Multi-Medium Disruption Sensing

by Nick Clark | Published April 25, 2026

What the Eight-Medium Sensing Set Specifies

The architecture admits credentialed observations from sensors operating across eight physical media: RF (spectrum monitors, SDRs, protocol analyzers), optical (cameras, photometric arrays, lidar), acoustic (microphones, hydrophones, ultrasonic arrays), thermal (FLIR, IR cameras, infrared spot sensors), magnetic (magnetometers, coil arrays), seismic (geophones, accelerometers, fiber-optic distributed acoustic sensing), chemical (gas sensors, particle counters, spectrometers), and radiological (Geiger counters, scintillation detectors, neutron detectors).

Each contribution carries the standard credentialed-observation structure: signing authority, declared medium, declared modality and uncertainty, sensor identifier, temporal and spatial scope. The composite admissibility evaluator consumes contributions across all media simultaneously.

Why Single-Medium Sensing Cannot Distinguish Failure From Attack

A GPS-receiver position glitch could be: multipath in an urban canyon, satellite geometry, ionospheric scintillation, deliberate spoofing, or a hardware failure. Single-

medium sensing cannot distinguish among these candidates. Each cause has different operational consequences (ignore, wait, switch to fallback, raise alert, harden response), and the same observation appears the same way to the receiver.

Cross-medium correlation produces diagnostic information that single-medium observation does not. Adversarial GPS spoofing typically correlates with anomalies in adjacent RF bands, unusual radar patterns, or coordinated optical events. Pure environmental disruption tends to correlate across media in patterns reflecting natural causes (weather correlates with optical attenuation + RF refraction + acoustic propagation changes). The correlation pattern itself attributes the cause.

How the Composite Signature Library Operates

Each candidate cause has a credentialed composite signature: the expected observable pattern across multiple media when this cause is operating. The signatures are published by credentialed authorities (FCC for spectrum-related signatures, defense authorities for adversarial signatures, meteorological authorities for environmental signatures) and consumed by the operating system's admissibility evaluator.

When observations across media correlate with a known signature, the architecture produces a credentialed attribution observation: the cause is identified, the supporting cross-medium evidence is recorded, and downstream consumers can respond appropriately. When observations don't match a known signature, the architecture produces a 'novel disruption' observation that propagates to the credentialing authorities for analysis and potential signature library expansion.

What This Enables for Adversarial-Aware Operation

Defense and commercial-drone operators in contested environments gain structural diagnostic capability. Single-medium hardening produces resilience against specific attacks but cannot distinguish attack types or environmental causes; multi-medium sensing produces the diagnostic information that operational response actually requires.

Critical-infrastructure operators (utilities, ports, hospitals, transportation) face increasingly sophisticated multi-vector attacks. Multi-medium sensing produces the cross-vector visibility that single-vector security tooling cannot. The patent positions the primitive at the layer adversarial-aware operation requires as multi-vector attacks become operational reality.