White Paper

Resilient PNT Solutions for Telemetry During GNSS Outage Test Scenarios

Lisa Perdue and John Fischer
Executive Summary

GNSS (Global Navigation Satellite System) is key to effective situational awareness, providing critical Positioning, Navigation and Timing (PNT) telemetry data for mobile military operations.

Yet GPS/GNSS jamming and spoofing attacks are on the rise. The combination of low-cost hardware, open source software and tutorials on YouTube have fostered the proliferation of these malicious acts. Beyond intentional disruption, other factors such as environmental conditions and conflicts with other electronic systems can result in unreliable or even unavailable GNSS data. The disruption of GNSS for increasing periods of time through jamming/spoofing must now be an essential test component in most test scenarios today. How can you still provide reliable Time-Space Position Information (TSPI) during periods of GNSS denial?

Key mobile military operations that rely on continuous and trusted PNT telemetry data from GNSS include SatCom on the Move (SOTM), Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR), Airborne Communications Relay, Synthetic Aperture Radar, and Combat Search and Rescue (CSAR). Techniques and technologies used in battlefield systems to provide alternative sources of PNT data during a GNSS outage can also be used on the test range.

This white paper will identify technologies, best practices and strategies for GNSS jamming/spoofing detection and protection systems, and testing protocols to maintain a state of PNT readiness.

Introduction

To say that GNSS, including GPS, is widely used in telemetry would be an understatement. In fact, it is used almost exclusively, and with good reason: No other open service available globally today can provide the nanosecond level timing and centimeter level positioning of GNSS systems.

GNSS signals have always been highly susceptible to interference, but in the last decade, the means to generate signals harmful to GNSS reception has become more available to anyone interested in denying GNSS service to a specific area. That, added to the inherent GNSS vulnerabilities in the system’s design, makes it necessary to have equipment that can perform even in a GNSS-denied environment.

There are no backup systems available globally today that provide the same access level and precision as GNSS, so it is imperative that PNT systems are designed to continue to operate in a fielded environment. With a military telemetry system, that often means a GNSS-denied environment for some period.
Using a layered approach with technologies that fit the platform based on size, weight, power, and cost, a Resilient Positioning, Navigation and Timing (RPNT) system can be achieved. These layers are broken down into technology categories: Antenna technologies, GNSS receivers, angle of arrival techniques, filtering the GNSS signal using digital signal processing, detection algorithms that run on the GNSS receiver output, additional internal and external sensors, internal system integrity checks, and alternate signals where available.

To properly evaluate and harden GNSS based systems, it is important to have a test plan to first understand the current system state and performance in a GNSS denied environment, and then evaluate the improvements made by adding the applicable layers of protection, detection and mitigation. As new threats emerge, it is necessary to test and re-test to understand the impact of the new threats and continue to evaluate new technologies as they become available.

**Applications of PNT in Telemetry**

GNSS is used to provide time and position data for many telemetry applications. The extent to which GNSS signals provide critical synchronization and accurate position information to systems is not always obvious. For example, in a Satcom on the Move system, GNSS-derived low-phase, high-stability frequency is necessary to synchronize the receiver and transmitter. This type of system uses a directional antenna, so GNSS also provides position, UTC time, and, when combined with an IMU, attitude information to precisely steer the antenna.

Similarly, an airborne communications relay has the same needs, but may also need to provide precise timestamping to a crypto module. These precise time stamps are derived from GNSS signals.

In an intelligence, surveillance, reconnaissance (ISR) mission, there is antenna or lens steering, time stamping and georeferencing of images, ranging, time of arrival and angle of arrival processing, and receiver synchronization. Here, a low-phase noise, high-stability frequency reference is needed along with accurate UTC time, accurate 1PPS signal, position and attitude information. GNSS allows us to easily supply all the necessary signals to ensure proper system performance.

One of the more challenging synchronization and position applications is synthetic aperture radar (SAR). Because this system is used to create 2D or 3D images or reconstructions using radio waves, timing synchronization and accurate positioning information are critical and there is very little room for error. Figure 1 shows the timing and position signal used in such an application.

![Figure 1. Positioning and Timing in SAR](image)
A Layered Approach

Many technologies and techniques exist to detect when there is an issue with the GNSS signal. The issue could be a GNSS system error, unintentional interference, intentional jamming, or signal spoofing. With so many different applications, integrations and platforms using GNSS, it is not possible to develop a ‘one size fits all’ method to solve the issue. Instead, a layered approach allows the system designer or integrator to choose the best technologies and techniques to fit the needs of the mission.

The first category to examine is the antenna. This is where the signals first enter any system. The most common type of anti-jam antenna is a controlled reception pattern antenna (CRPA). These antennas vary in their number of elements but are typically found in two, four, seven, or eight element configurations, and there may be others.

In addition to the multi-element antenna, some antenna electronics are necessary to perform the adaptive signal processing. The multi-element antenna and antenna electronics can be housed in the same enclosure, or they can be separated to accommodate different platform installations.

CRPA antennas work by using spatial filters \(^1\), to attenuate the signal in the direction of the jammer(s) and amplify the wanted signals. Typically, the more elements the antenna has, the bigger it is, the more it costs, and the more power it needs. A two-element solution is much smaller and costs less than an eight-element system. Keeping in mind that the number of jammers or interfering signals that can be handled by the CRPA antenna is \(N-1\), where \(N\) is the number of antenna elements in the CRPA, it is possible to select an antenna solution that balances SWaP-C and performance for the mission.

A second type of anti-jam antenna is a horizon blocking antenna, such as Orolia's 8230AJ passive anti-jam outdoor antenna. This antenna has a fixed reception pattern, but it attenuates the signal more at the horizon than at the zenith. Figure 2 shows the antenna pattern of a horizon blocking antenna. The black lines show the pattern of the anti-jam antenna vs. a standard fixed reception pattern antenna.

GNSS receivers themselves can also provide some protection and added resiliency into the system. Whenever possible, a military grade SAASM or M-Code receiver such as the SecureSync with SAASM should be used. These receivers utilize encrypted GPS signals that are inherently anti-spoof and can also provide some protection against jamming and interference compared to a commercial receiver.

However, when an expensive military receiver is not feasible, there are other ways to use commercial receivers to detect problems with the GNSS signals or mitigate interference. First, one should choose a multi-frequency receiver that can operate independently on any frequency band. There are a variety of receiver types commercially available today, from L1/L5 band receivers typically found in low-end applications such as cellular phones, to L1/L2/L5/L6 receivers typically found in highly scientific applications.
such as ionosphere monitoring. Using this type of receiver will allow the positioning and timing information to continue to be provided to the system -- for example, if only the L1 band is jammed.

Another way to use GNSS receivers for PNT resiliency is to install more than one in the system and set them to use different constellations. This allows the output of each receiver to be validated by the system, and it allows for identification of a specific GNSS system error or denial of service.

In the same way that it is possible to use multiple receivers for detection of problems with a GNSS constellation, it is also possible to use multiple antennas to detect a spoofing attack. In the live sky, the signals are all coming from different directions. Typically, in a spoofing attack, the GNSS signals are all coming from the same direction (wherever the transmit antenna is located). Using multiple small, embedded antennas and receivers, a small detection device can alert the system or user to the presence of spoofing. A good example is GPSdome, the industry’s first non-ITAR GPS anti-jammer. This type of anti-jammer can also be used to mitigate spoofing signals and allow the system to continue to operate as normal.

The next technique is to use digital signal processing to remove some of the jamming signals, with a solution such as ThreatBlocker. With ThreatBlocker, The RF signal is down-converted by an analog to digital converter, the processing is done on the IQ data in an FPGA, then the signal is up-converted to RF again by a digital-to-analog converter. This technique uses a set of algorithms and, unlike conventional techniques that only focus on removing narrow-band jamming over a small frequency range, is highly effective against jammers that vary in frequency or phase [2]. Figure 3 shows the block diagram of a device utilizing this technology [3]. In this diagram, the specific technique is called BLISS (Blind Interference Signal Suppression).

Another technique used to detect GNSS signal interference is to look at the raw data output of the receiver and check that data for validity and anomalies. The GPS navigation message has many fields of data that can be checked. Checking these fields for valid and consistent information lets you detect spoofing signals. The invalid data is flagged by the algorithms and checks as out of range, invalid pattern, or inconsistent data. When enough small errors are found, the system alerts that spoofing has been detected. Different weights can be assigned to the different algorithms so that the solution can be tailored to the environment the system will operate in. In Figure 3 right, this weighting solution is BroadShield, Orolia’s proprietary jamming and spoofing detection solution that is also available to integrate into a SecureSync®, VersaSync or VersaPNT time and frequency reference. In the system illustrated above, BroadShield is used to activate BLISS within ThreatBlocker.

In addition to GPS, it is important to use additional sensors and internal oscillators to have a variety of available data sources. This lets your system continue to operate if GNSS is not available or usable. Timing-based systems typically use a high-quality OCXO (Oven-Controlled Crystal Oscillator)
or atomic clock. When power and space are not an issue, a rubidium oscillator can be combined with an OCXO when low-phase noise is needed. Where a low SWaP solution is necessary, the choice becomes an OCXO, a chip scale atomic clock (CSAC) or miniature atomic clock (MAC). Often a trade-off needs to be made when selecting an oscillator; a lower power solution may sacrifice phase noise performance, for example. Table 1 shows a comparison of three common oscillator types.

GNSS is typically used to discipline the oscillator. Discipling the oscillator with GPS or GNSS through SecureSync allows for traceable UTC and compensates for phase and frequency changes due to aging, temperature and environment. When the GNSS signal is lost, the SecureSync system can still provide accurate time for hours or even days. Using just the disciplined oscillator to provide accurate timing without GNSS input is called “holdover.”

Similarly, for position, an inertial measurement unit (IMU) along with GNSS can be used to provide accurate six degrees of freedom position information (X, Y, Z, pitch, roll, yaw). An IMU combined with processing, such as VersaPNT, provides an optimal estimation of position, velocity and acceleration indicated by the sensor, using Extended Kalman filtering processing or an inertial navigation system (INS).

GNSS and the IMU in an INS can be loosely coupled or tightly coupled. In a loosely coupled system, the inertial trajectory is computed separately from the GNSS trajectory, then the two are combined. In a tightly coupled system, the GNSS and IMU data are processed together at the same time [4]. Figure 4 shows an example of a tightly coupled system.

<table>
<thead>
<tr>
<th>Timebase Performance</th>
<th>OCXO¹</th>
<th>CSAC²</th>
<th>Miniature Atomic Clock³</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency variation with again</td>
<td>One month</td>
<td>One year</td>
<td>One month</td>
</tr>
<tr>
<td>Phase Noise dBc/Hz</td>
<td>10Hz</td>
<td>100Hz</td>
<td>1kHz</td>
</tr>
<tr>
<td>-129</td>
<td>-145</td>
<td>-155</td>
<td>-165</td>
</tr>
<tr>
<td>Size</td>
<td>12.7 x 21.6 x 9.5 mm</td>
<td>40.64 x 35.31 x 11.43 mm</td>
<td>18.3 x 50.8 x 50.8 mm</td>
</tr>
<tr>
<td>Weight/Volume</td>
<td>~2cm³</td>
<td>&lt;35g/&lt;17cm³</td>
<td>85g/49.5cm³</td>
</tr>
<tr>
<td>Power</td>
<td>1200mW Warmup</td>
<td>140mW Warmup</td>
<td>14W Warmup</td>
</tr>
<tr>
<td>180mW Operating</td>
<td>120mW Operating</td>
<td>5W Operating</td>
<td></td>
</tr>
</tbody>
</table>

¹Magic Xtal MX037/14P  ²Microsemi SA.45s  ³Microsemi SA.35m

Table 1. Oscillator Comparison

---

**Figure 4. Tightly Coupled INS**
An INS can operate without GNSS for seconds or sometimes minutes. The drift and accuracy of the IMU is dependent on what type of IMU is used. On the low end (but still suitable for many applications) is the Micro Electro-Mechanical Systems (MEMS) IMU. On the high end of performance are Fiber Optic Gyros (FOG), and Ring Laser Gyros (RLG). While the MEMS IMU can be very small (10mm) and inexpensive, the FOG and RLG are large and costly. Again, the proper performance, price and size balance is needed to meet the requirements of the integration platform or mission.

Other sensors that can be used to provide additional position or motion information into the system include Lidar, radar, odometers, wheel ticks, and cameras. Although these additional sensors may not be enough to provide accurate timing and position information by themselves, when combined with GNSS, oscillators and/or IMUs, the information can increase the accuracy of the system, provide more data for integrity checks and allow single and multi-reference validity check algorithms to run.

There may be other external systems available to back up or augment GNSS. A regional system that can be used when available is eLORAN. This is a high-powered, terrestrial, low-frequency system that is being researched as a backup to GNSS globally, but today it is only available in a small part of the world. An alternate spaced-based system, Satellite Time and Location (STL) from Satelles, is an encrypted signal transmitted by Iridium satellites. STL is a subscription-based service for a global alternative signal [5]. Available local systems may include pseudolites or other ground transmitter-based systems.

Regardless of the external signals or external and internal sensors used, it is important to validate the signals. Signal validation can be done on each individual reference, then compared to the IMU for positioning or to the internal oscillator for timing references. For example, if the IMU is showing no movement, and the GNSS receiver is reporting that the system is moving at 20 m/s, there is a contradiction, and the system or the operator should be notified that an issue may exist. After each individual reference has been validated, it is possible to compare the references for continuous integrity checks, identify outliers and select the best possible combination of signals.

**Vulnerability Testing**

As discussed earlier, the GNSS receiver(s), whether military or commercial, is at the core of many PNT systems. Although the layered approach is the best available method for hardening systems against GNSS system error or attacks, the individual receiver chosen for integration is also important. To evaluate receivers and systems against spoofing attacks, a spoofing test system such as the BroadSim or GSG-8 simulator should be used. The test system should contain two GNSS simulators, one to act as the ‘live sky’ signal, and one to act as the ‘spoof’ signal. If U.S. military encrypted signals are needed, BroadSim is appropriate; if they are not, GSG-8 is appropriate. This test system allows the tester to vary the three important parameters needed to test spoofing: time, position, and power level [6]. These parameters are shown in figure 5 below.

![Figure 5. Important Parameters for Spoofing Testing](image-url)
The time parameter refers to the timing accuracy of the spoofing signals to the live signals. This offset is controllable to the nanosecond level in the test system.

Another time to consider in the test design is the capture time. This is how long the spoofing signal is applied before attempting to re-direct the receiver.

The position provided by the spoofer must be accurate to that of the receiver that will be spoofed. Exactly how close the spoofer must be to the receiver position is a variable parameter and can be different based on receiver settings, receiver manufacturer and initial conditions (moving vs. stationary). Using two simulators allows full control of both positions so that many different test cases can be designed and executed to understand the receiver's limitations. The more accurate the spoofer must be to successfully take control of the receiver, the more difficult it will be for an attacker to spoof the receiver.

The spoofing signal should be greater than the live signal to capture the receiver. The spoofing test system allows full control of the power levels to determine how much greater the power should be. Too much power will jam the receiver. The test system allows testing of the receiver to determine whether the receiver gives any indicators when it receives a signal that is only a few dB higher than the transmitted signal.

Several test cases were designed to observe the effects of varying the critical parameters and attempting to spoof the receiver.

- Four TIME offset test cases were created. For these cases, the position offset was 0 meters and the power level of the spoofer was 2dB higher than the live sky simulator. Offsets of 1 nanosecond, 100 nanoseconds, 500 nanoseconds, and 1.5 microseconds were tested.

- Three POSITION offset test cases were created. For these test cases, the time offset was set to 1 nanosecond and the power level of the spoofer was 2dB higher than the live sky simulator. Offsets of 50 meters, 250 meters, and 500 meters.

- Three POWER offset test cases were created. For these test cases, the time offset was set to 1 nanosecond and the position offset was set to 0 meters. Offsets of 2dB, 1dB, and 0dB were tested.

- Multi-GNSS. In this case, the live sky simulator was set to simulate GPS and GLONASS. The spoofer was set to GPS-only. The position offset was set to 0 meters, the time offset was set to 1 nanosecond, and the power level of the spoofer was 2dB higher than the live sky simulator.

These test cases can be used to evaluate the receiver performance, and new test cases can be developed and run on the test system as well. Figure 6 shows the test cases.

<table>
<thead>
<tr>
<th>Time Offsets</th>
<th>Position Offsets</th>
<th>Power Level Offsets</th>
<th>Multi-GNSS Offsets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 ns</td>
<td>50 m</td>
<td>2 dB</td>
<td>Live Sky</td>
</tr>
<tr>
<td>100 ns</td>
<td>250 m</td>
<td>1 dB</td>
<td>Multi-GNSS</td>
</tr>
<tr>
<td>500 ns</td>
<td>500 m</td>
<td>0 dB</td>
<td>Spoofing</td>
</tr>
<tr>
<td>1.5 usec</td>
<td></td>
<td></td>
<td>GPS-only</td>
</tr>
</tbody>
</table>

*Figure 6. Example Test Cases for Spoofing Testing*
Conclusion

Engineers and integrators who design and develop systems for military and commercial telemetry should be aware of the reliance of their systems on GNSS. From Satcom on the Move to Synthetic Aperture Radar, GNSS provides the accurate timing and positioning information that allows these systems to operate properly. In order to design a resilient system that can continue to operate accurately in GNSS denied environments, a layered approach should be considered. By layering in the technologies and techniques currently available to such systems, a very robust system can be developed within the size, weight, power, and cost of the program.

In addition to considering layers at the design stage, a GNSS vulnerability test system should be utilized during development and throughout the product lifecycle to ensure that the system continues to operate correctly, even in the face of new threat developments. By simulating the environment that the system will operate in, continuous improvement is possible, even in the lab.

References


About the Authors

Lisa Perdue is the product manager for Simulation & IDM at Orolia and a world-leading expert in testing critical GPS and GNSS systems. She has trained hundreds of engineers and technicians who are responsible for high-reliability positioning, navigation and timing (PNT) applications. She took a lead role in the development of the first GNSS Vulnerability Test System and speaks widely on the topic.

John Fischer is VP of Advanced R&D at Orolia, where he has specialized in GNSS, wireless, positioning navigation and timing (PNT) and related systems for more than 15 years. Prior to joining Orolia, he was a founding member of two wireless telecom startups: Aria Wireless and Clearwire Technologies.

About Orolia

With a presence in over 100 countries, Orolia provides virtually failsafe GPS/GNSS and PNT solutions to support military and commercial applications worldwide. Orolia is the world leader in Resilient Positioning, Navigation and Timing (PNT) solutions that improve the reliability, performance and safety of critical, remote or high-risk operations.