

Simulation-Based Embedded-Pattern Calibration for Array-Aided GNSS Spoofing Detection: A NavIC L5 Study

Mathews V. Manoj

Department of Electronics and Communication Engineering, Muthoot Institute of Technology and Science, APJ Abdul Kalam Technological University, Kerala, India

Abstract

GNSS spoofing can mislead a receiver by replacing authentic satellite signals with counterfeit signals that produce a plausible but incorrect navigation solution. Array-based methods can help identify this situation by comparing an antenna array's direction-dependent response with satellite geometry predicted from ephemerides. This study evaluates electromagnetic simulation as a low-cost calibration source for a four-element NavIC L5 array. Embedded element patterns exported from CST Microwave Studio are used in a detector that tracks disagreement between expected and observed array signatures. In the reported simulations, a power-matched attack changed carrier-to-noise density by 3.9 dB and was not detected by the conventional C/N check; the proposed detector responded in 63 s. Reported horizontal position error was 2,400 m without mitigation and 6 m after mitigation. The detector identified the simulated attack in 48 of 48 spoofer geometries and in trials involving one to four transmitters. A benign-condition evaluation reported 0.00% false alarms in its stated nominal cases, while abrupt entry into a severe urban-canyon condition produced a mean false-alarm rate of 1.50% and a worst-run value of 11.97%. All results are simulation-based; validation using a fabricated array and controlled hardware-in-the-loop testing remains necessary.

Keywords: NavIC; GNSS spoofing; antenna arrays; embedded element patterns; electromagnetic simulation; array calibration; hidden Markov model; PNT resilience.

1. Introduction

Satellite navigation receivers estimate position and time from signals transmitted by satellites. A spoofing attack attempts to make a receiver track counterfeit signals and report a false solution. Because authentic satellite signals are weak, a carefully controlled counterfeit signal may not produce an obvious change in a conventional signal-strength indicator. Direction-based array methods provide a complementary defence by checking whether the observed spatial signature agrees with the direction predicted for each satellite [1], [2].

The practical barrier is calibration. Array-based detection depends on a sufficiently accurate model of each element's response, including mutual coupling and element-specific effects. Chamber measurements can provide this information but add cost and require specialist facilities. This work examines whether embedded element patterns generated in electromagnetic simulation can provide a reproducible starting point for a NavIC L5 receiver. The detector and mitigation results discussed below are simulation results, not field validation.

2. Array Design and Electromagnetic Simulation

A probe-fed rectangular patch was designed for the NavIC L5 centre frequency of 1176.45 MHz on 2.0 mm FR-4 (relative permittivity 4.4; loss tangent 0.02). Patch length was adjusted to tune resonance and feed offset to improve matching. Four elements are arranged at 127.5 mm spacing on a 245 mm square ground plane.

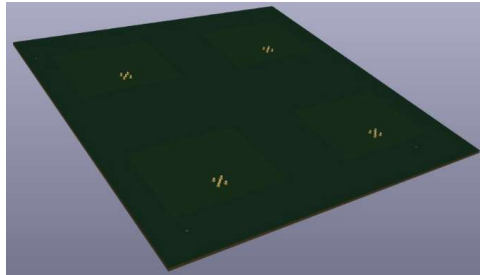


Figure 1. CST model of the four-element NavIC L5 array used in the original project report.

Parameter	Reported value	Parameter	Reported value
Patch width	77.6 mm	Patch length	59.1 mm
Substrate	FR-4, 2.0 mm	Feed offset	15.0 mm
Element spacing	127.5 mm	Board size	245 mm square
Array reflection	-21 dB	-10 dB bandwidth	1.165–1.189 GHz
Mutual coupling	-23 to -27 dB	Radiation efficiency	36.6%

Table 1. Selected antenna and array parameters reproduced from the original report.

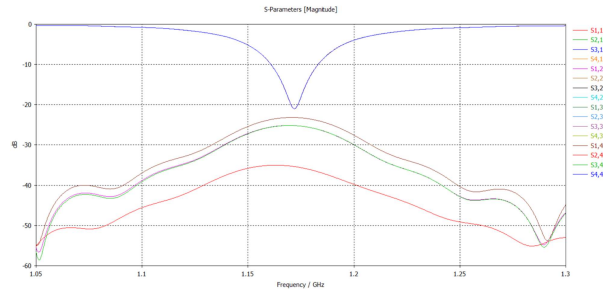


Figure 2. Simulated reflection response and frequency behaviour from the original report.

The four complex embedded element patterns exported from CST are used as the calibration input. These patterns retain modelled element asymmetry and mutual-coupling effects that are not represented by a simple ideal array-factor approximation. The original report states that this difference allowed the simulation to resolve three additional spoofer geometries in the 48-case sweep.

3. Detection and Mitigation Method

For each tracked satellite, the simulated receiver forms a complex snapshot across the four array channels. Satellite ephemerides provide the expected direction, and the embedded patterns provide the corresponding expected array signature. The detector evaluates agreement between the predicted and observed signatures; a sustained reduction in this match is treated as evidence of a spatial inconsistency. Carrier-to-noise density and inter-satellite coherence are retained as secondary observables.

A four-state hidden Markov model estimates nominal, degraded, denied and deceived states over time. Following a deception decision, the simulation estimates the dominant interferer signature from the snapshot covariance matrix and evaluates a spatial-null mitigation approach. This description is limited to the model implemented in the project; it does not establish real-time receiver performance.

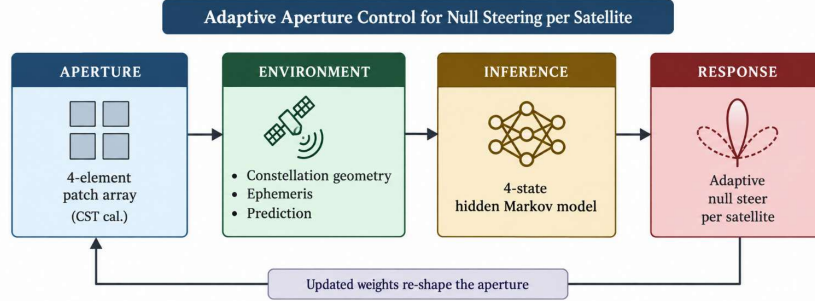


Figure 3. System-level architecture diagram reproduced from the original project report.

4. Simulation Protocol

The evaluation used open orbital elements and simulated array responses. No radio-frequency signals were transmitted. Two attack cases were considered: a crude high-power attack and a power-matched attack intended to keep the conventional signal-strength indicator near its prior level. The study also swept spoofer geometry across the visible hemisphere, tested one to four transmitters, and evaluated benign scenarios including multipath, blockage, fading and an abrupt urban-canyon transition.

5. Results

Metric	Crude attack	Power-matched attack
C/N density change	18.0 dB	3.9 dB
Conventional C/N check	Detected in 6 s	Not detected
Proposed detector latency	4 s	63 s
Position error, no mitigation	3,564 m	2,400 m
Position error, with mitigation	6 m	6 m

Table 2. Reported outcomes for the two simulated attack cases.

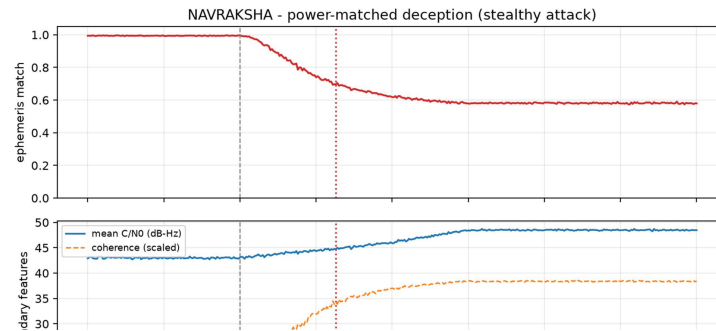


Figure 4. Time-series output for the power-matched deception scenario, reproduced from the original report.

In the power-matched scenario, the conventional C/N check did not trigger, while the proposed detector responded in 63 s. The reported position error fell from 2,400 m without mitigation to 6 m with mitigation. Across the geometry sweep, the detector identified the simulated attack in 48 of 48 cases, with reported latency from 7 to 93 s and a median of 33 s. Detection was reported for all tested cases involving one through four transmitters.

6. Benign Conditions and Discussion

The project report gives 0.00% false alarms for the stated clean-sky, multipath, steady urban-canyon, blockage/fading and multipath-onset cases. The separate abrupt canyon-entry case produced a reported mean false-alarm rate of 1.50% and a worst-run rate of 11.97%. This difference matters: a steady propagation condition and a sudden environmental transition are not equivalent test cases.

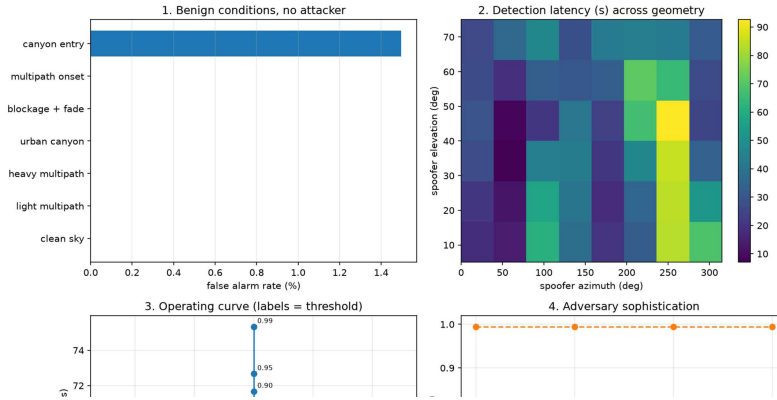


Figure 5. Summary of evaluation results across the tested conditions, reproduced from the original project report.

The results suggest that simulation-derived embedded element patterns can be a useful calibration input for array-aided spoofing detection within the tested environment. They do not demonstrate operational robustness. A physical implementation may differ because of fabrication tolerances, feed and connector effects, platform scattering, temperature variation and installation-dependent coupling. The reported radiation efficiency of 36.6% also indicates a trade-off associated with the selected FR-4 substrate.

The canyon-entry false alarms identify an unresolved design issue. The original report notes that a dwell-time requirement added about 30 s of latency while reducing false alarms only marginally. An adaptive baseline reduced false alarms more substantially but also absorbed the slowly developing multi-transmitter attack. Further work should evaluate adaptation against an independent reference and avoid allowing baseline updates to mask gradual deception.

7. Limitations and Next Steps

This study is simulation-only. It does not include measurements from a fabricated array, conducted hardware-in-the-loop tests or field trials. Performance is conditional on the EM model, orbital data, attack-generation assumptions and decision logic. Next steps are to fabricate and measure the array; compare measured and simulated embedded patterns; conduct lawful, shielded hardware-in-the-loop tests; and publish the exact CSV files, scripts, configuration files and plotting code required to reproduce the tables and figures.

8. Conclusion

This paper evaluated electromagnetic simulation as a calibration source for a four-element NavIC L5 array used in spoofing detection. Embedded element patterns from CST were used to predict array signatures from satellite geometry, and a temporal detector tracked disagreement with simulated observations. In the reported power-matched attack, the conventional C/N check did not trigger, the detector responded in 63 s, and the position error after mitigation was 6 m compared with 2,400 m without mitigation. The detector identified all 48 tested spoofer geometries and all reported one-to-four-transmitter trials. The non-zero false-alarm rate during abrupt canyon entry and the absence of physical validation remain important limitations.

Ethics and safety statement

All results were obtained through simulation. No RF signals were transmitted. Any future physical validation should use lawful, conducted and shielded test arrangements.

Data and code availability

Source code and supporting project files: <https://github.com/MathewsV-Manoj/ISPA-antispoofing-project>.

References

- [1] P. Y. Montgomery, "Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in Proceedings of the ION International Technical Meeting, 2011.
- [2] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, 2016.
- [3] A. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," Journal of Applied Research and Technology, vol. 13, no. 1, 2015.
- [4] Indian Space Research Organisation, IRNSS Signal-in-Space ICD for SPS, Version 1.1, August 2017.