Multi-Source Adversarial Attribution

by Nick Clark | Published April 25, 2026

What Multi-Source Corroboration Specifies

The architecture treats single-sensor disruption observations as provisional input rather than as final attribution. An observation produced by one sensor (a GPS receiver detecting position anomaly, an SDR detecting band-edge interference) is admissible into the disruption-modeling pipeline but does not by itself constitute attributed cause.

Attribution requires aggregation across multiple credentialed sensors with corroborating evidence. The aggregator (a credentialed analysis function) consumes the contributing observations, evaluates their consistency, and produces a credentialed attribution observation. The attribution observation references the contributing sensors, the supporting evidence, and the credentialing authority that signs the attribution itself.

Why Authority Without Aggregation Is Insufficient

A single sensor's claim 'this is jamming' or 'this is GPS spoofing' has limited operational and legal weight. Operational response based on a single-sensor claim is fragile — sensor failure, miscalibration, or single-sensor adversarial attack can

produce false attribution that drives expensive or harmful response. Legal response based on a single-sensor claim has evidentiary weakness that adversarial counsel can exploit.

Multi-source corroboration solves both. Operational response can require corroboration thresholds appropriate to the consequences of action. Legal response gains evidentiary foundation when multiple credentialed sensors corroborate. The architecture supports the operational and legal foundations that single-source attribution lacks.

How Corroboration Composes With Composite Signatures

Multi-source corroboration and composite-signature matching are complementary mechanisms. Composite signatures specify the cross-medium pattern that characterizes a cause. Multi-source corroboration specifies the cross-sensor consistency that supports the attribution.

An operating attribution requires both: the observed observations match a credentialed signature (the cross-medium pattern), and the observations come from multiple credentialed sensors with consistent reporting (the cross-sensor corroboration). When both criteria are met, the attribution observation is signed by the credentialed attribution authority. When one or both criteria fail, the observation propagates as 'partial-attribution' or 'novel-disruption' rather than as confident attribution.

What This Enables for Legally Sound Attribution

Defense operations gain attribution that supports legal-grade response. Counter-UAS engagement, counter-jamming actions, attribution-based restrictions on potential adversaries all require attribution that survives legal review. Multi-source

corroboration with credentialed attribution authority produces attribution that meets the standard.

Civilian critical-infrastructure attribution (cyber-physical attack attribution, GPS spoofing attribution for liability allocation, RF interference attribution for spectrum-license enforcement) gains the same legal foundation. The patent positions the primitive at the layer that legally-sound adversarial attribution requires across defense and civilian use cases.