Nick Clark · Published April 25, 2026 · PDF

How to Detect GPS Jamming or Spoofing

GNSS jamming knocks your receiver offline and spoofing quietly walks it to the wrong place, and a receiver watching only its own signal cannot always tell the difference between a clean fix and a fabricated one. This guide describes an architectural approach: treat GPS as one of several independent sensing channels and cross-check them, so a single degraded or forged channel cannot mask a real disruption. It describes an architecture disclosed in U.S. Provisional Application No. 64/049,409, not a shipping library, and it is grounded in the Environmental Disruption inventive step.

What You Are Building

You are building a way to know, at runtime, when the position or time your system reads from GNSS can no longer be trusted, and to say so before a bad fix propagates into a decision. Two distinct failures matter. Jamming raises the noise floor so the receiver loses lock or reports degraded quality: loud, but at least visible. Spoofing is worse, because a spoofer feeds your receiver plausible signals that resolve to a clean-looking fix at a position or time of the attacker's choosing. The receiver reports high confidence and is wrong.

This is a problem for anyone whose actuation depends on position or time and whose environment might be contested or simply noisy: drones and ground robots, port and rail automation, timing-dependent infrastructure, survey and inspection platforms. The

goal here is detection and honest degradation, not magically continuing to navigate through a jammer.

The approach described here comes from the Environmental Disruption inventive step disclosed in U.S. Provisional Application No. 64/049,409. It is an architecture you implement, not a package you install.

Why the Obvious Approaches Fall Short

The usual first moves are worth understanding on their own terms, because they are genuinely useful and the gap is structural, not a matter of any one technique being bad.

Receiver-side quality metrics. Modern GNSS receivers expose carrier-to-noise ratios, automatic-gain-control levels, and lock status. A sudden AGC swing or collapsing C/N0 is a strong jamming indicator. This works well for jamming and is cheap. It is weaker against a competent spoofer, which can present signal levels that look normal.

Cryptographic signal authentication. Some GNSS services add message-level authentication so a receiver can verify that navigation data came from the real constellation. This raises the bar for spoofing meaningfully. It depends on the signal and receiver supporting it, does nothing about jamming, and does not by itself confirm that the geometry your receiver solved is physically consistent with where you actually are.

Consistency checks against inertial or other onboard sensors. Comparing GNSS against an inertial measurement unit or odometry catches many spoofs that try to teleport the fix. This is one of the most effective single-box defenses. Its limits are that the check lives inside one unit, an attacker who ramps the spoof slowly can stay within the inertial drift envelope, and the sensors compared often share failure conditions.

The common thread: each of these watches a single medium or a single unit. A spoofer only has to be convincing on the one channel you are watching. The structural fix is to make the position claim answerable to several physically independent channels at once, with distinct failure modes, so that fabricating agreement across all of them is far harder than fooling any one.

The Architecture

The disclosed approach treats detection as a composition of primitives rather than a single spoofing classifier. The relevant pieces from the filing are the environmental disruption sensing primitive (its departure detector, classifier, corroboration evaluator, source attribution, active probe, and spoofing detection), cross-medium composite detection, and the position and time primitives that fuse GNSS with mesh-derived and other external sources.

Baseline and departure. The foundation is a governance-characterized baseline for each sensed field, established across defined spatial, temporal, and operational conditions. A departure detector flags when a sensed field deviates from that baseline beyond policy-defined thresholds. In GNSS terms, the sensed field is the radio-frequency environment: the baseline captures what the RF field and the receiver's own reported quality look like under normal conditions, and a departure is a deviation from it. The spec frames radio-frequency disruption sensing as analyzing deviations in a radio-frequency field within a coverage volume. Jamming shows up here directly as an RF-field departure.

Classification, not a binary alarm. A disruption classifier maps each detected departure to a policy-defined disruption class, where a disruption is defined broadly as any departure from baseline attributable to a source, and that source may be adversarial, accidental, environmental, or instrumental. This matters: an RF departure could be a jammer, or it could be a nearby transmitter or weather. The architecture is built to attribute cause, not just raise a flag.

Multi-source corroboration. A corroboration evaluator aggregates departure detections across multiple sensing agents and produces corroboration scores. One receiver seeing an anomaly is a weaker signal than several independent agents in the area agreeing. This is where detection stops being a property of one box.

The spoofing-detection mechanism. The filing calls out a dedicated spoofing-detection mechanism that evaluates three things to separate genuine field measurements from adversarially fabricated ones: signal-integrity attestation, temporal coherence, and spatial coherence. Spatial and temporal coherence are the levers that catch a clean-looking-but-false fix: a spoofed position that is internally plausible but inconsistent with where independent channels place you in space, or with an independently held time reference, fails coherence even when its signal quality looks fine.

Cross-medium composite detection. This is the core of the structural answer. Disruption observations from two or more physically distinct field classes are combined into composite determinations that no single field class could produce alone. Each participating field class is governed by a physically distinct sensing apparatus with distinct failure modes, which makes the composite result robust to single-medium sensor failure, single-medium jamming, and single-medium spoofing. The filing gives composite signatures as examples, including a radio-frequency-and-optical signature in which a coordinated jamming event produces concurrent RF amplitude departures and optical-lidar return anomalies. The general principle is orthogonal physical channels corroborating each other.

Independent position and time references. The filing discloses a mesh-derived coordinate primitive and a mesh-derived time primitive that produce position and time cooperatively from ranging and timing exchanges among agents, without dependence on a central positioning or timing authority. Both include an evidential-fusion mechanism that combines the mesh-derived estimate with externally sourced estimates, explicitly including satellite navigation and satellite time, through the composite admissibility evaluator of Chapter 4. Both include adversarial-rejection mechanisms

that reject spoofed, injected, or otherwise inadmissible range or time observations. Practically, this gives you a position and time you can hold that does not come from GNSS, against which a GNSS fix can be checked. When the two disagree beyond their propagated uncertainty, that is your spatial or temporal coherence failure with teeth behind it.

Active probing to resolve cause. When a passive departure is ambiguous, a governed active-probe mechanism can emit a credentialed probe signal chosen so its expected response differs across the competing cause hypotheses, then update those hypotheses from the response. The spec gives radio-frequency active probes that analyze backscatter and channel-state responses to distinguish, among other things, jammers from propagation artifacts. Probing is gated by an admissibility evaluator covering spectrum licensing, mission interference, adversarial awareness, and power budget, and suppressed probes are still recorded.

Graduated response and lineage. Output is not a bare alarm. A graduated-response generator produces a response proportional to the classified disruption and its authority, and a lineage recorder records every detection, classification, attribution, probe, and consequence, so a detection event can be reconstructed after the fact.

How to Approach the Build

You are implementing primitives, not importing them. A workable order:

1. Instrument the RF channel and characterize a baseline. Pull the quality signals your receiver exposes (C/N0 per satellite, AGC, lock state) and record what normal looks like across your real operating conditions. Your departure detector fires when these leave the characterized envelope. This alone gives you competent jamming detection.
2. Stand up at least one position or time source independent of GNSS. This is the load-bearing step for spoofing. It may be the mesh-derived coordinate or time primitive from the filing, or an inertial, visual-inertial, or ranging source you already have, as

long as it does not share GNSS's failure mode. The point is a reference to cross-check against.

3. Implement the coherence tests. Continuously compare the GNSS-derived position and time against the independent reference, propagating uncertainty on both sides so the threshold is meaningful rather than a fixed number. A disagreement beyond combined uncertainty is a spoofing candidate. This realizes the spatial-coherence and temporal-coherence tests the spec names.
4. Emit structured observations, then corroborate. Have each detector emit a departure observation with its evidence rather than a local boolean, and feed them to a corroboration evaluator that scores agreement across independent agents and across field classes. An illustrative, spec-faithful interface sketch, not shipping code:

```
DepartureObservation {
  field_class      // e.g. radio_frequency, optical, position, time
  baseline_ref     // which characterized baseline this departs from
  magnitude        // how far past threshold
  evidence         // raw metrics supporting the departure
  authority_cred   // who is asserting this
}
```

   The composite engine correlates these in time and space and maps the correlated set to a composite class. A concurrent RF departure plus an optical-return anomaly is the multi-spectrum-denial signature from the filing; an RF-quiet position-versus-reference disagreement points at a stealthier spoof.

5. Add active probing only where admissible. If passive evidence cannot separate jammer from artifact, and you hold valid spectrum authorization and the power budget, an RF probe can help. Gate it behind an admissibility check and record the decision either way.

6. Make the output graduated and logged. Translate corroborated determinations into proportional responses (flag, derate reliance on GNSS, hold last trusted reference, hand off) rather than a single kill switch, and record the full chain for post-incident review.

What This Does Not Give You

This is an architecture, not a drop-in library. Nothing here is downloadable, benchmarked, or production-proven, and there is no package that "just works." You implement the detectors, the baselines, the fusion, and the responses yourself, and the quality of your baseline characterization and the true independence of your secondary channels determine how well it performs.

It does not let you navigate through a jammer; it lets you detect the condition and degrade honestly. Spoofing detection depends entirely on having a reference that does not share GNSS's failure mode. If every channel you fuse ultimately derives from the same satellite signal, you have not achieved the independence the architecture relies on, and a spoofer that also spoofs those derived channels defeats the check. The filing does not state detection rates, latencies, or guarantees, and neither should any implementation built from it. Cross-medium composite detection raises confidence through independent corroboration; it does not promise a false-positive or false-negative bound.

Disclosure Scope

The approach described in this guide is disclosed in U.S. Provisional Application No. 64/049,409. This guide is educational: it explains an architectural approach so a skilled developer can understand and build it. It is not a warranty, not a benchmark, and not an offer of software, and it does not grant any license. Where it references third-party technologies such as GNSS signal authentication or inertial navigation, those are

described neutrally and for context only. Every statement about how the disclosed approach works is grounded in that filing; where the filing is silent on a number or guarantee, this guide makes no such claim.

Environmental Disruption (/environmental-disruption)

All 40 steps → (/inventive-steps)

Cross-medium signatures. Governed active probing. Adversarial-aware sensing.

Provisional application

PRIMARY TECHNICAL DISCLOSURE

- Environmental Disruption: Cross-Medium Sensing With Governed Active Probing (/articles/environmental-disruption-cross-medium-sensing-with-governed-active-probing)

SECONDARY TECHNICAL

- Multi-Medium Environmental Sensing (/articles/environmental-disruption/multi-medium-sensing)
- Baseline Departure Detection (/articles/environmental-disruption/baseline-departure-detection)
- Governed Active Probe (/articles/environmental-disruption/governed-active-probe)
- Spectrum-Licensing-Gated Probing (/articles/environmental-disruption/spectrum-licensing-gating)
- Adversarial Awareness in Governed Active Probing (/articles/environmental-disruption/adversarial-awareness-cost)
- Cross-Medium Composite Signatures (/articles/environmental-disruption/cross-medium-composite-signatures)
- Multi-Source Corroboration (/articles/environmental-disruption/multi-source-corroboration)
- Lineage Evidence Admissibility (/articles/environmental-disruption/lineage-evidence-admissibility)
- Graduated Environmental Response (/articles/environmental-disruption/graduated-response)

APPLICATIONS · GENERAL

- Critical Infrastructure Protection: Cross-Medium Environmental Disruption Detection for the Power, Water, and Communications Grid (/articles/environmental-disruption/critical-infrastructure-protection)

- Multi-INT Fusion for Contested Defense ISR: A Multi-Medium Sensing Architecture (/articles/environmental-disruption/defense-isr-environmental)
- Multi-Medium Disaster Monitoring: Cross-Hazard Sensor Fusion for Earthquake, Wildfire, and Flood Early Warning (/articles/environmental-disruption/disaster-monitoring-multi-medium)
- Multi-Source Earthquake Detection and Early Warning Without Trusting Any Single Sensor (/articles/environmental-disruption/earthquake-multi-source-detection)
- Maritime Domain Awareness: Multi-Medium Sensor Fusion With Verifiable Evidence Lineage for Dark-Vessel and IUU-Fishing Enforcement (/articles/environmental-disruption/maritime-domain-awareness)
- Multi-Medium Wildfire Detection: Cross-Modality Sensor Fusion for Early Ignition Alerts (/articles/environmental-disruption/wildfire-detection-multi-medium)
- CISA Critical Infrastructure Cybersecurity Compliance: Cross-Modality Detection and CIRCIA Incident Reporting (/articles/environmental-disruption/cisa-eo-13800)
- GNSS Jamming and Spoofing Detection: Architecting FCC and EO 13905 PNT Resilience (/articles/environmental-disruption/fcc-gnss-protection)
- FCC Part 15 Unlicensed RF Compliance: Adversarial-Resistant Sensing for DFS and 6 GHz AFC (/articles/environmental-disruption/fcc-part-15-unlicensed)

APPLICATIONS · SPECIFIC

- Anduril Sentry Tower vs Multi-Medium Credentialed Disruption Sensing (/articles/environmental-disruption/anduril-sentry-tower)
- Dedrone Alternative: Governed Multi-Medium Counter-UAS Detection Beyond Single-Vendor Fusion (/articles/environmental-disruption/dedrone-counter-uas)
- HawkEye 360 Alternative: Multi-Medium Credentialed Sensing Beyond RF-Only Geolocation (/articles/environmental-disruption/hawkeye-360-rf)
- Capella Space SAR vs governed multi-medium fusion (/articles/environmental-disruption/capella-sar)
- Maxar Imagery vs Governed Multi-Medium Disruption Sensing (/articles/environmental-disruption/maxar-imagery)
- Planet Labs Imagery vs Multi-Medium Governed Sensing (/articles/environmental-disruption/planet-labs-imaging)
- Slingshot Aerospace vs Governed Multi-Medium Space Sensing (/articles/environmental-disruption/slingshot-aerospace)
- Spire Global vs Governed Multi-Medium Environmental Disruption Sensing (/articles/environmental-disruption/spire-rf-monitoring)
- Cognex Machine Vision vs Governed Multi-Medium Sensing (/articles/environmental-disruption/cognex-machine-vision)

– Keyence Vision Sensors vs Governed Multi-Medium Sensing (/articles/environmental-disruption/keyence-vision-sensors)

Environmental Disruption overview → (/environmental-disruption)