Geolocation of Terrestrial GNSS Spoofing Signals from Low Earth Orbit

Zachary Clements*, Patrick Ellis†, Mark Psiaki‡, and Todd E. Humphreys*
*Department of Aerospace Engineering and Engineering Mechanics, The University of Texas at Austin
†Spire Global
‡Department of Aerospace and Ocean Engineering, Virginia Tech

BIOGRAPHIES

Zachary Clements (BS, Electrical Engineering, Clemson University) is a graduate student in the department of Aerospace Engineering and Engineering Mechanics at The University of Texas at Austin, and a member of the UT Radionavigation Laboratory. His research interests include GNSS signal processing, spoofing detection, software-defined radio, and emitter geolocation.

Patrick Ellis is the Director of the Advanced Signal Processing Group at Spire Global, Inc., where he leads an international team of researchers dedicated towards utilizing LEO satellites for passive signal inferences. He holds a Ph.D. and M.S. in Electrical Engineering from the University of California at Santa Cruz and specializes in the development of statistically-based state estimation algorithms and systems for aPNT, localization, tracking, and geolocation purposes.

Mark L. Psiaki is Professor and Kevin T. Crofton Faculty Chair of Aerospace and Ocean Engineering at Virginia Tech. He is also Professor Emeritus of Mechanical and Aerospace Engineering at Cornell University. He holds a Ph.D. in Mechanical and Aerospace Engineering from Princeton University. He is a Fellow of both the ION and the AIAA. His research interests are in the areas of navigation, spacecraft attitude and orbit determination, remote sensing, and general methods for estimation, filtering, and detection.

Todd Humphreys (BS, MS, Electrical Engineering, Utah State University; PhD, Aerospace Engineering, Cornell University) is a 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 problems in secure, collaborative, and high-integrity perception, with an emphasis on navigation, collision avoidance, and precise timing. 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), the Qualcomm Innovation Fellowship (2017), the Walter Fried Award (2012, 2018), and the Presidential Early Career Award for Scientists and Engineers (PECASE, 2019). He is a Fellow of the Institute of Navigation and of the Royal Institute of Navigation.

ABSTRACT

This paper explores single-satellite single-pass geolocation of terrestrial Global Navigation Satellite System (GNSS) spoofing signals from Low Earth Orbit (LEO). GNSS spoofers transmit an ensemble of false GNSS signals intending that the victim(s) receiver will accept them as authentic signals and infer a false position fix and/or a clock offset. Receivers in LEO provide a unique opportunity to detect, classify, and geolocate terrestrial GNSS interference. Single-satellite-based transmitter geolocation is possible from Doppler measurements alone, assuming a carrier can be extracted from an interference signal. There are proven single-satellite Doppler-based geolocation algorithms, but they only apply to emitters transmitting at a constant frequency. By contrast, GNSS spoofers transmit signals whose carrier frequency contains an unknown time-varying frequency component that imitates the Doppler corresponding to each individual spoofed navigation satellite. This paper develops a single-pass single-satellite technique that removes the unknown time-varying frequency component added by GNSS spoofers so that a Doppler (range-rate) time history can be extracted for geolocation. It is shown that the true range rate between the terrestrial spoofer and LEO-based receiver manifests in the spoofed receiver clock offset rate estimate. Monte Carlo simulations are developed that investigate how transmitter motion, transmitter clock offset rate, and spoofed clock offset rate affect geolocation accuracy. The proposed method is validated by simulating the reception of terrestrial GNSS spoofing signals on a LEO-based receiver and achieving under 10 km accuracy. Additionally, recent real-world GPS spoofing signals captured by a LEO-based receiver are analyzed.

Preprint of the 2022 ION GNSS+ Conference Denver, CO, Sept. 19-23, 2022

INTRODUCTION

Global Navigation Satellite Systems (GNSS) such as GPS provide meter-accurate positioning while offering global accessibility, all-weather operation, and radio-silent reception. However, GNSS is fragile: its service is easily denied by jammers or deceived by spoofers. GNSS spoofers are becoming easily-accessible and low-cost, threatening GNSS-reliant systems [1]–[3]. Scientific satellites have received spoofing-like GPS interference over Ukraine and the Middle East [4], [5]. GNSS interference is not limited to military applications: the civilian maritime and airline industries have frequent encounters widespread GNSS jamming and spoofing. Corrupted Automatic Identification System (AIS) and Automatic Dependent Surveillance-Broadcast (ADS-B) messages from vehicles are frequently reported [6]. GNSS interference manifests as irregularities in AIS and ADS-B reports as these systems derive their position from GNSS. Ships near in Shanghai have fallen as victims to GNSS spoofing [7].

Fortunately, extensive progress in on-board GNSS spoofing detection and mitigation has recently been made [8]. Reliable spoofing detection techniques even exist for challenging environments such as dynamic platforms in urban areas where strong multipath and in-band noise are common [9]–[13]. Although reliable spoofing detection techniques exist, GNSS security can be further enhanced by accurately geolocating the source of interference.

Detecting and geolocating radio frequency (RF) signals is a coveted capability as it facilitates search-and-rescue, tracking, and spectrum monitoring. LEO-based receivers are a proven asset for detecting, classifying, and geolocating terrestrial GNSS interference [14]. Emitter geolocation from Low Earth Orbit (LEO) offers worldwide coverage with a frequent refresh rate, making it possible to maintain a common operating picture of terrestrial emitters, e.g. GNSS jammers and spoofers. Moreover, LEO satellites' stand-off distance from terrestrial interference sources permits tracking authentic GNSS signals, enabling precise time-tagged data captures from time-synchronized LEO-based receivers and precise orbit determination.

General stationary emitter localization with multiple receivers has been extensively studied [15], [16]. Time-synchronized receivers can exploit time- and frequency-difference of arrival (T/FDOA) to estimate the emitter location. In T/FDOA techniques, the differential Doppler and differential delay are first estimated, followed by the estimation of transmitter location. Another multi-satellite technique is direct geolocation, which is a single-step search over a geographical grid enabling estimation of the transmitter location directly from the observed signals [17]. Direct geolocation outperforms the two-step method in low signal-to-noise ratio (SNR) environments and short data segment scenarios.

Geolocation of moving emitters with multiple receivers using T/FDOA measurements is explored in [18]–[21]. Geolocating moving transmitters becomes challenging as the transmitter's unknown velocity induces a Doppler shift. Rather than only estimating the position as in the stationary case, the velocity must also be estimated. Accurately geolocating a moving transmitter with a single receiver is impossible [22].

Several commercial enterprises such as Spire Global and Hawkeye360 have dedicated constellations for spectrum monitoring and interference geolocation efforts. These LEO constellations offer distributed time-synchronized LEO-based receivers whose data can provide accurate emitter geolocation. However, planning simultaneous multi-satellite captures to enable T/FDOA-based and direct geolocation can be difficult and expensive. This paper focuses on single-satellite platforms.

Single-satellite interference source geolocation accuracy is dependent on the transmitted waveform. Accurately locating emitters with arbitrary waveforms using a single LEO receiver is impossible in general: if the signal's carrier cannot be tracked, only coarse received-signal-strength (RSS) techniques can be applied for localization. However, if a carrier can be extracted, accurate single-satellite-based emitter geolocation is possible from Doppler measurements alone [23], [24].

The underlying technique of Doppler-based positioning was pioneered by research scientists at Johns Hopkins Applied Physics Laboratory, who solved the orbit of Sputnik-1 by analyzing the Doppler shift of the satellite's transmitted signal in 1957. Following this, the United States Navy deployed the first satellite-based geopositioning system (known as Transit) in 1960, which adopted this technique. The Transit satellites transmitted carrier frequencies at 150 and 400 MHz. Ground stations constantly looked for these transmissions and calculated the received Doppler. From Doppler curve(s), an initial estimated ground station position, and the transmitted orbit parameters, a least-squares estimator could produce a location estimate with errors as small as 100 meters [25]. In recent developments, a new global navigation concept is studied that relies on carrier Doppler shift measurements from a large LEO constellation [26].

A Doppler-based positioning technique much like that of Transit can be reversed for LEO-based emitter geolocation. If a LEO-based receiver can extract a Doppler history from an emitter, a geolocation estimate can be made. Doppler-based geolocation algorithms are effective because the range-rate between LEO-based receivers and terrestrial emitters varies rapidly

over short captures. Performance bounds and error characterization for LEO-based single-satellite Doppler geolocation are presented in [27], [28].

Doppler-based emitter geolocation with a single LEO-based receiver was also proven by the University of Texas at Austin Radionavigation Lab (RNL). In collaboration with Cornell University, the RNL developed a software-defined multi-frequency GNSS receiver called FOTON that has been operating on the International Space Station (ISS) since 2017 [29]. Although emitter geolocation was not its original purpose, this single software-defined receiver has proven effective at locating emitters. Its data have been used to locate a powerful 70-watt matched-code jammer operating in Syria to better than 300 meters [30]. Localizing the emitter in Syria hinged on two lucky breaks: (1) the emitter was transmitting a GPS-like signal from which a Doppler history could be extracted, and (2) the emitter's signals had quasi-cosntant carrier frequency as transmitted. In addition to exploiting received Doppler, this work took into account transmitter clock rate errors to refine the geolocation estimate.

One of the key assumptions of the prior work is that the emitter transmits at a quasi-constant carrier frequency. The prior Doppler-based geolocation techniques falter if a transmitter introduces any significant level of complexity to carrier-phase behavior, such as frequency modulation or clock dithering. Assuming a nominally-constant transmitter carrier frequency is appropriate for GNSS matched-code jammers, but is fallacious for GNSS spoofers. GNSS spoofers do not transmit at a constant center frequency: they add an extra unknown time-varying frequency component to the spoofed signals that imitate the range-rate between spoofed GNSS satellite and the intend spoofed location. The extra unknown time-varying frequency component renders raw observed Doppler-based geolocation ineffective.

The range-rate between the LEO receiver and the terrestrial spoofer is common for each spoofed signal. If all of the spoofing signals are processed, a GNSS receiver's navigation solution estimator lumps any range-rate term that is common across all satellites into the receiver clock offset rate. Therefore, the time history of the receiver clock offset rate can be used for geolocation because it contains the range-rate between LEO receiver and terrestrial spoofer. Embedded in the range-rate time history is information about the transmitter's position.

This paper makes three primary contributions. First, this paper introduces a methodology to remove the unknown time-varying frequency component added by the GNSS spoofer, allowing the true range-rate between LEO-based spoofer and terrestrial spoofer to be extracted for geolocation. Second, the receiver clock rate offset time history can be corrupted by transmitter motion, transmitter clock rate error, and the spoofing induced receiver clock rate offset. Monte Carlo simulations are developed that investigate how these parameters affect geolocation accuracy. Additionally, the proposed method is validated by simulating the reception of a terrestrial GNSS spoofing signals on a LEO-based receiver. Lastly, recent real-world GPS spoofing signals captured by a LEO-based receiver are analyzed.

MEASUREMENT MODEL

This paper's solution is meant for single-pass, single-satellite captures of terrestrial GNSS spoofers. Doppler-based methods are an effective way of performing accurate single-satellite transmitter geolocation when a range-rate can be extracted. The Doppler measurement can be derived from the carrier phase measurement. This section builds on work found in [31], where the full derivation of Doppler can be found. It presents the received Doppler measurement model utilizing the aforementioned carrier phase derivation and develops a new Doppler measurement model for receiving GNSS spoofing signals on a quickly-moving platform, e.g., a LEO-based GNSS receiver.

Doppler Measurement for Authentic Signals

Any model of GNSS measurements must take into account three "clocks" for keeping track of time: (1) true time t, (2) receiver time t_{r}, and (3) satellite time t_{s}. True time can be considered as equivalent to GPS time. Receiver time refers to the time system of the receiver clock and and satellite time refers to the time system of the satellite clock. The relationship between true time t, receiver time t_{r} and the receiver clock offset $\delta t_{\mathrm{r}}(t_{\mathrm{r}})$, expressed as a function of t_{r} is

$$t = t_{\mathrm{r}} - \delta t_{\mathrm{r}}(t_{\mathrm{r}}) \tag{1}$$

The relationship between true time t, satellite time t_{s} and satellite clock offset $\delta t_{\mathrm{s}}(t)$ is

$$t = t_{\mathrm{s}} - \delta t_{\mathrm{s}}(t) \tag{2}$$

The two fundamental GNSS measurements, pseudorange and carrier phase, incorporate these timing models. These measurements are fed into a position, velocity, and timing (PVT) estimator whose goal is to estimate the state $\boldsymbol{x} = [\boldsymbol{r}_{\mathrm{r}}^{\mathsf{T}},\ \delta t_{\mathrm{r}},\ \boldsymbol{v}_{\mathrm{r}}^{\mathsf{T}},\ \delta \dot{t}_{\mathrm{r}}]^{\mathsf{T}}$, where $\boldsymbol{r}_{\mathrm{r}}$ is the receiver position, $\boldsymbol{v}_{\mathrm{r}}$ is the receiver velocity, and $\delta \dot{t}_{\mathrm{r}}$ is the receiver clock offset rate. The GNSS satellite's clock error is broadcast via the satellite's navigation message. The phenomenon underlying the psuedorange and carrier phase measurements is the "time of flight" of the signal, δt_{TOF}, which requires further timing notation to accurately describe the transmission and reception of alignment features. The notation for timing events in this paper is as follows: t_{r} is the time of reception of the alignment feature in receiver time and $\hat{t}$ is the time of transmission of the alignment feature in true time. The time of reception and time of transmission are related by $\hat{t} = t_{\mathrm{r}} - \delta t_{\mathrm{r}}(t_{\mathrm{r}}) - \delta t_{\mathrm{TOF}}$.

This paper will focus on the carrier phase measurement, since the Doppler measurement follows from it. The measured carrier phase is the difference between a receiver-generated replica of the nominal carrier phase and the received carrier phase. Let λ denote the signal wavelength, c the speed of light, $\Delta r(t_{\mathrm{r}}, \delta t_{\mathrm{TOF}})$ the range between the receiver at t_{r} and GNSS satellite at $\hat{t}$, ϕ_0 the initial phase of the receiver, ψ_0 the initial phase of the transmitter, I_ϕ the excess delay due to the ionosphere, T the excess delay due to the troposphere, and w_ϕ the measurement noise. The carrier phase measurement, denoted as $\lambda\phi(t_{\mathrm{r}})$, is then modeled as

$$\lambda\phi(t_{\mathrm{r}}) = \Delta r(t_{\mathrm{r}}, \delta t_{\mathrm{TOF}}) + c[\delta t_{\mathrm{r}}(t_{\mathrm{r}}) - \delta t_{\mathrm{s}}(\hat{t})] + \lambda(\phi_0 - \psi_0) + I_\phi + T + \lambda w_\phi(t_{\mathrm{r}}) \tag{3}$$

The Doppler measurement is related to the received carrier phase through a time derivative with respect to t_{r}:

$$f_{\mathrm{d}}(t_{\mathrm{r}}) \triangleq -\frac{d\phi(t_{\mathrm{r}})}{dt_{\mathrm{r}}} = -\frac{1}{\lambda}\frac{d}{dt_{\mathrm{r}}}\left[\Delta r(t_{\mathrm{r}}, \delta t_{\mathrm{TOF}})\right] - \frac{c}{\lambda}\left[\frac{d}{dt_{\mathrm{r}}}\delta t_{\mathrm{r}}(t_{\mathrm{r}}) - \frac{d}{dt_{\mathrm{r}}}\delta t_{\mathrm{s}}(\hat{t})\right] - \dot{I}_\phi - \dot{T} + w_{\mathrm{d}} \tag{4}$$

Let $\hat{\boldsymbol{r}}_{\mathrm{g}}(t_{\mathrm{r}})$ be the unit vector from the GNSS satellite position $\boldsymbol{r}_s(\hat{t})$ to the receiver position $\boldsymbol{r}_{\mathrm{r}}(t_{\mathrm{r}})$. The Doppler measurement can be expanded as

$$f_{\mathrm{d}}(t_{\mathrm{r}}) = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{g}}^{\mathsf{T}}(t_{\mathrm{r}}) \cdot \left[\boldsymbol{v}_{\mathrm{r}}(t_{\mathrm{r}}) - \frac{d}{dt_{\mathrm{r}}}\boldsymbol{r}_s(\hat{t})\right] - \frac{c}{\lambda}\left[\frac{d}{dt_{\mathrm{r}}}\delta t_{\mathrm{r}}(t_{\mathrm{r}}) - \frac{d}{dt_{\mathrm{r}}}\delta t_{\mathrm{s}}(\hat{t})\right] - \dot{I}_\phi - \dot{T} + w_{\mathrm{d}} \tag{5}$$

Taking a look at the time derivative of $\boldsymbol{r}_{\mathrm{s}}$ and invoking the chain rule

$$\frac{d\boldsymbol{r}_{\mathrm{s}}}{dt_{\mathrm{r}}} = \frac{d\boldsymbol{r}_{\mathrm{s}}}{d\hat{t}}\,\frac{d\hat{t}}{dt_{\mathrm{r}}} \tag{6}$$

$$= \boldsymbol{v}_{\mathrm{s}}(\hat{t})\frac{d}{dt_{\mathrm{r}}}\left(t_{\mathrm{r}} - \delta t_{\mathrm{r}}(t_{\mathrm{r}}) - \delta t_{\mathrm{TOF}}\right) \tag{7}$$

$$= \boldsymbol{v}_{\mathrm{s}}(\hat{t})\left[1 - \delta \dot{t}_{\mathrm{r}}(t_{\mathrm{r}})\right] \tag{8}$$

Now let $\boldsymbol{v}_{\mathrm{r}}(t_{\mathrm{r}})$ denote the receiver velocity, $\boldsymbol{v}_{\mathrm{s},i}(\hat{t})$ the satellite velocity, $\delta \dot{t}_{\mathrm{r}}(t_{\mathrm{r}})$ the receiver clock offset rate, and $\delta \dot{t}_{\mathrm{s}}(\hat{t})$ the satellite's clock offset rate. The full Doppler equation for the ith GNSS satellite becomes

$$f_{\mathrm{d},i}(t_{\mathrm{r}}) = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{g}}^{\mathsf{T}}(t_{\mathrm{r}})\left\{\boldsymbol{v}_{\mathrm{r}}(t_{\mathrm{r}}) - \boldsymbol{v}_{\mathrm{s},i}(\hat{t})\left[1 - \delta \dot{t}_{\mathrm{r}}(t_{\mathrm{r}})\right]\right\} - \frac{c}{\lambda}\left\{\delta \dot{t}_{\mathrm{r}}(t_{\mathrm{r}}) - \delta \dot{t}_{\mathrm{s},i}(\hat{t})\left[1 - \delta \dot{t}_{\mathrm{r}}(t_{\mathrm{r}})\right]\right\} - \dot{I}_\phi - \dot{T} + w_{\mathrm{d}} \tag{9}$$

The measurement geometry of a typical GNSS application is shown in Fig. 1. For the benign scenario of the received Doppler seen by a generic receiver emanating from a moving GNSS satellite, the Doppler equation can be further simplified. Because $[1 - \delta \dot{t}_{\mathrm{r}}(t_{\mathrm{r}})]$ is nearly 1, and $\dot{I}_\phi$ and $\dot{T}$ are negligible at most elevations, they can be removed. Additionally, dropping the time indices for visual clarity forms the simplified Doppler equation corresponding to the ith satellite

$$f_{\mathrm{d},i} = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{g}}^{\mathsf{T}}\left\{\boldsymbol{v}_{\mathrm{r}} - \boldsymbol{v}_{\mathrm{s},i}\right\} - \frac{c}{\lambda}\left\{\delta \dot{t}_{\mathrm{r}} - \delta \dot{t}_{\mathrm{s},i}\right\} + w_{\mathrm{d}} \tag{10}$$

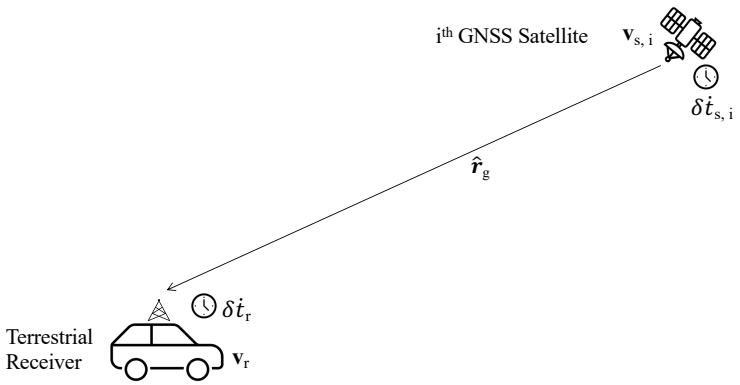

Fig. 1: The observed Doppler of an authentic GNSS satellite at a terrestrial receiver is pictured. The observed Doppler is dependent on the the unit vector from the GNSS satellite position to receiver position $\hat{\boldsymbol{r}}_{\mathrm{g}}(t_{\mathrm{r}})$, the receiver velocity $\boldsymbol{v}_{\mathrm{r}}(t_{\mathrm{r}})$, the satellite velocity $\boldsymbol{v}_{\mathrm{s},i}(\hat{t})$, the receiver clock offset rate $\delta\dot{t}_{\mathrm{r}}(t_{\mathrm{r}})$, and the satellite's clock offset rate $\delta\dot{t}_{\mathrm{s},i}(\hat{t})$.

Doppler Measurement for Spoofing Signals

GNSS spoofers broadcast an ensemble of false signals with the intent that the victim receiver will accept them as authentic signals and infer a false position fix and/or a false clock offset. In this paper, the *inferred* or *induced* position is the false position fix the spoofer induces the receiver to register. This section will demonstrate how the time history of true range-rate between a LEO-based receiver and a terrestrial spoofer can be extracted from GNSS spoofing signals.

Let f_{tr} contain the Doppler components due to the true range-rate between a LEO-based receiver and a terrestrial spoofer, the clock offset rate of the LEO receiver, and the clock offset rate of the terrestrial spoofer. Now let $f_{\mathrm{I},i}$ contain the Doppler components due to the range-rate between the spoofed position and the ith spoofed GNSS satellite, the clock offset rate induced by the spoofing, and the clock offset rate of the the ith spoofed GNSS satellite. Then the Doppler model may be written

$$f_{\mathrm{d},i}(t_{\mathrm{r}}) = f_{\mathrm{tr}}(t_{\mathrm{r}}) + f_{\mathrm{I},i}(t_{\mathrm{r}}) \tag{11}$$

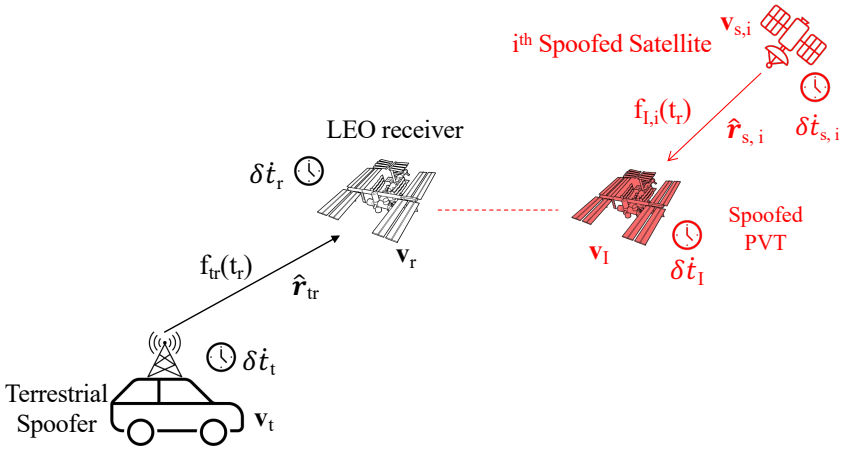

Fig. 2: The Doppler of a terrestrial GNSS spoofing signal as observed from LEO is pictured. $\hat{\boldsymbol{r}}_{\mathrm{tr}}$ denotes the unit vector from the terrestrial spoofer to the LEO-based receiver, $\boldsymbol{v}_{\mathrm{r}}$ the LEO receiver's velocity, $\boldsymbol{v}_{\mathrm{t}}$ the terrestrial spoofer's velocity, $\delta\dot{t}_{\mathrm{r}}$ the true receiver clock rate offset, $\delta\dot{t}_{\mathrm{t}}$ the terrestrial spoofer's clock rate offset, $\hat{\boldsymbol{r}}_{\mathrm{sI},i}$ the unit vector from the ith spoofed satellite to the inferred spoofed position, $\boldsymbol{v}_{\mathrm{I}}$ the inferred spoofed velocity, $\boldsymbol{v}_{\mathrm{s},i}$ the ith spoofed GNSS satellite velocity, $\delta\dot{t}_{\mathrm{I}}$ the inferred clock rate offset, and $\delta\dot{t}_{\mathrm{s},i}$ the ith spoofed GNSS satellite clock rate offset.

Let $\hat{\boldsymbol{r}}_{\mathrm{tr}}$ denote the unit vector from the terrestrial spoofer to the LEO-based receiver, $\boldsymbol{v}_{\mathrm{r}}$ the LEO receiver's velocity, $\boldsymbol{v}_{\mathrm{t}}$ the terrestrial spoofer's velocity, $\delta\dot{t}_{\mathrm{r}}$ the true receiver clock rate offset, $\delta\dot{t}_{\mathrm{t}}$ the terrestrial spoofer's clock rate offset, $\hat{\boldsymbol{r}}_{\mathrm{sI},i}$ the unit

vector from the ith spoofed satellite to the spoofed position, $\boldsymbol{v}_{\mathrm{I}}$ the spoofed velocity, $\boldsymbol{v}_{\mathrm{s},i}$ the ith spoofed GNSS satellite velocity, $\delta\dot{t}_{\mathrm{I}}$ the inferred clock rate offset, and $\delta\dot{t}_{\mathrm{s},i}$ the ith spoofed GNSS satellite clock rate offset. The measurement geometry for receiving a terrestrial GNSS spoofing signal on a LEO receiver is shown in Fig. 2. Note that (11) can be expanded as (dropping time indices)

$$f_{\mathrm{d},i} = \underbrace{-\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{tr}}^{\mathsf{T}}\left\{\boldsymbol{v}_{\mathrm{r}}-\boldsymbol{v}_{\mathrm{t}}\right\}-\frac{c}{\lambda}\left\{\delta\dot{t}_{\mathrm{r}}-\delta\dot{t}_{\mathrm{t}}\right\}}_{f_{\mathrm{tr}}}\underbrace{-\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{sI},i}^{\mathsf{T}}\left\{\boldsymbol{v}_{\mathrm{I}}-\boldsymbol{v}_{\mathrm{s},i}\right\}-\frac{c}{\lambda}\left\{\delta\dot{t}_{\mathrm{I}}-\delta\dot{t}_{\mathrm{s},i}\right\}}_{f_{I,i}}+w_{\mathrm{d}} \tag{12}$$

The common-mode Doppler components across the spoofing signals are emphasized below

$$f_{\mathrm{d},i} = \underbrace{-\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{tr}}^{\mathsf{T}}\left\{\boldsymbol{v}_{\mathrm{r}}-\boldsymbol{v}_{\mathrm{t}}\right\}-\frac{c}{\lambda}\left\{\delta\dot{t}_{\mathrm{r}}-\delta\dot{t}_{\mathrm{t}}\right\}}_{\text{common}}-\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{sI},i}^{\mathsf{T}}\left\{\boldsymbol{v}_{\mathrm{I}}-\boldsymbol{v}_{\mathrm{s},i}\right\}-\frac{c}{\lambda}\{\underbrace{\delta\dot{t}_{\mathrm{I}}}_{\text{common}}-\delta\dot{t}_{\mathrm{s},i}\}+w_{\mathrm{d}} \tag{13}$$

Eq. (12) can be rewritten to group the common terms across the spoofing signals as follows:

$$f_{\mathrm{d},i} = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{sI},i}^{\mathsf{T}}\left\{\boldsymbol{v}_{\mathrm{I}}-\boldsymbol{v}_{\mathrm{s},i}\right\}-\frac{c}{\lambda}\left\{\underbrace{\frac{\hat{\boldsymbol{r}}_{\mathrm{tr}}^{\mathsf{T}}\left\{\boldsymbol{v}_{\mathrm{r}}-\boldsymbol{v}_{\mathrm{t}}\right\}}{c}-\delta\dot{t}_{\mathrm{t}}+\delta\dot{t}_{\mathrm{I}}+\delta\dot{t}_{\mathrm{r}}}_{\text{common}}-\delta\dot{t}_{\mathrm{s},i}\right\}+w_{\mathrm{d}} \tag{14}$$

A standard GNSS navigation solution estimator applied to this measurement model will lump the common-mode Doppler due to true range rate into a single quantity $\gamma(t_{\mathrm{r}})$ [32]. The GNSS receiver will assume the ith Doppler to be:

$$f_{\mathrm{d},i} = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{sI},i}^{\mathsf{T}}\left\{\boldsymbol{v}_{\mathrm{I}}-\boldsymbol{v}_{\mathrm{s},i}\right\}-\frac{c}{\lambda}\left\{\gamma-\delta\dot{t}_{\mathrm{s},i}\right\}+w_{\mathrm{d}} \tag{15}$$

The quantity $\gamma(t_{\mathrm{r}})$ will be interpreted by a spoofed receiver as the receiver clock rate error, even though $\gamma(t_{\mathrm{r}})$ encompasses much more than this:

$$\gamma(t_{\mathrm{r}}) = \frac{\hat{\boldsymbol{r}}_{\mathrm{tr}}^{\mathsf{T}}(t_{\mathrm{r}})\left\{\boldsymbol{v}_{\mathrm{r}}(t_{\mathrm{r}})-\boldsymbol{v}_{\mathrm{t}}(t_{\mathrm{r}})\right\}}{c}-\delta\dot{t}_{\mathrm{T}}(t_{\mathrm{r}})+\delta\dot{t}_{\mathrm{I}}(t_{\mathrm{r}})+\delta\dot{t}_{\mathrm{r}}(t_{\mathrm{r}}) \tag{16}$$

$$= \frac{\hat{\boldsymbol{r}}_{\mathrm{tr}}^{\mathsf{T}}(t_{\mathrm{r}})\boldsymbol{v}_{\mathrm{r}}(t_{\mathrm{r}})}{c}-\frac{\hat{\boldsymbol{r}}_{\mathrm{tr}}^{\mathsf{T}}(t_{\mathrm{r}})\boldsymbol{v}_{\mathrm{t}}(t_{\mathrm{r}})}{c}-\delta\dot{t}_{\mathrm{t}}(t_{\mathrm{r}})+\delta\dot{t}_{\mathrm{I}}(t_{\mathrm{r}})+\delta\dot{t}_{\mathrm{r}}(t_{\mathrm{r}}) \tag{17}$$

Notice that the form of (15) is identical to (10). The term that has changed is the receiver clock rate error, which was replaced with $\gamma(t_{\mathrm{r}})$. In other words, the PVT receiver's estimator will infer the state $\boldsymbol{x} = [\ \boldsymbol{r}_{\mathrm{I}}^{\mathsf{T}},\ \delta t_I,\ \boldsymbol{v}_{\mathrm{I}}^{\mathsf{T}},\ \gamma\ ]^T$, which is composed of the spoofed position and velocity, as well as the new receiver clock offset rate $\gamma(t_{\mathrm{r}})$. The PVT estimator attributes common-mode deviations across received signals to the receiver's clock rate offset. Importantly, $\gamma(t_{\mathrm{r}})$ is unaffected by the unknown added Doppler frequency component of each individual spoofing signal.

The time history of $\frac{c}{\lambda}\cdot\gamma(t_{\mathrm{r}})$ can ultimately be used for geolocation because the component caused by the range-rate between the LEO-based receiver and the terrestrial spoofer appears in the first term. Information containing the transmitter location is embedded in $\hat{\boldsymbol{r}}_{\mathrm{tr}}(t)$. The true time histories of the LEO-based receiver's clock rate estimate $\delta\dot{t}_{\mathrm{r}}(t_{\mathrm{r}})$ and receiver velocity $\boldsymbol{v}_{\mathrm{r}}(t_{\mathrm{r}})$ can be found from separate processing of authentic GNSS signals. After $\delta\dot{t}_{\mathrm{r}}(t)$ is found, it can be subtracted from $\gamma(t_{\mathrm{r}})$. The terms that remain – $\boldsymbol{v}_{\mathrm{t}}$, $\delta\dot{t}_{\mathrm{t}}$, $\delta\dot{t}_{\mathrm{I}}$ – corrupt the geolocation solution. The estimator will not be able to distinguish between $\hat{\boldsymbol{r}}_{\mathrm{tr}}^{\mathsf{T}}(t)\boldsymbol{v}_{\mathrm{r}}(t)/c$ and the corrupting terms, but $\gamma(t_{\mathrm{r}})$ is dominated by the true range-rate between the LEO receiver and the terrestrial spoofer because the LEO receiver is moving extremely fast. This means $\frac{c}{\lambda}\cdot\gamma(t_{\mathrm{r}})$ can still provide an accurate geolocation estimate despite the presence of the corrupting terms.

Based on the above Doppler measurement model, a non-linear least-squares estimator for the time history $\frac{c}{\lambda}\cdot\gamma(t_{\mathrm{r}})$ can be developed to estimate the unknown transmitter position and transmitter clock frequency bias from a collection of single-pass Doppler measurements, as found in [30]. The following section investigates how $\boldsymbol{v}_{\mathrm{t}}(t_{\mathrm{r}})$, $\delta\dot{t}_{\mathrm{t}}(t_{\mathrm{r}})$, and $\delta\dot{t}_{\mathrm{I}}(t_{\mathrm{r}})$ affect geolocation accuracy.

ANALYSIS OF CORRUPTING TERMS

This section investigates how transmitter motion $\boldsymbol{v}_{\mathrm{t}}(t_{\mathrm{r}})$, transmitter clock offset rate $\delta\dot{t}_{\mathrm{t}}(t_{\mathrm{r}})$, and spoofed clock offset rate $\delta\dot{t}_{\mathrm{I}}(t_{\mathrm{r}})$ affect the geolocation accuracy using $\gamma(t_{\mathrm{r}})$. This is accomplished by performing a simulation of a particular,

representative scenario of capturing terrestrial spoofing signals on a LEO receiver. The LEO-based receiver trajectory was taken from a segment of the ISS orbit on day 144 of 2018. The simulated transmitter position was taken to be 45N latitude, 45E longitude, 0 m altitude. The geometry of the simulation is shown in Fig. 3.

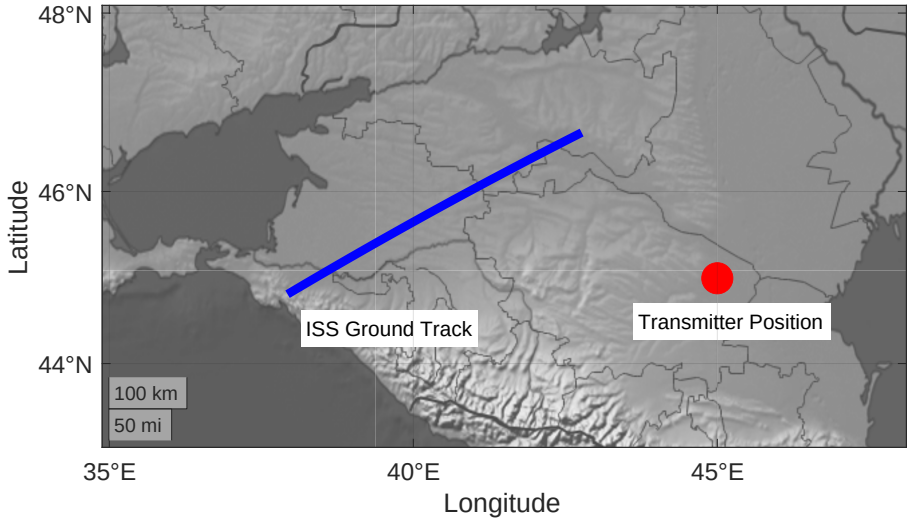

Fig. 3: The ground track of the ISS orbit during day 144 of 2018 spanning approximately 60 seconds. The simulated emitter position is marked at 45N latitude, 45 longitude, 0 m. This chosen transmitter location does not carry any significance.

Transmitter Movement

As shown in Eq. 17, unknown transmitter motion corrupts the geolocation solution. If the transmitter is stationary, this term is completely removed and has no effect on $\gamma(t_{\mathrm{r}})$. This section aims to empirically quantify the magnitude of geolocation error if the transmitter is falsely assumed to be stationary while in actuality the transmitter was moving.

In this simulation, the LEO-based receiver trajectory is identical across each trial, with $\delta\dot{t}_{\mathrm{t}}$ and $\delta\dot{t}_{\mathrm{I}}$ set to zero, and $\delta\dot{t}_{\mathrm{r}}$ removed. For each trial, the transmitter moves at a constant 10 m/s in a specified radial direction (azimuth) constrained to the curved surface of the Earth. The transmitter begins moving at the start of each capture from the original transmitter location at 45N latitude, 45E longitude, and 0 m altitude. 360 trials are performed, one for each degree in azimuth from the original transmitter location.

For each trial, the true Doppler time history between the LEO receiver and moving transmitter is calculated. The calculated Doppler time history is then fed to the non-linear least-squares estimator for stationary transmitters. The final geolocation solution is recorded for each trial and the offset from the initial transmitter location is calculated.

The magnitude of final geolocation offset from the initial position over azimuth of transmitter motion is shown in Fig. 4. The maximum geolocation solution offset from original position was 2,293 m. This occurred when the transmitter was moving at 18° and 198° azimuth, which is in the direction of/against LEO receiver motion. The transmitter location will be best resolved in the direction of satellite motion in nominal non-linear least-squares estimation for a stationary transmitter. The greatest error arises when the transmitter is moving in/against the direction of LEO receiver motion because the estimator has greater sensitivity to position and velocity errors in these directions. It follows that the azimuth causing the least error was when the transmitter was moving orthogonally to satellite motion.

Furthermore, Fig. 4 shows the final geolocation solution in the east-north plane. When the transmitter was moving in the exact opposite direction of the LEO receiver (the green diamond), the final geolocation solution was closest to the LEO receiver. For this specific trial, the line-of-sight velocity (LOS) changes at the fastest rate of any direction. Because the non-linear least-squares estimator assumes the transmitter is stationary, quickly changing LOS velocities are indicative of the transmitter being closer to the LEO receiver.

This simulation shows that reasonable geolocation accuracy is attainable even if the transmitter is moving because the motion of the LEO receiver is much faster than the motion of the transmitter. This analysis is also valid for transmitters with constant

frequency because the time-varying component due to spoofing is removed in $\gamma(t_r)$.

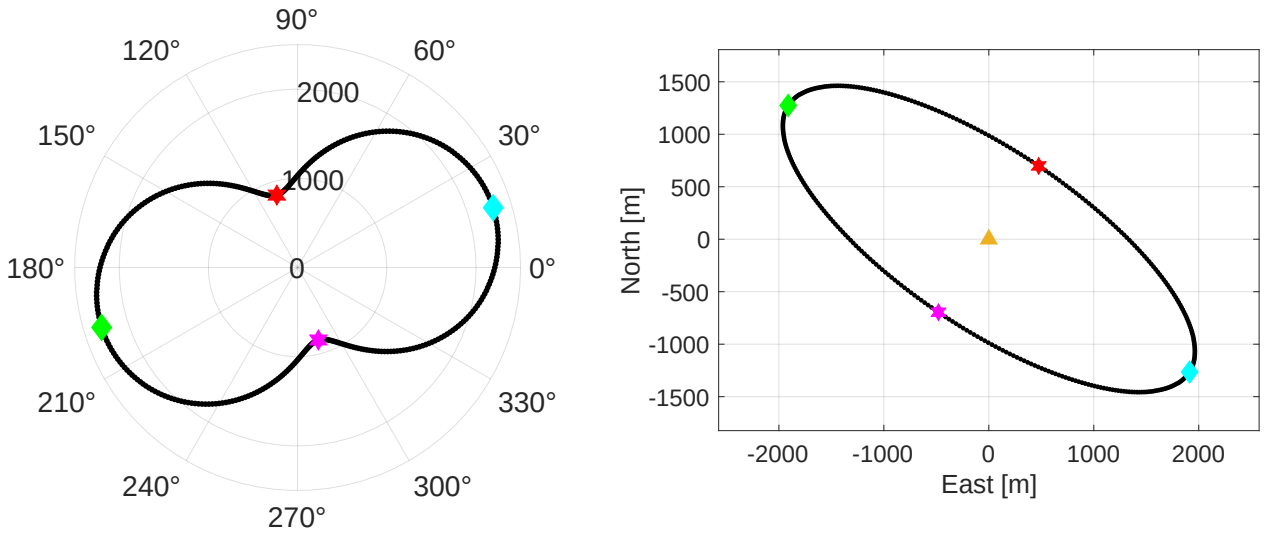

Fig. 4: Left: The magnitude of final geolocation offset from the initial position over azimuth of transmitter motion is shown. The diamonds indicate when the motion of the transmitter was in/against (cyan/green) the direction of LEO receiver motion, and the stars indicate when the transmitter was moving orthogonally towards/against (red/magenta) the direction of LEO receiver motion. The maximum geolocation offset from original position was 2.293 km, occurring when the transmitter was moving direction of/against LEO receiver motion. Right: The final geolocation solution for each trial is shown on the right in the east-north plane centered at the initial position.

Transmitter Clock and Spoofed Clock Offset Rate

The effect of instability in the transmitter clock and the spoofed clock offset rate are investigated in this section. These two corrupting parameters are grouped together because the spoofer is expected to constrain the induced clock offset rate at or near zero. This is because spoofing will be suspected by the victim if the spoofed clock offset rate grows too rapidly to be explained by the expected levels of clock drift for the receiver's given oscillator type.

It is assumed the transmitter is operating in steady-state conditions so that $\delta\dot{t}_t$ can be modeled as constant over a short (e.g., 60-second) data capture interval. When $\delta\dot{t}_t$ is modeled as constant over a capture interval, actual transmitter clock instability gives rise to Doppler measurement errors. The transmitter clock rate error $\delta\dot{t}_t$ is modeled as a random walk process that evolves as:

$$\delta\dot{t}_t(t_{k+1}) = \delta\dot{t}_t(t_k) + v(t_k) \tag{18}$$

where $v(t_k)$ is a discrete-time Gaussian random process with $\mathbb{E}[v(t_k)] = 0$ and $\mathbb{E}[v(t_k)v(t_j)] = 2\pi^2 h_{-2}\delta t\delta_{k,j},\ \forall k, j$, where h_{-2} is the first parameter of the standard clock model based on the fractional frequency error power spectrum, as given in [33, Chap. 8]; $\delta t = t_{k+1} - t_k$ is the uniform sampling interval; and $\delta_{k,j}$ is the Kronecker delta.

The impact of such errors on geolocation accuracy was analyzed via Monte Carlo simulation for four levels of transmitter clock quality: (1) laboratory-grade oven-controlled crystal oscillator (OCXO), (2) low-quality OCXO, (3) temperature-compensated crystal oscillator (TCXO), and (4) TCXO with added errors from the spoofed clock offset rate. The spoofed clock offset rate in clock quality type (4) is modeled as zero-mean Gaussian noise, so the combination of transmitter instability and spoofed clock offset rate is simulated as a low-quality clock.

First, an error-free Doppler time history was generated based on this scenario as shown in Fig. 3 with a measurement rate of 20 Hz. Then, for each instance of the Monte Carlo simulation, an independent realization of a Doppler error random process consistent with the clock model being analyzed was generated and added to the error-free Doppler. Doppler error was modeled as a random walk process consistent with (18). 1000 Monte Carlo trials were conducted for each of the four clock quality levels. Transmitter horizontal location estimation errors were observed to be zero-mean and apparently Gaussian, and

they were consistent with the formal error ellipses of the associated least-squares estimator. The semi-major and semi-minor axis of the error ellipses for the four clock types are reported in Table (I). These error ellipse values only correspond to this specific geometry, as these values change with receiver-transmitter geometry. For this geometry, only marginal geolocation is achievable if the terrestrial spoofer has a combination of a poor clock and is inducing a large spoofed clock offset rate.

TABLE I: Marginal contribution of transmitter frequency instability to a single-pass geolocation error ellipse for this geometry. The size of the 95% horizontal geolocation error ellipse, in meters, is characterized by the semi-major and semi-minor axes.

Clock Quality	h_{-2}	semi-major (m)	semi-minor (m)
TCXO with $\delta\dot{t}_{\mathrm{I}}$	3×10^{-19}	6351.74	1561.60
TCXO	3×10^{-21}	619.56	154.11
Low-quality OCXO	3×10^{-23}	61.48	15.35
OCXO	3×10^{-25}	5.74	1.50

GEOLOCATION OF A SIMULATED TERRESTRIAL SPOOFER

The developed technique was verified by simulating the reception of spoofing signals from a stationary terrestrial simulator-spoofer on a LEO-based receiver. A simulator-spoofer is a type of GNSS spoofer that transmits an ensemble of self-consistent GNSS signals generated from either a simulation engine or previously recorded authentic GNSS signals. A simulator-spoofer is easily realizable, as any good GNSS signal simulator can produce a self-consistent ensemble of spoofing signals. Another way to produce an ensemble of self-consistent spoofing signals is to record authentic GNSS signals and then transmit the recording at a later time. If a recording of authentic signals is used, the victim(s) will infer the position and velocity of the receiver used in the original recording.

For the spoofer in this simulation, a simulator-spoofer was selected with the self-consistent ensemble of spoofing signals being recorded authentic GNSS signals captured atop the Aerospace building at the University of Texas at Austin. The recording was 80 seconds long and complex sampled at 25 Msps with 16-bit quantization on in-phase and quadrature (IQ). The simulator-spoofer was selected to be positioned at 45N latitude, 45E longitude, and 0 m altitude. The LEO receiver trajectory was taken from a historical trajectory from the ISS. The original Doppler shift of each signal in the recording acts as the additional time-varying frequency component $f_{\mathrm{I},i}$ added by the spoofer.

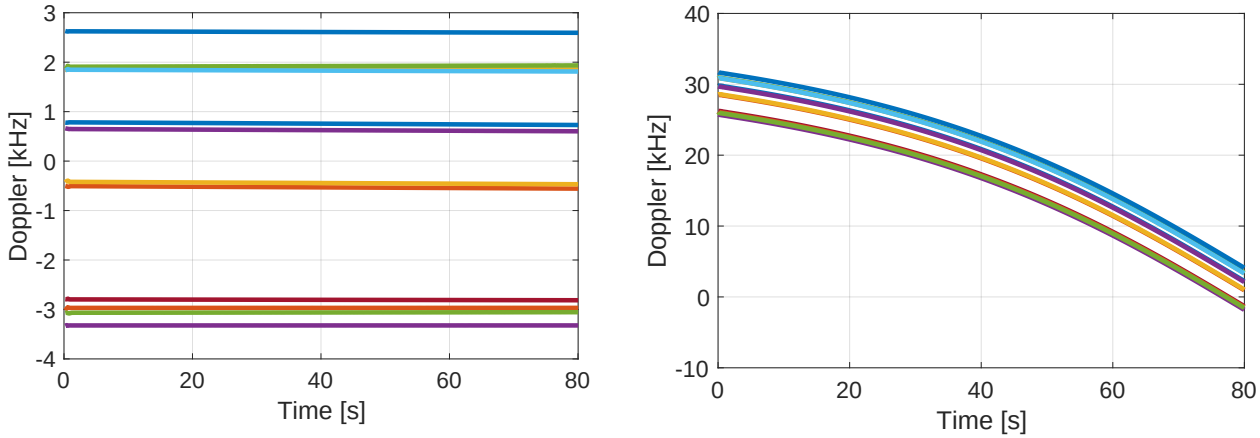

Fig. 5: On the left are the Doppler time histories of each of the authentic GNSS signals in the original recording. On the right are the Doppler time histories after frequency shifting the original data to imitate the reception of terrestrial spoofing signals on a LEO receiver according to the geometry in Fig. 3.

Doppler effects arising from relative motion between the LEO receiver and ground transmitter are considerable in the L-band for the Earth-to-LEO channel. A comprehensive Doppler model is required, consisting of both a frequency shift and compression/dilation of the baseband signal. If the frequency shift was added but not compression/dilation of the baseband signal, the GNSS receiver will notice unusual code/carrier divergence. The recorded data atop the Aerospace building was resampled and frequency shifted according as if it were received on the ISS as shown in Fig. 3.

The generic complex baseband representation of a sampled GNSS signal at each sample k, where $k = 1, 2, ..., N$ for N samples, is expressed

$$r_k = \sqrt{P} D(t_k - \tau_k) C(t_k - \tau_k) \exp(j2\pi\Theta_k) \tag{19}$$

where P is the received signal power, $D(t_k)$ is the binary navigation data modulation, $C(t_k)$ is the binary spreading code, τ_k is the code phase, and $\exp(j\Theta_k)$ is the carrier with phase Θ_k. This is the form of the original recorded data that is to be frequency shifted and compressed/dilated. Once resampled and frequency shifted, the original Doppler between GNSS satellite and receiver represents $f_{\mathrm{I,\,i}}$ in Eq. 11.

The amount frequency shift and compression/dilation of the baseband signal is governed by the range-rate between a LEO receiver and a terrestrial spoofer. First, the true time history of the LOS velocity between the LEO receiver and the terrestrial spoofer for this geometry was calculated. Then, the LOS velocity time history is converted to a Doppler time history by dividing by the signal's nominal wavelength.

Recall that a signal's instantaneous frequency is the time derivative of the phase $f(t) = d\theta(t)/dt$. The frequency shift and compression/dilation of the baseband signal can only be achieved by working at the phase level. A polynomial approximation of the Doppler (frequency shift) time history is taken. This allows an instantaneous Doppler to exist at each sample time and allows the time history of instantaneous frequency shifts to be integrated. The polynomial approximation is integrated to get the corresponding phase shift at each sample, denoted as $\tilde{\Theta}_k$. The frequency shift is added to the original signal by multiplying the original signal by the complex exponential of phase shifts $\exp(j2\pi\tilde{\Theta}_k)$ at each sample k.

Let t_k denote the time of the kth sample. The original signal must be resampled at times $\tilde{t}_k = t_k + \tilde{\Theta}_k/f_c$ where f_c is the nominal center frequency. Resampling is achieved by interpolating the original signal at the time indices $\tilde{t}_k$. Linear interpolation is sufficient because the original recording was at 16-bit quantization. This returns the proper compression/dilation of the baseband signal consistent with the frequency shift.

The new baseband signal at the kth sample for the reception of a terrestrial spoofer on an LEO receiver $\tilde{r}_k$ is expressed as

$$\tilde{r}_k = \sqrt{P} D(\tilde{t}_k - \tau_k) C(\tilde{t}_k - \tau_k) exp(j2\pi\Theta_k) \exp(j2\pi\tilde{\Theta}_k) \tag{20}$$

The resampled and frequency shifted binary recording was processed with the RNL's GRID GNSS software-defined receiver [29], [34], [35] with all spoofing defenses disabled. The PVT estimator inferred the position and velocity of the original recording. The new Doppler measurements containing the range-rate between the LEO receiver and the terrestrial spoofer are shown in Fig. 5. The time history of the receiver clock offset rate was extracted, converted to a Doppler frequency time history, and then plotted with Doppler from range-rate between a LEO receiver and a terrestrial spoofer in Fig. 6.

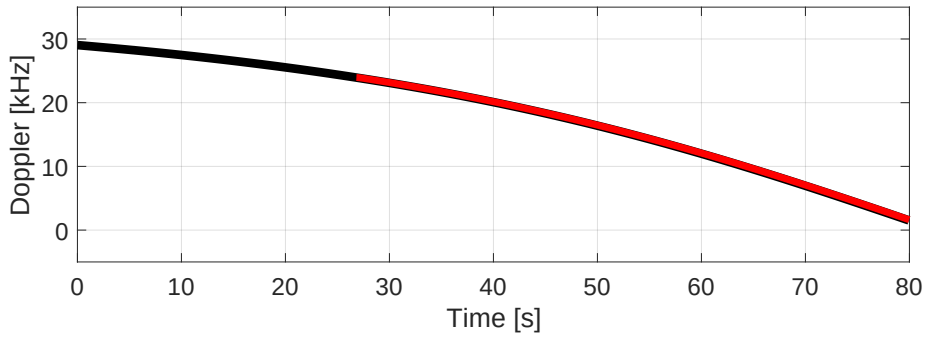

Fig. 6: The true Doppler from range-rate between LEO receiver and terrestrial spoofer is shown in black and the Doppler from receiver clock offset rate is shown in red. They match nearly perfectly, meaning the receiver clock offset rate can be used for geolocation. The receiver clock offset rate begins at around 26 seconds when the first navigation solution becomes available.

The Doppler time histories are nearly identical, showing that the time-varying frequency competent added to each signal has been removed. The Doppler time history from the receiver clock offset rate was served as measurements to the non-linear least-squares estimator. The estimated geolocation solution from these measurements was off .8 km from the true location as

shown in Fig. 7 . Furthermore, the residuals from the estimator were nearly zero-mean. This shows that if all of the spoofing signals are processed, a GNSS receiver's navigation solution estimation lumps any term that is common across all satellites into the receiver clock offset rate. The time history of the receiver clock offset rate can be exploited for geolocation because it contains the the range-rate between a LEO receiver and a terrestrial spoofer.

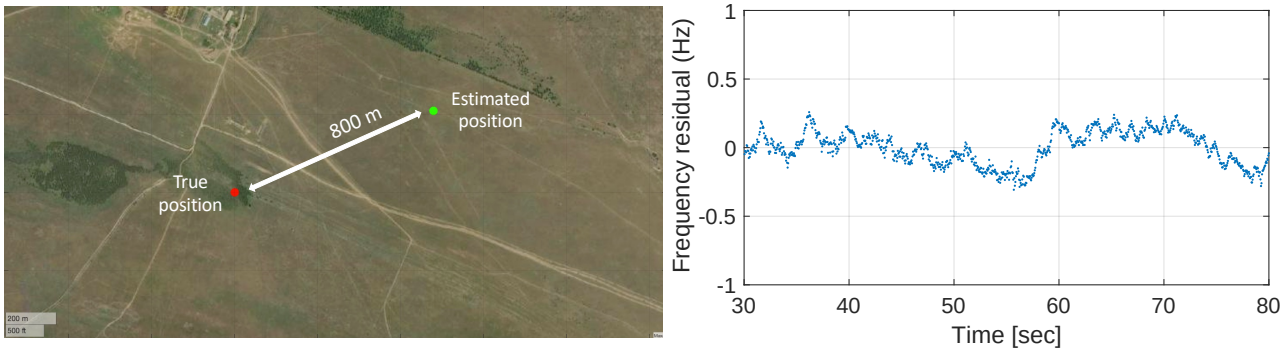

Fig. 7: The estimated geolocation solution from the receiver clock offset rate was off .8 km from the true position. Furthermore, the residuals from the estimator were nearly zero-mean. The time history of the receiver clock offset rate can be used for geolocation because it contains the the range-rate between LEO receiver and terrestrial spoofer.

RECENT CAPTURE OF REAL-WORLD GNSS SPOOFING SIGNALS ON A LEO RECEIVER

The RNL and Cornell University developed a software-defined multi-frequency GNSS receiver called FOTON that is operational on the ISS [29]. FOTON is a part of the GROUP-C (GPS Radio Occultation and Ultraviolet Photometry-Colocated) experiment, which is intended to provide ionospheric electron density profiles, scintillation measurements, and lower atmosphere profiles. FOTON continuously logs the coherent 10 ms IQ accumulations produced by the custom on-board GNSS receiver. Additionally, the FOTON receiver front-end is also capable of low level raw captures of the 5.714286 Msps intermediate frequency (IF) samples for an interval of up to 70 seconds.

On day 97 of 2022, a raw capture was recorded while the ISS was flying over Turkey and headed towards Syria, as shown in Fig. 8. The spectral characteristics of the capture is illustrated in Fig. 9. There is strong interference present in both the L1 and L2 bands. In this capture, there were a total of ten GPS-like interference signals that were acquired and tracked. There was a single GPS L1 C/A matched-code jamming signal, and nine GPS L1 C/A spoofing signals. The matched-code jamming signal did not have any navigation data, whereas the spoofing signals were modulated with fake navigation data. The false navigation data on the spoofing signals passed all parity and sync as specified by [36]. There was no evidence of GPS L2C or Galileo E1 matched-code jammers or spoofers.

Fig. 8: Ground track for interference-affected capture on day 97 of 2022. The capture spans approximately 60 seconds.

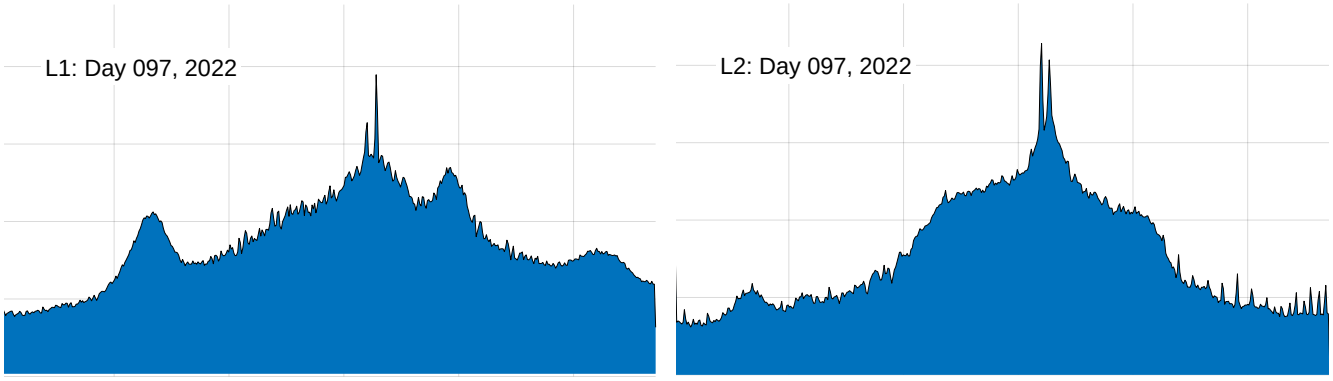

Fig. 9: Power spectra centered near the GPS L1 (left) and L2 (right) frequencies from interference-affected data captured on day 97 of 2022. The frequency spans approximately 3 MHz.

It was quickly determined that the matched-code jammer and spoofer were different transmitters by looking at the time history of the carrier-to-noise ratio (CNR). The matched-code jammer's average CNR was 45.7 dB-Hz, whereas the spoofing signals' average CNR was 35.2 dB-Hz. All nine spoofing signals have a nearly identical fading pattern, indicating that they originated from the same source.

The Doppler time histories for all ten interference signals are shown in Fig. 10. The Doppler time history for the matched-code jamming signal and the spoofing signals have a different shape, further indicating that they originated from different transmitters. The overall shape of the Doppler time history for the nine spoofing signals is the same. This is because the change in Doppler due to the changing LEO ISS orbital geometry is significantly larger than the change in Doppler due to the intended spoofing. Additionally, Fig. 10 shows the Doppler difference between a pair of spoofed signals. The Doppler difference changes fast enough indicating that the spoofing is intending to mimic a highly dynamic receiver. If it were mimicking a stationary receiver, the Doppler difference would have been nearly constant.

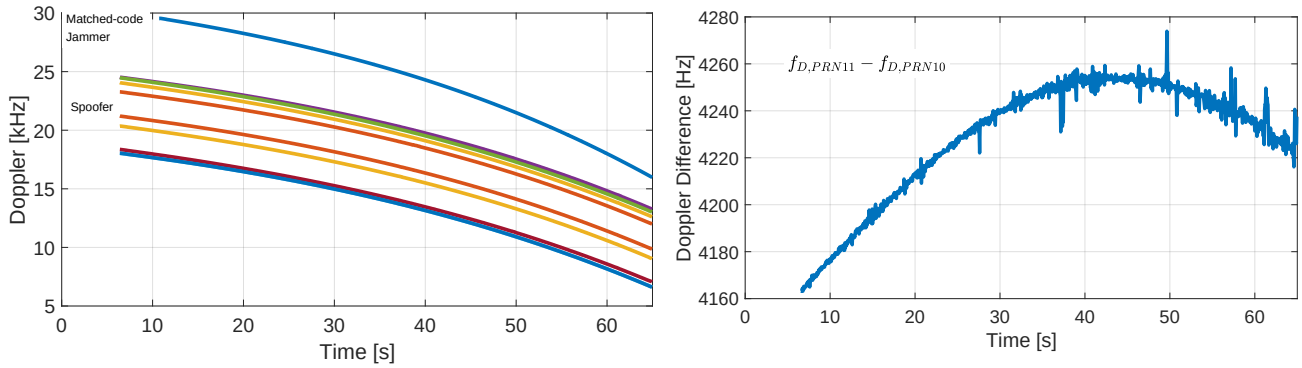

Fig. 10: Right: Doppler time history corresponding to the single matched-code jammer and the nine spoofing signals from the day 97 capture. Left: Doppler difference of spoofed GPS L1 C/A PRN 11 and GPS L1 C/A PRN 10. The Doppler difference changes fast enough indicating that the spoofing is intending to mimic a highly dynamic receiver.

It was determined that the spoofer in this capture was a simulator-spoofer rather than a receiver-spoofer. The spoofed signals time of week (TOW) message was off by 168 from the authentic signals' TOW. A receiver-spoofer would have transmitted spoofed signals with a TOW much closer to true time. The navigation data on each spoofing signal were decoded and the ephemeris and clock parameters were extracted. The extracted parameters appeared to be reasonable. The ephemeris and clock parameters of the authentic GPS satellites at the corresponding TOW were retrieved from the National Oceanic and Atmospheric Administration's (NOAA) website and compared to the spoofed navigation data. These two sets of navigation data were completely different. If this spoofer were a receiver-spoofer, the navigation data would have been close to the authentic values, if not exactly the same. Therefore, these spoofing signals were from a simulator.

Standard GPS pseudorange-based navigation solutions were performed using the pseudoranges for subsets of five spoofed signals. All combinations produced poor results, as the RMS pseudorange residuals were on the order of 1000 km. There was no one satellite that obviously produced most of the error and some of the satellites had large negative elevations at the optimal solution. Therefore, the spoofer in this capture does not appear to be a proper, self-consistent, spoofer. Additionally, spoofed PRN 16 and PRN 22 had identical navigation data and Doppler time histories, meaning the same spoofed signal configuration was used for both of these signals.

Unfortunately, the developed technique in this paper cannot be applied because this spoofer is not self-consistent. However, even without knowing the intended position and velocity of the spoofed receiver, the spoofer can be geolocated to sub 100 km accuracy because the change in Doppler due to the changing LEO ISS orbital geometry is large over the 60 seconds (about 10 kHz) whereas the change in Doppler due to the intended spoofing is small (40 Hz).

The Doppler time histories of the single matched-code jammer signal and six of the spoofing signals were individually served as measurements to the non-linear least-squares estimator to estimate the transmitter position. The final geolocation solutions are shown in Fig. 11. Each solution had zero-mean Gaussian frequency residuals. The maximum distance between two transmitter position estimates from the spoofing signals was 60 km.

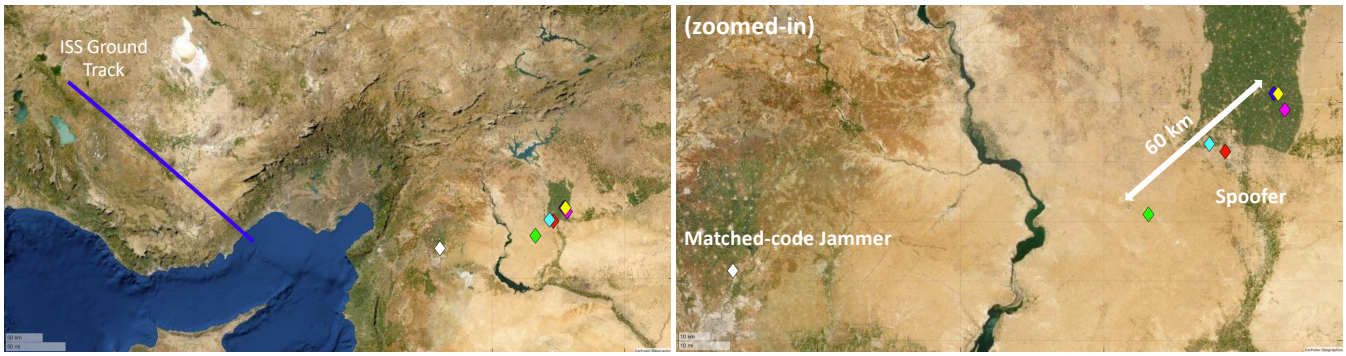

Fig. 11: The Doppler time histories of the single matched-code jammer signal and six of the spoofing signals were individually served as measurements to the non-linear least-squares estimator to estimate a transmitter position solution. The white marker corresponds to the matched-code jammer and the colored markers correspond to the spoofing signals. Less than 100 km geolocation accuracy of GNSS spoofers can be achieved if the observed Doppler from the spoofing signals are used for geolocation.

CONCLUSIONS

A single-satellite single-pass geolocation technique for terrestrial GNSS spoofing signals from LEO has been developed and verified. GNSS spoofers transmit signals whose carrier frequency contains an unknown time-varying frequency component that imitates the Doppler corresponding to each individual spoofed navigation satellite. The developed technique removed the unknown time-varying frequency component so that a Doppler (range-rate) time history was extracted for geolocation. It is shown that the true range rate between the terrestrial spoofer and LEO-based receiver manifests in the spoofed receiver clock offset rate estimate. Monte Carlo simulations have been developed that investigate how transmitter motion, transmitter clock offset rate, and spoofed clock offset rate affect geolocation accuracy. The proposed method has been validated by simulating the reception of a terrestrial GNSS spoofing signals on a LEO-based receiver and achieved under 10 km accuracy. Additionally, recent real-world GPS spoofing signals captured by a LEO-based receiver have been analyzed.

ACKNOWLEDGMENTS

Research 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.

REFERENCES

[1] Psiaki, M. L. and Humphreys, T. E., *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, Vol. 1, chap. Civilian GNSS Spoofing, Detection, and Recovery, Wiley-IEEE, 2020, pp. 655–680.

[2] Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., and Kintner, Jr., P. M., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Savannah, GA, 2008.

[3] Humphreys, T. E., "Interference," *Springer Handbook of Global Navigation Satellite Systems*, Springer International Publishing, 2017, pp. 469–503.

[4] Divis, D. A., "Scientists document possible drone jamming," *Inside unmanned systems*, Sept. 2015, pp. 14.

[5] Murrian, M. J., Narula, L., Humphreys, T. E., O'Hanlon, B. W., and Budzien, S., "Characterizing GNSS Interference from Low-Earth Orbit," *Inside GNSS*, Vol. 15, No. 1, 2020, pp. 54–59.

[6] Liu, Z., Lo, S., and Walter, T., "GNSS Interference Characterization and Localization Using OpenSky ADS-B Data," *Multidisciplinary Digital Publishing Institute Proceedings*, Vol. 59, No. 1, 2020.

[7] Harris, M., "Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai," *MIT Technology Review*, 11 2019.

[8] Psiaki, M. L. and Humphreys, T. E., "GNSS Spoofing and Detection," *Proceedings of the IEEE*, Vol. 104, No. 6, 2016, pp. 1258–1270.

[9] Montgomergy, P. Y., Humphreys, T. E., and Ledvina, B. M., "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer," *Proceedings of the ION International Technical Meeting*, Anaheim, CA, Jan. 2009.

[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] Gross, J. N., Kilic, C., and Humphreys, T. E., "Maximum-likelihood power-distortion monitoring for GNSS-signal authentication," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 55, No. 1, 2018, pp. 469–475.

[12] Psiaki, M. L., O'Hanlon, B. W., Powell, S. P., Bhatti, J. A., Wesson, K. D., Humphreys, T. E., and Schofield, A., "GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase," *Proceedings of the ION GNSS+ Meeting*, Institute of Navigation, Tampa, FL, 2014.

[13] Clements, Z., Yoder, J. E., and Humphreys, T. E., "Carrier-phase and IMU based GNSS Spoofing Detection for Ground Vehicles," *Proceedings of the ION International Technical Meeting*, Long Beach, CA, 2022.

[14] LaChapelle, D. M., Narula, L., and Humphreys, T. E., "Orbital War Driving: Assessing Transient GPS Interference from LEO," *Proceedings of the ION GNSS+ Meeting*, St. Louis, MO, 2021.

[15] Ho, K. and Chan, Y., "Geolocation of a known altitude object from TDOA and FDOA measurements," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 33, No. 3, July 1997, pp. 770–783.

[16] Bhatti, J., *Sensor Deception Detection and Radio-Frequency Emitter Localization*, Ph.D. thesis, The University of Texas at Austin, Aug. 2015.

[17] Weiss, A., "Direct Geolocation of Wideband Emitters Based on Delay and Doppler," *Signal Processing, IEEE Transactions on*, Vol. 59, No. 6, June 2011, pp. 2513–2521.

[18] Sidi, A. and Weiss, A., "Delay and Doppler Induced Direct Tracking by Particle Filter," *Aerospace and Electronic Systems, IEEE Transactions on*, Vol. 50, No. 1, January 2014, pp. 559–572.

[19] Witzgall, H., "Two-sensor tracking of maneuvering transmitters," *2018 IEEE Aerospace Conference*, IEEE, 2018, pp. 1–7.

[20] Musicki, D., Kaune, R., and Koch, W., "Mobile Emitter Geolocation and Tracking Using TDOA and FDOA Measurements," *Signal Processing, IEEE Transactions on*, Vol. 58, No. 3, March 2010, pp. 1863–1874.

[21] Ho, K. and Xu, W., "An accurate algebraic solution for moving source location using TDOA and FDOA measurements," *Signal Processing, IEEE Transactions on*, Vol. 52, No. 9, Sept 2004, pp. 2453–2463.

[22] 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.

[23] Ellis, P., Rheeden, D. V., and Dowla, F., "Use of Doppler and Doppler Rate for RF Geolocation Using a Single LEO Satellite," *IEEE Access*, Vol. 8, 2020, pp. 12907–12920.

[24] Becker, K., "An efficient method of passive emitter location," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 28, No. 4, 1992, pp. 1091–1104.

[25] Parkinson, B. W., Stansell, T., Beard, R., and Gromov, K., "A HISTORY OF SATELLITE NAVIGATION," *NAVIGATION: Journal of the Institute of Navigation*, Vol. 42, No. 1, 1995, pp. 109–164.

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

[27] Ellis, P. B. and Dowla, F., "Single Satellite Emitter Geolocation in the Presence of Oscillator and Ephemeris Errors," *2020 IEEE Aerospace Conference*, IEEE, 2020, pp. 1–7.

[28] Ellis, P. and Dowla, F., "Performance bounds of a single LEO satellite providing geolocation of an RF emitter," *2018 9th Advanced Satellite Multimedia Systems Conference and the 15th Signal Processing for Space Communications Workshop (ASMS/SPSC)*, IEEE, 2018, pp. 1–5.

[29] 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*, Vol. 61, No. 1, Mar. 2014, pp. 53–64.

[30] Murrian, M. J., Narula, L., Iannucci, P. A., Budzien, S., O'Hanlon, B. W., Powell, S. P., and Humphreys, T. E., "First Results from Three Years of GNSS Interference Monitoring from Low Earth Orbit," *Navigation, Journal of the Institute of Navigation*, Vol. 68, No. 4, 2021, pp. 673–685.

[31] Psiaki, M. L. and Mohiuddin, S., "Modeling, analysis, and simulation of GPS carrier phase for spacecraft relative navigation," *Journal of Guidance, Control, and Dynamics*, Vol. 30, No. 6, 2007, pp. 1628.

[32] Teunissen, P. J., *Springer Handbook of Global Navigation Satellite Systems*, chap. Carrier Phase Integer Ambiguity Resolution, Springer, 2017, pp. 661–685.

[33] Brown, R. G. and Hwang, P. Y., *Introduction to Random Signals and Applied Kalman Filtering*, Wiley, 2012.

[34] Clements, Z., Iannucci, P. A., Humphreys, T. E., and Pany, T., "Optimized Bit-Packing for Bit-Wise Software-Defined GNSS Radio," *Proceedings of the ION GNSS+ Meeting*, St. Louis, MO, 2021.

[35] Nichols, H. A., Murrian, M. J., and Humphreys, T. E., "Software-Defined GNSS is Ready for Launch," *Proceedings of the ION GNSS+ Meeting*, Denver, CO, 2022.

[36] GPS Directorate, "Systems Engineering and Integration Interface Specification IS-GPS-200L," 2020, http://www.gps.gov/technical/icwg/.