THE NEXT GENERATION OF ADVANCED SPOOFING SIMULATION

SAFRAN

The Next Generation of Advanced Spoofing Simulation

About GNSS Simulation

As the sophistication of GPS/GNSS spoofing attacks increase, the tools used to test against these threats must also evolve. Software-defined simulators with advanced spoofing scenarios help ensure that critical systems can operate in these environments.

Advanced Spoofing: Why Now?

Until a few years ago, a GNSS spoofing attack required expensive, high-end equipment in the $50,000- $500,000 range. Today, low tech equipment and open source software can enable anyone to spoof for as little as $100.

Consider the 2017 Black Sea attack: Russia simply used a high-power spoofer that transmitted the location of an on-land airport so that all nearby ships in the Black Sea thought that they were at the airport. In July 2019 in the port of Shanghai, the vessel Manukai was also a victim of mysterious spoofing: a ship appeared on a captain's navigation screens, and suddenly disappeared.*

A more sophisticated attack could occur with a fixed target, such as a financial building or a cell phone tower. With more precise location information about GPS or Positioning, Navigation and Timing (PNT) data-reliant equipment, a spoofer could change the time to disrupt financial trading time stamps. Or, in a cell network, it could cause a node to become out of sync with the cellular network so that users could no longer transmit or receive calls.

Another popular use of spoofing is to disable the ability for anyone to locate assets in a specific area by providing false location data, and that can also be a concern for GPS/GNSS users.

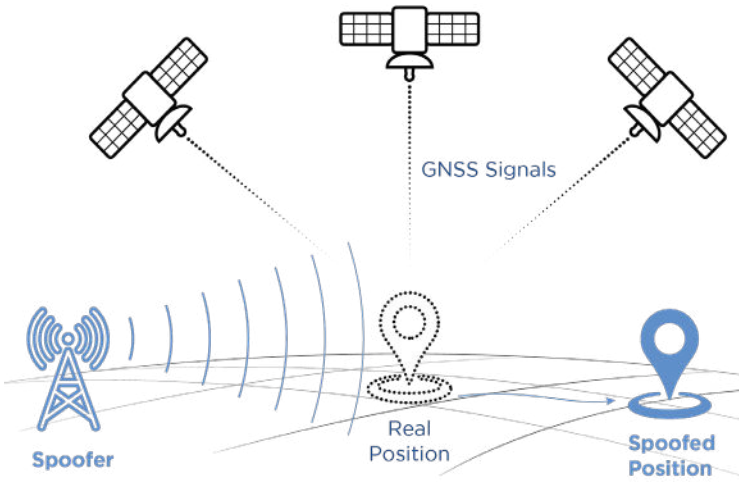
*MIT Technology Review, November 15, 2019

https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

What is a Spoofing Threat?

GNSS spoofing is an attempt to deceive the receiver under attack by broadcasting false GNSS signals. These fake signals may have a modified navigation message, pseudorange, and timing information. When the receiver uses false signals instead of real signals, the receiver is said to be spoofed. After the attacker has tricked the receiver into using the false signals, the attacker can further manipulate the false GNSS signals to achieve the goal of the attack.

Spoofing attacks can be used to disrupt navigation systems, cause accidents on the road, disable and capture drones, and cause network and datacenter issues by disrupting the very accurate timing that is necessary for those operations. Receivers today have varying degrees of spoofing protection built in, but determining how vulnerable they are requires comprehensive spoofing simulation to test their response to an attack.



Which Industries are Highly Vulnerable to Spoofing?


Maritime


Aviation


Critical infrastructure


Defense


Transportation

Safran's Advanced Spoofing Simulation Technology

Advanced spoofing simulation is a powerful, intuitive tool that enables users to quickly create and automate a multitude of dynamic spoofing scenarios. Safran's advanced GNSS simulators can simulate both spoofers and repeaters using the same equipment. Complicated test setups are history thanks to the innovative Skydel Advanced Spoofing option. It's also no longer necessary to purchase and synchronize multiple simulators or try to use simulator echo functions that were designed for other purposes.

GSG-8 simulates encrypted signals for the European Union and Allied Forces, which make it ideal for Navigation Warfare (NAVWAR) testing. The advanced spoofing option is available on both these simulation platforms, along with Safran's Wavefront and Anechoic systems. Safran's Wavefront system is designed especially for CRPA testing. It is the only wavefront simulator available today with advanced spoofing that is natively designed for wavefront simulation.

All Safran advanced simulators leverage our powerful Skydel Software Engine and are built on a software-defined architecture. Each features an intuitive user interface that makes it easy to add multiple spoofers to GNSS simulations. By unifying the simulation of the spoofer signals into a single system, spoofing testing is now easier than ever.

Advanced Simulator Platform

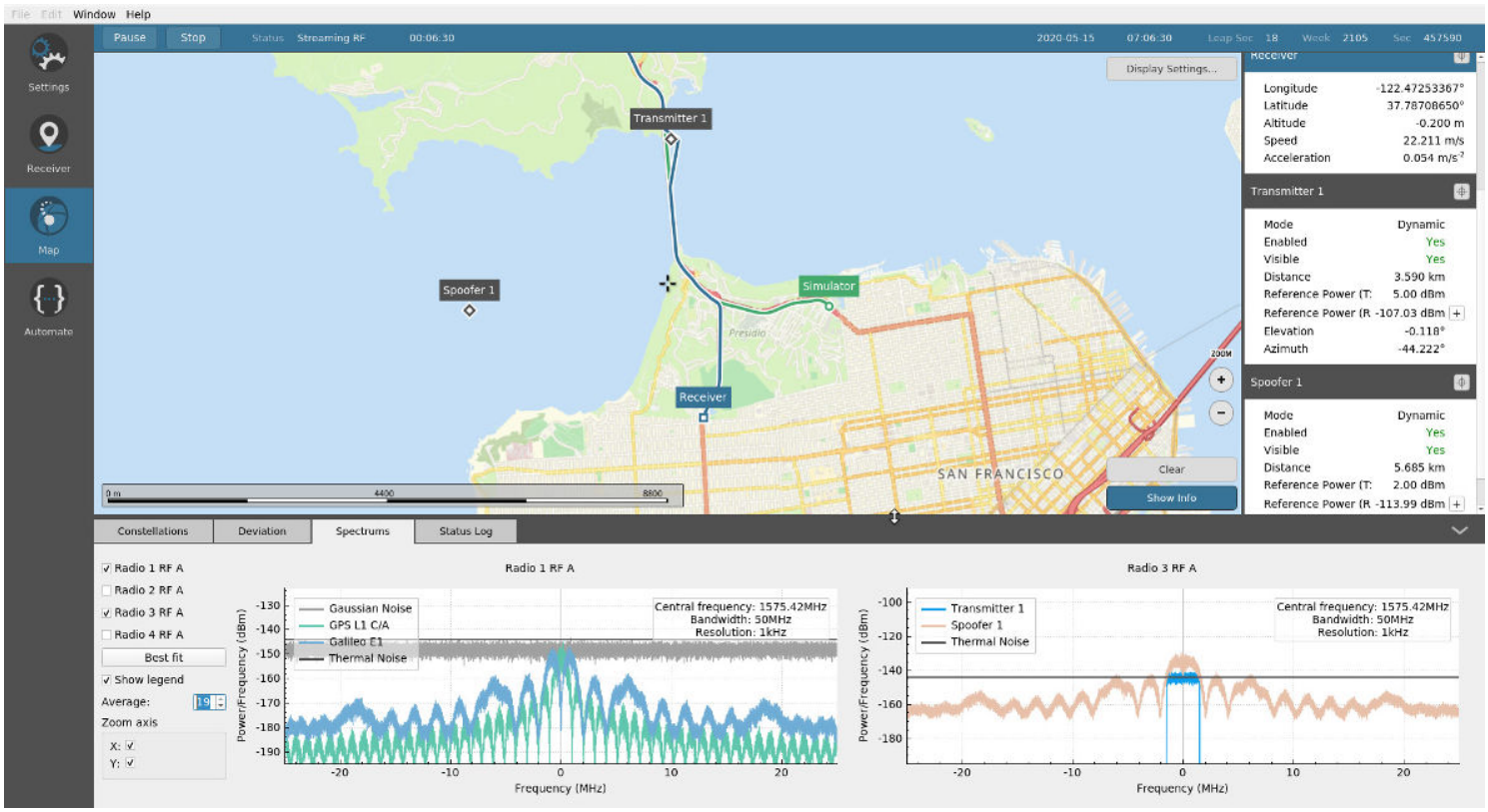
ADVANCED JAMMING CAPABILITIES

- Unlimited number of interference signals can be generated with 1 RF output
- Jamming can be turned on and off through the Skydel GUI and API
- Users can specify the location, power, antenna pattern and modulation of jamming transmitters
- Simulators will calculate the power received at the UUT based on the location and distance to the transmitter
- Enables users to create real-world threat scenarios to better support the warfighter

ADVANCED SPOOFING CAPABILITIES

- Simulate multiple spoofers simultaneously
- Each spoofer can generate any GNSS signal
- Each spoofer has an independent trajectory and antenna pattern
- Skydel software automatically determines signal dynamics between each spoofer and receiver antenna
- Full control of navigation message, pseudoranges and time synchronization
- Control truth and spoofed constellations independently for increased flexibility and realism

Comprehensive data sheets with specifications are available for Safran´s simulators.



POWERED BY TRUST

sales@nav-timing.safrangroup.com
safran-navigation-timing.com

SAFRAN

July 10, 2023