

# Characterizing Terrestrial GNSS Interference from Low Earth Orbit

Matthew J. Murrian, Lakshay Narula, and Todd E. Humphreys  
*The University of Texas at Austin, Austin, TX*

## BIOGRAPHIES

Matthew Murrian (BS, Mechanical Engineering, University of Central Florida; MS, Aerospace Engineering, University of Texas at Austin) is a systems engineer for Coherent Technical Services, Inc. and is pursuing a Ph.D. at The University of Texas at Austin in the Radionavigation Laboratory. He specializes in the application of estimation techniques to tracking and navigation, and in software-defined radio development. He previously served as a U.S. Navy submarine officer.

Lakshay Narula (B.Tech., Electronics Engineering, IIT (BHU), India; MS, Electrical Engineering, The University of Texas at Austin) is a Ph.D. candidate with the Department of Electrical and Computer Engineering at The University of Texas at Austin, and a Graduate Research Assistant at the UT Radionavigation Lab. His research interests include application of estimation theory and sensor fusion to all-weather localization and secure perception for automated systems. Lakshay has previously been a visiting student at the Position Location and Navigation (PLAN) Group at University of Calgary, Calgary, AB, Canada, and a GNSS systems engineer at Accord Software & Systems, Bangalore, India. He was a recipient of the 2017 Qualcomm Innovation Fellowship.

Todd Humphreys (BS, MS, Electrical Engineering, Utah State University; PhD, Aerospace Engineering, Cornell University) is an associate professor in the department of Aerospace Engineering and Engineering Mechanics at The University of Texas at Austin, where he directs the Radionavigation Laboratory. He specializes in the application of optimal detection and estimation techniques to secure and robust perception for automated systems and centimeter-accurate location. His awards include The University of Texas Regents' Outstanding Teaching Award (2012), the National Science Foundation CAREER Award (2015), the Institute of Navigation Thurlow Award (2015), and the Presidential Early Career Award for Scientists and Engineers (PECASE, 2019).

## ABSTRACT

Observation of terrestrial GNSS interference (jamming and spoofing) from low-earth orbit (LEO) is a uniquely effective technique for characterizing the scope, strength, and structure of interference and for estimating transmitter locations. Such details are useful for situational awareness, interference deterrence, and for developing interference-hardened GNSS receivers. This paper explores the performance of LEO interference monitoring and presents the results of a two-year study of global interference, with emphasis on a particularly powerful interference source active in Syria during 2018. Via Doppler positioning, the Syrian transmitter is located to within 220 meters, an achievement without precedent in the open literature.

## INTRODUCTION

The years 2017 and 2018 saw unprecedented GNSS interference activity, from the eastern Mediterranean to Norway and Finland [1]. Syria, in particular, emerged as a testbed for electronic warfare capabilities. In April 2018, General Raymond Thomas, commander of U.S. Special Operations Command, referred to the region as “the most aggressive electronic warfare environment on the planet” [2].

Space-based observation of terrestrial GNSS interference offers world-wide coverage. Moreover, sensing in LEO offers sufficient stand-off distance from terrestrial interference sources to permit tracking authentic GNSS signals, allowing precise position, velocity, and timing of a LEO receiver to be determined, which, in turn, aids estimation of interference transmitter locations. A single LEO-based sensor is sufficient to characterize the strength, spectral properties, structural content, and even the location of terrestrial interference sources, provided a Doppler time history can be extracted from some component of the interference signal. Through time- or frequency-difference of arrival techniques, multiple synchronized LEO-based sensors could additionally provide location information for interference sources from which no carrier can be extracted [3], [4].

Spaceborne GNSS sensors have been used for remote sensing via radio occultation [5] and reflectometry [6], [7]. However, despite increasing concern over GNSS signal interference [8]–[11], space-based monitoring of terrestrial GNSS interference has not been previously proposed or studied in the open literature. Moreover, the recent survey of GNSS interference localization techniques in [12] makes no mention of single-receiver Doppler-based localization, whether space-based or not. General time- and frequency-difference-of-arrival (TDOA and FDOA) interference localization has been extensively studied [4], [13], [14], and such techniques have been applied for terrestrial interference localization from geostationary orbit [15]–[17]. Application of T/FDOA for localization from LEO can be viewed as an extension of such demonstrations that enables localization of GNSS interference signals, which can be much weaker. However, interference localization using a single satellite has only been explored in [18], which presents only simulation results that unrealistically assumes perfect-tone interference with a known and constant frequency.

This paper presents the results of a two-year study of terrestrial GNSS interference as observed through a software-defined GNSS receiver operating since February 2017 on the International Space Station (ISS). The so-called FOTON receiver, developed by The University of Texas at Austin and Cornell University, is part of a larger science experiment called GPS Radio Occultation and Ultraviolet Photometry—Colocated (GROUP-C), an unclassified experiment aboard the ISS, part of the Space Test Program—Houston Payload 5 (STP-H5) payload. Serendipitous observations of GNSS interference in the occultation data are an important early result of GROUP-C’s scientific objective to characterize GPS signals in the LEO environment. This paper characterizes the interference signals detected and their effects.

Three levels of FOTON data are available for interference analysis: (1) raw 5.7 Msps IF samples output by the FOTON front-end’s analog-to-digital converter, (2) 100-Hz data-modulation-wiped complex IQ correlation products, and (3) 1-Hz standard GNSS observables [19]. This paper focuses on interference observations extracted from raw IF samples and from 1-Hz standard observables.

This paper makes two primary contributions. First, it introduces the concept and presents an analysis of expected performance for terrestrial GNSS interference monitoring from LEO. Second, it presents the results of a two-year study of global GNSS interference, with emphasis on a powerful interference source active in Syria during 2018.

## LEO INTERFERENCE MONITORING PERFORMANCE

This section explores performance in terms of sensitivity, visit interval, and source location accuracy for GNSS interference monitoring from LEO.

### Sensitivity

*Detection via  $C/N_0$  Monitoring:* A simple and effective interference detection test can be formulated solely from the standard carrier-to-noise density ratio,  $C/N_0$ , produced by a GNSS receiver. In the presence of interference,  $C/N_0$  actually measures the carrier-to-interference-and-noise density ratio, CINR. Let  $C$  be the received authentic signal power for a particular satellite-and-signal combination [e.g., the GPS L1 C/A signal corresponding to pseudo-random number (PRN) code 4],  $N_0$  be the (approximately flat) receiver thermal noise power density near the frequency band of interest, and  $I_0$  be the spectrally-flat-equivalent interference noise power density, whose relationship with the actual interference power spectrum is described in [11]. Then CINR is defined as

$$\text{CINR} \triangleq \frac{C}{N_0 + I_0}$$

When compensated for satellite- and receiver-side antenna gain patterns and for spreading loss along the satellite-to-receiver path, and absent signal blockage, strong scintillation, and “flex-power” satellite power adjustments, CINR variations are primarily driven by multipath, which is characterized by a log-normal distribution [10]. Let  $z$  be a vector of CINR measurements expressed in dB for a particular frequency band, with predictable variations due to antenna gain pattern and spreading loss removed. A hypothesis test for interference can be formulated in terms of the common decrease in the elements of  $z$  due to an increase in  $I_0$ . More precisely, the distribution of  $z$  under the null ( $H_0$ ) and alternate ( $H_1$ ) hypotheses may be modeled as

$$H_0 : z \sim \mathcal{N}(\boldsymbol{\mu}, P) \tag{1a}$$

$$H_1 : z \sim \mathcal{N}(\boldsymbol{\mu} - \delta \mathbf{1}, P) \tag{1b}$$

where  $\boldsymbol{\mu} \in \mathbb{R}^{n_z}$ ,  $P \in \mathbb{R}^{n_z \times n_z}$ ,  $\mathbf{1}$  denotes an all-ones column vector of the same length as  $\boldsymbol{\mu}$ , and  $\delta > 0$  is the amount in dB by which all CINR values drop due to interference under  $H_1$ .

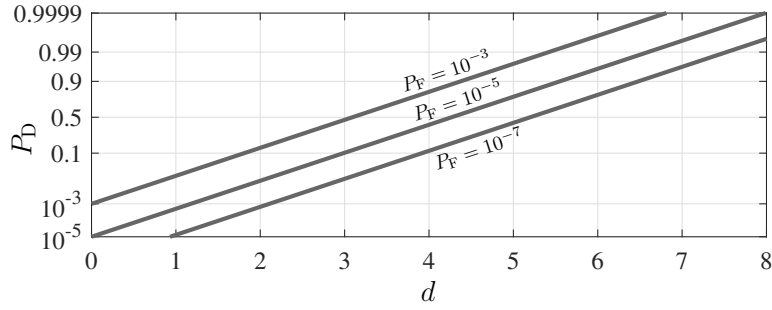


Fig. 1: Detection probability for the test in (2) as a function of  $d$  for three different values of false alarm probability.

The model in (1) conservatively assumes that  $\mathbf{z}$ 's covariance matrix,  $P$ , is identical for  $H_0$  and  $H_1$ . In practice, although the receiver's multipath environment remains unchanged from  $H_0$  to  $H_1$ , interference sources can cause time variations in  $I_0$  that inflate  $P$  in the positive definite sense. But because the magnitude of increase in  $P$  is impossible to know *a priori*, the less-sensitive model presented above is assumed.

The model in (1) is a special case of the general Gaussian problem, for which the likelihood ratio test can be reduced to [20]

$$l(\mathbf{z}) = \mathbf{1}^T P^{-1} \mathbf{z} \underset{H_1}{\overset{H_0}{\geq}} \nu \quad (2)$$

This test is optimal despite  $\delta$  being unknown *a priori* because the sufficient statistic  $l(\mathbf{z})$  is independent of  $\delta$ : the test is uniformly most powerful with respect to  $\delta$ . Note that  $P$  may not be diagonal because the elements of  $\mathbf{z}$  may be correlated through dependence on the spacecraft attitude or because  $\mathbf{z}$  may contain multiple elements for the same satellite-signal pair taken over a sliding window of time.

A linear transformation of a Gaussian vector,  $l(\mathbf{z})$  is itself Gaussian. The performance of the test in (2) can be completely characterized by the normalized distance between the means of  $l(\mathbf{z})$  under  $H_0$  and  $H_1$ :

$$d \triangleq \frac{\mathbb{E}[l|H_0] - \mathbb{E}[l|H_1]}{\sqrt{\text{Var}(l|H_0)}} = \delta \sqrt{\mathbf{1}^T P^{-1} \mathbf{1}} \quad (3)$$

Fig. 1 shows how the performance improves with increasing  $d$ .

If the CINR measurements in  $\mathbf{z}$  are taken at a single epoch of time, and if the effect of multipath on each measurement is only weakly coupled through the spacecraft attitude, then  $P$  may be modeled as diagonal. In the simplest case,  $P = \sigma_z^2 I$  and  $d$  reduces to

$$d = \delta \sqrt{n_z} / \sigma_z \quad (4)$$

For the ISS FOTON receiver, the ISS's extended shape and large solar panels create an unfavorable multipath environment, resulting in a relatively high  $\sigma_z \approx 1.5$  dB. More compact LEO satellites such as the main sounding rocket payload in [19] enjoy  $\sigma_z < 1$  dB.

Approximate LEO interference detection sensitivity in the L1 GNSS band using only CINR measurements can be obtained by letting  $\sigma_z = 1$  dB and  $n_z = 15$ , which assumes single-epoch tests, a horizontally-oriented hemispherical-gain antenna, and full constellations of GPS, Galileo, and BDS III satellites. From (4) and Fig. 1, a drop in CINR of  $\delta > 1.4$  dB is required at  $P_F = 10^{-5}$  to yield  $P_D > 0.9$ . Conservatively assuming that the interference power is spread evenly across the 4-MHz bandwidth covering the most-widely-used civil L1 GNSS signals, then  $I_0 = P_1 - 66$  dBW/Hz, where  $P_1$  is the received interference power in dBW. Assuming  $N_0 = -204$  dBW/Hz, a CINR drop by  $\delta = 1.4$  dB implies  $P_1 = -142$  dBW. Denote spreading loss by  $L$  dB, receiver antenna gain by  $G_r$  dB, and interference source effective isotropic radiated power by  $P_{\text{EIRP}}$  dBW. Then

$$P_{\text{EIRP}} = P_1 - G_r + L \quad (5)$$

Spreading loss at L1 from the surface along the shortest distance to a typical LEO altitude of 400 km is  $L = 148.5$  dB. Then, supposing  $G_r = 3$  dB, the minimum EIRP of an interference source detectable solely from CINR measurements with  $P_F \leq 10^{-5}$  and  $P_D > 0.9$  is approximately  $P_{\text{EIRP}} = 3.5$  dBW.

*Detection via Received Power Monitoring:* Received power monitoring for interference detection is in principle no more sensitive than CINR monitoring, but avoids the requirement to assemble  $z$  only from authentic GNSS signals, which can be difficult under spoofing interference. In fact, received power monitoring requires no tracking of signals at all.

For systems with multi-bit-quantized sampling, total received power  $P_T$  can be estimated from the dynamic gain setting of an automatic gain control (AGC) unit in the front-end digitizer, or directly from the pre-correlation samples in a constant-gain system, assuming sufficient dynamic range to avoid quantization saturation. The hypothesis test model is identical to (1) with  $z = P_T \in \mathbb{R}$  and  $n_z = 1$ . Its performance is governed by (4), with  $\delta$  re-defined as the increase in  $P_T$  under  $H_1$ , and  $\sigma_z^2$  as the variance of the unmodelable components of  $P_T$ .

A low-multipath LEO satellite will exhibit similar  $\sigma_z$  to that of a static terrestrial GNSS receiver, or approximately 0.25 dB for a 4-MHz bandwidth [11]. This implies  $\delta = 1.4$  dB and the remainder of the sensitivity analysis is identical to that of the foregoing section, yielding an approximate minimum detectable EIRP of  $P_{\text{EIRP}} = 3.5$  dBW.

*Detection via Signal Acquisition:* A potent type of GNSS interference, called matched-spectrum interference, allocates its signal power to match the spectrum of a target authentic GNSS signal, thus maximizing  $I_0$  for a receiver tracking that signal [11]. When a matched-spectrum interferer employs a standard GNSS spreading code to achieve the requisite spectrum-matching, it becomes a matched-code interferer, which is extremely effective at denying GNSS service to surrounding receivers at cold-start. However, matched-code interference is itself vulnerable to high-sensitivity detection because a distant receiver can acquire the interference signal just as it does an authentic GNSS signal. Moreover, a receiver in LEO can despread the matched-code interference with the known spreading code, thus extracting a pure carrier tone from whose Doppler time history the source may be geolocated, an example of which will be provided later on.

Consider the sensitivity of matched-code interference detection via signal acquisition from LEO. Denote the LEO receiver's acquisition threshold by  $\nu_a$  dB-Hz. Detection via acquisition is possible when  $P_1 - N_0 > \nu_a$ , with  $P_1$  expressed in dBW and  $N_0$  in dBW/Hz. For the same values of  $N_0$ ,  $G_r$ , and  $L$  assumed previously, and conservatively supposing  $\nu_a = 30$  dB-Hz, the minimum detectable EIRP of a terrestrial interference source is approximately  $P_{\text{EIRP}} = -28.5$  dBW. Thus, detection of matched-code interference by signal acquisition is more than 1000 times more sensitive than detection of unpredictable wideband interference via  $C/N_0$  monitoring or received power monitoring.

## Detection Frequency

A terrestrial interference source is potentially detectable by LEO satellite monitoring several times a day. Consider a LEO satellite in a near-ISS orbit: circular, 400-km altitude, and  $55^\circ$  inclination. Assuming the detection test and parameters given previously, Fig. 2 shows the average number of times per day that such a satellite could detect an interference source as a function of  $P_{\text{EIRP}}$  and latitude. Sources with  $P_{\text{EIRP}} = 3.5$  dBW are detectable only when the satellite's ground track crosses directly through the source's location. As  $P_{\text{EIRP}}$  rises, detection becomes possible even as the satellite ground track passes ever further from the source, leading to a higher frequency of detections. This behavior saturates for  $P_{\text{EIRP}} \geq 17$  dB, yielding a minimum of 3 detections per day for all latitudes within  $75^\circ$  of the equator.

Besides the average detection frequency shown in Fig. 2, it is instructive to consider the maximum time between detections for a given  $P_{\text{EIRP}}$ . Analysis of the ground-track lattice formed by a LEO satellite with the above orbital parameters reveals that the lattice is sufficiently dense to guarantee detection of transmitters with  $P_{\text{EIRP}} > 6.1$  dBW every 4 days, and detection of transmitters with  $P_{\text{EIRP}} > 3.65$  dBW every 17 days, for all latitudes within  $55^\circ$  of the equator.

## Geolocation Accuracy

*TDOA and FDOA:* Time- and frequency-difference-of-arrival techniques have been explored over the past decades for space-based terrestrial interference localization. These techniques require at least two time-synchronized satellites. Reference [17] studied interference localization for the Eutelsat system, presenting theoretical models and real-world campaigns assessing the performance of combined FDOA and TDOA techniques. Accuracies from tens to hundreds of km were theorized and demonstrated. The authors identified satellite ephemeris errors as the dominant source of location error.

In [16], TDOA-based interference localization was analyzed for the scenario of three geostationary satellites able to simultaneously observe the interfering signal. The analysis showed that localization accuracy is improved by increased

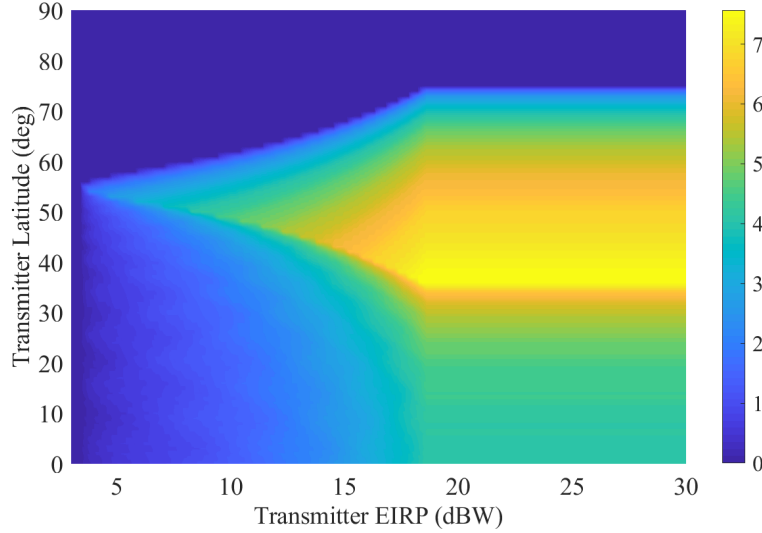


Fig. 2: Number of times per day that a LEO satellite on a circular,  $55^\circ$  inclination, 400-km altitude orbit could detect a given terrestrial transmitter as a function of the transmitter's  $P_{\text{EIRP}}$  and absolute-value latitude, averaged over a 30-day interval.

orbital spacing between the observing satellites and by reduced TDOA measurement error. In this scenario, a transmitter at a latitude greater than  $40^\circ$  can be localized to 2 km (one sigma) with a satellite spacing of  $2^\circ$  if the TDOA measurements have a standard deviation of less than 3.88 ns. Alternatively, a satellite spacing of  $30^\circ$  would yield the same location precision for TDOA measurements of less than  $0.832 \mu\text{s}$  standard deviation.

Joint TDOA/FDOA localization from two LEO satellites was studied in [21]. It was shown that two LEO satellites flying in parallel formation could provide on the order of 1 km (95%) localization from an orbital altitude of 800 km, with 50 km inter-satellite baseline, TDOA measurement errors of 10 ns, and FDOA measurement errors of 4 Hz for signals centered at  $f_c = 3$  GHz. It was also shown that localization accuracy improves with reduced orbital altitudes. One can adapt the analysis in [21] to the problem of localizing interference sources at an arbitrary frequency  $f_i$  by assuming similarly-sized TDOA measurement errors but FDOA measurement errors reduced by the factor  $\frac{f_i}{f_c}$ . For GNSS signals at the L1 frequency, and an orbital altitude of 400 km, better than 1 km (95%) localization might be expected.

*Single-satellite-based transmitter geolocation:* Assuming a carrier can be extracted from an interference signal, single-satellite-based transmitter geolocation is possible from Doppler measurements alone. Consider the following measurement model for the Doppler frequency of a static transmitter as observed by a moving receiver. In this expression,  $c$  is the speed of light;  $\lambda$  is the carrier wavelength at GPS L1;  $\hat{r}_G$  is the unit vector pointing from the transmitter to receiver;  $\mathbf{v}_R$  is receiver velocity and  $\delta\dot{t}_R$  is the receiver clock frequency error, both at the time of signal receipt;  $\delta\dot{t}_T$  is the transmitter clock frequency error at the time of signal transmission; and  $w$  is an error term for thermal noise and other unmodeled effects (e.g., ionospheric and tropospheric delay rates).

$$f_D = \left(\frac{1}{\lambda}\right) \hat{r}_G^T \mathbf{v}_R - \frac{c}{\lambda} (\delta\dot{t}_R - \delta\dot{t}_T [1 - \delta\dot{t}_R]) + w \quad (6)$$

Suppose  $\mathbf{v}_R$  and  $\delta\dot{t}_R$  are known (e.g., measured by an onboard GNSS receiver). The remaining unknowns are transmitter position,  $\mathbf{r}_T$ , which is embedded in  $\hat{r}_G$ , and transmitter clock frequency error  $\delta\dot{t}_T$ . Assuming a static transmitter, position is modeled as an unknown constant. Transmitter clock frequency error can be modeled as a random walk process

$$\delta\dot{t}_T(t_{k+1}) = \delta\dot{t}_T(t_k) + v(k)$$

where  $v(k)$  is discrete-time white zero-mean Gaussian noise. The variance of  $v(k)$ , expressed in sec/sec, can be written in terms of  $\Delta t \triangleq t_{k+1} - t_k$  and a clock stability parameter  $h_{-2}$ :  $\sigma_v^2 = 2\pi^2 h_{-2} \Delta t$  [22].

TABLE I: Results of Monte Carlo simulations for single-pass geolocation for a transmitter clock of various qualities. Semi-major and semi-minor axes are of the 95% horizontal error ellipse, in meters.

Clock Quality	$h_{-2}$	Semi-major Axis	Semi-minor Axis
Low-quality TCXO	$1 \times 10^{-20}$	118609	3625
TCXO	$2.9 \times 10^{-21}$	78262	1897
Low-quality OCXO	$3 \times 10^{-23}$	7954	151
OCXO	$3 \times 10^{-25}$	794	15

It should be noted that a transmitter could introduce arbitrary variations in carrier frequency, e.g., frequency modulation, frequency hopping, etc. Such complex behaviors, if not discovered and appropriately modeled, could confound geolocation efforts. Here, it is assumed that a nominally constant carrier frequency is intended by the transmitter and that it is operating in steady-state conditions without any significant events. Specifically, abrupt oscillator frequency steps and ramps will generally only occur during equipment warm-up or due to temperature changes. Temperature changes may occur for any number of reasons: weather changes, wind gusts, change in lighting conditions, personnel access to equipment enclosures, etc.

Using the above Doppler measurement model, a batch optimization problem can be formulated for estimation of  $r_T$ , which is embedded in  $\hat{r}_G$ , and transmitter clock frequency error  $\delta\dot{t}_T$ . Linearization of the measurement model is straightforward, permitting standard application of nonlinear least squares estimation [23].

Where Doppler measurements from multiple satellite passes (observations of the same transmitter on subsequent orbits) are used, the unknown state should be augmented to include a constant Doppler offset for each pass. Measurements from multiple signals observed simultaneously from the transmitter can be used but their mutual correlation must be considered. Analysis of interference data collected from the ISS showed correlated errors between signals to be large in comparison to independent errors (in the case of the interference source observed in Syria). In this case, the marginal benefit of using multiple signals was small at the expense of substantial additional computational burden. Instead, if independent errors are assumed to be zero mean (as in the case of thermal noise) and the true Doppler of each signal can be assumed identical then measurements from multiple signals can be averaged to produce a single measurement with reduced noise. Consider that, say,  $C/N_0$  could be used to combine measurements through a weighted average. This technique of combining measurements enjoys the marginal benefit of using additional signals but with a minimal impact on computational burden. Error modeling is also simplified as mutual correlation no longer needs to be considered.

Assuming otherwise steady-state conditions, the quality of the transmitter clock oscillator will still have a noticeable effect on phase stability and, therefore, Doppler measurement errors. The impact of clock oscillator quality on geolocation accuracy has been analyzed through Monte Carlo simulation for statistical models representative of four clock qualities ranging between a low-quality TCXO and a laboratory-grade OCXO.

For each of the four clock oscillator qualities, 1000 Monte Carlo simulations were run. Each simulation was based on the real-world interference observed in Syria on day 144 of 2018. The true transmitter location was simulated at 35.4N latitude, 35.95E longitude, 48m altitude. The simulated trajectory was that of the ISS-installed FOTON receiver during a period of that same interference observation interval; 8.7 seconds in duration, 20 Hz measurement rate, with 64.115 km of total receiver displacement. A truth Doppler time history was generated based on this scenario. For each instance of the Monte Carlo simulation, a realization of a Doppler error random process was then generated and added to the truth Doppler. Doppler error was modeled as a random walk process;  $x_e(k+1) = x_e(k) + v(k)$  where  $v(k)$  is drawn at each time from  $\mathcal{N}(0, Q_{2,2})$ .  $x_e(0)$  was initialized to 0 for all simulations.

Table I shows that transmitter clock stability has a large effect on single-pass geolocation accuracy. It can also be seen that the error ellipse is highly eccentric. Note that the semi-minor axis will be largely oriented in the direction of satellite motion from the perspective of the transmitter; e.g., if the satellite is moving West to East then transmitter location will be best resolved in that direction. It follows that additional satellite passes provide the most benefit when they geometrically dissimilar (relative to the transmitter) to previous passes.

## ANALYSIS OF INTERFERENCE FROM SYRIA

This section presents an analysis of a particular interference source active on the east coast of the Mediterranean Sea during the two years of this paper’s study. The analysis illustrates the techniques that can be applied generally to study GNSS interference sources from LEO.



Fig. 3: Ground tracks for interference-affected captures on days 74, 144, and 151 of 2018. Each capture spans approximately 70 seconds.

Ground processing of FOTON’s raw IF samples using The University of Texas’s latest software-defined GNSS receiver [24] enabled analysis and tracking of all radio frequency signals near GPS L1 and L2. Particularly strong interference signals captured on three days in the first half of 2018 along the ground tracks shown in Fig. 3 exhibited the following characteristics:

- False GPS L1 C/A signals with spreading codes from 1 to 32 were present in the data.
- All false signals spread by the GPS L1 C/A spreading codes exhibited a nearly common and constant carrier frequency near GPS L1.
- No discernible navigation data were modulated on the false GPS L1 signals, rendering them ineffective at spoofing, but particularly effective at denying GPS service (jamming).
- No false Galileo E1 signals were detected.
- Civil GPS signals at L2 were subject to narrowband interference, but were not spoofed as on L1.
- The false signals at L1 exhibited unexplained fading and spectral characteristics.
- The interference at L1 caused approximately 6 dB of  $C/N_0$  degradation of authentic GNSS signals for a narrowband ( $\sim 3$  MHz) receiver at a distance of 1340 km.

**Power Spectral Characteristics**

Figs. 4 through 7 illustrate the spectral characteristics, IQ profiles, and Doppler history for interference captured on days 74, 144, and 151 of 2018.

**Transmitter EIRP**

The drop in  $C/N_0$  observed at the ISS when 1340 km from the source was approximately 6 dB. Assume that the interference acts as multi-access interference, whose spectral density is  $I_0 = (2/3)P_1T_C$  [11], where  $P_1$  is the received interference power and  $T_C = 1023^{-1}$  ms is the GPS L1 C/A spreading code chip interval. Then the carrier-power-to-noise-plus-interference-density ratio is

$$CINR = \frac{C}{N_0 + I_0}$$

Assuming  $N_0 = -204$  dBW/Hz, a drop by 6 dB implies  $P_1 = -137.4$  dBW. Removing the 3 dB added by the received antenna, the total interference power impinging on a 0 dBi antenna at the location of the ISS would be approximately -140 dBW.

The spreading loss at L1 for a distance of 1340 km is 159 dB. Thus, the EIRP of the interference source is

$$P_{EIRP} = -140 + 159 \approx 20 \text{ dBW}$$

which implies a 100-W transmitter.

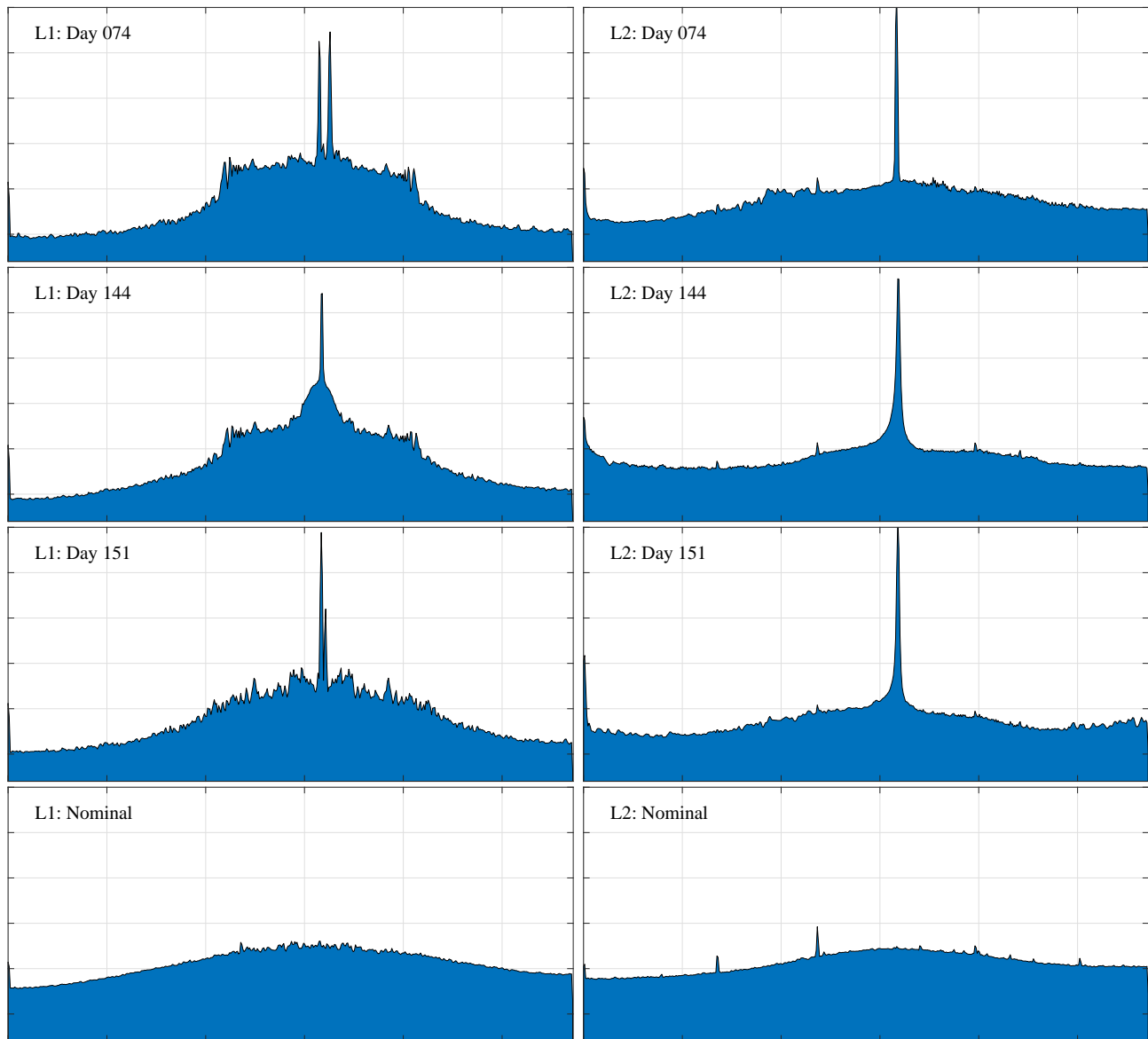


Fig. 4: Power spectra centered near the GPS L1 (left column) and L2 (right column) frequencies from interference-affected data captured on days 74, 144, and 151 of 2018 (top three rows), and from nominal data captured on day 158 of 2018 (bottom row). The frequency span is approximately 3 MHz wide, scaled linearly with 0.5 MHz divisions. All ordinate axes are in dB and scaled equivalently for ease of comparison. Spectra are estimated by Welch's method [25] from 1-second data intervals with a 5.6-kHz frequency resolution.

### Source Localization

Analysis of raw IF data captured on days 74, 144, and 151 of 2018 revealed strong GNSS interference sources in both GPS L1 and L2 frequencies. GPS L1 contained structured interference bearing a carrier (nominally centered at GPS L1), GPS L1 C/A spreading code, and no apparent BPSK symbols. Close comparison of each spreading code offered evidence of a common clock but the potential for independently controlled carrier frequency. Specifically, a comparison of post-fit Doppler measurement residuals showed high error correlation between each PRN channel. Independently controlled carrier frequency was evidenced by infrequent occasions of constant Doppler offsets between PRN channels, but with continued high error correlation. The absence of BPSK symbols on these PRN channels of structured interference provided a convenient and effective method to distinguish between authentic and spoofed signals. Each interference channel was observed to be aligned with respect to spreading code start time. While some authentic GPS L1 C/A signals were effectively jammed, the majority of authentic signals were still trackable owing

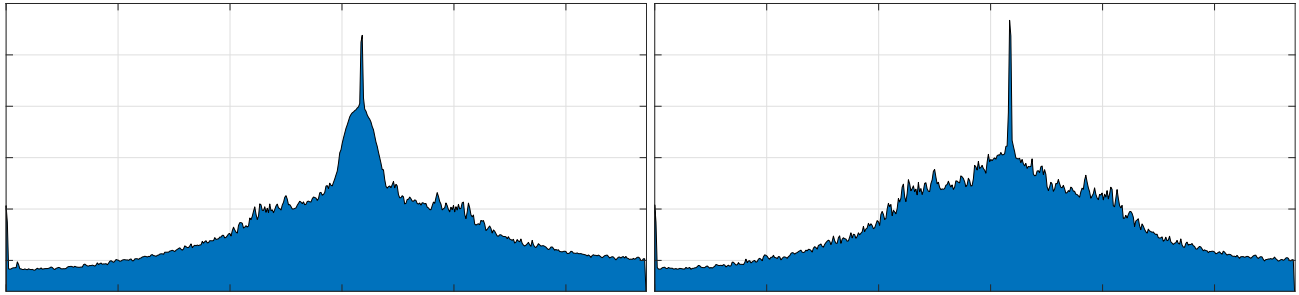


Fig. 5: Power spectra near L1 for the day 144 capture showing maximum (left) and minimum (right) phases of the waxing and waning wideband ( $\sim 0.25$  MHz) central interference prominence. The prominence oscillates with a period of approximately 5 seconds. The L1: Day 144 plot in Fig. 4 catches the prominence waning two seconds after the maximum shown in the top plot above.

to sufficient spreading code start time misalignment at the receiver. Additionally, other constellations and signal types were unaffected by this interference source. Thus, a receiver navigation solution could still be formed despite GPS L1 and L2 interference.

A receiver navigation solution was first estimated on days 74, 144, and 151 of 2018 using an Extended Kalman Filter with pseudorange and carrier-derived Doppler measurements. A nearly-constant acceleration dynamics model was used to propagate the receiver state estimate between measurement updates. With these time histories of receiver state treated as fixed priors, a batch estimator for interference source position and clock bias was then formulated using observed interference Doppler as measurements. It was assumed that the interference source observed on all three days originated from the same transmitter and that the transmitter was stationary. These assumptions allowed multiple days of Doppler measurements, collected on non-repeating ground-tracks, to be combined to form an observable and better constrained estimate. If these assumptions were untrue, they could be expected to manifest in post-fit measurement residuals. Consistent with the assumption of a stationary transmitter, transmitter altitude was assumed to be near ground-level and was included as a pseudo-measurement. Additionally, a quasi-constant transmitter frequency was assumed during each capture. Comparing transmitter frequency estimates between captures revealed nearly identical values; this provided evidence to support the assumption that the same transmitter was being observed. Transmitter frequency was also evaluated with a quasi-constant ramp model but the quasi-constant frequency model was concluded to be sufficient.

Fig. 7 shows time histories of Doppler and post-fit residuals for false PRN 10 collected on day 144. The standard deviation of post-fit residuals is 2.3 Hz. Fig. 8 shows the estimated position of a single interference source, whose location, determined to better than 220 meters (95%), coincides with an airbase in Syria.

### Implications for Civil GNSS

Assuming standard free-space path loss and a uniform transmitter antenna pattern, for a commercial airliner passing near the transmitter at an altitude of  $\sim 10$  km, the received power into a 0 dBi antenna would be -86 dBW, assuming the interference signals are attenuated by 10 dB due to the aircraft's fuselage. This would imply an interference-to-authentic signal power ratio of 49 dB, which would cause a drop in  $C/N_0$  of approximately 39 dB, enough to deny GNSS service to the aircraft.

### GLOBAL INTERFERENCE SURVEY VIA RECEIVER-REPORTED $C/N_0$

While the raw IF data captures from the ISS FOTON receiver enable detailed monitoring of GNSS interference signals and their structure, such captures are limited to short durations and have limited availability. In contrast, the 1-Hz standard GNSS observables and 100-Hz data-wiped complex IQ correlation products have been logged nearly continuously over the last two years. These data facilitate a world-wide analysis of strong GPS interference, as well as provide insight in to persistent/intermittent nature of interference sources.

The carrier power  $C$  of an authentic signal is modeled as  $C(j, f, r_{sr}, z_s, z_r)$ , where  $j$  is the GPS SV ID,  $f$  is the frequency band (L1 or L2),  $r_{sr}$  is the range between the GPS satellite antenna and the ISS FOTON antenna,  $z_s$  is the angle between the GPS satellite boresight direction and the direction to the ISS antenna (satellite off-boresight angle), and  $z_r$  is the angle between the ISS antenna boresight direction and the direction to the GPS satellite (receiver off-boresight angle). Based on the receiver-reported CINR, a hypothesis test must detect whether ( $H_1$ ) or not ( $H_0$ )

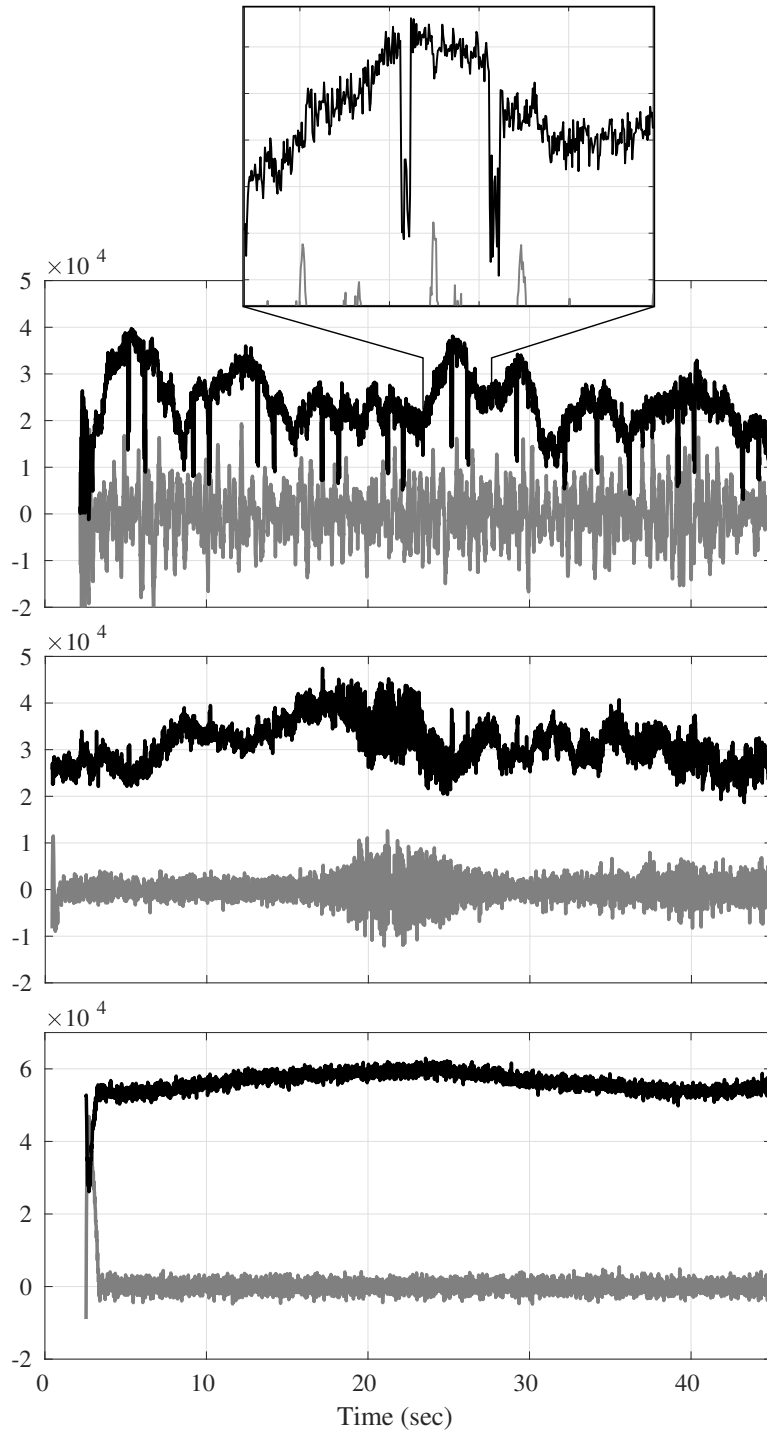


Fig. 6: In-phase (black) and quadrature (gray) 10-ms accumulation time histories for the strongest false signal from the day 74 capture (top), the strongest authentic signal from the day 74 capture (middle), and the strongest signal from the day 158 nominal capture (bottom). The inset on the top panel shows an amplified view of two sudden amplitude fades in the received false signal. The maximum carrier-to-noise ratio  $C/N_0$  over the intervals shown are, from the top, 42.5, 46.8, and 52.5 dB-Hz.

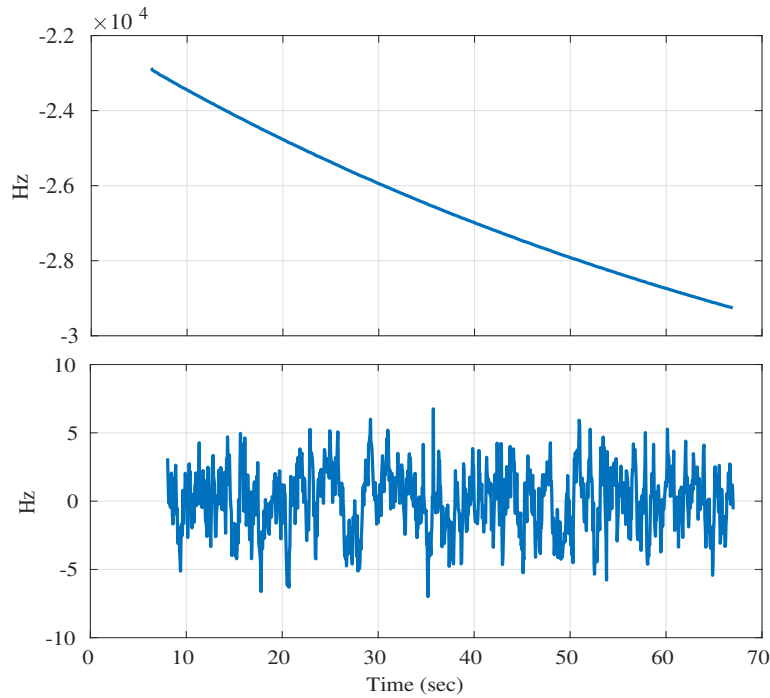


Fig. 7: Top: Doppler time history corresponding to the false PRN 10 signal from the day 144 capture. Bottom: Post-fit residuals of the Doppler time history assuming the estimated transmitter location and clock rate offset. The standard deviation of the post-fit residuals is 2.3 Hz.



Fig. 8: Estimated transmitter location overlaid on 95 and 99% horizontal error ellipses. The location is coincident with an airbase on the coast of Syria.

the receiver is experiencing interference. Under a given  $P_F$ , this requires that the statistics  $\mathbb{E}[l|H_0]$  and  $\text{Var}(l|H_0)$  be known. This section assumes that the ISS receiver is in an interference-free condition when the ISS is over deep ocean bodies, and such data are treated as being reported under  $H_0$ .

To isolate the variations in reported CINR due to interference, the data are first pre-processed to eliminate the predictable sources of carrier power variation. First, the dependence of  $C$  on  $r_{sr}$  is removed by compensating for the free space path loss.

$$\hat{C}(j, f, z_s, z_r) = C(j, f, r_{sr}, z_s, z_r) \times \left( \frac{4\pi r_{sr} f}{c} \right)^2$$

Modeling of interference-free  $C/N_0$  is complicated by the ISS's local multipath environment. The ISS antenna is flanked by solar panels that move with respect to the antenna, causing a non-stationary signal obstruction and multipath

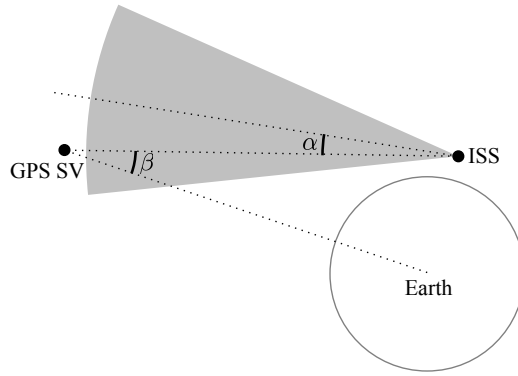


Fig. 9: For receiver off-boresight angle  $\alpha \leq 15^\circ$ , the satellite off-boresight angle  $\beta$  is restricted between  $14.2^\circ \leq \beta \leq 15.2^\circ$

environment. Nevertheless, a window of  $0^\circ$  to  $15^\circ$  off-boresight angles is guaranteed to be free of obstructions, and only the signals received in this window are considered for interference detection in this analysis. This restricts the geometry between GPS satellites and the ISS, such that the satellite off-boresight angle only varies between  $14.2^\circ$  and  $15.2^\circ$  (see Fig. 9). The GPS SV antenna gain pattern can be assumed to be relatively constant over  $\pm 0.5^\circ$ , and thus  $\hat{C}(j, f, z_s, z_r)$  is assumed independent of  $z_s$ .

The mean and variance of ISS-reported range-compensated-CINR values,  $\hat{C}/N_0$ , collected over deep ocean are maintained as control data in a three-dimensional grid of SV ID, frequency band, and receiver off-boresight angle. For a world-wide analysis of GPS interference events, a hypothesis test is performed on the test statistic derived from  $\hat{C}/N_0$  values that fall within the  $0^\circ$  to  $15^\circ$  receiver off-boresight window. The test is performed separately for GPS L1 and L2 frequency since the interference characteristics are frequency dependent. If the reported test statistics falls below  $\mathbb{E}[l|H_0] - 3\sqrt{\text{Var}(l|H_0)}$ , the receiver is declared to be under interference. This threshold honors a  $P_F$  of approximately  $1.35 \times 10^{-3}$ .

Fig. 10 shows the ratio of number of potential interference events recorded at GPS L1 frequency to total number of hypothesis tests performed at each location for the detection threshold mentioned above. As expected, a high ratio of potential interference events is reported to the east of the triangulated location of the Syrian GPS interference (marked as the red dot in Fig. 10). The high value of the statistic suggests that the interference activity in Syria was relatively persistent over the time of data recording on the ISS. Fig. 11 shows the same ratio at GPS L2 frequency. In addition to the expected interference over the Syrian region, Fig. 11 suggests strong ongoing GPS L2 interference over mainland China.

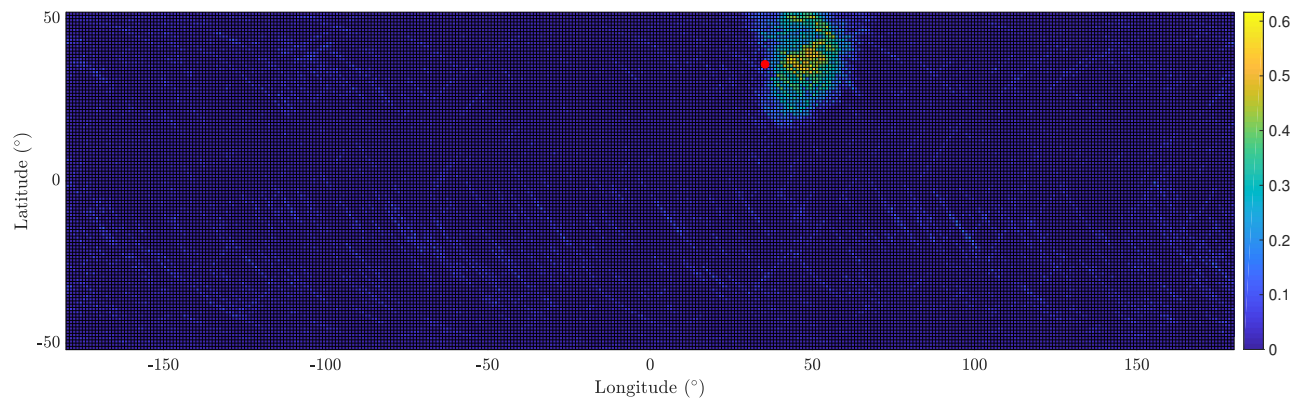


Fig. 10: Ratio of number of potential GPS L1 interference events recorded to total number of hypothesis tests performed. Red dot indicated the estimated origin of the Syrian interference.

It must be noted that the above method of counting potential interference events based on  $C/N_0$  degradation ignores cases where interference might lead to complete loss of track of some or all GPS signals. However, the data from the ISS shows that FOTON does not lose track of GPS signals even when flying by the strong interference source in

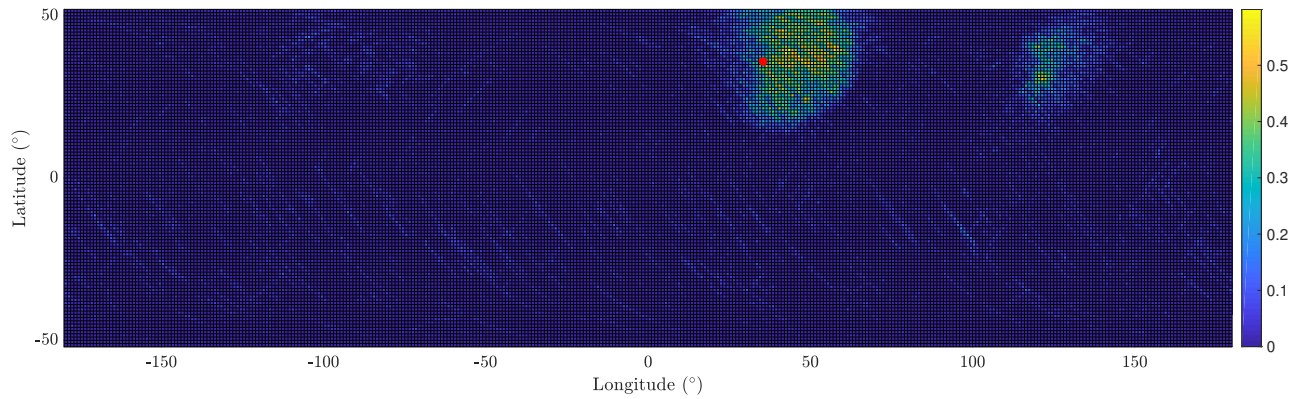


Fig. 11: Ratio of number of potential GPS L2 interference events recorded to total number of hypothesis tests performed. Red dot indicated the estimated origin of the Syrian interference.

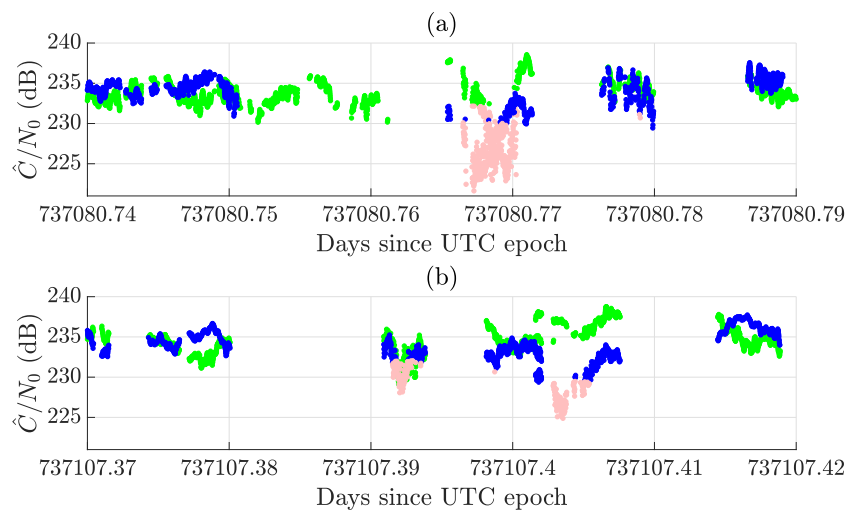


Fig. 12: Time histories of range-compensated receiver-reported CINR as the ISS flies over potential GPS interference zones over Syria and China.

Syria. In fact, the reported CINR over Syria is well above the weakest signal that FOTON is capable of tracking. As a result, it was concluded that in cases where FOTON seems to track few or no GPS signals, it is likely due to some abnormal behavior of the receiver, and not due to a potential interference event.

In addition to the global average analysis summarized in Figs. 10 and 11, it is instructive to examine the time history of receiver reported CINR as a function of time when the ISS flies by the interference hot spots mentioned above. Fig. 12 shows two segments of such time histories for signals within the admissible receiver off-boresight window as the ISS goes over the strong interference regions in Syria (Fig. 12(a)) and China (Fig. 12(b)). Green and blue data points represent interference-free L1 and L2 frequency signals, respectively, while red data points represent epochs at which the receiver is reported to be under interference. Both GPS L1 and L2 are declared under interference in Fig. 12(a) where the ISS flies over the Syria, while only GPS L2 is declared under interference in Fig. 12(b). The brief dip in  $\hat{C}/N_0$  in Fig. 12(b) prior to the major dip over mainland China is in fact caused by the Syrian interference. Gaps in the time histories indicate period with no tracked signals in the admissible off-boresight window.

One might be skeptical about categorizing such drops in reported CINR to be potential interference events, while complete tracking failure events had earlier been attributed to abnormal FOTON behavior. However, during the above drops in reported CINR, it was observed that the carrier-phase measurements generated by FOTON were relatively clean. Carrier-phase is the most sensitive measurement made by the FOTON receiver, and is expected to fall apart earliest in case of any malfunction of the FOTON receiver. As a result, it is believed that such drop in CINR for all tracked signals is most likely explained by intentional/unintentional GPS interference.

## CONCLUSIONS

Low-earth-orbiting instruments capable of receiving signals in GNSS bands are a powerful tool for characterizing GNSS interference emanating from terrestrial sources. Data from one such instrument, the FOTON software-defined GNSS receiver, which has been operational on the International Space Station since February 2017, reveal interesting patterns of GNSS interference. A particularly powerful and constant interference source was active in Syria during 2017 and 2018. Its 100-W (EIRP) transmissions at the GPS L1 frequency contain signals modulated by all 32 GPS L1 C/A spreading codes, but with no data modulation, indicating that the signals' purpose is denial of GNSS service. Via Doppler positioning, the Syrian transmitter was located to within 220 meters, an achievement without precedent in the open literature. A global analysis of carrier-to-noise-density ratio measurements also revealed persistent interference in mainland China.

## ACKNOWLEDGMENTS

This work has been supported by the National Science Foundation under Grant No. 1454474 (CAREER).

## REFERENCES

- [1] C4ADS, "Above us only stars: Exposing GPS spoofing in Russia and Syria," April 2019, <https://c4ads.org/reports>.
- [2] Brimelow, B., "General reveals that US aircraft are being 'disabled' in Syria — the 'most aggressive' electronic warfare environment on Earth," April 2018, <https://goo.gl/9B2NF4>.
- [3] Bhatti, J. and Humphreys, T. E., "Hostile control of ships via false GPS signals: Demonstration and detection," *Navigation*, Vol. 64, No. 1, 2017, pp. 51–66.
- [4] Bhatti, J., *Sensor Deception Detection and Radio-Frequency Emitter Localization*, Ph.D. thesis, The University of Texas at Austin, Aug. 2015.
- [5] Ao, C., Hajj, G., Meehan, T., Dong, D., Iijima, B., Mannucci, A., and Kursinski, E., "Rising and setting GPS occultations by use of open-loop tracking," *Journal of Geophysical Research: Atmospheres (1984–2012)*, Vol. 114, No. D4, 2009.
- [6] Jin, S. and Komjathy, A., "GNSS reflectometry and remote sensing: New objectives and results," *Advances in Space Research*, Vol. 46, No. 2, 2010, pp. 111–117.
- [7] Zavorotny, V. U., Gleason, S., Cardellach, E., and Camps, A., "Tutorial on remote sensing using GNSS bistatic radar of opportunity," *IEEE Geoscience and Remote Sensing Magazine*, Vol. 2, No. 4, 2014, pp. 8–45.
- [8] Psiaki, M. L., Humphreys, T. E., and Stauffer, B., "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," *IEEE Spectrum*, Vol. 53, No. 8, August 2016, pp. 26–53.
- [9] Psiaki, M. L. and Humphreys, T. E., "GNSS Spoofing and Detection," *Proceedings of the IEEE*, Vol. 104, No. 6, 2016, pp. 1258–1270.
- [10] Wesson, K. D., Gross, J. N., Humphreys, T. E., and Evans, B. L., "GNSS Signal Authentication Via Power and Distortion Monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 54, No. 2, April 2018, pp. 739–754.
- [11] Humphreys, T. E., *Springer Handbook of Global Navigation Satellite Systems*, chap. Interference, Springer, 2017, pp. 469–504.
- [12] Dempster, A. G. and Cetin, E., "Interference localization for satellite navigation systems," *Proceedings of the IEEE*, Vol. 104, No. 6, 2016, pp. 1318–1326.
- [13] Griffin, C. and Duck, S., "Interferometric radio-frequency emitter location," *IEE Proceedings-Radar, Sonar and Navigation*, Vol. 149, No. 3, 2002, pp. 153–160.
- [14] Amar, A. and Weiss, A. J., "Localization of narrowband radio emitters based on Doppler frequency shifts," *IEEE Transactions on Signal Processing*, Vol. 56, No. 11, 2008, pp. 5500–5508.
- [15] Smith, W. W. and Steffes, P. G., "Time delay techniques for satellite interference location system," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 25, No. 2, 1989, pp. 224–231.
- [16] Ho, K. and Chan, Y., "Solution and performance analysis of geolocation by TDOA," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 29, No. 4, 1993, pp. 1311–1322.
- [17] Haworth, D., Smith, N., Bardelli, R., and Clement, T., "Interference localization for EUTELSAT satellites—the first european transmitter location system," *International journal of satellite communications*, Vol. 15, No. 4, 1997, pp. 155–183.
- [18] Kalantari, A., Maleki, S., Chatzinotas, S., and Ottersten, B., "Frequency of arrival-based interference localization using a single satellite," *2016 8th Advanced Satellite Multimedia Systems Conference and the 14th Signal Processing for Space Communications Workshop (ASMS/SPSC)*, IEEE, 2016, pp. 1–6.
- [19] Lightsey, E. G., Humphreys, T. E., Bhatti, J. A., Joplin, A. J., O'Hanlon, B. W., and Powell, S. P., "Demonstration of a Space Capable Miniature Dual Frequency GNSS Receiver," *Navigation, Journal of the Institute of Navigation*, Vol. 61, No. 1, 2014, pp. 53–64.
- [20] Trees, H. L. V., *Detection, Estimation, and Modulation Theory*, Wiley, 2001.
- [21] Shilong, W., Jingqing, L., and Liangliang, G., "Joint FDOA and TDOA location algorithm and performance analysis of dual-satellite formations," *2010 2nd International Conference on Signal Processing Systems*, Vol. 2, IEEE, 2010, pp. V2–339.
- [22] Brown, R. G. and Hwang, P. Y., *Introduction to Random Signals and Applied Kalman Filtering*, Wiley, 2012.

- [23] Crassidis, J. L. and Junkins, J. L., *Optimal estimation of dynamic systems*, Chapman and Hall/CRC, 2011.
- [24] Humphreys, T. E., Narula, L., and Murrian, M. J., "Deep urban unaided precise GNSS vehicle positioning," *IEEE Intelligent Transportation Systems Magazine*, 2019, To be published.
- [25] Welch, P., "The use of fast Fourier transform for the estimation of power spectra: a method based on time averaging over short, modified periodograms," *IEEE Transactions on audio and electroacoustics*, Vol. 15, No. 2, 1967, pp. 70–73.