Single-Satellite-Based Geolocation of Broadcast GNSS Spoofers from Low Earth Orbit

Zachary L. Clements*, Patrick B. Ellis†, Iain Goodridge†, Matthew J. Murrian†, Mark L. 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

***Abstract*—This paper presents an analysis and experimental demonstration of single-satellite single-pass geolocation of a terrestrial broadcast Global Navigation Satellite System (GNSS) spoofer from Low Earth Orbit (LEO). The proliferation of LEO-based GNSS receivers offers the prospect of 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 for the emitter. This paper presents a technique crafted specifically for indiscriminate broadcast-type GNSS spoofing signals. Furthermore, it explores how unmodeled oscillator instability and worst-case spoofer-introduced signal variations degrade the geolocation estimate. The proposed geolocation technique is validated by a controlled experiment, in partnership with Spire Global, in which a LEO-based receiver captures broadcast GNSS spoofing signals transmitted from a known ground station on a non-GNSS frequency band.**

***Index Terms*—GNSS spoofing; emitter geolocation; interference localization; spectrum monitoring.**

I. 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. A GNSS spoofer emits an ensemble of false GNSS signals intending that the victim receiver(s) accept them as authentic GNSS signals, thereby inferring a false position fix and/or clock offset [1], [2]. A successful spoofing attack may lead to serious consequences.

The academic community has long warned the public about the threat of GNSS spoofing [3]–[5]. Within the past decade, significant progress has been made in GNSS spoofing detection and mitigation [1], [2], [6]–[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]–[14]. Consistency checks between the estimated signal and onboard inertial sensors can provide quick and reliable spoofing detection [15]–[18]. Monitoring the clock state can also be used to detect spoofing [19]–[21]. Cryptographic authentication techniques are currently being developed and implemented to verify received signals [22]–[27].

Although the recent advances in GNSS spoofing detection have been inspiring, many older GNSS receivers in current operation are unable to incorporate such defenses, leaving them vulnerable to attacks. For example, the civilian maritime and airline industries are encountering GNSS jamming and spoofing at an alarming rate [28]–[34]. Anomalous positioning information broadcast by ships in Automatic Identification System (AIS) messages, and airplanes in Automatic Dependent Surveillance-Broadcast (ADS-B) messages, indicate recent widespread jamming and spoofing. These civilian aircraft and ships ensnared by GNSS spoofing are likely unintended targets caught in the electronic warfare crossfire near ongoing conflict zones.

GNSS spoofing attacks can be sorted into two categories, targeted spoofing and broadcast spoofing. In targeted spoofing, an attacker transmits spoofing signals for a specific (possibly-moving) target it wishes to deceive. This type of attack involves the attacker tailoring a spoofing trajectory for its specific target, causing a gradual pull-off from the victim's true trajectory, and compensating for the relative motion between the spoofer and the target to minimize target's probability of detection [35]. Targeted spoofing is a sophisticated, expensive, and difficult-to-detect attack that requires the attacker to have the ability to precisely track the target and craft spoofing signals in accordance with the target's motion, all in real-time. Due to its complexity and narrow scope, this form of spoofing is the least common. Other GNSS receivers besides the targeted victim can also be captured by these signals, but a non-targeted receiver can more easily detect such spoofing. Moreover, targeted spoofing may involve narrow beamforming, making reception by non-target receivers unlikely.

Broadcast spoofing is less expensive, less complex, and wider in geographic extent than targeted spoofing, and thus more common. In broadcast spoofing, an attacker transmits spoofing signals broadly with the intent to deceive all GNSS receivers within a wide area. Because broadcast spoofing is non-targeted, victim GNSS receivers typically see a sudden jump in position and/or timing, which is trivial to detect with basic spoofing detection checks. Yet despite being easy to detect, broadcast spoofing remains effective at denying GNSS access to victims lacking proper defenses. When a GNSS receiver cannot confidently differentiate between authentic and spoofing signals, it is rendered useless—or worse: hazardously misleading. The spoofers recently affecting the aviation and maritime industries appear to be of the broadcast type.

Given that many currently deployed GNSS receivers are unable to defend themselves even against easy-to-detect broadcast spoofing, GNSS users need to be warned of hazardous GNSS-challenged environments. The proliferation of LEO-based GNSS receivers provides the potential of unprecedented

spectrum awareness, enabling GNSS interference detection, classification, and geolocation with worldwide coverage [36]–[41]. Existing and proposed LEO constellations provide worldwide coverage with frequent revisit rates, allowing for an always-updating operating picture, a noted shortfall in current capabilities [42]. 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 [39], [40], [43]–[45]. Multiple time-synchronized receivers can exploit time- and frequency-difference-of-arrival (T/FDOA) measurements to estimate the emitter location. The authors of the current paper were able to geolocate over 30 GNSS interference sources across the Near East from a dual-satellite time-synchronized capture [39], [40]. However, planning simultaneous multi-satellite captures to enable T/FDOA-based geolocation can be difficult to coordinate and expensive, whereas single-satellite collects are straightforward and less costly. Accordingly, this paper focuses on single-satellite geolocation.

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. But if a signal's carrier can be tracked, or Doppler can be otherwise measured, then accurate single-satellite-based emitter geolocation is possible from Doppler measurements alone, provided that the emitter's carrier frequency is quasi-constant [37], [46]–[48]. But 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 specially, as they do not transmit at a constant carrier frequency: they add an unknown time-varying frequency component to each spoofing signal, imitating the range-rate between the corresponding spoofed GNSS satellite and the counterfeit spoofed location [35]. A key contribution of the current paper 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. A single-receiver spoofer geolocation technique based on counterfeit clock observables is also presented in [49]. However, [49] only considers the spoofed pseudorange measurements and depends on a stationary receiver initialization period, which is not possible in LEO.

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

This paper makes four primary contributions. First, it presents a single-satellite, single-pass GNSS spoofer geolocation technique that extracts a range-rate between a LEO-based receiver and a terrestrial broadcast spoofer from captured raw samples. Second, it offers an experimental demonstration of the technique with a truth solution. Third, it derives an analytic expression for how transmitter clock instability degrades the single-satellite geolocation solution. Fourth, it investigates the geolocation positioning errors as a function of worst-case spoofed clock behavior.

Preliminary conference versions of this paper were published in [50], [51]. The current version significantly extends these with contributions three and four mentioned above.

II. Signal Models

A. GNSS Spoofing Signals

The goal of a broadcast GNSS spoofer is to deceive the victim receiver(s) into inferring a false position, velocity, and timing (PVT) solution, denoted $\tilde{\boldsymbol{x}} = [\, \boldsymbol{r}_{\tilde{\mathrm{r}}}^{\mathsf{T}},\ \delta t_{\tilde{\mathrm{r}}},\ \boldsymbol{v}_{\tilde{\mathrm{r}}}^{\mathsf{T}},\ \delta \dot{t}_{\tilde{\mathrm{r}}} \,]^{\mathsf{T}}$, where $\boldsymbol{r}_{\tilde{\mathrm{r}}}$ is the spoofed position in Earth-centered-Earth-fixed (ECEF) coordinates, $\delta t_{\tilde{\mathrm{r}}}$ is the spoofed clock bias increment, $\boldsymbol{v}_{\tilde{\mathrm{r}}}$ is the spoofed velocity, and $\delta \dot{t}_{\tilde{\mathrm{r}}}$ is the spoofed clock drift increment. To achieve a successful attack, the spoofer must generate an ensemble of self-consistent signals. To this end, the attacker must (1) select a counterfeit 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 corresponding navigation message, code phase time history, and carrier phase time history consistent with (1) and (2).

A general baseband signal model for broadcast spoofing signals is now presented. The ensemble of spoofing signals transmitted by the spoofer, denoted

$$x(t) = \sum_{n=1}^{N} s_n(t) \tag{1}$$

contains N spoofing signals, where the nth spoofing signal is denoted $s_n(t)$ for $n = 1, 2, ..., N$. The nth spoofing baseband signal takes the form

$$s_n(t) = A_n D_n\left[t - \tau_n(t)\right] C_n\left[t - \tau_n(t)\right] \exp\left[j 2\pi \theta_n(t)\right] \tag{2}$$

where A_n is the carrier amplitude, $D_n(t)$ is the data bit stream, $C_n(t)$ is the spreading code, $\tau_n(t)$ is the code phase, and $\theta_n(t)$ is the negative beat carrier phase [1]. The Doppler of the nth spoofing signal is related to $\theta_n(t)$ by

$$\tilde{f}_n(t) = \frac{d}{dt}\theta_n(t) \tag{3}$$

The spoofer adds a 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, (2) the spoofed receiver clock drift, and (3) the spoofed satellite clock drift. Additionally, the spoofed code phase and carrier phase time histories must be mutually consistent to avoid code-carrier divergence. Accordingly, the

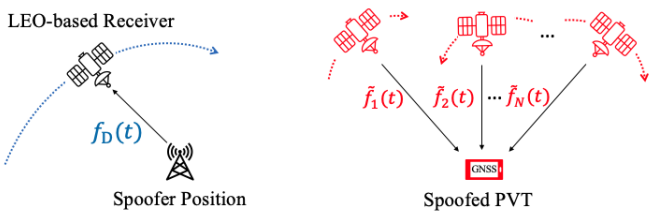


Fig. 1: Shown here are the Doppler components in single-satellite spoofer geolocation. The Doppler components corresponding to (5) are shown on the left. The Doppler components for each spoofing signal corresponding to (4) are shown in red to the right.

Doppler of the nth transmitted spoofing signal may be modeled as

$$\tilde{f}_n(t) = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{r}}n}^{\mathsf{T}}(t)\left(\boldsymbol{v}_{\tilde{\mathrm{r}}}(t) - \boldsymbol{v}_{\tilde{\mathrm{s}}n}(t)\right) - \frac{c}{\lambda}\left(\delta\dot{t}_{\tilde{\mathrm{r}}}(t) - \delta\dot{t}_{\tilde{\mathrm{s}}n}(t)\right) \tag{4}$$

where λ is the carrier wavelength, c is the speed of light, $\hat{\boldsymbol{r}}_{\tilde{\mathrm{r}}n}$ is the unit vector pointing from the nth spoofed navigation satellite to the spoofed position, both in ECEF coordinates, $\boldsymbol{v}_{\tilde{\mathrm{r}}}$ is the spoofed receiver velocity, $\boldsymbol{v}_{\tilde{\mathrm{s}}n}$ is the nth spoofed navigation satellite velocity, and $\delta\dot{t}_{\tilde{\mathrm{s}}n}$ is the spoofed clock drift of the nth navigation satellite. One can immediately appreciate that the Doppler frequency is different for each spoofing signal. Had this been a targeted spoofer, there would be an additional Doppler term in (4) that compensates for the relative motion between the victim and spoofer, but in the case of broadcast spoofing, this term is zero.

B. Received Doppler Model

First consider a scenario in which a moving receiver captures a transmitted signal having a constant carrier frequency. The received Doppler $f_{\mathrm{D}}(t)$ at the moving receiver can be modeled as

$$f_{\mathrm{D}}(t) = -\frac{1}{\lambda}\hat{\boldsymbol{r}}^{\mathsf{T}}(t)\left(\boldsymbol{v}_{\mathrm{r}}(t) - \boldsymbol{v}_{\mathrm{t}}(t)\right) - \frac{c}{\lambda}\left(\delta\dot{t}_{\mathrm{r}}(t) - \delta\dot{t}_{\mathrm{t}}(t)\right) \tag{5}$$

where $\hat{\boldsymbol{r}}$ is the unit vector pointing from the transmitter to the receiver, $\boldsymbol{v}_{\mathrm{r}}$ is the velocity of the receiver, $\boldsymbol{v}_{\mathrm{t}}$ is the velocity of the transmitter, $\delta\dot{t}_{\mathrm{r}}$ is the clock drift of the receiver, and $\delta\dot{t}_{\mathrm{t}}$ is the clock drift of the transmitter. Note that this is a simplified Doppler model that neglects higher-order terms. A complete Doppler model is presented in [52]. For the purposes of this paper, the simplified model is adequate, as will be confirmed by the experimental results.

Now consider a scenario in which a moving receiver captures an ensemble of transmitted spoofing signals from a stationary terrestrial spoofer ($\boldsymbol{v}_{\mathrm{t}}(t) = 0$), as shown in Fig. 1. An analysis of how spoofer motion affects the geolocation solution is given in a prior version of this paper [50]. But would-be spoofers are typically stationary; otherwise, they face the additional difficulty of compensating for their motion to avoid producing easily-detectable false signals. Therefore, a stationary spoofer will be assumed for the rest of this paper.

Each observed signal at the receiver will contain a common Doppler shift f_{D} due to the the relative motion between the transmitter (spoofer) and the receiver. Each observed signal will also manifest a common frequency shift due to the clock drift of the transmitter and the clock drift of the receiver. Dropping time indices for clarity, the observed Doppler of the nth spoofing signal at the moving receiver, f_n, may be written as

$$\begin{aligned} f_n =& f_{\mathrm{D}} + \tilde{f}_n \\ =& -\frac{1}{\lambda}\hat{\boldsymbol{r}}^{\mathsf{T}}\boldsymbol{v}_{\mathrm{r}} - \frac{c}{\lambda}\left(\delta\dot{t}_{\mathrm{r}} - \delta\dot{t}_{\mathrm{t}}\right) \\ & -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{r}}n}^{\mathsf{T}}\left(\boldsymbol{v}_{\tilde{\mathrm{r}}} - \boldsymbol{v}_{\tilde{\mathrm{s}}n}\right) - \frac{c}{\lambda}\left(\delta\dot{t}_{\tilde{\mathrm{r}}} - \delta\dot{t}_{\tilde{\mathrm{s}}n}\right) \end{aligned} \tag{6}$$

What makes single-satellite GNSS spoofer geolocation difficult is the $\tilde{f}_n$ term: it is typically unknown, time-varying, and different for each spoofing signal. In the case of the matched-code jammer discovered in [37], $\tilde{f}_n = 0$. One may suppose that the operator's intent in that case was not to deceive victim receivers into inferring false locations like a spoofer. When $\tilde{f}_n = 0$, the observed Doppler can be modeled as the range-rate between transmitter and receiver, with a constant measurement bias over the capture to account for the clock drift of the transmitter. Contrariwise, naive geolocation with the observed Doppler modeled as in (6) yields final position estimates that are biased because the spoofing signals contain the unmodeled $\tilde{f}_n(t)$ term. In the following section, a technique is presented that removes $\tilde{f}_n(t)$ and extracts $\hat{\boldsymbol{r}}^{\mathsf{T}}(t)\boldsymbol{v}_{\mathrm{r}}(t)$, the range-rate time history between transmitter and receiver, which can be exploited for geolocation.

III. Conceptual Overview of Broadcast GNSS Spoofer Geolocation

This section presents an overview of the technique originally presented in [50], [51] for spoofer geolocation. The common Doppler components across all spoofing signals from (6) are indicated below:

$$\begin{aligned} f_n =& \underbrace{-\frac{1}{\lambda}\hat{\boldsymbol{r}}^{\mathsf{T}}\boldsymbol{v}_{\mathrm{r}} - \frac{c}{\lambda}\left(\delta\dot{t}_{\mathrm{r}} - \delta\dot{t}_{\mathrm{t}}\right)}_{\text{common}} \\ & -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{r}}n}^{\mathsf{T}}\left(\boldsymbol{v}_{\tilde{\mathrm{r}}} - \boldsymbol{v}_{\tilde{\mathrm{s}}n}\right) - \frac{c}{\lambda}\Big(\underbrace{\delta\dot{t}_{\tilde{\mathrm{r}}}}_{\text{common}} - \delta\dot{t}_{\tilde{\mathrm{s}}n}\Big) \end{aligned} \tag{7}$$

All common Doppler terms can be lumped into a single term

$$\gamma(t) = \frac{1}{c}\hat{\boldsymbol{r}}^{\mathsf{T}}(t)\boldsymbol{v}_{\mathrm{r}}(t) + \delta\dot{t}_{\mathrm{r}}(t) - \delta\dot{t}_{\mathrm{t}}(t) + \delta\dot{t}_{\tilde{\mathrm{r}}}(t) \tag{8}$$

so that (6) may be written

$$f_n = -\frac{1}{\lambda}\hat{\boldsymbol{r}}_{\tilde{\mathrm{r}}n}^{\mathsf{T}}\left(\boldsymbol{v}_{\tilde{\mathrm{r}}} - \boldsymbol{v}_{\tilde{\mathrm{s}}n}\right) - \frac{c}{\lambda}\left(\gamma - \delta\dot{t}_{\tilde{\mathrm{s}}n}\right) \tag{9}$$

Upon processing an ensemble of spoofing signals, a GNSS receiver's PVT estimator produces, at each navigation epoch, the state estimate

$$\hat{\boldsymbol{x}}(t) = \left[\,\hat{\boldsymbol{r}}_{\tilde{\mathrm{r}}}^{\mathsf{T}}(t),\ \hat{\xi}(t),\ \hat{\boldsymbol{v}}_{\tilde{\mathrm{r}}}^{\mathsf{T}}(t),\ \hat{\gamma}(t)\,\right]^{\mathsf{T}} \tag{10}$$

which is composed of the estimated spoofed position, the estimated receiver clock bias $\hat{\xi}(t)$, the estimated spoofed velocity, and the estimated receiver clock drift $\hat{\gamma}(t)$ [53]. A brief review of PVT estimation from pseudorange and Doppler

measurements is provided in [51], [54]. Note that the estimated receiver clock bias $\hat{\xi}(t)$ will include $\delta t_{\tilde{\mathrm{r}}}$ as a component but will not in general equal $\delta t_{\tilde{\mathrm{r}}}$.

The estimated clock drift $\hat{\gamma}(t)$, on the other hand, will track $\gamma(t)$ closely provided that the PVT estimator is configured with a clock model whose process noise intensity is sufficient to accommodate the variations in $\gamma(t)$ due to spoofing. Expressed in s/s, $\hat{\gamma}(t)$ contains all common Doppler terms, since the PVT estimator attributes common-mode frequency deviations across received signals to the receiver's clock drift. Importantly, $\hat{\gamma}(t)$ is unaffected by the unknown non-common Doppler components from $\tilde{f}_n(t)$ for all $n \in \{1, 2, ..., N\}$.

The time history $\hat{\gamma}(t)$ is the key to spoofer geolocation because it depends strongly on the range-rate between the LEO-based receiver and the terrestrial spoofer. In particular, information about the transmitter's location is embedded in $\hat{\boldsymbol{r}}^{\mathsf{T}}(t)\boldsymbol{v}_{\mathrm{r}}(t)$, which for a LEO-based receiver is typically the dominant component in $\gamma(t)$. A nonlinear least-squares estimator based on $\hat{\gamma}(t)$ is developed in the next section to estimate the spoofer's position.

For a targeted spoofing attack in which the spoofer attempts to compensate for true spoofer-to-victim line-of-sight velocity, $\gamma(t)$ could contain an extra term. If this term were to vary rapidly with time, it would cause trouble for this paper's technique. Relatedly, if the targeted victim's position and velocity were somehow accurately known to the LEO-based receiver, this paper's technique could produce accurate results provided that the estimator presented in the next section were updated to account for the known victim motion. Finally, if the targeted victim receiver is stationary, this paper's technique can be applied without modification.

The other three terms in $\gamma(t)$, namely $\delta\dot{t}_{\mathrm{r}}(t)$, $\delta\dot{t}_{\mathrm{t}}(t)$, and $\delta\dot{t}_{\tilde{\mathrm{r}}}(t)$, are nuisance terms that potentially degrade geolocation accuracy. Fortunately, their contributions are typically minor or can be estimated. Consider $\delta\dot{t}_{\mathrm{r}}(t)$. If the satellite's GNSS receiver and the radio frequency (RF) front-end capturing spoofing signals are driven by the same oscillator, then $\delta\dot{t}_{\mathrm{r}}(t)$ is automatically estimated by the onboard GNSS receiver, provided it is not significantly affected by the spoofing, and and thus $\delta\dot{t}_{\mathrm{r}}(t)$ can be compensated.

It is worth mentioning that one of the core assumptions in any geolocation system is that the capture platform has knowledge of its PVT; otherwise, geolocation is impossible. In the scenario assumed in this paper, the LEO-based receiver has access to its PVT from an onboard GNSS receiver that is robust to terrestrial interference. Despite the presence of spoofing signals, code- and carrier-tracking of the authentic GNSS signals is maintained due to sufficient separation of the false and authentic signals in the code-Doppler space, as achieved in [37]. Furthermore, robustness is achieved if a zenith-facing antenna feeds the onboard GNSS receiver's RF front-end, as the gain directed towards Earth will be strongly attenuated. Finally, PVT can be trivially maintained by a multi-constellation receiver when only single-constellation spoofing signals are present.

The terms $\delta\dot{t}_{\mathrm{t}}(t)$ and $\delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ originate from the spoofer. Specifically, $\delta\dot{t}_{\mathrm{t}}(t)$ originates from the spoofer's hardware, while $\delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ originates from its spoofer's software. The former arises due to the clock drift in the spoofer. It can often be accurately modeled as constant over short (e.g., 60-second) capture intervals and estimated as part of the geolocation process [37]. The spoofed clock drift $\delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ arises from the spoofer's attack configuration, and will manifest at the victim as an increment to the victim's clock drift. It can be troubling for geolocation, but a potential attacker would typically opt to keep $\delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ near constant, because if $\delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ grows too rapidly to be explained by the expected variation in clock drift for the receiver's oscillator type, the victim receiver could flag the anomaly and thereby detect the spoofing attack.

This constraint can be generalized to the sum $\delta\dot{t}_{\mathrm{t}}(t) + \delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ and summarized as follows: if the spoofer allows extraordinary frequency instability in its own oscillator so that $\delta\dot{t}_{\mathrm{t}}(t)$ changes too rapidly, or if it attempts to induce a quickly-varying spoofed clock drift so that $\delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ changes too rapidly, geolocation accuracy is degraded but, on the other-hand, the spoofing attack becomes trivially detectable.

Section VI explores the consequences for geolocation of cases where $\delta\dot{t}_{\mathrm{t}}(t)$ departs from a constant model. It also presents an analysis of how aggressively an attacker can ramp $\delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ without being detected by an optimal spoofing detection strategy that monitors the receiver clock drift, and an analysis of how the rate of change in $\delta\dot{t}_{\mathrm{t}}(t) + \delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ translates to geolocation error.

IV. Spoofer Geolocation with $\gamma(t)$

This section presents the measurement model, derives the measurement noise covariance matrix, and presents the nonlinear least-squares estimator for single-satellite spoofer geolocation.

A. Measurement Model

When a GNSS receiver processes spoofing signals, it first generates spoofed GNSS observables. These GNSS observables are beset with errors, modeled as zero-mean additive white Gaussian noise (AWGN), arising from thermal noise, local electromagnetic interference, and other minor effects. At every navigation epoch, the noisy spoofed GNSS observables are fed to the receiver's PVT estimator to produce an optimal estimate of the spoofed PVT solution, including $\hat{\gamma}(t)$.

Let $\gamma[i] = \gamma(i\Delta t)$ and $\hat{\gamma}[i] = \hat{\gamma}(i\Delta t)$, where Δt is the constant PVT solution interval and $i \in \mathcal{I} = \{1, 2, ..., I\}$ is the solution index within a given data capture interval. Let $z[i]$ denote the ith measurement to be used for spoofer geolocation, modeled as

$$z[i] = c\hat{\gamma}[i] = c\gamma[i] + w_{\mathrm{a}}[i], \quad i \in \mathcal{I} \tag{11}$$

The velocity-equivalent estimation error $w_{\mathrm{a}}[i]$, which has units of m/s, is a discrete-time noise process with $\mathbb{E}[w_{\mathrm{a}}[i]] = 0$ and $\mathbb{E}[w_{\mathrm{a}}[i]w_{\mathrm{a}}[j]] = \sigma_{\mathrm{a}}^2\delta_{ij}$, for all $i, j \in \mathcal{I}$. Section IV-B will justify this model's assumption that $w_{\mathrm{a}}[i]$ is white (uncorrelated in time) for a sufficiently large Δt that is larger than the settling time of its phase lock loop (PLL) or frequency lock loop (FLL), and the settling time of any Kalman filter used for obtaining the spoofed fix.

As stated before, $\delta\dot{t}_{\mathrm{r}}$ is assumed to be known and fully compensated; accordingly, it will be neglected hereafter. Additionally, $\delta\dot{t}_{\tilde{\mathrm{r}}}$ is part of the spoofer's attack configuration and, for now, will be modeled as constant due to the constraints mentioned in the prior section.

A more comprehensive model is considered for $\delta\dot{t}_{\mathrm{t}}(t)$. Let $\delta\dot{t}_{\mathrm{t}}[i] = \delta\dot{t}_{\mathrm{t}}(i\Delta t), i \in \mathcal{I}$. Over a capture interval, $\delta\dot{t}_{\mathrm{t}}[i]$ is modeled as

$$c\delta\dot{t}_{\mathrm{t}}[i] = c\delta\dot{t}_{\mathrm{t}}[0] + b[i], \quad i \in \mathcal{I} \tag{12}$$

where $\delta\dot{t}_{\mathrm{t}}[0]$ represents the spoofer oscillator's constant frequency bias and $b[i]$ is a Gaussian random walk process expressed as

$$b[i] = \sum_{k=1}^{i} v[k], \quad i \in \mathcal{I} \tag{13}$$

where $v[k]$ is a discrete-time Gaussian random process with $\mathbb{E}\left[v(k)\right] = 0$, $\mathbb{E}\left[v[k]v[j]\right] = \sigma_v^2\delta_{kj}$ and $\mathbb{E}\left[w_{\mathrm{a}}[k]v[j]\right] = 0$ for all $k, j \in \mathcal{I}$, and $b[0] = 0$. Using the model in [55, Chap. 8], σ_v^2 can be characterized as

$$\sigma_v^2 = 2\pi^2 h_{-2}\Delta t c^2 \tag{14}$$

where h_{-2} is the first parameter of the standard clock model based on the fractional frequency error power spectrum [37]. Scaling by c^2 converts to units of $(\mathrm{m/s})^2$.

Note that $\delta\dot{t}_{\mathrm{t}}[0]$ and $\delta\dot{t}_{\tilde{\mathrm{r}}}$ can be combined into a single measurement bias b_0 that is constant across the capture interval. Furthermore, the AWGN and Gaussian random walk can also be combined into a single noise term $w[i]$. Thus we have

$$b_0 = -c\delta\dot{t}_{\mathrm{t}}[0] + c\delta\dot{t}_{\tilde{\mathrm{r}}} \tag{15}$$

$$w[i] = w_{\mathrm{a}}[i] + b[i], \quad i \in \mathcal{I} \tag{16}$$

Given all of this, (11) is rewritten so that the final measurement model takes the form

$$z[i] = \hat{\boldsymbol{r}}_i^{\mathsf{T}}\boldsymbol{v}_{\mathrm{r},i} + b_0 + w[i], \quad i \in \mathcal{I} \tag{17}$$

The associated measurement covariance matrix R for the process $w[i]$ is now derived. Clearly, $w[i]$ is zero-mean, but because it contains a Gaussian random walk term, it is correlated over time. The $[i, j]$th element of its measurement covariance matrix is

$$\begin{aligned}
R[i,j] &= \mathbb{E}\left[w[i]w[j]\right] \\
&= \mathbb{E}\left[\left(w_{\mathrm{a}}[i] + \sum_{k=1}^{i} v[k]\right)\left(w_{\mathrm{a}}[j] + \sum_{l=1}^{j} v[l]\right)\right] \\
&= \mathbb{E}\left[w_{\mathrm{a}}[i]w_{\mathrm{a}}[j]\right] + \mathbb{E}\left[\left(\sum_{k=1}^{i} v[k]\right)\left(\sum_{l=1}^{j} v[l]\right)\right] \\
&= \mathbb{E}\left[w_{\mathrm{a}}[i]w_{\mathrm{a}}[j]\right] + \sum_{k=1}^{i}\sum_{l=1}^{j}\mathbb{E}\left[v[k]v[l]\right] \\
&= \sigma_{\mathrm{a}}^2\delta_{ij} + \sigma_v^2\,\min\{i,j\}
\end{aligned} \tag{18}$$

From this result, the measurement covariance matrix containing the AWGN and Gaussian random walk can be written as

$$R = R_{\mathrm{a}} + R_{\mathrm{b}} \tag{19}$$

where

$$R_{\mathrm{a}} = \sigma_{\mathrm{a}}^2\,\mathbb{I}_{I\times I} \tag{20}$$

$$R_{\mathrm{b}} = \sigma_v^2\,M_{I\times I} \tag{21}$$

where $\mathbb{I}_{I\times I}$ is the identity matrix and M is an $I \times I$ matrix with $M[i,j] = \min\{i,j\}$, $i \in \mathcal{I}$. Note that this covariance matrix is a general result that can be applied to any range-rate-based positioning technique where the transmitter clock state is unknown.

B. Effects of Estimated $\gamma[i]$

One might question the choice to model the estimation error process $w_{\mathrm{a}}[i] = c(\hat{\gamma}[i] - \gamma[i])$ as white, since $\hat{\gamma}[i]$ is the product of a state estimator and it is well known that state estimation errors are correlated in time. At epoch i, let $\tilde{\boldsymbol{x}}[i]$ denote the sequential PVT estimator's full state estimation error, $W[i]$ its feedback gain, $F[i]$ its state transition matrix, and $P[i]$ its state covariance. The covariance between sequential state errors is given by [56, Chap. 5]

$$\mathbb{E}\left[\tilde{\boldsymbol{x}}[i+1]\tilde{\boldsymbol{x}}^{\mathsf{T}}[i]\right] = \left[\mathbb{I} - W[i+1]H[i+1]\right]F[i]P[i] \tag{22}$$

The correlation between $w_{\mathrm{a}}[i+1]$ and $w_{\mathrm{a}}[i]$ for $i \in \mathcal{I}$ can be determined by analysis of this equation since $w_{\mathrm{a}}[i]$ is an element of $\tilde{\boldsymbol{x}}[i]$.

Consider a scenario where the spoofer induces a static location with a typical GPS satellite geometry. The state estimated by an affected receiver consists of the position, clock bias, and clock drift, as in (10). Assume the receiver's PVT estimator applies a dynamics model consistent with a static position and the clock process noise model from [55]. Furthermore, assume that measurement errors are independent, zero-mean, and Gaussian with standard deviations of 1 m and 0.5 m/s respectively for the spoofed pseudorange and Doppler measurements.

A key tuning parameter in this model is the process noise of the receiver clock drift, which is governed by the h_{-2} coefficient, as in (14). Fig. 2 shows the Pearson correlation coefficient for $w_{\mathrm{a}}[i]$ between subsequent navigation epochs over various values of modeled h_{-2} as a function of the time between epochs. As the process noise and time between epochs is increased, the time correlation of sequential estimation errors is reduced. This type of analysis can be performed to help determine the measurement interval length beyond which errors in the sequential estimates $\hat{\gamma}[i]$ can be accurately approximated as AWGN. For example, Fig. 2 indicates that, for $h_{-2} \geq 3 \times 10^{-19}$, measurements spaced by 100 ms or more may be treated as independent.

If h_{-2} were increased even further, the navigation filter becomes a sequence of point solutions and, in effect, the white noise-model of $w_{\mathrm{a}}[i]$ is undoubtedly correct. The selection of h_{-2} becomes a tuning parameter for the system designer. This analysis involving nominal h_{-2} values becomes relevant because currently deployed LEO-based GNSS receivers can perform this technique and may not have the flexibility to change their own process noise.

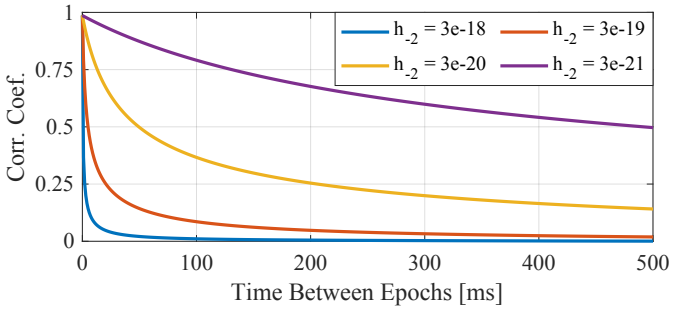


Fig. 2: The Pearson correlation coefficient between sequential estimation errors $w_{\text{a}}[i]$ as a function of time between estimation epochs for various values of h_{-2}. As the receiver's modeled process noise intensity increases, the time correlation between between estimation errors decreases.

C. Range-rate Nonlinear Least-Squares

Now that the measurements and the measurement covariance have been defined, a batch nonlinear least-squares estimator may be developed to solve for the state $\boldsymbol{x}$

$$\boldsymbol{x} = \begin{bmatrix} \boldsymbol{r}_{\text{t}} \\ b_0 \end{bmatrix} \tag{23}$$

where $\boldsymbol{r}_{\text{t}}$ is the transmitter's ECEF position and b_0 is the unknown measurement bias. Let $\boldsymbol{z}$ represent the $I \times 1$ stacked measurement vector. The standard weighted nonlinear least-squares cost function is

$$J(\boldsymbol{x}) = \frac{1}{2} \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})\right]^{\mathsf{T}} R^{-1} \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})\right] \tag{24}$$

where $\boldsymbol{h}(\boldsymbol{x})$ is the nonlinear measurement model function. The optimal estimate of $\boldsymbol{x}$ minimizes the cost J.

The linearized measurement model H is an $I \times 4$ matrix that takes the form

$$H = \begin{bmatrix} \frac{dh_1}{d\boldsymbol{r}_{\text{t}}} & 1 \\ \vdots & \vdots \\ \frac{dh_I}{d\boldsymbol{r}_{\text{t}}} & 1 \end{bmatrix} \tag{25}$$

where

$$\frac{dh_i(\boldsymbol{x})}{d\boldsymbol{r}_{\text{t}}} = \boldsymbol{v}_{\text{r}}^{\mathsf{T}} \frac{\left(\hat{\boldsymbol{r}}_i \hat{\boldsymbol{r}}_i^{\mathsf{T}} - \mathbb{I}_{3\times 3}\right)}{\rho_i} \tag{26}$$

is the 1×3 Jacobian of the ith range-rate measurement. The range between the receiver and the transmitter at the ith measurement is denoted ρ_i. This measurement model Jacobian is equivalent to columns 1, 2, 3, and 8 of the Jacobian presented in [52], up to a scale factor.

Enforcing an altitude constraint significantly improves the problem's observability. This can be incorporated as an additional pseudo-measurement of the transmitter's altitude with respect to the WGS-84 ellipsoid, modeled as

$$z[I+1] = h_{\text{alt}}(\boldsymbol{x}) + w_{\text{alt}} \tag{27}$$

where the measurement error $w_{\text{alt}} \sim \mathcal{N}(0, \sigma_{\text{alt}}^2)$ is assumed to be independent of those for $z[i], i \in \mathcal{I}$. The measurement's 1×4 Jacobian is

$$H_{\text{alt}} = \left[\cos(\phi_{\text{lat}})\cos(\lambda_{\text{lon}}), \cos(\phi_{\text{lat}})\sin(\lambda_{\text{lon}}), \sin(\phi_{\text{lat}}), 0\right] \tag{28}$$

where ϕ_{lat} and λ_{lon} are the latitude and longitude of $\boldsymbol{r}_{\text{t}}$, respectively. The measurement vector $\boldsymbol{z}$, vector-valued function $\boldsymbol{h}(\boldsymbol{x})$, Jacobian H, and error covariance R are all augmented appropriately to include the altitude pseudo-measurement.

Finally, the estimation error's Cramér-Rao lower bound (CRLB) can be approximated as

$$P_{\boldsymbol{xx}} = \left(H^{\mathsf{T}} R^{-1} H\right)^{-1} \tag{29}$$

V. Experimental Results

The single-satellite geolocation technique described above was verified in a joint demonstration between the University of Texas Radionavigation Laboratory (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 satellite performed a raw signal capture. This section details the experimental setup and results. Preliminary results were presented in [51], which contains a comprehensive description of the special adaptations made to deal with the spoofer's non-GNSS carrier frequency.

A. Experimental Design

The UT RNL provided a baseband binary file containing an ensemble of GNSS spoofing signals to be transmitted, a filtered and downsampled version of the "clean static" recording in the TEXBAT dataset [57]. The original recording was a high-quality 16-bit 25 Msps (complex) recording of authentic GNSS signals centered at GPS L1 from a stationary antenna on top of the former Aerospace Engineering building at UT Austin. The front-end in the original recording was driven by 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. Additionally, onboard the satellite, the S-band capture device and onboard GNSS receiver were driven by the same oscillator, allowing precise time-tagging and compensation.

The spoofing file was transmitted from a ground station located in Perth, Australia. The transmitter was driven by a temperature-controlled crystal oscillator (TCXO). The transmitted spoofing signals were centered at S-band to avoid interfering with the GNSS bands. While the ground station was transmitting the spoofing file, an overhead LEO satellite performed a raw signal capture over 20 seconds, centered at the S-band carrier and sampled at 5 Msps (complex). In practice, all processing would be done by an onboard receiver. The duration of the raw capture should be as long as a frame in the spoofed navigation message, or 30 seconds in the case of GPS L1/CA, to ensure that the entire spoofed satellite ephemeris for each spoofed satellite could be decoded. Fig. 3 shows locations relevant to the demonstration. In the context of this paper, the physical location of the transmitter (spoofer) is in Perth, Australia and the spoofed location sits atop the former Aerospace Engineering building in Austin, Texas. Note that this spoofer could also be characterized as a meacon with a long delay from reception to transmission. The goal is to geolocate the spoofer's position in Perth.

Fig. 3: Left: The spoofed location atop the former Aerospace Engineering building in Austin, Texas. Center: The actual spoofer location, a Spire Global ground station located in Perth, Australia. Right: The ground track of the Spire Global LEO satellite during the 20-second signal capture.

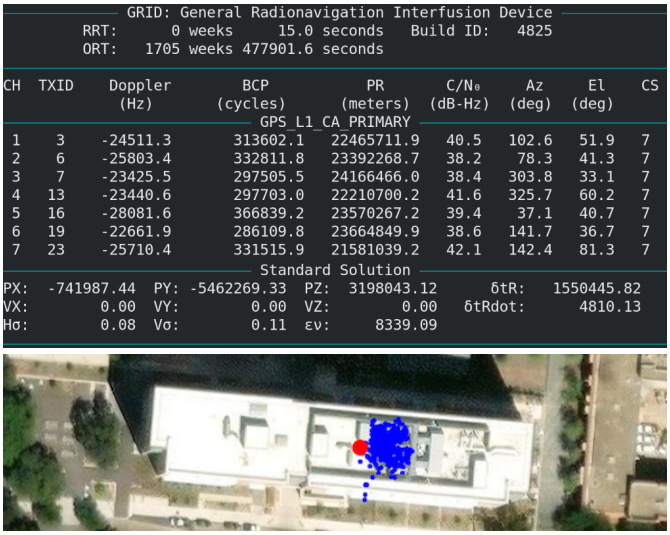


Fig. 4: Top: UT RNL's GRID receiver display when processing the spoofing signals. Bottom: A scatter of GRID-derived position solutions. The red dot is the spoofed position. The 3D bias is 45.9 m, mostly concentrated in the vertical direction. This error is attributed to the S-band carrier.

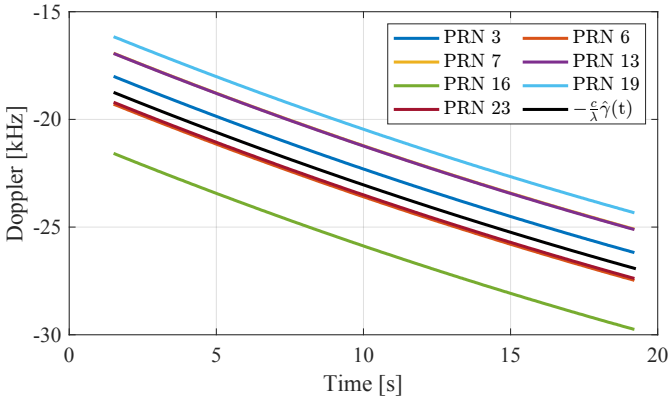


Fig. 5: Measured Doppler time history of each received spoofing signal. Also shown is the Doppler-equivalent time history $\hat{\gamma}(t)$ (black trace), which is used for geolocation.

B. Experimental Spoofer Geolocation with $\gamma(t)$

The transmitted spoofing signals captured in LEO were processed with the UT RNL's GRID software-defined GNSS receiver [58]–[60]. Fig. 4 shows the PVT solution obtained by processing the pseudorange and Doppler measurements of the spoofing signals. The position solution is slightly biased due to the code-carrier divergence caused by shifting the original L1-centered signal to the S-band carrier [51]. On GRID's display, the 4,810 m/s clock drift (labeled `δtRdot`) is immediately noticeable. Of course, no oscillator on a GNSS receiver would experience a clock drift so extreme.

To coax GRID into properly processing the S-band spoofing signals, special modifications to the receiver's configuration and PVT estimator had to be made. Reconfiguring such parameters is trivial within GRID's software-defined architecture. The bandwidths of the receiver's delay lock loop (DLL) and PLL were increased to maintain lock despite the code-carrier divergence introduced by the S-band carrier. The bandwidth of the DLL was set to 1.7 Hz and the bandwidth of the PLL was set to 40 Hz, introducing more noise. To minimize spurious variations in $\hat{\gamma}(t)$, the receiver's dynamics model was set to 'static', consistent with an assumed static spoofed location. The receiver's innovations-based anomaly monitor was disabled to prevent rejection of the PVT solution due to the unusually high estimated clock drift-rate. Other considerations related to the S-band carrier are detailed in [51].

A Doppler-equivalent time-history $\hat{\gamma}(t)$ over 17.75 seconds is shown as the black trace in Fig. 5 along with the raw measured Doppler of each spoofing signal. The GNSS receiver allowed itself to be spoofed and the true range-rate between the LEO-based receiver and the terrestrial transmitter was lumped in the receiver's clock drift estimate as explained in Section III. The measured Doppler time history of each spoofing signal, as given in (6), follows the shape of $\hat{\gamma}(t)$ because the range-rate between the spoofer and LEO-based receiver is dominant in all traces. The deviation in the measured Doppler time history of each spoofing signal from $\hat{\gamma}(t)$ is $\tilde{f}_n(t)$, as presented earlier.

The time history of $\hat{\gamma}(t)$ was fed to the nonlinear least-squares estimator described in Section IV. The final position fix, shown in Fig. 6, was within 68 meters of the true location.

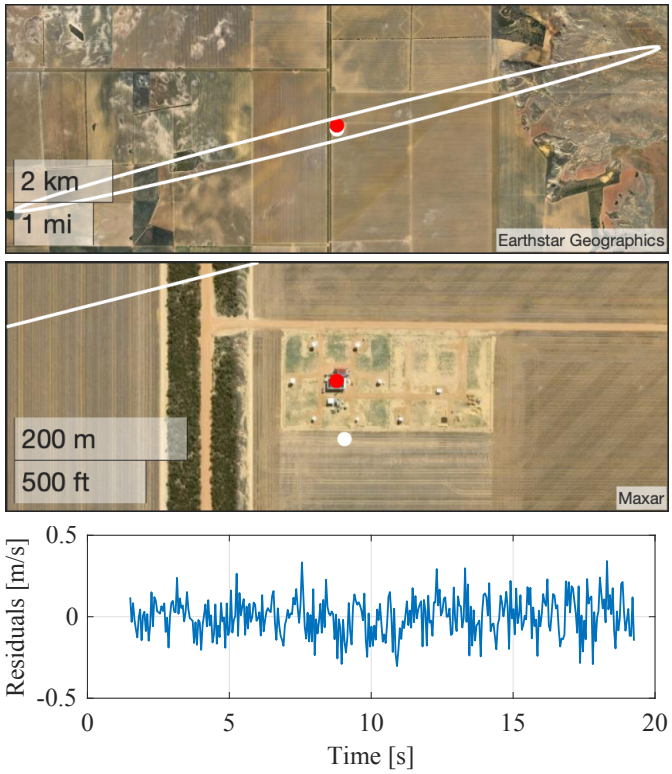
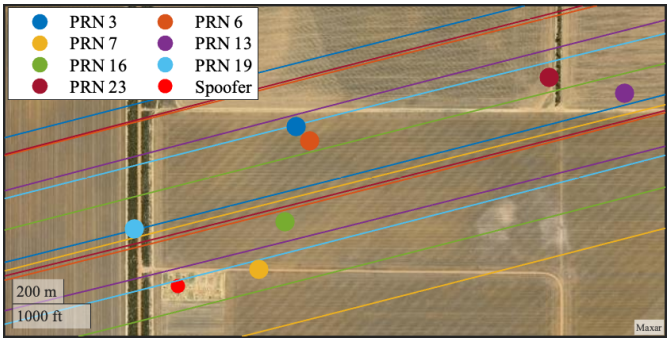


Fig. 6: Top two figures: Final spoofer position estimate (white) based on $\hat{\gamma}(t)$. Shown in red is the true spoofer location. The error of the final estimate is 68 m. The true emitter is contained within the 95% horizontal error ellipse, derived from (29), which has a semi-major axis of 6.7 km. Bottom: Post-fit residuals of $\hat{\gamma}(t)$ time history are unbiased and have a standard deviation of 0.12 m/s.

Importantly, the true emitter position lay within the estimate's horizontal 95% error ellipse. For the measurement covariance matrix, σ_{a} was set to 0.15 m/s, and σ_v was set to 0.0163 m/s, which is consistent with the transmitter's TCXO. The error ellipse's eccentricity is dictated by the receiver-transmitter geometry. Shown in Fig. 6 are the Doppler post-fit residuals, which are zero-mean with a standard deviation of 0.12 m/s. Such small and unbiased residuals indicate that the estimator's model for $\hat{\gamma}(t)$ is highly accurate. This experiment provides a validation of this paper's geolocation technique.

C. Experimental Spoofer Geolocation with GNSS Observables

This paper's advocated technique requires a means of getting ephemerides and clock models of the spoofed navigation satellites implied in the spoofing. But for cases in which the GNSS receiver onboard a LEO satellite cannot be configured to produce a PVT solution from the spoofed signals, yet does produce standard Doppler observables for each spoofed signal, traditional Doppler-based geolocation as in [37] can be applied to estimate the spoofer's location. Of course, as shown earlier, this will yield a biased estimate of the spoofer's position because the time-varying frequency term $\tilde{f}_n(t)$ is unmodeled. However, if the spoofing signals induce a static terrestrial



PRN	3	6	7	13	16	19	23
Error [m]	772	763	322	1,897	487	281	1,661

Fig. 7: Geolocation using the observed Doppler time history of each spoofed PRN. Each individual spoofer position estimate is biased due to the unmodeled frequency component.

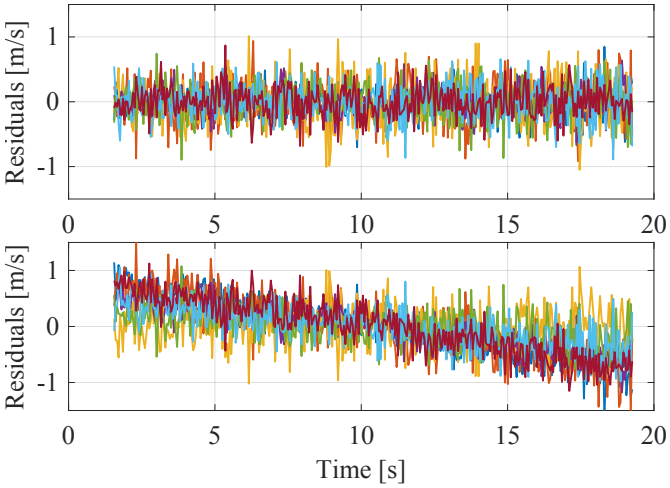


Fig. 8: Top: Range-rate residuals with respect to the estimated spoofer position. Bottom: Range-rate residuals with respect to the true spoofer position. Note: the colors used in this figure to denote different PRNs are the same as those given in the legend for Fig. 7.

location, the position bias due to the nonzero $\tilde{f}_n(t)$ is small enough that the geolocation solution remains useful.

The position bias is relatively small because the Doppler time rate of change between a stationary receiver on the surface of the Earth and a GNSS satellite in medium Earth orbit is never more than 1 Hz/s, and typically much smaller. Thus the range-rate between the LEO-based receiver and the physical spoofer is the dominant term in $f_n(t)$. Shown in Fig. 7 are the biased position fixes and corresponding error ellipses when each $f_n(t)$ time history is fed as measurements to the nonlinear least-squares estimator as described in Section IV. Only two of the seven 95% error ellipses contain the true spoofer position. The spread of the spoofer position estimates is relatively tight, with the maximum error being 1.9 km. Depending on the desired accuracy requirements, this level of accuracy may be sufficient. Note that if the spoofer's induced

trajectory were dynamic rather than static, the spread of the geolocation estimates would be larger, as shown in [50].

Shown in Fig. 8 are the range-rate residuals with respect to the estimated spoofer positions (top panel) and the true spoofer position (bottom panel). In the range-rate residuals with respect to the true spoofer position, the time-varying frequency component is visible, especially for PRNs 13 and 23, which also yield the final spoofer position estimates with the largest amount of error.

VI. Spoofer Clock Instability Error Analysis

This section analyzes how transmitter clock instability translates to range-rate-based geolocation positioning error. It is important to characterize such errors as they manifest in real-world applications. In this section, assume that $\delta\dot{t}_{\tilde{\mathrm{r}}} = 0$ so that the effects of actual—not induced—clock instability may be considered in isolation. The marginal contribution of transmitter clock instability to horizontal positioning error scales directly with the transmitter oscillator quality, specified by h_{-2} in (14). This general result applies to any clock quality and any capture geometry.

As an example consider the capture scenario in Section V for a 20-second capture over Perth. Table I shows the contribution of transmitter clock instability to the 95% horizontal error ellipse semi-major and semi-minor axes in the absence of all other error sources. The orientation of the error ellipse is determined by the capture geometry. In general, the semi-major axis lies in the cross-track direction of the satellite's motion, while the semi-minor lies in the along-track direction. Table I shows that single-satellite range-rate-based geolocation is sensitive to the transmitter clock quality. Thus, a spoofer could in theory use a low-quality oscillator to degrade geolocation accuracy. But its spoofing signals would then more easily be detected by victim receivers, as will be discussed in the next section, rendering it a less-effective spoofer.

Clock Quality	h_{-2}	Semi-major [m]	Semi-minor [m]
Low-quality TCXO	3×10^{-19}	51,449	2,033
TCXO	3×10^{-21}	5,145	203
Low-quality OCXO	3×10^{-23}	514	20
OCXO	3×10^{-25}	51	2

TABLE I: Theoretical marginal contribution of transmitter clock instability to the 95% horizontal error ellipse for the capture scenario specified in Section V in the absence of all other error sources.

The importance of correctly modeling R is emphasized here using Monte Carlo trials to compare two key metrics in geolocation: root mean square error (RMSE) between the true and estimated spoofer position, and containment percentage.

For the RMSE comparison, the true range-rate time history for the 20 second capture scenario specified in Section V was computed. For each Monte Carlo trial, both a realization of Gaussian random walk consistent with a specified h_{-2} and AWGN with σ_a = 0.1 m/s were added to the true range-rate. The noisy range-rate measurements were served to the nonlinear least-squares estimator with the correct measurement

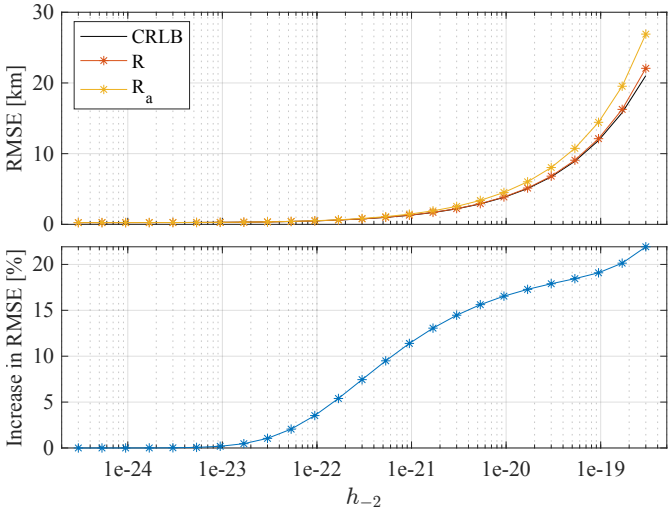


Fig. 9: Top: Monte Carlo sample RMSE as a function of h_{-2} with the capture geometry specified in Section V, for an estimator applying the correct (R) and incorrect (R_{a}) measurement covariance. Bottom: Percentage increase in sample RMSE when R_{a} is applied rather than R.

covariance R as specified in (19), and then with an incorrect measurement covariance equal to R_{a} (i.e., R_{b} in (19) was set to zero). After the 10,000 Monte Carlo trials, the sample RMSE was calculated for the sets of geolocation estimates corresponding to R and R_{a}. This was repeated with various h_{-2} values representative of a range of oscillators from low-quality TCXO to OCXO. The results are shown in Fig. 9.

One notes that the sample RMSE exhibited when using the correct measurement covariance R nearly achieves the CRLB. By contrast, erroneously modeling the measurement noise as AWGN, as is the case when only R_{a} is used, ignores the time correlation introduced by the transmitter clock instability, resulting in a greater-than 20% increase in RMSE when the transmitter is driven by a low-quality TCXO. To be sure, the degradation in RMSE is only noticeable for $h_{-2} > 3 \times 10^{-23}$, corresponding to a low-quality OCXO or worse. The increase in RMSE becomes more prominent when a low-quality oscillator drives the transmitter because in this case the unmodeled Gaussian random walk process is the dominant contributor to the measurement noise, increasing the correlation between measurements.

Although taking R_{a} alone as the measurement covariance is incorrect, an *unbiased* estimate is still achieved. Nonetheless, the associated estimated state error covariance becomes erroneously low. Using the correct measurement covariance produces an unbiased minimum-variance estimate with properly sized state error covariance.

In addition to yielding a worse RMSE, using R_{a} results in a significantly worse containment percentage within the corresponding theoretical 95% error ellipse. Containment percentage is the percentage of trials in which the true transmitter position lies within the theoretical 95% error ellipse centered at the estimated location.

A separate study of 10,000 Monte Carlo trials was con-

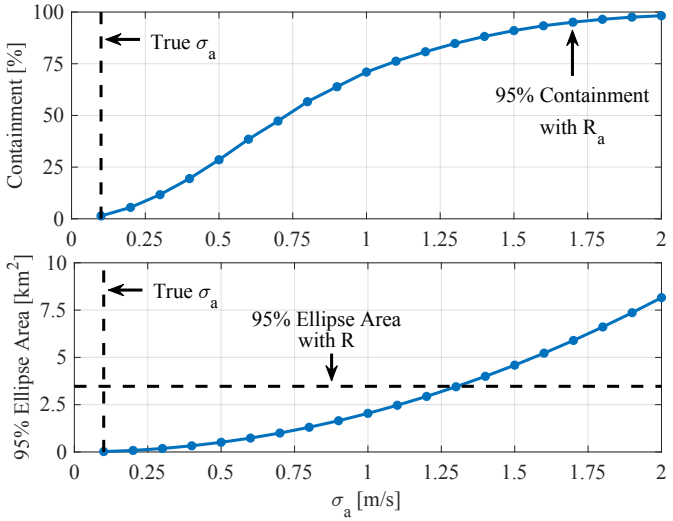


Fig. 10: Top: Monte Carlo containment percentage when the theoretical 95% error ellipse has been calculated with R_a alone [setting $R_b = 0$ in (19)], for various values of the underlying parameter σ_a. Bottom: Area of the corresponding theoretical 95% error ellipse as a function of σ_a. The horizontal line shows the area of the of the theoretical 95% error ellipse with the correct full measurement covariance R. The vertical lines in both plots indicate the true value of σ_a assumed in the Monte Carlo simulations.

ducted, again with the capture geometry specified in Section V. For each trial, both a realization of AWGN with σ_a = 0.1 m/s and a Gaussian random walk consistent with a TCXO with $h_{-2} = 3 \times 10^{-21}$ were added to the true range-rate. When the correct measurement covariance R was used, the corresponding theoretical 95% error ellipse contained the transmitter in 95.31% of trials, as expected by a properly modeled estimator. The area of this 95% error ellipse was 3.47 km^2.

By contrast, when R_b was neglected and only R_a was used, there was significant degradation in the containment percentage. For a case with R_a based on σ_a = 0.1 m/s, the containment percentage fell to 1.38%. Fig. 10 shows the containment percentage for identical cases except with various different values of modeled σ_a. As one would expect, increasing the modeled σ_a improves containment percentage. If σ_a were increased to 1.7 m/s, a 95% containment percentage with R_a is achieved. But this artificial inflation of σ_a comes at the cost of having a larger 95% error ellipse. Fig. 10 also shows the area of the theoretical 95% error ellipse for various values of σ_a. The area of the 95% error ellipse for σ_a = 1.7 m/s is 5.90 km^2, which is a 70% increase in the 95% error ellipse area when compared using to the correct measurement covariance. If σ_a were set to maintain the same 95% error ellipse area as the correct measurement covariance, a containment percentage of only 84.8% is achieved.

Properly modeling transmitter instability is thus essential in range-rate-based geolocation so that the minimum-variance estimate is calculated and the theoretical containment percentage is maintained.

VII. Controlling Spoofing Detection While Degrading Geolocation Accuracy

Researchers have developed formidable defenses against spoofing based on receiver clock state monitoring [19]–[21]. A would-be spoofer has little flexibility to meddle with the spoofed clock drift $\delta\dot{t}_{\tilde{r}}(t)$ if intending to avoid detection by such defenses. It follows that a stealthy spoofer is scarsely able to purposefully degrade geolocation accuracy.

But consider a conspicuous spoofer—one willing to accept a potentially high spoofing detection rate among affected receivers performing optimal time-based spoofing detection. In this case, the spoofer is allowed more flexibility to manipulate $\delta\dot{t}_{\tilde{r}}(t)$ with the aim of either (1) inflating victim receivers' timing error, or (2) confounding geolocation based on this paper's technique. This section derives and analyzes the attack configuration that maximally increases geolocation error while maintaining a specified detection rate among affected receivers implementing an optimal receiver clock drift monitoring spoofing detection strategy.

A. Optimal Spoofing Detection via Clock Drift Monitoring

An optimal spoofing detection technique via receiver clock drift monitoring is presented here. Consider a time interval that spans $k \in \mathcal{K} = \{1, 2, ..., K\}$ uniformly sampled navigation epochs. At the kth epoch, the distribution of a GNSS receiver's measured clock drift $\delta\dot{t}_u$ is modeled as

$$c\delta\dot{t}_u[k] \sim \mathcal{N}\left(c\delta\dot{t}_u[k-1],\, \sigma_u^2\right) \tag{30}$$

where

$$\sigma_u^2 = \sigma_m^2 + q \tag{31}$$

is the steady-state measurement variance. Here, σ_m^2 is the component of the variance due to the measurement noise and clock dynamics function, and q is the process noise for $c\delta\dot{t}_u$, which is related to the time between navigation epochs Δt and the GNSS receiver clock parameter h^u_{-2} by [55]

$$q = 2\pi^2 h^u_{-2} \Delta t c^2 \tag{32}$$

Let

$$\eta_k = \frac{c\delta\dot{t}_u[k] - c\delta\dot{t}_u[k-1]}{\sigma_u} \sim \mathcal{N}(0,1) \tag{33}$$

be the normalized increment in measured receiver clock drift at the kth epoch. Assume that increments are independent so that $\mathbb{E}[\eta_k \eta_j] = \delta_{ij}$ for all $k, j \in \mathcal{K}$.

Optimal spoofing detection amounts to a hypothesis test that attempts to distinguish the null hypothesis H_0 (receiver unaffected by spoofing) from the alternative hypothesis H_1 (receiver captured by spoofing). Note that this section focuses solely on $\delta\dot{t}_{\tilde{r}}[k]$, the spoofed clock drift increment, while assuming that the spoofer's transmitter clock drift $\delta\dot{t}_t(t) = 0$, which is opposite the preceding section's assumption. Additionally, this analysis assumes a static GNSS receiver performing detection so that the focus is on time-based spoofing detection. Let

$$\mu_k = \frac{c\delta\dot{t}_{\tilde{r}}[k] - c\delta\dot{t}_{\tilde{r}}[k-1]}{\sigma_u} \tag{34}$$

be the normalized spoofed clock drift increment across one inter-epoch interval, with initialization value $c\delta\dot{t}_{\tilde{\mathrm{r}}}[0] = 0$ at $k = 0$, the moment when the spoofer captures the receiver.

Let θ_k represent the receiver's estimated clock drift increment at the kth epoch under either hypothesis. With the foregoing setup, this can be modeled as

$$H_0 : \theta_k = \eta_k \,, \quad k \in \mathcal{K} \tag{35}$$
$$H_1 : \theta_k = \eta_k + \mu_k \,, \quad \mu_k \neq 0, \quad k \in \mathcal{K} \tag{36}$$

A two-sided locally most powerful spoofing detection hypothesis test is applied because the receiver will not know the value of μ_k under H_1. For a single epoch, the detection statistic $\Lambda^*(\theta_k)$ is

$$\Lambda^*(\theta_k) = \theta_k^2 \tag{37}$$

and has the following distributions under H_0 and H_1

$$H_0 : \Lambda^*(\theta_k) \sim \chi_1^2 \tag{38}$$
$$H_1 : \Lambda^*(\theta_k) \sim \chi_1^2\left(\lambda\right), \quad \lambda = \mu_k^2 \tag{39}$$

where χ_n^2 and $\chi_n^2(\lambda)$ denote, respectively, the chi-squared and noncentral chi-squared distributions with n degrees of freedom and noncentrality parameter λ.

Consider detection based on data taken over a time interval that spans K navigation epochs. Let $\boldsymbol{\theta} = \left[\theta_1, \theta_2, ..., \theta_K\right]^{\mathsf{T}} \in \mathbb{R}^K$ and $\boldsymbol{\mu} = \left[\mu_1, \mu_2, ..., \mu_K\right]^{\mathsf{T}} \in \mathbb{R}^K$. The joint test statistic then becomes

$$\Lambda^*(\boldsymbol{\theta}) = \sum_{k\in\mathcal{K}} \theta_i^2 = \boldsymbol{\theta}^{\mathsf{T}}\boldsymbol{\theta} \tag{40}$$

with the following distributions under H_0 and H_1:

$$H_0 : \Lambda^*(\boldsymbol{\theta}) \sim \chi_K^2 \tag{41}$$
$$H_1 : \Lambda^*(\boldsymbol{\theta}) \sim \chi_K^2\left(\lambda\right), \quad \lambda = \sum_{k\in\mathcal{K}} \mu_i^2 = \boldsymbol{\mu}^{\mathsf{T}}\boldsymbol{\mu} \tag{42}$$

An optimal-decision constant false alarm rate threshold ν^* for a fixed probability of false alarm P_{F} can be calculated from

$$P_{\mathrm{F}} = P\left(\Lambda^*(\boldsymbol{\theta}) > \nu^* | H_0\right) = 1 - F(\nu*; K) \tag{43}$$

where $F(\nu*; K)$ is the cumulative distribution function of χ_K^2 evaluated at the detection threshold ν^*. The probability of detection is

$$P_{\mathrm{D}}(\boldsymbol{\mu}) = P\left(\Lambda^*(\boldsymbol{\theta}) > \nu^* | H_1\right) = 1 - F(\nu*; K, \lambda) \tag{44}$$
$$= Q_{K/2}\left(\sqrt{\lambda}, \sqrt{\nu^*}\right) \tag{45}$$

where $F(\nu*; K, \lambda)$ is the cumulative distribution function of $\chi_K^2\left(\lambda\right)$, and $Q_m\left(\alpha, \beta\right)$ is the Marcum Q function with $m = K/2$. The hypothesis test becomes

$$\Lambda^*(\boldsymbol{\theta}) \underset{H_0}{\overset{H_1}{\gtrless}} \nu^* \tag{46}$$

The spoofer must optimize its attack configuration against this optimal spoofing detection strategy.

B. Expression for Geolocation Error

One of the assumptions made when developing the estimator presented in Section IV was that $\delta\dot{t}_{\tilde{\mathrm{r}}}$ is constant. If instead $\delta\dot{t}_{\tilde{\mathrm{r}}}(t)$ is time-varying, the measurements $\hat{\gamma}[i]$ for all $i \in \mathcal{I}$ used for geolocation become be perturbed, increasing geolocation error. Let $\epsilon[i]$ represent the unmodeled time-varying $c\delta\dot{t}_{\tilde{\mathrm{r}}}[i]$ for all $i \in \mathcal{I}$. Then at the ith measurement epoch, $c\hat{\gamma}[i] = c\gamma[i] + \epsilon[i]$. Let the vector of measurement perturbations over the capture interval be represented as $\boldsymbol{\epsilon} = \left[\epsilon[1],\ \epsilon[2],\ ...,\ \epsilon[I]\right]^{\mathsf{T}} \in \mathbb{R}^I$, and let $\tilde{\boldsymbol{x}} = \left[\tilde{e}, \tilde{n}, \tilde{b}\right]^{\mathsf{T}}$ denote the geolocation estimation error in the east direction, north direction, and frequency bias, where $\tilde{e}$ and $\tilde{n}$ are defined in the East-North-Up (ENU) frame centered at the true spoofer position. Let $\tilde{H} \in \mathbb{R}^{I\times 3}$ denote the measurement Jacobian with respect to $\tilde{\boldsymbol{x}}$. The error $\tilde{\boldsymbol{x}}$ can be calculated as

$$\tilde{\boldsymbol{x}} = \left(\tilde{H}^{\mathsf{T}} R^{-1} \tilde{H}\right)^{-1} \tilde{H}^{\mathsf{T}} R^{-1} \boldsymbol{\epsilon} = B\boldsymbol{\epsilon} \tag{47}$$

The horizontal position error vector $\boldsymbol{e}_{\mathrm{h}}$ is defined as

$$\boldsymbol{e}_{\mathrm{h}} = \left[\tilde{e}, \tilde{n}\right]^{\mathsf{T}} \tag{48}$$

Let $\tilde{B}$ be the first two rows of B, and define the matrix $A \in \mathbb{R}^{I\times I}$ as

$$A = \tilde{B}^{\mathsf{T}}\tilde{B} \tag{49}$$

The absolute horizontal positioning error e_{h} due to the perturbation $\boldsymbol{\epsilon}$ can then be computed as

$$e_{\mathrm{h}} = \sqrt{\boldsymbol{e}_{\mathrm{h}}^{\mathsf{T}}\boldsymbol{e}_{\mathrm{h}}} = \sqrt{\boldsymbol{\epsilon}^{\mathsf{T}} A \boldsymbol{\epsilon}} \tag{50}$$

Thus, the squared horizontal geolocation error e_{h}^2 is related to the perturbation $\boldsymbol{\epsilon}$ by the quadratic form $\boldsymbol{\epsilon}^{\mathsf{T}} A \boldsymbol{\epsilon}$.

The spoofer seeks the perturbation $\boldsymbol{\epsilon}$ that maximizes e_{h} so that it can maximally degrade the accuracy of geolocation by a single sensor platform performing range-rate-based geolocation via this paper's technique. Suppose that $\boldsymbol{\epsilon}$ is subject to the constraint $\|\boldsymbol{\epsilon}\| \leq \zeta$, which will be defined in the next section. The optimization problem then becomes

$$\boldsymbol{\epsilon}^* = \underset{\|\boldsymbol{\epsilon}\|\leq\zeta}{\operatorname{argmax}}\, \boldsymbol{\epsilon}^{\mathsf{T}} A \boldsymbol{\epsilon} \tag{51}$$

To solve this problem, A is factorized as $A = QDQ^{\mathsf{T}}$, where Q is orthogonal and $D = \mathrm{diag}(d_1, d_2, ..., d_I)$ is a diagonal matrix composed of eigenvalues of A, which are all positive. Assume that the columns of Q contain the unitary eigenvectors corresponding to eigenvalues ordered such that $d_1 \geq d_2 \geq ... \geq d_I$. Then

$$\boldsymbol{\epsilon}^{\mathsf{T}} A \boldsymbol{\epsilon} = \boldsymbol{\epsilon}^{\mathsf{T}} Q D Q^{\mathsf{T}} \boldsymbol{\epsilon} = \boldsymbol{y}^{\mathsf{T}} D \boldsymbol{y} \tag{52}$$

where $\|\boldsymbol{\epsilon}\| = \|Q^{\mathsf{T}}\boldsymbol{\epsilon}\| = \|\boldsymbol{y}\|$. The value of $\boldsymbol{y}$ that respects $\|\boldsymbol{y}\| \leq \zeta$ and maximizes $\boldsymbol{y}^{\mathsf{T}} D \boldsymbol{y}$ is given by $\boldsymbol{y}^* = \left[\zeta, 0, 0, ..., 0\right]^{\mathsf{T}}$. Let $\mathbf{v}^* \in \mathbb{R}^I$ denote the unitary eigenvector corresponding to the largest eigenvalue of A. The optimal $\boldsymbol{\epsilon}$ for this optimization problem is then

$$\boldsymbol{\epsilon}^* = \pm Q\boldsymbol{y}^* = \pm\zeta\mathbf{v}^* \tag{53}$$

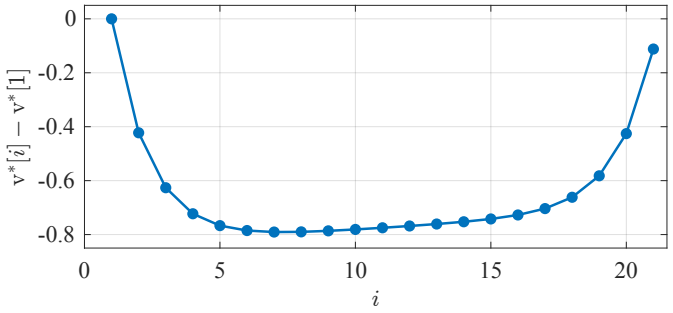


Fig. 11: The attack trajectory $\mathrm{v}[i]^* - \mathrm{v}^*[1]$ that maximizes e_h for the LEO-based receiver geometry shown in Fig. 3.

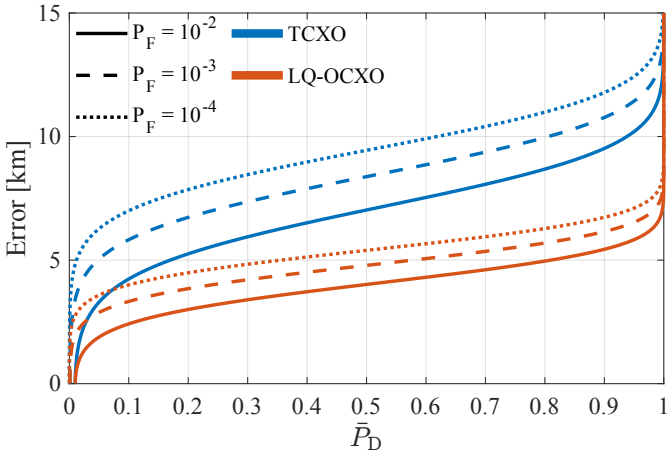


Fig. 12: Worst-case geolocation error for a spoofer that optimizes $c\boldsymbol{\delta\dot{t}}_\mathrm{r}$ for receivers performing 1-Hz spoofing detection tests with σ_m = 0.05 m/s and for the LEO-based receiver geometry shown in Fig. 3. The geolocation error is shown over a range of $\bar{P}_\mathrm{D}$ for two representative victim receiver clock quality levels and three representative values of P_F.

C. Jointly Optimized Spoofer Clock Drift Selection

Now that an optimal spoofing detector based on receiver clock drift has been presented, and a perturbation $\boldsymbol{\epsilon}^*$ that maximizes horizontal geolocation error subject to the constraint $\|\boldsymbol{\epsilon}^*\| < \zeta$ has been defined, a spoofer can develop an attack configuration for $c\delta\dot{t}_\mathrm{r}(t)$ that maximizes e_h while maintaining a specified probability of detection. It is assumed that the spoofer has perfect knowledge of the LEO-based receiver's position and velocity, which is representative of a worst-case scenario.

Let $c\boldsymbol{\delta\dot{t}}_\mathrm{r} = c\left[\delta\dot{t}_\mathrm{r}[1], \delta\dot{t}_\mathrm{r}[2], ..., \delta\dot{t}_\mathrm{r}[I]\right]^\mathsf{T} \in \mathbb{R}^I$ represent the spoofer's discretized time-varying attack configuration for $\delta\dot{t}_\mathrm{r}(t)$. Suppose the spoofer sets $c\boldsymbol{\delta\dot{t}}_\mathrm{r} = \boldsymbol{\epsilon}^*$. Then the vector of spoofed clock drift increments over $K = I - 1$ navigation epochs is equivalent to

$$\boldsymbol{\mu} = \frac{\zeta}{\sigma_\mathrm{u}} C\mathbf{v}^* \in \mathbb{R}^K \tag{54}$$

where

$$C = \begin{bmatrix} -1 & 1 & 0 & \dots & 0 \\ 0 & -1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & -1 & 1 \end{bmatrix} \in \mathbb{R}^{K \times I} \tag{55}$$

The only task remaining for the spoofer is to determine the value of ζ so that $\boldsymbol{\epsilon}^*$ can be scaled appropriately. Suppose the spoofer is willing to allow a detection probability $\bar{P}_\mathrm{D}$ for the detection test in (46). Based on the parameters σ_u, I, and P_F, the parameter ζ can be chosen to maintain an expected probability of detection $\bar{P}_\mathrm{D}$. Given the functional form of the probability of detection in (45), ζ must satisfy the equation

$$Q_{K/2}\left(\frac{\zeta}{\sigma_\mathrm{u}}\|C\mathbf{v}^*\|, \sqrt{\nu^*}\right) = \bar{P}_\mathrm{D} \tag{56}$$

Following this, the spoofed clock drift trajectory $c\boldsymbol{\delta\dot{t}}_\mathrm{r}^*$ that maximizes the geolocation error while maintaining a specified probability of detection can be represented as

$$c\boldsymbol{\delta\dot{t}}_\mathrm{r}^* = \pm\zeta\left(\mathbf{v}^* - \mathbf{1}\mathrm{v}^*[1]\right) \tag{57}$$

where $\mathbf{1}$ is the appropriately sized vector of all ones and $\mathrm{v}^*[1]$ is the first element of $\mathbf{v}^*$. Note that subtracting $\mathbf{1}\mathrm{v}^*[1]$ ensures $c\boldsymbol{\delta\dot{t}}_\mathrm{r}[1] = 0$, consistent with initialization of the spoofing attack. This subtraction does not change the optimization processes, it only affects the estimated frequency bias b_0, which is merely a nuisance parameter.

To illustrate the application of this analysis, consider the following example. Suppose a spoofer wishes to choose $\boldsymbol{\delta\dot{t}}_\mathrm{r}^*$ to maximally degrade geolocation by a LEO-based receiver capturing its signals over 21 seconds with the geometry shown in Fig. 3. Further suppose the LEO-based receiver computes measurements at 1 Hz, so that I = 21, and sets R with σ_v consistent with a TCXO and $\sigma_\mathrm{a} = 0.1$ m/s. The attack trajectory $\mathbf{v}^* - \mathbf{1}\mathrm{v}^*[1]$ that maximizes horizontal geolocation error is shown in Fig. 11. It is interesting to note that the spoofer allocates the greatest detection risk (largest increments) at the beginning and end of the 21-second capture, while maintaining lower risk (smaller increments) in the interim.

Now assume that spoofing-affected receivers are performing navigation solutions once per second with σ_m = 0.05 m/s. Shown in Fig. 12 is the maximum horizontal geolocation error given a triad of $\bar{P}_\mathrm{D}$, P_F, and affected receiver clock quality. For example, if the spoofer accepts a detection rate of $\bar{P}_\mathrm{D}$ = 0.5 by receivers equipped with a TCXO having their spoofing detector set with $P_\mathrm{F} = 10^{-3}$, the maximum e_h due to $c\boldsymbol{\delta\dot{t}}_\mathrm{r}^*$ is 8.4 km.

To give the reader an idea of how capture geometry affects the maximum horizontal geolocation error, consider the same scenario, but with a 21-second detection-and-geolocation segment beginning 30 seconds earlier. This capture geometry is more favorable for geolocation. It results in a maximum horizontal geolocation error of 2.2 km. On the other hand, consider a 21-second segment beginning 30 seconds after the original. This capture geometry is worse for geolocation. It results in a maximum horizontal geolocation error of 23.5 km. It is important to note that this worst-case error is not a limitation of this paper's technique, but a limit of single-satellite range-rate-based geolocation of GNSS spoofers in general. And it should be remembered that the foregoing

analysis is for a worst-case situation in which the spoofer knows the LEO-based receiver's position and velocity time history.

VIII. Conclusion

This paper presented a single-satellite, single-pass technique for locating GNSS spoofers from LEO. The technique was validated in a controlled experiment in partnership with Spire Global in which a LEO-based receiver captured GNSS spoofing signals transmitted from a ground station. An analytic expression for how actual transmitter clock instability degrades the geolocation solution was derived. Finally, geolocation positioning error as a function of worst-case spoofed clock behavior subject to a constraint on probability of detection was investigated.

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] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

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

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

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

[5] T. E. Humphreys, "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.

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

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

[8] K. Radoš, M. Brkić, and D. Begušić, "Recent advances on jamming and spoofing detection in GNSS," *Sensors*, vol. 24, no. 13, p. 4210, 2024.

[9] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, pp. 739–754, April 2018.

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

[11] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, T. E. Humphreys, and A. Schofield, "GNSS spoofing detection using two-antenna differential carrier phase," in *Proceedings of the ION GNSS+ Meeting*, (Tampa, FL), Institute of Navigation, 2014.

[12] B. O'Hanlon, M. Psiaki, J. Bhatti, and T. Humphreys, "Real-time spoofing detection using correlation between two civil GPS receiver," in *Proceedings of the ION GNSS Meeting*, (Nashville, Tennessee), Institute of Navigation, 2012.

[13] J. Gross and T. E. Humphreys, "GNSS spoofing, jamming, and multipath interference classification using a maximum-likelihood multi-tap multipath estimator," *Proceedings of the ION International Technical Meeting*, Jan. 2017.

[14] B. O'Hanlon, J. Bhatti, T. E. Humphreys, and M. Psiaki, "Real-time spoofing detection in a narrow-band civil GPS receiver," in *Proceedings of the ION GNSS Meeting*, (Portland, Oregon), Institute of Navigation, 2010.

[15] Z. Clements, J. E. Yoder, and T. E. Humphreys, "Carrier-phase and IMU based GNSS spoofing detection for ground vehicles," in *Proceedings of the ION International Technical Meeting*, (Long Beach, CA), pp. 83–95, 2022.

[16] Z. Clements, J. E. Yoder, and T. E. Humphreys, "GNSS spoofing detection: An approach for ground vehicles using carrier-phase and inertial measurement data," *GPS World*, vol. 34, no. 2, pp. 36–41, 2023.

[17] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "An INS monitor to detect GNSS spoofers capable of tracking vehicle position," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, pp. 131–143, Feb. 2018.

[18] B. Kujur, S. Khanafseh, and B. Pervan, "Optimal INS monitor for GNSS spoofer tracking error detection," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, no. 1, 2024.

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

[20] P. Y. Hwang and G. A. McGraw, "Receiver autonomous signal authentication (RASA) based on clock stability analysis," in *Proceedings of the IEEE/ION PLANS Meeting*, pp. 270–281, IEEE, 2014.

[21] A. Khalajmehrabadi, N. Gatsis, D. Akopian, and A. F. Taha, "Real-time rejection and mitigation of time synchronization attacks on the Global Positioning System," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 8, pp. 6425–6435, 2018.

[22] T. E. Humphreys, "Detection strategy for cryptographic GNSS antispoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013.

[23] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proceedings of the IEEE/ION PLANS Meeting*, May 2014.

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

[25] T. Mina, A. Kanhere, A. Shetty, and G. Gao, "GPS spoofing-resilient filtering using self-contained sensors and chimera signal enhancement," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, no. 2, 2024.

[26] J. Anderson, S. Lo, A. Neish, and T. Walter, "Authentication of satellite-based augmentation systems with over-the-air rekeying schemes," *NAVIGATION: Journal of the Institute of Navigation*, vol. 70, no. 3, 2023.

[27] J. Anderson, S. Lo, and T. Walter, "Authentication security of combinatorial watermarking for GNSS signal authentication," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, no. 3, 2024.

[28] C4ADS, "Above us only stars: Exposing GPS spoofing in Russia and Syria," April 2019. https://c4ads.org/reports.

[29] S. Gebrekidan, "Electronic warfare confounds civilian pilots, far from any battlefield." The New York Times, Nov. 2023.

[30] J. Arraf, "Israel fakes GPS locations to deter attacks, but it also throws off planes and ships." NPR, April 2024.

[31] A. Tangel and D. FitzGerald, "Electronic warfare spooks airlines, pilots and air-safety officials." Wall Street Journal, Sept. 2024.

[32] M. Felux, P. Fol, B. Figuet, M. Waltert, and X. Olive, "Impacts of global navigation satellite system jamming on aviation," *NAVIGATION: Journal of the Institute of Navigation*, vol. 71, no. 3, 2024.

[33] G. S. Workgroup, "GPS spoofing: Final report of the GPS spoofing workgroup," tech. rep., OPSGROUP, 2024.

[34] O. Osechas, F. Fohlmeister, T. Dautermann, and M. Felux, "Impact of GNSS-band radio interference on operational avionics," *NAVIGATION*, vol. 69, no. 2, 2022.

[35] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[36] D. M. LaChapelle, L. Narula, and T. E. Humphreys, "Orbital war driving: Assessing transient GPS interference from LEO," in *Proceedings of the ION GNSS+ Meeting*, (St. Louis, MO), 2021.

[37] M. J. Murrian, L. Narula, P. A. Iannucci, S. Budzien, B. W. O'Hanlon, M. L. Psiaki, and T. E. Humphreys, "First results from three years of GNSS interference monitoring from low Earth orbit," *NAVIGATION*, vol. 68, no. 4, pp. 673–685, 2021.
[38] A. McKibben, R. McKnight, B. C. Peters, Z. Arnett, and S. Ugazio, "Interference effects on a multi-GNSS receiver on-board a cubesat in LEO," in *Proceedings of the ION GNSS+ Meeting*, (Denver, CO), pp. 1245–1258, 2023.
[39] Z. Clements, P. Ellis, and T. E. Humphreys, "Dual-satellite geolocation of terrestrial GNSS jammers from low Earth orbit," in *Proceedings of the IEEE/ION PLANS Meeting*, (Monterey, CA), pp. 458–469, 2023.
[40] Z. Clements, P. Ellis, and T. E. Humphreys, "Pinpointing GNSS interference from low Earth orbit," *Inside GNSS*, vol. 18, no. 5, pp. 42–55, 2023.
[41] C. Chew, T. M. Roberts, and S. Lowe, "Rfi mapped by spaceborne gnss-r data," *NAVIGATION: Journal of the Institute of Navigation*, vol. 70, no. 4, 2023.
[42] M. J. Berkowitz, "America's asymmetric vulnerability to navigation warfare: Leadership and strategic direction needed to mitigate significant threats," *National Security Space Association*, July 2024. https://nssaspace.org/wp-content/uploads/2024/07/NAVWAR-FINAL.pdf.
[43] A. Sidi and A. Weiss, "Delay and Doppler induced direct tracking by particle filter," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 50, pp. 559–572, January 2014.
[44] D. Musicki, R. Kaune, and W. Koch, "Mobile emitter geolocation and tracking using TDOA and FDOA measurements," *IEEE Transactions on Signal Processing*, vol. 58, pp. 1863–1874, March 2010.
[45] K. Ho and Y. Chan, "Geolocation of a known altitude object from TDOA and FDOA measurements," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 33, pp. 770–783, July 1997.
[46] P. Ellis, D. V. Rheeden, and F. Dowla, "Use of Doppler and Doppler rate for RF geolocation using a single LEO satellite," *IEEE Access*, vol. 8, pp. 12907–12920, 2020.
[47] P. Ellis and F. Dowla, "Performance bounds of a single LEO satellite providing geolocation of an RF emitter," in *2018 9th Advanced Satellite Multimedia Systems Conference and the 15th Signal Processing for Space Communications Workshop (ASMS/SPSC)*, pp. 1–5, IEEE, 2018.
[48] P. B. Ellis and F. Dowla, "Single satellite emitter geolocation in the presence of oscillator and ephemeris errors," in *2020 IEEE Aerospace Conference*, pp. 1–7, IEEE, 2020.
[49] X. Chen, Y. Morton, W.-X. Yu, and T.-K. Truong, "GNSS spoofer localization with counterfeit clock bias observables on a mobile platform," *IEEE Sensors Journal*, 2023.
[50] Z. Clements, P. Ellis, M. L. Psiaki, and T. E. Humphreys, "Geolocation of terrestrial GNSS spoofing signals from low Earth orbit," in *Proceedings of the ION GNSS+ Meeting*, (Denver, CO), pp. 3418–3431, 2022.
[51] Z. Clements, I. Goodridge, P. Ellis, M. J. Murrian, and T. E. Humphreys, "Demonstration of single-satellite GNSS spoofer geolocation," in *Proceedings of the ION International Technical Meeting*, (Long Beach, CA), pp. 361–373, 2024.
[52] M. L. Psiaki, "Navigation using carrier Doppler shift from a LEO constellation: TRANSIT on steroids," *NAVIGATION*, vol. 68, no. 3, pp. 621–641, 2021.
[53] C. Günther, "A survey of spoofing and counter-measures," *NAVIGATION*, vol. 61, no. 3, pp. 159–177, 2014.
[54] D. Odijk, "Positioning model," in *Springer Handbook of Global Navigation Satellite Systems*, pp. 605–638, Springer International Publishing, 2017.
[55] R. G. Brown and P. Y. Hwang, *Introduction to Random Signals and Applied Kalman Filtering*. Wiley, 2012.
[56] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*. New York: John Wiley and Sons, 2001.
[57] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas Spoofing Test Battery: Toward a standard for evaluating GNSS signal authentication techniques," in *Proceedings of the ION GNSS Meeting*, 2012.
[58] Z. Clements, P. A. Iannucci, T. E. Humphreys, and T. Pany, "Optimized bit-packing for bit-wise software-defined GNSS radio," in *Proceedings of the ION GNSS+ Meeting*, (St. Louis, MO), pp. 3749–3771, 2021.
[59] H. A. Nichols, M. J. Murrian, and T. E. Humphreys, "Software-defined GNSS is ready for launch," in *Proceedings of the ION GNSS+ Meeting*, (Denver, CO), 2022.
[60] T. Pany, D. Akos, J. Arribas, M. Z. H. Bhuiyan, P. Closas, F. Dovis, I. Fernandez-Hernandez, C. Fernández-Prades, S. Gunawardena, T. Humphreys, Z. M. Kassas, J. A. L. Salcedo, M. Nicola, M. L. Psiaki, A. Rügamer, Y.-J. Song, and J.-H. Won, "GNSS software defined radio: History, current developments, and standardization efforts," *NAVIGATION*, vol. 71, no. 1, 2024.