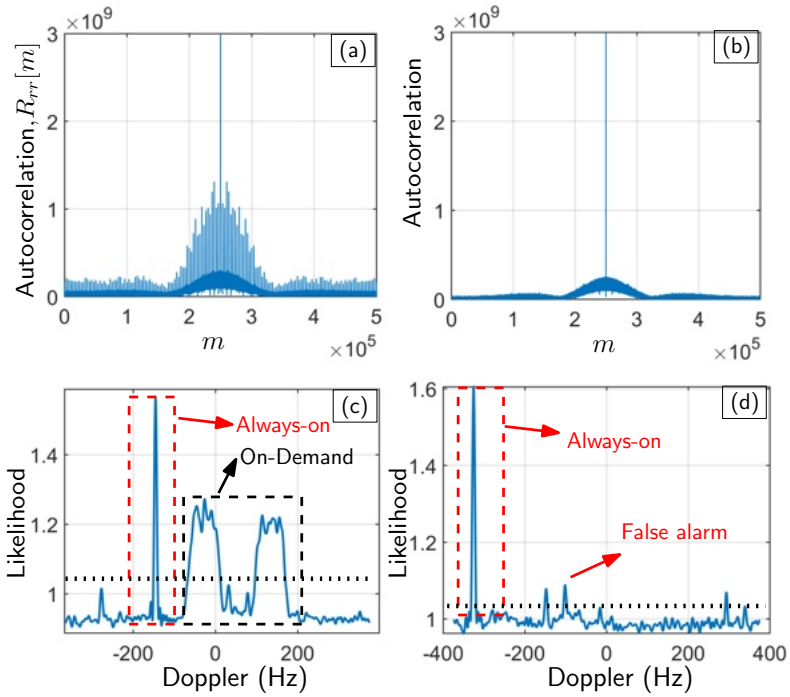


Figure 5.13: Autocorrelation and Likelihood at $t = 606$ s and $t = 607$ s: (a) and (b) demonstrate autocorrelation at $t = 606$ s and $t = 607$ s, respectively. It can be seen that at $t = 606$ s the RS is showing a time autocorrelation and at $t = 607$ s the time autocorrelation is lost. (c) and (d) demonstrate the likelihood function at $t = 606$ s and $t = 607$ s, respectively. Two components can be seen in the likelihood functions (the red box and the black box) at $t = 606$ s. The component in the black box is not being transmitted at $t = 607$ s.

Remark 4: Starlink RSs may dynamically change during one satellite pass [142]. A method that only relies on a static design based on an RS with good time correlation properties may not provide continuous navigation observables. The proposed method cognitively detects all the available RSs which results in better carrier-phase and delay tracking results.

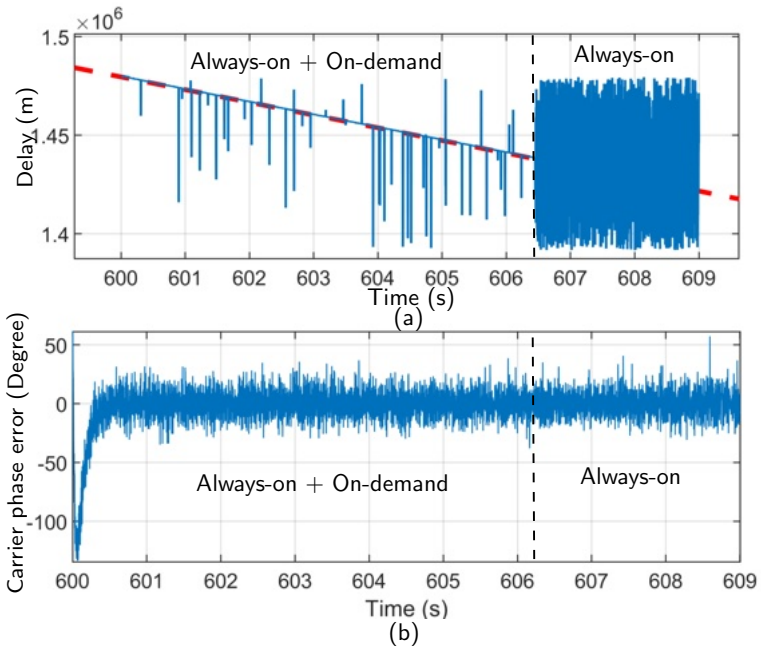


Figure 5.14: Now you are beaming, Now you are not: (a) Code phase tracking, and (b) carrier phase tracking of Starlink-45694. As it was expected, at a time epoch between $t = 606$ s and $t = 607$ s the code phase tracking is lost. This is due to the fact that the on-demand signal which has suitable time autocorrelation properties is not active anymore at this time epoch. However, Fig. 5.14(b) shows that the carrier phase tracking loop is still locked.

5.8.2 Effect of Antenna Gain on Tracking Loops

In this subsection, the effect of the antenna gain on the tracking results is assessed. Fig. 5.15 demonstrates the carrier phase error for the two values of CPI= 40 and CPI = 300 in the previous experiment. As it can be seen in Fig. 5.15, the standard deviation of the carrier phase error for CPI = 300 is smaller than when CPI = 40. A larger coherent accumulation time results in a better RS detection performance. Since the satellite is moving away from the receiver, the SNR is getting weaker and the carrier phase error increases over time. To assess the effect of antenna gain on the standard deviation of carrier phase tracking, an experiment was conducted on the roof of electroscience laboratory (ESL) in Columbus,

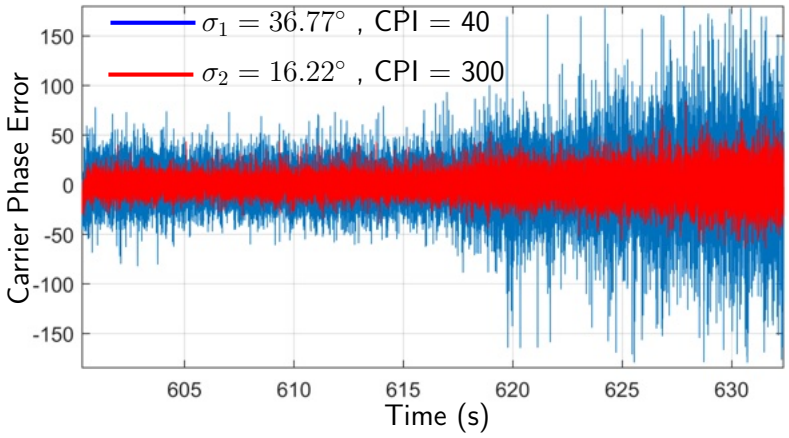


Figure 5.15: Carrier phase error for CPI = 40 and CPI = 300. Increasing the CPI results in a better carrier phase tracking performance. Since the satellite is moving away from the receiver, the carrier phase error eventually increases.

Ohio, USA. A similar hardware setup was used except for the LNB which was equipped with a 60 cm dish to increase the antenna gain.

Fig. 5.16(a) demonstrates the location were the experiment was conducted, and Fig 5.16(b) demonstrates the likelihood function. Comparing the likelihood function in Fig. 5.16(b) and Fig. 5.13(c) shows that the always-on signal is detected. 5.16(c) demonstrates the carrier phase tracking results. It can be seen that the standard deviation of carrier-phase error is reduced to 10.2 degrees. The estimated Doppler and the Doppler from the TLE files are plotted in 5.16(d). While the on-demand signals are absent and the delay is not tracked, the receiver successfully exploits always-on signal and provides carrier phase tracking. A receiver that only relies on SSS and PSS of starlink downlink will fail to provide any navigation observable in such a scenario.

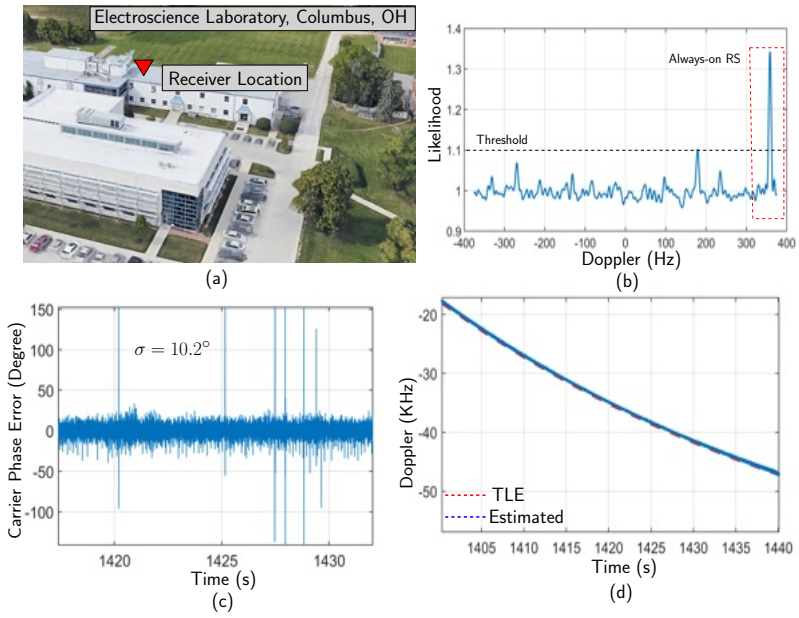


Figure 5.16: (a) Experiment Layout. (b) Likelihood function. (c) Carrier-phase tracking. (d) The estimated Doppler versus the Doppler from the TLE files.

5.8.3 Differential Doppler Positioning

To demonstrate the performance of the proposed receiver, a base with a known position and a stationary rover with an unknown position were equipped with the proposed receiver. The base was equipped with an Ettus E312 USRP with a consumer-grade Ku antenna and LNB downconverter to receive Starlink signals in the Ku band, and the rover was equipped with USRP 2974 with the same downconverter. The sampling rate was set to 2.5 MHz, and the carrier frequency was set to 11.325 GHz. The samples of the received signals were stored for off-line post-processing.

5.8.3.1 Positioning Results

To evaluate the performance of the proposed differential Doppler positioning framework, two baselines between the base and rover are considered, namely 1.004 km and 8.65 m. The ground truth with which the position estimate was compared was taken from the navigation solution produced by the USRP's on-board GPS receiver.

In the first experiment a Base-Rover Baseline of 1.004 km is considered. Over the course of the experiment, the receivers on-board the base and the rover were listening to three Starlink LEO SVs, namely Starlink 44740, 48295, and 47728. The satellites were visible for 320 seconds.

The rover's initial position estimate was set to be approximately 200 km away from the base. The rover's position was estimated via the differential Doppler positioning framework described in Section 6.5.2. The 2D position error is 3.9 m. Fig. 5.17 presents the experiment environment, skyplot of the satellites, and the positioning results.

Next, a shorter baseline of 8.65 m was considered. Similar to the previous case, over the course of this experiment, the receivers on-board the base and the rover were listening to three Starlink LEO SVs, namely Starlink 48466, 48295, and 45582.

The rover's initial position estimate was set to be approximately 200 km away from the base. The rover's position was estimated through the differential Doppler positioning framework described in Subsection 6.5.2. The 2D position error was found to be 83 cm. Fig. 5.18 presents the experiment layout, sky plot of the satellites, and the navigation results.

Figure 5.17: Environment layout and positioning results for 1.004 km baseline.

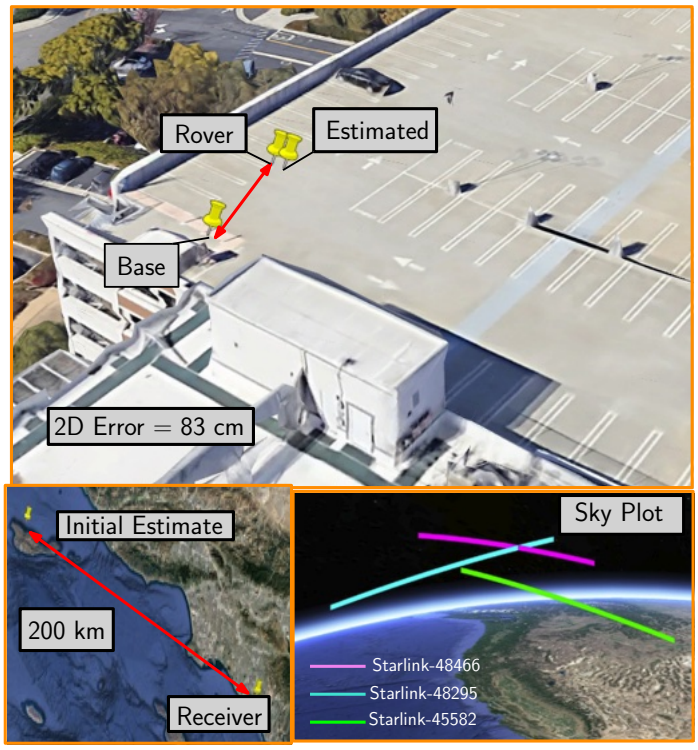


Figure 5.18: Environment layout and positioning results for 8.6 m baseline.

Chapter 6: Navigation with Multi-Constellation LEO Satellites

6.1 Unveiling Starlink LEO Satellite OFDM-Like Signal Structure Enabling Precise Positioning

Research has shown that one could exploit low Earth orbit (LEO) space vehicles (SVs) broadband communication signals for navigation purposes [73]. Navigation with *mega-constellations* can be considered in a standalone fashion or in fusion with other existing technologies [174]. Although LEO SV signals suffer from higher Doppler effect, signals received from LEO SVs can be about 30 dB stronger than signals received from medium Earth orbit (MEO) SVs, where global navigation satellite systems (GNSS) SVs reside [141].

The first positioning results with Starlink SV signals were presented in [105, 147]. These dissertations, exploit a train of pure tones in the downlink of Starlink SV signals to obtain carrier phase and Doppler measurements. Starlink downlink signals occupy 250 MHz bandwidth of the Ku band to provide a highrate broadband connectivity [38]. However, to the best of authors knowledge, nothing beyond the pure tones transmitted in the downlink of the Starlink SVs have been ever detected and tracked in the current literature. In this letter, assuming that the Starlink signals follow an orthogonal frequency devision multiplexing (OFDM)-like model, the reference signals (RSs) of the downlink signals

are detected, and the corresponding OFDM frame length is estimated. Via a sequential detection algorithm, the RSs of multiple Starlink SVs are estimated and the whole available signal bandwidth is exploited and deployed in tracking loops to provide code-phase and carrier-phase observables.

This letter makes the following contributions. First, the OFDM-like frame length of Starlink signals is estimated. Second, by considering an OFDM-based signal model for the Starlink downlink signals, a sequential detection method is presented to detect multiple Starlink SVs and exploit the whole available bandwidth. Third, the estimated RSs corresponding to the Starlink SVs are used in tracking loops to obtain carrier and code phase observables.

6.2 Received Signal Model

6.2.1 OFDM-Like Signal Frame Length

SpaceX uses a 250 MHz signal bandwidth at the Ku-band for the satellite-to-user downlink [38]. Starlink SVs broadcast nine pure tones which are approximately 43.9 KHz apart. In this letter, these tones are referred to as *central tones* since they are located at the center of the 250 MHz bandwidth. At the first glance, a white signal containing the central tones are visible in the spectrum [105]. It should be pointed out that, due to the high dynamics of the Starlink SVs, the downlink signals suffer from Doppler rates which can be of the order of thousands of Hertz per second. The Doppler rate distorts the frequency components and imposes a whitening effect on the transmitted signals. Fig. 6.1, Demonstrates the spectrum of Starlink downlink signals after the Doppler rate wipe-off.

The details of the Doppler rate wipe-off process are provided later. It can be seen that along with the central tones, OFDM-like subcarriers are also visible in the spectrum of Starlink downlink signals. OFDM signals contain frames in which some periodic RSs reside, and are

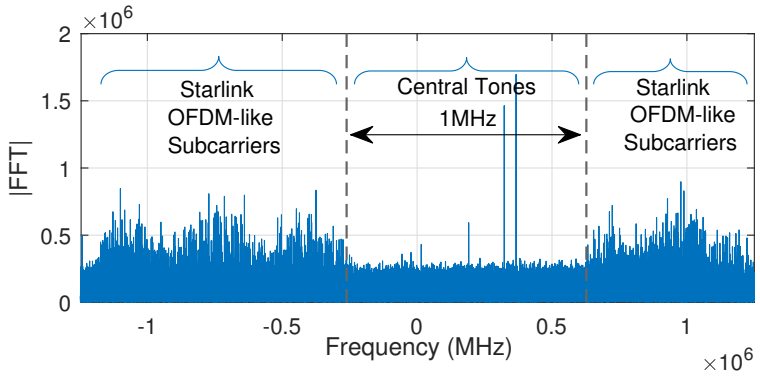


Figure 6.1: The spectrum of Starlink downlink signals after Doppler rate wipe-off: The central tones are appeared along with OFDM-like subcarriers.

sent for synchronization purposes. The frame length, i.e., the period of the synchronization signals can be obtained according to the autocorrelation function of a time segment of the received signal. The autocorrelation of a large enough time segment of the received signal will result in an impulse train, and the distances between two consecutive impulses are equal the OFDM frame length. Fig. 6.2(a), demonstrates the autocorrelation of a 100 ms time segment of the Starlink downlink signal after Doppler rate wipe-off. It can be seen that the distance between the impulses of the resulting train is approximately 1.32 ms. Also, as a reference, Fig. 6.2(b) shows the same processing on a 40 ms time segment of a 5G (new radio) NR signal which results in a frame length estimation of 10 ms which corroborates the standard frame length of 5G NR downlink signals.

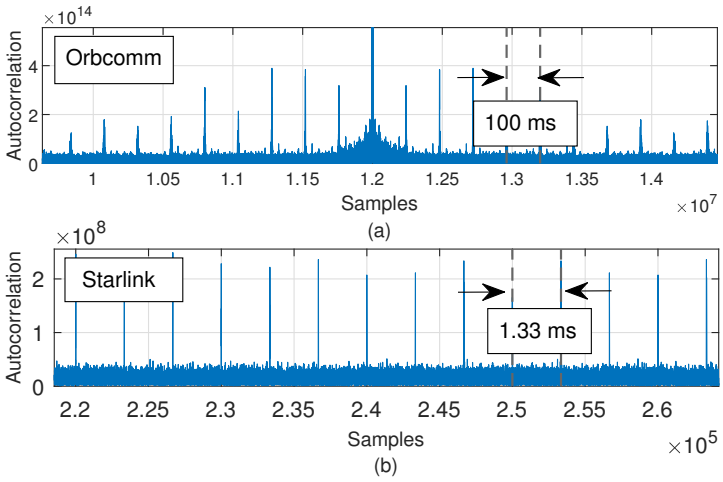


Figure 6.2: Autocorrelation of the recorded signal after Doppler wipe-off: (a) Autocorrelation of the 100 ms of Starlink Downlink signal shows a frame length of approximately 1.32 ms. (b) Autocorrelation of 40 ms of 5G NR downlink signal which shows the frame length of 10 ms (5G NR standard frame length).

6.2.2 Baseband Signal Model

Based on the signal analysis in the previous subsection, the downlink signals from multiple Starlink SVs are modeled as unknown RSs of OFDM-like signals in the presence of noise [149]. Therefore, the baseband received signal samples can be written as

$$r[n] = \sum_{i=1}^{N} \alpha_i(\tau_n) c_i(\tau_n - t_{s_i}[n]) \exp\left(j\theta_i(\tau_n)\right) + w[n], \tag{6.1}$$

where $r[n]$ is the received signal at the nth time instant; N is the total number of Starlink SVs; $\alpha_i(\tau_n)$ is the complex channel gain between the receiver and the ith Starlink SV; τ_n is the sample time expressed in the receiver time; $c_i[n] \triangleq c_i(\tau_n)$ represents the samples of the complex periodic RS with a period of L samples; $t_{s_i}[n]$ is the instantaneous code-delay corresponding to the receiver and the ith Starlink SV at the nth time instant; $\theta_i(\tau_n) = 2\pi f_{D_i}[n] T_s n$ is the carrier phase in radians, where $f_{D_i}[n]$ is the instantaneous Doppler frequency at the nth time instant and T_s is the sampling time, and $w[n]$ captures the effect of noise and transmitted

data, and it is modeled as a complex zero-mean independent and identically distributed noise with variance σ_w^2.

It is observed that during the processing interval, the instantaneous Doppler frequency and the instantaneous code-delay are almost linear functions of time, i.e., $f_{D_i}[n] = f_{D_i} + \beta_i n$, and $t_{s_i}[n] = t_{s_i} + \gamma_i n$, where f_{D_i} is referred to Doppler, t_{s_i} is the code-delay, β_i is the Doppler rate, and γ_i is referred to as the Doppler stretch corresponding to the ith Starlink satellite. The coherent processing interval (CPI) is defined as the time interval in which the channel gain $\alpha_i(\tau_n)$, Doppler f_{D_i}, code-delay t_{s_i}, the Doppler rate β_i, and the Doppler stretch γ_i are all constant. The received signal at the nth time instant when the Doppler rate is wiped-off is denoted by $r'[n] \triangleq \exp(-j2\pi\beta_i n^2) r[n]$. Assuming a constant Doppler rate, one can define $c_i'(\tau_n) \triangleq c_i((1-\gamma_i)\tau_n - t_{s_i})$. Due to the priodicity of the RS, $c'(\tau_n)$ is also periodic with period $L' \triangleq \frac{L}{1-\gamma_i}$. Moreover, one can define $s_i[n] \triangleq \alpha_i c'(\tau_n) \exp(j2\pi f_{D_i} T_s n)$, to obtain $r'[n] = \sum_{i=1}^{N} s_i[n] + w[n]$. Due to the periodicity of $c'(\tau_n)$, $s_i[n]$ has the following property

$$s_i[n + mL'] = s_i[n] \exp\left(j\omega_i mL'\right) \quad 0 \le n \le L' - 1, \tag{6.2}$$

where $\omega_i = 2\pi f_{D_i} T_s$ is the normalized Doppler, corresponding to the ith Starlink SV, and $-\pi \le \omega_i \le \pi$. A vector of L' observation samples corresponding to the mth period of the signal is formed as $\mathbf{z}_m \triangleq [r'[mL'], r'[mL'+1], \ldots, r'[(m+1)L'-1]]^{\mathsf{T}}$. The CPI vector is constructed by concatenating K number of $\mathbf{z}_m$ vectors to form the $KL' \times 1$ vector

$$\mathbf{y} = \sum_{i=1}^{N} \mathbf{H}_i \mathbf{s}_i + \mathbf{w}, \tag{6.3}$$

where $\mathbf{s}_i = [s_i[1], s_i[2], \ldots, s_i[L']]^{\mathsf{T}}$, and the $KL' \times L'$ Doppler matrix is defined as $\mathbf{H}_i \triangleq [\mathbf{I}_{L'}, \exp(j\omega_i L')\mathbf{I}_{L'}, \ldots, \exp(j\omega_i (M-1)L')\mathbf{I}_{L'}]^{\mathsf{T}}$, where $\mathbf{I}_{L'}$ is an $L' \times L'$ identity matrix, and $\mathbf{w}$ is the noise vector.

6.3 Receiver Structure

This section presents the structure of the proposed receiver. The proposed receiver consists of two main stages: (i) acquisition and (ii) tracking. Each of these stages are discussed next.

6.3.1 Acquisition: Sequential Matched Subspace Detection

In this dissertation, the acquisition stage is modeled as a *sequential matched subspace detection* problem. The reader is referred to [149, 180] for further interpretations of matched subspace detectors. In the first step of the proposed sequential algorithm, the presence of a single Starlink SV is tested and if the null hypothesis is accepted then $\hat{N} = 0$, which means that no Starlink SV is detected to be present in the environment under the test. If the test rejects the null hypothesis, the algorithm verifies the presence of at least one source and performs the test to detect the presence of other SVs in the presence of the previously detected SVs, sequentially. The unknown Doppler and the RS of each satellite are estimated at each step.

6.3.1.1 Sequential Matched Subspace Detector

In order to test the presence of $\mathbf{s}_i$, at the ith stage of the acquisition algorithm, the observation vector (6.3) can be written as $\mathbf{y} = \mathbf{H}_i\mathbf{s}_i + \mathbf{B}_{i-1}\boldsymbol{\theta}_{i-1} + \mathbf{w}$, where, $\mathbf{B}_{i-1} \triangleq [\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_{i-1}]$, $\boldsymbol{\theta}_{i-1} \triangleq [\mathbf{s}_1^{\mathsf{T}}, \mathbf{s}_2^{\mathsf{T}}, \ldots, \mathbf{s}_{i-1}^{\mathsf{T}}]^{\mathsf{T}}$. The generalized likelihood ratio (GLR) test for detecting $\mathbf{s}_i$ at each stage can be written as [149]

$$\mathscr{L}(\mathbf{y}) = \frac{\|\mathbf{H}_i^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{y}\|^2}{\|\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{y}\|^2} \underset{\mathscr{H}_0^i}{\overset{\mathscr{H}_1^i}{\gtrless}} \eta_i, \tag{6.4}$$

where $\mathscr{H}_1^i$ is the hypothesis that $\mathbf{s}_i$ is present at the ith stage of the acquisition, $\mathscr{H}_0^i$ is the hypothesis that $\mathbf{s}_i$ is absent, $\mathbf{y}^{\mathsf{H}}$ is the hermitian transpose of $\mathbf{y}$, $\mathbf{P}_{\mathbf{X}} \triangleq \mathbf{X}(\mathbf{X}^{\mathsf{H}}\mathbf{X})^{-1}\mathbf{X}^{\mathsf{H}}$, denotes projection matrix to the column space of $\mathbf{X}$, and $\mathbf{P}_{\mathbf{X}}^{\perp} \triangleq \mathbf{I} - \mathbf{P}_{\mathbf{X}}$. The threshold η_i is a predetermined threshold at the ith stage. The ML estimate of ω_i is obtained by maximizing the likelihood function under $\mathscr{H}_1^i$ which yields

$$\hat{\omega}_i = \arg\max_{\omega_i} \|\mathbf{H}_i^{\mathsf{H}}\mathbf{P}_{\mathbf{B}_{i-1}}^{\perp}\mathbf{y}\|^2, \tag{6.5}$$

and is used to construct $\mathbf{P}_{\mathbf{B}_{i-1}}$ and $\mathbf{H}_i$. The least squares (LS) estimate of the ith Starlink RS, i.e., $\mathbf{s}_i$, is given by $\hat{\mathbf{s}}_i = \frac{1}{\lambda_i}\mathbf{H}_i^{\mathsf{H}}\mathbf{P}_{\mathbf{B}_{i-1}}^{\perp}\mathbf{y}$, where $\lambda_i\mathbf{I} = \mathbf{H}_i^{\mathsf{H}}\mathbf{P}_{\mathbf{B}_{i-1}}^{\perp}\mathbf{H}_i$. If the null hypothesis at the ith level of the sequential algorithm is accepted, the algorithm is terminated and the estimated number of Starlink SVs will be $\hat{N} = i - 1$.

6.3.2 Tracking

After obtaining coarse estimates of the Doppler frequencies and estimates of the RSs in the acquisition step, the receiver refines and maintains these estimates. Specifically, phase-locked loops (PLLs) are employed to track the carrier phases of the detected RSs and carrier-aided delay-locked loops (DLLs) are used to track the RSs' code phases as in [149]. Each detected source has its own dedicated tracking loop.

6.4 Experimental Results

A stationary National Instrument (NI) universal software radio peripheral (USRP) 2945R was equipped with a consumergrade Ku antenna and low-noise block (LNB) downconverter to receive Starlink signals in the Ku-band. The sampling rate was set to 2.5 MHz and the carrier frequency was set to 11.325 GHz to record Ku signals over a period of 800 s. Six SVs

were broadcasting nine pure tones during this period, and the algorithm detected OFDM-like signals in the downlink of three of these Starlink SVs. To avoid redundancy, the acquisition and tracking results of one of the OFDM transmitting SVs are presented next.

6.4.1 Acquisition

The detection threshold was set $\eta_i = 1.02$, and K was set to 220. Doppler estimation was performed by searching for the maximizer of the likelihood function (6.5) according to with a step size of 1 Hz. The acquisition stages in the proposed receiver is shown in Fig. 6.3. As it can be seen in this figure, in the first stage of the acquisition, one source is detected at frequency -249.288 Hz. In the second stage of the acquisition the next source is detected at 207.212 Hz. Finally, In the third stage, the Doppler subspace of the first two sources are nulled and the resulting likelihood is less than the threshold or equivalently $\hat{N} = 2$. It should be pointed out that the detected sources can be either a satellite or a false alarm (multipath or other unwanted sources). It will be demonstrated that if at the acquisition stage a false alarm happens and a source is mistakenly detected, the carrier phase error will not converge in the tracking loops. In this case, the proposed receiver should neglect the detected source. Fig. 6.4 demonstrates the correlation properties of the estimated RSs. The slope of the autocorrelation function shows that all the available bandwidth (2.5 MHz in this experiment) is exploited.

6.4.2 Tracking

Fig. 6.5 demonstrates the carrier phase error for the two detected sources. As it can be seen in Fig. 6.5, the carrier phase error for the source located at 207.212 Hz is not

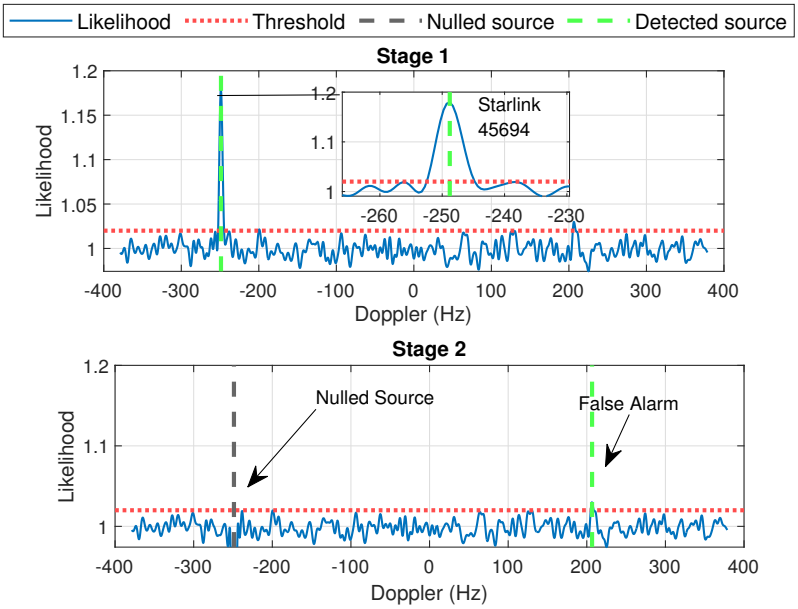


Figure 6.3: Acquisition stages in the proposed receiver for Starlink downlink signals showing the likelihood function (6.4) at each stage and the detected and nulled sources.

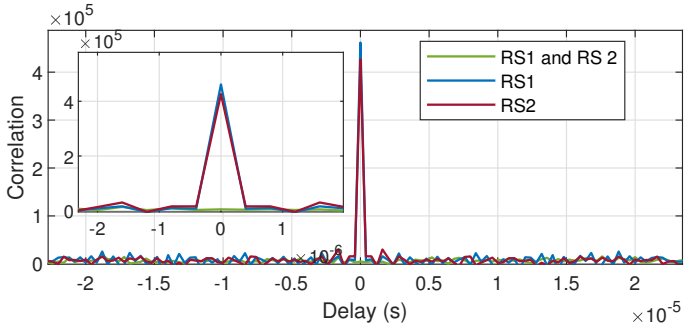


Figure 6.4: Autocorrelation function of the estimated RS of Starlink 45694 (RS 1), Starlink 45693 (RS 2), and their crosscorrelation function.

converging. Hence, the proposed receiver does not accept this source. The navigation results can be seen in Fig. 6.6. The experimental setup and the navigation framework is similar to the setup in [147]. Six starlink satellite was tracked using the proposed receiver. While all the six satellites broadcast the pure tones, three of them also transmit OFDM-like signals

(SVs indicated by green squares). The receiver position was initialized as the centroid of all SV positions, projected onto the surface of the earth, yielding an initial position error of 179 km. The receiver is equipped with an altimeter to know its attitude. The final 2-D position with the pure tones was shown to be 10 m in [147]. When the OFDM-based Doppler measurements are added the error was reduced to 6.5 m.

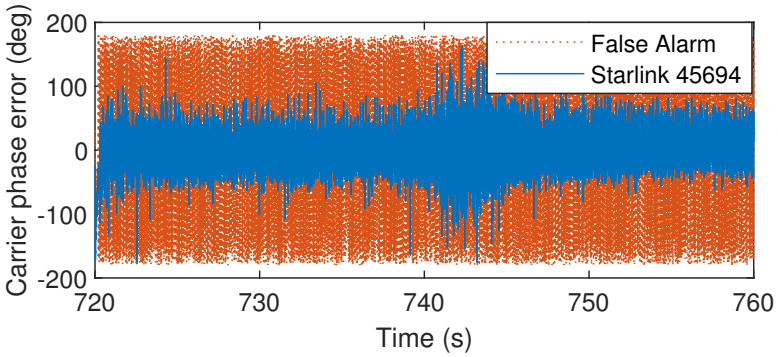


Figure 6.5: Carrier phase error for the source at -249.288 Hz (Starlink 45694) and the source at 207.212 Hz (False alarm).

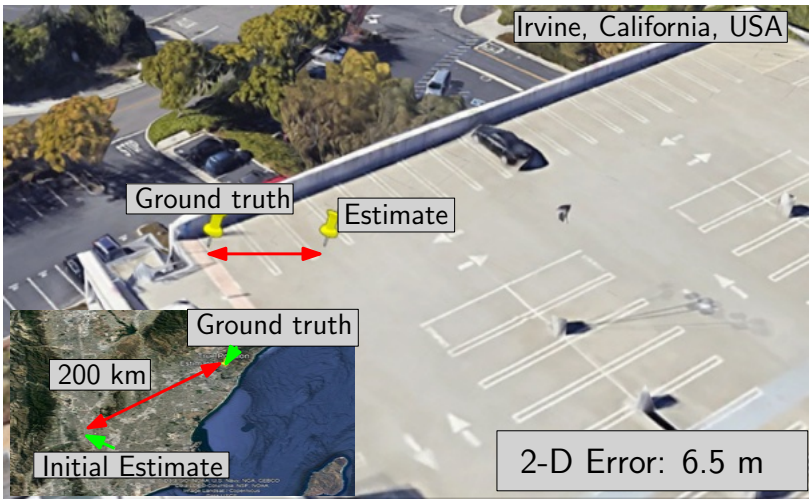


Figure 6.6: Environment layout, skyplot of satellites, and positioning results.

6.5 Differential Positioning with Starlink LEO SV Signals

This section presents experimental results of differential Doppler positioning with signals from unknown Starlink LEO SVs via the proposed framework. The baseline is considered to be 1.004 km. In what follows, the experimental setup is first discussed. Next, the navigation framework and the results from the acquisition and tracking stages of the Starlink receivers are demonstrated. Finally, receiver differential Doppler positioning results are presented.

6.5.1 Experimental Setup

To demonstrate the performance of the proposed method, a stationary scenario is considered in which the base was equipped with an Ettus E312 universal software radio peripheral (USRP) with a consumer-grade Ku antenna and low-noise block (LNB) downconverter to receive Starlink signals in the Ku band, and the rover was equipped with USRP 2974 with the same downconverter. An Octoclock was used to synchronize between the clocks of the

USRPs and the downconverters at the base and the rover. The sampling rate was set to 2.5 MHz, and the carrier frequency was set to 11.325 GHz, which is one of the Starlink downlink frequencies. The samples of the received signals were stored for off-line post-processing. The experimental setup is shown in Fig. 6.7.

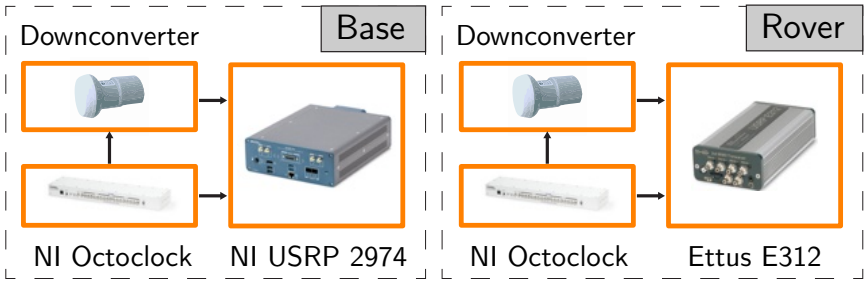


Figure 6.7: Base/rover experimental setup of the differential Doppler Starlink positioning framework.

6.5.2 Differential Doppler Positioning Framework

Pseudorange rate observables can be formed from the tracked Doppler frequencies. For the ith LEO SV, the pseudorange rate observable at time-step κ, which represents the discrete time at $t_\kappa = t_0 + \kappa T$ for an initial time t_0 and sampling time T, expressed in meters per second, is modeled as

$$\begin{aligned} z_{i_r}(\kappa) &= -c\frac{f_{D_{i_r}}(\kappa)}{F_c} \\ &= \frac{\dot{\boldsymbol{r}}_{\mathrm{SV}_i}^{\mathsf{T}}(\kappa')\left[\boldsymbol{r}_r - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa')\right]}{\|\boldsymbol{r}_r - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa')\|} + a_{i_r} \\ &\quad + c\cdot\left[\delta t_r(\kappa) - \delta t_{\mathrm{SV}_i}(\kappa')\right] \\ &\quad + c\delta t_{iono_{i_r}}(\kappa) + c\delta t_{tropo_{i_r}}(\kappa) + v_{z_{i_r}}(\kappa), \end{aligned} \tag{6.6}$$

where c is the speed of light; F_c is the carrier frequency; κ' represents discrete-time at $t_\kappa = t_0 + \kappa T - \delta t_{\text{TOF}_i}$, with δt_{TOF_i} being the true time-of-flight of the signal from the ith LEO SV to the receiver; $\boldsymbol{r}_r$ and $\boldsymbol{r}_{\text{SV}_i}(\kappa)$ are the receiver's and ith LEO SV 3-D position vectors; $\dot{\boldsymbol{r}}_{\text{SV}_i}(\kappa)$ is the ith LEO SV 3-D velocity vector; a_{i_r} is the Doppler ambiguity at the rover; $\delta \dot{t}_r$ and $\delta \dot{t}_{\text{SV}_i}$ are the clock drifts of receiver and ith LEO SV, respectively; $\delta \dot{t}_{iono_{i_r}}$ and $\delta \dot{t}_{tropo_{i_r}}$ are the ionospheric and tropospheric delay rates, respectively; and $v_{z_{i_r}}(\kappa)$ is the measurement noise, which is modeled as a zero-mean, white Gaussian random sequence with variance $\sigma^2_{i_r}(\kappa)$. The value of $\sigma^2_{i_r}(\kappa)$ is the first diagonal element of $\tilde{\mathbf{P}}_{\kappa|\kappa}$, expressed in m^2/s^2. It is worth noting the introduction of the constant bias a_{i_r}, due to the unknown Doppler frequency ambiguity f_a, which was introduced since the exact carrier frequency is unknown. In what follows, the effect of time-of-flight in the LEO SV position is neglected, i.e., $\boldsymbol{r}_{\text{SV}_i}(\kappa') \approx \boldsymbol{r}_{\text{SV}_i}(\kappa)$. This approximation introduces an error in the LEO SV position which is approximately common between the base and the rover. It should also pointed out that the error introduced by this approximation is of the order of a few meters, which is negligible compared to the position error in the TLE files which can be as high as a few kilometers. LEO SVs' positions can be estimated through TLE files and orbit determination algorithms (e.g., SGP4 [208]). Assuming a first-order clock model for both the receiver and LEO SV [185], the clock drifts can be considered as constant.

In differential Doppler positioning, in addition to the receiver whose position is to be estimated (denoted as the rover), one has access to Doppler measurements from the same LEO SV at another reference receiver (denoted as the base) whose position is known [62, 101, 235]. Essentially, this framework consists of a rover receiver (r) and a base receiver (b) in an environment comprising M visible LEO SVs. The objective is to estimate the position of the rover receiver, given knowledge about the base's position and Doppler

observables produced by the base on the same LEO SVs. Similar to (6.6), for the ith LEO SV, the pseudorange rate observable for the base at time-step κ, can be modeled as

$$\begin{aligned} z_{i_b}(\kappa) = & \frac{\dot{\boldsymbol{r}}_{\mathrm{SV}_i}^{\mathsf{T}}(\kappa)\left[\boldsymbol{r}_b - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\right]}{\|\boldsymbol{r}_b - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\|} + a_{i_b} + c\cdot(\delta t_b - \delta t_{\mathrm{SV}_i}) \\ & + c\delta t_{iono_{i_b}}(\kappa) + c\delta t_{tropo_{i_b}}(\kappa) + v_{z_{i_b}}(\kappa). \end{aligned} \tag{6.7}$$

By subtracting the tracked Doppler frequencies measured at the base from what is measured at the rover, the common terms, which are the SV clock drifts will vanish, which leads to less number of unknown terms that need to be estimated. For the differential Doppler positioning framework, the measurement to the ith LEO SV can be defined by subtracting the pseudorange rate observables at the base and the rover and adding a "known term" according to

$$\begin{aligned} \tilde{z}_{i_{r,b}}(\kappa) &= z_{i_r}(\kappa) - z_{i_b}(\kappa) + \frac{\dot{\boldsymbol{r}}_{\mathrm{SV}_i}^{\mathsf{T}}(\kappa)\left[\boldsymbol{r}_b - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\right]}{\|\boldsymbol{r}_b - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\|} \\ &= \frac{\dot{\boldsymbol{r}}_{\mathrm{SV}_i}^{\mathsf{T}}(\kappa)\left[\boldsymbol{r}_r - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\right]}{\|\boldsymbol{r}_r - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\|} + (a_{i_r} - a_{i_b}) \\ &\quad + c\cdot(\delta t_r - \delta t_b) + c\cdot\left[\delta t_{iono_r}(\kappa) - \delta t_{iono_{i_b}}(\kappa)\right] \\ &\quad + c\cdot\left[\delta t_{tropo_r}(\kappa) - \delta t_{tropo_{i_b}}(\kappa)\right] + v_{\tilde{z}_{i_{r,b}}}(\kappa). \end{aligned} \tag{6.8}$$

The LEO SV position and velocity vectors in (6.8) are obtained from TLE+SGP4 [135]. It can be assumed that the difference between ionospheric and tropospheric delay rates at the base and rover are negligible, which is reasonable when the base and the rover are relatively close to each other (e.g., a few kilometers apart). The ambiguity at both the base a_{i_b} and rover a_{i_r} can be resolved by analyzing the Doppler profile for each SV. The variance of the measurement noise term $v_{\tilde{z}_{i_{r,b}}}(\kappa) \triangleq v_{z_{i_r}}(\kappa) - v_{z_{i_b}}(\kappa)$ is $\sigma^2_{i_{r,b}}(\kappa) = \sigma^2_{i_r}(\kappa) + \sigma^2_{i_b}(\kappa)$.

Therefore, the final differential Doppler poisoning measurement model for the ith LEO SV is obtained as

$$\tilde{z}_{i_{r,b}}(\kappa) = -c\frac{\left[f_{D_{i_r}}(\kappa) - f_{D_{i_b}}(\kappa)\right]}{F_c} + \frac{-\dot{\boldsymbol{r}}_{\mathrm{SV}_i}^{\mathsf{T}}(\kappa)\left[\boldsymbol{r}_b - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\right]}{\|\boldsymbol{r}_b - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\|} \tag{6.9}$$

$$\tilde{z}_{i_{r,b}}(\kappa) = \frac{\dot{\boldsymbol{r}}_{\mathrm{SV}_i}^{\mathsf{T}}(\kappa)\left[\boldsymbol{r}_r - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\right]}{\|\boldsymbol{r}_r - \boldsymbol{r}_{\mathrm{SV}_i}(\kappa)\|} + c\cdot(\delta\dot{t}_r - \delta\dot{t}_b) + v_{\tilde{z}_{i_{r,b}}}(\kappa). \tag{6.10}$$

In this framework, by increasing the number of LEO SVs, the number of unknowns remains constant, i.e., only the rover position vector and the difference between the base and rover clock drift, defined as $\Delta\dot{t}_{r,b} \triangleq c\cdot(\delta\dot{t}_r - \delta\dot{t}_b)$, should be estimated. It should be noted that the success of the differential Doppler positioning method is dependent on the capability of a receiver in resolving the Doppler difference between the base and rover.

Using a weighted nonlinear least squares (WNLS) estimator, one could estimate the vector $\boldsymbol{x} \triangleq \left[\boldsymbol{r}_r{}^{\mathsf{T}}, \Delta\dot{t}_{r,b}\right]^{\mathsf{T}}$. Let $\tilde{\boldsymbol{z}}$ denote the vector of all pseudorange rate observables, and let $\boldsymbol{v}_{\tilde{z}}$ denote the vector of all measurement noise, which is modeled as a zero-mean Gaussian random vector with a diagonal covariance $\mathbf{R}(\kappa)$ whose diagonal elements are given by $\sigma^2_{i_{r,b}}(\kappa)$. Subsequently, one can readily write the measurement equation $\boldsymbol{z} = \boldsymbol{g}(\boldsymbol{x}) + \boldsymbol{v}_z$, where $\boldsymbol{g}(\boldsymbol{x})$ is a vector-valued function that maps the vector $\boldsymbol{x}$ to the pseudorange rate observables according to (6.9). An iterative WNLS estimator with weight matrix $\mathbf{R}^{-1}(\kappa)$ yields an estimate of $\boldsymbol{x}$, denoted by $\hat{\boldsymbol{x}}$.

6.5.3 Tracking and Positioning Results

The ground truth with which the position estimate was compared was taken from the navigation solution produced by the USRP's on-board GPS receiver. Over the course of the experiment, the receivers on-board the base and the rover were listening to three Starlink LEO SVs, namely Starlink 44740, 48295, and 47728. The SVs were visible for 320 seconds and their trajectories can be seen in Fig. 6.8.

Fig. 6.9 shows the measured differential Doppler for the three LEO SVs. The spike in the estimated differential Doppler is due to channel outage and burst error, which is common in satellite communications.

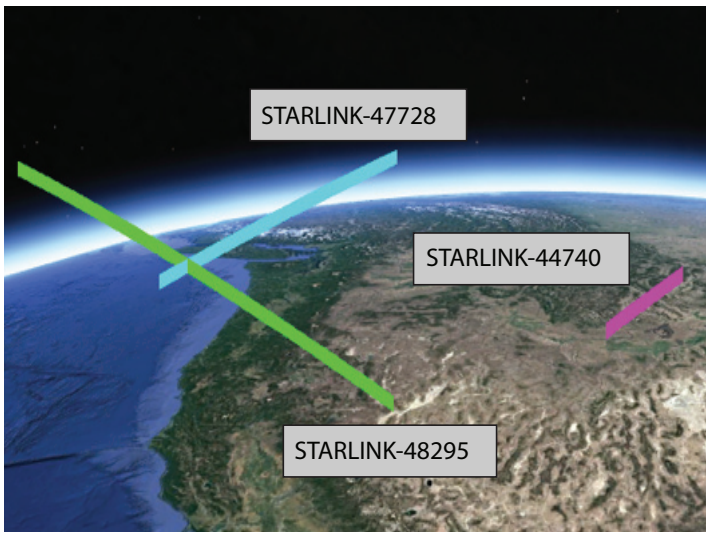


Figure 6.8: Starlink LEO SVs' trajectories.

The rover's initial position estimate was set to be approximately 200 km away from the base. The rover's position was estimated via the differential Doppler positioning framework

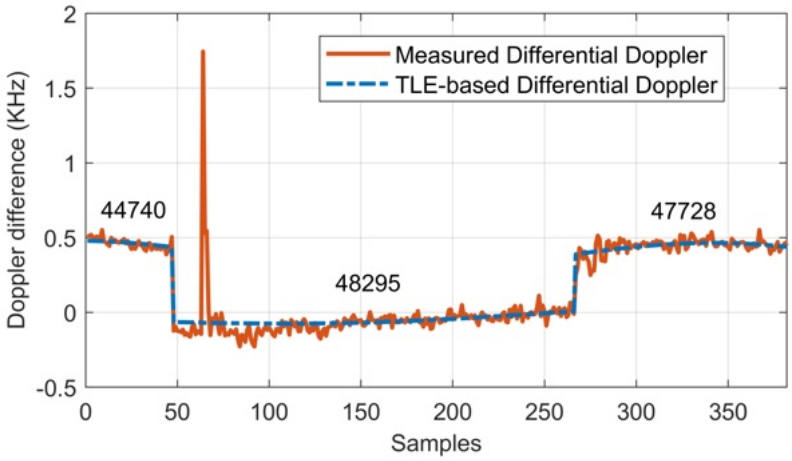


Figure 6.9: Measured Doppler difference between the base and the rover versus the predicted Doppler difference between the base and the rover based on TLE+SGP4 calculations.

described in Section [147]. The 3–D position error was found to be 33.4 m. The 2–D position error reduced to 5.6 m. Fig. 6.10 summarizes the positioning results.

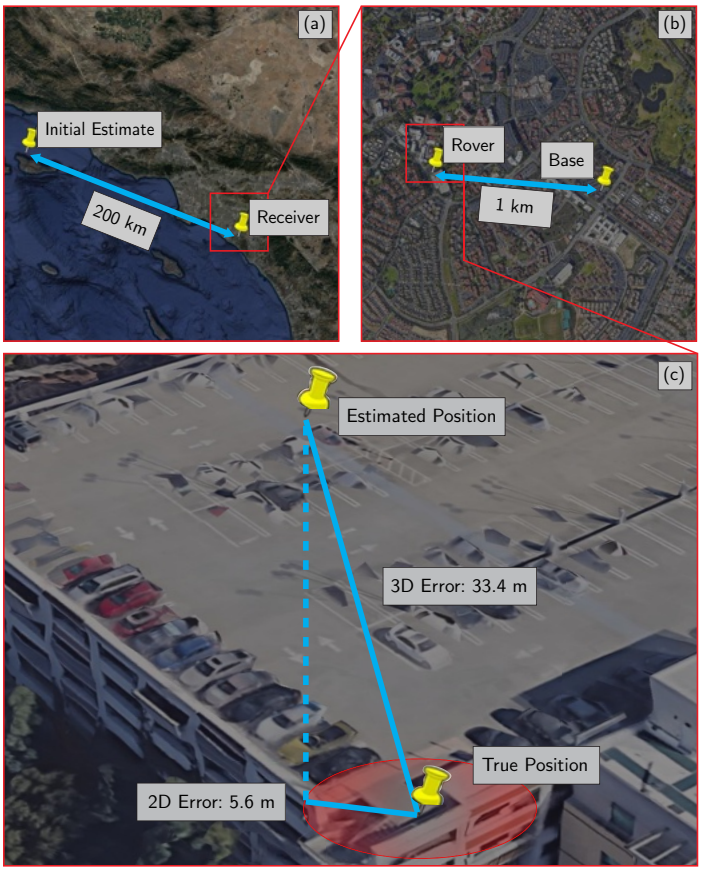


Figure 6.10: (a) Rover's initial position estimate, (b) Base's and rover's position, and (c) Rover's true and estimated position.

6.6 Differential Navigation with Orbcomm LEO SV Signals

This section presents experimental results of a UAV navigating with signals from Orbcomm LEO SVs. First, the experimental setup is discussed. Then, the navigation framework and achieved results are presented.

6.6.1 Experimental Setup

To demonstrate the differential LEO framework with Orbcomm SVs, the rover was a DJI Matrice 600 UAV equipped with an Ettus E312 USRP, a high-end VHF antenna, and a

small consumer-grade GPS antenna to discipline the on-board oscillator. The base was a stationary receiver equipped with an Ettus E312 USRP, a custom-made VHF antenna, and a small consumer-grade GPS antenna to discipline the on-board oscillator. The receivers were tuned to a 137 MHz carrier frequency with 2.4 MHz sampling bandwidth, which covers the 137–138 MHz band allocated to Orbcomm SVs. Samples of the received signals were stored for off-line post-processing. The LEO Doppler measurements were produced at a rate of 4.8 kHz and were downsampled to 10 Hz. The the base's position was surveyed on Google Earth, and the UAV trajectory was taken from its on-board navigation system, which uses GNSS SVs (GPS and GLONASS), an inertial measurement unit (IMU), and other sensors. The hovering horizontal precision of the UAV is reported by DJI to be 1.5 m. The experimental setup is shown in Fig. 6.11. The UAV traversed a total trajectory of 782 m.

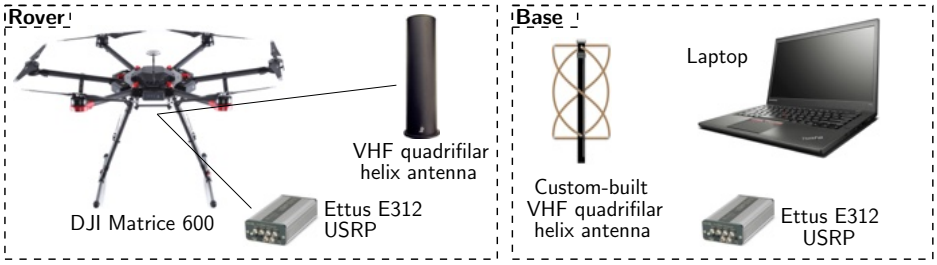


Figure 6.11: Base/rover experimental setup of the CD-LEO framework.

6.6.2 Differential Doppler Navigation Framework

Over the course of the experiment, the receivers on-board the base and the UAV were listening to 2 Orbcomm SVs, namely FM 108 and FM 116.

The Doppler measurements, described in [151], were fed to an EKF to estimate the state vector $\boldsymbol{x} \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, \Delta \dot{t}_{r,b}\right]^{\mathsf{T}}$, where $\boldsymbol{r}_r$ and $\dot{\boldsymbol{r}}_r$ are the UAV's 3–D position and velocity vectors, respectively, and $\Delta \dot{t}_{r,b} = c \cdot (\delta \dot{t}_r - \delta \dot{t}_b)$ is the clock drift difference between the base and rover. A white noise acceleration model was used for the UAV's dynamics, and a standard double integrator driven by process noise was used to model the clock bias and drift dynamics [72]. As such, the discrete-time dynamics model of $\boldsymbol{x}$ is given by

$$\boldsymbol{x}(k+1) = \mathbf{F}\boldsymbol{x}(k) + \boldsymbol{w}(k), \tag{6.11}$$

where $\mathbf{F} = \text{diag}\left[\mathbf{F}_{\text{pv}}, F_{\text{clk}}\right]$ with

$$\mathbf{F}_{\text{pv}} = \begin{bmatrix} \mathbf{I}_3 & T\mathbf{I}_3 \\ \mathbf{0}_{3\times 3} & \mathbf{I}_3 \end{bmatrix}, \quad F_{\text{clk}} = 1, \tag{6.12}$$

and T is the time interval between two measurements and $\boldsymbol{w}$ is the process noise, which is modeled as a zero-mean white random sequence with covariance matrix $\mathbf{Q} = \text{diag}\left[\mathbf{Q}_{\text{pv}}, Q_{\text{clk}}\right]$, where $Q_{\text{clk}} = c^2 S_{\tilde{w}_{\delta t}} T$, $\mathbf{Q}_{\text{pv}} = \mathbf{T} \otimes \tilde{\mathbf{Q}}_{\text{pv}}$, with

$$\mathbf{T} = \begin{bmatrix} \frac{T^3}{3} & \frac{T^2}{2} \\ \frac{T^2}{2} & T \end{bmatrix}, \quad \tilde{\mathbf{Q}}_{\text{pv}} = \text{diag}\left[\tilde{q}_x, \tilde{q}_y, \tilde{q}_z\right],$$

where $\otimes$ denotes the Kronecker product, the x, y, z acceleration process noise spectra of the white noise acceleration model were set to $\tilde{q}_x = \tilde{q}_y = 1$ m^2/s^3, $\tilde{q}_z = 0.01$ m^2/s^3, the time interval between two measurements was $T = 0.01$ s, and the receiver's clock process noise spectra were chosen to be $S_{\tilde{w}_{\delta t}} = 7.9 \cdot 10^{-25}$ which is that of a typical temperature-compensated crystal oscillator (TCXO) [72]. Note that $\boldsymbol{r}_r$ is expressed in an ENU frame centered at the UAV's true initial position. A prior for the UAV position and velocity was obtained from the UAV's on-board navigation system. The prior was used to initialize the EKF. The initial covariance matrix was set to $\mathbf{P}(0) = \text{diag}[4 \cdot \mathbf{I}_{3\times 3}, 0.01 \cdot \mathbf{I}_{3\times 3}, 0.1]$. The measurement noise covariance was set to $\mathbf{R} = (0.25) \cdot \mathbf{I}_{2\times 2}$.

6.6.3 Tracking and Navigation Results

Unlike OFDMA and CDMA-based signals where the signal power per degree of freedom is small, in classic modulation schemes, e.g., *M*ary phase shift keying (PSK), a relatively larger power is dedicated to each degree of freedom. In other words, the allocated signal power per each time/frequency unit is relatively higher than spread spectrum techniques [206]. The Orbcomm constellation utilizes the classic symmetric differential phase shift keying (SDPSK) as the modulation scheme for the downlink signals [172]. SDPSK is defined by a "zero" data state causing $-\frac{\pi}{2}$ phase shift and the "one" data state causing $+\frac{\pi}{2}$ phase shift. In order to increase the effective power of the periodic beacon in the Orbcomm constellation, the observation samples are raised to a power-of-two, which turns the SDPSK modulated signal into a fixed sequence of binary samples, which is considered as the RS for the proposed receiver.

Fig. 6.12 and Fig. 6.13 show the estimated differential Doppler tracking results and the differential Doppler from the TLE files for the two detected Orbcomm SVs.

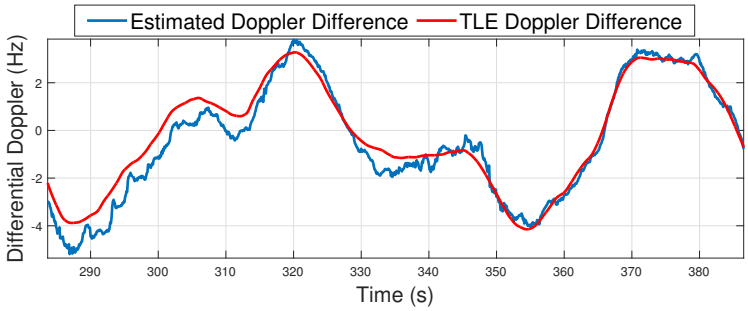


Figure 6.12: Measured Doppler difference between the base and the rover versus the predicted Doppler difference between between the base and the rover based on TLE+SGP4 calculations for FM 108.

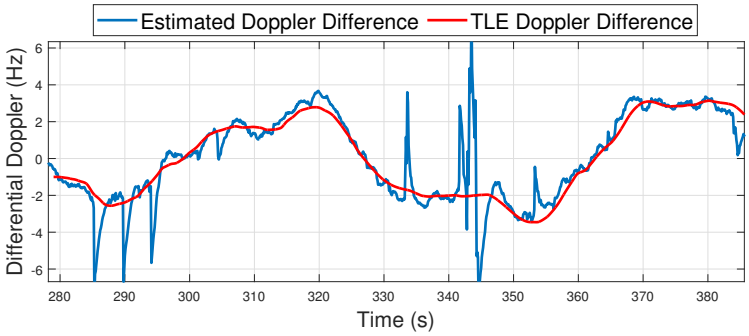


Figure 6.13: Measured Doppler difference between the base and the rover versus the predicted Doppler difference between between the base and the rover based on TLE+SGP4 calculations for FM 116.

Fig. 6.14 shows the true UAV trajectory and the estimated trajectory achieved with the proposed differential navigation framework. The 3–D position RMSE along the 782 m trajectory was calculated to be 18.87 m. It should be pointed out that the EKF used TLE+SGP4 were used to estimate the Orbcomm LEO SV states. Despite the LEO SV position estimates suffering from errors on the order of kilometers, the UAV's navigation solution was rather accurate, considering that only 2 SVs where used without other sensors.

6.6.4 Iridium NEXT System Overview

The Iridium NEXT constellation is the next-generation Iridium constellation which provides voice and data information coverage to satellite phones, pagers, and integrated transceivers over the entire Earth surface on the L-band [60].

6.6.4.1 Iridium NEXT LEO Satellite Constellation

The Iridium Next constellation consists of 75 active satellites that orbit the Earth in 6 different orbital planes spaced 30° apart [60]. The planes are near-polar orbits with 86.4°

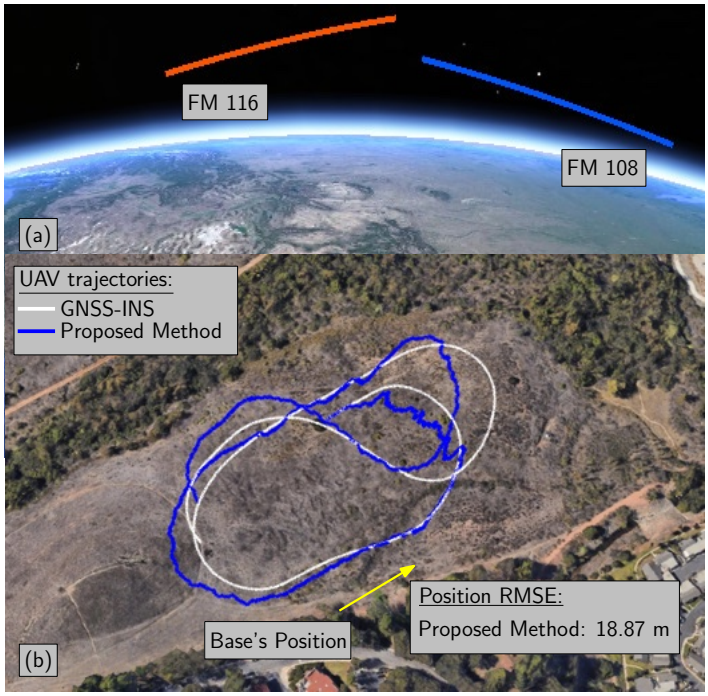


Figure 6.14: (a) Trajectories of the 2 Orbcomm LEO SVs. (b) Experimental results showing a UAV navigating for 782 m with 2 Orbcomm LEO SV signals using the proposed framework.

inclination angle and 780 km orbital altitude. Originally, the Iridium constellation was designed to incorporate 66 satellites (gathered in 6 groups of 11) in order to provide coverage for the entire Earth surface. Later, Iridium decided to enlarge the initial constellation (referred to as the NEXT campaign) by launching 12 extra satellites in order to provide 24/7 real-time coverage, which would add two extra satellites on each of the original orbital planes. Unfortunately, 3 of them are not active since they experienced technical difficulties once they were launched and thus the current constellation remains at 75 satellites.

6.6.4.2 Iridium NEXT Downlink Signals

Iridium NEXT signals are transmitted over the 1616–1626.5 MHz band, which is part of the L-band. There are 252 carriers in both the uplink and downlink channels, with carrier

spacings of 41.6667 kHz with a required bandwidth of 35 kHz [60]. These carrier frequencies are grouped into sub-bands of 8 carriers, with the 32nd group containing 4 carriers. A small portion of the Iridium NEXT spectrum, namely 1626–1626.5 MHz is assigned for paging and acquisition [60]. On this part of the spectrum are 5 simplex downlink channel with the same frequency spacing as the standard channels and with 35 kHz of bandwidth. Doppler measurements are extracted from the simplex downlink channels.

Iridium NEXT uses a TDMA scheme for downlink channel multiplexing. The signal structure over the uplink and downlink channels consists of signal bursts that are sent periodically over the TDMA frame. Each burst is composed of an unmodulated tone, succeeded by a unique word and the information data. On the simplex channel, Iridium NEXT satellites transmit the ring alert as well as paging/acquisition messages, which have the same burst structure as the standard carriers. As such, the pure tone transmitted at the beginning of each burst can be used to extract Doppler measurements. However, the burst duration is 2.56 ms and the burst period is about 1700 times longer at 4.32 seconds.

6.6.5 Multi Constellation Tracking

6.6.6 Tracking LEO Satellite Signals

After obtaining coarse estimates of the Doppler frequencies and estimates of the RSs in the acquisition step, the receiver refines and maintains these estimates. In what follows, closed loop tracking architectures are presented that are used to refine the and track the Doppler and carrier phase estimates: (i) phase-locked loops (PLLs) which are employed to track the carrier phases of the detected RSs and carrier-aided delay-locked loops (DLLs) are used to track the RSs' code phases, and (ii) Kalman Filter-Based Doppler Tracking.

Remark 2: Carrier-phase changes more rapidly compared to the Doppler frequency. It is straightforward to show that the Cramér-Rao lower bound of a random variable which changes slowly is smaller than a random variable that changes rapidly in time [91]. Carrier-phase, and carrier-aided code phase tracking convergence typically requires a higher signal power compared to Kalman Filter-Based Doppler tracking. Therefore, in weak signal scenarios, in a case that the PLL and DLL loops does not converge, the Kalman Filter-based Doppler tracking might be able to keep track of the Doppler.

6.6.6.1 Carrier Phase Tracking

Specifically, phase-locked loops (PLLs) are employed to track the carrier phases of the detected RSs and carrier-aided delay-locked loops (DLLs) are used to track the RSs' code phases.

The PLL consists of a phase discriminator, a loop filter, and a numerically-controlled oscillator (NCO). Since the receiver is tracking a periodic RS, an `atan2` discriminator, which remains linear over the full input error range of $\pm\pi$, could be used without the risk of introducing phase ambiguities. It was found that the receiver could easily track the carrier phase with a second-order PLL with a loop filter transfer function

$$F_{\mathrm{PLL}}(s) = \frac{2\kappa\omega_n s + \omega_n^2}{s}, \tag{6.13}$$

where $\kappa \equiv \frac{1}{\sqrt{2}}$ is the damping ratio and ω_n is the undamped natural frequency, which can be related to the PLL noise-equivalent bandwidth $B_{n,\mathrm{PLL}}$ by $B_{n,\mathrm{PLL}} = \frac{\omega_n}{8\zeta}(4\zeta^2+1)$ [131]. The loop filter transfer function in (6.35) is discretized at a sampling period $T_{\mathrm{sub}} \triangleq LT_s$, which is the time interval at which the loop filters are updated (commonly referred to as the subaccumulation interval). The discretized transfer function is realized in state-space. The

output of the loop filter at time-step k, denoted by $v_{\text{PLL},k}$, is the rate of change of the carrier phase error, expressed in rad/s. The Doppler frequency estimate at time-step k is deduced by dividing $v_{\text{PLL},k}$ by 2π. The carrier phase estimate at time-step k is updated according to

$$\hat{\phi}_k = \hat{\phi}_{k-1} + v_{\text{PLL},k} \cdot T_{\text{sub}}, \tag{6.14}$$

where $\hat{\phi}_0 \equiv 0$. A measure of the change in distance rate between the transmitter and receiver can be formed from the carrier phase as $z(k) = \frac{c}{2\pi F_c} v_{\text{PLL},k}$, where c is the speed-of-light and F_c is the carrier frequency.

6.6.6.2 Kalman Filter-Based Doppler Tracking

The time-varying component of the continuous-time true Doppler is a function of (i) the true range rate between the LEO SV and the receiver, denoted by $\dot{d}(t)$ and (ii) the time-varying difference between the receiver's and LEO SV's clock bias rate, denoted by $\dot{b}(t)$ and expressed in meters per second. Hence,

$$\omega(t) = 2\pi \left[-\frac{\dot{d}(t)}{\lambda} + \frac{\dot{b}(t)}{\lambda} + f_a \right], \tag{6.15}$$

where λ is the carrier wavelength. The clock bias is assumed to have a constant drift, i.e., $b(t) = a(t - t_0) + b_0$. Moreover, simulations with LEO SVs show that the following kinematic model for $d(t)$ holds for short period of times

$$\dddot{d}(t) = \tilde{w}(t), \tag{6.16}$$

where $\tilde{w}$ is a zero-mean white noise process with power spectral density $q_{\tilde{w}}$. Let k denote the time index corresponding to $t_k = kT + t_0$, where $T = M \cdot L \cdot T_s$ is the sampling interval, also known as subaccumulation period, and $M \cdot L$ is the number of subaccumulated samples.

The discrete-time kinematic model of the Doppler state vector $\boldsymbol{\omega}_k \triangleq [\omega_k, \dot{\omega}_k]^{\mathsf{T}}$ is given by

$$\boldsymbol{\omega}_{k+1} = \mathbf{F}\boldsymbol{\omega}_k + \mathbf{w}_k, \tag{6.17}$$

$$\mathbf{F} \triangleq \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \quad \mathbf{Q} \triangleq q_{\tilde{w}} \begin{bmatrix} \frac{T^3}{3} & \frac{T^2}{2} \\ \frac{T^2}{2} & T \end{bmatrix}, \tag{6.18}$$

where $\mathbf{F}$ is the discrete-time state transition matrix, $\mathbf{w}_k$ is the discrete-time process noise with zero mean and covariance matrix $\mathbf{Q}$. The initial state is given by $\boldsymbol{\omega}_0 = \left[2\pi f_a + \frac{2\pi}{\lambda}(a - \dot{d}(t_0)), -\frac{2\pi}{\lambda}\ddot{d}(t_0)\right]^{\mathsf{T}}$.

Let $\hat{\boldsymbol{\omega}}_{k|l}$ denote the KF estimate of $\boldsymbol{\omega}_k$ given all the measurements up to time-step $l \leq k$, and $\tilde{\mathbf{P}}_{k|l}$ denote the corresponding estimation error covariance. The initial estimate $\hat{\boldsymbol{\omega}}_{0|0}$ with a corresponding $\tilde{\mathbf{P}}_{0|0}$ are provided from the acquisition stage. The KF-based tracking algorithm time update and the measurement update are discussed next.

6.6.6.3 Kalman Filter Time Update

The KF time update equations are straightforwardly given by

$$\hat{\boldsymbol{\omega}}_{k+1|k} = \mathbf{F}\hat{\boldsymbol{\omega}}_{k|k}, \tag{6.19}$$

$$\tilde{\mathbf{P}}_{k+1|k} = \mathbf{F}\tilde{\mathbf{P}}_{k|k}\mathbf{F}^{\mathsf{T}} + \mathbf{Q}. \tag{6.20}$$

6.6.6.4 Kalman Filter Measurement Update

The KF measurement update equations is carried out based on the ML estimate of the Doppler. The Doppler wipe-off is performed as $\tilde{r}_k[i] = r[i + kML]\exp\left[-j\hat{\theta}_{k+i|k}\right]$, where $\hat{\theta}_{k+i|k}$ is obtained according to $\hat{\theta}_{k+i|k} = \hat{\omega}_{k|k} iT_s + \hat{\dot{\omega}}_{k|k}\frac{i^2}{2}T_s^2$, for $i = 0, \ldots, ML-1$. The vector $\tilde{\mathbf{y}}_{k+1}$ is constructed as $\tilde{\mathbf{y}}_{k+1} = [\tilde{r}_k[0], \tilde{r}_k[2], \ldots, \tilde{r}_k[ML-1]]^{\mathsf{T}}$. Similar to (6.3), one can show that

$$\tilde{\mathbf{y}}_{k+1} = \tilde{\mathbf{H}}_{k+1}\mathbf{s} + \tilde{\mathbf{w}}_{\mathrm{eq}_{k+1}}, \tag{6.21}$$

where the residual Doppler matrix is

$$\begin{aligned}&\tilde{\mathbf{H}}_{k+1}\\&\triangleq [\mathbf{I}_L, \exp(j\Delta\omega_k L)\,\mathbf{I}_L, \ldots, \exp(j\Delta\omega_{k+1}(M-1)L)\,\mathbf{I}_L]^{\mathsf{T}},\end{aligned} \tag{6.22}$$

and $\Delta\omega_{k+1} = \omega_{k+1} - \hat{\omega}_{k+1|k}$. The proposed KF innovation is given by

$$\nu_{k+1} = \text{argmax}_{\Delta\omega_{k+1}} \frac{1}{M} \|\tilde{\mathbf{H}}_{k+1}^{\mathsf{H}} \tilde{\mathbf{y}}_{k+1}\|^2, \tag{6.23}$$

which is a direct measure of the Doppler error.

6.6.6.5 Kalman Filter Initialization

The initial estimates of the Doppler $\hat{\omega}_{0|0}$ and the Doppler rate $\hat{\dot{\omega}}_{0|0}$ are obtained from the acquisition stage. Let Δf_D and $\Delta \dot{f}_D$ denote the sizes of the Doppler and Doppler rate search bins. It is assumed that the initial Doppler and Doppler rate errors are uniformly distributed within one bin, and their initial probability density functions (pdfs) are bounded by Gaussian pdfs with zero-mean and standard deviations $\frac{\Delta f_D}{3}$ and $\frac{\Delta \dot{f}_D}{3}$, respectively. Therefore, the KF is initialized with

$$\begin{aligned}\hat{\boldsymbol{\omega}}_{0|0} &= \left[2\pi \hat{f}_D(0), 2\pi \hat{\dot{f}}_D(0)\right]^{\mathsf{T}},\\ \tilde{\mathbf{P}}_{0|0} &= \text{diag}\left[\frac{4\pi^2}{9}\Delta f_D^2, \frac{4\pi^2}{9}\Delta \dot{f}_D^2\right].\end{aligned} \tag{6.24}$$

The tracking results can be seen in Fig. 6.15. The results are compared wit Doppler frequency obtained from TLE+SGP4 propagator.

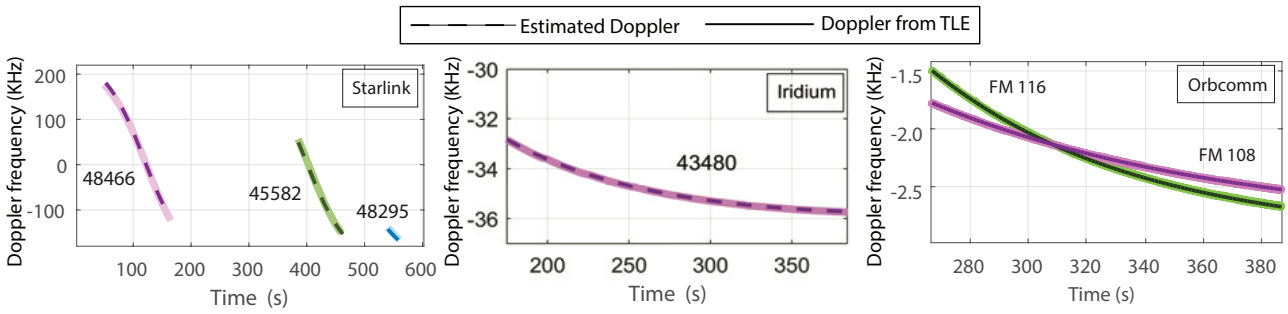


Figure 6.15: Doppler tracking results of three constellations: (i) Starlink, (ii) Iridium Next, and (iii) Orbcomm.

6.7 Estimation of Doppler Stretch with Application to Tracking Globalstar Satellite Signals

This section considers Globalstar satellite signals. To the best of the author's knowledge, this section shows the first tracking results of Globalstar signals. One of the challenges of opportunistic navigation with Globlastar satellites is *Doppler compensation*. In Globalstar LEO satellite system, the Doppler is compensated to a nominal value at the satellite or at the ground station [181]. Doppler compensation takes place based on the center of each satellite transmitter beams. When the Doppler is compensated, the measured Doppler by a ground receiver is different from the real Doppler, which renders the measured Doppler unusable for opportunistic navigation. This section utilizes spectrum distortion to recover the Doppler frequency and track Globalstar satellite signals. The idea behind the presented method is that even though the Doppler is compensated, it can be be estimated coarsely at the receiver, based on the time compression or expansion of the received signal due to the original Doppler. This compression/expansion effect changes the apparent chipping rate at the receiver and distorts the spectrum of the transmitted signal.

6.8 Signal Model

Consider a LEO satellite that moves with a constant radial velocity v relative to the receiver. The velocity is positive if the LEO satellite moves away from the receiver. Thus, the distance between the LEO satellite and the receiver is $r(t) = r(0) + vt$. Denote the transmitted signal by $p(t)\exp(j\omega_c t)$, where $p(t)$ is a waveform, $\omega_c = 2\pi f_c$, and f_c is the carrier frequency. The received signal can be modeled as

$$y(t) = \alpha p(t - \tau(t))\exp[j\omega_c(t - \tau(t))] + w(t), \tag{6.25}$$

where α is the channel gain, $w(t)$ is an additive noise, and

$$\tau(t) = \frac{r(t)}{c} = t_0 + \gamma t, \tag{6.26}$$

where $t_0 \triangleq \frac{r(0)}{c}$, $\gamma \triangleq \frac{v}{c}$ is the Doppler stretch, and c is the speed of light. Hence, the received signal can be written as

$$y(t) = \alpha' p[(1-\gamma)t - t_0]\exp(-j2\pi f_D t)\exp(j\omega_c t) + w(t), \tag{6.27}$$

where $f_D = f_c\gamma$ is the Doppler frequency, and $\alpha' = \alpha\exp(-j\omega_c t_0)$ is the equivalent channel gain. It can be inferred from (6.27) that the Doppler effect results in the time expansion or time compression of the transmitted signal. In other words, the relative velocity of the transmitter and the receiver results in two changes in the characteristics of the transmitted signal: (i) the phase which appears as the Doppler frequency shift and (ii) the time scale which appears as time expansion or time compression. However, in some applications, the expansion or compression is negligible. More precisely, denoting the bandwidth and the duration of the transmitted signal by B and T, respectively, if

$$BT \ll \frac{c}{2|v|}, \tag{6.28}$$

the stretching effect can be neglected [236], i.e., (6.27) can be approximated as

$$y(t) \approx \alpha' p(t-t_0)\exp(-j2\pi f_D t)\exp(j\omega_c t) + w(t), \tag{6.29}$$

which is referred to as the narrow-band model for the transmitted signal. Intuitively, a periodic signal can be considered as a linear combination of constant frequency complex exponential components, i.e., $\exp(j2\pi ft)$, where f is within the bandwidth of the transmitted signal. For each complex exponential component, the Doppler changes the carrier frequency by $|\gamma|f$, which results in the variation of phase rotation over the signal duration of $\frac{T}{1-\gamma}$ by $2\pi|\gamma|fT/(1-\gamma)$. Hence, $2|v|BT/c \ll 1$ should hold in order for the variations of the phase rotations for all the complex exponential components to be equal.

6.8.1 Globalstar Forward Link Signals

Globalstar LEO satellites employ CDMA. For a given Forward CDMA Channel, the spreading and modulation process is applied as shown in Fig. 6.16. The spreading sequence structure is comprised of an inner PN sequence pair and an outer PN sequence. The inner sequence has a chip rate of $R_{c_{in}} = 1.2288$ Mcps and a length of $L_{c_{in}} = 2^{10}$ chips. The outer PN sequence has 1200 outer chips per second and a length of 288 outer PN chips. One inner PN sequence period exactly fits into a single outer PN chip. The outer PN modulates the inner PN sequence to produce the actual spreading sequence resulting in a period of 240 ms. It should be noted that the inner PN sequence pair identifies the satellite orbital plane; there are eight different pairs. The outer PN sequence identifies the satellite. Each satellite beam is identified by a time offset of the outer PN sequence for the corresponding orbit. The gateways perform precorrection of time and frequency in their transmitted waveform to compensate for time delay and Doppler variations due to satellite motion for the feeder link.

Considering inner and outer PN sequences, the overall length of PN sequence for Globalstar signals is $L_c = 288 \times 2^{10}$ chips an the period of the PN sequence is $T_c = 0.24$ s. However, accroding to (6.27), and due to the high speed of the LEO satellites relative to the receiver, the apparent period of the transmitted signal at the receiver might be different from T_c. This is due to the time expansion or time compression effect.

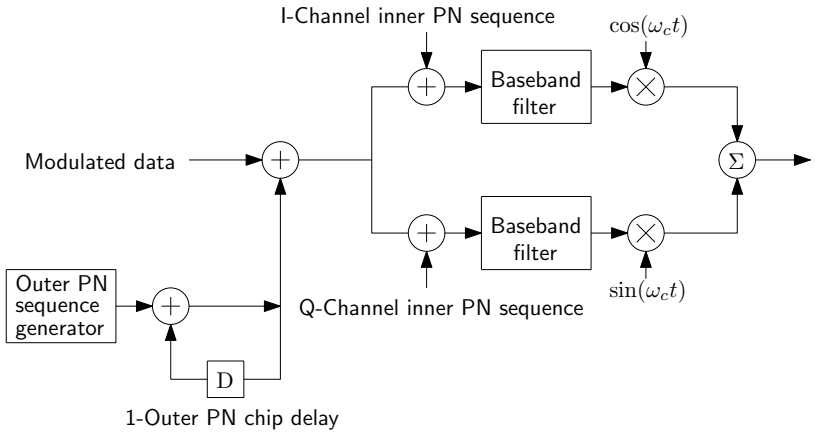


Figure 6.16: Block diagram of forward link spreading in Globalstar CDMA based downlink signals. In this diagram the + sign is used to show the spreading operation [181].

Remark 1: According to (6.27), the apparent period is $T_{c_{\text{app}}} = \frac{T_c}{1-\gamma}$ and, consequently, the apparent chipping rate is $R_{c_{\text{app}}} = R_c - \varepsilon$, where $\varepsilon = \gamma R_c$ hereafter is referred to as chipping rate offset (CRO).

It should be pointed out that the relation ship between the CRO and the Doppler is $\varepsilon = \frac{R_c}{f_c} f_D$. For instance, for a transmitted signal at carrier frequency 2481.77 MHz with a chipping rate of $R_c = 1.2288$ MHz and a Doppler frequency of 20 kHz will result in $\varepsilon \approx 10$ Hz.

Assuming that the sampling frequency is F_s, the number of samples of one period of the PN sequence is $N_c = \frac{L_c}{R_c} F s$. Therefore, the apparent number of samples of the PN sequence is

$$N_{c_{\text{app}}} = \frac{N_c R_c}{R_c - \varepsilon} = \frac{L_c F_s}{R_c - \varepsilon}. \tag{6.30}$$

Factorizing R_c, expanding the Taylor series results around $\varepsilon = 0$, and retaining the first terms results in

$$N_{c_{\text{app}}} \approx \frac{L_c F_s}{R_c} \left(1 - \frac{\varepsilon}{R_c}\right). \tag{6.31}$$

Therefore, the apparent number of samples of the PN sequence will change by

$$k = \left\lfloor \frac{N_c F_s \varepsilon}{R_c^2} \right\rceil \tag{6.32}$$

samples, where $\lfloor \cdot \rceil$ denotes rounding to the closest integer.

6.9 Chipping Rate Offset Estimation

As mentioned previously, due to the high Doppler frequencies of LEO satellites, the apparent chipping rate can be different from its original value and the difference between these two values is referred to as the CRO.

6.9.1 Doppler compensation

In a wideband communication system, when the bandwidth and signal duration do not satisfy (6.28), the narrowband signal model (6.29) will not hold and conventional Doppler and delay estimation/tracking schemes will not work properly [236]. Hence, a Doppler tracking algorithm should be aided by a CRO estimator. In this section, another motivation for CRO estimation is presented. In some LEO satellites, the Doppler is corrected/compensated

at the gateway [181]. *Doppler compensation* is performed to reduce the apparent Doppler frequency at the user terminals. Using phased array antennas, *spot beams* can be used to enhance coverage and reduce interference [30]. Doppler compensation can be performed at the gateway according to the center of a spot beam (see Fig. 6.17). Therefore, the user will experience a Doppler which is different from f_D in (6.27). Hence, the estimated Doppler will not match with that of the TLE files.

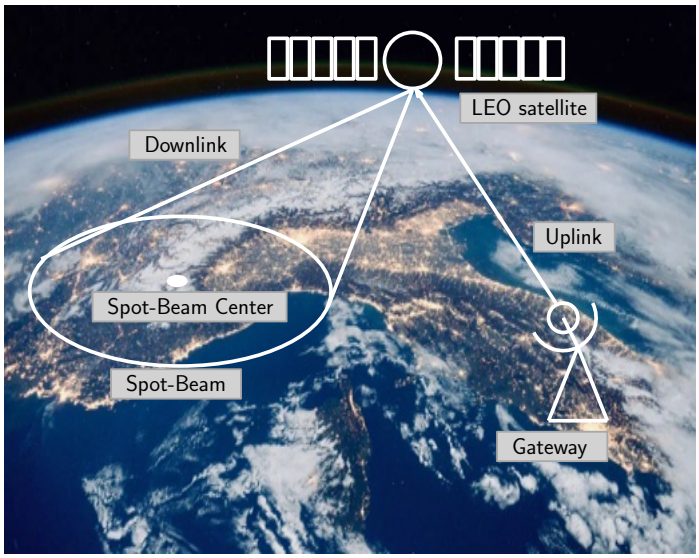


Figure 6.17: Gateway to user terminal link and the spot beam.

6.9.2 Recovering the Original Doppler Frequency

Denoting the estimated Doppler of the center of spot beam at the gateway by $\hat{f}_{D_{\mathrm{G}}}$, the received signal model can be expressed as

$$y(t) = \alpha' p\left[(1-\gamma)t - t_0\right] \exp\left[-j2\pi\left(f_D - \hat{f}_{D_{\mathrm{G}}}\right)t\right] \cdot \exp\left(j\omega_c t\right) + w(t). \tag{6.33}$$

After carrier wipe-off and sampling, the discrete-time model can be expressed as

$$y[n] = \alpha' p[(1-\nu)n - n_0] \exp\left(j2\pi \frac{f_D - \hat{f}_{D_{\mathrm{G}}}}{F_s} n\right) + w[n]. \tag{6.34}$$

Consequently, a Doppler estimator yields an estimate of the *compensated* Doppler, i.e., $f_D - \hat{f}_{D_{\mathrm{G}}}$, rather than the *true* Doppler. It should be pointed out that γ still contains the effect of the Doppler frequency. Therefore, estimating γ provides an estimate of the Doppler frequency according to $f_D = \gamma f_c$. The maximum likelihood estimator is used to estimate ε and consequently the PN sequence. The detected PN sequence was used to acquire and track the Globlstar satellite signal using the receiver implementation discussed in [107]. It should be pointed out that the detected PN sequence has a time-varying length. In other words, the length of the PN sequence depends of the Doppler frequency which changes with time. Therefore, the main difference between the proposed receiver and the CDMA receiver presented in [107] is that the delay estimation is performed using the PN sequence with the apparent length.

6.9.3 CRO-Aided Tracking Loops

After obtaining an estimate of γ, phase-locked loops (PLLs) are employed to track the carrier phases of the detected satellite and carrier-aided delay-locked loops (DLLs) are used

to track the code phase of the PN sequence. Fig. 6.18 shows the block diagram of the CRO-aided tracking loops [146].

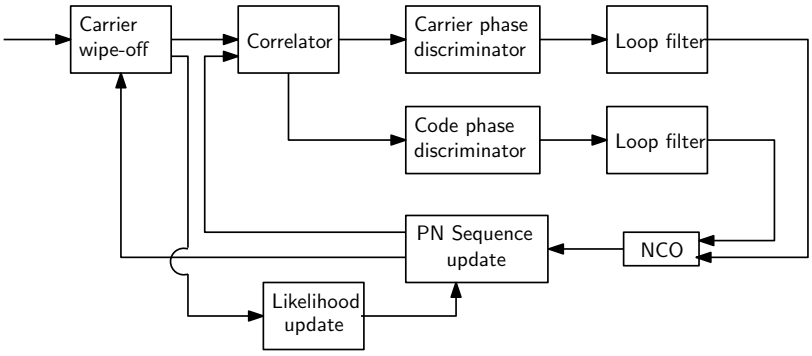


Figure 6.18: Block diagram of CRO-aided tracking loops.

Using a maximum-likelihood (ML) estimator of γ, the apparent chipping rate of the locally generated PN sequence is adjusted according to $R_{c_{rmapp}} = R_c - \varepsilon$.

The PLL consists of a phase discriminator, a loop filter, and a numerically-controlled oscillator (NCO). It was found that the receiver could track the carrier phase with a second-order PLL with a loop filter transfer function

$$F_{\text{PLL}}(s) = \frac{2\kappa\omega_n s + \omega_n^2}{s}, \tag{6.35}$$

where $\kappa \equiv \frac{1}{\sqrt{2}}$ is the damping ratio and ω_n is the undamped natural frequency, which can be related to the PLL noise-equivalent bandwidth $B_{n,\text{PLL}}$ by $B_{n,\text{PLL}} = \frac{\omega_n}{8\zeta}(4\zeta^2 + 1)$ [131]. The loop filter transfer function in (6.35) is discretized at a sampling period $T_{\text{sub}} \triangleq \frac{L_c}{F_s}$, which is the time interval at which the loop filters are updated and is typically known as the subaccumulation interval. The discretized transfer function is realized in state-space. The output of the loop filter at time-step k, denoted by $v_{\text{PLL},k}$, is the rate of change of the carrier

phase error, expressed in rad/s. The Doppler frequency estimate at time-step k is deduced by dividing $v_{\mathrm{PLL},k}$ by 2π. The carrier phase estimate at time-step k is updated according to

$$\hat{\theta}_k = \hat{\theta}_{k-1} + v_{\mathrm{PLL},k} \cdot T_{\mathrm{sub}}, \tag{6.36}$$

where $\hat{\theta}_0 \equiv 0$.

The carrier-aided DLL employs an early-minus-late discriminator. The early and late correlations at time-step k used in the discriminator are denoted by Z_{e_k} and Z_{l_k}, respectively, which are calculated by correlating the received signal with an early and a delayed version of the estimated PN sequence, respectively. The time shift between Z_{e_k} and Z_{l_k} is defined as the early-minus-late time, denoted by ξ. The DLL loop filter is a simple gain K_{DLL}, with a noise-equivalent bandwidth $B_{n,\mathrm{DLL}} = \frac{K_{\mathrm{DLL}}}{4} \equiv 0.5$ Hz. The output of the DLL loop filter v_{DLL} is the rate of change of the code phase, expressed in s/s. Assuming low-side mixing at the radio frequency front-end, the code phase estimate is updated according to

$$\hat{t}_{s_{k+1}} = \hat{t}_{s_k} - \left(v_{\mathrm{DLL},k} + \frac{v_{\mathrm{PLL},k}}{2\pi f_c} \right) \cdot T_{\mathrm{sub}}. \tag{6.37}$$

The code phase estimate can be used to deduce the pseudorange observables.

6.10 Experimental Results

This section validates the proposed receiver experimentally. The objective of these experiments are to: (i) compare the measured Doppler with the Doppler from the TLE files to visualize the Doppler compensation effect and (ii) compare the variation in the pseudorange estimated by the receiver to the variation in range between the stationary receiver and the Globalstar satellites obtained by the TLE files. For this purpose, the stationary receiver was equipped with a costumer-grade GAT-17MP Globalstar antenna and

a small consumer-grade GPS. The satellite signals were down-mixed and sampled via a single-channel universal software radio peripheral (USRP) 2974 driven by a GPS-disciplined oscillator (GPSDO). Samples of the received signals were stored for off-line post-processing.

Fig. 6.19 demonstrates the estimated Doppler by the receiver and the Doppler obtained from the TLE files. It can be seen that the measured Doppler is dramatically different from the Doppler profile obtained from the TLE files. As mentioned previously, Doppler compensation is performed to reduce the apparent Doppler frequency at the user terminals. Doppler compensation is performed at the gateway according to the center of the spot beam. Due to the distance between the center of the spot beam and the user terminal, the user terminal experiences a Doppler frequency which is relatively smaller than what is expected from the Doppler from the TLE files.

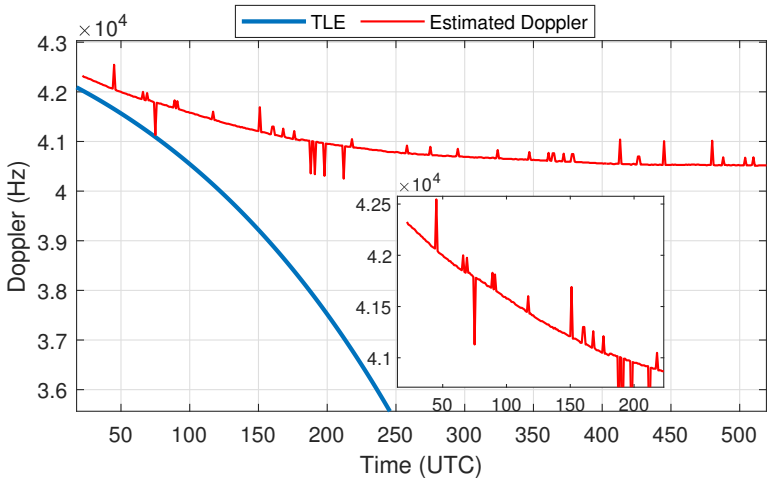


Figure 6.19: The estimated Doppler frequency and the Doppler obtained from TLE files.

The CRO ε is estimated and used to estimate the transmitted PN sequence. The likelihood function of the ML estimator for different values of ε is demonstrated in Fig. 6.20. The estimated PN sequence was used to acquire and track the Globlstar satellite using the receiver implementation discussed in [107]. The tracking tracking results versus those obtained from TLE are plotted in Fig. 6.21.

As can be seen from this figure, the proposed method is tracking the pseudorange of one of Globalstar satellites which was available in a window of 190 s at the time of experiment. The average error between the measured pseudornage and the pseudorange predicted is approximately 111.12 m over a window of 190 s.

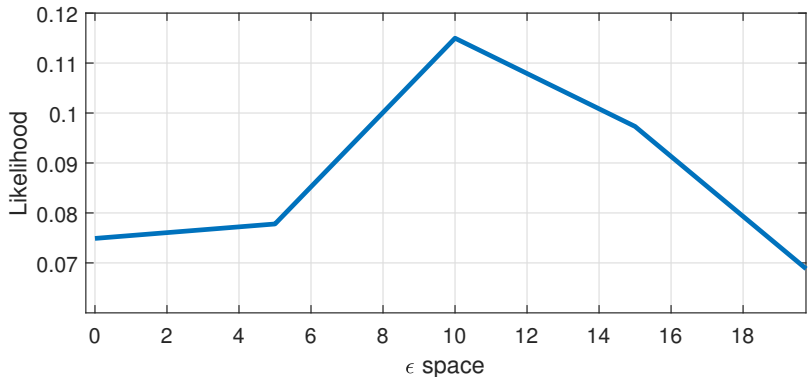
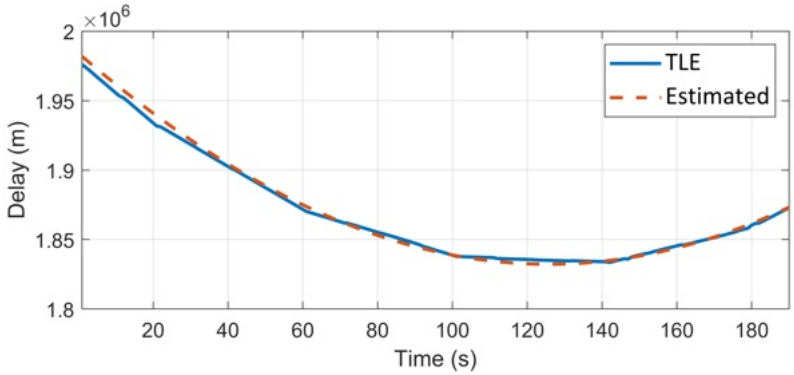


Figure 6.20: The likelihood function for the ML estimator of Globalstar forward link signals for different values of epsilon.

(a)



(b)

Figure 6.21: (a) Trajectory of Globalstar satellite GS 37743. (b) Comparing the delay tracking results obtained by the proposed receiver with the delays obtained from the TLE.

6.11 Deciphering GPS Signals

6.11.1 Received Baseband Signal Model

Let $s(t)$ denote the beacon signal consisting of L consecutive symbols with symbol duration T_{symb}. Each symbol is drawn from an arbitrary MPSK constellation. The beacon signal is continuously transmitted at a period of $L \cdot T_{\text{symb}}$. After channel propagation and baseband sampling at an interval T_s, the received signal can be modeled as

$$y[n] = \sum_{i=-\infty}^{\infty} \alpha d_i \exp\left[j\left(2\pi\Delta f[n]n + \theta_0\right)\right] s[n - iL - n_d[n]] + w[n], \tag{6.38}$$

where $y[n]$ is the complex baseband sample at the nth time slot; $N = L\frac{T_{\text{symb}}}{T_s}$ is the length of the beacon in samples; $\Delta f[n] \triangleq f_D[n]T_s$ is the normalized Doppler frequency and f_D is the true Doppler frequency in Hz; θ_0 is the initial beat carrier phase; $w[n]$ models noise and interference; α is an unknown complex amplitude; d_i is a low rate data symbol drawn from the same constellation of the beacon signal, e.g., navigation bits in GPS signals; and n_d is the unknown delay of the received beacon signal which can be modeled as

$$n_d[n] = \left\lfloor \frac{t_d[n]}{T_s} \right\rceil, \qquad t_d[n] \triangleq t_{d_0} - \frac{\Delta f_D[n]}{f_c} n, \tag{6.39}$$

where t_{d_0} is the initial delay in seconds of the received beacon signal and f_c is the carrier frequency.

It is worth noting that the signal model in (6.38) is descriptive of the majority of BON scenarios. In some cases, (6.38) directly applies, i.e., the received signal consists purely of one signal of interest and observation noise. In other scenarios, such as CDMA-based communication systems, the presence of interference should also be taken into account. For example, there is a total of 128 logical channels multiplexed onto one cdma2000 forward-link channel: (i) one pilot channel, (ii) one sync channel, (iii) up to seven paging channels, and (iv) traffic on the remaining channels. Each of these logical channels is spread orthogonally by a 128-Walsh code, multiplexed with the rest of the channels, and the resulting signal is multiplied by a complex PRN sequence which consists of a pair of maximal-length sequences. The CDMA signal is then filtered to limit its bandwidth before transmission. In such a system, and CDMA systems in general, the signal on the pilot channel simplifies to the complex PRN sequence, which is the beacon of interest. Therefore, one can look at the CDMA signal as the sum of two terms: (i) the signal on the pilot channel, or the beacon signal, and (ii) the sum of the signals on the remaining channels. Due to

the properties of Walsh codes and assuming the symbols on the sync, paging, and traffic channels are uncorrelated, one can model the sum of the signals on the remaining channels as noise. In fact, for a large number of logical channels such as in cdma2000, the *central limit theorem* practically applies and the resulting noise can be modeled as a zero-mean Gaussian random variable. Consequently, the CDMA signal can be modeled according to (6.38), where $s[n]$ is the beacon on the pilot channel, and $w[n]$ captures channel noise and interference from the rest of the logical channels.

6.12 THE BON FRAMEWORK

The core of the BON framework comprises: (i) detection of multiple SOPs, (ii) blind Doppler tracking, (iii) coherent accumulation, and (iv) beacon signal decoding (see Fig. 6.22).

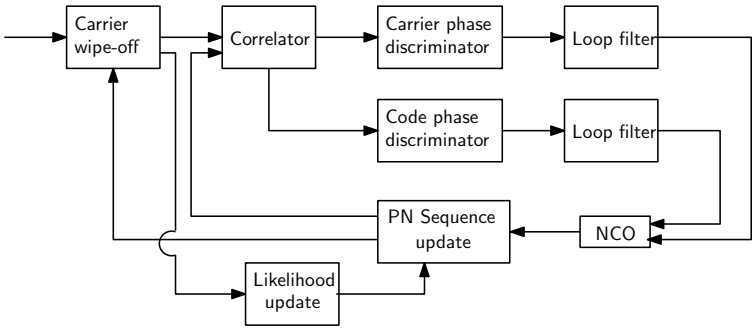


Figure 6.22: BON framework.

This paper mainly focuses on the blind Doppler estimation and the beacon signal decoding steps. However, properly designed algorithms for signal activity detection of

multiple SOPs in the bandwidth of interest and the coherent integration of the observations are essential steps to cognitively decipher the SOPs. It should be pointed out that signal activity detection of multiple SOPs may also include an additional modulation classification step to identify the modulation type of the beacon signals of the corresponding SOPs. Spectrum sensing techniques in cognitive radio systems, e.g, the energy detector [117], and blind modulation classification methods, e.g., [39] and the references therein, can be employed to detect the presence of SOPs and classify the modulation type of their beacon signal. In the BON framework developed in this paper, a heuristic algorithm for *joint signal activity detection and modulation classification* is presented. The algorithm performs a nonlinear operation to wipe-off the data symbols and turn the received signal into a pure tone. Then, the fast Fourier transform (FFT) of the resulting signal is taken to detect the tone and estimate its location in the frequency spectrum. For instance, for MPSK modulated data, raising the received signal to the power of M wipes off the data symbols. For an MPSK signal where M is unknown, the signal is raised to varying powers until a pure tone is observed in the FFT. The value of M for which the tone appears determines the order of the PSK modulation of the unknown signal. Next, the Doppler frequency of the resulting tone is tracked and the beacon symbols are subsequently decoded using the methods discussed in the following subsections. It is important to note that this operation can be performed simultaneously on multiple SOPs with different Doppler frequencies. In the sequel, M is assumed to be known via the aforementioned procedure.

6.12.1 Blind Doppler Estimation

6.12.1.1 Coherent Processing Interval for Doppler Estimation

As mentioned previously, blind Doppler estimation is one of the main challenges that has to be addressed in the BON framework. To this end, a blind Doppler estimation algorithm is discussed next. Define a coherent processing interval (CPI) of length I samples in which the Doppler frequency is assumed to be constant. Therefore, for a CPI index k, the Doppler within the kth CPI can be expressed as $f_D[n] = f_{D_k}$ for $kI \leq n \leq (k+1)I-1$. The blind Doppler estimator in the BON framework processes one CPI at a time to estimate the time history of the Doppler frequency. Define the vector of wiped-off observations in the kth CPI as

$$\bar{\boldsymbol{y}}_k^M \triangleq \left[(y[kI])^M, (y^M[kI+1])^M, \ldots, (y^M[(k+1)I-1])^M\right]^{\mathsf{T}}, \tag{6.40}$$

which can now be approximated by samples of a pure tone with normalized Doppler frequency $M\Delta f$. The Doppler tracking algorithm relies on estimating the frequency of this tone in each CPI, and is stated in Algorithm 2. Define the vector of estimated Doppler frequencies as

$$\hat{\boldsymbol{f}}_D^K \triangleq \left[\hat{f}_{D_0}, \hat{f}_{D_1}, \ldots, \hat{f}_{D_{K-1}}\right]^{\mathsf{T}}.$$

Algorithm 2 summarizes the steps to obtain $\hat{\boldsymbol{f}}_D^K$ from $\{\bar{\boldsymbol{y}}_k^M\}_{k=0}^{K-1}$.

6.12.2 Coherent Integration

In this subsection, it is assumed that $I = N$. The following results can be extended to $I > N$. Given an estimate of the Doppler frequency, an estimate of the change in the beacon

Algorithm 2 Blind Doppler estimator

Input: $\{\bar{\mathbf{y}}_k^M\}_{k=0}^{K-1}$

Output: $\hat{\boldsymbol{f}}_D^K$

For $k \in \{0,\ldots,K-1\}$

· Find $\hat{b}_k = \arg\max\left\{\left|\text{FFT}\left(\bar{\mathbf{y}}_k^M\right)\right|\right\}$.

· Calculate $\Delta\hat{f}_k = \begin{cases} \frac{\hat{b}_k}{M\cdot I} & \hat{b}_k \le \frac{I}{2} \\ \frac{I-\hat{b}_k}{M\cdot I} & \hat{b}_k > \frac{I}{2} \end{cases}$

· Calculate $\hat{f}_{D_k} = \frac{\Delta\hat{f}_k}{T_s}$.

End

signal delay $\hat{t}_{d_k}$ at the kth CPI can be formed according to

$$\hat{t}_{d_k} = \sum_{l=0}^{k-1} \frac{\hat{f}_{D_l}}{f_c} NT_s.$$

Subsequently, the Doppler frequency can be wiped-off from the original observation, resulting in

$$\hat{y}_k[m] \triangleq y[m+kI]\exp\left[-j\left(2\pi\Delta\hat{f}_k m + \hat{\theta}_k\right)\right] \otimes \delta[m+kI-\hat{n}_{d_k}], \qquad 0 \le m \le N-1, \tag{6.41}$$

where $\hat{n}_{d_k} = \left\lfloor \frac{\hat{t}_{d_k}}{T_s} \right\rceil$, $\hat{\theta}_k \triangleq 2\pi f_c \hat{t}_{d_k}$ is the estimated carrier phase, and $\otimes$ denotes the circular convolution. Subsequently, F frames of the resulting signal are accumulated according to

$$\tilde{y}[m] = \frac{1}{F}\left(\hat{y}_0[m] + \sum_{k=0}^{F-1} \hat{d}_k \hat{y}_k[m]\right) \approx \alpha' s[m-n_0] + w'[m], \tag{6.42}$$

where $n_0 \triangleq \lfloor \frac{t_{d_0}}{T_s} \rfloor$ is the initial beacon signal delay; w' models the resulting noise; α' is a constant complex amplitude capturing the channel effect, initial beat carrier phase, and the residual Doppler; and $\hat{d}_k = \Pi_{\kappa=0}^{k} \tilde{d}_r$ is the estimate of the low rate data, where

$$\tilde{d}_r = \text{sgn}\left\{\text{Re}\left\{\sum_{m=0}^{N-1} \hat{y}_r[m]\hat{y}_{r-1}[m]^*\right\}\right\}; \tag{6.43}$$

where $\text{Re}\{\cdot\}$ denotes the real part. Note that the signal part of the right-hand side of (6.42) is a shifted version of the beacon signal with a complex scaling. Let the vector $\boldsymbol{z}$ of length L

denote the resampled vector $\tilde{\boldsymbol{z}} \triangleq [\tilde{y}[0], \ldots \tilde{y}[N-1]]^T$ down to the symbol rate. The vector $\boldsymbol{z}$ is then fed to the beacon decoding algorithm to decipher the beacon signal.

6.12.3 Blind Beacon Decoding

After wiping-off the Doppler, performing coherent integration, and resampling, the symbols of the beacon signal are decoded. The decoding problem can be modeled as

$$\boldsymbol{z} = \bar{\alpha}\boldsymbol{s} + \bar{\boldsymbol{w}}, \tag{6.44}$$

where $\bar{\alpha}$ is the unknown complex amplitude and $\bar{\boldsymbol{w}}$ the resulting noise vector after resampling. Consider the set $\mathscr{L}$ consisting of all M^L combinations of L-dimensional vectors $\boldsymbol{q}$ whose elements are the integers between 0 to $M-1$. For MPSK signals, a beacon sequence is given by $\boldsymbol{s} = \exp\left(\frac{j2\pi}{M}\boldsymbol{q}\right)$, where $\boldsymbol{q} \in \mathscr{L}$. The maximum likelihood (ML) decoder of $\boldsymbol{q}$ is

$$\hat{\boldsymbol{q}} = \arg\max_{\boldsymbol{q}\in\mathscr{L}} \left| \boldsymbol{z}^H \exp\left(\frac{j2\pi}{M}\boldsymbol{q}\right)\right|, \tag{6.45}$$

where $(\cdot)^*$ and $(\cdot)^H$ are the complex conjugate and Hermitian operators, respectively.

A naïve solution to the optimization problem (6.45) consists of a brute-force search over all possible values of $\boldsymbol{q}$, which has exponential complexity. The order of the brute-force search is M^L. In an effort to solve (6.45) in less than quadratic complexity, the methods described in [126] and later again in [196] are used to decode the beacon signal. It can be shown that the complexity of the algorithms proposed in [126] and [196] are on the order $L\log_2 L$.

6.13 EXPERIMENTAL RESULTS

In order to demonstrate the capability of the BON framework in cognitively deciphering a signal of interest, an experiment was conducted with real GPS signals. The GPS L1 C/A signals contain PRN codes at 1.023 Mega chips per second (Mcps), modulated by binary PSK (BPSK) ($M = 2$) navigation bits at 50 bits per second (bps). Multiple GPS satellites transmit simultaneously in the same channel using CDMA. In what follows, the experimental setup is first described. Next, GPS PRNs are decoded using the BON framework. The decoded PRNs are then used in an SDR to produce pseudorange measurements on GPS satellites and in turn solve for a stationary receiver's position.

6.13.1 Experimental Setup

The setup consists of a GPS antenna, which was mounted on the roof of the Winston Chung Hall at the University of California, Riverside, USA. The GPS signals were down-mixed and sampled via a National Instruments universal software radio peripheral (USRP), driven by a GPS-disciplined oscillator (GPSDO). The samples of the received signals were stored for off-line post-processing.

6.13.2 Deciphering GPS PRNs with the BON Framework

6.13.2.1 Multiple Signal Detection

A heuristic method to detect and localize multiple SOPs in the frequency-domain was proposed in Section 6.12. In order to detect and classify multiple SOPs, the observations are raised to the power of M to wipe off the PRNs and the low rate data symbols and detect the

resulting pure tone. Since GPS satellites transmit BPSK signals, when the received signal is raised to the power $M = 2$, the data is wiped off and results in complex exponentials with twice the Doppler frequencies. This allows the BON framework to detect several satellites that transmit in the same channel, and multiple peaks will be seen in the Fourier transform of the dataless signal, as shown in Fig. 6.23.

6.13.2.2 Blind Doppler Estimation

Next, the peaks shown in Fig. 6.23 are tracked over time by performing Algorithm 2 on sequential CPIs of the stored samples, producing Doppler frequency estimates to each satellite, as shown in Fig. 6.24(b). The CPI is considered to be $I = 120N$. The estimated Doppler was compared with the Doppler calculated from the known receiver position and the satellite positions obtained from the two-line element (TLE) files and orbit determination software (e.g., SGP4 [211]). TLE files contain the Keplerian elements parameterizing the orbits of LEO satellites and are made publicly available and updated daily by the North American Aerospace Defense Command (NORAD) [152]. As it can be seen in Fig. 6.24(b) and 6.24(c), the blind chirp parameter estimator successfully tracks the Doppler frequency of multiple SOPs producing negligible residuals when subtracted from the Doppler frequencies obtained from TLE and SGP4.

6.13.2.3 Beacon Signal Decoding

Once the Doppler frequencies are estimated, the residual carrier is wiped off from the received signal, compensated for delays due to Doppler, and coherently accumulated. The navigation bits are wiped off by two successive frames to determine whether a transition

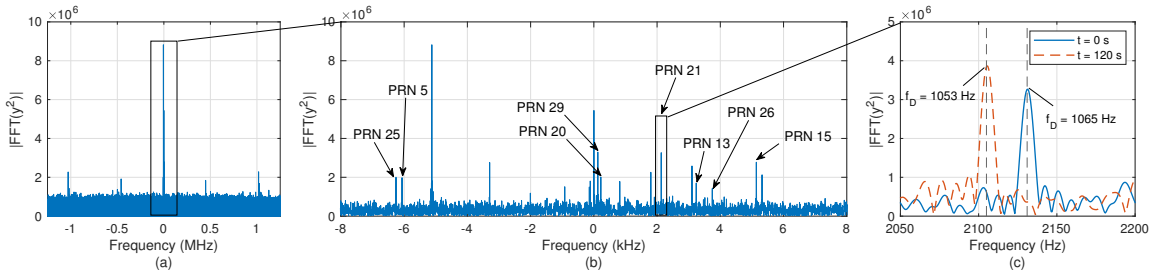


Figure 6.23: (a) Joint signal activity detection and modulation classification of the beacon signals: Recall that the frequency component of power of two will be double that of the original signal. (b) Multiple satellite detection: FFT peaks corresponding to different GPS satellites. (c) FFT peaks of PRN 21 at $t = 0$ s and $t = 120$ s.

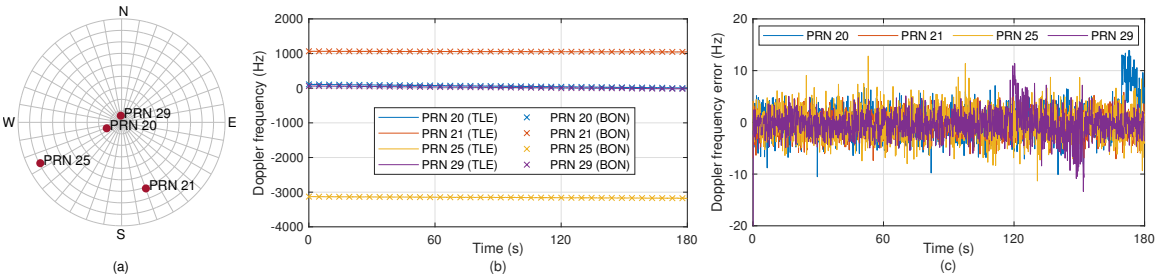


Figure 6.24: (a) Skyplot of 4 of the visible GPS satellites. (b) Time history of (i) the Doppler frequency of 4 of the GPS satellites obtained from the TLE and SGP4 orbit determination software and (ii) the estimated Doppler frequencies of the corresponding satellites using the BON framework. (c) Errors between the Doppler frequencies obtained from the TLE and the ones obtained using the BON framework.

occurred or not. The resulting accumulations are decimated to the chipping rate of GPS PRNs and processed by the beacon decoding algorithm of the BON framework. A scatter plot of the accumulated signal before beacon signal decoding is shown in Fig. 6.25(a) for the 4 satellites. While the scatter plots of PRNs 20, 21, and 25 look significantly noisy, their effective SNR is high enough for the blind beacon decoding algorithm to decode the PRNs with less than 10% chip error, as shown in Table I. The correlation function between the decoded and true PRNs of the 4 GPS satellites are shown in Fig. 6.25(b). In addition to

Table I, the correlation plots in Fig. 6.25(b) also demonstrate that the PRN of each of the 4 satellites was adequately decoded.

Table 6.1: The percentage of correctly decoded GPS PRN chips using the BON framework

PRN number	PRN 20	PRN 21	PRN 25	PRN 29
Percentage of correctly decoded Chips	96%	94%	91%	99.9%

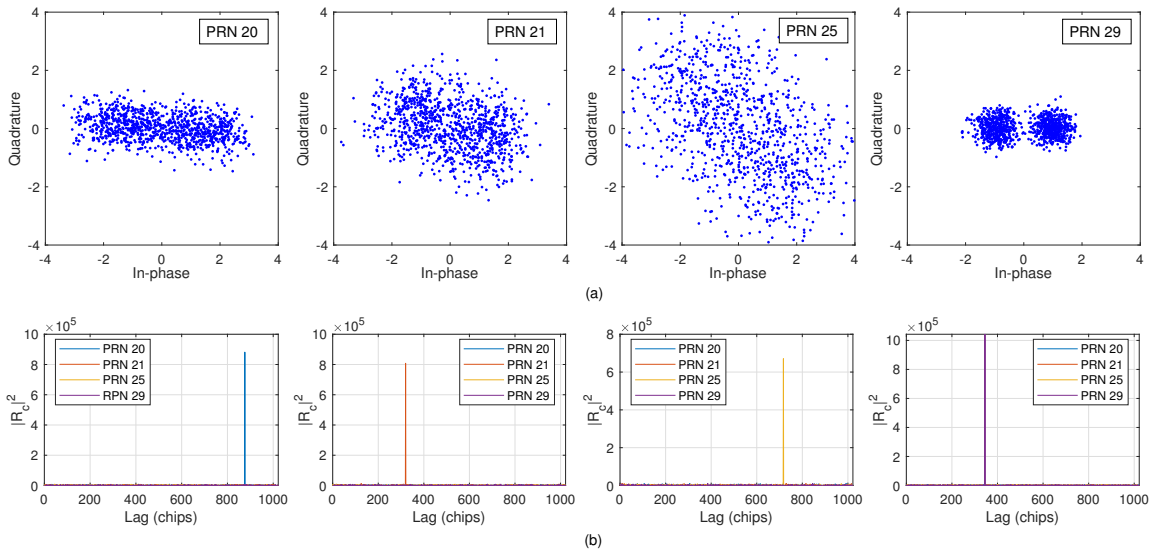


Figure 6.25: (a) Scatter plots of the coherent accumulation for the 4 satellites before beacon detection. (b) Correlations between the decoded PRN of each satellite and the true PRNs.

6.13.2.4 Producing Navigation Observables from Decoded PRNs

The decoded beacons are then used to produce pseudorange observables from the received GPS signals. The initial Doppler is known from the previous steps. The code phases are also known to be zero, since the decoded beacon has the phase of the PRN at the

time of initial reception. Therefore, signal acquisition is already performed; however, it is shown in Fig. 6.26(a) for illustration purposes. The initial Doppler and code phase estimates are used to initialize an SDR's tracking loops: a third-order phase-locked loop (PLL) with a carrier-aided delay-locked loop (DLL) with the dot product discriminator. The in-phase and quadrature components of the tracked prompt correlation for PRN 21 are shown in Fig. 6.26(b) for a period of 5 seconds. Since GPS signals are exploited opportunistically in this paper, it is not assumed that the receiver can decode the navigation message. As a result, the code phase estimate expressed in meters will be considered as the pseudorange estimate. The delta range of PRN 21 measured using the BON framework is shown in Fig. 6.26(c) along with the delta range estimated via TLE and SGP4 software. The delta range is a pseudorange from which the initial value is subtracted.

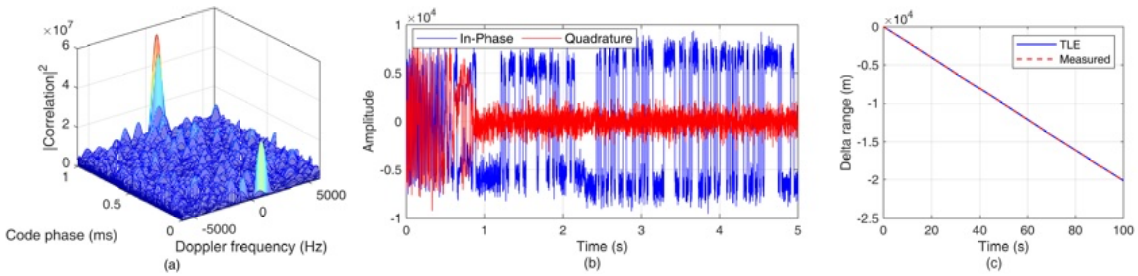


Figure 6.26: (a) Signal acquisition for PRN 21 using the decoded beacon. (b) Signal tracking of PRN 21 over a period of 5 seconds. (c) Delta range computed from the TLE and the code phase measured by the BON receiver expressed in meters.

6.13.3 Navigation Solution

This section presents the navigation solution from the BON framework. The altitude $r_{r,z}$ of the stationary antenna which collected the GPS signals is assumed to be known; hence,

only the two-dimensional (2-D) states $r_{r,x}$ and $r_{r,y}$ are estimated. The pseudorange from the ith satellite at time-step k can be modeled as

$$\rho_i(k) = \|\boldsymbol{r}_r - \boldsymbol{r}_{s_i}(k)\| + b_i + \varepsilon_i(k), \qquad k = 1,2,\ldots, \tag{6.46}$$

where $\boldsymbol{r}_r \triangleq [r_{r,x}, r_{r,y}, r_{r,z}]^\mathsf{T}$ is the three-dimensional (3-D) position of the receiver, $\boldsymbol{r}_{s_i}$ is the 3-D position vector of the ith satellite obtained from the TLEs, b_i is a bias term that captures the unknown bias between the receiver's and ith satellite's clocks, and ε_i is the measurement error capturing ionospheric and tropospheric delays and measurement noise. The pseudorange measurements for all satellites at all time-steps are stacked in one measurement vector $\boldsymbol{\rho}$ and a batch nonlinear least-squares (NLS) estimator is implemented to solve for $\boldsymbol{x} \triangleq [\boldsymbol{r}_r^\mathsf{T}, b_1, \ldots, b_S]^\mathsf{T}$, where S is the total number of visible satellites. The receiver's position in the NLS was initialized around 150 km from the true receiver's position, and all the biases $\{b_i\}_{i=1}^S$ were initialized with zeros. The resulting position error with 4 satellites over a 110-second period was found to 54.4 meters. The experimental setup and results are shown in Fig. 6.27.

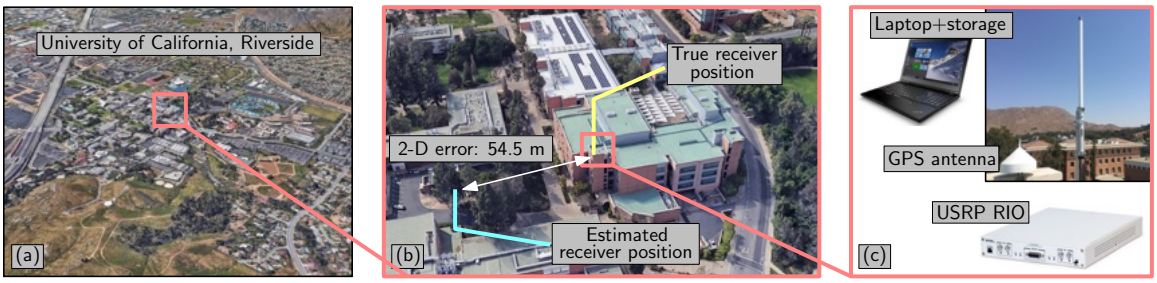


Figure 6.27: (a) Experimental environment. (b) True and estimated receiver positions. (c) Experimental hardware setup.

Chapter 7: Conclusion

In this chapter, we summarize the status of the work presented in this dissertation, and outline future plans.

7.1 Summary

This dissertation addressed the following challenges of navigation with signals of unknown and dynamic nature. First, unlike public networks where the broadcast RSs are known at the UE and are universal across network operators, in private networks, the signal specifications of some RSs may not be available to the public or are subject to change. Second, in cellular LTE networks, several RSs (e.g., cell-specific reference signal (CRS)) are broadcast at regular and known time intervals, regardless of the number of UEs in the environments. *Ultra-lean* design refers to minimizing these *always-on* transmissions. 5G NR and modern communication systems transmit some of the RSs only when necessary or *on-demand* which results in a dynamic the RS signals.

A receiver architecture was proposed to cognitively extract navigation observables from 3G, 4G, 5G, and LEO-based signals. Unlike conventional opportunistic receivers which require knowledge of the signal structure, particularly the RSs, the proposed receiver only

relied on the periodicity of the RSs and requires knowledge of only the carrier frequency of the signal. To exploit the full available bandwidth and improve ranging accuracy, the proposed receiver was designed to estimate all the RSs contained in the transmitted signals corresponding to multiple sources. Navigation observables (pseudorange and carrier phase) were subsequently derived from the estimated RSs. The proposed receiver operated in two stages: (i) acquisition and (ii) tracking. The acquisition stage of the proposed receiver was modeled as a sequential detection problem where the number of gNBs and their corresponding RSs and Doppler frequencies were unknown. The generalized likelihood ratio (GLR) test for sequentially detecting active sources was derived and used to estimate the number of unknown sources and their RSs. In order for the receiver to refine and maintain the Doppler and RS estimates provided by the acquisition stage, tracking loops were designed. A sufficient condition on the Doppler estimation error to ensure that the proposed GLR asymptotically achieves a constant false alarm rate (CFAR) was derived. The output of the tracking loops, namely carrier phase and code phase, were then used to estimate the receiver's position.

Extensive experimental results are presented demonstrating the capabilities of the proposed receiver with real 3G, 4G, 5G, and LEO SV signals on ground and aerial platforms.

7.2 Contributions

In this section, a summary of contributions is presented. The contributions of the proposal are either presented in peer-reviewed journal papers and under review journal papers.

Contributions of peer-reviewed journal paper [149]:

- A cognitive opportunistic navigation (CON) receiver design was presented, which could estimate the unknown beacons of a gNB. The cognitive nature of the proposed receiver enabled estimating both 5G NR always-on and on-demand beacons which are not necessarily always-on. Using extensive experiments, it was shown that the estimated beacons possess higher bandwidth compared to conventional 5G opportunistic navigation receivers, which allowed for producing more precise navigation observables.

- A sequential GLR-based detector was derived to detect the presence of multiple gNBs on the same channel and provide an estimate of the number of active gNBs. The detector relied on matched subspace detection, where the signal subspace was defined by the Doppler frequencies of the gNBs. The sequential GLR detector estimated the number of gNBs, and their Doppler frequencies, and it provided an initial estimate of their unknown beacons, which are then used and refined in the tracking loops.

- A sufficient condition on the Doppler estimation error to ensure that the proposed GLR asymptotically achieves a CFAR was derived.

- Extensive experimental results were presented demonstrating the capabilities of the proposed CON receiver with real 5G signals on ground and aerial platforms. On a ground vehicle, it was demonstrated that the CON receiver yields a reduction of 10% and 37.7% in the estimated delay and Doppler root mean squared error (RMSE), respectively, over that achieved with a conventional opportunistic navigation 5G receiver that had complete knowledge of the transmitted beacons but only relied on

always-on beacons. On a UAV, it was demonstrated that the proposed CON receiver enables the UAV to navigate over a 416 m trajectory with two 5G NR gNBs achieving a position RMSE of 4.35 m. To evaluate the performance of the CON receiver in a scenario where the beacons are always-on, another experiment was conducted in which a UAV navigated with LTE eNodeBs, achieving a position RMSE of 2.07 m, which is identical to the performance achieved with a conventional opportunistic navigation 4G receiver that had complete knowledge of the transmitted beacons.

Contributions of peer-reviewed journal paper [148]:

- Matched subspace detectors were proposed for two different scenarios: (i) beacons with IC, e.g., the symbols of the beacon are drawn from M-ary PSK (MPSK) modulation set, and (ii) beacon with NIC, i.e., the beacon signal are not constrained to take integer values and can assume any arbitrary complex-valued number.
- A near-optimal, low complexity algorithm was proposed to reduce the complexity of the detector with IC. The effect of the symbol errors in the detected beacon signal on the carrier-to-noise ratio (CNR) was characterized analytically. The proposed matched subspace detectors were capable of detecting multiple unknown signals in the environment with relatively low computational complexity.
- For the NIC scenario, closed-form expressions for the probability of detection and false alarm were derived. The effective SNR was calculated and the effect of Doppler estimation error on the performance of the detector was analyzed.
- Experimental results were presented showing an application of the proposed cognitive approach by enabling an UAV to detect and exploit terrestrial cellular signals for

navigation purposes. In one experiment, the UAV achieved submeter-level accurate navigation over a trajectory of 1.72 km, by exploiting signals from four 3G cdma2000 transmitters.

- The OFDM frame of 5G signals was reconstructed in a blind fashion. On-demand and always-on beacons are demonstrated in the OFDM signal structure of real 5G signals.

Contributions of peer-reviewed [147]

- A model for the Starlink LEO SV's downlink signals was presented.
- An algorithm was proposed to (i) acquire the Starlink LEO SV signals and (ii) track the Doppler frequency of each detected SV.
- Next to [105], the first experimental positioning results with Starlink downlink signals were presented.
- In [105], an adaptive Kalman filter was used to track the carrier phase of Starlink LEO SVs. However, the method presented in [105] relied on tracking the phase of a single carrier. When a more complicated signal structure was used in the downlink signal, e.g., OFDMA, a more sophisticated method should be developed to exploit the entire signal bandwidth for navigation purposes. Indeed, the method in [105] was not capable of exploiting the entire signal bandwidth, and it only relied on tracking a single frequency component. In this paper, by considering a general model for the Starlink downlink signals, the unknown parameters of the signal were estimated for the first time for Starlink LEO SVs, and were subsequently used to detect the Starlink LEO SVs and track their corresponding Doppler frequencies. The proposed method enabled one to estimate the synchronization signals of the Starlink LEO SVs.

Contributions from Under Review Journal Papers are:

- The methods presented in [8, 148, 149] relied on the difference between the Doppler frequencies of the transmitters to acquire and track the unknown sources. However, the acquisition and tracking of unknown sources may fail in the following extreme scenarios: (i) an almost static scenario that may lead to a *Doppler subspace overlap* and (ii) a high dynamic scenario where the receiver or the transmitter are moving with high dynamics which results in an *intensive Doppler rate*. These two extreme scenarios introduce the following challenges in the acquisition and tracking of the unknown sources:

  The almost static scenario: In a scenario where the receiver and the transmitter are almost static, the Doppler frequencies of the transmitting sources will be very close to each other. This event is referred to as the Doppler subspace overlap. Distinguishing between the sources with Doppler subspace overlap becomes very challenging for the cognitive navigation framework.

  Intensive Doppler rate scenario: In cognitive navigation frameworks, the unknown and dynamic parameters of the beacons are estimated via a coherent accumulation of the received samples over time. High values of Doppler rate limit the coherence time, i.e., the time interval that the channel between the transmitter and the receiver is static. A limited coherence time affects the unknown source acquisition and tracking performance. Therefore, considering the effect of the Doppler rate in the signal model and selecting a proper coherent processing interval (CPI) play a key role in intensive Doppler rate scenarios.

One of the proposed solutions to overcome the mentioned challenges is designing a receiver architecture which can jointly estimate the unknown beacons of multiple sources in almost static and intensive Doppler rate scenarios. Similar to [149], the roles of providing a fine estimate of the RS, and tracking the code and carrier phases are played by the tracking loops. The major difference would be properly designed adaptive gains which are selected based on the detector performance analysis. The adaptive gains are provided by the acquisition stage and are designed based on the source detection performance. Feeding this information to the tracking loops establishes a link between the acquisition and tracking loops which is necessary for the mentioned challenging scenarios, and distinguishes the proposed architecture from conventional navigation algorithms.

- Analyzing the effect of Doppler rate estimation error on the autocorrelation function and providing a closed-form solution for the autocorrelation attenuation in the presence of Doppler rate error and comparing the analytic solution with the experimental results.

- Providing experimental results for cognitive sensing of 5G gNBs by enabling a ground vehicle to cognitively sense (detect and track) an unknown 5G gNB in the environment, estimating the position of the gNB in a blind fashion

- Justification of the generic signal model in by: (i) analyzing the behavior of autocorrelation function in the time and Frequency domain to prove that the Fourier transform preserves the correlation properties, and (ii) performing extensive cellular and LEO satellite-based experiments to estimate the channel impulse response.

- One of the challenges of navigation with LEO satellites is poorly known satellite ephemeris. The satellites' ephemerides can be predicted from two-line element (TLE)

files and an SGP4 propagator. However, the satellite' ephemerides obtained with the TLE files may end up with errors on the order of several kilometers. Differential positioning methods assess measurement errors for each satellite using a stationary surveyed reference antenna and broadcasts error corrections to many users [157]. Satellite errors removed by differential methods include clock calibration, ephemeris errors, ionospheric delays, and tropospheric delays [175]. Theoretical and practical considerations of differential navigation methods have been studied in the navigation literature. In particular, studies focusing on LEO-based differential frameworks include: (i) joint GPS-LEO navigation [170], (ii) integrity monitoring of precise point positioning—realtime kinematic (PPP–RTK) positioning [215], (iii) LEO SVs flying in formation [201], (iv) ionospheric sensing [120], and (v) differential carrier phase [103].

Demonstrating the performance of the proposed receiver by a base with a known position and a stationary rover with an unknown position equipped with the proposed receiver is one of the objectives of this proposal. A short and long baseline will be considered to evaluate the positioning performance. It will be shown that despite the fact that the satellites' ephemerides were poorly known, the proposed framework is capable of estimating the rover's two-dimensional (2D) position with a meter level in the short and the long baseline scenarios.

- Presenting experimental results with other LEO SV satellite signals such as Orbcomm LEO satellites.

- Demonstrating the capability of the proposed framework in detecting new types of beacons. It will be fictitiously assumed that the Starlink satellites *multiplex* the 5G

NR beacons as a new component in their downlink signals to evaluate the framework performance.

.1 Derivation of likelihood function (5.10)

For a known $\mathscr{W}_i$, the singular value decomposition (SVD) of the matrix $\mathbf{B}_{i-1}$ can be written as

$$\mathbf{B}_{i-1} = [\mathbf{W}_{i-1}\ \mathbf{U}_{i-1}] \begin{bmatrix} \mathbf{\Sigma}_{i-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{W}'^{\mathsf{H}}_{i-1} \\ \mathbf{U}'^{\mathsf{H}}_{i-1} \end{bmatrix} \tag{1}$$

where $\mathbf{W}_{i-1}$ and $\mathbf{U}_{i-1}$ are $KL \times (i-1)L$ and $KL \times (KL-(i-1)L)$ orthogonal matrices that span the column space of $\mathbf{B}_{i-1}$ and orthogonal column space of $\mathbf{B}_{i-1}$, respectively. In other words, $\mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{B}_{i-1} = \mathbf{0}$. Therefore,

$$\mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{y} = \mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{H}_i\mathbf{s}_i + \mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{w}_{\mathrm{eq_i}}. \tag{2}$$

As it was mentioned previously, the complex envelope of the OFDM signals can be considered to be asymptotically white and Gaussian [153]. Here, the GLR test is derived assuming that $\mathbf{w}_{\mathrm{eq}_i} \sim \mathscr{N}(\mathbf{0}, \sigma_w^2\mathbf{I})$. It should be noted that since $\mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{U}_{i-1} = \mathbf{I}$, the statistical characteristics of noise is preserved, i.e., $\mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{w}_{\mathrm{eq_i}} \sim \mathscr{N}(\mathbf{0}, \sigma_w^2\mathbf{I})$. By multiplying the observation vector by $\mathbf{U}^{\mathsf{H}}_{i-1}$, (19) can be written as

$$\begin{cases} \mathscr{H}_0^i: & \mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{y} = \mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{w}_{\mathrm{eq_i}}, \\ \mathscr{H}_1^i: & \mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{y} = \mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{H}_i\mathbf{s}_i + \mathbf{U}^{\mathsf{H}}_{i-1}\mathbf{w}_{\mathrm{eq_i}}. \end{cases} \tag{3}$$

For the linear detection problem (3), the GLR can is derived as [90, Section 9.4.3]

$$\mathscr{L}_i(\mathbf{y}|\mathscr{W}_i) = \frac{\mathbf{y}^{\mathsf{H}}\mathbf{P}_{\mathbf{S_i}}\mathbf{y}}{\mathbf{y}^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B_{i-1}}}\mathbf{P}^{\perp}_{\mathbf{S_i}}\mathbf{P}^{\perp}_{\mathbf{B_{i-1}}}\mathbf{y}}, \tag{4}$$

where $\mathbf{P}_{\mathbf{S_i}} \triangleq \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{H}_i$ and

$$\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} \triangleq \mathbf{U}_{i-1}\mathbf{U}^{\mathsf{H}}_{i-1} = \mathbf{I} - \mathbf{B}_{i-1}\left(\mathbf{B}^{\mathsf{H}}_{i-1}\mathbf{B}_{i-1}\right)^{-1}\mathbf{B}^{\mathsf{H}}_{i-1}. \tag{5}$$

.2 Proof of Lemma 1 in Chapter 1

The matrices $\mathbf{H}_i$ and $\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}$ can be written as

$$\mathbf{H}_i = \mathbf{h}_i \otimes \mathbf{I}_L, \quad \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} = \bar{\mathbf{P}}^{\perp}_{i-1} \otimes \mathbf{I}_L, \tag{6}$$

where, $\mathbf{h}_i \triangleq [1, \exp(j\omega_i L), \ldots, \exp(j\omega_i (K-1)L)]^{\mathsf{T}}$, $\bar{\mathbf{P}}^{\perp}_{i-1} \triangleq \left(\mathbf{I} - \mathbf{b}_{i-1}\left(\mathbf{b}^{\mathsf{H}}_{i-1}\mathbf{b}_{i-1}\right)\mathbf{b}^{\mathsf{H}}_{i-1}\right)$, $\mathbf{b}_{i-1} \triangleq [\mathbf{h}_1, \ldots, \mathbf{h}_{i-1}]$, and $\otimes$ denotes the Kronecker product. Hence, one can write

$$\mathbf{H}^{\mathsf{H}}_i \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} \mathbf{H}_i = \left(\mathbf{h}^{\mathsf{H}}_i \bar{\mathbf{P}}^{\perp}_{i-1} \mathbf{h}_i\right) \otimes \mathbf{I}_L. \tag{7}$$

The scalar $\mathbf{h}^{\mathsf{H}}_i \bar{\mathbf{P}}^{\perp}_{i-1} \mathbf{h}_i$ can be written as

$$\begin{aligned} \mathbf{h}^{\mathsf{H}}_i \bar{\mathbf{P}}^{\perp}_{i-1} \mathbf{h}_i = c_{ii} - \left[c_{i1}, \ldots, c_{i(i-1)}\right] \\ \cdot \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1(i-1)} \\ c_{21} & c_{22} & \ldots & c_{2i} \\ \vdots & \ddots & \ddots & \vdots \\ c_{i1} & c_{i2} & \ldots & c_{(i-1)(i-1)} \end{bmatrix}^{-1} \begin{bmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{(i-1)i} \end{bmatrix}, \end{aligned} \tag{8}$$

which is the Schur complement of $\mathbf{C}_{i-1}$ of matrix $\mathbf{C}_i$ in (31), with $c_{ij} \triangleq \sum_{k=0}^{K-1} \exp\left(j(\omega_j - \omega_i)Lk\right)$.

.3 Proof of Theorem 1 in Chapter 1

Proof: To prove that the likelihood ensures the CFAR property, the asymptotic distributions of the numerator and the denominator of the likelihood in (5.10) are determined under the null hypothesis. It is then shown that as $K \to \infty$, the asymptotic distribution of the likelihood is not a function of unknown parameters if the Doppler frequencies and their estimates satisfy the conditions described in Theorem 1.

According to (4.14), under the null hypothesis of the second stage, i.e., $\mathscr{H}_0^2$, the received signal vector can be written as $\mathbf{y} = \mathbf{B}_1\boldsymbol{\theta}_1 + \mathbf{w}_{\text{eq}_2}$, where in a scenario with two sources with Doppler frequencies ω_1 and ω_2 one has $\mathbf{B}_1 = \mathbf{H}_1$ and $\boldsymbol{\theta}_1 = \mathbf{s}_1$. Hence, replacing $\mathbf{y} = \mathbf{B}_1\boldsymbol{\theta}_1 + \mathbf{w}_{\text{eq}_2}$ in the numerator of the likelihood (5.10) results in

$$\begin{aligned} N(\mathbf{y}) = \mathbf{s}_1^{\mathsf{H}}\mathbf{H}_1^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{S}_2}\mathbf{H}_1\mathbf{s}_1 + \mathbf{w}_{\text{eq}_2}^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{S}_2}\mathbf{w}_{\text{eq}_2} \\ + 2\Re\left\{\mathbf{s}_1^{\mathsf{H}}\mathbf{H}_1^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{S}_2}\mathbf{w}_{\text{eq}_2}\right\}, \end{aligned} \tag{9}$$

where $\hat{\mathbf{P}}_{\mathbf{S}_2} \triangleq \hat{\mathbf{P}}^{\perp}_{\mathbf{H}_1}\hat{\mathbf{H}}_2\left(\hat{\mathbf{H}}_2^{\mathsf{H}}\hat{\mathbf{P}}^{\perp}_{\mathbf{H}_1}\hat{\mathbf{H}}_2\right)^{-1}\hat{\mathbf{H}}_2^{\mathsf{H}}\hat{\mathbf{P}}^{\perp}_{\mathbf{H}_1}$, and $\Re\{\cdot\}$ denotes the real part. Since, for all values of $i \neq j$, one has $\mathbf{H}_i^{\mathsf{H}}\mathbf{H}_i = K\mathbf{I}_L$, and $\mathbf{H}_i^{\mathsf{H}}\mathbf{H}_j = \exp\left(j(\omega_j-\omega_i)(K-1)L/2\right)\frac{\sin\left(\frac{(\omega_j-\omega_i)KL}{2}\right)}{\sin\left(\frac{(\omega_j-\omega_i)L}{2}\right)}\mathbf{I}_L$, it can be shown that

$$\begin{aligned} \mathbf{s}_1^{\mathsf{H}}\mathbf{H}_1^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{S}_2}\mathbf{H}_1\mathbf{s}_1 = \left|\mathscr{S}(\omega_1,\hat{\omega}_2) - \frac{\mathscr{S}(\omega_1,\hat{\omega}_1)\mathscr{S}(\hat{\omega}_1,\hat{\omega}_2)}{K}\right|^2 \\ \times \frac{K}{K^2 - |\mathscr{S}(\hat{\omega}_1,\hat{\omega}_2)|^2}\mathbf{s}_1^{\mathsf{H}}\mathbf{s}_1, \end{aligned} \tag{10}$$

where $\mathscr{S}(\omega_1,\omega_2) \triangleq \frac{\sin\left(\frac{(\omega_1-\omega_2)KL}{2}\right)}{\sin\left(\frac{(\omega_1-\omega_2)L}{2}\right)}$. If the Doppler estimation error of ω_1, defined as $\Delta\omega_1 \triangleq \omega_1 - \hat{\omega}_1$, satisfies $|\Delta\omega_1 L| \ll \frac{1}{K}$, and the difference between the estimate of the Doppler frequencies of the 2nd gNB and the 1st gNB satisfies $|\hat{\omega}_2 L - \hat{\omega}_1 L| > \frac{1}{K}$; then, the following

limit holds

$$\lim_{K\to\infty}\left|\mathscr{S}(\omega_1,\hat{\omega}_2)-\frac{\mathscr{S}(\omega_1,\hat{\omega}_1)\mathscr{S}(\hat{\omega}_1,\hat{\omega}_2)}{K}\right|^2 \times\frac{K}{K^2-|\mathscr{S}(\hat{\omega}_1,\hat{\omega}_2)|^2}\mathbf{s}_1^{\mathsf{H}}\mathbf{s}_1=0. \tag{11}$$

The last term on the right hand side of (9) is a random variable with mean $\mathbb{E}\left\{\mathbf{s}_1^{\mathsf{H}}\mathbf{H}_1^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{S}_2}\mathbf{w}_{\mathrm{eq}_2}\right\}=0$ and variance $\sigma^2\mathbf{s}_1^{\mathsf{H}}\mathbf{H}_1^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{S}_2}\mathbf{H}_1\mathbf{s}_1$, which according to (11), asymptotically tends to zero as $K\to\infty$. Therefore,

$$\lim_{K\to\infty}N(\mathbf{y})=\mathbf{w}_{\mathrm{eq}_2}^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{S}_2}\mathbf{w}_{\mathrm{eq}_2}, \tag{12}$$

.4 GLR Detector for (3.4)

It should be pointed out that the derivation of the GLR detector for (3.4) is similar to that of the matched subspace detector in [180] and the general linear model in [90]. The main difference here is the structure of the subspace matrix $\mathbf{H}$ which simplifies the detector. The integer constraint should also be considered for the derivation of the detector. For the completeness of the dissertation, this appendix presents the derivation of the GLR detector for (3.4). To this end, the ML estimates of the unknown parameters, i.e., α, σ^2, Δf, and $\mathbf{s}$, are substituted in the pdfs of the observation vector $\mathbf{z}$ under each hypothesis. Under $\mathscr{H}_1$, the pdf of the observation vector $\mathbf{z}$ is $f(\mathbf{y}|\mathscr{H}_1) = \frac{1}{\left(\pi\sigma^2\right)^{KL}} \exp\left(-\frac{1}{\sigma^2}\|\mathbf{y}-\alpha\mathbf{H}\mathbf{s}\|^2\right)$. Under $\mathscr{H}_0$, the pdf of the observation vector $\mathbf{z}$ is $f(\mathbf{z}|\mathscr{H}_0) = \frac{1}{\left(\pi\sigma^2\right)^{KL}} \exp\left(-\frac{1}{\sigma^2}\|\mathbf{y}\|^2\right)$. By maximizing the above pdfs over α and σ^2, the ML estimates of these variable are obtained as $\hat{\alpha} = \frac{1}{KL}\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}$, $\widehat{\sigma}^2_{\mathscr{H}_1} = \frac{1}{KL}\|\mathbf{y}-\hat{\alpha}\mathbf{H}\mathbf{s}\|^2$, and $\widehat{\sigma}^2_{\mathscr{H}_0} = \frac{1}{KL}\|\mathbf{y}\|^2$. The estimation of the noise variance under $\mathscr{H}_1$ can be expanded as

$$\begin{aligned}\widehat{\sigma}^2_{\mathscr{H}_1} = &\frac{1}{KL}\|\mathbf{y}\|^2 - \frac{2}{(KL)^2}|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2 \\ &+ \frac{1}{(KL)^3}|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{H}\mathbf{s}. \end{aligned} \tag{13}$$

The elements of the vector $\mathbf{s}$ are drawn from MPSK modulation. Therefore, $\mathbf{s}^{\mathsf{H}}\mathbf{s} = L$ and since $\mathbf{H}^{\mathsf{H}}\mathbf{H} = K$, one can obtain $\widehat{\sigma}^2_{\mathscr{H}_1} = \frac{1}{KL}\|\mathbf{y}\|^2 - \frac{1}{(KL)^2}|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2$. Consequently, the likelihood ratio is

$$\frac{f(\mathbf{y}|\mathscr{H}_1)}{f(\mathbf{y}|\mathscr{H}_0)} = \frac{\frac{1}{KL}\|\mathbf{y}\|^2}{\frac{1}{KL}\|\mathbf{y}\|^2 - \frac{1}{(KL)^2}|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2}.$$

It can be seen that the likelihood ratio is a monotonically increasing function of $\frac{|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2}{K^2\|\mathbf{y}\|^2}$. Therefore, by maximizing the likelihood over the integer vector $\mathbf{q}$ and the unknown Doppler Δf,the GLR test for the constrained problem (3.4) is obtained by (3.5).

.5 Proof of Lemma 3.4.1

In order to calculate the number of search candidates, first the coherent detector of $\mathbf{q}$ for a given phase complex amplitude α is considered. Note that the coherent detector does not depend on the magnitude of α, but only depends on its phase ϕ. More precisely, for a given value of ϕ, one has $\left\{\hat{\mathbf{q}}_\phi, \hat{\Delta f}\right\} = \underset{\mathbf{q},\Delta f}{\operatorname{argmax}} \Re\left\{\exp(-j\phi)\mathbf{z}^{\mathsf{H}}\exp\left(\frac{j2\pi}{M}\mathbf{q}\right)\right\}$ [126]. Due to the nature of i.i.d noise and the independence of the elements of $\mathbf{q}$, the coherent detector simplifies to a SBS MPSK detector for a given Δf and ϕ. Hence, the lth element of $\hat{\mathbf{q}}_\phi$, denoted by $\hat{q}_{\phi_l}$, is obtained by mapping the phase of $\exp(j\phi)z_l$, where z_l is the lth element of $\mathbf{z}$, to the closest multiple of $\frac{2\pi}{M}$, i.e.

$$\hat{q}_{\phi_l} = \text{round}\left[(\phi_l + \phi)\frac{M}{2\pi}\right] \bmod M, \tag{14}$$

where mod is the modulus operator and $\phi_l \triangleq \angle z_l$. Thus, for a given Δf, one can find the optimal $\mathbf{q}$ by searching over all possible values for ϕ. However, it can be readily shown from (14), that $\hat{\mathbf{q}}_\phi$ and $\hat{\mathbf{q}}_{\phi+\frac{2\pi}{M}}$ result in the same likelihood function in (6.45). Consequently, the search space for ϕ is limited to the interval $[0, \frac{2\pi}{M})$.

Since ϕ is limited to the interval $[0, \frac{2\pi}{M})$, the lth detected MPSK symbol $\hat{q}_{\phi_l}$ can take on two values, based on which symbol in the MPSK constellation is closest to it. Define $\mathbf{c}_1 \triangleq \hat{\mathbf{q}}_{\phi=0}$ and $\mathbf{c}_2 \triangleq \hat{\mathbf{q}}_{\phi=\frac{2\pi}{M}}$, where it can be shown through (14) that $c_{2_l} = (c_{1_l} + 1) \bmod M$, where c_{1_l} and c_{2_l} are the lth elements of $\mathbf{c}_1$ and $\mathbf{c}_2$, respectively. It can also be shown using (14) that the boundary angle between two symbols in the MPSK constellation is given by $\gamma_l \triangleq \frac{2\pi}{M}c_{1_l} + \frac{\pi}{M} - \phi_l$ [196]. Subsequently, each candidate MPSK symbol will be given by

$$\hat{q}_{\phi_l} = \begin{cases} c_{1_l} & \phi \leq \gamma_l, \\ c_{2_l} & \phi > \gamma_l. \end{cases} \tag{15}$$

For convenience of notation, define $\left\{\left(c'_{1_l}, \gamma'_l\right)\right\}_{l=0}^{L-1}$ as the set of the sorted values of $\left(c_{1_l}, \gamma_l\right)$ in an ascending order of γ_l such that $\gamma'_{l+1} \geq \gamma'_l$. Consequently, each candidate $\hat{\mathbf{q}}_\phi$ is of the form

$$\left[c'_{1_1} + 1 - u(\gamma'_1 - \phi), \ldots, c'_{1_L} + 1 - u(\gamma'_L - \phi)\right]^{\mathsf{T}}, \tag{16}$$

where $u(\cdot)$ is the unit step function. Equation (16) implies that for different values of ϕ, L different candidates $\mathscr{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_L\}$ are available. Each candidate should be plugged in (6.45) to get the optimal $\hat{\mathbf{q}}$. Finally, by searching over Doppler, one can get the total number of DL search candidates.

.6 Proof of Lemma 1

The autocorrelation of a time segment of length L' of the observation samples $r[n]$ is equal to

$$R_{rr}[m] = \frac{|\alpha_i|^2 \exp\left(j2\pi(f_{D_{i_0}} mT_s + \frac{\beta_i}{2} 2m^2 T_s^2)\right)}{L'} \times \sum_{k=0}^{L'-1} c_i[m+k-t_{s_i}[n]] c_i^{\star}[k-t_{s_i}[n]] \times \exp\left(j2\pi\beta_i mkT_s^2\right) + \frac{1}{L'} \sum_{k=0}^{L'-1} w_{\mathrm{eq_i}}[m+k] w_{\mathrm{eq_i}}^{\star}[k]. \quad (17)$$

By modeling the OFDM-based RSs as a wide sense cyclostationary (WSCS) random process and assuming a large enough L', the following equality holds [24]

$$R_{rr}[m] = \bar{\alpha}_i^2 \frac{1}{L'} \times \bar{\mathscr{A}_{c_i}}(m,0) \sum_{k=0}^{L'-1} \exp\left(j2\pi\beta_i mkT_s^2\right) + R_{ww}[m]. \quad (18)$$

where $\bar{\alpha}_i \triangleq |\alpha_i|^2 \exp\left(j2\pi(f_{D_{i_0}} mT_s + \frac{\beta_i}{2} 2m^2 T_s^2)\right)$, $\bar{\mathscr{A}_{c_i}}(m,0) \triangleq \mathrm{E}\{c_i[m+k]c_i^{\star}[k]\}$, and $\mathrm{E}\{X\}$ denotes the expected value of the random variable X. Solving the geometric sequence on the right hand of (18) proves Lemma 1.

.7 Derivation of likelihood function

The binary hypothesis test in (4.13) can be written as

$$\begin{cases} \mathscr{H}_0^i: & \mathbf{A}\boldsymbol{\theta}_i = \mathbf{0} \\ \mathscr{H}_1^i: & \mathbf{A}\boldsymbol{\theta}_i \neq \mathbf{0}. \end{cases} \tag{19}$$

Where, $\mathbf{A} = [\mathbf{I}_L, \mathbf{0}, \ldots, \mathbf{0}]$ is an $L \times iL$ matrix. Given $\mathscr{W}_i$, for the general linear detection model (19), the GLR is derived as [90, Section 9.4.3]

$$\mathscr{L}(\mathbf{y}) = \frac{\left(\mathbf{A}\hat{\boldsymbol{\theta}}\right)^{\mathsf{H}} \left(\mathbf{A}\left(\mathbf{B}_i^{\mathsf{H}}\mathbf{B}_i\right)^{-1}\mathbf{A}^{\mathsf{H}}\right)^{-1} \left(\mathbf{A}\hat{\boldsymbol{\theta}}\right)}{\mathbf{y}\left(\mathbf{I}_L - \mathbf{B}_i\left(\mathbf{B}_i^{\mathsf{H}}\mathbf{B}_i\right)^{-1}\mathbf{B}_i^{H}\right)}, \tag{20}$$

Since, $\mathbf{y} = \mathbf{H}_i\mathbf{s}_i + \mathbf{B}_{i-1}\boldsymbol{\theta}_{i-1} + \mathbf{w}_{\mathrm{eq}_i}$, the least squares estimation of $\mathbf{s}_i$ is denoted by

$$\hat{\mathbf{s}}_i = \mathbf{J}_i^{-1}\mathbf{H}_i^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{y}. \tag{21}$$

where $\mathbf{J}_i = \left(\mathbf{H}_i^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{H}_i\right)$. Also, $\mathbf{P}_{\mathbf{X}} \triangleq \mathbf{X}(\mathbf{X}^{\mathsf{H}}\mathbf{X})^{-1}\mathbf{X}^{\mathsf{H}}$, denotes the projection matrix to the column space of $\mathbf{X}$, and

$$\mathbf{P}^{\perp}_{\mathbf{X}} \triangleq \mathbf{I}_L - \mathbf{X}\left(\mathbf{X}^{\mathsf{H}}\mathbf{X}\right)\mathbf{X}^{\mathsf{H}}, \tag{22}$$

denotes the projection matrix onto the space orthogonal to the column space of $\mathbf{X}$.

Using the matrix inversion lemma, one can show that

$$\left(\mathbf{B}_i^{\mathsf{H}}\mathbf{B}_i\right)^{-1} = \begin{bmatrix} \mathbf{Q}_1 & \mathbf{Q}_2 \\ \mathbf{Q}_3 & \mathbf{Q}_4 \end{bmatrix}, \tag{23}$$

$$\mathbf{Q}_1 = \mathbf{J}_i^{-1},$$

$$\mathbf{Q}_2 = \left(\mathbf{H}_i^{\dagger}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} - \mathbf{J}_i^{-1}\mathbf{H}_i^{\mathsf{T}}\right)(\mathbf{B}_{i-1}^{\dagger})^{\mathsf{H}},$$

$$\mathbf{Q}_3 = \mathbf{Q}_2^{\mathsf{H}},$$

$$\mathbf{Q}_4 = \mathbf{B}_{i-1}^{\dagger}\left(\mathbf{I}_L + \mathbf{H}_i\mathbf{J}_i^{-1}\mathbf{H}_i^{\mathsf{H}}\right)\left(\mathbf{B}_{i-1}^{\dagger}\right)^{\mathsf{H}},$$

where $\mathbf{H}^{\dagger} \triangleq \left(\mathbf{H}^{\mathsf{H}}\mathbf{H}\right)^{-1}\mathbf{H}^{\mathsf{H}}$.

It should be pointed out that the observation vector can be written as $\mathbf{y} = \mathbf{B}_i\boldsymbol{\theta}_i + \mathbf{w}_{\mathrm{eq_i}}$. Hence, the least squares estimation is obtained as

$$\hat{\boldsymbol{\theta}} = \left(\mathbf{B}_i\mathbf{B}_i\right)^{-1}\mathbf{B}_i^{\mathsf{H}}\mathbf{y}. \tag{24}$$

In the numerator of (20), one has

$$\begin{aligned}\mathbf{A}_i\hat{\boldsymbol{\theta}}_i &= \mathbf{A}_i\begin{bmatrix}\mathbf{Q}_1 & \mathbf{Q}_2\\ \mathbf{Q}_3 & \mathbf{Q}_4\end{bmatrix}\mathbf{B}_i^{\mathsf{H}}\mathbf{y}\\ &= \left(\mathbf{Q}_1\mathbf{H}_i^{\mathsf{H}} + \mathbf{Q}_2\mathbf{B}_{i-1}\right)\mathbf{y}\\ &= \mathbf{J}_{i-1}^{-1}\mathbf{H}_i^{\mathsf{H}}\left(\mathbf{I}_L - \mathbf{P}_{\mathbf{B}_{i-1}}\right)\mathbf{y}.\end{aligned}$$

Therefore, using (21), one has

$$\mathbf{A}_i\hat{\boldsymbol{\theta}}_i = \hat{\mathbf{s}}_i. \tag{25}$$

Moreover, using (23), one has

$$\mathbf{B}_i\left(\mathbf{B}_i^{\mathsf{H}}\mathbf{B}_i\right)^{-1}\mathbf{B}_i^{\mathsf{H}} = \mathbf{I}_L - \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} + \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{H}_i\mathbf{J}_i^{-1}\mathbf{H}_i^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}. \tag{26}$$

Replacing (25) and (26) in (20) yields

$$\mathscr{L}_i(\mathbf{y}|\mathscr{W}_i) = \frac{\mathbf{y}^{\mathsf{H}}\mathbf{P}_{\mathbf{S_i}}\mathbf{y}}{\mathbf{y}^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B_{i-1}}}\mathbf{P}^{\perp}_{\mathbf{S_i}}\mathbf{P}^{\perp}_{\mathbf{B_{i-1}}}\mathbf{y}}. \tag{27}$$

The matrices $\mathbf{H}_i$ and $\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}$ can be written as

$$\mathbf{H}_i = \mathbf{h}_i \otimes \mathbf{I}_L, \quad \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} = \bar{\mathbf{P}}^{\perp}_{i-1} \otimes \mathbf{I}_L, \tag{28}$$

where, $\mathbf{h}_i \triangleq [1, \exp(j\omega_i L), \ldots, \exp(j\omega_i(K-1)L)]^{\mathsf{T}}$, $\bar{\mathbf{P}}^{\perp}_{i-1} \triangleq \left(\mathbf{I}_L - \mathbf{B}_{i-1}\left(\mathbf{B}_{i-1}^{\mathsf{H}}\mathbf{B}_{i-1}\right)\mathbf{B}_{i-1}^{\mathsf{H}}\right)$, $\mathbf{B}_{i-1} \triangleq [\mathbf{h}_1, \ldots, \mathbf{h}_{i-1}]$, and $\otimes$ denotes the Kronecker product. Hence, one can write

$$\mathbf{H}_i^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{H}_i = \left(\mathbf{h}_i^{\mathsf{H}}\bar{\mathbf{P}}^{\perp}_{i-1}\mathbf{h}_i\right) \otimes \mathbf{I}_L. \tag{29}$$

The scalar $\mathbf{h}_i^{\mathsf{H}}\bar{\mathbf{P}}_{i-1}^{\perp}\mathbf{h}_i$ can be written as

$$\mathbf{h}_i^{\mathsf{H}}\bar{\mathbf{P}}_{i-1}^{\perp}\mathbf{h}_i = c_{ii} - \left[c_{i1},\ldots,c_{i(i-1)}\right] \cdot \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1(i-1)} \\ c_{21} & c_{22} & \ldots & c_{2i} \\ \vdots & \ddots & \ddots & \vdots \\ c_{i1} & c_{i2} & \ldots & c_{(i-1)(i-1)} \end{bmatrix}^{-1} \begin{bmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{(i-1)i} \end{bmatrix}, \tag{30}$$

which is the Schur complement of $\mathbf{C}_{i-1}$ of matrix $\mathbf{C}_i$ where

$$\mathbf{C}_i = \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1i} \\ c_{21} & c_{22} & \ldots & c_{2i} \\ \vdots & \ddots & \ddots & \vdots \\ c_{i1} & c_{i2} & \ldots & c_{ii} \end{bmatrix}, \tag{31}$$

with $c_{ij} \triangleq \sum_{k=0}^{K-1} \exp\left(j(\omega_j - \omega_i)Lk\right)$. Hence, the following equality holds

$$\mathbf{H}_i^{\mathsf{H}}\mathbf{P}_{\mathbf{B}_{i-1}}^{\perp}\mathbf{H}_i = \lambda_i \mathbf{I}_L, \tag{32}$$

where the scalar λ_i is the Schur complement of block $\mathbf{C}_{i-1}$. Consequently, the likelihood (5.10) at the ith stage can be simplified as

$$\frac{\|\lambda_i^{-1}\hat{\mathbf{H}}_i^{\mathsf{H}}\mathbf{P}_{\mathbf{B}_{i-1}}^{\perp}\mathbf{y}\|^2}{\|\mathbf{P}_{\mathbf{B}_{i-1}}^{\perp}\mathbf{y}\|^2 - \|\lambda_i^{-1}\hat{\mathbf{H}}_i^{\mathsf{H}}\mathbf{P}_{\hat{\mathbf{B}}_{i-1}}^{\perp}\mathbf{y}\|^2} \underset{\mathscr{H}_0^i}{\overset{\mathscr{H}_1^i}{\gtrless}} \eta_i. \tag{33}$$

where η_i is a predetermined threshold at the ith stage.

Bibliography

[1] 3GPP. Study on NR positioning support. TR 38.855, 3rd Generation Partnership Project (3GPP), March 2019.

[2] 3GPP2. Recommended minimum performance standards for cdma2000 spread spectrum base stations. December 1999.

[3] A. Abdallah and Z. Kassas. Deep learning-aided spatial discrimination for multipath mitigation. In *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, pages 1324–1335, April 2020.

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

[5] A. Abdallah and Z. Kassas. UAV navigation with 5G carrier phase measurements. In *Proceedings of ION GNSS Conference*, pages 3294–3306, September 2021.

[6] A. Abdallah and Z. Kassas. Opportunistic navigation using sub-6 GHz 5G downlink signals: A case study on a ground vehicle. In *Proceedings of European Conference on Antennas and Propagation*, pages 1–5, 2022.

[7] A. Abdallah, J. Khalife, and Z. Kassas. Experimental characterization of received 5G signals carrier-to-noise ratio in indoor and urban environments. In *Proceedings of IEEE Vehicular Technology Conference*, pages 1–5, April 2021.

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

[9] A. Abdallah, K. Shamaei, and Z. Kassas. Assessing real 5G signals for opportunistic navigation. In *Proceedings of ION GNSS Conference*, pages 2548–2559, 2020.

[10] 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*, pages 1–6, December 2018.

[11] 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*, 17(8):4939–4954, August 2018.

[12] 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*, pages 1–6, April 2018.

[13] G. Afifi and Y. Gadallah. Autonomous 3-D UAV localization using cellular networks: Deep supervised learning versus reinforcement learning approaches. *IEEE Access*, 9:155234–155248, 2021.

[14] M. Agiwal, A. Roy, and N. Saxena. Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys Tutorials*, 18(3):1617–1655, February 2016.

[15] C. Ardito, J. Morales, J. Khalife, A. Abdallah, and Z. Kassas. Performance evaluation of navigation using LEO satellite signals with periodically transmitted satellite positions. In *Proceedings of ION International Technical Meeting Conference*, pages 306–318, 2019.

[16] I. Atitallah, A. Kammoun, M. Alouini, and T. Al-Naffouri. Optimal design of large dimensional adaptive subspace detectors. *IEEE Transactions on Signal Processing*, 64(19):4922–4935, 2016.

[17] K. Avval. Cellular-based localization for mobile devices with structured motion. Master's thesis, University of Toronto, Canada, 2020.

[18] M.-S. Baek, S. Kwak, J.-Y. Jung, H. Kim, and D.-J. Choi. Implementation methodologies of deep learning-based signal detection for conventional MIMO transmitters. *IEEE Transactions on Broadcasting*, 65(3):636–642, 2019.

[19] J. Baenke, K. Chaudhuri, A. Deshpande, A. Halder, M. Irizarry, N. Saxena, S. Sharma, and R. Yang. Millimeter-Wave downlink coverage extension strategies. *IEEE Communications Magazine*, 58(9):74–78, 2020.

[20] Y. Bar-Shalom, X. Li, and T. Kirubarajan. *Estimation with Applications to Tracking and Navigation*. John Wiley & Sons, New York, NY, 2002.

[21] J. Barnes, A. Chi, R. Andrew, L. Cutler, D. Healey, D. Leeson, T. McGunigal, J. Mullen, W. Smith, R. Sydnor, R. Vessot, and G. Winkler. Characterization of frequency stability. *IEEE Transactions on Instrumentation and Measurement*, 20(2):105–120, May 1971.

[22] J. Benedetto, I. Konstantinidis, and M. Rangaswamy. Phase-coded waveforms and their design. *IEEE Signal Processing Magazine*, 26(1):22–31, 2009.

[23] F. Boccardi, R. Heath, A. Lozano, T. Marzetta, and P. Popovski. Five disruptive technology directions for 5G. *IEEE Communications Magazine*, 52(2):74–80, February 2014.

[24] H. Bolcskei. Blind estimation of symbol timing and carrier frequency offset in wireless OFDM systems. *IEEE Transactions on Communications*, 49(6):988–999, 2001.

[25] M. Braasch and A. Dempster. Tutorial: GPS receiver architectures, front-end and baseband signal processing. *IEEE Aerospace and Electronic Systems Magazine*, 34(2):20–37, 2019.

[26] R. Cassel, D. Scherer, D. Wilburne, J. Hirschauer, and J. Burke. Impact of improved oscillator stability on LEO-based satellite navigation. In *Proceedings of ION International Technical Meeting*, pages 893–905, January 2022.

[27] H. Chen and H. Wymeersch. Phone signals can help you find your way in cities even without GPS. *Nature*, 611:454–455, November 2022.

[28] L. Chen, O. Julien, P. Thevenon, D. Serant, A. Pena, and H. Kuusniemi. TOA estimation for positioning with DVB-T signals in outdoor static tests. *IEEE Transactions on Broadcasting*, 61(4):625–638, 2015.

[29] X. Chen, Q. Wei, F. Wang, Z. Jun, S. Wu, and A. Men. Super-resolution time of arrival estimation for a symbiotic FM radio data system. *IEEE Transactions on Broadcasting*, 66(4):847–856, December 2020. doi: 10.1109/TBC.2019.2957666.

[30] Y. Chi, J. Park, and S. Park. Hybrid multibeamforming receiver with high-precision beam steering for low Earth orbit satellite communication. *IEEE Transactions on Antennas and Propagation*, 71(7):5695–5707, July 2023.

[31] D. Ciuonzo, A. De Maio, and D. Orlando. On the statistical invariance for adaptive radar detection in partially homogeneous disturbance plus structured interference. *IEEE Transactions on Signal Processing*, 65(5):1222–1234, 2017.

[32] A. Combernoux, F. Pascal, and G. Ginolhac. Performance of the low-rank adaptive normalized matched filter test under a large dimension regime. *IEEE Transactions on Aerospace and Electronic Systems*, 55(1):459–468, 2019.

[33] E. Conte, A. Filippi, and S. Tomasin. ML period estimation with application to vital sign monitoring. *IEEE Signal Processing Letters*, 17(11):905–908, 2010.

[34] J. del Peral-Rosado, R. Estatuet-Castillo, J. Lopez-Salcedo, G. Seco-Granados, Z. Chaloupka, L. Ries, and J. Garcoa-Molina. Evaluation of hybrid positioning scenarios for autonomous vehicle applications. In *Proceedings of ION International Technical Meeting Conference*, pages 2541–2553, January 2017.

[35] J. del Peral-Rosado, J. López-Salcedo, F. Zanier, and G. Seco-Granados. Position accuracy of joint time-delay and channel estimators in LTE networks. *IEEE Access*, 6:25185–25199, 2018.

[36] J. Del Peral-Rosado, P. Nolle, S. Razavi, G. Lindmark, D. Shrestha, F. Gunnarsson, F. Kaltenberger, N. Sirola, O. Särkkä, J. Roström, K. Vaarala, P. Miettinen, G. Pojani, L. Canzian, H. Babaroglu, E. Rastorgueva-Foi, J. Talvitie, and D. Flachs. Design considerations of dedicated and aerial 5G networks for enhanced positioning services. In *Proceedings of Workshop on Satellite Navigation Technology*, pages 1–12, April 2022.

[37] J. del Peral-Rosado, R. Raulefs, J. López-Salcedo, and G. Seco-Granados. Survey of cellular mobile radio localization methods: From 1G to 5G. *IEEE Communications Surveys Tutorials*, 20(2):1124–1148, 2018.

[38] I. Del Portillo, B. Cameron, and E. Crawley. A technical comparison of three low earth orbit satellite constellation systems to provide global broadband. *Acta Astronautica*, 159:123–135, 2019.

[39] O. Dobre, A. Abdi, Y. Bar-Ness, and W. Su. Survey of automatic modulation classification techniques: Classical approaches and new trends. *IET communications*, 1(2):137–156, 2007.

[40] A. Drutsa, G. Gusev, and P. Serdyukov. Periodicity in user engagement with a search engine and its application to online controlled experiments. *ACM Transactions on the Web (TWEB)*, 11(2):1–35, 2017.

[41] H. Dun, C. Tiberius, and G. Janssen. Positioning in a multipath channel using OFDM signals with carrier phase tracking. *IEEE Access*, 8:13011–13028, 2020.

[42] A. Elgamoudi, H. Benzerrouk, G. Elango, and R. Landry. Gauss Hermite H∞ filter for UAV tracking using LEO satellites TDOA/FDOA measurement—part I. *IEEE Access*, 8:201428–201440, 2020.

[43] R. Faragher and R. Harle. Towards an efficient, intelligent, opportunistic smartphone indoor positioning system. *NAVIGATION, Journal of the Institute of Navigation*, 62(1):55–72, 2015.

[44] F. Farhangian and R. Landry. Multi-constellation software-defined receiver for Doppler positioning with LEO satellites. *Sensors*, 20(20):5866–5883, October 2020.

[45] A. Fascista, A. Coluccia, H. Wymeersch, and G. Seco-Granados. Millimeter-wave downlink positioning with a single-antenna receiver. *IEEE Transactions on Wireless Communications*, 18(9):4479–4490, 2019.

[46] G. Fokin and D. Volgushev. Software-defined radio network positioning technology design. problem statement. In *Proceedings of Systems of Signals Generating and Processing in the Field of on Board Communications*, pages 1–6, March 2022.

[47] P. Gadka, J. Sadowski, and J. Stefanski. Detection of the first component of the received LTE signal in the OTDoA method. *Wireless Communications and Mobile Computing*, pages 1–12, April 2019.

[48] J. Gante, L. Sousa, and G. Falcao. Dethroning GPS: Low-power accurate 5G positioning systems using machine learning. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 10(2):240–252, June 2020.

[49] G. Gao. *Towards navigation based on 120 satellites: Analyzing the new signals*. PhD thesis, Stanford University, 2008.

[50] Y. Gao, X. Zhao, S. Wang, Y. Xiang, C. Huang, and Y. Hua. Positioning via GEO communication satellites' signals of opportunity. *IET Radar, Sonar Navigation*, 15(11):1472–1482, July 2021.

[51] F. Gini and A. Farina. Vector subspace detection in compound-Gaussian clutter. part I: survey and new results. *IEEE Transactions on Aerospace and Electronic Systems*, 38(4):1295–1311, 2002.

[52] M. Giordani, M. Polese, A. Roy, D. Castor, and M. Zorzi. A tutorial on beam management for 3GPP NR at mmWave frequencies. *IEEE Communications Surveys Tutorials*, 21(1):173–196, 2019.

[53] S. Gonzalez and M. Brookes. PEFAC - a pitch estimation algorithm robust to high levels of noise. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 22(2):518–530, 2014.

[54] A. Graff, W. Blount, P. Iannucci, J. Andrews, and T. Humphreys. Analysis of OFDM signals for ranging and communications. In *Proceedings of ION GNSS Conference*, pages 2910–2924, 2021.

[55] J. Haidar-Ahmad, N. Khairallah, and Z. Kassas. A hybrid analytical-machine learning approach for LEO satellite orbit prediction. In *Proceedings of International Conference on Information Fusion*, pages 1–7, 2022.

[56] S. Han, T. Kang, and J. Seo. Smartphone application to estimate distances from LTE base stations based on received signal strength measurements. In *International*

Technical Conference on Circuits/Systems, Computers and Communications, pages 1–3, June 2019.

[57] M. Hartnett. Performance assessment of navigation using carrier Doppler measurements from multiple LEO constellations. Master's thesis, Air Force Institute of Technology, Ohio, USA, 2022.

[58] T. Hong, J. Sun, T. Jin, Y. Yi, and J. Qu. Hybrid positioning with DTMB and LTE signals. In *Proceedings of International Wireless Communications and Mobile Computing*, pages 303–307, July 2021. doi: 10.1109/IWCMC51323.2021.9498758.

[59] C. Huang, H. Qin, C. Zhao, and H. Liang. Phase - time method: Accurate Doppler measurement for Iridium NEXT signals. *IEEE Transactions on Aerospace and Electronic Systems*, 58(6):5954–5962, 2022.

[60] Iridium Constellation LLC. Iridium NEXT engineering statement. `http://licensing.fcc.gov/myibfs/download.do?attachment_key=1031348`, 2013.

[61] F. Izedi, M. Karimi, and M. Derakhtian. Joint DOA estimation and source number detection for arrays with arbitrary geometry. *Signal Processing*, 140:149–160, 2017.

[62] W. Hayek J. Saroufim and Z. Kassas. Simultaneous leo satellite tracking and differential leo-aided imu navigation. In *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2023.

[63] N. Jardak and R. Adam. Practical use of Starlink downlink tones for positioning. *Sensors*, 23(6):3234–3253, March 2023.

[64] N. Jardak and Q. Jault. The potential of LEO satellite-based opportunistic navigation for high dynamic applications. *Sensors*, 22(7):2541–2565, 2022.

[65] M. Jiang, H. Qin, C. Zhao, and G. Sun. LEO Doppler-aided GNSS position estimation. *GPS Solutions*, 26(1):1–18, 2022.

[66] Z. Jiao, L. Chen, X. Lu, Z. Liu, X. Zhou, Y. Zhuang, and G. Guo. Carrier phase ranging with DTMB signals for urban pedestrian localization and GNSS aiding. *Remote Sensing*, 15(2):423–446, 2023.

[67] C. Jin, W. Tay, K. Zhao, K. Voon Ling, and K. Sin. A 5G/GNSS integrated positioning method. In *Proceedings of ION GNSS Conference*, pages 2429–2443, September 2022.

[68] T. Kang, H. Lee, and J. Seo. Analysis of the maximum correlation peak value and RSRQ in LTE signals according to frequency bands and sampling frequencies. In *International Conference on Control, Automation and Systems*, pages 1182–1186, October 2019.

[69] T. Kang, H. Lee, and J. Seo. TOA-based ranging method using CRS in LTE signals. *Journal of Advanced Navigation Technology*, 23(5):437–443, October 2019.

[70] G. Karystinos and D. Pados. Rank-2-optimal adaptive design of binary spreading codes. *IEEE Transactions on Information Theory*, 53(9):3075–3080, 2007.

[71] Z. Kassas. Collaborative opportunistic navigation. *IEEE Aerospace and Electronic Systems Magazine*, 28(6):38–41, 2013.

[72] Z. Kassas. Position, navigation, and timing technologies in the 21st century. volume 2, chapter 38: Navigation with Cellular Signals of Opportunity, pages 1171–1223. Wiley-IEEE, 2021.

[73] Z. Kassas. Position, navigation, and timing technologies in the 21st century. volume 2, chapter 43: Navigation from low Earth orbit – Part 2: models, implementation, and performance, pages 1381–1412. Wiley-IEEE, 2021.

[74] Z. Kassas, A. Abdallah, C. Lee, J. Jurado, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, S. Wachtel, and R. Tay. Protecting the skies: GNSS-less accurate aircraft navigation with terrestrial cellular signals of opportunity. In *Proceedings of ION GNSS Conference*, pages 1014–1025, September 2022. doi: 10.33012/2022.18579.

[75] Z. Kassas, A. Abdallah, and M. Orabi. Carpe signum: seize the signal – opportunistic navigation with 5G. *Inside GNSS Magazine*, 16(1):52–57, 2021.

[76] Z. Kassas, V. Ghadiok, and T. Humphreys. Adaptive estimation of signals of opportunity. In *Proceedings of ION GNSS Conference*, pages 1679–1689, September 2014.

[77] Z. Kassas and T. Humphreys. Observability analysis of collaborative opportunistic navigation with pseudorange measurements. *IEEE Transactions on Intelligent Transportation Systems*, 15(1):260–273, February 2014.

[78] Z. Kassas and T. Humphreys. Receding horizon trajectory optimization in opportunistic navigation environments. *IEEE Transactions on Aerospace and Electronic Systems*, 51(2):866–877, April 2015.

[79] Z. Kassas, N. Khairallah, and S. Kozhaya. Ad astra: Simultaneous tracking and navigation with megaconstellation LEO satellites. *IEEE Aerospace and Electronic Systems Magazine*, 2023. accepted.

[80] Z. Kassas, J. Khalife, A. Abdallah, and C. Lee. I am not afraid of the GPS jammer: resilient navigation via signals of opportunity in GPS-denied environments. *IEEE Aerospace and Electronic Systems Magazine*, 37(7):4–19, July 2022.

[81] Z. Kassas, J. Khalife, A. Abdallah, C. Lee, J. Jurado, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, S. Wachtel, and R. Tay. Flight demonstration of high altitude aircraft navigation with cellular signals. *IEEE Intelligent Transportation Systems Magazine*, 15(4):150–165, 2023.

[82] Z. Kassas, J. Khalife, A. Abdallah, C. Lee, J. Jurado, S. Wachtel, J. Duede, Z. Hoeffner, T. Hulsey, R. Quirarte, and R. Tay. Assessment of cellular signals of opportunity for high-altitude aircraft navigation. *IEEE Aerospace and Electronic Systems Magazine*, 37(10):4–19, October 2022.

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

[84] 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*, pages 111–124, September 2017.

[85] Z. Kassas, S. Kozhaya, H. Kanj, J. Saroufim, S. Hayek, M. Neinavaie, N. Khairallah, and J. Khalife. Navigation with multi-constellation LEO satellite signals of opportunity: Starlink, Oneweb, Orbcomm, and Iridium. In *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, pages 338–343, April 2023.

[86] Z. Kassas, M. Maaref, J. Morales, J. Khalife, and K. Shamaei. Robust vehicular localization and map matching in urban environments through IMU, GNSS, and cellular signals. *IEEE Intelligent Transportation Systems Magazine*, 12(3):36–52, June 2020.

[87] Z. Kassas, J. Morales, and J. Khalife. New-age satellite-based navigation – STAN: simultaneous tracking and navigation with LEO satellite signals. *Inside GNSS Magazine*, 14(4):56–65, 2019.

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

[89] Z. Kassas, M. Neinavaie, J. Khalife, N. Khairallah, J. Haidar-Ahmad, S. Kozhaya, and Z. Shadram. Enter LEO on the GNSS stage: Navigation with Starlink satellites. *Inside GNSS Magazine*, 16(6):42–51, 2021.

[90] S. Kay. *Fundamentals of statistical signal processing: Detection Theory*, volume II. Prentice-Hall, Upper Saddle River, NJ, 1993.

[91] S. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*, volume I. Prentice-Hall, Upper Saddle River, NJ, 1993.

[92] T. Kazaz, G. Janssen, J. Romme, and A.-J. Van der Veen. Delay estimation for ranging and localization using multiband channel state information. *IEEE Transactions on Wireless Communications*, 21(4):2591–2607, April 2022.

[93] M. Kerpicci, M. Prvulovic, and A. Zajić. A hierarchical approach for multiple periodicity detection in software code analysis. *IEEE Access*, 10:106936–106945, 2022.

[94] N. Khairallah and Z. Kassas. An interacting multiple model estimator of LEO satellite clocks for improved positioning. In *Proceedings of IEEE Vehicular Technology Conference*, pages 1–5, 2022.

[95] J. Khalife and Z. Kassas. Navigation with cellular CDMA signals – part II: Performance analysis and experimental results. *IEEE Transactions on Signal Processing*, 66(8):2204–2218, April 2018.

[96] J. Khalife and Z. Kassas. Precise UAV navigation with cellular carrier phase measurements. In *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, pages 978–989, April 2018.

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

[98] J. Khalife and Z. Kassas. Opportunistic UAV navigation with carrier phase measurements from asynchronous cellular signals. *IEEE Transactions on Aerospace and Electronic Systems*, 56(4):3285–3301, August 2020. doi: 10.1109/TAES.2019.2948452.

[99] J. Khalife and Z. Kassas. Differential framework for submeter-accurate vehicular navigation with cellular signals. *IEEE Transactions on Intelligent Vehicles*, 2022. accepted, doi: 10.1109/TIV.2022.3187957.

[100] J. Khalife and Z. Kassas. On the achievability of submeter-accurate UAV navigation with cellular signals exploiting loose network synchronization. *IEEE Transactions on Aerospace and Electronic Systems*, 58(5):4261–4278, October 2022.

[101] J. Khalife and Z. Kassas. Performance-driven design of carrier phase differential navigation frameworks with megaconstellation LEO satellites. *IEEE Transactions on Aerospace and Electronic Systems*, 59(3):2947–2966, June 2023.

[102] J. Khalife, M. Neinavaie, and Z. Kassas. Blind Doppler estimation from LEO satellite signals: A case study with real 5G signals. In *Proceedings of ION GNSS Conference*, pages 3046–3054, September 2020.

[103] J. Khalife, M. Neinavaie, and Z. Kassas. Navigation with differential carrier phase measurements from megaconstellation LEO satellites. In *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, pages 1393–1404, April 2020.

[104] J. Khalife, M. Neinavaie, and Z. Kassas. Blind Doppler tracking from OFDM signals transmitted by broadband LEO satellites. In *Proceedings of IEEE Vehicular Technology Conference*, pages 1–6, April 2021.

[105] J. Khalife, M. Neinavaie, and Z. Kassas. The first carrier phase tracking and positioning results with Starlink LEO satellite signals. *IEEE Transactions on Aerospace and Electronic Systems*, 56(2):1487–1491, April 2022.

[106] J. Khalife, K. Shamaei, S. Bhattacharya, and Z. Kassas. Centimeter-accurate UAV navigation with cellular signals. In *Proceedings of ION GNSS Conference*, pages 2321–2331, September 2018.

[107] 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*, 66(8):2191–2203, April 2018.

[108] M. Koivisto, J. Talvitie, E. Rastorgueva-Foi, Y. Lu, and M. Valkama. Channel parameter estimation and TX positioning with multi-beam fusion in 5G mmWave networks. *IEEE Transactions on Wireless Communications*, pages 1–1, 2021.

[109] M. Korso, R. Boyer, A. Renaux, and S. Marcos. Statistical resolution limit for source localization with clutter interference in a MIMO radar context. *IEEE Transactions on Signal Processing*, 60(2):987–992, 2012.

[110] S. Kozhaya, J. Haidar-Ahmad, A. Abdallah, Z. Kassas, and S. Saab. Comparison of neural network architectures for simultaneous tracking and navigation with LEO satellites. In *Proceedings of ION GNSS Conference*, pages 2507–2520, September 2021.

[111] S. Kozhaya, H. Kanj, and Z. Kassas. Multi-constellation blind beacon estimation, Doppler tracking, and opportunistic positioning with OneWeb, Starlink, Iridium NEXT, and Orbcomm LEO satellites. In *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, pages 1184–1195, April 2023.

[112] S. Kozhaya and Z. Kassas. Blind receiver for LEO beacon estimation with application to UAV carrier phase differential navigation. In *Proceedings of ION GNSS Conference*, pages 2385–2397, 2022.

[113] S. Kraut, L. Scharf, and L. McWhorter. Adaptive subspace detectors. *IEEE Transactions on Signal Processing*, 49(1):1–16, 2001.

[114] I. Lapin, G. Granados, J. Samson, O. Renaudin, F. Zanier, and L. Ries. STARE: Real-time software receiver for LTE and 5G NR positioning and signal monitoring. In *Proceedings of Workshop on Satellite Navigation Technology*, pages 1–11, April 2022. doi: 10.1109/NAVITEC53682.2022.9847544.

[115] I. Lapin, G. Seco-Granados, O. Renaudin, F. Zanier, and L. Ries. Joint delay and phase discriminator based on ESPRIT for 5G NR positioning. *IEEE Access*, 9:126550–126563, 2021.

[116] J. Lee, G. Gil, and Y. Lee. Exploiting spatial sparsity for estimating channels of hybrid MIMO systems in millimeter wave communications. In *Proceedings of IEEE GLOBECOM*, pages 3326–3331, December 2014.

[117] W. Lee and I. Akyildiz. Optimal spectrum sensing framework for cognitive radio networks. *IEEE Transactions on Wireless communications*, 7(10):3845–3857, 2008.

[118] M. Leng, F. Quitin, W. Tay, C. Cheng, S. Razul, and C. See. Anchor-aided joint localization and synchronization using SOOP: Theory and experiments. *IEEE Transactions on Wireless Communications*, 15(11):7670–7685, November 2016.

[119] N. Levanon. Quick position determination using 1 or 2 LEO satellites. *IEEE Transactions on Aerospace and Electronic Systems*, 34(3):736–754, July 1998.

[120] T. Li, L. Wang, W. Fu, Y. Han, H. Zhou, and B. Chen. Bottomside ionospheric snapshot modeling using the LEO navigation augmentation signal from the Luojia-1A satellite. *GPS Solutions*, 26(1):1–13, 2022.

[121] Z. Liu, L. Chen, X. Zhou, Z. Jiao, G. Guo, and R. Chen. Machine learning for time-of-arrival estimation with 5G signals in indoor positioning. *IEEE Internet of Things Journal*, 2023. accepted.

[122] J. Lopez-Salcedo, J. Peral-Rosado, and G. Seco-Granados. Survey on robust carrier tracking techniques. *IEEE Communications Surveys Tutorials*, 16(2):670–688, February 2014.

[123] W. Ma, C. Qi, and G. Li. High-resolution channel estimation for frequency-selective mmwave massive MIMO systems. *IEEE Transactions on Wireless Communications*, 19(5):3517–3529, 2020.

[124] M. Maaref and Z. Kassas. Autonomous integrity monitoring for vehicular navigation with cellular signals of opportunity and an IMU. *IEEE Transactions on Intelligent Transportation Systems*, 23(6):5586–5601, June 2022.

[125] M. Maaref, J. Khalife, and Z. Kassas. Lane-level localization and mapping in GNSS-challenged environments by fusing lidar data and cellular pseudoranges. *IEEE Transactions on Intelligent Vehicles*, 4(1):73–89, March 2019.

[126] K. Mackenthun. A fast algorithm for multiple-symbol differential detection of MPSK. *IEEE Transactions on Communications*, 42(234):1471–1474, February 1994.

[127] P. Markopoulos and G. Karystinos. Noncoherent Alamouti phase-shift keying with full-rate encoding and polynomial-complexity maximum-likelihood decoding. *IEEE Transactions on Wireless Communications*, 16(10):6688–6697, 2017.

[128] 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.

[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*, pages 1–6, December 2018.

[130] J. Merwe, S. Bartl, C. O'Driscoll, A. Rügamer, F. Förster, P. Berglez, A. Popugaev, and W. Felber. GNSS sequence extraction and reuse for navigation. In *Proceedings of ION GNSS+ Conference*, pages 2731–2747, 2020.

[131] P. Misra and P. Enge. *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press, second edition, 2010.

[132] J. Morales and Z. Kassas. Optimal collaborative mapping of terrestrial transmitters: receiver placement and performance characterization. *IEEE Transactions on Aerospace and Electronic Systems*, 54(2):992–1007, April 2018.

[133] J. Morales and Z. Kassas. Stochastic observability and uncertainty characterization in simultaneous receiver and transmitter localization. *IEEE Transactions on Aerospace and Electronic Systems*, 55(2):1021–1031, April 2019.

[134] J. Morales and Z. Kassas. Tightly-coupled inertial navigation system with signals of opportunity aiding. *IEEE Transactions on Aerospace and Electronic Systems*, 57(3):1930–1948, 2021.

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

[136] J. Morales, P. Roysdon, and Z. Kassas. Signals of opportunity aided inertial navigation. In *Proceedings of ION GNSS Conference*, pages 1492–1501, September 2016.

[137] H. More, E. Cianca, and M. Sanctis. Positioning performance of LEO mega constellations in deep urban canyon environments. In *Proceedings of International Symposium on Wireless Personal Multimedia Communications*, pages 256–260, 2022.

[138] J. Mortier, G. Pages, and J. Vila-Valls. Robust TOA-based UAS navigation under model mismatch in GNSS-denied harsh environments. *Remote Sensing*, 12(18):2928–2947, September 2020.

[139] T. Mortlock and Z. Kassas. Performance analysis of simultaneous tracking and navigation with LEO satellites. In *Proceedings of ION GNSS Conference*, pages 2416–2429, September 2020.

[140] J. Muyuan, Q. Honglei, C. Zhao, and S. Guiyu. LEO Doppler-aided GNSS position estimation. *GPS Solutions*, 26(1):1–18, 2022.

[141] A. Nardin, F. Dovis, and J. Fraire. Empowering the tracking performance of LEO-based positioning by means of meta-signals. *IEEE Journal of Radio Frequency Identification*, 5(3):244–253, 2021.

[142] M. Neinavaie and Z. Kassas. Unveiling beamforming strategies of Starlink LEO satellites. In *Proceedings of ION GNSS Conference*, pages 2525–2531, 2022.

[143] M. Neinavaie and Z. Kassas. Unveiling Starlink LEO satellite OFDM-like signal structure enabling precise positioning. *IEEE Transactions on Aerospace and Electronic Systems*, 2022. accepted.

[144] M. Neinavaie, J. Khalife, and Z. Kassas. Blind opportunistic navigation: Cognitive deciphering of partially known signals of opportunity. In *Proceedings of ION GNSS Conference*, pages 2748–2757, September 2020.

[145] M. Neinavaie, J. Khalife, and Z. Kassas. Blind Doppler tracking and beacon detection for opportunistic navigation with LEO satellite signals. In *Proceedings of IEEE Aerospace Conference*, pages 1–8, 2021.

[146] M. Neinavaie, J. Khalife, and Z. Kassas. Doppler stretch estimation with application to tracking Globalstar satellite signals. In *Proceedings of IEEE Military Communications Conference*, pages 647–651, November 2021.

[147] M. Neinavaie, J. Khalife, and Z. Kassas. Acquisition, Doppler tracking, and positioning with Starlink LEO satellites: First results. *IEEE Transactions on Aerospace and Electronic Systems*, 58(3):2606–2610, June 2022.

[148] M. Neinavaie, J. Khalife, and Z. Kassas. Cognitive detection of unknown beacons of terrestrial signals of opportunity for localization. *IEEE Transactions on Wireless Communications*, 2022. accepted.

[149] M. Neinavaie, J. Khalife, and Z. Kassas. Cognitive opportunistic navigation in private networks with 5G signals and beyond. *IEEE Journal of Selected Topics in Signal Processing*, 16(1):129–143, 2022.

[150] M. Neinavaie, J. Khalife, and Z. Kassas. Detection of constrained unknown beacon signals of terrestrial transmitters and LEO satellites with application to navigation. In *Proceedings of IEEE Vehicular Technology Conference*, pages 1–5, September 2022.

[151] M. Neinavaie, Z. Shadram, S. Kozhaya, and Zaher M. Kassas. First results of differential Doppler positioning with unknown Starlink satellite signals. In *Proceedings of IEEE Aerospace Conference*, pages 1–14, March 2022.

[152] North American Aerospace Defense Command (NORAD). Two-line element sets. `http://celestrak.com/NORAD/elements/`.

[153] H. Ochiai and H. Imai. On the distribution of the peak-to-average power ratio in OFDM signals. *IEEE Transactions on Communications*, 49(2):282–289, 2001.

[154] C. Olone, H. Dhillon, and R. Buehrer. Single-anchor localizability in 5G millimeter wave networks. *IEEE Wireless Communications Letters*, 9(1):65–69, 2020.

[155] M. Orabi, J. Khalife, and Z. Kassas. Opportunistic navigation with Doppler measurements from Iridium Next and Orbcomm LEO satellites. In *Proceedings of IEEE Aerospace Conference*, pages 1–9, March 2021.

[156] M. Pan, P. Liu, S. Liu, W. Qi, Y. Huang, X. You, X. Jia, and X. Li. Efficient joint DOA and TOA estimation for indoor positioning with 5G picocell base stations. *IEEE Transactions on Instrumentation and Measurement*, 71:1–19, 2022.

[157] B. Parkinson and P. Enge. Differential GPS. *Global Positioning System: Theory and applications.*, 2:3–50, 1996.

[158] S. Parkvall, Y. Blankenship, R. Blasco, E. Dahlman, G. Fodor, S. Grant, E. Stare, and M. Stattin. 5G NR release 16: Start of the 5G evolution. *IEEE Communications Standards Magazine*, 4(4):56–63, 2020.

[159] K. Pesyna, Z. Kassas, J. Bhatti, and T. Humphreys. Tightly-coupled opportunistic navigation for deep urban and indoor positioning. In *Proceedings of ION GNSS Conference*, pages 3605–3617, September 2011.

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

[161] C. Pinell. Receiver architectures for positioning with low Earth orbit satellite signals. Master's thesis, Lulea University of Technology, School of Electrical Engineering, Sweden, 2021.

[162] Z. Ping and C. Hao. A survey of positioning technology for 5G. *Journal of Beijing University of Posts and Telecommunications*, 41(5):1–12, 2018.

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

[164] A. Popleteev. *Indoor positioning using FM radio signals*. PhD thesis, University of Trento, Italy, 2011.

[165] F. Prol, R. Ferre, Z. Saleem, P. Välisuo, C. Pinell, E. Lohan, M. Elsanhoury, M. Elmusrati, S. Islam, K. Celikbilek, K. Selvan, J. Yliaho, K. Rutledge, A. Ojala, L. Ferranti, J. Praks, M. Bhuiyan, S. Kaasalainen, and H. Kuusniemi. Position, navigation, and timing (PNT) through low earth orbit (LEO) satellites: A survey on current status, challenges, and opportunities. *IEEE Access*, 10:83971–84002, 2022.

[166] M. Psiaki. Navigation using carrier Doppler shift from a LEO constellation: TRANSIT on steroids. *NAVIGATION, Journal of the Institute of Navigation*, 68(3):621–641, September 2021.

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

[168] M. Psiaki and B. Slosman. Tracking digital FM OFDM signals for the determination of navigation observables. *NAVIGATION, Journal of the Institute of Navigation*, 69(2), 2022. doi: 10.33012/2019.17120.

[169] L. Pucci, E. Paolini, and A. Giorgetti. System-level analysis of joint sensing and communication based on 5G new radio. *IEEE Journal on Selected Areas in Communications*, 40(7):2043–2055, 2022.

[170] M. Rabinowitz. *A Differential Carrier-Phase Navigation System Combining GPS with Low Earth Orbit Satellites for Rapid Resolution of Integer Cycle Ambiguities*. PhD thesis, Stanford University, USA, 2000.

[171] 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*, pages 1–7, July 2018.

[172] S. Reid. ORBCOMM system overview, December 2001.

[173] T. Reid, B. Chan, A. Goel, K. Gunning, B. Manning, J. Martin, A. Neish, A. Perkins, and P. Tarantino. Satellite navigation for the age of autonomy. In *Proceedings of IEEE/ION Position, Location and Navigation Symposium*, pages 342–352, 2020.

[174] T. Reid, T. Walter, P. Enge, D. Lawrence, H. Cobb, G. Gutt, M. O'Conner, and D. Whelan. Position, navigation, and timing technologies in the 21st century. volume 2, chapter 43: Navigation from low Earth orbit – Part 1: Concept, Current Capability, and Future Promise, pages 1359–1379. Wiley-IEEE, 2021.

[175] J. Rife. Collaborative vision-integrated pseudorange error removal: Team-estimated differential GNSS corrections with no stationary reference receiver. *IEEE Transactions on Intelligent Transportation Systems*, 13(1):15–24, 2011.

[176] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, and E. Pasiliao. RFAL: adversarial learning for RF transmitter identification and classification. *IEEE Transactions on Cognitive Communications and Networking*, 6(2):783–801, 2019.

[177] S. Ruffini, J. Stefano, M. Johansson, B. Pohlman, and M. Sandgren. 5G synchronization requirements and solutions. *Ericsson technology review*, 2021(1):2–13, 2021.

[178] R. Sabbagh and Z. Kassas. Observability analysis of receiver localization via pseudorange measurements from a single LEO satellite. *IEEE Control Systems Letters*, 7(3):571–576, 2023.

[179] G. Santana, R. Cristo, and K. Branco. Integrating cognitive radio with unmanned aerial vehicles: An overview,. *Sensors*, 21(3):830–856, 2021.

[180] L. Scharf and B. Friedlander. Matched subspace detectors. *IEEE Transactions on signal processing*, 42(8):2146–2157, 1994.

[181] L. Schiff and A. Chockalingam. Signal design and system operation of Globalstar TM versus IS-95 CDMA – Similarities and differences. *Wireless Networks*, 6(1):47–57, February 2000.

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

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

[184] K. Shamaei and Z. Kassas. A joint TOA and DOA acquisition and tracking approach for positioning with LTE signals. *IEEE Transactions on Signal Processing*, pages 2689–2705, 2021.

[185] K. Shamaei and Z. Kassas. Receiver design and time of arrival estimation for opportunistic localization with 5G signals. *IEEE Transactions on Wireless Communications*, 20(7):4716–4731, 2021. doi: 10.1109/TWC.2021.3061985.

[186] 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*, pages 1–6, April 2019.

[187] U. Singh, M. Shankar, and B. Ottersten. Opportunistic localization using LEO signals. In *Proceedings of Asilomar Conference on Signals, Systems, and Computers*, pages 894–899, 2022.

[188] N. Souli, P. Kolios, and G. Ellinas. Relative positioning of autonomous systems using signals of opportunity. In *Proceedings of IEEE Vehicular Technology Conference*, pages 1–6, 2020.

[189] N. Souli, P. Kolios, and G. Ellinas. Adaptive frequency band selection for accurate and fast positioning utilizing SOPs. In *Proceedings of International Conference on Unmanned Aircraft Systems*, pages 1309–1315, 2022.

[190] N. Souli, P. Kolios, and G. Ellinas. Online relative positioning of autonomous vehicles using signals of opportunity. *IEEE Transactions on Intelligent Vehicles*, 7(4):873–885, 2022. doi: 10.1109/TIV.2021.3124727.

[191] N. Souli, R. Makrigiorgis, P. Kolios, and G. Ellinas. Cooperative relative positioning using signals of opportunity and inertial and visual modalities. In *Proceedings IEEE Vehicular Technology Conference*, pages 1–7, 2021.

[192] N. Souli, R. Makrigiorgis, P. Kolios, and G. Ellinas. Real-time relative positioning system implementation employing signals of opportunity, inertial, and optical flow modalities. In *Proceedings of International Conference on Unmanned Aircraft Systems*, pages 229–236, June 2021.

[193] W. Stock, C. Hofmann, and A. Knopp. LEO-PNT with Starlink: Development of a burst detection algorithm based on signal measurements. In *Proceedings of International ITG Workshop on Smart Antennas and Conference on Systems, Communications, and Coding*, pages 1–6, February 2023.

[194] K. Strandjord, Y. Morton, and P. Wang. Evaluating the urban signal environment for GNSS and LTE signals. In *Proceedings of ION GNSS+ Conference*, pages 2166–2182, 2021.

[195] K. Sun. Adaptive code tracking loop design for GNSS receivers. In *Proceedings of IEEE/ION Position, Location and Navigation Symposium*, pages 282–290, April 2012.

[196] W. Sweldens. Fast block noncoherent decoding. *IEEE Communications Letters*, 5(4):132–134, April 2001.

[197] A. Tadaion, M. Derakhtian, S. Gazor, M. Nayebi, and M. Aref. Signal activity detection of phase-shift keying signals. *IEEE Transactions on Communications*, 54(8):1439–1445, August 2006.

[198] K. Takeda, H. Xu, T. Kim, K. Schober, and X. Lin. Understanding the heart of the 5G air interface: An overview of physical downlink control channel for 5G new radio. *IEEE Communications Standards Magazine*, 4(3):22–29, 2020.

[199] Z. Tan, H. Qin, L. Cong, and C. Zhao. New method for positioning using IRIDIUM satellite signals of opportunity. *IEEE Access*, 7:83412–83423, 2019.

[200] Z. Tan, H. Qin, L. Cong, and C. Zhao. Positioning using IRIDIUM satellite signals of opportunity in weak signal environment. *Electronics*, 9(1):37, 2019.

[201] U. Tancredi, A. Renga, and M. Grassi. Validation on flight data of a closed-loop approach for GPS-based relative navigation of LEO satellites. *Acta Astronautica*, 86:126–135, 2013.

[202] G. Tang and A. Peng. 5G receiver design based on downlink intermittent signals tracking algorithm. In *Proceedings of China Satellite Navigation Conference*, pages 462–471, 2022.

[203] S. Tenneti and P. Vaidyanathan. Nested periodic matrices and dictionaries: New signal representations for period estimation. *IEEE Transactions on Signal Processing*, 63(14):3736–3750, 2015.

[204] S. Thompson, S. Martin, and D. Bevly. Single differenced Doppler positioning with low Earth orbit signals of opportunity and angle of arrival estimation. In *Proceedings of ION International Technical Meeting Conference*, pages 497–509, January 2021.

[205] J. Tian, L. Fangchi, T. Yafei, and L. Dongmei. Utilization of non-coherent accumulation for LTE TOA estimation in weak los signal environments. *EURASIP Journal on Wireless Communications and Networking*, 2023(1):1–31, 2023.

[206] D. Tse and P. Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[207] S. Upadhya. Pitch detection in time and frequency domain. In *2012 International Conference on Communication, Information & Computing Technology (ICCICT)*, pages 1–5. IEEE, 2012.

[208] D. Vallado and P. Crawford. SGP4 orbit determination. In *Proceedings of AIAA/AAS Astrodynamics Specialist Conference and Exhibit*, pages 6770–6799, August 2008.

[209] A. Van Dierondonck. *Global Positioning System: Theory and Applications*, chapter 8: GPS Receivers, pages 329–408. American Institute of Aeronautics and Astronautics, Washington D.C., 1996.

[210] W. Van Uytsel, T. Janssen, R. Halili, and M. Weyn. Exploring positioning through pseudoranges using low earth Orbit satellites. In *Proceedings of International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pages 278–287, 2022.

[211] J. Vetter. Fifty years of orbit determination: Development of modern astrodynamics methods. *Johns Hopkins APL Technical Digest*, 27(3):239–252, November 2007.

[212] M. Vlachos, P. Yu, and V. Castelli. On periodicity detection and structural periodic similarity. In *Proceedings of the 2005 SIAM international conference on data mining*, pages 449–460. SIAM, 2005.

[213] G. Wang, X. Han, Y. Wang, and S. Dong. Maintaining the status quo: Simultaneous estimation and elimination for multiple interference in transform domain vehicular communication. *IEEE Transactions on Vehicular Technology*, 71(3):3058–3074, 2022.

[214] G. Wang, Q. Ren, and Y. Su. The interference classification and recognition based on SF-SVM algorithm. In *2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, pages 835–841, 2017.

[215] K. Wang, A. El-Mowafy, W. Wang, L. Yang, and X. Yang. Integrity monitoring of PPP-RTK positioning; part II: LEO augmentation. *Remote Sensing*, 14(7):1599–1620, March 2022.

[216] P. Wang, Y. Cheng, and B. Dong. Augmented convolutional neural networks with transformer for wireless interference identification. In *2021 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2021.

[217] P. Wang, Y. Cheng, and B. Dong. Multi-Depth adaptive networks for wireless interference identification. In *ICC 2021 - IEEE International Conference on Communications*, pages 1–6, 2021.

[218] P. Wang and Y. Morton. Multipath estimating delay lock loop for LTE signal TOA estimation in indoor and urban environments. *IEEE Transactions on Wireless Communications*, 19(8):5518–5530, 2020.

[219] Z. Wang, G. Li, and H. Chen. Adaptive persymmetric subspace detectors in the partially homogeneous environment. *IEEE Transactions on Signal Processing*, 68:5178–5187, 2020.

[220] 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*, pages 783–795, September 1998.

[221] M. Wax and A. Adler. Detection of the number of signals by signal subspace matching. *IEEE Transactions on Signal Processing*, 69:973–985, 2021.

[222] Q. Wei, X. Chen, and Y. Zhan. Exploring implicit pilots for precise estimation of LEO satellite downlink Doppler frequency. *IEEE Communications Letters*, 24(10):2270–2274, 2020.

[223] F. Wen, J. Kulmer, K. Witrisal, and H. Wymeersch. 5G positioning and mapping with diffuse multipath. *IEEE Transactions on Wireless Communications*, 20(2):1164–1174, 2021.

[224] R. Whiton. Cellular localization for autonomous driving: A function pull approach to safety-critical wireless localization. *IEEE Vehicular Technology Magazine*, 17(4):28–37, 2022.

[225] R. Whiton, J. Chen, T. Johansson, and F. Tufvesson. Urban navigation with LTE using a large antenna array and machine learning. In *Proceedings of IEEE Vehicular Technology Conference*, pages 1–5, 2022.

[226] Q. Wu, J. Xu, Y. Zeng, D. Kwan, N. Al-Dhahir, R. Schober, and A. Swindlehurst. A comprehensive overview on 5G-and-beyond networks with UAVs: From communications to sensing and intelligence. *IEEE Journal on Selected Areas in Communications*, 39(10):2912–2945, 2021.

[227] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson. 5G mmWave positioning for vehicular networks. *IEEE Wireless Communications*, 24(6):80–86, December 2017.

[228] A. Xhafa, J. del Peral-Rosado, J. López-Salcedo, and G. Seco-Granados. Evaluation of 5G positioning performance based on UTDoA, AoA and base-station selective exclusion. *Sensors*, 22(1):101–118, 2021.

[229] D. Yacong. *Channel Estimation for Massive MIMO Systems Based on Sparse Representation and Sparse Signal Recovery*. PhD thesis, University of California, San Diego, 2018.

[230] C. Yang and H. Shao. WiFi-based indoor positioning. *IEEE Communications Magazine*, 53(3):150–157, March 2015.

[231] J. Yang, X. Wang, M. Rahman, S. Park, H. Kim, and Y. Wu. A new positioning system using DVB-T2 transmitter signature waveforms in single frequency networks. *IEEE Transactions on Broadcasting*, 58(3):347–359, September 2012.

[232] L. Yin, Q. Ni, and Z. Deng. A GNSS/5G integrated positioning methodology in D2D communication networks. *IEEE Transactions on Signal Processing*, 36(2):351–362, February 2018.

[233] A. Zaimbashi, M. Derakhtian, and A. Sheikhi. GLRT-based CFAR detection in passive bistatic radar. *IEEE Transactions on Aerospace and Electronic Systems*, 49(1):134–159, 2013.

[234] C. Zhao, H. Qin, and Z. Li. Doppler measurements from multiconstellations in opportunistic navigation. *IEEE Transactions on Instrumentation and Measurement*, 71:1–9, 2022.

[235] C. Zhao, H. Qin, N. Wu, and D. Wang. Analysis of baseline impact on differential doppler positioning and performance improvement method for LEO opportunistic navigation. *IEEE Transactions on Instrumentation and Measurement*, pages 1–10, 2023.

[236] T. Zhao and T. Huang. Cramer-Rao lower bounds for the joint delay-Doppler estimation of an extended target. *IEEE Transactions on Signal Processing*, 64(6):1562–1573, 2016.

[237] Y. Zhuang, Z. Syed, Y. Li, and N. El-Sheimy. Evaluation of two WiFi positioning systems based on autonomous crowdsourcing of handheld devices for indoor navigation. *IEEE Transactions on Mobile Computing*, 15(8):1982–1995, August 2016.

[238] H. Zou, M. Jin, H. Jiang, L. Xie, and C. Spanos. WinIPS: WiFi-based non-intrusive indoor positioning system with online radio map construction and adaptation. *IEEE Transactions on Wireless Communications*, 16(12):8118–8130, 2017.

[239] C. Zucca and P. Tavella. The clock model and its relationship with the Allan and related variances. *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, 52(2):289–296, February 2005.