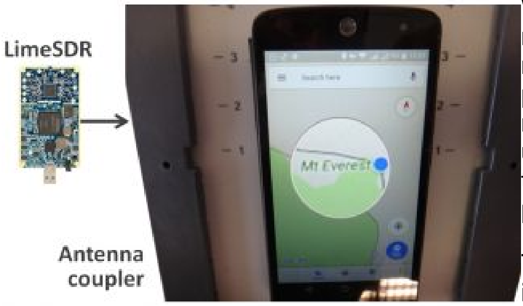
HOW SPOOFING AFFECTS SURVEY AND MAPPING

What is GNSS Spoofing?



With spoofing attacks on the rise, survey-grade GNSS receivers need to be protected by interference mitigation technology utilizing the latest security techniques to ensure reliable positioning.

The survey and mapping industry has been benefiting for years from GPS/GNSS precise positioning technology. While GNSS spoofing is recognized as a real threat for unmanned aerial vehicles (UAVs or ‘drones’), its influence on survey and mapping equipment is still underestimated. Reliable data capture is important across various mapping use cases, from man-based surveying and mobile mapping all the way to UAV photogrammetry. Ensuring dependable positioning requires the use of robust equipment, designed in such a way that alleviates all possible vulnerabilities. The use of GNSS receivers which are robust against jamming and spoofing is key to trustworthy data capture anytime, anywhere.

GPS/GNSS Spoofing vs Jamming

Both jamming and spoofing are a type of GNSS radio interference that happens when weak GNSS signals are overpowered by stronger radio signals on the same frequency. Jamming is a kind of ‘white noise’ interference, causing loss of accuracy and potentially loss of positioning. This type of interference can come from adjacent electronic devices or external sources such as radio amateurs in the area. Spoofing is an intelligent form of interference which fools the user into thinking that he/she is in a false location. During a spoofing attack, a radio transmitter located nearby sends fake GPS signals into the target receiver. For example, even a cheap software-defined radio (SDR) can make a smartphone believe it’s on Mount Everest (see Figure 1)!

GNSS users are experiencing ever-more cases of jamming, and spoofing events are on the rise too – especially in recent years since it has become easier and more affordable to create malicious spoofing systems. There are plenty of examples, from Finland – which experienced a week-long spoofing attack in 2019 – to China where multiple vessels have been the target of a spoofing attack. Hence, jamming and spoofing protection is no longer a ‘nice to have’ feature but a critical component of a GNSS receiver.

Spoofing Incidents Are on the Rise

C4ADS, an NGO conducting data-driven analysis of conflict and security matters, concluded that Russia has been extensively using spoofing to divert aerial drones from entering airspace in the vicinity of governmental figures, airports and ports. And some of the most enthusiastic spoofers are fans of the augmented reality mobile game ‘Pokémon Go’, who use SDRs to spoof their GPS position and catch elusive Pokémon without having to leave their rooms.

Such attacks usually target a specific receiver. However, the spoofing transmission will actually affect all GPS receivers in the vicinity. For example, an SDR can affect all GPS receivers within a 1km radius of the spoofing source, and the signal can be amplified for further propagation. This means that survey or mapping jobs in densely populated areas are at a higher risk of such 'indirect' spoofing attacks.

Figure 1: Even a cheap SDR can overpower GNSS signals and spoof a single-frequency smartphone GPS into believing it is on Mount Everest.

How to Spoof-proof a Receiver

A spoofer can either rebroadcast GNSS signals recorded at another place and time, or generate and transmit modified satellite signals. Therefore, to combat spoofing, GNSS receivers need to be able to distinguish spoofed signals from authentic signals. Once a satellite signal is flagged as spoofed, it can be excluded from positioning calculations.

There are various levels of spoofing protection that a receiver can offer. Using the analogy of a home intrusion detection system, it can be based on a simple entry alarm system or a more complex movement detection system. For added security, the home owner could decide to install video image recognition, breaking-glass sound detection or a combination of the above. An unprotected GNSS receiver is like a house with an unlocked door; it is vulnerable to even the simplest forms of spoofing. Secured receivers, on the other hand, can detect spoofing by looking for signal anomalies or by using signals designed to prevent spoofing, such as Galileo OSNMA and E6 or the GPS military code.

Advanced interference mitigation technologies, such as the Septentrio AIM+, use sophisticated signal-processing algorithms to mitigate jamming and flag spoofing. For spoofing detection, AIM+ checks for various anomalies in the GNSS signal, such as unusually high signal power. It also works together with RAIM+ integrity algorithms to ensure range (distance to satellite) validity by comparing range information from various satellites. AIM+ won't even be fooled by an advanced GNSS signal generator, Spirent GSS9000. Even with realistic power levels and actual navigation data within the signal, it can still identify it as a 'non-authentic' signal. Other advanced anti-spoofing techniques such as using a dual-polarized antenna are currently being researched.

Figure 2: GNSS spoofing could be used to manipulate movement of aerial drones.

Satellite Navigation Data Authentication

Various countries are investing in spoofing resilience by building security directly into their GNSS satellites. With Open Service Navigation Message Authentication (OSNMA), the European Galileo is the first satellite system to introduce an anti-spoofing service directly on a civil GNSS signal.

OSNMA is a free service on the Galileo E1 frequency that enables authentication of the navigation data on Galileo. Such navigation data carries information about satellite location and, if altered, will result in wrong receiver positioning computation. As a close partner of ESA, the European GNSS manufacturer Septentrio has been contributing to the design and testing of the Galileo system since its inception. Today, as the OSNMA system is entering its testing phase, Septentrio receivers have successfully been used to test the OSNMA signals. The US GPS system is also experimenting with satellite-based anti-spoofing for civil users with its recent authentication system called Chimera.

Figure 3: European Galileo satellites provide an open authentication service on the E1 signal and a commercial authentication service on the E6 signal. (Image courtesy: European Space Agency)

Advanced Interference Mitigation Technology

OSNMA is a part of the puzzle comprising the AIM+ interference defence system. The anti-jamming component suppresses the widest variety of interferers, from simple, continuous narrow-band signals to the most complex, wideband and pulsed transmissions. The anti-spoofing component consists of signal anomaly detection, OSNMA, RAIM+ as well as other algorithms.

Future-proof GNSS Receivers

Interference mitigation technology such as AIM+ protects accurate positioning today. To ensure the best protection for tomorrow too, GNSS manufacturers are offering future-proof technology which allows users to take advantage of new GNSS security services like ONSMA and Chimera as soon as they become available. Utilizing future-proof GNSS receivers in survey, mapping and UAV equipment enables integrators to reduce their time to market with resilient products. Secured GNSS means trustworthy precise positioning and peace of mind for everyone who relies on this technology.

Further Reading

https://www.septentrio.com/en/advanced-interference-monitoring-mitigation-aim

https://septentrio-my.sharepoint.com/:b:/p/marketing/EU99N82bWyZPsvd4Dp9g5lwBEwqQLgeT8i7wtW64TEk-tw?e=S0fGFD