ONE-PAGE SUMMARY

NavSentinel: A Resilient and Unspoofable GNSS Receiver

Vision Statement: What if we could make GPS-dependent transportation systems immune to spoofing cyber-attacks by fielding a receiver that identifies counterfeit signals within seconds and maintains continuous high-precision positioning and timing, even under sustained attack?

PROPOSAL INFORMATION

Project Title: NavSentinel: A Resilient and Unspoofable GNSS Receiver

Applicant Type: Entity / Organization

Team Lead: Dr. Samer Khanafseh, Principal & Managing Director, TruNav LLC

Team Members: Dr. Boris Pervan, Professor, Mechanical & Aerospace Engineering, Illinois Institute of Technology (Co-PI)

Topic Area(s): Enabling and Foundational Technologies

ABSTRACT

Modern transportation — commercial aviation, autonomous vehicles, maritime vessels, and precision agriculture — depends on GPS/GNSS for positioning, velocity, and timing. Yet GPS signals are open, unauthenticated, and received below the noise floor, making them inherently vulnerable to spoofing: the broadcast of counterfeit satellite signals that steer a receiver to a false position or time. Once theoretical, spoofing is now an operational crisis. Thousands of commercial flights have reported GPS anomalies over conflict zones, and documented incidents have placed aircraft miles off course. Current receivers can only detect-and-deny: they discard GPS entirely, leaving the platform blind, and remain brittle against more sophisticated, evolving threats.

NavSentinel turns spoofing from an undetectable threat into a measurable and correctable signal inconsistency between GNSS signals and physical motion. It is a software-defined, single-antenna GNSS receiver architecture that detects, isolates, and eliminates spoofed signals in real time — without additional antennas, without direction-of-arrival hardware, and with only a low-cost commercial inertial sensor. The architecture is designed for integration by receiver OEMs as firmware on SDR/FPGA platforms, enabling broad adoption across aviation, defense, and autonomous vehicle markets.

NavSentinel integrates three innovations. First, TrustNav, an Optimal INS Monitor, cross-checks GPS position against the motion solution from a low-cost inertial measurement unit (IMU). Because a spoofer cannot simultaneously falsify both the GPS signal and the vehicle's physical motion, any inconsistency triggers an alert within seconds, with false-alarm probability $\leq 10^{-5}$ and missed-detection probability as low as 10^{-7}. Second, a signal-processing layer separates authentic satellite signals from the overlaid counterfeit — recovering a true position estimate even while the spoofer is active. Third, a Dual Kalman Filter fuses both outputs into a continuously navigated, integrity-assured solution. Together, these form a detect–separate–track pipeline with sub-decimeter spoofing sensitivity using a single antenna.

Each component has been independently validated. TrustNav was funded by the U.S. Air Force (SBIR Phase II, 2022–2024) and its software prototype was delivered to and evaluated on the Air Force's GNSSTA platform. The signal-separation technique, based on the Complex Cross-Ambiguity Function (CCAF), is published in IEEE Transactions on Aerospace and Electronic Systems (2025) and validated against live spoofing signals. A U.S. non-provisional patent (Application No. 19/223,149) is filed on TrustNav.

Under this Stage 2 award, the team will develop and validate an FPGA software prototype, conduct hardware-in-the-loop and field testing against live spoofing environments (including national interference exercises such as NavFest and PNTAX), and advance regulatory engagement for aviation certification. The 30-month program totals approximately $1.4M in three phases: algorithm fusion and optimization (months 1–6, $300K); FPGA prototyping and SDR implementation (months 7–18, $650K); and field validation and pilot integration (months 19–30, $450K). Revenue will be generated through licensing agreements with avionics and defense OEMs.

NavSentinel's potential impact spans every GPS-dependent sector. By making sophisticated spoofing detectable and rejectable with commodity hardware and a firmware update, it closes the single largest open gap in global navigation security today — protecting lives, critical infrastructure, and national security assets that depend on trusted GPS.