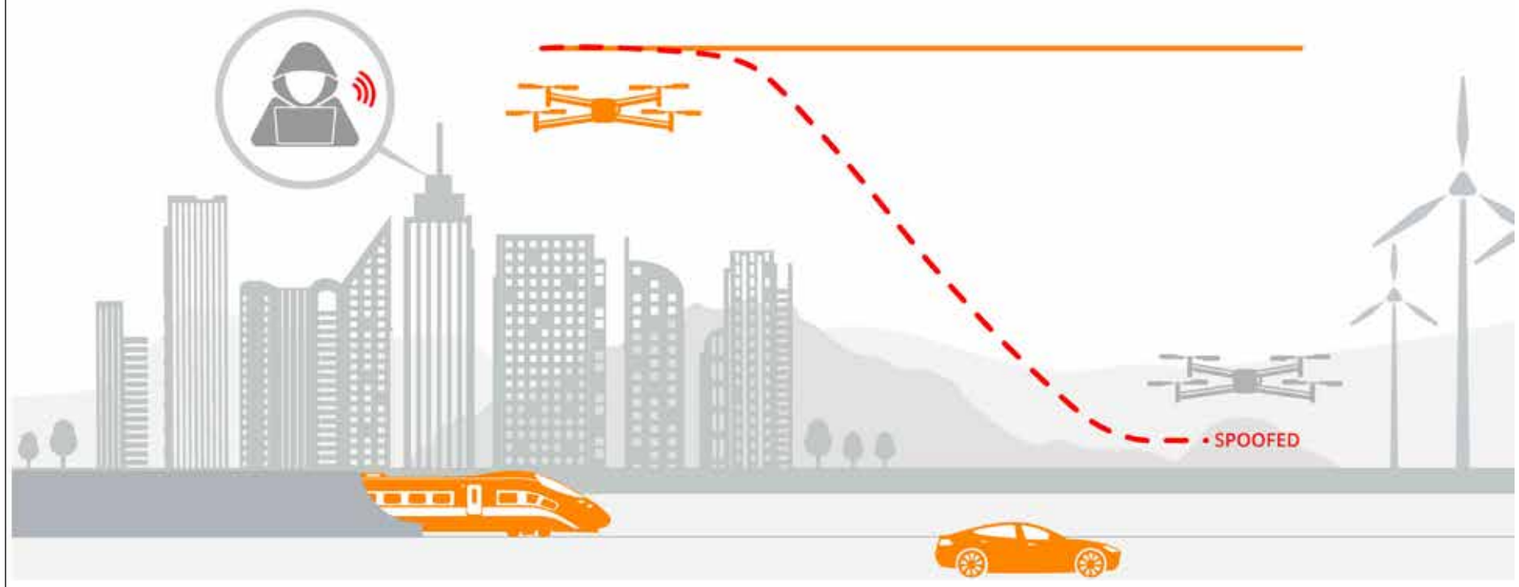


JAMMING AND SPOOFING

Maria Simsky is Technical Content Writer at Septentrio.

Maria Simsky *explains why secure GPS receivers are crucial for GNSS/INS systems*

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 (Global positioning system/ Global Navigation Satellite System) receiver it is crucial to understand 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 Inertial Measurement Unit (IMU) 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 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 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 board of vehicles that trying to avoid paying any road tolls.

Spoofing is an intelligent form of interference, which makes the receiver believe it is at a false location. It 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 highway as it was supposed to. Consequently, both jamming and spoofing can have an adverse effect on INS systems, which make use of GNSS positioning.

While GNSS provides absolute positioning, the IMU measures relative movement, which 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), where the position starts to drift. Jamming can also result in measurement outliers, which impact GNSS/INS algorithms (ie 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 can be hijacked if the spoofer uses small increments in positioning, which can go undetected by common anti-spoofing methods.

Using sensors other than GNSS such as an IMU or odometry can help flag spoofing by detecting inconsistencies between GNSS and the other sensors. While such sensors help reduce spoofing risks, they are not sufficient to provide full protection because they only output relative positioning – which is subject to drift. For example, GNSS/INS systems can have a drift of a metre or more when visibility of GNSS satellites is lost for longer periods. Spoofers can exploit this to hijack positioning gradually, in increments comparable with the expected drift.

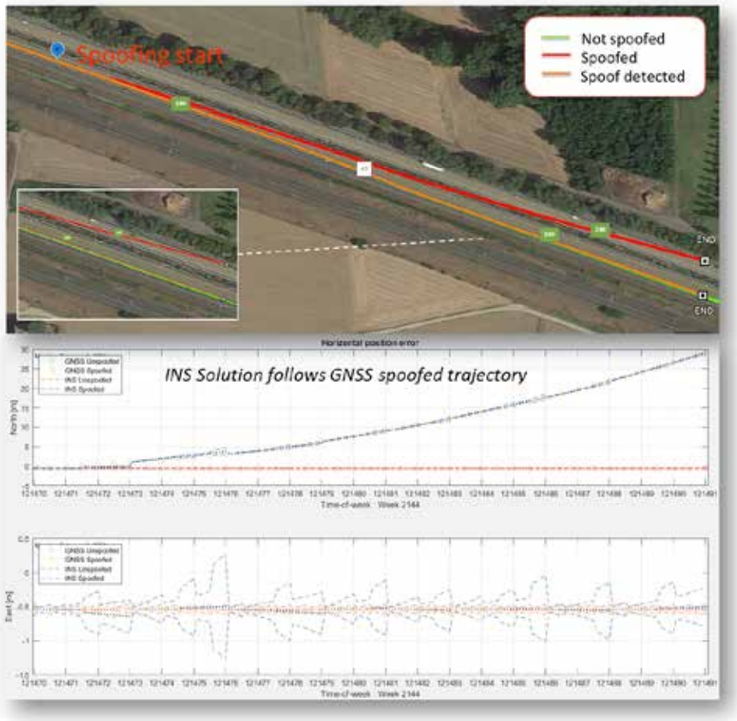
If the spoofing attack keeps positioning increments within the allowed thresholds, which are set to allow for drift, it will go undetected by such a mechanism. That is why, for best system protection and anti-spoofing resilience should be built into several system components on both GNSS and INS levels.

The vulnerability of this common INS spoofing check is shown in the road test below, 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.

As shown in the road test, an INS system will be more resilient if the GNSS receiver can indicate spoofing or, even better, if it 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 strong internal anti-spoofing defence system or a warning system

A GNSS receiver which implements security measures in its design will include spoofing resilience at various levels. Both the GNSS receiver as well as the INS have their own mechanisms for spoofing protection, however the best resilience comes from the combination of detection and mitigation mechanisms working together on component level.

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 increasing threats, which 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, which includes a GNSS receiver. Smart GNSS technology protects receivers from jamming and spoofing at the core level, ensuring safe and reliable system operation ●



The red line is a GNSS/ INS system with a common spoofing check that has been hijacked by a spoofer using small positioning increments. The orange line is a system that stays on track due to spoofing being detected.

Picture credits: Septentrio