Zaher (Zak) M. Kassas, Mohammad Neinavaie, Joe Khalife, Shaghayegh Shahcheraghi, and Joe Saroufim

The Truth Is Out There

Cognitive sensing and opportunistic navigation with unknown terrestrial and nonterrestrial signals

©SHUTTERSTOCK.COM/CINEMANIKOR

Future technologies, from the massive Internet of Things to highly automated transportation systems, will require a fundamental shift in the design of future communication networks, toward integrating sensing, communication, and security [1]. A desired attribute in these networks, whether terrestrial or nonterrestrial, is the ability to localize the user equipment (UE) to a high degree of accuracy in an uninterruptible fashion [2]. Estimation of the time of arrival (TOA), direction of arrival (DOA), and/or frequency of arrival (FOA) of multiple UEs/targets are core enablers for joint sensing and communication in beyond 5G technologies [3].

Radio-frequency (RF) positioning, navigation, and timing (PNT) receivers typically rely on known reference signals (RSs) transmitted by the source to draw TOA, DOA, and FOA measurements. RSs are periodic signals transmitted for synchronization purposes. RSs are designed based on their distinctive bandwidth and correlation properties and the physical channel [4].

RF PNT techniques in the literature can be classified into *network-based* (active) and *UE-based* (passive) approaches. Network-based approaches require the UE to transmit on the uplink channel. As such, they suffer from a number of drawbacks: 1) the UE's privacy is compromised since the UE's location is revealed to the network, 2) localization services are limited only to paying subscribers and from a particular provider, and 3) additional bandwidth is required to accommodate uplink transmission. In contrast, UE-based approaches exploit passively broadcast downlink signals without the need to be a subscriber of the network. A well-known example of UE-based approaches is a global navigation satellite system (GNSS) (e.g., GPS), which is, essentially, a dedicated system for PNT purposes.

Aside from dedicated systems, research over the past decade has shown that one can exploit so-called signals of opportunity (e.g., cellular, digital television, satellite communication, etc.), which are signals not transmitted for PNT purposes [5]. Whether dedicated or opportunistic, UE-based approaches are more attractive than network-based

Digital Object Identifier 10.1109/MSP.2024.3472496
Date of current version: 21 November 2024

approaches, with opportunistic approaches being particularly attractive since they 1) do not require additional overhead or bandwidth allocation, 2) preserve the UE's privacy, 3) do not require paying a subscription to the network, and 4) enable the UE to exploit signals from multiple providers simultaneously, which improves the positioning accuracy. This article focuses on UE-based opportunistic approaches with terrestrial and nonterrestrial signals (see "A Generic Signal Model").

RSs are designed based on their distinctive bandwidth and correlation properties and the physical channel.

Communication systems employ a synchronization *beacon* for receiver timing and/or carrier recovery. The beacon signals for *public* (e.g., cellular 3G, 4G, and 5G) and *private* [e.g., broadband low-Earth orbit (LEO) satellites] networks can be categorized into two classes (Figure 1):

- *Beacons with integer constraint (IC)*: The samples of the beacon with IC are drawn from a finite alphabet set, e.g., M-phase-shift keying modulation. An example of a beacon with IC is the pseudorandom noise (PRN) sequence in GPS [6]. This type of beacon is used in code-division multiple access (CDMA)-based networks, such as cellular 3G [7] and Globalstar LEO satellites [8]. Orbcomm [9] and Iridium [10] LEO satellites also employ beacons with IC.

A Generic Signal Model

The channel between the ith source and the user equipment (UE) is considered to have a single tap with the complex channel gain α_i. The received baseband signal samples can be modeled as

$$r[n]=\sum_{i=1}^{N}\alpha_i(c_i(\tau_r[n])+d_i(\tau_r[n]))\exp(j\theta_i[\tau_n])+w[n] \tag{S1}$$

where $r[n]$ is the received signal at the nth time instant; $\alpha_i[n]$ is the complex channel gain between the UE and the ith source at the nth time instant; and $\tau_r[n]\triangleq\tau_n-t_{s_i}[n]$, where $t_{s_i}[n]$ is the code-delay corresponding to the UE and the ith source at the nth time instant, and τ_n is the sample time expressed in the receiver time. Moreover, N is the number of unknown sources; $c_i[n]$ represents the samples of the continuous-time waveform $c_i(t)$ of the periodic RS corresponding to the ith source with a period of L samples; $\theta_i[\tau_n]=2\pi\int_0^{\tau_n}f_D(\tau)d\tau+\theta_0$ is the beat carrier phase in radians, which includes the effect of the receiver and transmitter clock errors, relativity, and atmospheric delays, with f_D being the Doppler frequency, $T_s=\tau_{n+1}-\tau_n$ being the sampling time, and θ_0 being the constant initial phase; $d_i[n]$ represents the samples of some data transmitted from the ith source; and $w[n]$ is a zero-mean independent and identically distributed noise with $\mathbb{E}\{w[m]w^*[n]\}=\sigma_w^2\delta[m-n]$, where $\delta[n]$ is the Kronecker delta function, and $w^*[n]$ denotes the complex conjugate of random variable $w[n]$.

The received signals can be expressed in terms of the equivalent RS from the ith source, denoted by $s_i[n]$, and the equivalent noise, denoted by w_{eq_i}, which are defined as

$$s_i[n]\triangleq\alpha_i c_i[\tau_n-t_{s_i}[n]]\exp(j\theta_i[\tau_n]) \tag{S2}$$

$$w_{\text{eq}_i}[n]\triangleq d_i[\tau_n-t_{s_i}[n]]\exp(j\theta_i[\tau_n])+w[n]. \tag{S3}$$

Hence, the baseband samples can be rewritten as

$$r[n]=\sum_{i=1}^{N}(s_i[n]+w_{\text{eq}_i}[n]). \tag{S4}$$

In this article, the Doppler frequency is modeled as a linear chirp, i.e., $f_{D_i}[n]=f_{D_{i0}}+\beta_i T_s n$, where $f_{D_{i0}}$ is the initial Doppler frequency, and β_i is the Doppler rate. The received signal at the nth time instant when the Doppler rate is wiped off can be expressed as $r'[n]=\exp(-j2\pi\beta_i T_s^2 n^2)r[n]$. Due to the periodicity of $c(\tau_n)$, $s_i[n]$ has the following property:

$$s_i[n+mL]=s_i[n]\exp(j\omega_i mL)\quad 0\le n\le L-1 \tag{S5}$$

where $\omega_i=2\pi f_{D_{i0}}T_s$ is the normalized Doppler corresponding to the ith transmitting source, and $-\pi\le\omega_i\le\pi$. A vector of L observation samples corresponding to the mth period of the signal is formed as $\mathbf{z}_m\triangleq[r'[mL],r'[mL+1],\ldots,r'[(m+1)L-1]]^{\mathrm{T}}$. The coherent processing interval (CPI) is defined as the number of periods of an RS in a time interval during which the Doppler frequency f_{D_i}, Doppler rate β_i, code delay $t_{s_i}[n]$, and channel gain α_i are constant. The CPI vector is constructed by concatenating K aggregates of $\mathbf{z}_m$ vectors to form the $KL\times 1$ vector:

$$\mathbf{y}=\sum_{i=1}^{N}\mathbf{H}_i\mathbf{s}_i+\mathbf{w} \tag{S6}$$

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

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

where $\mathbf{I}_L$ denotes an $L\times L$ identity matrix; and $\mathbf{w}$ is the noise vector.

- *Beacons with no IC (NIC)*: The samples of beacons with NIC can be any arbitrary number in the time domain. Examples of NIC beacons are the primary synchronization signal (PSS) and secondary synchronization signal (SSS) in orthogonal frequency-division multiplexing (OFDM)-based systems, such as cellular 4G LTE and 5G New Radio (NR). While these signals are originally drawn from a finite alphabet at the transmitter, they are inputted to an inverse discrete Fourier transform. Therefore, in the time domain, the beacon's elements are arbitrary complex numbers. Most modern communication systems, including 5G and Starlink LEO satellites, currently employ this type of beacon [11], [12].

UE-based approaches exploit passively broadcast downlink signals without the need to be a subscriber of the network.

In the navigation literature, navigation observables are ranges or angles deduced from the TOA, DOA, or phase differences, based on a comparison between received signals and receiver-generated beacons. Knowledge of the RSs transmitted by terrestrial sources (e.g., cellular 3G CDMA [13], 4G LTE [14], and 5G NR [15]) and nonterrestrial sources (e.g., Orbcomm [16] and Iridium [17] LEO satellites) enabled the design of so-called opportunistic navigation receivers, which could exploit the source's downlink signal to produce TOA, DOA, and FOA measurements. Highly accurate navigation capabilities have been demonstrated exclusively with these measurements in the absence of GNSS signals [18]. Notably, it was shown that cellular TOA measurements could navigate unmanned aerial vehicles (UAVs) to submeter-level accuracy [19] and pedestrians indoors [20], ground vehicles [21], and high-altitude aircraft [22] to meter-level accuracy.

Generating a replica of the beacon by the UE is not straightforward in the following cases:

1) *Private networks*: For public networks, one can refer to publicly available protocols [e.g., 3rd Generation Partnership Project (3GPP)] to design a receiver capable of extracting navigation observables from received signals by acquiring and tracking the timing and phase of the beacons. However, in private networks (e.g., communication systems with closed protocols), there is little to no detail about their signal structure, which hinders the design of conventional opportunistic navigation receivers (i.e., those exploiting the known RSs in the downlink signals). This is particularly the case for broadband LEO satellite providers (e.g., Starlink, OneWeb, Kuiper, etc.), which are planning to aggregately launch, over this decade, tens of thousands of satellites (referred to as *megaconstellations*). In such a case, can one sense and exploit unknown signals for PNT?
2) *Ultra-lean transmission*: In previous cellular network generations, several beacon signals (e.g., cell-specific RSs) were broadcasted at regular and known time intervals, regardless of the number of UEs in the environments. *Ultra-lean design* refers to minimizing these always-on transmissions. Modern communication systems, such as 5G NR, transmit some of the beacon signals only when necessary, or on demand [23]. Conventional opportunistic navigation receivers will either fail to operate or be unable to exploit the entire available bandwidth when the RSs are dynamic. For instance, while the RSs allocated to a single LTE channel have a predetermined

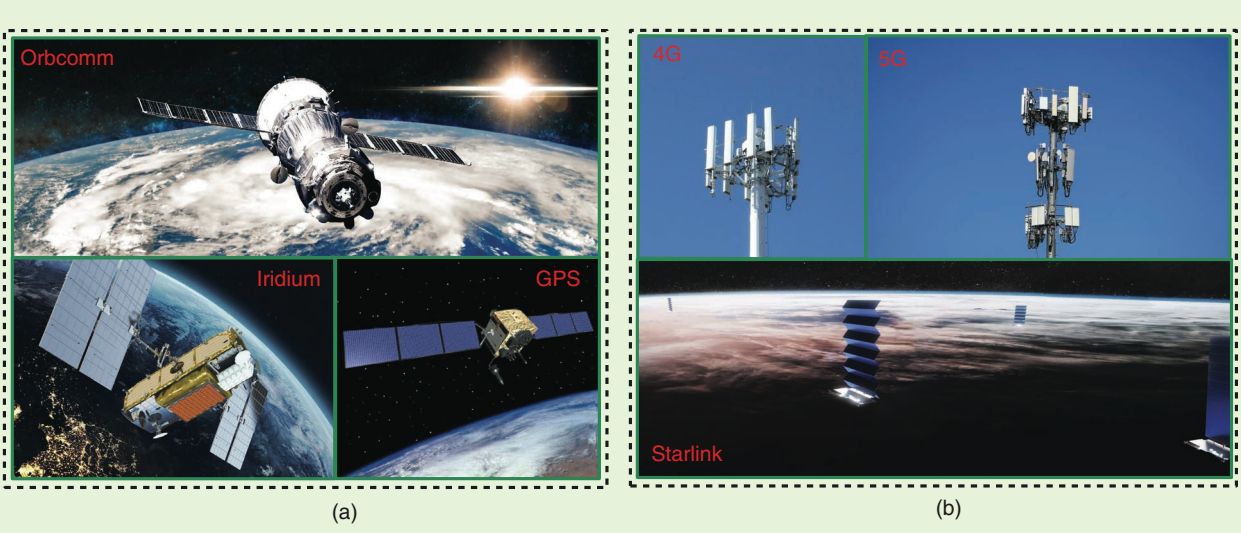

FIGURE 1. The communication signals that are cognitively sensed, tracked, and exploited for navigation via the COSON framework presented in this article. (a) Beacons with integer constraint (IC): GPS, Orbcomm, and Iridium satellites. (b) Beacons with no IC (NIC): cellular 4G and 5G and Starlink satellites. (Sources: GPS: https://www.af.mil/News/Article-Display/Article/115915/first-gps-iif-satellite-on-station/; Orbcomm: https://www.orbcomm.com/en/partners/connectivity/satellite; Iridium: https://www.iridium.com/company/; 4G: https://medium.com/@artiedarrell/lte-and-interferance-on-horizons-network-4bc530e7ef51; 5G: https://www.nbcnews.com/tech/tech-news/faa-clears-verizon-t-turn-5g-cell-towers-rcna14018; Starlink: https://www.dailymail.co.uk/sciencetech/article-11490151/How-Elon-Musks-Starlink-3-000-satellites-works.html.)

bandwidth of up to 20 MHz, the allocated bandwidth for the RSs in a single 5G channel is dynamic; i.e., it adaptively changes based on the transmission mode and can go up to 100 and 400 MHz for frequency ranges 1 and 2 frequency (FR1 and FR2), respectively [12]. On the other hand, Starlink LEO satellite downlink signals occupy 250 MHz of bandwidth of the Ku-band to provide high-rate broadband connectivity, but while some of the downlink RSs (PSS and SSS) have been reverse engineered [24], the full allocated bandwidth RSs are unknown [11] and subject to change. In such a case, can a UE that is not subscribed to the network detect "on-demand" beacons and exploit the entire bandwidth to generate navigation observables?

Cognitive sensing and opportunistic navigation (COSON) has been recently introduced to address these emerging challenges [25], [26], [27], [28]. A spectral approach to COSON focusing on LEO satellites was developed in [29]. In this article's context, *sensing* is defined as the detection of the presence of a transmitting source, whether terrestrial or nonterrestrial, in the environment, whose signals are unknown a priori. Upon detection, salient RS parameters are estimated.

COSON can be thought of as an instantiation of integrated sensing and communication, but, instead of having the "luxury" to design signals with ISAC capabilities, COSON 1) senses arbitrary, unknown communication signals and 2) exploits them for PNT purposes. In this article, *COSON* is defined as a system capable of sensing unknown signals in the environment, blindly learning their beacons, and exploiting them for PNT purposes. Endowed with COSON, a receiver may 1) localize unknown sources and/or 2) exploit these sources to navigate. Essentially, this article argues that "the truth is out there" and that one can sense and exploit unknown signals, whether "legacy" non-ISAC signals or ISAC-devised.

Essentially, this article argues that "the truth is out there" and that one can sense and exploit unknown signals, whether "legacy" non-ISAC signals or ISAC-devised.

This article gives a tutorial of COSON, which has been successfully applied to terrestrial and nonterrestrial signals. The article is organized as follows. The "COSON" section describes the COSON framework. The "Experimental Demonstrations" section shows extensive experimental results demonstrating the successful application of COSON to exploit terrestrial and nonterrestrial signals with IC and NIC beacons (see Figure 1)—namely, cellular 4G and 5G, GPS, and Starlink, Orbcomm, and Iridium LEO—to localize stationary antennas and navigate UAVs and a ground vehicle. The final section gives concluding remarks.

COGNITIVE SENSING AND OPPORTUNISTIC NAVIGATION

The COSON framework is composed of the following stages:

1) *Blind signal acquisition*: This step performs 1) spectrum sensing and signal activity detection, 2) blind beacon estimation, 3) initial Doppler and Doppler rate estimation, and 4) blind source enumeration.
2) *Blind signal tracking and beacon refinement*: The initial estimate of the Doppler frequency corresponding to each source is fed to tracking loops along with the estimated beacon. The delay and Doppler are tracked over time via the tracking loops, which could employ conventional phase-locked loops (PLLs) and delay-locked loops (DLLs) or be Kalman filter (KF)-based. The estimated beacon is also refined in this stage.
3) *Interference and multipath classification*: A blindly detected source in the acquisition stage can be either 1) a valid source (e.g., a cellular tower or an LEO satellite) or 2) a false alarm due to interfering signals and/or nonline-of-sight or multipath components. This step determines whether the detected source is a valid source or a false alarm.
4) *Sensing and navigation*: The final stage is to blindly localize the valid sources (sensing) and/or blindly navigate the UE by feeding the obtained navigation observables into a filter.

The COSON stages are discussed next. Figure 2 illustrates the first three stages, with examples from terrestrial and nonterrestrial signals. The forthcoming discussion refers to this figure.

Signal acquisition

The detection of an unknown source in the presence of other interfering signals has been studied via the paradigm of matched subspace detectors in the detection theory literature [30]. Matched subspace detectors are used frequently in radar signal processing [31], [32] and have been recently adopted for COSON [25], [26], [27], [28]. In what follows, the detection of beacons with IC and NIC is discussed as well as the estimation of the beacon period.

Detection of beacons with NIC (cellular 4G and 5G and Starlink LEO satellite signals)

NIC beacons can assume any arbitrary complex-valued numbers. The autocorrelation of a large enough time segment of the received signal will result in a train of an impulse-like function whose shape depends on the autocorrelation properties of the synchronization signals. OFDM-based systems organize their signals in a frame whose length is equal to the period of the synchronization signals. In high-Doppler-dynamics scenarios (e.g., LEO satellites), a smaller frame length is selected to avoid Doppler spread [33]. The challenges of the detection of beacons with NIC are 1) the presence of multiple interfering unknown sources, 2) the effect of Doppler estimation error on the detection performance, and 3) the selection of the detection threshold.

To address the aforementioned challenges, a generalized version of the matched subspace detector with successive interference cancellation was developed in [25] and [28]. The signal subspace was defined by the Doppler frequencies of the unknown sources. Signal activity detection of unknown sources relies on the Doppler subspace. A hypothesis-testing problem was solved sequentially in

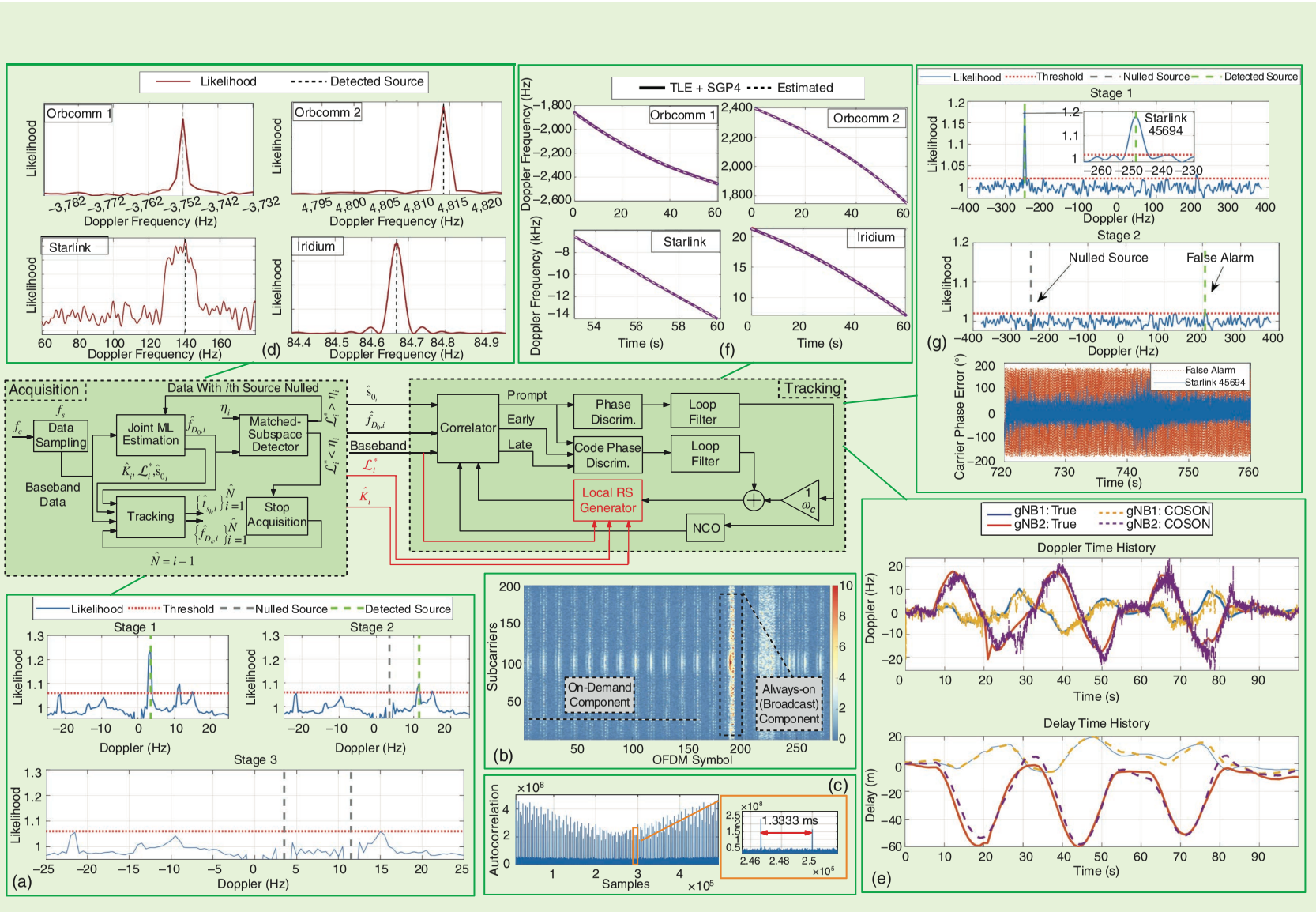

FIGURE 2. The first three stages of COSON with examples from terrestrial and nonterrestrial signals. (a) The acquisition of two 5G gNBs on a UAV. (b) The blindly estimated 5G frame. (c) The estimation of the Starlink RS period. (d) The acquisition of one iridium, one Starlink, and two Orbcomm LEO satellites on a ground vehicle. (e) The delay and Doppler tracking of two 5G gNBs on a ground vehicle. (f) The Doppler tracking of one Iridium, one Starlink, and two Orbcomm LEO satellites on a ground vehicle. (g) The acquisition and tracking of a Starlink satellite and a false alarm source.

multiple stages to detect the active sources in the environment (see "Hypothesis Testing"). At each stage, a test was performed to detect the most powerful source by comparing a likelihood with a predetermined threshold, while the Doppler subspace of the previously detected sources were nulled. The so-called *general linear detector* [34] was modified based on the *generic signal model* and used at each stage of the sequential detection algorithm (see "Sequential Matched Subspace Detection").

The estimated number of active sources is denoted by $\hat{N}$; in the first stage of the algorithm, the presence of a single source is tested. If the null hypothesis is accepted, $\hat{N} \equiv 0$, which means that no source is detected to be present in the environment. If the test rejects the null hypothesis, the algorithm asserts the presence of at least one source and performs the test to detect the presence of other sources in the presence of the previously detected source. The unknown signal parameters of each detected source are estimated at each stage. If the null hypothesis at the ith stage of the algorithm is accepted, the algorithm terminates, and the estimated number of sources is $\hat{N} \equiv i-1$.

At each stage, the likelihood is compared with a predetermined threshold, selected based on the probability of a false alarm. A detector is referred to as a *constant false alarm rate* (*CFAR*) detector if the probability of a false alarm does not depend on the noise variance and/or other unknown parameters. The CFAR properties of the detector were investigated in [25] along with theoretical limits of the detection of multiple sources in the presence of Doppler estimation error. The choice of the optimal coherent processing interval (CPI) length was studied in [27]. Figure 2(a) shows the acquisition stages of two 5G base stations (also known as gNodeB, gNB) transmitting on the same frequency, on a UAV: the likelihood function at each stage and detected and nulled sources.

Detection of beacons with IC (GPS and Orbcomm and Iridium LEO satellite signals)

For IC beacons, the IC of the beacon symbols in the matched subspace detector leads to a class of integer-least-square (ILS) problems [35]. One example of beacons with IC is the PRN sequence in CDMA-based communication systems. A low computational complexity approach to estimate the beacon symbols is symbol-by-symbol (SBS) estimation, which suffers from a poor performance in low-signal-to-noise-ratio (SNR) regimes. In [36], SBS estimation was adopted to blindly estimate the symbols of the PRN sequences of Galileo and Compass satellites, utilizing a 1.8-m high-gain antenna to accumulate enough signal power. The optimal algorithm proposed in [35] can be used to solve the ILS problem with a polynomial computational complexity.

A fundamental challenge of the detection methods with IC is the computational complexity of the ILS problem, which involves a search over a discrete space that depends on the modulation order and beacon length. The length of beacon sequences is typically very large. For instance, the length of the beacon for GPS PRNs is $2^{10}-1$. A near-optimal beacon detector with linear computational complexity was developed in [26], which was shown to significantly outperform SBS estimation in a low-SNR regime. Another matched subspace-based approach for the detection of signals with IC, such as

Hypothesis Testing

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

$$\begin{cases} \mathcal{H}_0\text{: } i\text{th source is absent} \\ \mathcal{H}_1\text{: } i\text{th source is present.} \end{cases} \tag{S7}$$

Under $\mathcal{H}_1$, the signal can be modeled as

$$\boldsymbol{y} = \mathbf{H}_i \mathbf{s}_i + \mathbf{B}_{i-1}\boldsymbol{\theta}_{i-1} + \mathbf{w}_{\text{eq}_i} \tag{S8}$$

where $\mathbf{B}_{i-1} \triangleq [\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_{i-1}]$ and $\boldsymbol{\theta}_{i-1} \triangleq [\mathbf{s}_1^\top, \mathbf{s}_2^\top, \ldots, \mathbf{s}_{i-1}^\top]^\top$ store the chirp parameters and estimated RS in the previous steps, respectively. The decision criteria for the source detection are developed based on the generalized likelihood ratio (GLR). The likelihood of the GLR detector is [25]

$$\mathcal{L}_i(\mathbf{y}) = \frac{\mathbf{y}^{\mathrm{H}} \mathbf{P}_{\mathbf{S}_i} \mathbf{y}}{\mathbf{y}^{\mathrm{H}} \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} \mathbf{P}^{\perp}_{\mathbf{S}_i} \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} \mathbf{y}} \tag{S9}$$

where $\mathbf{y}^{\mathrm{H}}$ denotes the Hermitian transpose of $\mathbf{y}$, $\mathbf{P}_{\mathbf{X}} \triangleq \mathbf{X}(\mathbf{X}^{\mathrm{H}}\mathbf{X})^{-1}\mathbf{X}^{\mathrm{H}}$ denotes the projection matrix to the column space of $\mathbf{X}$, and $\mathbf{P}^{\perp}_{\mathbf{X}} \triangleq \mathbf{I} - \mathbf{P}_{\mathbf{X}}$ denotes the projection matrix onto the space orthogonal to the column space of $\mathbf{X}$. Also, $\mathbf{S}_i \triangleq \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} \mathbf{H}_i$

Sequential Matched Subspace Detection

The maximum likelihood (ML) estimate $\hat{\omega}_i$ is obtained by maximizing the likelihood function (S9), which yields

$$\hat{\omega}_i = \underset{\omega_i}{\operatorname{argmax}} \left\| \mathbf{H}_i^{\mathrm{H}} \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}} \mathbf{y} \right\|^2 \tag{S10}$$

which is used to construct $\mathbf{P}_{\mathbf{B}_{i-1}}$ and $\mathbf{H}_i$. The algorithm's sequential structure allows for single-variable estimation of the Doppler frequency at each stage, as denoted in (10). For example, during the first stage, a 1D search is performed to find the ML estimate of ω_1, denoted as $\hat{\omega}_1$. In the second stage, $\hat{\omega}_1$, is used to form a projection matrix that eliminates the subspace of the first source. At each subsequent stage, the previously estimated Doppler values are used to conduct a 1D search for $\hat{\omega}_i$, which is then used to generate the corresponding projection and Doppler matrices for that stage, represented by $\mathbf{P}_{\mathbf{B}_{i-1}}$ and $\mathbf{H}_i$. More details can be found in [25].

Iridium and Orbcomm, was proposed in [37]. In this framework, to acquire the Doppler frequency of signals with IC, the samples of Orbcomm and Iridium were raised to the powers of two and four, respectively. Figure 2(d) shows the acquisition of one Iridium, one Starlink, and two Orbcomm LEO satellites on a ground vehicle. Further details of this framework are discussed in [37].

Estimation of the period of the beacon

Beacon detection in COSON relies on knowledge of the beacon period. In public networks, the beacon period is typically specified in the protocol description. For 5G, depending on the network operator, the synchronization signals and physical broadcast channel (SS/PBCH) can have a periodicity of 5 ms, 10 ms, 20 ms, 40 ms, 80 ms, or 160 ms.

However, the beacon period for private networks is unknown and subject to change. Period estimation has been studied in the literature [38].

The COSON framework is able to update the estimated beacon dynamically in the tracking process.

A fundamental challenge that could arise in period estimation is the Doppler rate effect. A nonstationary transmitter and/or maneuvering UE could result in significant Doppler rate values. Unlike the Doppler effect, which does not change the magnitude of the autocorrelation function, the Doppler rate has a destructive effect on the autocorrelation function [27].

The autocorrelation of a large enough time segment of the received signal results in a train of an impulse-like function whose shape depends on the autocorrelation properties of the RSs. The distance between two consecutive impulses is equal to the beacon period. A Doppler rate wipe-off process was proposed in [39], which enabled the estimation of Starlink's OFDM period to be about 1.3333 ms. Figure 2(c) shows the autocorrelation of a 100-ms time segment of the Starlink downlink signal after Doppler rate wipe off. When this cognitive beacon estimation process was applied to 5G signals, it estimated the 5G NR frame length from a terrestrial gNB to be 10 ms, which corroborates the standard frame length of 5G NR downlink signals [27].

Blind signal tracking and refinement

Conventional tracking loops track the time variations of the code phase and carrier phase via DLL and PLL, respectively, or a KF. DLL/PLL loops are composed of three constituent blocks: 1) a code/carrier phase discriminator, which is in charge of providing output measurements that, on average, are proportional to the code/carrier phase error to be compensated; 2) a loop filter, which acts as narrow low-pass filter that smooths the variability caused by thermal noise at the phase detector output; and 3) a numerically controlled oscillator for generating the local carrier replica based on the corrections imposed by the loop filter output [40].

In 5G and beyond networks, ultra-lean transmission allows the network to transmit some of the beacons only when it is necessary, and the transmitted beacons are subject to change. The COSON framework is able to update the estimated beacon dynamically in the tracking process. Some of the core blocks of the COSON tracking loop are similar to conventional code/carrier phase tracking architectures. The difference between the COSON tracking loop and conventional loops is highlighted in red in Figure 2. The main difference is the local RS generator with adaptive gains, which performs beacon sequence updates in the tracking process.

The RS in the tracking loop for the ith source is initialized with the RS estimated in the acquisition stage $\hat{\mathbf{s}}_{\text{acq}_i}$ (i.e., $\hat{\mathbf{s}}_{0_i} \equiv \hat{\mathbf{s}}_{\text{acq}_i}$). Let $\hat{t}_{s_k,i}$ and $\hat{f}_{D_k,i}$ be the code phase and the Doppler estimates of the ith source at time step k in the tracking loop, respectively. The estimated RS is updated by coherently accumulating the measurement at the kth step of the tracking loop when the delay and Doppler are wiped off. If the subspace spanned by the columns of $\mathbf{S}_i = \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{H}_i$ is viewed as the ith source's signal subspace and the orthogonal subspace as the noise subspace, then the likelihood $\mathcal{L}_i^*$ can be interpreted as the ith source SNR estimate. Readers are referred to [30] for further interpretations of matched subspace detectors.

The loop gain of the so-called RS-locked loop (RSLL) is designed based on the acquisition performance. If the ith source estimated SNR $\mathcal{L}_i^*$ is large, the tracking loop relies more on the acquisition by diluting the contribution of new measurements in the estimation of the RS. Hence, the metric $\mathcal{L}_i^*$ informs the tracking loops about the detection performance of the ith source. When dealing with unknown signals, the transition from acquisition to tracking has a dramatic effect on the convergence and performance of the tracking loops [27]. Selecting the loop gain as such is necessary to converge when the RSs are very close in the Doppler space. Figure 2(b) shows a cognitively reconstructed 5G frame via the RSLL, showing successful estimation of both always-on and on-demand components. Figure 2(e) shows delay and Doppler tracking of two 5G gNBs on a ground vehicle, while Figure 2(f) shows Doppler tracking of one Starlink, and one Iridium, and two Orbcomm satellites on a ground vehicle. It is worth noting that KF-based tracking was adopted here. The tracking results are illustrated after normalizing the estimated Doppler frequency [37].

Interference and multipath classification

The detected sources in the acquisition stage can be either a valid source or a false alarm (e.g., interfering signals and/or multipath components). Classifying detected signals falls into the paradigm of interference classification [41]. Due to the limited information about the unknown environment in which the UE is operating, interference classification should be performed in a blind fashion. The features considered in interference classification algorithms in the literature are either specifically designed based on the signal model or require a training phase, which may not be possible in a blind scenario. A valid signal for the COSON framework is the line-of-sight (LOS) component of the transmitted signal. In the presence

of an LOS component, the amplitude gain is often characterized by a Rician distribution. The carrier phase error in the tracking loops depends on the LOS signal power. The COSON approach uses the variance of the carrier phase error as the classification feature to distinguish a valid source from a false alarm [25]. Figure 2(g) shows blind detection of a Starlink satellite, where the acquisition stage returned two sources to be present: one corresponded to a Starlink satellite, while the other corresponded to a false alarm.

Sensing and navigation

The navigation observables produced by the tracking loops can be used to sense the environment, localizing transmitting sources, and/or navigating the UE. In [27], it was shown how a mobile ground vehicle with knowledge of its states could cognitively localize an unknown 5G gNB transmitter to within a few meters. The following section presents extensive navigation results of multiple platforms with terrestrial and nonterrestrial sources.

Experimental demonstrations

This section presents experimental demonstrations showing the broad applicability of the COSON framework to cognitively sense and exploit various terrestrial and nonterrestrial signals for PNT. Table 1 summarizes the experimental demonstrations presented herein.

Experiment 1: UAV navigation with 4G signals

This experiment was conducted with real cellular LTE signals received on a UAV to evaluate the performance of COSON in an environment in which some LTE base stations (also known as eNodeBs) were transmitting on the same carrier frequency. The UAV's navigation solution obtained from the cognitively acquired and tracked LTE eNodeBs are compared with the navigation solution obtained from the receiver developed in [42], which was matched to the known LTE beacons (obtained from 3GPP).

A DJI Matrice 600 UAV was equipped with a National Instrument (NI) universal software radio peripheral (USRP) 2955 and four consumer-grade cellular antennas. The USRP channels were tuned to 1955, 2145, 2125, and 739 MHz carrier frequencies, respectively, which are 4G LTE frequencies allocated to the U.S. cellular providers AT&T, T-Mobile, and Verizon. The sampling rate for each channel was set to 10 Msps and the sampled LTE signals were stored for postprocessing. To obtain the UAV's ground truth trajectory, the UAV was also equipped with a Septentrio AsteRx-i V GNSS-aided inertial navigation system (INS), which is a dual-antenna, multifrequency GNSS receiver with real-time kinematics, coupled with a Vectornav VN-100 microelectromechanical systems (MEMS) industrial-grade inertial measurement unit (IMU).

The UAV traversed a trajectory of 609 m in 160 s in Aliso Viejo, CA, USA. The LTE samples were processed through COSON, and the conventional receiver was matched to the known beacons [42]. A total of 11 4G eNodeBs, whose positions were mapped prior to the experiment [43], were acquired by COSON. The mapped eNodeBs were validated via Google Maps, whose accuracy was considered to be the ground truth for the mapped positions. After manual data association, it was found that only six of them pertained to the ones detected by the conventional receiver, while the rest pertained to unknown eNodeBs in the environment that were not detected by the conventional receiver. For a fair navigation solution comparison, both receivers were used to track the six common eNodeBs to produce carrier phase measurements, which were fused via two extended KFs (EKFs) to estimate the UAV's trajectory. The 2D position root-mean-square error (RMSE) of the COSON and conventional receivers were both calculated to be 2.1 m. The main sources of navigation error include the eNodeBs' and receiver's clock errors, the eNodeBs' position error, and unmodeled effects (e.g., multipath). The experimental results are summarized in Figure 3. Additional details and analysis can be found in [25].

Table 1. Summary of experiments.

Signal Type	Frequency (MHz)	Provider	Receiver Type	Signal Specification	Measurement Model	Number of Sources	Navigation Filter	Duration (s)	Distance Traversed (m)	2D Position RMSE (m)
4G	739 1,955 2,125 2,145	AT&T, T-Mobile, and Verizon	UAV	OFDM (NIC)	Carrier phase	6	EKF	175	609	2.1
5G	632.55	T-Mobile	UAV	OFDM (NIC)	Carrier phase and code phase	2	EKF	100	416	4.2
GPS	1,575.42	U.S. Dept. of Defense	Stationary	CDMA (IC)	Code phase	4	NLS	110	0	54.5
Starlink	11,325	SpaceX	Stationary	OFDM (NIC)	Doppler	6	WNLS	800	0	6.5
Multi-LEO			Ground vehicle				EKF	60	540	11.6
Orbcomm	137			SD-QPSK (IC)	Doppler	2				
Iridium	1,626.2708			DE-QPSK (IC)	Doppler	1				
Starlink	11,325			OFDM (NIC)	Doppler	1				

WNLS: weighted nonlinear least squares.

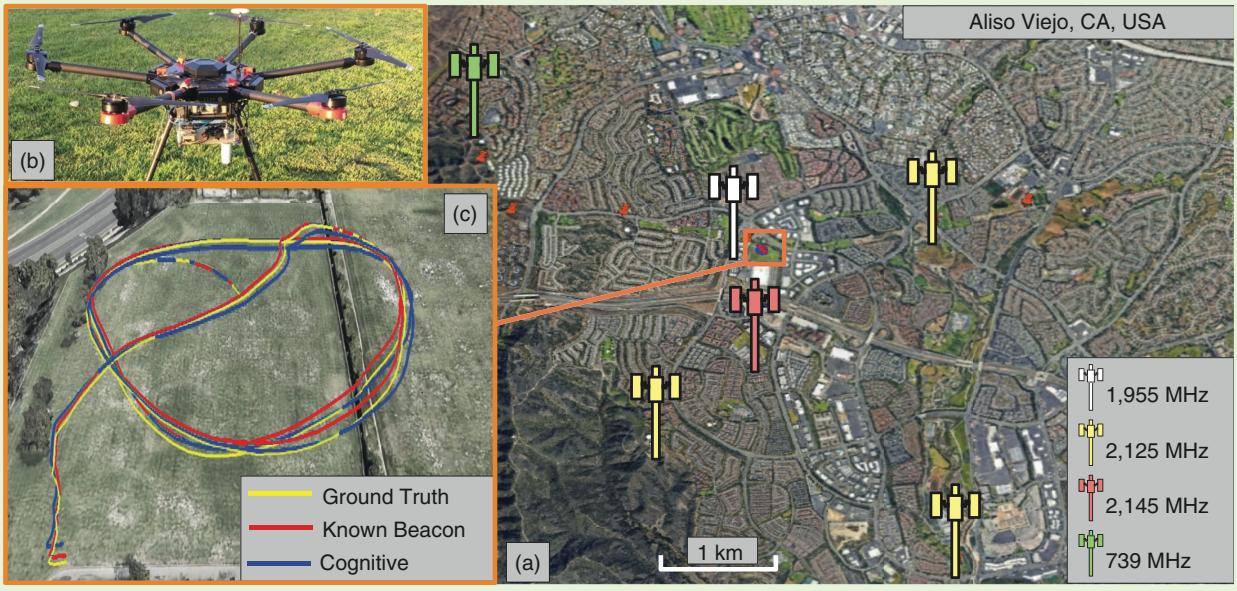

FIGURE 3. The 4G experimental results: the (a) environment layout, (b) UAV, and (c) UAV trajectory: ground truth and estimated with the known beacon versus COSON.

Experiment 2: UAV navigation with 5G signals

This experiment was conducted with real cellular 5G signals received on a UAV to show the navigation solution with both always-on and on-demand components. The UAV's navigation solution obtained from the cognitively acquired and tracked 5G signals are compared with the navigation solution obtained from the receiver developed in [15], which was matched to the known 5G beacons (obtained from 3GPP).

An Autel X-Star Premium UAV was equipped with a single-channel Ettus 312 USRP connected to a consumer-grade cellular antenna and a small consumer-grade GPS antenna to discipline the onboard oscillator. The USRP was tuned to the cellular carrier frequency 632.55 MHz, which is a 5G frequency allocated to the U.S. cellular provider T-Mobile. Samples of the received signals were stored for offline postprocessing.

The UAV traversed a trajectory of 416 m in 100 s in Santa Ana, CA, USA. Two 5G gNBs, whose positions were mapped prior to the experiment [43], were detected using COSON and the conventional receiver. The mapped gNBs were validated via Google Maps, whose accuracy was considered to be the ground truth for the mapped positions. Both receivers tracked the carrier phase and code phase of the gNBs. EKFs were used to fuse the code phase observables to estimate the UAV's trajectory. The 2D position RMSEs of the COSON and conventional receivers were 4.2 and 4.6 m, respectively. The reason COSON achieved a lower RSME is that the conventional receiver used only the always-on signals, while the COSON receiver exploited all of the available bandwidth of the received signal, which, in turn, resulted in a more accurate TOA estimation. The main sources of navigation error include the gNBs' and receiver's clock errors, the gNBs' position error, and unmodeled effects (e.g., multipath). The experimental results are summarized in Figure 4. Additional details and analysis can be found in [26].

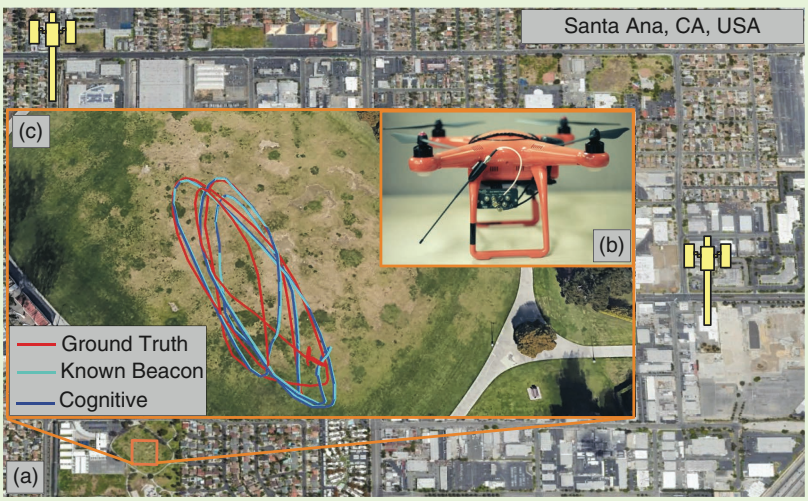

FIGURE 4. The 5G experimental results: the (a) environment layout, (b) UAV, and (c) UAV trajectory: ground truth and estimated with the known beacon versus COSON.

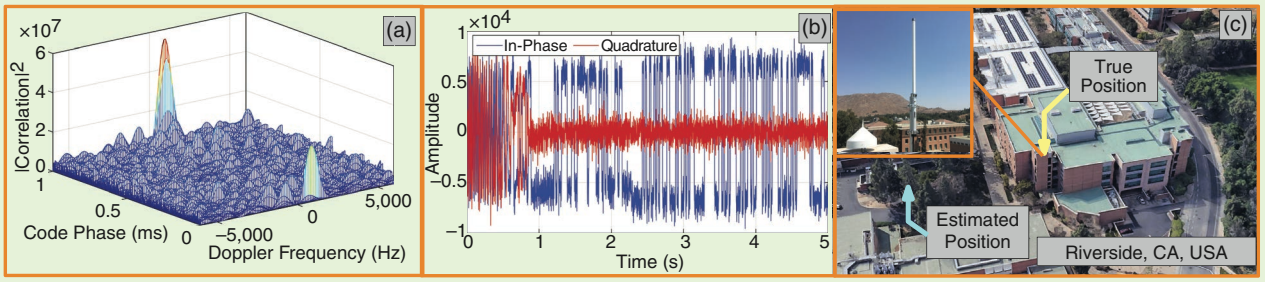

FIGURE 5. GPS experimental results: the (a) blind acquisition of GPS PRN 21, (b) in-phase and quadrature components of PRN 21 from the tracked signal, and (c) environment layout showing the true antenna position and estimated position.

Experiment 3: Stationary positioning with GPS signals

This experiment was conducted with real GPS L1 coarse acquisition signals (C/A) received on a stationary antenna to show successful deciphering of GPS PRN sequences. A GPS antenna was mounted on the roof of the Winston Chung Hall at the University of California, Riverside, CA, USA. The GPS signals were downmixed and sampled via an NI USRP-2955, tuned to the GPS L1 frequency 1,575.42 MHz, and driven by a GPS-disciplined oscillator. Samples of the received signals were stored for offline postprocessing.

GPS satellite signals were blindly detected, and, with sufficiently long CPI, the Doppler was estimated and tracked. Next, the residual carrier was wiped off from the received signal, Doppler-compensated, and coherently accumulated. The navigation message bits were wiped off by two successive frames to determine whether a transition occurred or not. The GPS beacon of four GPS PRNs were decoded (PRN 20, 21, 25, and 29). The percentage of correctly decoded PRN chips ranged between 91% and 99.9%.

The decoded PRNs were then used to produce pseudorange observables from the received GPS signals. The initial Doppler and code phase estimates were used to initialize a software-defined receiver's tracking loops, which employed a third-order PLL with a carrier-aided DLL with the dot product discriminator. Figure 5(a) shows the blind acquisition of PRN 21, and Figure 5(b) shows the in-phase and quadrature components of the tracked prompt correlation of PRN 21.

The produced pseudorange measurements for the four GPS satellites at all time steps were stacked into a measurement vector, and a batch nonlinear least-squares (NLS) estimator was implemented to estimate the antenna's position and bias terms capturing the unknown bias between the receiver's and each of the satellite's clocks. The GPS satellites' positions were obtained by decoding the GPS satellites' navigation message. The receiver's position in the NLS was initialized around 150 km from the true receiver's position. The estimated receiver's 2D position converged to within 54.5 m from the true receiver's position. The main sources of positioning error include incorrectly decoded PRN chips, atmospheric delays, satellites' ephemerides errors, the receiver's clock errors, and unmodeled effects (e.g., multipath). Figure 5(c) shows the true and estimated positions. Additional details and analysis can be found in [44].

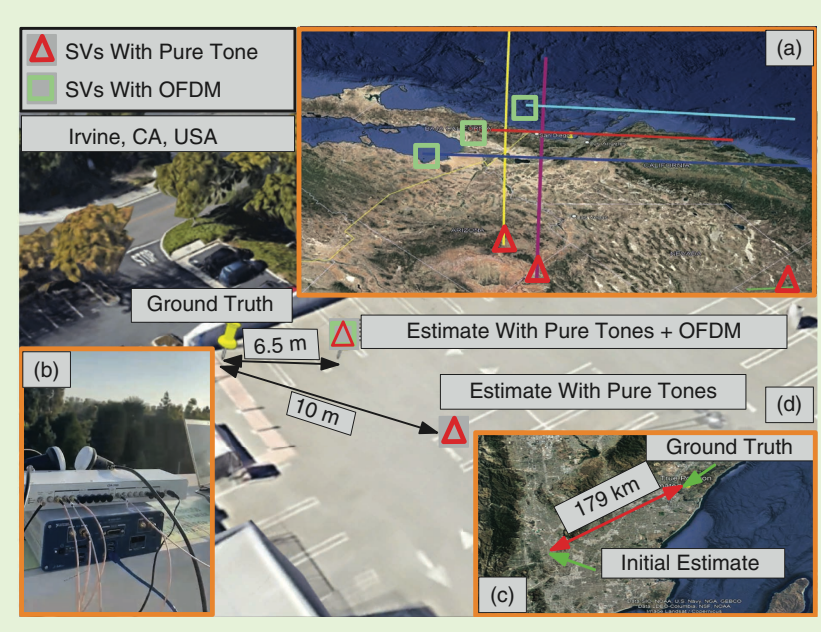

FIGURE 6. Starlink LEO experimental results: (a) Starlink satellite trajectories, (b) the hardware setup, (c) the initial estimate relative to the true position, and (d) the positioning results with six Starlink space vehicles (SVs).

Experiment 4: Stationary positioning with Starlink LEO satellite signals

This experiment was conducted with real Starlink LEO signals received on a stationary antenna to show successful acquisition, Doppler tracking, and positioning. An NI USRP-2945R

was equipped with a consumer-grade Ku antenna and a low-noise block (LNB) downconverter to receive Starlink signals in the Ku-band. The sampling rate was set to 2.5 MHz, and the carrier frequency was set to 11.325 GHz to record Ku signals over a period of 800 s.

The COSON receiver detected six Starlink LEO satellites. While all six satellites broadcasted pure tones, the COSON receiver concluded that three of them also transmitted OFDM-like signals. The receiver's position was estimated via a weighted NLS from Doppler measurements extracted from the three satellites with pure tones and the three satellites with pure tones and OFDM-like signals. The receiver's position estimate was initialized as the centroid of all satellite positions, projected onto the surface of Earth, yielding an initial position error of 179 km. The satellites' positions were obtained from two-line element (TLE) files and simplified perturbations (SGP4) software. The simplified models of perturbing forces—which include nonuniform Earth gravitational field, atmospheric drag, solar radiation pressure, third-body gravitational forces (e.g., the gravity of the moon and sun), and general relativity—cause kilometer-level errors in a propagated satellite orbit, with most of the error being concentrated in the satellite's direction of motion [45]. To account for the ephemeris errors, the TLE epoch time was adjusted for each satellite [46]. This was achieved by minimizing the pseudorange rate residuals for each satellite. The final 2D position error with the six satellites' pure tones was 10 m. When Doppler measurements from the three satellites transmitting OFDM-like signals were incorporated, the error reduced to 6.5 m. It is worth highlighting that it was later discovered that, upon applying the COSON framework developed in [29], all six Starlink LEO satellites were actually transmitting OFDM signals, and the full Starlink OFDM beacon, spanning the whole time-frequency resource grid, was reconstructed [47].

Instead of having the "luxury" of designing signals with ISAC capabilities, COSON senses arbitrary, unknown terrestrial and nonterrestrial communication signals and exploits them for PNT purposes.

The main sources of positioning error in this experiment include incorrectly estimated RSs, the impact of the highly dynamic channel on tracking, satellites' ephemerides errors, atmospheric delays, satellites' and the receiver's clock errors, and unmodeled effects (e.g., multipath). Figure 6 summarizes the experimental results. Additional details and analysis can be found in [39].

Experiment 5: Ground vehicle navigation with multiconstellation LEO satellite signals

This experiment was conducted with real signals from three LEO constellations (Starlink, Orbcomm, and Iridium), received on a ground vehicle. The vehicle was equipped with an NI USRP-2955, USRP-312, and USRP-2974 and three different types of antennas (GPS survey antenna, a very-high-frequency quadrifilar helix antenna, and LNBs). The USRPs were tuned to the carrier frequencies 137; 1,626.2708; and 11,325 MHz, which correspond to the downlink of Orbcomm, Iridium, and Starlink LEO satellites. The objective of the experiment is to show the vehicle navigating without GNSS signals by cognitively exploiting downlink LEO signals. The ground vehicle traversed a trajectory of 540 m in 60 s in Columbus, OH, USA. Access to GNSS signals was cut off for the last 492 m, traversed in 40 s.

COSON acquired one Starlink, one Iridium, and two Orbcomm satellites and tracked their Doppler. The produced Doppler was fused with each vehicle's IMU measurements via the simultaneous tracking and navigation (STAN) framework. STAN estimates the vehicle's states simultaneously with the states of the LEO satellites while aiding the INS in a tightly coupled fashion via an EKF [48]. The satellites' states in STAN are initialized by propagating TLE data via SGP4 software in an open-loop fashion until the time of the LEO satellites' visibility. All three USRPs were time stamped by the same computer, synced to the Internet, and used to log the recorded data. The recorded time represents the receiver's time, which is common to all extracted observables. However, each TLE suffers from some timing error; hence, the TLE + SGP4 time of each satellite was then synchronized with the receiver's time in postprocessing. The synchronization was achieved by adjusting each TLE epoch time to minimize the Doppler residuals until the start of the navigation window, after which the LEO satellites' states were estimated in a closed-loop fashion via STAN.

The 2D position RMSE of the LEO-aided INS was 11.6 m. In contrast, cutting off the GNSS signals from the vehicle's GNSS-aided INS system ballooned the RMSE to 87.7 m. The main sources of navigation error include the impact of the highly dynamic channel on tracking, satellites' ephemerides errors, atmospheric delays, satellites' and the receiver's clock errors, IMU errors, and unmodeled effects (e.g., multipath). Figure 7 summarizes the experimental results. Additional details and analysis can be found in [37].

Conclusion

This article presented a promising paradigm termed *COSON*. It can be thought of as an instantiation of ISAC, but, instead of having the "luxury" of designing signals with ISAC capabilities, COSON senses arbitrary, unknown terrestrial and nonterrestrial communication signals and exploits them for PNT purposes. The article overviewed COSON's four stages: 1) blind signal acquisition, 2) blind signal tracking and beacon refinement, 3) interference and multipath classification, and 4) sensing and navigation. Extensive experimental results were presented showcasing the broad applicability of COSON in sensing and exploiting terrestrial (cellular 4G and 5G) and nonterrestrial (GPS and Starlink, Orbcomm, and Iridium LEO) signals without assuming prior knowledge of the signals, achieving meter-level accuracy without GNSS signals.

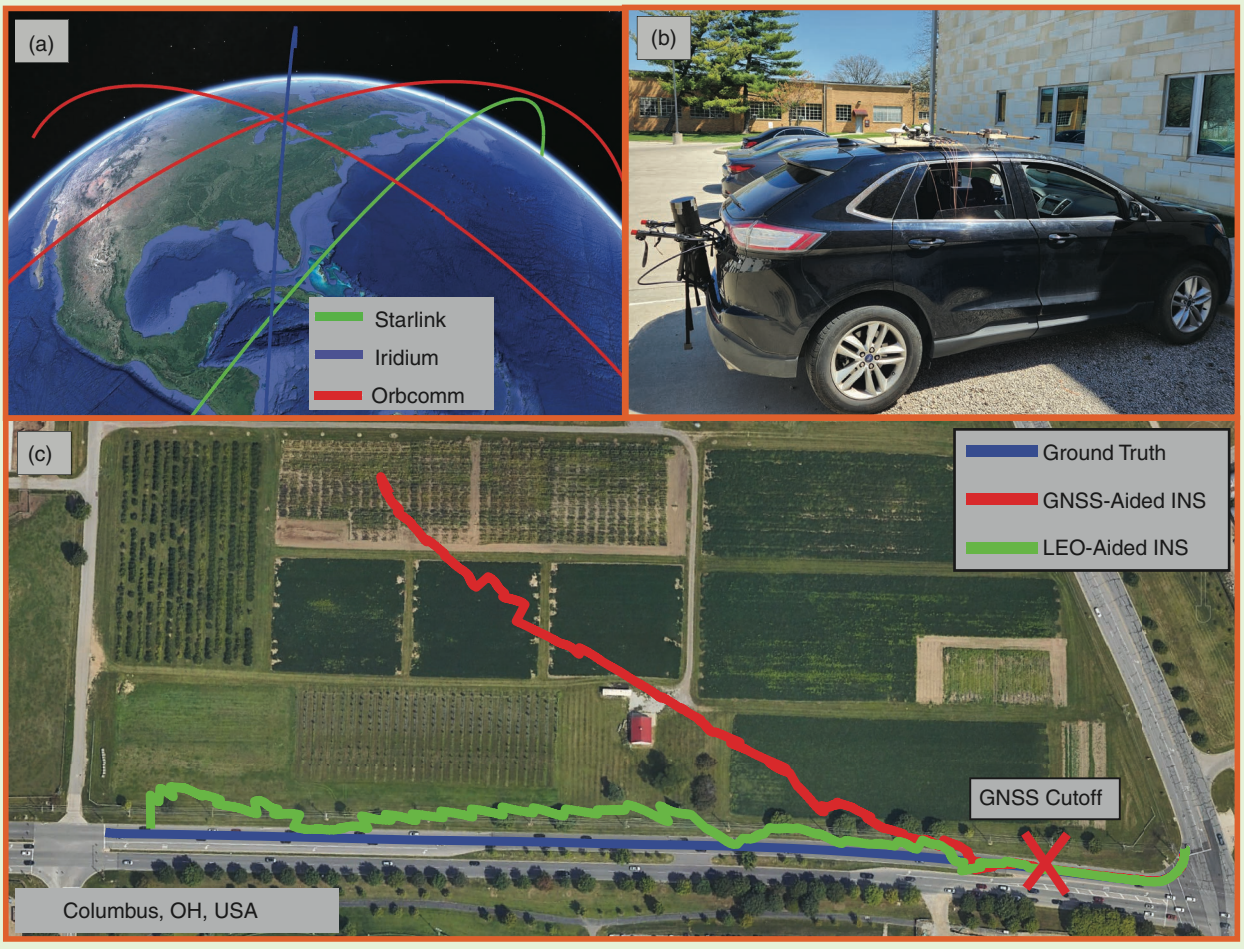

FIGURE 7. Multiconstellation LEO experimental results: (a) satellite trajectories, (b) the ground vehicle, and (c) the vehicle trajectory: ground truth and estimated with GNSS-aided INS versus COSON LEO-aided INS.

Acknowledgments

This work was supported in part by the Office of Naval Research under Grants N00014-19-1-2511, N00014-22-1-2242, and N00014-22-1-2115; the Air Force Office of Scientific Research under Grant FA9550-22-1-0476; the National Science Foundation under Grant 2240512; and the U.S. Department of Transportation under Grant 69A3552348327 for the Center for Automated Vehicles Research with Multimodal AssurEd Navigation (CARMEN+) University Transportation Center.

Authors

Zaher (Zak) M. Kassas (zkassas@ieee.org) is the TRC Endowed Chair in Intelligent Transportation Systems Professor of Electrical and Computer Engineering at The Ohio State University, director of the Autonomous Systems Perception, Intelligence, & Navigation (ASPIN) Laboratory, and director of the U.S. Department of Transportation Center for Automated Vehicles Research with Multimodal AssurEd Navigation (CARMEN+). He is Fellow of IEEE and the Institute of Navigation (ION) and a Distinguished Lecturer of the IEEE Aerospace and Electronic Systems Society and the IEEE Intelligent Transportation Systems Society.

Mohammad Neinavaie (mneinava@uci.edu) received his Ph.D. degree in electrical and computer engineering from The Ohio State University. He is a wireless systems engineer at Apple and was a member of the ASPIN Laboratory. He is a Member of IEEE.

Joe Khalife (khalifej@uci.edu) received his Ph.D. degree in electrical engineering and computer science from University of California, Irvine. He is wireless systems engineer at Apple and was a member of the ASPIN Laboratory. He is a Member of IEEE.

Shaghayegh Shahcheraghi (shahcheraghi.1@buckeyemail.osu.edu) is an electrical and computer engineering Ph.D. student at The Ohio State University and a member of ASPIN Laboratory.

Joe Saroufim (saroufim.1@buckeyemail.osu.edu) is an electrical and computer engineering Ph.D. student at The Ohio State University and a member of the ASPIN Laboratory.

References

[1] Z. Wei, F. Liu, C. Masouros, N. Su, and A. Petropulu, "Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security," *IEEE Commun. Mag.*, vol. 60, no. 4, pp. 65–71, Apr. 2022, doi: 10.1109/MCOM.002.2100972.

[2] A. Behravan et al., "Positioning and sensing in 6G: Gaps, challenges, and opportunities," *IEEE Veh. Technol. Mag.*, vol. 18, no. 1, pp. 40–48, Mar. 2023, doi: 10.1109/MVT.2022.3219999.

[3] C. Barneto, T. Riihonen, S. Liyanaarachchi, M. Heino, N. Gonzalez-Prelcic, and M. Valkama, "Beamformer design and optimization for joint communication and full-duplex sensing at mm-waves," *IEEE Trans. Commun.*, vol. 70, no. 12, pp. 8298–8312, Dec. 2022, doi: 10.1109/TCOMM.2022.3218623.

[4] K. Mishra, M. Shankar, V. Koivunen, B. Ottersten, and S. Vorobyov, "Toward millimeter-wave joint radar communications: A signal processing perspective," *IEEE Signal Process. Mag.*, vol. 36, no. 5, pp. 100–114, Sep. 2019, doi: 10.1109/MSP.2019.2913173.

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

[6] A. Flores. "NAVSTAR GPS space segment/navigation user interfaces" Gps.gov. Available: https://www.gps.gov/technical/icwg/IS-GPS-200N.pdf

[7] 3GPP2, "Physical layer standard for cdma2000 spread spectrum systems (C.S0002-E)," 3rd Generation Partnership Project 2 (3GPP2), TS C.S0002-E, Jun. 2011. [Online]. Available: https://www.3gpp2.org/Public_html/Specs/C.S0002-D_v2.0_051006.pdf

[8] R. Hendrickson, "Globalstar for the military," in *Proc. IEEE Military Commun. Conf.*, vol. 3, Monterey, CA, USA, Nov. 1997, pp. 1173–1178.

[9] S. Reid, *ORBCOMM System Overview (TS A80TD0008 - Revision G)*. Dulles, VA: ORBCOMM LLC, Dec. 2001.

[10] S. Shahcheraghi, F. Gourabi, M. Neinavaie, and Z. Kassas, "Joint Doppler and azimuth DOA tracking for positioning with Iridium LEO satellites," in *Proc. of ION GNSS+ Conf.*, Sep. 2023, pp. 2373–2383.

[11] I. Del Portillo, B. Cameron, and E. Crawley, "A technical comparison of three low earth orbit satellite constellation systems to provide global broadband," *Acta Astronaut. (U.K.)*, vol. 159, pp. 123–135, Jun. 2019, doi: 10.1016/j.actaastro.2019.03.040.

[12] 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 Commun. Standards Mag.*, vol. 4, no. 3, pp. 22–29, Sep. 2020, doi: 10.1109/MCOMSTD.001.1900048.

[13] J. Khalife, K. Shamaei, and Z. Kassas, "Navigation with cellular CDMA signals – part I: Signal modeling and software-defined receiver design," *IEEE Trans. Signal Process.*, vol. 66, no. 8, pp. 2191–2203, Apr. 2018, doi: 10.1109/TSP.2018.2799167.

[14] M. Driusso, C. Marshall, M. Sabathy, F. Knutti, H. Mathis, and F. Babich, "Vehicular position tracking using LTE signals," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3376–3391, Apr. 2017, doi: 10.1109/TVT.2016.2589463.

[15] K. Shamaei and Z. Kassas, "Receiver design and time of arrival estimation for opportunistic localization with 5G signals," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4716–4731, Jul. 2021, doi: 10.1109/TWC.2021.3061985.

[16] C. Zhao, H. Qin, and Z. Li, "Doppler measurements from multiconstellations in opportunistic navigation," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–9, Jan. 2022, doi: 10.1109/TIM.2022.3147315.

[17] C. Huang, H. Qin, C. Zhao, and H. Liang, "Phase-time method: Accurate Doppler measurement for Iridium NEXT signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 6, pp. 5954–5962, Dec. 2022, doi: 10.1109/TAES.2022.3180702.

[18] Z. Kassas and A. Abdallah, "No GPS no problem: Exploiting cellular OFDM-based signals for accurate navigation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 6, pp. 9792–9798, Dec. 2023, doi: 10.1109/TAES.2023.3304286.

[19] J. Khalife and Z. Kassas, "On the achievability of submeter-accurate UAV navigation with cellular signals exploiting loose network synchronization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 5, pp. 4261–4278, Oct. 2022, doi: 10.1109/TAES.2022.3162770.

[20] Z. Liu, L. Chen, X. Zhou, Z. Jiao, G. Guo, and R. Chen, "Machine learning for time-of-arrival estimation with 5G signals in indoor positioning," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 9782–9795, Jun. 2023, doi: 10.1109/JIOT.2023.3234123.

[21] C. Yang, M. Arizabaleta-Diez, P. Weitkemper, and T. Pany, "An experimental analysis of cyclic and reference signals of 4G LTE for TOA estimation and positioning in mobile fading environments," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 37, no. 9, pp. 16–41, 2022, doi: 10.1109/MAES.2022.3186650.

[22] Z. Kassas et al., "I can hear you loud and clear: GNSS-less high altitude aircraft navigation with terrestrial cellular signals of opportunity," *IEEE Trans. Aerosp. Electron. Syst.*, early access, Jul. 1, 2024, doi: 10.1109/TAES.2024.3418943.

[23] S. Parkvall et al., "5G NR release 16: Start of the 5G evolution," *IEEE Commun. Standards Mag.*, vol. 4, no. 4, pp. 56–63, 2020, doi: 10.1109/MCOMSTD.011.1900018.

[24] T. Humphreys, P. Iannucci, Z. Komodromos, and A. Graff, "Signal structure of the Starlink Ku-band downlink," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 5, pp. 6016–6030, Oct. 2023, doi: 10.1109/TAES.2023.3268610.

[25] M. Neinavaie, J. Khalife, and Z. Kassas, "Cognitive opportunistic navigation in private networks with 5G signals and beyond," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 1, pp. 129–143, Jan. 2022, doi: 10.1109/JSTSP.2021.3119929.

[26] M. Neinavaie, J. Khalife, and Z. Kassas, "Cognitive detection of unknown beacons of terrestrial signals of opportunity for localization," *IEEE Trans. Wireless Commun.*, vol. 22, no. 8, pp. 5613–5627, Aug. 2023, doi: 10.1109/TWC.2023.3235681.

[27] M. Neinavaie and Z. Kassas, "Cognitive sensing and navigation with unknown OFDM signals with application to terrestrial 5G and Starlink LEO satellites," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 1, pp. 146–160, Jan. 2024, doi: 10.1109/JSAC.2023.3322811.

[28] S. Shahcheraghi and Z. Kassas, "A computationally efficient approach for acquisition and Doppler tracking for PNT with LEO megaconstellations," *IEEE Signal Process. Lett.*, vol. 31, pp. 2400–2404, Apr. 2024, doi: 10.1109/LSP.2024.3431441.

[29] S. Kozhaya, H. Kanj, and Z. Kassas, "Multi-constellation blind beacon estimation, Doppler tracking, and opportunistic positioning with OneWeb, Starlink, Iridium NEXT, and Orbcomm LEO satellites," in *Proc. IEEE/ION Position Location Navigation Symp.*, Monterey, CA, USA, Apr. 2023, pp. 1184–1195.

[30] L. Scharf and B. Friedlander, "Matched subspace detectors," *IEEE Trans. Signal Process.*, vol. 42, no. 8, pp. 2146–2157, Aug. 1994, doi: 10.1109/78.301849.

[31] F. Gini and A. Farina, "Vector subspace detection in compound-Gaussian clutter. part I: Survey and new results," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 38, no. 4, pp. 1295–1311, Oct. 2002, doi: 10.1109/TAES.2002.1145751.

[32] D. Ciuonzo, A. De Maio, and D. Orlando, "On the statistical invariance for adaptive radar detection in partially homogeneous disturbance plus structured interference," *IEEE Trans. Signal Process.*, vol. 65, no. 5, pp. 1222–1234, Mar. 2017, doi: 10.1109/TSP.2016.2620115.

[33] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. press, 2005.

[34] S. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, vol. II. Upper Saddle River, NJ: Prentice-Hall, 1993.

[35] P. Markopoulos and G. Karystinos, "Noncoherent Alamouti phase-shift keying with full-rate encoding and polynomial-complexity maximum-likelihood decoding," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6688–6697, Oct. 2017, doi: 10.1109/TWC.2017.2728524.

[36] G. Gao, "Towards navigation based on 120 satellites: Analyzing the new signals," Ph.D. dissertation. Stanford Univ. Press, Stanford, CA, USA, 2008.

[37] S. Shahcheraghi, J. Saroufim, and Z. Kassas, "Acquisition, Doppler tracking, and differential LEO-aided IMU navigation with uncooperative satellites," *IEEE Aerosp. Electron. Syst. Mag.*, 2024. submitted for publication.

[38] S. Tenneti and P. Vaidyanathan, "Nested periodic matrices and dictionaries: New signal representations for period estimation," *IEEE Trans. Signal Process.*, vol. 63, no. 14, pp. 3736–3750, Jul. 2015, doi: 10.1109/TSP.2015.2434318.

[39] M. Neinavaie and Z. Kassas, "Unveiling Starlink LEO satellite OFDM-like signal structure enabling precise positioning," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 60, no. 2, pp. 2486–2489, Apr. 2024, doi: 10.1109/TAES.2023.3265951.

[40] J. Lopez-Salcedo, J. Peral-Rosado, and G. Seco-Granados, "Survey on robust carrier tracking techniques," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 670–688, Feb. 2014, doi: 10.1109/SURV.2013.082713.00228.

[41] G. Wang, X. Han, Y. Wang, and S. Dong, "Maintaining the status quo: Simultaneous estimation and elimination for multiple interference in transform domain vehicular communication," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 3058–3074, Mar. 2022, doi: 10.1109/TVT.2022.3144734.

[42] K. Shamaei and Z. Kassas, "LTE receiver design and multipath analysis for navigation in urban environments," *Navig. J. Inst. Navig.*, vol. 65, no. 4, pp. 655–675, Dec. 2018, doi: 10.1002/navi.272.

[43] J. Morales and Z. Kassas, "Optimal collaborative mapping of terrestrial transmitters: Receiver placement and performance characterization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 992–1007, Apr. 2018, doi: 10.1109/TAES.2017.2773238.

[44] M. Neinavaie, J. Khalife, and Z. Kassas, "Blind opportunistic navigation: Cognitive deciphering of partially known signals of opportunity," in *Proc. ION GNSS+ Conf.*, Sep. 2020, pp. 2748–2757.

[45] S. Hayek, J. Saroufim, and Z. Kassas, "Ephemeris error correction for tracking non-cooperative LEO satellites with pseudorange measurements," in *Proc. of IEEE Aerospace Conf.*, Big Sky, MT, USA, 2024, pp. 1–9.

[46] S. Hayek, J. Saroufim, and Z. Kassas, "Analysis and correction of LEO satellite propagation errors with application to navigation," in *Proc. of ION GNSS+ Conf.*, Sep. 2024.

[47] S. Kozhaya, J. Saroufim, and Z. Kassas, "Unveiling Starlink for PNT," *Navig. J. Inst. Navig.*, 2024. Submitted for publication.

[48] Z. Kassas, N. Khairallah, and S. Kozhaya, "Ad astra: Simultaneous tracking and navigation with megaconstellation LEO satellites," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 39, no. 9, pp. 46–71, Sep. 2024, doi: 10.1109/MAES.2023.3267440.

SP