Improvements to Steady State Spoof Detection with Experimental Validation using a Dual Polarization Antenna

Fabian Rothmaier, Stanford University
Yu-Hsuan Chen, Stanford University
Sherman Lo, Stanford University

BIOGRAPHY (IES)

Fabian Rothmaier is a PhD candidate at the GPS Laboratory at Stanford University. He received his B. Engr. degree from the University of Applied Sciences Bremen, Germany in 2015 and his M. Sc. degree from Stanford University in 2017.

Yu-Hsuan Chen is a research engineer at the Stanford GPS Laboratory. He received his Ph.D. in Electrical Engineering from National Cheng Kung University, Taiwan in 2011.

Sherman Lo is a senior research engineer at the GPS Laboratory at Stanford University. He received his Ph.D. in Aeronautics and Astronautics from Stanford University in 2002. He has and continues to work on navigation robustness and safety, often supporting the FAA. He has conducted research on Loran, alternative navigation, SBAS, ARAIM, GNSS for railways and automobile. He also works on spoof and interference mitigation for navigation. He has published over 100 research papers and articles. He was awarded the ION Early Achievement Award.

ABSTRACT

Recent work has demonstrated that signal-geometry-based approaches are a powerful mean for a GNSS receiver to detect spoofing. These techniques, leveraging the spatial diversity in the received signals, usually rely on all or at least most signals being spoofed for successful detection.
This paper presents several complimentary improvements to these techniques to allow for robust spoof detection even in the presence of light multipath and a mixture of spoofed and genuine satellites. The improved spoof detection can accomplish this while satisfying a constraint on the false alert probability. For this, the paper makes three main contributions: 1) Using the example of a Dual Polarization Antenna (DPA) as a case study, it presents a characterization of measurement quality based on data and physics-derived features. 2) It introduces a hypothesis test iteration algorithm that breaks an m-ary hypothesis test of an unknown number of spoofed satellites from an unknown number of independent signal sources down into a sequence of binary hypothesis tests that identifies the largest subset of satellites triggering an alarm. 3) It derives a likelihood-ratio based decision threshold independent of prior probabilities similar to a Neyman-Pearson test. It is applicable to any spoof defense employing hypotheses tests resulting in conditional probabilities.
The theoretical work is supported by Monte Carlo simulations and tested on data collected by a DPA during a government sponsored live spoofing event. Despite the low quality of azimuth-only spatial measurements, the presence of multipath and the spoofing of only a subset of GPS satellites, more than half of the attacks are detected within a few measurement epochs. No false alarms are raised by a large margin.
Compared to the same data processed without individually characterizing the measurement quality and using binary “all satellites nominal” vs. “all satellites spoofed” hypotheses, a 2-3 - fold improvement in detection is achieved using the derived decision threshold.

INTRODUCTION

With around as many GNSS receivers in the world as people with access to electricity, satellite navigation has become a ubiquitous technology that is constantly relied on [1]. More so, it is being used increasingly to support autonomy in applications such as drones, vessels, railway and autonomous cars. Especially in the absence of human operators in the loop as it is the case in autonomous applications, GNSS receivers will need to be able to provide high integrity in all environments – even in the presence of interference such as spoofing.
The vulnerability of current receivers to spoofing has been demonstrated e.g. in [2] and [3], and GNSS interference is recognized as "serious threats to the continued safety of air transport" [4].

Robust defenses to GNSS spoofing are a field of active research. Many possible detection means have been proposed, however there is no single panacea. The most fruitful strategy will likely rely on a combination of different approaches. This is because any single or even combination of strategies can likely be overcome with enough knowledge, planning, skill and resources. The goal is to make it much too costly or not worthwhile given the effort required for an attacker to attempt to overcome our implemented defense. Essentially, the better our defense, the more expensive it will be to mount a successful attack. [5] gives a comprehensive overview of attack and defense strategies.
Promising results have demonstrated detection during the initial phase of an attack by monitoring automatic gain control (AGC)/input power, carrier to noise ratio (CN0)/signal power and/or the correlation function in [6], [7] and [8]. A major limitation of these techniques is that they work only during the initial capture phase of an event. These so-called "transient detectors" cannot detect an attack once the spoofer has captured the receiver. If he succeeds in dragging the victim off the original correlation function unnoticed, e.g. by jamming the victim's receiver first, the attack will likely continue unnoticed.
It is useful to couple a "steady state detection", whereby detection can occur at any time, not just during the capture phase. One steady state detection approach is to use the spatial diversity present in GNSS signals. Generally at the expense of hardware changes, like using a dithering antenna [9], two antennas [10], an entire array or antennas [11]–[13] or a Dual Polarization Antenna (DPA) [14], metrics reflecting the different Directions Of Arrival (DOA)s of the GNSS signals are derived. Under nominal conditions, these metrics will be different for each satellite, as an antenna receives signals from satellites distributed across the entire sky. Signals transmitted from a spoofer on the other hand will arrive from a single or a few directions, if an expensive attack using multiple transmitting antenna's is mounted. Figure 1 shows a birds-eye view of the concept for four satellites: angles/directions of signals *i* and *j* are different when coming from the authentic satellites but near identical when coming from a single spoofing source.
This underlines the hypothesis inherent to signal-geometry-based approaches: that all or at least multiple satellite signals will be broadcasted from the same source by the attacker. The cited literature demonstrates strong results for situations when all GPS signals are malicious and transmitted from a single antenna and shows an analysis of false alert and missed detection rates for the respective cases.

This paper makes three contributions to spoof detection based on measured DOAs. First, it shows a theoretical derivation of a more general framework to generate detection thresholds that guarantee a chosen false alert probability for hypothesis-test based detection approaches. It shows the dependence of the DOA based method on satellite geometry and measurement accuracy and can be used to examine its limitations. The second contribution is the development of a hypothesis-test framework for spatial processing-based approaches that is functional even with only a subset of satellites spoofed and in the presence of multipath. The paper shows how these considerations are necessary to satisfy the guaranteed false alert probability. The third contribution is a characterization of the DOA measurement uncertainty based on limited data from a DPA, overcoming the "curse of dimensionality" [15].

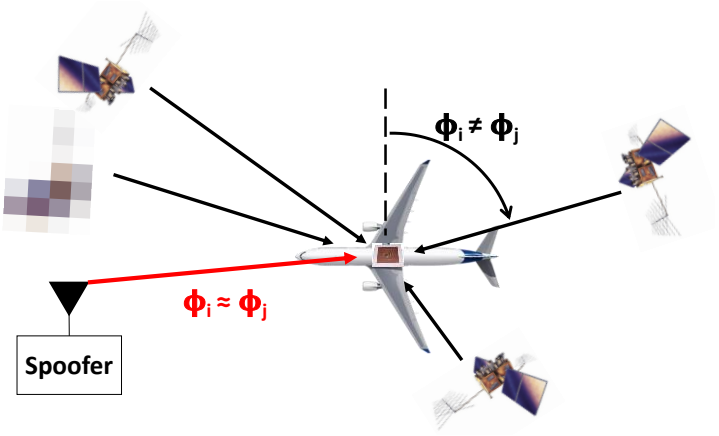

Figure 1: The signal-geometry-based concept from a birds-eye perspective: Genuine signal directions (black) are diverse, while all spoofing signal directions (red) align

Figure 2 shows the three main processing steps of spatial processing-based spoof detection. The improvements made to each are highlighted by red frames with a reference to some of the applicable equations throughout this paper. The remaining paper covers these improvements in four main sections plus a summary and conclusions. Section II describes the DPA, how azimuthal

directions of arrival are detected, and a characterization of the measurement uncertainty in the measurement module. In section III, hypotheses for both nominal and spoofed conditions are formulated. Based on data collected during nominal conditions and during a government sponsored live spoofing event, we present adjustments to the hypotheses module that hold up during realistic conditions for realistic fit probabilities $p(\boldsymbol{y}|H_0)$ and $p(\boldsymbol{y}|H_1)$. In the next section we develop equations for a detection threshold γ_{th} within the executive monitor. The threshold is independent of any assumed prior probability and satisfies a maximum false alert probability constraint based on Bayes Rule and is similar to a Neyman-Pearson likelihood ratio test.
In section V we show the improvement gained through the contributions described in the previous sections when processing data collected during a government sponsored live spoofing event. The last section summarizes the paper's contributions and draws conclusions for future work.

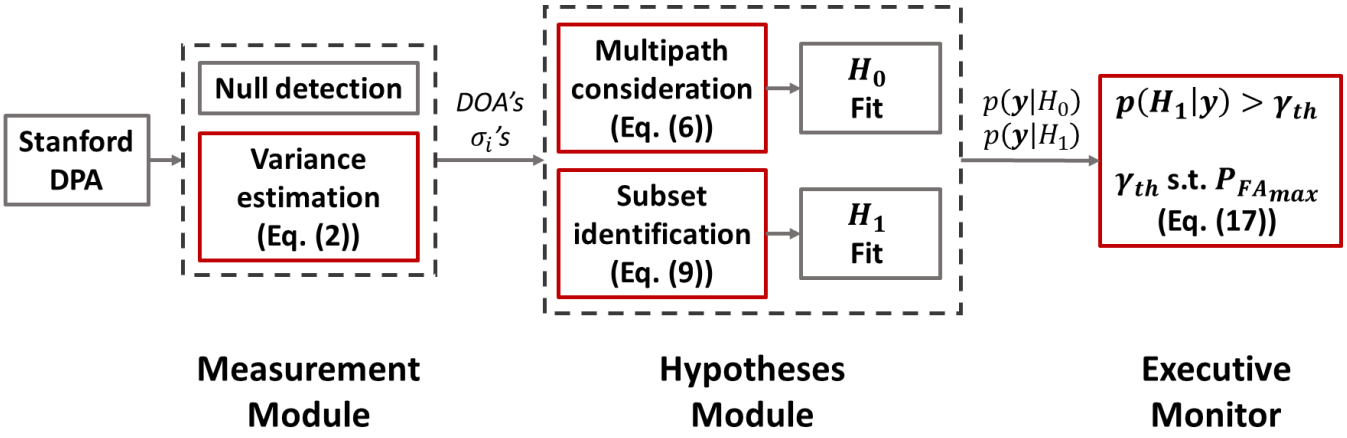

Figure 2: The main processing steps of DOA based spoof detection. Red frames indicate modules created or changed by this paper. Variables above arrows are passed from one module to the next.

II. DPA MEASUREMENTS

1. Background

There are a range of ways to detect the direction of arrival of GNSS satellites with respect to the antenna's attitude, in general at the expense of hardware changes. The methods described in [9]–[13] do so by using a single vibrating antenna or multiple antennas. At least the signal's azimuthal direction of arrival can already be estimated with a single element Dual Polarization Antenna (DPA). A printed circuit board version of a DPA developed at Stanford is shown in Figure 3, along with a histogram of the obtained azimuth estimate errors. It is 3 inch by 3 inch in size. This makes it fit in the ARINC 743 standard prescribing the form factor of aviation GNSS antennas and uses only COTS electronics. A detailed description of its implementation is given in [16], the original concept is developed in [17] and shall be referred to for more detail on the following brief explanation.

The DPA is based on the fact that GNSS signals are broadcasted by the satellites as Right Hand Circular Polarized (RHCP). When RHCP waves hit and then travel along a conducting surface, say the fuselage of an aircraft, the boundary conditions require that the waves propagate with linear polarization. Linear polarization mean they have both Right and Left Hand Circular Polarized (LHCP) components. A GNSS antenna on the aircraft, when exposed to a signal that first impacts the surface around the antenna, is therefore stimulated by both RHCP and LHCP energy with RHCP also coming through direct reception of signals along the line of sight to the satellite.

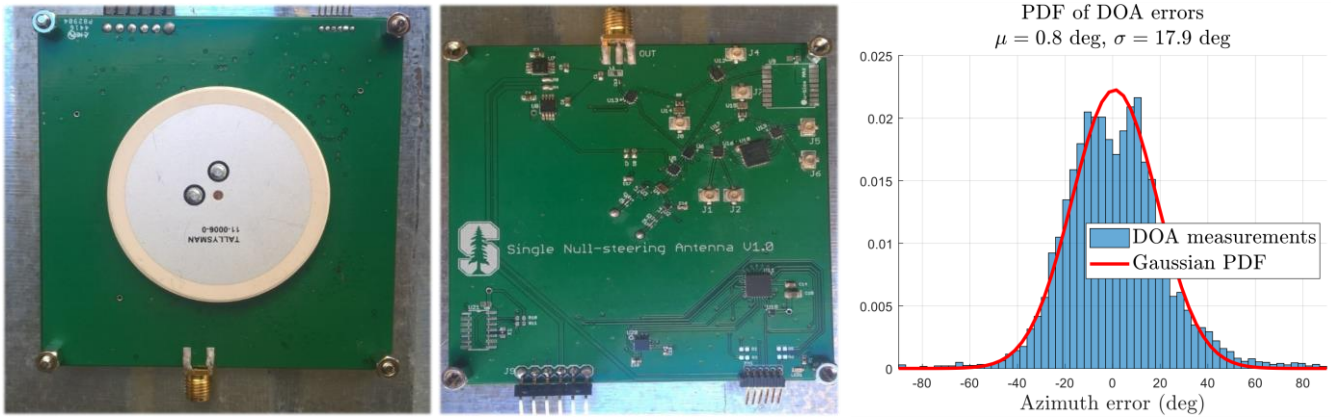

Figure 3: DPA PCB implementation and histogram of azimuth estimate errors

The relationship between the RHCP and LHCP component on the incoming linearly polarized signal depends on the azimuthal Direction Of Arrival (DOA) of the signal relative to the antenna. As the incoming signal rotates its azimuthal DOA relative to the antenna, RHCP and LHCP signals experience opposite phase shifts proportional to the azimuthal direction of arrival as depicted in Figure 4. Combining the signals leads to additive superposition when the phase shifts align (0 deg difference), and destructive superposition for opposite phase shifts (+/-180 deg difference). A Variable Phase Shifter (VPS) is used to continuously shift the phase of the generally stronger RHCP signal. Different VPS shifts cause opposite phase shifts and thereby destructive superposition at different azimuth directions. This destructive superposition causes a drop in carrier-to-noise ratio (CN0) as seen by the receiver, resulting in a periodic null in the CN0 of each satellite, at the moment in time corresponding to the VPS shift related to the signal's azimuthal DOA.

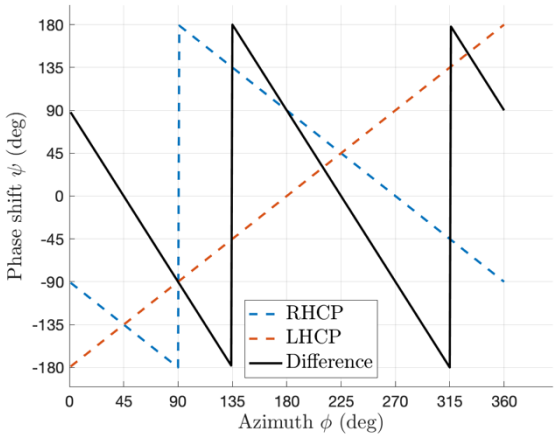

Figure 4: Phase shifts depending on azimuth

Obtaining azimuthal DOA information from this single element antenna comes with a few limitations. Azimuth estimation is based on detecting a drop or null in measured CN0 due to destructive superposition. A deep, well pronounced null is dependent on a sufficiently strong LHCP signal, which is depending on external factors such as the satellite's elevation. As can be seen from the phase shift plot in Figure 4, every determined azimuth value further comes with a 180 degree ambiguity as two azimuth values 180 degree apart correspond to the same difference in phase shift between RHCP and LHCP signals. This effectively doubles the uncertainty already inherent in the measurement errors plotted in Figure 3.

2. Measurement characterization

Despite the mentioned challenges connected with azimuth estimation based on a DPA, the plot in Figure 3 shows an important characteristic: the angle measurement errors seem to be distributed according to a zero-mean Gaussian distribution. Another useful characteristic is that the quality of measurements is dependent on a sufficiently strong LHCP signal causing a deep null, which can then be detected robustly as the minimum of a second order polynomial fit as seen in the left plot of Figure 5. This section examines how this characteristic can be used to derive an expected variance for each measurement. This variance can be used to weigh the azimuth measurements. In other words, for each azimuth measurement, we will now determine an individual variance to replace the general value of $(17.9\ deg)^2\ \sigma^2$ from Figure 3.

The selection of possible features for this inference task is motivated by the physics inherent to each measurement that were just described. A strong LHCP signal leads to a deep, sharp null that can be precisely detected and associated to a phase shift, which translates to an accurate azimuth estimate.
The associated features with each measurement are:

i. null depth in (dB) as the height of a second order polynomial fit to the CN0 values around the null, referred to as "null depth" (see left plot of Figure 5)

ii. null sharpness as defined by the coefficient of the second order term of a second order polynomial fit to the CN0 values, referred to as "null curvature" (see left plot of Figure 5)
iii. null shape as the root mean squared error (RMSE) of the CN0 to a negative Lorentzian function in (dB), referred to as "null fit RMSE" (see right plot of Figure 5)

Figure 5 shows examples of nulls and these features. Measured CN0 is depicted in blue, second order polynomial fits (left plots) and Lorentzian curve fits (right plot) are shown as red lines, red stars indicate the determined null time. We notice a large variation among nulls in shape and size. This underlines that every null and hence azimuth measurement should not be valued equally.

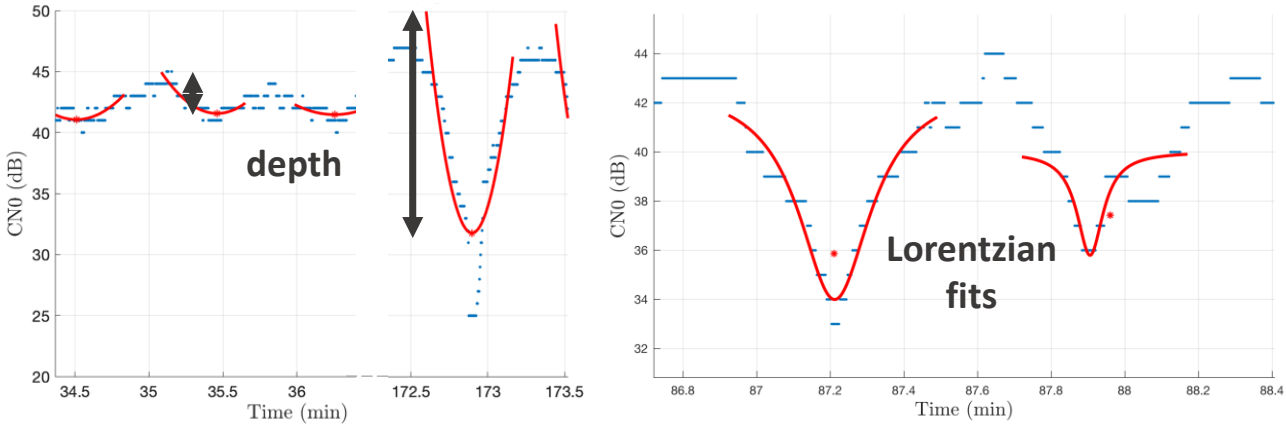

Figure 5: Null features for flat / deep nulls and second order polynomial fits (left), Lorentzian fit to well and poorly fitting nulls (right). Blue indicates measured signal strength; curve fits are drawn in red. Null features are indicated in black.

To assess the utility of each feature for assessing the goodness of its associated azimuth measurement, the data is sorted into bins for small ranges of null depth, curvature and fit RMSE each. We calculate the variance of the measurements in each bin to set up a classic linear regression task of with the data x, feature vector $\phi(x) = [depth(x), curvature(x), fitRMSE(x)]^T$ and labels $y = 1 \,/\, Variance(bin(x))$ [15]. We encounter however an issue known as the "curse of dimensionality" – that is as we go to higher dimensions, our data becomes increasingly sparsely distributed. The total number of bins is the product of the number of bins for each feature. If we split the range of null depth values into e.g. only three bins, say 0 - 5 dB, 5 - 10 dB and 10 – maximum(depth(x)) dB and did the same with curvature and fit RMSE, we would already end up with 27 bins in total. For a reasonable regression analysis, we'd like at least 10 bins per feature, leading to at least 1000 bins in total. The label y for each bin is the inverse of the error variance. This statistical figure should be calculated from a significant number of values, setting a minimum number of datapoints per bin. Since we only have a limited amount of measurement data, it is desirable to reduce the number of features and thereby bins as much as possible.

Data from 6 hours of measurements taken from the top of the Durand building on the Stanford University campus, a four story building whose roof is roughly 15 m from the ground. The location has a fairly unobstructed sky view and is used for an initial analysis of the feature importance. The data contains thousands of nulls for GPS, GLONASS and WAAS satellites. Figure 6 shows bar graphs of the resulting standard deviation σ for bins with at least 50 nulls, with pruned feature vectors limited to $\phi(x) = [depth(x), curvature(x)]^T$ (left plot) and $\phi(x) = [depth(x), fitRMSE(x)]^T$ (right plot). Due to the tight spacing and low values of the fit RMSE values, their inverse is used in the plot for clarity. Both plots show a vast difference in measurement accuracy, with σ's varying between 15 and 50 degree. This underlines the importance of individual measurement weights.
We can observe a clear reduction in σ in the left plot for both an increased depth as well as a higher curvature. Both features carry valuable information when estimating the standard deviation. The plot on the right shows a more surprising result. While we observe again a reduction in σ with increasing null depth, larger values of $1/fitRMSE$ representing better fitting nulls do not indicate any statistically significant improvement in azimuth measurement quality.

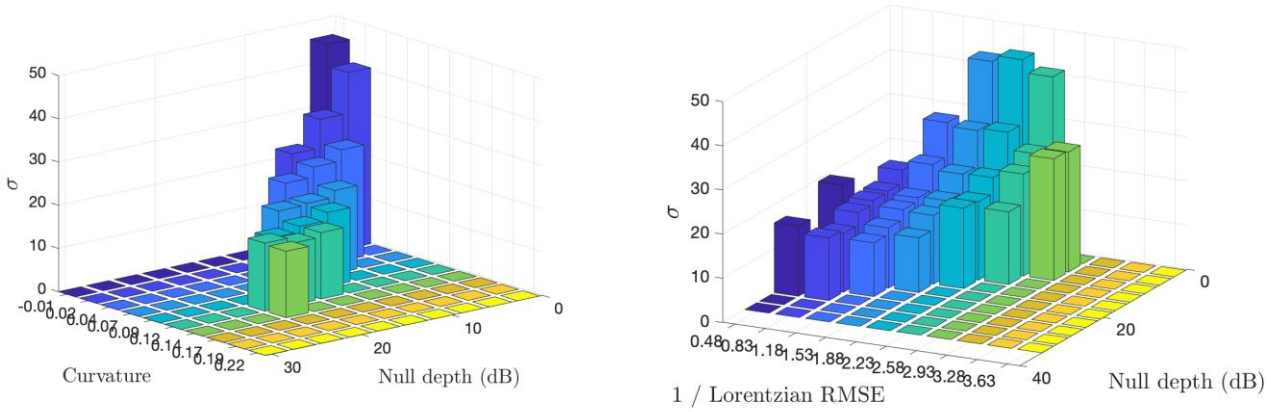

Figure 6: Standard deviation for bins using pruned feature vectors and bins with more than 50 data points; data collected on the roof of Durand building on Stanford campus

Based on this result, the fit RMSE is removed from the feature vector. Including intercept term, we now formulate the regression problem by Equation (1), where x_i represents a null, y_i represents the $1\ /\ Variance(bin(x_i))$ null weight and θ is the feature weight vector. Solving it for the considered data set and rounding conservatively results in the vector $\theta^* = [0.1, 0.5, 55]$. We use this feature weight vector to calculate an individual σ_i for each azimuth measurement using Equation (2).

$$\theta^* = arg\min_{\theta} \sum_{i=1}^{N} ([1, depth(x_i), curvature(x_i)]\,\theta - y_i)^2 \tag{1}$$

$$\frac{1}{\sigma_i^2} = \phi(x)^T\theta^* = [1, depth(x_i), curvature(x_i)]\,\theta^* \tag{2}$$

Measurement errors normalized by σ_i should ideally be distributed as a Standard Normal distribution. Figure 7 shows histograms from multiple measurement campaigns with the values normalized by their respective σ_i, together with Standard Normal probability density functions (pdfs). All three plots show data collected by the same antenna and should therefore have very similar behavior. The left histogram shows the same data collected on the top of Durand building as Figure 3 but normalized by $1/\sigma_i$. The data fits the standard Normal distribution well as expected. The long tails still present in Figure 3 (i.e. large measurement errors that occur with much greater frequency than anticipated by the normal fit) have now disappeared, they were successfully identified as poor measurements with large expected uncertainty. The center histogram shows nominal data collected during a government sponsored field exercise. It looks similar to the rooftop data, but still has a much higher probability or frequency of measurements at the tails (high standard deviation) than anticipated by the modeled Standard Normal distribution. The plot on the right-hand side shows the spread of azimuth values about their mean at each epoch while live spoofing is present, recorded during the same government sponsored event. Despite our efforts to normalize the data with realistic σ_i values, the distribution is far from Gaussian. To explain both the tails of the center histogram as well as the distribution of the live spoofing data on the right, we have to go one step further and reconsider the assumptions made when defining a "nominal" and "spoofing" hypothesis in the next section.

III. HYPOTHESIS FORMULATION

The baseline hypothesis for nominal conditions, from now on referred to as the null hypothesis H_0, is that measurement errors are Gaussian about the direction of the actual satellites (i.e zero mean), conditionally independent given the direction of the actual satellites and uncorrelated in time. Under the spoofed hypothesis H_1, all measurements are assumed to be Gaussian distributed about the direction of the spoofing source. Leveraging the fact that the sum of *k* independent Standard Gaussian variables is distributed according to a χ^2 distribution of k degrees of freedom [18], we can calculate the fit to (or conditional probability of) each hypothesis. In light of the data in Figure 7 we shall now revisit the assumptions of both hypotheses and re-derive the equations leading to the conditional probabilities required for a hypothesis test.

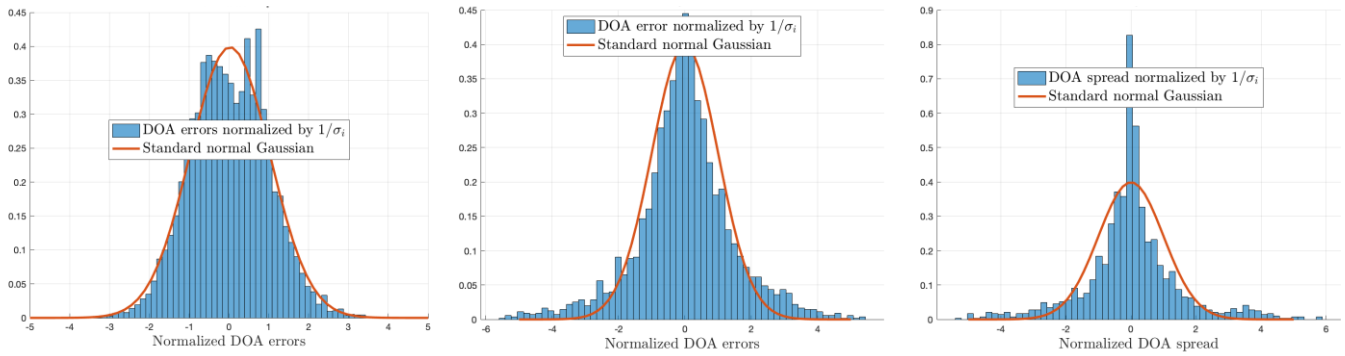

Figure 7: Normalized DOA error (left and center) and spread (right) distribution for measurements collected on a rooftop (left), in the field (center) and during live spoofing (right)

1. Nominal Hypothesis

The nominal hypothesis therefore does not only assume spoofing-free but also multipath-free conditions. These conditions are important for unbiased azimuth measurements, as the azimuth detection based on null detection measures the difference in phase shift between RHCP and LHCP signals shown in Figure 4. It relies on both signals coming from the same azimuthal direction corresponding to the Line Of Sight (LOS) to the signal source. In [19] the authors show how multipath signals are received by a DPA as strong LHCP signals. This throws off the azimuth measurement, as RHCP and LHCP now arrive at the antenna from different directions; their phase difference does not correspond to the LOS anymore.
These conditions match well the clean conditions encountered on a rooftop, where the measurements for the left histogram in Figure 7 were taken. The center diagram on the other hand shows data collected with an antenna mounted on the roof of a car with a roof rack and in an environment similar to a half full parking lot. A scenario where light multipath is present, causing occasional outlier measurements that create the visible tails of the center histogram and violate the multipath-free assumption of the nominal hypothesis.

How do we adjust this hypothesis to take into account at least light multipath present in most GNSS applications? We cannot simply exclude all measurements from consideration that don't match the null hypothesis. The test would lose all its value for spoof detection, as all spoofed signals would simply be excluded from the hypothesis and thereby from the detection algorithm! We can however leverage another integrity algorithm already in place: Receiver Autonomous Integrity Monitoring (RAIM). It detects faults on single GPS satellites, and Advanced RAIM (ARAIM) will do so for multiple constellations. [20] Excluding a single GPS satellite from the hypothesis test can be done safely, as protection against wrong information from a single satellite is provided by RAIM.

We now assess the effect of having an outlier measurement and examine how to determine which, if any, satellite should be excluded. We start by considering the equations underlying the null hypothesis. In the following equations and for the remainder of this paper, vector quantities will be denoted by bold characters for clarity. All angles about the vertical axis are measured with respect to true north unless stated otherwise.
As described thoroughly by [9] and [11], due to the generally unknown antenna attitude, an attitude estimation problem has to be solved prior to any direction of arrival based spoof detection. This is significantly more straightforward in this case than in the cited literature for two reasons. First, this approach works solely with azimuth but no elevation measurements. This reduces the three-dimensional attitude estimation problem to a one-dimensional heading estimation problem. Second, we have Gaussian azimuthal Direction Of Arrival measurements at our disposal, without any integer ambiguities as variables as in the cited carrier-phase difference based approaches. The azimuth measurements $\boldsymbol{y}$ to a set $\boldsymbol{S}$ of $|\boldsymbol{S}|$ satellites are modelled by Equation (3) for the vector of satellite azimuths $\boldsymbol{\phi}$ and the antenna's heading ψ. The solution of the heading estimation problem to be solved is described by Equation (4) and represents the Maximum Likelihood Estimate (MLE) of the heading value ψ^*. It is worth noting that due to the wrapping of angles, Equation (4) is not necessarily convex and can have local minima. But since the domain of ψ is limited to [0 2π], a solution can nevertheless be easily found employing a selection of the optimization techniques described in [21] or Matlab's fmincon function.
The conditional probability of the measurements given the traditional null hypothesis is given by the χ^2 probability density function (pdf) of $|\boldsymbol{S}|$ degrees of freedom evaluated at the cost associated with the solution to Equation (4). We state it in Equation (5).

$$\boldsymbol{y} = \boldsymbol{\phi} - \psi + \boldsymbol{\epsilon} \quad , \quad \epsilon \sim N(0, R) \text{ with } R = \begin{bmatrix} \sigma_1^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_N^2 \end{bmatrix} \tag{3}$$

$$\psi^* = \underset{\psi}{\operatorname{argmin}} \sum_{i=1}^{N} \left(\frac{y_i - \phi_i + \psi}{\sigma_i} \right)^2 \tag{4}$$

$$p(\boldsymbol{y} \mid H_0) = \chi^2_{PDF} \left(\sum_{i=1}^{|\boldsymbol{S}|} \left(\frac{y_i - \phi_i + \psi^*}{\sigma_i} \right)^2, |\boldsymbol{S}| \right) \tag{5}$$

Equations (3) through (5) directly answer the question of the impact of a single outlier measurement. The χ^2 pdf is evaluated at the sum of squared normalized azimuth measurement errors. An outlier with an abnormally large error enters the equation as a squared term, amplifying its impact drastically.
This effect can be illustrated with a simple example for 5 satellites. An example set of absolute errors would be e.g. [0.3, 0.5, 0.7, 1.0, 1.2] times the respective σ_i, leading to a conditional probability of 15.3%. For illustrative purposes let's assume satellite 3 is affected by multipath. This increases the measurement error to e.g. 3 σ_3. The resulting conditional probability is reduced to 1.49%, a single multipath measurement reduced the conditional probability value by more than 90%. We will see in the next sections how this could easily cause a false alert and more importantly make any theoretically guaranteed false alert probability obsolete.

Hence we would like a good outlier exclusion to remove the measurement whose removal leads to the largest likelihood of the data, if a removal improves the conditional probability at all. The revised conditional probability $\hat{p}(y \mid H_0)$ is given by Equation (6). It is the max over the original, unadjusted conditional probability and the probability with the maximum outlier removed. Equation (6) hides the fact that this is in fact a two-step process, where $|\boldsymbol{S}|$ $\psi^*_{(j)}$ need to be calculated by solving Equation (4) while excluding the *jth* satellite.

$$\hat{p}(\boldsymbol{y} \mid H_0) = \max \left(p(\boldsymbol{y} \mid H_0), \quad \max_j \chi^2_{PDF} \left(\sum_{i=1, i \neq j}^{|\boldsymbol{S}|} \left(\frac{y_i - \phi_i + \psi^*_{(j)}}{\sigma_i} \right)^2, |\boldsymbol{S}| - 1 \right) \right) \tag{6}$$

It is possible that this approach excludes satellites that were not necessarily outliers. Going back to the prior example, the exclusion given by Equation (6) would exclude the measurement 5, with 1.2 σ_5 if no multipath were present. This would increase the conditional probability of the remaining normalized measurement errors [0.3, 0.5, 0.7, 1.0] to 18.3%. We do not consider this effect a significant problem for two reasons: one, an increase from 15.3% to 18.3% is far less dramatic than the decrease to 1.49% potentially suffered without this step. Secondly and most importantly, as we will see in chapter IV, spoof detection is phrased as an optimization problem satisfying a false alert probability constraint. It will become clear that an incorrectly elevated conditional probability given the null hypothesis will only support meeting this constraint.

2. Spoofed Hypothesis

A basic spoof (alternate) hypothesis is that all signals are spoofed and from the same direction. The most obvious conclusion from the right plot in Figure 7 is however that not all satellites are coming from the same direction. This could be because the spoofed signals are transmitted from multiple antennas or because a mix of spoofed and genuine signals is detected. Similar to the nominal hypothesis, we will now re-derive the underlying equations and lay out an algorithm to exclude satellites from the spoofed hypothesis.

Just like for the nominal hypothesis, calculating the conditional probability of the measured DOAs given H_1 requires solving a minimization problem first to estimate the azimuthal direction of the origin of the spoofed signals $\bar{\phi}$ (Equation (7)). About this direction the measurements are assumed to be Normally distributed. Like Equation (4), Equation (7) is potentially nonconvex but nevertheless does not pose a challenge to solve.
The conditional probability is given by a χ^2 pdf evaluated at the cost associated with the solution to Equation (7). Setting the number of degrees of freedom for this evaluation makes an assumption about how many independent signals the spoofer transmits for this source. Are e.g. all malicious signals transmitted with the same signal strength and carrier phase, the CN0

values measured by the DPA and ensuing determined azimuths will be far from independent for the different satellites. When receiving spoofed signals for *k* different satellites, anything between 1 and k independent characteristics (in the DPA case signal strength and phase values) will be detected. Modelling this uncertainty, the conditional probability of a set of *k* measurements given the spoofed hypothesis is calculated as the maximum between the χ^2 pdf for k and 1 degree of freedom as given by Equation (8). The variable *k* is used deliberately instead of $|\boldsymbol{S}|$ to emphasize that potentially only a subset of satellites is spoofed, constraining $k \leq |\boldsymbol{S}|$.

$$\bar{\phi}^* = \underset{\bar{\phi}}{\operatorname{argmin}} \sum_{i=1}^{k} \left(\frac{y_i - \bar{\phi}}{\sigma_i}\right)^2 \tag{7}$$

$$p(\boldsymbol{y} \mid H_1)_k = \max\left(\chi^2_{PDF}\left(\sum_{i=1}^{k}\left(\frac{y_i - \bar{\phi}^*}{\sigma_i}\right)^2, k\right), \chi^2_{PDF}\left(\sum_{i=1}^{k}\left(\frac{y_i - \bar{\phi}^*}{\sigma_i}\right)^2, 1\right)\right) \tag{8}$$

As stated in the beginning of this section, we expect the possibility of only a subset of satellites being spoofed. We therefore need to be able to remove satellites from the consideration. Similar to the outlier rejection under H_0, we do so by excluding the satellite whose removal leads to the maximum likelihood as done in Equation (9). While Equation (9) covers only the removal of a single satellite, this step can be performed recursively until a minimum number of satellites.

$$p(\boldsymbol{y} \mid H_1)_{k-1} = \max\left(\max_j \chi^2_{PDF}\left(\sum_{i=1, i\neq j}^{k}\left(\frac{y_i - \bar{\phi}^*_{(j)}}{\sigma_i}\right)^2, k-1\right), \max_j \chi^2_{PDF}\left(\sum_{i=1, i\neq j}^{k}\left(\frac{y_i - \bar{\phi}^*_{(j)}}{\sigma_i}\right)^2, 1\right)\right) \tag{9}$$

3. The hypothesis test loop

In the previous two subsections we derived equations for the conditional probabilities of a set of measurements under either hypothesis. In the nominal case we accounted for the possibility of multipath on a satellite causing biased outlier measurements. In the spoofed case, we account for the possibility that an unknown number of spoofed signals are transmitted from an unknown number of independent sources resulting in independent signal characteristics. We defined a procedure for removing a satellite from the computation for both cases. Figure 8 shows skyplots of four example cases, with the ephemeris-based location of each GPS satellite in red, and the location with null detection-based azimuth in blue. On the top left we see the ideal nominal case, all satellites are close to the location in the ephemeris. On the top right the ideal spoofed case, all satellites are detected to come from the same azimuth direction. On the bottom right the case of a spoofed subset, only the circled satellites G5, G8, G9, G13 and G23 are detected to come from a similar direction. On the bottom left the multipath case; all satellites are detected approximately at their respective correct locations, except for the circled satellite G22 which is almost 90 degrees off.

Following the greedy approach outlined in the previous sections, we define a hypothesis test loop that scans the measurements $\boldsymbol{y}$ for the presence of spoofing. It efficiently finds the largest subset of satellites that raises an alarm, as long as that subset contains more satellites than the minimum number of satellites required for the hypothesis tests. This minimum is to be set by the designer. It is dependent on the quality of the spatial measurements and on how few signals are expected to come from one direction. More precise angular measurements generally allow for a lower minimum number. A lower minimum allows the algorithm to detect spoofing with fewer satellites broadcasted from the same transmitter. A value between 2 and 5 is realistic. Following this algorithm allows us to break the M-ary hypothesis down into a sequence of binary hypothesis tests.
If a spoofing alarm is raised for a subset of satellites, the algorithm can be run again on the remaining set to identify possible additional spoofing sources.

Start with set $\boldsymbol{S}$ of all satellites in view
Calculate $\hat{p}(\boldsymbol{y} \mid H_0)$, $p(\boldsymbol{y} \mid H_1)_{|\boldsymbol{S}|}$
While $|\boldsymbol{S}| \geq$ *minimum number of satellites*
    If raise_alarm($\hat{p}(\boldsymbol{y} \mid H_0), p(\boldsymbol{y} \mid H_1)_{|\boldsymbol{S}|}$) *break; else* *# stop if current set $\boldsymbol{S}$ is considered spoofed*
    Remove jth satellite from $\boldsymbol{S}$ to calculate $p(\boldsymbol{y} \mid H_1)_{|\boldsymbol{S}|-1}$ *# this reduces $|\boldsymbol{S}|$ by 1*

A single feature is missing to perform this loop at each measurement epoch: the raise_alarm() function. In the next section we will answer this fundamental question of when to alert, discussing the tradeoff between missed detections and false alerts.

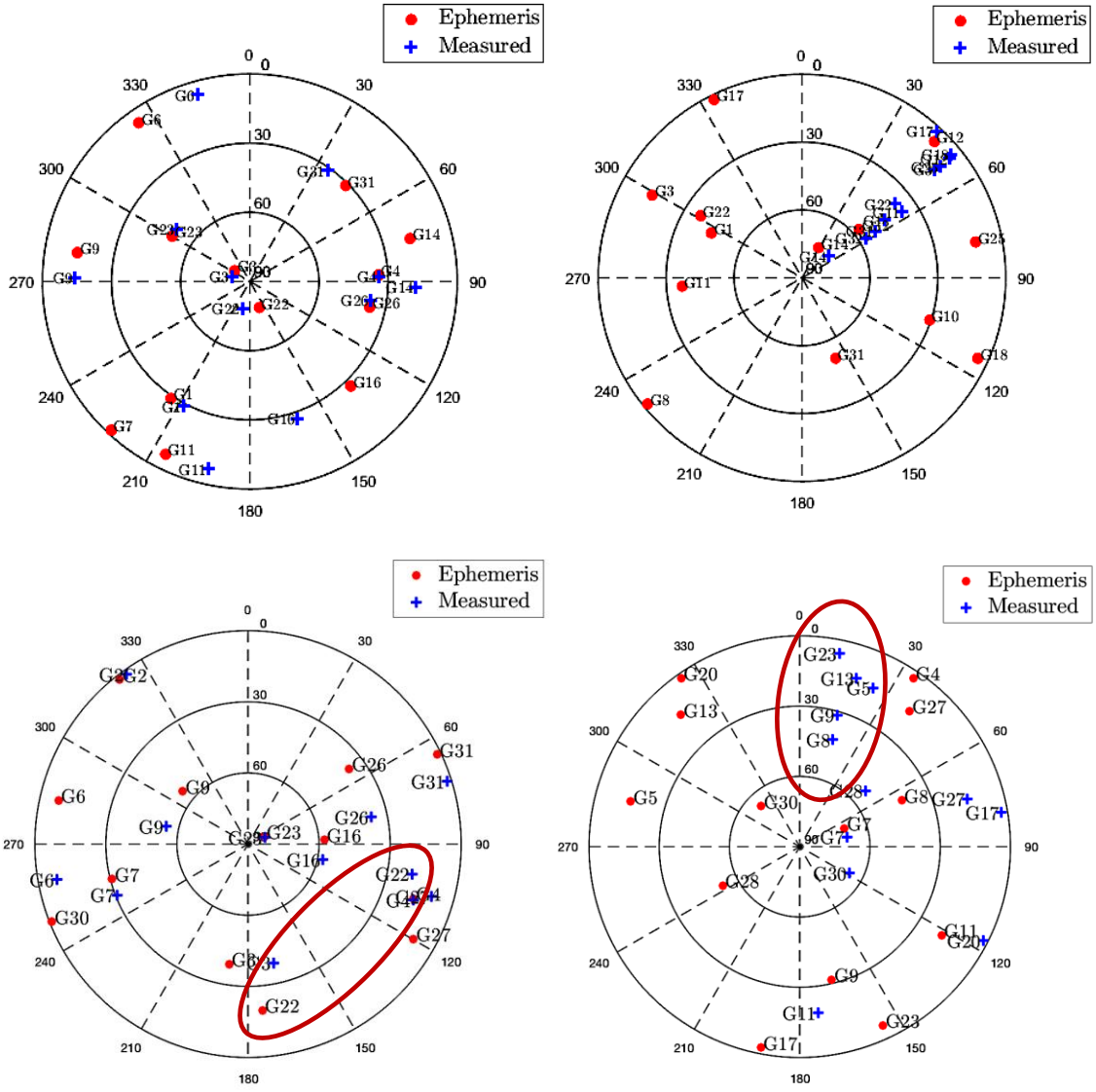

Figure 8: Skyplots with examples of four different scenarios. Ideal nominal (top left), ideal spoofed (top right), subset spoofing (bottom right), multipath (bottom left)

IV. A CONSTRAINT ON FALSE ALERTS

In the prior two sections, we derived individual standard deviations based on measurement features for every measurement for an accurate normalization in the χ^2 statistic. We took care to construct hypotheses with real world conditions in mind, allocating for light multipath, subset spoofing and different transmission characteristics of the spoofer. These efforts could be summarized under one goal: to derive the most realistic conditional probabilities of the measurements given either hypothesis. In this section we take the last step of deriving a detection threshold given these conditional probabilities.

Given that spoofing is a rare event, any spoofing defense implemented in a receiver should first and foremost not do noticeable harm in terms of causing false alarms. False alarms reduce availability and continuity and if the rate is high enough, the user

may experience this far more than a true alarm. Also, manufacturers are unlikely to want to add spoof detection if the end user perceives it as providing negative value by causing noticeable disruption of service.

The problem of setting an alert threshold given some decision metrics is therefore generally defined by the optimization problem in Equation (10).

$$\begin{aligned} &maximize && alerts \\ &\text{s.t.} && p(false\ alert) \leq P_{FA_{max}} \end{aligned} \tag{10}$$

The constraint can be rephrased as the probability of the joint events "alert" and "nominal conditions", which is rewritten as the conditional probability of an alert given the null hypothesis and the probability of the null hypothesis in Equation (11).

$$p(false\ alert) = p(alert, H_0) = p(alert \mid H_0)\, p(H_0) \leq P_{FA_{max}} \tag{11}$$

For most applications it is reasonable to assume $p(H_0)$ close to 1, in any case $0 < p(H_0) < 1$ holds. The original constraint is therefore still satisfied if $p(H_0)$ is dropped from the equation as we show in Eq. (12). An alert will further be raised if the posterior probability of H_1 given the measurements $\boldsymbol{y}$ is above some threshold, namely the alert threshold γ_{th} we intend to determine. We take these two aspects into account by rewriting the constraint from Equation (10) in the form of Equation (13). $p(H_1 \mid \boldsymbol{y})$ here denotes the posterior probability of H_1 given the measurement. The overall conditioning on H_0 reminds us that the measurements $\boldsymbol{y}$ are distributed according to the null hypothesis, Normally about the satellite's azimuth directions as in Eq. (3).

$$p(alert \mid H_0)\, p(H_0) \leq p(alert \mid H_0) \leq P_{FA_{max}} \tag{12}$$

$$p(\, p(H_1 \mid \boldsymbol{y}) > \gamma_{th} \mid \boldsymbol{y} \sim H_0) \leq P_{FA_{max}} \tag{13}$$

The left hand side of Equation (13) could be rephrased as follows: the probability that the probability of H_1 given the measurements is above γ_{th}, in a situation where the measurements are distributed according to the null hypothesis. It is equal to the probability of raising an alert, even though the measurements are distributed according to H_0.
Applying Bayes Rule leads to:

$$p\left(\frac{p(\boldsymbol{y} \mid H_1)p(H_1)_{prior}}{p(\boldsymbol{y} \mid H_0)p(H_0)_{prior} + p(\boldsymbol{y} \mid H_1)p(H_1)_{prior}} > \gamma_{th} \mid \boldsymbol{y} \sim H_0\right) \leq P_{FA_{max}} \tag{14}$$

$$p\left(\frac{1}{\frac{p(\boldsymbol{y} \mid H_0)p(H_0)_{prior}}{p(\boldsymbol{y} \mid H_1)p(H_1)_{prior}} + 1} > \gamma_{th} \mid \boldsymbol{y} \sim H_0\right) \leq P_{FA_{max}} \tag{15}$$

Collecting random variables on one the left hand side of the inequality and constants on the right:

$$p\left(\frac{p(\boldsymbol{y} \mid H_0)}{p(\boldsymbol{y} \mid H_1)} < \left(\frac{1}{\gamma_{th}} - 1\right)\frac{p(H_1)_{prior}}{p(H_0)_{prior}} \mid \boldsymbol{y} \sim H_0\right) \leq P_{FA_{max}} \tag{16}$$

The optimal test in the sense of the Neyman-Pearson lemma consists of the ratio of the probability densities of the measurement data given the two hypotheses [22]. Since $p(\boldsymbol{y}|H_0)$ and $p(\boldsymbol{y}|H_1)$ were computed using MLE values for ψ and $\bar{\phi}$ (by solving Equations (4)and (7), respectively) instead of integrating over the entire distribution, this test is more practical but slightly less powerful than the optimal Neyman-Pearson test.
Equation (16) conveys an important message. Finding the optimal detection threshold depends on the ratio of conditional probabilities given either hypothesis, as well as the prior probabilities for either hypothesis. This is emphasized by rewriting the optimization problem from Equation (10) in the following form:

$$\begin{aligned} &minimize && \gamma_{th} \\ &\text{s.t.} && p\left(\frac{p(\boldsymbol{y} \mid H_0)}{p(\boldsymbol{y} \mid H_1)} < \tilde{\gamma} \mid \mathbf{y} = \boldsymbol{\phi} - \psi + \boldsymbol{\epsilon}\right) \leq P_{FA_{max}} \\ & && \gamma_{th} = \frac{1}{\tilde{\gamma}\,\frac{p(H_0)_{prior}}{p(H_1)_{prior}} + 1} \end{aligned} \tag{17}$$

We denote the likelihood ratio by $\Lambda(\boldsymbol{y})$ as in Eq. (18). The optimal detection threshold to maximize alerts while meeting a false alert probability constraint can thus be broken down into a likelihood ratio test $p(\Lambda(\boldsymbol{y}) < \tilde{\gamma} \mid H_0) \leq P_{FA_{max}}$. $\tilde{\gamma}$ is found by solving Equation (19).

$$\Lambda(\boldsymbol{y}) = \frac{p(\boldsymbol{y} \mid H_0)}{p(\boldsymbol{y} \mid H_1)} \tag{18}$$

$$\int_{-\infty}^{\tilde{\gamma}} \mathrm{p}(\Lambda(\boldsymbol{y}) \mid \boldsymbol{y} \sim H_0)\, d\Lambda(\boldsymbol{y}) = P_{FA_{max}} \tag{19}$$

The only real analysis to be done for a detection threshold is finding the cumulative distribution function (cdf) of $\Lambda(\boldsymbol{y})$ and solving Equation (19) for $\tilde{\gamma}$. γ_{th} is then a mapping using the *known* prior probabilities selected by the designer as shown in Eq. (17). Satisfying the false alert probability constraint is only a question of the distributions of conditional probabilities, but independent of arbitrarily chosen prior probabilities.

Deriving an analytical solution to the cdf of $p(\boldsymbol{y} \mid H_0)$ / $p(\boldsymbol{y} \mid H_1)$ in Equation (19) can be very difficult or even impossible. For any signal-geometry-based approach as the one discussed in this paper it will depend solely on the available satellite geometry (in this case represented by $\boldsymbol{\phi}$) and the measurement quality expressed through $\boldsymbol{\epsilon}$. The so-called sufficient statistic is a function of these two variables. It is a function of the data which has the property that $\Lambda(\boldsymbol{y})$ can be written in terms of it. The interested reader is referred to chapter 2.2 in [22] for more details on the topic. Should an analytical expression for the cdf not be available, a series of Monte Carlo (MC) analyses can be run offline to populate a table of thresholds $\tilde{\gamma}$ as a function of the sufficient statistic.
To accommodate constraints in memory or processing on the receiver, a lower bound on $\tilde{\gamma}$ (and γ_{th} respectively) can be used. Such a bound could be precomputed off a MC simulation of a poor geometry. This geometry would then constitute the worst applicable geometry the detector can be used on.

To illustrate this result better, we show an example of a cdf and pdf of $\Lambda(\boldsymbol{y})$ based on $1e7$ MC runs in Figure 9, for both nominal (black) and spoofed (blue) conditions. All values are based off a constellation of 5 satellites, distributed at azimuth angles of [36;110;52;73;166] degree and measurement σ_i's of [25;20;17;22;29] degree. The spoofing source for the blue distributions is located in between the actual satellites at 57 degree azimuth. The auxiliary threshold $\tilde{\gamma}$ is set to satisfy a maximum false alert probability of $P_{FA_{max}} = 1e\text{-}5$ which is equal to the black cdf at this point. For ease of plotting, the natural log of the ratio of conditional probabilities is used. The plot marks the log of the maximum $\tilde{\gamma}$ satisfying the false alert probability as -6.367. In other words, $p(\boldsymbol{y} \mid H_1)$ needs to be $1 \,/\, \exp(-6.367) = 582.3$ times higher than $p(\boldsymbol{y} \mid H_0)$ to raise an alert. The receiver's capability to detect an attack that follows the definition of H_1 is given by the portion of the H_1-based distribution to the left of the determined alert threshold $\tilde{\gamma}$. From the blue cdf plot we can easily read off that approximately 40% of measurements would flag an attack in this scenario.
Larger spacing between satellites, more satellites in view and a higher measurement accuracy would separate the two distributions further, leading to a higher detection rate.

A detection probability of 40% does not sound impressive at first glance. Two aspects need to be kept in mind: this detection percentage is highly dependent on the measurement accuracy and spatial diversity of the true signals. With multiple antennas using a short baseline of 0.1 m the direction of arrival can be estimated with an accuracy of 3 deg, drastically changing the odds of detection [5]. Rerunning the above MC with this accuracy results in a vast gap between the two distributions. We detect every attack without a single false alert with a large margin.
The second aspect is that we get multiple chances of detection. To overcome simple sanity checks a receiver can run on the position solution, a spoofing attack requires some time to lure the victim off course to not cause e.g. unreasonable accelerations.

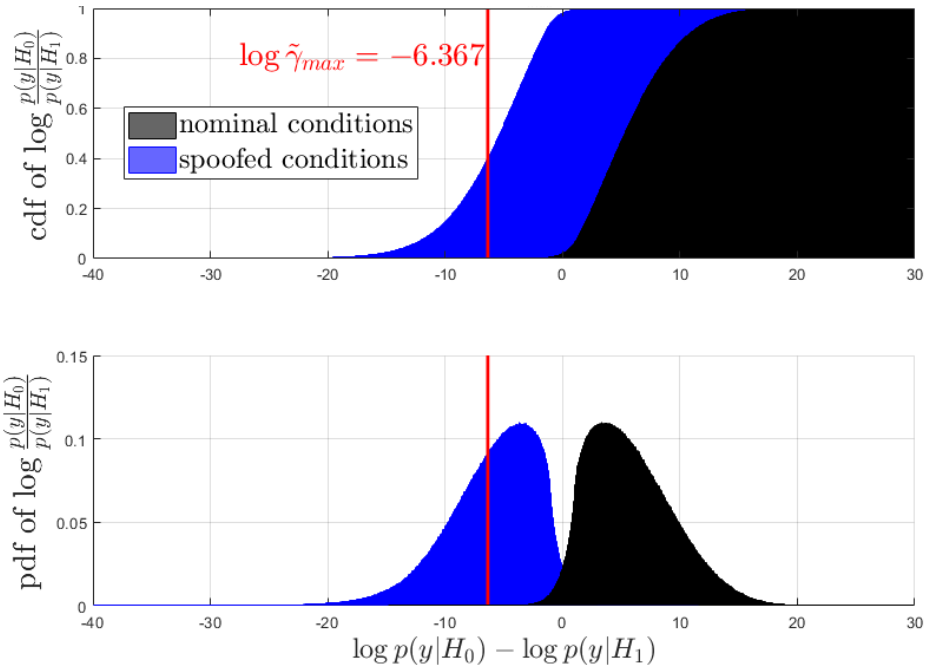

Figure 9: cdf and pdf of the log likelihood ratio for satellites at [36;110;52;73;166] (deg) azimuth and measurement σ_i's of [25;20;17;22;29] (deg). In black the distribution of measurements under nominal conditions, in blue when receiving signals from a spoofer at 57 degree azimuth. The log of $\tilde{\gamma}_{max}$ allowed to satisfy $P_{FA_{max}} = 1e\text{-}5$ is marked in red.

This gives the receiver multiple measurement epochs to detect an attack before any actual harm is done. Since these measurements are independent, a single-measurement detection rate of 40% increases in success the more measurements are collected, e.g. to $1 - 0.6\text{^}5 = 92.2\%$ probability of at least one alert after 5 measurement epochs. The longer the attack lasts, the higher its probability of getting detected. This is one of the great strengths of steady-state detection techniques.

Continuing the example of Figure 9, a detection threshold γ_{th} can be calculated based on $\tilde{\gamma}$ and depending on the chosen priors. Table 1 shows the respective γ_{th} values for a range of prior probabilities of spoofing $p(H_1)_{prior}$ (where of course $p(H_0)_{prior} = 1 - p(H_1)_{prior}$). We keep in mind that the calculated values of γ_{th} are the threshold of $p(H_1|\boldsymbol{y})$ above which an alert is raised. Table 1 can then be interpreted as follows: the more a spoofing attack is expected (higher $p(H_1)_{prior}$), the more convinced the receiver has to be of spoofing after processing the measurement to not risk a false alert. Or on a more intuitive level: the more suspicious we go into the situation (higher $p(H_1)_{prior}$), the more careful we have to be not to alarm incorrectly (higher γ_{th}).

Table 1: Alert thresholds for different prior probabilities with $\tilde{\gamma}$ from the example shown in Figure 9

$p(H_1)_{prior}$	γ_{th}
0.01%	5.5%
0.1%	36.8%
1%	85.5%
10%	98.5%

V. RESULTING DETECTION PERFORMANCE

We tested the theoretical derivations of the past three sections on GPS and GLONASS data collected during a live spoofing event sponsored by the US government. Data was recorded during a total of 39 episodes of spoofing, always from a single source transmitter. Each episode was fairly short compared to the measurement frequency, resulting in 1-7 measurement epochs per spoofed episode. During most spoofed epochs we received not exclusively spoofed but a mix of genuine and spoofed

signals. Each constellation was processed separately, for a total of 442 measurement epochs of which 129 were spoofed during the 39 episodes of consecutive spoofing.

An alarm was declared if the log-likelihood difference $\Lambda(\boldsymbol{y}) = \log p(\boldsymbol{y} \mid H_0) - \log p(\boldsymbol{y} \mid H_1) < \tilde{\gamma} = -6.4$ following the results from section IV. We show the results for three different processing methods. Figure 10 shows a graphical depiction of the modules and steps employed in each method. Table 2 shows the numerical results for the three methods. In Figure 11 we show histograms of the resulting $\log p(\boldsymbol{y} \mid H_0) - \log p(\boldsymbol{y} \mid H_1)$ values for all three approaches, separated into nominal epochs (blue bars) and spoofed epochs (red bars).

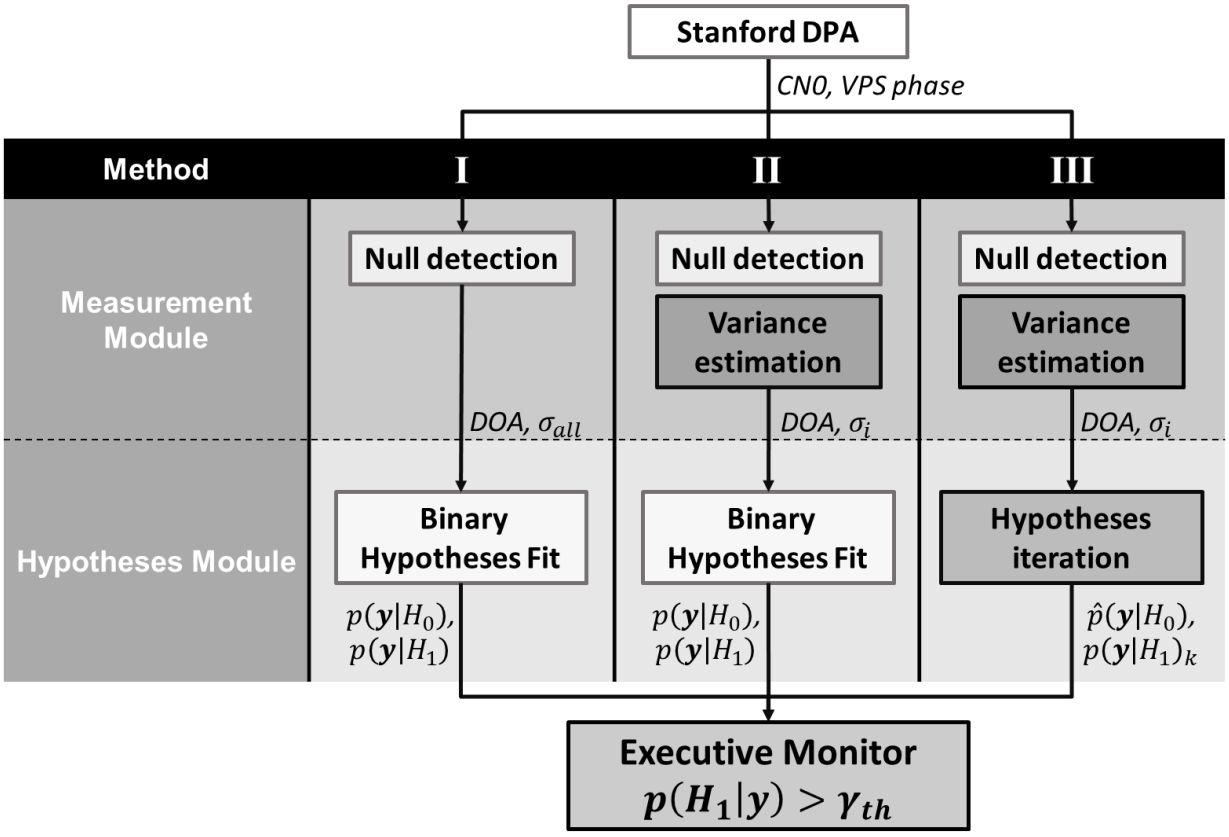

Figure 10: Schematic of the building blocks we use in each of the three processing methods. Method I serves as baseline, Method II adds variance estimation, Method III additionally takes advantage of the presented hypotheses iteration loop. Processing steps presented in this paper are highlighted in dark.

The first method in column 1, the baseline, ignores sections II and III of this paper or any updates introduced to the measurement or hypotheses modules. It uses a general measurement of $\sigma = 25deg$ and tests binary "all nominal" vs. "all spoofed" hypotheses. The second method in the middle column leverages the individual σ_i's computed according to the weights derived in section II, but still uses the binary hypothesis formulation. It employs the updates introduced to the measurement module. The third method in the last column takes full advantage of sections II and III, considering subset spoofing of down to 5 satellites. It uses all features presented in this paper and originally shown in Figure 2.

The first method alarms at least once during every fourth spoofing episode and detects only 17 out of the 129 spoofed epochs overall. No false alert is generated, and the lowest log-likelihood difference value during nominal conditions is -2.47, significantly above the alarm threshold of -6.4. In the left histogram of Figure 11 actually spoofed and actually nominal epochs are not very well separated.
The second method shows an increase in correct detections, alarming correctly during 17 of the 39 episodes. It also raises one false alarm with a lowest log-likelihood difference during nominal conditions of -7.25. Using individual σ_i's has made the algorithm significantly more aggressive. In the middle histogram of Figure 11 we can see more extreme values appear both on

the positive and negative side, between -20 and 100 (where before values were between -10 and 50). The false alert guarantee computed in section IV is clearly violated, as the assumptions underlying the "all nominal" and "all spoofed" hypotheses are not matched by the data.
The third method shows another improvement in detections, alarming correctly during 23 out of 39 episodes without raising a false alarm. The lowest log-likelihood difference during nominal conditions has increased back up to -3.85. On the right histogram of Figure 11 the truly nominal and truly spoofed cases now seem much better separated with less extreme values. Introducing the more realistic hypotheses has led to a better identification of both nominal and spoofed cases.

Table 2: Result summary using three different processing approaches on the data collected during the live spoofing event. 129 epochs were spoofed during 39 episodes of consecutive spoofing

	Method 1 **One σ, binary hypotheses**	**Method 2** **σ_i's, binary hypotheses**	**Method 3** **σ_i's, variable hypotheses**
Detections	10 episodes / 17 epochs	17 episodes /27 epochs	23 episodes / 47 epochs
Min $log \frac{p(y_t \mid H_0)}{p(y_t \mid H_1)}$ while nominal	-2.47	-7.25	-3.85
False Alerts	0	1	0

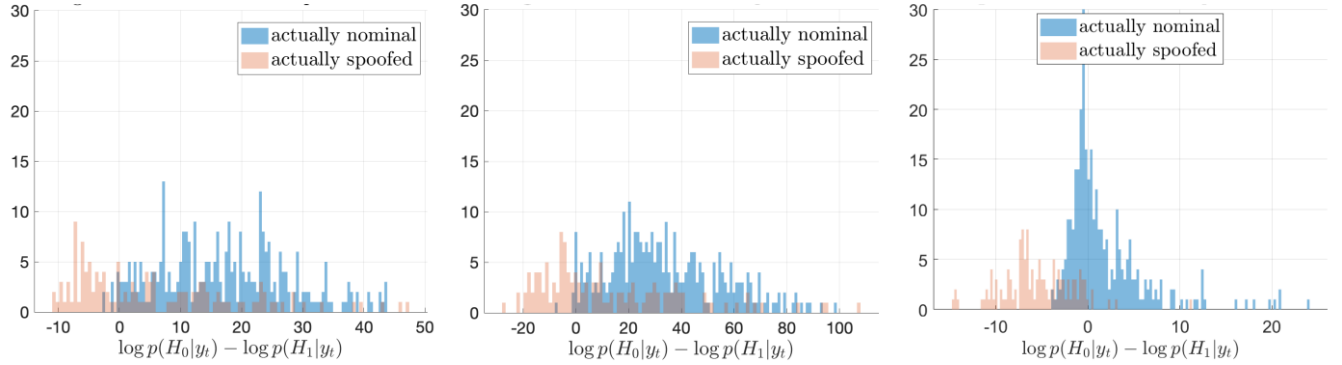

Figure 11: Log-likelihood differences for three processing approaches on the data collected during the live spoofing event. From left to right: method 1, method 2, method 3

A significant number of attacks remained undetected even when using method 3. These were either very short episodes during which only one or two measurements were collected, or episodes where only a small number of closely aligned satellites were spoofed, creating a challenging detection scenario. But as outlined in the previous section, a missed detection generally means the attacker got lucky. All attacks would have been detected eventually, if they had continued.

VI. SUMMARY AND CONCLUSIONS

This paper has critically analyzed three main steps of spatial processing-based spoof detection under real world conditions. It presented a characterization of measurement quality based on limited data and physics-derived features from a dual polarization antenna. It introduced a hypothesis test iteration algorithm that breaks an m-ary hypothesis test of an unknown number of spoofed satellites down into a sequence of binary hypothesis tests that identifies the largest subset of satellites causing an alarm. And it derived an alarm threshold framework useable by any hypothesis-based approach. It is independent of prior probabilities and satisfies a false alert probability constraint analogous to a Neyman-Pearson test.
The theoretical work is supported by Monte Carlo simulations and finally tested on data collected during a government sponsored live spoofing event. Despite the low quality of angular measurements, the presence of multipath and the spoofing of only a subset of GPS satellites, more than half of the attacks are detected within a few measurement epochs. No false alarms are detected by a large margin.
Future work includes examining the algorithm's performance under more severe multipath conditions, to determine at what point the considerations around the "nominal" hypothesis from chapter III.1 are insufficient. More work needs to be done for a derivation of an analytical expression of the log-likelihood used in the derivation of the decision threshold in chapter IV. It

should then be leveraged to precisely outline the capabilities and limitations of signal-geometry-based detection approaches as a function of satellite geometry and measurement accuracy. Most missed detections of the most sophisticated method (method three) in the data analyzed in section V were either short episodes with only very few spoofed measurement epochs or spoofing of a subset of satellites that were closely spaced in the sky. This emphasizes a limitation of signal-geometry-based approaches that should be studied further using the results of section IV. Given the conditional independence between measurement epochs however, all of these attacks would have been detected if they had persisted for longer. The log-likelihood based threshold further seems promising for a sequential processing approach. The conditionally independent measurements at consecutive epochs could be modelled as a Hidden Markov Model to be processed in a Histogram Filter for another leap in performance.

ACKNOWLEDGMENTS

The authors thank the Federal Aviation Administration (FAA) and the Stanford Center for Position Navigation and Time (SCPNT) for sponsoring this research. The authors also thank the US government for providing us with an opportunity to test under live GPS spoofing. The authors thank Prof. J. David Powell for his invaluable advice and guidance during this research.

REFERENCES

[1] European Global Navigation Satellite Systems Agency, *GNSS Market Report 2017*, no. 5. 2017.

[2] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O. Hanlon, and P. M. Kintner, "Assessing the Spoofing Threat : Development of a Portable GPS Civilian Spoofer," *Proc. 21st Int. Tech. Meet. Satell. Div. Inst. Navig. (ION GNSS 2008) Sept. 16 - 19, 2008 Savannah Int. Conv. Cent. Savannah, GA*, pp. 2314–2325, 2009.

[3] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection," *NAVIGATION*, vol. 64, no. 1, pp. 51–66, 2016.

[4] RASG-MID, "RASG-MID SAFETY ADVISORY – 14 April 2019 GUIDANCE MATERIAL RELATED TO GNSS VULNERATBILITIES," 2019.

[5] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[6] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS-Signal authentication," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 1, pp. 469–475, 2019.

[7] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter, and P. Enge, "Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers," in *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, 2018, pp. 672–689.

[8] A. Pirsiavash, A. Broumandan, and G. Lachapelle, "Two-Dimensional Signal Quality Monitoring For Spoofing Detection," in *Navitec 2016*, 2016, no. 14-16 December, pp. 14–16.

[9] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data," *26th Int. Tech. Meet. Satell. Div. Inst. Navig.*, pp. 2949–2991, 2013.

[10] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, T. E. Humphreys, and A. Schofield, "GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase," *Proc. 27th Int. Tech. Meet. Satell. Div. Inst. Navig.*, pp. 2776–2800, 2014.

[11] M. Appel, A. Konovaltsev, and M. Meurer, "Robust Spoofing Detection and Mitigation based on Direction of Arrival Estimation," *Proc. ION GNSS+ 2015*, pp. 3335–3344, 2015.

[12] M. Appel *et al.*, "Experimental validation of GNSS repeater detection based on antenna arrays for maritime applications," *CEAS Sp. J.*, vol. 11, no. 1, pp. 7–19, 2019.

[13] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *J. Appl. Res. Technol.*, vol. 13, no. 1, pp. 45–57, 2015.

[14] S. Lo, Y.-H. Chen, H. Jain, and P. Enge, "Robust GNSS Spoof Detection using Direction of Arrival: Methods and Practice," *Proc. 31st Int. Tech. Meet. Satell. Div. Inst. Navig. (ION GNSS+ 2018)*, pp. 2891–2906, 2018.

[15] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, 2nd ed. New York: Springer-Verlag, 2017.

[16] Y. Chen, F. Rothmaier, D. M. Akos, S. Lo, and P. Enge, "PCB Implementation of a Single Null-steering Antenna and its Anti-spoofing / jamming Testing," *Proc. 2017 Int. Tech. Meet. Inst. Navig.*, 2017.

[17] E. McMilin, "Single Antenna Null-Steering for Gps & Gnss Aerial Applications," Stanford University, 2016.

[18] W. Mendenhall and T. Sincich, *Statistics for Engineering and the Sciences*, 4th ed. Englewood Cliffs, New Jersey:

Prentice Hall, 1995.
[19] D. Egea-Roca *et al.*, “GNSS Measurement Exclusion and Weighting with a Dual Polarized Antenna: The FANTASTIC project,” in *ICL-GNSS 2018 - 2018 8th International Conference on Localization and GNSS: Seamless Indoor-Outdoor Localization, Proceedings*, 2018, no. June.
[20] J. Blanch *et al.*, “Baseline advanced RAIM user algorithm and possible improvements,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 51, no. 1, pp. 713–732, 2015.
[21] M. J. Kochenderfer and T. A. Wheeler, *Algorithms for Optimization*, 1st ed. Cambridge, Massachusetts: The MIT Press, 2018.
[22] H. L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I*. 2001.