Received: 29 September 2019 | Revised: 18 June 2020

DOI: 10.1002/navi.393

ORIGINAL ARTICLE

WILEY ION

GNSS interferometric reflectometry signature-based defense

Steven W. Lewis[1] | **C. Edward Chow**[1] | **Felipe Geremia-Nievinski**[2] | **Dennis M. Akos**[3] | **Sherman Lo**[4]

[1] Department of Computer Science, University of Colorado at Colorado Springs, Colorado Springs, CO, USA

[2] Departamento de Geodésia, Universidade Federal do Rio Grande do Sul, Porto Alegre, Brazil

[3] Department of Aerospace Engineering Sciences, University of Colorado Boulder, Boulder, CO, USA

[4] Department of Aeronautics and Astronautics, Stanford University, Stanford, CA, USA

Correspondence
Steven W. Lewis, Department of Computer Science, University of Colorado at Colorado Springs, Colorado Springs, CO, USA, 80918.
Email: slewis@uccs.edu

Funding information
Plate Boundary Observatory operated by UNAVCO for EarthScope, Grant/Award Numbers: National Science Foundation No. EAR-0350028, National Science Foundation No. EAR-0732947; National Cybersecurity Center in coordination with the Space Information Sharing and Analysis Center, Colorado Springs, CO, USA; College of Engineering and Applied Sciences, University of Colorado at Colorado Springs.

Abstract

Global navigation satellite system (GNSS) signals are vulnerable to radio frequency interference (RFI) and spoofing. RFI detection has become trivial with many detection algorithms available and built into GNSS receivers; this is not the case with spoofing. GNSS spoofing can involve generating false GNSS signals with one or more altered components of GNSS satellite transmissions: radio frequency (RF) carrier, pseudorandom noise codes, and/or the broadcast navigation messages. We present GNSS interferometric reflectometry (GNSS-IR) signature-based defense: a new methodology to defend wireless space-based positioning, navigation, and timing (PNT) transmissions against spoofing by leveraging existing, fixed GNSS receivers used in GNSS-dependent critical infrastructure and key resource sectors. GNSS-IR signature-enabled defense provides spoofing and RFI detection without any changes to existing architecture by conducting input validation of GNSS receiver observables against the generated GNSS-IR truth calibration signatures. This paper includes an overview of the theory, methodology, and results of live-sky signature variability experiments.

KEYWORDS

Interference and Spectrum Management, Jamming, Next Generation GNSS Integrity, Reflectometry, Spoofing Detection, Timing and Scientific Applications

1 | INTRODUCTION

GNSS-IR involves the forward and inverse analysis of the interferometric patterns resulting from the superposition of reflected and direct line-of-sight (LOS) radio waves transmitted from GNSS satellites (Figure 1). A receiver processes these transmissions producing observables that are used for positioning and timing [pseudorange or code phase is the main observable]. The code and carrier phases, along with the resultant received signal power, are

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.
© 2020 The Authors. *NAVIGATION* published by Wiley Periodicals LLC on behalf of Institute of Navigation.

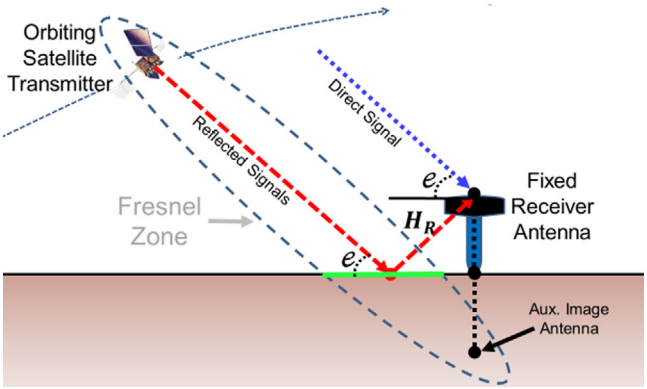

FIGURE 1 GNSS-Interferometric Reflectometry Overview [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

impacted by the interactions between the direct and indirect signals and noise.

The empirical model of the combined signal power of the direct, line-of-sight, and reflected signals is as follows (Larson & Small, 2016):

$$SNR\ (\mathrm{e}) = A\,(\mathrm{e}) \sin\left(\frac{4\pi H_R}{\lambda} \sin \mathrm{e} + \phi\right). \quad (1)$$

As the elevation (e) of a transmitting satellite changes with respect to the local horizon, the reflected signals of wavelength (λ) are primarily impacted by the near-reflection or First Fresnel Zone (FFZ) characteristics and properties (Figure 1). These include the dielectric constants, surface roughness, and the distance between the antenna and reflector(s) (H_R). The reflected, sometimes called multipathed, signals experience attenuation and delay, impacting the amplitude (A) and phase delay (ϕ), respectively. The power and phase differences between the reflected signals and direct signals cause constructive and destructive interference in the auto-correlation function (ACF) of the receiver. The resultant combined signal power produces dampened sinusoidal interference patterns. Furthermore, with a fixed or stationary receiver and transmitting satellites that have repeating ground tracks (such as in the GPS), these signatures repeat every sidereal day. While not fully explored in this paper, a similar phenomenon is seen in the interferometric code and carrier observations. It is important to point out that we have chosen to use the term signal-to-noise ratio (SNR) for simplicity, and not carrier-to-noise density, C/N0; a thorough and detailed explanation of these terms can be found in Joseph (2010). SNR is normally expressed in decibels, so the formulas below are to be converted to logarithmic scale when necessary:

$$SNR_{dB} = 10 \cdot \log_{10}(SNR). \quad (2)$$

GNSS interferometric reflectometry was first used in ocean altimetry experiments described in (Anderson, 2000) and leveraged previous work of the Passive Reflectometry and Interferometry System (PARIS) (Martin-Neira, 1993; Martin-Neira, Caparrini, Font-Rossello, Lannelongue, & Vallmitjana, 2001). The use of GNSS multipathed signals has broadened to a wide array of new applications such as hydrology and vegetation studies (Larson & Small, 2014, 2016; Small et al., 2010). More recently, an open-source, flat surface geometric optics simulator was released to the public and an extended physical optics simulator was developed (Geremia-Nievinski et al., 2016; Nievinski & Larson, 2014). Both have exposed GNSS-IR research and exploration to new disciplines to include cybersecurity of wireless channels as presented in this paper.

These GNSS-IR signatures are unique to each satellite-receiver pair due to the unique multipath conditions around the receiver antenna. By defining "truth" or expected signatures, one can then implement input validation of new, received signal power, code, and carrier observations to provide wireless channel security much like RF fingerprinting (Ureten & Serinken, 2007). Our paper presents an overview of the theory of our novel defense, an explanation of the methodology used to generate truth calibration signatures and subsequent input validation methods of new observations and, finally, the results from signature variability experiments using field data.

2 | THEORY OVERVIEW

A spoofer attempts to establish malicious, one-way wireless [tracking] channels with target receivers to mimic and replace the true, authentic wireless channels of the GNSS satellites to cause disruption or produce false, yet plausible, PNT solutions. There are many possible ways to implement a spoofer (Psiaki & Humphreys, 2016). In order to be successful, a spoofer must produce a signal with a precisely aligned code and carrier in order to surreptitiously capture the tracking loop of a receiver. Alternatively, a spoofer can attempt a capture when a receiver's tracking loop is disadvantaged, such as during a cold or warm start or following a disruption. Disruption of the tracking loop, however, is self-evident through straightforward received signal power monitoring, so we have scoped this paper on defense against a signature-matched spoofer with the smallest published power advantage (+1.3 dB) that attempts to take over the tracking loop surreptitiously.

The basic premise of GNSS-IR signature-based defense rests on existing, foundational signal propagation theory: a spoofer's wireless channel to a target receiver will have its own direct and reflected amplitude and phase

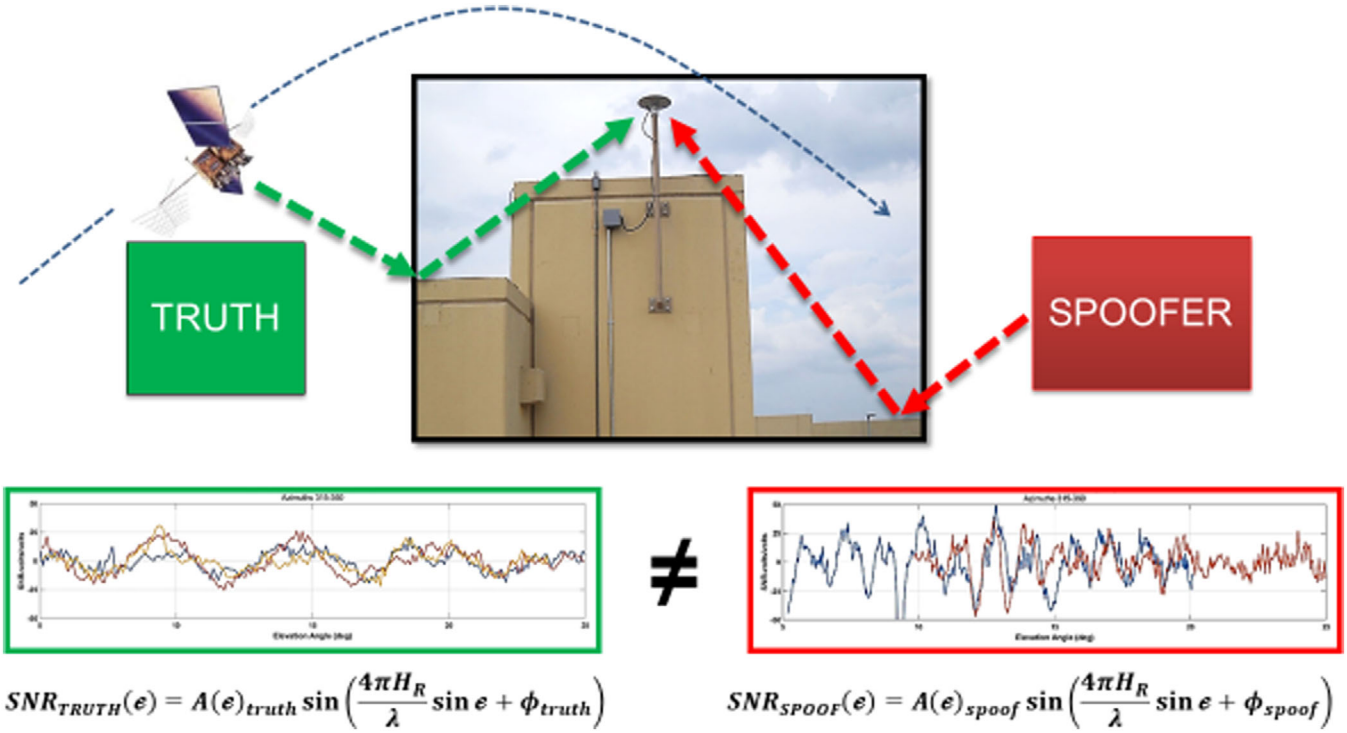

FIGURE 2 GNSS-IR Signature-based Spoofing Defense Theory Overview [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

contributions producing a different signature than truth (Figure 2). In order to successfully spoof a target receiver without being detected by GNSS-IR signature-based defenses, a spoofer must address key technical challenges. It must ensure that its composite amplitude and phase contributions from both its direct and reflected signals are very close to the truth composite direct and reflected signals. This means that a spoofer must compensate for the diverse, time-variant FFZ contributions of the interferometric quantities for all GNSS-IR signatures at a given fixed receiver. This would be very hard for a single spoofer to solve without having prior knowledge of all signatures, having a common line-of-sight with each spoofed satellite, and preventing additional reflected contributions.

3 | GNSS-IR SIGNATURE COMPOSITE AMPLITUDE AND PHASE

We can describe the theoretical model of the truth signature interferometric quantities (i) of amplitude (A) and phase (ϕ) as follows:

$$SNR = \frac{A^2_{composite\ power}}{A^2_{noise\ power}} \tag{3}$$

$$A^2_{composite\ power} = A^2_{direct\ signals} \cdot \left[1 + A_i^2 + \sqrt{2} \cdot A_i \cdot cos\left(\phi_i\right)\right] \tag{4}$$

$$A_i = \frac{A_{reflected\ signals}}{A_{direct\ signals}} \tag{5}$$

$$\phi_i = \phi_{reflected} - \phi_{direct}. \tag{6}$$

The theoretical model above would require detailed knowledge of many physical quantities (such as antenna gain pattern and surface permittivity). In practice, it can be fit by an empirical model involving polynomials of the following form:

$$SNR \approx P + A \cdot cos\left(\phi\right) \tag{7}$$

$$P = P_0 + P_1 \cdot sin\left(e\right) \tag{7a}$$

$$A = A_0 + A_1 \cdot sin\left(e\right) \tag{7b}$$

$$\phi = \phi_0 + \phi_1 \cdot sin\left(e\right) \tag{7c}$$

$$\phi_1 = \frac{4 \cdot \pi}{\lambda} \cdot H_R, \tag{7d}$$

where P is power, P_0 is the average SNR, and P_1 is the trend line slope from rise to set; where A is amplitude, A_0 is the average amplitude, and A_1 is a dampening factor; where

ϕ_0 is the arbitrary phase-shift and ϕ_1 is a linear coefficient proportional to H_R; and where λ is the carrier wavelength and H_R is the distance between the antenna and the reflector(s).

We can then show the relationship between the theoretical model and the empirical model as follows:

$$SNR \approx P_0 + A_0 \cdot \cos\left[\phi_0 + \phi_1 \cdot \sin(e)\right] \tag{8}$$

$$\phi_1 = \text{avg}\left\{\frac{\phi_i}{\sin(e)}\right\} \tag{8a}$$

$$\phi_0 = \text{avg}\{\phi_i - \phi_1 \cdot \sin(e)\} \tag{8b}$$

$$A_0 = \text{avg}\left\{\frac{\sqrt{2} \cdot A^2_{direct} \cdot A^2_{reflected}}{A^2_{noise}}\right\} \tag{8c}$$

$$P_0 = \text{avg}\left\{\frac{A^2_{direct} \cdot A^2_{reflected}}{A^2_{noise}}\right\}, \tag{8d}$$

where avg{x} is the averaging operator evaluated between the elevation range selected for a specific satellite.

The spoofed composite amplitude and phase will rarely be equal to the true signal paths as follows. The spoofed direct amplitude could attempt to start smaller than the true direct amplitude and attempt to take over the tracking loop very slowly so that the receiver does not notice, or simply step in and overpower it. It is impractical to spoof the phase due to the difficulty of estimating and controlling the free space propagation effects on both the genuine and spoofed signals. Even a sophisticated spoofer, capable of calculating these errors and attempting to compensate for the uncertainties, could only provide limited predictions for a single target, as many of the errors are temporal and location dependent. Because of these phase-matching complexities, a moving spoofer attempting to spoof all visible tracked GNSS satellites used in a plausible PNT solution is impractical. Furthermore, assuming a spoofer is near-Earth and not implemented as a broadcasting satellite that is in a similar orbit as the truth GNSS satellite it is trying to spoof, its radio transmissions will be more like a spherical wave and not like a plane wave.

Adding a spoofed signal further changes the signal environment by adding additional direct and reflected signals and altering the signal and noise power levels within the RF spectrum of interest. In particular, there are a few cases that must be examined: a spoofed signal that is not being tracked by the target receiver, a spoofed signal that is in the process of taking over the target receiver, and a spoofed signal that has taken over the tracking loop and is being tracked by the target receiver. Let's use primed quantities, amplitude (A') and phase (ϕ'), in compact phasor notation to denote the spoofed direct (d) path and spoofed reflected (r) path:

$$A'_d \angle \phi'_d \tag{9}$$

$$A'_r \angle \phi'_r. \tag{10}$$

Now, let's consider the spoofed reflected signal normalized by the spoofed direct signal as an example in terms of the spoofed interferometric (i) amplitude and phase:

$$A'_i \angle \phi'_i \tag{11}$$

$$A'_i = \frac{A'_r}{A'_d} \tag{12}$$

$$\phi'_i = \phi'_r - \phi'_d. \tag{13}$$

In general, the extended composite signal amplitude (A^*_c) that includes both the truth composite (A_c) and spoofed composite (A'_c) amplitude results from the phasor sum of the four paths in the complex domain:

$$(A^*_c)^2 = \left|(A_d \angle \phi_d) + (A_r \angle \phi_r) + \left(A'_d \angle \phi'_d\right) + \left(A'_r \angle \phi'_r\right)\right|^2 \tag{14}$$

$$(A_c)^2 = \left|(A_d \angle \phi_d) + (A_r \angle \phi_r)\right|^2 \tag{15}$$

$$\left(A'_c\right)^2 = \left|\left(A'_d \angle \phi'_d\right) + \left(A'_r \angle \phi'_r\right)\right|^2. \tag{16}$$

Expanding this equation, we find there are multiple interactions between paths, yielding six different phase differences instead of only one interferometric phase (ϕ_i):

$$\phi_r - \phi_d = \phi_i \tag{17}$$

$$\phi'_d - \phi_d \tag{18}$$

$$\phi'_r - \phi_d \tag{19}$$

$$\phi'_d - \phi_r \tag{20}$$

$$\phi'_r - \phi_r \tag{21}$$

$$\phi'_r - \phi'_d = \phi'_i. \tag{22}$$

With further exploration, we can try to simplify the sum and make some assumptions for specific scenarios:

1. a spoofer with a highly directive antenna would likely reduce A'_r to approximately zero;
2. a spoofer that has taken over the target receiver would have $A'_d > A_d$ and A^*_c would be close to A'_c;

3. a spoofer in the middle of an attack, on the other hand, would likely have $A'_d \approx A_d$, but $\phi'_d \neq \phi_d$ and would likely produce SNR with a high-rate interference pattern involving both the truth and spoofed direct paths;
4. an advanced spoofer injects a synthetic reflection by broadcasting a spoofed composite signal instead of just a spoofed direct signal. In this case, ϕ'_i would have to be very close to ϕ_i in order for A'_c to match a truth GNSS-IR signature, A_c.

These assumptions, however, must also take into account the additional noise added by the spoofer prior to tracking loop takeover and the complexity of generating the interferometric phase offsets over time without FFZ incursions or contributions. A highly directive antenna would also have to assume an unobstructed, direct LOS to a target receiver's antenna. It is already recommended practice for critical infrastructure receiver antennas to be placed towards the center of the roof when possible to avoid this particular scenario (US Department of Homeland Security, 2016). Furthermore, the additional GNSS-IR observables along with code-carrier linear combinations can also be leveraged to detect a spoofer during the onset of attack or drag-off.

4 | FFZ CHARACTERISTICS AND CONTRIBUTIONS

Not only is a spoofer's task of precise code and carrier time alignment difficult, but its composite interferometric quantities are highly dependent on the FFZ characteristics and contributions. As described in Hristov (2000), the elliptical dimensions for the FFZ are dependent upon the carrier wavelength, the distance between the transmitter and receiver, and the distance between the reflective surface(s) and receiver antenna. In the case of a GPS satellite, its transmitting antenna is approximately 20,200 km away from fixed receivers in critical infrastructure sectors and moves across the local sky. A fixed spoofer can be assumed to be implemented at a much lower height than a satellite and is also limited by the curvature of the Earth in addition to any size, weight, and power constraints based on an attacker's resources and available standoff distance. In these cases, the location and shape of a GPS satellite's FFZ will change over time, while a fixed spoofer's FFZ will remain fixed and likely have different dimensions and be at a different location.

The varying physical characteristics of the reflective, refractive, and dispersive surfaces within the FFZs also create additional challenges that a spoofer must potentially overcome. The FFZ of a spoofer and truth satellites are highly likely to be different and contain different surfaces, especially in a complex built environment. Many fixed receivers in critical infrastructure sectors such as the communications, transportation, financial, and power grid sectors are installed on and around structures such as buildings, radio towers, and other constructions. The antenna's distance from the reflective surfaces, or reflectors, may vary due to the complex, diverse structures in the built environment within the FFZ of the antenna. These differences in distance from the reflective surfaces (H_R) further increase the complexity of the truth signatures that a spoofer must attempt to match.

Applying these principles to a well-known experiment conducted in 2012 (Shepard et al., 2012), it is clear to recognize that the GNSS-IR signatures at the target receiver would likely not have matched truth GNSS-IR signatures. The spoofer was installed on an overlooking hill with a standoff distance of 0.62 km and used false GPS signals that were 10 dB stronger than the truth signals. Making a similar comparison using the GPS PRN 138 L1 waveform broadcast from a wide area augmentation system (WAAS) hosted payload aboard the geostationary satellite ANIK F1R with GPS PRN 17 L1, we can easily see the prominent difference the reflected contribution makes. GNSS signals (not geostationary satellites) are dynamic causing changing interaction effects within the FFZ as seen in Figure 3 with GPS PRN 17. Analysis using a static satellite, such as the geostationary WAAS ANIK F1R satellite (GPS PRN 138), serves as a good proxy for a static spoofer. Analysis of this satellite demonstrates the much smaller signal power variance, and hence a well-controlled, LOS static spoofer should have good control over the power variance of its signals when received at the monitor receiver. Hence, a spoofer with a highly directive antenna, amplitude-matching capability, and direct LOS access would be a more challenging threat as it may be able to mimic some of the natural signal power variations if it is known. However, if this type of spoofer attempts drag-off by shifting the code or carrier to alter the PNT solution, the interferometric phase will likely cause uncorrelated amplitude oscillations when compared to a truth signature.

5 | METHODOLOGY

GNSS-IR signature-based defense involves input validation of received signal power observations. The method is divided into the following steps shown in Figure 4: generate calibration signatures, perform input validation, update calibration signatures, and generate alarms.

The first step is to generate a truth or calibration signature (CalSig) for each tracked satellite at a given fixed receiver. As GNSS-IR signatures are impacted by FFZ

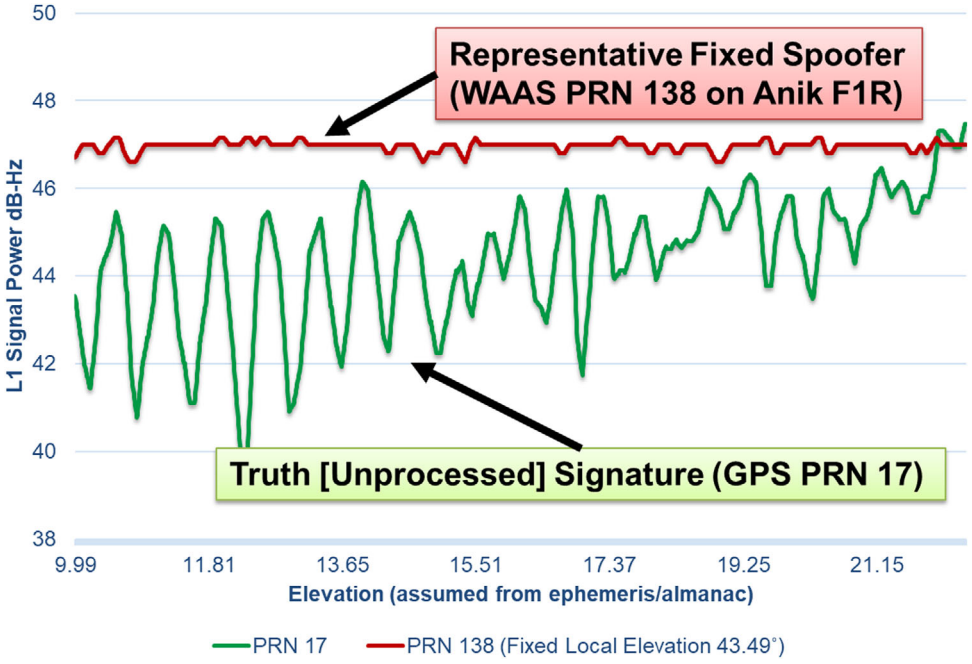

FIGURE 3 Representative results from the 2012 University of Texas live-sky spoofing event using WAAS PRN 138 as a representative-fixed spoofer versus signature from GPS PRN 17 [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

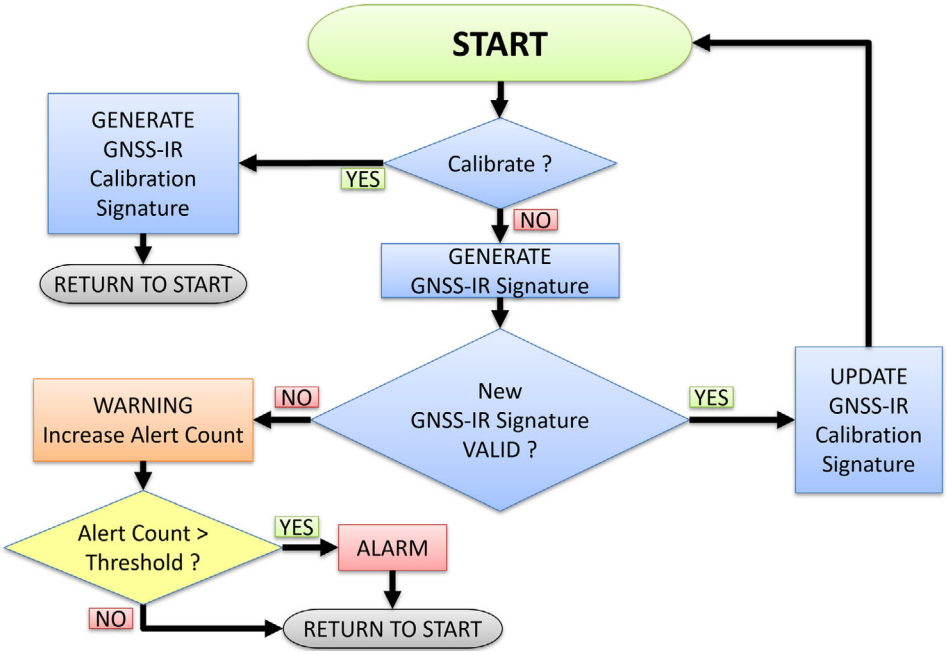

FIGURE 4 Overview of GNSS-IR Signature-based Defense Methodology [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

characteristics such as rain and human activity, it is important to collect satellite signatures over several passes to provide a good estimate of truth. For our initial experiments, we explored a five-day rolling window to adequately address common variations found in roof installations with controlled access and water mitigation as is common in many critical infrastructure sectors.

A GNSS-IR calibration signature (CalSig) was divided into the rise and set. For example, with a single GPS satellite, this is up to two passes per 24-hour period producing

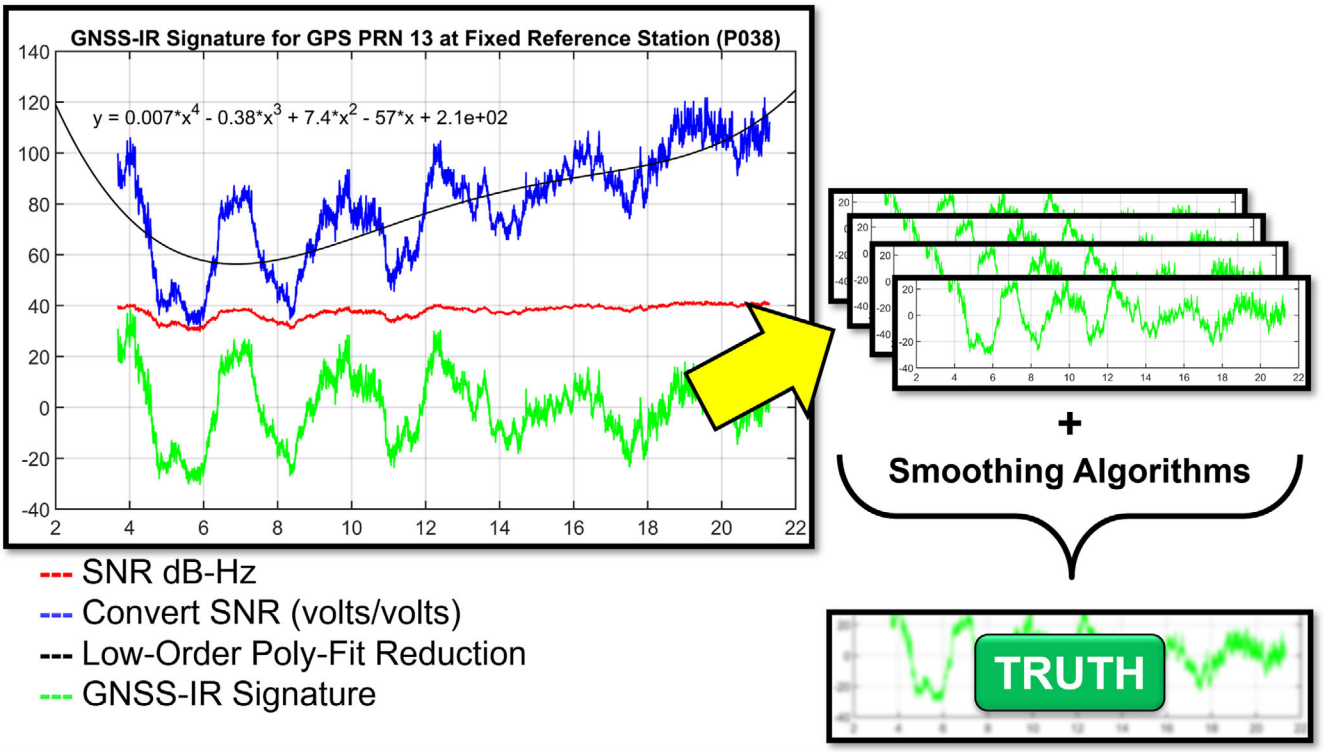

FIGURE 5 Overview of "Truth" Calibration Signature Generation [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

four signatures. To avoid typical receiver configuration constraints, satellite passes that do not exceed 10 degrees are excluded. The received signal power observation component for each signature is converted to volts/volts and reduced with a fourth-order polynomial fit curve. It is assumed that the first signature collected is genuine, and we exclude any signature with a Pearson correlation coefficient less than 0.9 during the initial and subsequent five-day windows. For initialization, this process occurs for the first five days of good observations, and then each five-day averaged window is smoothed. For this paper, we have used a simple rolling average and are exploring other methods to include Kalman filter-based smoothing (see Figure 5).

While multipath modeling with probability density functions (PDF) can be explored with both Rician and Rayleigh distributions, complete mathematical models for both noise and signal are not always useful as pointed out in Kay (2013). As such, we have chosen to explore using a CalSig to capture a noise model. The first method to characterize the noise is focused on quantifying the offset or residual (y) of a new observation (NewObs) from the truth, calibration signature (CalSig) at elevation (e) using Equation (9):

$$y = \left| NewObs\,(e) - \widehat{CalSig}\,(e) \right| . \tag{23}$$

6 | SIMULATIONS

Figure 6 shows the detection results for a simulated GNSS-IR signature-matching spoofer with +1.3 dB power advantage over the truth. This attempts to address the worst case for a static receiver as described in Humphreys et al. (2012):

Figure 7 shows the results of a simulated spoofer that does not have a matching GNSS-IR signature. At 30 degrees elevation, we simulated a 3 dB power advantage to represent an attempt to take over the target receiver's tracking loop. In this case, we used the more common testing practice of a 3 dB power advantage to ensure the non-signature-matched spoofer would more consistently hold a power advantage as its power mimics the expected oscillations. These simulations assume a "clean" takeover of the ACF. Figure 8 shows the detector output when no spoofing is present. Additional work is required to evaluate the detector performance (probability of detection, missed detection, and false detection) then establish a useful alarm threshold and measure time to alert.

An alternative way to characterize the noise is to skip removal of the low-order polynomial fit curve in the derivation of CalSig and simply calculate the normalized difference (r') of the unreduced volts/volts observations of the CalSig and NewObs at elevation (e) as follows:

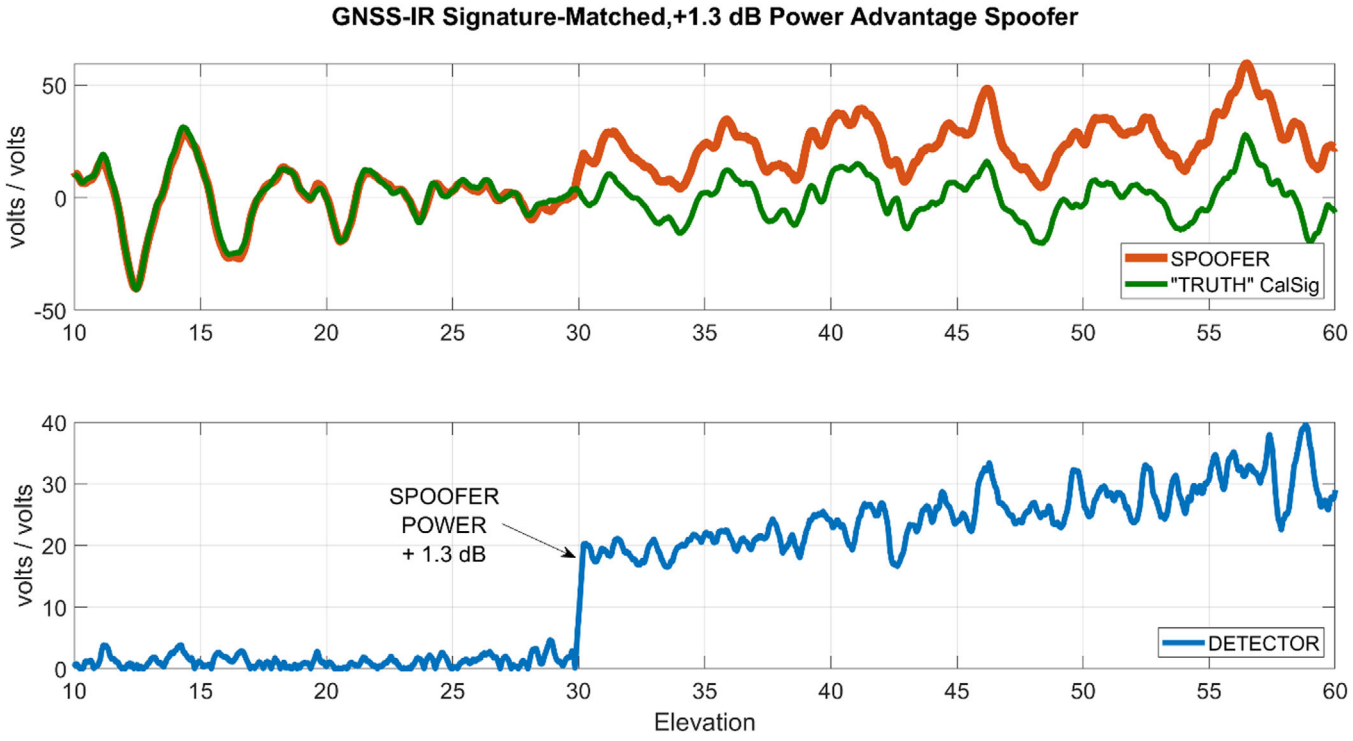

FIGURE 6 Demonstration of input validation detection algorithm with a simulated ideal, GNSS-IR signature-matched spoofer with a 1.3 dB advantage [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

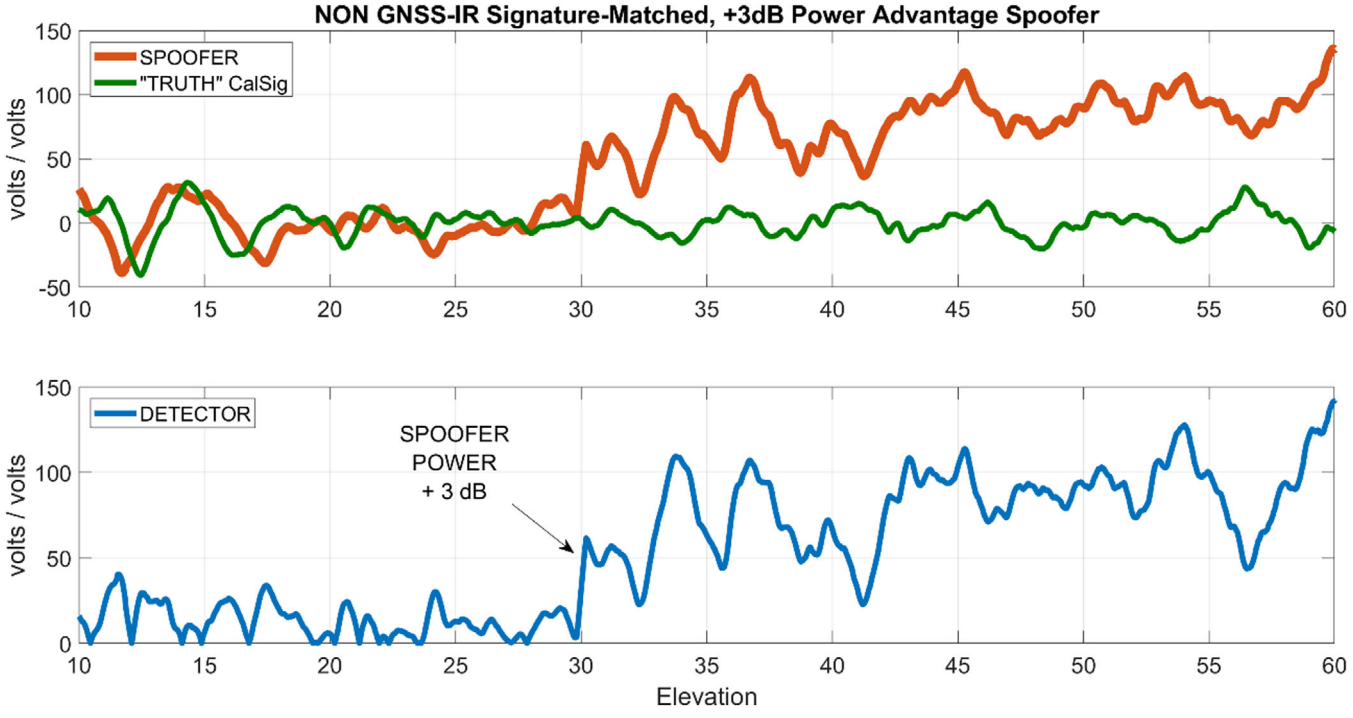

FIGURE 7 Demonstration of input validation detection algorithm with simulated non-GNSS-IR signature-matched spoofer with a 3 dB advantage [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

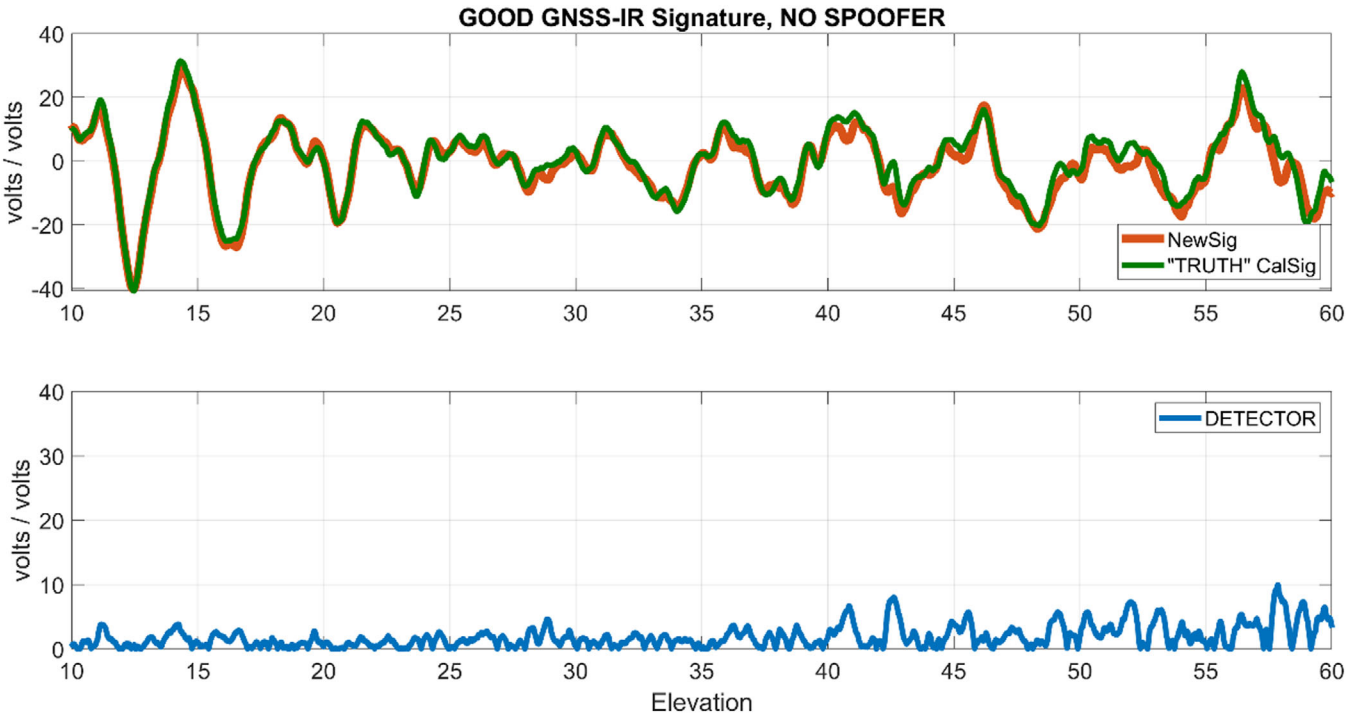

FIGURE 8 Demonstration of input validation with no spoofer present using field data [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

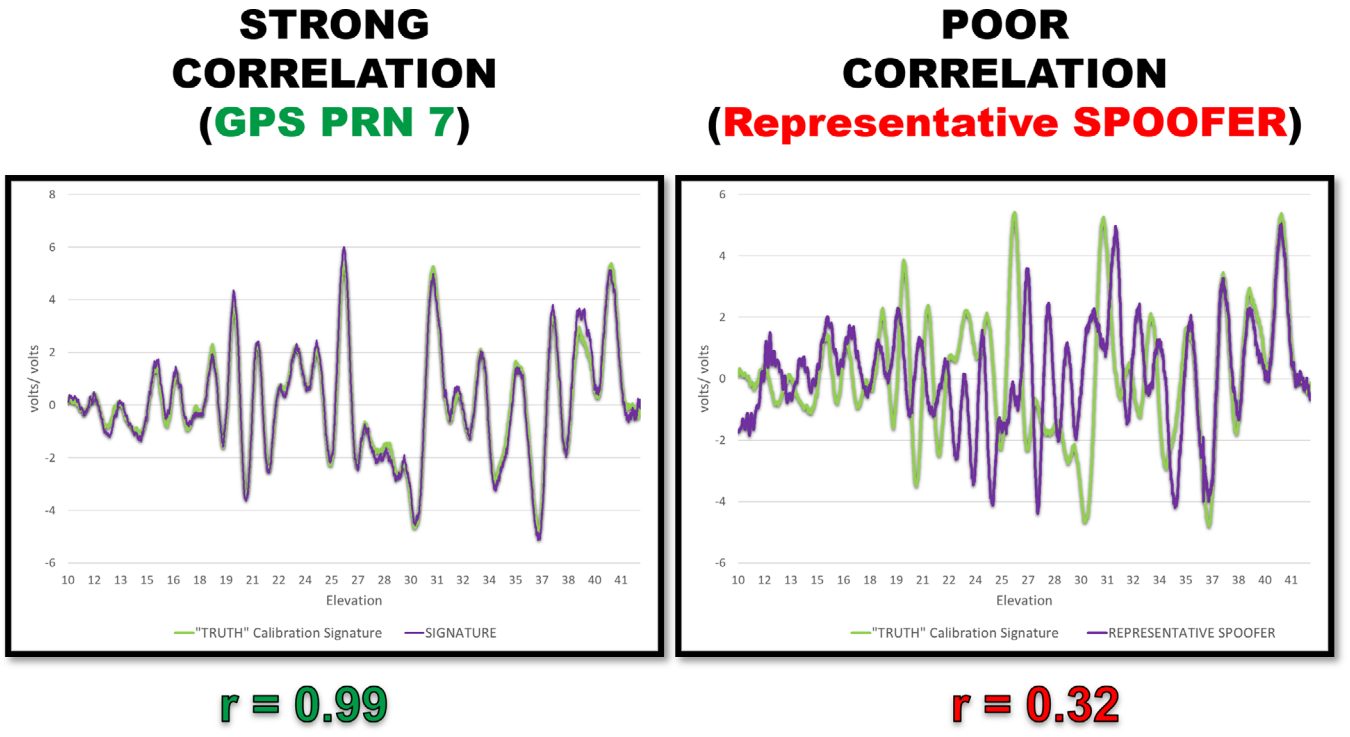

FIGURE 9 Simple input validation of (left) matching observations with strong correlation and (right) a truth signature and a representative spoofer with poor correlation. Both plots show the resulting Pearson correlation coefficient (r) [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

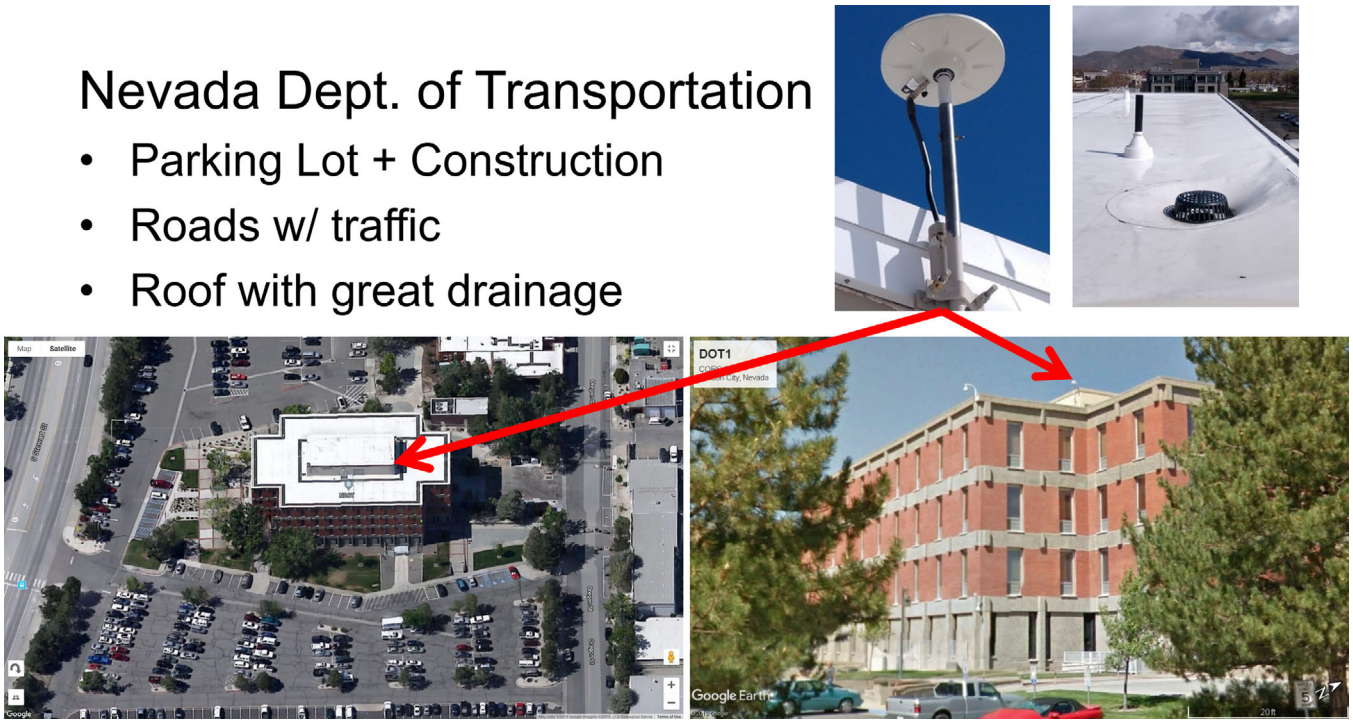

FIGURE 10 Photos of the fixed site DOT1 in Carson City, Nevada [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

$$r' = \frac{\widehat{CalSig}^2(e) - NewObs^2(e)}{\widehat{CalSig}^2(e)}. \tag{24}$$

In both detection cases, outliers would drive a confidence loop of alerts and subsequent detection alarm as shown in Figure 4. As an example, Figure 9 shows the Pearson correlation between a truth signature and new observations. On the left, the new observations are from the legitimate satellite, GPS PRN 7. On the right, a representative spoofer signature is demonstrated using the signature from GPS PRN 5 with a different FFZ at the same site. It is clear from both a visual inspection and the Pearson correlation coefficient (r) of 0.32 that the signatures do not match. However, for our method to be useful in the real world, it is necessary to find an optimal or near-optimal test statistic based on a signal model and noise statistic. Our approach was to explore signature variability with no spoofing present by first examining the Pearson correlation coefficient for signatures across several days and multiple fixed sites. We then used the variance of the residuals from the output of the detectors, Equation (23) and Equation (24), to characterize the noise with no spoofing present and then under simulated spoofing conditions. For our initial experiments, we focused on representative-fixed receivers in critical infrastructure that are on the roof of buildings with adequate water mitigation to avoid pooling water. There is still a need for future exploration of rain and snow impacts on signature variability.

7 | LIVE-SKY, SIGNATURE VARIABILITY EXPERIMENTS

The goal of our experiment was to determine if signature variability is adequate for useful detection of anomalous conditions due to RFI or spoofing without unmanageable noise variance from FFZ dynamics. We tested the worst case: high dynamics in the FFZ, a parking lot with highly varied traffic during signature generation. Our evaluation statistics used were the Pearson correlation coefficient across multiple seven-day windows at each site and the variance of the detector output.

8 | EXPERIMENT SETUP

We conducted several experiments using an actual critical infrastructure fixed reference station at the Nevada Department of Transportation in Carson City, Nevada (DOT1) and our own representative-fixed site in Colorado Springs (see Figure 10 and Figure 14). DOT1 has a Trimble NETR9 receiver with a Trimble TRM57971.00 antenna located at latitude 39° 09′ 22.31460″ North and longitude 119° 45′

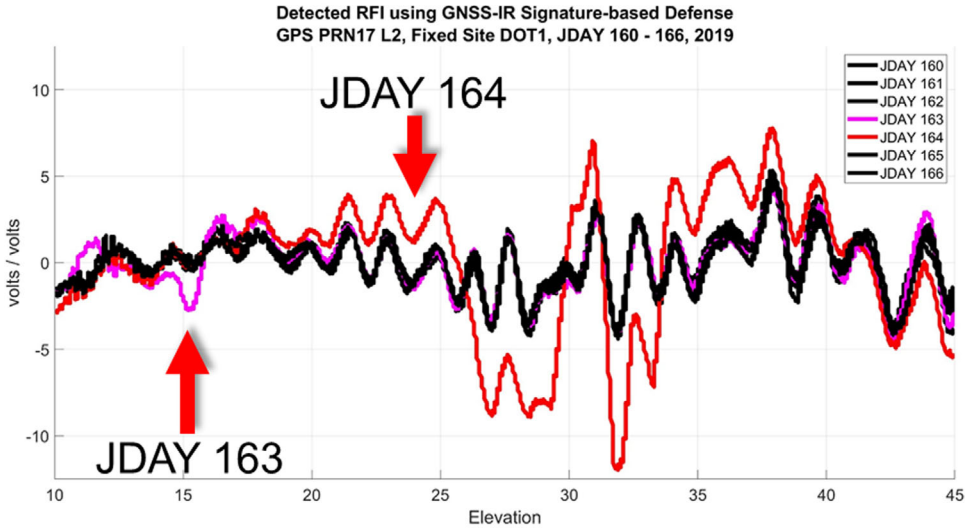

FIGURE 11 Real-World RFI event detected with GNSS-IR Signature-based Defense at DOT1 in Carson City, Nevada on June 12 & 13, 2019 [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

48.38475″ West as shown in Figure 10. The receiver is configured for both GPS and GLONASS with a mask angle of 5 degrees and the Trimble proprietary Everest Multipath mitigation algorithm disabled. DOT1 is real-time capable; however, we used the 5 Hz archived data from the University NAVSTAR Consortium (UNAVCO). The FFZ reflectors consisted of dual roof elevations with common roof polymer-coated concrete; metal and PVC drainage pipes; metal flashing; lightning rods; small, fixed dipole antennas; and connected cabling. In addition, the FFZ included the ground elevation surfaces composed of arid soil, evergreen and deciduous trees, concrete, asphalt, and a varied number of metal vehicles.

9 | EXPERIMENT RESULTS

We first collected signatures from June 9–15, 2019 at DOT1 as described in the setup above. The first set was during the night when the parking lot was relatively empty and stable. While multiple satellites showed a Pearson correlation coefficient above 0.98, we focused on GPS PRN07 that had a rising signature with an FFZ over the large parking lot on the south side of the building. We then collected signatures during the morning of those same dates. This is when employees were arriving to work and hence providing results in a more dynamic reflection environment. In this case, we used GPS PRN17 with a rising signature over the same parking lot.

To our surprise, we discovered RFI events on June 12 -13 between 7:43 am and 8:30 am local time for roughly 20 minutes each day (see Figure 11). We reported the events to the appropriate US authorities for civil GNSS disruptions, the US Coast Guard Navigation Center. They conducted a thorough investigation and confirmed it was caused by an unknown RFI source. We checked other fixed sites in and around Nevada but did not find any correlated event; it appears to have been a low-powered source near DOT1. GNSS-IR signature-based defense can indeed be used to detect RFI and jamming; however, characterization will be needed to distinguish this from spoofing.

As we conducted multiple seven-day window signature variability tests, we also discovered other observations worth noting. In particular, we noticed the signal power levels changing abruptly on satellites across the GPS constellation (see Figure 12). These events were observed at multiple fixed stations across the world and appear to be related to the GPS Notice Advisory to NAVSTAR Users (NANU) 2017005 and the public announcement by the US Air Force of an L1 C/A power level increase test for the block IIR-M and IIF GPS satellites that started in January 2017 and are further explored in (Steigenberger et al., 2019). Implementation of GNSS-IR signature-based defense will have to account for this to prevent false alarms. Fortunately, these types of events are distinct and appear correlated across L1 and L2 at multiple fixed sites.

While we did not have access to in situ rain measurements at DOT1, a weather station within three miles local to the DOT1 station reported 0.01 inches of rain sometime on both June 11 and 12. Not only does the roof where DOT1 is mounted have adequate drainage, but this amount of precipitation is not significant enough to produce noticeable variations to the signatures (although something worth exploring in a future paper to include snow). The Pearson correlation coefficient across seven days in a low dynamic environment and the five days without detection events in a higher dynamic environment was above 0.98 in our experiment (see Figure 13).

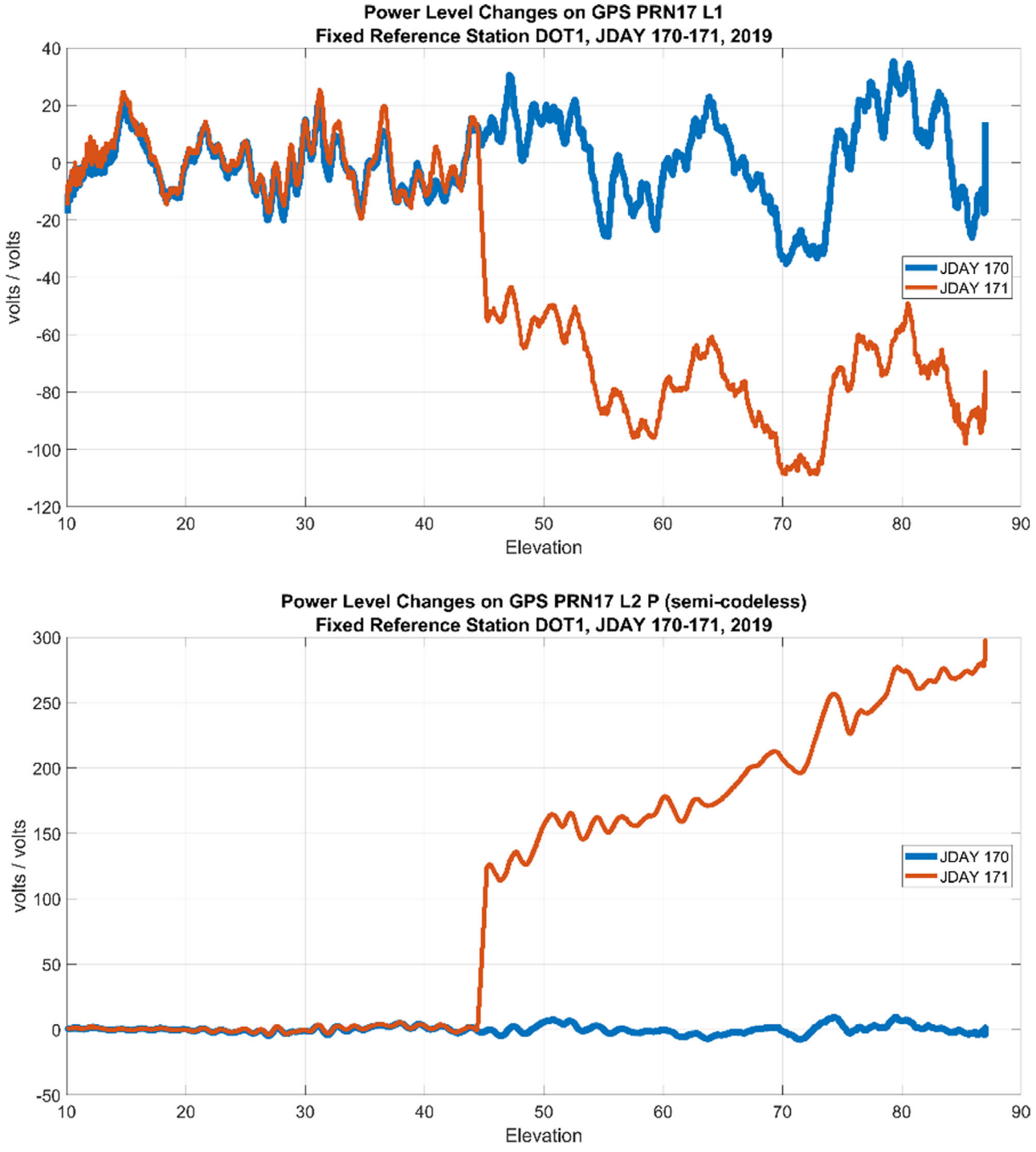

FIGURE 12 Observed Satellite Signal Power Changes during GNSS-IR Signature Variability Experiment. (top) GPS L1 power level on PRN17 decreased at approximately the same time that (bottom) L2 on the same satellite vehicle increased [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

10 | EVALUATION OF PERFORMANCE

It is important to understand how GNSS-IR signature-based defense will perform in a representative environment under nominal, non-nominal, and spoofing conditions. From June 23–27, 2019 (J-Day 174–178), we used our station in Colorado Springs, Colorado, shown in Figure 14, as a representative critical infrastructure building roof. This allowed us to manipulate site configuration and maintain control of FFZ characteristics. Our site consisted of two Septentrio PolaRx5 receivers and two tripod-mounted Septentrio PolaNt Choke Ring B3/E6

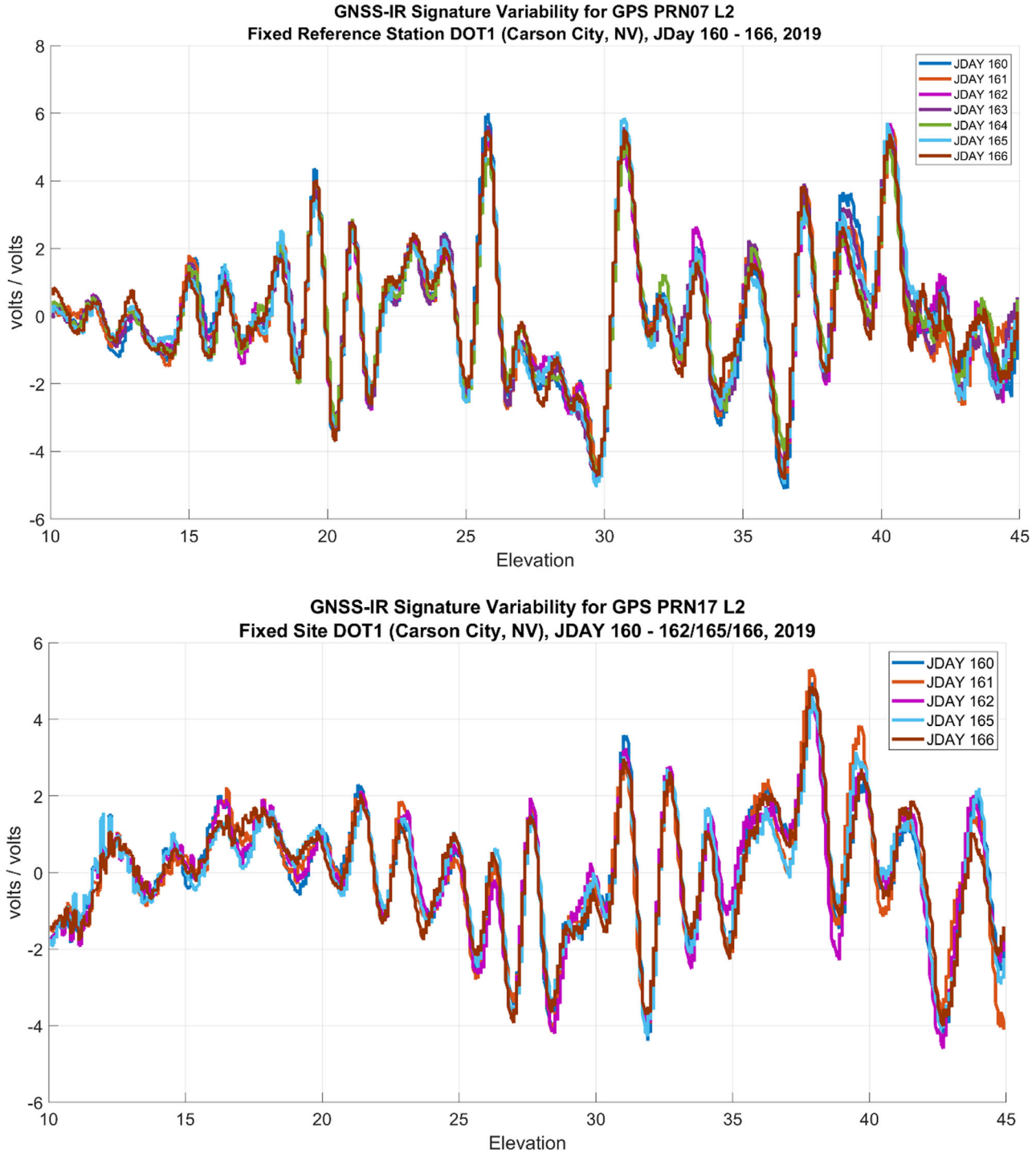

FIGURE 13 Results from DOT1 from June 9–15 during (top) the night in a low-dynamic environment and (bottom) during the morning as people arrive to work and park metal reflectors, also called cars, within the FFZ. The Pearson Correlation Coefficient was above 0.98 in both cases with a confirmed RFI event removed [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

antennas. The taller antenna was approximately 1.8 m above the surface of the roof, and the shorter antenna was approximately 1.1 m above the surface of the roof. We configured our site with 1 Hz tracking of all available GNSS signals (GPS, Galileo, GLONASS, BeiDou, and WAAS) with a mask angle of 0 degrees and disabled multipath mitigation algorithms. The roof had access control to manage human traffic and water drainage to limit the impact of pooling rain in the near-reflection zones. Unlike DOT1, the roof had a single elevation and no contributing parking lot

FIGURE 14 View of our representative-fixed critical infrastructure site with dual receivers and antennas in Colorado Springs, Colorado [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

in the FFZs due to installation constraints. The FFZ reflectors consisted of metal reflectors to include multiple, large air conditioning units with large vertical decorative metal panels for concealment. In addition, there was a pyramid-shaped glass skylight, a metal pigeon trap, and lightning rods and cables on the polymer-coated concrete and metal roof. Using this site, we explored the normalized, unreduced signatures using the PDF of the residuals (r′) produced from Equation (24) for each signature (10–max elevation).

Under nominal conditions, using GPS PRN 5 as an example, visual inspection of the signatures from the taller antenna shows a strong correlation across five days of signatures (see Figure 15). Closer inspection of the signatures using the PDF of r′ reveals spurious noise on day 1 resulting in a variance of 0.0022 and a mean of 0.0547 (dashed line PDF in Figure 16). However, the PDF of r′ for days 2–5 shows a lower variance of 0.0011 and a mean much closer to zero. This phenomenon was observed across multiple satellite signatures from both antennas during the same timeframe. Unfortunately, we did not have a rain gage and were not onsite during the experiment. However, we were able to obtain historical weather data from Colorado State University's Colorado Climate Center (http://www.climate.colostate.edu). The Colorado Springs Municipal Airport, within two miles of our station, reported 0.25 inches of precipitation on June 22 and a trace of rain on June 23 (day 1) and June 26 (day 4). The maximum air temperature was 66° Fahrenheit (F) on June 22 and 23, while the temperature reached 90°F on June 26, which likely hastened evaporation of any rain. The exact cause of the spurious noise on day 1 is unknown but is likely to have been caused by precipitation on June 22 and June 23.

We set the upper-bound detection threshold (T) at $+5\sigma$ (0.2380 residual volts/volts) of the combined detector residuals (r′) for days 1–5 as shown by the thick solid line PDF on the left in Figure 16. We intentionally chose this threshold in order to assess the performance against a non-nominal spurious noise and a simulated signature-matched spoofer with a +1.3 dB power advantage as shown by a dotted red line PDF on the right in Figure 16. A residual (r′) below the threshold was classified as a zero for no spoofing present, H(0). A residual (r′) equal to or above T was classified as the value 1 for spoofing present, H(1). Without consideration for spurious noise, the detector performed very well with only minor false detection during spurious noise (Figure 17). Using straightforward binary hypothesis Neyman-Pearson testing with this one example of spurious noise as the worst-case null hypothesis (no spoofing) and the simulated spoofer as the true hypothesis (spoofing present), it was determined that a probability of false alarm of approximately 1×10^{-5} can be achieved with a threshold of 0.25043. It is important to again point

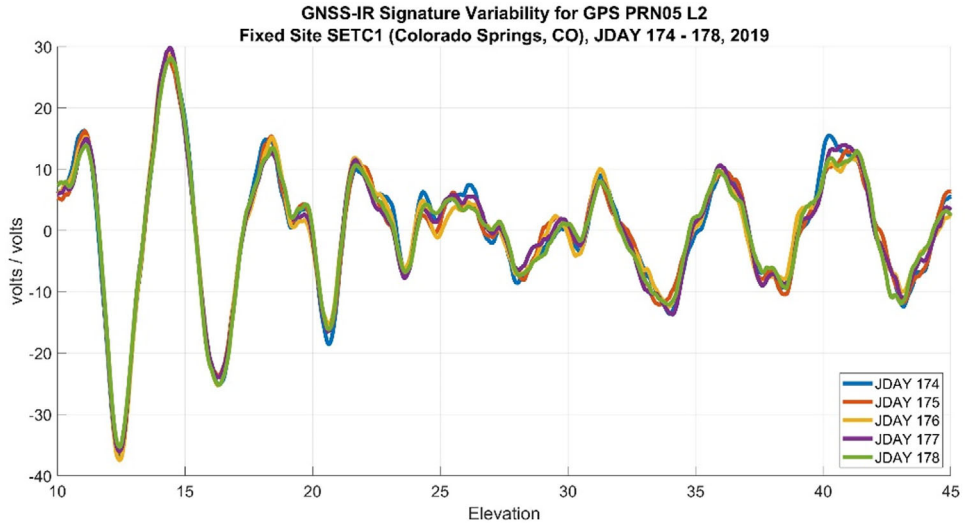

FIGURE 15 GNSS-IR signatures for GPS PRN 5 (L2C) from Colorado Springs Site from June 23–27, showing a strong correlation [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

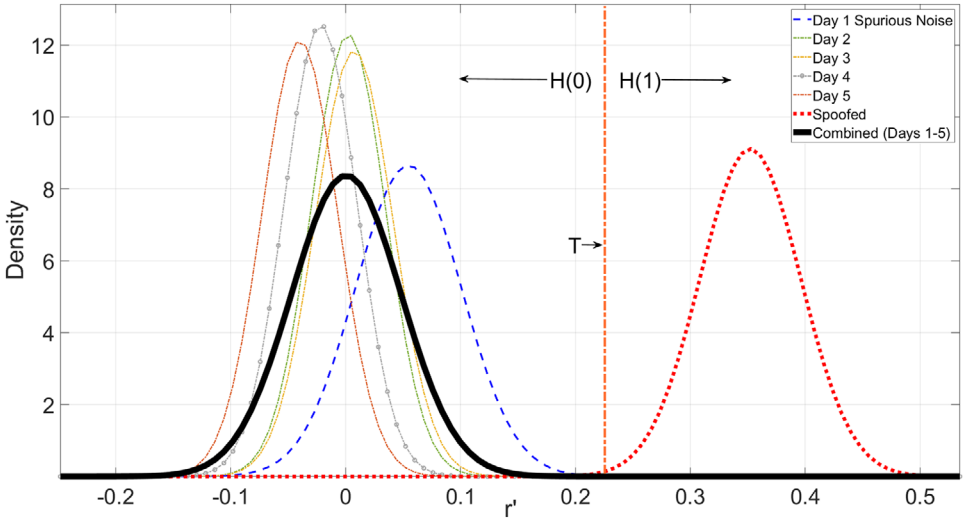

FIGURE 16 The PDFs of the normalized detector residuals (r′) from the GNSS-IR signatures for GPS PRN 7 from June 23–27, 2019 using at our representative-fixed site in Colorado Springs, CO [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

out that this evaluation included a simulated signature-matched spoofer with a +1.3 dB power advantage and assumes reflectors with relatively stable configuration and dielectric properties.

Observations collected from a shorter antenna produced improved results. Both the variance and mean of the detector residuals (r′) for all signatures were lower (see Figure 18). In particular, the spurious noise on day 1 produced a variance of 0.0015 and a mean of 0.0310 and did not cause any false positives with the same detection threshold. It appears that antenna height plays a role in not only the frequency of the signature oscillation but can also help mitigate the variance in the noise as well. Although considerations must be made for other contributing reflectors such as constructions that are not coincident to the primary reflector.

11 | FUTURE WORK

This paper is intended to only be a proof of concept of the feasibility of the new GNSS-IR signature-based defense approach. The results from the signature variability experiment using both the Pearson correlation and proposed

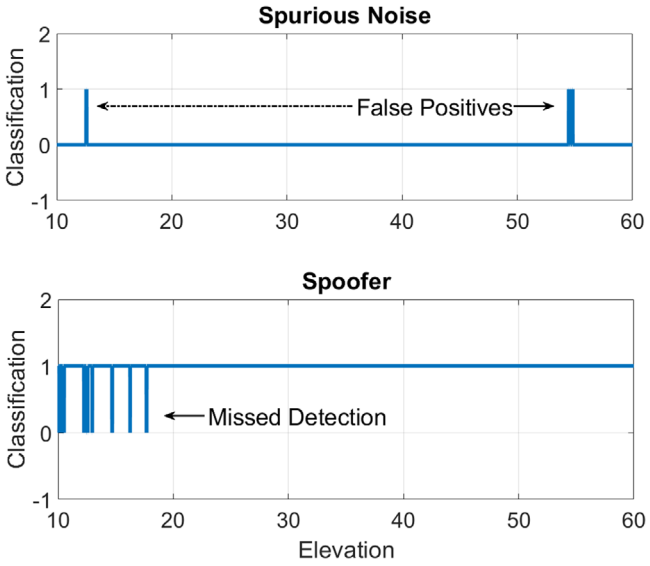

FIGURE 17 Detector results of the taller antenna with T = 0.238 showing (top) false positives from spurious noise, and (bottom) missed detection for spoofer [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

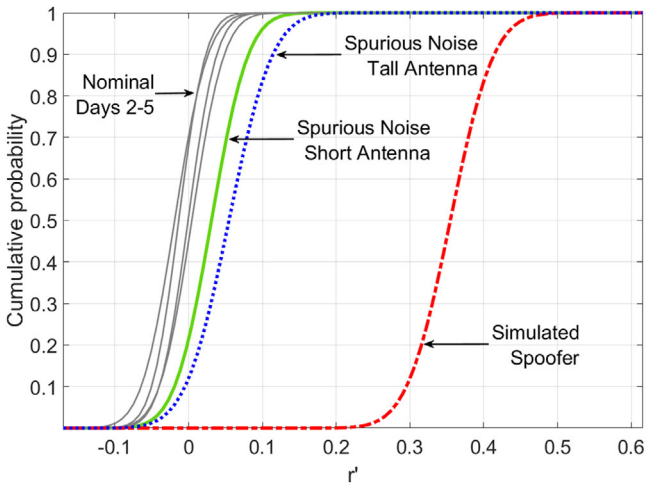

FIGURE 18 Cumulative probability density function for a simulated signature-matched spoofer with +1.3 dB power advantage showing improved results from an antenna mounted at a lower height above the reflectors [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com and www.ion.org]

noise statistics have shown there are still challenges to overcome for an operational design. While our method is intended for critical infrastructure with water mitigation in the FFZs, it is likely that snow and rain will still impact the signatures. One possible method to deal with these issues and strengthen spoofing defenses is to use two antennas of different heights that share relatively common FFZs. This would ensure that the signatures collected by both antennas are impacted by any common dynamic changes in their FFZs while requiring a spoofer to generate two different signatures for each tracked satellite. It would be difficult to prevent a receiver from tracking the spoofed signature intended for the other antenna. The next steps in our research include additional live-sky performance evaluation and performance envelope quantification. Unfortunately, live-sky GNSS disruption testing remains elusive for many in this field due to government regulations and significant coordination and cost requirements.

12 | CONCLUSION

Nations continue to trust GPS data in many critical infrastructure applications. At some point, our vulnerabilities will be exploited resulting in delayed emergency services, power grid outages, failed communication networks, or misguided disaster relief. Many critical infrastructure and key resources (CIKR) rely on fixed GNSS receivers. We have demonstrated that these prolific fixed GNSS receivers can be leveraged as spoofing and RFI detection sensors without any modifications. We have developed a new method of exploiting the existing observables from GNSS receivers to defend fixed receivers within CIKR sectors from data and measurement spoofing. GNSS interferometric reflectometry signature-based defense employs a truth calibration signature by which to perform input validation against new observations and alert users. This will offer GPS dependent systems time to employ backup or alternate PNT systems, maintain service availability, and protect our nation's critical infrastructure and key resources.

ORCID

Steven W. Lewis https://orcid.org/0000-0002-5070-7691
C. Edward Chow https://orcid.org/0000-0002-6870-2952
Felipe Geremia-Nievinski https://orcid.org/0000-0002-3325-1987
Dennis M. Akos https://orcid.org/0000-0003-4393-6442
Sherman Lo https://orcid.org/0000-0002-4814-6506

REFERENCES

Anderson, K. D. (2000). Determination of water level and tides using interferometric observations of GPS signals. *Journal of Atmospheric and Oceanic Technology*, *17*(8), 1118–1127. https://doi.org/10.1175/1520-0426(2000)017⟨1118:DOWLAT⟩2.0.CO;2

Geremia-Nievinski, F., Silva, M. F. E., Boniface, K., & Monico, J. F. G. (2016). GPS diffractive reflectometry: Footprint of a coherent radio reflection inferred from the sensitivity kernel of multipath SNR. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, *9*(10), 4884–4891. https://doi.org/10.1109/JSTARS.2016.2579599

Hristov, H. D. (2000). *Fresnel zones in wireless links, zone plate lenses, and antennas*. Artech House.

Humphreys, T. E., Bhatti, J. A., Shepard, D. P., & Wesson, K. D. (2012, September). The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques. *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, 3569–3583.

Joseph, A. (2010, December 2). GNSS solutions: Measuring GNSS signal strength. *InsideGNSS*. https://insidegnss.com/measuring-gnss-signal-strength/

Kay, S. (2013). *Fundamentals of statistical signal processing, volume III: Practical algorithm development*. Pearson.

Larson, K. M., Gutmann, E. D., Zavorotny, V. U., Braun, J. J., Williams, M. W., & Nievinski, F. G. (2009). Can we measure snow depth with GPS receivers? *Geophysical Research Letters*, *36*(17), L17502. https://doi.org/10.1029/2009GL039430

Larson, K. M., & Small, E. E. (2014). Normalized microwave reflection index: A vegetation measurement derived from GPS networks. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, *7*(5), 1501–1511. https://doi.org/10.1109/JSTARS.2014.2300116

Larson, K. M., & Small, E. E. (2016). Estimation of snow depth using L1 GPS signal-to-noise ratio data. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, *9*(10), 4802–4808. https://doi.org/10.1109/JSTARS.2015.2508673

Martin-Neira, M. (1993). A Passive Reflectometry and Interferometry System (PARIS)—Application to ocean altimetry. *ESA Journal*, *17*(4), 331–355.

Martin-Neira, M., Caparrini, M., Font-Rossello, J., Lannelongue, S., & Vallmitjana, C. S. (2001). The PARIS concept: An experimental demonstration of sea surface altimetry using GPS reflected signals. *IEEE Transactions on Geoscience and Remote Sensing*, *39*(1), 142–150. https://doi.org/10.1109/36.898676

Nievinski, F. G., & Larson, K. M. (2014). Forward modeling of GPS multipath for near-surface reflectometry and positioning applications. *GPS Solutions*, *18*(2), 309–322. https://doi.org/10.1007/s10291-013-0331-y

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the Institute of Electrical and Electronics Engineers*, *104*(6), 1258–1270. https://doi.org/10.1109/jproc.2016.2526658

Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2012). Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle. *GPS World*, *23*(8), 30–33.

Small, E. E., Larson, K. M., & Braun, J. J. (2010). Sensing vegetation growth with reflected GPS signals. *Geophysical Research Letters*, *37*(12). https://doi.org/10.1029/2010GL042951

Steigenberger, P., Thölert, S., & Montenbruck, O. (2019). Flex power on GPS Block IIR-M and IIF. *GPS Solutions*, *23*. https://doi.org/10.1007/s10291-018-0797-8

Ureten, O., & Serinken, N. (2007). Wireless security through RF fingerprinting. *North*, *32*(1), 27–33. https://doi.org/10.1109/CJECE.2007.364330

US Department of Homeland Security. (2016). *Improving the operation and development of Global Positioning System (GPS) equipment used by critical infrastructure*. https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf

How to cite this article: Lewis SW, Chow EC, Nievinski FG, Akos DM & Lo S. GNSS interferometric reflectometry signature-based defense. *NAVIGATION*. 2020;67:727–743. https://doi.org/10.1002/navi.393