DDoS-Resilient Positioning Through Mesh Cooperation

by Nick Clark | Published April 25, 2026

The Threat Landscape

Documented incidents: Black Sea spoofing (2017), Eastern Mediterranean GPS-denial during regional conflicts, Strait of Hormuz incidents, ongoing Northern European GPS-interference, U.S.-Mexico border RF-environment incidents. The pattern is increasing in frequency and sophistication.

Single-modality positioning systems are structurally vulnerable. Multi-modality cooperative ranging produces structural alternative.

What the Mesh Stack Provides

UWB time-of-flight, lidar reflection, radar, optical fiducial range, RFID proximity, BLE RSSI, magnetic dipole, GNSS pseudorange (when available), inertial integration, visual SLAM correspondence. Each modality contributes credentialed observations.

Successful adversarial operations against the stack would require coordinated denial across multiple modalities while passing credentialing, timing, and cross-modality consistency checks. The attacker burden is structural rather than implementation-dependent.

Operational Resilience

Maritime operations gain structural defense in spoofing-prone regions. Aviation operations gain GPS-denial-resilient positioning. Defense operations gain contested-environment-survivable positioning. Emergency-response operations gain disaster-area positioning resilience.