Evaluation of Theory- and Data-driven Methods for GPS Spoofing Detection

Mira Partha, *Stanford University*
Marta Cortinovis, *Stanford University*

ABSTRACT

The ability to detect GPS spoofing is a critical requirement for safe, reliable GPS usage. However, the task of spoofing detection is a non-trivial one. With many different attack strategies possible, the manifestation of spoofing attacks in observed GPS signals varies widely. As adversaries develop more and more sophisticated spoofing techniques, it becomes increasingly important to develop better detection methods. There are two major classes of methods to consider: theory-driven methods, which utilize domain knowledge and known principles regarding GPS systems; and data-driven methods, which purely consider signal values agnostic to their physical significance.

In this work, we explore a representative detection method for each class. For theory-driven methods, we examine signal power monitoring, wherein we leverage variation in the received signal power to identify interference in the noisy GPS L1 C/A signal. For data-driven methods, we investigate the use of Support Vector Machines looking at carrier-to-noise values and receiver clock error rate. Each method is developed and evaluated using the Texas Spoofing Test Battery (TEXBAT) dataset. We find that both methods easily detect more unsophisticated spoofing attacks, but struggle on more sophisticated attacks such as power-managed scenarios. We enumerate several avenues for each method class that merit further exploration, to improve accuracy of GPS spoofing detection for even more sophisticated attacks.

I. INTRODUCTION

The Global Positioning System (GPS) constellation provides essential position, navigation, and timing services for countless applications worldwide, including transportation, power grids, precision agriculture, emergency responses, finance, telecommunications, and scientific research (UN, 2023). However, the civilian segment of GPS is highly susceptible to spoofing attacks, due to lack of signal encryption. Spoofing refers to the broadcasting of false signals with the intent that the target receiver will misinterpret them as authentic signals. Spoofing is different from jamming, which instead masks GPS signals with noise to create interference without generating new counterfeit signals. A spoofer replicates the radio frequency carrier, pseudo-random spreading code, and data bits of the authentic GPS signal it is attempting to interfere with, providing the target receiver with false position, velocity, and timing (PVT) information (Manfredini et al., 2018). Given the significant reliance on GPS for vital activities worldwide, it is crucial to develop spoofing detection techniques, as well as mitigation strategies to fight off spoofing attacks.

The methods employed to generate spoofed signal characteristics vary, as detailed in (Psiaki and Humphreys, 2016). One common form of a spoofing attack involves broadcasting counterfeit signals synchronized in code-phase and Doppler with the authentic ones and gradually increase the false signal power to deceive the target receiver into tracking the false signals. Another form involves preliminary jamming of the target receiver to disrupt tracking of the true signal and initiate re-acquisition on the counterfeit one. The chances of locking onto the false signal are higher if the false signal power is much higher than the authentic one. However, reproduction of the signal characteristics is challenging, particularly with security enhanced signals. Alternatively, a spoofer may employ meaconing. Meaconing is a type of spoofing where the true GPS signals are recorded re-transmitted, typically though a repeater, with a high enough gain to overwhelm the true signals at the target receiver antenna. In theory, meaconing may spoof any GPS signal, regardless of encryption. Nulling is a more advanced spoofing technique, where the spoofer transmits two signals: one with false PVT information, and the other as the negative of the true signal. This is done to completely erase the authentic signal, leaving only the false signal, although this technique is quite challenging to pull off.

In this paper we explore two methods for GPS spoofing detection, one theory-driven and one data-driven. In Section 2, we cover related work on both theory- and data-driven methods as applied to detecting spoofing attacks. Section 3 formally outlines the task of GPS spoofing detection, which we address in this paper. Section 4 describes the Texas Spoofing Test Battery (TEXBAT) spoofing dataset, which we utilized for all our experiments. In Section 5, we detail the two detection methods that we explored as part of this work: received power monitoring as a theory-based method, and a Support Vector Machine (SVM) for a data-driven technique. Section 6 delineates the results obtained from our experiments with both methods. Finally, in Section 7, we discuss potential improvements and extensions of this work for further exploration. Approaches were developed and evaluated with Python-based routines, which can be found in our **GitHub repository**.

II. RELATED WORK

Several spoofing detection efforts focus on enhancing user-segment technology against spoofing attacks. Space-segment spoofing detection and mitigation strategies are also being actively investigated; particularly, Chips Message Robust Authentication (CHIMERA) will launch onboard of the Navigation Technology Satellite 3 in late 2023, providing signal security enhancement to the GPS civilian C/A signal (Cameron, 2019). However, these space-segment centered strategies suffer from significant financial hurdles. User-segment detection strategies are often low-cost and easier to implement, often requiring little to no additional software or hardware. For instance, monitoring total received power can be achieved through an existing component of the GPS signal processing ensemble, and has been shown in provide insightful information about whether as signal is spoofed or not (Akos, 2012;Lo et al., 2018). Signal power monitoring is another notable user-segment spoofing detection method, where distortions in the correlation function of a signal are used as indicators of spoofing (Pini et al., 2018). (Manfredini et al., 2018) and (Lemmenes et al., 2016) investigated the application of both signal quality and received power monitoring, highlighting the need for both approaches to compensate for each other's downfalls. These approaches are categorized in this report as theory-driven: they relay on differences between the expected, or theorized, signal behavior and the observed signal behavior at each time step

Purely theory-driven methods such as thresholding on received power work well for many kinds of attacks; but these methods do often fail on more sophisticated spoofing attacks, for example, attacks with careful power management. Overall, detection is limited by the empirically derived thresholds, which can easily result in false detection when conditions change from those during which the empirical models were originally determined. For example, a method to detect GPS spoofing by thresholding on C/N_0 values could fail when satellite elevation angles change and causes the C/N_0 values to decrease (Zhu et al., 2022). Many existing detection methods also require additional hardware. For instance, absolute power detection requires adding Application-Specific Integrated Circuit and Analog-to-Digital calibration at the front end (Zhu et al., 2022). The additional hardware requirements make such detection methods more expensive and impractical to deploy. Most theory-driven methods also consider different signals independently (i.e. looking only at absolute power, or only at code correlator outputs), rather than performing detection by using multiple signals in aggregate. More insidious spoofing attacks may be indistinguishable from noise in individual signals, being only detectable in signal covariances. For a method to be capable of detecting extremely subtle attacks, it is necessary to capture the interrelationships between different signals.

A number of data-driven approaches, both supervised and unsupervised (Khoei et al., 2022), have been developed to detect spoofing attacks. The algorithms used include probabilistic methods like the Naive Bayes algorithm (Ismail and Reza, 2022), tree-based methods (Aissou et al., 2021), conventional and convolutional neural networks (Borhani-Darian et al., 2020; Maynard, 2022), support vector machines (Zhu et al., 2022; Semanjski et al., 2019), and LSTM networks (Jullian et al., 2022). The particular signals used as input for the methods also vary widely, from C/N_0 and power, to correlator outputs and ranging measurements. The SVM method we explore in this paper is inspired by a number of these works.

III. PROBLEM STATEMENT

The task of detecting GPS spoofing can be viewed as a classification problem: a set of observed measurements must be classified as having originated under either spoofed or non-spoofed conditions. With a more sophisticated detector, one could even envision classification into multiple classes, for a system that can distinguish between clean, spoofing, jamming, and multipath / other interference scenarios. But the simplest form of the detection problem is binary classification of received signals as either authentic or counterfeit; this is the formulation we follow in this work. Depending on the spoofing detection technique implemented, this condition may be evaluated at different steps of GPS signal processing. It can be evaluated on individual signal features, such as C/N_0, pseudorange, Doppler, or correlation function components. It may also be evaluated on combined signal characteristics, like combined average received power, or positioning, velocity, and timing estimation trends. Indeed, the spoofing detection approaches we developed and outline in Section 5 make use of the multitude of features produced throughout signal processing.

Authentic and counterfeit GPS signal data is extracted from the Texas Spoofing Test Battery, which is a series of simulated spoofing scenarios compiled by researchers at the University of Texas-Austin's Radionavigation Laboratory. Documentation provided with the dataset allows us to determine whether the receiver is being interfered with or not by a spoofing attack. Therefore, we able to classify data with this binary spoofing metric, which allows us to use the dataset to asses the performance of the detection techniques developed. The following section presents relevant information about the dataset.

IV. TEXBAT GPS SPOOFING DATASET

The TEXBAT is a set of high-fidelity recordings of live static and dynamic GPS L1 C/A spoofing tests conducted by the Radionavigation Laboratory of the University of Texas-Austin (Humphreys et al., 2012). The dataset has helped establish the standard of GPS civilian spoofing detection techniques throughout the past 10 years, and has been utilized by groups throughout academia and industry (Todd Humphreys, 2015).

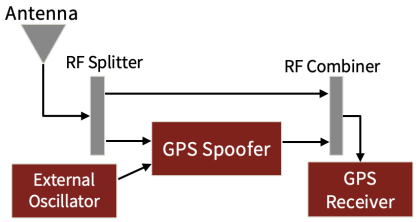

Figure 1: Real-Time Spoofing Testbed

An overview of the real-time testbed set-up is shown in Figure 1. The testbed draws real-time authentic GPS signals via a static or moving antenna, which are then sent both to the GPS spoofer to generate counterfeit GPS L1 C/A signals and the RF combiner ensemble. An external oscillator feeds a stable time reference to the spoofer. As detailed in (Humphreys et al., 2012), notable characteristics of the GPS spoofer include

- Phase alignment: positioning and timing deviations are introduces via code-phase shifting. However the spoofer cannot generate signals perfectly carrier-phase aligned with the authentic ones at the location of the target receiver. Originally, the spoofer adopted two modes to generate carrier-phase. On default mode, the rate of change of the carrier-phase varies proportionally to the rate of change of the code-phase of the signal. On frequency lock mode, the relative offset between the generated carrier-phase and the one of the authentic signal is maintained constant to the initial recorded offset. This mode minimizes potential rapid signal amplitude changes caused by the interaction between signals with different carrier-phase rates of change. The most recent release of the testbed (Todd Humphreys, 2015) is also capable of antipodal phase alignment, which enables the spoofer to first null the authentic signal targeted and smoothly take over locking and tracking.
- Navigation data bit prediction: the spoofer may either obtain the full 12.5 minute navigation data subframe to perform navigation data bit modulation, or predict the modulation.
- Variable output attenuation: prior to leaving the spoofer, false signals are passed through a digital attenuator to adjust the power advantage, the ratio of power of the counterfeit signals to that of the authentic ones as perceived by the target receiver.
- Noise padding: as mentioned in the previous section it is often useful for a spoofer to produce counterfeit signals that are overpowered relative to the authentic ones to mislead the target receiver into tracking the spoofed signals. The TEXBAT spoofer prevents unnaturally high C/N_0 signal values of overpowered signal via variable broadband interference.

The authentic and false signals are then downmixed and digitized with an RF Combiner, and in real-time, these signals are directly provided to a science grade UT/Cornell/ASTRA CASES sensor receiver. Scenarios may also be replayed to test the response of different receivers. The TEXBAT data presented in this report is the real-time dataset published by the Radionavigation Laboratory.

The data is compiled in raw binary data files as well as partially parsed mat files. In total, there are seven unique spoofing scenarios and a clean, un-spoofed, scenario. All scenarios have the same authentic GPS signals. The mat files are accompanied by text files detailing the contents of the files. For this reason, as well as being significantly smaller in size, we elected to use the mat files for experimentaiton. Only the static scenarios have corresponding mat files, where the GPS receiver antenna was not moving during simulation. These scenarios are detailed in Table 1, compiled from (Humphreys et al., 2012; Todd Humphreys, 2015). All the static spoofing scenarios are identified as "time-spoofing", where the spoofer gradually introduces a 2 μs offset in the receiver's perceived time. Power advantage varies from 10 dB to 1.3 dB. With a high power advantage, the authentic signals are forced into the noise floor, giving the receiver no choice but to track the counterfeit signals. The matched-power scenario implements frequency locking for carrier phase generation, while the sophisticated attack employs antipodal carrier phase generation. The sophisticated attack tries to pull off a perfect nulling-and-replacement attack, which is still impractical to do (Psiaki and Humphreys (2016);Wesson et al. (2018)); therefore, it must compensate with a low power advantage. All simulations are approximately 7 minutes long, and spoofing is noted to begin between 100 and 130 seconds. The attack lasts until the end of the simulation.

The data provided in the TEXBAT mat files contains time histories of the measured average received power (P_k) over three frequency bands at every time step (t_k) of internal receiver time. The bands are centered at the L1 frequency, 1575.42 MHz. The files also include time histories of pseudorange, C/N_0, beat carrier phase, apparent Doppler frequency, in-phase and symaccumulation components for various GNSS satellites visible at the time of testing. Finally, the files provide access to navigation data from PVT estimation, including Earth-Centered Earth-Fixed position and velocity with respect to receiver time, as well as receiver clock error and receiver clock error rate. Detailed analysis of the data from each scenarios, as well as

Table 1: Overview of Static TEXBAT Scenarios

Scenario	Spoofing Type	Power Advantage [dB]	Carrier Phase Generation
Clean	N/A	N/A	N/A
Overpowered	Time	10	Default
Matched-Power	Time	1.3	Frequency Locking
Sophisticated Attack	Time	1.3	Antipodal

suggested parsing steps to properly align data from different scenarios, can be found in (Lemmenes et al., 2016;Humphreys et al., 2012;Lemmenes et al., 2016). To extract the data and evaluate the spoofing detection approaches, we developed Python-based parsing routines, which can be found in our **GitHub repository**. Detailed descriptions of the approaches we developed follows.

V. APPROACH

1. Signal Power Characterization

The GPS broadcasted civilian navigation signal in the L1 frequency band ($s_{L1,C/A}$) over time (t) can be expressed in the following form

$$s_{L1,C/A}(t) = \sqrt{2P_{C1}}D(t)x(t)\cos\left(2\pi(f_{L1}+f_D)t+\theta_{L1}\right) \tag{1}$$

where P_{C1} is the signal power for signals carrying pseudo-random C/A code on L1, $D(t)$ denotes the navigation data bit stream modulation, $x(t)$ is the C/A code sequence, f_{L1} and f_D are the L1 and Doppler frequencies respectively, and θ_{L1} is the carrier phase offset (Pratap Misra and Per Enge, 2011;Wesson et al., 2018) This signal is subject to noise, which can be generally expressed as s_N. This component encompasses both the thermal noise and effects produced by the interaction with other multiple-access signals. In the event of spoofing, an interfering signal component, s_I, accompanies the received signal. This component has similar form to Eq.(1), but it does not contain $D(t)$ navigation modulation. Overall, the total L1 civilian signal perceived by a received may be modelled as

$$s(t) = s_{L1,C/A}(t) + s_N(t) + s_I(t) \tag{2}$$

Figure 2 provides an outline of how a common GPS receiver extracts position, velocity and timing (PVT) information from broadcasted signals. Signals are first received via an antenna and undergo processes to attenuate frequencies beyond a range of interest, amplify the low energy signal, and convert signals to a lower intermediate frequency to enable quantification and demodulation. Then, continuous analog signals are converted to a digital form through an Analog to Digital Converter (ADC). A key component of the ADC element is Automatic Gain Control (AGC), which controls the amplitude of an incoming signal to spread it out over quantization levels (Pratap Misra and Per Enge, 2011). It does so by scaling the incoming signal power with a time varying function. Generally, the incoming power is measured indirectly through the AGC setpoint (Psiaki and Humphreys, 2016). Following conversion to digital, signals pass through carrier wipeoff to remove carrier wave. At this point, the process of acquisition begins, searching for the appropriate frequency and code-delay parameters. Following successful acquisition, signal tracking via Delay Lock Loop (DLL) and Phase Lock Loop (PLL) commences to remain locked onto specific signals and produce PVT estimation.

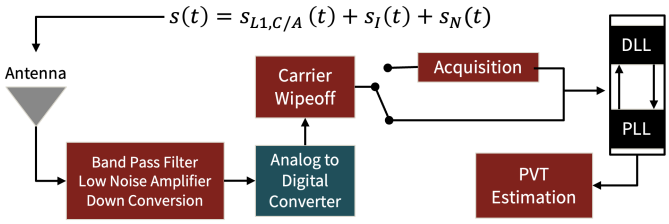

Figure 2: GPS Receiver Signal Processing Overview (Pratap Misra and Per Enge, 2011)

Throughout this process, we may extract and monitor the received combined signal power at different frequency bands. Specifically, we can analyze the average power P_k over time, which for an individual signal is given as the time average of the post-filtered signal squared over the interval $T = t_k - t_{k-1}$. As mentioned prior, common spoofing techniques increase the power of counterfeit signals relative to the authentic ones to deceive the target receiver in acquiring and tracking the false, more powerful signals. Considering Figure 2 above, a more powerful signal forces changes in the AGC gain values, pushing the

authentic signal components below the noise floor (Lemmenes et al., 2016). Thus the receiver acquires and locks onto the false signal, producing misleading PVT estimates. We leverage the combined power deviations measured by the receiver to detect interference. Such technique is also useful to avoid pitfalls in distinguishing between spoofed and multipath signals when a correlation function-based approach is employed.

Assuming that the time-history of received power follows a Gaussian distribution, given that the characterization of the noise is also Gaussian, then we can record un-spoofed variance (σ^2) and mean (μ) in average signal power over a time interval. These two parameters define the expected distribution of power, therefore we can set a threshold so that if the monitored power exceeds such threshold, then that particular average power value is flagged as containing interference. In other words, defining $f(t_k)$ as a binary interference metric at time step t_k,

$$f(t_k) = \begin{cases} 1 & |P_k| \leq \mu_{P_k} + 5\sigma_{P_k} \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

Eq. (3) has a maximum acceptable un-spoofed variance from the mean to 5σ, setting the probability of false alarm to less than one in a million. If the threshold is not exceeded, we believe the signal is authentic. Alternatively, the ACG gain values could be monitored, setting a threshold in a similar fashion to detect interference (Manfredini et al., 2018).

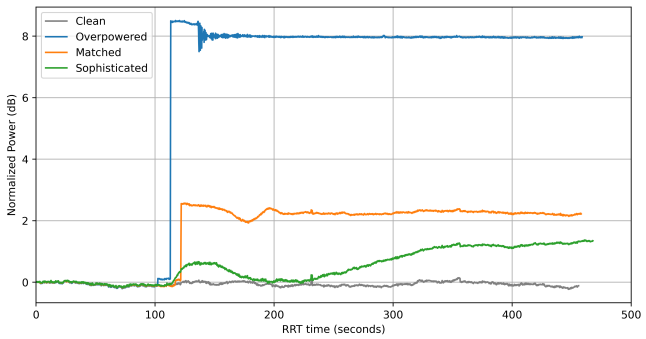

Figure 3: Normalized average received power across static scenarios for 2MHz frequency band

Figure 3 displays the normalized measured average received power at a 2MHz frequency band with respect to raw receiver time (RRT) across all four static TEXBAT scenarios. Notably, the overpowered scenario exhibits the greatest increase in average received power at approximately 115 seconds of about 8 dB. The matched-power scenario exhibits a sharp increase as well around 120 seconds, although the magnitude is of approximately 2 dB. The last scenario, the sophisticated spoofing attack, first exhibits a gradual increase in power of 1 dB up to the 155 second mark, fluctuating back down near 200 seconds, and steadily increasing till the end of the simulation. By employing frequency locking to generate the carrier phase of the false signal, signal amplitude changes caused by the interaction between signals with different carrier-phase rates of change are minimized. Since signal amplitude is related directly to the power of the signal, the average received power of the FL matched-power scenario exhibits smaller variations from the clean dataset. The 2MHz frequency band was chosen to evaluate the power monitoring detection technique as it captures the main lobe of the C/A power spectrum. To authenticate the military P(Y) signal, a larger frequency band should be utilized, given that the signal main power lobe is about 10 times wider than the one of the C/A signals (Humphreys et al., 2012). This data is used to evaluate Eq. (3) as a spoofing interference detection metric.

2. Support Vector Machine (SVM)-based Detection

Numerous data-driven methods for binary classification, both supervised and unsupervised, exist across different machine learning applications. Here, we choose to utilize Support Vector Machines (SVM), as they follow quite naturally from the power monitoring approach that we explore as our theory-driven method. SVMs essentially allow for complex, nonlinear thresholding of multiple measurements simultaneously. Below, we provide a brief overview of SVM theory, before outlining our method for constructing an SVM-based GPS spoofing detector.

The objective of an SVM is to find a decision boundary that optimally separates points from different classes. In the 2D case, where points have two 'features', this would be a line; in 3D it would be a plane; and for higher dimensions, the boundary would be an n-hyperplane. SVMs aim to maximize the distance between the boundary and the nearest points from either class;

these points, which would be the most difficult to classify, are called the *support vectors*. The region (parallel to the boundary) between the support vectors is called the *margin*.

The boundary can be written as the set of points satisfying

$$\mathbf{w}^T\mathbf{x} - b = 0 \tag{4}$$

where $\mathbf{w}$ is the (non-normalized) normal vector to the boundary. In the case where the data is linearly separable, we define two hyperplanes parallel to the boundary that run through each set of support vectors, which we call *gutters*. These hyperplanes are defined by the equations

$$\mathbf{w}^T\mathbf{x} - b = +1 \tag{5}$$

and

$$\mathbf{w}^T\mathbf{x} - b = -1 \tag{6}$$

where we represent our binary classes numerically as $y_i = +1$ and $y_i = -1$. This geometry is shown in Figure 4. The distance between the two hyperplanes is $\frac{2}{||w||}$, so maximizing the margin width is equivalent to minimizing $||w||$.

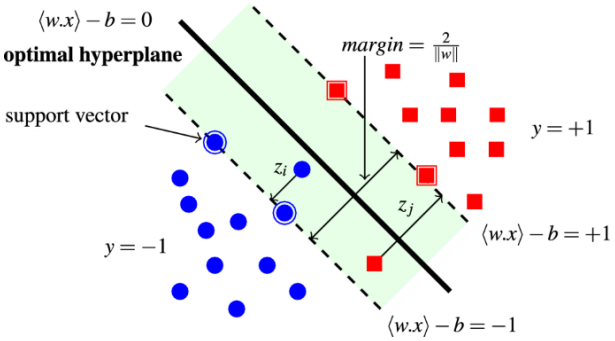

Figure 4: Support Vector Machine (SVM)

To ensure that points of each class lie on the correct side of the decision boundary (and outside the margin), we have the following constraint:

$$y_i(\mathbf{w}^T\mathbf{x_i} - b) \geq +1 \text{ for all } 1 \leq i \leq n \tag{7}$$

Combining these, we arrive at the optimization problem

$$\begin{aligned} \min_{\mathbf{w},b} \quad & ||w||_2^2 \\ \text{s.t.} \quad & y_i(\mathbf{w}^T\mathbf{x_i} - b) \geq +1 \forall i \in \{1, ..., n\} \end{aligned} \tag{8}$$

The solution to this determines our classifier as

$$\mathbf{x} \mapsto \text{sgn}(\mathbf{w}^T\mathbf{x} - b) \tag{9}$$

This is a quadratic constrained optimization problem, which can be solved using the Lagrangian multiplier method.

For data that is not linearly separable, we can use *kernel functions* to map data into higher dimensional spaces in which the data becomes linearly separable. As most real-world data is nonlinear, kernels are an essential technique for modeling complex relationships. There are many kernel functions used for various applications; but here we deal with the most common one, the Radial Basis Function (RBF):

$$k(\mathbf{x}, \mathbf{z}) = e^{\frac{-(x-z)^2}{\sigma^2}} \tag{10}$$

To apply the SVM algorithm to the problem of GPS spoofing, we follow the workflow shown in Figure 5.

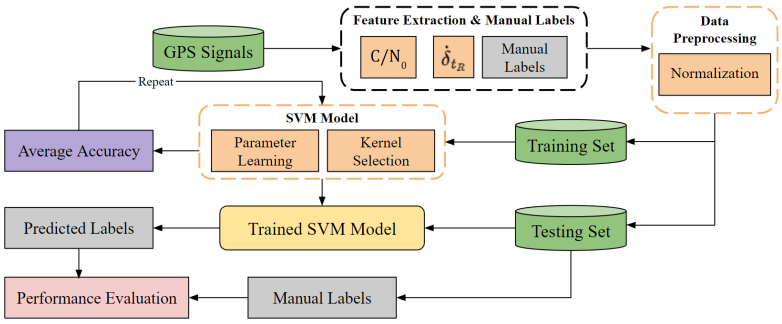

Figure 5: SVM-based detection of GPS spoofing (figure adapted from Zhu et al., 2022)

From the received GPS signals, features are chosen and extracted for use with the SVM. The choice of features is a critical one; we want to select signals that would be most effective for detecting GPS spoofing. For our initial exploration, we use the C/N_0 values for the 12 GPS satellites that were visible in our dataset, as well as the receiver clock error rate. We know that C/N_0 is a function of the path loss between the satellite and receiver antenna, so would logically be affected by spoofing attacks. Clock error also changes under both time and position spoofing, so receiver clock error rate was chosen as the final feature for use in the SVM. C/N_0 and receiver clock error rate for the static TEXBAT scenarios are plotted in Figure 6. (Features were also, in part, chosen for ease of extraction from the TEXBAT dataset.)

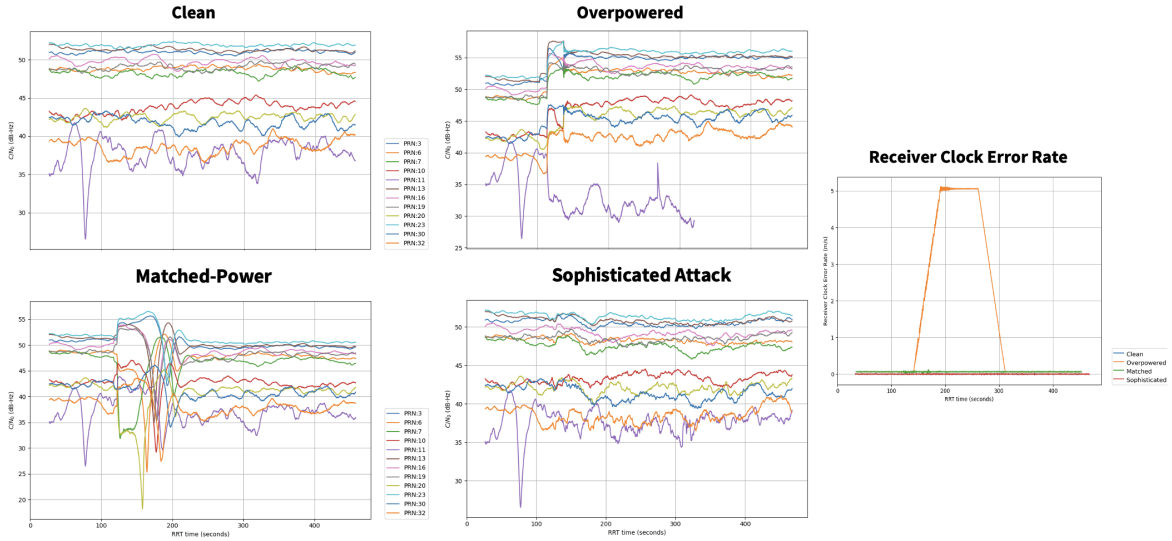

Figure 6: C/N_0 values for the 12 visible GPS satellites [left] and receiver clock error rate [right], plotted for static TEXBAT scenarios

Due to the dearth of data, rather than treating each scenario as an individual time series, time points are considered individually. All time points across all four TEXBAT scenarios are agglomerated into a global dataset. The data for each time point consists of thirteen features in total: the twelve C/N_0 values, and the clock error rate. Each point is also associated with a binary label corresponding to whether or not the receiver was under spoofing conditions at the time. With this, we end up with a dataset of $\tilde{8}$-9k points, which we can use for supervised learning.

The data is normalized, and then split into a training set (70%) and a test set (30%). The training set is used to learn the SVM decision boundary, in an iterative optimization process that involves computing accuracy and refining boundary parameters. Once learned, the trained SVM model is then applied to the test set, classifying every point as either 'spoofed' or 'not spoofed'. These predicted labels are compared against the ground truth labels from the TEXBAT scenarios to evaluate detection performance of the SVM.

The major limitation of this procedure is that we discard all temporal information, when in reality, subtle changes over time are the hallmark of spoofing attacks. This design choice was made due to the sparsity of data available; however with more data

available, other methods that account for time (such as recurrent/LSTM neural networks, or methods developed for time series analysis) would be worth exploring.

VI. RESULTS

1. Signal Power Monitoring

Following the steps outlined in Section 4.1, we proceed to characterize the clean, or nominal, mean and variance of the average received power. Unfortunately, we noticed discrepancies across the 4 scenarios. The received power of the clean scenario has a mean of 59.74 dB for the entire simulation, which is consistent with the mean of the FL matched-power scenario prior to spoofing (59.79 dB for the first minute of simulation). For the overpowered scenario, the mean for the first minute of simulation is 50.99 dB, and 51.02 dB for the matched-power scenario. We believe that since the FL matched-power data was generated with signal replay years after the other datasets, the receiver used was updated, and researches only replayed the clean and FL matched-power data with this new technology (Todd Humphreys, 2015). (Lemmenes et al., 2016) has noted this issue, and suggested an amplitude adjustment to the data, but it is not clear if the adjustment is meant for the data to be replayed or the data from the mat files. We were not able to resolve this discrepancy, so instead of following the original plan to solely characterize the nominal received power from the clean dataset, we evaluated the mean and variance of the average received power for each individual spoofed dataset over the first minute of simulation, which is guaranteed to be un-spoofed. Means and variances are reported below in Table, along with threshold bounds from Eq. (3).

Table 2: Nominal average power metrics and threshold

Scenario	**Mean** (μ) [dB]	**Variance** (σ^2) [dB]	**Threshold** [dB]
Overpowered	50.995	0.0013593	(50.810, 51.179)
Matched-Power	51.020	0.0012884	(50.840, 51.199)
Sophisticated Attack	59.785	0.0012844	(59.606, 59.965)

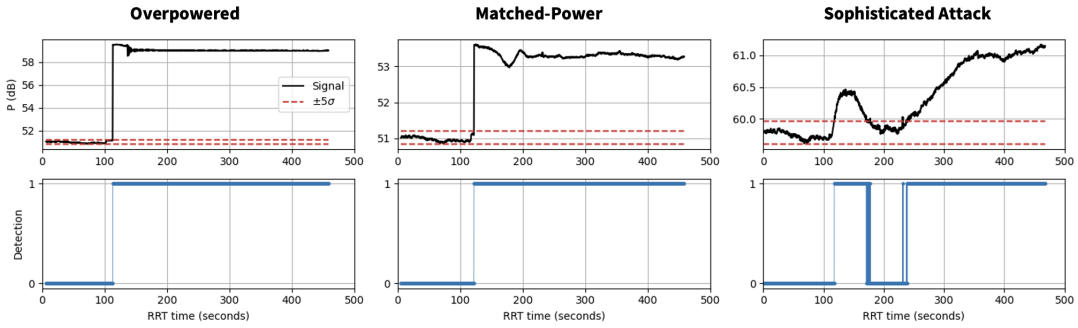

Figure 7: Average received power for each spoofing scenario [top] with corresponding interference detection results using Eq. (3) [bottom]

The performance of power monitoring as an interference detection method is shown in Figure 7. The binary interference metric switches on for the first time at 113 seconds for the overpowered scenario, at 122 seconds for the matched-power one, and at 118 seconds for the sophisticated spoofing attack. TEXBAT documentation does not provide an exact time when spoofing occurs, but spoofing is guaranteed to begin between 100 and 130 seconds. Therefore, the power monitoring interference metric successfully identifies that there is interference in the received signals close to the time when spoofing commences. However, once the spoofing attacks begins, it guaranteed to last until the end of the simulation. The interference metric for the sophisticated scenario flips frequently starting at 171 seconds, turning off completely at 178 seconds. At 231 seconds, there is a brief threshold violation, until the metric turns back on and remains equivalent to one at 239 seconds. Beyond low power advantage, the sophisticated attack employs an antipodal carrier-phase generation technique that enables nulling in the initial stage of spoofing and replacement of the authentic signal with a false one. Perfect nulling is extremely difficult to carry out: if it was perfect, there would be no difference in the received power history. Since this is not a perfect nulling-and-replacement attack, we are still able to detect interference through high power variations, but not as well as the other spoofing attacks. While this is still a reliable detection technique for overpowered spoofing attacks, it does require authentic received signal power characterization. Several factors influence this characterization, such as if the receiver antenna is stationary or not, if there are sudden changes in the power spectrum, or if there are unexpected changes in the antenna's effective temperature or the receiver noise temperature. In practice, receiver implementing received power monitoring should gather significant amounts of un-spoofed power data to minimize false interference detection.

2. Support Vector Machine (SVM)-based Detection

We found that, for our scenarios, a linear SVM using only C/N_0 and clock error rate achieved a detection accuracy of 81%, with a false positive (detecting spoofing during non-spoofed conditions) rate of 9.5%, and a false negative (failing to detect spoofing during an attack) rate of 9.8%. To improve performance, we train a second SVM, this time using a radial basis function kernel. Performance improved dramatically, suggesting that determining spoofing from GPS signals is a highly nonlinear process. The RBF SVM achieved a detection accuracy of 95%, with a false positive rate of 0.08%, and a false negative rate of 5.4%. These results, along with other commonly computed evaluation metrics, are displayed in Table 3.

Table 3: Support vector machine experimental results with two kernels

	Linear SVM	**RBF SVM**
Accuracy	80.78%	94.50%
Precision	84.93%	99.86%
Recall	84.50%	91.41%
False Positive Rate	9.45%	0.08%
False Negative Rate	9.77%	5.42%

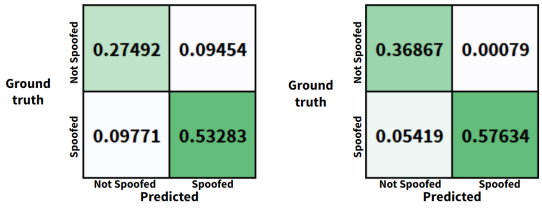

Figure 8: Confusion matrices for linear and RBF SVMs

Visualizing the detection output for each scenario yields additional insight into the SVM results, as shown in Figure 9. The linear SVM clearly performs quite poorly. The radial basis SVM achieves essentially perfect detection for the clean, overpowered, and matched-power scenarios; but it struggles somewhat on the sophisticated attack. This is unsurprising considering the features we used; twelve of our thirteen features were C/N_0 values, which are tied to power. We hypothesize that by using additional features with an RBF SVM, we would be able to detect even the more spoofing sophisticated attacks.

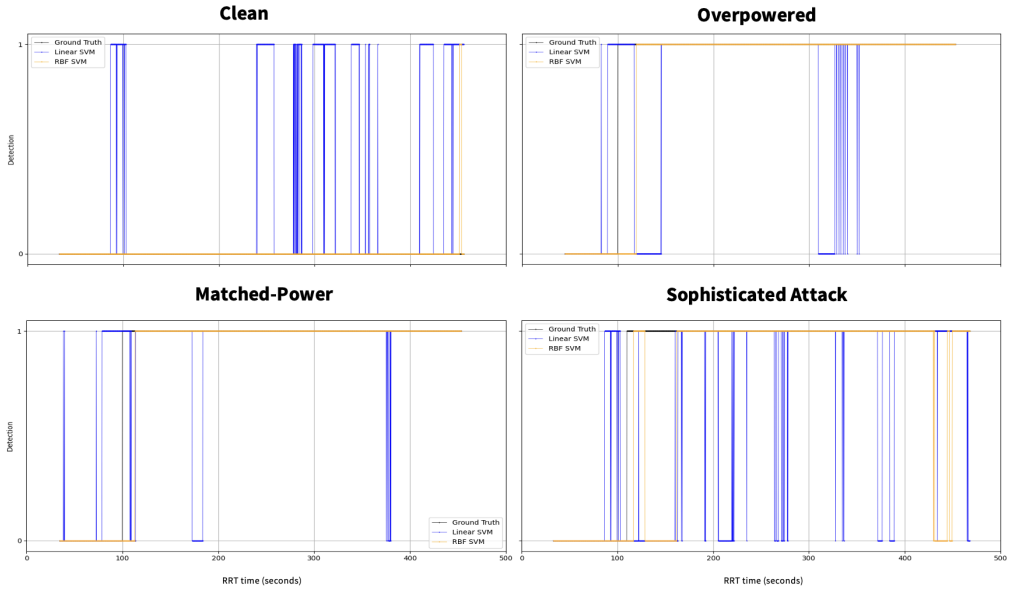

Figure 9: Detector outputs for linear and RBF SVMs superimposed atop the ground truth values for the four scenarios. The apparent time offsets are artifacts of data misalignment during plotting, not reflective of detection performance.

VII. CONCLUSION

The ability to detect and mitigate spoofing attacks is essential to ensure safe and reliable GPS usage for countless vital applications. Using the TEXBAT dataset, we were able to evaluate the performance of two different spoofing detection techniques. Received power monitoring successfully identified signal interference due to spoofing for the overpowered scenario as well as the matched-power one. It also successfully identified the beginning of the sophisticated spoofing attack, but struggled to recognize its entire duration. Additionally, this detection strategy requires extensive received signal power characterization, which is influenced by receiver antenna movement, data collection environment, and receiver technology.

Spoofing can also be detected using data-driven methods such as support vector machines. We found that an SVM-based detector can achieve reasonable accuracy using only C/N_0 and receiver clock error rate, particularly when using a radial basis function kernel. The SVM method is demonstrably very generalizable, as we learned a single SVM for all four scenarios in aggregate (as opposed to individual SVMs for each scenario), and still achieved good detection performance. With additional features, we expect that an SVM detector would be fully robust to the spoofing attack strategy used. The limitation of using a supervised learning method like an SVM, however, is that accurately time-stamped measurements from both clean and diverse spoofed conditions are required. Overall, an SVM-based detector is a highly promising method for detecting GPS spoofing.

Instead of average received power monitoring, the AGC gain value can be used used to establish a similar thresholding technique. Combining received power monitoring with another theory-based detection technique like signal quality monitoring might prove beneficial in detecting low-power spoofing. Signal quality monitoring focuses on distortions in the correlation function that occur based on the interaction between false and true signal components. If the counterfeit signal is overpowered, it will force the authentic one into the noise floor, producing a nominal correlation function. While signal quality monitoring would miss this interference, the received power monitor is instead quite effective at detecting overpowered attacks.

For further exploration with SVM-based detectors, we plan to use additional features such as the ratio and delta metrics from signal quality monitoring (which are derived from the in-phase and quadrature components of the code correlator output). We also plan to use moving averages and variances in place of raw signal values, which will address pitfalls such as C/N_0 changing due to altered satellite elevation angles rather than spoofing. Ultimately, our goal is to utilize more intelligent, data-driven methods for feature selection, such as principal component analysis. For the SVM models, we can experiment with different kernel functions, such as the polynomial and sigmoid kernels. We can also perform parameter tuning, particularly for the SVM regularization parameter which determines the weight assigned to misclassifications (and can therefore substantially affect results). We can also investigate non-SVM data-driven strategies, such as methods for time series anomaly detection and/or forecasting, or using convolutional neural networks to predict spoofing probability using Cross Ambiguity Function maps.

CONTRIBUTIONS OF TEAM MEMBERS

Group Member	Contribution to Project
Mira Partha	Performed literature survey on data-driven detection strategies; collaborated on developing parsing routines for TEXBAT; developed and analyzed support vector machine detection; authored sections 2, 5.2, 6.2; co-authored sections 1, 3, 7
Marta Cortinovis	Performed literature survey on theory-driven detection strategies; collaborated on developing parsing routines; developed and analyzed received power monitoring detection; authored sections 5.1, 4, 6.1; co-authored sections 1, 3, 7

ACKNOWLEDGEMENTS

We thank Professor Gao and Tara for their excellent instruction over the course of the quarter. This work would not have been possible without their guidance.

REFERENCES

Aissou, G., Slimane, H. O., Benouadah, S., and Kaabouch, N. (2021). Tree-based supervised machine learning models for detecting gps spoofing attacks on uas. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0649–0653.

Akos, D. M. (2012). Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *NAVIGATION*, 59(4):281–290.

Borhani-Darian, P., Li, H., Wu, P., and Closas, P. (2020). Deep neural network approach to detect gnss spoofing attacks. In

Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), pages 3241–3252.

Cameron, A. (2019). AFRL tests Chimera to battle spoofers and hackers. [Online]. Available: https://www.gpsworld.com/afrl-tests-chimera-to-battle-spoofers-and-hackers/.

Humphreys, T., Bhatti, J., Shepard, D., and Wesson, K. (2012). The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques. In *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, pages 3569 – 3583, Nashville.

Ismail, S. and Reza, H. (2022). Evaluation of naïve bayesian algorithms for cyber-attacks detection in wireless sensor networks. In *2022 IEEE World AI IoT Congress (AIIoT)*, pages 283–289.

Jullian, O., Otero, B., Stojilović, M., Costa, J. J., Verdú, J., and Pajuelo, M. A. (2022). Deep learning detection of gps spoofing. In Nicosia, G., Ojha, V., La Malfa, E., La Malfa, G., Jansen, G., Pardalos, P. M., Giuffrida, G., and Umeton, R., editors, *Machine Learning, Optimization, and Data Science*, pages 527–540, Cham. Springer International Publishing.

Khoei, T. T., Gasimova, A., Ahajjam, M. A., Shamaileh, K. A., Devabhaktuni, V., and Kaabouch, N. (2022). A comparative analysis of supervised and unsupervised models for detecting gps spoofing attack on uavs. In *2022 IEEE International Conference on Electro Information Technology (eIT)*, pages 279–284.

Lemmenes, A., Corbell, P., and Gunawardena, S. (2016). Detailed Analysis of the TEXBAT Datasets Using a High Fidelity Software GPS Receiver. In *Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016)*, pages 3027 – 3032, Portland.

Lo, S., Rothmaier, F., Miralles, D., Akos, D., and Walter, T. (2018). Developing a Practical GNSS Spoofing Detection Thresholds for Receiver Power Monitoring. In *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, pages 803 – 815, St. Louis.

Manfredini, E. G., Akos, D. M., Chen, Y.-H., Lo, S., Walter, T., , and Enge, P. (2018). Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers. In *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, pages 672 – 689, Reston.

Maynard, L. L. (2022). Gnss spoofing detection using machine learning and truncated singular value decomposition. In *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, pages 1137–1150.

Pini, M., Fantino, M., Cavaleri, A., Ugazio, S., and Presti, L. L. (2018). Signal Quality Monitoring Applied to Spoofing Detection. In *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, pages 1888–189, Portland.

Pratap Misra and Per Enge (2011). *Global positioning system: Signals, measurements, and performance*. Ganga-Jamuna Press, Boston, revised second edition.

Psiaki, M. L. and Humphreys, T. E. (2016). GNSS Spoofing and Detection. *Proceedings of the IEEE*, 104(6):1258–1270.

Semanjski, S., Muls, A., Semanjski, I., and De Wilde, W. (2019). Use and validation of supervised machine learning approach for detection of gnss signal spoofing. In *2019 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–6.

Todd Humphreys (2015). TEXBAT Data Sets 7 and 8. Technical report.

UN (2023). Global Navigation Satellite Systems (GNSS). [Online]. Available: https://www.unoosa.org/oosa/en/ourwork/psa/gnss/gnss.html.

Wesson, K. D., Gross, J. N., Humphreys, T. E., and Evans, B. L. (2018). GNSS Signal Authentication Via Power and Distortion Monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, 54(2):739–754.

Zhu, X., Hua, T., Yang, F., Tu, G., and Chen, X. (2022). Global positioning system spoofing detection based on support vector machines. *IET Radar, Sonar & Navigation*, 16(2):224–237.