Nick Clark · Published April 25, 2026 · PDF

How to Detect Environmental Threats Using Multiple Sensing Mediums

If you build perception for autonomous vehicles, robotics, or critical infrastructure, you have felt the single-channel problem: one jammer, one spoofed return, or one blinded sensor can hide a real event from your whole stack. This guide teaches an architecture for detecting disruption by fusing several physically independent sensing mediums so no single degraded or fabricated channel can mask a threat. The approach described here is disclosed in U.S. Provisional Application No. 64/049,409 as the Environmental Disruption inventive step; it is a design you implement yourself, not a shipping library.

What You Are Building

You are building a detector that decides whether the physical environment around an autonomous unit or a fixed installation has been disrupted, and that stays trustworthy even when one of its input channels is defeated. The word "disruption" here is deliberately broad. In the disclosed architecture it means any departure of a sensed field from its characterized baseline, whatever the cause: an adversary jamming a band, an accidental radio-frequency source, a weather event, or a failing instrument. The point of the design is that you do not have to know the cause up front to notice that something changed and to decide how confident you are that it is real.

The search that brings people here is usually some version of "how do I detect environmental threats using multiple sensing mediums," and the intent behind it is almost always the same frustration: a detector wired to a single medium is only as honest as that medium. A GPS-denial detector that watches only the radio-frequency band cannot tell you whether the drone it should have seen is really gone or merely silent. What you actually want is a detector whose confidence rises when several physically distinct channels agree, and whose blind spots do not all fail together.

This matters most to teams shipping autonomous navigation, security and intrusion sensing at fixed sites, and any operation where a missed event has real cost. The architecture below is medium-agnostic by construction, so it applies whether your channels are radar and lidar, or seismic and acoustic, or thermal and chemical.

Why the Obvious Approaches Fall Short

The conventional building blocks are real and useful, and this guide does not claim they are broken. Intrusion-detection systems, jamming detectors, spoofing detectors, and generic anomaly detectors all do a genuine job within their scope. The structural gap is in how they are scoped, not in whether they work.

First, most deployed detectors are narrowly bound to a single medium. A radio-frequency jamming detector reasons about the radio-frequency band; an optical anomaly detector reasons about pixels. Each is competent alone, but each shares its failure mode with everything downstream of it. If the medium is defeated, the detector built on it is defeated with it, and the rest of the system has no independent reason to doubt the silence.

Second, single-source detectors typically emit an unstructured alarm: a flag, a threshold crossing, a log line. An alarm is a terminal event. It does not carry who observed it, under what authority, with what corroboration, or with what evidence a later reviewer

could use to reconstruct the decision. When two such alarms disagree, there is often nothing structural to reconcile them with.

Third, and most importantly for threat work, a single channel cannot by itself distinguish a genuine measurement from a fabricated one. A spoofer's whole job is to make one channel lie convincingly. If that channel is the only witness, the lie stands.

The obvious fix, "just add more sensors," is necessary but not sufficient. Bolting a second medium onto a system that still treats each channel as an isolated alarm gives you two alarms that disagree and no principled way to combine them. What is missing is a shared structure in which observations from orthogonal physical channels are expressed the same way, correlated against each other, and combined into a single determination that is stronger than any input. That shared structure is the architecture.

The Architecture

The disclosed approach treats environmental disruption sensing as a single architectural primitive that is deliberately independent of any specific field type. The same mechanism operates across radio-frequency, optical, acoustic, thermal-infrared, magnetic, electric, seismic, barometric, chemical, radiological, and gravitational field classes, and admits new field classes through configuration rather than redesign. The design rests on a small number of cooperating parts.

A characterized baseline per field class. For each sensed field, you establish a baseline of what that field looks like under defined spatial, temporal, and operational conditions. A departure detector then identifies readings that cross defined departure thresholds against that baseline. This is the same baseline-and-deviation idea the disclosure applies to fixed sensing devices, where a device maintains a stored model of its coverage volume in a quiescent state and computes deviations from it. The baseline is what makes "disruption" a measurable thing rather than a guess.

A classifier and a source-attribution step. A detected departure is mapped to a disruption class. A separate attribution step tries to localize or identify the source, through multi-sensor triangulation, signature matching, or another chosen technique. Classification and attribution are kept distinct so that you can be confident something changed while still uncertain about who caused it.

Cross-medium composition, which is the heart of the design. Rather than letting each medium raise its own alarm, a cross-medium composite detection mechanism ingests disruption observations from two or more field classes and looks for temporal, spatial, and causal correlations among them. A composite-signature library holds patterns for events that are known to leave a characteristic mark across several mediums at once, and a composite-classification engine maps a correlated set of single-medium observations to a composite class. The disclosure gives concrete composite signatures, including: a radio-frequency-and-optical signature where a coordinated jamming effort shows up as concurrent radio-frequency amplitude departures and optical-lidar return anomalies; a radio-frequency-and-acoustic signature where a small aerial intrusion shows up as both radar-return departures and rotor-acoustic signatures; a thermal-and-chemical signature for combustion; and a seismic-and-acoustic signature for heavy equipment, structural failure, or explosive events.

The reason this composition is worth building is stated plainly in the disclosure: because each participating field class is sensed by a physically distinct apparatus with distinct failure modes, a composite determination is robust to single-medium sensor failure, single-medium jamming, and single-medium spoofing. Corroboration across orthogonal physical channels raises confidence above what any single medium can produce on its own. That is the whole thesis of the search query, made structural.

A spoofing-detection step that asks whether a measurement is genuine. The primitive includes a spoofing-detection mechanism that applies signal-integrity attestation, temporal-coherence tests, and spatial-coherence tests to distinguish

genuine field measurements from adversarially fabricated ones. This is what lets the system doubt a channel that is technically reporting data.

A governed active-probe step for when passive listening is ambiguous. When several cause hypotheses could explain the same departure, the architecture can emit a credentialed probe into the sensed field, chosen so that the expected responses differ as much as possible across the competing hypotheses, then update the hypothesis probabilities from what comes back. Probing is gated by an admissibility check covering spectrum licensing, interference with other operations, how much the probe reveals to an adversary, and power budget; probes that fail the check are suppressed and the suppression is recorded. Active probing is what moves the system from "something is wrong" toward "here is which explanation the evidence favors."

Graduated response instead of a binary alarm. The output is not alarm-or-nothing. Detection feeds a graduated response proportional to the classified disruption and its authority. Downstream, this is the difference between silently ignoring an event and slamming an autonomous unit to a stop; the response scales with how bad and how certain the situation is.

Lineage on everything. Each detection, classification, attribution, probe, response, and downstream consequence is recorded so the event can be reconstructed later. The composite output itself records the contributing single-medium observations, the correlation evidence, and the composite classification. This is what makes a determination auditable rather than a vanished flag.

Underneath, the disclosure frames each disruption reading as a governed observation carrying an authority credential, a spatial and temporal reference, and a payload, and it combines observations through a multi-factor evidential weighting that accounts for authority, staleness, the reliability of the contributing modality, and the contributor's track record. The practical takeaway is that you weight channels by how much they deserve to be believed, rather than counting votes.

How to Approach the Build

You implement this yourself. The steps below are the order the architecture suggests, not a package you install.

1. Enumerate your independent mediums and be honest about independence. List the field classes you can actually sense, then ask which ones fail together. Two radios on the same antenna are not independent. Radar and acoustic are. The strength of every later step depends on this being real physical independence, because that is the only thing a shared jammer or spoofer cannot cheaply defeat across all channels at once.

2. Build a baseline and a departure detector per medium. For each channel, define what "quiescent" means under your operational conditions and choose a deviation function against it. The disclosure lists options that map to how different the mediums are: simple subtraction or normalized difference, a statistical test, a spectral-distance metric, a point-cloud-registration residual, or a learned anomaly detector. Each departure should carry, at minimum, a deviation type, an estimated position, a timestamp, and a confidence.

3. Normalize every medium's output into one observation shape. This is the step teams skip and regret. Before you can correlate radar against acoustic, both must speak the same observation vocabulary. Define one structure, illustrative only and faithful to the disclosed fields:

```
DisruptionObservation {
  fieldClass       // e.g. radio_frequency | acoustic | thermal
  deviationType    // classifier output for this medium
  position         // where, relative to the sensor
  time             // when
  confidence       // this medium's own certainty
  authority        // who is asserting it
}
```

Treat this as a sketch to adapt, not a schema to copy.

4. Correlate across mediums by space, time, and cause. Feed the normalized observations into an aggregator that groups observations from different field classes pertaining to the same region and window, then tests whether their co-occurrence matches a known composite pattern. Start with a small composite-signature library drawn from the disclosed examples that fit your domain, and grow it from real incidents.

5. Add the spoofing and probe steps where the stakes justify them. Apply integrity, temporal-coherence, and spatial-coherence tests to any channel an adversary would target. Where passive observation leaves genuine ambiguity, design a probe whose response separates your hypotheses, and put an admissibility gate in front of it before you ever emit into the world.

6. Make the output graduated and logged. Map composite classifications to a proportional response, not a single alarm bit, and record the contributing observations and correlation evidence with every determination so you can reconstruct it later.

A useful sequencing note: steps 1 through 4 already deliver the core benefit the search intent asks for, corroboration across independent channels. Steps 5 and 6 harden it against a deliberate adversary and make it auditable.

What This Does Not Give You

This is an architecture, not a drop-in library, and there is nothing to download. You are implementing the mechanisms yourself against your own sensors, and every value that matters in practice, your thresholds, your composite signatures, your response mapping, your weighting factors, is yours to define. The disclosure describes the structure and gives named examples; it does not ship tuned parameters, and it states no benchmark numbers or performance guarantees, so neither does this guide.

The corroboration benefit is only as real as the physical independence of your channels. If your mediums share an antenna, a power rail, a clock, or a processing bottleneck, a single failure can take several of them down together and the composite determination inherits that weakness. The architecture assumes distinct apparatus with distinct failure modes; it cannot manufacture independence you did not build in.

It also will not, by itself, tell you the cause of a disruption. By design it separates noticing a departure from attributing it. Attribution and the active-probe step narrow the hypotheses, but the disclosure frames a disruption as cause-agnostic on purpose, and you should treat confident attribution as a further step you engineer, not a free output.

Finally, this is a disclosed method from a patent filing, not a production-proven product. It has not been presented here as benchmarked or productized. Where you have only one honest medium, or where your event leaves no cross-medium signature, multi-medium composition has nothing to compose and the design offers no magic.

Disclosure Scope

The architecture described in this guide, including cross-medium composite disruption detection, the governed active-probe mechanism, and the spoofing-detection and graduated-response elements, is disclosed in U.S. Provisional Application No. 64/049,409 as the Environmental Disruption inventive step. This guide is educational.

It explains an approach a developer can build and is not a warranty, a specification, or an offer of software, and nothing here should be read as a promise of performance, fitness, or freedom to operate.

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)