Signal Mode Transition Detection in Starlink LEO Satellite Downlink Signals

Mohammad Neinavaie and Zaher M. Kassas
Department of Electrical and Computer Engineering
The Ohio State University, Columbus, OH, USA
neinavaie.1@osu.edu, zkassas@ieee.org

***Abstract*—A receiver architecture for detection and tracking of Starlink orthogonal frequency division multiplexing (OFDM)-based signals is proposed. The proposed receiver enables exploiting all the transmitted periodic beacons of Starlink low Earth orbit (LEO) signals to draw carrier phase, code phase, and Doppler observables. The reference signals (RSs) of modern OFDM-based systems contain both always-on and on-demand components. These components can be unknown and *subject to dynamic transmission modes*. Thanks to a matched subspace-based detection algorithm, the proposed receiver is shown to be capable of *cognitive detection* of both always-on and on-demand components in the Starlink OFDM-based RSs. It is shown that despite the dynamic nature of Starlink RSs, the proposed matched subspace detector senses the *transition between the transmission modes* of Starlink RSs, and detects all the accessible RSs with a predetermined probability of false alarm. Experimental results are provided to validate the performance of the proposed receiver in transmission mode detection in Starlink downlink signals.**

***Index Terms*—Positioning, navigation, signals of opportunity, low Earth orbit satellite, Starlink, OFDM, 5G, on-demand.**

I. Introduction

Abundant man-made terrestrial and extraterrestrial signals of opportunity (SOPs) have been shown to possess promising features for positioning, navigation, and timing [1]–[4]. *High bandwidth and diverse* synchronization signals of orthogonal frequency division multiplexing (OFDM) signals in cellular fourth-generation (4G) long-term evolution (LTE) and 5G new radio (NR) systems enabled meter-level and decimeter-level navigation on ground vehicles [5], [6] and unmanned aerial vehicles (UAVs) [7], [8], respectively. Similarly to 4G LTE and 5G NR, Starlink low Earth orbit (LEO) space vehicles (SVs) also adopt OFDM [9] signals with considerably high bandwidth [10]. While a single LTE channel has a bandwidth of up to 20 MHz, the bandwidth of a single 5G NR channel goes up to 100 MHz and 400 MHz for FR1 and FR2, respectively [11]. On the other hand, Starlink downlink signals occupy 250 MHz bandwidth of the Ku band to provide high rate broadband connectivity [12]. The OFDM reference signals (RSs) are spread across the whole bandwidth, which promises *good correlation properties*, leading to high ranging and localization accuracy.

This work was supported in part by the Office of Naval Research (ONR) under Grant N00014-22-1-2242, in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-22-1-0476, and in part by the U.S. Department of Transportation (USDOT) under Grant 69A3552047138 for the CARMEN University Transportation Center (UTC).

SOP-based 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 [13]. Due to the unknown and dynamic nature of modern communication signals in private networks, such as Starlink, a navigation receiver that is based on reverse engineering the downlink signals either (i) fails to exploit the whole available bandwidth unless *all* RSs get determined or (ii) fails to operate if the operator changes their signal. As such, designing receivers that can cognitively acquire *partially known*, *unknown*, or *dynamic* beacon signals is an emerging need for the future of cognitive opportunistic navigation [14]–[17].

Cognitive opportunistic navigation [17] has recently been introduced to address the following challenges of navigation with SOPs in modern and private networks. First, opportunistic navigation frameworks usually exploit the broadcast RSs for navigation [13]. In public networks, these signals are known by 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 may not be available to the public or are subject to change, which makes acquiring and tracking these signals impossible for conventional opportunistic navigation receivers [17]. Second, conventional cellular networks broadcast RSs at regular and known time intervals, regardless of the number of UEs in the environments (e.g., the cell-specific reference signal (CRS) in LTE). Modern communication systems, such as 5G NR, minimize the transmission of *always-on* signals, by adopting an *ultra-lean* design which entails transmitting some of the RSs only when necessary or *on-demand* [18].

Matched subspace detectors have been widely adopted to solve the detection problem of sources with unknown parameters in the presence of other interfering sources [19], [20]. In the signal processing literature, matched subspace detectors were used to detect the unknown signal activities in multiple-input multiple-output (MIMO) radars, passive bistatic radars, and blind array signal processing [21]–[23]. Recently, machine learning approaches have also been proposed for unknown transmitter detection, identification, and classification [24], [25]. In the navigation literature, the detection of unknown signals has been studied to design frameworks that are capable of navigating with unknown or partially known signals. The problem of detecting Galileo and Compass satellites signals

was studied in [26], which revealed the spread spectrum codes for these satellites. Preliminary experiments on navigation with partially known signals from low and medium Earth orbit satellites were conducted in [14]–[16], [27]. In particular, a chirp parameter estimator was used in [14] to blindly estimate the GPS pseudorandom noise (PRN) codes. In [16], a blind channel estimator was proposed to exploit Orbcomm satellite signals for navigation purposes. In [15], OFDM signals were emulated from Orbcomm LEO SVs, and a fast Fourier transform (FFT)-based Doppler estimator was proposed to exploit these signals for navigation purposes.

The first positioning results with always-on Starlink SV signals were presented in [28]–[30]. Following these studies, [9] was the first to exploit Starlink's OFDM signals for navigation. The contribution of this paper is (i) the detection of transmission mode change between on-demand and always-on and (ii) tracking the carrier phase when the on-demand signal is not beamed towards the receiver.

The rest of this paper is organized as follows. Section II presents the received baseband signal model. Section III summarizes the receiver architecture. Section IV presents experimental results. Section V gives concluding remarks.

II. Signal Model

The frame structure in OFDM-based transmission is either fixed or identified based on the physical requirements [31]. Each OFDM frame contains always-on and on-demand RSs which are transmitted for synchronization and channel estimation purposes. The period of the RSs is usually equal to the frame length of the OFDM signal. Acquisition and tracking OFDM RSs require knowledge of the frame length. While the frame length is known in public networks, such as 5G NR, it is usually unknown (and subject to change) in private networks, e.g., Starlink LEO broadband system. For private networks, the frame length should be estimated and updated cognitively. Estimation of the frame length of Starlink LEO downlink is discussed in [9].

A. Baseband Signal Model

The common feature of always-on and on-demand RSs is periodicity. If a subcarrier is being periodically transmitted, it will get detected, estimated, and used to derive carrier phase, code phase, and Doppler observables. The channel between the ith satellite and the UE is considered to have a single tap with a complex channel gain α_i. Denoting a continuous-time beacon at time t by $c(t)$, and the discrete-time beacon at time instant n by $c[n]$, the received baseband signal samples can be modeled as

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

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 satellite at time instant n; 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 satellite at the nth time instant, and τ_n is the sample time expressed in the receiver time. Moreover, N is the number of unknown satellite RSs; $c_i^{\mathrm{I}}[n]$ and $c_i^{\mathrm{II}}[n]$ represent the samples of the always-on waveform $c_i^{\mathrm{I}}(t)$ and on-demand waveform $c_i^{\mathrm{II}}(t)$ periodic RSs corresponding to the ith satellite with a period of L samples, respectively; $\theta_i[n] = 2\pi f_{D_i}[n] T_s n$ is the carrier phase in radians, where $f_{D_i}[n]$ is the Doppler frequency at the nth time instant and T_s is the sampling time; $d_i[n]$ represents the samples of some data transmitted from the ith satellite; and $w[n]$ is a zero-mean independent and identically distributed noise with $\mathbb{E}\left\{w[m]w^*[n]\right\} = \sigma_w^2 \delta[m-n]$, where $\delta[n]$ is the Kronecker delta function, and $w^*[n]$ denotes the complex conjugate of random variable $w[n]$. By defining $c_i[n] \triangleq c_i^{\mathrm{I}}[n] + c_i^{\mathrm{II}}[n]$, the received signals can be expressed in terms of the equivalent RS from the ith satellite, denoted by $s_i[n]$, and the equivalent noise, denoted by w_{eq_i}, which are defined as

$$s_i[n] \triangleq \alpha_i[n] c_i(\tau_n - t_{s_i}[n]) \exp\left(j\theta_i[n]\right), \quad (2)$$

$$w_{\mathrm{eq}_i}[n] = \alpha_i[n] d_i(\tau_n - t_{s_i}[n]) \exp\left(j\theta_i[n]\right) + w[n]. \quad (3)$$

Using (2) and (3), the baseband samples can be rewritten as

$$r[n] = \sum_{i=1}^{N} \left(s_i[n] + w_{\mathrm{eq}_i}[n] \right). \quad (4)$$

Remark 1: In this paper, the Doppler frequency is modeled as a linear chirp, i.e., $f_{D_i}[n] = f_{D_{i_0}} + \beta_i T_s n$, where $f_{D_{i_0}}[n]$ is the initial Doppler frequency and $\beta_i[n]$ is the Doppler rate.

Definition 1: The CPI is defined as the number of periods of an RS in a time interval during which the Doppler $f_{D_{i_0}}$, Doppler rate β_i, delay t_{s_i}, and channel gain α_i, are considered to be constant.

III. Receiver Architecture

This section summarizes the receiver architecture.

A. Acquisition

The received signal at the nth time instant when the Doppler rate is wiped-off is denoted by $r'[n] \triangleq \exp(-j2\pi\beta_i T_s^2 n^2) r[n]$. Due to the periodicity of $c(\tau_n)$, $s_i[n]$ has the following property

$$s_i[n + mL] = s_i[n] \exp\left(j\omega_i mL\right) \quad 0 \le n \le L-1, \quad (5)$$

where $\omega_i = 2\pi f_{D_{i_0}} T_s$ is the normalized Doppler, corresponding to the ith transmitting satellite, and $-\pi \le \omega_i \le \pi$. A vector of L observation samples corresponding to the mth period of the signal is formed as $\mathbf{z}_m \triangleq [r'[mL], r'[mL+1], \ldots, r'[(m+1)L-1]]^{\mathsf{T}}$. The CPI vector is constructed by concatenating K number of $\mathbf{z}_m$ vectors to form the $KL \times 1$ vector

$$\mathbf{y} = \sum_{i=1}^{N} \mathbf{H}_i \mathbf{s}_i + \mathbf{w}, \quad (6)$$

where $\mathbf{s}_i = [s_i[1], s_i[2], \ldots, s_i[L]]^{\mathsf{T}}$, and the $KL \times L$ Doppler matrix is defined as $\mathbf{H}_i \triangleq [\mathbf{I}_L, \exp\left(j\omega_i L\right)\mathbf{I}_L, \ldots, \exp\left(j\omega_i (M-1)L\right)\mathbf{I}_L]^{\mathsf{T}}$, where $\mathbf{I}_L$ is an $L \times L$ identity matrix, and $\mathbf{w}$ is the noise vector.

Similar to [9], the concept of *sequential matched subspace detection* is used to provide an initial estimate for the unknown parameters which are: (i) the number of unknown satellites, (ii) corresponding RSs, and (iii) the chirp parameters. A hypothesis testing problem is solved sequentially in multiple stages to detect the active satellites in the environment. Unlike [17], where a constant Doppler subspace was used to distinguish between different satellites, in this paper, the matched subspace is defined based on the chirp parameters of each satellite. At each stage, a test is performed to detect the most powerful satellite, while the *chirp subspace* of the previously detected satellite RSs are nulled. The so-called *general linear detectors* [32] is used at each stage of the sequential detection algorithm. In the first stage of the sequential algorithm, the presence of a single satellite is tested and if the null hypothesis is accepted, then $\hat{N} \equiv 0$, which means that no satellite is detected to be present in the environment under the test. If the test rejects the null hypothesis, the algorithm asserts the presence of at least one satellite and performs the test to detect the presence of other satellites in the presence of the previously detected satellite. The unknown chirp parameters and the RSs of each satellite are estimated at each stage. In general, if the null hypothesis at the ith level of the sequential algorithm is accepted, the algorithm is terminated and the estimated number of satellites will be $\hat{N} = i - 1$. It should be pointed out that while [17] only considered the Doppler space to distinguish between different unknown satellite RSs, in this paper, the Doppler rate space is also used to define the satellite subspace.

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

$$\begin{cases} \mathcal{H}_0^i: & i\text{th satellite is absent} \\ \mathcal{H}_1^i: & i\text{th satellite is present.} \end{cases} \tag{7}$$

Under $\mathcal{H}_1^i$, the signal model can be expressed as

$$\mathbf{y} = \mathbf{H}_i \mathbf{s}_i + \mathbf{B}_{i-1}\boldsymbol{\theta}_{i-1} + \mathbf{w}_{\mathrm{eq}_i}, \tag{8}$$

where, $\mathbf{B}_{i-1} \triangleq [\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_{i-1}]$ and $\boldsymbol{\theta}_{i-1} \triangleq [\mathbf{s}_1^{\mathsf{T}}, \mathbf{s}_2^{\mathsf{T}}, \ldots, \mathbf{s}_{i-1}^{\mathsf{T}}]^{\mathsf{T}}$ stores the chirp parameters and estimated RS in the previous steps. The decision criterion for the satellite detection is developed based on the Generalize Likelihood Ratio (GLR) (see [32, Section 9.4.3]). The likelihood of the GLR detector is derived as

$$\mathcal{L}_i(\mathbf{y}|\omega_i, \beta_i) = \frac{\mathbf{y}^{\mathsf{H}}\mathbf{P}_{\mathbf{S_i}}\mathbf{y}}{\mathbf{y}^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B_{i-1}}}\mathbf{P}^{\perp}_{\mathbf{S_i}}\mathbf{P}^{\perp}_{\mathbf{B_{i-1}}}\mathbf{y}}, \tag{9}$$

for a given normalized Doppler frequency, Doppler rate, and CPI, denoted by ω_i, and β_i. Vector $\mathbf{y}^{\mathsf{H}}$ is the Hermitian transpose of $\mathbf{y}$, $\mathbf{P}_{\mathbf{X}} \triangleq \mathbf{X}(\mathbf{X}^{\mathsf{H}}\mathbf{X})^{-1}\mathbf{X}^{\mathsf{H}}$, 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, $\mathbf{S}_i = \mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{H}_i$. It should be pointed out that $\mathbf{H}_i^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{H}_i = \lambda_i \mathbf{I}$, where the scalar λ_i is the Schur complement of block $\mathbf{C}_{i-1}$, i.e., the upper $(i-1)\times(i-1)$ block of the matrix $\mathbf{C}_i$, whose ijth element is [17]

$$c_{ij} \triangleq \sum_{k=0}^{K-1} \exp\left(j(\omega_j - \omega_i)Lk\right). \tag{10}$$

It can be seen from (10) that the elements of the matrix $\mathbf{C}_i$, and consequently the scalar λ_i, are scalar functions of the Doppler frequency difference between the ith satellite and the previously detected satellites.

The simplified likelihood can be written as [17]

$$\mathcal{L}_i^*(\mathbf{y}) = \arg\max_{\omega_i, \beta_i} \frac{\|\lambda_i^{-1}\hat{\mathbf{H}}_i^{\mathsf{H}}\hat{\mathbf{P}}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{y}\|^2}{\|\hat{\mathbf{P}}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{y}\|^2 - \|\lambda_i^{-1}\hat{\mathbf{H}}_i^{\mathsf{H}}\hat{\mathbf{P}}^{\perp}_{\hat{\mathbf{B}}_{i-1}}\mathbf{y}\|^2}. \tag{11}$$

The likelihood should be compared with a predetermined threshold η_i which is designed based on a particular probability of false alarm.

The ML estimates of the chirp parameters, i.e., $\hat{f}_{D_i}$, $\hat{\beta}_i$, can be obtained by maximizing $\mathcal{L}_i(\mathbf{y})$. Accordingly, the least squares (LS) estimate of the ith satellite $\mathbf{s}_i$, is given by

$$\hat{\mathbf{s}}_{\mathrm{acq}_i} = \lambda_i^{-1}\mathbf{H}_i^{\mathsf{H}}\mathbf{P}^{\perp}_{\mathbf{B}_{i-1}}\mathbf{y}. \tag{12}$$

B. Tracking

The initial estimate of the Doppler frequencies corresponding to each Starlink LEO SV and the associated likelihood functions are fed to the tracking stage along with the estimated RSs. By employing a phase-locked loop (PLL) and a delay-locked loop (DLL), the Doppler and delay are tracked over time. The tracking loops are based on the design discussed in [17], with compensation for compression and stretching due to high LEO dynamics.

IV. Experimental Results

This section presents experimental results with the receiver discussed in Section III showing successful detection of Starlink mode transition between on-demand and always-on. It also shows that while the DLL fails to track the code phase when the on-demand signal is turned off, the PLL continues to track the carrier phase of the always-on signal.

A. Starlink RS Transmission Modes and Correlation Properties

Starlink LEO SVs transmit nine pure tones located in a roughly, 1 MHz gap at the center of the transmission bandwidth of the Ku band. The pure tones were exploited for Doppler positioning in [28]–[30]. In this subsection, more details about the RSs of Starlink LEO SVs and their corresponding properties are assessed. In particular, it will be shown that two types of RSs with two different correlation properties are being transmitted.

In this experiment, a stationary National Instrument (NI) universal software radio peripheral (USRP) 2945R consumer-grade Ku antenna and low-noise block (LNB) downconverter to receive Starlink signals in the Ku-band in the parking structure of the University of California, Irvine. 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 origin points of time instants shown in the figures are considered to be the recording start time in each experiment. Six SVs were detected during the period of 800 s.

1) Always-on and On-demand RSs: The trajectories of the tracked satellites are plotted in Fig. 1. To avoid redundancy, this subsection analyzes the transmission modes and the correlation properties of the RSs corresponding to one of the six detected satellites in the experiment, namely SV 6 (Starlink-45694). The signals from other Starlink LEO SVs in this experiment follow the same pattern.

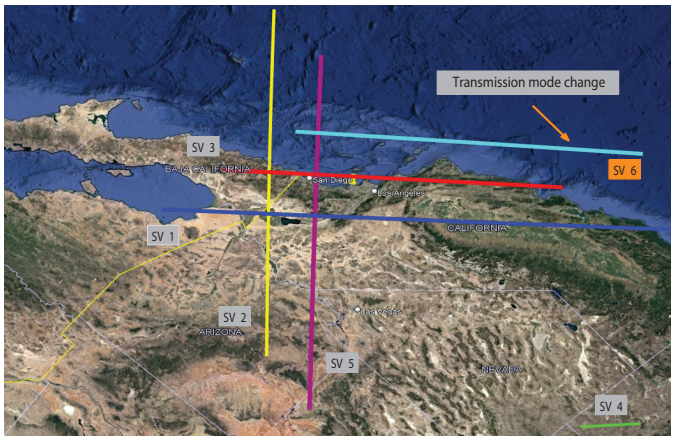

Fig. 1. Skyplot of the six satellites tracked in the experiment. The position on the trajectory of SV 6 in which the transmission mode occurred is indicated with an orange arrow.

Fig. 2 concentrates on the time epochs in which a transmission mode change has occurred. The autocorrelation and the likelihood functions at time epochs of $t = 606$ s and $t = 607$ s are plotted in Fig. 2. The RS structure and correlation properties change in the transition between these two time epochs for Starlink-45694. Fig. 2(a) and (b) demonstrate the autocorrelation function at $t = 606$ s and $t = 607$ s. The amplitude of the impulses follows the sinc-function behavior, which is due to the Doppler rate effect. These impulses are approximately 1.33 ms apart. However, at $t = 607$ s, the ambiguity function impulses disappeared. While the autocorrelation function is suggesting that the periodic RSs are not being transmitted at $t = 607$ s, the likelihood function shows a surprising behavior. At $t = 606$ s, the likelihood includes two different components which are shown in a black and a red box in Fig. 2(c).

Recall that when the likelihood passes the threshold, the existence of an RS with a period of approximately 1.33 ms is guaranteed by the detector with a certain probability of detection. The likelihood at $t = 607$ s shows that the component in the black box is not being transmitted anymore, while the component in the red box is *still on*. The signal in the red box is periodic with a period of 1.33 ms, which is associated with the OFDM RSs. However, as it can be seen in Fig. 2(b), the signal in the red box does not have good *time correlation* properties. The signal in the red box is continuously transmitted when the boradband OFDM signal is active and is referred to as always-on RS in this paper. The behavior of the signal in the black box is similar to 5G NR on-demand RSs which are not always active and, therefore, are referred to as on-demand RSs in this paper.

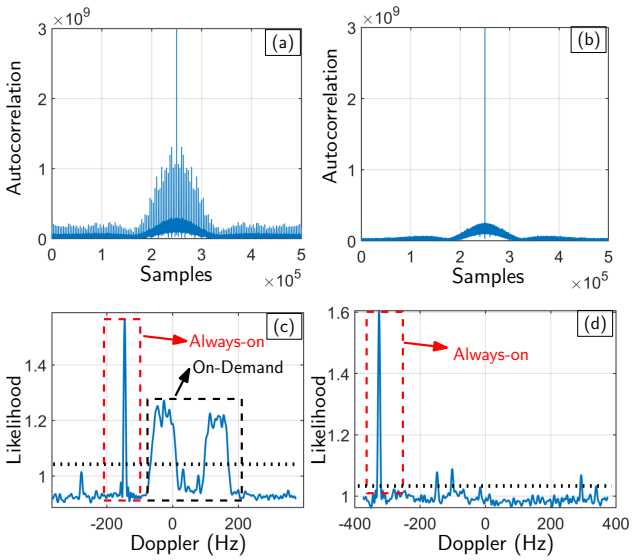

Fig. 2. (a) and (b) demonstrate the autocorrelation at $t = 606$ s and $t = 607$ s, respectively. It can be seen that at $t = 606$ s, the RS is showing a time autocorrelation and at $t = 607$ s the time autocorrelation is lost. (c) and (d) demonstrate the likelihood function at $t = 606$ s and $t = 607$ s, respectively. Two components can be seen in the likelihood functions (the red box and the black box) at $t = 606$ s. The component in the black box is not being transmitted at $t = 607$ s.

Fig. 3 shows the code phase and carrier phase tracking results for Starlink-45694 during this time interval. The tracking results give a better understanding of the correlation properties of the two detected RSs in the feedback tracking loops. The bandwidth of the PLL was set to 65 Hz and the bandwidth of the DLL was set to be 0.02 Hz.

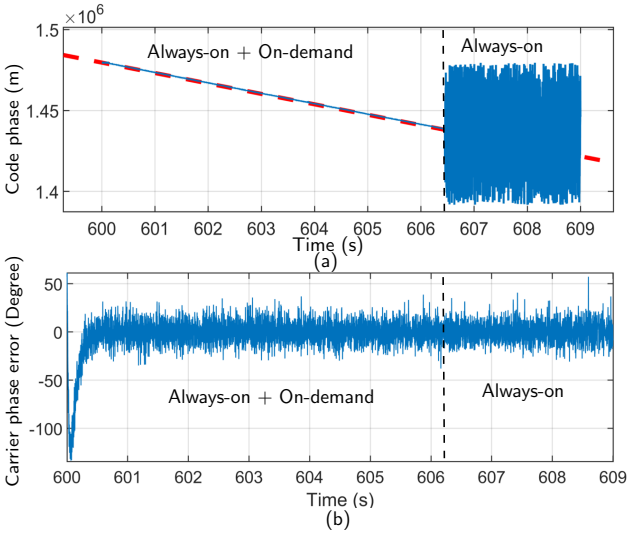

Fig. 3. (a) Code phase tracking, and (b) carrier phase tracking of Starlink-45694. As it was expected, at a time epoch between $t = 606$ s and $t = 607$ s the code phase tracking is lost. This is due to the fact that the on-demand signal which has suitable time autocorrelation properties is not active anymore at this time epoch. However, Fig. 3(b) shows that the carrier phase tracking loop is still locked.

As expected, at a time epoch between $t = 606$ s and $t = 607$ s, code phase tracking is lost. This is due to the fact that the on-demand signal, which has suitable time autocorrelation properties, is not active anymore at this time

epoch. However, Fig. 3(b) shows that the carrier phase tracking loop is still locked. This is due to the fact that the always-on signal (the signal in the red box in Fig. 2(c)) is showing good frequency correlation properties. The frequency-domain correlation property of the always-on signal guarantees carrier phase tracking even if the on-demand signal is not active.

Remark 2: Starlink RSs may dynamically change during one satellite pass. A method that only relies on a static design based on an RS with good time correlation properties may not provide continuous navigation observables. The proposed method cognitively detects all available RSs and yields continuous carrier and code phase tracking (when applicable).

V. Conclusion

Signal mode transition between on-demand and always-on in Starlink satellite downlink signals was studied. Via a matched subspace-based detection algorithm, all the transmitted periodic beacons of Starlink LEO signals were detected to draw navigation observables. It was shown that similar to the RSs of modern OFDM-based systems, the RSs of Starlink downlink signals contain both always-on and on-demand components. The proposed method was able to detect the transmission mode change in Starlink downlink signals and maintain carrier phase tracking when the on-demand component was not beamed towards the receiver.

References

[1] 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, doi: 10.1002/9781119458555.ch35.

[2] N. Jardak and Q. Jault, "The potential of LEO satellite-based opportunistic navigation for high dynamic applications," *Sensors*, vol. 22, no. 7, pp. 2541–2565, 2022.

[3] M. Hartnett, "Performance assessment of navigation using carrier Doppler measurements from multiple LEO constellations," Master's thesis, Air Force Institute of Technology, Ohio, USA, 2022.

[4] F. Prol, R. Ferre, Z. Saleem, P. Välisuo, C. Pinell, E. Lohan, M. Elsanhoury, M. Elmusrati, S. Islam, K. Celikbilek, K. Selvan, J. Yliaho, K. Rutledge, A. Ojala, L. Ferranti, J. Praks, M. Bhuiyan, S. Kaasalainen, and H. Kuusniemi, "Position, navigation, and timing (PNT) through low earth orbit (LEO) satellites: A survey on current status, challenges, and opportunities," *IEEE Access*, vol. 10, pp. 83 971–84 002, 2022.

[5] J. Peral-Rosado, J. Lopez-Salcedo, S. Kim, and G. Seco-Granados, "Feasibility study of 5G-based localization for assisted driving," in *Proceedings of International Conference on Localization and GNSS*, June 2016, pp. 1–6.

[6] 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 Aerospace and Electronic Systems Magazine*, vol. 37, no. 9, pp. 16–41, 2022.

[7] J. Del Peral-Rosado, P. Nolle, S. Razavi, G. Lindmark, D. Shrestha, F. Gunnarsson, F. Kaltenberger, N. Sirola, O. Särkkä, J. Roström, K. Vaarala, P. Miettinen, G. Pojani, L. Canzian, H. Babaroglu, E. Rastorgueva-Foi, J. Talvitie, and D. Flachs, "Design considerations of dedicated and aerial 5G networks for enhanced positioning services," in *Proceedings of Workshop on Satellite Navigation Technology*, April 2022, pp. 1–12.

[8] 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.

[9] M. Neinavaie and Z. Kassas, "Unveiling Starlink LEO satellite OFDM-like signal structure enabling precise positioning," *IEEE Transactions on Aerospace and Electronic Systems*, 2023, accepted.

[10] S. Liu, Z. Gao, Y. Wu, D. Kwan Ng, X. Gao, K. Wong, S. Chatzinotas, and B. Ottersten, "LEO satellite constellations for 5G and beyond: How will they reshape vertical domains?" *IEEE Communications Magazine*, vol. 59, no. 7, pp. 30–36, July 2021.

[11] J. del Peral-Rosado, R. Raulefs, J. López-Salcedo, and G. Seco-Granados, "Survey of cellular mobile radio localization methods: From 1G to 5G," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 1124–1148, 2018.

[12] I. Del Portillo, B. Cameron, and E. Crawley, "A technical comparison of three low earth orbit satellite constellation systems to provide global broadband," *Acta Astronautica*, vol. 159, pp. 123–135, 2019.

[13] 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.

[14] 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.

[15] 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. 1–5.

[16] 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*, 2021, pp. 1–8.

[17] 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.

[18] 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.

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

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

[21] M. Korso, R. Boyer, A. Renaux, and S. Marcos, "Statistical resolution limit for source localization with clutter interference in a MIMO radar context," *IEEE Transactions on Signal Processing*, vol. 60, no. 2, pp. 987–992, 2012.

[22] A. Zaimbashi, M. Derakhtian, and A. Sheikhi, "GLRT-based CFAR detection in passive bistatic radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 1, pp. 134–159, 2013.

[23] 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.

[24] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, and E. Pasiliao, "RFAL: adversarial learning for RF transmitter identification and classification," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 783–801, 2019.

[25] M. Baek, S. Kwak, J. Jung, H. Kim, and D. Choi, "Implementation methodologies of deep learning-based signal detection for conventional MIMO transmitters," *IEEE Transactions on Broadcasting*, vol. 65, no. 3, pp. 636–642, 2019.

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

[27] 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.

[28] 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.

[29] 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.

[30] M. Neinavaie, Z. Shadram, S. Kozhaya, and Z. M. Kassas, "First results of differential Doppler positioning with unknown Starlink satellite signals," in *Proceedings of IEEE Aerospace Conference*, March 2022, pp. 1–14.

[31] 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.

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