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

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

Abstract—A receiver architecture is proposed to cognitively extract navigation observables from fifth generation (5G) new radio (NR) signals of opportunity. Unlike conventional opportunistic receivers which require knowledge of the signal structure, particularly the reference signals (RSs), the proposed cognitive opportunistic navigation (CON) receiver requires knowledge of only the frame duration and carrier frequency of the signal. In 5G NR, some of these RSs are only transmitted on demand, which limits the existing opportunistic navigation frameworks to signals which are on always-on; hence, limiting the exploitable RS bandwidth. To exploit the full available bandwidth and improve ranging accuracy, the proposed CON receiver is designed to estimate all the RSs contained in the transmitted signals corresponding to multiple 5G base stations, (i.e., gNBs). Navigation observables (pseudorange and carrier phase) are subsequently derived from the estimated RSs. The proposed receiver operates in two stages: (i) acquisition and (ii) tracking. The acquisition stage of the CON receiver is modeled as a sequential detection problem where the number of gNBs and their corresponding RSs and Doppler frequencies are unknown. The generalized likelihood ratio (GLR) test for sequentially detecting active gNBs is derived and used to estimate the number of gNBs and their RSs. In order for the receiver to refine and maintain the Doppler and RS estimates provided by the acquisition stage, tracking loops are designed. A sufficient condition on the Doppler estimation error to ensure that the proposed GLR asymptotically achieves a constant false alarm rate (CFAR) is derived. The output of the tracking loops, namely carrier phase and code phase, are then used to estimate the receiver’s position. Extensive experimental results are presented demonstrating the capabilities of the proposed CON receiver with real 5G signals on ground and aerial platforms, with an experiment showing the first navigation results with real 5G signals on an unmanned aerial vehicle (UAV) navigating using the CON receiver over a 416 m trajectory with a position root mean-squared error (RMSE) of 4.35 m.

Index Terms—5G, new radio, cognitive radio, signals of opportunity, navigation, positioning.

I. INTRODUCTION

Current capabilities offered by fourth generation (4G) mobile communications will not meet the demands of emerging applications such as Internet of Things (IoT) and autonomous vehicles [1], [2]. To address such demands, fifth generation (5G) has been developed, with a focus on features such as enhanced mobile broadband, ultra-reliable low-latency communications, and massive machine type communications [3]. Based on the performance requirements set by the international telecommunication union (ITU), the third generation partnership project (3GPP) began 5G standardization in 2015 and released its first specifications on a 5G system in June 2018, which included both the new air interface, known as new radio (NR), and 5G core network (5GC) [4]. One main characteristic of 5G signals is high data rate, which necessitates a higher transmission bandwidth and more sophisticated multiplexing techniques. The scarcity of unlicensed spectrum in lower frequencies called for using millimeter waves (mmWaves) for NR signal transmission [5]. The high path loss of propagated mmWave signals can be compensated for by beamforming techniques and massive multiple-input multiple-output (mMIMO) antenna structures [6]. Beamforming in 5G requires the knowledge of the user’s location, which means that 5G-based positioning is not only an auxiliary service, but is essential for resource allocation and beamforming for high data rate transmission [7]. Different types of positioning techniques have been evaluated by the 3GPP in Release 15 and 16 [8].

Cellular positioning techniques in the literature can be classified into network-based and opportunistic approaches [9], [10]. Network-based approaches require two-way communication with the network and the transmission of a pre-specified positioning reference signal (PRS) and some system parameters such as the number of transmission antennas and the beamforming matrix. Network-based positioning capabilities in wireless communication systems have been defined since 4G systems [11]. In a contrast to network-based approaches, in opportunistic approaches, the user equipment (UE) estimates its position from downlink signals, without communicating back with the network. As such, opportunistic approaches are more attractive than network-based approaches since: they (i) do not require additional overhead or bandwidth, (ii) preserve the UE’s privacy, (iii) do not require paying subscription to the network, and (iv) enable the UE to exploit signals from multiple

Authorized licensed use limited to: The Ohio State University. Downloaded on October 12,2022 at 17:21:12 UTC from IEEE Xplore. Restrictions apply.
cellular providers simultaneously, which improves the positioning accuracy.

Opportunistic navigation frameworks usually rely on the broadcast reference signals (RSs), which are used to derive direction-of-arrival (DOA) and time-of-arrival (TOA) [12]. These signals are known at the UE and are universal across network operators. Hence, they can be exploited for positioning without the need for the UE to be a network subscriber. In cellular long-term evolution (LTE) networks, several RSs, such as the cell-specific reference signal (CRS), are broadcast at regular and known time intervals, regardless of the number of UEs in the environments. This always-on type of transmitted RSs reduces the network’s energy efficiency and increases operational expenses and interference. One of the main features of 5G signals is ultra-lean transmission, which minimizes the transmission of always-on signals. For instance, CRS which used to be an always-on RS in LTE, is not necessarily being continuously transmitted in 5G signals. Up until now, 5G opportunistic navigation methods relied on the always-on signals, e.g., the primary and secondary synchronization signals (PSS and SSS, respectively) and the physical broadcast channel (SB/PBCH) block, none of which use the entire signal bandwidth [13]–[15].

This paper presents a cognitive opportunistic navigation framework (CON) by developing a 5G receiver architecture to simultaneously detect the active gNBs in the environment, estimate the number of gNBs and their unknown RSs which are not necessarily always-on, and exploit them to derive navigation observables in a cognitive fashion. There are four main RSs in 5G signals: demodulation RSs, phase tracking RSs, sounding RSs, and channel state information (CSI) RSs. These RSs are only transmitted on demand, which limits the efficacy of conventional opportunistic navigation frameworks which rely on always-on RSs. For instance, while the receiver proposed in [14] was the first 5G-based opportunistic navigation receiver, it relies on the always-on SB/PBCH block. The downside of relying only on the SB/PBCH block is the limited bandwidth. Higher signal bandwidth translates to more accurate TOA estimates. In order to exploit the full ranging accuracy achievable with 5G signals, the proposed CON receiver is designed to cognitively estimate the RSs present in the entire bandwidth and exploit them to obtain navigation observables (pseudoranges and carrier phase). Not only the proposed receiver is capable of exploiting RSs which are not always-on, but the cognitive nature of the proposed receiver enables opportunistic navigation with future communication standards with unknown or partially known signal specifications. The proposed receiver architecture relies solely on the periodicity of the RSs and requires very limited information about the 5G signal, namely it only assumes knowledge of the frame duration and the carrier frequency. It should be pointed out that an energy detector can be used to provide an estimate of the carrier frequency and using the current literature, e.g., the period estimator in [16], the frame duration can also be estimated in a pre-processing stage. One main challenge faced by the CON receiver is the problem of distinguishing signals from multiple 5G base stations, i.e., gNBs, multiplexed over the same channel. This task is relatively simple when the RSs are known, as RSs are usually designed to have desirable autocorrelation and cross-correlation properties. Since this paper does not assume knowledge of the RSs, it is desirable for the CON receiver to be able to detect multiple gNBs and distinguish their signals. To this end, a subspace-based detection scheme leveraging the Doppler frequency subspace is proposed to estimate the number of available gNBs and estimate their RSs.

Specifically, the contributions of this work are as follows:

- A CON receiver design is presented, which could estimate the unknown RSs of a gNB. The cognitive nature of the proposed receiver enables estimating both always-on and on-demand RSs which are not necessarily always-on. Using extensive experiments, it is shown that the estimated RSs possess higher bandwidth compared to conventional 5G opportunistic navigation receivers, which allows for producing more precise navigation observables.

- A sequential generalized likelihood ratio (GLR) detector is derived to detect the presence of multiple gNBs on the same channel and provide an estimate of the number of active gNBs. The detector relies on matched subspace detection, where the signal subspace is defined by the Doppler frequencies of the gNBs. The sequential GLR detector estimates the number of gNBs, and their Doppler frequencies, and it provides an initial estimate of their unknown RSs, which are then used and refined in the tracking loops.

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

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

The rest of the paper is organized as follows. Section II surveys related research on navigation with 4G and 5G signals. Section III describes the received baseband signal model. Section IV presents the proposed CON receiver architecture. Section V presents the experimental results. Section VI gives concluding remarks.
II. RELATED WORK

1) Opportunistic Navigation: Over the past decade, opportunistic navigation has been demonstrated in the literature with different types of signals, also known as signals of opportunism (SOPs). SOP examples include cellular [9], [10], digital television [17], [18], AM/FM [19], [20], Wi-Fi [21], [22], and low-earth orbit (LEO) satellite signals [23], [24]. Among SOPs, cellular signals have attracted considerable attention due to their desirable attributes, including: (i) large transmission bandwidth, (ii) high carrier-to-noise ratio, and (iii) desirable geometric diversity [25]. While meter-level and decimeter-level SOP-based navigation solutions were demonstrated on ground vehicles and UAVs, respectively, the aforementioned approaches relied on the knowledge of a subset of the RSs transmitted by the SOP. These methods would fail if (i) the receiver enters an unknown SOP environment where the number of active SOPs and their corresponding RSs are unknown, or (ii) some signal parameters change due to the dynamic nature of wireless protocols. This paper addresses these issues by estimating all available RSs within the SOP with minimal prior knowledge.

2) Positioning With 5G Signals: The characteristics of mmWave signals were evaluated for positioning in [26]. Cramér-Rao lower bounds (CRLBs) of the direction-of-departure (DOD), DOA, and TOA for both uplink and downlink mmWave signals were derived in [27], [28], showing sub-meter positioning error, and sub-degree orientation error. To exploit the sparsity of mmWave channels, tools relying on compressed sensing were proposed in [29], [30] to estimate DOD, DOA, and TOA of the UE, showing sub-meter level position error via simulation results. The DOD and UE’s position were estimated in a two-stage Kalman filter using the signal strength from multiple base stations in [31], which yielded sub-meter-level three-dimensional (3-D) position accuracy. The joint estimation of the position and orientation of the UE, as well as the location of reflectors or scatterers in the absence of the line-of-sight (LOS) path, were considered in [32], showing less than 15m position RMSE and less than 7° orientation RMSE. A two-way distributed localization protocol was proposed in [33] to remove the effect of the clock bias in TOA estimates. In [7], a positioning method for multiple-output single-input systems was proposed, where the DOD and TOA of the received signal were used to localize a UE. In [34], estimation of signal parameters via rotational invariant techniques (ESPRIT) was used to estimate the DOA and DOD of the signal. Experimental results in [14] and [13] showed meter-level navigation using TOA estimates from 5G signals. The results presented therein rely only on the PSS and SSS for TOA estimation. It is shown that the proposed receiver yields a narrower RS autocorrelation function, which translates to more accurate TOA estimates. Moreover, the proposed receiver architecture can be readily adapted to any type of signal containing periodic RSs.

Detection of Unknown Signals in the Presence of Noise and Interference: The acquisition stage of the CON receiver is modeled as a sequential matched subspace detection problem, which comprises estimating the number of gNBs, an initial estimate of normalized Doppler, and an initial estimate of the RSs. 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 literature [35]–[37]. Matched subspace detectors are used frequently in radar signal processing, e.g., in source localization in multiple-input multiple-output (MIMO) radars [38] and passive bistatic radar [39]. In [40], the design of subspace matched filters in the presence of mismatch in the steering vector was addressed. The performance of low-rank adaptive normalized matched subspace detectors was studied in [41].

In [42], the idea of subspace matching was used to present a solution to the problem of detecting the number of signals in both white and colored noise. In [43], the structure of the noise covariance matrix was exploited to enhance the matched subspace detection performance. In [44], adaptive vector subspace detection in partially homogeneous Gaussian disturbance was addressed. Recently, machine learning approaches have been proposed for unknown transmitter detection, identification, and classification [45], [46]. 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. The problem of detecting Galileo and Compass satellites signals was studied in [47], which revealed the spread spectrum codes for these satellites. Preliminary experiments on navigation with partially known signals from low and medium Earth orbit satellites were conducted in [48]–[51]. In particular, a chirp parameter estimator was used in [49] to blindly estimate the GPS pseudorandom noise (PRN) codes. In [50], a blind channel estimator was proposed to exploit Orbcomm satellite signals for navigation purposes. In [51], OFDM signals were emulated from Orbcomm LEO satellites and an FFT-based Doppler estimator was proposed to exploit these signals for navigation purposes. While these approaches yielded useful insights, they either exploited signals that have a simpler structure compared to 5G or proposed different receiver structures than the one developed in this paper. In particular, this paper uses the concept of matched subspace detection to design a full receiver architecture, whose performance is analyzed analytically and is subsequently tested experimentally with real 5G signals. It is shown that the proposed receiver is capable of detecting the number of active gNBs, along with their corresponding RSs and Doppler frequencies with only the prior knowledge of the frame duration and the carrier frequency.

III. RECEIVED BASEBAND SIGNAL MODEL

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

A. Brief Review of NR RSs

NR adopts orthogonal frequency division multiplexing (OFDM) scheme, as was the case in 4G. In OFDM-based transmission, the symbols are mapped onto multiple carrier frequencies, referred to as subcarriers, with a particular spacing known as subcarrier spacing. Unlike the 4G signal standard, which considers a fixed subcarrier spacing of 15 kHz, subcarrier spacing values of $15 \times 2^\mu$, with $\mu \in \{0, 1, 2, 3\}$ are supported.
by NR. The system selects subcarrier spacing values based on carrier frequency, and/or other requirements and scenarios. Once the subcarrier spacing is configured, the frame structure is identified. An NR frame has a duration of 10 ms and consists of 10 subframes with durations of 1 ms [4]. In the proposed receiver, only the frame duration and carrier frequency are assumed to be known. In the frequency-domain, each subframe is divided into numerous resource grids, each of which has multiple resource blocks with 12 subcarriers. The number of resource grids in the frame is provided to the UE from higher level signalling. A resource element is the smallest element of a resource grid that is defined by its symbol and subcarrier number [4].

To provide frame timing to the UE, a gNB broadcasts synchronization signals (SS) on pre-specified symbol numbers. An SS includes PSS and SSS, which provide symbol and frame timing, respectively. The PSS and SSS are transmitted along with the PBCH signal and its associated demodulation reference signal (DM-RS) on a block called SS/PBCH block. The SS/PBCH block consists of four consecutive OFDM symbols and 240 consecutive subcarriers. The SS/PBCH block has a periodicity of 20 ms and is transmitted numerous times on one of the half frames, also known as SS/PBCH burst.

B. Signal Model

As it was mentioned previously, the SS/PBCH block is not transmitted on the whole signal’s bandwidth. Therefore, methods which only rely on SS/PBCH block, cannot exploit the full ranging accuracy that can be achieved by 5G signals. Other periodic RSs are not necessarily always-on and the cognitive receiver should be able to exploit them to be able to achieve the available ranging accuracy. In this paper, with a focus on exploiting navigation observables using the RSs in the entire 5G bandwidth, the 5G NR signal is modeled as an unknown periodic signal in the presence of interference and noise. If an RS is being periodically transmitted, it will be detected by the receiver, estimated, and used to derive navigation observables. The estimated RS has the following property

\[ s_{i}[n] = s_{i}[n] + w_{eq_{i}}[n] \quad (5) \]

where \( w_{eq_{i}}[n] \) will be used at the receiver to obtain the navigation observables.

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

One can form a vector of \( L \) observation samples corresponding to the \( k \)th period of the signal as

\[ y_{k} \triangleq [r[(k-1)L+1], r[(k-1)L+2], \ldots, r[kL]]^{T}. \quad (6) \]

Considering a CPI of length \( K \times L \) samples, the observation vector is constructed as \( y = [y_{1}^{T}, y_{2}^{T}, \ldots, y_{K}^{T}]^{T} \). Therefore,

\[ y = \sum_{i=1}^{N} \mathbf{H}_{i} s_{i} + \mathbf{w}_{eq_{i}}, \quad (7) \]

where \( s_{i} = [s_{i}[1], s_{i}[2], \ldots, s_{i}[L]]^{T}, \mathbf{w}_{eq_{i}} \) is the equivalent noise vector corresponding to the \( i \)th source, and the \( KL \times L \) Doppler matrix corresponding to the \( i \)th source is defined as

\[ \mathbf{H}_{i} \triangleq [\mathbf{I}_{L}, \exp(j\omega_{i}L), \ldots, \exp(j\omega_{i}(K-1)L)]^{T} \mathbf{I}_{L} \]

where \( \mathbf{I}_{L} \) is an \( L \times L \) identity matrix.

IV. CON RECEIVER STRUCTURE

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

A. Acquisition

In this paper, the acquisition stage is modeled as a sequential matched subspace detection problem. The acquisition stage comprises estimating the number of gNBs, an initial estimate
of normalized Doppler, and the RSSs, i.e., $N, \omega_i$, and $s_i$, respectively. At each step of the acquisition, a test is performed to detect the most powerful gNB when the subspace of the previously detected gNBs are nulled. In the following subsection, matched subspace detection is overviewed and the hypothesis test for detection of multiple gNBs is formulated.

1) Matched Subspace Detector: As it was mentioned previously, in the first step of the proposed sequential algorithm, the presence of a single gNB is tested and if the null hypothesis is accepted, then $\tilde{N} = 0$, which means that no gNB is detected to be present in the environment under the test. If the test rejects the null hypothesis, the algorithm verifies the presence of at least one source and performs the test to detect the presence of other gNBs in the presence of the previously detected gNBs. The unknown Doppler and the RS of each gNB are estimated at each step.

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 gNBs will be $\tilde{N} = i – 1$.

In order to test the presence of $s_i$ at the $i$th stage of the acquisition algorithm, the observation vector can be written as

$$y = H_i s_i + B_{i-1} \theta_{i-1} + w_{eq},$$

$$B_{i-1} = [H_1, H_2, \ldots, H_{i-1}], \theta_{i-1} = [s_1^T, s_2^T, \ldots, s_{i-1}^T]^T.$$  (10)

The following binary hypothesis test is used to detect the $i$th gNB:

$$\mathcal{H}_0^i: \ y = B_{i-1} \theta_{i-1} + w_{eq},$$

$$\mathcal{H}_1^i: \ y = H_i s_i + B_{i-1} \theta_{i-1} + w_{eq}.$$  (11)

For a given set of Doppler frequencies, $\mathcal{W}_i = \{\omega_1, \omega_2, \ldots, \omega_i\}$, the GLR at the $i$th stage is derived as (see Appendix A)

$$L_i(y|\mathcal{W}_i) = \frac{y^H P_{S_i} y}{y^H P_{B_{i-1}} P_{S_i} P_{B_{i-1}}^{-1} y},$$  (12)

where $y^H$ is the Hermitian transpose of $y$, $P_X \triangleq X(X^H X)^{-1} X^H$, denotes the projection matrix to the column space of $X$, and $P_{S_i} \triangleq I - X(X^H X)^{-1} X^H$, denotes the projection matrix onto the space orthogonal to the column space of $X$, and $S_i = P_{B_{i-1}} H_i$. Intuitively, in (12) the subspace of previously detected gNBs, i.e., $B_{i-1}$, is nulled to detect the $i$th gNB.

Remark 1 (Vector space interpretation of (12)): If the subspace spanned by the columns of $S_i$ is $P_{B_{i-1}} H_i$, viewed as the $i$th gNB’s signal subspace, and the orthogonal subspace as the noise subspace, then the likelihood (12) can be interpreted as an estimated signal to noise ratio (SNR). The reader is referred to [35] for further interpretations of matched subspace detectors.

Remark 2: At the $i$th stage of the proposed sequential algorithm, the GLR requires an estimate of the set $\mathcal{W}_i$. The sequential nature of the algorithm enables a single variable estimation of the Doppler frequency at each step. For instance, at the first step of the algorithm, a single dimensional search is required to obtain the maximum likelihood (ML) estimate of $\omega_1$, denoted by $\hat{\omega}_1$. In the second stage of the algorithm, $\hat{\omega}_1$ is used to construct the projection matrix to null the subspace of the first gNB. Consequently, at the $i$th step of the algorithm, invoking the previously estimated Doplplers, a single dimensional search is required to estimate $\omega_i$, and construct the estimated projection matrix and the estimated Doppler matrix for the corresponding stage, denoted by $P_{S_i}$ and $H_i$, respectively.

The following lemma simplifies the likelihood function (12).

**Lemma 1:** In the likelihood function (12), the following equality holds

$$H_i^H P_{B_{i-1}} H_i = \lambda_i I,$$  (14)

where the scalar $\lambda_i$ is the Schur complement of block $C_{i-1}$, i.e., the upper $(i - 1) \times (i - 1)$ block of the matrix $C_i$, where

$$C_i = \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1i} \\ c_{21} & c_{22} & \ldots & c_{2i} \\ \vdots & \vdots & \ddots & \vdots \\ c_{i1} & c_{i2} & \ldots & c_{ii} \end{bmatrix},$$  (15)

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

**Proof:** See Appendix B.

According to Lemma 1, the likelihood (12) at the $i$th stage can be simplified as

$$L_i(y) = \frac{y^H \lambda_i^{-1} H_i^H P_{B_{i-1}} y}{y^H P_{B_{i-1}} y^2},$$  (16)

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

$$\hat{\omega}_i = \arg \max_{\omega_i} ||H_i^H P_{B_{i-1}} y||^2,$$

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

For a known $\omega_i$, the least squares (LS) estimate of the $i$th source, i.e., $s_i$, is given by

$$\hat{s}_i = \frac{1}{\lambda_i} H_i^H P_{B_{i-1}} y,$$  (18)

It should be noted that the estimated RS, i.e., $\hat{s}_i$, contains the effect of the channel between the gNB and the UE. Small values of $|\alpha_i|$ degrades the estimation quality of the desired RS and, consequently, affects the acquisition and tracking performance. It should also be pointed out that $\frac{1}{\lambda_i} H_i^H P_{B_{i-1}} y = s_i + w_{acq}$. In other words, for a known Doppler frequency, the LS estimator of the $i$th source is an unbiased estimator, i.e., $\hat{E}(\hat{s}_i) = s_i$. However, since the true Doppler is not known to the CON receiver, the ML estimate of the Doppler is used to compute the LS estimate of the $i$th RS instead. Moreover, it can be shown that

$$\frac{1}{\lambda_i} H_i^H P_{B_{i-1}} y = \beta_{acq} I,$$  (19)

*Consider $p \times p$ matrix $A$, $p \times 1$ vectors $b$ and $c$ and scalar $d$. For the matrix $\begin{bmatrix} A & b \\ c^T & d \end{bmatrix}$, the Schur complement of block $A$ is defined as $d - c^T A^{-1} b$. 
where $\beta_{\text{acq}}$ is some complex scalar. As such, the LS estimate of the RS using the ML estimate of the Doppler becomes

$$\hat{s}_i = \frac{1}{\hat{k}_i} \hat{H}_i^H \hat{P}_{B,i} s_i + \hat{w}_{\text{acq}},$$  \hfill (20)

where $\hat{w}_{\text{acq}} = \frac{1}{\hat{k}_i} \hat{H}_i^H \hat{P}_{B,i} \hat{w}_{\text{eq}}$. Furthermore, the asymptotically efficient property of the ML estimator results in $|\beta_{\text{acq}}| \to 1$ as $K \to \infty$ [52].

2) Asymptotic CFAR Property: The Doppler estimation error affects the probability of detection and the probability of false alarm. For known subspaces and the corresponding projection matrices, using Theorem 7.1 in [53], one can show that the probability of false alarm for the $i$th stage of the likelihood in (12) asymptotically tends to

$$P_{\text{fa},i} = \exp \left( -L \eta_i \right) \sum_{n=0}^{L-1} \frac{(L \eta_i)^n}{n!}, \hfill (21)$$

for a large number of observation samples. In other words, the detector is not a function of unknown parameters for known Doppler frequencies, which means that it ensures CFAR property. Next, the effect of Doppler estimation error on the probability of false alarm is assessed. The following theorem gives a sufficient condition to ensure the CFAR property for a scenario with two gNBs for a large enough CPI.

**Theorem 1:** Consider two gNBs with Doppler frequencies $\omega_1$ and $\omega_2$ and corresponding estimates $\hat{\omega}_1$ and $\hat{\omega}_2$, respectively. Define the Doppler estimation error of $\omega_1$ as $\Delta \omega_1 = \hat{\omega}_1 - \omega_1$. As $K \to \infty$, sufficient conditions for the matched subspace detector in (12) to be a CFAR detector in the second stage are

(i) $|\Delta \omega_1| \ll \frac{1}{K}$ and (ii) $|\Delta \omega_2| \ll \frac{1}{K}$.

**Proof:** See Appendix C.

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

It should be pointed out that in the experiments, (21) is used to select the threshold for a given probability of false alarm. According to Theorem 7.1 in [53], (21) holds for a large number of observation samples and for known subspaces. Due to the asymptotic efficiency property of the ML estimator, it is assumed that the subspace estimation error tends to zero for a large number of observation samples. In the experiments, the number of samples in a CPI is selected to be large and (21) holds asymptotically. The acquisition algorithm is summarized in Algorithm 1.

**Algorithm 1:** Sequential Matched Subspace Detector.

**Input:** $y$, $P_{B_0}$

**Output:** $\hat{N}$, $\hat{\omega}_i$, and $\hat{s}_i$ for $i = 1, \ldots, \hat{N}$

1: Initialization: $i = 1$, $P_{B_0} = I$
2: Calculate $L_i(y)$ according to (16) and the threshold using (21).
3: if $L_i(y) < \eta_i$ then
   4: $N = i - 1$.
5: Break
6: end if
7: Estimate $\omega_i$ according to (17), and construct $\hat{H}_i$,
   $\hat{P}_{B_{i-1}}$, and $\hat{\lambda}_i$
8: $\hat{s}_i = \frac{1}{\hat{k}_i} \hat{H}_i^H \hat{P}_{B_{i-1}} Y$
9: $i \leftarrow i + 1$, update $\hat{P}_{B_{i-1}}$ using $\hat{\omega}_i$, and go to step 2.

B. Tracking

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

1) RS Estimate Update: The acquisition step provides a coarse initial estimate of the RS, denoted by $\hat{s}_{\text{acq}}[n]$. From (20), the $n$th symbol of the estimated RS can be expressed as $\hat{s}_{\text{acq}}[n] = \beta_{\text{acq}} x[n] + \hat{w}_{\text{acq}}[n]$, where $\beta_{\text{acq}}$ is obtained according to (19) and $x[n]$ is the $n$th element of vector $x$. Recall that $\beta_{\text{acq}}$ depends on the Doppler estimation error in the acquisition stage. Let $\hat{t}_{\text{acq}}$ and $\hat{f}_{D_{\text{acq}}}$ be the code phase and the Doppler estimates at time-step $k$ in the tracking loop, respectively. In this step of the tracking loop, the RS estimate is updated by coherently integrating the observations after delay compensation and Doppler wipe-off. As such, the RS estimate at the $k$th iteration of the tracking loops is given by

$$\hat{s}_k[n] = \frac{k}{k + 1} \hat{s}_{k-1}[n] + \frac{1}{k + 1} y_k[n] + \hat{t}_{\text{acq}}[n] \exp \left( -j2\pi \hat{f}_{D_{\text{acq}}}[n] \right)$$
where $n_{dm}$ is the rounding operation to the closest integer.

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

$$F_{PLL}(s) = \frac{2\pi\alpha s + \frac{\omega_0^2}{s}}{s}, \quad (23)$$

where $\alpha \equiv \frac{1}{\sqrt{2}}$ is the damping ratio and $\omega_0$ is the undamped natural frequency, which can be related to the PLL noise-equivalent bandwidth $B_{n,PLL}$ by $B_{n,PLL} = \frac{\omega_0}{\pi} (4\zeta^2 + 1)$ [54]. The loop filter transfer function in (23) is discretized at a sampling period $T_{sub} \triangleq LT_s$, which is the time interval at which the loop filters are updated and is typically known as the subaccumulation interval. The discretized transfer function is realized in state-space. The output of the loop filter at time-step $k$, denoted by $v_{PLL,k}$, is the rate of change of the carrier phase error, expressed in rad/s. The Doppler frequency estimate at time-step $k$ is deduced by dividing $v_{PLL,k}$ by $2\pi$. The loop filter transfer function in (23) is discretized and realized in state-space. The noise-equivalent bandwidth is chosen to range between 4 and 8 Hz. The carrier phase estimate at time-step $k$ is updated according to

$$\hat{\theta}_k = \hat{\theta}_{k-1} + v_{PLL} \cdot T_{sub}, \quad (24)$$

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

3) DLL: The carrier-aided DLL employs an early-minus-late discriminator. The early and late correlations at time-step $k$ used in the discriminator are denoted by $Z_{c_k}$ and $Z_{l_k}$, respectively, which are calculated by correlating the received signal with an early and a delayed version of the estimated RS, respectively. The time shift between $Z_{c_k}$ and $Z_{l_k}$ is defined as the early-minus-late time, denoted by $\xi$. The DLL loop filter is a simple gain $K_{DLL}$, with a noise-equivalent bandwidth $B_{n,DLL} = K_{DLL} \equiv 0.5$ Hz. The output of the DLL loop filter $v_{DLL}$ is the rate of change of the code phase, expressed in s/s. Assuming low-side mixing at the radio frequency front-end, the code phase estimate is updated according to

$$\hat{\tau}_{k+1} = \hat{\tau}_k - \left( v_{DLL,k} + \frac{v_{PLL,k}}{2\pi f_c} \right) \cdot T_{sub}, \quad (25)$$

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

V. EXPERIMENTAL RESULTS

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

A. CON With Real 5G Signals: Comparison With a Conventional 5G Receiver on a Ground Vehicle

The first experiment aims to compare the acquisition and tracking performance of the CON receiver with the conventional 5G receiver [14] which only relies on the always-on RSs. The experimental setup and results for the experiment with real 5G NR signals are discussed next.

1) Experimental Setup and Environmental Layout: In this experiment, a ground vehicle was equipped with a quad-channel National Instrument (NI) universal software radio peripheral (USRP)-2955 and four consumer grade 800/1900 MHz cellular antennas to sample 5G signals near Fairview Road in Costa Mesa, California, USA. Only one channel from the USRP was used and was tuned to a 872 MHz carrier frequency, which is a 5G NR frequency allocated to the U.S. cellular provider AT&T. The sampling rate was set to 10 Mega-samples per second (MSPs) and the sampled 5G signals were stored on a laptop for post-processing. In order to obtain ground-truth, the vehicle was equipped with a Septentrio AsteRx-i V GNSS-aided inertial navigation system (INS), which is a dual antenna, multi-frequency GNSS receiver with real-time kinematics (RTK) capabilities. The GNSS receiver is coupled with a Vectornav VN-100 micro electromechanical systems (MEMS) inertial measurement unit (IMU) to estimate the position and orientation of the ground vehicle at a rated horizontal accuracy of 0.6 cm in clear sky conditions (RTK performance). The vehicle traversed a trajectory of 4.1 km in 315 seconds. Fig. 2 shows the environment layout and the vehicle trajectory. The acquisition results are presented next.

2) Signal Model Validation: The signal model (1) considers a channel with a single tap, which corresponds to the LOS path with an arbitrary complex channel gain $\alpha_i$. In other words, the channel is modeled as $h_i[n] = \alpha_i \delta[n - |t_{g,n}]|$, where $\alpha_i$ is the complex channel gain between the $i$th gNB and the UE, $t_{g,n}$ is the code-delay corresponding to the UE and the $i$th gNB, and $\delta[\cdot]$ is the rounding operation to the closest integer. Note that this channel models flat fading, where multiple received “close” signal paths are combined into a single $\alpha_i$. To justify the signal
TABLE I

<table>
<thead>
<tr>
<th>Parameter</th>
<th>LTF</th>
<th>5G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier frequency</td>
<td>1955, 2145, 2125, and 739 MHz [12]</td>
<td>632.55, and 872 MHz [13]</td>
</tr>
<tr>
<td>Sampling rate</td>
<td>10 MHz</td>
<td>10 MHz</td>
</tr>
<tr>
<td>( \eta )</td>
<td>1.012 for ( P_{fa} = 10^{-4} ) (21)</td>
<td>1.007 for ( P_{fa} = 10^{-4} ) (21)</td>
</tr>
<tr>
<td>( B_{n, PLL} )</td>
<td>4-8 Hz (empirically)</td>
<td>4-8 Hz (empirically)</td>
</tr>
<tr>
<td>( B_{n, DLL} )</td>
<td>0.5 Hz (empirically)</td>
<td>0.5 Hz (empirically)</td>
</tr>
<tr>
<td>( T_{sub} )</td>
<td>10 ms [12]</td>
<td>20 ms [13]</td>
</tr>
<tr>
<td>( K )</td>
<td>40 (empirically)</td>
<td>40 (empirically)</td>
</tr>
</tbody>
</table>

Fig. 2. Experimental setup and vehicle trajectory for the 5G NR experiment with ground vehicle.

model in the tested scenario, two test points are considered for the ground vehicle (see Fig. 3(a)). In this figure, the term clear LOS refers to a scenario where the signal is not blocked by an obstacle, e.g., a building. The two test points, i.e., receiver location 1 and receiver location 2, are considered based on the existence of the clear LOS with respect to the 5G gNB. Receiver location 1 has a clear LOS and is also closer to the gNB. On the other hand, receiver location 2 is blocked by a building and does not have a clear LOS. The magnitude of the channel impulse response for both locations are plotted in Fig. 3(b). The magnitudes of the channel impulse responses are estimated by reconstructing the frame as described in [13]. As it can be seen in this figure, the channel impulse response for receiver location 2 is weaker than that of receiver location 1 which is due to blockage of the signal by an obstacle. The complex channel gain in (1) captures this effect by attenuating the LOS signal. If the acquisition of a gNB is performed when the receiver does not have a clear LOS, e.g., receiver location 2, the detection performance will be degraded, which in turn affects the tracking performance. Fig. 4 demonstrates the likelihood at the first stage of acquisition for receiver location 1 and 2. As can be seen in Fig. 4, the likelihood is degraded at receiver location 2 due to signal blockage. Note that in both receiver locations, \( |h(\tau)| \) does not exhibit multiple taps (i.e., \( h_i[n] = \sum_{j=1}^{M} \alpha_{i,j} \delta[n - t_{h_i,j}[n]] \)), where \( M \) is the number of paths), which corresponds to the impulse response of a frequency selective channel. While the considered signal model is simple, yet valid for the conducted experiments, more sophisticated channel models, e.g., frequency selective channels, can be considered in future work [55].

3) Acquisition Results: The recorded 5G signals were processed in two ways for comparison: (i) using the proposed CON receiver and (ii) using the conventional 5G receiver proposed in [14]. The conventional 5G receiver detected 1 gNB with an initial Doppler frequency of \(-7.2\) Hz. Note that the limited
number of gNBs was expected as 5G gNBs are sparsely deployed at the present time. The location of the gNB was mapped prior to the experiment. Next, the signal acquisition stage was applied to detect the ambient 5G gNB. The detection threshold was set such that $P_{fa} = 10^{-4}$, which yielded $\eta = 1.008$, $K$ was set to 40, and $T_{sub}$ was set to 20 ms. Doppler estimation was performed by searching for the maximizer of the likelihood function according to (17) with a step size of 1 Hz. The acquisition stages in the CON receiver is shown in Fig. 5. As it can be seen in this figure, in the first stage of the acquisition, one gNB is detected at frequency $-7$ Hz. In the second stage, the Doppler subspace of this gNB is nulled and the resulting likelihood is less than the threshold for all Doppler frequencies. This implies that, no other gNBs are detected in the second stage of the acquisition or equivalently $\hat{N} = 1$.

4) Tracking Results: After acquiring the Doppler and RSs, the tracking loops are initialized and the signal is tracked. Fig. 6 show the resulting Doppler frequency and delay, expressed in meters, obtained using the CON and conventional receivers. As it can be seen in Fig. 6(b) the estimated delays for the CON and the conventional receivers are slightly drifting away from the ground-truth which is due to the clock drifts. The effect of clock drift is considered in the carrier phase model (see equation (26)). Note that the initial value of the delays were subtracted out to facilitate comparison. The Doppler and delay RMSE values were calculated from ground-truth for both receivers and are summarized in Table II, which shows that the CON receiver outperforms the conventional one.

A main reason behind the CON receiver performing better than a conventional 5G receiver is that the former exploits the RSs in the entire bandwidth, making the bandwidth of estimated RS higher than the RSs used in the conventional receiver (mainly, PSS and SSS). Fig. 7 shows this: the normalized autocorrelation function of the RS estimated with the CON receiver is narrower than that of a 5G PSS.

Remark 3: The conventional and the proposed cognitive methods use tracking loops which involve the same computational complexity. The main difference between the computational complexity of the proposed cognitive receiver and a conventional receiver stems from the acquisition stage. The number of complex operations is considered as a metric for computational complexity. In the likelihood function (12), the size of the projection matrices increases with the detection stage, i.e., $i$. However, in [56] (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 $O((5KL)^2 + KL)N)$.

B. CON With Real 5G Signals: The First Navigation Results on a UAV

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

1) Experimental Setup and Environment Layout: In this experiment, the navigator was an Autel Robotics X-Star Premium UAV equipped with a single-channel Ettus 312 USRP connected to a consumer-grade 800/1900 MHz cellular antenna and a small consumer-grade GPS antenna to discipline the on-board oscillator. The cellular receivers were tuned to the cellular
Next, the signal acquisition stage was performed. In the following, it is assumed that after acquiring the Doppler and the delay of the downlink signals from the gNBs, the tracking loops are initialized and the signal is tracked. The acquisition results are presented next.

2) Acquisition Results: Next, the signal acquisition stage was applied to detect the ambient 5G gNBs. The CON 5G receiver detected 2 gNBs with initial Doppler frequencies of 3.5 Hz and 11.5 Hz. The location of the gNBs was mapped prior to the experiment. The acquisition stages in the CON receiver are shown in Fig. 9. Fig. 10 shows the resulting Doppler frequencies and delays.

3) Tracking Results: After acquiring the Doppler and the RSs, the tracking loops are initialized and the signal is tracked. Fig. 10 shows the resulting Doppler frequencies and delays, expressed in meters, obtained using the CON receiver.

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

\[
z_i(k) = ||r_r(k) - r_s_i||_2 + c\delta t_r(k) - c\delta t_s_i + v_i(k),
\]

where \( r_r \) and \( r_s_i \) are the three-dimensional (3–D) position vectors of the UAV-mounted receiver and the \( i \)-th gNB, respectively; \( c \) is the speed of light; \( \delta t_r \) is the UAV-mounted receiver’s clock bias; \( \delta t_s_i \) models the \( i \)-th gNB’s clock bias and carrier phase ambiguity; and \( v_i(k) \) is the measurement noise, which is modeled as a zero-mean Gaussian random variable with variance \( \sigma_i^2 \) [57]. Note that since the UAV’s altitude is known, e.g., using an altimeter, only its two-dimensional (2–D) position is estimated. The time reference for the transmitter and receiver clocks is chosen such that \( \delta t_s_i(k_0) = 0 \).

Using the position estimate at \( k_0 \) and the fact that \( \delta t_r(k_0) = 0 \), the gNBs clock biases can be estimated from \( z_i(k_0) \) resulting in the estimate \( \delta t_s_i \). Next, define the corrected carrier phase measurement \( \bar{z}_i(k) \triangleq z_i(k) + \delta t_s_i \), which can be approximated as

\[
\bar{z}_i(k) \approx ||r_r(k) - r_s_i||_2 + c\delta t_r(k) + v_i(k), \quad \forall k > k_0.
\]

Subsequently, the corrected carrier phase measurements were fed to an extended Kalman filter (EKF) to solve the state vector \( x(k) \triangleq [r_r(k), \dot{r}_r(k), \delta t_r(k), \delta t_s_i(k)]^T \), where \( \dot{r}_r(k) \) is the UAV’s 2–D velocity vector and \( \delta t_r(k) \) is the receiver’s clock drift. A nearly constant velocity model was used for the UAV’s position and velocity dynamics, and a standard double integrator driven by process noise was used to model the clock bias and drift dynamics [58]. As such, the discrete-time dynamics model of \( x \) are given by

\[
x(k+1) = Fx(k) + w(k),
\]

where \( F \) is the state transition matrix obtained according to [58] and \( w(k) \) is the process noise vector, which is modeled as a
Fig. 11. Ground-truth and estimated trajectories using CON receiver for 5G NR signals on a UAV. The CON receiver yielded a UAV position RMSE of 4.35m. Map data: Google Earth.

zero-mean Gaussian random vector with covariance matrix $Q$ obtained according to [58]. The UAV’s $x, y$ acceleration process noise spectra in the nearly constant velocity model were set to $\tilde{q}_x = \tilde{q}_y = 10 \text{ m}^2/\text{s}^3$, and the receiver’s clock process noise was chosen to be that of a typical temperature-compensated crystal oscillator (TCXO) [58]. Note that $r_r(k)$ is expressed in an East-North-Up (ENU) frame centered at the UAV’s true initial position. The EKF state estimate was initialized at $\hat{x} = 0_{6 \times 1}$ with an initial covariance of $\Sigma = 4 \cdot I_{6 \times 6}$. The measurement noise covariance was set to $R = 2 \cdot I_{2 \times 2}$.

The position RMSE of the UAV was calculated to be 4.35 m with the aforementioned parameters. The true and estimated UAV trajectories are shown in Fig. 11.

5) Effect of False Alarm: The effect of a false alarm on the performance of the tracking loops is assessed next. It will be demonstrated that if at the acquisition stage a false alarm happens and a gNB is mistakenly detected, the carrier phase error will not converge in the tracking loops. In this case, the proposed method should neglect the detected source. To demonstrate this experimentally, Fig. 12 plots the likelihood function. In this experiment, the acquisition stage is forced to detect a false alarm, i.e., the acquisition stage is confirming the existence of a source which does not exist. Fig. 13 demonstrates the carrier phase error for the valid gNB and the false alarm gNB. As it can be seen in Fig. 13, the carrier phase error for the valid gNB converges whereas the carrier phase error for the false alarm is not. It should also be noted that $P_{fa}$ can be selected based on the operating environments.

C. CON With LTE Signals: Comparing With a Conventional Receiver When the RSs are Always-On

This experiment was conducted with real LTE signals on a UAV to (i) compare the navigation performance with a receiver which exploits all the available RSs in a scenario where the RSs are always-on, and (ii) to evaluate the performance of the CON receiver in an environment with multiple LTE eNodeBs operating in the same carrier frequency. The experimental setup and results are discussed next.

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

2) Acquisition Results: The recorded LTE signals were processed in two ways for comparison: (i) using the proposed CON receiver and (ii) using the conventional LTE receiver developed in [59]. The conventional LTE receiver detected 11 eNodeBs over the 4 channels. The locations of the eNodeBs were mapped prior to the experiment and are shown in Fig. 14. Next, the signal acquisition stage was applied to detect the ambient LTE eNodeBs. The detection threshold was set such that $P_{fa} = 10^{-4}$, which yielded $\eta_i = 1.012$, $K$ was set to 40, and $T_{sub}$ was set to 10 ms for all $i$. Doppler estimation was performed in a similar as the previous experiment. The acquisition stages for the 1955 MHz carrier frequency are shown in Fig. 15. In particular, Fig. 15 shows how the likelihood function changes as sources are detected and nulled by the CON receiver. The conventional
LTE receiver detected two eNodeBs at the 1955 MHz carrier frequency, denoted by eNodeB 1 and eNodeB 2 in Fig. 14, with eNodeB 1 having a Doppler frequency of $-18.5$ Hz and eNodeB 2 having a Doppler frequency of $-17.5$ Hz. The CON receiver detected 3 eNodeBs at the 1955 MHz carrier frequency with Doppler frequencies $-22$ Hz, $-18$, and $18$ Hz. The eNodeBs detected by the CON receiver were manually associated with the ones detected by the conventional receiver by matching the Doppler and delay profiles. Sophisticated data association techniques could be employed to perform this step; however, it is out of the scope of the current paper. After performing data association, it was found that only one of the Doppler frequencies detected by the CON receiver pertains to the ones detected by the conventional receiver. Specifically, the CON receiver detected eNodeB 1 at a $-18$ Hz Doppler frequency, which is 0.5 Hz off from the one estimated by the conventional receiver. This error is due to the 1 Hz step size used in the Doppler search. For $K = 40$, the condition from Theorem 1 for the CON receiver to be able to distinguish between eNodeB 1 and eNodeB 2 at the specified $P_{fa} = 10^{-4}$ is that the difference between their Doppler frequencies must be greater than 1.25 Hz. However, the Doppler frequency difference between eNodeB 1 and 2 measured by the conventional receiver is 1 Hz which violates the aforementioned condition. This direct consequence of Theorem 1 explains why the CON receiver could not detect eNodeB 2. Similar acquisition results are obtained with the remaining carrier frequencies. A total of 11 eNodeBs were acquired by the CON receiver. After manual data association, it is found that only 6 of them pertain to the ones detected by the conventional receiver (eNodeBs 1, 4, 5, 7, 8, and 10) and the rest pertain to unknown eNodeBs that were not detected by the conventional receiver.

3) Tracking Results: After acquiring the Doppler frequencies and the RSs, the tracking loops are initialized and the signals are tracked. Fig. 16 shows the resulting carrier phases, expressed in meters, obtained using the CON and conventional receivers for the eNodeBs acquired on the 1955 MHz carrier frequency. The carrier phase expressed in meters is a smoother estimate of the true range than the RS delays. The subsequent analyses focus on carrier phase measurements since they will be used to compute the navigation solution. The carrier phase RMSE values are summarized in Table III. Note that eNodeBs 2, 3, 6, 9, and 11 are not included in Table III since they were not detected by the CON receiver; however, as mentioned previously, the CON receiver acquired and tracked 5 unknown eNodeBs that were not detected by the conventional LTE receiver. One example is shown in Fig. 16. For fair comparison, only the common eNodeBs will be used to compute a navigation solution.

4) Navigation Solution: The navigation framework discussed in SubSection V-A is employed to compute the UAV’s 2-D position from the navigation observables produced by the CON and conventional receivers. Two position estimates were calculated using six carrier phase measurements from the eNodeBs in Table III: (i) for the conventional receiver and (ii) for the CON receiver. The position RMSE of the conventional and CON receivers were both calculated to be 2.07 m. The true and estimated UAV trajectories are shown in Fig. 17.
A CON receiver architecture was proposed to extract navigation observables from 5G signals, without requiring knowledge of the 5G RSs. To exploit the full ranging accuracy that can be achieved with 5G signals, the proposed CON receiver was designed to estimate the RSs from multiple 5G gNBs and exploit them for navigation purposes. The acquisition stage of the CON receiver was modeled as a sequential detection problem. The GLR test was derived to sequentially estimate the number of active gNBs, their RSs, and Doppler frequencies. Tracking loops were also designed in order to refine and maintain the estimates provided by the acquisition stage. Real 5G signals were used to assess the capabilities of the proposed CON receiver. Extensive experimental results were presented demonstrating the capabilities of the proposed CON receiver with real 5G and 4G signals on ground and aerial platforms. On a ground vehicle, it was demonstrated that the CON receiver yields a reduction of 10% and 37.7% in the estimated delay and Doppler RMSE, respectively, over that achieved with a conventional opportunistic navigation 5G receiver. On a UAV, it was demonstrated that the CON receiver enables the UAV to navigate over 416 m trajectory with 5G NR gNBs, achieving a position RMSE of 4.35 m.

Appendix A

Derivation of Likelihood Function (12)

For a known \( \mathcal{W}_i \), the singular value decomposition (SVD) of the matrix \( B_{i-1} \) can be written as

\[
B_{i-1} = [W_{i-1} \ U_{i-1}] \begin{bmatrix} \Sigma_{i-1} & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} W_{i-1}^H \\ U_{i-1}^H \end{bmatrix}
\]

(29)

where \( W_{i-1} \) and \( U_{i-1} \) are \( KL \times (i-1)L \) and \( KL \times (K-L-(i-1)L) \) orthogonal matrices that span the column space of \( B_{i-1} \) and orthogonal column space of \( B_{i-1} \), respectively. In other words, \( U_{i-1}^H B_{i-1} = 0 \). Therefore,

\[
U_{i-1}^H y = U_{i-1}^H H_i s_i + U_{i-1}^H w_{\text{eq}}.
\]

(30)

As it was mentioned previously, the complex envelope of the OFDM signals can be considered to be asymptotically white and Gaussian [60]. Here, the GLR test is derived assuming that \( w_{\text{eq}} \sim \mathcal{N}(0, \sigma_w^2 I) \). It should be noted that since \( U_{i-1}^H U_{i-1} = I \), the statistical characteristics of noise is preserved, i.e., \( U_{i-1}^H w_{\text{eq}} \sim \mathcal{N}(0, \sigma_w^2 I) \). By multiplying the observation vector by \( U_{i-1}^H \), (11) can be written as

\[
\begin{align*}
H_i^0 : U_{i-1}^H y &= U_{i-1}^H w_{\text{eq}}, \\
H_i^1 : U_{i-1}^H y &= U_{i-1}^H H_i s_i + U_{i-1}^H w_{\text{eq}}.
\end{align*}
\]

(31)

For the linear detection problem (31), the GLR can is derived as [53, Section 9.4.3]

\[
\mathcal{L}_i(y|W_i) = \frac{y^H P_{S_i} y}{y^H P_{B_{i-1}} P_{S_i} P_{B_{i-1}}^H y},
\]

(32)

where \( P_{S_i} = P_{B_{i-1}} H_i \) and

\[
P_{B_{i-1}} = U_{i-1}^H = I - B_{i-1} (B_{i-1}^H B_{i-1})^{-1} B_{i-1}^H.
\]

(33)

Appendix B

Proof of Lemma 1

The matrices \( H_i \) and \( P_{B_{i-1}} \) can be written as

\[
H_i = h_i \otimes I_L, \quad P_{B_{i-1}} = \tilde{P}_{i-1} \otimes I_L,
\]

(34)

where, \( h_i \triangleq [1, \exp(j \omega_L), \ldots, \exp(j \omega (K-1)L)]^T, \quad \tilde{P}_{i-1} \triangleq (I - B_{i-1} (B_{i-1}^H B_{i-1})^{-1} B_{i-1}) \), \( B_{i-1} \triangleq \{h_1, \ldots, h_i\} \), and \( \otimes \) denotes the Kronecker product. Hence, one can write

\[
H_i^H \tilde{P}_{i-1} H_i = (h_i^H \tilde{P}_{i-1}^H h_i) \otimes I_L.
\]

(35)

The scalar \( h_i^H \tilde{P}_{i-1}^H h_i \) can be written as

\[
h_i^H \tilde{P}_{i-1}^H h_i = c_{ii} - \sum_{i=1}^{K-1} \exp(j \omega_j - \omega_i) L K_i.
\]

(36)

which is the Schur complement of \( C_{i-1} \) of matrix \( C_i \) in (15), with \( c_{ij} \triangleq \sum_{k=0}^{K-1} \exp(j \omega_j - \omega_i) L k \).

Appendix C

Proof of Theorem 1

Proof: To prove that the likelihood ensures the CFAR property, the asymptotic distributions of the numerator and the denominator of the likelihood in (12) are determined under the null hypothesis. It is then shown that as \( K \to \infty \), the asymptotic distribution of the likelihood is not a function of unknown parameters if the Doppler frequencies and their estimates satisfy the conditions described in Theorem 1.

According to (9), under the null hypothesis of the second stage, i.e., \( H_0^i \), the received signal vector can be written as

\[
y = B_1 \theta_1 + w_{\text{eq}2},
\]

where in a scenario with two sources with Doppler frequencies \( w_1 \) and \( w_2 \) one has \( B_1 = H_1 \) and \( \theta_1 = s_1 \).

Hence, replacing \( y = B_1 \theta_1 + w_{\text{eq}2} \) in the numerator of the likelihood (12) results in

\[
N(y) = s_1^H H_1^H \tilde{P}_{s_1} H_1 s_1 + w_{\text{eq}2}^H \tilde{P}_{s_2} w_{\text{eq}2} + 2 \Re \left\{ s_1^H H_1^H \tilde{P}_{s_1} w_{\text{eq}2} \right\},
\]

(37)
where $\mathbf{P}_{s2} \triangleq \mathbf{P}_{H2} \mathbf{H}_2^{-1} \mathbf{H}_2^H \mathbf{P}_{H2}^{-1}$, and $\mathbb{R}\{\cdot\}$ denotes the real part. Since, for all values of $i \neq j$, one has $\mathbf{H}_i^H \mathbf{H}_j = K L_i$, and $\mathbf{H}_i^H \mathbf{H}_j = \exp(j(\omega_j - \omega_i)(K - 1)/2) \sin\left(\frac{\omega_j - \omega_i}{2}\right) \mathbf{I}_L$, it can be shown that

$$s_1^H \mathbf{H}_1^H \mathbf{P}_{s2} \mathbf{H}_1 s_1 = \left| S(\omega_1, \omega_2) - S(\omega_1, \hat{\omega}_1) S(\omega_2, \hat{\omega}_2) \right|^2 \frac{K}{K^2 - |S(\omega_1, \omega_2)|^2 s_1^H s_1},$$  

(38)

where $S(\omega_1, \omega_2) \triangleq \frac{\sin(\omega_1 - \omega_2)}{\sin(\omega_1 - \omega_2) K L}$ is the Doppler estimation error of $\omega_1$, defined as $\Delta \omega_1 \triangleq \omega_1 - \hat{\omega}_1$, and $|\Delta \omega_1| \ll \frac{\pi}{T_r}$, and the difference between the estimate of the Doppler frequencies of the 2nd gNB and the 1st gNB satisfies $|\omega_2 - \omega_1| > \frac{\pi}{T_r}$; then, the following limit holds

$$\lim_{K \to \infty} \frac{K}{K^2 - |S(\omega_1, \omega_2)|^2 s_1^H s_1} = 0.$$  

(39)

The last term on the right hand side of (37) is a random variable with mean $\mathbb{E}\{s_1^H \mathbf{H}_1^H \mathbf{P}_{s2} \mathbf{w}_{eq2}\} = 0$ and variance $\sigma_w^2 s_1^H \mathbf{P}_{s2} \mathbf{H}_1 s_1$, which according to (39), asymptotically tends to zero as $K \to \infty$. Therefore, with probability one. Using similar steps for the denominator of (12), denoted by $D(y)$, it can be shown that

$$\lim_{K \to \infty} D(y) = w_{eq2}^H \left( \mathbf{P}_{H1} - \mathbf{P}_{s2} \right) w_{eq2},$$

(41)

with probability one. According to equation (2.29) in [53], since $\mathbf{P}_{s2}$ and $\mathbf{P}_{H1}$ are idempotent matrices, $\sigma_n^2 \sim \chi^2_{2L_1}$, and $\frac{D(y)}{\sigma_n^2} \sim \chi^2_{2(K-1)}$ as $K \to \infty$. Hence, the asymptotic distribution of the likelihood (12) is not a function of the noise variance and the unknown Doppler frequencies which proves the CFAR property.

REFERENCES

143

Mohammad Neinavaie (Graduate Student Member, IEEE) received the M.S. degree in digital communication systems from Shiraz University, Shiraz, Iran. He is a Ph.D. Student with the University of California, Irvine, CA, USA, and a Member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. His research interests include opportunistic navigation, cognitive radio, wireless communication systems, and software-defined radio.

Joe Khalife received the B.E. degree in electrical engineering, the M.S. degree in computer engineering from the Lebanese American University (LAU), Beirut, Lebanon, and the Ph.D. degree in electrical engineering and computer science from the University of California, Irvine, CA, USA. He is a Postdoctoral Fellow with the University of California, Irvine, and a Member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. From 2012 to 2015, he was a Research Assistant with LAU, and has been a Member of the ASPIN Laboratory since 2015. His research interests include opportunistic navigation, autonomous vehicles, and software-defined radio. He was the recipient of the 2016 IEEE/ION Position, Location, and Navigation Symposium (PLANS) Student Paper Award and the 2018 IEEE Walter Fried Award.

Zaher (Zak) M. Kassas (Senior Member, IEEE) received the B.E. degree in electrical engineering from the Lebanese American University (LAU), Beirut, Lebanon, and the M.S. degree in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, 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, TX, USA. He is an Associate Professor with the University of California, Irvine, CA, USA, and the Director of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He is also the Director of the U.S. Department of Transportation Center: CARMEN (Center for Autonomous Vehicle, and software-defined radio). He was the recipient of the 2018 National Science Foundation (NSF) Faculty Early Career Development Program (CAREER) Award, and 2019 Office of Naval Research (ONR) Young Investigator Program (YIP) Award, the 2018 IEEE Walter Fried Award, 2018 Institute of Navigation (ION) Samuel Burka Award, 2018 ION Col. John D. Stickel Award. He is the Senior Editor for the IEEE TRANSACTIONS ON INTELLIGENT VEHICLES and an Associate Editor for the IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS and the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. His research interests include cyber-physical systems, estimation theory, navigation systems, autonomous vehicles, and intelligent transportation systems.