Spectrum-Centric Hypothesis Testing for GNSS Spoofing Detection: A Nominal-Only Mahalanobis Baseline on Raw I/Q Data

Anandhu Anilkumar Binu
anandhu.anilkumarbinu@studenti.unipd.it

January 2026

Abstract

Global Navigation Satellite Systems (GNSS) are critical to modern timing and positioning infrastructures, yet their radio-frequency (RF) signals are fragile and vulnerable to spoofing attacks designed to preserve apparent navigation-domain consistency. While many existing detection approaches rely on receiver-internal metrics or decoded navigation observables, it remains an open empirical question whether spoofing induces statistically measurable differences at the raw RF signal level.

This work presents a hypothesis-driven proof of concept based on *spectrum-centric* analysis of raw GNSS I/Q data. Treating nominal GNSS recordings as samples from a null distribution, we construct a nominal-only statistical test using interpretable RF features and the Mahalanobis distance. The test is trained exclusively on clean GNSS captures and evaluated on spoofed scenarios, without access to receiver internals or navigation solutions.

Experimental results on a public GNSS I/Q dataset demonstrate that spoofed signals produce statistically significant deviations from nominal RF behavior in a subset of observations. These findings reject the null hypothesis that spoofed and nominal GNSS RF environments are indistinguishable, thereby establishing the existence of an RF-domain effect induced by spoofing and motivating further investigation of spectrum-centric GNSS integrity monitoring.

1 Problem Statement and Hypothesis

GNSS spoofing attacks aim to manipulate receiver position or time estimates while maintaining signal structures that appear nominal at the navigation layer [2]. As a result, detection mechanisms operating on navigation-domain consistency or receiver-internal metrics may exhibit significant latency or fail entirely for carefully crafted RF-layer attacks.

This study addresses the following statistical hypotheses:

H_0: Spoofed GNSS signals are statistically indistinguishable from nominal GNSS signals at the raw RF (I/Q) level.

H_1: Spoofing induces statistically detectable deviations in the RF statistics of GNSS signals, even when navigation-domain consistency is preserved.

The objective of this proof of concept is not to maximize spoofing detection performance, but to test whether the null hypothesis H_0 can be rejected under realistic and minimally assumptive conditions.

2 Dataset and Experimental Context

The PoC is evaluated using an open-access GNSS raw I/Q dataset published on Zenodo by Wang *et al.* [5]. The dataset contains complex baseband GNSS recordings acquired under both nominal and spoofed conditions over two separate days (October 18 and October 19).

Each scenario includes:

- **Clean captures**, containing only authentic GNSS satellite signals;
- **Spoofed captures**, where authentic signals are mixed with two additional spoofing PRNs.

Files follow a structured naming convention:

- `S*.mat`: nominal (clean) scenarios used to estimate the null distribution;
- `SS*.mat`: spoofed scenarios used for hypothesis testing.

Sampling rates (25–50 MHz) and quantization resolutions (8–16 bit) vary across dataset categories, enabling robustness testing under realistic RF front-end configurations.

3 Raw I/Q Representation

GNSS signals are represented as complex baseband samples

$$x[n] = I[n] + jQ[n], \tag{1}$$

where $I[n]$ and $Q[n]$ denote the in-phase and quadrature components.

This representation preserves full amplitude and phase information and constitutes the most information-rich signal form available prior to receiver tracking loops. Operating directly on raw I/Q data enables RF-level analysis that is independent of proprietary GNSS receiver internals [3].

4 Windowing of the I/Q Stream

The continuous I/Q stream is segmented into fixed-duration windows of length T_{win} (typically 1 ms). For sampling frequency f_s, each window contains

$$N = T_{\text{win}} \cdot f_s \tag{2}$$

samples.

Windowing enables low-latency statistical testing, temporal localization of anomalies, and conversion of long recordings into independent analysis units without requiring GNSS decoding or synchronization.

5 Spectral Feature Extraction

For each window, spectral features are derived from the power spectral density (PSD) estimated using Welch's method [6]. PSDs are computed separately for real and imaginary components and summed to ensure numerical stability for complex-valued signals.

Each window is mapped to a seven-dimensional feature vector:

$$\mathbf{f} = \left[P_{\text{tot}}, P_{\text{noise}}, H_{\text{spec}}, F_{\text{spec}}, \sigma^2_{\text{PSD}}, \kappa_{\text{amp}}, \sigma_{\text{amp}}\right]^\top. \tag{3}$$

These features capture complementary aspects of the RF environment, including total power, spectral structure, and amplitude statistics, and are selected for interpretability and statistical robustness.

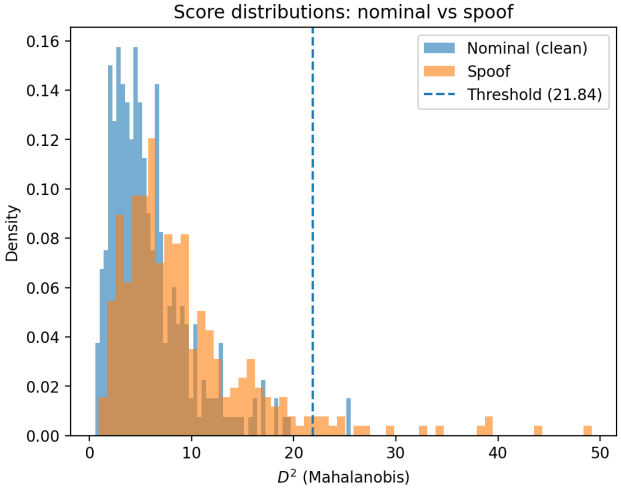

Figure 1: Distribution of Mahalanobis scores for nominal (clean) and spoofed GNSS windows. The dashed line indicates the threshold derived from the 99.5% quantile of nominal data.

6 Nominal-Only Mahalanobis Test Statistic

Feature vectors extracted from clean files are standardized and used to estimate a covariance matrix via the Ledoit–Wolf shrinkage estimator [4]. For each window, a squared Mahalanobis distance

$$D^2 = (\mathbf{f} - \boldsymbol{\mu})^\top \boldsymbol{\Sigma}^{-1} (\mathbf{f} - \boldsymbol{\mu}) \tag{4}$$

is computed.

Under the null hypothesis H_0, large values of D^2 correspond to low-probability deviations from nominal RF behavior [1]. A decision threshold τ is selected as a high quantile of the nominal score distribution, defining the statistical significance level α of the test.

7 Experimental Results

7.1 Score Distributions

Spoofed windows exhibit a heavier right tail in Mahalanobis distance relative to nominal windows. Although the distributions overlap substantially— reflecting the GNSS-like nature of the spoofing—the presence of high-score outliers demonstrates statistically significant deviations from the null distribution.

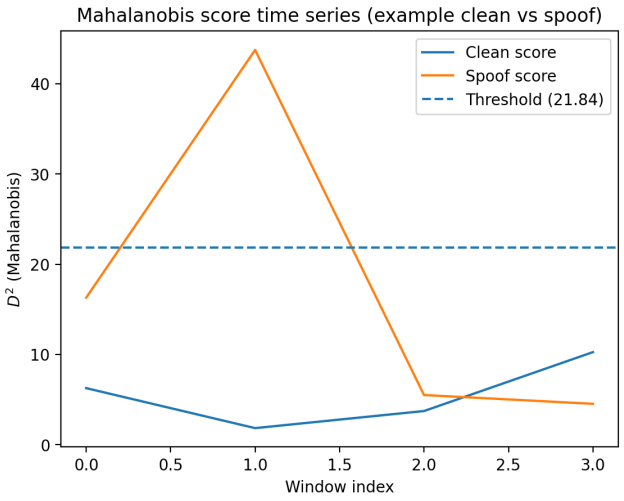

Figure 2: Example time series of Mahalanobis scores for a clean and a spoofed recording. The spoofed signal exhibits threshold exceedances within a small number of windows.

7.2 Time-Series Detection Behavior

Clean recordings remain consistently below threshold, while spoofed recordings produce sharp excursions above τ. Each threshold exceedance corresponds to rejection of the null hypothesis at the chosen significance level.

7.3 Threshold Sensitivity

Lower thresholds correspond to more aggressive hypothesis testing at the expense of increased false rejections of H_0, while conservative thresholds enforce strict statistical confidence with minimal false alarms.

7.4 Quantitative Performance Summary

Using a threshold corresponding to the 99.5% nominal quantile ($\tau = 21.84$), the test yields a **window-level false rejection rate of 0.62%** under H_0 and a **window-level rejection rate of 5.31%** under spoofed conditions.

Aggregating window-level statistics at the file level yields rejection of H_0 in **21.25%** of spoofed recordings, indicating that approximately one in five spoofed files contains at least one RF window that is statistically inconsistent with nominal behavior.

7.5 Temporal Aggregation and Event-Level Interpretation

The reported window-level rejection rates should be interpreted in the context of the extremely short analysis window ($T_{\text{win}} = 1$ ms). A single window represents a minimal unit of RF evidence. In an operational integrity-monitoring context, decisions would rely on temporal aggregation of evidence, such as persistence of threshold exceedances or multiple exceedances within a sliding time window.

Such temporal aggregation does not require retraining or modification of the underlying statistical model; it is a post-processing decision logic applied to the score time series. Under this interpretation, the file-level rejection rate already reflects the integrity-relevant question of whether *any* statistically inconsistent RF behavior is observed during a recording.

8 Discussion

8.1 Hypothesis Testing, Not a Finished Detector

This proof of concept should be interpreted as a hypothesis test and an existence proof, not as a complete operational spoofing detection system. The scientific contribution is the rejection of the null hypothesis H_0 that spoofed and nominal GNSS RF environments are statistically indistinguishable at the raw I/Q level.

8.2 Operating Point Selection

Figure 3 illustrates the trade-off between false rejections under H_0 and rejection rates under spoofed conditions as the detection threshold is varied. The operating point reported in this study is intentionally conservative and prioritizes statistical confidence over sensitivity.

8.3 Generalization and Dataset Limitations

Evaluation on a single public dataset limits claims of universal generalization. Feature standardization mitigates sensitivity to absolute gain and scaling, but cross-device and cross-collection validation remains future work.

8.4 Adversarial and Physical Considerations

A hypothetical perfect spoofer could attempt to match the nominal feature distribution; however, real-world spoofing chains are constrained by hardware imperfections such as clock jitter, DAC quantization, and non-linear amplification. The observed deviations are consistent with such physical constraints.

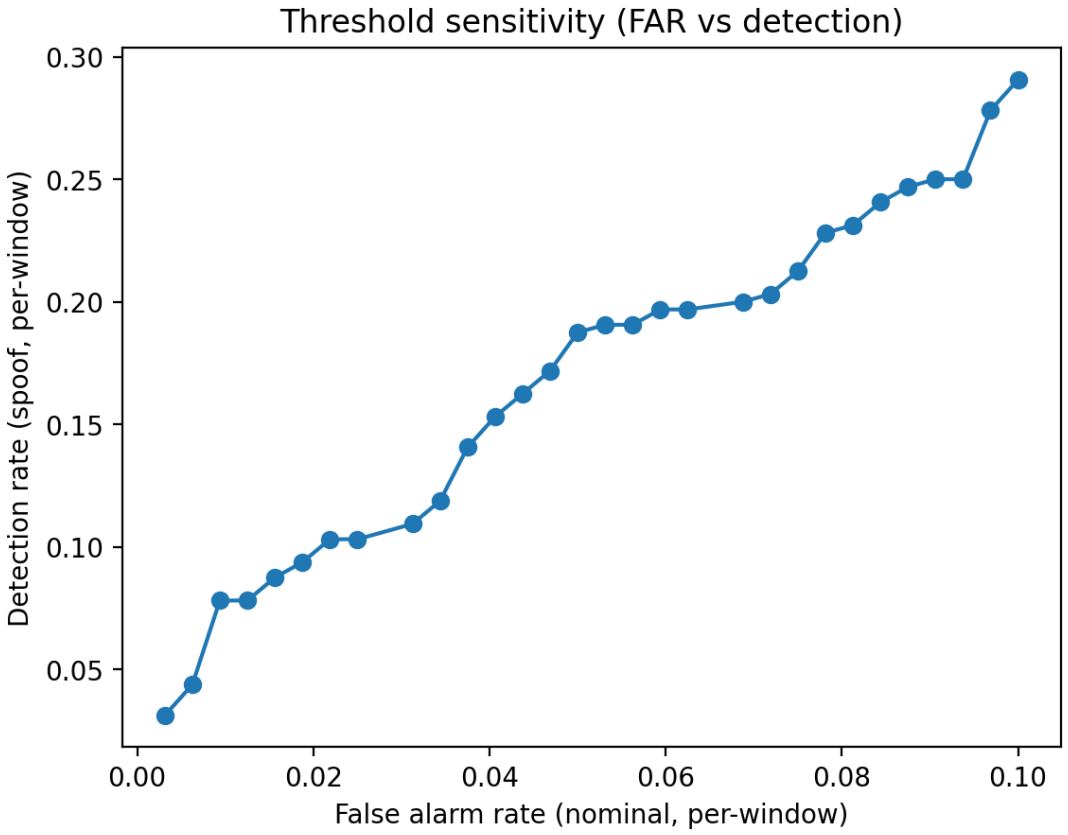

Figure 3: Threshold sensitivity curve showing the trade-off between false alarm rate (nominal windows) and rejection rate under spoofed conditions as the operating threshold is varied.

9 Conclusion

This work empirically invalidates the assumption that spoofed GNSS signals are necessarily indistinguishable from nominal signals at the RF layer. Using a nominal-only statistical test on raw I/Q features, we demonstrate that spoofing can be statistically subtle yet detectable in the spectral domain. While intentionally conservative, the presented baseline establishes a scientifically grounded reference for future spectrum-centric GNSS integrity research.

References

[1] Christopher M. Bishop. *Pattern Recognition and Machine Learning*. Springer, New York, 2006.

[2] Todd E. Humphreys, Boris M. Ledvina, Mark L. Psiaki, Brian W. O'Hanlon, and Paul M. Kintner. Assessing the spoofing threat: Development of a portable gps civilian spoofer. *Proceedings of the ION GNSS Conference*, pages 2314–2325, 2008.

[3] Elliott D. Kaplan and Christopher J. Hegarty. *Understanding GPS: Principles and Applications*. Artech House, Boston, MA, 2nd edition, 2005.

[4] Olivier Ledoit and Michael Wolf. A well-conditioned estimator for large-dimensional covariance matrices. *Journal of Multivariate Analysis*, 88(2):365–411, 2004.

[5] Wenhao Wang, Joonas Sankari, Elena Simona Lohan, and Mikko Valkama. Data-quality and cross-training aspects in gnss rf fingerprinting with raw i/q measurement data. *IEEE Transactions on Aerospace and Electronic Systems*, 2024. URL `https://zenodo.org/records/10401234`. Dataset available on Zenodo.

[6] Peter D. Welch. The use of fast fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms. *IEEE Transactions on Audio and Electroacoustics*, 15(2):70–73, 1967.