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

Mohammad Neinavaie, Student Member, IEEE, and Zaher M. Kassas, Senior Member, IEEE

Abstract—A receiver architecture for cognitive sensing and navigation with orthogonal frequency division multiplexing (OFDM)-based systems is proposed. The proposed receiver enables exploiting all the transmitted periodic beacon signals of 5G new radio (NR) and Starlink low Earth orbit (LEO) signals to draw navigation observables. Reference signals (RSs) of modern OFDM-based systems, such as 5G NR, contain both always-on and on-demand components. These components can be unknown or known but subject to change. To leverage all transmitted signals for navigation purposes, the RS signals should be detected and tracked cognitively. Similar to conventional navigation receivers, the proposed architecture involves acquisition and tracking stages. However, both stages are supplemented by the unorthodox capability of estimating and updating the RS signals. The acquisition stage instructs the tracking stage by reporting performance metrics, which are used to adjust the tracking loop gains to update the RS accordingly. A chirp model is considered 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 frame length estimation is analyzed. 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 in a blind fashion for navigation purposes, achieving a two-dimensional (2D) root-mean squared error (RMSE) of 4.2 m over a total trajectory of 416 m; (ii) enabling a ground vehicle that traversed a trajectory of 1.79 km to cognitively sense an unknown gNB (blindly detect, track, and exploit transmitted always-on and on-demand signals), localizing it with a 2D error of 5.83 m; and (iii) tracking Starlink LEO OFDM signals, producing Doppler measurements, which were fused to localize a stationary receiver with a 2D error of 6.5 m, starting from an initial estimate 179 km away from the receiver’s true position.

I. 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 [1]. Several features in 5G and beyond cellular networks depend on the ability to localize the user equipment (UE) to a high degree of accuracy [2]. 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 [3].

Similar to 4G long-term evolution (LTE), 5G new radio (NR) adopts orthogonal frequency division multiplexing (OFDM) [4]. In addition, new constellations of broadband low Earth orbit (LEO) space vehicles (SVs) will transmit OFDM-type signals [5]. 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 [6]. 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 [7]. 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 [8].

Navigation receivers typically rely on known RSs transmitted by the sources to draw TOA, DOA, and FOA measurements [9]. 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 [10] 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 [11]. 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 [12], [13].

The problem of cognitively exploiting on-demand and
always-on 5G NR signals has been previously studied in [10], [14], [15]. These methods rely on the difference between the Doppler frequencies of received signals 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:** When the receiver and 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 paper 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 sources 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 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 author’s knowledge, this link between the acquisition and tracking stages is not considered in both classic GNSS receivers, e.g., [16], [17], and the state-of-the-art joint detection and tracking techniques, e.g., [10]. One of the contributions of this paper 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 179 km away, the final 2D error converges to 6.5 m.

The rest of this paper is organized as follows. Section II surveys relevant related work. Section III presents the received baseband signal model. Section IV presents different stages of the proposed receiver. Section V presents experimental results for the utilization of the adaptive cognitive receiver in UAV navigation. Section VI gives concluding remarks.

II. Related Work

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

1) Positioning with 5G NR: Positioning with 5G signals has been studied in the literature [18]–[23]. 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 [24]. 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 [25]. Since beamforming in 5G requires the knowledge of the user’s location, 5G-based positioning is essential for resource allocation [26]. The signal characteristics of mmWave for positioning were studied in [27]. [2] focuses on the integrated positioning methodology of GNSS and device-to-device (D2D) measurements in 5G communication networks. In [20], 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 [28] 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 paper 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.

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 [29]–[32]. 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 [33], [34]. Preliminary results for navigation with partially known signals from low and medium Earth orbit satellites were conducted in [12], [13], [35]. In particular, a chirp parameter estimator was used in [35] to blindly estimate the GPS pseudorandom noise (PRN) codes.

In [10], [14], 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 paper, 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.

3) Navigation with Starlink LEO SV Signals: The first positioning results with Starlink SV signals were presented in [36]–[38]. These papers exploited a train of pure tones in the downlink of Starlink SV signals to provide carrier-phase and Doppler measurements. Starlink downlink signals occupy 250 MHz bandwidth of the Ku-band to provide a high-rate broadband connectivity [8]. In this paper, 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.

III. SIGNAL MODEL

A. 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 [7]. Due to the high Doppler dynamics in LEO satellites, a smaller frame length should be selected to avoid Doppler spread [39]. 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. 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. 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 IV-A.

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 [7]. 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. 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.

B. 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.

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

The channel between the $i$th source and the UE is considered to have a single tap with the complex channel gain $\alpha_i$. The received baseband signal samples can be modeled as

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

where $r[n]$ is the received signal at the $n$th time instant; $\alpha_i[n]$ represents the channel delay corresponding to the UE and the $i$th source at the $n$th time instant; $\tau_i[n]$ is the code-delay corresponding to the UE and the $i$th source at the $n$th time instant, and $\tau_i$ is the sampled 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 $i$th 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 $n$th time instant and $T_s$ is the sampling time; $d_i[n]$ represents the samples of some transmitted from the $i$th source; and $w[n]$ is a zero-mean independent and identically distributed noise with $\mathbb{E}\left\{ w[n]w^*[n] \right\} = \sigma^2_n \delta(m-n)$, where $\delta[m]$ 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 $i$th source, denoted by $s_i[n]$, and the equivalent noise, denoted by $w_{eq_i}$, which are defined as

$$s_i[n] = \alpha_i c_i[\tau_n - t_s[n]] \exp(j\theta_i[\tau_n]),$$

$$w_{eq_i}[n] = d_i[\tau_n - t_s[n]] \exp(j\theta_i[\tau_n]) + w[n].$$

Hence, the baseband samples can be rewritten as

$$r[n] = \sum_{i=1}^{N} (s_i[n] + w_{eq_i}[n]).$$

Remark 1: In this paper, the Doppler frequency is modeled as a linear chirp, i.e., $f_{D_i}[n] = f_{D_{0i}}[n] + \beta_i[n]T_s n$, where $f_{D_{0i}}[n]$ 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 $f_{D_{0i}}[n]$, Doppler rate $\beta_i[n]$, delay $t_s[n]$, and channel gains $\alpha_i$ are considered to be constant.

IV. Receiver Architecture

This section describes the proposed receiver.

A. 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 [6].

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 [6]

$$A_c(m, n) = \frac{1}{L} \sum_{k=0}^{L-1} c[m+k]c^*[k]\exp\left(-\frac{j2\pi kn}{L}\right).$$

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 [7]. 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 gives a closed-form solution for the autocorrelation function in the presence of Doppler rate.

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

$$R_{rr}[m] = \bar{\alpha}_i \tilde{A}_c(m, 0) \sin\left(\frac{2\pi \beta T^2_s mL'}{\sin(\frac{2\pi \beta T^2_s m})}\right) + R_{ww}[m],$$

where $|\bar{\alpha}_i| = 1$, $\tilde{A}_c(m, 0) = \mathbb{E}\{A_c(m, 0)\}$ is the expected value of the periodic ambiguity function of the RS corresponding to the $i$th satellite and $R_{ww}[m]$ is the autocorrelation function of noise.

Proof: See Appendix A.

Note that the term $\frac{\sin(2\pi \beta T^2_s mL')}{\sin(2\pi \beta T^2_s m)}$ in (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 $\tilde{A}_c(m, 0)$ contains a periodic train of impulse-like functions with a period of $L$ samples (the RS period). For a nonzero Doppler rate, due to sinc-like behavior of the term $\frac{\sin(2\pi \beta T^2_s mL')}{\sin(2\pi \beta T^2_s m)}$, the autocorrelation function $R_{rr}[m]$ is not periodic as the periodic impulse-like functions are attenuated by the effect of 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 V-C. Fig. 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. 3, the actual Doppler rates of the Starlink LEO SV was estimated using the receiver that will be described in Section IV. The estimated Doppler rate is partially wiped-off to obtain the different $\beta$ values in Fig. 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.,

$$R_{rr}[0] = \bar{\alpha}_i L' \tilde{A}_c(0, 0) + R_{ww}[0].$$

Assuming white Gaussian noise, i.e., $R_{ww}[m] = 0$ for $m \neq 0$, (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 $\tilde{A}_c(m, 0) \frac{\sin(2\pi \beta T^2_s mL')}{\sin(2\pi \beta T^2_s m)}$ in (6). The train of the impulse-like functions, i.e., $\tilde{A}_c(m, 0)$, is associated with the ambiguity function of the always-on and on-demand RSs which have good correlation properties. The period of $\tilde{A}_c(m, 0)$ is approximately 1.33 ms. It can be seen in Fig. 3 that the amplitude of the impulse train follow the sinc function-like behavior of $\frac{\sin(2\pi \beta T^2_s mL')}{\sin(2\pi \beta T^2_s m)}$ which matches the results of Lemma 1.

It should be pointed out that for large Doppler rate values, the term $\frac{\sin(2\pi \beta T^2_s mL')}{\sin(2\pi \beta T^2_s m)}$ approaches a Kronecker delta. Therefore, large values of Doppler rate will attenuate the impulses. On the other hand,

$$\lim_{\beta \to 0} \frac{\sin(2\pi \beta T^2_s mL')}{\sin(2\pi \beta T^2_s m)} = L' \quad \forall m,$$

which is the case in Fig. 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 $\beta$ is the actual Doppler rate of the satellite and $e_\beta$ is the estimation error for the Doppler rate. $\beta^*$ denotes an arbitrarily guessed Doppler rate value. The received signal at the $\nu$th time instant when the Doppler rate is wiped off by $\beta^*$ is denoted by $r'[n]$

$$r'[n] \triangleq \exp(-j2\pi \beta^* T^2_s n^2) r[n].$$

The $r'[n]$ contains a residual Doppler rate denoted by $\hat{\beta} = \beta - \beta^*$. Note that if $\beta^* = \beta$, the Doppler rate is wiped off perfectly and, since $\lim_{\beta \to 0} \frac{\sin(2\pi \beta T^2_s mL')}{\sin(2\pi \beta T^2_s m)} = L'$, it is expected from Lemma 2 that

$$R_{rr'}[m] = \bar{\alpha}_i \tilde{A}_c(m, 0) L' + R_{ww}[m],$$

for $\beta^* = \beta$.

B. Acquisition

The received signal at the $\nu$th time instant when the Doppler rate is wiped-off according to $r'[n] \triangleq \exp(-j2\pi \beta^* T^2_s n^2) r[n]$. Due to the periodicity of $e(\tau_n)$, $s_i[n]$ has the following property

$s_i[n + mL] = s_i[n] \exp(j \omega_i mL) \quad 0 \leq n \leq L - 1,$

where $\omega_i = 2\pi f_{D_{\nu}} T_s$ is the normalized Doppler corresponding to the $i$th transmitting source, and $-\pi \leq \omega_i \leq \pi$. A vector of $L$ observation samples corresponding to the $m$th period of the signal is formed as $z_m = [r'[mL], r'[mL+1], \ldots, r'[((m+1)L - 1)]^T$. The CPI vector is constructed by concatenating $K$ aggregates of $z_m$ vectors to form the $KL \times 1$ vector.
The likelihood of the GLR detector is the Doppler subspace matrix in (12), an alternative derivation (13) is derived in [29]. Based on the specific characteristics of detection is developed based on the generalize likelihood ratio
\[
\lambda_i = \frac{\mathbf{H}_i^H \mathbf{P}_{\mathbf{B}_{i-1}} \mathbf{H}_i}{\mathbf{y}^H \mathbf{P}_{\mathbf{B}_{i-1}} \mathbf{y}}.
\]

where
\[
\mathbf{s}_i = [s_i[1], \ldots, s_i[L]^T]; \quad \mathbf{y} = \sum_{i=1}^{N} \mathbf{H}_i \mathbf{s}_i + \mathbf{w},
\]
where \(\mathbf{H}_i \triangleq [\mathbf{I}_L, \exp(j\omega_1 L) \mathbf{I}_L, \ldots, \exp(j\omega_1 (M-L) L) \mathbf{I}_L]^T\), where \(\mathbf{I}_L\) denotes an \(L \times L\) identity matrix; and \(\mathbf{w}\) is the noise vector.

Similar to [10], 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 [10], where a constant Doppler subspace was used to distinguish between different sources. In this, paper 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 [40] 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 \(\bar{N} \equiv 0\), 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 source, and the corresponding CPIs are estimated at each stage.

In general, if the null hypothesis at the \(i\)th level of the sequential algorithm is accepted, the algorithm is terminated and the estimated number of sources will be \(\bar{N} \equiv i - 1\).

The detection problem of \(i\)th RS is defined as a binary hypothesis test

\[
\mathcal{H}_0^i : \text{ith source is absent} \\
\mathcal{H}_1^i : \text{ith source is present}.
\]

Under \(\mathcal{H}_1^i\), the signal model can be modeled as

\[
\mathbf{y} = \mathbf{H}_i \mathbf{s}_i + \mathbf{B}_{i-1} \theta_{i-1} + \mathbf{w}_{\text{eq},i},
\]
where \(\mathbf{B}_{i-1} \triangleq [\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_{i-1}]\) and \(\theta_{i-1} \triangleq [s_1^T, s_2^T, \ldots, s_{i-1}^T]^T\) 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 (13) is derived in [29]. Based on the specific characteristics of the Doppler subspace matrix in (12), an alternative derivation of the matched subspace detector is presented in Appendix B. The likelihood of the GLR detector is

\[
\mathcal{L}_i(\omega_i, \beta_i, K_i) = \frac{\mathbf{y}^H \mathbf{P}_{\mathbf{B}_{i-1}} \mathbf{y}}{\mathbf{y}^H \mathbf{P}_{\mathbf{B}_{i-1}} \mathbf{y}},
\]

for a given normalized Doppler frequency \(\omega_i\), Doppler rate \(\beta_i\), and CPI \(K_i\). The so-called general linear detector

\[
\mathbf{H}_i = \lambda_i \mathbf{I},
\]

where \(\lambda_i\) 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 \(i\)th element is (see Appendix B)

\[
c_{ij} = \sum_{k=0}^{K-1} \exp(j(\omega_j - \omega_i)k).
\]

It can be seen from (16) that the elements of the matrix \(\mathbf{C}_i\), and consequently the scalar \(\lambda_i\), are scalar functions of the Doppler frequency difference between \(i\)th source and the previously detected sources.

Remark 3: Similar calculation to Theorem 7.1 in [40] to derive the probability of detection results in

\[
P_{d_i} = \exp(-\rho_i + L \eta_i) \sum_{k=0}^{\infty} \frac{\rho_i^k}{k!} \sum_{n=0}^{L+k-1} \frac{(L \eta_i)^n}{n!},
\]

where \(P_{d_i}\) is the probability of detection of the \(i\)th source and \(\rho_i = \beta_{\text{acq}} \lambda_i \|s_i\|^2 / \sigma_w^2\),

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

The simplified likelihood can be written as (Appendix B)

\[
\mathcal{L}_i^*(\mathbf{y}) = \arg \max_{\omega_i, \beta_i, K_i} \frac{\|\lambda_i^{-1} \mathbf{H}_i^H \mathbf{P}_{\mathbf{B}_{i-1}} \mathbf{y}\|^2}{\|\mathbf{P}_{\mathbf{B}_{i-1}} \mathbf{y}\|^2 - \|\lambda_i^{-1} \mathbf{H}_i^H \mathbf{P}_{\mathbf{B}_{i-1}} \mathbf{y}\|^2}.
\]

The likelihood should be compared with predetermined threshold \(\eta_i\) 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 \(i\)th stage of the likelihood in (15) asymptotically tends to (cf. Theorem 7.1 in [40])

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

for a large number of observation samples. In the experimental results presented in Section V, (20) is used to determine the threshold.

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

\[
\hat{s}_{\text{acq},i} = \lambda_i^{-1} \mathbf{H}_i^H \mathbf{P}_{\mathbf{B}_{i-1}} \mathbf{y}.
\]

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.
complexity. In the likelihood function (15), the size of the projection matrices increases with the detection stage, i.e., \( i \). However, in [41] (Appendix 8B), a recursive formula is provided to calculate the projection matrix at the \( i \)th 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 \( O(K^2) \) where \( O(\cdot) \) 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 \( O((5KL)^2 + KL)N) \).

C. Tracking

The initial estimate of the chirp parameters \( \dot f_{D,i} \) and \( \dot \beta_i \), the estimated CPI \( \hat K_i \) and the associated likelihood functions \( \mathcal{L}^*_i \)'s are fed to the tracking stage along with the estimated RS. By employing 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.

1) RS-locked loop (RSLL): The RS in the tracking loop for the \( i \)th source is initialized with the RS estimated in the acquisition stage \( \hat s_{acq,i} \). Therefore, \( \hat s_{acq,i} = \hat s_{acq,i} \). Assuming that the ith source is being tracked, in this subsection the subscript \( i \) is dropped for convenience of notation. Let \( t_{sk} \) and \( \dot f_{D,i} \) be the code-phase and the Doppler estimates at time-step \( k \) in the tracking loop, respectively. In the \( k \)th time-step of the tracking loop, the estimated RS is updated by coherently accumulating the measurement at the \( k \)th step of the tracking loop when the delay and Doppler are wiped-off. If the subspace spanned by the columns of \( S_i = P_{\mathcal{B}_i}H_i \) is viewed as the \( i \)th source’s signal subspace, and the orthogonal subspace as the noise subspace, then the likelihood \( \mathcal{L}^*_i \) in (19) can be interpreted as an estimated SNR corresponding to the \( i \)th gNB. The reader is referred to [29] 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 \( j \)th source, i.e., \( \mathcal{L}^*_i \), 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 \( \mathcal{L}^*_i \) informs the performance of the detection of the \( j \)th 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 \( n \)th sample of the updated RS at \( k \)th time-step of tracking loop is calculated as

\[
\hat s_{k}[n] = \frac{k}{k+1} \hat s_{k-1}[n] + \frac{G_{i} \cdot y_k[n + \hat n_{d,k}] \exp(-j2\pi \dot f_{D,i} n)}{||y_k[n + \hat n_{d,k}]||}, \tag{22}
\]

where \( \hat n_{d,k} \triangleq \left\lfloor \frac{t_{sk}}{T_i} \right\rfloor \) and \( \lfloor \cdot \rceil \) denotes rounding to the closest integer, and \( G_{i} = \frac{1}{K_i} \cdot \frac{1}{\sigma_{i}^2} \) denotes the loop-gain for the RSLL.

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 \( \dot v_{PLL,k} \) in rad/s by \( 2\pi \). Assuming a zero initial carrier-phase, the estimate of the carrier-phase estimate at time-step \( k \) is updated according to \( \hat \theta_c = \hat \theta_{c,k-1} + v_{PLL,k} \cdot T_{sub} \), 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 \( \dot v_{DLL,k} \) is used to update code-phase of the received signals, assuming low-side mixing at the radio frequency front-end, according to

\[
\dot t_{sk+1} = \dot t_{sk} - \left( v_{DLL,k} + \frac{v_{PLL,k}}{2\pi f_c} \right) T_{sub}. \tag{23}
\]

Fig. 4 illustrates the proposed tracking loops.

![Fig. 4. Tracking loops: The main difference between the proposed tracking loop and conventional tracking loops [42] is the local RS generator with adaptive gains which is highlighted in red color as described in Section IV-C1.](image)

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 [42]. 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 IV-C1.

V. 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, (20) is used to calculate the threshold \( \rho_i \) for a probability of false alarm of \( 10^{-4} \) for all the stages.

A. 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 experimental layout is presented in Fig. 5. During the course of the experiment, the receiver was listening to two gNBs referred to as gNB1 and gNB2 in Fig. 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 \( \alpha \) is considered. More precisely, the channel impulse response is modeled as \( h[n] = \alpha \delta[n - n_d] \), where \( \alpha \) 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 \( \alpha \). Based on the underlying distribution of \( \alpha \), the considered \( h[n] \) can model a Rayleigh or Rician flat fading channel.

Recall from (16) and (17) that when the apparent Doppler frequencies of the unknown sources are close to each other, the effective SNR, i.e., \( \rho \), defined in (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 \( \rho_1 \). 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.

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. 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 null (red curve in 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. 6(b) demonstrates the carrier-phase errors corresponding to the two gNBs, showing that the two gNBs are being tracked.

2) Post-Acquisition and Post-Tracking Reconstructed Frame: After the detection of each gNB, (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 (21), and after the estimated RS is refined in the tracking loops using (22). Fig. 7 demonstrates the frame structure of the estimated RS for gNB1. Fig. 7(a) shows the resulting RS frame structure after acquisition, and Fig. 7(b) shows the refined estimated RS after tracking. Comparing the reconstructed frame in 7 with Fig. 2 shows that other than the broadcast signals (SS/PBCH block), several on-demand active subcarriers are also detected. As discussed in Section III, 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 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 (21) in the acquisition.

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 \( r_r \). The code-phase in (23) can be used to readily deduce the pseudorange observables. The pseudorange, expressed in meters, from the \( n \)-th gNB can be modeled as

\[
\begin{equation}
z_n(k) = \| r_r(k) - r_{s_n} \| + c \cdot (\delta t_r(k) - \delta t_{s_n}(k)) + v_n(k),
\end{equation}
\]

where \( r_{s_n} \) is the 2D position of the \( n \)-th gNB, \( c \) is the speed of light, \( \delta t_r \) and \( \delta t_{s_n} \) 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 \(\sigma_n^2\). The location of the gNBs were mapped prior to the experiment, therefore, \(r_{sn}\) is known. The terms \(c \cdot [\delta t_r(k) - \delta t_{sn}(k)]\) are combined into one term as they do not need to be estimated separately, yielding

\[
c\delta t_n(k) \triangleq c \cdot [\delta t_r(k) - \delta t_{sn}(k)]. \tag{25}
\]

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 \(\mu\)s [43]. 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

\[
c\delta t_n(k) \triangleq c\delta t_n(k) - c\delta t_n(0) \equiv c\delta t(k) + \epsilon_n(k), \quad \forall n \tag{26}
\]

where \(c\delta t\) is a time-varying common bias term independent of the \(n\)th gNB, and \(\epsilon_n\) is the deviation of \(c\delta t_n\) from this common bias and is treated as measurement noise. Using (26), the TOA measurement (24) can be re-parametrized as

\[
z_n(k) = ||r_r(k) - r_{sn}|| + c\delta t(k) + c\delta t_{0n} + \eta_n(k), \tag{27}
\]

where \(c\delta t_{0n} \triangleq c\delta t_n(0)\) and \(\eta_n(k) \triangleq \epsilon_n(k) + v_n(k)\) is the overall measurement noise.

Note that \(c\delta t_{0n}\) can be obtained by knowing the initial receiver’s position and from the initial measurement \(z_n(0)\), according to \(c\delta t_{0n} \approx z_n(0) - ||r_r(0) - r_{sn}||\).

The TOA measurements were fed to an extended Kalman filter (EKF) to estimate the state vector \(x\) as

\[
x(k + 1) = Fx(k) + w(k), \tag{28}
\]

where \(F = \text{diag}[F_{pv}, F_{clk}]\),

\[
F_{pv} = \begin{bmatrix} I_2 & T I_2 \\ 0_{2 \times 2} & I_2 \end{bmatrix}, \quad F_{clk} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}, \tag{29}
\]

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

\[
Q_{pv} = \frac{T^3}{6} Q_{xy} T^2 Q_{xy}, \tag{30}
\]

\[
Q_{clk} = c^2 \begin{bmatrix} S_{\tilde{w}_x} T^2 + S_{\tilde{w}_x} T^2 & S_{\tilde{w}_x} T^2 \\ S_{\tilde{w}_x} T^2 & S_{\tilde{w}_x} T^2 \end{bmatrix}, \tag{31}
\]

\(Q_{xy} \triangleq \text{diag}[\tilde{q}_x, \tilde{q}_y]\), and the \(x, y\) acceleration process noise spectra of the white noise acceleration model were set to
\( \hat{q}_r = \hat{q}_y = 5 \text{ m}^2/\text{s}^3 \), the time interval between two measurements was \( T = 0.0267 \text{ s} \), and the receiver’s clock process noise spectra were chosen to be \( S_{\hat{w}_t} = 1.3 \times 10^{-22} \) and \( S_{\hat{w}_t} = 7.9 \times 10^{-25} \) which are that of a typical temperature-compensated crystal oscillator (TCXO) [45]. Note that \( r_r \) is expressed in an east-north-up (ENU) frame centered at the UAV’s true initial position. The EKF state estimate was initialized at \( \hat{x}(0) = 0_{6 \times 1} \) with an initial covariance of \( P(0) = \text{diag}[3 \cdot I_3 \times 2, I_2 \times 2, 10^{-2}, 10^{-4}] \). The measurement noise covariance was set to \( R = I_2 \times 2 \).

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 \( G_i = \frac{1}{K_i} \cdot \frac{1}{L_i} \), where \( L_i \) is the likelihood of the \( i \)th RS, and the \( K_i \) is the estimated CPI corresponding to the \( i \)th RS.

Fig. 8 demonstrates the position RMSE in terms of the RSLL loop gain.

\[
\begin{align*}
\text{Position RMSE} & \quad G_1 = \frac{1}{\hat{K}_1} = 0.005 \\
\text{Position RMSE} & \quad G_2 = \frac{1}{\hat{K}_2} = 0.002
\end{align*}
\]

According to the obtained values of \( \hat{K}_i \), and \( L_i^* \) in this experiment, the designed RSLL loop gains are \( G_1 = \frac{1}{\hat{K}_1} \cdot \frac{1}{L_1^*} = 0.002 \) and \( G_2 = \frac{1}{\hat{K}_2} \cdot \frac{1}{L_2^*} = 0.005 \). To assess the effect of 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 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 \( G_1 = \frac{1}{\hat{K}_1} \cdot \frac{1}{L_1^*} \), and \( G_2 = \frac{1}{\hat{K}_2} \cdot \frac{1}{L_2^*} \) 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. 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 CPls the error would be bounded between 4.2 to 5.8 m in the 416 m of flight trajectory. Fig. 9(b) shows the estimated trajectories via the proposed receiver and the receiver in [46] which only uses the SS/PBCH block, and the ground truth trajectory. Fig. 8 demonstrates the position RMSE in terms of the RSLL loop gain.

B. 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 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 AstRx 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. 10 shows the environment layout, the vehicle trajectory, and the experiment setup.
Fig. 11. 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.

The transmitter and receiver clock terms, i.e., $\delta t_s(k)$ and $\delta t_r(k)$ in (24), are both unknown to the receiver. Assuming a first-order clock model for both the gNB and the receiver, the combined clock term in (24) can be written as $c\delta t_s(k) = c \cdot \delta t_s(k) - \delta t_s(k) = \xi + \psi T$ where $\xi$ is the clock bias and $\psi$ is the clock drift [47]. Note that $\delta t_s(k)$ is known and the receiver uses pseudorange observables to estimate the gNB’s position $r_s$. Next, define the parameter vector $x = [r_s, \xi, \psi]^T$. Let $y$ denote the vector of all the pseudorange observables stacked together. Then, one can write the measurement equation given by $z = g(x) + v_z$, where $g(x)$ is a vector-valued function that maps the parameter vector $x$ to the pseudorange observables according to (24), and $v_z$ denotes the vector of all measurement noises stacked together. Next, a nonlinear least-squares (NLS) estimator was used to estimate $x$ denoted by $\hat{x}$. 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. 13.

Fig. 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. In this paper, cognitive sensing of the gNB is considered. The cognitive sensing of multipath and other interfering components can be considered in future work.

Fig. 14(a) demonstrates the autocorrelation of the estimated RS in comparison with the autocorrelation of the always-on signals (PSS, SSS, and PBCH block). It can be seen that the autocorrelation function of the estimated RS is sharper in comparison with the autocorrelation of the always-on signals which results in a better TOA tracking performance. In order to demonstrate the effect of better autocorrelation properties the estimated RS in comparison with the always-on components, the estimated Doppler is plotted in Fig. 14(b). It can be seen that the tracked Doppler using the method in [46] which only relies on always-on signals has a larger estimation variance compared to the proposed method.

C. Experiment 3: Stationary Positioning with Starlink LEO SV Signals

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 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.

1) Acquisition: The acquisition stages in the proposed receiver is shown in Fig. 15. As it can be seen in this figure,
in the first stage of the acquisition, one source is detected at the normalized Doppler 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 \( N = 1 \).

2) The effect of CPI on Tracking Performance: Fig. 16 demonstrates the carrier-phase error for the different values of \( K_1 = 40 \) and \( K_1 = 300 \) which was the ML estimate of the CPI obtained by maximizing (15) over different values of CPI. As it can be seen in Fig. 16, the standard deviation of the carrier-phase error for \( K_1 = 300 \) is smaller than that of the case where CPI is arbitrary selected to be \( K_1 = 40 \).

3) Navigation results: The navigation results can be seen in Fig. 17. The experimental setup and the navigation framework is similar to the setup in [37]. 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 179 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. 17.

VI. CONCLUSION

An adaptive cognitive receiver architecture was proposed to extract navigation observables from Starlink LEO SV and 5G NR signals, without requiring knowledge of the RSs. The cognitive nature of the proposed receiver enables estimating both always-on and on-demand RSs which are not necessarily always-on. The parameters of the proposed receiver is designed to enable deciphering RSs in both intensive and non-intensive Doppler scenarios. It was shown that the estimated
RSs contain both always-on and on-demand component of the transmitted signals. The proposed cognitive structure was modified based on an iterative algorithm for the ML CPI estimator. Tracking loops were also designed in order to refine and maintain the estimates of the RS provided by the acquisition stage and follow the delay and Doppler of the received signals. Experimental results were presented showing 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 a root-mean-square error (RMSE) which is bounded between 4.2 m and 5.8 m in a total trajectory of 416 m, (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, and (iii) exploiting Starlink OFDM signals for positioning a stationary receiver showing a two-dimensional error of 6.5 m when the initial estimate is 179 km away from the true position of the receiver.

APPENDIX A
PROOF OF LEMMA 1

The autocorrelation of a time segment of length \( L' \) of the observation samples \( r[n] \) is equal to

\[
R_{rr}[m] = \frac{\alpha_i^2 \exp \left( j2\pi(f_{D_{\text{w}}}(mT_s + \frac{\theta_i}{2}2m^2T_s^2) \right)}{L'} \\
\times \sum_{k=0}^{L'-1} c_i[m + k - t_{si}[n]] c_i^*[k - t_{si}[n]] \\
\times \exp \left( j2\pi\beta_i m k T_s^2 \right) + \frac{1}{L} \sum_{k=0}^{L'-1} w_{\text{eqi}}[m + k] w_{\text{eqi}}^*[k].
\]

By modeling the OFDM-based RSs as a wide sense cyclostationary (WSCS) random process and assuming a large enough \( L' \), the following equality holds [48]

\[
R_{rr}[m] = \tilde{\alpha}_i^2 \frac{1}{L'} \\
\times \tilde{A}_c_i(m, 0) \sum_{k=0}^{L'-1} \exp \left( j2\pi\beta_i m k T_s^2 \right) + R_{w_{\text{eqi}}}[m].
\]

where \( \tilde{\alpha}_i \triangleq \vert \alpha_i \vert^2 \exp \left( j2\pi(f_{D_{\text{w}}}(mT_s + \frac{\theta_i}{2}2m^2T_s^2) \right) \), \( \tilde{A}_c_i(m, 0) \triangleq \mathbb{E} \{ c_i[m + k] c_i^*[k] \} \), and \( \mathbb{E} \{ X \} \) denotes the expected value of the random variable \( X \). Solving the geometric sequence on the right hand of (33) proves Lemma 1.

APPENDIX B
DERIVATION OF LIKELIHOOD FUNCTION (15)

The binary hypothesis test in (13) can be written as

\[
\{ \mathcal{H}_0^i : \mathbf{A}\theta_i = 0 \} \\
\{ \mathcal{H}_1^i : \mathbf{A}\theta_i \neq 0 \}.
\]

Where, \( \mathbf{A} = [I_L, 0, \ldots, 0] \) is an \( L \times iL \) matrix. Given \( \mathcal{W}_i \), for the general linear detection model (34), the GLR is derived as [40, Section 9.4.3]

\[
\mathcal{L}(y) = \frac{\langle \mathbf{A}\hat{\theta} \rangle^H (\mathbf{A}^H \mathbf{B}_i^H \mathbf{B}_i \mathbf{A}^H)^{-1} \langle \mathbf{A}\hat{\theta} \rangle}{\mathbf{y}^H (I_L - \mathbf{B}_i (\mathbf{B}_i^H \mathbf{B}_i)^{-1} \mathbf{B}_i^H) \mathbf{y}},
\]

(35)

Since, \( \mathbf{y} = \mathbf{H}_i s_i + \mathbf{B}_i - \theta_i + \mathbf{w}_{\text{eqi}} \), the least squares estimation of \( s_i \) is denoted by

\[
\hat{s}_i = \mathbf{J}_i^H \mathbf{B}_i^H \mathbf{P}_{\mathbf{B}_i^{-1}} \mathbf{y}.
\]

(36)

where \( \mathbf{J}_i = (\mathbf{H}_i^H \mathbf{B}_i^{-1})^H \). Also, \( \mathbf{P}_{\mathbf{X}} \triangleq \mathbf{X} (\mathbf{X}^H \mathbf{X})^{-1} \mathbf{X}^H \), denotes the projection matrix to the column space of \( \mathbf{X} \), and \( \mathbf{P}_{\mathbf{X}}^\perp \triangleq \mathbf{I}_L - \mathbf{X} (\mathbf{X}^H \mathbf{X})^{-1} \mathbf{X}^H \),

(37)

denotes the projection matrix onto the space orthogonal to the column space of \( \mathbf{X} \).

Using the matrix inversion lemma, one can show that

\[
(B_i^H B_i)^{-1} = \begin{bmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{bmatrix},
\]

(38)

\[
Q_1 = \mathbf{J}_i^H, \\
Q_2 = (\mathbf{H}_i^H \mathbf{B}_i^{-1} - \mathbf{J}_i^{-1} \mathbf{H}_i^H) (B_i^{-1})^H, \\
Q_3 = Q_2^H, \\
Q_4 = B_i^{-1} (I_L - \mathbf{H}_i \mathbf{J}_i^{-1} \mathbf{H}_i^H) (B_i^{-1})^H,
\]

where \( \mathbf{H}_i^H \triangleq (\mathbf{H}_i^H \mathbf{H})^{-1} \mathbf{H}_i^H \).

It should be pointed out that the observation vector can be written as \( \mathbf{y} = \mathbf{B}_i \theta_i + \mathbf{w}_{\text{eqi}} \). Hence, the least squares estimation is obtained as

\[
\hat{\theta} = (B_i^H B_i)^{-1} B_i^H \mathbf{y}.
\]

(39)

In the numerator of (35), one has

\[
\mathbf{A}_i \hat{\theta}_i = \mathbf{A}_i \begin{bmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{bmatrix} B_i^H \mathbf{y} \\
= (Q_1 \mathbf{H}_i^H + Q_2 B_i^{-1}) \mathbf{y} \\
= \mathbf{J}_i^{-1} \mathbf{H}_i^H (I_L - \mathbf{P}_{\mathbf{B}_i^{-1}}) \mathbf{y}.
\]

Therefore, using (36), one has

\[
\mathbf{A}_i \hat{\theta}_i = \hat{s}_i.
\]

(40)

Moreover, using (38), one has

\[
\mathbf{B}_i (B_i^H B_i)^{-1} B_i^H = I_L - \mathbf{P}_{\mathbf{B}_i^{-1}} + \mathbf{P}_{\mathbf{B}_i^{-1}} \mathbf{H}_i \mathbf{J}_i^{-1} \mathbf{H}_i^H \mathbf{P}_{\mathbf{B}_i^{-1}}.
\]

(41)

Replacing (40) and (41) in (35) yields

\[
\mathcal{L}(y | \mathcal{W}_i) = \frac{y_{\text{eqi}}^H \mathbf{P}_{\mathbf{B}_i^{-1}} y}{y_{\text{eqi}}^H \mathbf{P}_{\mathbf{B}_i^{-1}} \mathbf{P}_{\mathbf{B}_i^{-1}} \mathbf{P}_{\mathbf{B}_i^{-1}} y}.
\]

The matrices \( \mathbf{H}_i \) and \( \mathbf{P}_{\mathbf{B}_i^{-1}} \) can be written as

\[
\mathbf{H}_i = \mathbf{h}_i \otimes I_L, \\
\mathbf{P}_{\mathbf{B}_i^{-1}} = \mathbf{P}_{\mathbf{B}_i^{-1}} \otimes I_L,
\]

(43)

where, \( \mathbf{h}_i \triangleq [1, \exp (j\omega_1 L), \ldots, \exp (j\omega_{(K-1)} L)]^T \), \( \mathbf{P}_{\mathbf{B}_i^{-1}} \triangleq \mathbf{I}_L - \mathbf{B}_i^{-1} (B_i^H B_i^{-1}) \mathbf{B}_i^{-1} \), and \( \mathbf{B}_i^{-1} \triangleq \)
\( h_1, \ldots, h_{i-1} \) and \( \otimes \) denotes the Kronecker product. Hence, one can write

\[ H^i P_{B_i} H_i = ( h^i P_{i-1} h_i ) \otimes I_{h_i}. \]  

(44)

The scalar \( h^i P_{i-1} h_i \) can be written as

\[
\begin{bmatrix}
    c_{11} & c_{12} & \cdots & c_{i,(i-1)} \\
    c_{21} & c_{22} & \cdots & c_{2i} \\
    \vdots & \vdots & \ddots & \vdots \\
    c_{11} & c_{22} & \cdots & c_{i,(i-1)i}
\end{bmatrix}^{-1}
\begin{bmatrix}
    c_{1i} \\
    c_{2i} \\
    \vdots \\
    c_{i,(i-1)i}
\end{bmatrix},
\]

(45)

which is the Schur complement of \( C_{i-1} \) of matrix \( C_i \) where

\[
C_i = \begin{bmatrix}
    c_{11} & c_{12} & \cdots & c_{i,i} \\
    c_{21} & c_{22} & \cdots & c_{2i} \\
    \vdots & \vdots & \ddots & \vdots \\
    c_{11} & c_{22} & \cdots & c_{i,i}
\end{bmatrix},
\]

(46)

with \( c_{ij} \equiv \sum_{k=0}^{K-1} \exp ( j(\omega_j - \omega_i) L k) \). Hence, the following equality holds

\[ H^i P_{B_i} H_i = \lambda_i L_i. \]  

(47)

where the scalar \( \lambda_i \) is the Schur complement of block \( C_{i-1} \). Consequently, the likelihood (15) at the \( i \)th stage can be simplified as

\[
\frac{|h^i P_{B_i - 1} y|^2}{|h^i P_{B_i - 1} y|^2} = \frac{\eta_i}{\eta_0}.
\]

(48)

where \( \eta_i \) is a predetermined threshold at the \( i \)th stage.

REFERENCES


Mohammad Neinavaie is a Ph.D. student at The Ohio State University and a member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He received a B.E. in electrical engineering and an M.S. in digital communication systems from Shiraz University, Iran. His research interests include opportunistic navigation, cognitive radio, wireless communication systems, and software-defined radio.

Zaher (Zak) M. Kassas (S’98-M’08-SM’11) is a professor at The Ohio State University and TRC Endowed Chair in Intelligent Transportation Systems. He is the 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. He received a B.E. in Electrical Engineering from the Lebanese American University, an M.S. in Electrical and Computer Engineering from The Ohio State University, and an M.S.E. in Aerospace Engineering and a Ph.D. in Electrical and Computer Engineering from The University of Texas at Austin. He is a 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 Burk Award, and ION Col. Thomas Thurlow Award. He is an Associate Editor of the IEEE Transactions on Aerospace and Electronic Systems and the 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. His research interests include cyber-physical systems, navigation systems, and intelligent transportation systems.