Summary

Title: NavSentinel: a Resilient and Unspoofable GNSS Receiver

Global Navigation Satellite Systems (GNSS) are vital for modern infrastructure, from aviation to automated vehicles. However, they are vulnerable to spoofing, a targeted attack where false signals broadcast by malicious actors creates incorrect positioning and timing information, which can have catastrophic consequences. Current spoofing detection methods have limitations, particularly against sophisticated, subtle attacks.

This proposal introduces a breakthrough approach to create an "unspoofable" GNSS receiver by combining two powerful, complementary techniques developed by our team at the Illinois Institute of Technology. The first is an Optimal Inertial Navigation System (INS) Monitor, which leverages a tightly-coupled INS/GNSS Kalman Filter. This monitor is exceptionally sensitive, capable of detecting even sub-decimeter level spoofing "tracking errors" within minutes, even during the initial "capture phase" when a spoofer subtly tries to take control without obvious position offsets. This provides an extremely early warning of an attack.

However, the INS monitor, while great for early detection, cannot inherently distinguish between the authentic and spoofed signals to maintain continuous, accurate navigation. This is where our second technique, Complex Cross Ambiguity Function (CCAF) Decomposition with Inverse Receiver Autonomous Integrity Monitoring (IRAIM), comes in. CCAF decomposition, optimized using Particle Swarm Optimization (PSO), can break down the received GNSS signal into its individual components: authentic, spoofed, and even multipath. By then applying "Inverse RAIM" and incorporating INS, the receiver can identify which set of signals belongs to the true uncorrupted source and which belongs to the spoofed one, even when the spoofed signals are power-matched and closely aligned with the true signals.

The core innovation is the fusion of these two methods. The highly sensitive INS monitor acts as the primary defense, detecting the earliest signs of spoofing. Upon detection, the CCAF decomposition is rapidly activated to isolate and remove the spoofed signals, allowing the receiver to continuously track and compute the position based solely on the authentic signals. This combined approach ensures not only rapid detection but also sustained high-precision navigation, overcoming the limitations of each method individually.

This project aligns perfectly with ARPA-I's mission to foster breakthrough transportation technologies that enhance safety, strengthen resilience against cyber threats, and maintain U.S. global leadership. Our plan includes hardware prototyping on an FPGA platform for real-time processing and rigorous validation at major interference testing events like NavFest, PNTAX, and JammerFest. The outcome will be an "unspoofable" GNSS receiver, ensuring robust and reliable PNT for critical applications across aviation, automated systems, and vital infrastructure.