Cognitive Detection of Unknown Beacons of Terrestrial Signals of Opportunity for Localization

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

***Abstract*—A cognitive approach is proposed to detect unknown beacons of terrestrial signals of opportunity (SOPs). Two scenarios are considered in the paper: (i) detection of unknown beacons with integer constraints (IC) and (ii) detection of unknown beacons with no integer constraint (NIC). An example of beacons with IC is the pseudo-noise (PN) sequences in cellular code division multiple access (CDMA) signals. On the other hand, the reference signals (RSs) in orthogonal frequency-division multiplexing (OFDM)-based systems can be considered as beacons signals with NIC. Matched subspace detectors are proposed for both scenarios, and it is shown experimentally that the proposed matched subspace detectors are capable of detecting cellular third-generation (3G) cdma2000 signals and fifth-generation (5G) OFDM signals. A low complexity method is derived to simplify the matched subspace detector with IC for M-ary phase shift keying (MPSK) modulation. The effect of symbol errors in the estimated beacon signal on the carrier to noise ratio (CNR) is characterized analytically. Closed-form expressions for the asymptotic probability of detection and false alarm are derived. Experimental results are presented showing an application of the proposed cognitive approach by enabling an unmanned aerial vehicle (UAV) to detect and exploit terrestrial cellular signals for navigation purposes. In one experiment, the UAV achieved submeter-level accurate navigation over a trajectory of 1.72 km, by exploiting signals from four 3G cdma2000 transmitters. In another experiment, the UAV achieves a position root mean-squared error (RMSE) of 4.63 m over a trajectory of 416 m, by exploiting signals from two 5G transmitters.**

***Index Terms*—cognitive radio, navigation, signals of opportunity, blind symbol detection.**

I. Introduction

Global navigation satellite system (GNSS) signals suffer from constraining limitations in deep urban environments and are prone to jamming and spoofing. In spite of these limitations, we live in a world rich with man-made signals of opportunity (SOPs), which have been demonstrated as feasible complements or alternatives to GNSS in challenging environments [1]. SOP navigation receivers typically rely on known synchronization sequences or beacons transmitted by SOP sources to draw time-of-arrival (TOA), direction-of-arrival (DOA), and frequency-of-arrival (FOA) measurements [2]–[5].

Cognitive opportunistic navigation [6] has been recently introduced to addresses the following challenges of navigation with SOPs:

This work was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-22-1-0476.

M. Neinavaie and Z. Kassas are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210. J. Khalife was the Department of Mechanical and Aerospace Engineering, University of California, Irvine, CA 92697. *Corresponding author: Z. Kassas*, email: zkassas@ieee.org

Unknown reference signals in private networks: Opportunistic navigation frameworks usually rely on the broadcast reference signals (RSs), which are used to derive DOA and TOA [3]. For public networks, these signals are known at the user equipment (UE) and are universal across network operators. Hence, they can be exploited for positioning without the need for the UE to be a network subscriber. However, in *private networks*, the signal specifications of some SOP sources may not be available to the public, which makes acquiring and tracking these signals impossible for conventional opportunistic navigation receivers [6]. Private networks and broadband providers do not usually disclose the transmitted signal structure to protect their intellectual property. For instance, very limited information is available about Starlink satellite signals.

Dynamic nature and ultra-lean transmission of the fifth-generation (5G) new radio (NR) and beyond networks: In cellular long-term evolution (LTE) networks, several RSs, such as the cell-specific reference signal (CRS), are broadcast at regular and known time intervals, regardless of the number of UEs in the environments. This *always-on* type of transmitted RSs reduces the network's energy efficiency and increases operational expenses and interference. One of the main features of 5G NR, is ultra-lean transmission, which minimizes the transmission of always-on signals. For instance, CRS which used to be an always-on RS in LTE, is not necessarily being continuously transmitted in 5G signals. On the other hand, the RSs in 5G networks and beyond can be dynamic and may continuously change [7]. As such, designing cognitive receivers that can cognitively acquire *partially known*, *unknown*, or *dynamic* beacon signals is an emerging need for the future of cognitive navigation [6], [8]–[10] [1].

This paper considers a cognitive opportunistic approach to detect the unknown beacon of terrestrial SOPs to enable exploitation of these signals for positioning and navigation purposes. Two scenarios are considered: (i) unknown beacon signals with integer constraints (IC) on the symbols of the beacon, and (ii) unknown beacon signals with no integer constraints (NIC). An example of beacons with IC is pseudo-noise (PN) sequences in cellular code division multiple access (CDMA), while an example of beacons with NIC are the RSs in orthogonal frequency-division multiplexing (OFDM)-based systems. Since the symbols of PN sequences in CDMA signals

[1] In this paper, only the length of the beacon signals is assumed to be known at the receiver. It should be pointed out that period estimation techniques, e.g., [11], can be used to estimate the length of the beacon sequence in a preprocessing stage.

are drawn from a set with a finite alphabet size, e.g., phase shift keying (PSK) set, they can be categorized as beacons with IC. On the other hand, the RSs in OFDM-based systems, e.g., secondary synchronization signal (SSS) in cellular LTE and 5G NR, are arbitrary complex numbers in the time domain and, therefore, can be categorized as beacon signals with NIC.

The main contributions of this paper are as follows:

- A cognitive opportunistic navigation method is proposed, whereby unknown beacons of terrestrial SOPs are detected, enabling exploitation of these signals for navigation purposes. To this end, matched subspace detectors are implemented practically for two different scenarios: (i) beacons with IC, e.g., the symbols of the beacon are drawn from M-ary PSK (MPSK) modulation set, and (ii) beacon with NIC, i.e., the beacon signal are not constrained to take integer values and can assume any arbitrary complex-valued number.
- A near-optimal algorithm which has a lower computational complexity compared to the traditional detectors with IC is proposed. The effect of the symbol errors in the detected beacon signal on the carrier-to-noise ratio (CNR) is characterized analytically. The proposed matched subspace detectors are shown to be capable of detecting multiple unknown real 5G NR and 3G signals with a relatively low computational complexity.
- For the NIC scenario, closed-form expressions for the probability of detection and false alarm are derived. The effective signal to noise ratio (SNR) is calculated and the effect of Doppler estimation error on the performance of the detector is analyzed. It is shown that the coherence processing interval (CPI) can be selected optimally in the sense that it maximizes the probability of detection. The estimated CPI is shown to provide better estimation of the beacon signal in a practical scenario. To the best of the authors' knowledge, the estimation of CPI has not been previously studied in the literature.
- Experimental results are presented showing an application of the proposed cognitive approach by enabling an unmanned aerial vehicle (UAV) to detect and exploit terrestrial cellular signals for navigation purposes. In one experiment, the UAV achieved submeter-level accurate navigation over a trajectory of 1.72 km, by exploiting signals from four 3G cdma2000 transmitters. In another experiment, the UAV achieves a position root mean-squared error (RMSE) of 4.63 m over a trajectory of 416 m, by exploiting signals from two 5G transmitters. It should be pointed out that the number of currently active 5G transmitters are relatively lower than that of the previous generations. The 5G NR navigation results will be improved dramatically with more active 5G transmitters.
- The OFDM frame of 5G signals are reconstructed in a blind fashion. On-demand and always-on beacons are demonstrated in the OFDM signal structure of real 5G signals. To the best of the authors' knowledge, the blind reconstruction of the OFDM frame of 5G signals has not been done in any other work in the current literature.

The rest of this paper is organized as follows. Section II surveys relevant related work. Section III presents the received baseband signal model. Section IV derives the generalized likelihood ratio (GLR) detector for beacons of terrestrial SOPs, when the elements of the beacons are drawn from MPSK modulation, while Section V analyzes the performance of the derived detector. Section VI derives the GLR detector for beacons of terrestrial SOPs when the elements of the beacons are arbitrary complex numbers. Section VII presents experimental results for cognitive detection of both beacons with IC and without NIC as well as an application of the proposed approach in the context of UAV navigation. Section VIII gives concluding remarks.

II. Related Work

A. Positioning with Terrestrial Signals

Opportunistic navigation with different SOPs has been demonstrated in the literature [12]. Cellular [13], digital television [14], AM/FM [15], Wi-Fi [16], and low Earth orbit (LEO) satellite signals [17], are SOP examples which have been considered in the literature. In particular, terrestrial signals have attracted considerable attentions due to their desirable attributes, namely: (i) abundance, (ii) diversity diversity in transmission frequency, (iii) high received carrier-to-noise ratio, and (iv) free usage. Moreover, some SOPs (e.g., cellular) transmit high bandwidth signals which yield precise TOA estimates and are placed in favorable geometric configuration, which yield low dilution of precision (DOP) measures.

Although meter-level and submeter-level SOP-based navigation solutions have been demonstrated on ground vehicles and UAVs, such results have been achieved with methods which require knowledge of the beacons transmitted by the SOP. These methods would fail if the beacon signal is unknown and/or some signal parameters change due to the dynamic nature of wireless protocols. The approach proposed in this paper addresses these issues by cognitively detecting all the active sources and estimating the underlying beacons with minimal prior knowledge for both CDMA and OFDM-based communication systems.

B. Detection of Signals with IC: CDMA

The detection problem for both IC and NIC scenarios leads to *matched subspace detectors*, which have been widely studied in the classic detection literature [18]–[21]. In the detection problem with IC, the integer constraint of the beacon symbols in the matched subspace detectors leads to a class of integer least square problems [22]–[24]. One example of beacons with IC is the PN sequence in CDMA-based communication systems. A low computational complexity approach to estimate the beacon symbols is the *symbol by symbol* (SBS) estimation which suffers from a poor performance in low SNR regimes. In [25], an SBS estimation scheme was considered to blindly estimate the symbols of the PN sequences of Galileo and Compass satellites, and a 1.8 m high-gain antenna was used to accumulate enough signal power. The optimal algorithm proposed in [23] and [24] can be used to solve the integer least squares problem with a polynomial computational complexity.

The computational and hardware complexity of the integer least squares problem are two of the main challenges that should be addressed in a cognitive opportunistic navigation framework. In this paper, a near optimal beacon detector with linear computational complexity is proposed to reduce the computational complexity of the detection problem of terrestrial signals with IC.

C. Signals with NIC: LTE and 5G

The beacon signals in LTE and 5G signals are not considered to be taking integer values and can assume any arbitrary complex-valued numbers. Therefore, they can be considered as beacons with NIC. The positioning capabilities of LTE signals have been investigated in the literature over the past few years [13], [26]–[29], and several software-defined receivers (SDRs) have been proposed to extract TOA and DOA from real and laboratory-emulated LTE signals [3], [30]–[33]. Experimental results demonstrated navigation solutions with different types of LTE RSs in different environments, achieving meter-level [30], [34], [35] and sub-meter-level [36] accuracy. Positioning with 5G signals has also been studied in the literature [37]–[39]. 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 considered for 5G [40]. To mitigate the high path loss of propagated mmWave signals different beamforming techniques and massive multiple-input, multiple-output (mMIMO) antenna structures are proposed for the 5G protocol [41]. Since beamforming in 5G requires the knowledge of the user's location, 5G-based positioning is essential for resource allocation [42]. The signal characteristics of mmWave for positioning were studied in [43]. The Cramér-Rao lower bounds (CRLBs) of the direction-of-departure (DOD), DOA, and TOA promisses a sub-meter positioning error and sub-degree orientation error with both uplink and downlink mmWave signals [44], [45]. A two-stage Kalman filter was used to estimate the DOD and UE's position using the signal strength from multiple base stations in [46], showing sub-meter-level three-dimensional (3-D) position accuracy. A two-way distributed localization protocol was proposed in [47] to remove the effect of the clock bias in TOA estimates. In [48], 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, showing less than 15 m position RMSE and less than 7 degree orientation RMSE. Using the DOD and TOA of the received signal, a positioning method for multiple-output single-input systems was proposed in [42]. In [49], estimation of signal parameters via rotational invariant techniques (ESPRIT) was used to estimate the DOA and DOD of the signal. [50] focuses on the integrated positioning methodology of GNSS and device to device (D2D) measurements in 5G communication networks. In [39], a tensor-based method for channel estimation in mmWave systems is presented which enables positioning and mapping using diffuse multipath in 5G mmWave communication systems. Experimental results in [51] 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 unknown beacons, of terrestrial SOPs, with IC (e.g., CDMA) and NIC (e.g., OFDM), which enables the exploitation of these SOPs, for navigation purposes. In other words, regardless of the communication scheme, the proposed cognitive framework is capable of detecting terrestrial SOPs, estimate the Doppler frequencies, and detect the beacon signals.

D. Cognitive Navigation

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 [25], which revealed the spread spectrum codes for these satellites. Preliminary experiments on navigation with partially known and unknown signals from low and medium Earth orbit satellites were conducted in [9], [10], [17], [52], [53]. While these approaches yielded useful insights, a more comprehensive study is required to develop a general framework for the detection of cellular CDMA and 5G signals. A cognitive method for navigation with 5G signals was also presented in [6].

The method presented in [6] considers beacons with NIC. The NIC-based method presented in this paper is computationally more efficient than the method presented in [6]. The acquisition stage in [6] requires a sequential detection scheme whose computational complexity grows as a polynomial function of the number of unknown sources in the environment. On the other hand, the detection method presented in this paper has a fixed computational complexity of the number of unknown sources. Moreover, this paper analyzes the detection performance of the NIC-based detector and assesses analytically the effect of Doppler estimation error.

III. Received Baseband Signal Model

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

$$y[n] = \alpha \exp\left(j2\pi\Delta f n\right) \sum_{i=-\infty}^{\infty} c[n - iL - n_d] + w[n], \quad (1)$$

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

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

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

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

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

$$\mathbf{y} = \alpha \mathbf{H}\mathbf{s} + \mathbf{w}_{\text{eq}}, \tag{2}$$

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

$$\mathbf{H} \triangleq [\mathbf{D}, \exp(j2\pi\Delta f L)\mathbf{D}, \ldots, \exp(j2\pi\Delta f (K-1)L)\,\mathbf{D})]^{\mathsf{T}}, \tag{3}$$

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

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

IV. Terresterial Signal Activity Detection with IC

In this section, GLR detector is derived to detect the beacon signals of terrestrial SOPs when the elements of the beacon $\mathbf{s}$ are drawn from MPSK modulation. One example of this type of beacons is the PN sequences in CDMA-based systems. Globalstar LEO satellites employ a 4PSK CDMA system. The spreading sequence structure is comprised of an inner PN sequence pair and an outer PN sequence which are drawn from 4PSK modulation scheme. Another example of this type of beacons is transmitted by Orbcomm satellites. The Orbcomm communication system utilizes the classic symmetric differential phase shift keying (SDPSK) as the modulation scheme for the downlink signals. The following Remark explains how (2) is descriptive of a CDMA-based system scenario.

Remark 2: In CDMA systems, several logical channels are multiplexed on the same physical channel. For example, there is a total of 128 logical channels multiplexed onto the cdma2000 physical forward channel: (i) one pilot channel, (ii) one sync channel, (iii) up to seven paging channels, and (iv) traffic on the remaining channels. Each of these logical channels is spread orthogonally by a 128-Walsh code, multiplexed with the rest of the channels, and the resulting signal is multiplied by a complex PN sequence which consists of a pair of maximal-length sequences. In such a system, and CDMA systems in general, the signal on the pilot channel simplifies to the complex PN sequence, which is the beacon of interest. Therefore, one can look at the CDMA signal as the sum of (i) the signal on the pilot channel, or the beacon signal and (ii) the sum of the remaining channels. Due to the properties of Walsh codes and assuming the symbols on the sync, paging, and traffic channels are uncorrelated, one can model the aforementioned second term as noise. In fact, for a large number of logical channels such as in cdma2000 and Globalstar, the *central limit theorem* practically applies and the resulting noise can be modeled as a zero-mean Gaussian random sequence with a determined variance [54]. Consequently, the CDMA signal can be modeled according to (1), where $s[n]$ is the beacon on the pilot channel, and $w[n]$ captures channel noise and the effect of the rest of the logical channels.

The following binary hypothesis test is considered

$$\begin{cases} \mathcal{H}_0: & \mathbf{y} = \mathbf{w}_{\text{eq}} \\ \mathcal{H}_1: & \mathbf{y} = \alpha\mathbf{H}\mathbf{s} + \mathbf{w}_{\text{eq}}, \end{cases} \tag{4}$$

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

$$\mathcal{L}_{\text{IC}} = \frac{\max_{\mathbf{q}\in\mathcal{S},\Delta f} |\exp\left(-\frac{j2\pi}{M}\mathbf{q}^{\mathsf{H}}\right)\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2}{K^2\|\mathbf{y}\|^2} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_{\text{IC}}, \tag{5}$$

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

A. Integer Least Squares Problem

To derive the constrained GLR detector in (5), the following integer least squares problem should be solved

$$\underset{\mathbf{q}\in\mathcal{S},\Delta f}{\text{argmax}} \left| \mathbf{z}^{\mathsf{H}} \exp\left(\frac{j2\pi}{M}\mathbf{q}\right)\right|, \tag{6}$$

where, $\mathbf{z} \triangleq \frac{1}{K}\mathbf{H}^{\mathsf{H}}\mathbf{y}$. A solution to the optimization problem (6) consists of a linear search over Doppler candidates and an exponential exhaustive search over all possible values of $\mathbf{q}$. Denoting the number of Doppler search candidates by D, the order of the overall search is DM^L. The detection algorithm presented in [23] can be used to solve (6), optimally, with a complexity of order $O(DL\log L)$. However, due to the large size of the beacon signals in practice, the resulting computational complexity of existing methods is still significant. The following Lemma establishes a reduced number of search candidates.

Lemma 1. *The optimal solution of the optimization problem (6) can be obtained by searching over DL candidates.*

Proof: See Appendix B.

In what follows, a low-complexity beacon signal detection (LCBSD) algorithm of complexity $O(DL)$ to solve (6) is presented. Next, using numerical analysis it is shown that the proposed LCBSD algorithm performs almost similarly as the maximum likelihood (ML) estimator.

B. LCBSD Algorithm

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

$$\hat{\alpha}_{\mathrm{ML}} = \frac{1}{L}\left[\exp\left(\frac{j2\pi}{M}\mathbf{q}\right)\right]^{\mathsf{H}}\mathbf{z}. \tag{7}$$

Let $\mathbf{q}_l$ and $\mathbf{z}_l$ denote the vectors containing the first l elements of $\mathbf{q}$ and of $\mathbf{z}$, respectively, and let $\hat{\mathbf{q}}_l$ denote the corresponding estimate. From (7), the estimate of α obtained from $\hat{\mathbf{q}}_l$ is

$$\hat{\alpha}_l = \frac{1}{l}\left[\exp\left(\frac{j2\pi}{M}\hat{\mathbf{q}}_l\right)\right]^{\mathsf{H}}\mathbf{z}_l. \tag{8}$$

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

$$\hat{q}_l \triangleq \underset{q_l\in\{0,1,\ldots,M-1\}}{\operatorname{argmax}} \Re\left\{\alpha_l z_l^{\mathsf{H}} \exp\left(\frac{j2\pi}{M}q_l\right)\right\}, \tag{9}$$

where $\Re\{\cdot\}$ denotes the real part, z_l is the lth observation, and q_l is the lth element of $\mathbf{q}$ and $\hat{q}_l$ its corresponding estimate. Solving (9) yields

$$\hat{q}_l = \operatorname{round}\left[\frac{(\angle z_l - \angle\hat{\alpha}_l)\,M}{2\pi}\right] \mod M. \tag{10}$$

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

V. Performance Analysis

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

A. Carrier-to-Noise Ratio and TOA Measurements Error Variance

The navigation performance in TOA-based navigation depends on two main factors: (i) the DOP and (ii) the TOA estimation error variance. The DOP is strictly a function of the geometry between the transmitters and receiver. However, the TOA estimation error variance is a function of the CNR. From (1), it can be seen that the carrier power is given by $C = |\alpha|^2$. SOP receivers correlate the received signal with known, local replicas of the beacons to draw TOA measurements. The correlation function peaks at the TOA. Consequently, the TOA estimation performance is determined by the peak-to-noise ratio, which, in the case of fully known beacon, is the CNR. In cognitive opportunistic navigation, this peak-to-noise ratio, or apparent CNR, is less than the actual CNR since the magnitude of the correlation function peak is reduced due to errors in the detected beacon symbols. It was mentioned in the previous section that the LCBSD algorithm yields an ambiguity of M in the SOP receiver's local beacon symbols. This ambiguity translates to an initial phase rotation in the correlation function; therefore, it does not affect its amplitude. As a result, the magnitude of the correlation peak will be preserved, which in turn preserves the CNR.

B. Probability of Error Definition

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

$$P_e \triangleq \min_{m\in\{0,1,\ldots,M-1\}} \frac{1}{L}\sum_{l=0}^{L-1} \Pr\left[((\hat{q}_l - m) \mod M) \neq q_l\right]. \tag{11}$$

Let $m^\star$ denote the minimizer. The above expression cannot be computed straightforwardly since $\Pr\left[((\hat{q}_l - m^\star) \mod M) \neq q_l\right]$ varies with l. To see this, the symbol error probability curves were computed numerically from 10^6 Monte Carlo noise $\mathbf{w}_{\mathrm{eq}}$ realizations for $L = 2^{11}$, $M = 4$, and SNR of 4 and 10 dBs, and are shown Fig. 1.

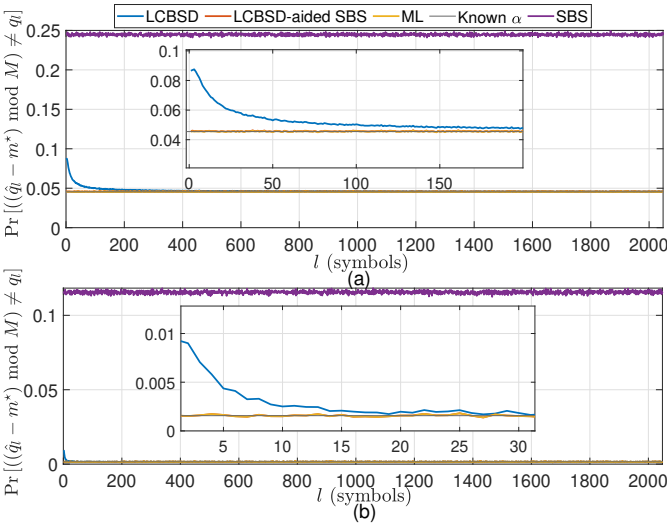

Fig. 1. Error probability $\Pr\left[((\hat{q}_l - m^\star) \mod M) \neq q_l\right]$ for (i) SBS detector (ii) the ML estimator, (iii) the proposed LCBSD algorithm, and (iv) the LCBSD-aided SBS detector versus l, for $L = 2^{10}$, $M = 4$: for (a) SNR = 4 dB, and (b) SNR = 10 dB.

Fig. 1 shows that the LCBSD performance converges to that of the ML as l increases. Comparing 1(a) and 1(b) shows that the rate of convergence is faster for larger values of SNR. It can be also seen that the ML and the proposed LCBSD algorithm outperform the SBS estimation dramatically. While SBS is adopted in [25], [52] for beacon symbol recovery, it yields a poor probability of error. LCBSD-aided SBS performs SBS estimation for all the beacon symbols after convergence of $\hat{\alpha}_l$. This step eliminates the transient of the LCBSD symbol error probability. It should be pointed out that in Fig. 1, the LCBSD-aided SBS, the ML method, and the method with known α are achieving *almost equal* probability of error in the considered SNR values. Moreover, Fig. 1 shows

that both the ML in [23] and the LCBSD error probabilities converge to the case that α is known. To this end, in the CNR analysis in Section V-C, the probability of error is assumed constant over l and is equal to that of SBS estimation when $\hat{\alpha}_l$ is known.

C. Apparent Carrier-to-Noise Ratio

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

$$\bar{C} = |\alpha|^2 \left| \mathbb{E}\left[\frac{1}{L} \sum_{l=0}^{L-1} s_l^* \hat{s}_l \right] \right|^2 = |\alpha|^2 \left| \frac{1}{L} \sum_{l=0}^{L-1} s_l^* \mathbb{E}\left[\hat{s}_l\right] \right|^2 . \quad (12)$$

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

$$\bar{C}/N_0 = |\alpha|^2\beta^2/N_0 = \beta^2 C/N_0, \quad (13)$$

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

D. Numerical Analysis

A numerical analysis is conducted to assess the effect of the proposed LCBSD algorithm in comparison to the ML algorithm on the apparent CNR. To this end, 10^6 Monte Carlo noise $\mathbf{w}_{\mathrm{eq}}$ realizations were generated for a beacon signal of length $L = 2^{11}$ with $M = \{2, 4\}$. The apparent CNR of the simplified GLR (SGLR) method in [22] is also compared with that of the proposed algorithm and the ML algorithm. The ratio β^2 is calculated and plotted as a function of the SNR, which is given by $\mathrm{SNR} = \frac{1}{\sigma^2}$. Fig. 2 shows that the proposed LCBSD algorithm is near optimal and obtains equal apparent CNR with the SGLR algorithm in [22] for BPSK and QPSK modulation schemes.

Remark 3: The method in [23] requires L divisions and the sorting operation, which can be accomplished by $L \log L$ complex operations. A total number of $L \log L + 4L - 3$ complex operations per Doppler bin is required for [23]. The total number of complex operations for the proposed method is $4L - 3$ per Doppler bin. It should be pointed out that the proposed method is as complex as the SBS algorithm after the convergence of $\hat{\alpha}_l$. In many practical scenarios, the coherence time of the channel might be of the order of tens to thousands of symbols [54]. During the channel coherence time, the algorithm does not need to keep updating $\hat{\alpha}_l$ after it converges. According to Fig. 1, the convergence rate of $\hat{\alpha}_l$ depends on the operating SNR and is relatively high.

VI. Terrestrial Signal Activity Detection with NIC

In this subsection, a GLR detector is proposed to detect the beacon signals when the elements of the beacon $\mathbf{s}$ are

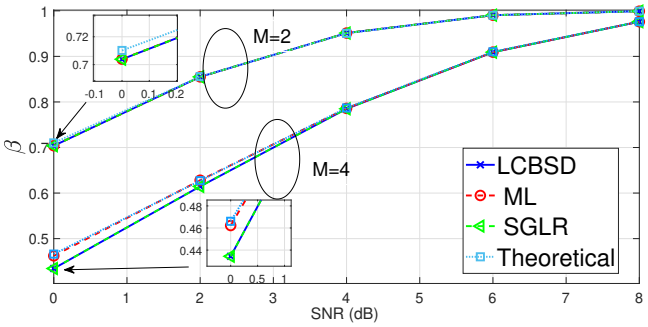

Fig. 2. Monte Carlo results for β^2 of (1) the ML estimator, (2) the proposed LCBSD algorithm, (3) the SGLR algorithm, and (4) the theoretical value (13) versus the SNR for $L = 2^{11}$ and $M = \{2, 4\}$.

arbitrary complex numbers. In OFDM-based systems such as LTE and 5G NR, the beacon sequences such as primary synchronization signal (PSS) and secondary synchronization signal (SSS) still have integer constraints. However, at the transmitter, the symbols are input to the inverse discrete Fourier transform (IDFT). Therefore, in the time domain, the equivalent beacon's elements are arbitrary complex numbers. The following Remark explains how (2) can be descriptive of an OFDM-based system.

Remark 4: NR adopts an OFDM scheme, as was the case in 4G LTE. In OFDM-based transmission, the symbols are mapped onto multiple carrier frequencies, referred to as subcarriers, with a particular spacing known as subcarrier spacing. Once the subcarrier spacing is configured, using a higher level signaling, the frame structure is identified. In LTE and 5G, a frame has a duration of 10 ms and consists of 10 subframes with durations of 1 ms [55]. To provide frame timing to the user, an OFDM-based system such as 5G NR, broadcasts synchronization signals (SS) on pre-specified symbol numbers. An SS includes a PSS and SSS, which provide symbol and frame timing, respectively. The SS and the data symbols are input to the IDFT. In [56], it is shown that the complex envelope of the OFDM signals can be considered to be asymptotically white and Gaussian. Therefore, in (2), $\mathbf{s}$ contains the complex elements of the IDFT of the SS and $\mathbf{w}_{\mathrm{eq}}$ captures the effect of receiver noise and data symbols which can be considered to be white Gaussian with variance σ^2.

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

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{w}_{\mathrm{eq}}, \quad (14)$$

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

$$\mathbf{H} \triangleq [\mathbf{I}_L, \exp(j2\pi\Delta f L)\mathbf{I}_L, \ldots, \exp(j2\pi\Delta f(K-1)L)\,\mathbf{I}_L)]^{\mathsf{T}}, \quad (15)$$

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

$$\begin{cases} \mathcal{H}_0: & \mathbf{y} = \mathbf{w}_{\mathrm{eq}} \\ \mathcal{H}_1: & \mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{w}_{\mathrm{eq}}. \end{cases} \quad (16)$$

The GLR detector for the testing hypothesis (4) is known as matched subspace detector, and is derived as [18]

$$\mathcal{L}_{\rm NIC} = \max_{\Delta f} \frac{\mathbf{y}^{\mathsf{H}}\mathbf{P}_{\mathbf{H}}\mathbf{y}}{\mathbf{y}^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{H}}\mathbf{y}}, \tag{17}$$

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

$$\frac{\mathbf{y}^{\mathsf{H}}\mathbf{P}_{\mathbf{H}}\mathbf{y}}{\mathbf{y}^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{H}}\mathbf{y}} = \frac{1}{\frac{\|\mathbf{y}\|^2}{\frac{1}{K^2}\|\mathbf{H}^{\mathsf{H}}\mathbf{y}\|^2} - 1}, \tag{18}$$

which is a monotonically increasing function of $\frac{\|\mathbf{H}^{\mathsf{H}}\mathbf{y}\|^2}{\|\mathbf{y}\|^2}$. Hence, the GLR detector (17) is equivalent to

$$\max_{\Delta f} \frac{\|\mathbf{H}^{\mathsf{H}}\mathbf{y}\|^2}{\|\mathbf{y}\|^2} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_{\rm NIC}, \tag{19}$$

where $\eta_{\rm NIC}$ is determined according to the desired probability of false alarm.

A. Derivation of Probability of Detection and False Alarm

In this subsection, closed-form expressions for the asymptotic probability of detection and false alarm are derived in the presence of Doppler estimation error and for a large CPI K. To this end, the pdfs of the numerator and the denominator of the likelihood function (17) are derived. Next, it is shown that the numerator and the denominator are statistically independent. Finally, for large values of K, the pdf of the ratio of the numerator and denominator is derived. The likelihood function (17) can be rewritten as

$$\frac{N(\mathbf{y})}{D(\mathbf{y})} = \frac{K(L-1)}{L}\frac{\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}_{\mathbf{H}}\mathbf{y}}{\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}^{\perp}_{\mathbf{H}}\mathbf{y}}, \tag{20}$$

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

$$\hat{\mathbf{s}} = (\hat{\mathbf{H}}^{\mathsf{H}}\hat{\mathbf{H}})^{-1}\hat{\mathbf{H}}^{\mathsf{H}}\mathbf{y} = \frac{1}{K}\hat{\mathbf{H}}\mathbf{H}\mathbf{s} + \frac{1}{K}\hat{\mathbf{H}}^{\mathsf{H}}\mathbf{w}_{\rm eq}. \tag{21}$$

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

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

$$\mathbf{v}^{\mathsf{H}}\mathbf{C}^{-1}\mathbf{v} \sim \begin{cases} \chi^2_{2r}, & \boldsymbol{\mu} = 0 \\ \chi'^2_{2r}(\lambda), & \boldsymbol{\mu} \neq 0, \end{cases} \tag{22}$$

where χ^2_{2r} denotes a chi-squared random variable with $2r$ degrees of freedom, $\chi'^2_{2r}(\lambda)$ denotes a noncentral chi-squared random variable with $2r$ degrees of freedom and non-centrality parameter λ, and $\lambda = \boldsymbol{\mu}^{\mathsf{H}}\mathbf{C}^{-1}\boldsymbol{\mu}$ [57].

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

$$\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}_{H}\mathbf{y} \sim \begin{cases} \chi^2_{2L} & \mathcal{H}_0 \\ \chi'^2_{2L}(\lambda) & \mathcal{H}_1, \end{cases} \tag{23}$$

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

$$\hat{\mathbf{H}}^{\mathsf{H}}\mathbf{H} = \rho\mathbf{I}, \tag{24}$$

where

$$\rho = \left|\frac{\sin(K\pi\Delta f_{\rm e}L)}{\sin(\pi\Delta f_{\rm e}L)}\right|, \tag{25}$$

and $\Delta f_{\rm e} = \Delta f - \widehat{\Delta f}$ is the Doppler estimation error. Hence, the non-centrality parameter of the numerator under $\mathcal{H}_0$ can be written as $\lambda = \frac{\rho\|\mathbf{s}\|^2}{\sigma^2}$. It should be pointed out that $0 \leq \rho \leq K$. The maximum value of ρ is obtained when $\Delta f_{\rm e} \to 0$. It will be shown that the probability of detection is characterized by λ. In other words, λ is the equivalent SNR for the GLR detector (17). Thus, when the Doppler estimation error $\Delta f_{\rm e}$ tends to zero, the equivalent SNR, i.e., λ, is maximized. It should be noted; however, that ρ, and in turn λ, may decay as the CPI increases in the case where $\Delta f_{\rm e}$ is not *small enough*. One can show that a sufficient condition for ρ to approach K as the latter increases is that

$$\Delta f_{\rm e} \ll \frac{1}{2KL}. \tag{26}$$

For the denominator of the likelihood function, one has

$$\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\hat{\mathbf{P}}^{\perp}_{H}\mathbf{y} = \left(\frac{\mathbf{H}\mathbf{s}}{\sigma} + \frac{\mathbf{w}}{\sigma}\right)^{\mathsf{H}}\hat{\mathbf{P}}^{\perp}_{H}\left(\frac{\mathbf{H}\mathbf{s}}{\sigma} + \frac{\mathbf{w}}{\sigma}\right) \tag{27}$$

The following Lemma is used to derive the pdf of (27).

Lemma 3: *If the $r \times 1$ vector $\mathbf{v}$ is distributed as $\mathbf{v} \sim \mathcal{CN}(\boldsymbol{\mu}, \mathbf{I})$, and $\mathbf{A}$ is an $r \times r$ Hermitian matrxi, $\mathbf{v}^{\mathsf{H}}\mathbf{A}\mathbf{v}$ has non-central complex chi-squared distribution with $\mathrm{rank}(\mathbf{A})$ degrees of freedom and non-centrality parameter $\boldsymbol{\mu}^{\mathsf{H}}\mathbf{A}\boldsymbol{\mu}$, if and only if $\mathbf{A}$ is an idempotent matrix* [57].

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

$$\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\mathbf{P}^{\perp}_{H}\mathbf{y} \sim \begin{cases} \chi^2_{2K(L-1)}, & \mathcal{H}_0 \\ \chi'^2_{2K(L-1)}(\lambda'), & \mathcal{H}_1, \end{cases} \tag{28}$$

where $\lambda' = \frac{1}{\sigma^2}\left(K - \frac{\rho}{K}\right)\|\mathbf{s}\|^2$, and ρ is defined in (25).

The pdf of numerator and denominator can be obtained using (23) and (28). Now, the independence of the numerator and the denominator of the likelihood function (17) is assessed using the following lemma.

Lemma 4: *Let the vector $\mathbf{v}$ be an $r \times 1$ complex Gaussian vector with mean $\boldsymbol{\mu}$ and covariance matrix $\mathbf{C}$, and let $\mathbf{A}$ and $\mathbf{B}$ be $r \times r$ Hermitian matrices. If $\mathbf{ACB} = \mathbf{0}$ then $\mathbf{v}^{\mathsf{H}}\mathbf{A}\mathbf{v}$ and $\mathbf{v}^{\mathsf{H}}\mathbf{B}\mathbf{v}$ are statistically independent* [57].

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

If (26) is satisfied, then

$$\lim_{K\to\infty}\frac{\sin(K2\pi\Delta f_{\rm e}L)}{\sin(2\pi\Delta f_{\rm e}L)} = K,$$

hence, according to (25), $\lim_{K\to\infty}\lambda' = 0$. A non-central chi-squared random variable with a non-centrality parameter of zero equals a central chi-square with the same parameters, under $\mathcal{H}_1$. Therefore, for a large number of K, one has $\frac{1}{\sigma^2}\mathbf{y}^{\mathsf{H}}\mathbf{P}^{\perp}_{H}\mathbf{y} \sim \chi'^2_{2K(L-1)}(0) \equiv \chi^2_{2K(L-1)}$, Finally, using the

following lemma, the pdf of the likelihood function can be obtained under both hypotheses.

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

$$f(x) = \exp\left(-\frac{\lambda}{2}\right) \sum_{k=1}^{\infty} \frac{(\lambda/2)^k}{k!} \frac{(r_1/r_2)^{\frac{1}{2}r_1+k}}{B\left(\frac{r_1+2k}{2}, \frac{r2}{2}\right)} x^{\frac{r_1}{2}+k-1} \left(1+\frac{r_1}{r_2}x\right)^{-\frac{1}{2}(r_1+r_2)-k}, \quad (29)$$

with r_1 and r_2 degrees of freedom, where λ is the noncentrality parameter, and $B\left(\frac{r_1+2k}{2}, \frac{r2}{2}\right)$ is the beta function defined as $B(x,y) \triangleq \int_0^1 t^{x-1}(1-t)^{y-1}dt$ [57].

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

$$P_{\mathrm{D}} = \mathcal{Q}_{F'_{2KL,2K(L-1)}(\lambda)}\left(\eta_{\mathrm{NIC}}\right), \quad (30)$$

and

$$P_{\mathrm{Fa}} = \mathcal{Q}_{F_{2KL,2K(L-1)}}\left(\eta_{\mathrm{NIC}}\right), \quad (31)$$

receptively, where $Q_{F'_{2KL,2K(L-1)}(\lambda)}(x)$ is the right tail probability of noncentral F-distribution defined as $Q_{F'_{2KL,2K(L-1)}(\lambda)}(x) \triangleq \int_x^{\infty} f(x)dx$, and $f(x)$ is defined in (29).

Remark 5: It can be observed from (30) that the probability of detection is characterized by λ. On one hand, if (26) is satisfied, then λ will tend to ∞ as K increases, in which case P_{D} tends to one. On the other hand, λ may approach zero as K increases if (26) is not satisfied, in which case P_{D} tends to zero. It should be pointed out that the prabability of false alarm is not a function of unknown parameters. Therefore, if (26) is satisfied then the detector is a constant false alarm rate (CFAR) detector.

B. Numerical Versus Theoretical Probability of Detection

Numerical simulations were conducted in order to compare the derived probability of detection with simulations. To this end, 5G signals were simulated and the CPI length was varied from $K = 10$ to $K = 50$ for a set of Doppler estimation errors of $\Delta f_{\mathrm{e}} \in \left\{0, 1.6\times10^{-5}, 2\times10^{-5}, 2.4\times10^{-5}\mathrm{Hz}\right\}$. It should be pointed out that these values are close to the typical Doppler estimation error values which are observed in the experiments. The SNR was considered to be 20 dB. A total of 10^6 Monte Carlo noise $\mathbf{w}_{\mathrm{eq}}$ realizations were used to numerically calculate P_{D}. The results are shown in Fig. 3. It can be seen from the figure that as the Doppler estimation error increases, the probability of detection decreases. It can be also seen that if the condition in (26) is violated, the probability of detection decays with the CPI. This is a direct consequence of Remark 5 which shows that the obtained theoretical analysis is corroborated with the numerical simulations.

Remark 6: The detection performance curves in Fig. 3 demonstrate an *optimal regime of CPIs* for a given Doppler

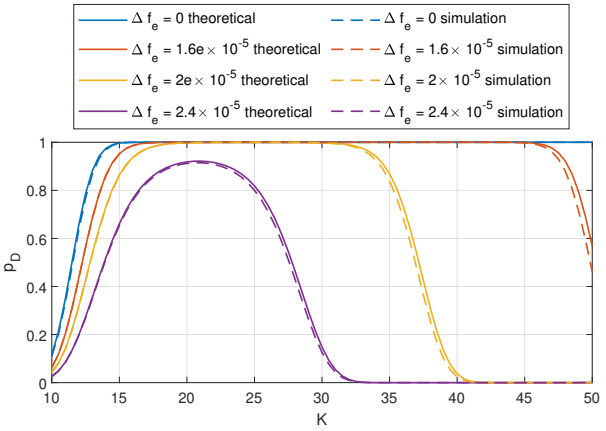

Fig. 3. Monte Carlo simulation results comparing theoretical (30) and simulated probability of detection. It can be seen that increasing the CPI improves the probability of detection if the Doppler estimation error satisfies (27).

estimation error. Assuming that the Doppler is estimated perfectly, increasing the CPI results in a higher probability of detection, which leads to a more reliable estimation of the beacon. Due to the Doppler estimation error in practice, an optimal regime of CPIs exists in which the probability of detection is maximized. If one thinks of the subspace spanned by the columns of $\mathbf{H}$ as the "signal subspace" and the orthogonal subspace as the "noise subspace," then the test statistic (17) is an estimated SNR for the proposed method. The ML estimation of the CPI can be obtained by maximizing (17) over different values of the CPI. It will be shown in Section VII that the ML estimation of the CPI can be obtained using the likelihood (17). It will be also shown that the estimated beacon using the ML estimate of the CPI is *cleaner* than the estimated beacon using an arbitrarily chosen CPI.

After obtaining coarse estimates of the Doppler frequencies and estimates of the beacons, the receiver refines and maintains these estimates. Specifically, conventional phase-locked loops (PLLs) are employed to track the carrier phases of the detected RSs and carrier-aided delay-locked loops (DLLs) are used to track the RSs' code phases [58].

VII. Experimental Results

This section presents experimental results demonstrating the proposed cognitive approach to detect unknown beacons of terrestrial SOPs with IC and NIC to enable cognitive opportunistic navigation of a UAV with real cdma2000 and 5G NR signals. In the detection algorithms, the thresholds are selected according to (31) for $P_{\mathrm{FA}} = .001$.

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

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

1) Experimental Setup: A UAV was equipped with an Ettus E312 universal software radio peripheral (USRP) to sample cdma2000 signals, a consumer-grade 800/1900 MHz

cellular antenna, and a small consumer-grade GPS antenna to discipline the on-board oscillator. The receiver was tuned to a 882.75 MHz carrier frequency, which is a cdma2000 channel allocated for the U.S. cellular provider Verizon Wireless. All the 3G base transceiver stations (BTSs) in this experiment transmit at 882.75 MHz. Samples of the received signals were stored for off-line post-processing. The ground-truth reference for the UAV trajectory was taken from its on-board navigation system, which uses a GNSS receiver, an inertial measurement unit (IMU), and other sensors. The UAV's total traversed trajectory was 1.72 km, which was completed in 3 minutes. Over the course of the experiment, the receiver on-board the UAV was listening to four BTSs, whose positions were mapped prior to the experiment. The experimental setup and environment is shown in Fig. 4.

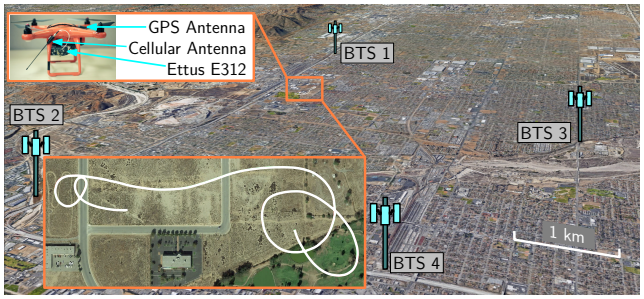

Fig. 4. Environment layout and UAV trajectory for the cdma2000 experiment.

2) Detection Results: The cdma2000 PN sequence was estimated from the forward link signal, using the LCBSD algorithm. Fig. 5 shows the likelihood function (5) in terms of Doppler frequency. As it can be seen, four BTSs are detected in this experiment. Fig. 6(a) shows a scatter plot of $\mathbf{z}$ in (6) which resembles the scatter plot of a rotated noisy 4PSK modulated signal. Fig. 6(b) shows the correlation function between the estimated and true cdma2000 forward channel PN sequence using the LCBSD algorithm, whose clean peak indicates that the estimated sequence can be reliably used to despread the cdma2000 signal. The value of β was found to be 0.486, which from Fig. 2, indicates that the receiver was operating in less than unity SNR regime.

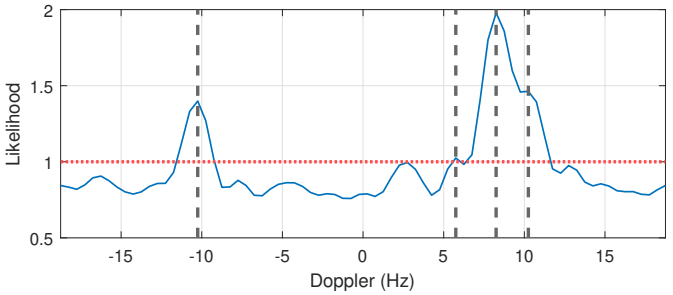

Fig. 5. The likelihood (5) in terms of Doppler frequency (solid blue) and the threshold (dotted red). Four BTSs are detected in this experiment.

3) Navigation Results: The detected PN sequence was used to acquire and track the received cdma2000 signals and produce TOA-like measurements using the receiver implementation discussed in [58]. It is worth noting that a carrier-aided delay-locked loop (DLL) was used to estimate the TOA, which

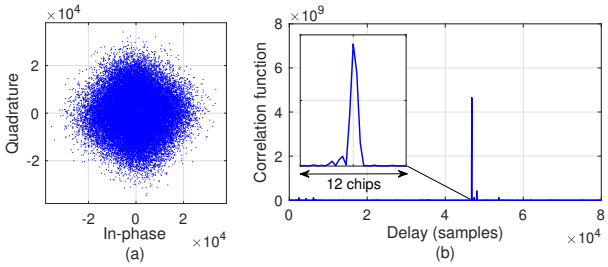

Fig. 6. (a) Scatter plot of $\mathbf{z}$ from real cdma2000 forward channel signals. (b) Correlation function between the detected and true cdma2000 PN sequence.

yields smoother and more precise estimates than a standalone DLL. Next, the estimation of the position of the UAV-mounted receiver, denoted $\boldsymbol{r}_r$, from TOA measurements from the four BTSs is discussed. The UAV's altitude was assume to be known, e.g., using an altimeter, and only its two-dimensional (2–D) position was estimated. The TOA, expressed in meters, from the n-th BTS, where $n \in \{1, 2, 3, 4\}$, can be modeled as

$$z_n(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_n}\| + c \cdot [\delta t_r(k) - \delta t_{s_n}(k)] + v_n(k), \quad (32)$$

where $\boldsymbol{r}_{s_n}$ is the 2–D position of the n-th BTS, c is the speed of light, δt_r and δt_{s_n} are the receiver and n-th BTS's clock biases, respectively, and v_n is the measurement noise, which is modeled as a zero-mean white Gaussian sequence with variance σ_n^2. The terms $c \cdot [\delta t_r(k) - \delta t_{s_n}(k)]$ are combined into one term as they do not need to be estimated separately, yielding $c\delta t_n(k) \triangleq c \cdot [\delta t_r(k) - \delta t_{s_n}(k)]$. The cellular BTSs possess tighter carrier frequency synchronization than time (code phase) synchronization (the code phase synchronization requirement as per the cellular protocol is reported to be within 10 μs in [59], and was experimentally observed to be within 3 μs in [60]). Therefore, the resulting clock biases in the TOA estimates will be very similar, up to an initial bias, as shown in Fig. 7. Consequently, one may leverage this relative frequency stability to eliminate parameters that need to be estimated.

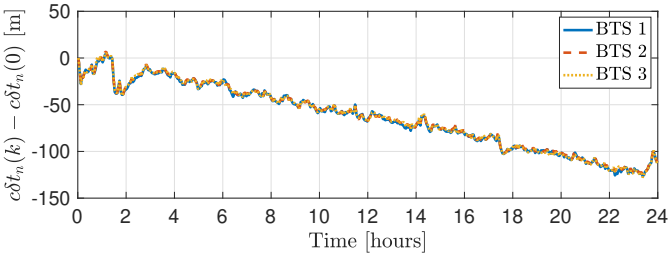

Fig. 7. Experimental data showing $c\delta t_n(k) - c\delta t_n(0)$ obtained from carrier phase measurements over 24 hours for three neighboring BTSs. It can be seen that the clock biases $c\delta t_n(k)$ in the carrier phase measurement are very similar, up to an initial bias $c\delta t_n(0)$ which has been removed.

Motivated by Fig. 7, the following re-parametrization is proposed

$$c\bar{\delta} t_n(k) \triangleq c\delta t_n(k) - c\delta t_n(0) \equiv c\delta t(k) + \epsilon_n(k), \quad \forall n \quad (33)$$

where $c\delta t$ is a time-varying common bias term independent of the nth BTS, and ϵ_n is the deviation of $c\bar{\delta} t_n$ from this common bias and is treated as measurement noise. Using

(33), the TOA measurement (32) can be re-parameterized as $z_n(k) = \|\boldsymbol{r}_r(k) - \boldsymbol{r}_{s_n}\| + c\delta t(k) + c\delta t_{0_n} + \eta_n(k)$, where $c\delta t_{0_n} \triangleq c\delta t_n(0)$ and $\eta_n(k) \triangleq \epsilon_n(k) + v_n(k)$ is the overall measurement noise. Note that $c\delta t_{0_n}$ can be obtained by knowing the initial receiver's position and from the initial measurement $z_n(0)$, according to $c\delta t_{0_n} \approx z_n(0) - \|\boldsymbol{r}_r(0) - \boldsymbol{r}_{s_n}\|$. This approximation ignores the contribution of the initial measurement noise.

The TOA measurements were fed to an extended Kalman filter (EKF) to estimate the state vector $\boldsymbol{x} \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, c\delta t, c\dot{\delta t}\right]^{\mathsf{T}}$, where $\dot{\boldsymbol{r}}_r$ is the UAV's 2–D velocity vector and $\dot{\delta t}$ is the clock drift. A white noise acceleration model was used for the UAV's dynamics, and a standard double integrator driven by process noise was used to model the clock bias and drift dynamics [13]. As such, the discrete-time dynamics model of $\boldsymbol{x}$ is given by

$$\boldsymbol{x}(k+1) = \mathbf{F}\boldsymbol{x}(k) + \boldsymbol{w}(k), \tag{34}$$

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

$$\mathbf{Q}_{\text{pv}} = \begin{bmatrix} \tilde{q}_x\frac{T^3}{3} & 0 & \tilde{q}_x\frac{T^2}{2} & 0 \\ 0 & \tilde{q}_y\frac{T^3}{3} & 0 & \tilde{q}_y\frac{T^2}{2} \\ \tilde{q}_x\frac{T^2}{2} & 0 & \tilde{q}_xT & 0 \\ 0 & \tilde{q}_y\frac{T^2}{2} & 0 & \tilde{q}_yT \end{bmatrix},$$
$$\mathbf{Q}_{\text{clk}} = c^2\begin{bmatrix} S_{\tilde{w}_{\delta t}}T + S_{\tilde{w}_{\dot{\delta} t}}\frac{T^3}{3} & S_{\tilde{w}_{\dot{\delta} t}}\frac{T^2}{2} \\ S_{\tilde{w}_{\dot{\delta} t}}\frac{T^2}{2} & S_{\tilde{w}_{\dot{\delta} t}}T \end{bmatrix}, \tag{35}$$

where the x, y acceleration process noise spectra of the white noise acceleration model were set to $\tilde{q}_x = \tilde{q}_y = 5$ m^2/s^3, the time interval between two measurements was $T = 0.0267$ s, and the receiver's clock process noise spectra were chosen to be $S_{\tilde{w}_{\delta t}} = 1.3 \times 10^{-22}$ and $S_{\tilde{w}_{\dot{\delta} t}} = 7.9 \times 10^{-25}$ which are that of a typical temperature-compensated crystal oscillator (TCXO) [13]. Note that $\boldsymbol{r}_r$ is expressed in an ENU frame centered at the UAV's true initial position. The EKF state estimate was initialized at $\hat{\boldsymbol{x}}(0) = \mathbf{0}_{6\times 1}$ with an initial covariance of $\mathbf{P}(0) = \text{diag}[3\cdot\mathbf{I}_{2\times 2}, \mathbf{I}_{2\times 2}, 10^{-2}, 10^{-4}]$. The measurement noise covariance was set to $\mathbf{R} = \mathbf{I}_{2\times 2}$.

The UAV's position was estimated using the aforementioned EKF and the total position RMSE was found to be 77.1 cm over the entire trajectory. The true and estimated trajectories are shown in Fig. 8.

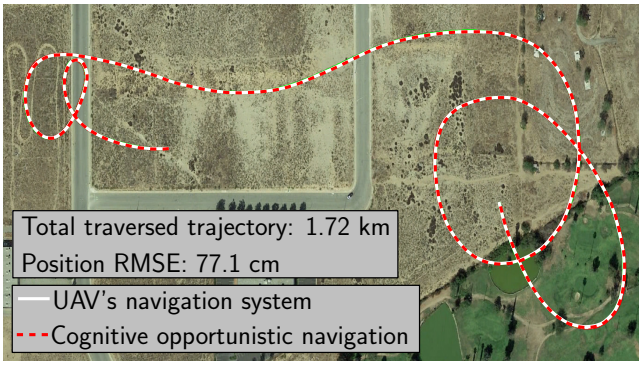

Fig. 8. True UAV trajectory and the estimated trajectory using the proposed cognitive opportunistic navigation framework.

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

In the second experiment, the GLR detector with no integer constraint (19) is used to detect 5G NR downlink signals. The location of the gNBs was mapped prior to the experiment.

1) Experimental Setup: In this experiment, the navigator was an Autel Robotics X-Star Premium UAV equipped with a single-channel Ettus 312 USRP connected to a consumer-grade 800/1900 MHz cellular antenna and a small consumer-grade GPS antenna to discipline the on-board oscillator. The cellular receivers were tuned to the cellular carrier frequency 632.55 MHz, which is a 5G NR frequency allocated to the U.S. cellular provider T-Mobile. All the 5G gNBs in this experiment use 632.55 MHz carrier frequency. Samples of the received signals were stored for off-line post-processing. The UAV traversed a trajectory of 416 m. Fig. 9 shows the environment layout and the vehicle trajectory. The acquisition results are presented next.

Fig. 9. Environment layout and UAV trajectory for the 5G NR UAV experiment.

2) Detection of 5G gNBs and the Corresponding RSs: Fig. 10 demonstrates the likelihood function (19) in terms of Doppler frequency. It can be seen that three different sources are detected at Doppler frequencies of 4 Hz, 12 Hz, and 15 Hz using the GLR test. In 5G NR, the always-on synchronization signal includes PSS and SSS, which provide symbol and frame timing, respectively. The PSS and SSS are transmitted along with the physical broadcast channel (PBCH) signal and its associated demodulation reference signal (DM-RS) on a block called SS/PBCH block. The SS/PBCH block consists of four consecutive OFDM symbols and 240 consecutive subcarriers [61]. Fig. 11, demonstrates the reconstructed OFDM frame of the estimated RS at 4 Hz. The always-on synchronization signals, i.e., SS/PBCH block, can be seen in the estimated OFDM frame (the block of symbols and subcarriers with the highest power in the red box). It can be seen that other than

the always-on beacons, on-demand beacons are also estimated which are spread periodically in different OFDM symbols and subcarries.

In 5G NR, the PSS is transmitted in one form of three possible sequences, each of which maps to an integer representing the sector ID of the gNB [61]. In order to assess the performance of the detector, the estimated RS of the source at 4 Hz is correlated with the three possible 5G NR PSSs, as shown in Fig. 12. A strong correlation between the estimated RS and the third PSS is observed, while the correlations with the first two are negligible. This implies that the gNB at 4 Hz was actually transmitting the third PSS in the sector within which the UAV was flying.

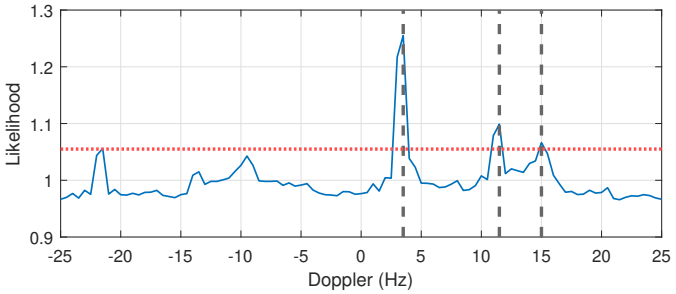

Fig. 10. The likelihood (19) in terms of Doppler frequency (solid blue) and the threshold (dotted red). Three gNBs are detected in this experiment.

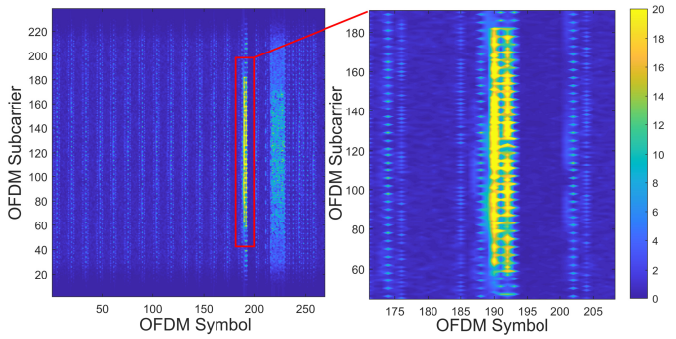

Fig. 11. The OFDM frame structure of the estimated RS. The always-on synchronization signals, i.e., SS/PBCH block, can be seen in the estimated OFDM frame (the block of symbols and subcarriers with the highest power located in the red box).

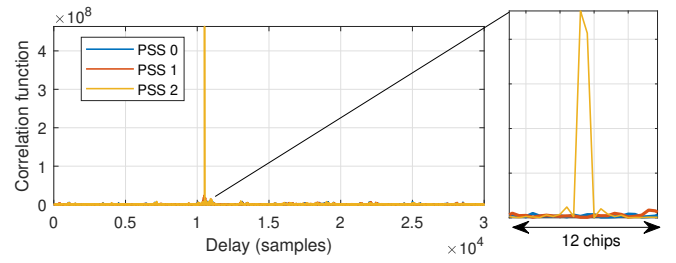

Fig. 12. Correlation of the detected RS with three different PSSs of 5G NR.

False alarm: A detected source can be either a valid transmitter or a *false alarm*. A false alarm may occur due to multipath or an unwanted interfering source. The estimated RSs are fed to tracking loops to get carrier phase and code phase observables. If a source is mistakenly detected, the tracking loops will fail to track the signal. Fig. 13 demonstrates the carrier phase error for the three detected sources at 4 Hz, 12 Hz, and 15 Hz. It can be seen that the carrier phase error of the two sources at 4 Hz and 12 Hz are converging, while the carrier phase error of the source at 15 Hz is not converging. Hence, the method identifies this source as a false alarm.

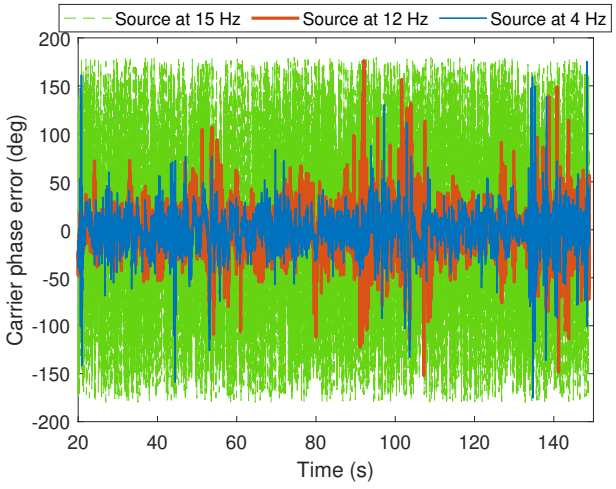

Fig. 13. Carrier phase error for the three detected RS at 4 Hz, 12 Hz, and 15 Hz. The carrier phase error of the detected source at 15 Hz is not converging.

ML estimation of the CPI: Fig. 14 demonstrates the likelihood function for different values of CPI. As discussed in Remark 6, the ML estimation of the CPI can be obtained by maximizing the likelihood function (17). A CPI of $K = 60$ maximizes the likelihood for the first gNB and a CPI of $K = 36$ maximizes the likelihood corresponding to the second gNB. It should be pointed out that the optimal choice of the CPI depends on the channel statistics and the dynamics of the UAV. In a scenario where the Doppler is changing rapidly, the ML estimate of the CPI becomes smaller. On the other hand, in a static scenario, the receiver will have more time to coherently accumulate the received samples and obtain a better estimate of the RS. Fig. 15 demonstrates the estimated PRNs for the first gNB for two different values of CPI: (i) an arbitrary CPI of $K = 20$, and (ii) the ML estimate of a CPI of $K = 60$. It can be seen that the estimated RS for $K = 60$ is cleaner than that of the arbitrarily chosen CPI.

3) Navigation Results: The estimated beacon is used to produce TOA measurements using the receiver implementation discussed in [6]. Note that since the UAV's altitude is known using an altimeter, only its two-dimensional position is estimated. Similar measurement models as in Section VII-A3 are considered. The TOA measurements were fed to an extended Kalman filter (EKF) to estimate the state vector $\boldsymbol{x} \triangleq \left[\boldsymbol{r}_r^{\mathsf{T}}, \dot{\boldsymbol{r}}_r^{\mathsf{T}}, c\delta t, c\dot{\delta t}\right]^{\mathsf{T}}$, where $\dot{\boldsymbol{r}}_r$ is the UAV's 2–D velocity vector and $\dot{\delta t}$ is the clock drift as discussed in Section VII-A3. The x, y acceleration process noise spectra in the nearly constant velocity model were set to $\tilde{q}_x = \tilde{q}_y = 5$ m^2/s^3, the time interval between two measurements was $T = 1$ s, and the receiver's clock process noise spectra were chosen to be $S_{\tilde{w}_{\delta t}} = 1.3 \times 10^{-22}$ and $S_{\tilde{w}_{\dot{\delta t}}} = 7.9 \times 10^{-25}$. The

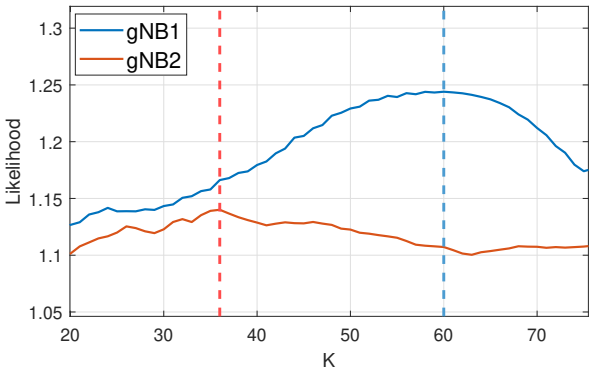

Fig. 14. The likelihood (19) in terms of different values of CPI.

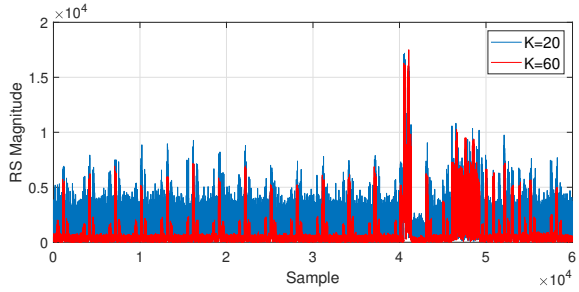

Fig. 15. The estimated RS at 4Hz for $K = 20$ and $K = 60$. The estimated RS for the optimal CPI ($K = 60$) is less noisy than the estimated RS for the arbitrarily chosen CPI ($K = 20$).

EKF state estimate was initialized at $\hat{\boldsymbol{x}}(0) = \mathbf{0}_{6\times1}$ with an initial covariance of $\mathbf{P}(0) = \text{diag}[3\cdot\mathbf{I}_{2\times2}, \mathbf{I}_{2\times2}, 10^{-2}, 10^{-4}]$. The measurement noise covariance was set to $\mathbf{R} = \mathbf{I}_{2\times2}$. The position RMSE of the UAV was calculated to be 4.63 m with the aforementioned parameters. The true and estimated UAV trajectories with the proposed method versus the receiver in [51] which uses the *known* beacon are shown in Fig. 16. It can be seen that the proposed cognitive opportunistic framework achieves lower position RMSE compared to the method presented in [51]. This is due to the fact that the method in [51] only relies on always-on signals, whereas the cognitive opportunistic navigation framework exploits all the available bandwidth of the received signal, which in turn results in a more accurate TOA estimation and, consequently, less positioning RMSE [6].

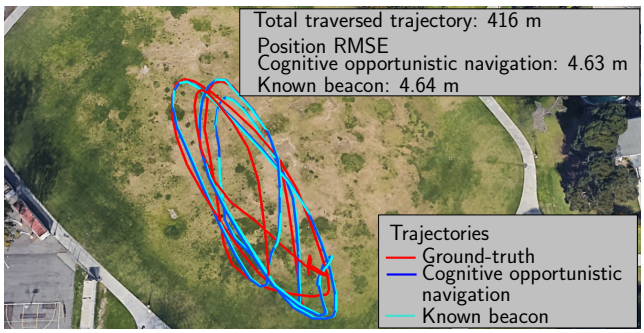

Fig. 16. UAV's ground-truth and estimated trajectories using the proposed cognitive opportunistic navigation framework versus the method in [51], which uses the known always-on beacons for 5G NR signals. Map data: Google Earth.

C. Signal Model Validation

In the signal model (1), a single tap channel which corresponds to the LOS path with arbitrary channel gain α is considered. More precisely, the channel impulse response is modeled as $h[n] = \alpha\delta[n - n_d]$, where α is the complex channel gain between the transmitter and the receiver, and n_d is the code-delay corresponding to the transmitter and the receiver. This channel model considers a *flat fading* scenario, where the effect of multiple "close" paths is considered in a single path gain α. Based on the underlying distribution of α, the considered $h[n]$ can model a *Rayleigh* or *Rician* flat fading channel [54]. To justify the single tap flat fading channel model for the UAV scenario, the channel impulse response between the UAV and one of the gNBs is assessed. The physical environment between the gNB and the UAV is demonstrated in Fig. 17. In this figure, the term clear LOS refers to a scenario where the signal is not blocked by an obstacle, e.g., a building. It can be seen that there is a clear LOS between the gNB and the UAV. The magnitude of the channel impulse response is plotted in Fig. 18(a). The magnitudes of the channel impulse responses are estimated by reconstructing the frame as described in [62]. Fig. 18(b) demonstrates the true and estimated code delay between the gNB and the UAV. It can be observed from Fig. 18 that the channel impulse response $|h(\tau)|$ does not exhibit multiple taps (i.e., $h[n] = \sum_{i=1}^{M}\alpha_i\delta[n - n_{d_i}]$, where M is the number of paths). Hence, considering a single tap flat fading model is valid for the conducted experiments. Frequency selective channels can be considered in future work.

VIII. Conclusion

This paper proposed the idea of cognitive opportunistic navigation as a solution for exploiting SOPs with partially known signal specifications. Two main challenges of a cognitive opportunistic framework were addressed. Two scenarios were considered in the paper: (i) detection of unknown beacons with IC and (ii) detection of unknown beacons with NIC. Matched subspace detectors were proposed for both scenarios and it is shown experimentally that the matched subspace detector with integer constraint on the beacon symbols was capable of detecting cdma200 signals. A low complexity method was derived to simplify the matched subspace detector with integer constraint. The effect of symbol errors in the estimated beacon signal on the CNR was characterized analytically. Moreover, the matched subspace detector with no integer constraint was used to detect real 5G NR signals. Experimental results were presented showing a UAV navigating with the proposed framework with real cdma2000 signals, achieving submeter-level accuracy over a trajectory of 1.72 km. Another experiment with beacons with NIC also shows navigation results with real 5G signals on a UAV navigating using the proposed framework over a 416 m trajectory with a position RMSE of 4.63 m.

Appendix A
GLR Detector for (4)

It should be pointed out that the derivation of the GLR detector for (4) is similar to that of the matched subspace

Fig. 17. The environment layout and the physical channel between the gNB and the UAV.

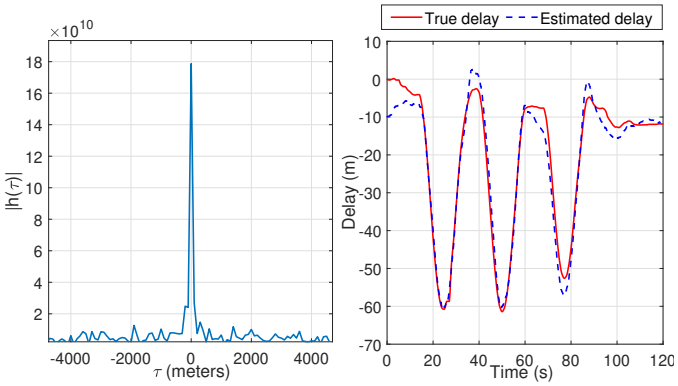

Fig. 18. (a) The channel impulse response magnitude between the gNB and the UAV at $t = 0$. (b) The code-delay corresponding to the corresponding between the gNB and the UAV during the course of the experiment.

detector in [18] and the general linear model in [57]. The main difference here is the structure of the subspace matrix $\mathbf{H}$ which simplifies the detector. The integer constraint should also be considered for the derivation of the detector. For the completeness of the paper, this appendix presents the derivation of the GLR detector for (4). To this end, the ML estimates of the unknown parameters, i.e., α, σ^2, Δf, and $\mathbf{s}$, are substituted in the pdfs of the observation vector $\mathbf{z}$ under each hypothesis. Under $\mathcal{H}_1$, the pdf of the observation vector $\mathbf{z}$ is $f(\mathbf{y}|\mathcal{H}_1) = \frac{1}{(\pi\sigma^2)^{KL}} \exp\left(-\frac{1}{\sigma^2}\|\mathbf{y} - \alpha\mathbf{H}\mathbf{s}\|^2\right)$. Under $\mathcal{H}_0$, the pdf of the observation vector $\mathbf{z}$ is $f(\mathbf{z}|\mathcal{H}_0) = \frac{1}{(\pi\sigma^2)^{KL}} \exp\left(-\frac{1}{\sigma^2}\|\mathbf{y}\|^2\right)$. By maximizing the above pdfs over α and σ^2, the ML estimates of these variable are obtained as $\hat{\alpha} = \frac{1}{KL}\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}$, $\widehat{\sigma}^2_{\mathcal{H}_1} = \frac{1}{KL}\|\mathbf{y} - \hat{\alpha}\mathbf{H}\mathbf{s}\|^2$, and $\widehat{\sigma}^2_{\mathcal{H}_0} = \frac{1}{KL}\|\mathbf{y}\|^2$. The estimation of the noise variance under $\mathcal{H}_1$ can be expanded as

$$\widehat{\sigma}^2_{\mathcal{H}_1} = \frac{1}{KL}\|\mathbf{y}\|^2 - \frac{2}{(KL)^2}|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2 + \frac{1}{(KL)^3}|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{H}\mathbf{s}. \quad (36)$$

The elements of the vector $\mathbf{s}$ are drawn from MPSK modulation. Therefore, $\mathbf{s}^{\mathsf{H}}\mathbf{s} = L$ and since $\mathbf{H}^{\mathsf{H}}\mathbf{H} = K$, one can obtain $\widehat{\sigma}^2_{\mathcal{H}_1} = \frac{1}{KL}\|\mathbf{y}\|^2 - \frac{1}{(KL)^2}|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2$. Consequently, the likelihood ratio is

$$\frac{f(\mathbf{y}|\mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} = \frac{\frac{1}{KL}\|\mathbf{y}\|^2}{\frac{1}{KL}\|\mathbf{y}\|^2 - \frac{1}{(KL)^2}|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2}.$$

It can be seen that the likelihood ratio is a monotonically increasing function of $\frac{|\mathbf{s}^{\mathsf{H}}\mathbf{H}^{\mathsf{H}}\mathbf{y}|^2}{K^2\|\mathbf{y}\|^2}$. Therefore, by maximizing the likelihood over the integer vector $\mathbf{q}$ and the unknown Doppler Δf,the GLR test for the constrained problem (4) is obtained by (5).

Appendix B
Proof of Lemma 1

In order to calculate the number of search candidates, first the coherent detector of $\mathbf{q}$ for a given phase complex amplitude α is considered. Note that the coherent detector does not depend on the magnitude of α, but only depends on its phase ϕ. More precisely, for a given value of ϕ, one has $\left\{\hat{\mathbf{q}}_\phi, \hat{\Delta f}\right\} = \underset{\mathbf{q},\Delta f}{\operatorname{argmax}} \Re\left\{\exp(-j\phi)\mathbf{z}^{\mathsf{H}}\exp\left(\frac{j2\pi}{M}\mathbf{q}\right)\right\}$ [63]. Due to the nature of i.i.d noise and the independence of the elements of $\mathbf{q}$, the coherent detector simplifies to a SBS MPSK detector for a given Δf and ϕ. Hence, the lth element of $\hat{\mathbf{q}}_\phi$, denoted by $\hat{q}_{\phi_l}$, is obtained by mapping the phase of $\exp(j\phi)z_l$, where z_l is the lth element of $\mathbf{z}$, to the closest multiple of $\frac{2\pi}{M}$, i.e.

$$\hat{q}_{\phi_l} = \text{round}\left[(\phi_l + \phi)\frac{M}{2\pi}\right] \mod M, \quad (37)$$

where mod is the modulus operator and $\phi_l \triangleq \angle z_l$. Thus, for a given Δf, one can find the optimal $\mathbf{q}$ by searching over all possible values for ϕ. However, it can be readily shown from (37), that $\hat{\mathbf{q}}_\phi$ and $\hat{\mathbf{q}}_{\phi+\frac{2\pi}{M}}$ result in the same likelihood function in (6). Consequently, the search space for ϕ is limited to the interval $[0, \frac{2\pi}{M})$.

Since ϕ is limited to the interval $[0, \frac{2\pi}{M})$, the lth detected MPSK symbol $\hat{q}_{\phi_l}$ can take on two values, based on which symbol in the MPSK constellation is closest to it. Define $\mathbf{c}_1 \triangleq \hat{\mathbf{q}}_{\phi=0}$ and $\mathbf{c}_2 \triangleq \hat{\mathbf{q}}_{\phi=\frac{2\pi}{M}}$, where it can be shown through (37) that $c_{2_l} = (c_{1_l} + 1) \bmod M$, where c_{1_l} and c_{2_l} are the lth elements of $\mathbf{c}_1$ and $\mathbf{c}_2$, respectively. It can also be shown using (37) that the boundary angle between two symbols in

the MPSK constellation is given by $\gamma_l \triangleq \frac{2\pi}{M} c_{1_l} + \frac{\pi}{M} - \phi_l$ [64]. Subsequently, each candidate MPSK symbol will be given by

$$\hat{q}_{\phi_l} = \begin{cases} c_{1_l} & \phi \leq \gamma_l, \\ c_{2_l} & \phi > \gamma_l. \end{cases} \tag{38}$$

For convenience of notation, define $\left\{\left(c'_{1_l}, \gamma'_l\right)\right\}_{l=0}^{L-1}$ as the set of the sorted values of (c_{1_l}, γ_l) in an ascending order of γ_l such that $\gamma'_{l+1} \geq \gamma'_l$. Consequently, each candidate $\hat{\mathbf{q}}_\phi$ is of the form

$$\left[c'_{1_1} + 1 - u(\gamma'_1 - \phi), \ldots, c'_{1_L} + 1 - u(\gamma'_L - \phi)\right]^{\mathsf{T}}, \tag{39}$$

where $u(\cdot)$ is the unit step function. Equation (39) implies that for different values of ϕ, L different candidates $\mathcal{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_L\}$ are available. Each candidate should be plugged in (6) to get the optimal $\hat{\mathbf{q}}$. Finally, by searching over Doppler, one can get the total number of DL search candidates. ■

REFERENCES

[1] Z. Kassas, J. Khalife, A. Abdallah, and C. Lee, "I am not afraid of the GPS jammer: resilient navigation via signals of opportunity in GPS-denied environments," *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, no. 7, pp. 4–19, July 2022.

[2] P. Gadka, J. Sadowski, and J. Stefanski, "Detection of the first component of the received LTE signal in the OTDoA method," *Wireless Communications and Mobile Computing*, pp. 1–12, April 2019.

[3] K. Shamaei and Z. Kassas, "A joint TOA and DOA acquisition and tracking approach for positioning with LTE signals," *IEEE Transactions on Signal Processing*, pp. 2689–2705, 2021.

[4] M. Pan, P. Liu, S. Liu, W. Qi, Y. Huang, X. You, X. Jia, and X. Li, "Efficient joint DOA and TOA estimation for indoor positioning with 5G picocell base stations," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–19, 2022.

[5] A. Xhafa, J. del Peral-Rosado, J. López-Salcedo, and G. Seco-Granados, "Evaluation of 5G positioning performance based on UTDoA, AoA and base-station selective exclusion," *Sensors*, vol. 22, no. 1, pp. 101–118, 2021.

[6] M. Neinavaie, J. Khalife, and Z. Kassas, "Cognitive opportunistic navigation in private networks with 5G signals and beyond," *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no. 1, pp. 129–143, 2022.

[7] S. Parkvall, Y. Blankenship, R. Blasco, E. Dahlman, G. Fodor, S. Grant, E. Stare, and M. Stattin, "5G NR release 16: Start of the 5G evolution," *IEEE Communications Standards Magazine*, vol. 4, no. 4, pp. 56–63, 2020.

[8] M. Neinavaie, J. Khalife, and Z. Kassas, "Blind opportunistic navigation: Cognitive deciphering of partially known signals of opportunity," in *Proceedings of ION GNSS Conference*, September 2020, pp. 2748–2757.

[9] J. Khalife, M. Neinavaie, and Z. Kassas, "Blind Doppler tracking from OFDM signals transmitted by broadband LEO satellites," in *Proceedings of IEEE Vehicular Technology Conference*, April 2021, pp. 1–6.

[10] M. Neinavaie, J. Khalife, and Z. Kassas, "Blind Doppler tracking and beacon detection for opportunistic navigation with LEO satellite signals," in *Proceedings of IEEE Aerospace Conference*, March 2021, pp. 1–8.

[11] E. Conte, A. Filippi, and S. Tomasin, "ML period estimation with application to vital sign monitoring," *IEEE Signal Processing Letters*, vol. 17, no. 11, pp. 905–908, 2010.

[12] J. Raquet *et al.*, "Position, navigation, and timing technologies in the 21st century," J. Morton, F. van Diggelen, J. Spilker, Jr., and B. Parkinson, Eds. Wiley-IEEE, 2021, vol. 2, Part D: Position, Navigation, and Timing Using Radio Signals-of-Opportunity, ch. 35–43, pp. 1115–1412.

[13] Z. Kassas, "Position, navigation, and timing technologies in the 21st century," J. Morton, F. van Diggelen, J. Spilker, Jr., and B. Parkinson, Eds. Wiley-IEEE, 2021, vol. 2, ch. 38: Navigation with Cellular Signals of Opportunity, pp. 1171–1223.

[14] C. Yang and A. Soloviev, "Mobile positioning with signals of opportunity in urban and urban canyon environments," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2020, pp. 1043–1059.

[15] X. Chen, Q. Wei, F. Wang, Z. Jun, S. Wu, and A. Men, "Super-resolution time of arrival estimation for a symbiotic FM radio data system," *IEEE Transactions on Broadcasting*, vol. 66, no. 4, pp. 847–856, December 2020.

[16] H. Zou, M. Jin, H. Jiang, L. Xie, and C. Spanos, "WinIPS: WiFi-based non-intrusive indoor positioning system with online radio map construction and adaptation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 8118–8130, 2017.

[17] J. Khalife, M. Neinavaie, and Z. Kassas, "The first carrier phase tracking and positioning results with Starlink LEO satellite signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 2, pp. 1487–1491, April 2022.

[18] L. Scharf and B. Friedlander, "Matched subspace detectors," *IEEE Transactions on signal processing*, vol. 42, no. 8, pp. 2146–2157, 1994.

[19] S. Kraut, L. Scharf, and L. McWhorter, "Adaptive subspace detectors," *IEEE Transactions on Signal Processing*, vol. 49, no. 1, pp. 1–16, 2001.

[20] F. Gini and A. Farina, "Vector subspace detection in compound-Gaussian clutter. part I: survey and new results," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 38, no. 4, pp. 1295–1311, 2002.

[21] F. Izedi, M. Karimi, and M. Derakhtian, "Joint DOA estimation and source number detection for arrays with arbitrary geometry," *Signal Processing*, vol. 140, pp. 149–160, 2017.

[22] A. Tadaion, M. Derakhtian, S. Gazor, M. Nayebi, and M. Aref, "Signal activity detection of phase-shift keying signals," *IEEE Transactions on Communications*, vol. 54, no. 8, pp. 1439–1445, August 2006.

[23] G. Karystinos and D. Pados, "Rank-2-optimal adaptive design of binary spreading codes," *IEEE Transactions on Information Theory*, vol. 53, no. 9, pp. 3075–3080, 2007.

[24] P. Markopoulos and G. Karystinos, "Noncoherent Alamouti phase-shift keying with full-rate encoding and polynomial-complexity maximum-likelihood decoding," *IEEE Transactions on Wireless Communications*, vol. 16, no. 10, pp. 6688–6697, 2017.

[25] G. Gao, "Towards navigation based on 120 satellites: Analyzing the new signals," Ph.D. dissertation, Stanford University, 2008.

[26] S. Han, T. Kang, and J. Seo, "Smartphone application to estimate distances from LTE base stations based on received signal strength measurements," in *International Technical Conference on Circuits/Systems, Computers and Communications*, June 2019, pp. 1–3.

[27] A. Soderini, P. Thevenon, C. Macabiau, L. Borgagni, and J. Fischer, "Pseudorange measurements with LTE physical channels," in *Proceedings of ION International Technical Meeting*, January 2020, pp. 817–829.

[28] P. Wang and Y. Morton, "Multipath estimating delay lock loop for LTE signal TOA estimation in indoor and urban environments," *IEEE Transactions on Wireless Communications*, vol. 19, no. 8, pp. 5518–5530, 2020.

[29] R. Whiton, J. Chen, T. Johansson, and F. Tufvesson, "Urban navigation with LTE using a large antenna array and machine learning," in *Proceedings of IEEE Vehicular Technology Conference*, 2022, pp. 1–5.

[30] K. Shamaei and Z. Kassas, "LTE receiver design and multipath analysis for navigation in urban environments," *NAVIGATION, Journal of the Institute of Navigation*, vol. 65, no. 4, pp. 655–675, December 2018.

[31] N. Ikhtiari, "Navigation in GNSS denied environments using software defined radios and LTE signals of opportunities," Master's thesis, University of Canterbury, Christchurch, New Zealand, 2019.

[32] A. Abdallah and Z. Kassas, "Deep learning-aided spatial discrimination for multipath mitigation," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2020, pp. 1324–1335.

[33] I. Lapin, G. Granados, J. Samson, O. Renaudin, F. Zanier, and L. Ries, "STARE: Real-time software receiver for LTE and 5G NR positioning and signal monitoring," in *Proceedings of Workshop on Satellite Navigation Technology*, April 2022, pp. 1–11.

[34] F. Pittino, M. Driusso, A. Torre, and C. Marshall, "Outdoor and indoor experiments with localization using LTE signals," in *Proceedings of European Navigation Conference*, May 2017, pp. 311–321.

[35] P. Wang, Y. Wang, and J. Morton, "Signal tracking algorithm with adaptive multipath mitigation and experimental results for LTE positioning receivers in urban environments," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 4, pp. 2779–2795, August 2022.

[36] J. Khalife and Z. Kassas, "On the achievability of submeter-accurate UAV navigation with cellular signals exploiting loose network synchronization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 5, pp. 4261–4278, October 2022.

[37] C. Olone, H. Dhillon, and R. Buehrer, "Single-anchor localizability in 5G millimeter wave networks," *IEEE Wireless Communications Letters*, vol. 9, no. 1, pp. 65–69, 2020.

[38] M. Koivisto, J. Talvitie, E. Rastorgueva-Foi, Y. Lu, and M. Valkama, "Channel parameter estimation and TX positioning with multi-beam fusion in 5G mmWave networks," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2021.

[39] F. Wen, J. Kulmer, K. Witrisal, and H. Wymeersch, "5G positioning and mapping with diffuse multipath," *IEEE Transactions on Wireless Communications*, vol. 20, no. 2, pp. 1164–1174, 2021.

[40] J. Baenke, K. Chaudhuri, A. Deshpande, A. Halder, M. Irizarry, N. Saxena, S. Sharma, and R. Yang, "Millimeter-Wave downlink coverage extension strategies," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 74–78, 2020.

[41] M. Giordani, M. Polese, A. Roy, D. Castor, and M. Zorzi, "A tutorial on beam management for 3GPP NR at mmWave frequencies," *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 173–196, 2019.

[42] A. Fascista, A. Coluccia, H. Wymeersch, and G. Seco-Granados, "Millimeter-wave downlink positioning with a single-antenna receiver," *IEEE Transactions on Wireless Communications*, vol. 18, no. 9, pp. 4479–4490, 2019.

[43] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, "5G mmWave positioning for vehicular networks," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 80–86, December 2017.

[44] Z. Abu-Shaban, X. Zhou, T. Abhayapala, G. Seco-Granados, and H. Wymeersch, "Error bounds for uplink and downlink 3D localization in 5G millimeter wave systems," *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 4939–4954, August 2018.

[45] Z. Abu-Shaban, X. Zhou, T. Abhayapala, G. Seco-Granados, and H. Wymeersch, "Performance of location and orientation estimation in 5G mmwave systems: Uplink vs downlink," in *Proceedings of IEEE Wireless Communications and Networking Conference*, April 2018, pp. 1–6.

[46] E. Rastorgueva-Foi, M. Costa, M. Koivisto, K. Leppanen, and M. Valkama, "User positioning in mmw 5G networks using beam-RSRP measurements and Kalman filtering," in *Proceedings of International Conference on Information Fusion*, July 2018, pp. 1–7.

[47] Z. Abu-Shaban, H. Wymeersch, T. Abhayapala, and G. Seco-Granados, "Distributed two-way localization bounds for 5G mmwave systems," in *Proceedings of IEEE Globecom Workshops*, December 2018, pp. 1–6.

[48] R. Mendrzik, H. Wymeersch, and G. Bauch, "Joint localization and mapping through millimeter wave MIMO in 5G systems," in *Proceedings of IEEE Global Communications Conference*, December 2018, pp. 1–6.

[49] W. Ma, C. Qi, and G. Li, "High-resolution channel estimation for frequency-selective mmwave massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3517–3529, 2020.

[50] L. Yin, Q. Ni, and Z. Deng, "A GNSS/5G integrated positioning methodology in D2D communication networks," *IEEE Transactions on Signal Processing*, vol. 36, no. 2, pp. 351–362, February 2018.

[51] A. Abdallah and Z. Kassas, "UAV navigation with 5G carrier phase measurements," in *Proceedings of ION GNSS Conference*, September 2021, pp. 3294–3306.

[52] J. Merwe, S. Bartl, C. O'Driscoll, A. Rügamer, F. Förster, P. Berglez, A. Popugaev, and W. Felber, "GNSS sequence extraction and reuse for navigation," in *Proceedings of ION GNSS+ Conference*, 2020, pp. 2731–2747.

[53] M. Neinavaie, J. Khalife, and Z. Kassas, "Acquisition, Doppler tracking, and positioning with Starlink LEO satellites: First results," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 3, pp. 2606–2610, June 2022.

[54] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[55] K. Takeda, H. Xu, T. Kim, K. Schober, and X. Lin, "Understanding the heart of the 5G air interface: An overview of physical downlink control channel for 5G new radio," *IEEE Communications Standards Magazine*, vol. 4, no. 3, pp. 22–29, 2020.

[56] H. Ochiai and H. Imai, "On the distribution of the peak-to-average power ratio in OFDM signals," *IEEE Transactions on Communications*, vol. 49, no. 2, pp. 282–289, 2001.

[57] S. Kay, *Fundamentals of statistical signal processing: Detection Theory*. Prentice-Hall, Upper Saddle River, NJ, 1993, vol. II.

[58] J. Khalife, K. Shamaei, and Z. Kassas, "Navigation with cellular CDMA signals – part I: Signal modeling and software-defined receiver design," *IEEE Transactions on Signal Processing*, vol. 66, no. 8, pp. 2191–2203, April 2018.

[59] 3GPP2, "Recommended minimum performance standards for cdma2000 spread spectrum base stations," December 1999.

[60] J. Khalife and Z. Kassas, "Precise UAV navigation with cellular carrier phase measurements," in *Proceedings of IEEE/ION Position, Location, and Navigation Symposium*, April 2018, pp. 978–989.

[61] K. Shamaei and Z. Kassas, "Receiver design and time of arrival estimation for opportunistic localization with 5G signals," *IEEE Transactions on Wireless Communications*, vol. 20, no. 7, pp. 4716–4731, 2021.

[62] A. Abdallah, K. Shamaei, and Z. Kassas, "Assessing real 5G signals for opportunistic navigation," in *Proceedings of ION GNSS Conference*, 2020, pp. 2548–2559.

[63] K. Mackenthun, "A fast algorithm for multiple-symbol differential detection of MPSK," *IEEE Transactions on Communications*, vol. 42, no. 234, pp. 1471–1474, February 1994.

[64] W. Sweldens, "Fast block noncoherent decoding," *IEEE Communications Letters*, vol. 5, no. 4, pp. 132–134, April 2001.

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 an M.S. in digital communication systems from Shiraz University. His research interests include opportunistic navigation, cognitive radio, wireless communication systems, and software-defined radio.

Joe Khalife (S'15-M'20) was a postdoctoral fellow at the University of California, Irvine and member of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He received a B.E. in Electrical Engineering, an M.S. in Computer Engineering from the Lebanese American University (LAU) and a Ph.D. in Electrical Engineering and Computer Science from the University of California, Irvine. He is a recipient of the 2016 IEEE/ION Position, Location, and Navigation Symposium (PLANS) Best Student Paper Award, 2018 IEEE Walter Fried Award, and 2021 IEEE AESS Robert T. Hill Best Dissertation Award. His research interests include opportunistic navigation, autonomous vehicles, and software-defined radio.

Zaher (Zak) M. Kassas (S'98-M'08-SM'11) is a professor at The Ohio State University and director of the Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory. He is also director of the U.S. Department of Transportation Center: CARMEN (Center for Automated Vehicle Research with Multimodal AssurEd Navigation), focusing on navigation resiliency and security of highly automated transportation systems. 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 2018 National Science Foundation (NSF) Faculty Early Career Development Program (CAREER) award, 2019 Office of Naval Research (ONR) Young Investigator Program (YIP) award, 2022 Air Force Office of Scientific Research (AFOSR) YIP award, 2018 IEEE Walter Fried Award, 2018 Institute of Navigation (ION) Samuel Burka Award, and 2019 ION Col. Thomas Thurlow Award. He is a Senior Editor of the IEEE Transactions on Intelligent Vehicles and an Associate Editor of 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.