NavSentinel: A Resilient and Unspoofable GNSS Receiver

*"What if we could **make GPS-dependent transportation immune to spoofing** — detecting counterfeit signals in seconds and navigating through the attack?"*

Team Lead: Dr. Samer Khanafseh, TruNav LLC | **Team Member:** Dr. Boris Pervan, Illinois Institute of Technology | **Topic Area:** Enabling and Foundational Technologies

Problem & Objectives

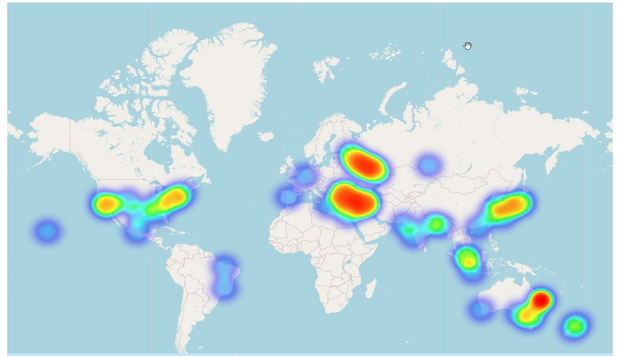
- **GNSS** is the **nervous system** of modern **transportation**.
- **Spoofers** can inject counterfeit signals → false position & time → **risks to safety, logistics, security**.
- **Existing** defenses **detect-and-deny** and **fail** against **evolving threats.**
- **Goal:** a **GNSS receiver that never yields corrupted PNT**, even through covert capture-phase attacks.

Solution & Performance

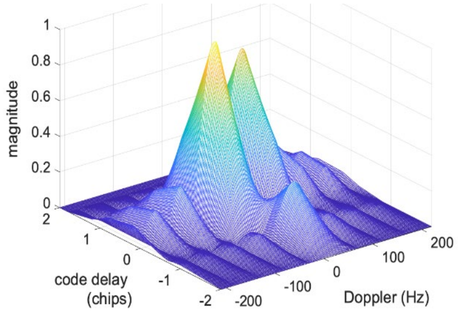
- **NavSentinel** – **a real-time detect-separate-track** architecture, composed of:
  1. TrustNav: INS/GNSS monitor **detects sub-decimeter spoofing**.
  2. CCAF/iRAIM **separates authentic & spoofed** components and **tracks the true signal**.
- **Key metrics** (target):
  - **Detection** within **seconds** with $P_{md} < 10^{-7}$
  - **False-alarm** probability $< 10^{-5}$
  - **Position error decimeter-level under attack**
  - **Continuous operation through sustained attack**

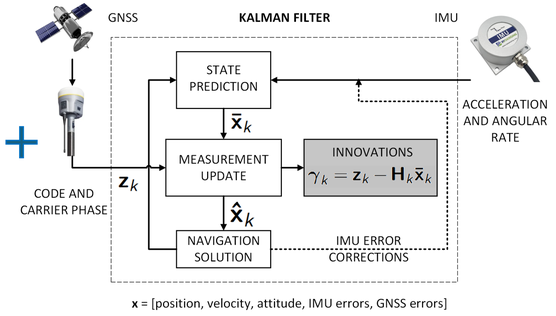
Path to Market

- **Phase 1 (M1-6, $300K): Fuse** and optimize algorithms.
- **Phase 2 (M7-18, $650K): Prototype** on FPGA + Lab tests.
- **Phase 3 (M19-30, $450K): Field trials** (NavFest/PNTAX), **pilot integration** with OEM partners.
- **Commercial** hook: **OEM licensing +** safety-critical add-on → **$200 B anti-spoof market** by 2030.
- **IP: Patent App. No.** 19/223,149 (TrustNav)

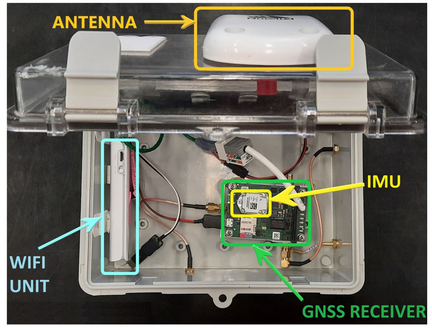


Interference Detection & Localization from Aircraft ADS-B GPS Position Reports





x = [position, velocity, attitude, IMU errors, GNSS errors]



CARNATIONS
ILLINOIS TECH
TruNav

Contact: Dr. Samer Khanafseh
Email: samer@trunav.net
www.trunav.com