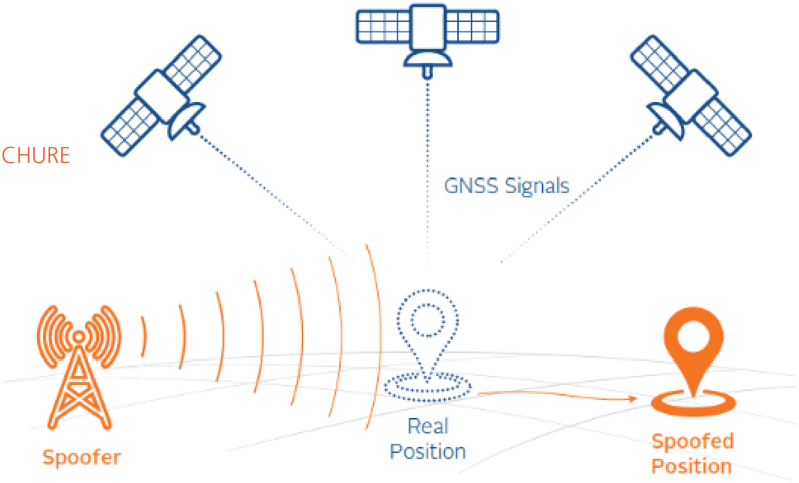
The Inside Scoop on GPS Spoofing

May 19, 2020
By Tyler Hohman, Director of Products, Orolia Defense & Security

JAMMING AND SPOOFING RESOURCE CENTER

THE NEXT GENERATION OF ADVANCED SPOOFING SIMULATION BROCHURE



Most in our industry are aware of the threat that GPS interference poses, both in the US and overseas. GPS jamming is commonplace. **Spoofing**, however, is different than jamming in that it can be utilized in a far more devious manner.

Both jamming and spoofing have a common goal – to disrupt signals and critical Positioning, Navigation and Timing (PNT) data, and make things more difficult for the opposing party. What is the difference? Jamming is the degradation or denial of GPS signals and PNT data while spoofing is the deliberate and conducted deception of GPS signals and corruption of PNT data.

The technology required to spoof a GPS receiver in a non-sophisticated or non-advanced way is becoming more readily available through low-cost software-defined hardware and open-source software. Taking these low-cost, unsophisticated systems and converting them into highly disruptive electronic attack systems can be easily achieved and has occurred in recent events. Consider the 2017 Black Sea attack: Russia used a high-power spoofer to transmit the location of an on-land airport so that all nearby ships in the sea observed their vessel as being at the local airport (on land).

This is an example of an unsophisticated attack that benefits the perpetrator because it causes confusion and deception to those around the spoofing area. A more sophisticated attack could occur if an adversary spoofed a specific target, such as a financial building or a cell phone tower. The spoofer would know the exact location of the GPS equipment in the building or cell tower and could create a spoofing scenario to slowly drift time away from the real time- which could disrupt trading time stamps. Or, in a cell network, it could cause a node to become out of sync with the network so that users could no longer transmit or receive calls in that specific cell tower area.

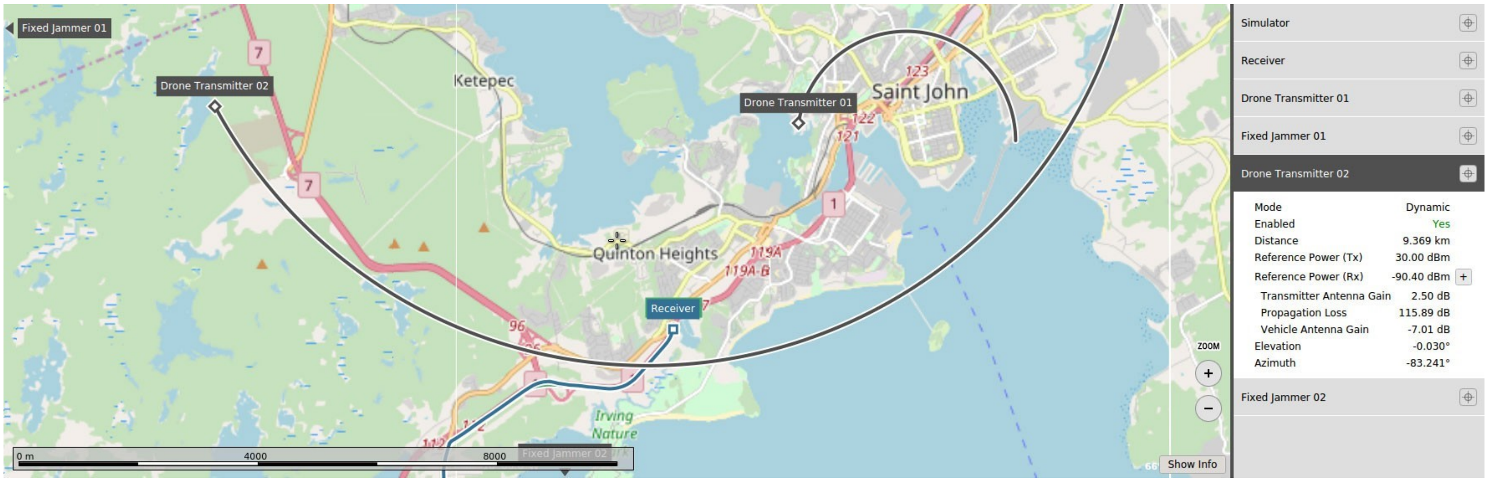
Here is an example of how these types of interference could cause disruptions to local users. A neighboring ship appears on a captain's navigation screens and suddenly disappears from the screen. A few minutes later, the screen shows the neighboring ship back at the dock, then moving again, then back at the dock, then gone completely. Mystified, the ship's captain decides to rely on his binoculars and scans the dockside, only to find that the other ship has been stationary at the dock the entire time.

Worse, when it comes time for the ship to head for its own berth, its bridge begins emitting multiple alarms: Both of its GPS units have lost their signals, and they are unable to provide an accurate position or they are reporting a position that is clearly incorrect (such as on land).

If this sounds familiar, it's because it actually happened to the Manukai in July 2019 in the port of Shanghai, as reported by MIT Technology Review. New research and new, never before seen data shows that the Manukai and thousands of other Shanghai vessels have fallen victim to a mysterious new attack that can spoof GPS systems in a new way. It is still unclear who is behind this spoofing attack but one thing is clear: According to MIT Technology Review, "there is an invisible electronic war over the future of navigation in Shanghai, and GPS is losing."

Due to the accessibility and affordability of the hardware needed to carry out spoofing, it has been likened to a party trick. Although the threat has been familiar to military users for some time, the commercial market is just beginning to see the effects and is beginning to adopt and integrate anti-jam and anti-spoofing capabilities.

The need is more urgent than ever to test GPS and PNT reliant systems to ensure they perform effectively under conditions where GPS jamming and spoofing are present. Orolia offers a variety of GPS/GNSS simulation solutions, from essential to advanced, that can simulate representative jamming and spoofing interference, as well as solutions to detect and mitigate against these attacks.



Mode	Dynamic
Enabled	Yes
Distance	9.369 km
Reference Power (Tx)	30.00 dBm
Reference Power (Rx)	-90.40 dBm
Transmitter Antenna Gain	2.50 dB
Propagation Loss	115.89 dB
Vehicle Antenna Gain	-7.01 dB
Elevation	-0.030°
Azimuth	-83.241°

Spoofing simulation capabilities include the ability to simulate multiple spoofers simultaneously. Each spoofer can generate any GNSS signal, and each has an independent trajectory antenna pattern. The Skydel Simulation Engine software automatically determines signal dynamics between each spoofer and receiver antenna.

Testing and hardening your systems are important steps – but it doesn't stop there. The best way to fully protect your systems from spoofing attacks is to take a layered approach – which means mitigating the source of the spoofing, in real-time. Orolia offers a variety of solutions to achieve this for different circumstances, including:

BroadShield – Embedded GPS jamming and spoofing detection with a kill switch

BroadSense Nano – GPS jamming and spoofing detection and situational awareness

GPSdome Anti-Jammer – A device that sits between the receiver and the antenna and detects jamming and spoofing

GPS/GNSS Anti-Jam Antenna – Blocks signals from the horizon, where most jamming occurs

ThreatBlocker – In-line GPS jamming and spoofing data, detection and protection

STL – Alternative independent GPS/GNSS signal that is highly resistant to spoofing and provides backup in the event of a GPS/GNSS outage

According to the February 12 PNT Executive Order, there is renewed emphasis on the importance of protecting critical infrastructure. As the world leader in resilient PNT solutions, Orolia is poised to help with turnkey solutions that detect and mitigate GPS/GNSS interference. For more information, Request a Demo or complete a Request for Quote now.

About Tyler Hohman

Tyler Hohman is the Director of Products at Orolia Defense & Security, an organization specializing in PNT performance, requirements, testing, integration and threat mitigation. Hohman's career has focused on GNSS simulation and threat mitigation technologies. Prior to Orolia Defense & Security, Hohman worked as the Chief Operations Officer at Talen-X developing PNT solutions, becoming proficient in NAVWAR technology and broadening his business expertise. Hohman actively participates in industry events and holds a bachelor's degree in Electrical Engineering from The University of Dayton. Hohman has attended the Ohio State University in pursuit of his Master's in Electrical Engineering.