Anti-Spoofed Observation Rejection

by Nick Clark | Published April 25, 2026

What Anti-Spoofed Rejection Specifies

Observation admissibility evaluation includes spoofing-resistance checks: credential validity (the contributing-unit signature verifies against published keying material), timing consistency (the observation timestamp falls within the expected window relative to mesh time), modality plausibility (the observation falls within physical constraints for the declared modality), and cross-modality consistency (the observation agrees with parallel observations from other modalities).

Observations failing any check are recorded as credentialed rejection events and excluded from the position solution. The rejection itself enters lineage; downstream audit can reconstruct what was rejected and why.

Why Spoofing Defense Operates Structurally

GNSS spoofing has produced operational incidents across maritime, aviation, and critical-infrastructure contexts. Single-modality spoofing defenses (signal-quality monitoring, multi-antenna spatial filtering) work against some spoofing patterns and fail against others.

Multi-modality cooperative ranging produces structural spoofing resistance. A spoofer would need to defeat multiple modalities simultaneously while producing

observations that pass credential, timing, and cross-modality checks. The attacker's burden is structural rather than implementation-dependent.

How Rejection Composes With Solution

The admissibility evaluator runs each incoming observation through the rejection checks. Observations passing all checks enter the solver; observations failing checks enter a rejection record with declared rejection reason.

The rejection record is governance-credentialed. The evaluator signs the rejection, the rejection criteria are declared, and the record enters lineage. Downstream audit can identify systematic rejection patterns that may indicate sustained adversarial interference.

What This Enables for Contested Positioning

Defense operations in contested electromagnetic environments gain positioning that survives sustained spoofing pressure. The architecture supports operation profiles where adversarial interference is expected rather than exceptional.

Civilian operations gain the same structural protection. Maritime and aviation positioning under increasing GNSS-spoofing prevalence can rely on multi-modality cooperative ranging where single-modality positioning becomes operationally untenable.