Demonstration of Single-Satellite GNSS Spoofer Geolocation

Zachary Clements*, Iain Goodridge†, Patrick Ellis‡, Matthew J. Murrian†, and Todd E. Humphreys*
*Department of Aerospace Engineering and Engineering Mechanics, The University of Texas at Austin
†Spire Global
‡Formerly Spire Global

BIOGRAPHIES

Zachary Clements (B.S., Clemson University; M.S., University of Texas at Austin) is a P.h.D. 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, software-defined radio, and statistical estimation with an emphasis on GNSS interference localization from low Earth orbit. He won the 2023 IEEE Walter Fried Award for best overall paper at the IEEE/ION PLANS conference for his work on GNSS interference detection, classification and geolocation from low Earth orbit.

Iain Goodridge is a seasoned professional and currently the Senior Director of Radio Frequency Geolocation Products at Spire Global. With a focus on the development and customer adoption of cutting-edge radio frequency geolocation solutions from low Earth orbit, Iain brings over a decade of expertise in the industry. Known for his strategic mindset and innovative approach, he has successfully launched groundbreaking products into existing markets, solidifying his reputation as a leader in the field.

Patrick B. Ellis (B.S. Bradley University; M.S., Ph.D., University of California at Santa Cruz) is currently a GNSS Wireless Systems Engineer at Apple Inc. There he specializes in statistical signal processing, algorithmic development, physics based modeling, hardware optimization, and sensor fusion. Previously he was the Technical Lead of the Advanced Signal Processing Group at Spire Global, where he designed and led solutions for LEO space-based RF geolocation for both the government and private sectors. Additionally, he was a Sr. Research Engineer at the Southwest Research Institute where he worked in the Defense and Intelligence Division on direction finding antenna arrays, antenna array calibrations, and small satellite communication systems.

Matthew J. Murrian (BS, Mechanical Engineering, University of Central Florida; MS, Aerospace Engineering, University of Texas at Austin) is currently the Director of RF Intelligence at Spire Global. He was formerly a chief engineer at Coherent Technical Services, Inc. and a member of the UT Radionavigation Laboratory. He specializes in digital signal processing, software-defined radio, and multi-sensor navigation and perception. He is the lead developer of GRID GNSS software-defined radio.

Todd E. Humphreys (B.S., M.S., Utah State University; Ph.D., Cornell University) holds the Ashley H. Priddy Centennial Professorship in Engineering in the department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin. He is Director of the Wireless Networking and Communications Group and of the UT Radionavigation Laboratory, where he specializes in the application of optimal detection and estimation techniques to positioning, navigation, and timing. His awards include the UT Regents' Outstanding Teaching Award (2012), the NSF CAREER Award (2015), the ION Thurlow Award (2015), the PECASE (NSF, 2019), the IEEE Walter Fried Best Paper Award (2012, 2020, 2023), and the ION Kepler Award (2023). He is a Fellow of the Institute of Navigation and of the Royal Institute of Navigation.

ABSTRACT

This paper offers an experimental demonstration of single-satellite single-pass geolocation of a terrestrial Global Navigation Satellite System (GNSS) spoofer from Low Earth Orbit (LEO). The proliferation of LEO-based receivers can provide unprecedented spectrum awareness, enabling persistent GNSS interference detection and geolocation. Accurate LEO-based single-receiver emitter geolocation is possible when a range-rate time history can be extracted, traditionally accomplished

Preprint of the 2024 ION ITM Conference Long Beach, CA, Jan. 22-26, 2024

through Doppler measurements. However, Doppler-based measurement techniques assume the emitter transmits at a quasi-constant center frequency. This assumption is not true for GNSS spoofers, as they transmit an ensemble of spoofing signals wherein each spoofed signal's carrier frequency contains an unique unknown time-varying frequency component that imitates the Doppler corresponding to the spoofed navigation satellite and spoofed location. This paper presents a technique that removes the unknown time-varying frequency component across each signal so that the range-rate time history between receiver and transmitter can be extracted and exploited for geolocation. If a GNSS receiver allows itself to be spoofed, the range-rate between the receiver and the spoofer will manifest in the GNSS receiver's clock drift estimate. This technique is verified by a controlled experiment in partnership with Spire Global, in which a LEO-based receiver captures GNSS spoofing signals transmitted from a known ground station on a non-GNSS frequency band.

1. INTRODUCTION

The combination of easily-accessible low-cost GNSS spoofers and the emergence of increasingly-automated GNSS-reliant systems prompts a need for multi-layered defenses against GNSS spoofing. GNSS spoofers broadcast an ensemble of false GNSS signals intending that the victim receiver(s) will accept them as the authentic GNSS signals and subsequently infer a false position fix and/or a clock offset [1], [2]. A successful spoofing attack may lead to devastating consequences.

The academic community has long warned the public about the threat of GNSS spoofing [3]–[5]. Within the past decade, significant progress in has been made in onboard GNSS spoofing detection and mitigation [1]. 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 [6]–[11]. Consistency checks between the estimated signal and onboard inertial sensors can provide quick and reliable spoofing detection [12]–[14]. Monitoring the clock state can also be used to detect spoofing [15]. Cryptographic authentication techniques are currently being developed and implemented [16], [17].

Although the recent advances in onboard GNSS spoofing detection have been inspiring, many of the older GNSS receivers in current operation are unable to incorporate these defenses, leaving them vulnerable to attacks. For example, the civilian maritime and airline industries are encountering GNSS jamming and spoofing at an alarming rate. Anomalous positioning information broadcast by ships in Automatic Identification System (AIS) messages, and airplanes in Automatic Dependent Surveillance-Broadcast (ADS-B) messages are indicative of wide-spread jamming and spoofing. Ships and airplanes near the Eastern Mediterranean, the Baltic region, and Shanghai have fallen victim to spoofing, as they seemingly teleport to new locations.

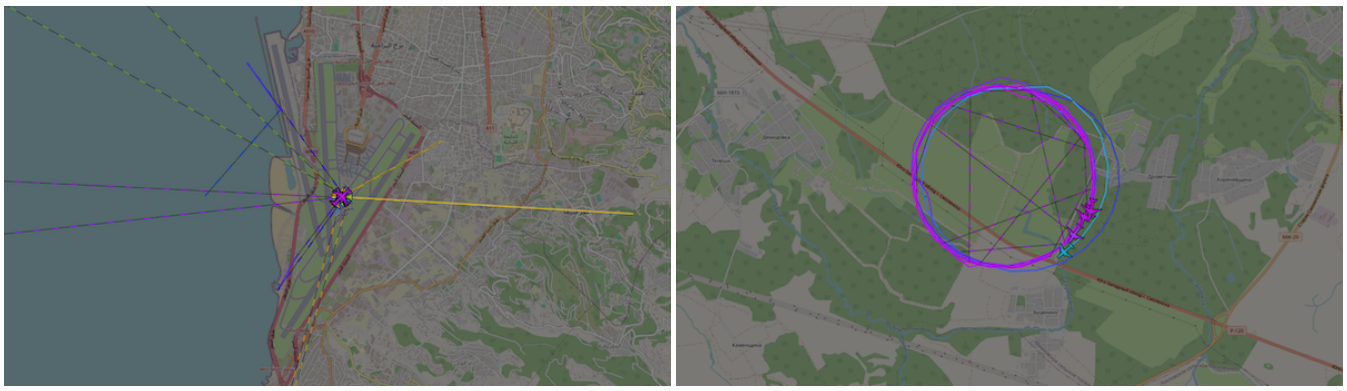

Fig. 1: Screenshots from the website ADS-B Exchange [18], the world's largest community of unfiltered ADS-B/Mode S/MLAT feeders. These screenshots show recent incidents of GNSS spoofing affecting aviation. The majority of spoofing induces false static locations, typically the location of airports (left). But within the past month, GNSS receivers have been spoofed to make them appear to be flying in circles (right).

Fig. 1 displays recent examples of aircraft ensnared by to GNSS spoofing, likely as unintended targets caught in the electronic warfare crossfire near ongoing conflict zones. From the ADS-B logs, one can infer that the most common spoofing attack is to transmit an ensemble of spoofing signals that is consistent with a single static location, typically a major airport. This type of spoofing is most likely used as a defense against commercial off-the-shelf drones, as these drones have built-in protocols to avoid protected airspace (e.g., surrounding airports). In a more alarming trend, spoofing attacks have caused

aircraft to be spoofed in circular trajectories. These spoofers appear to not be targeting individual GNSS receivers, but rather broadcasting their signals for general GNSS denial. However, an attacker could in theory tailor a spoofing trajectory for a specific target, causing a gradual pull-off from its true trajectory, luring the victim into restricted airspace. Given that many currently-deployed GNSS receivers are unable to defend themselves even against easy-to-detect broad-area spoofing attacks, such targeted attacks are a clear and present threat.

The traditional approach for GNSS security has been to develop onboard receiver spoofing detection and mitigation techniques. The future of GNSS security takes a more active approach: global, accurate, and persistent localization of the emitters threatening GNSS receivers. The proliferation of LEO-based receivers provides unprecedented spectrum awareness, enabling GNSS interference detection, classification, and geolocation [19]–[24]. Dedicated LEO constellations provide worldwide coverage with frequent revisit rates, allowing for an always-updating operating picture. Several commercial enterprises have seized the opportunity to deploy constellations of LEO satellites to provide spectrum monitoring and emitter geolocation as a service (e.g., Spire Global and Hawkeye360).

With multiple time-synchronized receivers, geolocation of emitters producing arbitrary wideband signals is possible and has been extensively studied [22], [23], [25]–[27]. Multiple time-synchronized receivers can exploit time- and frequency-difference-of-arrival (T/FDOA) measurements to estimate the emitter location. The authors of ththe current paper were able to geolocate over 30 GNSS interference sources across the Eastern Mediterranean and Ukraine from a dual-satellite time-synchronized capture [22], [23]. However, planning simultaneous multi-satellite captures to enable T/FDOA-based and direct geolocation can be difficult to coordinate and expensive, whereas single-satellite collects are straightforward and less costly. This paper focuses on single-satellite platforms.

Accurate single-satellite-based emitter geolocation is possible from Doppler measurements alone, provided that the emitter is transmitting at a quasi-constant frequency [20], [21], [28]–[30]. However, accurate single-satellite geolocation of emitters with arbitrary waveforms is impossible in general: if the signal's carrier cannot be tracked, only coarse received-signal-strength techniques can be applied for geolocation. In 2018, members of The University of Texas at Austin Radionavigation Lab (UT RNL) were able to geolocate a powerful 70-watt matched-code jammer operating in Syria to better than 300 meters using Doppler-based techniques [20]. One of the crucial assumptions of Doppler-based single-satellite geolocation is that the emitter transmits at a quasi-constant carrier frequency. Under this assumption, and assuming perfect stability of the reeciver clock, the received Doppler is equivalently the range-rate, up to a constant bias and scaling. If a transmitter introduces any significant level of complexity to the carrier-phase behavior, such as frequency modulation or clock dithering, the accuracy of Doppler-based single-satellite techniques degrades.

GNSS spoofers must be treated differently, as they do not transmit at a constant center frequency: they add an extra unknown time-varying frequency component to each spoofed signal, imitating the range-rate between the corresponding spoofed GNSS satellite and the counterfeit spoofed location. This added unknown time-varying frequency component renders raw observed Doppler-based geolocation for GNSS spoofers inaccurate. One of the key results in [21] is a technique that removes the unknown time-varying frequency component added by GNSS spoofers so that a range-rate time history can be extracted for geolocation. Furthermore, an analysis of how actual transmitter clock error and transmitter motion degrade the geolocation estimate is performed in [21]. A single-receiver spoofer geolocation technique based on counterfeit clock observables is also presented in [31], and makes a similar observation to [21], namely, that the spoofed clock bias of a mobile drone can be used for geolocation. However, [31] only considers the spoofed pseudorange measurements, whereas [21] and the current paper incorporate both pseudorange and Doppler measurements, and [31] depends on a static initialization period, which is not possible in LEO.

The key observation of [21] is that each spoofed navigation signal will share a common frequency shift due to the range-rate between the LEO receiver and terrestrial spoofer. If a GNSS receiver processes enough spoofing signals to form a navigation solution, the estimator will lump the common frequency shift of each signal from the shared range-rate into the receiver clock offset rate (clock drift) estimate. Therefore, the time history of the spoofed receiver clock offset rate can be exploited for geolocation because the range-rate between LEO receiver and terrestrial spoofer is embedded in this measurement.

This paper offers an experimental demonstration of the single-satellite single-pass geolocation technique introduced in [21]. This demonstration is the first of its kind in the public domain. In this experiment, conducted in partnership with Spire Global, an ensemble of self-consistent spoofing signals was transmitted from a ground station and captured by an overhead LEO receiver. The transmitted signals were centered at S-band to avoid interference in the GNSS bands and for FCC and ITU compliance. The GNSS spoofing signals were processed by the UT RNL GRID receiver [32], [33] to generate a clock offset rate time history, followed by geolocation of the GNSS spoofer.

2. MEASUREMENT MODELS

2.1 GNSS Spoofing Signals

The goal of a GNSS spoofer is to deceive the victim receiver(s) into inferring a false position, velocity, and timing (PVT) solution, denoted $\tilde{\boldsymbol{x}} = [\, \boldsymbol{r}_{\tilde{\mathrm{R}}}^{\mathrm{T}},\ \delta t_{\tilde{\mathrm{R}}},\ \boldsymbol{v}_{\tilde{\mathrm{R}}}^{\mathrm{T}},\ \delta \dot{t}_{\tilde{\mathrm{R}}} \,]^{\mathrm{T}}$, where $\boldsymbol{r}_{\tilde{\mathrm{R}}}$ is the spoofed position, $\delta t_{\tilde{\mathrm{R}}}$ is the spoofed clock offset, $\boldsymbol{v}_{\tilde{\mathrm{R}}}$ is the spoofed velocity, and $\delta \dot{t}_{\tilde{\mathrm{R}}}$ is the spoofed clock offset rate. In order for the spoofer to achieve a successful attack, it must generate an ensemble of self-consistent signals. To this end, the attacker must (1) select a PVT solution for the victim to infer, (2) select an ensemble of GNSS satellites to spoof, and (3) for each spoofed navigation satellite, generate a signal with a navigation message, code phase time history, and carrier phase time history consistent with (1) and (2).

The spoofer must add an unique Doppler component to each spoofing signal that mimics the combined Doppler of the following components: (1) the range-rate between the spoofed satellite and spoofed position and velocity, (2) the spoofed receiver clock state, and (3) the clock state of the spoofed satellite. Additionally, the code phase and carrier phase time histories must be mutually consistent to avoid code-carrier divergence. Following this, the Doppler of the ith transmitted spoofing signal, denoted $\tilde{f}_i$, may be modeled as [21]

$$\tilde{f}_i(t) = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{R}},i}^{\mathrm{T}}(t)\left(\boldsymbol{v}_{\tilde{\mathrm{R}}}(t) - \boldsymbol{v}_{\tilde{\mathrm{s}},i}(t)\right) - \frac{c}{\lambda}\left(\delta \dot{t}_{\tilde{\mathrm{R}}}(t) - \delta \dot{t}_{\tilde{\mathrm{s}},i}(t)\right) \tag{1}$$

where λ is the carrier wavelength, c is the speed of light, $\hat{\boldsymbol{r}}_{\tilde{\mathrm{R}},i}$ is the unit vector pointing from the ith spoofed navigation satellite to the spoofed position in Earth-centered-Earth-fixed (ECEF) coordinates, $\boldsymbol{v}_{\tilde{\mathrm{R}}}$is the spoofed receiver velocity, $\boldsymbol{v}_{\tilde{\mathrm{s}},i}$ is the ith spoofed navigation satellite velocity, and $\delta \dot{t}_{\tilde{\mathrm{s}},i}$ is the spoofed frequency error of the ith navigation satellite.

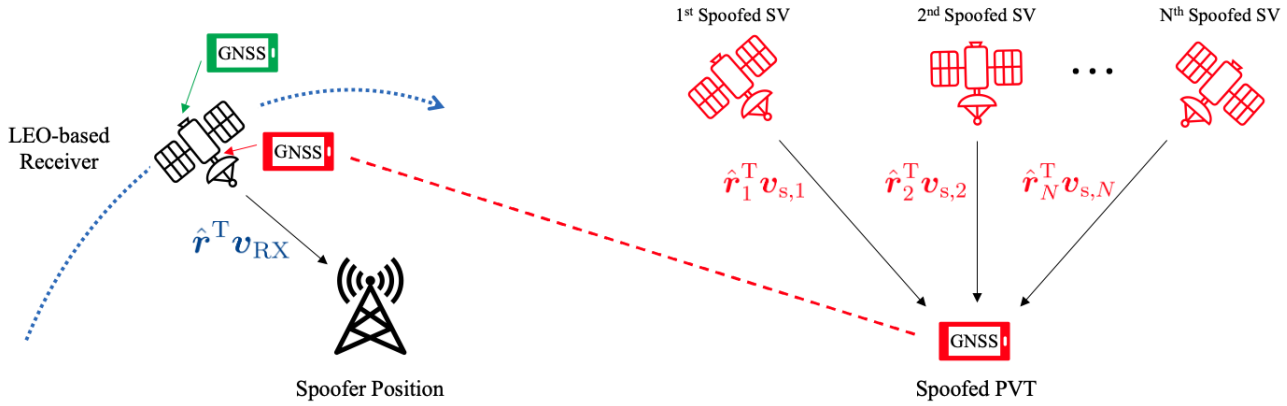

Fig. 2: A scenario in which a LEO-based satellite receives GNSS spoofing signals from a static terrestrial GNSS spoofer. The LEO-based satellite has a zenith-facing antenna that feeds the authentic GNSS signals to the onboard GNSS receiver, allowing for a precise PVT solution. The satellite also has a nadir-facing antenna which receives the spoofing signals. If the spoofing signals captured by the nadir-facing antenna are processed by a GNSS receiver, the receiver will produce the PVT solution induced by the spoofer. All of the observed spoofed signals will be subject to a common Doppler shift due to the range-rate between the spoofer and the LEO-based receiver.

Now consider the scenario where a dynamic receiver captures an ensemble of transmitted spoofing signals from a static terrestrial spoofer, as shown in Fig. 2. It is likely that a would-be spoofer is static, otherwise would be difficult for the spoofer to compensate for its own motion, resulting in easily-detectable false signals. Each observed signal at the receiver will contain the same corresponding Doppler shift due to the the relative motion between the spoofer and the receiver. Each observed signal will also see the same frequency shift due to the actual frequency error of the transmitter and the actual frequency error of the receiver. In a properly-designed capture platform, the frequency error of the receiver is known and can

be compensated for. Dropping the time indices for clarity, the observed Doppler of the ith spoofing signal at the dynamic receiver f_i may be written as [21]

$$\begin{aligned} f_i &= \tilde{f}_i - \frac{1}{\lambda}\hat{\boldsymbol{r}}^{\mathsf{T}}\boldsymbol{v}_{\mathrm{RX}} - \frac{c}{\lambda}\left(\delta\dot{t}_{\mathrm{RX}} - \delta\dot{t}_{\mathrm{TX}}\right) \\ &= -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{R}},i}^{\mathsf{T}}\left(\boldsymbol{v}_{\tilde{\mathrm{R}}} - \boldsymbol{v}_{\tilde{\mathrm{s}},i}\right) - \frac{c}{\lambda}(\delta\dot{t}_{\tilde{\mathrm{R}}} - \delta\dot{t}_{\tilde{\mathrm{s}},i}) - \frac{1}{\lambda}\hat{\boldsymbol{r}}^{\mathsf{T}}\boldsymbol{v}_{\mathrm{RX}} - \frac{c}{\lambda}\left(\delta\dot{t}_{\mathrm{RX}} - \delta\dot{t}_{\mathrm{TX}}\right) \end{aligned} \tag{2}$$

where $\hat{\boldsymbol{r}}$ is the unit vector pointing from the transmitter (spoofer) to the LEO-based receiver, $\boldsymbol{v}_{\mathrm{RX}}$ is the velocity of the LEO-based receiver, $\delta\dot{t}_{\mathrm{RX}}$ is the actual frequency error of the receiver, and $\delta\dot{t}_{\mathrm{TX}}$ is the actual frequency error of the transmitter (spoofer).

What makes single-satellite GNSS spoofer geolocation difficult is the $\tilde{f}_i$ term, as it is unknown, time-varying, and different across each spoofed signal. In the case of the matched-code jammer discovered in [20], $\tilde{f}_i = 0$. One may suppose that the operator's intent was not to deceive victim receivers into inferring false locations like a spoofer. In this case, the raw observed Doppler can be modeled as the range-rate between transmitter and receiver, with a constant measurement bias over the capture due to the clock drift of the transmitter. Contrariwise, geolocation with the raw observed Doppler modeled as 2 will yield final position estimates that are biased because the spoofing signals contain the unmodeled $\tilde{f}_i(t)$ term, which is time-varying and unknown. In the next section, a technique will be presented that removes $\tilde{f}_i(t)$ and extracts the range-rate between transmitter and receiver.

2.2 Observed Doppler Model of Authentic Signals

As a brief review, a standalone GNSS receiver estimates its PVT with pseudorange and Doppler measurements. [34]. The GNSS receiver's PVT estimator's goal is to achieve an optimal estimate of 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's position, δt_{R} is the receiver's clock offset, $\boldsymbol{v}_{\mathrm{R}}$ is the receiver's velocity, and $\delta\dot{t}_{\mathrm{R}}$ is the receiver's clock offset rate. The Doppler measurement can be derived from the carrier phase measurement; a full derivation can be found in [21], [35]. Now, consider the approximate Doppler measurement model for authentic navigation signals. Dropping the time indices, the approximate Doppler measurement model corresponding to the ith satellite's Doppler $f_{\mathrm{d},i}$ is

$$f_{\mathrm{d},i} = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{R},i}^{\mathsf{T}}\left(\boldsymbol{v}_{\mathrm{R}} - \boldsymbol{v}_{\mathrm{s},i}\right) - \frac{c}{\lambda}\left(\delta\dot{t}_{\mathrm{R}} - \delta\dot{t}_{\mathrm{s},i}\right) + w_{\mathrm{d},i} \tag{3}$$

where $\hat{\boldsymbol{r}}_{\mathrm{R},i}$ is the unit vector pointing from the ith navigation satellite to the receiver in ECEF coordinates, $\boldsymbol{v}_{\mathrm{R}}$ is the receiver velocity, $\boldsymbol{v}_{\mathrm{s},i}$ is the ith navigation satellite velocity, $\delta\dot{t}_{\mathrm{R}}$ is the frequency error of the receiver, $\delta\dot{t}_{\mathrm{s},i}$ is the frequency error of the ith navigation satellite, and $w_{\mathrm{d},i}$ is zero-mean Gaussian noise. This is only an approximate model, as the full Doppler measurement model contains a $\delta\dot{t}_{\mathrm{R}}\delta\dot{t}_{\mathrm{s},i}$ term. But, because this term is nearly zero, it is negligible and can be dropped. The ith GNSS satellite's transmitted navigation message contains its position, velocity, and clock frequency error, meaning $\boldsymbol{v}_{\mathrm{s},i}$ and $\delta\dot{t}_{\mathrm{s},i}$ are known. Assuming the receiver is static, the state to be estimated becomes $\boldsymbol{x} = [\,\boldsymbol{r}_{\mathrm{R}}^{\mathsf{T}},\ \delta t_{\mathrm{R}},\ \delta\dot{t}_{\mathrm{R}}\,]^{\mathsf{T}}$. The Doppler measurement then reduces to

$$f_{\mathrm{d},i} = \frac{1}{\lambda}\hat{\boldsymbol{r}}_{\mathrm{R},i}^{\mathsf{T}}\boldsymbol{v}_{\mathrm{s},i} - \frac{c}{\lambda}\left(\delta\dot{t}_{\mathrm{R}} - \delta\dot{t}_{\mathrm{s},i}\right) + w_{\mathrm{d},i} \tag{4}$$

Notice that $\delta\dot{t}_{\mathrm{R}}$ is the only term that is common across all Doppler measurements. The significance of this observation will be revealed in the following section.

3. SINGLE-SATELLITE SPOOFER GEOLOCATION

As discussed in the prior section, the observed Doppler of the ith spoofing signal is a combination of the physical range-rate between the the transmitter and receiver, and a Doppler component that mimics the motion between the ith spoofed satellite

and the spoofed position and velocity. The common-mode Doppler components across all spoofing signals from (2) are emphasized below

$$f_i = \underbrace{-\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{R}},i}^{\mathsf{T}}\left(\boldsymbol{v}_{\tilde{\mathrm{R}}} - \boldsymbol{v}_{\tilde{\mathrm{s}},i}\right) - \frac{c}{\lambda}\Big(\overbrace{\delta\dot{t}_{\tilde{\mathrm{R}}}}^{\text{common}} - \delta\dot{t}_{\tilde{\mathrm{s}},i}\Big)}_{\text{Spoofed Component}} \underbrace{\overbrace{-\frac{1}{\lambda}\hat{\boldsymbol{r}}^{\mathsf{T}}\boldsymbol{v}_{\mathrm{RX}} - \frac{c}{\lambda}\left(\delta\dot{t}_{\mathrm{RX}} - \delta\dot{t}_{\mathrm{TX}}\right)}^{\text{common}}}_{\text{Physical Range-rate and Clocks}} + w_{\mathrm{d},i} \tag{5}$$

The common Doppler terms across all spoofed signals can be rearranged as follows

$$f_i = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{R}},i}^{\mathsf{T}}\left(\boldsymbol{v}_{\tilde{\mathrm{R}}} - \boldsymbol{v}_{\tilde{\mathrm{s}},i}\right) + \frac{c}{\lambda}\delta\dot{t}_{\tilde{\mathrm{s}},i} \underbrace{-\frac{1}{\lambda}\hat{\boldsymbol{r}}^{\mathsf{T}}\boldsymbol{v}_{\mathrm{RX}} - \frac{c}{\lambda}\left(\delta\dot{t}_{\mathrm{RX}} - \delta\dot{t}_{\mathrm{TX}}\right) - \frac{c}{\lambda}\delta\dot{t}_{\tilde{\mathrm{R}}}}_{\text{Common Terms}} + w_{\mathrm{d},i} \tag{6}$$

All of the common Doppler terms can be lumped into a single term γ:

$$f_i = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{R}},i}^{\mathsf{T}}\left(\boldsymbol{v}_{\tilde{\mathrm{R}}} - \boldsymbol{v}_{\tilde{\mathrm{s}},i}\right) - \frac{c}{\lambda}\left(\gamma - \delta\dot{t}_{\tilde{\mathrm{s}},i}\right) + w_{\mathrm{d},i} \tag{7}$$

For the case in which the spoofer attempts to make the victim infer a static location,

$$f_i = \frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{R}},i}^{\mathsf{T}}\boldsymbol{v}_{\tilde{\mathrm{s}},i} - \frac{c}{\lambda}\left(\gamma - \delta\dot{t}_{\tilde{\mathrm{s}},i}\right) + w_{\mathrm{d},i} \tag{8}$$

where

$$\gamma(t) = \frac{1}{c}\hat{\boldsymbol{r}}^{\mathsf{T}}(t)\boldsymbol{v}_{\mathrm{RX}}(t) + \delta\dot{t}_{\mathrm{RX}} - \delta\dot{t}_{\mathrm{TX}} + \delta\dot{t}_{\tilde{\mathrm{R}}} \tag{9}$$

The apparent clock offset rate of the victim is $\gamma(t)$, which contains all common Doppler terms. Notice that the form of (3) is identical that of (7) and the form of (4) is identical that of (8). The only term that has changed is the receiver clock offset rate, which was replaced with $\gamma(t)$. In other words, the GNSS receiver's PVT estimator will infer the state $\boldsymbol{x}(t) = [\, \boldsymbol{r}_{\tilde{\mathrm{R}}}(t)^{\mathsf{T}},\ \delta t_{\tilde{\mathrm{R}}}(t),\ \boldsymbol{v}_{\tilde{\mathrm{R}}}(t)^{\mathsf{T}},\ \gamma(t)\,]^{\mathsf{T}}$, which is composed of the spoofed position, spoofed velocity, and the new receiver clock offset rate $\gamma(t)$. The PVT estimator will attribute common-mode frequency deviations across received signals to the receiver's clock offset rate. At each navigation epoch, the PVT estimator will produce an optimal estimate of $\gamma(t)$. Importantly, $\gamma(t)$ is unaffected by the unknown time-varying Doppler component of each individual spoofing signal.

The other three terms, $\delta\dot{t}_{\mathrm{RX}}$, $\delta\dot{t}_{\mathrm{TX}}$, and $\delta\dot{t}_{\tilde{\mathrm{R}}}$ are potential sources that can contribute to geolocation error. However, their contributions are typically minor. If the satellite's GNSS receiver and the front-end controlling the sampling for the capture containing the spoofing signals are driven by the same oscillator, the $\delta\dot{t}_{\mathrm{RX}}$ is known from the onboard GNSS receiver output. It is also assumed the transmitter is operating in steady-state conditions so that $\delta\dot{t}_{\mathrm{TX}}$ can be modeled as constant over a short (e.g., 60-second) data capture and can be estimated [20]. An analysis on how $\delta\dot{t}_{\mathrm{TX}}$ corrupts the geolocation estimate was conducted in [20], [21]. The spoofed clock offset rate $\delta\dot{t}_{\tilde{\mathrm{R}}}$ can also be modeled as constant. This is because 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, spoofing will be suspected by the victim. In other words, if the spoofer introduces any complexity or dithering to its oscillator, or attempts to imbue a quickly-varying spoofed clock offset rate, the ability to geolocate is degraded, however, the spoofing signals will be easy to detect at victim receivers.

The time history of $\gamma(t)$ can ultimately be used for geolocation because the range-rate between the LEO-based receiver and the terrestrial spoofer appears in the first term. Information about the transmitter's location is embedded in he time-history of $\hat{\boldsymbol{r}}^{\mathsf{T}}(t)\boldsymbol{v}_{\mathrm{RX}}(t)$. Based on the above Doppler measurement model, a nonlinear least-squares estimator for the time history of $\gamma(t)$ can be developed to estimate the unknown transmitter position and clock frequency bias [20]. In this case, the constant frequency bias come from the addition of $\delta\dot{t}_{\mathrm{TX}}$ and $\delta\dot{t}_{\tilde{\mathrm{R}}}$. Furthermore, an altitude constraint on the emitter's position should be incorporated to significantly improve the observability.

4. EXPERIMENTAL SETUP

The developed single-satellite geolocation technique applying specifically to GNSS spoofers was verified in a joint demonstration between the UT RNL and Spire Global. In this experiment, an ensemble of self-consistent spoofing signals was transmitted from a ground station while an overhead LEO receiver performed a raw capture. This section details the experimental setup and special adaptations that had to made to transmit the signals.

4.1 Experimental Design

The UT RNL provided a baseband binary file containing an ensemble of GNSS spoofing signals to be transmitted. The spoofing file was a filtered and downsampled version of the "clean static" recording in the TEXBAT dataset [36]. The original recording was a high-quality 16-bit 25 Msps (complex) recording of authentic GNSS signals centered at GPS L1 from a static antenna on top of the former Aerospace Engineering building. The front-end in the original recording was disciplined to a 10-MHz oven controlled crystal oscillator (OCXO). Lowpass filtering and downsampling of the original file was required to ensure the transmitted signal was contained within Spire's available bandwidth so no aliasing would occur.

The spoofing file was transmitted from a ground station located in Perth, Australia. The transmitted spoofing signals were centered at S-band to avoid interference in the GNSS bands and for FCC and ITU compliance. Spire Global owns a 5 MHz slice of S-band, centered at 2032.5 MHz. While the ground station was transmitting the spoofing file, an overhead LEO-based receiver performed a raw capture. This was a 20-second capture centered at 2032.5 MHz, sampled at 5 Msps complex. In practice, the duration of the raw capture should be as long as a frame in the spoofed navigation message, so in the case of GPS L1/CA, that would be 30 seconds. This ensures that the entire spoofed satellite ephemeris for each spoofed satellite can be decoded. Fig. 3 shows the relevant portions of the demonstration. In the context of this paper, the physical location of the spoofer is in Perth, Australia and the spoofed PVT the target will infer is a static location atop the former Aerospace Engineering building in Austin, Texas. The goal is to geolocate the spoofer's position in Perth, Australia using a raw capture from an overhead LEO-based receiver.

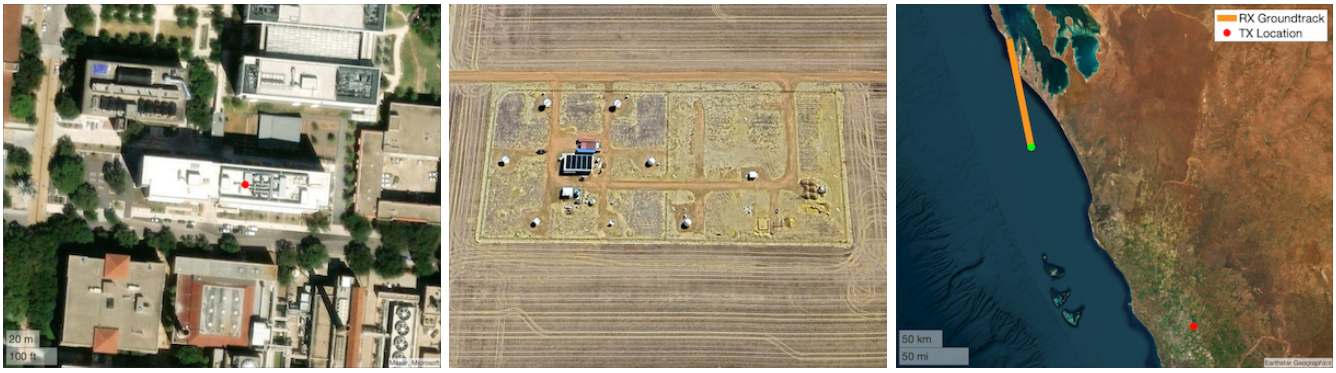

Fig. 3: The UT RNL provided a baseband binary file containing an ensemble of GNSS spoofing signals that would spoof a target receiver to the top of the former Aerospace Engineering building in Austin, Texas (left). This spoofing file was transmitted on a slice of S-band owned by Spire Global from a ground station located in Perth, Australia (middle). An overhead LEO satellite performed a 20 second raw capture (right).

4.2 Adaptations for the S-band Transmitter

As mentioned before, the spoofing signals were transmitted at S-band to avoid interference on the GNSS bands. The original Doppler component added to each spoofing signal was with respect to the original GPS L1 frequency, whereas the Doppler due to the range-rate between the receiver and transmitter was with respect to the S-band frequency. Because of this, several adaptations had to be made when processing the received samples.

If the GNSS receiver processing the spoofing signals makes the assumption that all Doppler shifts are with respect to the GPS L1 frequency, although the true carrier is at S-band, the receiver clock offset rate $\gamma(t)$ will have a different scaling factor. The received Doppler of the ith spoofing signal follows

$$f_i = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{R}},i}^{\mathsf{T}}\left(\boldsymbol{v}_{\tilde{\mathrm{R}}} - \boldsymbol{v}_{\tilde{\mathrm{s}},i}\right) - \frac{c}{\lambda}\left(\delta\dot{t}_{\tilde{\mathrm{R}}} - \delta\dot{t}_{\tilde{\mathrm{s}},i}\right) - \frac{1}{\lambda_{\mathrm{S}}}\hat{\boldsymbol{r}}^{\mathsf{T}}\boldsymbol{v}_{\mathrm{RX}} - \frac{c}{\lambda_{\mathrm{S}}}\left(\delta\dot{t}_{\mathrm{RX}} - \delta\dot{t}_{\mathrm{TX}}\right) + w_{\mathrm{d},i} \tag{10}$$

where λ_{S} is the wavelength of the S-band carrier. Once again, all common terms can be lumped into the frequency common term $\gamma_{\mathrm{S}}(t)$:

$$f_i = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{R}},i}^{\mathsf{T}}\left(\boldsymbol{v}_{\tilde{\mathrm{R}}} - \boldsymbol{v}_{\tilde{\mathrm{s}},i}\right) - \frac{c}{\lambda}\left(\gamma_{\mathrm{S}} - \delta\dot{t}_{\tilde{\mathrm{S}},i}\right) + w_{\mathrm{d},i} \tag{11}$$

Here, $\gamma_{\mathrm{S}}(t)$ is defined as

$$\gamma_{\mathrm{S}}(t) = \frac{\lambda}{c\lambda_{\mathrm{S}}}\hat{\boldsymbol{r}}^{\mathsf{T}}(t)\boldsymbol{v}_{\mathrm{RX}}(t) + \frac{\lambda}{\lambda_{\mathrm{S}}}\left(\delta\dot{t}_{\mathrm{RX}} - \delta\dot{t}_{\mathrm{TX}}\right) + \delta\dot{t}_{\tilde{\mathrm{R}}} \tag{12}$$

Of course, this is just a constant scaling factor of the measurements, which the estimator can easily compensate for. The actual processing of the received spoofing signals by the GNSS receiver becomes more involved. When the GNSS receiver processes the spoofing signals, it will see strong code-carrier divergence. The original compression and dilation of the baseband signal and its Doppler shift was at GPS L1. However, there will be an additional compression and dilation of the baseband signal and Doppler shift, but this time with respect to the S-band frequency. This results in disagreeing tracking loops, namely, the GNSS receiver's delay lock loop (DLL) and phase lock loop (PLL).

To emphasize this, consider the GNSS signal model during an accumulation period. Let v_{LOS} be the line-of-sight velocity of the original GPS navigation satellite with respect to the original receiver, which is modeled as constant over an accumulation interval. Let $\beta = v_{\mathrm{LOS}}/c$, F_{c} be the original signal's center frequency, $\bar{F}_{\mathrm{c}}$ be the original receiver's capture center frequency, and $C(t)$ be the signal's spreading code. Then the baseband model of the original recorded signal $r(t)$ is

$$r(t) = C\left[(t-t_0)(1-\beta)\right]\exp\left[j2\pi[F_{\mathrm{c}}(1-\beta) - \bar{F}_{\mathrm{c}}](t-t_0)\right] \tag{13}$$

Now, consider $s_{\mathrm{TX}}(t)$, the signal when transmitted at the S-band frequency F_{S}:

$$s_{\mathrm{TX}}(t) = C\left[(t-t_0)(1-\beta)\right]\exp\left[j2\pi[F_{\mathrm{c}}(1-\beta) - \bar{F}_{\mathrm{c}} + F_{\mathrm{S}}](t-t_0)\right] \tag{14}$$

The signal as received by LEO-based receiver depends on $v_{\mathrm{LOS,\,S}}$, the line-of-sight velocity from the S-band transmitter to the LEO-based receiver, and on $\bar{F}_{\mathrm{S}}$, the center frequency of the capture at the LEO-based receiver. Let $\beta_{\mathrm{S}} = v_{\mathrm{LOS,\,S}}/c$ and $A(t)$ be the received amplitude of the signal. Then received signal during an accumulation interval, $s_{\mathrm{RX}}(t)$, is

$$s_{\mathrm{RX}}(t) = A(t)C\left[(t-t_0)(1-\beta)(1-\beta_{\mathrm{S}})\right]\exp\left[j2\pi[F_{\mathrm{c}}(1-\beta) - \bar{F}_{\mathrm{c}} + F_{\mathrm{S}}(1-\beta_{\mathrm{S}}) - \bar{F}_{\mathrm{S}}](t-t_0)\right] \tag{15}$$

Now, assume that $\bar{F}_{\mathrm{c}} = F_{\mathrm{c}}$, $\bar{F}_{\mathrm{S}} = F_{\mathrm{S}}$, and $\beta\beta_{\mathrm{S}} = 0$. Then $s_{\mathrm{RX}}(t)$ becomes

$$s_{\mathrm{RX}}(t) = A(t)C\left[(t-t_0)(1-\beta-\beta_{\mathrm{S}})\right]\exp\left[j2\pi[-F_{\mathrm{c}}\beta - F_{\mathrm{S}}\beta_{\mathrm{S}}](t-t_0)\right] \tag{16}$$

The carrier Doppler of this signal appears to be $F_{\mathrm{D}} = F_{\mathrm{c}}\beta + F_{\mathrm{S}}\beta_{\mathrm{S}}$. If the GNSS receiver assumes that the carrier of the received signal is at GPS L1, the PLL-aided DLL will apply a spreading code replica $C\left[(t-t_0)(1-\beta_{\mathrm{DLL}})\right]$ with

$$\beta_{\mathrm{DLL}} = \frac{-F_{\mathrm{D}}}{F_{\mathrm{c}}} = \frac{-F_{\mathrm{c}}\beta + F_{\mathrm{S}}\beta_{\mathrm{S}}}{F_{\mathrm{C}}} = \beta + \frac{F_{\mathrm{S}}}{F_{\mathrm{c}}}\beta_{\mathrm{S}} \tag{17}$$

whereas the correct value is $\beta^{*}_{\mathrm{DLL}} = \beta + \beta_{\mathrm{S}}$. One potential work-around is to change the GNSS receiver's configuration so that it it knows that it is tracking a signal at F_{S} rather than $F_{\mathrm{c}} = F_{\mathrm{L1}}$. In doing so

$$\beta^{\mathrm{S}}_{\mathrm{DLL}} = \frac{-F_{\mathrm{D}}}{F_{\mathrm{c}}} = \frac{F_{\mathrm{c}}}{F_{\mathrm{S}}}\beta + \beta_{\mathrm{S}} \tag{18}$$

Note that since $\beta_{\mathrm{S}} \gg \beta$, $\beta^{\mathrm{S}}_{\mathrm{DLL}}$ is closer to β^{*}_{DLL} than β_{DLL} is. However, neither β_{S} nor $\beta^{\mathrm{S}}_{\mathrm{DLL}}$ are actually correct. To fully compensate for this effect, β or β_{S} must be truly known to do proper carrier-aided code tracking, otherwise there will always be an error. The solution to the code-carrier divergence problem invoked by this paper will be discussed in the next section.

5. EXPERIMENTAL RESULTS

5.1 Geolocation with Receiver Clock Offset Rate $\gamma(t)$

This section presents the experimental results with the advocated technique in this paper. The transmitted spoofing signals were captured and processed with the UT RNL's GRID software-defined GNSS receiver [32], [33]. Shown in Fig. 4 is the processed PVT solution of the pseudorange and Doppler measurements of the spoofing signals. On GRID's display, the large Doppler shifts across each signal are immediately noticeable. Once again, this large Doppler shift manifests because

of the range-rate between the LEO-based receiver and terrestrial transmitter. GRID was also able to compute the spoofed PVT solution corresponding to the top of the Aerospace Engineering building. The position solution is slightly biased, but that is explained by the code-carrier divergence from the S-band carrier presented in the prior section.

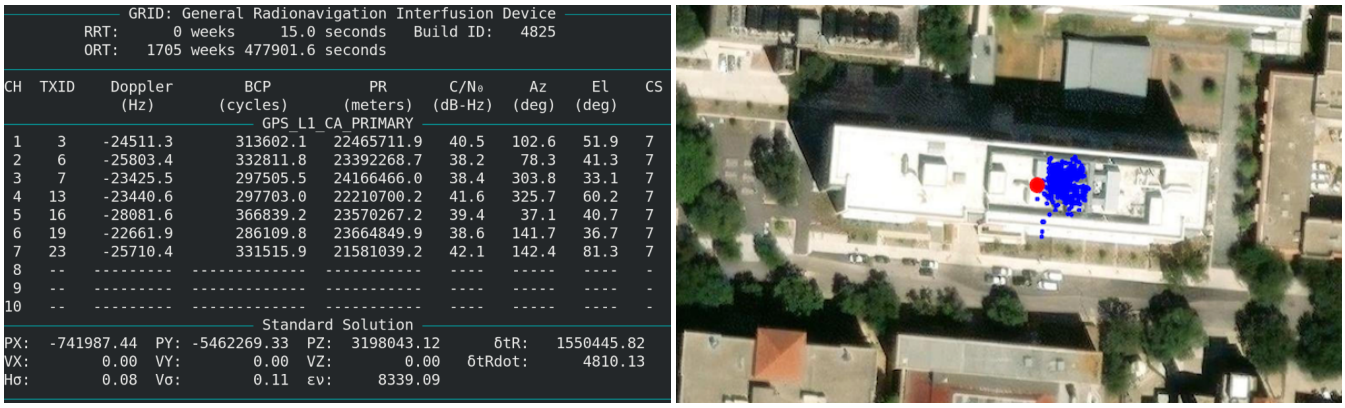

Fig. 4: Shown on the left is the UT RNL's GRID receiver processing the spoofing signals. Shown on the right is a scatter of position solutions obtained by GRID. Immediately noticeable are the large Doppler shifts and clock offset rate estimate (in m/s). This is due to the range-rate between LEO-based receiver and terrestrial spoofer.

To coax GRID into properly processing the S-band spoofing signals, special modifications to the receiver's estimator had to be made. Firstly, the spoofing signals were processed by GRID to extract the navigation data bits of each spoofing signal. Because this was only a 20 second capture, the full precise ephemerides were also retrieved. Now that the spoofed navigation message and the exact data bits are fully known, the receiver can calculate a full PVT solution. The next stage of processing involved importing the precise ephemerides into the receiver, which allowing for a full navigation solution to be calculated towards the end of the 20 second capture. A polynomial fit was taken to this solution so that the navigation solution at the beginning of the capture could be extrapolated. Finally, the spoofing signals were processed again in a complete "hot start" mode wherein the precise ephemerides and receiver state are both fully known, allowing for a navigation solution to be calculated for the full 20 second capture.

Additionally, a few other considerations had to be made. The bandwidth of the receiver's tracking loops, namely the DLL and PLL, were increased to help maintain lock despite the code-carrier divergence introduced by the S-band carrier. The bandwidth of the DLL was set to 1.5 Hz and the bandwidth of the PLL was set to 40 Hz, introducing more noise. Under nominal operation for a static receiver on the surface of the Earth, such as a high quality reference station, the DLL bandwidth can be as small as .003 Hz and the PLL bandwidth as small as 5 Hz. Furthermore, changes to the receiver's clock model had be made to account for the quickly drifting receiver clock, induced by the range-rate between LEO-based receiver and terrestrial transmitter. The clock model used set $h_0 = 5 \times 10^{-18}$ and $h_{-2} = 3 \times 10^{-18}$, allowing the estimator to accept the quickly-varying clock offset rate.

Given all of this, $\gamma(t)$ could be calculated over the entire 20 second capture, as shown in Fig. 5. The GNSS receiver allowed itself to be spoofed and the true range-rate between LEO-based receiver and terrestrial transmitter was lumped in the receiver's clock offset rate estimate. The time-history of $\gamma(t)$ was fed to the nonlinear least-squares estimator and the final position fix is shown in Fig. 6. The final position error was 361 meters, but most importantly, the true emitter position lay within the 95% error ellipse. The error ellipse is highly eccentric. However, the error ellipse's eccentricity is solely dictated by the receiver-transmitter geometry. Shown in Fig. 7 are the Doppler residuals with respect to the true emitter position and the final estimated position. The post-fit Doppler residuals with respect to the estimated spoofer position are zero-mean and Gaussian, which exactly what is expected from a properly modeled system with Gaussian noise.

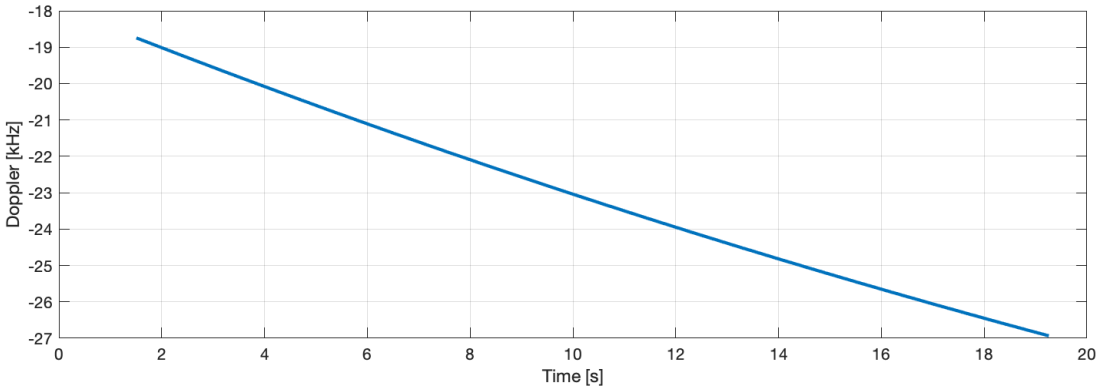

Fig. 5: Time history of $\gamma(t)$, which contains the frequency time history due to the range-rate between the LEO receiver and the physical location of the spoofer. This time history is exploited for geolocation.

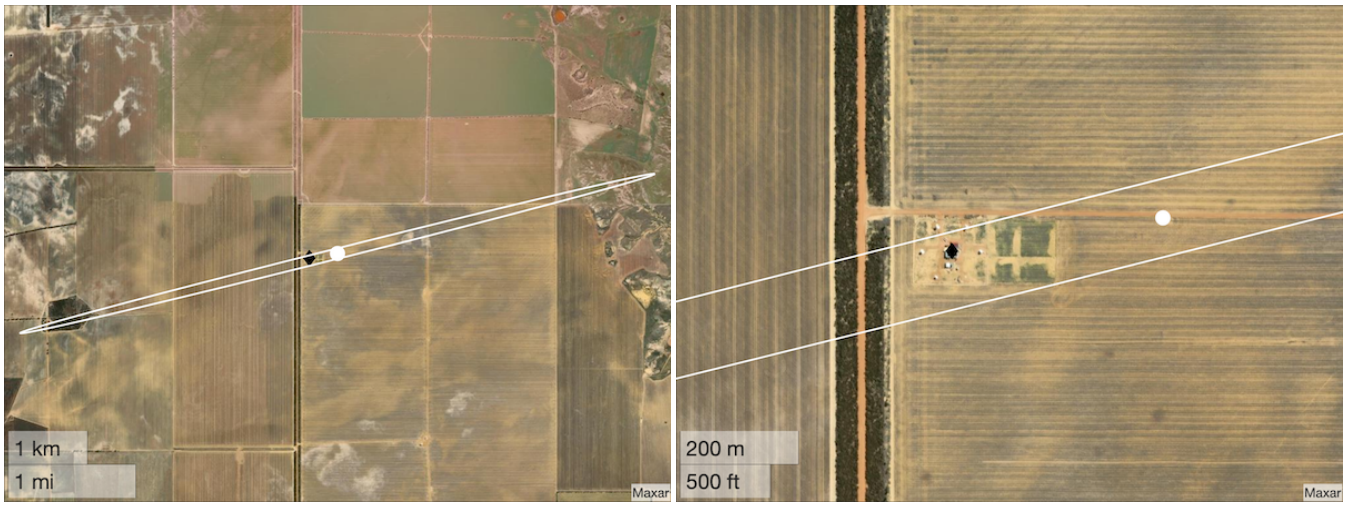

Fig. 6: Final spoofer position estimate using $\gamma(t)$. The true emitter position is shown as the black diamond. The error of the final estimate is 361 meters. The emitter is contained by the 95% error ellipse, which has a semi-major of 4.1 km.

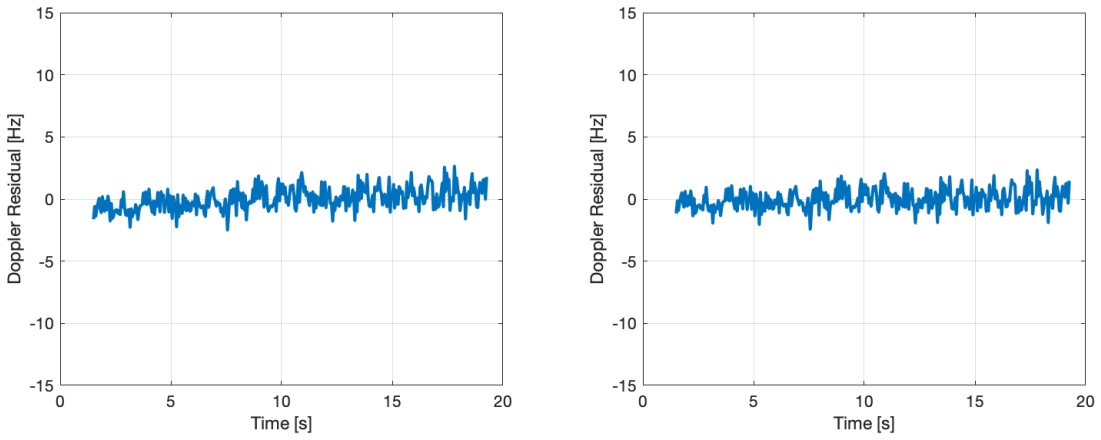

Fig. 7: Doppler residuals with respect to truth (left) and final position estimate (right). The post-fit Doppler residuals with respect to the estimated spoofer position are zero-mean and Gaussian.

5.2 Geolocation with Raw Received Doppler

Now, suppose that a LEO-based receiver was only able to downlink GNSS observables. Furthermore, envision a scenario where the receiver tracking spoofing signals from a terrestrial spoofer. One could attempt to geolocate the spoofer by using the Doppler time history of each spoofed signal. Of course, as shown earlier, this will yield a biased estimate of the spoofer's position because the time-varying frequency term is completely ignored. However, if the spoofer is spoofing the victim(s) to a static location on the surface of the Earth, the bias might not be that large. This is because the Doppler rate between a static receiver on the surface of the Earth and a GPS satellite in medium Earth orbit (MEO) is never more than 1 Hz per second, typically much smaller. The range-rate between the LEO-based receiver and the physical location spoofer will be the dominating term in the Doppler time history. The Doppler time history for each spoofed signal in this experiment is shown in Fig. 8. The Doppler time history of each spoofed signal maintains the same overall shape because the dominating term is the range-rate between receiver and spoofer.

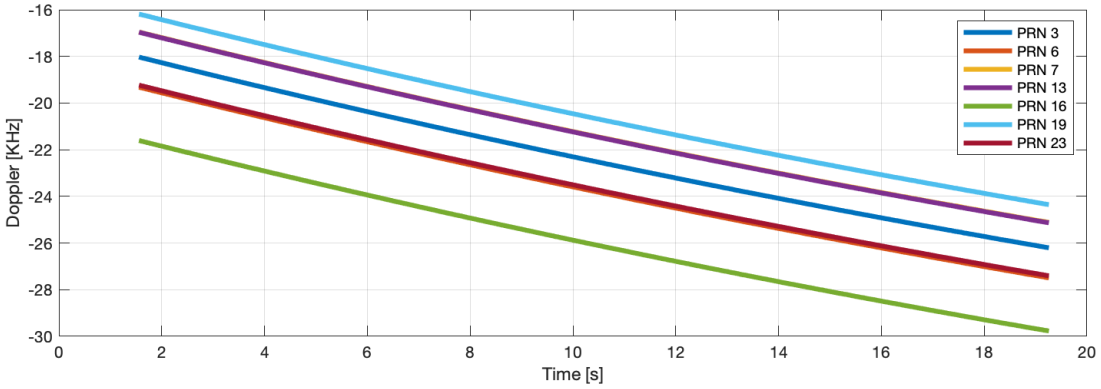

Fig. 8: Observed Doppler time history of each spoofing signal at the LEO-based receiver. The dominating term in the Doppler time history is the range-rate between receiver and spoofer, which is the same across all signals.

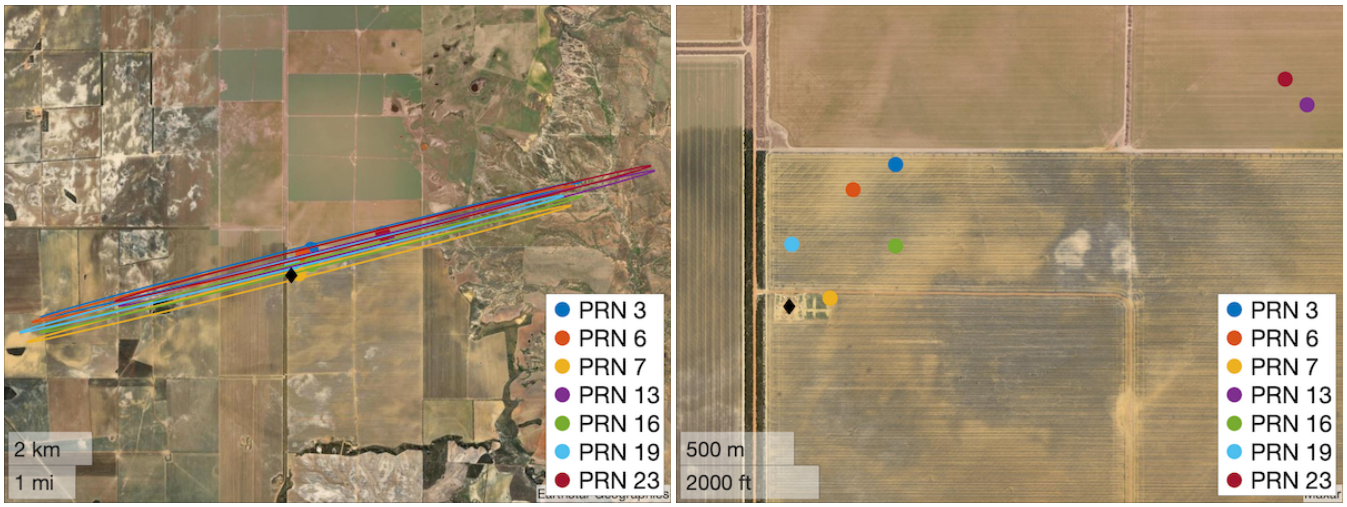

Fig. 9: Geofixes with their corresponding 95% error ellipses by using each observed Doppler time history of each spoofed PRN. Although each individual estimate is biased, the final spread of the spoofer position estimates is tight. The black diamond is the true emitter position. Only one of the seven 95% error ellipses contain the true emitter position.

	PRN 3	PRN 6	PRN 7	PRN 13	PRN 16	PRN 19	PRN 23
Error [m]	775	582	183	2,434	536	272	2,389

TABLE I: Error of the estimated position of the spoofer from each observed Doppler time history.

When the Doppler time histories of each spoofing signal are served as measurements to the nonlinear least-squares estimator, the final position fixes are shown in Fig. 9 and their final error in Table I. Only one of the seven 95% error ellipses contain the true emitter position, however, the final spread of the spoofer position estimates is tight, with the maximum error being 2.4 km. Depending on the desired accuracy requirements, this level of accuracy may be sufficient.

Shown in Fig. 10 are the Doppler residuals with respect to the true emitter position and the final estimated position. In the Doppler residuals with respect to the true emitter position, the time-varying frequency component is visible. The time-varying frequency component of PRN 13 and PRN 23 are the most dramatic, and yield the final spoofer position estimate with the most amount of error. This is because the nonlinear least-squares estimator aims to find the state the best fits the given measurements. The post-fit Doppler residuals with respect to the estimated spoofer position are zero-mean and Gaussian.

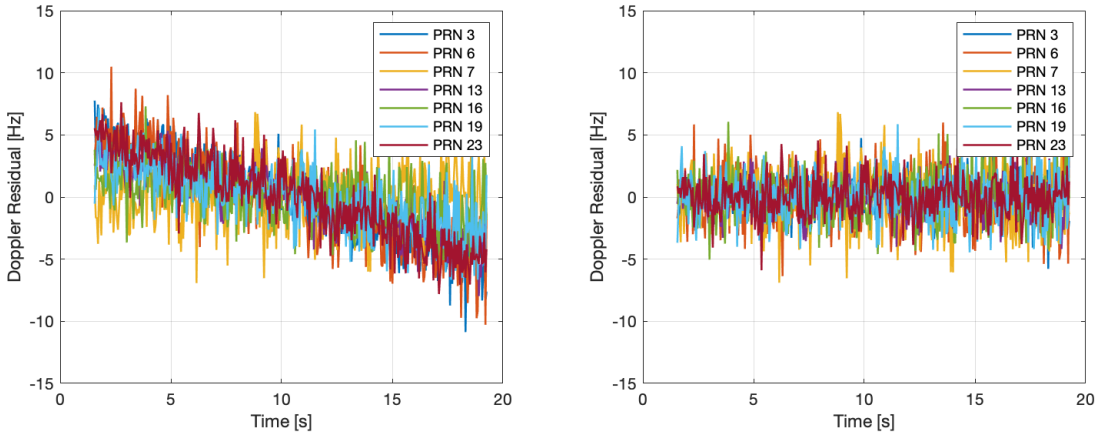

Fig. 10: Shown here are the Doppler residuals with respect to the true emitter position (left) and the final estimated position (right). The linear time-varying term on the left plot is due to the range-rate between spoofed location and spoofed GPS satellite. The PRN 13 and PRN 23 have the most dramatic time-varying frequency component, yielding final estimated spoofer positions with the most error.

However, this technique is not always effective. When the spoofer is spoofing the victim(s) to a highly dynamic trajectory, the time-varying terms due to the spoofed dynamics are no longer negligible. As shown in the prior work [21], a spoofer was found in the raw samples captured from the ISS. It was determined that the spoofer was intending the victims to infer a highly dynamic trajectory. After serving the Doppler time history of each spoofing signal to the nonlinear estimator, the spread of final position estimates was 60 km, which is much larger than what was seen in this experiment.

6. CONCLUSION

This paper presented and verified single-satellite single-pass geolocation technique specifically for GNSS spoofers from LEO. The developed technique removed the unknown time-varying frequency component across each spoofing signal so that the range-rate time history between receiver and spoofer could be extracted and exploited for geolocation. This was accomplished by processing the spoofing signals and extracting a time history of the receiver clock drift. This paper also detailed a controlled experiment in partnership with Spire Global, in which a LEO-based receiver captured GNSS spoofing signals transmitted from a known ground station on a non-GNSS frequency band.

ACKNOWLEDGMENTS

This work was supported by the U.S. Department of Transportation under Grant 69A3552348327 for the CARMEN+ University Transportation Center, 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., "GNSS Spoofing and Detection," *Proceedings of the IEEE*, Vol. 104, No. 6, 2016, pp. 1258–1270.

[2] Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., and Lachapelle, G., "Review article: GPS vulnerability to spoofing threats and review of antispoofing techniques," *International Journal of Naivgation and Observation*, 2012, pp. 1–16.

[3] Humphreys, T. E., "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," *United States House of Representatives Committee on Homeland Security: Subcommittee on Oversight, Investigations, and Management*, July 2012.

[4] Scott, L., "Anti-spoofing and authenticated signal architectures for civil navigation systems," *Proceedings of the ION GNSS Meeting*, 2003, pp. 1542–1552.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] O'Hanlon, B., Psiaki, M., Bhatti, J., and Humphreys, T., "Real-Time Spoofing Detection Using Correlation Between two Civil GPS Receiver," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Nashville, Tennessee, 2012.

[10] Gross, J. and Humphreys, T. E., "GNSS Spoofing, Jamming, and Multipath Interference Classification using a Maximum-Likelihood Multi-Tap Multipath Estimator," *Proceedings of the ION International Technical Meeting*, Jan. 2017.

[11] O'Hanlon, B., Bhatti, J., Humphreys, T. E., and Psiaki, M., "Real-Time Spoofing Detection in a Narrow-Band Civil GPS Receiver," *Proceedings of the ION GNSS Meeting*, Institute of Navigation, Portland, Oregon, 2010.

[12] 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, pp. 83–95.

[13] Clements, Z., Yoder, J. E., and Humphreys, T. E., "GNSS Spoofing Detection: An Approach for Ground Vehicles Using Carrier-Phase and Inertial Measurement Data," *GPS World*, Vol. 34, No. 2, 2023, pp. 36–41.

[14] Tanil, C., Khanafseh, S., Joerger, M., and Pervan, B., "An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 54, No. 1, Feb. 2018, pp. 131–143.

[15] Jafarnia-Jahromi, A., Daneshmand, S., Broumandan, A., Nielsen, J., and Lachapelle, G., "PVT solution authentication based on monitoring the clock state for a moving GNSS receiver," *European navigation conference (ENC)*, Vol. 11, 2013.

[16] Humphreys, T. E., "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 49, No. 2, 2013, pp. 1073–1090.

[17] Fernandez-Hernandez, I., Winkel, J., O'Driscoll, C., Cancela, S., Terris-Gallego, R., López-Salcedo, J. A., Seco-Granados, G., Dalla Chiara, A., Sarto, C., Blonski, D., et al., "Semi-Assisted Signal Authentication for Galileo: Proof of Concept and Results," *IEEE Transactions on Aerospace and Electronic Systems*, 2023.

[18] Exchange, A.-B., "ADS-B Exchange," Jan. 2024, https://globe.adsbexchange.com/?r.

[19] 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.

[20] 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.

[21] Clements, Z., Ellis, P., Psiaki, M. L., and Humphreys, T. E., "Geolocation of Terrestrial GNSS Spoofing Signals from Low Earth Orbit," *Proceedings of the ION GNSS+ Meeting*, Denver, CO, 2022, pp. 3418–3431.

[22] Clements, Z., Ellis, P., and Humphreys, T. E., "Dual-Satellite Geolocation of Terrestrial GNSS Jammers from Low Earth Orbit," *Proceedings of the IEEE/ION PLANS Meeting*, Monterey, CA, 2023, pp. 458–469.

[23] Clements, Z., Ellis, P., and Humphreys, T. E., "Pinpointing GNSS Interference from Low Earth Orbit," *Inside GNSS*, Vol. 18, No. 5, 2023, pp. 42–55.

[24] McKibben, A., McKnight, R., Peters, B. C., Arnett, Z., and Ugazio, S., "Interference Effects on a Multi-GNSS Receiver On-Board a CubeSat in LEO," *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, 2023, pp. 1245–1258.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] Chen, X., Morton, Y., Yu, W.-X., and Truong, T.-K., "GNSS Spoofer Localization with Counterfeit Clock Bias Observables on a Mobile Platform," *IEEE Sensors Journal*, 2023.

[32] 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, pp. 3749–3771.

[33] 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.

[34] Braasch, M. S., *Springer Handbook of Global Navigation Satellite Systems*, chap. Multipath, Springer, 2017, pp. 443–468.

[35] 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.

[36] Laboratory, T. R., "Texas Spoofing Test Battery (TEXBAT)," July 2017, http://radionavlab.ae.utexas.edu/texbat.