PROTECTING YOUR POSITION

MARIA SIMSKY EXPLORES HOW GPS/GNSS RECEIVERS CAN BE IMBUED WITH GREATER RESILIENCE AGAINST THE GROWING THREATS OF JAMMING AND SPOOFING

With the growth of automation and robotisation in many industries, from agriculture and delivery drones to self-driving cars, the demand for accurate and affordable navigation is on the rise. When selecting a GPS/GNSS[1] positioning receiver it is crucial to understand the vulnerabilities of these sensors and the effect they could have on the navigation system. For robots and autonomous devices, availability is key to ensuring continuous and reliable service. Safety also needs to be considered for robots and drones operating close to people. GNSS jamming or spoofing needs to be detected and flagged immediately so that other sensors can take over.

Most autonomous navigation technologies include an Inertial Navigation System (INS), which consists of a GNSS receiver and an IMU (Inertial Measurement Unit) sensor. While the GNSS receiver provides absolute positioning in terms of geographic global coordinates, the IMU measures heading, pitch and roll angles which give orientation information of a moving system.

Spoofing is a real threat to GNSS-based INS systems, which is mitigated most effectively by incorporating security mechanisms into all system sub-components. However, since spoofing takes place on the level of the GNSS signal, a number of sophisticated methods can be employed within the receiver to detect and mitigate spoofing. Receivers that are designed with security and robustness in mind, are resilient to GNSS vulnerabilities such as jamming and spoofing. Taking advantage of such robust GNSS technology is also cost-effective, allowing companies to focus their development on sensor fusion and navigation.

Jamming and spoofing are real

Jamming is a kind of radio interference which overpowers weak GNSS signals, causing accuracy degradation and possibly even loss of positioning. Unintentional jamming sources include radio amateurs, maritime and aeronautical radiolocation systems as well as electronic devices located close to the GNSS receiver. There are also intentional jamming devices called "jammers", which are sometimes found on vehicles trying to avoid road tolls.

Spoofing is an intelligent form of interference which makes the receiver believe it is at a false location. Spoofing has appeared in the news in a spectacular experiment where a Tesla car was "misled" to take an exit from a highway rather than following the intended route[2]. Consequently, both jamming and spoofing can have an adverse effect on INS systems that make use of GNSS positioning. For more information on spoofing visit https://www.septentrio.com/en/learn-more/insights/osnma-latest-gnss-anti-spoofing-security.

How can INS get jammed and spoofed?

While GNSS provides absolute positioning, the IMU measures relative movement but is subject to cumulative error called drift and needs regular "recalibration". In a GNSS/INS system both sensors are fused in such a way that the GNSS provides regular IMU "calibration" and the IMU provides angles and extrapolation or "smoothing" of GNSS.

Jamming, which results in loss of positioning, means that the GNSS receiver can no longer be used as part of the INS solution. This can lead to longer INS initialisation times or a switch to dead-reckoning mode (IMU solution only) and where the position will start to drift. Jamming can also result in measurement outliers that impact GNSS/INS algorithms (i.e., deep or tight coupling). However, it is spoofing which poses the highest security risk for GNSS/INS systems. During a spoofing attack, an INS solution could be "hijacked" if the spoofer uses small increments in positioning that can go undetected by common anti-spoofing methods.

Vulnerability of the common INS anti-spoofing method

Using sensors other than GNSS, e.g., an IMU or odometry, can help flag spoofing by detecting inconsistencies between GNSS and the other sensors. While such sensors help mitigate the risk, they are insufficient to provide full protection as they only output relative positioning that is subject to drift. For example, the GNSS/INS systems can have a drift of a meter or more when visibility of GNSS satellites is lost for longer periods. Spoofers can exploit this drift phenomenon to gradually hijack positioning in increments comparable to the expected drift.

Fig.1 demonstrates a common mechanism used by GNSS/INS systems to detect spoofing. The system is initialised and starts receiving new GNSS, IMU and/or odometry data, which is continuously checked for consistency.

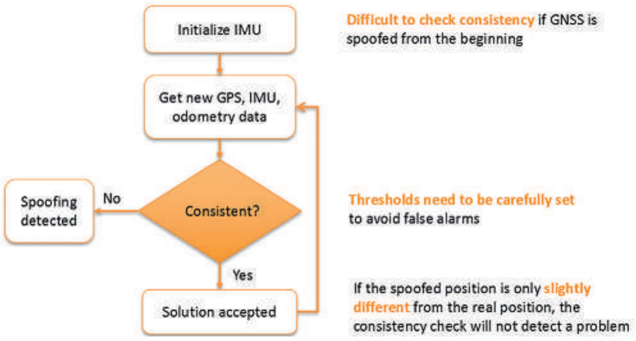
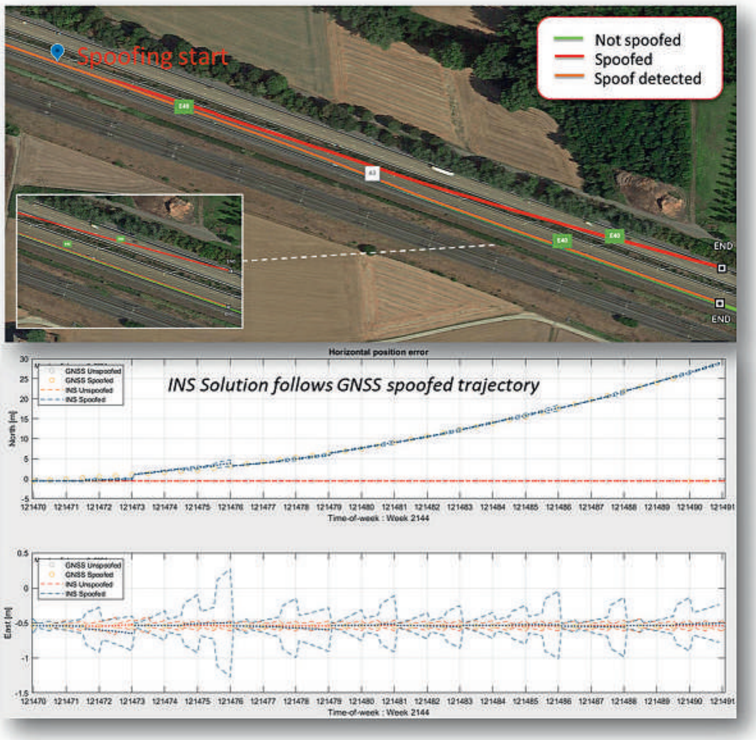

Initialize IMU
Get new GPS, IMU, odometry data
Consistent?
No
Spoofing detected
Yes
Solution accepted
Difficult to check consistency if GNSS is spoofed from the beginning
Thresholds need to be carefully set to avoid false alarms
If the spoofed position is only slightly different from the real position, the consistency check will not detect a problem

Fig.1: GNSS/INS systems commonly check positioning for outliers to detect spoofing. However, if the spoofer uses small positioning increments, which are within thresholds allowing for drift, it would go undetected by this mechanism. Image: ©2022 septentrio.com



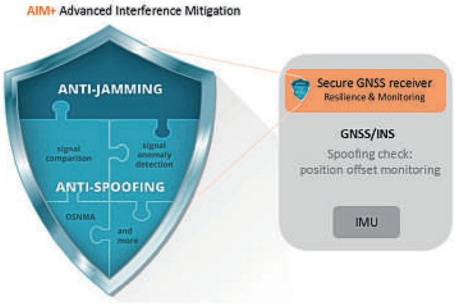


Fig.3: The best GNSS/INS spoofing protection comes from resilience built into multiple system components. On the GNSS receiver side anti-spoofing security can be incorporated on hardware and software level, such as in the Septentrio AIM+ technology.

Above: Fig.2: The red line is a GNSS/INS system with a common spoofing check, which is "hijacked" by a spoofer that uses small positioning increments. The orange line is a GNSS/INS system which stays on track due to spoofing being detected by the GNSS receiver. Image: ©2022 septentrio.com

If the spoofing attack keeps positioning increments within the allowed thresholds for drift, it would go undetected by such a mechanism. That is why, for best system protection, anti-spoofing resilience should be built into the several system components on both GNSS and INS levels.

Spoofing is best detected within GNSS

The vulnerability of this common INS spoofing check is shown in Fig.2 and where the spoofing attack is executed gradually, in small increments perpendicular to the direction of motion. The magnitude of these spoofed increments is small enough to be below the drift threshold of the IMU, which makes it acceptable for the INS system shown by the red line.

The system shown by the orange line, with anti-spoofing built into the GNSS receiver, rejects the spoofed signal and switches to dead-reckoning, which allows it to stay on the right track. If the spoofing attack is limited to a few signals, then the GNSS receiver can even avoid the attack by discarding these spoofed signals from its positioning solution.

Secure GNSS receivers protect INS systems

As shown in Fig.3, an INS system will be more resilient if the GNSS receiver can indicate spoofing or, even better, can mitigate spoofing by itself. Thus, when integrating GNSS/INS solutions it remains crucial to understand the role of protection mechanisms in GNSS and to select a GNSS receiver with a strong internal anti-spoofing defence system or a warning system. Septentrio receivers also provide lots of information about GNSS signals, allowing users to get insights into the spoofed signal such as time stamps and power levels.

A GNSS receiver which implements security measures in its design will include spoofing resilience at various levels. For example, the Septentrio AIM+ Advanced Interference Mitigation technology is a jigsaw puzzle of various anti-jamming and anti-spoofing components built into receiver hardware as well as software:

- Signal processing (HW): signal authentication (OSNMA), signal comparison and anomaly detection, satellite consistency check in tracking
- Measurement engine (SW): quality checks of raw measurements
- Positioning engine (SW): receiver autonomous integrity monitoring (RAIM+) and proprietary algorithms

Both the GNSS receiver as well as the INS have their own mechanisms for spoofing protection. However, the best resilience comes from detection and mitigation mechanisms working together at component level.

Maintaining security at the receiver core

As in any field affiliated with security, continuous improvement is needed to maintain effective anti-spoofing and anti-jamming mechanisms. GNSS manufacturers have a responsibility to strive for the most effective security methods in view of the growing threats that confront today's GNSS users. By investing in GNSS receivers with built-in resilience, integrators can leave the security maintenance to the GNSS manufacturer and focus their efforts on core business and sensor fusion. In fact, the concepts discussed in this article are valid not only for GNSS/INS systems but for any sensor fusion system that includes a GNSS receiver. Smart GNSS technology protects receivers from jamming and spoofing at the core level, ensuring safe and reliable system operation.

[1] GNSS: Global Navigation Satellite System including the American GPS, European Galileo, Russian GLONASS, Chinese BeiDou, Japan's QZSS and India's NavIC. These satellite constellations broadcast positioning information to receivers which use it to calculate their absolute position.

[2] Tesla Model 3 spoofed off the Highway – Regulus Navigation System hack causes car to turn on its own. https://www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-navigation-system-hack-causes-car-to-turn-on-its-own

Maria Simsky is Technical Content Writer with Septentrio, a designer and manufacturer of multi-frequency multi-constellation GPS/GNSS positioning technology headquartered in Leuven, Belgium (https://www.septentrio.com/en)