orolia

The Global Leader in Resilient PNT

# Tech Brief
# Resiliency in PNT: GPS/GNSS Jamming and Spoofing

John Fischer
*Vice President of Advanced Research & Development, Orolia*

## Introduction

GPS has been in use for two decades for military and commercial positioning and navigation. In recent years, additional constellations have been added – GLONASS, Galileo and Beidou. These four Global Navigation Satellite Systems (GNSS) provide reliable, accurate worldwide coverage.

Over the years, accuracy and reliability have evolved so that one-meter accuracy is routinely achievable, and downtime events are extremely rare. Through international cooperation, these GNSS systems share common frequency bands, and affordable, multi-constellation navigation can be accomplished with a single receiver. The various signals are spaced close enough together to make reception efficient, but not so close as to interfere with each other.

Reliance on GNSS is now commonplace. However, all these GNSS systems share a common vulnerability: their signals are very weak. GNSS satellites operate from Mid-Earth Orbit (MEO), approximately 20,000-25,000 km above the earth, to provide the best coverage and geometry for triangulation. As such, the transmitted signal is extremely weak upon arrival at the surface of the earth – so weak that it is weaker than the surrounding radio noise. Special signal processing techniques recover the GNSS signal from the background noise, but the weak signal strength at the user's receivers makes GNSS navigation very susceptible to interference.

## GNSS — Global Navigation Satellite Systems

### GPS

- Since 1980s
- 31 sats
- GPS III Launch Dec 2018

### GLONASS

- Refurb 2012
- Operating well with 24 sats

### Galileo

- 18 of 24 sats operational since 2016
- Full capability 2020

### Beidou

- Regional initially building out to full global coverage by 2020

### *Regional Systems*

Japan - QZSS

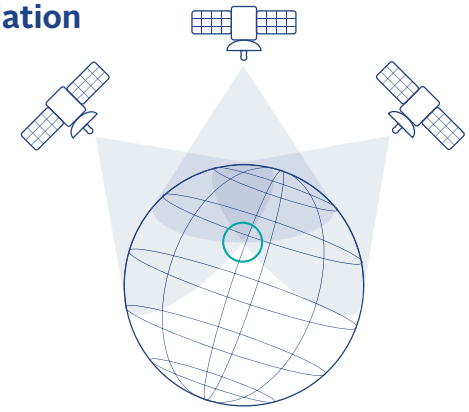
India - NAVIC

## How GNSS Works

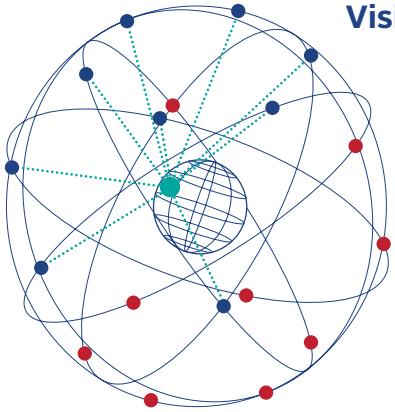
Each GNSS constellation consists of approximately 20-30 orbiting satellites. Typically, a user on the earth can see six to ten satellites at any one time from any given constellation.

These satellites do not track the user. Rather, they behave like a set of lighthouses, all sending out a radio pulse at the same time. The user receives each of these pulses at different times, based on his or her distance from each satellite. This Time Difference Of Arrival (TDOA) provides a measurement of distance based on the known propagation velocities of radio signals. The satellites also send data reporting their precise positions in the sky, so that by knowing your distance from each satellite and the satellites' positions, you can calculate your position on earth.

**Triangulation**



**Visible sat - 12**



A side benefit of this method is precise time determination. The fact that all the satellites transmit at exactly the same instant (within one billionth of a second or nanosecond) yields a precision time mark.

The satellites repeat their pulse transmissions at exactly one-second intervals synchronized with Universal Coordinated Time (UTC), so that reception of GNSS signals provides users with precise synchronization to UTC.

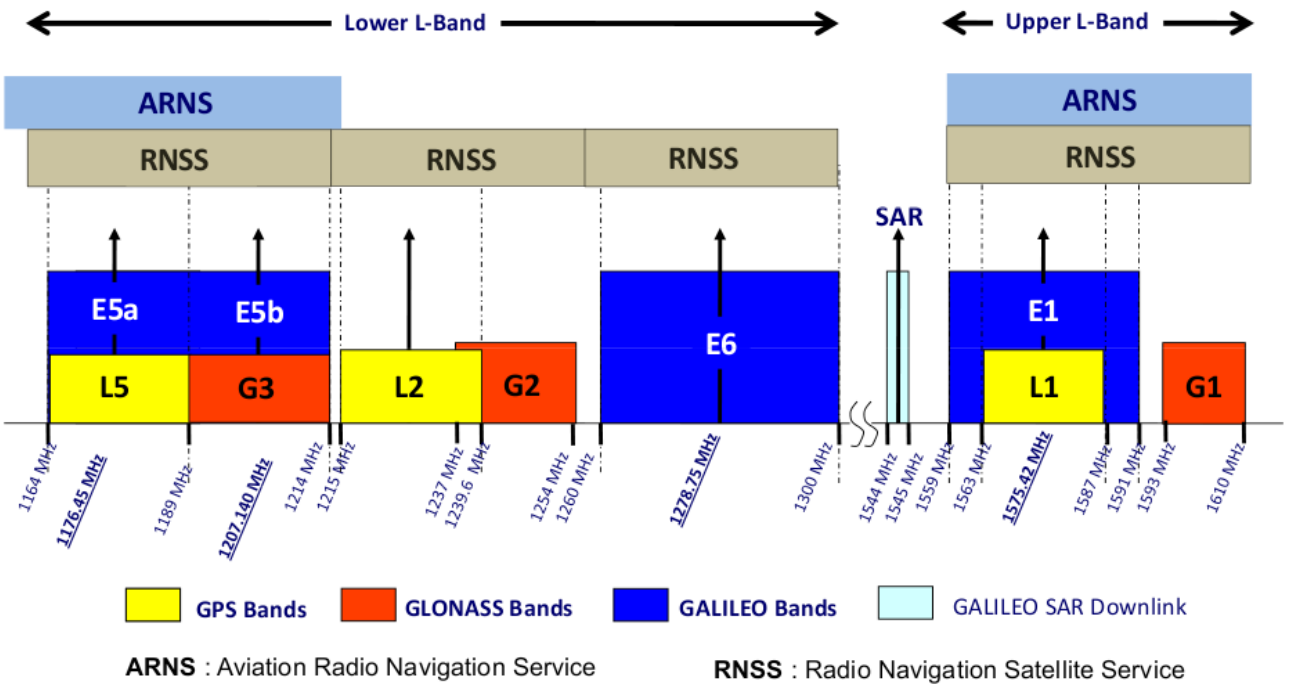
## Jamming and Spoofing

**Jamming** is the presence of a competing signal that prevents the GNSS receiver from decoding the true satellite signal. Remember, the GNSS signals are so weak at the earth's surface that they are below the surrounding background noise level. Consequently, it does not take much of an interfering signal to jam the receiver.

Jamming from other radio transmission sources can be intentional (malicious) or unintentional. For example, radars or communications transmitters, though operating in a different frequency band, may leak a tiny bit of energy into the GNSS bands. Conversely, the GNSS receiver, though it has filters tuned to listen to the GNSS bands only, may "hear" energy from these other transmitters because they are relatively strong by comparison.

There are four main bands dedicated to Radio Navigation Satellite Service (RNSS), in which the GNSS constellations operate:

1. L1/E1/G1 1559 – 1610 MHz
2. L2/G2 1215 – 1254 MHz
3. L5/E5/G3 1164 – 1214 MHz
4. E6 1260 – 1300 MHz




*Courtesy Navipedia*

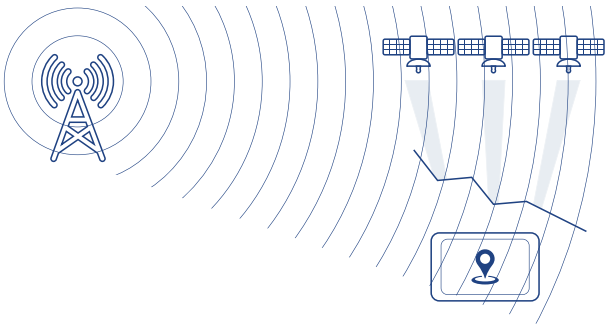
Most commercial receivers today only operate in the L1 band. This was the first band deployed and has been operational for several decades. Historically, the L2 band was the encrypted band for GPS and GLONASS that the military used. In recent years, however, the L5/E5, E6, and L2C (Civilian) bands have started being deployed, and the next generation of GNSS receivers will operate in all these bands.

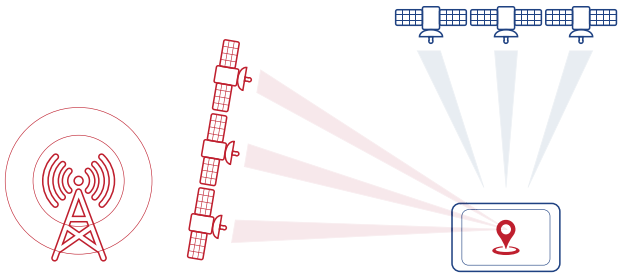
Unfortunately, with today's commercial L1 band-only receivers, it is easy to jam the entire L1 band and defeat all the GNSS constellations. Cheap one-watt jammers, though illegal in most countries, are readily available on the internet. Advertised as privacy jammers, they can defeat GNSS reception for several kilometers around their radiation pattern.

As the next generation of new, multi-frequency receivers begins to be deployed, it will be necessary to jam all the GNSS bands to defeat position and navigation. That being said, it will also be fairly easy to build a multi-frequency jammer. Doing so will be only slightly more complex, so the threat will still be present.

**Spoofing** is the intentional transmission of fake GNSS signals to divert users from their true position. Spoofing requires sophisticated equipment to recreate the satellite signals, so it is more difficult to do. But, if done correctly, it is more difficult to detect than jamming. The growth in capability of Software Defined Radios (SDR) and the increase in their affordability is making spoofing easier to implement.

Another method of spoofing is to record a valid signal at one location at a specific time and then to replay it at a different time and location. This is sometimes called meaconing, or a playback attack, and can also be a dangerous threat.





## GNSS Jamming

*Jamming creates noise which prevents GNSS receivers from locking on to authentic GNSS satellites.*

## GNSS Spoofing

*Spoofing mimics authentic GNSS satellites to hijack GNSS receiver tracking loops*

## Detection and Mitigation — Jamming

Jamming is relatively easy to detect, and there are several ways to guard against it. Because the valid signals from the true GNSS satellites are below the surrounding background noise level, detecting any energy in these bands means that there is interference. The difference between intentional and unintentional jamming is an operational concern only – with cooperation, the unintentional jammer may be mitigated at the transmission side, whereas with intentional jamming, there is no cooperation.

The first line of defense for jam resistance is at the antenna: Do not allow the jamming signal into the receiver in the first place. A simple defense method is to use a horizon-blocking antenna. Most interference, whether intentional or unintentional, comes from the surface whereas the valid signals come from the satellites at higher elevation angles. An antenna that blocks energy from below approximately 20-30 degrees' elevation will block surface interferers at all frequency bands.

However, there are two limitations to this approach:

- The best geometry for horizontal position triangulation is obtained from the horizon-based satellites. By eliminating these satellites from the navigation solution, accuracy decreases. We call this Geometric Dilution of Precision (GDOP). With modern multi-constellation receivers, this effect is minimized compared to older single-constellation receivers, because many more satellites are now in view. The degradation is typically only a few meters.
- For vehicles such as aircraft or ships, the horizon can change as the vehicle pitches and rolls, interfering with the antenna's view. As the antenna's horizon varies, even some of the higher elevation satellites may be blocked and multipath reflections may increase, further degrading accuracy.

Better performance can be achieved with smart antenna technology. Controlled Radiation Pattern Antennas (CRPA) are devices that have multiple focused beams under software control that can steer these beams to track the real satellites and steer away from interference. These devices are expensive, though – $20,000 or more. Used on military vehicles today, this technology could be applied to commercial navigation for high-value or critical applications, where many lives are at risk.

The next line of defense is signal filtering. When powerful, wideband jammers are used, there is little that can be done with filtering, but the cheap jammers that are prevalent today are low power and narrow in frequency, sweeping through the GNSS band to wreak havoc. Modern Digital Signal Processing (DSP) techniques can eliminate these types of interference. In-line filtering devices can be placed between existing antenna and receiver installations and achieve a high degree of rejection. The next generation of receivers is expected to have some of this filtering capability already installed as standard.

## Controlled Radiation Pattern Antennas (CRPA) are the first defense in combatting jamming and spoofing


Orolia 8230AJ


InfiniDome 1.01

Antcom 4 element

SATIMO
Galileo/GPS

GAJT 710MS

- Solutions range from affordable (~$1K) to very expensive (~$50K) and are available today
- Beams are focused on the satellite signals and focused away from the interference
- Can provide 20 - 50 dB of jamming protection
- The most effective means of Anti-Jam (AJ) protection as the energy never enters the receiver

## Detection and Mitigation — Spoofing

Spoofing detection is more difficult, especially when the spoofer is high quality. It is very difficult to discern between fake and real satellite signals when the simulated signals are recreated with high fidelity. Again, CRPA antennas are the best defense here, because a spoofer typically generates and transmits all the various (fake) satellites signals at one location; the real satellites signals come from all over the sky. Therefore, the CRPA antenna, which tracks the real signals in elevation and azimuth angles, will reject fake multiple signals coming from a single direction.

Even without a CRPA antenna, there are other techniques to recognize fake signals:

- The signal strength from the real satellites does not vary much, since the satellites always remain relatively far away. However, fake signals generated by a spoofer can be very strong when transmitted nearby at the surface and will vary greatly as objects moves. Only the most sophisticated spoofer can account for motion and adjust its transmitted signal level accordingly. To do so requires tracking the object's course.
- Receivers will receive both fake and real signals simultaneously. When the navigation processing becomes fooled by the fake signals, range measurements will typically jump to the new erroneous values. Step changes are not possible in real physical systems, so this is usually an indication of spoofing.
- The data streams from each satellite may also indicate discontinuities as the receiver switches from tracking the real signal to the fake; the same goes for time indication. This will be especially detectable with a meaconing or playback attack, because time will jump backwards when the replay starts.
- Radio waves experience Doppler shifts the same as sound waves do as objects move. The Doppler shifts for the real satellites will all be different as the object moves either towards or away from them depending on their position in the sky. However, the Doppler shift caused by the object's motion due to a spoofer is the same for all the satellites signals because they are all arriving from the same direction. This uniformity of Doppler is another indication of spoofing. Again, only the most sophisticated spoofer can account for an object's motion to adjust its Doppler shift for each individual satellite, and to do so requires tracking the object's course.

Detection software can be added to existing systems to detect and protect against jamming and spoofing.

## Countermeasures

What can be done if the jamming or spoofing breaks through these defenses? Though GNSS is one of the best ways of determining Position, Navigation and Timing (PNT), there are other sensors and methods.

- For position and navigation, an Inertial Navigation System (INS) provides position coordinates and velocity vectors by measuring movement with accelerometers and gyroscopes. However, there is always error in this method, because even the slightest inaccuracy in acceleration and angular measurement gets accumulated to a growing drift error over time.
- For timing, a precise clock can provide short-term accurate time. Atomic clocks are affordable today and can provide $10^{-11}$ or better accuracy, but again, over time, even this tiny error will accumulate.

The best use of these devices is to combine their measurements with the time and position updates from the GNSS receiver. When GNSS is available, the INS and Clock are "disciplined" to the GNSS solution to limit their error drift. Then, when proper GNSS is denied by either jamming or spoofing, the INS and Clock ignore the GNSS corrections and "flywheel," maintaining a PNT solution independent of GNSS, by using their disciplined or corrected parameters. Error drift in this situation is now much lower than it would have been if no GNSS were previously used.

Early detection of jamming and spoofing is key. If the disciplining algorithm does not disconnect from the bad GNSS solution early, it will become polluted with erroneous measurements.

Another countermeasure is to use Alternative Navigation sources to augment the GNS/INS PNT solution. Two signals are available today:

- eLoran – a low frequency, 100KHz high power signal transmitted from terrestrial towers.
- STL – Satellite Time and Location – a microwave signal transmitted from Low Earth Orbiting (LEO) satellites.

Unfortunately, eLoran is not available in most of the world and build-out of transmitters has been slow. Some areas, such as South Korea and the United Kingdom, are building transmission sites but many other countries, including the USA, have yet to embrace it.

On the other hand, STL offers global coverage and is available today. Though less accurate than GNSS, it has two distinct advantages over GNSS:

- Its signal is ~1000x stronger than GNSS because it originates from LEO satellites orbiting ~800 km above the earth instead of 22,000 km.
- The signal is encrypted to avoid any spoofing possibility.

The chart below shows the full comparison:

STL can be used in a similar manner as GNSS to discipline the INS and atomic clock to provide a resilient PNT solution. When all signals are available, the best navigation solution is obtained. STL, because if its inherent anti-spoofing and anti-jamming characteristics, can provide authentication of the more accurate GNSS signals when both are available. When GNSS is denied, STL can provide the error drift limiting function, maintaining position accuracy acceptable for open sea navigation and mobile land operations.

In the future, there may be other alternative signals available as more LEO satellites are planned for launch.

| | 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<br>~10 minutes to converge |
| Anti-Spoof | GPS: only for military use<br>Galileo: PRS – future | **Yes, encrypted signal** |
| Anti-Jam | Weak signal – easily jammed | **Yes: 30 – 40 dB stronger** |
| Coverage | Global<br>Precision degrades at poles<br>GLONASS – better at high Lat | Global<br>**Coverage increases at poles** |

Other augmentation methods may become practical in the future:

- Radar aiding of the hybrid INS/GNSS navigation system.
- Hydrographic chart and sonar correlation with the INS/GNSS Nav system.
- Celestial navigation – this age-old method is seeing renewed use with automated video systems mapping the night sky and providing navigation data outputs. For daytime operation, polarized light detection sensors map the day sky and, with sophisticated signal processing, provide heading information.
- Crowd-sourced or collaborative navigation via AIS and Radar reports – in GNSS denied situations, one's own position can be inferred by multiple reports from other ships and shore-based references, and by some knowledge of their relative proximity. Signal strength and ranging are two method to estimate proximity to these remote nodes. As the number of reporting nodes grow, the position estimate will converge on a fairly accurate position.
- Spoofing detection of erroneous AIS Reports – using similar techniques as those used for GNSS spoof detection, false AIS reports can be noted and alarms set.

For more information, visit www.orolia.com or contact sales@orolia.com.

## About the Author

John Fischer has worked with global navigation satellite systems (GNSS), wireless, positioning navigation and timing (PNT) and specialized systems for more than 15 years. Prior to joining Orolia, 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, 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. He graduated with master's and bachelor's degrees in electrical engineering and computing engineering from the State University of New York at Buffalo.

**Orolia US Headquarters**

1565 Jefferson Road Suite 460
Rochester, NY 14623 USA
Phone: +1 585 321 5800

**Orolia European Headquarters**

Parc Technopolis, Bât. Sigma
3 Avenue du Canada
91974 Les Ulis, Cedex, France
Phone: +33 (O)1.64.53.39.80

www.orolia.com
sales@orolia.com

02 July, 2019 - Resiliency in PNT: Jamming and Spoofing