Making Time Sensitive Networks Resilient Against Threats: Recent Advances

By John Fischer, VP, Advanced R&D and
Jeremy Onyan, Director, Time Sensitive Networks

May 2018

Executive Summary

Today's time sensitive networks rely on available and accurate positioning, navigation and timing (PNT) signals to provide leaders with the information required to make timely and effective decisions. Signals provided by global navigation satellite systems (GNSS) such as GPS represent the gold standard in terms of availability and accuracy. However, the proliferation of GNSS-degrading and denying devices across state and non-state actors puts this critical information overmatch capability in jeopardy. Traditional PNT devices utilize various alternative internal components to maintain holdover of the PNT data during loss of GNSS input but are susceptible to drift over time. This white paper discusses alternative signals that are suitable for time sensitive networks.

A combination of these alternative PNT signals with traditional GNSS references makes PNT applications resilient against GNSS jamming and spoofing and suitable for operation in GPS-denied environments.

Fig. 1: Datacenter

Who Should Read This White Paper?

- Network Engineers
- Network Architects
- Chief Technology Officers
- Communications Engineers
- Information System Security Engineers
- Validation Engineers and Test Engineers
- Application Engineers
- Systems and Requirements Analysts
- System Administrators

The Evolution of Resilient PNT

Many of our civil infrastructures are reliant on GPS (Global Positioning System) to provide the trusted PNT data that allows their time sensitive networks to operate accurately and precisely. Financial markets, communications systems, and public utilities all trust on GPS to provide this information.

As GPS and other GNSS signals become ubiquitous in how we operate, threats to the availability and integrity of GPS signals are growing. Modern state and criminal threat actors have little difficulty gaining access to portable devices that can jam and spoof GPS signals. As GPS use spreads into more mobile applications farther afield, even natural and urban terrain must be accounted for when considering PNT availability.

To combat threats to GPS signal availability and trust, other techniques and signals of opportunity must be considered as alternate sources of PNT information when GPS is not available. Although GPS will remain the most accurate system for now, correctly integrating combinations of other signals is the recipe for resilient systems that can survive operations for the duration of GPS signal loss.

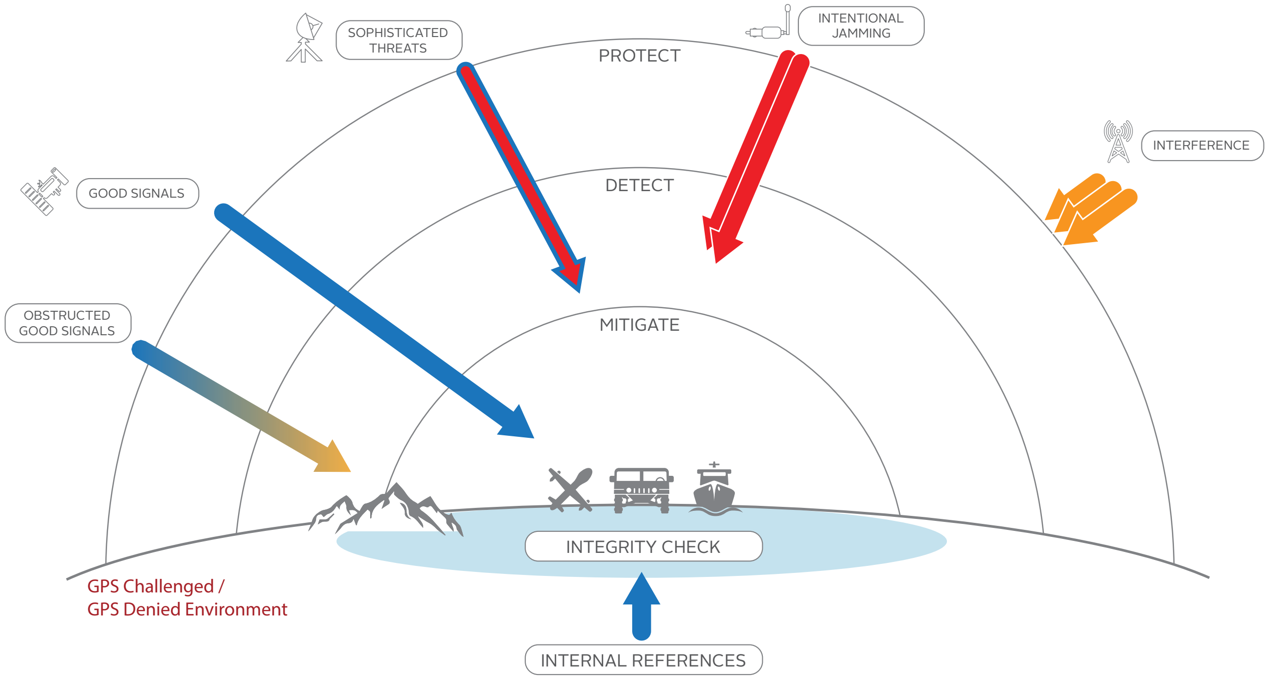


Fig. 1: GPS threat mitigation

GNSS – A Brief Recap

GPS is probably the most well-known GNSS constellation. It is operated by the U.S. Dept. of Defense and consists of over 24 active satellites and several spares orbiting the earth at an altitude of approximately 20,000 km. To determine one's position on earth, at least four satellites must be received. All satellites transmit synchronized pulses at regular intervals. Even though the pulses from the satellites in view travel at (or near) the speed of light, they will not quite reach the receiver at the same time because they travel different distances. Using the signal delays of three satellites, the receiver calculates the x, y and z coordinates of its current position (the "3D fix").

The fourth signal is required for the start-of-transmission time mark: This time mark needs to be extremely accurate to measure the miniscule transmission delays in between the other three satellite signals.

Reliance on GNSS

Not only the military relies on trusted GPS time: The U.S. Department of Homeland Security has identified 16 industries as critical to the U.S. infrastructure:

- Chemical sector
- Commercial facilities
- Communications sector
- Critical manufacturing
- Dams sector
- Defense industrial base
- Emergency services
- Energy sector
- Financial services
- Food & agriculture
- Government facilities
- Health & public health
- Information technology
- Nuclear reactors, materials & waste
- Transportation system
- Water & wastewater

Considering the scope of reliance on GPS and GNSS, the question arises: Which technologies are suitable to supplement GPS?

A brief overview of GNSS vulnerabilities may help to better understand potential threats, thus providing direction towards detection and mitigation technologies that are available today.

GNSS Vulnerabilities

Compared to other RF signal levels, GNSS signals are exceptionally weak. The satellites are orbiting at approximately 11,000 miles above the surface of the earth and the transmission power of a GPS satellite transmitter is in the 10-100W range. By the time the signal reaches Earth, it is weaker than the atmospheric background noise level in its band (this is referred to as a negative signal-to-noise level). In other words, if you tuned a standard RF receiver into the GPS L1 frequency band of 1575.42 MHz, for example, you would hear or see nothing but background noise.

A GNSS receiver can extract this weak signal from the noise by utilizing its processing gain because it "knows" which signal pattern to look for: After the search pattern correlates with the actual signal pattern – a match has been detected – the decoding of the data stream begins and the positions for the satellites in view can be extracted as well as their distances from the receiver. As soon as this data is available, the receiver can calculate its position.

Although modern multi-GNSS receivers can receive several GNSS constellations simultaneously and therefore offer better coverage in locations with limited view of the sky (e.g., in "urban canyons"), a shortcoming of GNSS-based PNT applications remains the low signal strength, which makes all GNSS signals particularly vulnerable to disruption.

To better understand the threats against GNSS, the GNSS vulnerabilities are typically divided into two categories: jamming and spoofing.

Jamming

The terms "jamming" and "interference" are often used synonymously. Jamming generally refers to intentional interference by means of a radio-frequency signal. Interference sometimes is used in the context of natural causes such as atmospheric phenomena. The effect is the same for both: The ability of the GNSS receiver to extract GNSS signal information from the background noise is impaired or rendered impossible.

There also is unintentional jamming: RF transmitters bleeding into the GNSS frequency bands are often times the source of this.

Illegal consumer-grade GPS jammers (sometimes referred to as Personal Privacy Devices [PPD]) fall under the category of intentional jamming, even though they typically target a different receiver. For example, nearby stationary receivers are "merely" collateral victims of the jamming event. These devices may become more popular over time as public concern over personal privacy grows.

Military receivers use the encrypted SAASM GPS signal to ensure that the signal received can be trusted, Encrypted signals are considered safe against spoofing because you are assured of their authenticity. Yet, even these signals can still be jammed with minimal technical effort: A 1–10 W jammer can deny GPS coverage for a large area, no matter whether the signals are encrypted or not. The new M-code, which replaces the SAASM encryption technology, is slightly less prone to jamming, but by no means immune. And for civilian or commercial use, SAASM is not available.

Fig. 3: A mobile GPS jammer targeting the onboard GPS-tracking device

Spoofing

Spoofing, which is sometimes also referred to as complex jamming or GPS hacking, is the act of broadcasting false signals with the intent of deceiving a GNSS receiver into accepting the false signals as genuine.

From a technical perspective, spoofing GNSS receivers is more challenging than jamming, but the consequences can be more severe because the receiver actually uses the manipulated signals for PNT calculations, and neither the system nor the operator realizes that the indicated PNT data has been corrupted. Spoofing can relocate the receiver, which is not possible with jamming.

The first step of a spoofing attack is to synchronize the spoofing equipment to the live sky signal to capture the receiver that is already tracking the real signal. This includes synchronizing to the live sky time signal, position signals and the power level — if any of these are too far off, the receiver may get jammed, or it actively rejects the spoofed signal.

After the synchronization has been successful, the power level can be increased gradually, thus masking the real signal, and the manipulation of the position and timing data can begin.

Spoofing is not an easy undertaking, especially if the spoofing target is moving fast. But it has been done, and the threat is considered real -- and growing -- by both government departments and private critical infrastructure operators.

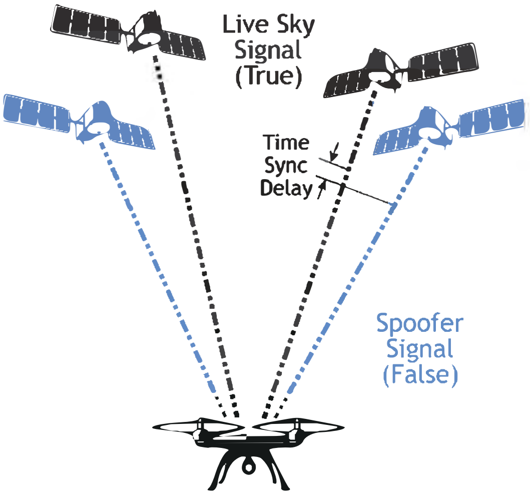


Fig. 4: Spoofing – schematic diagram

Examples of Spoofing and Jamming

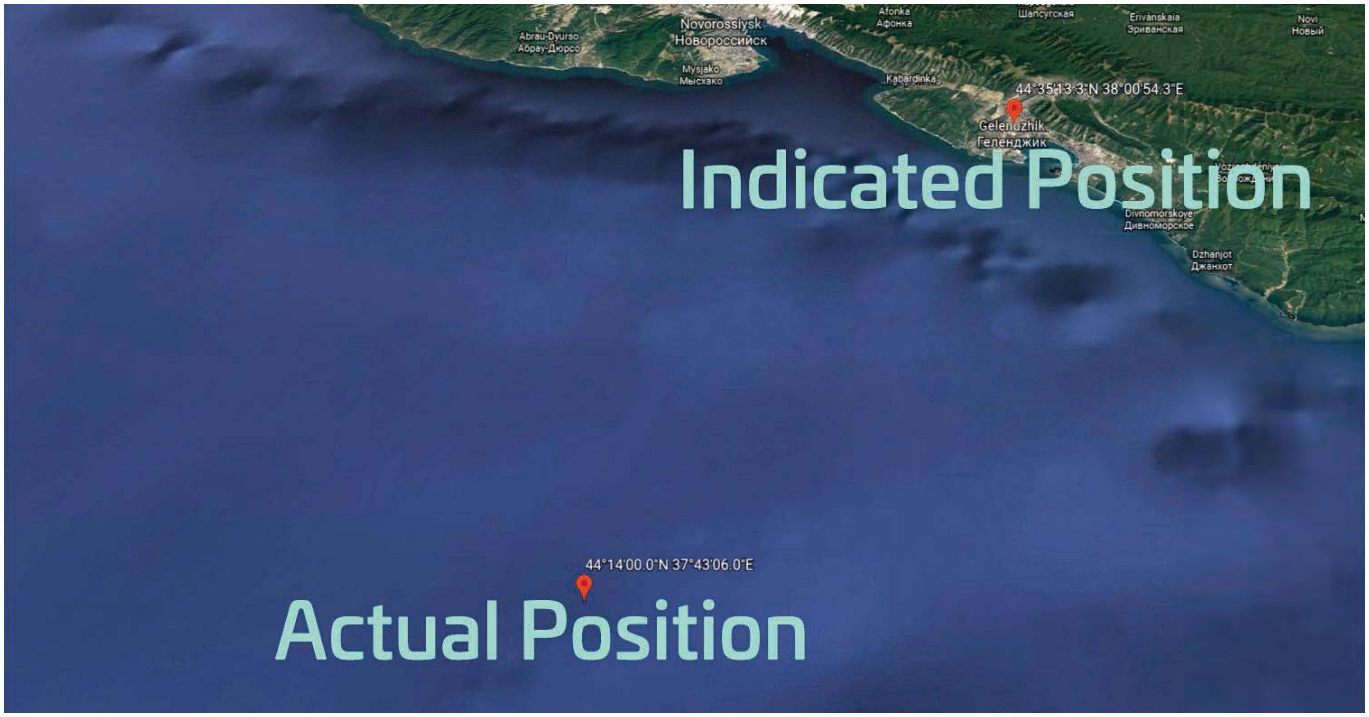


Fig. 5: Presumed Spoofing incident, Black Sea, 2017 (Image: Courtesy of Google Earth)

- A major datacenter was experiencing issues with its GNSS-based timing systems. For unknown reasons, GNSS reception was being intermittently lost. Though the timing system used time servers with internal atomic clocks, this datacenter was critical to network operations and any signal loss was an issue. Installation of an anti-jam antenna proved that the signal loss was a result of RF interference; a nearby trucing company was being visited by trucks using privacy jammpers that interfered with GNSS reception.
- As reported in July 2017 by maritime media, some 20 ships in the Black Sea were placed by their AIS (Automatic Identification System) to a location that was reported to be 25 NM off their actual positions. Tracking websites such as MarineTraffic reportedly used the incorrect AIS data and temporarily "relocated" the affected vessels inland. The spoofing event may have been caused by a Russian system. Russia is believed to have worked extensively with GPS disruption technology, and continues to maintain their own terrestrial Loran system to supplement GLONASS. http://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea
- On a non-disclosed day in the summer of 2015, several ships leaving a non-U.S. port were reported to suddenly have lost the GPS signal, causing problems with the ship's surface search radar, gyro units and other electronic navigation equipment. As a result, the vessels lost their position fixes, several n avigation-related data inputs and collision avoidance capabilities. Following this incidence, the U.S Coast Guard issued a Safety Alert in January 2016, warning mariners about the potential

consequences of losing the GPS signal ("Trust But Verify").
https://rntfnd.org/2016/01/19/uscg-issues-safety-alert-gpsgnss-trust-but-verify/

- In August 2013 the U.S. Federal Communications Commission (FCC) proposed a fine of nearly $32,000 for an individual whose illegal use of a GPS jamming device near the Newark Airport interfered with an aviation safety system in 2012. It took several years and highly specialized equipment to identify that a jammer was being used.
https://transition.fcc.gov/eb/Orders/2013/FCC-13-106A1.html

As these examples demonstrate, signal disruptions can either cause a signal to become unreadable, or they can undermine the authenticity of the signal -- it can no longer be trusted. To combat threats to GPS signal availability and trust, other techniques and signals of opportunity must be implemented into resilient PNT systems to make them operational in GPS-denied environments.

Interference Detection and Mitigation

The tactics and technology used to combat jamming are referred to as **Interference Detection and Mitigation** (IDM). Protection against jamming and spoofing also falls under the "combatting interference" umbrella, as does testing of GNSS components and PNT systems against jamming and spoofing.

When it comes to answering the question: **"What makes a PNT application resilient against spoofing and jamming?"** the short answer is: **"Integrating a strong and well-coordinated IDM solution into a PNT system makes it resilient against jamming and spoofing."**

The long answer is best illustrated by Figure 6 below, which depicts the different technologies that can be used to augment a PNT solution to obtain a technically well-diversified selection of alternative PNT sources. These sources can be dedicated navigation systems, but can also be unrelated technologies such as cellular systems, which were designed for a different purpose, yet can – under certain circumstances – provide useful PNT data.

The overarching objective in the selection of sources should always be a mix of different technologies and different platforms; e.g., terrestrial vs. space-based, microwave vs. long wave etc., thereby decreasing the likelihood that an interference impacts more than one PNT sources.

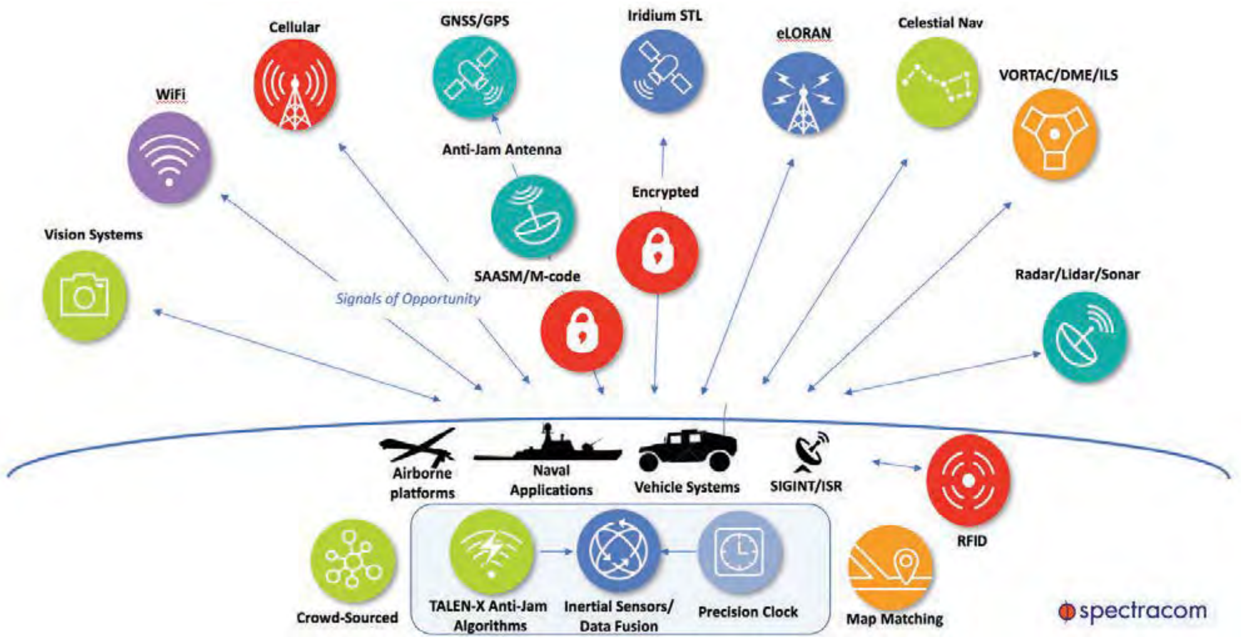


Fig. 6: Overview of alternative signals for resilient PNT

Protecting against Interference

The objective here is to prevent the unwanted or corrupted signals and data from entering the system in the first place. This can be accomplished by using electrically steerable directional antennas, which are also called Controlled Reception Pattern antennas (CRPA), or "smart" antennas. Although conventional antennas offer the full hemispherical coverage so they can receive signals from the entire sky and thus can listen to 8 – 12 satellites simultaneously in order to obtain the best navigation solution, CRPAs are equipped with technology that enables them to focus narrow beams directly at the satellites, then track them as the move along their trajectory. These devices offer a significant degree of jamming protection but are expensive and larger than regular GNSS antennas.

Another technological approach to protect a GNSS receiver against jamming is the horizon-blocking antenna: This type of antenna will reject signals transmitted near the horizon, because these are more likely to be ground-based jammers.

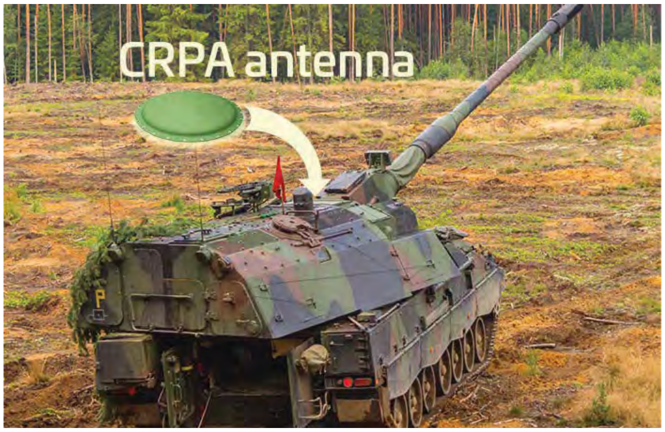


Fig. 7: CRPA antenna application

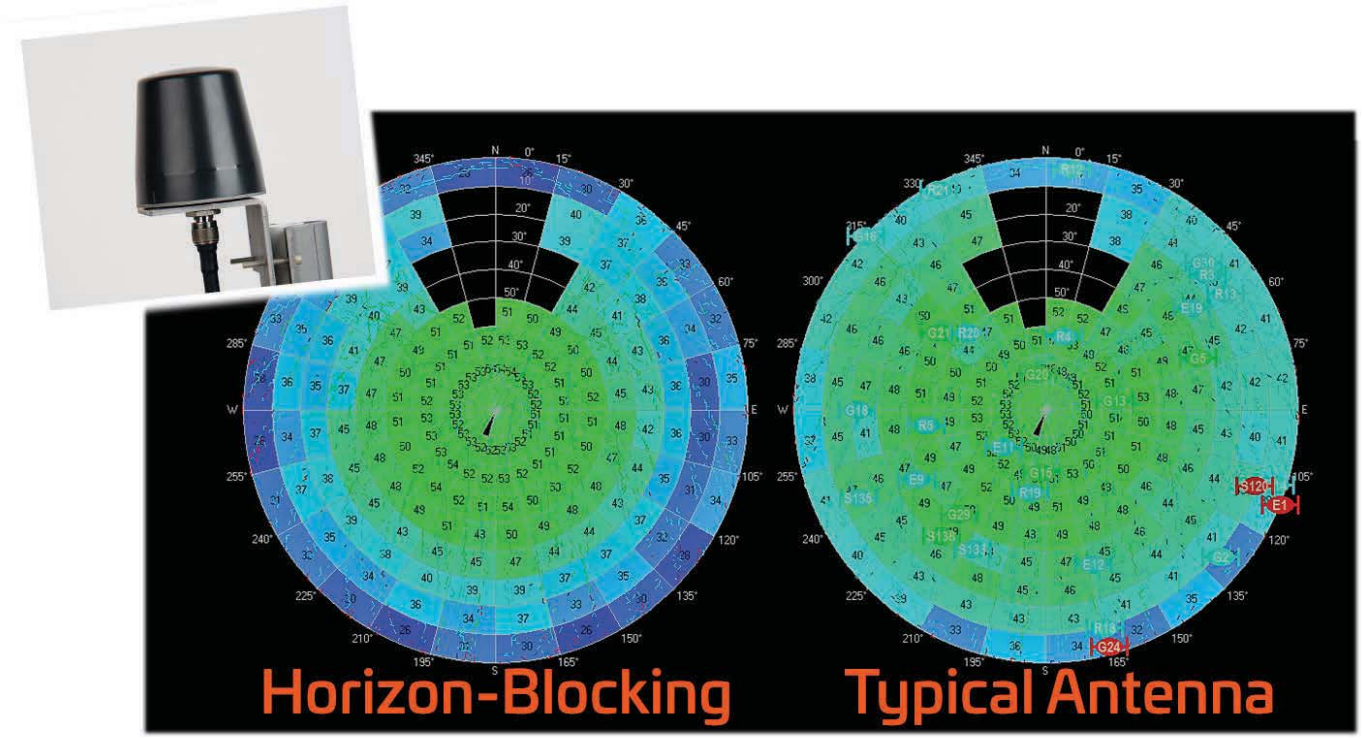


Fig. 8: Horizon-blocking antenna (left) vs. typical antenna

Detecting Interference

The prompt and correct detection of an interference event involves the use of all available information to alert and notify the user(s) of a GNSS-based PNT system about the presence of a threat. GNSS receivers are increasingly often equipped with jamming-detection functionality that will inform the user of a jamming/ denial situation, offering at least the option of quicker diagnostics in the event of an unexpected signal loss.

Also, multi-GNSS chipsets in modern receivers often offer integrity monitoring between GNSS systems. However, the level of monitoring capability varies widely and system integrators often have little control over these settings.

A new approach to detecting jamming or spoofing attacks is a software solution called BroadShield that can be installed on GNSS-based time servers, where it monitors the GPS signal frequency band by applying error detection algorithms. BroadShield can detect whether a GNSS receiver is being spoofed and, in the event of a signal loss, can provide valuable information as to why the signal has been lost. The software's algorithms can discern a jamming event caused by natural events that cause the signal to weaken. If a monitoring signal threshold value is exceeded, the time server will emit an alarm and invalidate the GPS reference before it can pollute the internal time base. Now, when the time server transitions into Holdover, it "flywheels" on the previous pure reference signal.

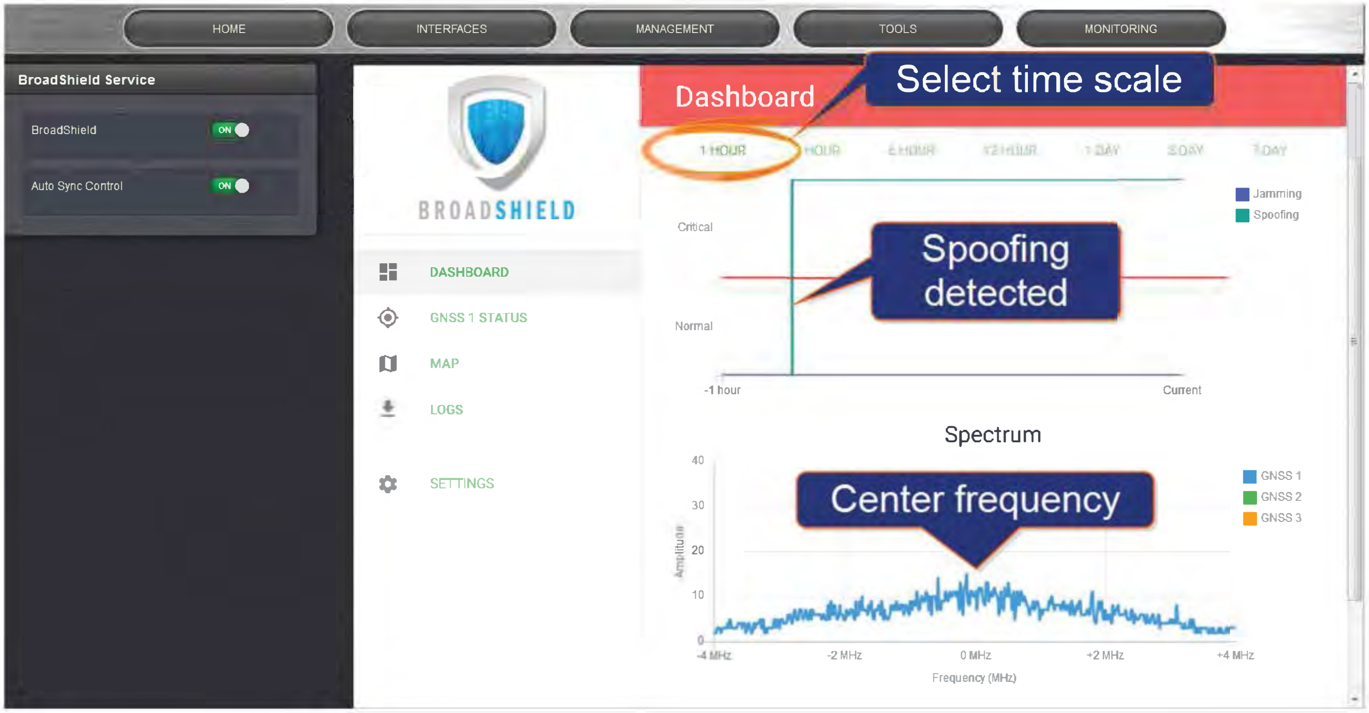


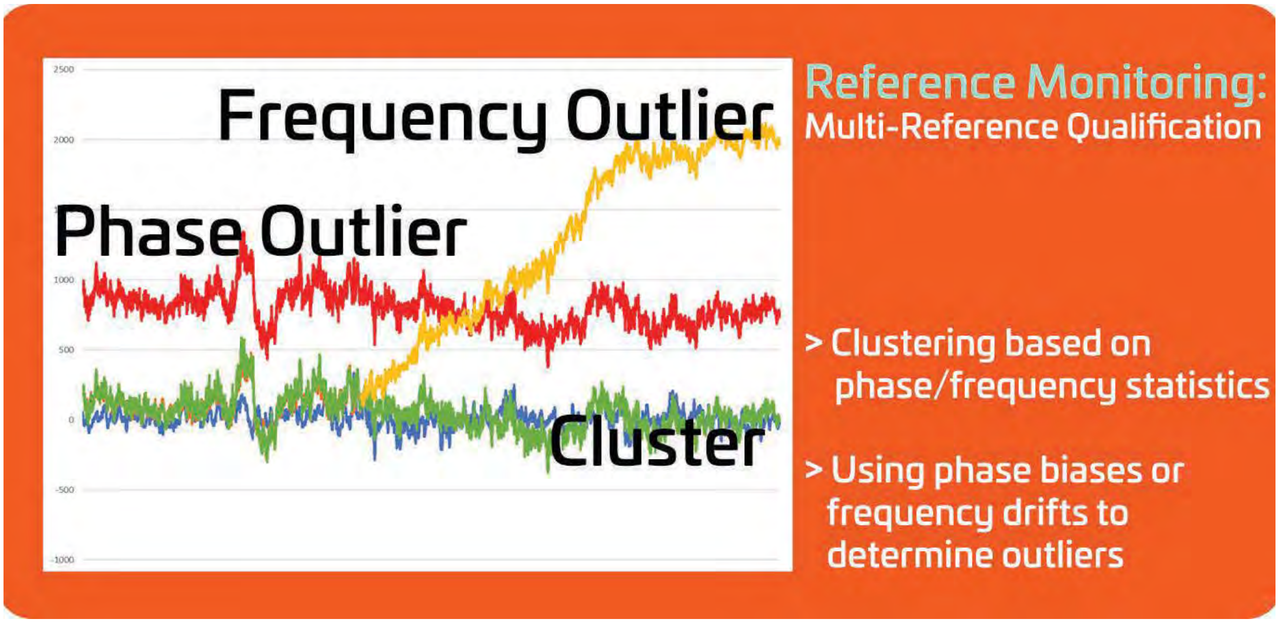
Fig. 9: BroadShield Web UI: dashboard panel

Smart Reference Monitoring Software

This type of software can run on time servers such as the SecureSync or PRISMA VelaSync. The software will compare these references continuously: If the GNSS reference exceeds a software-determined phase-error-based validity threshold value, which suggests a jamming or spoofing event, the software will automatically issue an alarm to inform the user. It can also be programmed to disable the GNSS reference and fall back to the next best reference without any user interaction, thus making this software module both an interference detection tool and an interference mitigation tool. The validity threshold is calculated using long-term averages and standard deviations.

When comparing live phase measurements against these thresholds, short term phase drifts and jumps can be detected. This technology would catch an incident like the 13-microsecond GPS glitch that occurred in January 2016. http://www.bbc.com/news/technology). Alternatively, the reference monitoring software can also utilize certain characteristics of the onboard oscillator of a time serve, such as aging and temperature stability, to calculate frequency thresholds, which are then used to validate live frequency measurements.

Reference monitoring also offers the possibility of using clustering techniques to group references together based on phase/frequency statistics, with the ability to compare them, allowing the detection of outliers (shown in **red** and **yellow** in Fig. 10).



Reference Monitoring:
Multi-Reference Qualification

> Clustering based on phase/frequency statistics

> Using phase biases or frequency drifts to determine outliers

Fig. 10: Smart reference monitoring signal plot

Mitigating Interference

Interference mitigation is the second aspect of the IDM approach. Mitigation in this context means that after isolating the unwanted signal, quickly rejecting and replacing it, causing minimal system degradation. Essentially, this involves the use of augmentation technologies and diversification strategies to supplement GPS/GNSS, thus reducing the dependence on it.

For military applications, the first mitigation measure is to utilize SAASM/M-Code whenever possible, and/or to use multi-frequency receivers. Another approach is to use several independent GNSS receivers in one PNT system e.g., one per constellation. Then the live signals can be compared to each other to detect suspicious changes in any of the constellations that could be caused by spoofing (similar to reference monitoring software).

Another well-established technical approach to deal with temporary loss of GNSS signals is holdover solutions, such as oscillators for timing and Inertial Navigation Systems (INS) for navigation systems. The latter use accelerometers to measure acceleration and gyroscopes to measure direction (heading). These devices measure movement without any outside reference and are immune to jamming. High-end INS systems are capable of bridging long durations without external references, but the fundamental problem of errors that build up over time is still an issue.

Other technologies lend themselves to becoming augmentation systems to add resiliency to a PNT system. Some of these concepts are based on existing technology such as **eLORAN**. Others have their origin in non-PNT applications, such as **vision-based** systems.

A concept growing in popularity is to **crowdsource** navigation: If a PNT solution integrated into a mobile platform loses its PNT reference signals, it may still be able to communicate with nodes on a network that have a known position. In that case, the PNT solution can infer its position by determining the distance to the nodes. On wireless networks it is quite easy to measure the range by precisely measuring the time delays of the data sent back and forth.

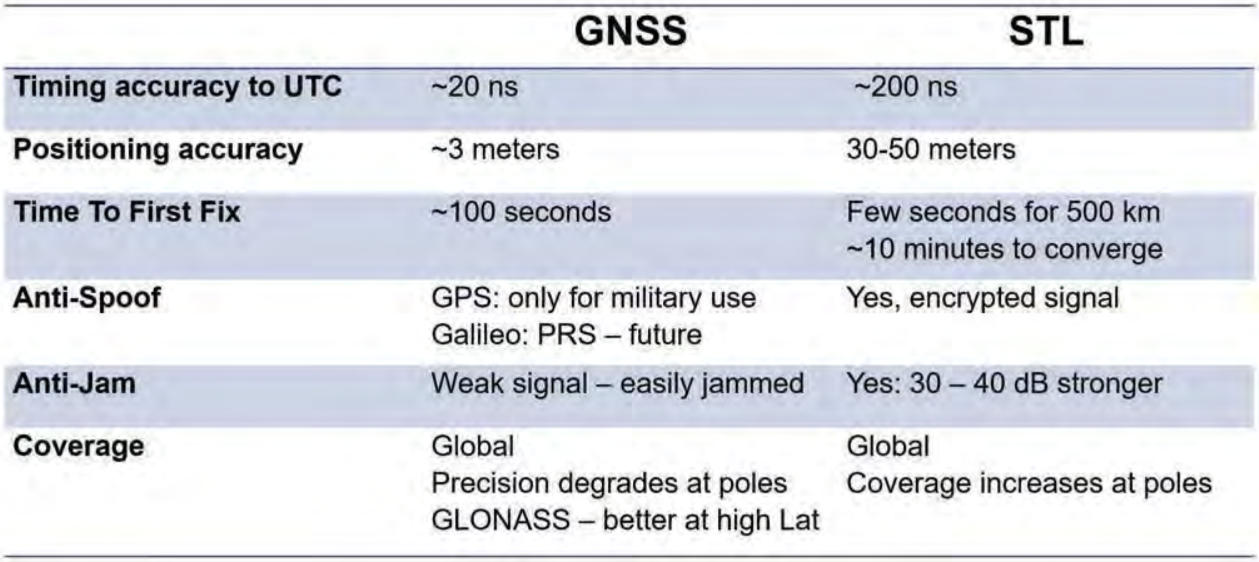
Signals of Opportunity such as WiFi and cellular signals also can fall into the crowdsource category, since these opportune signals are often "borrowed" from systems that were not designed for PNT purposes.

There is a new technology available today that is suitable to harden GNSS-based time and frequency references, and in some cases even to replace the GNSS reference. This system is called STL (Satellie Time and Location) and its signal is broadcast by the Iridum® satellites.

STL

Satelles' Satellite Time & Location (STL) service provides an alternate space-based PNT source to the GPS constellation. It uses the Iridium system's pager channels to provide a PNT signal accessible by terrestrial receivers. This system is operational and available today. Because the satellites orbit Earth on a much closer orbit, the signal is >30 dB stronger than GNSS signals. The signal can, in fact, be received indoors, and it is more resistant to jamming and interference.

The STL signal is encrypted; users are assigned a subscriber key to decrypt the signal. This service is available for civilian use in approved countries.



	GNSS	STL
Timing accuracy to UTC	~20 ns	~200 ns
Positioning accuracy	~3 meters	30-50 meters
Time To First Fix	~100 seconds	Few seconds for 500 km ~10 minutes to converge
Anti-Spoof	GPS: only for military use Galileo: PRS – future	Yes, encrypted signal
Anti-Jam	Weak signal – easily jammed	Yes: 30 – 40 dB stronger
Coverage	Global Precision degrades at poles GLONASS – better at high Lat	Global Coverage increases at poles

Table 1: GNSS and STL: Comparison of key specifications

How Does STL work?

The Iridium satellites used for STL operate in the Low Earth Orbit (LEO), which means they can provide a strong signal (using spot beams) on account of the relative proximity to Earth. The low altitude shortens the orbit to around 100 minutes, which is significantly less than the GPS 12-hour orbit.

Noteworthy also is the geo-location security that STL offers: The decryption codes are associated with unique data packets that indicate from which satellite and beam the message was received. These packets can only be heard in a region on Earth at a given time, therefore offering irrefutable evidence of one's position – for example, a vessel located at a specific location at a specific time, thus offering security for shipboard positioning and communication system. This makes STL a powerful cybersecurity authentication factor. And since it is an encrypted signal, it cannot be spoofed.

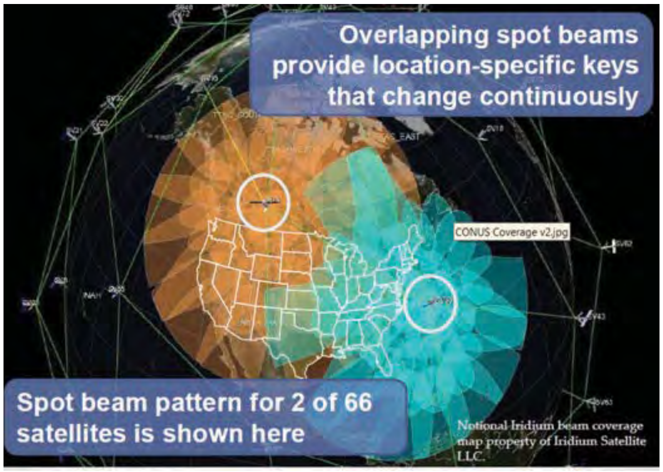

Overlapping spot beams provide location-specific keys that change continuously
CONUS Coverage v2.jpg
Spot beam pattern for 2 of 66 satellites is shown here
Notional Iridium beam coverage map property of Iridium Satellite LLC.

Fig. 11: STL spot beam pattern

Positioning Determination from STL

STL position and navigation is generally less precise due to the geometries of a lower, faster-moving constellation where only two or three satellites are in view. The Iridium orbits were designed for optimizing communication connectivity, not navigation. Also, the narrow bandwidth of the transmitted signal limits the range accuracy. Its positioning error is 10x-50x greater than the standard GPS Figure of Merit (FOM). This is not precise enough for most fast-moving applications. However, STL can be utilized to augment GPS position and navigation operations in a degraded environment by combining it with an INS (Inertial Navigation System) plus radar or AIS (Maritime Automatic Identification System). Tracking the range and Doppler updates from each satellite will assist in reducing the INS drift.

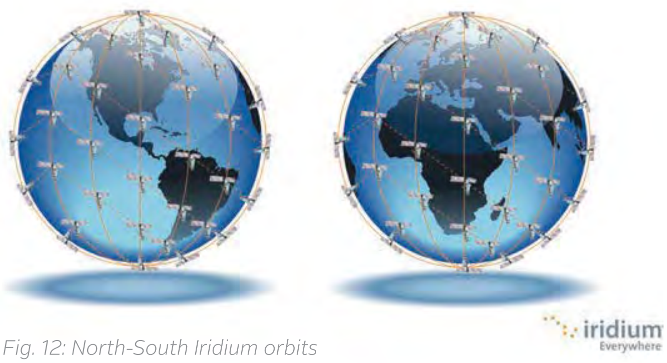


Fig. 12: North-South Iridium orbits

Note also that the North-South orbits of the Iridium satellites results in increased coverage near the poles due to converging orbits. This makes STL very suitable for Arctic navigation.

Overall, STL presents a very effective means to make timing applications resilient. In combination with other signals or inertial measurements, STL can also increase resilience of certain positioning and navigation applications.

Interference Testing

Another vital aspect of hardening GNSS receivers in PNT systems is to test the equipment for its actual vulnerability against jamming and spoofing. This involves the process of continuous improvement through threat replication in the lab to innovate and adopt new detection and mitigation strategies.

The U.S. military carries out **live sky tests** to evaluate aerial platforms, for example, using its own GPS jamming equipment. Its objective is to generate a realistic, live-sky degraded GPS environment, even though this requires a great deal of preparation work to avoid or minimize disruption to civilian air traffic, regional first responders, etc.

Threats can also be simulated with **GPS/GNSS simulators:** These simulators can be used in the test lab to understand how a receiver under test reacts in a spoofing or jamming situation, or to evaluate existing mitigation technologies.

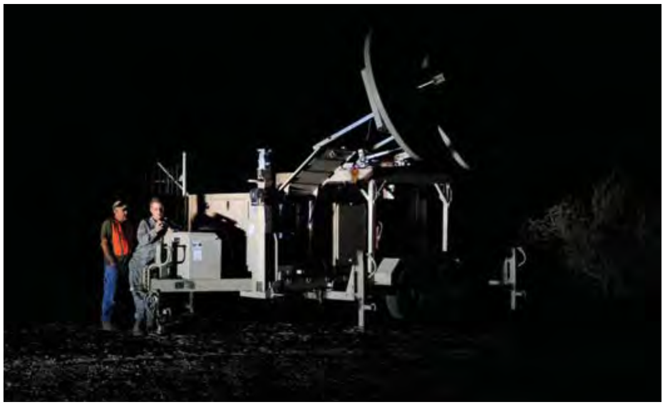


Fig. 13: A military live-sky RF jamming test system (U.S. Air Force photo by Cole Johnson)

Tests can also be carried out in special lab chambers that prevent leakage of RF jammer signals, or by means of simulation, using **vulnerability test systems (VTS)** that are built around the above-mentioned GNSS simulators. These systems can either feed the simulated GNSS data directly into the receiver under test, using a standardized interface, or transmit the signal via RF. The VTS systems simulate not only the live-sky GNSS signals, but also the spoofing signals. The latter can be modified separately (e.g., signal strength, time sync signal, or individual satellites coming into/going out of view) in real-time or in advance via a test script, allowing a wide range of test scenarios.

The test objective is to harden a system by understanding how its GNSS receiver reacts to spoofing, implement a mitigation technique and then iteratively test and modify the improved system.

Some PNT equipment manufacturers such as Spectracom/Orolia also offer **IDM test services** that involve the testing of customer equipment against possible threats, as well as a vulnerability risk assessment and mitigation recommendations.

Conclusion

The technologies available to make PNT systems resilient are continually evolving. Operators of assured PNT systems – military or civilian – find themselves increasingly challenged by threats to the availability and integrity of GNSS signals. Although some hardening and sensor fusion technologies are still under development, others already exist and will continue to evolve.

GPS and other GNSS systems will also benefit from technological advancements in the future, some of which will make their signals less susceptible to interference. Worldwide availability and accuracy make it unlikely that GNSS will be replaced by another technology in the foreseeable future. By combining GNSS-based PNT equipment with detection and mitigation systems, we will continue to rely on trusted GNSS as the main source for positioning, navigation and timing.

About The Authors

For more than 15 years, **John Fischer** has worked with global navigation satellite systems (GNSS), wireless, positioning navigation and timing (PNT),and specialized systems for customers at Spectracom, an Orolia brand.

Prior to joining Spectracom, he specialized in wireless telecom as a founding member of two startups: Aria Wireless in 1990 and Clearwire Technologies in 1997. At Clearwire, he served as Chief Technology Officer in creating wireless broadband equipment for Internet connectivity.

Early in his career, John worked as a systems engineer in radar, EW and command and control systems at Sierra Research and Comptek Research. He holds Masters and Bachelor of Science degrees in electrical engineering and computing engineering from the State University of New York at Buffalo.

Jeremy Onyan, Director of Time Sensitive Networks, holds a Bachelor of Science in Economics from the University at Buffalo. He has over 13 years of Global Sales and Management experience. Jeremy is recognized as an industry thought leader in timing for enterprise applications, especially in Finance and Big Data.

About Orolia

As PNT experts with a deep and rich history in critical timing and synchronization, Orolia works aggressively to integrate assured positioning, navigation and timing technologies into all our products. Solutions to detect and mitigate interference are part of our core DNA. Solutions include:

- GPS and GNSS technology covering all satellite-based time and positioning signals including encrypted military SAASM and M-Code receivers, GPS, Galileo, GLONASS, IRNSS, and QZSS.
- In-house time and frequency equipment manufacturing that include compact Rubidium standards and space-qualified Hydrogen Maser standards.
- High-power satellite-based technology STL (Satellite Time and Location) that penetrates buildings, obstructions and is resilient to jammers, which can be used as a secure signal of opportunity to complement GPS and other GNSS satellite signals
- BroadShield jamming and spoofing detection systems that use over 75 proprietary detection algorithms to detect interference and spoofing within the GPS signal and GPS spectrum.
- Alternative PNT signals and Signals of Opportunity receivers leveraging available signals such as eLORAN to increase the probability of maintaining accurate PNT information.
- Vulnerability test systems that can evaluate the effects of interference, jamming and spoofing on systems that rely on GNSS signals.
- Integration of various inertial sensors including MEMS-based and FOG-based sensors that offer a level of stand-alone performance in the absence of GPS references for position and navigation systems.
- Smarter use of the entire PNT ecosystem, including feature-rich GPS reception hardware and intelligent software techniques, reception from multiple constellations, multi-frequency signals, and augmentation systems.

www.orolia.com

www.spectracom.com

orolia ENTERPRISE

USA

Orolia USA Inc.

1565 Jefferson Road
Suite 460
Rochester, NY 14623
Phone: +1.585.321.5800

France

Spectracom SAS

Parc Technopolis, Bat. Sigma
3 Avenue du Canada
91974 Les Ulis, Cedex
Phone +33(0) 16453-3980

Singapore

Orolia Asia Pacific office

1 Changi Business Park Crescent
Changi Business Park
Singapore 486025

For More Information:

Vicom
Leading the way in test and measurement

Vicom Australia

1064 Centre Rd
Oakleigh South
Vic 3167 Australia
1300 360 251
info@vicom.com.au
www.vicom.com.au

Vicom New Zealand

Grd Floor, 60 Grafton Road
Auckland 1010
New Zealand
+64 9 379 4596
info@vicom.co.nz
www.vicom.co.nz

www.orolia.com

www.spectracom.com