This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

Signal Structure of the Starlink Ku-Band Downlink

Todd E. Humphreys, Member, IEEE
The University of Texas at Austin, Austin, TX, USA

Peter A. Iannucci, Member, IEEE
The University of Texas at Austin, Austin, TX, USA

Zacharias M. Komodromos, Student Member, IEEE
The University of Texas at Austin, Austin, TX, USA

Andrew M. Graff, Student Member, IEEE
The University of Texas at Austin, Austin, TX, USA

***Abstract*— We develop a technique for blind signal identification of the Starlink downlink signal in the 10.7 to 12.7 GHz band and present a detailed picture of the signal's structure. Importantly, the signal characterization offered herein includes the exact values of synchronization sequences embedded in the signal that can be exploited to produce pseudorange measurements. Such an understanding of the signal is essential to emerging efforts that seek to dual-purpose Starlink signals for positioning, navigation, and timing, despite their being designed solely for broadband Internet provision.**

***Index Terms*— low Earth orbit, positioning, signal identification, Starlink, time synchronization**

Manuscript received XXXXX 00, 0000; revised XXXXX 00, 0000; accepted XXXXX 00, 0000.
Research was sponsored by the Army Research Office under Cooperative Agreement W911NF-19-2-0333. Additional support was provided by the U.S. Department of Transportation (USDOT) under the University Transportation Center (UTC) Program Grant 69A3552047138 (CARMEN), and by affiliates of the 6G@UT center within the Wireless Networking and Communications Group at The University of Texas at Austin. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein. *(Corresponding author: T. Humphreys)*

Todd E. Humphreys is with the Department of Aerospace Engineering and Engineering Mechanics at The University of Texas at Austin, Austin, TX 78712 (e-mail: todd.humphreys@utexas.edu). Peter A. Iannucci is with the Department of Aerospace Engineering and Engineering Mechanics at The University of Texas at Austin, Austin, TX 78712 (e-mail: iannucci@mit.edu). Zacharias M. Komodromos is with the Department of Electrical and Computer Engineering at The University of Texas at Austin, Austin, TX 78712 (e-mail: zackkomo@utmail.utexas.edu). Andrew M. Graff is with the Department of Electrical and Computer Engineering at The University of Texas at Austin, Austin, TX 78712 (e-mail: andrewgraff@utexas.edu).

0018-9251 © 2023 IEEE

I. Introduction

In addition to revolutionizing global communications, recently-launched broadband low-Earth-orbit (LEO) mega-constellations are poised to revolutionize global positioning, navigation, and timing (PNT). Compared to traditional global navigation satellite systems (GNSS), they offer higher power, wider bandwidth, more rapid multipath decorrelation, and the possibility of stronger authentication and zero-age-of-ephemeris, all of which will enable greater accuracy and greater resilience against jamming and spoofing [1]–[5].

With over 3000 satellites already in orbit, SpaceX's Starlink constellation enjoys the most mature deployment among LEO broadband providers. Recent demonstrations of opportunistic Doppler-based positioning with Starlink signals [6]–[8] open up exciting possibilities. But whether Starlink signals are more generally suitable for opportunistic PNT—not only via Doppler positioning—and whether they could be the basis of a full-fledged GNSS, as proposed in [5], remains an open question whose answer depends on details of the broadcast signals, including modulation, timing, and spectral characteristics. Yet whereas the orbits, frequencies, polarization, and beam patterns of Starlink satellites are a matter of public record through the licensing databases of the U.S. Federal Communications Commission [9], details on the signal waveform itself and the timing capabilities of the hardware producing it are not publicly available.

We offer two contributions to address this knowledge gap. First, we develop a technique for blind signal identification of the Starlink downlink signal in the 10.7 to 12.7 GHz band. The technique is a significant expansion of existing blind orthogonal frequency division multiplexing (OFDM) signal identification methods (see [10]–[12] and the references therein), which have only been successfully applied to simulated signals. Insofar as we are aware, blind identification of operational OFDM signals, including exact determination of synchronization sequences, has not been achieved previously. The technique applies not only to the Starlink Ku-band downlink but generally to all OFDM signals except as regards some steps required to estimate synchronization structures that are likely unique to Starlink.

Second, we present a detailed characterization of the Starlink downlink signal structure in the 10.7 to 12.7 GHz band. This applies for the currently-transmitting Starlink satellites (versions 0.9, 1.0, and 1.5), but will likely also apply for version 2.0 and possibly later generations, given the need to preserve backward compatibility for the existing user base. Our signal characterization includes the exact values of synchronization sequences embedded in the signal that can be exploited to produce pseudorange measurements. Combining multiple pseudorange measurements to achieve multi-laterated PNT, as is standard in traditional GNSS, enables faster and more accurate opportunistic position fixes than the Doppler-based positioning explored in [6]–[8], [13]. and can additionally

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

offer nanosecond-accurate timing, whereas even under the optimistic scenario envisioned in [13], extracting timing from Doppler-based processing of LEO signals yields errors on the order of 0.1 to 1 ms.

II. Signal Capture

To facilitate replication of our work, and as a prelude to our presentation of the signal model, we begin with a detailed description of our signal capture system.

One might reasonably wonder whether a standard consumer Starlink user terminal (UT) could be modified to capture wideband (hundreds of MHz) raw signal samples for Starlink signal identification. Not easily: operating the UT as development hardware, which would permit capture of raw signal samples, requires defeating security controls designed specifically to prevent this. Moreover, the clock driving the UT's downmixing and sampling operations is of unknown quality and would therefore taint any timing analysis of received signals.

We opted instead to develop our own system for Starlink signal capture. Composed of off-the-shelf hardware and custom software, the system enables signal capture from one Starlink satellite at a time with downmixing and sampling referenced to a highly-stable GPS-disciplined oscillator.

Whereas the consumer Starlink UT operates as a phased array of many separate antenna elements, our antenna is a steerable 90-cm offset parabolic dish with a beamwidth of approximately 3 degrees. Starlink orbital ephemerides provided publicly by SpaceX guide our selection and tracking of overhead satellites. Only one or two Starlink satellites illuminate a coverage cell at any one time with a data-bearing beam [5]. To guarantee downlink activity, we solicit data by downloading a high-definition video stream through a standard Starlink UT co-located with our signal capture system.

Fig. 1 outlines our signal capture hardware and signal pathways. A parabolic dish focuses signals onto a feedhorn connected to a low-noise block (LNB) with a conversion gain of 60 dB and a noise figure of 0.8 dB. The LNB is dual-band, downconverting either 10.7–11.7 GHz (the lower band) to 950–1950 MHz, or 11.7–12.75 GHz (the upper band) to 1100–2150 MHz. The antenna's nominal gain is 40 dBi at 12.5 GHz, but there are losses of at least 4-5 dB due to lack of a circular-to-linear polarizer and to feedhorn misalignment.

The signal capture system allows selection between narrowband ($\sim$ 60 MHz) and wideband ($\sim$ 1 GHz) signal capture modes. For the narrowband mode, the output of the LNB is fed to a transfer switch that diverts the signal through a tunable bandpass filter for image rejection. Downstream hardware then performs downmixing (consistent with the selected band), additional bandpass filtering, and 16-bit complex sampling at 62.5 Msps. The downmixing operation in the LNB and the downmixing and sampling operations in the downstream hardware are phase-locked to a common GPS-disciplined oven-controlled crystal oscillator (OCXO) to minimize the effects of receiver clock variations on the received signals. A 3-TB data storage array permits archival of several hours of continuous data.

Anti-alias filtering prior to sampling reduces the usable bandwidth of the narrowband mode to approximately 60 MHz. Although this is much narrower than a single Starlink channel, multiple overlapping captures can be combined for a comprehensive analysis of all embedded narrowband structures, as will be shown. However, the narrowband mode cannot support a synoptic signal analysis. A second capture mode—the wideband mode—addresses this deficiency. Based on direct digital downconversion of 12-bit samples at 4096 Msps (real), the wideband mode is capable of alias-free capture of the LNB's entire lower band and most of its upper band. The wideband mode's limitations are storage, timing, and noise figure: our current hardware permits only 1-second segments of contiguous data to be captured before exhausting the onboard memory, the sampling is not driven by the same clock used for LNB downmixing (due to hardware limitations), and the noise figure results in captured signals with a signal-to-noise ratio (SNR) that is significantly worse than for the narrowband mode.

For the analysis described subsequently, signal identification was based on narrowband-mode-captured data except for estimation of the primary synchronization sequence.

III. Signal Model

Given its widespread use in wireless communications, one might expect OFDM [14]–[18] to be the basis of the Ku-band Starlink downlink. However, OFDM has historically been avoided in satellite communications systems because its high peak-to-average-power ratio leads to inefficient transmit power conversion [19]. Nonetheless, inspection of the Starlink power spectrum generated from captured data reveals spectrally-flat frequency blocks with sharp edges, hallmarks consistent with an OFDM hypothesis. Proceeding under the assumption of an OFDM model, the problem of general signal identification narrows to one of identifying the values of parameters fundamental to OFDM signaling. This section introduces such parameters as it presents a generic OFDM signal model and a received signal model.

A. Generic OFDM Signal Model

The serial data sequence carrying an OFDM signal's information is composed of complex-valued symbols drawn from the set $\{X_{mik} \in \mathbb{C} : m, i, k \in \mathbb{N},\ k < N,\ i < N_{\text{sf}}\}$ at a rate F_{s}, known as the channel bandwidth. The subscript k is the symbol's index within a length-N subsequence known as an OFDM symbol, i is the OFDM symbol's index within a length-N_{sf} sequence of OFDM symbols known as a frame, and m is the frame index. Each symbol X_{mik} encodes one or more

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

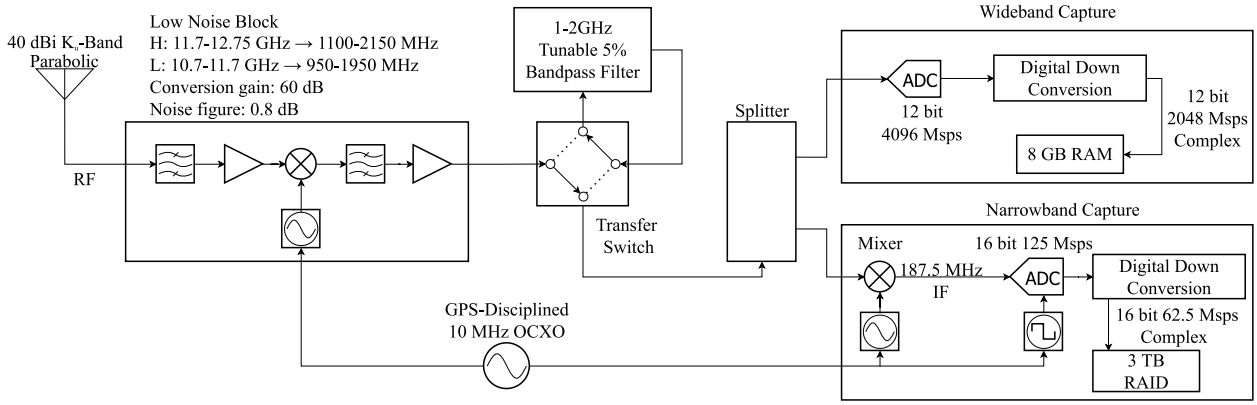

Fig. 1: Block diagram of the Starlink signal capture process.

bits of information depending on the modulation scheme (e.g., 1 for BPSK, 2 for 4QAM, 4 for 16QAM, etc.), with higher-order modulation demanding higher SNR to maintain reception at a given acceptably-low bit-error rate (BER) [18]. OFDM is a highly spectrally efficient case of multicarrier signaling in which each X_{mik} modulates one of N mutually orthogonal subcarriers with overlapping spectra. Let $T = N/F_\mathrm{s}$ be the interval over which N information symbols arrive, and $F = F_\mathrm{s}/N = 1/T$ be the subcarrier spacing, chosen as indicated to ensure subcarrier orthogonality over the interval T. Then the baseband time domain signal produced by the ith OFDM symbol of the mth frame is expressed as

$$x'_{mi}(t) = \sum_{k=0}^{N-1} X_{mik} \exp\left(j2\pi F t k\right), \quad 0 \le t < T \tag{1}$$

One recognizes this expression as a scaled inverse discrete Fourier transform, commonly implemented as an IFFT. Thus, one can think of each X_{mik} as a complex-valued frequency-domain coefficient. To prevent inter-symbol interference (ISI) arising from channel multipath, OFDM prepends a cyclically-extended guard interval of length $T_\mathrm{g} = N_\mathrm{g}/F_\mathrm{s}$, called the cyclic prefix, to each OFDM symbol. Due to the time-cyclic nature of the IFFT, the prepending operation can be modeled by a simple modification of (1):

$$x_{mi}(t) = \sum_{k=0}^{N-1} X_{mik} \exp\left(j2\pi F(t - T_\mathrm{g}) k\right), \quad 0 \le t < T_\mathrm{sym}$$

With the addition of the cyclic prefix, the OFDM symbol interval becomes $T_\mathrm{sym} = T + T_\mathrm{g}$, with T being the useful (non-cyclic) symbol interval. The function $x_{mi}(t)$ is called a time-domain OFDM symbol, or simply an OFDM symbol when there is little risk of confusion with its frequency-domain representation.

In all wireless OFDM protocols, subsequences of OFDM symbols are packaged into groups variously called slots, frames, or blocks. We will use the term frame to describe the smallest grouping of OFDM symbols that is self-contained in the sense that it includes one or more symbols with predictable elements to enable receiver time and frequency synchronization. Let N_sf be the number of OFDM symbols in a frame, $T_\mathrm{f} \ge N_\mathrm{sf} T_\mathrm{sym}$ be the frame period, and

$$g_\mathrm{s}(t) = \begin{cases} 1, & 0 \le t < T_\mathrm{sym} \\ 0, & \text{otherwise} \end{cases}$$

be the OFDM symbol support function. Then the time-domain signal over a single frame can be written

$$x_m(t) = \sum_{i=0}^{N_\mathrm{sf}-1} x_{mi}(t - iT_\mathrm{sym}) g_\mathrm{s}(t - iT_\mathrm{sym}) \tag{2}$$

Over an infinite sequence of frames, this becomes

$$x(t) = \sum_{m \in \mathbb{N}} x_m(t - mT_\mathrm{f}) \tag{3}$$

B. Received Signal Model

As $x(t)$ passes through the LEO-to-Earth channel and later through the receiver signal conditioning and discretization operations, it is subject to multipath-induced fading, noise, Doppler, delay, filtering, and digitization.

In our signal capture setup, the receiving antenna is highly directional, positioned atop a building with a clear view of the sky, and only used to track satellites with elevation angles above 50 degrees. Accordingly, the received signal's delay spread is negligible—similar to the wooded case of [20]. In this regime, the coherence bandwidth appears to be limited primarily by atmospheric dispersion in the Ku-band, which, as reported in [21], amounts to sub-millimeter delay sensitivity to dry air pressure, water vapor, and surface air temperature for a 200 MHz-wide signal. In view of these favorable characteristics, we adopt a simple additive Gaussian white noise model for the LEO-to-Earth channel.

Doppler effects arising from relative motion between the satellite and ground receiver are considerable in the Ku band for the LEO-to-Earth channel. In fact, they are so significant that, for a channel of appreciable bandwidth, Doppler cannot be modeled merely as imposing a frequency shift in the received signal, as in [10], [11], or simply neglected, as in [12]. Instead, a more comprehensive Doppler model is required, consisting of

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

both a frequency shift and compression/dilation of the baseband signal.

Let v_{los} be the magnitude of the line-of-sight velocity between the satellite and receiver, modeled as constant over an interval T_{f}, and let $\beta \triangleq v_{\text{los}}/c$, where c is the free-space speed of light. Note that lack of frequency synchronization between the transmitter and receiver clocks gives rise to an effect identical to motion-induced Doppler. In what follows, we treat β as parameterizing the additive effects of motion- and clock-error-induced Doppler, and we refer to β as the carrier frequency offset (CFO) parameter.

For an OFDM channel bandwidth F_{s}, the compression/dilation effects of Doppler are negligible only if $\beta F_{\text{s}} T_{\text{sync}} \ll 1$, where T_{sync} is an interval over which OFDM symbol time synchronization is expected to be maintained to within a small fraction of $1/F_{\text{s}}$. Violation of this condition causes ISI in OFDM receiver processing as the receiver's discrete Fourier transform operation, implemented as an FFT, becomes misaligned with time-domain OFDM symbol boundaries. In the context of standard OFDM signal reception, T_{sync} may be as short as T_{sym}, whereas for the signal identification process described in the sequel, $T_{\text{sync}} > N_{\text{sf}} T_{\text{sym}}$.

Consider a transmitter in LEO at 300 km altitude, a stationary terrestrial receiver, elevation angles above 50 degrees, and relative (transmitter-vs-receiver) clock quality consistent with a temperature-compensated crystal oscillator. The resulting β is limited to $|\beta| < 2.5 \times 10^{-5}$. Suppose $T_{\text{sync}} = 1$ ms. Then, to ensure $\beta F_{\text{s}} T_{\text{sync}} < 0.1$, F_{s} would be limited to 4 MHz, well below the Starlink channel bandwidth. Therefore our Doppler model must include both a frequency shift and compression/dilation of the baseband signal.

With these preliminaries, we may introduce the baseband analog received signal model as

$$y_a(t) = x((t-\tau_0)(1-\beta)) \times \exp\left(j2\pi\left[F_{\text{c}}(1-\beta) - \bar{F}_{\text{c}}\right](t-\tau_0)\right) + w(t) \tag{4}$$

where F_{c} is the center frequency of the OFDM channel, $\bar{F}_{\text{c}} \approx F_{\text{c}}$ is the center frequency to which the receiver is tuned, τ_0 is the delay experienced by the signal along the least-time path from transmitter to receiver, and $w(t)$ is complex-valued zero-mean white Gaussian noise whose in-phase and quadrature components each have (two-sided) spectral density $N_0/2$. Let the symbols $\{X_{mik}\}$ be scaled such that $x(t)$ has unit average power over nonzero OFDM symbols. Then, during such symbols and within the channel bandwidth F_{s}, $\text{SNR} = 1/N_0 F_{\text{s}}$.

In a late stage of the signal capture pipeline shown in Fig. 1, the analog signal $y_a(t)$ is discretized. Let F_{r} be the receiver's sampling rate and $h(t)$ be the impulse response of a lowpass prefilter with (two-sided) 3-dB bandwidth $F_h < F_{\text{r}}$ and rolloff such that power is negligible for frequencies $|f| > F_{\text{r}}/2$, permitting alias-free complex sampling. Then the baseband digitized received signal model is

$$y(n) = \int_{-\infty}^{\infty} h(n/F_{\text{r}} - \tau) y_a(\tau)\, d\tau, \quad n \in \mathbb{Z} \tag{5}$$

Note that, strictly speaking, (4) and (5) apply only to the narrowband capture mode. Accounting for the distinct mixing and sampling clocks in the wideband mode would require a more elaborate model.

IV. Signal Identification Preliminaries

Here we summarize and augment the terminology and notation previously introduced to allow a clear statement of the identification problem to be solved. Then, to develop intuition about the solution procedure presented in the following section, we explain how signal cyclostationarity is exploited to estimate key signal parameters.

A. Terminology and Parameters of Interest

We assume the frequency spectrum allocated for a multi-band OFDM signal is divided into OFDM *channels* within which power spectral density is approximately uniform. Adjacent channels are separated by *guard bands*. Each channel is composed of N orthogonal *subcarriers* whose spectra overlap. A *frequency-domain OFDM symbol* is a vector of N complex-valued coefficients whose kth element modulates the kth subcarrier.

The IFFT of a frequency-domain OFDM symbol, when prepended by a *guard interval* (cyclic prefix), becomes a *time-domain OFDM symbol*. Subsequences of such symbols are packaged into *frames* in which one or more OFDM symbols carry predictable elements, called *synchronization sequences*, that enable receiver time and frequency synchronization. As transmitted, an OFDM signal's carrier phase remains stable within each frame. Frames are separated from each other by at least the *frame guard interval*. There may be further logical subframe structure (e.g., slots, header segments), but these are not addressed in this paper's signal identification process.

Note that three distinct structures share the term "guard": the empty spectrum between channels (*guard band*), the time between frames (*frame guard interval*), and the (cyclic) prefix in a time-domain OFDM symbol (*OFDM symbol guard interval*).

The OFDM parameters of interest for this paper's signal identification problem are summarized in Table I.

B. Problem Statement

This paper's blind signal identification problem can be stated as follows: Given one or more frame-length segments of received data modeled by (5), estimate the value of the independent parameters listed in Table I with sufficient accuracy to enable determination of the symbols $\{X_{mik}\}$ that apply within the captured time interval over the bandwidth F_h. Also identify and evaluate any synchronization sequences present within a frame.

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

TABLE I: Parameters of Interest

Independent Parameters	
F_s	Channel bandwidth; information symbol rate
N	Number of subcarriers in bandwidth F_s
N_g	Num. of intervals $1/F_\mathrm{s}$ in an OFDM symbol guard interval
T_f	Frame period
T_fg	Frame guard interval
N_sf	Number of non-zero symbols in a frame
N_sfd	Number of data symbols in a frame
F_{ci}	Center frequency of ith channel
Derived Parameters	
$T = N/F_\mathrm{s}$	Useful (non-cyclic) OFDM symbol interval
$T_\mathrm{g} = N_\mathrm{g}/F_\mathrm{s}$	Symbol guard interval
$T_\mathrm{sym} = T+T_\mathrm{g}$	OFDM symbol duration incl. guard interval
$F = F_\mathrm{s}/N$	Subcarrier spacing
$F_\delta = F_{ci}-F_{c(i-1)}$	Channel spacing
$F_\mathrm{g} = F_\delta-F_\mathrm{s}$	Width of guard band between channels

Note that this signal identification problem is more demanding than those treated in the existing blind OFDM signal identification literature, in five ways. First, no prior identification procedures were truly blind: they operated on simulated signals generated by the researchers themselves. As will be shown, simulated signals, which assume independent and identically-distributed (iid) information symbols $\{X_{mik}\}$, bear characteristics markedly different from operational OFDM signals. Second, prior studies either neglected Doppler effects or modeled only a bulk frequency shift arising from Doppler. Third, the goal of prior work has been limited to distinguishing known OFDM waveforms from each other [10], [12], or from single-carrier systems [11]. As such, they do not estimate the comprehensive set of independent parameters required to recover the symbols $\{X_{mik}\}$. For example, [10] estimates the useful symbol interval T and the symbol guard interval T_g, but not F_s, N, and N_g independently. Fourth, existing approaches assume the receiver bandwidth F_h is wider than F_s, which is not the case for our narrowband capture mode. Fifth, prior studies have not been concerned with identifying and characterizing any synchronization sequences in OFDM frames. Yet such sequences are key to standard OFDM signal processing and are especially important for efforts to dual-purpose OFDM signals for PNT.

C. Exploiting Signal Cyclostationarity

A fundamental concept exploited in feature-based signal identification is signal cyclostationarity [10], [22]. While all communications signals exhibit cyclostationarity, it is especially pronounced in OFDM signals due to the cyclic prefix present in each OFDM symbol.

To simplify explanations in this subsection, assume that $\beta = 0$, that the receiver sampling rate F_r is identical to the OFDM channel bandwidth F_s, and that the receiver filter bandwidth $F_h \approx F_\mathrm{s}$. Then, letting $\mathbb{E}[\cdot]$ denote the expectation operation, define the autocorrelation function

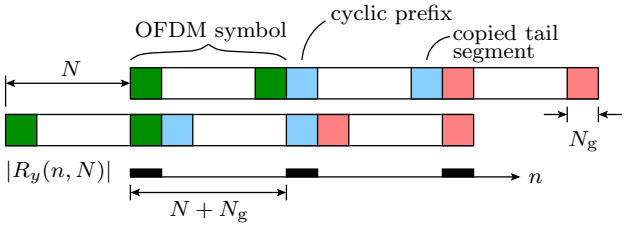

Fig. 2: Graphical explanation for why $R_y(n,N)$ is cyclic in n with period $N+N_\mathrm{g}$.

of the received discrete-time signal $y(n)$ as

$$R_y(n,\tau) = \mathbb{E}\left[y(n+\tau)y^*(n)\right] \tag{6}$$

where $y^*(n)$ is the complex conjugate of $y(n)$. If the coefficients $\{X_{mik}\}$ are iid and selected randomly from among the possible constellation values, then $R_y(n,\tau)$ may be nonzero only at $\tau \in \{0, N, -N\}$ [10]. As illustrated in Fig. 2, nonzero autocorrelation at $\tau \in \{N, -N\}$ arises because $y(n)$ is shifted against itself in such a way that cyclic prefixes are aligned perfectly with the portions of the symbols of which they are a copy. Fig. 2 also makes clear that $R_y(n,N)$ is cyclic in n with period $N+N_\mathrm{g}$. Moreover, within a sequence of nonzero OFDM symbols, $\mathbb{E}[y(n)] = \mathbb{E}\left[y(n+N+N_\mathrm{g})\right]$. These attributes imply that $y(n)$ is wide-sense cyclostationary [18]. The autocorrelation function $R_y(n,\tau)$ is the key to determining N and N_g without the need for prior time and frequency determination. Since $R_y(n,\tau)$ is periodic in n with period $N+N_\mathrm{g}$ for certain values of τ, it can be expanded in a Fourier series as

$$R_y(n,\tau) = \sum_{\alpha\in\mathcal{A}(\xi)} R_y^\alpha(\tau)\exp\left(j2\pi n\alpha\right) \tag{7}$$

where $\mathcal{A}(\xi) = \{p/\xi : p \in \mathbb{Z}\}$. The particular set $\mathcal{A}(N+N_\mathrm{g})$ contains the so-called cyclic frequencies. The Fourier coefficient $R_y^\alpha(\tau)$, also called the cyclic autocorrelation function, equals

$$R_y^\alpha(\tau) = \lim_{M\to\infty}\frac{1}{M}\sum_{n=0}^{M-1} R_y(n,\tau)\exp\left(-j2\pi n\alpha\right) \tag{8}$$

Given the nature of $R_y(n,\tau)$, the function $R_y^\alpha(\tau)$ is only nonzero when $\tau = N$ and when α is one of the cyclic frequencies from the set $\mathcal{A}(N+N_\mathrm{g})$. This fact underlies the following estimators for N and N_g. Let $\mathcal{S}$ be the set of possible values of N. Then an estimator for N is obtained as

$$\hat{N} = \underset{\tau\in\mathcal{S}}{\operatorname{argmax}}\left|R_y^0(\tau)\right| \tag{9}$$

Similarly, let $\mathcal{S}_\mathrm{g}$ be the set of all possible values of $N+N_\mathrm{g}$. Then, assuming $\hat{N}$ is an accurate estimate of N, an estimator for N_g is obtained as

$$\hat{N}_\mathrm{g} = -\hat{N} + \underset{\xi\in\mathcal{S}_\mathrm{g}}{\operatorname{argmax}}\sum_{\alpha\in\mathcal{A}(\xi)}\left|R_y^\alpha(\hat{N})\right| \tag{10}$$

A graphical depiction of the functions being maximized in (9) and (10) is provided in the next subsection. Note

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

that because these estimators involve an autocorrelation limited approximately to offsets $|\tau| \leq N$, which amounts to a short time interval of $T = N/F_s$, they are robust to nonzero Doppler, provided that $\beta F_c T \ll 1$.

The mathematical structure of these two estimators is similar to the cyclic-correlation-based method presented in [10] except that they are intended to operate successively rather than jointly, which makes them more computationally efficient without loss of accuracy.

Observe that both estimators are based on the cyclic autocorrelation function given in (8). In practice, this function is approximated as

$$R_y^\alpha(\tau) \approx \frac{1}{M} \sum_{n=0}^{M-1} y(n+\tau) y^*(n) \exp(-j2\pi n\alpha) \quad (11)$$

where M is a number much larger than the cyclic period $N + N_g$, such as the number of samples in one frame, or even multiple frames if frame-to-frame correlation is of interest.

V. Signal Identification Procedure

We present here our solution to the signal identification problem posed in Section B. To facilitate replication, we present the solution in the form of a step-by-step procedure.

A. Estimation of N

We first construct $\mathcal{S}$, the set of possible values of N. Here we exploit the constraints that designers of OFDM signals must respect when choosing N. Naturally, they wish to maximize the signal's total data throughput, which for an OFDM signal with all subcarriers fully modulated is

$$d_{\text{OFDM}} = \frac{b_s F_s N}{N + N_g} \quad \text{bits/s} \quad (12)$$

Here, b_s is the number of bits per symbol (e.g., 2 for 4QAM modulation). Observe that, for given F_s and b_s, increasing d_{OFDM} implies increasing N/N_g. But N_g is lower-bounded by the physical characteristics of the channel: it must be large enough that $T_g = N_g/F_s$ exceeds the channel's delay spread. Thus, designers are motivated to increase N insofar as possible to maximize throughput. But they must respect a practical upper bound on N related to the subcarrier spacing $F = F_s/N$: a narrower F puts greater demands on CFO estimation. Let $\tilde{\beta}$ be the error in a receiver's estimate of the CFO parameter β. To avoid inter-carrier interference (ICI), which degrades BER, $\tilde{\beta}$ must satisfy

$$\tilde{\beta} F_c < \epsilon F \quad (13)$$

where F_c is the OFDM channel's center frequency and ϵ is limited to a few percent [17]. Assume that known synchronization symbols present within a frame allow modulation wipeoff on N_{sync} contiguous samples, exposing the underlying coherent carrier signal from which β can be estimated. Then a lower bound on the variance of $\tilde{\beta} F_c$ is given by the Cramér-Rao bound for the frequency estimation problem with unknown phase and amplitude [23]:

$$\text{var}(\tilde{\beta} F_c) \geq \frac{6 F_s^2}{\text{SNR} \cdot N_{\text{sync}} (N_{\text{sync}}^2 - 1)(2\pi)^2} \quad (14)$$

Based on this expression, the constraint on ϵ can be approximated as

$$\epsilon \approx \frac{N}{2\pi} \sqrt{\frac{6}{\text{SNR} \cdot N_{\text{sync}}^3}} < 0.02 \quad (15)$$

Designers will wish to minimize N_{sync}, since deterministic samples devoted to synchronization do not carry information. Suppose $N_{\text{sync}} = 2^{10}$ and SNR = 10 dB. Then N must satisfy $N < 5316$ to ensure $\epsilon < 0.02$.

Another practical constraint on N is that it must be a power of two for efficient IFFT and FFT operations at the transmitter and receiver. No OFDM waveform of which we are aware deviates from this norm.

Combining the power-of-two constraint with reasonable values of N satisfying (15), one can construct $\mathcal{S}$ as

$$\mathcal{S} = \{2^q : q \in \mathbb{N},\ 9 \leq q \leq 12\} \quad (16)$$

The development leading to (9) assumed that $F_h \approx F_r = F_s$. But of course, in the context of blind identification of operational OFDM signals, the relationship of the receiver's sampling rate F_r to F_s is unknown *a priori*. As will be revealed, the key to accurate estimation of both N and F_s is the power-of-two constraint on N.

Let $\bar{F}_s$ be a guess of F_s obtained by inspection of the power spectrum of $y(n)$. This can be accomplished by a single wideband capture or by a sweep of overlapping narrowband captures that collectively span a whole channel. Note that, besides $\bar{F}_s$, one may also obtain from this inspection a guess of the channel center frequency F_c. Bear in mind that even at high SNR it is not possible to exactly determine F_s from the power spectrum because subcarriers near the boundaries of an OFDM channel may be left unmodulated to provide a frequency guard interval [17]. Let $N_r = \lfloor N F_r / F_s \rceil$ be the approximate number of receiver samples in the useful symbol interval $T = N/F_s$, where $\lfloor \cdot \rceil$ denotes rounding to the nearest integer. Also let $\eta = F_r/\bar{F}_s$ be the estimated sampling rate ratio, and suppose that $|\bar{F}_s - F_s|/F_s < p$ for some $0 < p \ll 1$. Then for each $b \in \mathcal{S}$, a set of corresponding values of N_r can be constructed that accounts for the uncertainty in $\bar{F}_s$:

$$\mathcal{S}_{rb} = \{\tau \in \mathbb{N} : b\eta(1-p) \leq \tau \leq b\eta(1+p)\} \quad (17)$$

The full set of possible values of N_r is the union of these:

$$\mathcal{S}_r = \bigcup_{b \in \mathcal{S}} \mathcal{S}_{rb} \quad (18)$$

In other words, for every $b \in \mathcal{S}$, $\mathcal{S}_r$ contains an interval of corresponding possible values of N_r whose width depends on the assumed accuracy of $\bar{F}_s$. For convenience, define $f_r : \mathcal{S}_r \to \mathcal{S}$ as the function that maps possible values in $\mathcal{S}_r$ to the corresponding value in $\mathcal{S}$; i.e., $\forall \tau \in \mathcal{S}_{rb}$, $f_r(\tau) = b$.

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

With these preliminaries we may recast the estimator in (9) for the case in which F_s is only approximately known and may be significantly different from F_r:

$$\hat{N} = f_\mathrm{r}\left(\operatorname*{argmax}_{\tau\in\mathcal{S}_\mathrm{r}} \left|R_y^0(\tau)\right|\right) \tag{19}$$

Here, $R_y^0(\tau)$ is calculated by (11). This estimator works well for simulated OFDM signals, but must be augmented with a validation step when applied to operational signals due to the phenomenon manifest in Fig. 3. The blue trace in the top panel shows that captured Starlink data exhibit a clear peak in $\left|R_y^0(\tau)\right|$ at $\tau = N_\mathrm{r}$. But the peak's magnitude is less than that at other plausible values $\tau \in \mathcal{S}_\mathrm{r}$ due to a prominent central lobe in the empirical cyclic autocorrelation function. This lobe is due to a slower autocorrelation rolloff with increasing $|\tau|$ as compared to a simulated OFDM signal with equivalent N_r, β, SNR, F_h, and F_r (gray trace). The slow rolloff indicates significant redundancy in the received signal $y(n)$ at short offsets. Such redundancy doubtless stems from some combination of (i) strong error correction coding, (ii) inherent redundancy in the data stream owing to light or negligible data compression in an effort to achieve low latency, and (iii) adjacent-OFDM-symbol correlation caused by pilot symbols. The regular scalloped profile of the rolloff suggests that (i) and (iii) may be the most important factors.

In any case, to prevent the maximization in (19) from choosing a value of τ at which $\left|R_y^0(\tau)\right|$ is large only because of the prominent central autocorrelation lobe, $\hat{N}$ is accepted as valid only if

$$\frac{\max_{\tau\in\mathcal{S}_{rb}} \left|R_y^0(\tau)\right|}{\min_{\tau\in\mathcal{S}_{rb}} \left|R_y^0(\tau)\right|} > \nu, \quad b = \hat{N} \tag{20}$$

for some threshold ν. The point of this test is to ensure that the peak value is sufficiently distinguished from others in its neighborhood, a condition that does not hold within the wide central lobe of $\left|R_y^0(\tau)\right|$. If this validation step fails, then $\mathcal{S}$ is redefined as $\mathcal{S} \leftarrow \mathcal{S} \setminus \hat{N}$ and (19) is applied again, etc. Empirically, we find that for Starlink Ku-band downlink signals a threshold value $\nu = 10$ dB is adequate to ensure that spurious maxima are excluded. Note that one must choose p sufficiently large to ensure exploration of off-peak values in the validation test. This is especially important when F_h is significantly smaller than F_r, in which case the peak at $\left|R_y^0(N_\mathrm{r})\right|$ may be several samples wide.

B. Estimation of F_s

Having obtained $\hat{N}$, it is straightforward to obtain a more accurate estimate of F_s. For $b = \hat{N}$, define

$$\hat{N}_\mathrm{r} = \operatorname*{argmax}_{\tau\in\mathcal{S}_{rb}} \left|R_y^0(\tau)\right| \tag{21}$$

Note that $\hat{N}_\mathrm{r}/\hat{N} \approx F_\mathrm{r}/F_\mathrm{s}$ and that, owing to the way blocks of bandwidth are allocated by regulatory agencies, F_s is extremely likely to be an integer multiple of 1 MHz.

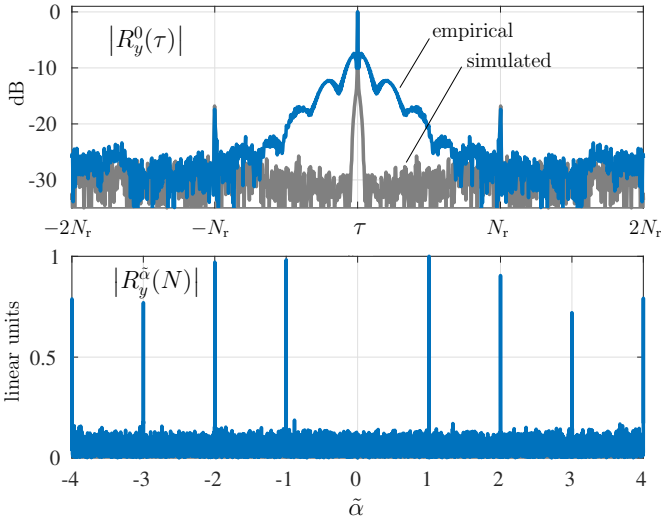

Fig. 3: Top: Cyclic autocorrelation function at $\alpha = 0$ for an empirical Starlink signal with SNR $= 5.5$ dB captured through the narrowband pipeline with capture interval approximately centered on an $\bar{F}_\mathrm{s}$-wide OFDM channel (blue), and for a simulated OFDM signal with iid Gaussian 4QAM symbols (gray). The simulated signal has been Doppler-adjusted, passed through a simulated AWGN channel, lowpass filtered, and resampled at 62.5 MHz to match the empirical signal's Doppler, SNR, bandwidth, and sampling rate. The total number of samples M used to estimate $R_y^\alpha(\tau)$ via (11) amounts to 10 ms of samples at $F_\mathrm{r} = 62.5$ MHz, which turn out to span just over 7 frames. Bottom: Cyclic autocorrelation as a function of the normalized frequency $\tilde{\alpha} = \alpha(N + N_\mathrm{g})$ for $\alpha \in \{p/(N + N_\mathrm{g}) : p \in \mathbb{R}\}$, derived from the same empirical data as the blue trace in the top panel but resampled at $F_\mathrm{s} = 240$ MHz. The peak at the fundamental cyclic frequency corresponding to the period $N_\mathrm{g} + N$ appears at $\tilde{\alpha} = 1$; other peaks appear at harmonics of this fundamental.

Therefore, for F_r and F_s expressed in MHz, an estimator for F_s is given by

$$\hat{F}_\mathrm{s} = \left\lfloor \frac{\hat{N} F_\mathrm{r}}{\hat{N}_\mathrm{r}} \right\rceil \tag{22}$$

The key to this estimator's accuracy is the power-of-two constraint on $\hat{N}$.

C. Resampling

Estimation of the remaining OFDM parameters of interest is facilitated by resampling $y(n)$ at $\hat{F}_\mathrm{s}$. Recall from (5) that $y(n)$ is natively sampled at F_r after lowpass filtering with bandwidth F_h. For the narrowband capture mode, resampling at $\hat{F}_\mathrm{s}$ implies a sampling rate increase, which can be modeled as [18]

$$y_\mathrm{r}(m) = \sum_{n\in\mathbb{Z}} y(n)\mathrm{sinc}(mF_\mathrm{r}/\hat{F}_\mathrm{s} - n) \tag{23}$$

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

where $\text{sinc}(x) = \sin(\pi x)/(\pi x)$. Note that the useful frequency content of the signal, $|f| < F_h$, remains unchanged. For the wideband capture mode, resampling at $\hat{F}_\text{s}$ implies conversion to a lower sampling rate after lowpass filtering with a new lower F_h. For notational simplicity, in what follows we will drop the subscript from y_r. Thus, $y(n)$ will hereafter denote the received signal with bandwidth F_h (possibly less than the original) and sampling rate $\hat{F}_\text{s}$.

D. Estimation of N_g

Estimation of N_g begins by constructing the set $\mathcal{S}_\text{g}$ of possible values of $N + N_\text{g}$. As with $\mathcal{S}$, this is informed by design constraints. From (12) it is clear that signal designers will wish to minimize N_g, but this is subject to the constraint that $T_\text{g} = N_\text{g}/F_\text{s}$ exceeds the channel's delay spread under all but the most extreme operating conditions. Worst-case 95% root-mean-square delay spread for the Ku-band was found in [20] to be $T_\text{d} = 108$ ns. Conservatively considering a range of values from half to twice this amount, and assuming that, for ease of implementation, N_g is even, one can construct $\mathcal{S}_\text{g}$ as

$$\mathcal{S}_\text{g} = \left\{2q + b : b \in \mathcal{S},\ q \in \mathbb{N},\ T_\text{d}\hat{F}_\text{s}/4 \le q \le T_\text{d}\hat{F}_\text{s}\right\} \tag{24}$$

With $y(n)$ sampled at $\hat{F}_\text{s}$, estimation of N_g then proceeds as in (10) except that $R_y^\alpha(\hat{N})$ is calculated via (11) and $\mathcal{A}(\xi)$ is reduced to the finite set $\mathcal{A}(\xi) = \{p/\xi : p \in \mathbb{Z}, |p| \le N_p\}$. for some finite N_p.

The accuracy of this estimator as a function of N_p is analyzed in [10], where it is shown that no improvement attains to values of N_p above N/N_g. In practice, when applied to Starlink signals captured via the narrowband mode, estimator performance was reliable for N_p as low as 1 provided that the number of samples M in (11) covered at least one frame ($M \ge T_\text{f}F_\text{s}$) and that SNR > 3.5 dB.

The lower panel in Fig. 3 shows a version of $|R_y^\alpha(N)|$ from empirical Starlink data at SNR $= 5.5$ dB that has been normalized so that the cyclic frequencies are integers. The span of cyclic frequencies shown corresponds to $N_p = 4$.

E. Estimation of T_f

Each frame contains one or more OFDM symbols with predictable elements, called synchronization sequences, that enable receiver time and frequency synchronization. A peak emerges in the cyclic autocorrelation $R_y^0(\tau)$ when one synchronization sequence is aligned with its counterpart from a nearby frame. Thus, estimation of the frame period T_f is also based on $R_y^0(\tau)$ as calculated in (11), but now with the number of samples M large enough to cover multiple adjacent frames.

Let $N_\text{f} = T_\text{f}F_\text{s}$ be the frame period expressed in number of samples, and let $\mathcal{S}_\text{f}$ be the set of possible values of N_f. By inspection of the empirical signal spectrogram during a period of sparse traffic, one can easily obtain an upper bound T_m on the smallest active signal interval. Observe that this may be a loose upper bound on T_f because the smallest active interval observed may actually be multiple frames. One can then construct a conservative $\mathcal{S}_\text{f}$ as follows:

$$\mathcal{S}_\text{f} = \left\{q \in \mathbb{N} : \hat{N} + \hat{N}_\text{g} < q \le \hat{F}_\text{s}T_\text{m}\right\} \tag{25}$$

Considerations of expected signal numerology are once again useful in the case of estimating T_f. While T_f need not be an integer number of milliseconds, N_f is likely to be an integer for ease of signal generation, and, more importantly, the frame rate $F_\text{f} = 1/T_\text{f}$ is almost certainly integer number of Hz for ease of frame scheduling across the constellation. Therefore, for $\hat{F}_\text{s}$ expressed in Hz, an effective estimator for T_f is given by

$$\hat{T}_\text{f} = \left\lfloor \hat{F}_\text{s}\left(\underset{\tau\in\mathcal{S}_\text{f}}{\text{argmax}}\left|R_y^0(\tau)\right|\right)^{-1}\right\rfloor^{-1} \tag{26}$$

Note that, as for the estimators of N and N_g, this estimator for T_f is robust to nonzero Doppler provided that $\beta F_\text{c} T_\text{ss} \ll 1$, where T_ss is the longest time interval of any contiguous synchronization sequence.

F. Symbol and Carrier Frequency Synchronization

Estimating the remaining parameters in Table I and any synchronization sequences requires both OFDM symbol synchronization and carrier frequency synchronization. Such synchronization must be carried out blindly, since the very sequences designed to enable it are unknown.

Let n_{mik} be the index of the kth sample in the ith OFDM symbol of the mth frame, assuming zero-based indexing of k, i, and m. For some $m, i \in \mathbb{N}$ with $i < N_\text{sf}$, we wish to find n_{mi0} and the value of the CFO parameter β that applies at n_{mi0}, denoted β_{mi}.

When frame traffic is low enough that gaps are present between frames, it is possible to observe an abrupt increase in sample energy $|y(n)|^2$ at the beginning of a frame, which allows approximation of n_{m00}, the index of the first sample in the first OFDM symbol of the frame. By adding integer multiples of $\hat{N} + \hat{N}_\text{g}$, one can then approximate n_{mi0} for all $i \in (0, N_\text{sf})$. Let $\bar{n}_{mi0}$ be an approximate value for n_{mi0}. Then $\mathcal{S}_{mi}$, the set of possible values of n_{mi0}, may be constructed as

$$\mathcal{S}_{mi} = \{n \in \mathbb{Z} : |n - \bar{n}_{mi0}| \le d\} \tag{27}$$

with d large enough to account for uncertainty in $\bar{n}_{mi0}$.

Let $\mathcal{B}_{mi}$ be the set of possible values of β_{mi}. One might think that the range of *a priori* uncertainty in β_{mi} is small because, for known receiver location and time, and known transmitting satellite ephemeris, the line of sight velocity v_los can be readily calculated, from which β can be calculated as $\beta = v_\text{los}/c$. But recall from Section B that β also accounts for any frequency offset between the transmitter and receiver oscillators.

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

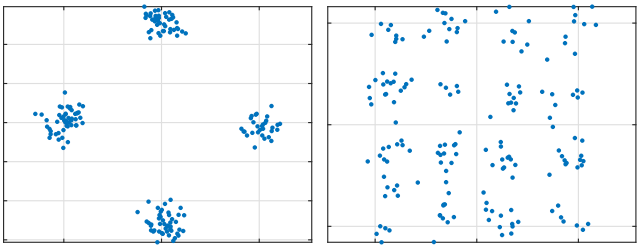

Fig. 4: Empirical Starlink symbol constellations for 4QAM (left) and 16QAM (right) OFDM modulation.

In the present context, such an offset may arise not only because of disagreement between the oscillators, but also due to uncertain knowledge of F_c, the center frequency of the OFDM channel captured to produce $y(n)$. As a consequence, the range of β_{mi} values included in $\mathcal{B}_{mi}$ may be several times larger than what would be predicted based on v_los/c alone. Let $\bar{\beta}_{mi}$ be a prior estimate of β_{mi} based on ephemeris calculations and any other relevant prior information, β_m be the maximum offset from $\bar{\beta}_{mi}$ considered, and $\Delta\beta = \epsilon\hat{F}_\mathrm{s}/\hat{N}\bar{F}_\mathrm{c}$ be the search stride, chosen to satisfy (13), where $\bar{F}_\mathrm{c}$ is both an *a priori* estimate of F_c obtained by inspection of the power spectrum of $y(n)$, and the exact center of the band captured to produce $y(n)$. Then $\mathcal{B}_{mi}$ may be constructed as

$$\mathcal{B}_{mi} = \left\{ q\Delta\beta : q \in \mathbb{Z},\ \left| q\Delta\beta - \bar{\beta}_{mi} \right| \le \beta_\mathrm{m} \right\} \tag{28}$$

By a simultaneous search through the values in $\mathcal{S}_{mi}$ and $\mathcal{B}_{mi}$, one may estimate n_{mi0} and β_{mi0} with sufficient accuracy to enable standard receiver processing of each corresponding OFDM symbol in $y(n)$, leading to recovery of the relevant original information symbols $\{X_{mik}\}$. Fig. 4 shows the successful result for a portion of one frequency-domain OFDM symbol with 4QAM modulation and another symbol with 16QAM modulation. Tight constellation clusters like those in the left panel only emerge when SNR is sufficiently high (15 dB in this case) and when the estimates of n_{mi0} and β_{mi} are accurate enough that ISI and ICI are negligible. Otherwise, the clusters become elongated (due to mild ISI or ICI), or they experience a complete collapse toward the origin (severe lack of synchronization). Clearly then, symbol constellations can be used to develop a score function that increases with synchronization accuracy.

Let $\mathrm{SC} : \mathcal{S}_{mi} \times \mathcal{B}_{mi} \to \mathbb{R}_+$ be such a function, with trial synchronization values $n \in \mathcal{S}_{mi}$ and $\beta \in \mathcal{B}_{mi}$ as arguments. Algorithm 1 shows the computations underlying SC. First, an OFDM-symbol-length block of samples is isolated starting at the trial index n. The block is then resampled and frequency shifted to undo the effects of nonzero β, after which its cyclic prefix is discarded and the remaining samples are converted to the frequency domain via an FFT. The resulting received information symbols in $\boldsymbol{Y}$ cluster as shown by the examples in Fig. 4. Assuming b_s bits per symbol, 2^{b_s} clusters will be present. These are identified automatically via k-means clustering. For $b_\mathrm{s} \le 2$, the function's output s is the empirical SNR, calculated as the mean of the squared magnitude of each cluster's centroid divided by twice the cluster's variance. Note that s is insensitive to rotations of the constellation due to the unknown reference phase of the symbols $\{X_{mik}\}$.

Algorithm 1: $\mathrm{SC}(n, \beta)$

Input : $n \in \mathcal{S}_{mi},\ \beta \in \mathcal{B}_{mi}$
Output: $s \in \mathbb{R}_+$

$\boldsymbol{y} = [y(n), y(n+1), \ldots, y(n+\hat{N}+\hat{N}_\mathrm{g}-1)]$
$\boldsymbol{t}_y = [0 : \hat{N}+\hat{N}_\mathrm{g}-1]/\hat{F}_\mathrm{s}$
$[\boldsymbol{y}, \boldsymbol{t}_y] = \texttt{resample}(\boldsymbol{y}, \boldsymbol{t}_y, (1-\beta)\hat{F}_\mathrm{s})$
for $i = 0 : \hat{N}+\hat{N}_g-1$ **do**
  $\boldsymbol{y}(i) = \boldsymbol{y}(i)\exp\left(j2\pi\beta\bar{F}_\mathrm{c}\boldsymbol{t}_y(i)\right)$
end
$\boldsymbol{y} = \boldsymbol{y}(\hat{N}_\mathrm{g} : \hat{N}_\mathrm{g}+\hat{N}-1)$
$\boldsymbol{Y} = \texttt{fft}(\boldsymbol{y})$
$[\boldsymbol{c}, \boldsymbol{\sigma}] = \texttt{kmeans}(\boldsymbol{Y}, 2^{b_\mathrm{s}})$
for $i = 0 : 2^{b_\mathrm{s}}-1$ **do**
  $\boldsymbol{s}(i) = |\boldsymbol{c}(i)|^2/2\boldsymbol{\sigma}^2(i)$
end
$s = \texttt{mean}(\boldsymbol{s})$

With SC, construction of the estimator for n_{mi0} and β_{mi0} is straightforward:

$$\hat{n}_{mi0},\ \hat{\beta}_{mi} = \underset{\substack{n \in \mathcal{S}_{mi} \\ \beta \in \mathcal{B}_{mi}}}{\operatorname{argmax}}\ \mathrm{SC}(n, \beta) \tag{29}$$

This estimator was found to work well on both types of standard OFDM symbol modulation found in the captured Starlink signal frames, namely 4QAM ($b_\mathrm{s} = 2$) and 16QAM ($b_\mathrm{s} = 4$), even when the signals' SNR was too low to ensure error-free cluster identification, as in the right panel in Fig. 4. But the estimator failed unexpectedly when applied to the first OFDM symbol interval in each frame. Closer examination revealed that this interval does not contain an OFDM symbol but rather a repeating pseudorandom time-domain sequence. Nonetheless, estimates of n_{m00} and β_{m00} were accurately obtained as $\hat{n}_{m00} = \hat{n}_{m10} - \hat{N} - \hat{N}_\mathrm{g}$ and $\hat{\beta}_{m0} = \hat{\beta}_{m1}$.

G. Estimation of the Synchronization Sequences

Estimating the synchronization sequences embedded in each Starlink frame is one of this paper's key contributions. To this end, one must first locate the sequences, i.e., determine which OFDM symbol intervals within a frame contain predictable features. Recall that, by definition, synchronization sequences are predictable from the perspective of the user terminal. For public-access OFDM signals such as Wi-Fi, WiMAX, LTE, etc., they are not only predictable but constant from frame to frame. Presuming the same for Starlink signals, locating such sequences within a frame is a matter of isolating individual OFDM symbol intervals and correlating these

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

across multiple frames to determine whether the candidate intervals contain features that repeat from frame to frame. Isolating OFDM symbol intervals is possible at this stage because $\hat{n}_{mi0}$, $\hat{N}$, and $\hat{N}_{\rm g}$, and are available.

This procedure revealed that the first OFDM symbol in each Starlink frame, the one starting at sample index n_{m00}, contains a synchronization sequence. The interval was found to lack any discernible constellation structure when viewed in the frequency domain. But its cross-correlation against first symbol intervals in neighboring frames revealed a pattern of peaks indicating that the interval is composed of 8 repetitions of a time-domain-rendered subsequence of symbols of length $\hat{N}/8$, with the first instance inverted. (A complete model of this synchronization sequence is presented in a later section.) Estimation of the exact symbol values was only possible using data obtained via the wideband capture mode, since the subsequence's frequency content spans the whole of $F_{\rm s}$. Despite the low SNR of the wideband capture mode, knowledge of $\hat{\beta}_{m0}$, $\hat{n}_{mi0}$, $\hat{N}$, and $\hat{N}_{\rm g}$ allowed the 8 subsequence repetitions to be stacked and summed coherently to reveal the unique subsequence values, which will be presented in a following section. The 8 subsequence repetitions are prepended by a cyclic prefix of length $\hat{N}_{\rm g}$. Borrowing language from the LTE specification, we call the full $(\hat{N}+\hat{N}_{\rm g})$-length sequence the primary synchronization sequence (PSS). It was found that the PSS is not only identical across all frames from the same Starlink satellite, but also identical across all satellites in the constellation.

The second OFDM symbol interval, which starts at sample index n_{m10}, was also found to contain a $(\hat{N}+\hat{N}_{\rm g})$-length synchronization sequence, which we call the secondary synchronization sequence (SSS). Unlike the PSS, the SSS was found to be a standard OFDM symbol, with 4QAM modulation. Estimating the information symbols $\{X_{m1k}\}_{k=0}^{N-1}$ was possible even with narrowband-mode-captured data because the received symbols that fell within the narrowband mode's bandwidth were clearly observable (to within a phase offset), as shown in the left panel of Fig. 4. In other words, with the high-SNR narrowband data, those elements of $\boldsymbol{Y}$ in Algorithm 1 corresponding to frequencies within the 62.5-MHz narrowband window could be confidently assigned to one of four clusters. At this stage, it was not known whether the SSS was anchored with an absolute initial phase so that the symbols $\{X_{m1k}\}_{k=0}^{N-1}$ would be constant across m, or differentially encoded so that only $X^*_{m1(k+1)}X_{m1k}$ would be constant, for $k \in [0, N-2]$. Moreover, the estimates $\hat{n}_{m10}$ for various m were not precise enough at this stage to ensure that corresponding constellation clusters could be associated with each other from frame to frame. Therefore, only differential values were initially estimated, with $Y^*_{m1(k+1)}Y_{m1k}$ being an estimate of $X^*_{m1(k+1)}X_{m1k}$, where Y_{m1k} is the kth element of $\boldsymbol{Y}$ in Algorithm 1 for OFDM symbol $i=1$ of frame m.

By successively shifting the 62.5-MHz capture band across an OFDM channel of width $F_{\rm s}$ in repeated captures, and by ensuring sufficient frequency overlap, it was possible to confidently estimate each $X^*_{m1(k+1)}X_{m1k}$ such that the full sequence $\{X_{m1k}\}_{k=0}^{N-1}$ could be determined to within two unknown symbols, X_{m12} and $X_{m1(N/2)}$. The first of these is unobservable from the differential estimates due to the presence of a mid-channel "gutter" in which $X_{mik}=0$ for $k \in \{0,1,N-2,N-1\}$; the second is unobservable because it lies at the bottom edge of the frequency band. By searching through all possible combinations of these two unknown symbols, re-generating for each trial combination a candidate time-domain OFDM SSS (prepended by the appropriate cyclic prefix), concatenating this candidate SSS with the known time-domain PSS, and maximizing correlation against the first two OFDM symbol intervals in received data frames, all while resampling and frequency shifting the received data to account for nonzero β as in Algorithm 1, it was possible to estimate X_{m12} and $X_{m1(N/2)}$ and thereby completely determine the SSS. As with the PSS, it was found that the SSS is identical across all satellites in the Starlink constellation.

The last nonzero OFDM symbol in each frame, the one starting at sample index n_{mi0} with $i=301$, was also found to contain a $(\hat{N}+\hat{N}_{\rm g})$-length synchronization sequence, which we call the coda synchronization sequence (CSS). Like the SSS, the CSS is a standard 4QAM OFDM symbol whose information symbols $\{X_{mik}\}_{i=301,k=0}^{i=N-1}$ can be determined by inspection. The CSS symbol constellation is rotated by 90 degrees with respect to the SSS: whereas the SSS exhibits the diamond configuration shown in the left panel of Fig. 4, the CSS's constellation clusters form a box aligned with the horizontal and vertical axes.

The penultimate nonzero OFDM symbol in each frame, the one starting at sample index n_{mi0} with $i=300$, was found to contain some information symbols that are constant from frame to frame. But, unlike the SSS and the CSS, not all the information symbols are constant. We call the predictable elements of this symbol the coda-minus-one synchronization sequence (CM1SS).

H. Estimation of $N_{\rm sf}$, $N_{\rm sfd}$, *and* $T_{\rm fg}$

Equipped with $\hat{n}_{mi0}$, $\hat{N}$, $\hat{N}_{\rm g}$, $\hat{T}_{\rm f}$, and knowledge that the first two OFDM symbol intervals in each frame are synchronization sequences, it is trivial to estimate $N_{\rm sf}$, $N_{\rm sfd}$, and $T_{\rm fg}$. The estimated OFDM symbol duration is $\hat{T}_{\rm sym}=(\hat{N}+\hat{N}_{\rm g})/\hat{F}_{\rm s}$, and thus the estimated number of whole symbol intervals in one frame is $\lfloor \hat{T}_{\rm f}/\hat{T}_{\rm sym} \rfloor$, where $\lfloor\cdot\rfloor$ denotes the floor function. The final interval was found to be vacant. Thus, the estimated number of non-zero symbols in a frame is

$$\hat{N}_{\rm sf} = \lfloor \hat{T}_{\rm f}/\hat{T}_{\rm sym} \rfloor - 1 \tag{30}$$

Counting the PSS, SSS, CM1SS, and CSS as synchronization symbols, the estimated number of non-

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

synchronization symbols in a frame is

$$\hat{N}_{\text{sfd}} = \hat{N}_{\text{sf}} - 4 \tag{31}$$

Finally, the estimated frame guard interval—the vacant interval between successive frames—is

$$\hat{T}_{\text{fg}} = \hat{T}_{\text{f}} - \hat{N}_{\text{sf}}\hat{T}_{\text{sym}} \tag{32}$$

I. Estimation of $F_{\text{c}i}$

Estimation of $F_{\text{c}i}$, the center frequency of the ith Starlink OFDM channel, is complicated by the exponential in (4) being a function of both β and the offset $F_{\text{c}} - \bar{F}_{\text{c}}$. This implies that an error in the *a priori* estimate $\bar{F}_{\text{c}i}$ results in a frequency offset just as with nonzero β. But the two effects can be distinguished by recognizing that compression or dilation of the modulation $x(t)$ in (4) is solely a function of β. Therefore, determination of $F_{\text{c}i}$ begins by estimating the β that applies for the ith channel as expressed via $x(t)$, which may be done by measuring a sequence of frame arrival times.

Assume that the local receiver clock used for downmixing and sampling the received signal is short-term stable and GPS-disciplined, as with the 10-MHz OCXO in Fig. 1, so that it may be considered a true time reference. Let $\{\hat{n}_{m00}\}_{m\in\mathcal{M}}$ be the estimated indices of samples that begin a frame for channel i, as determined by (29) or by correlation against the known PSS and/or SSS. Note that the set of frame indices in $\mathcal{M}$ may not have a regular spacing. Let the nominal time $t(m)$ and the received time $t_{\text{r}}(m)$ of frame $m \in \mathcal{M}$ be

$$t(m) = m\hat{T}_{\text{f}}, \quad t_{\text{r}}(m) = \hat{n}_{m00}/\hat{F}_{\text{s}}$$

For intervals up to one second, which a study of frame timing revealed as the cadence at which clock corrections are applied onboard the Starlink satellites, the relationship between $t(m)$ and $t_{\text{r}}(m)$ can be accurately modeled as a second-order polynomial

$$t_{\text{r}}(m) = a_0 + a_1\left(t(m) - t(m_0)\right) + a_2\left(t(m) - t(m_0)\right)^2$$

where $m_0 = \min\mathcal{M}$. Let $\{\hat{a}_i\}_{i=0}^2$ be coefficient estimates obtained via least squares batch estimation. Then $\bar{\beta}_{m_0 0} = \hat{a}_1$ is the modulation-estimated β value that applies at the beginning of frame m_0. Let $\hat{\beta}_{m_0 0}$ be the value of β that applies at the same instant, as estimated by (29). Also, recall that $\bar{F}_{\text{c}i}$ is both the *a priori* estimate of $F_{\text{c}i}$ assumed in (29) and the exact center of the band captured to produce the $y(n)$. Then

$$\hat{F}_{\text{c}i} = \left\lfloor \frac{\bar{F}_{\text{c}i}}{1 + \bar{\beta}_{m_0 0} - \hat{\beta}_{m_0 0}} \right\rceil \tag{33}$$

is an estimator of $F_{\text{c}i}$, where $\hat{F}_{\text{c}i}$ and $\bar{F}_{\text{c}i}$ are expressed in MHz. Rounding to the nearest MHz is justified for the same reasons given in connection with (22).

VI. Results

Application of the foregoing blind signal identification procedure yields the parameter values given in Table II for the Starlink Ku-band downlink. Figs. 5 and 6 offer graphical representations of the channel and frame layouts. The PSS was found to be composed of eight repetitions of a length-$N/8$ subsequence prepended by a cyclic prefix. As shown in Fig. 6, the cyclic prefix and the first instance of the repeated subsequence have inverted polarity relative to the remainder of the PSS. The time-domain expression of the PSS can be written as

$$x_{m0}(t) = \sum_{k=-N_{\text{g}}}^{N-1} \operatorname{sinc}\left[tF_{\text{s}} - k - N_{\text{g}}\right] p_k \tag{34}$$

$$p_k = \exp\left(j\pi\left[\mathbf{1}_{\mathcal{P}}(k) - \frac{1}{4} - \frac{1}{2}\sum_{\ell=0}^{k \bmod \frac{N}{8}} b_\ell\right]\right) \tag{35}$$

$$b_\ell = 2\left(\left\lfloor \frac{q_{\text{pss}}}{2^\ell} \right\rfloor \bmod 2\right) - 1 \tag{36}$$

where $\mathbf{1}_{\mathcal{P}}(k)$ is the indicator function, equal to unity when $k \in \mathcal{P}$ and zero otherwise, and $\mathcal{P} = \{k \in \mathbb{Z} : k < N/8\}$. The indicator function rotates the phase by π for $k < N/8$ to invert the cyclic prefix and the first repetition of the PSS subsequence. The PSS subsequence $(p_k)_{k=N/8}^{2N/8-1}$ is a symmetric differential phase shift keying (symmetric DPSK) encoding of a length-127 maximal-length linear-feedback shift register (LFSR) sequence (m-sequence). In this modulation, each bit of the m-sequence indicates a positive or negative $\pi/2$ phase rotation. The m-sequence can be generated using a 7-stage Fibonacci LFSR with primitive polynomial $1 + D^3 + D^7$ and initial state $(a_{-1}, \ldots, a_{-7}) = (0, 0, 1, 1, 0, 1, 0)$, following the convention in [24]. Suppose that the LFSR's output $a_0, a_1, \ldots, a_{126}$ is stored as a 127-bit number with a_0 as MSB and a_{126} as LSB. Appending this number with a 0 yields the 128-bit hexadecimal number that appears in (36):

$$q_{\text{pss}} = \texttt{C1B5 D191 024D 3DC3 F8EC 52FA A16F 3958}$$

To ensure correct interpretation of (35) and (36), we list the first 8 values of the PSS subsequence:

$$p_k = \exp\left(j\pi\left[1/4 + q_k/2\right]\right), \quad k \in \{N/8, \ldots, N/8 + 7\}$$
$$(q_{N/8}, \ldots, q_{N/8+7}) = (0, 1, 2, 1, 0, 1, 0, 1)$$

The time-domain expression of the SSS can be written as $x_{m1}(t)$ from (3) with the complex coefficients given by

$$X_{m1k} = \begin{cases} \exp(j\theta_k), & k \in \{2, \ldots, N-3\} \\ 0, & \text{otherwise} \end{cases} \tag{37}$$

$$\theta_k = s_k\pi/2 \tag{38}$$

$$s_k = \left\lfloor \frac{q_{\text{sss}}}{4^{k-2}} \right\rfloor \bmod 4 \tag{39}$$

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

TABLE II: Starlink Downlink Signal Parameter Values

Parameter	Value	Units
F_{s}	240	MHz
N	1024	
N_{g}	32	
T_{f}	1/750	s
T_{fg}	$68/15 = 4.5\overline{33}$	μs
N_{sf}	302	
N_{sfd}	298	
T	$64/15 = 4.2\overline{66}$	μs
T_{g}	$2/15 = 0.1\overline{33}$	μs
T_{sym}	4.4	μs
F	234375	Hz
$F_{\mathrm{c}i}$	$10.7 + F/2 + 0.25(i - 1/2)$	GHz
F_{δ}	250	MHz
F_{g}	10	MHz

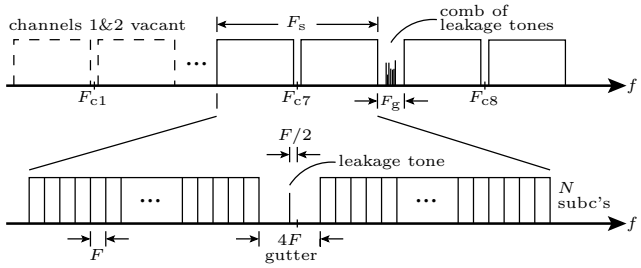

Fig. 5: Channel layout for the Ku-band Starlink downlink.

where q_{sss} is the hexadecimal number

$q_{\mathrm{sss}} =$ BD 565D 5064 E9B3 A949 58F2 8624 DED5
6094 6199 F5B4 0F0E 4FB5 EFCB 473B 4C24
B2D1 E0BD 01A6 A04D 5017 DE91 A8EC C0DA
09EB FE57 F9F1 B44C 532F 161C 583A 4249
0A5C 09F2 A117 F9A2 8F9B 2FD5 47A7 4C44
BABB 4BE8 5DA6 A62B 1235 E2AD 084C 0018
0142 A8F7 F357 DEC4 F313 16BC 58FA 4049
09A3 FCA7 F88E 4219 02B6 A258 0AE8 0308
03F6 5809 DB34 7F59 0DBC 46F0 10EB E3A2
5C06 0D74 429F C46B DF9B 6371 9279 798D
232C 5ABA 2741 22FF 66AD 7E44 9F44 CB40
C49C 24A1 E262 9F5B FE82 CE53 1FDC 34F8
C64A 43A9 63F4 0D5B 71BD E6FB 2F13 492D
6F2E 8544 B21D 4497 22C6 3518 0342 CD00
26A1 E7F7 E80E 91B1 75E8 52F9 1976 7E5A
F9B6 E909 AF36 2F52 18E2 B908 DC00 5803

To ensure correct interpretation of (39), we provide the first 8 values of s_k corresponding to nonzero X_{m1k}:

$$(s_2, \ldots, s_{10}) = (3, 0, 0, 0, 0, 2, 1, 1)$$

The CSS and the CM1SS will be presented in a later publication to provide adequate space for a detailed presentation and discussion of their characteristics.

VII. Discussion

Our blind signal identification process reveals a Starlink Ku-band downlink signal that is elegantly simple. Unlike LTE and 5G New Radio (5G NR), whose bandwidth and duplexing scheme may vary from region to region, and whose cyclic prefix length may vary with time, Starlink employs fewer modes of operation. This section offers observations on salient features of the Starlink signal.

A. Channel Layout

As shown in Fig. 5, a total of eight channels, each with a bandwidth of $F_{\mathrm{s}} = 240$ MHz, span the band allocated for Starlink's Ku-band downlink. In principle, multiple channels could be active simultaneously within a service cell. We assume that neighboring cells are serviced with different channels to avoid inter-cell interference, as described in [5], but we were not able to verify this with our limited experimental setup. The lower two channels, those centered at F_{c1} and F_{c2}, are currently vacant. This likely reflects a concession SpaceX has made to avoid interfering with the 10.6-10.7 GHz radio astronomy band.

Each channel's central four subcarriers are vacant, leaving a mid-channel gutter. Reserving such a gutter is a common practice in OFDM; otherwise, leakage from a receiver's mixing frequency may corrupt central information symbols. In Starlink's case, a transmitter-side leakage tone is present in some gutters for some satellites. For example, a leakage tone was found in the gutter of channel 5 on the Starlink satellite with identifier 3262, channel 6 on Starlink 3503, and channel 5 on Starlink 2409, whereas for other satellites no leakage tones were observed for the same channels. Interestingly, the ith channel's center frequency, $F_{\mathrm{c}i}$, is $F/2$ higher than the channel's midpoint, which lies in the center of the mid-channel gutter. A gutter leakage tone, if present, resides at the channel midpoint.

A guard band with a generous bandwidth $F_{\mathrm{g}} = 10$ MHz separates adjacent channels. Within some guard bands there appears a comb of 9 leakage tones uniformly spaced over a bandwidth of approximately 350 kHz. For example, such combs were observed between channels 5 and 6 on Starlink 2024, between channels 5 and 6 on Starlink 1184, and between channels 7 and 8 on Starlink 2423, whereas for other satellites no combs were observed between the same channels. Interestingly, the between-channel combs of tones, when present, persist between frames, whereas the mid-channel gutter leakage tones, when present, only appear during the interval of a broadcast frame.

We suspect that the between-channel tones may be the tones tracked in [6], [7] and [8] to perform Doppler-based positioning with Starlink. We note that neither the mid-channel gutter tones nor the between-channel tones appear deliberate: their presence and amplitudes are not consistent from satellite to satellite, and the between-channel tones appear to vary in amplitude with beam adjustments.

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

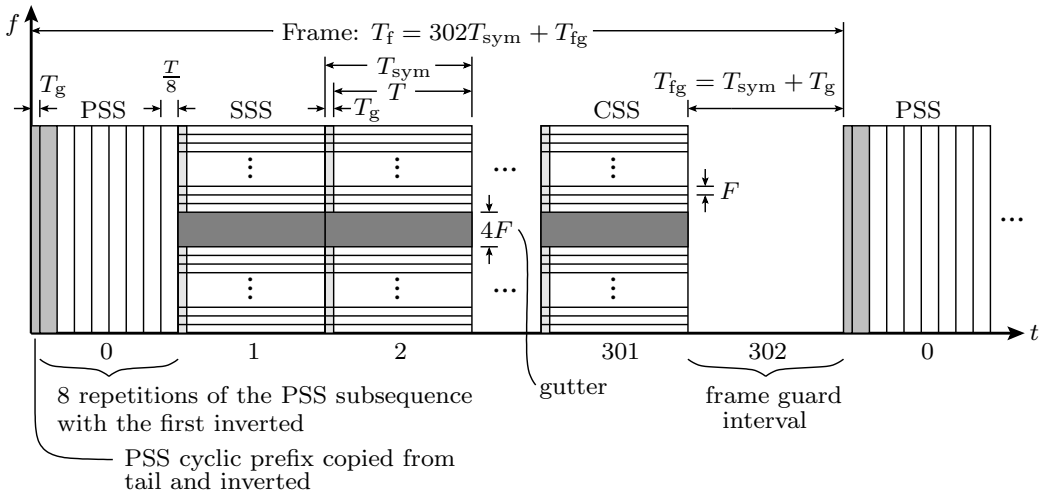

Fig. 6: Frame layout for the Ku-band Starlink downlink along time-frequency dimensions.

B. Frame Layout

As shown in Fig. 6, each frame consists of 302 intervals of length $T_\mathrm{sym} = 4.4$ μs plus a frame guard interval T_fg, for a total frame period of $T_\mathrm{f} = 1/750$ s. Each frame begins with the PSS, which is natively represented in the time domain, followed by the SSS, which is formatted as a standard 4QAM OFDM symbol. Each frame ends with the CM1SS followed by the CSS and the frame guard interval. A subsequent frame may be immediately present or not, depending on user demand.

The known information symbols of the SSS and CSS allow a receiver to perform channel estimation across all subcarriers at the beginning and end of each frame, permitting within-frame interpolation. The purpose of the CM1SS, which arrives just before the CSS and is only partially populated with information symbols that repeat from frame to frame, is unclear, but its predictable elements are no doubt also useful for channel estimation.

In each frame, the OFDM symbols with index $i \in \{2, 3, 4, 5\}$ appear to contain header (control plane) information—likely including satellite, channel, and modulation schedules. We infer this from an abrupt 90-degree shift in constellation orientation between symbol $i = 5$ and $i = 6$, which we interpret as denoting a transition from header to payload symbols. Such a shift in orientation may be seen between the left and right panels of Fig. 4. The first seven or so payload symbols (from $i = 6$ to approximately $i = 12$) are sometimes 16QAM modulated, with the remainder of the symbols 4QAM modulated. We presume that the 16QAM symbols are destined for users whose received SNR is sufficient to support decoding them (about 15 dB, depending on channel coding).

The previously-mentioned $4F$-wide mid-channel gutter is present in all OFDM symbols contained in a frame, but not in the PSS.

C. Synchronization Sequences

The synchronization sequences are of special import for efforts to dual-purpose Starlink signals for PNT. As with the spreading codes of civil GNSS signals, the synchronization sequences can be predicted by a passive (receive only) radio and thus used to construct a local signal replica whose correlation with the received signal yields standard pseudorange and Doppler observables, the raw ingredients for a PNT solution.

Fig. 7 shows correlation against the PSS yielding sharp peaks at the beginning of each frame. The distinctive shape of the 11-tined comb shown in the figure's inset results from the repetition and inversion of the subsequence $(p_k)_{k=N/8}^{2N/8-1}$ of which the PSS is composed. Note that adjacent frames may have different power levels despite being received from the same satellite and beam, evidence that the system employs user-subset-specific power adaptation within a service cell. Note too the absence of frames during some intervals, which suggests that user data demand was well below system capacity during the interval shown. It should be pointed out, however, that frame occupancy never dropped below 1 in 30 (one frame every 40 ms) throughout the scores of data intervals we studied. We intuit that a steady stream of frames, albeit sparse, is required to support initial network entry. Thus, even during periods of little or no user demand, frame arrival from each satellite will be regular and dense enough to support opportunistic PNT.

Importantly, phase coherence is maintained throughout each frame, and the phase relationship between the synchronization sequences appears to be constant across frames and satellites. This implies that time-domain representations of the synchronization sequences (with their respective cyclic prefixes) can be combined to extend the coherent integration interval over each frame, increasing receiver sensitivity and observable measurement accuracy. This technique enables production of pseudorange and Doppler observables below -6 dB SNR, well below the

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

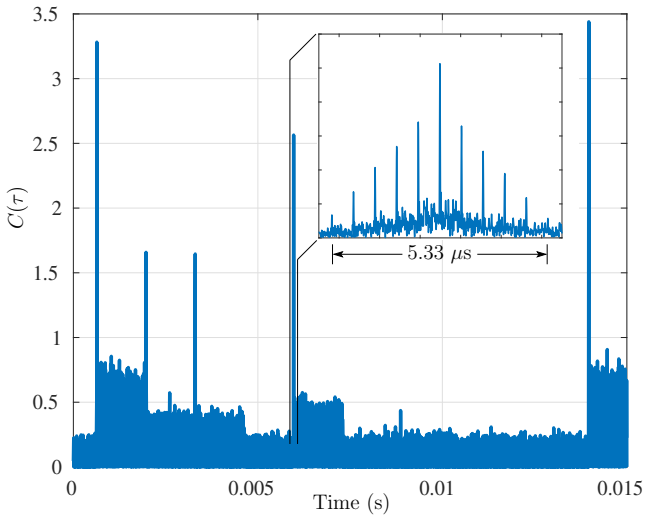

Fig. 7: Correlation of narrowband-mode-received Starlink data against a local PSS replica after Doppler compensation.

SNR required to support communication. Thus, receivers exploiting Starlink for PNT need not be equipped with high gain antennas and may even be able to extract observables from satellites not servicing their cell.

Unlike GNSS spreading codes, however, the Starlink synchronization sequences are are not unique to each satellite. This presents a satellite assignment ambiguity problem that must be solved combinatorially based on approximate user location, known satellite ephemerides, and measured Doppler and frame arrival time.

It seems clear why the PSS is composed of repeating subsequences: in high SNR conditions, the search in Doppler and frame start time entailed by (29) for initial network entry can be made more efficient by correlating against a single PSS subsequence and then taking the FFT of the resulting complex accumulations with maximum modulus to refine the Doppler estimate. The shorter initial coherent integration interval is more forgiving of errors in β. If this fails due to insufficient single-subsequence-correlation SNR, multiple subsequences can be coherently accumulated for a slower but more sensitive search.

That the PSS is based on an m-sequence is also logical, given such sequences' excellent autocorrelation properties [24]. Encoding the m-sequence as a series of $\pi/2$ phase shifts appears intended to reduce spectral leakage compared to a conventional binary encoding. The rationale for differentially encoding the PSS is less clear. Symmetric DPSK is known to improve data demodulation robustness to the Doppler and timing uncertainty common in satellite communications [25]. But this does not apply to coherent correlation against a known PSS (or portion thereof) for frequency and time synchronization. Most likely, the differential encoding is meant to offer an additional means for trading off search sensitivity for increased efficiency.

We were unable to identify the SSS as a canonical sequence. Its frequency-domain complex coefficients manifest good autocorrelation properties, but not the constant-amplitude zero autocorrelation of m-sequences or of the Zadoff-Chu sequences used for the PSS in LTE. We suspect the SSS may be a mixture of two scrambled m-sequences, as with the SSS from LTE.

D. Gap to Capacity

It is interesting to examine the Starlink signal structure in terms of its design margins. What balance did its designers strike in trading off data throughput for communications reliability or cost?

1. *Spectral Occupancy*

The 10-MHz guard band between channels reduces Starlink's spectral occupancy to $F_\mathrm{s}/F_\delta = \frac{24}{25}$. Leaving such a wide unused bandwidth between channels, which amounts to over 42 subcarrier intervals, suggests that Starlink intends to activate more than one channel at a time in a given service cell and wishes to keep the costs of UTs low by reducing their sampling rate and RF filtering requirements.

2. *OFDM Symbol Occupancy*

The ratio of the useful symbol interval to to the full OFDM symbol interval is $T/T_\mathrm{sym} = N/(N+N_\mathrm{g}) = \frac{32}{33}$, which reflects a fairly efficient design. Compared to LTE, for which N/N_g ranges from 12.8 (more efficient) to 4 (more margin for delay spread), Starlink's ratio is 32. Clearly, Starlink designers are taking advantage of the low delay spread in the space-to-Earth channel. Even still, $T_\mathrm{g} = N_\mathrm{g}/F_\mathrm{s} = 130$ ns exceeds the worst-case 95% root-mean-square delay spread for the Ku-band, found in [20] to be $T_\mathrm{d} = 108$ ns.

3. *Frame Occupancy*

One can view the frame occupancy as $N_\mathrm{sfd}T_\mathrm{sym}/T_\mathrm{f} = \frac{298}{303.03}$. If one additionally discounts OFDM symbols with index $i \in \{2,3,4,5\}$, which appear to contain header information, then occupancy becomes $\frac{294}{303.03}$. The number of OFDM symbol intervals devoted to synchronization sequences—four every 1.33 ms—is unusually high compared to terrestrial OFDM waveforms. For example, LTE transmits two synchronization sequences once every 5 ms. By bookending each frame with two synchronization sequences, Starlink designers ensure that UTs can perform channel equalization and Doppler (CFO) estimation with unusually high accuracy. This reduces frame occupancy, but bodes well for dual-use of Starlink signals for PNT: the greater fraction of predictable elements in each frame, the longer a PNT-oriented receiver can coherently integrate and thus produce pseudorange and Doppler observables at lower SNR.

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

4. *Channel Occupancy*

Due to the $4F$-wide gutter, the channel occupancy is at most $(N-4)/N = \frac{1020}{1024}$, but is likely somewhat lower: Besides revealing the location of synchronization sequences, the symbol-by-symbol frame-to-frame correlation analysis described in Section G suggests the presence of pilot subcarriers that are intermittently modulated with predictable information symbols.

Another measure of channel occupancy is the subcarrier spacing F. Recall that the number of subcarriers N in F_s must be a power of two for efficient OFDM processing, and that, *ceteris paribus*, d_{OFDM} in (12) rises with increasing N. Could Starlink designers have chosen $N = 2048$ rather than $N = 1024$, thus narrowing F by a factor of two and increasing d_{OFDM} by 1.54%? Likely so: assuming $N_{\text{sync}} = 2^{10}$ (fewer than the samples in the PSS) and SNR = 5 dB (the threshold for 4QAM decoding assuming a benign channel and strong coding), the constraint (15) could be comfortably met for $N = 2048$.

VIII. Conclusions

We have developed and applied a blind signal identification technique to uncover the frequency- and time-domain structure of the Starlink Ku-band downlink signal. We further identified four synchronization sequences that can be used to passively exploit Starlink signals for pseudorange-based positioning, navigation, and timing (PNT), and explicitly evaluated two of these. The results in this paper illuminate the path to use of Starlink signals as a backup to traditional GNSS for PNT.

REFERENCES

[1] T. G. Reid, A. M. Neish, T. Walter, and P. K. Enge, "Broadband LEO constellations for navigation," *Navigation, Journal of the Institute of Navigation*, vol. 65, no. 2, pp. 205–220, 2018.

[2] T. G. R. Reid, T. Walter, P. K. Enge, D. Lawrence, S. Cobb, G. Gutt, M. O'Connor, and D. Whelan, *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*. Wiley-IEEE, 2020, vol. 1, ch. Navigation from Low Earth Orbit: Part 1: Concept, Capability, and Future Promise., pp. 1359–1380.

[3] Z. M. Kassas, *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*. Wiley-IEEE, 2020, vol. 1, ch. Navigation from Low Earth Orbit: Part 2: Models, Implementation, and performance, pp. 1381–1412.

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

[5] P. A. Iannucci and T. E. Humphreys, "Fused low-earth-orbit GNSS," *IEEE Transactions on Aerospace and Electronic Systems*, pp. 1–1, 2022.

[6] M. Neinavaie, J. Khalife, and Z. M. Kassas, "Exploiting Starlink signals for navigation: First results," in *Proceedings of the ION GNSS+ Meeting*, St. Louis, Missouri, Sept. 2021, pp. 2766–2773.

[7] ——, "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, 2022.

[8] J. Khalife, M. Neinavaie, and Z. M. Kassas, "The first carrier phase tracking and positioning results with Starlink LEO satellite signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 2, pp. 1487–1491, 2022.

[9] SpaceX, "Revised SpaceX Gen2 non-geostationary satellite system, Technical Attachment," https://licensing.fcc.gov/myibfs/download.do?attachment_key=12943362, Aug. 2021, SAT-AMD-20210818-00105.

[10] A. Bouzegzi, P. Ciblat, and P. Jallon, "New algorithms for blind recognition of OFDM based systems," *Signal Processing*, vol. 90, no. 3, pp. 900–913, 2010.

[11] A. Gorcin and H. Arslan, "An OFDM signal identification method for wireless communications systems," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 12, pp. 5688–5700, 2015.

[12] M. S. Chaudhari, S. Kumar, R. Gupta, M. Kumar, and S. Majhi, "Design and testbed implementation of blind parameter estimated OFDM receiver," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–11, 2021.

[13] M. L. Psiaki, "Navigation using carrier Doppler shift from a LEO constellation: TRANSIT on steroids," *Navigation, Journal of the Institute of Navigation*, vol. 68, no. 3, pp. 621–641, 2021.

[14] L. Cimini, "Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing," *IEEE transactions on communications*, vol. 33, no. 7, pp. 665–675, 1985.

[15] W. Y. Zou and Y. Wu, "COFDM: an overview," *IEEE transactions on broadcasting*, vol. 41, no. 1, pp. 1–8, 1995.

[16] J. Armstrong, "OFDM for optical communications," *Journal of lightwave technology*, vol. 27, no. 3, pp. 189–204, 2009.

[17] A. Ancora, I. Toufik, A. Bury, and D. Slock, *LTE–The UMTS Long Term Evolution: From Theory to Practice*. Wiley, 2011, vol. 1, ch. 5: Orthogonal Frequency Division Multiple Access (OFDMA), pp. 123–143.

[18] J. Proakis and M. Salehi, *Digital communications 5th Edition*. McGraw-Hill, 2007.

[19] T. Jiang and Y. Wu, "An overview: Peak-to-average power ratio reduction techniques for ofdm signals," *IEEE Transactions on broadcasting*, vol. 54, no. 2, pp. 257–268, 2008.

[20] E. L. Cid, M. G. Sanchez, and A. V. Alejos, "Wideband analysis of the satellite communication channel at Ku-and X-bands," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2787–2790, 2015.

[21] T. Hobiger, D. Piester, and P. Baron, "A correction model of dispersive troposphere delays for the ACES microwave link," *Radio Science*, vol. 48, no. 2, pp. 131–142, 2013.

[22] O. A. Dobre, "Signal identification for emerging intelligent radios: Classical problems and new challenges," *IEEE Instrumentation & Measurement Magazine*, vol. 18, no. 2, pp. 11–18, 2015.

[23] D. Rife and R. Boorstyn, "Single tone parameter estimation from discrete-time observations," *IEEE Transactions on information theory*, vol. 20, no. 5, pp. 591–598, 1974.

[24] E. H. Dinan and B. Jabbari, "Spreading codes for direct sequence cdma and wideband cdma cellular networks," *IEEE communications magazine*, vol. 36, no. 9, pp. 48–54, 1998.

[25] J. Winters, "Differential detection with intersymbol interference and frequency uncertainty," *IEEE Transactions on Communications*, vol. 32, no. 1, pp. 25–33, 1984.

Biographies

Todd E. Humphreys (Member, IEEE; B.S., M.S., Utah State University; Ph.D., Cornell University) holds the Ashley H. Priddy Centennial Professorship in Engineering in the Department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin. He is Director of the Wireless Networking and Communications Group and of the Radionavigation Laboratory, where he specializes in the application of optimal detection

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3268610

and estimation techniques to positioning, navigation, and timing. His awards include the UT Regents' Outstanding Teaching Award (2012), the NSF CAREER Award (2015), the ION Thurlow Award (2015), and the PECASE (NSF, 2019). He is Fellow of the ION and of the RIN.

Peter A. Iannucci (Member, IEEE; B.S., Electrical Engineering Computer Science and Physics, MIT; Ph.D., Networks and Mobile Systems, CSAIL, MIT) is a postdoctoral research fellow in the Radionavigation Laboratory at The University of Texas at Austin. His research interests include collaborative navigation, multi-spectral mapping, and re-purposing broadband Internet satellites for radionavigation.

Zacharias M. Komodromos (Student Member, IEEE; B.S., Electrical Engineering, Iowa State University) is a Ph.D. student in the Department of Electrical and Computer Engineering at The University of Texas at Austin and a member of the Radionavigation Laboratory. His research interests include wireless communications and re-purposing broadband Internet satellites for positioning, navigation, and timing.

Andrew M. Graff (Student Member, IEEE; B.S., M.S., Electrical and Computer Engineering, The University of Texas at Austin) is a Ph.D. student in the Department of Electrical and Computer Engineering at The University of Texas at Austin and a member of the Radionavigation Laboratory. His research interests include estimation theory, wireless signal processing, array processing, and secure and robust sensing. He was a recipient of the 2020 Qualcomm Innovation Fellowship.

Authorized licensed use limited to: Univ of Science and Tech Beijing. Downloaded on July 22,2023 at 09:59:15 UTC from IEEE Xplore. Restrictions apply.
© 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.