RESILIENT PNT / TSPI ALTERNATIVE SOLUTIONS FOR TELEMETRY DURING GNSS OUTAGE TEST SCENARIOS

John Fischer, Lisa Perdue
Orolia
Rochester, NY, USA
John.Fischer@orolia.com
Lisa.Perdue@orolia.com

ABSTRACT

GNSS 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 one 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 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 GNSS, including GPS, is widely used in telemetry would be an understatement. In fact, it is almost exclusively used, 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 have been made more available to anyone interested in denying GNSS service to a specific area. That, added to the GNSS system

vulnerabilities that exist due to the system design, make it necessary to have equipment that can perform its function even in a GNSS denied environment.

There are no backup systems available globally today that can 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 of time.

Using a layered approach with technologies that fit a platform based on the size, weight, power, and cost, a resilient positioning, navigation, and timing system can be achieved. These layers are broken down into technology categories: Antenna technologies, GNSS receivers, angle of arrival techniques, filtering of the GNSS signal using digital signal processing, detection algorithms run on the GNSS receiver output, additional internal and external sensors, internal system integrity checks, and alternate signals where available.

In order 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 in 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 on the market.

APPLICATIONS OF PNT IN TELEMETRY

GNSS is used to provide time and position data for many applications related to telemetry. 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 for synchronization of the receiver and transmitter. This type of system uses a directional antenna, so GNSS also provides position, UTC time, and, combined with an IMU, attitude information in order 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 timestamps are derived from GNSS signals.

In an intelligence, surveillance, reconnaissance (ISR) mission, there is antenna or lens steering, timestamping and geo-referencing 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). As this system is used to create 2D or 3D images or reconstructions using radio waves, timing synchronization and accurate positioning information are critical to the application, and there is very little room for error. Figure 1 shows the timing and position signal used in such an application.

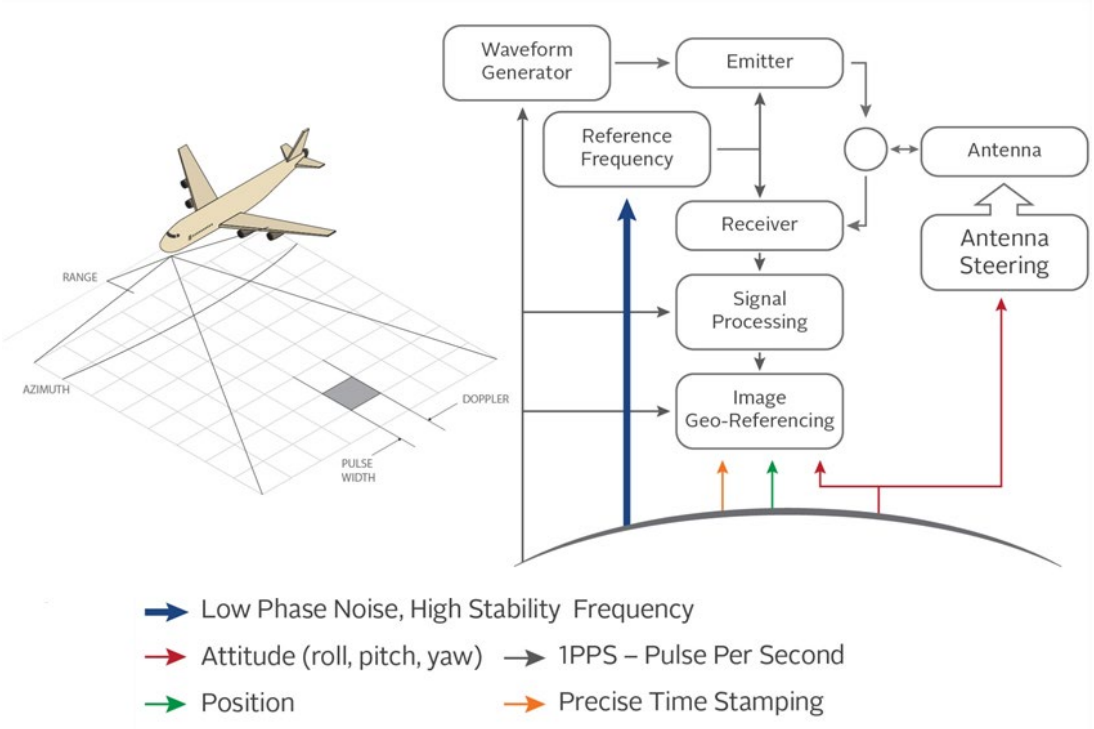

Figure 1. Positioning and Timing in SAR

A LAYERED APROACH

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 solving 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. Afterall, 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 range in their number of elements but are typically found in two, four, seven, or eight element configurations, although 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 the 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 lower cost 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.

This type of 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 that of a standard fixed reception pattern antenna.

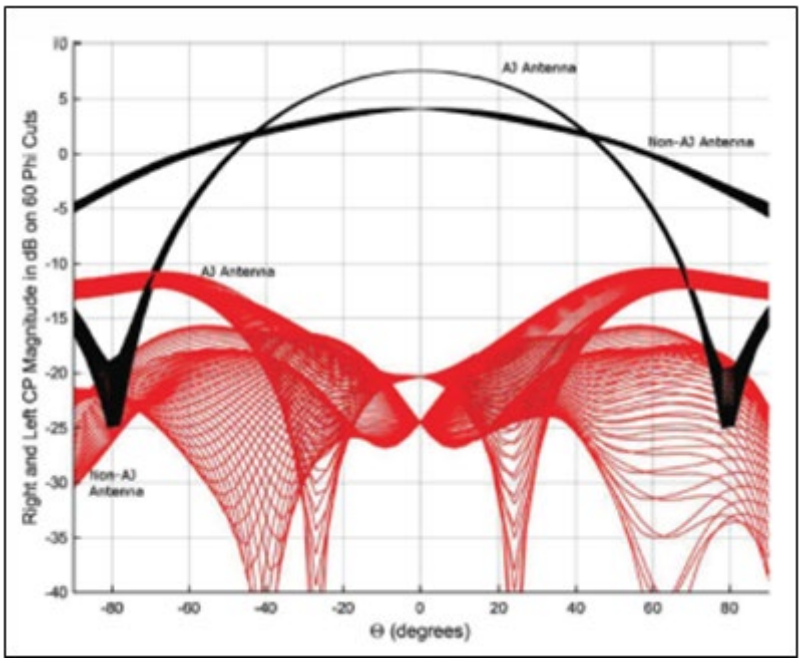

Figure 2. Horizon Blocking Antenna Pattern

GNSS receivers themselves can also provide some protection and added resiliency into the system. Whenever possible, a military grade SAASM or M-Code receiver should be used. These receivers utilize encrypted GPS signals that are inherently anti-spoof and can also provide some protection against jamming and interference when compared to a commercial receiver. When using an expensive, military receiver is not feasible however, 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 is capable of operating 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. Utilizing 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 of the receivers 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 particular 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. This type of system can also be used to mitigate the spoofing signals and allow the system to continue to operate as normal.

The next technique is a digital signal processing technique that allows the removal of some of the jamming signals. 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 mentioned technique is called BLISS (Blind Interference Signal Suppression).

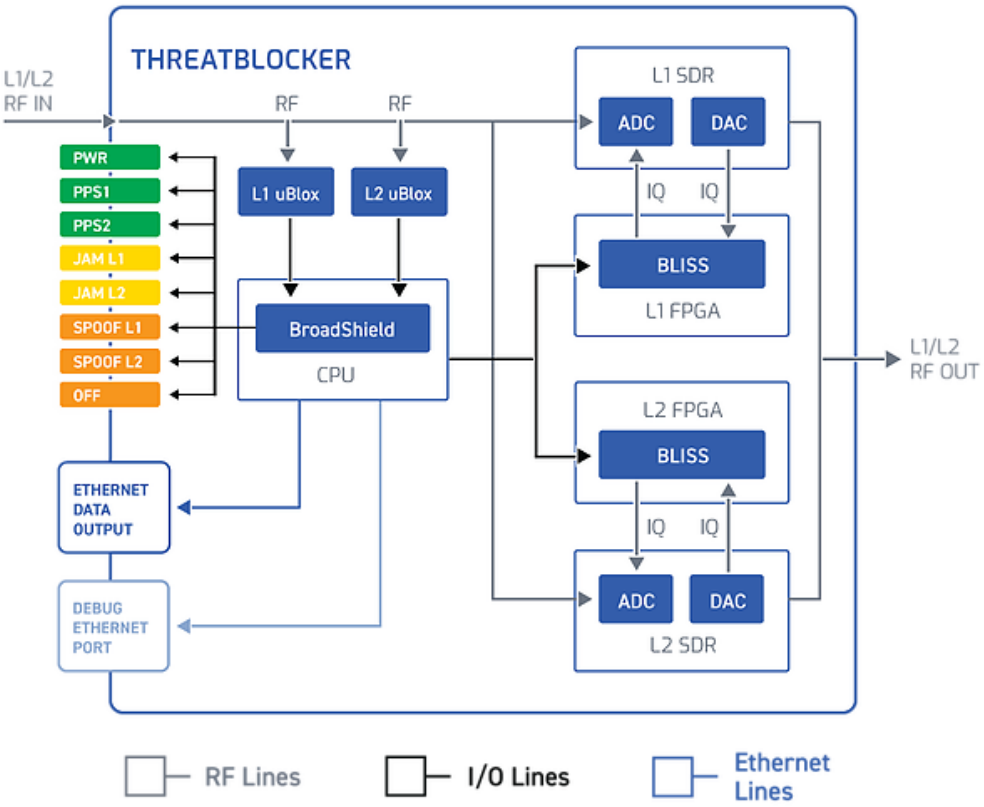

Figure 3. Block Diagram of Device Utilizing BLISS

Another technique used to detect whether or not a GNSS signal has been interfered with is by looking at the raw data output of the receiver and checking 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, allows for detection of 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 allowing the solution to be tailored

to the environment the system will be operating in. In Figure 3 above, this solution is labeled BroadShield and in that system it is used to activate BLISS.

In addition to GPS, it is important to use additional sensors and internal oscillators to have a variety of data sources available. This allows the system to continue to operate in the event GNSS is not available or not usable. For timing-based systems typically a high quality OCXO or atomic clock is used. When power and space are not an issue, a rubidium oscillator is used and 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.

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

Timebase Performance	OCXO[1]				CSAC[2]				Miniature Atomic Clock[3]			
Frequency variation with aging	One month		One year		One month		One year		One month		One year	
	$4x10^{-9}$		$2x10^{-8}$		$9x10^{-10}$		$1x10^{-8}$		$1x10^{-10}$		$1x10^{-9}$	
Phase Noise dBc/Hz	10Hz	100Hz	1kHz	10kHz	10Hz	100Hz	1kHz	10kHz	10Hz	100Hz	1kHz	10kHz
	-129	-145	-155	-165	-70	-113	-128	-135	-87	-114	-130	-140
Size	12.7 x 21.6 x 9.5 mm				40.64 x 35.31 x 11.43 mm				18.3 x 50.8 x 50.8 mm			
Weight/Volume	~$2cm^3$				<35g/<$17cm^3$				85g/$49.5cm^3$			
Power	1200mW Warmup 180mW Operating				140mW Warmup 120mW Operating				14W Warmup 5W Operating			

Table 1. Oscillator Comparison

GNSS is typically used to discipline the oscillator. Discipling the oscillator with GPS or GNSS allows for traceable UTC and compensates for phase and frequency changes due to aging, temperature and environment. When the GNSS signal is lost, the system can still provide accurate time for hours, or even days in some cases. 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 6 degrees of freedom position information (X, Y, Z, pitch, roll, yaw). An IMU combined with processing provides an optimal estimation of position, velocity and acceleration as 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 is processed together, simultaneously [4]. Figure 4 shows an example of a tightly coupled system. 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 the 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.

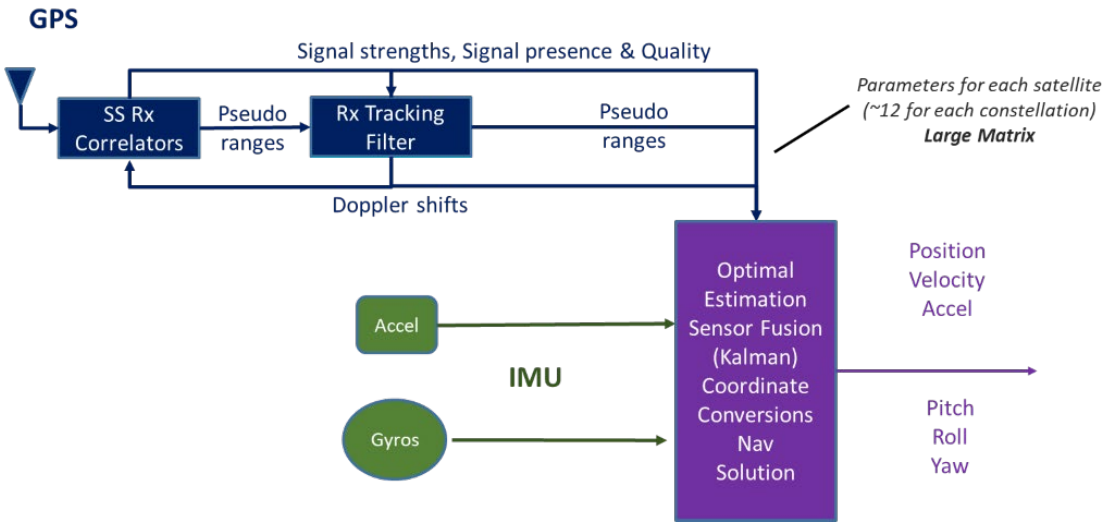

Figure 4. Tightly Coupled INS

Other sensors that can be used to provide additional position or motion information into the system include: Lidar, radar, odometers, wheel ticks, and cameras. While these additional sensors may not be enough to provide accurate timing and position information alone, when combined with GNSS, oscillators and/or IMUs the information can be used to 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 use as a backup or augmentation to GNSS. A regional system that can be used when it is available is eLORAN. It 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 from Satelles, is an encrypted signal transmitted by the Iridium satellites. It is a subscription service that users can purchase to access the signal globally [5]. Available local systems may include pseudolites or other groundtransmitter-based systems.

Regardless of the external signals, the external sensors, and the internal sensors used, it is important to validate the signals. Signal validation can be done on each individual reference, 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 the system is moving at 20m/s, there is a contradiction and the system or the operator should be notified that an issue may exist. Once the signal validation has passed on each individual reference, it is possible to compare the references to each other for continuous

integrity checks, to identify outliers, and select the best possible combination of signals for system operation.

VULNERABILITY TESTING

As discussed in the previous section, the GNSS receiver(s), whether military or commercial, is at the core of many PNT systems. While 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 should be used. The test system contains two GNSS simulators, one to act as the 'live sky' signal, and one to act as the 'spoofer' signal. 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.

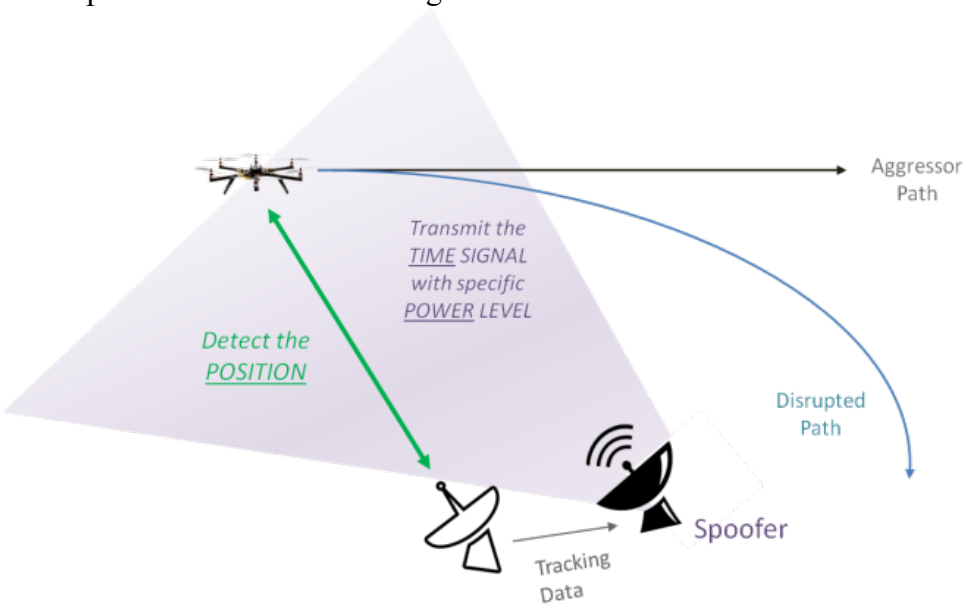

Figure 5. Important Parameters for Spoofing Testing

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 to 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 the two positions so many different test cases can be designed and executed to understand the receiver 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 in order 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 try and determine if there are any indicators given by the receiver when a signal only a few dB higher than the transmitted signal is received.

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 thespoofer 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 is 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.

Figure 6. Example Test Cases for Spoofing Testing

CONCLUSION

Engineers and integrators that 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 allow 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, the system will operate in, continuous improvement is possible, even in the lab.

REFERENCES

[1] Jones, M. (2017, April 12). Anti-jam technology: Demystifying the CRPA. Retrieved from https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/.

[2] A New Tool To Fight GPS Jammers. (2019, March 31). Retrieved from https://aerospace.org/article/new-tool-fight-gps-jammers.

[3] (n.d.). GPS Jamming and Spoofing Protection. Retrieved from https://www.talen-x.com/threatblocker.

[4] (n.d.). Loosely Coupled and Tightly Coupled. Retrieved from https://www.novatel.com/support/waypoint-software-getting-started/first-project-example/processing/loosely-coupled-and-tightly-coupled/.

[5] Satelles. (2019, June 25). Technology. Retrieved from https://www.satellesinc.com/technology-2/.

[6] Perdue, L., Sasaki, H., & Fischer, J. (2015). Testing GNSS Receivers to Harden Against Spoofing Attacks. *International Symposium on GNSS 2015.*