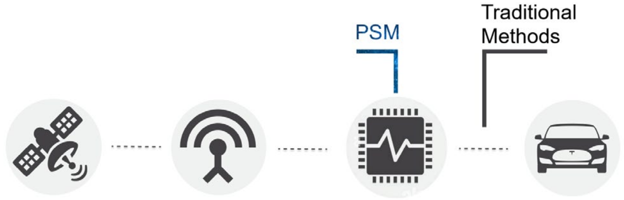
PEAK SUPPRESSION MONITOR

Global Navigation Satellite System (GNSS) receivers provide critical position, velocity, and timing (PVT) capabilities to military, civil, and commercial users around the world. Vulnerabilities in these receivers make them susceptible to malicious interference such as spoofing and jamming. Spoofing is broadcasting counterfeit GNSS signals to trick a GNSS receiver into using these false signals and obtaining an incorrect PVT solution.

MITRE's Peak Suppression monitor (PSM) is the first self-contained, chip-level algorithm that detects GNSS spoofing and jamming before it corrupts the receiver's PVT solution. The PSM technology can detect all known GNSS spoofing and jamming attacks including:

- Asynchronous and synchronous lift-off
- High-powered and matched-powered
- Knock-off jamming
- Carrier-to-Noise Matching
- Meaconing attacks



Benefits

PSM is a software solution with low complexity, unlike other anti-spoof solutions, which require access to Inertial Measurement Units or other hardware. PSM's simplicity also makes it extremely low power and computationally inexpensive. PSM also proactively detects spoofing and jamming before corrupting the receiver's PVT solution.

Software Only

Other solutions require access to Inertial Measurement Units or other hardware

Low Power

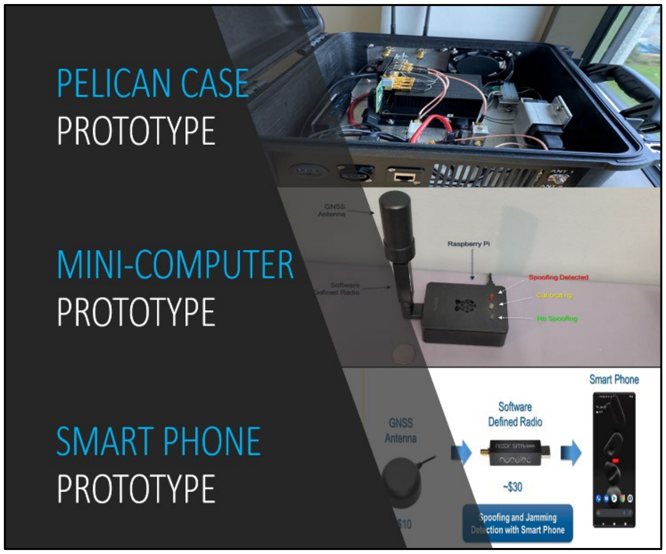
PSM's simplicity makes it extremely low power to use

Proactive Detection

PSM can detect spoofing & jamming before the GNSS receiver

REAL-TIME INTERFERENCE DETECTION

The PSM technology can be embedded into GNSS receivers or chip-set devices. MITRE has developed three real-time prototypes of the PSM technology using commercial hardware to test and demonstrate PSM's effectiveness. The first prototype is a Pelican case form factor that can be easily carried onto an aircraft and provide spoofing and jamming alerts to an electronic flight bag (EFB) via Bluetooth. The second prototype uses a small and inexpensive Raspberry Pi minicomputer. The third prototype is a smartphone platform in which the PSM technology is embedded in an Android Pixel 5 phone, which gives the user spoofing and jamming alerts.



PELICAN CASE PROTOTYPE

MINI-COMPUTER PROTOTYPE

SMART PHONE PROTOTYPE

Applications

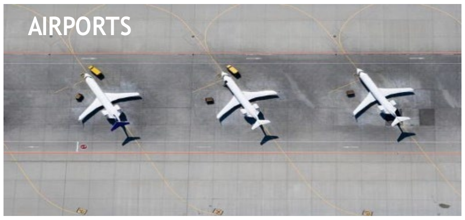
- AVIATION – Air navigation is increasingly reliant on GPS for precision approaches as legacy systems are decommissioned. If GPS signals near an airport are unreliable, pilots must know immediately their system is compromised.
- MARITIME – Many ships depend on GPS navigation. Pilots need to know when their GPS navigation systems have been compromised, which could result in substantial losses.
- FINTECH – Electronic transactions are often based on GPS-derived time. Even a millisecond delay can result in transactions with out-of-date prices, resulting in lost revenue.
- VEHICLES – Smart vehicles are dependent on GPS technology. Onboard navigation systems must be alerted to spoofing attacks, which could pose a critical safety risk.
- TELECOM – Telecommunications equipment uses GPS for precision timing and the telecom backbone relies on GPS for synchronization.
- ENERGY – A power grid's synchronization increasingly relies on GPS-derived timing. Spoofing attacks on power grid timing receivers can cause grid instability.

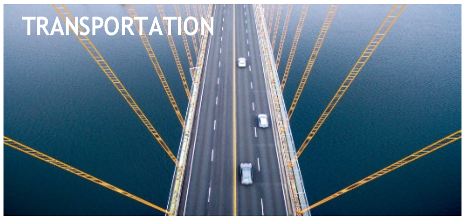
Licensing Opportunities

The MITRE Corporation is seeking licensees for commercial development of the PSM technology. PSM prototype technology has been demonstrated in field and laboratory settings and is available for licensing to qualified companies.

For more information, please contact: techtransfer@mitre.org

APPLICATIONS FOR PSM





MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

mitre.org