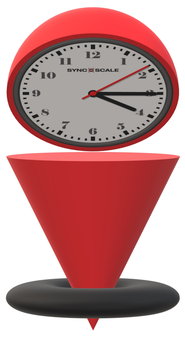
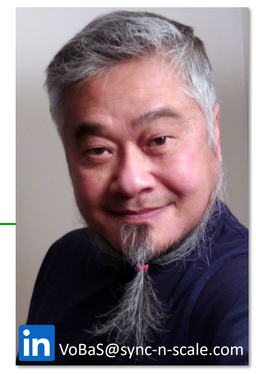
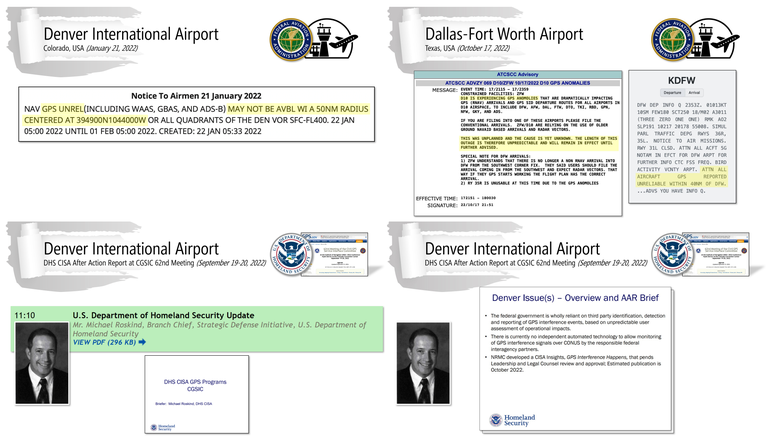
Detecting Manipulated Spaceborne Positioning and Timing Using Ground-Based Commercial-Off-The-Shelf Assets and Services



This poster describes a proof-of-concept ground-based harness for detecting manipulated GPS positioning and timing signals in real-time by cross-checking with information coming from additional sources. This trustworthy and resilient general-purpose computing platform is constructed of commercial-off-the-shelf systems and components. It makes simultaneous use of GPS and Iridium satellite constellations to get and keep UTC-accuracy, and to acquire its contemporaneous geographical location for effective detection and report of signal manipulation attacks.



The Incidents



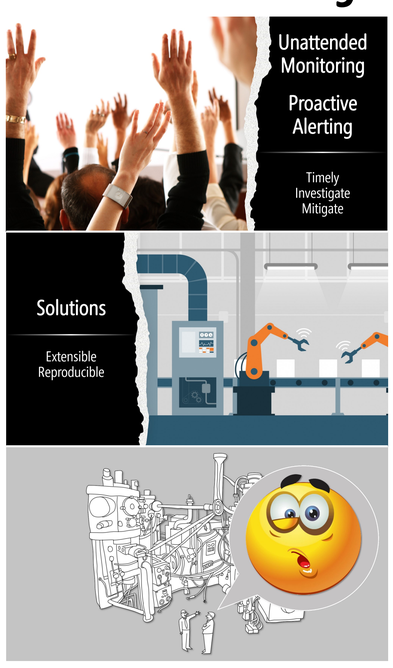
On January 21st, 2022 Air Traffic Control warned pilots of unreliable GPS reception within a 50-nautical-mile radius centered at Denver International Airport in Colorado. On October 17th, advisory was issued by the US Federal Aviation Administration warning of GPS anomalies over a 40-nautical-mile swath of airspace near the Dallas-Fort Worth airport in Texas.

Findings from the US Department of Homeland Security highlighted two unmet needs: *(i)* reliance on third party identification, detection and reporting of GPS interference and *(ii)* lack of independent automated technology for monitoring of GPS interference signals over the continental United States.

Implications and Threats

A 50 nautical mile radius around Denver International Airport affects areas north as far as Fort Collins, along the I-25 corridor, and also includes communities in the Denver metro area, Boulder, Longmont and Greeley. These notices might not reach thousands of non-aviation businesses and critical infrastructure operators in these regions who might be similarly affected, yet unaware of it. Loss of spaceborne positioning and timing signals can be detected and mitigated through technologies, but manipulation attacks (such as spoofing) are more difficult to discern. These include asynchronous attacks like meaconing and the more severe threat of synchronous attacks which can cause smooth and gradual time shifts in their targets. Commercial GNSS satellite simulators are easily accessible by malicious actors to conduct spoofing attacks in mobile tactics. This can result in interference, confusion and obscuring the intended targets.

Needs and Challenges



We argue that independent automated technologies are needed for unattended monitoring of spaceborne signal interference, with timely alerts for investigation and mitigation. These solutions should be readily reproducible and extensible, and involve a repertoire of mathematical and statistical algorithms for detecting a wide range of attacks. However, the proposed solutions thus far in literature are typically complex and not economically feasible to operate or deploy outside controlled environments, and therefore lack meaningful sensory coverage and mobility in real-world scenarios. In contrast, this poster provides a practical guide for assembling a ground-based harness for detecting manipulated GPS positioning and timing using mature technologies, in-market products, and services.

This proof-of-concept is for detecting manipulated GPS positioning and timing in real-time. It consists of two tamper-resistant industry-standard computing systems that are enclosed in a hardened chassis and connected by an Ethernet crossover cable. No additional networking infrastructure is needed. The first system uses GPS signals to maintain UTC-accuracy and geolocation awareness, while the second system uses signals from the Iridium satellite constellation to monitor the accuracy performance of the first system.

Methods and Tools

Both constellations are independently operated and have characteristics that make them, as a whole, difficult to render completely inoperational. The systems use commercial receivers, U-Blox for GPS and Satelles for Iridium, to capture signals using industry standard formats. The positioning and timing information is then delivered to Windows Server OS through a PCI Express bus inside a secure, tamper-resistant system enclosure. Each Windows Server core operating system is also configured with Windows Subsystem for Linux, running Ubuntu. This allows for the seamless operation of both Windows and Linux apps on the Windows desktop. In addition to being functional for implementing commercial-off-the-shelf software products and services, the harness is also a rich development environment for solution developers, providing access to ecosystems of freeware, shareware, and open-source software to meet different needs. A fuller description of this proof-of-concept harness can be found at the QR code.