I Can Hear You Loud and Clear: GNSS-Less Aircraft Navigation With Terrestrial Cellular Signals of Opportunity

ZAHER M. KASSAS, Fellow, IEEE
The Ohio State University, Columbus, OH USA

ALI A. ABDALLAH, Student Member, IEEE
University of California, Irvine, CA USA

SHAGHAYEGH SHAHCHERAGHI, Student Member, IEEE
The Ohio State University, Columbus, OH USA

JOE J. KHALIFE, Member, IEEE
University of California, Irvine, CA USA

CHIAWEI LEE
JUAN JURADO, Member, IEEE
STEVEN WACHTEL
JACOB DUEDE
ZACHARY HOEFFNER
THOMAS HULSEY
RACHEL QUIRARTE
US Air Force, Washington, DC USA

RUNXUAN TAY
Republic of Singapore Air Force, Singapore

Manuscript received 20 April 2023; revised 22 September 2023 and 2 May 2024; accepted 21 June 2024. Date of publication 1 July 2024; date of current version 6 December 2024.

DOI. No. 10.1109/TAES.2024.3418943

Refereeing of this contribution was handled by M. Uijt de Haag.

This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-22-1-0476, in part by the Office of Naval Research (ONR) under Grant N00014-19-1-2511, in part by the National Science Foundation (NSF) under Grant 2240512, in part by the Laboratory Directed Research and Development Program at Sandia National Laboratories, and in part by the U.S. Department of Transportation for the CARMEN+ University Transportation Center (UTC) under Grant 69A3552348327.

Authors' addresses: Zaher M. Kassas and Shaghayegh Shahcheraghi are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH, USA, E-mail: (zkassas@ieee.org); Ali A. Abdallah and Joe J. Khalife were with the Department of Electrical Engineering and Computer Science, University of California, Irvine, CA, USA; Chiawei Lee, Juan Jurado, Steven Wachtel, Jacob Duede, Zachary Hoeffner, Thomas Hulsey, and Rachel Quirarte are with the US Air Force, Washington, DC, USA; RunXuan Tay is with the Republic of Singapore Air Force, Singapore 534236. *(Corresponding author: Zaher M. Kassas.)*

Aircraft navigation without global navigation satellite system (GNSS) signals is considered. To this end, a high-sensitivity receiver design is presented that could exploit terrestrial cellular signals of opportunity. The receiver operates on downlink orthogonal frequency division multiplexing (OFDM) signals transmitted by long-term evolution (LTE) eNodeBs. Two challenges encountered on high-altitude aircraft are addressed: weak signal power and insufficiently accurate initial Doppler estimation. A so-called ultimate reference signal is proposed, which exploits all available LTE resources transmitted by eNodeB's multiple antenna ports. A time-domain-based receiver design is presented to extract carrier phase observables without the need to reconstruct the received OFDM frame. The proposed approach is shown to significantly improve the receiver's sensitivity, amplifying the received power by nearly 21 dB, while also improving the carrier phase estimation accuracy. To evaluate the efficacy of the proposed receiver, experimental results are presented of an aircraft flying over two regions in California, USA: Region A: Edwards Air Force Base (rural) and Region B: Palmdale (semi-urban). For three aircraft maneuvers (climbing teardrop, descending teardrop, and grid), the results were consistent: more than 100 eNodeBs were trackable, some of which were more than 100 km away, at altitudes as high as about 11,000 ft with carrier-to-noise ratio over 40 dB-Hz. Upon fusing the carrier phase observables with altimeter data via an extended Kalman filter, a sustained accurate navigation solution was achieved. Over trajectories of 43.6 and 56.8 km in regions A and B, traversed in 455 and 601 s, a 3-D position root mean-squared error of 6.8 and 8.2 m was achieved by exploiting an average of about 22 and 11 eNodeBs, respectively.

I. INTRODUCTION

A search of the phrase "Global Positioning System (GPS)" on the aviation safety reporting system (ASRS) returns 4992 GPS-related incidents from January 2000 to April 2023 [1]. The ASRS is a publicly available reporting system established by NASA to identify and address issues reported by frontline personnel in aviation. A deeper look at the data reveals that the vast majority of these incidents are due to navigation-related malfunction or failures. In particular, of the nearly 200 listed aircraft components, 710 issues were reported with "GPS and other satellite navigation," "navigation equipment and processing," and "GPS module (UAS) [unmanned aircraft systems]."

Over the past few years, global navigation satellite system (GNSS) radio frequency interference (RFI) incidents skyrocketed, jeopardizing safe and efficient aviation operations. RFI sources include repeaters and pseudolites, GNSS jammers, and systems transmitting outside the GNSS frequency bands [2]. According to EUROCONTROL, a pan-European, civil–military organization dedicated to supporting European aviation, there were 4,364 GNSS outages reported by pilots in 2018, which represents more than a 2000% increase over the previous year [3]. What is alarming is that while the majority of RFI hotspots appear to be due to conflict zones, they affected civil aviation at distances of up to 300 km from these zones. The majority of RFI (about 81%) affected en-route flights, even though this is where RFI should be at its lowest, as the aircraft is far away from a ground-based interferer. In 2019, the International Civil Aviation Organization (ICAO) issued a Working Paper titled "An Urgent Need to Address Harmful Interferences to GNSS," where it concluded that harmful RFI to GNSS would prevent the full continuation of safety and efficiency benefits of GNSS-based services [4]. ICAO followed this by an "Action Required" letter for "Strengthening of Communications, Navigation, and Surveillance (CNS) Systems Resilience and Mitigation of Interference to Global Navigation Satellite System (GNSS)" [5].

In 2021, the National Institute of Standards and Technology issued a report on "Foundational PNT profile: Applying the cybersecurity framework for the responsible use of positioning, navigation, and timing (PNT) services," where it identified signals of opportunity (SOPs) and terrestrial RF sources (e.g., cellular) as a mitigation category that apply to the PNT profile [6]. To exploit SOPs for PNT [7], the following challenges have to be addressed:

1) estimating the unknown SOP transmitter states (position and clock errors);
2) designing receivers capable of extracting navigation observables (code phase, carrier phase, and Doppler);
3) dealing with relatively unstable clocks and loosely synchronized networks;
4) mitigating multipath.

Researchers over the past decade have presented approaches to overcome these challenges, leading to revealing the tremendous promise of SOPs, cellular in particular, as alternative PNT sources [8], [9], [10], [11], [12], [13], [14], [15], [16], [17].

A. Related Work: PNT With Cellular Signals

Among cellular generations, the fourth-generation (4G) long-term evolution (LTE), which adopts orthogonal frequency division multiplexing (OFDM), possesses desirable attributes for PNT purposes: abundance, geometric diversity, frequency diversity, high received power, and high bandwidth. Cellular LTE signals have shown high ranging and localization accuracy [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], even in urban and indoor environments experiencing severe multipath [28], [29], [30], [31], [32] and environments under intentional GPS jamming [33]. Experimental results with LTE signals demonstrated meter-level positioning accuracy on ground vehicles [34], [35], [36], [37] and submeter-level positioning accuracy on unmanned aerial vehicles (UAVs) [38], [39].

PNT with LTE signals can be categorized into two techniques: network-based and user equipment (UE)-based. The network-based technique utilizes a dedicated signal called the positioning reference signal (PRS). PRS-based positioning suffers from a number of drawbacks:

1) the user's privacy is compromised, since the user's location is revealed to the network;
2) localization services are limited only to paying subscribers and from a particular cellular provider;
3) ambient LTE signals transmitted by other cellular providers are not exploited;
4) additional bandwidth is required to accommodate the PRS, which caused the majority of cellular providers to choose not to transmit the PRS in favor of dedicating more bandwidth for traffic channels.

The UE-based technique, also known as opportunistic navigation, exploits other reference signals (RSs), which are not dedicated for positioning services. There are three RSs in LTE systems that can be exploited for positioning purposes: primary synchronization signal (PSS), secondary synchronization signal (SSS), and cell-specific reference signal (CRS).

Among LTE's downlink RSs, the CRS is particularly attractive due to its high bandwidth. Due to OFDM's spectral nature, the CRS is transmitted on distinct OFDM symbols and subcarriers, also known as logical ports. In [40], a maximum likelihood-based method to estimate the first path was proposed, which utilized one antenna port. The signal diversity provided via multiple antenna ports was exploited for cycle slip detection in LTE carrier phase measurements in [41]. Positioning in multipath environments was studied in [42] and [43], both of which considered one antenna port. The effect of antenna ports on time of arrival (TOA) estimation using CRS was investigated in [44]. The study showed that different channel responses were recorded for different antenna ports, which can diversify the incoming signals and improve positioning. A tracking algorithm that adaptively mitigated multipath in LTE positioning receivers, while utilizing CRS from one antenna port, was proposed in [45]. Exploiting two antenna ports was considered in [46], where signals from each port were treated as the separate measurements, while Lapin et al. [47] tracked signals from each port independently. However, none of the aforementioned studies considered the *simultaneous* exploitation of *all* antenna ports as a *single* navigation source. In general, to extract navigation observables from OFDM signals, existing methods have approached the receiver design from a communication systems perspective [43].

This article exploits additional available LTE resources in generating the receiver's locally generated code, which offers two advantages: 1) increase the power by exploiting more available resource elements (REs), which in turn results in improving the acquisition, and 2) construct a "pseudorandom noise (PRN)"-like code that possesses a higher bandwidth, and thus, improving the precision of navigation observables (code phase, carrier phase, and Doppler).

B. Related Work: Aircraft PNT With Cellular Signals

The potential of cellular LTE signals for high-altitude aircraft PNT has been largely unstudied [48], [49]. To the best of the authors' knowledge, the first such studies appeared in [50], [51], and [52]. The results therein were achieved from a collaboration between the United States Air Force (USAF) and the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory through a week-long flight campaign called "SNIFFER: SOPs for Navigation In Frequency-Forbidden EnviRonments." ASPIN Laboratory's LTE software-defined receiver (SDR) [53] was flown on a Beechcraft C-12 Huron, a fixed-wing USAF aircraft, to collect ambient cellular LTE signals for flight runs over two regions in California, USA: 1) Region A (rural): Edwards Air Force Base (AFB) and 2) Region B (semiurban): Palmdale. The flights spanned different altitudes and a multitude of trajectories including straight segments, banking turns, benign and aggressive maneuvers, and ascending/descending teardrops with a descent rate ranging between 0 to 1500 ft/min. The flights were performed by members of the USAF Test Pilot School.

The main conclusions from the studies in [50], [51], and [52] were the following.

1) Cellular LTE signals are surprisingly powerful at both a) high altitudes, exhibiting carrier-to-noise ratio (CNR) of 25–55 dB-Hz at altitudes of 2,000–23,000 ft above ground level (AGL), and b) horizontal distances as far as 50 km, exhibiting CNR of about 30 dB-Hz, while flying at about 16,000 ft AGL.
2) The two-ray model fits the measured CNR sufficiently well for towers more than 10 km away, while flying at an altitude of 16,000 ft AGL. For towers closer than 10 km, the antenna radiation pattern should be incorporated into the two-ray model to improve model fitting.
3) The LTE SDR was able to acquire and track five LTE eNodeBs in Regions A and B. In addition, 3G code-division multiple-access (CDMA) base transceiver stations were acquired and tracked with the SDR developed in [54]: six in Region A and nine in Region B. Upon fusing the LTE and CDMA carrier phase observables with altimeter measurements via an extended Kalman filter (EKF), a 3-D position root-mean-squared error (RMSE) of 10.53 and 4.96 m were achieved in Regions A and B, respectively, over trajectories of 51 and 57 km traversed in 9 and 11 minutes, respectively.

C. Contributions

This article considers the problem of navigating an aircraft during GNSS outages, by exploiting signals from cellular SOP towers with known positions, starting with an estimate about the aircraft's initial state. This article presents an opportunistic OFDM-based LTE navigation receiver design that exploits all available resources from various antenna ports simultaneously. Unlike previous generation receivers, the proposed receiver exploits the orthogonality property of OFDM signals without the need for reconstructing the received OFDM frame. The proposed approach significantly improves the receiver's sensitivity, amplifying the received power by a factor up to 21 dB, while also improving the carrier phase estimation accuracy.

Upon reprocessing the raw LTE samples on which the receiver in [50], [51], and [52] operated, the number of acquirable and trackable LTE eNodeBs grew *dramatically*, from 5 to more than 100. Some of these findings were initially reported in [55], but without providing any details of the receiver design, navigation filter formulation, or EKF errors.

This article makes the following contributions. First, it discusses the challenges with using OFDM signals for high-altitude aircraft navigation, namely: 1) weak signal power and 2) insufficiently accurate initial Doppler estimation. Second, it proposes the so-called ultimate RS (URS) for OFDM-based LTE opportunistic navigation to simultaneously exploit all available LTE resources. Third, it develops a time-domain-based receiver design to extract carrier phase observables from received LTE signals. Finally, it evaluates the navigation performance with the SNIFFER data. For three different maneuvers (climbing teardrop, descending teardrop, and grid) in Regions A and B, the results were consistent: more than 100 eNodeBs were trackable, some of which were more than 100 km away, at altitudes as high as $\sim$11,000 ft with CNR over 40 dB-Hz. Upon fusing the carrier phase observables with altimeter data via an EKF, initialized with the aircraft's state produced by its onboard GPS-inertial navigation system (INS), a sustained accurate navigation solution along the aircraft's trajectory was achieved. Over trajectories of 43.6 and 56.8 km in regions A and B, traversed in 455 and 601 s, a 3-D position RMSE of 6.8 and 8.2 m was achieved by exploiting an average of about 22 and 11 eNodeBs, respectively.

The rest of this article is organized as follows. Section II overviews the LTE frame structure. Section III discusses the challenges associated with OFDM-based high-altitude aircraft navigation. Section IV introduces the URS and analyzes its correlation properties. Section V details the proposed receiver design. Section VI discusses SNIFFER's hardware setup and flight regions. Section VII shows the proposed receiver output over various flight trajectories in Regions A and B. Section VIII formulates the EKF navigation framework. Section IX provides the navigation results in Regions A and B. Finally, Section X concludes this article.

II. LTE FRAME STRUCTURE

This article proposes an opportunistic navigation approach; thus, it only considers the LTE downlink signal, which uses OFDM with cyclic prefix (CP) as a modulation technique. An LTE frame has a duration of 10 ms and consists of ten subframes, each with a duration of 1 ms. A frame can also be decomposed into two half-frames, where subframes 0–4 form half-frame 0 and subframes 5–9 form half-frame 1.

In the time domain, each subframe breaks down into numerous slots, each of which contains 14 OFDM symbols for a normal CP length. There are two slots in each subframe, where each slot has seven OFDM symbols. The subcarrier spacing in LTE is fixed and defined as $\Delta f = 15$ kHz. In the frequency domain, a slot can be decomposed into multiple resource grids (RGs), where each RG consists of a large number of resource blocks (RBs). An RB is broken down into the smallest elements of the frame, called REs. The indices of an RE are the subcarrier frequency (k) and symbol time (l) [11]. Fig. 1 depicts the LTE frame structure.

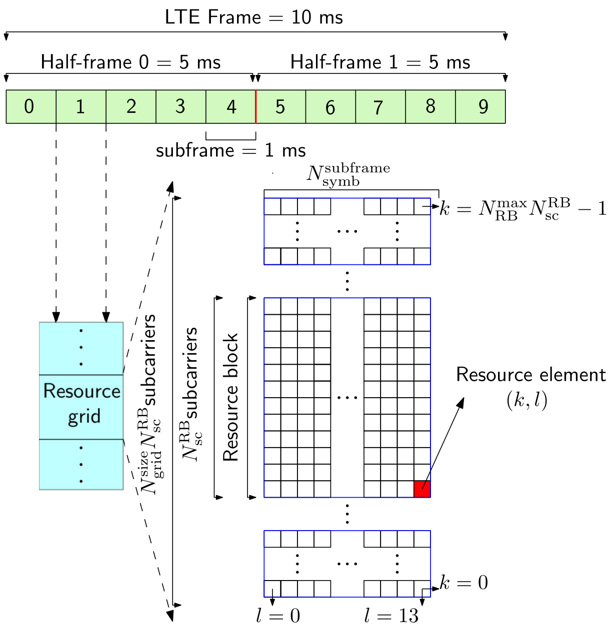
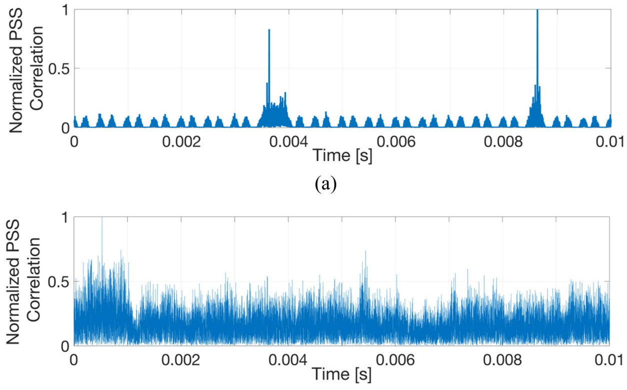


Fig. 1. LTE frame structure.



(a)

(b)

Fig. 2. Acquisition output of the state-of-the-art LTE receiver [53]: (a) on a ground-based receiver and (b) on an aircraft at 5,500 ft AGL.

III. CHALLENGES OF OFDM-BASED HIGH-ALTITUDE AIRCRAFT NAVIGATION

Signals received from terrestrial transmitters by high-altitude aircraft suffer from high path loss due to long-range wireless propagation. By design, cellular transmitters are optimized for ground-based UEs—the eNodeB's antennas are tilted downward to prevent intercell interference and provide service for ground-based UEs via the antenna's main lobe [56].

OFDM-based navigation receivers in the literature were designed for ground platforms or low-altitude UAVs operating in close proximity to the eNodeBs, where the UE is within the eNodeB's antenna's main lobe or some of the more powerful sidelobes. Employing such receivers on high-altitude aircraft revealed challenges in acquiring and tracking terrestrial cellular signals, especially from eNodeBs exhibiting low CNRs. Fig. 2(a) shows the acquisition results of LTE's PSS with the state-of-the-art LTE navigation receiver [53] on a ground-based receiver. The same receiver was able to acquire and track LTE signals on low-altitude UAVs, achieving submeter-level accuracy [38], [41]. However, upon testing this receiver on LTE cellular data collected on an aircraft at 5,500 ft AGL, the receiver failed to acquire the PSS, as shown in Fig. 2(b).

Another challenge on high-altitude aircraft is the OFDM receiver's ability to estimate, in the acquisition stage, the initial Doppler with sufficient accuracy to achieve lock in the tracking loops. Such accuracy is limited due to the small duty factor $r_{\text{T,SS}}$ of the synchronization signals (SSs), defined as the ratio between the number of exploited symbols in a frame to the total number of symbols in a frame. This limitation becomes more severe on high-dynamics platforms, where Doppler shifts have a wider range.

IV. ULTIMATE RS

This section proposes the URS to address the challenges discussed in Section III: weak received signal power and inaccurate initial Doppler frequency estimation. The 3GPP standard defines what are known as antenna ports for the LTE cellular system. Antenna ports do not necessarily correspond to physical antennas, but rather are logical entities distinguished by their reference sequences. A single logical antenna port can include multiple RSs that correspond to the same physical antenna. Correspondingly, a single antenna port can be spread across multiple transmit antennas. The formal definition of an antenna port is: An antenna port is defined such that the channel over which an OFDM symbol on the antenna port is conveyed can be inferred from the channel over which another symbol on the same antenna port is conveyed [57]. There is one RG per antenna port, and the antenna ports used for transmission of a physical channel or signal depend on the number of antenna ports configured for the physical channel or signal.

In the proposed approach, the CRS is exploited, which spans the entire bandwidth of the LTE system and is known for the UE. For CRS, the associated antenna ports p can be $p = 0$, $p \in \{0, 1\}$, or $p \in \{0, 1, 2, 3\}$. Although different antenna ports do not have to correspond to different physical antennas for all RSs, the CRS is a special RS that has a one-to-one mapping. Fig. 3 shows the LTE OFDM frame and the corresponding CRS resources for all antenna ports. The depicted frame corresponds to a simulated LTE downlink frame with 20 MHz system bandwidth (the highest possible bandwidth), i.e., the number of used subcarriers are 1200, each with 15 kHz spacing [58], with a 2-MHz guard bands for LTE transmission.

The LTE receiver in [53] exploited only one OFDM symbol of the CRS resources, corresponding to $p = 0$ (shown in blue in Fig. 3). The total number of OFDM symbols in an OFDM frame is 140; therefore, exploiting only one symbol results in such receiver having a duty factor of $r_{\text{T,CRS}_{\text{old}}} = \frac{1}{140} = 0.71\%$. For simplicity of notation, the subscript CRS_{old} will be denoted by CRS, which corresponds to the previous-generation LTE receiver.

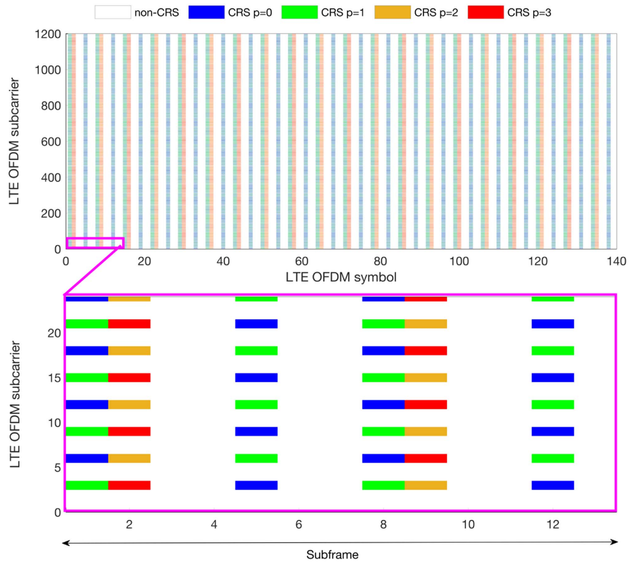


Fig. 3. CRS allocation within the LTE OFDM frame for all antenna ports. The vertical axes show the subcarrier index of each RE, whereas the horizontal axes show the symbol index. In the lower figure, one subframe that consists of 14 symbols is zoomed upon to better illustrate the spread of CRS across subcarriers and symbols.

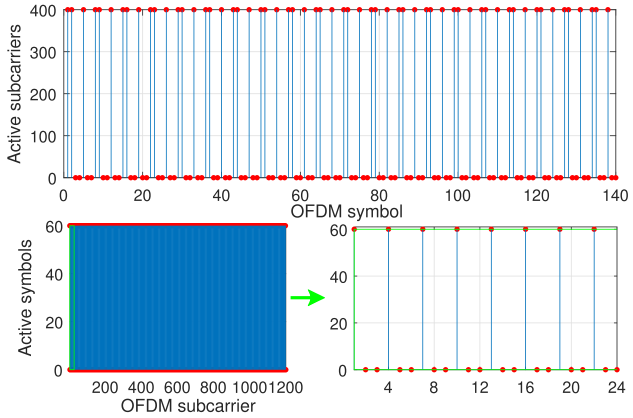


Fig. 4. Top: number of active subcarriers for each URS symbol. Bottom: number of active symbols for each URS subcarrier.

In the proposed approach, where various available ports are exploited, the combined CRSs from different antenna ports define the so-called URS. In other words, the combined OFDM REs depicted in Fig. 3 represent the URS. To study the URS's spectral efficiency $r_{\text{B,URS}}$ and duty factor $r_{\text{T,URS}}$, the number of active subcarriers and symbols was obtained, as shown in Fig. 4. Assuming that a URS symbol is active if ten or more subcarriers are active within that symbol results in having 60 active symbols; hence, $r_{\text{T,URS}} = \frac{60}{140} = 42.86\%$ (in contrast to $r_{\text{T,CRS}} = 0.71\%$). For the bandwidth ratio, Fig. 4 shows that $r_{\text{B,URS}} = r_{\text{B,CRS}} = 100\%$.

In light of the aforementioned analysis, the following advantages can be pointed out.

1) The proposed URS exploits 24 000 REs compared with 200 REs in the past receiver, which means that the received LTE *power* is amplified by a factor of $120 \approx 21$ dB. Thus, using the URS addresses the challenge of weak signals, which arises in high-altitude aircraft navigation, among other applications (e.g., indoor and deep urban navigation). Fig. 5 shows the relative normalized magnitude of the CRS-based and the proposed URS-based squared autocorrelation function (ACF), assuming unity equivalent power among all REs. The ratio of their corresponding ACFs gives the gain factor. The CRS-based and the URS-based normalized squared ACFs are 6.29687×10^{-5} and 1, respectively, resulting in the gain factor of $r_{\text{gain}} = \sqrt{\frac{1}{6.29687\times10^{-5}}} = 126.02$. This increase in gain is due to the added CP REs before converting the LTE frame to a serial data by taking the inverse fast Fourier transform (IFFT) of each OFDM symbol. This step will be discussed in the process of generating the URS replica.

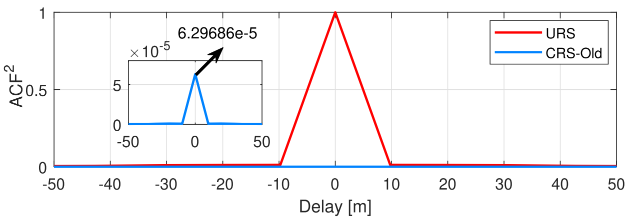


Fig. 5. Comparison of CRS-based and proposed URS-based ACF.

2) The proposed URS improves the duty cycle by a factor of 60, which improves the carrier phase estimation accuracy and initial Doppler shift estimation.

V. TIME-DOMAIN LTE URS-BASED RECEIVER

This section proposes a time-domain-based receiver that operates on the proposed URS to exploit time orthogonality and extract navigation observables from received LTE OFDM signals. State-of-the-art LTE navigation receivers only consider the orthogonality of the synchronization and channel estimation RSs in the frequency domain, i.e., the transmitted OFDM frame is always reconstructed from the received time-domain serial data. Then, the navigation observables are estimated by utilizing the RS with the highest bandwidth. LTE navigation receivers adopted such approach by following the design outlined in LTE communication receivers. However, in communication applications, it is necessary to reconstruct the OFDM frame in order to extract various system information, which allows for two-way communication between the UE and the eNodeB. In contrast, in opportunistic UE-based navigation applications, the ultimate objective is to obtain navigation observables by utilizing the most available frequency (bandwidth) and time (duty factor) resources in the received signal.

The proposed receiver exploits the orthogonality property of OFDM signals in both frequency and time, where all available REs are combined and used simultaneously in a time-domain-based URS, denoted by $\boldsymbol{URS}_i^t$, where t denotes the time domain and i is the eNodeB physical cell

ID. The rest of this section presents: 1) URS generation and 2) receiver stages: acquisition and tracking.

A. URS Generation

1) *Frequency Domain:* In the frame structure, the CRS sequence $r_{l,n_s}(k)$ is defined as

$$r_{l,n_s}(k) = \frac{1}{\sqrt{2}}\,[1 - 2 \cdot s(2\,k)] + j\frac{1}{\sqrt{2}}\,[1 - 2 \cdot s(2k + 1)]$$
$$k = 0, 1, \ldots, 2\,N_{\mathrm{RB}}^{\max,\mathrm{DL}} - 1,$$

where n_s is the slot number within the frame and $N_{\mathrm{RB}}^{\max,\mathrm{DL}}$ is the largest downlink bandwidth configuration. The pseudorandom sequence $s(\cdot)$ is defined as

$$\begin{aligned} s(n) &= [x_1(n + N_c) + x_2(n + N_c)] \bmod 2\\ x_1(n + 31) &= [x_1(n + 3) + x_1(n)] \bmod 2\\ x_2(n + 31) &= [x_2(n + 3) + x_2(n + 2) + x_2(n + 1) + x_2(n)]\\ &\quad \bmod 2, \end{aligned}$$

where $N_c = 1600$, and the first maximal length sequence (m-sequence) shall be initialized with $x_1(0) = 1,\ x_1(n) = 0,\ n = 1, 2, \ldots, 30$. The initialization of the second m-sequence is given by

$$s_{\mathrm{init}} = 2^{10} \cdot \left(7 \cdot (n_s' + 1) + l + 1\right) \cdot (2i + 1) + 2i + N_{\mathrm{CP}}$$

where it is initialized at the start of each OFDM symbol as

$$n_s' = \begin{cases} 10\lfloor n_s/10 \rfloor + n_s \bmod 2, & \text{if frame structure type 3}\\ n_s, & \text{otherwise} \end{cases}$$

$$N_{\mathrm{CP}} = \begin{cases} 1, & \text{for normal CP}\\ 0, & \text{for extended CP.} \end{cases}$$

The CRS sequence $r_{l,n_s}(k)$ is allocated within the LTE frame according to

$$\begin{aligned} k &= 6\ \mathrm{m} + (v + v_{\mathrm{shift}}) \bmod 6\\ l &= \begin{cases} 0, N_{\mathrm{symb}}^{\mathrm{DL}} - 3 & \text{if } p \in \{0, 1\}\\ 1, & \text{if } p \in \{2, 3\} \end{cases}\\ m &= 0, 1, \ldots, 2\,N_{\mathrm{RB}}^{\mathrm{DL}} - 1, \end{aligned}$$

where $N_{\mathrm{RB}}^{\mathrm{DL}}$ is the downlink bandwidth configuration of received LTE signals, and the variables v and v_{shift} define the position in the frequency domain for different RSs, where v is given by

$$v = \begin{cases} 0, & \text{if } p = 0 \text{ and } l = 0\\ 3, & \text{if } p = 0 \text{ and } l \neg 0\\ 3, & \text{if } p = 1 \text{ and } l = 0\\ 0 & \text{if } p = 1 \text{ and } l \neg 0\\ 3(n_s \bmod 2), & \text{if } p = 2\\ 3 + 3(n_s \bmod 2), & \text{if } p = 3, \end{cases}$$

and $v_{\mathrm{shift}} = i \bmod 6$ for CRS.

2) *Time Domain:* After allocating all CRS REs in the LTE frame and assigning zero to the rest of REs, the resulting frame represents the frequency-domain URS denoted as $\mathbf{URS}_i^f$. The $\mathbf{URS}_i^f$ is converted into a serial time-domain-based sequence $\boldsymbol{URS}_i^t$ by zero-padding $\left(\frac{1}{2}N_{\mathrm{RB}}^{\max,\mathrm{DL}} - N_{\mathrm{RB}}^{\mathrm{DL}}\right)$ REs on both sides of the signal in the frequency domain. Then, the IFFT is taken, and the CP elements are added, which are nothing but an identical copy of the portion of the OFDM symbol appended before the OFDM symbol to prevent intersymbol interference. This procedure is the exact procedure occurring at the eNodeB, except for having zeros instead of having data in the data-allocated REs, which is necessary to prevent interference and guarantee orthogonality of the $\boldsymbol{URS}_i^t$.

B. Acquisition

The objective of this stage is to determine which eNodeBs are in the receiver's proximity and to obtain a coarse estimate of their corresponding code start times and Doppler frequencies. Assuming that the carrier frequencies of surrounding eNodeBs are known to the UE, the UE samples the LTE spectrum with a sufficient sampling rate to capture the entire LTE system bandwidth and convert the signals to baseband by wiping off the carrier frequency. The received discrete-time signal is denoted by $x[n]$, where n is a discrete-time instance. Then, a search over the code start time and Doppler frequency is performed to detect the presence of a signal in $x[n]$ at $n = 0$. For LTE, there are 504 possible URS sequences resulting from the possible CRS sequences, denoted by $\{\boldsymbol{URS}_i^t\}_{i=0}^{503}$. Analogously to GPS, $\boldsymbol{URS}_i^t$ can be thought of as the "LTE PRN" on which the receiver operates.

One main advantage of the time-domain SDR is the ability to perform a GPS-like frequency-acquisition search to estimate the initial Doppler shift, especially with the increase in the duty factor that the proposed URS offers. The search results in a coarse estimate of the initial Doppler frequency $\hat{f}_{D_0}$ and code start time $\hat{t}_{s_0}$, which are then fed to the tracking loops. It is worth mentioning that the proposed URS excluded the SSs due to the fact that the SSs are not unique for every eNodeB and will cause interference, especially at high altitudes, where numerous eNodeBs are hearable due to the clear line-of-sight.

One main challenge in the acquisition stage is the computational burden, where the Doppler search is performed for 504 possible URSs. As a point of reference, this is 15 times more than GPS L1 C/A's possible PRNs. In light of this, the proposed SDR employs two optimization measures to reduce the computational complexity of the acquisition stage.

The first measure is to combine different sectors of the same eNodeB, i.e., Cell IDs with different PSS but the same SSS). This is possible since the SSs are not utilized in the proposed URS. In other words, the three sectors of a particular eNodeB will have one PRN, which can be expressed as

$$\boldsymbol{URS}_{i'}^t = \underbrace{\boldsymbol{URS}_{i=i'}^t}_{\text{PSS = 0}} + \underbrace{\boldsymbol{URS}_{i=i'+1}^t}_{\text{PSS = 1}} + \underbrace{\boldsymbol{URS}_{i=i'+2}^t}_{\text{PSS = 2}},$$
$$\text{for } i' = \{0, 3, 6, \ldots, 501\},$$

where each one of the three URS sequences represents a sector in the corresponding eNodeB. This design reduces the number of possible URSs by a factor of 3.

The second measure is combining the search over Doppler values, which has an integer difference of LTE frame frequency spacing, i.e., $\frac{1}{t_{\text{frame}}} = 100$ Hz. The Doppler search range can be expressed as

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

where $f_{\max}$ is the maximum search value and f_{step} is the search step. If $f_{\max} > \frac{1}{t_{\text{frame}}} = 100$ Hz, a new search range can be defined as

$$f_0 \equiv \left[-100 : f_{\text{step}} : 100\right].$$

Then, the Doppler search range can be rewritten as

$$f_{D,\text{search}} \in \left[\cdots, -\underbrace{3f_0, -\overbrace{2f_0, f_0, 2}^{\text{one sample}}f_0, 3}_{\text{Circular shift of two samples}} f_0, \cdots\right].$$

In this way, higher search ranges are nothing but f_0 with integer circularly shifted version of the locally generated URSs.

C. Tracking

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

The PLL consists of a phase discriminator, a loop filter, and a numerically controlled oscillator (NCO). Since the URS is a data-less pilot channel, an `atan2` discriminator, which remains linear over the full input error range of $\pm\pi$, could be used without the risk of having phase ambiguities. Even with the dynamics of the C-12 aircraft, it was found that a second-order PLL is sufficient to maintain track of the carrier phase. The loop filter transfer function is given by

$$F_{\text{PLL}}(s) = \frac{2\zeta\omega_n s + \omega_n^2}{s}, \tag{1}$$

where ζ is the damping ratio and ω_n is the undamped natural frequency, which can be related to the PLL's noise-equivalent bandwidth $B_{n,\text{PLL}}$ by $B_{n,\text{PLL}} = \frac{\omega_n}{8\zeta}(4\zeta^2 + 1)$ [59]. The output of the loop filter at the mth subaccumulation $\upsilon_{\text{PLL},m}$ is the rate of change of the carrier phase error, expressed in rad/s. The Doppler frequency estimate is obtained as $\hat{f}_{D_m} = \frac{\upsilon_{\text{PLL},m}}{2\pi}$. The carrier phase estimate is computed as

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

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

The carrier-aided DLL employs the noncoherent dot-product discriminator, in which the prompt, early, and late correlations are denoted by S_{p_m}, S_{e_m}, and S_{l_m}, respectively. The DLL loop filter is a simple gain K, with a noise-equivalent bandwidth $B_{n,\text{DLL}} = \frac{K}{4}$. The output of the DLL loop filter $\upsilon_{\text{DLL},m}$ is the rate of change of the code phase, expresses in s/s. Assuming low-side mixing, the code start time is updated according to

$$\hat{t}_{s_{m+1}} = \hat{t}_{s_m} - (\upsilon_{\text{DLL},m} + \hat{f}_{D_m}/f_c) \cdot N_s T_s, \tag{3}$$

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

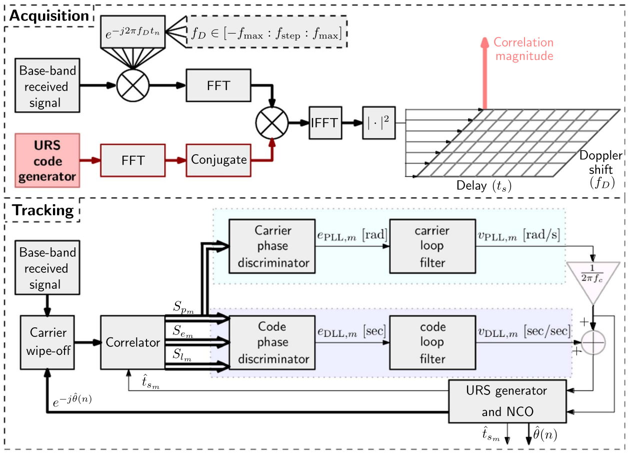


Fig. 6. Block diagram of the proposed receiver. Thick lines represent complex-valued quantities.

Fig. 6 summarizes the acquisition and tracking stages of the proposed receiver. Note the similarities between the proposed receiver's tracking stage and the tracking stage of a conventional GNSS receiver [60]: virtually all building blocks are identical (carrier wipe-off, correlators, filters, discriminators, and NCO), with the main difference being the PRN generator being replaced with the URS generator.

VI. SNIFFER: HARDWARE SETUP AND FLIGHT REGIONS

This section overviews the hardware setup used for data collection and processing in the SNIFFER flight campaign. It also describes the flight regions and aircraft maneuvers.

A. Hardware Setup

The hardware was assembled on a rack, which was mounted on the C-12 aircraft. The rack was equipped with the following.

1) A quad-channel universal software radio peripheral (USRP)-2955.
2) A desktop computer equipped with solid-state drive for data storage.
3) A laptop computer running real-time LTE acquisition, which was operated during the flight by a flight engineer to determine when, where, and what cellular LTE channels were available to tune the USRP-2955 accordingly. The USRP-2955 was connected to the laptop via a peripheral component interconnect express cable.
4) A GPS antenna to a) feed GPS measurements to the aircraft navigation system and b) discipline the USRP's onboard GPS-disciplined oscillator.

Fig. 7. USAF pilots and ASPIN researchers with the C-12 aircraft. Left to right: Hulsey, Tay, Abdallah, Quirarte, Kassas, Khalife, Hoeffner, and Wachtel.

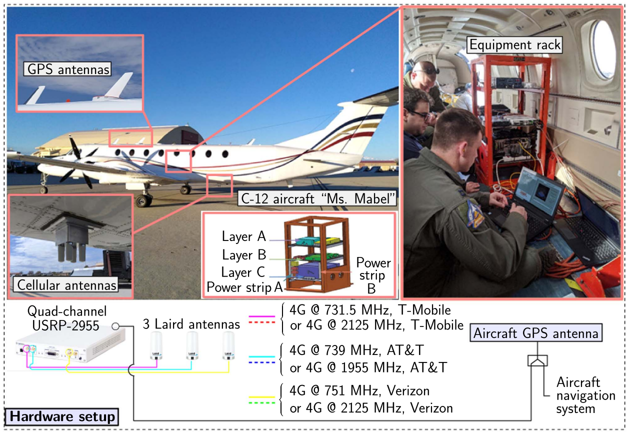


Fig. 8. Hardware setup with which the C-12 aircraft was equipped.

Three consumer-grade 800/1900 MHz Laird cellular antennas were mounted to the bottom of the C-12 and were connected to the USRP-2955. The USRP was tuned to listen to three carrier frequencies corresponding to the U.S. cellular providers: T-Mobile, AT&T, and Verizon. The sampling rate of each cellular channel was 10 mega samples per second. The previous generation LTE SDR and the proposed receiver were used to postprocess the stored data. Fig. 7 shows the C-12 aircraft, known as Ms. Mabel, along with ASPIN researchers and USAF pilots. Fig. 8 shows the hardware setup with which the C-12 aircraft was equipped.

B. Flight Regions and Aircraft Maneuvers

A flight campaign over four consecutive days was conducted during which samples of LTE signals were stored for postprocessing. The flights took place over two regions in California, USA, shown in Fig. 9: 1) Region A (rural): Edwards AFB and 2) Region B (semi-urban): Palmdale.

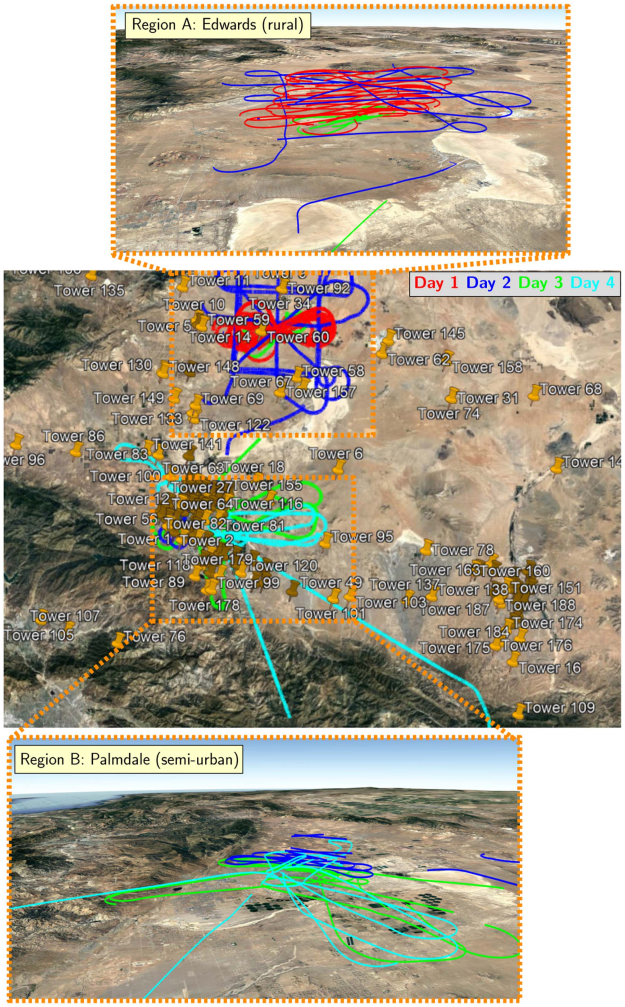


Fig. 9. Regions A and B in Southern California, USA, over which the flight campaign took place. The orange pins represent cellular LTE eNodeBs. The flight trajectories over the four days are shown in different colors.

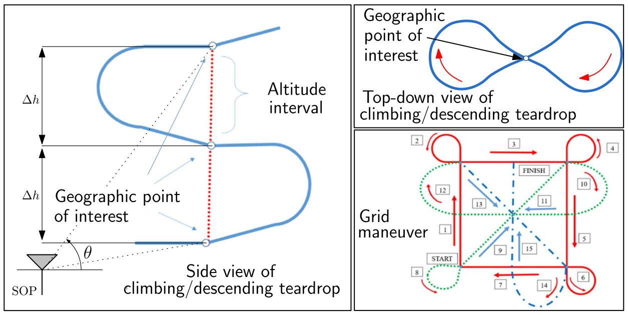


Fig. 10. Maneuvers performed by the C-12 aircraft. The altitude step is denoted by Δh, and θ denotes the elevation angle.

The C-12 flew at altitudes up to 23,000 feet AGL and performed two types of maneuvers. The first was a climbing/descending teardrop-like patterns. These patterns were used to assess the ability to acquire eNodeBs at different altitude and to characterize the CNR. The second was a grid-like pattern with many turns and straight elements. These patterns were used to stress-test the proposed LTE navigation receiver's tracking loops. The navigation solution was computed from the proposed receiver's output and was compared with the aircraft's ground truth, which was obtained from the C-12's on-board Honeywell H764-ACE EGI INS/GPS. Fig. 10 illustrates the maneuvers, where the "geographic point of interest" refers to the "center" of the climbing/descending teardrop, which the aircraft flew through as it ascended/descended vertically in order to assess the received signal as a function of altitude.

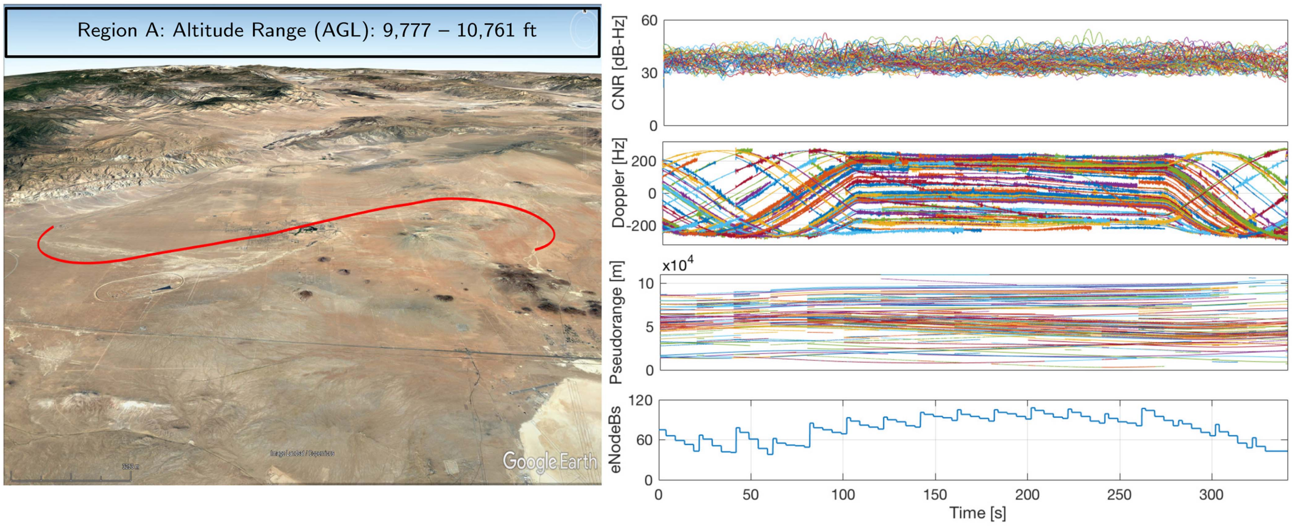


Fig. 11. Left: climbing teardrop aircraft trajectory in Region A. Right: receiver's output: CNR, Doppler, pseudorange, and number of tracked eNodeBs.

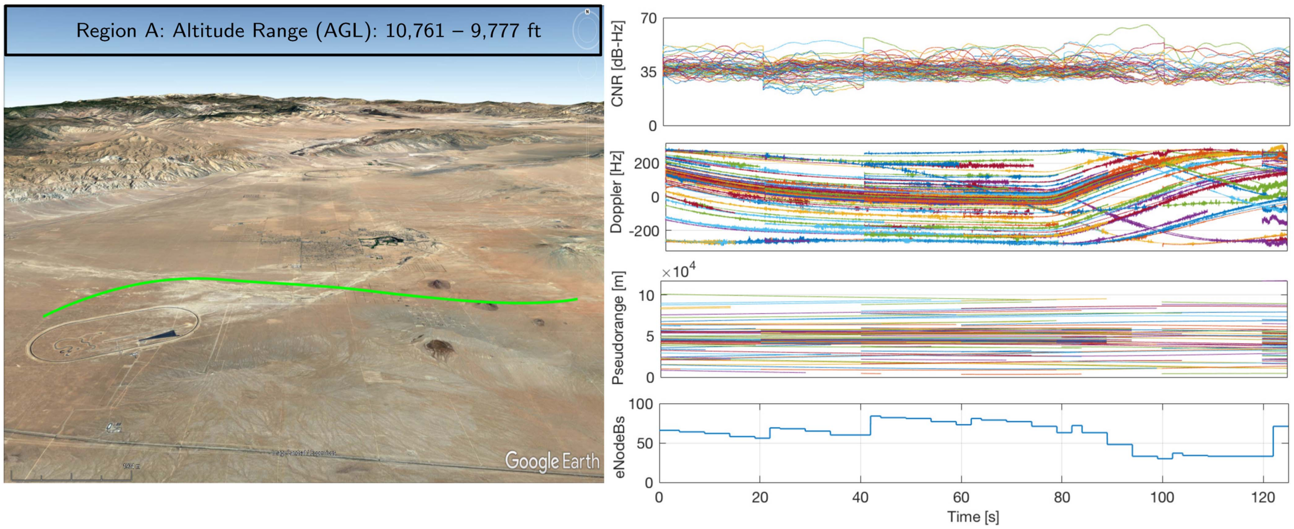


Fig. 12. Left: descending teardrop aircraft trajectory in Region A. Right: receiver's output: CNR, Doppler, pseudorange, and number of tracked eNodeBs.

VII. CELLULAR LTE SIGNAL CHARACTERIZATION

This section presents experimental results evaluating the proposed LTE receiver described in Section V.

The PLL and DLL settings were $\zeta \equiv \frac{1}{\sqrt{2}}$, $B_{n,\text{PLL}} \equiv 12$ Hz, and $B_{n,\text{DLL}} \equiv 0.05$ Hz. Figs. 11–16 show the navigation observables produced by the receiver (pseudorange and Doppler) along with the CNR and number of tracked LTE eNodeBs during various flight trajectories.

The following conclusions can be made from these results. First, as discussed in Section IV, the proposed receiver, by design, possesses much higher sensitivity compared with the receiver used in [50] and [51] (cf., Fig. 5, which compares the ACF of each receiver design). This higher sensitivity enabled the receiver to acquire and track much weaker signals from farther away eNodeBs, increasing the number of hearable eNodeBs by an order of magnitude. Essentially, reprocessing the raw LTE samples, which were used in [51] and [52], increased the acquirable and trackable eNodeBs *from about a dozen to more than 100*. Second, in rural and semiurban regions, no matter the aircraft maneuvers, tens of eNodeBs were simultaneously trackable, some of which were more than 100 km away. A significant factor behind the change in the number of tracked eNodeBs during the aircraft's flight is attributed to the aircraft's body and wings causing signal blockage and severe attenuation during banking. Third, co-channel interference does not seem to be problematic for eNodeBs within tens of kilometers from the aircraft, as the proposed receiver was able to track all such eNodeBs with sufficiently high

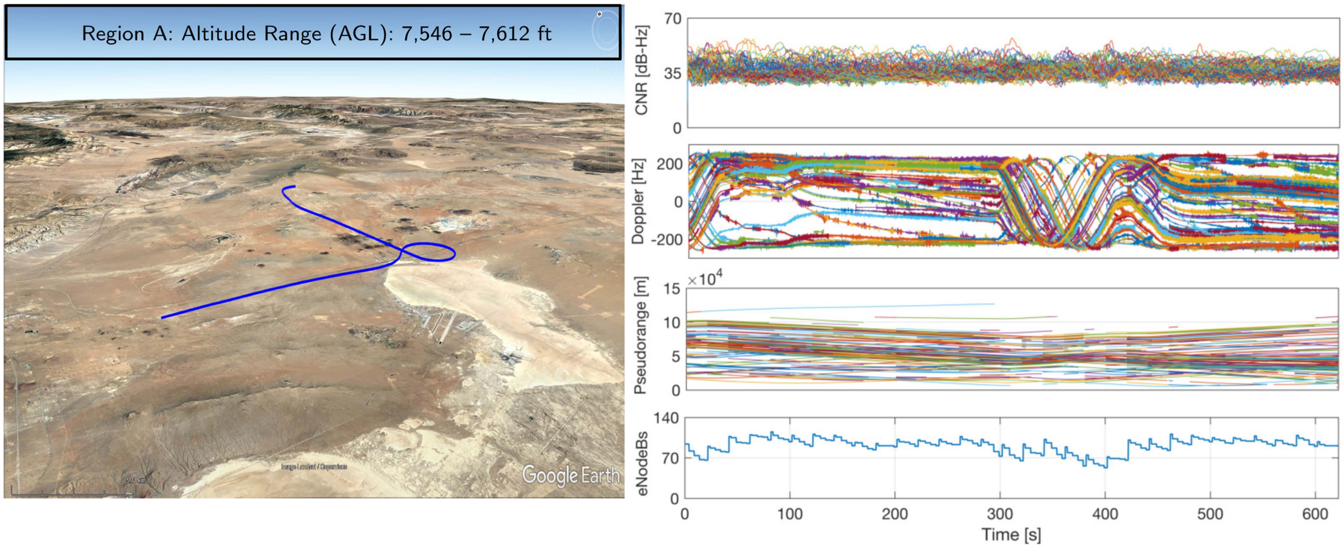


Fig. 13. Left: grid aircraft trajectory in Region A. Right: receiver's output: CNR, Doppler, pseudorange, and number of tracked eNodeBs.

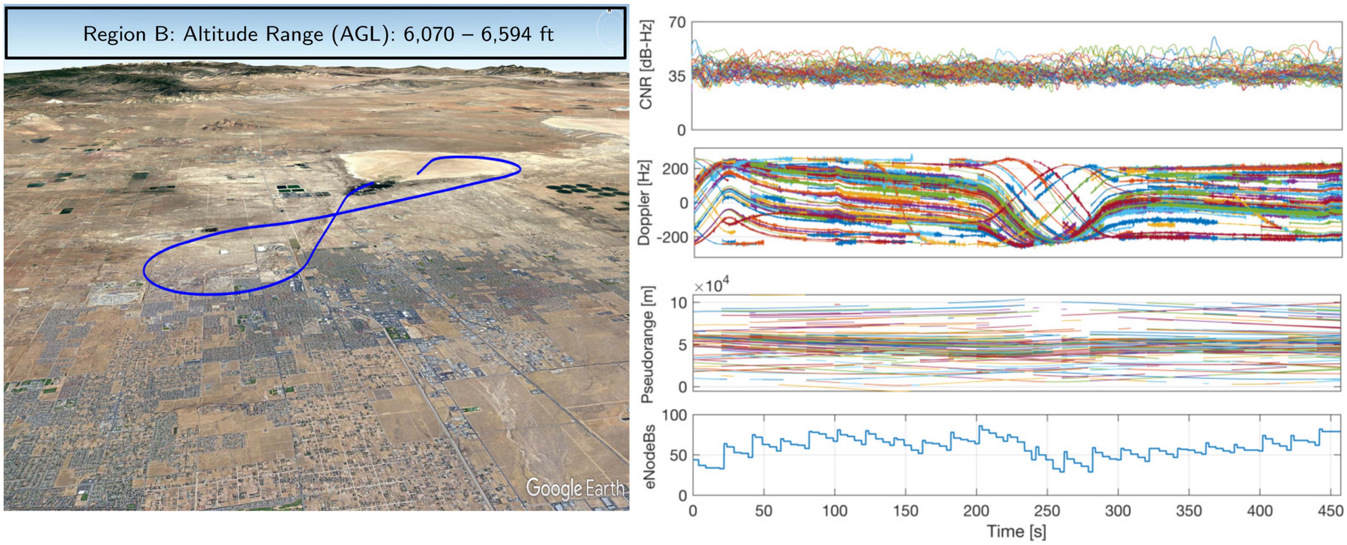


Fig. 14. Left: climbing teardrop aircraft trajectory in Region B. Right: receiver's output: CNR, Doppler, pseudorange, and number of tracked eNodeBs.

CNR. Complete characterization of co-channel interference warrants a study by itself, which is deferred to future work.

VIII. NAVIGATION FRAMEWORK

This section formulates the EKF-based aircraft navigation framework, which will be used to evaluate the navigation observables produced by the proposed receiver. First, the aircraft dynamics and cellular LTE measurement models are described. Next, the EKF model and settings are specified.

A. Aircraft Dynamics Model

Depending on the aircraft's motion and sensor suite, different dynamic models can be used to describe its dynamics. This article aims to assess a baseline performance of aircraft navigation with observables produced exclusively with the proposed cellular receiver. As such, a simple, yet effective continuous Wiener process acceleration model is employed, which upon discretization at a constant sampling interval T, is given by

$$\boldsymbol{x}_{\text{pva}}(k+1) = \mathbf{F}_{\text{pva}}\,\boldsymbol{x}_r(k) + \boldsymbol{w}_{\text{pva}}(k), \quad k = 0, 1, 2, \ldots \quad (4)$$

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

where $\boldsymbol{x}_{\text{pva}} \triangleq [\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, \ddot{\boldsymbol{r}}_r^{\mathsf{T}}]^{\mathsf{T}}$, $\boldsymbol{r}_r \triangleq [x_r, y_r, z_r]^{\mathsf{T}}$ is the 3-D position of the aircraft expressed in a North–East–Down (NED) frame, and $\boldsymbol{w}_{\text{pva}}$ is a discrete-time zero-mean white noise

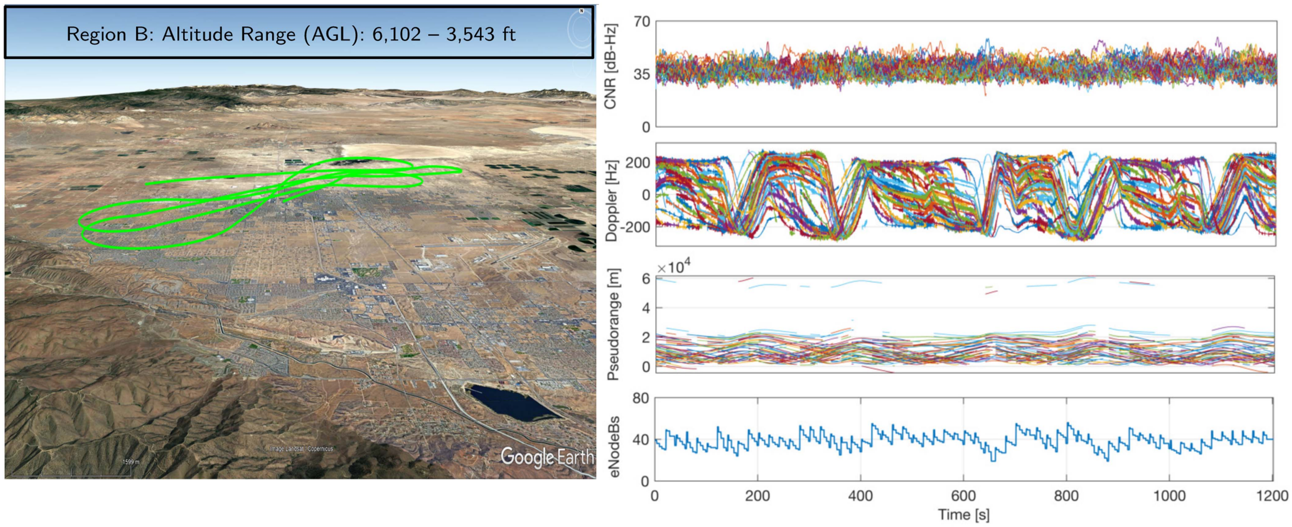


Fig. 15. Left: descending teardrop aircraft trajectory in Region B. Right: receiver's output: CNR, Doppler, pseudorange, and number of tracked eNodeBs.

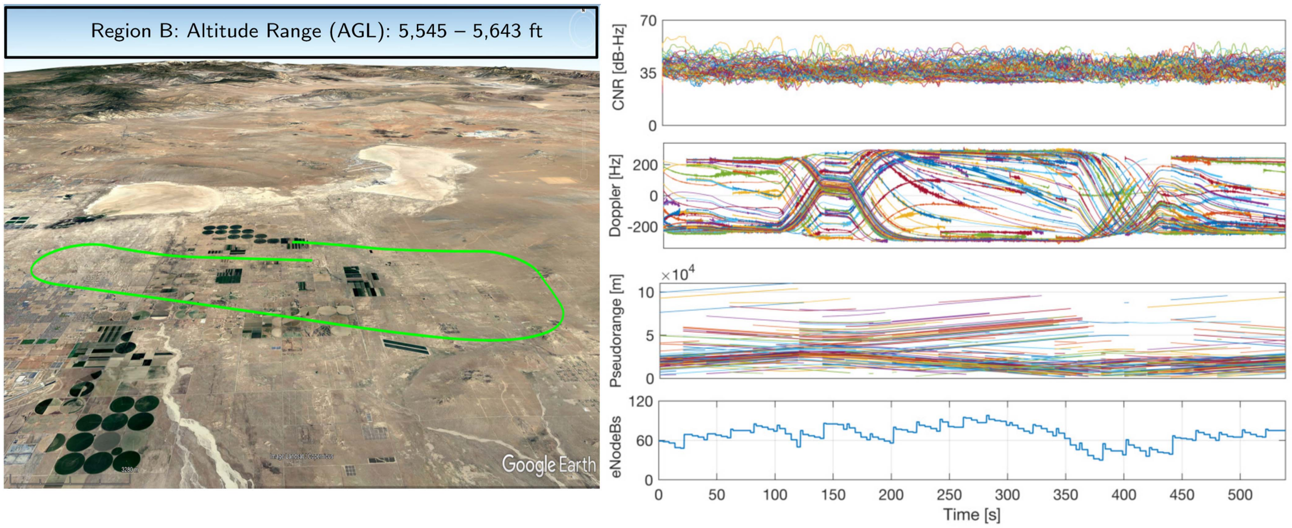


Fig. 16. Left: grid aircraft trajectory in Region B. Right: receiver's output: CNR, Doppler, pseudorange, and number of tracked eNodeBs.

sequence with covariance $\mathbf{Q}_{\text{pva}}$ given by

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

where $\otimes$ denotes the Kronecker product, and $\tilde{\mathbf{S}}_{\text{NED}} \triangleq \text{diag}[\tilde{q}_N, \tilde{q}_E, \tilde{q}_D]$, where $\tilde{q}_N$, $\tilde{q}_E$, and $\tilde{q}_D$ are the NED jerk continuous-time noise power spectra, respectively. It should be noted that more complicated dynamic models can be used to describe the aircraft's dynamics, e.g., Singer acceleration, mean-adaptive acceleration, circular motion, curvilinear motion, and coordinated turn, among others [61]. Of course, if an INS is available, its measurements can be used to describe the aircraft's motion, while aiding the INS with cellular signals [62].

B. Clock Error Dynamics Model

Wireless standards require cellular transmitters to be synchronized to within a few microseconds, which is order of magnitudes higher than the nanosecond requirements in GNSS. As such, the transmitters' clock errors, which are dynamic and stochastic, must be accounted for in the navigation filter. A typical model for the dynamics of the clock error states is the so-called two-state model, composed of the clock bias δt and clock drift $\dot{\delta t}$, given by

$$\boldsymbol{x}_{\text{clk}}(k+1) = \mathbf{F}_{\text{clk}} \boldsymbol{x}_{\text{clk}}(k) + \boldsymbol{w}_{\text{clk}}(k), \tag{5}$$

where $\boldsymbol{w}_{\text{clk}}$ is a discrete-time zero-mean white noise sequence with covariance $\mathbf{Q}_{\text{clk}}$ and

$$\mathbf{F}_{\text{clk}} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \quad \mathbf{Q}_{\text{clk}} = \begin{bmatrix} S_{\tilde{w}_{\delta t}} T + S_{\tilde{w}_{\dot{\delta t}}} \frac{T^3}{3} & S_{\tilde{w}_{\dot{\delta t}}} \frac{T^2}{2} \\ S_{\tilde{w}_{\dot{\delta t}}} \frac{T^2}{2} & S_{\tilde{w}_{\dot{\delta t}}} T \end{bmatrix}. \tag{6}$$

The power spectra $S_{\tilde{w}_{\delta t}}$ and $S_{\tilde{w}_{\dot{\delta t}}}$ are determined by the quality of the oscillator from which the clock signal is derived [63].

C. SOP Measurement Model

In order to get the highest possible precision, carrier phase observables produced by the proposed receiver will be used for navigation, which after some manipulations can be modeled as [33]

$$z_n(k) = \left\| \boldsymbol{r}_r(k) - \boldsymbol{r}_{s_n} \right\|_2 + c\delta t_n(k) + v_n(k), \quad n = 1, 2, \ldots, N, \tag{7}$$

where $\boldsymbol{r}_{s_n}$ is the nth LTE eNodeB's 3-D position vector; c is the speed of light; δt_n is the overall clock error in the nth carrier phase measurement, which combines the effect of receiver and eNodeB clock biases and the initial carrier phase ambiguity; N is the total number of eNodeBs; and $v_n(k)$ is the measurement noise, which is modeled as a discrete-time zero-mean white Gaussian sequence with variance $\sigma_n^2(k)$. The measurement noise variance can be modeled as a function of the CNR [51].

D. Altimeter Measurement Model

Since for a high-flying aircraft, terrestrial cellular transmitters appear to have similar altitudes, their vertical dilution of precision will be very large. To circumvent this issue, and since access to the aircraft's raw altimetry data was unavailable, the measurement-update step in the EKF fused altimeter data z_{alt} was derived from the aircraft's on-board navigation system (Honeywell H764-ACE EGI INS/GPS) with the cellular carrier phase measurements. This yielded altimeter measurements that are more accurate than what is achievable with a typical aviation-grade altimetry systems, in which the standard atmospheric model is known to have larger deviations.

E. EKF Model

Let $\boldsymbol{x} \triangleq [\boldsymbol{x}_{\text{pv}}^{\mathsf{T}}, \boldsymbol{x}_{\text{clk}_1}^{\mathsf{T}}, \ldots, \boldsymbol{x}_{\text{clk}_N}^{\mathsf{T}}]^{\mathsf{T}}$ denote the state to be estimated, where $\boldsymbol{x}_{\text{clk}_n} \triangleq [c\delta t_n, c\dot{\delta t}_n]^{\mathsf{T}}$. Using (4) and (5), one can write the dynamics of $\boldsymbol{x}$ as

$$\boldsymbol{x}(k+1) = \mathbf{F}\boldsymbol{x}(k) + \boldsymbol{w}(k), \tag{8}$$

where $\mathbf{F} \triangleq \text{diag}[\mathbf{F}_{\text{pva}}, \mathbf{F}_{\text{clk}}, \ldots, \mathbf{F}_{\text{clk}}]$, and $\boldsymbol{w}(k)$ is the overall process noise vector, which is a zero-mean white sequence with covariance $\mathbf{Q} \triangleq \text{diag}[\mathbf{Q}_{\text{pva}}, \bar{\mathbf{Q}}_{\text{clk}}]$, and

$$\bar{\mathbf{Q}}_{\text{clk}} \triangleq \begin{bmatrix} \mathbf{Q}_{\text{clk}_r} + \mathbf{Q}_{\text{clk}_{s_1}} & \mathbf{Q}_{\text{clk}_r} & \cdots & \mathbf{Q}_{\text{clk}_r} \\ \mathbf{Q}_{\text{clk}_r} & \mathbf{Q}_{\text{clk}_r} + \mathbf{Q}_{\text{clk}_{s_2}} & \cdots & \mathbf{Q}_{\text{clk}_r} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{Q}_{\text{clk}_r} & \mathbf{Q}_{\text{clk}_r} & \cdots & \mathbf{Q}_{\text{clk}_r} + \mathbf{Q}_{\text{clk}_{s_N}} \end{bmatrix},$$

where $\mathbf{Q}_{\text{clk}_r}$ and $\{\mathbf{Q}_{\text{clk}_{s_n}}\}_{n=1}^{N}$ have the same form as in (6), except that $S_{\tilde{w}_{\delta t}}$ and $S_{\tilde{w}_{\dot{\delta t}}}$ are replaced with the receiver and nth eNodeB's clock process noise spectra, respectively. Note that the cross-correlations in $\bar{\mathbf{Q}}_{\text{clk}}$ come from combining the effect of the receiver and cellular eNodeB clocks in the same state. Since the receiver clock bias is common to all clock states, the cross-correlations in $\bar{\mathbf{Q}}_{\text{clk}}$ will be the receiver clock's process noise covariance [64].

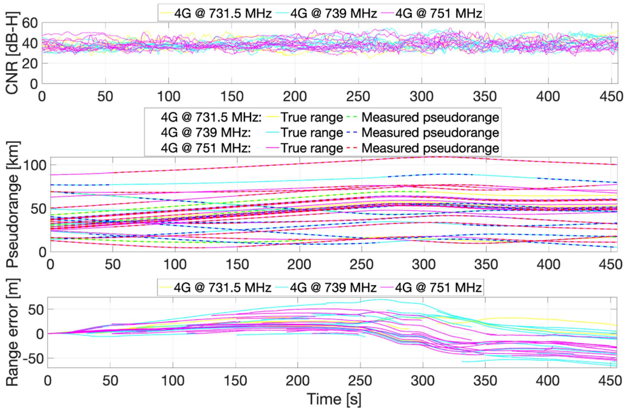


Fig. 17. Region A results. (a) Time history of CNRs for all eNodeBs used to compute the navigation solution in Region A. (b) Time history of pseudoranges estimated by the proposed receiver and corresponding true range. The initial values of the pseudoranges and ranges were subtracted out for ease of comparison. (c) Time history of the pseudorange error (pseudorange minus the true range). The initial values of the pseudorange errors were subtracted out for ease of comparison.

The measurement vector defined by $\boldsymbol{z}(k) \triangleq [z_{\text{alt}}(k), z_1(k), \ldots, z_N(k)]^{\mathsf{T}}$ is used to estimate $\boldsymbol{x}$ in the EKF. In vector form, the measurement equation is given by

$$\boldsymbol{z}(k) = \boldsymbol{h}\left[\boldsymbol{x}(k)\right] + \boldsymbol{v}(k), \tag{9}$$

where $\boldsymbol{h}[\boldsymbol{x}(k)]$ is a vector-valued function defined as $\boldsymbol{h}[\boldsymbol{x}(k)] \triangleq [h_{\text{alt}}[\boldsymbol{x}(k)], h_1[\boldsymbol{x}(k)], \ldots, h_N[\boldsymbol{x}(k)]]^{\mathsf{T}}$ with $h_{\text{alt}}[\boldsymbol{x}(k)] = z_r(k) + v_{\text{alt}}(k)$, $h_n[\boldsymbol{x}(k)] \triangleq \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_n}\|_2 + c\delta t_n(k)$, and $\boldsymbol{v}(k) \triangleq [v_{\text{alt}}(k), v_1(k), \ldots, v_N(k)]^{\mathsf{T}}$ is the measurement noise vector, which is modeled as zero-mean white Gaussian random vector with covariance $\mathbf{R}(k) \triangleq \text{diag}[\sigma_{\text{alt}}^2(k), \sigma_1^2(k), \ldots, \sigma_N^2(k)]$.

Given the dynamics and measurement models in (8) and (9), the EKF produces an estimate of $\boldsymbol{x}(k)$ using all measurements up to time-step k, denoted by $\hat{\boldsymbol{x}}(k|k)$, and an associated estimation error covariance denoted by $\mathbf{P}(k|k)$. The EKF is initialized from two successive position priors obtained from the aircraft's GPS/INS navigation solution, according to the framework discussed in [64]. The EKF process and measurement noise covariances settings are described next.

F. EKF Settings

The measurement rate was $T = 0.01$ s; the jerk process noise spectra were chosen to be $\tilde{q}_N = \tilde{q}_E = 5\ \text{m}^2/\text{s}^5$ and $\tilde{q}_D = 1\ \text{m}^2/\text{s}^5$; and the receiver's and eNodeBs' clock process noise covariance matrices were chosen to be

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

$$\mathbf{Q}_{\text{clk},s_n} = \begin{bmatrix} 3.59 \times 10^{-5} & 3.54 \times 10^{-9} \\ 3.54 \times 10^{-9} & 7.09 \times 10^{-7} \end{bmatrix}. \tag{11}$$

The altimeter measurement error variance $\sigma_{\text{alt}}^2(k)$ was set to 5 m^2. The cellular measurement noise variances were

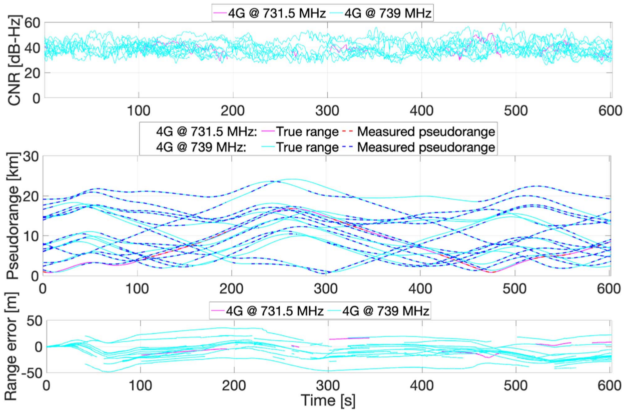


Fig. 18. Region B results. (a) Time history of CNRs for all eNodeBs used to compute the navigation solution in Region A. (b) Time history of pseudoranges estimated by the proposed receiver and corresponding true range. The initial values of the pseudoranges and ranges were subtracted out for ease of comparison. (c) Time history of the pseudorange error (pseudorange minus the true range). The initial values of the pseudorange errors were subtracted out for ease of comparison.

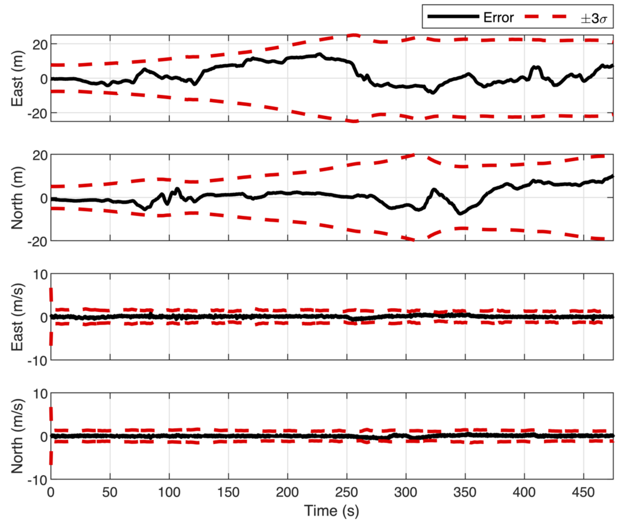


Fig. 19. EKF plots showing the time history of the position and velocity errors in Region A as well as the $\pm 3\sigma$ bounds.

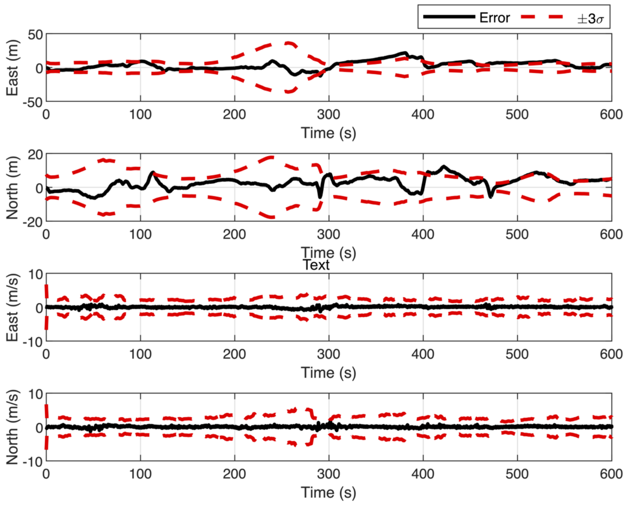


Fig. 20. EKF plots showing the time history of the position and velocity errors in Region B as well as the $\pm 3\sigma$ bounds.

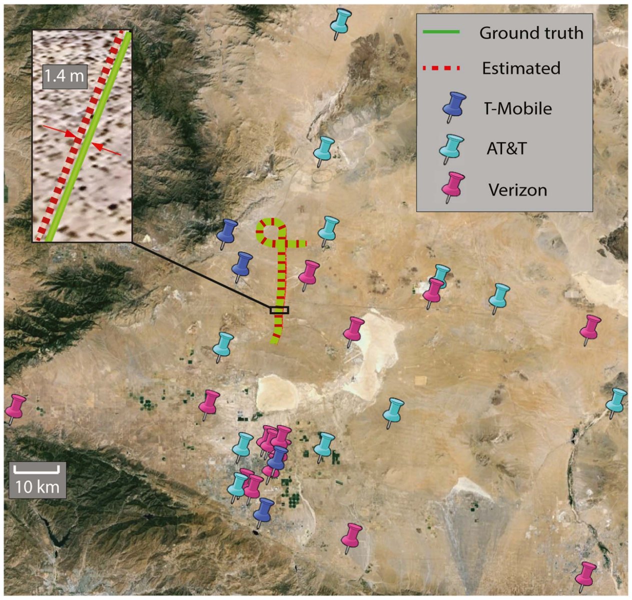


Fig. 21. Experimental environment and aircraft navigation results in Region A showing: eNodeB positions, true aircraft trajectory, and aircraft trajectory estimated using cellular SOPs. The aircraft traversed a total distance of 42.6 km in 455 s during the experiment. The position RMSE over the trajectory was 7.00 m.

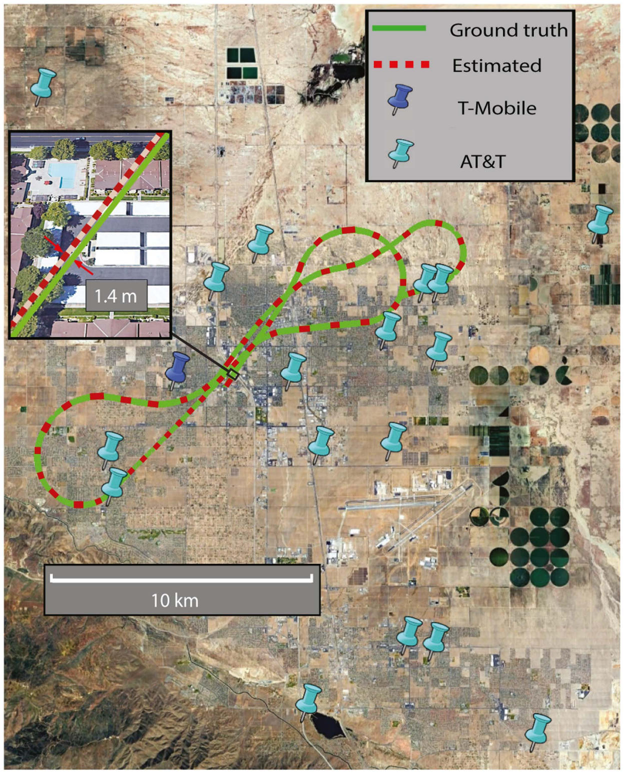


Fig. 22. Experimental environment and aircraft navigation results in Region B showing: eNodeB positions, true aircraft trajectory, and aircraft trajectory estimated using cellular SOPs. The aircraft traversed a total distance of 56.8 km in 601 s during the experiment. The position RMSE over the trajectory was 8.29 m.

TABLE I
Navigation Performance With Cellular LTE Signals

Metric	Region A	Region B
Total number of unique eNodeBs used	32	18
Number of $\{\min, \max\}$ eNodeBs used	17–27	5–17
Cellular frequency (MHz)	731.5 739 751	731.5 739
Flight duration (sec)	455	601
Flight length (km)	42.6	56.8
Altitude AGL (ft)	7,530 – 7,598	3,540 – 4,573
Position RMSE (m)	7.00	8.29
Velocity RMSE (m/s)	0.34	0.41
Position error standard deviation (m)	3.37	4.11
Velocity error standard deviation (m/s)	0.18	0.22
Maximum position error (m)	14.16	21.59
Maximum velocity error (m/s)	3.82	3.20

calculated as a function of the CNR and receiver parameters as discussed in [51]. The values taken by the measurement noise variances ranged between $0.3 - 11.0$ m^2 in Region A and $0.7 - 35.0$ m^2 in Region B.

IX. AIRCRAFT NAVIGATION RESULTS

This section presents aircraft navigation results in regions A and B utilizing the navigation observables produced by the LTE navigation receiver described in Section V, fused with altimeter measurements via the EKF discussed in Section VIII. To this end, given the knowledge of aircraft's trajectory (from its onboard GPS-INS system), LTE eNodeBs were mapped, cross checked via Google Earth, and got associated with the produced pseudoranges to assess the ranging error.

Figs. 17 and 18 show the produced CNR, pseudoranges, and range error to the mapped eNodeBs. Figs. 19 and 20 show the EKF error plots and the $\pm 3\sigma$ bounds. It can be seen from these plots that the EKF errors remain bounded throughout the aircraft's trajectory. The variations in the σ-bounds are due to a combination of: relative geometry between the aircraft and eNodeBs, number of tracked eNodeBs, and model mismatch between the aircraft's maneuvers (especially during banking) and assumed aircraft dynamical model. Figs. 21 and 22 show the aircraft trajectory in Regions A and B and eNodeB positions. Table I summarizes the navigation performance in Regions A and B. It is worth emphasizing that the reported performance is expected to improve if an INS is coupled with the LTE navigation observables (e.g., via a tightly coupled SOP-aided INS [62]) and/or the observables from all tracked eNodeBs are fused in the EKF.

X. CONCLUSION

This article presented a high-sensitivity receiver enabling aircraft navigation with OFDM-based LTE SOPs. The proposed approach was tested on LTE samples recorded on an aircraft during the SNIFFER flight campaign. It was shown that while a previous state-of-the-art LTE navigation SDR was able to acquire and track five LTE eNodeBs in two flight regions, upon reprocessing the LTE samples with the proposed receiver, the number of acquirable/trackable eNodeBs grew *dramatically* to more than 100, some of which were more than 100 km away. Upon fusing the carrier phase observables with altimeter data via an EKF, a sustained accurate navigation solution was achieved. Over trajectories of 43.6 and 56.8 km, traversed in 455 and 601 s, a 3-D position RMSE of 6.8 and 8.2 m was achieved by exploiting an average of about 22 and 11 eNodeBs, respectively.

While the results revealed in this article are promising for aircraft navigation, particular needs of military operations versus civil aviation (e.g., low-altitude urban air mobility) must be addressed if cellular SOPs are to be used in practice. For instance, while this article focused on showing that the ranging/accuracy aspects, issues of integrity, availability, and continuity were not studied and warrant further studies. In addition, how can we deal with potentially irreconcilable conflicts between the long timeline of civil aviation operation versus the short timeline of cellular technology? What commitments should we require from governing bodies (e.g., 3GPP) or local cellular operators? The authors hope that this article will initiate a robust discussion by standards bodies, government agencies, and aviation stakeholders into utilizing (or dual-purposing) the existing cellular infrastructure as a complementary PNT solution.

ACKNOWLEDGMENT

The authors would like to thank Edwards AFB and Holloman AFB for inviting the ASPIN Laboratory to conduct experiments on Air Force aircraft in the “SNIFFER: Signals of opportunity for Navigation In Frequency-Forbidden EnviRonments” flight campaign. The authors would also like to thank Joshua Morales, Kimia Shamaei, Mahdi Maaref, Kyle Semelka, MyLinh Nguyen, and Trier Mortlock for their help with preparing for data collection and Ali Kaiss for his help with data processing. Distribution Statement A. Approved for public release; Distribution is unlimited 412TW-PA-20146.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. This article describes objective technical results and analysis. Any subjective views or opinions that might be expressed in this article do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

REFERENCES

[1] ASRS/NASA, “ASRS database online.” Accessed: Apr. 15, 2023. [Online]. Available: https://asrs.arc.nasa.gov/search/database.html

[2] E. Blasch et al., “Cyber awareness trends in avionics,” in *Proc. IEEE/AIAA Digit. Avionics Syst. Conf.*, 2019, pp. 1–8.

[3] EUROCONTROL, Aviation Intelligence Unit, “Does radio frequency interference to satellite navigation pose an increasing threat to network efficiency, cost-effectiveness and ultimately safety?,” 2021. [Online]. Available: https://www.eurocontrol.int/sites/default/files/2021-03/eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf

[4] International Civil Aviation Organization (ICAO), “An urgent need to address harmful interferences to GNSS,” 2019. [Online]. Available: https://www.iata.org/contentassets/e45e5219cc8c4277a0e80562590793 da/address-harmful-interferences-gnss.pdf

[5] International Civil Aviation Organization (ICAO), “Strengthening of communications, navigation, and surveillance (CNS) systems resilience and mitigation of interference to Global Navigation Satellite System (GNSS),” 2020. [Online]. Available: https://rntfnd.org/wp-content/uploads/ICAO-Letter-GNSS-Resilience-Aug-2020.pdf

[6] M. Bartock et al., “Foundational PNT profile: Applying the cybersecurity framework for the responsible use of positioning, navigation, and timing (PNT) services,” National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Tech. Rep. NISTIR 8323, Feb. 2021.

[7] J. Raquet et al. *Position, Navigation, and Timing Technologies in the 21st Century*, J. Morton, F. van Diggelen, J. Spilker, Jr., and B. Parkinson, Eds., vol. 2. New York, NY, USA: Wiley, 2021, pp. 1115–1412.

[8] J. del Peral-Rosado et al., “Evaluation of hybrid positioning scenarios for autonomous vehicle applications,” in *Proc. ION Int. Tech. Meeting Conf.*, 2017, pp. 2541–2553.

[9] N. Ikhtiari, “Navigation in GNSS denied environments using software defined radios and LTE signals of opportunities,” Master’s thesis, Dept. Elect. Comput. Eng., Univ. Canterbury, Christchurch, New Zealand, 2019.

[10] J. Gante, L. Sousa, and G. Falcao, “Dethroning GPS: Low-power accurate 5G positioning systems using machine learning,” *IEEE Trans. Emerg. Sel. Topics Circuits Syst.*, vol. 10, no. 2, pp. 240–252, Jun. 2020.

[11] Z. Kassas, “Navigation with cellular signals of opportunity,” in *Position, Navigation, and Timing Technologies in the 21st Century*, vol. 2, J. Morton, F. van Diggelen, J. Spilker, Jr., and B. Parkinson, Eds., Wiley-IEEE, 2021, ch. 38, pp. 1171–1223.

[12] N. Souli, P. Kolios, and G. Ellinas, “Online relative positioning of autonomous vehicles using signals of opportunity,” *IEEE Trans. Intell. Veh.*, vol. 7, no. 4, pp. 873–885, Dec. 2022.

[13] 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*, vol. 22, no. 1, pp. 101–118, 2021.

[14] A. Abdallah, J. Khalife, and Z. Kassas, “Experimental characterization of received 5G signals carrier-to-noise ratio in indoor and urban environments,” in *Proc. IEEE Veh. Technol. Conf.*, 2021, pp. 1–5.

[15] G. Fokin and D. Volgushev, “Software-defined radio network positioning technology design. Problem statement,” in *Proc. Syst. Signals Generating Process. Field Board Commun.*, 2022, pp. 1–6.

[16] H. Chen and H. Wymeersch, “Phone signals can help you find your way in cities even without GPS,” *Nature*, vol. 611, pp. 454–455, Nov. 2022.

[17] A. Ivanov, D. Koshnicharova, K. Tonchev, and V. Poulkov, “Localization in cellular and heterogeneous networks for 5 G and beyond: A review,” *J. Mobile Multimedia*, vol. 19, no. 1, pp. 47–72, 2023.

[18] 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*, vol. 6, pp. 25185–25199, 2018.

[19] 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 *Proc. Int. Conf. Control Autom. Syst.*, 2019, pp. 1182–1186.

[20] P. Gadka, J. Sadowski, and J. Stefanski, “Detection of the first component of the received LTE signal in the OTDoA method,” *Wireless Commun. Mobile Comput.*, pp. 1–12, Apr. 2019.

[21] S. Han, T. Kang, and J. Seo, “Smartphone application to estimate distances from LTE base stations based on received signal strength measurements,” in *Proc. Int. Tech. Conf. Circuits/Syst. Comput. Commun.*, 2019, pp. 1–3.

[22] K. Shamaei and Z. Kassas, “A joint TOA and DOA acquisition and tracking approach for positioning with LTE signals,” *IEEE Trans. Signal Process.*, vol. 69, pp. 2689–2705, 2021.

[23] J. Mortier, G. Pages, and J. Vila-Valls, “Robust TOA-based UAS navigation under model mismatch in GNSS-denied harsh environments,” *Remote Sens.*, vol. 12, no. 18, pp. 2928–2947, Sep. 2020.

[24] 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 *Proc. Int. Conf. Unmanned Aircr. Syst.*, 2021, pp. 229–236.

[25] T. Kazaz, G. Janssen, J. Romme, and A. Van der Veen, “Delay estimation for ranging and localization using multiband channel state information,” *IEEE Trans. Wireless Commun.*, vol. 21, no. 4, pp. 2591–2607, Apr. 2022.

[26] C. Yang, M. Arizabaleta-Diez, P. Weitkemper, and T. Pany, “An experimental analysis of cyclic and reference signals of 4G LTE for TOA estimation and positioning in mobile fading environments,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 37, no. 9, pp. 16–41, Sep. 2022.

[27] P. Wang and Y. Morton, “Impact analysis of inter-cell interference in cellular networks for navigation applications,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 1, pp. 685–694, Feb. 2023.

[28] A. Abdallah and Z. Kassas, “Multipath mitigation via synthetic aperture beamforming for indoor and deep urban navigation,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 8838–8853, Sep. 2021.

[29] K. Strandjord, Y. Morton, and P. Wang, “Evaluating the urban signal environment for GNSS and LTE signals,” in *Proc. ION GNSS Conf.*, 2021, pp. 2166–2182.

[30] R. Whiton, J. Chen, T. Johansson, and F. Tufvesson, “Urban navigation with LTE using a large antenna array and machine learning,” in *Proc. IEEE Veh. Technol. Conf.*, 2022, pp. 1–5.

[31] M. Pan et al., “Efficient joint DOA and TOA estimation for indoor positioning with 5G picocell base stations,” *IEEE Trans. Instrum. Meas.*, vol. 71, 2022, Art. no. 8005219.

[32] Z. Liu, L. Chen, X. Zhou, N. Shenand, and R. Chen, “Multipath tracking with LTE signals for accurate TOA estimation in the application of indoor positioning,” *Geo-Spatial Inf. Sci.*, vol. 26, no. 1, pp. 31–43, 2023.

[33] 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 Aerosp. Electron. Syst. Mag.*, vol. 37, no. 7, pp. 4–19, Jul. 2022.

[34] J. del Peral-Rosado et al., “Physical-layer abstraction for hybrid GNSS and 5G positioning evaluations,” in *Proc. IEEE Veh. Technol. Conf.*, 2019, pp. 1–6.

[35] A. Soderini, P. Thevenon, C. Macabiau, L. Borgagni, and J. Fischer, “Pseudorange measurements with LTE physical channels,” in *Proc. ION Int. Tech. Meeting*, 2020, pp. 817–829.

[36] T. Hong, J. Sun, T. Jin, Y. Yi, and J. Qu, “Hybrid positioning with DTMB and LTE signals,” in *Proc. Int. Wireless Commun. Mobile Comput.*, 2021, pp. 303–307.

[37] M. Maaref and Z. Kassas, “Autonomous integrity monitoring for vehicular navigation with cellular signals of opportunity and an IMU,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 6, pp. 5586–5601, Jun. 2022.

[38] J. Khalife and Z. Kassas, “On the achievability of submeter-accurate UAV navigation with cellular signals exploiting loose network synchronization,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 5, pp. 4261–4278, Oct. 2022.

[39] J. Khalife and Z. Kassas, “Differential framework for submeter-accurate vehicular navigation with cellular signals,” *IEEE Trans. Intell. Veh.*, vol. 8, no. 1, pp. 732–744, Jan. 2023.

[40] W. Xu, M. Huang, C. Zhu, and A. Dammann, “Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system,” *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 3, pp. 339–356, 2016.

[41] K. Shamaei and Z. Kassas, “Sub-meter accurate UAV navigation and cycle slip detection with LTE carrier phase measurements,” in *Proc. ION GNSS Conf.*, 2019, pp. 2469–2479.

[42] P. Wang and Y. Morton, “Multipath estimating delay lock loop for LTE signal TOA estimation in indoor and urban environments,” *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5518–5530, Aug. 2020.

[43] H. Dun, C. Tiberius, and G. Janssen, “Positioning in a multipath channel using OFDM signals with carrier phase tracking,” *IEEE Access*, vol. 8, pp. 13011–13028, 2020.

[44] C. Yang, T. Pany, and P. Weitkemper, “Effect of antenna ports on TOA estimation with 4 G LTE signals in urban mobile environments,” in *Proc. ION GNSS Conf.*, 2020, pp. 2166–2181.

[45] P. Wang, Y. Wang, and J. Morton, “Signal tracking algorithm with adaptive multipath mitigation and experimental results for LTE positioning receivers in urban environments,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 4, pp. 2779–2795, Aug. 2022.

[46] M. Driusso, C. Marshall, M. Sabathy, F. Knutti, H. Mathis, and F. Babich, “Vehicular position tracking using LTE signals,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3376–3391, Apr. 2017.

[47] I. Lapin, G. Granados, J. Samson, O. Renaudin, F. Zanier, and L. Ries, “STARE: Real-time software receiver for LTE and 5 G NR positioning and signal monitoring,” in *Proc. Workshop Satell. Navigation Technol.*, 2022, pp. 1–11.

[48] E. Kim and Y. Shin, “Feasibility analysis of LTE-based UAS navigation in deep urban areas and DSRC augmentation,” *Sensors*, vol. 19, no. 9, pp. 4192–4207, Apr. 2019.

[49] B. Stevens and M. Younis, “Detection algorithm for cellular synchronization signals in airborne applications,” *IEEE Access*, vol. 9, pp. 55555–55566, 2021.

[50] Z. Kassas et al., “Received power characterization of terrestrial cellular signals on high altitude aircraft,” in *Proc. IEEE Aerosp. Conf.*, 2022, pp. 1–8.

[51] Z. Kassas et al., “Assessment of cellular signals of opportunity for high-altitude aircraft navigation,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 37, no. 10, pp. 4–19, Oct. 2022.

[52] Z. Kassas et al., “Flight demonstration of high altitude aircraft navigation with cellular signals,” *IEEE Intell. Transp. Syst. Mag.*, vol. 15, no. 4, pp. 150–165, Jul./Aug. 2023.

[53] K. Shamaei and Z. Kassas, “LTE receiver design and multipath analysis for navigation in urban environments,” *J. Inst. Navigation*, vol. 65, no. 4, pp. 655–675, Dec. 2018.

[54] J. Khalife, K. Shamaei, and Z. Kassas, “Navigation with cellular CDMA signals–part I: Signal modeling and software-defined receiver design,” *IEEE Trans. Signal Process.*, vol. 66, no. 8, pp. 2191–2203, Apr. 2018.

[55] Z. Kassas et al., “Protecting the skies: GNSS-less aircraft navigation with terrestrial cellular signals of opportunity,” in *Proc. ION GNSS Conf.*, 2022, pp. 1014–1025.

[56] X. Lin et al., “The sky is not the limit: LTE for unmanned aerial vehicles,” *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 204–210, Apr. 2018.

[57] 3GPP, “Evolved universal terrestrial radio access (E-UTRA); physical channels and modulation,” *3rd Gener. Partnership Project (3GPP)*, Tech. Rep. TS 36.211, 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36211.htm

[58] 3GPP, “Evolved universal terrestrial radio access (E-UTRA); user equipment (UE) radio transmission and reception,” *3rd Gener. Partnership Project (3GPP)*, Tech. Rep. TS 136. 101, Jun. 2011. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/36101.htm

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

[60] M. Braasch and A. Dempster, “Tutorial: GPS receiver architectures, front-end and baseband signal processing,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 34, no. 2, pp. 20–37, Feb. 2019.

[61] X. Li and V. Jilkov, “Survey of maneuvering target tracking. Part I: Dynamic models,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 39, no. 4, pp. 1333–1364, Oct. 2003.

[62] J. Morales and Z. Kassas, “Tightly-coupled inertial navigation system with signals of opportunity aiding,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 3, pp. 1930–1948, Jun. 2021.

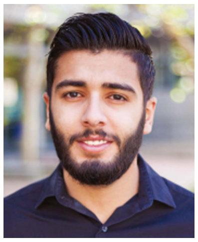
[63] J. Barnes et al., “Characterization of frequency stability,” *IEEE Trans. Instrum. Meas.*, vol. 20, no. 2, pp. 105–120, May 1971.

[64] J. Khalife and Z. Kassas, “Opportunistic UAV navigation with carrier phase measurements from asynchronous cellular signals,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 4, pp. 3285–3301, Aug. 2020.

Zaher M. Kassas (Fellow, IEEE) received the B.E. degree (with Honors) in electrical engineering from Lebanese American University, Beirut, Lebanon, the M.S. degree in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, and the M.S.E. degree in aerospace engineering and the Ph.D. degree in electrical and computer engineering from The University of Texas at Austin, Austin, Texas.

He is the TRC Endowed Chair in intelligent transportation systems, Professor of electrical and computer engineering with The Ohio State University, and Director of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He is also Director of the U.S. Department of Transportation Center: CARMEN (Center for Automated Vehicle Research with Multimodal AssurEd Navigation), focusing on navigation resiliency and security of highly automated transportation systems. His research interests include cyber-physical systems, navigation systems, and intelligent transportation systems.

Dr. Kassas was the recipient of the National Science Foundation (NSF) CAREER award, Office of Naval Research (ONR) Young Investigator Program (YIP) award, Air Force Office of Scientific Research (AFOSR) YIP award, IEEE Walter Fried Award, Institute of Navigation (ION) Samuel Burka Award, ION Col. Thomas Thurlow Award, and IEEE Harry Rowe Mimno Award. He is an Associate Editor for IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS and a Senior Editor for IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. He is a Fellow of the ION, and a Distinguished Lecturer of the IEEE Aerospace and Electronic Systems Society.



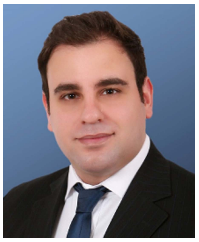
Ali A. Abdallah (Student Member, IEEE) received the B.E. in electrical engineering from the Lebanese American University, Beirut, Lebanon, and the M.S. and Ph.D. degrees from the Department of Electrical Engineering and Computer Science, University of California, Irvine, CA, USA.

He was a Member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory.

Mr. Abdallah was the recipient of the Best Student Paper Award at the 2020 IEEE/ION Position, Location, and Navigation Symposium (PLANS).

Shaghayegh Shahcheraghi (Student Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Shiraz University, Shiraz, Iran, and the M.S. degree in telecommunication engineering from Politecnico Di Milano, Milan, Italy. She is currently working toward the Ph.D. degree in electrical and computer engineering with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH, USA.

She is currently a Member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. Her research interests include cognitive sensing, 5G, and opportunistic navigation.



Joe J. Khalife (Member, IEEE) received the B.E. degree in electrical engineering and the M.S. degree in computer engineering from Lebanese American University, Beirut, Lebanon, and the Ph.D. degree in electrical engineering and computer science from the University of California, Irvine, CA, USA.

He was a Postdoctoral Fellow with the University of California and a Member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory.

Dr. Khalife was the recipient of 2016 IEEE/ION Position, Location, and Navigation Symposium (PLANS) Best Student Paper Award, 2018 IEEE Walter Fried Award, and 2021 IEEE AESS Robert T. Hill Best Dissertation Award.

Chiawei Lee received the B.S. degree in aerospace engineering from the University of California, Los Angeles, CA, USA, and the M.S. degree in aero/astro engineering from Stanford University, Stanford, CA.

He is an Assistant Professor and an Instructor Flight Test Engineer with U.S. Air Force Test Pilot School, Edwards, OH, USA. He is currently the Test Management Program Director where he oversees about a dozen student and staff led flight test projects each year. In addition, he is the Chief Test Safety Officer responsible for the safe execution of curriculum and flight test project safety packages.

Juan Jurado (Member, IEEE) received the B.S. degree in electrical engineering from Texas A&M University, College Station, TX, USA, the M.S. degree in electrical engineering from the Air Force Test Pilot School, Edward, CA, USA, and the M.S. degree in flight test engineering and Ph.D. degree in electrical engineering from the Air Force Institute of Technology, Wright-Patterson AFB, OH, USA.

Previously, he was the Director of Engineering for the 413th Flight Test Squadron and oversaw various C-130, V-22, and H-1 flight test programs. He is a U.S. Air Force Lieutenant Colonel and the Director of Education with the U.S. Air Force Test Pilot School. His research interests include aircraft performance modeling, online sensor calibration, image processing, visual–inertial navigation, and statistical sensor management for multisensor navigation problems.

Steven Wachtel received the B.S. degree in mechanical engineering from The Ohio State University, Columbus, OH, USA, the M.S. degree in flight test engineering from the U.S. Air Force Test Pilot School, Edwards, CA, USA, and the M.S. degree in systems engineering from the Air Force Institute of Technology, Dayton, OH, USA.

He is a U.S. Air Force Captain and a Flight Test Engineer, assigned to the 780th Test Squadron, Eglin AFB, Valparaiso, FL, USA.

Jacob Duede received the B.S. degree in mechanical engineering from the U.S. Air Force Academy, Washington, DC, USA, the M.S. degree in engineering from the University of Arkansas, Fayetteville, AR, USA, the M.S. degree in flight test engineering from Air University. In 2020, he graduated from the U.S. Air Force Test Pilot School at Edwards Air Force Base, CA.

He was trained as a Communication/Navigation/Mission Systems apprentice on C-17 Globmaster II aircraft and stationed at McChord Air Force Base, WA. He was a Commissioned Officer with the U.S. Air Force Academy. He attended the Undergraduate Pilot Training with Columbus Air Force Base, MS, USA. He is a Major with the U.S. Air Force. He is a Senior Pilot with more than 2000 hours.

Zachary Hoeffner received the B.S. degree in nuclear engineering from the U.S. Air Force Academy, Washington, DC, USA, the M.S. degree in flight test engineering from the U.S. Air Force Test Pilot School, Edwards, CA, USA, and the M.S. degrees in engineering physics and applied physics, and nuclear engineering from the Air Force Institute of Technology.

He is a Flight Test Engineer with the U.S. Air Force.

Thomas Hulsey received the B.S. degree in aerospace engineering from the Missouri University of Science and Technology, Rolla, MO, USA, the M.S. degree in aeronautical engineering from the Air Force Institute of Technology, Dayton, OH, USA, and the M.S. degree in experimental flight test engineering from the United States Air Force Test Pilot School, Edwards, CA, USA.

He is a U.S. Air Force Flight Commander of operations engineering.

Rachel Quirarte received the B.S. degree in aeronautical engineering from the U.S. Air Force Academy, Washington, DC, USA, the M.S. degree in flight test engineering from the U.S. Air Force Test Pilot School, Edwards, CA, USA, and the M.S. degree in mechanical engineering from Rice University, Houston, TX, USA.

She is a KC-46 and KC-135 Programmatic Flight Commander and Test Pilot with the 418th Flight Test Squadron, U.S. Air Force.

RunXuan Tay received the B.S. degree in electrical engineering from the University of California, San Diego, CA, USA, and the M.S. degree in flight test engineering from the U.S. Air Force Test Pilot School, Edwards, CA.

He is currently a Test Pilot with the Air Warfare Center, Republic of Singapore Air Force, where he works on fixed wing test programs.