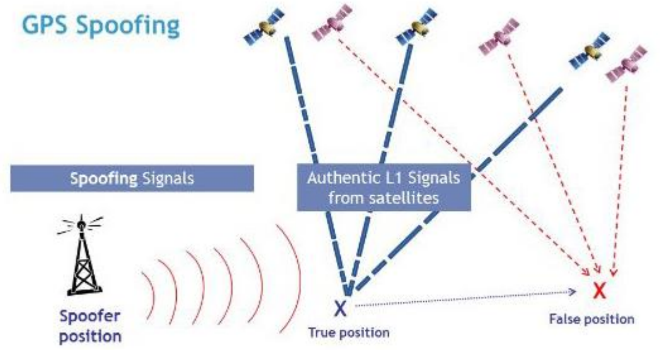
Inertial Labs
Attitude is Everything

The Inertial Labs INS-D-OEM with Spoofing Protection

What is Spoofing?

Satellite constellations use RF signals to transmit information to GNSS receivers. These signals contain information on the satellite ephemeris, clock bias parameters, almanac, satellite health status and other information. Receivers use these signals to compute position (and timing) information in global coordinates of longitudinal and latitudinal location. Spoofers transmit signals with higher relative power (a dominating signal strength) than the GNSS/GPS signals that are typically received by receivers. These signals contain false positioning information which results in the receiver believing false data. This used to be a complicated and expensive process that only militaries could perform, but with technological advances and the growing pervasiveness of the internet, GPS spoofing transmitters can be found easily and inexpensively by members of the civilian population.



Categorizing Attacks

Non-Overlapped

A non-overlapped spoofing attack's spoofing signal is not synchronized with the authentic GNSS signals. In this type of attack, the correlation peaks between the spoofing and the authentic GNSS signals are asynchronous. Non-overlapped spoofing attacks are effective during a cold start where the spoofing signal has a higher power than the authentic signal, this can deceive the device depending on the receiver search strategy. When a signal is in the tracking stage, the other regions of the cross-ambiguity function are not visible to the receiver. As a result, the higher power spoofing signal may not affect the tracking procedure if the delays or Doppler frequencies are not aligned.

Overlapped

In a more sophisticated attack, a spoofer can synchronize its code phase and Doppler frequency with those of the authentic signals. In an overlapped attack, the correlation peaks of spoofing and authentic signals combine to constructively or destructively change the shape of the correlation peak. This type of spoofing attack can be generated by a receiver-based spoofing device where the spoofer knows the time, number of observable satellites, the location and parameters of the target receiver. Detecting an overlapped spoofing attack is much more challenging as the distortions caused by spoofing signals appear similar to multipath errors.

Relative Power

The power of the receiver is an integral feature for any spoofing attack in order to deceive the target receiver. The power level of spoofing signals in comparison to that of authentic signals can highly impact the effectiveness and error limit of spoofing interference. Trying to identify spoofing attacks based on their relative power is difficult as it requires information of about the propagation channel, antenna gain pattern, and the orientation of the spoofer's signal.

How Do You Detect Spoofing?

As noted in the previous section, spoofing attacks tend to have some signature characteristics which can be used to detect spoofed signals.

Input Power Analysis

A common way to spoof a receiver is to jam it and then provide false signals. This type of attack can be detected by closely monitoring the input power to detect additional power from interference signals. Monitoring the input power is achieved by observing the gain of the automatic gain control (AGC) module.

Structural Power Content Analysis

Structural power content analysis utilizes the cyclo-stationarity, or the statistical properties that vary cyclically, of a GNSS signal to detect excessive amounts of structured signal power in the received data set. Received baseband data is filtered within the GNSS signal bandwidth, and then multiplied by their delayed version to remove the Doppler effect. As a result, the signal has a line spectrum, which consists of only a few lines of specific wavelengths generated by the multiplication of cyclo-stationary signals. Then the signal and its noise components are filtered by comb filters. A detection test statistic is calculated based on the filter outputs of the signal and comparing it to the threshold of an attack.

Effective C/N$_0$

The most common method of spoofing detection is by analyzing the effective C/N$_0$ and is available in most commercially sold receivers. The upper limit of a receiver's C/N$_0$ value can be defined for any given receiver. A very high C/N$_0$ value can be an indicator of a spoofing attack. Additionally, the jamming signals can affect the effective C/N$_0$ values by increasing the noise floor entirely.

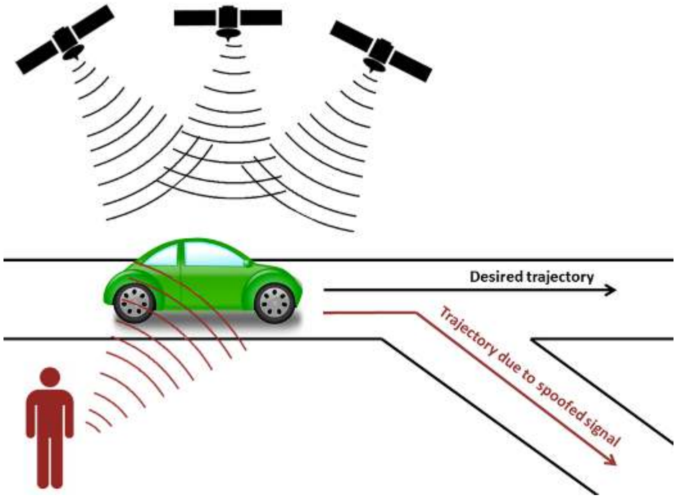
Signal Quality Monitoring (SQM)

Distortion on the shape of the correlation peak can be caused by the interaction between authentic and spoofing signals during overlapped attacks. Signal quality monitoring tests are focused on this distortion to detect any asymmetric, abnormally sharp, or elevated correlation peaks. Though originally used to monitor the correlation peak quality effected by multipath signals, users have found success in using SQM metrics to identify spoofing attacks.

Dangers of Spoofing

As GPS technology is becoming more widespread, there is an increasing reliance on GPS as a part of the world's critical infrastructure. Secure, stable, and resilient position, navigation, and timing (PNT) is necessary for the functioning of the world's critical infrastructure. Nearly all sectors of the economy rely on accurate PNT information to provide services for civil, commercial, or military applications. With GPS technology being ubiquitously used for accurate PNT, spoofing is a very serious threat to this infrastructure that so many everyday systems such as cars, phones, and computers rely on.

As the use of autonomous vehicles for both commercial and military applications becomes more widespread, the dangers of GNSS spoofing become more prevalent. Unmanned underwater vehicles (UUV), unmanned ground vehicles (UGV), automated guided vehicles (AGV), and Unmanned Aerial Vehicles (UAV) can be drastically impacted by GNSS spoofing. GNSS spoofing can redirect unmanned vehicles to incorrect locations which can cause crashes that can be fatal and cause millions of dollars in damage.



Protecting Against Spoofing

With the prevalence and dangers of spoofing in mind, there are a few general ways to prevent GNSS spoofing. For instance, some GPS signals are designed to provide protection from spoofing attacks by providing security in the satellite itself, an example of this is found in the Galilea OS-NMA E6 frequency band or the GPS military code.

Additionally, GNSS receivers can detect a spoofed signal from a mix of authentic and spoofed signals. Once a spoofed signal is detected, it should remove that signal from consideration for any positioning calculation.

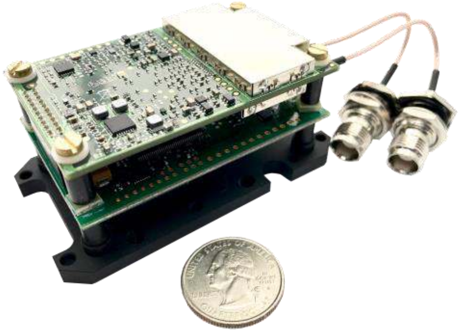
The INS-D-OEM with Spoofing Protection

The Inertial Labs INS-D-OEM features the top-of-the-line dual antenna Novatel OEM7220 GNSS receiver. It contains a real-time spoofing detection unit that employs some of the most effective detection metrics. These metrics include input power analysis by monitoring the gain of the automatic gain control module, structural power content analysis based on the filter outputs, signal quality monitoring to monitor the peak quality affected by multipath signals, and clock monitoring using spoofing signals from a single-antenna source based on the position solution of a moving receiver. These detection metric outputs are fed to an onboard central spoofing detection unit, which makes decisions as to whether the unit is under a spoofing attack every two seconds. The spoofing detection unit minimizes false detection likelihood from the presence of jamming and multipath signals, while identifying spoofing attacks with a high degree of certainty.

What Do You Think?

Here at Inertial Labs, we care about our customers satisfaction and want to continuously be able to provide solutions that are specifically tailored to problems that are occurring today, while vigorously developing products to tackle the problems of tomorrow. Your opinion is always important to us! Whether you are a student, an entrepreneur, or an industry heavyweight. Share your thoughts on our products, recommendations you have, or just say hello at opinions@inertiallabs.com.

Inertial Labs
Attitude is Everything



HEXAGON | NovAtel

GPS-Aided INS-D-OEM

Specification	Performance
Dynamic Heading Accuracy	0.08 deg (2-meter baseline)
Dynamic Pitch & Roll	0.08 deg
Position (RTK)	0.01 m + 1 ppm
GNSS Receiver Type	Dual GNSS Antenna
IMU Grade	MEMS Tactical Grade
Size	85 X 47 X 36 mm
Weight	150 grams

Contact Information

Address: 39959 Catoctin Ridge Street,
Paeonian Springs, VA 20129 U.S.A.
Website: www.inertiallabs.com

Inertial Labs
Attitude is Everything

IEEE | ABS | ISO 9001:2015 CERTIFIED COMPANY | CE | STANDARD MIL-STD 810G | ITAR FREE

About Inertial Labs Inc.

Established in 2001, Inertial Labs is a leader in position and orientation technologies for commercial, industrial, aerospace and defense applications. Inertial Labs has a worldwide distributor and representative network covering 20+ countries across 6 continents and a standard product line spanning from Inertial Measurement Units (IMU) to GPS-Aided Inertial Navigation Systems (INS). With application breadth on Land, Air, and Sea; Inertial Labs covers the gambit of inertial technologies and solutions.

MADE IN USA

Inertial Labs
Attitude is Everything

Scan me!!!

Inertial Labs, Inc.
39959 Catoctin Ridge Street,
Paeonian Springs, VA
20129 USA
phone: +1 (703) 880 4222
sales@inertiallabs.com
www.inertiallabs.com