HEXAGON | NovAtel

White Paper

Spoofed or jammed?

Busting the myths of GNSS interference and mitigation

If your on-the-job activities require knowing exactly where you are and where you are going, you undoubtedly rely on Global Navigation Satellite Systems (GNSS) for accurate positioning, navigation and timing (PNT). GNSS refers to the collection of satellite positioning systems, or constellations, from various countries and regions **(Figure 1)**. Radio frequency (RF) signals from GNSS are used for PNT in a variety of industries and military domains — from land-based to airborne and marine applications — many of which demand high accuracy, reliability and availability.

A critical challenge faced by those relying on assured PNT (APNT) are threats to GNSS signals, particularly in denied, disrupted, intermittent or limited (D/DIL) GNSS environments. These include military theatres and marine littoral regions with crowded RF zones due to nearshore and onshore activities — like the Black Sea and Mediterranean Sea whose shores comprise countries with high commercial and industrial activities, as well as military unrest. Regions with strategic positions, such as Scandinavia, are also often subject to GNSS threats by opposing regimes.

Any disruption to GNSS signal transmission can result in partial or complete loss of PNT, meaning you're effectively navigating (driving, flying or sailing) blind. Threats to GNSS signals can be unintentional or intentional (see inset). There have been many documented cases of unintentional interference, ranging from faulty TV receivers to other non-GNSS transmitting sources leaking into GNSS frequency bands. If the interfering signal is intentionally transmitted in the GNSS frequency range, it is called jamming.

Another threat to GNSS positioning is spoofing, which refers to intentionally sending fake GNSS signals to a receiver, so it calculates a false position, making the user believe they are in a different location or time than they actually are. This type of threat is of particular concern in safety-critical applications across all industries — whether commercial or military — that rely on accurate GNSS-enabled PNT.

Why are GNSS signals prone to jamming and spoofing?

The RF spectrum is split into designated uses, so GNSS signal bands are fixed and of known frequencies **(Figure 1)**, making them susceptible to jammers and spoofers emitting signals within the same frequency range.

To make matters worse, by the time GNSS signals have travelled 20,000 – 25,000 km from the medium-Earth orbit (MEO) satellites to the receiver on the Earth's surface, they are at a very low power level (-130 dBm or 10^{-13} mW) — 600 quadrillion (that's 15 zeros) times weaker than a 60W lightbulb!

This low power level makes the GNSS signals susceptible to interference from more powerful signals transmitted in the same frequency range. This is why powerful interference can overwhelm a GNSS receiver, and why protection and augmentation should be considered.

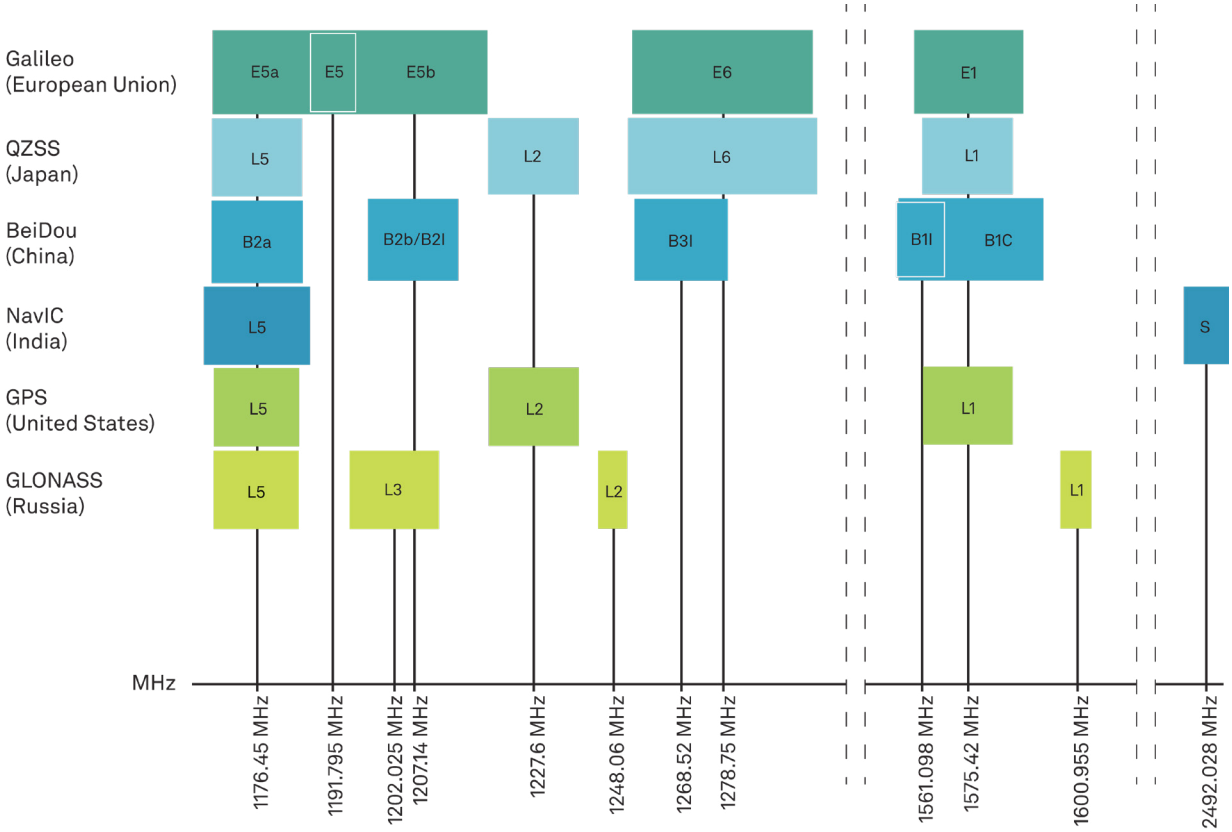

Figure 1. GNSS constellations and signals.

What is the difference between jamming and spoofing?

The main distinguishing factor between jamming and spoofing from the user perspective is the effect it has on the receiver's ability to provide PNT. Jamming shows up as a loss of PNT information, because the GNSS signal is overpowered by the jamming signal. Spoofing, on the other hand, tricks the receiver into reporting incorrect PNT information.

An analogy to compare the difference between jamming and spoofing is a robber cutting the security camera feed, so the guard sees grey static on the monitor screen (jamming), versus the robber replacing the feed with video that shows the same view from another time making the security guard think all is well (spoofing). This is why, from a GNSS user perspective, spoofing is of greater concern. Unlike jamming, you may not know you're being spoofed.

Jamming is done by overwhelming the GNSS receiver with higher power RF signals. Although illegal in most jurisdictions, very low-power jammers known as "personal privacy devices" can be bought on the Internet and used for this purpose. Even a simple, low-power jammer can overpower GNSS signals within a large area, denying PNT.

The effectiveness of jammers primarily depends on their output power and range (distance to the target receiver). A low-power jammer close by could have the same effect as a high-power jammer transmitting from farther away. Other characteristics for jammers include whether they target narrowband or wideband frequencies, and if they are transmitted as a continuous wave (either on a selected frequency or a sweep over the spectrum) or pulsed at a certain rate at a lower power level (chirping). **Figure 2** shows examples of several types of jamming signals.

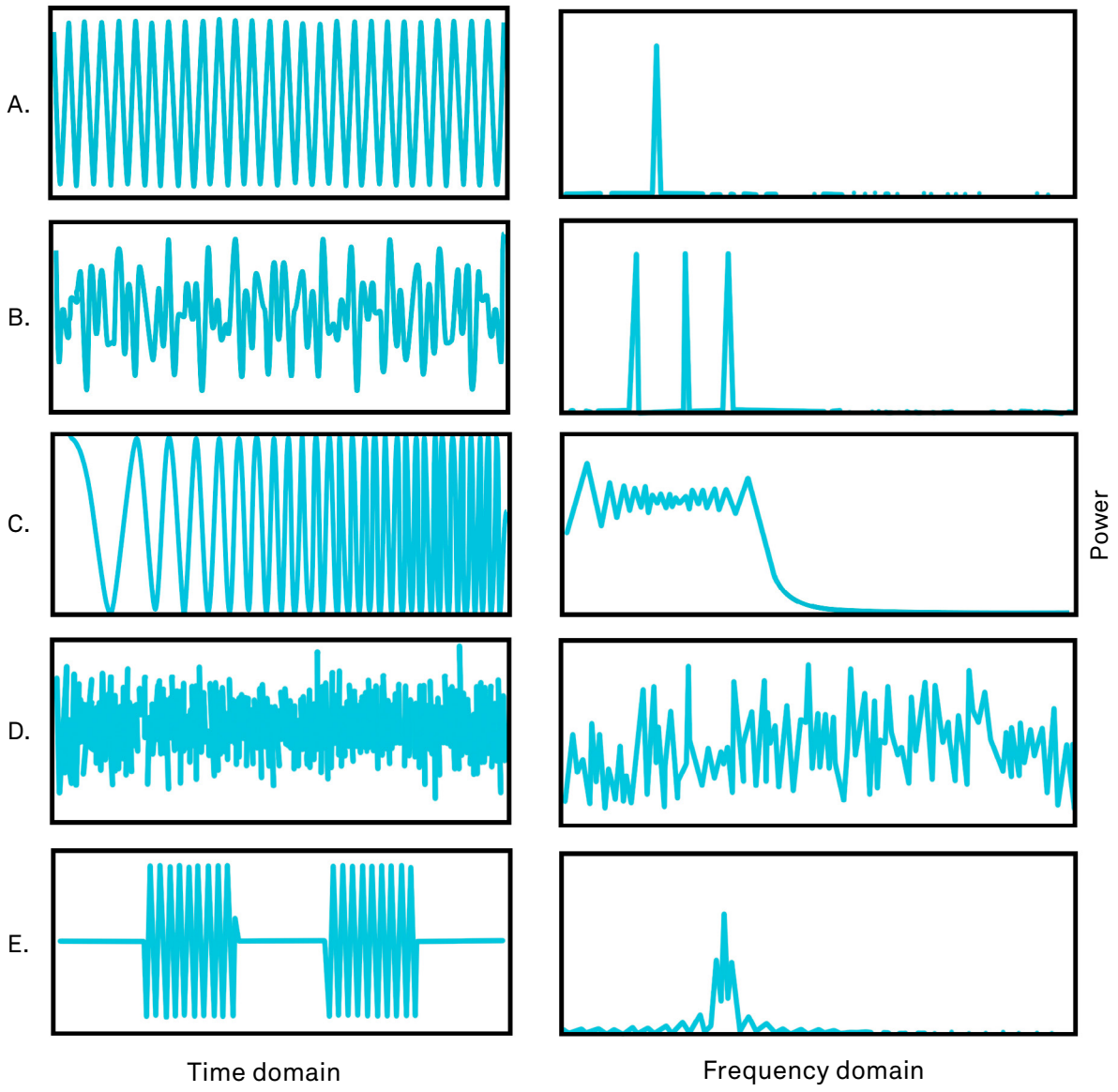

Figure 2. Types of jamming. A. Continuous wave narrowband. B. Continuous wave multi-tone. C. Chirping. D. Wideband. E. Pulse. (Jahromi et al., 2015)

What are the different types of spoofing?

Regardless of the source of spoofing attacks, they can be classified as non-overlapped, overlapped, and by their **relative power** compared to the authentic GNSS signals. **Figure 3** illustrates four types of spoofing attacks.

Non-overlapped spoofing attacks are when the code and carrier phase (delay and Doppler frequency) of the spoofing signals are not synchronized with the authentic GNSS signals.

Overlapped spoofing attacks are more sophisticated in that the code phase and Doppler frequency of the spoofing signals are synchronized with the authentic GNSS signals. This type of attack requires that the spoofer know the current time, observable satellites, location and parameters of the target receiver.

The article "Nobody's Fool: Spoofing Detection in a High-Precision Receiver" from the July/August 2020 issue of Inside GNSS provides a more detailed look at detecting various types of spoofing attacks.

Spoofing is often a two-step process that requires using a jammer to first disrupt the receiver from tracking authentic GNSS signals and then using a radio transmitter to send false signals to the target receiver. The false signals can either be created by a signal generator or a rebroadcast of recorded GNSS signals, called meaconing. If the receiver hasn't started tracking authentic GNSS signals (e.g., upon startup), only the second step would be needed to capture the receiver.

A simple example of spoofing is using an inexpensive software-defined radio (SDR) to make a smartphone think it's outside in the park catching Pokémon characters when it's still in the house. Conceptually, more serious spoofing attacks using sophisticated GNSS signal simulators are the same, but the consequences can be dire — like a plane landing where it shouldn't or a ship sailing into unfriendly waters.

Spoofing attacks can be further classified by their relative power compared to the authentic GNSS signals and whether the fake signals are synchronized with various aspects of the authentic GNSS signals or not (see inset). If the target is moving, the spoofer also needs to know its velocity and course to adjust the transmitted spoofing signal level (and Doppler shift) to fool the target receiver.

From this introduction, it's easy to see why jamming and spoofing protection has become a critical component of GNSS equipment. Now we'll discuss what you can do to prevent getting jammed or spoofed — or both!

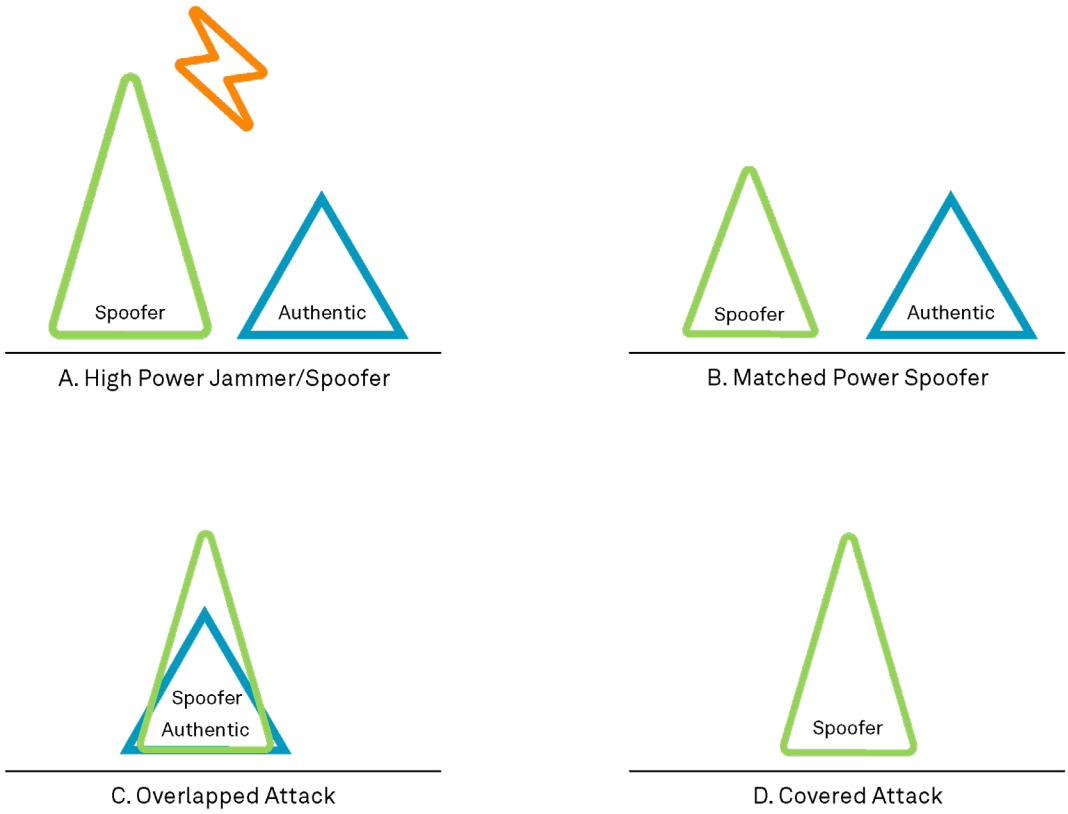

Figure 3. Types of spoofing attacks. A. Jam/Spoof: High power jamming signal followed by spoofing signal. B. Matched power: Spoofing power is matched to the authentic signal. C. Overlapped: Correlation function of authentic and spoofing signals overlaps. D. Covered: Spoofer masks reception of the authentic signals. (Broumandan et al., 2020)

How are jamming and spoofing mitigated?

The first line of defence for interference in any GNSS positioning solution is to detect and reject or suppress as much interference as possible before it affects PNT. At the basic level, a GNSS solution includes the satellite signals, an antenna and a receiver. Mitigation strategies for jamming and spoofing have been devised at each of these three levels as detailed below. Each of these components work together to create an additive effect against interference. Together, they give the user peace of mind that their PNT is protected, and they can safely carry out their operations.

Signal-based protection
For military applications, there are encrypted GNSS signal codes to mitigate against jamming and spoofing. For example, the GPS P(Y) Code is an encrypted binary code of 1s and 0s transmitted on the L1 and L2 frequencies. The P(Y) Code changes 10.23 million times per second and consists of a unique sequence of 6.18 trillion 1s and 0s per satellite that updates weekly. The P(Y) Code requires a Selective Availability Anti-Spoofing Module (SAASM) receiver with a valid decryption key (an export controlled good in many nations, including Canada and the United States).

M-Code is another military GPS L1/L2 signal designed to further improve anti-jamming. The M-Code is designed to be autonomous, meaning that users can calculate their positions using only the M-Code signal. In contrast, for receivers to use the P(Y) Code, they must typically first lock onto the public C/A Code and then transfer to lock onto the P(Y) Code. The M code signal places most of its energy at the edges, away from the existing P(Y) and C/A carriers. In addition, the M-Code will be transmitted from higher gain antennas that increase the signal strength, making it less prone to being overpowered by a jammer. **Figure 4** illustrates the GPS signal codes.

A second signal-based protection method is authentication, which involves cryptographic techniques to safeguard GNSS signals from being used by unauthorised users or manipulated by counterfeit transmitters. This includes the newly developed Galileo E1-B Open Service Navigation Message Authentication (OSNMA) and the future GPS L1C signal Chimera (Chips Message Robust Authentication).

Antenna-based protection
High-quality GNSS antennas provide another layer of defence against interference as they increase the received signal strength in the GNSS frequency band, while rejecting signals that are out-of-band. Some GNSS "anti-jam" antennas reduce the low-elevation signal gain to mitigate jammers originating at the horizon; however, this approach also blocks legitimate, low-elevation satellites. The protection these antennas provide is limited, as they can still be defeated if the jammer moves out of/away from the horizon, or if there are multiple jammers.

Adaptive antenna arrays such as Controlled Reception Pattern Antennas (CRPA) and associated anti-jam electronics provide a higher level of protection by continuously controlling the amount of signal received from any direction. By using multiple, separate antenna elements, CRPA electronics adaptively change the apparent gain of the antenna array to create lower gain "nulls" toward the source of interference (null forming).

A CRPA system can null in n-1 directions where n is the number of elements. So, a 7-element system can null in 6 directions and so on. But it isn't that simple and other factors such as the geometry of the CRPA and the signal processing algorithm used (see inset) can make a big difference. For advanced applications, such as military aircraft, employing additional sensors to determine the GNSS satellite locations and the platform's position and heading, the system can also steer maximum gain towards legitimate GNSS signals (beam steering).

Some CRPA systems further leverage signal processing techniques to discern the bearing and elevation angle of the interfering signal — a form of situational awareness called direction-finding, which is important in mission-critical applications. Depending on the type of spoofing, CRPAs and associated electronics also provide collateral anti-spoofing capability because they detect anomalous signals — those above a certain power threshold — and mitigate them by nulling.

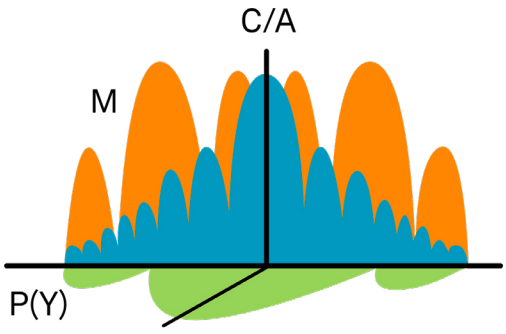

Figure 4. GPS signal codes.

Receiver-based protection
Beyond using GNSS receivers that can track encrypted codes, advanced GNSS receivers include proprietary firmware algorithms, or digital filters, that can detect and remove interfering signals by reducing their power (see inset). This includes out-of-band signals as well as higher power, in-band jamming signals.

Multi-constellation, multi-frequency (MCMF) receivers that simultaneously track multiple GNSS constellations are effective against some spoofers because they would have to produce and transmit all possible GNSS signals simultaneously to fool the target receiver. While that can be done in the laboratory, it is very hard to do in the field — especially if the target is moving.

Because spoofing signals cannot always be distinguished from authentic GNSS signals based on frequency or power level, digital filter algorithms on the receiver focus on detection metrics to alert the user — another form of situational awareness. So, while a receiver may be spoofed, the user won't be fooled by the resulting falsified PNT measurements and can make informed decisions to keep their people and assets safe.

Complementary equipment
In addition to CRPAs and high-precision GNSS receivers, users can employ alternate sensors as an added level of protection. The typical approach is to use inertial navigation systems (INS) that provide positioning via information provided by accelerometers and gyroscopes in an inertial measurement unit (IMU), as these measurements cannot be targeted by jammers.

Ideally, the INS is "deeply coupled" to the GNSS receiver through sensor fusion for reliable, continuously available 3D position, velocity and attitude, even during periods of GNSS signal unavailability. Deep coupling describes how the raw inertial measurements are used to enhance signal tracking for GNSS positioning algorithms. Through deep coupling, the INS measurements enable rapid reacquisition of GNSS signals for advanced positioning precision. In addition, the outputs of various types of motion sensors, such as cameras, radar, LiDAR and odometry distance measuring instruments (DMI) can be used in the algorithm to augment GNSS PNT.

How do signal processing and digital filter algorithms work?

CRPA electronics
The antenna electronics of CRPA arrays use adaptive **beamforming**, a spatial filtering signal processing technique, to direct the array for **null forming** (ignore interfering signals from a particular direction) and, with added sensors, **beam steering** (amplify authentic signals from another direction) **(Figure 5)**. Beam steering requires a receiver and IMU, as well as additional computation contributing to size, weight and power (SWaP) requirements and cost.

There are two main types of beamforming algorithms: **space-time adaptive processing (STAP)** and **space-frequency adaptive processing (SFAP).** STAP detects and mitigates interference based on the spatial (direction) and time (period) domains. SFAP detection is based on direction and frequency, which extends the nulling capability of the array by adding frequency-based degrees of freedom beyond the n-1 spatial degrees of freedom afforded by the multiple antenna elements.

In practice, this means SFAP can selectively null narrowband interference without attenuating other frequencies from the same direction. More advanced proprietary algorithms use a combination of both STAP and SFAP techniques to better mitigate against the range of interference types.

Receiver firmware
In use cases that cannot employ a CRPA due to controlled goods restrictions, SWaP or cost limitations, high-performance GNSS receivers use proprietary firmware algorithms to detect jamming and spoofing signals and alert the user that their PNT is under attack. This enables the user to monitor, quantify and remove interference sources.

These algorithms include RF spectrum analysis — like that provided by a spectrum analyzer — to show how much signal power is sensed across the GNSS frequency bands **(Figure 6A)**. Interference can be seen in the spectral analysis output plot **(Figure 6B)**. Signal processing and digital filters, such as a notch or bandpass filter **(Figure 6C & D)**, can then be applied to mitigate the interference allowing the receiver to continue tracking the authentic GNSS signals and provide protected APNT.

The article "Try to spoof us. But fool us? Not a chance." From the 2021 issue of Velocity provides a more detailed look at receiver firmware algorithms.

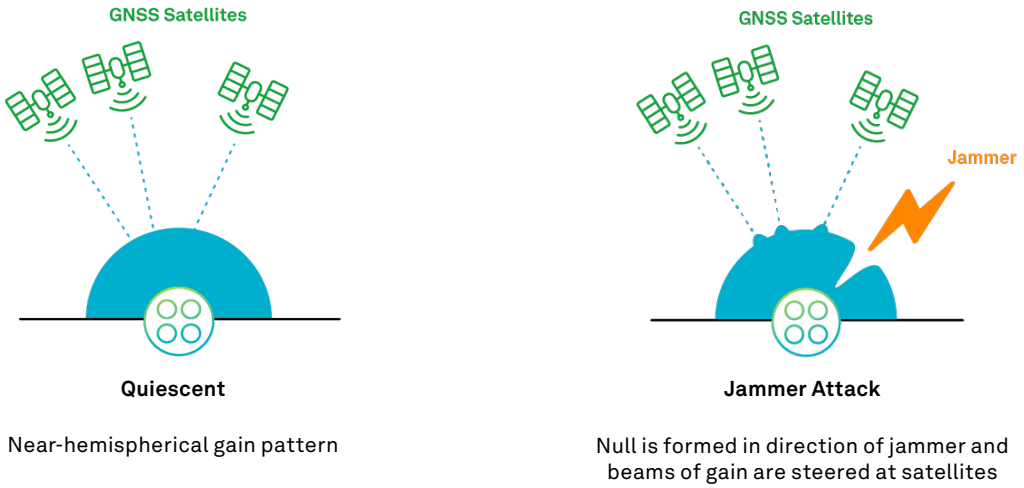

Figure 5. Graphical representation of a CRPA array gain pattern before and during a jammer attack.

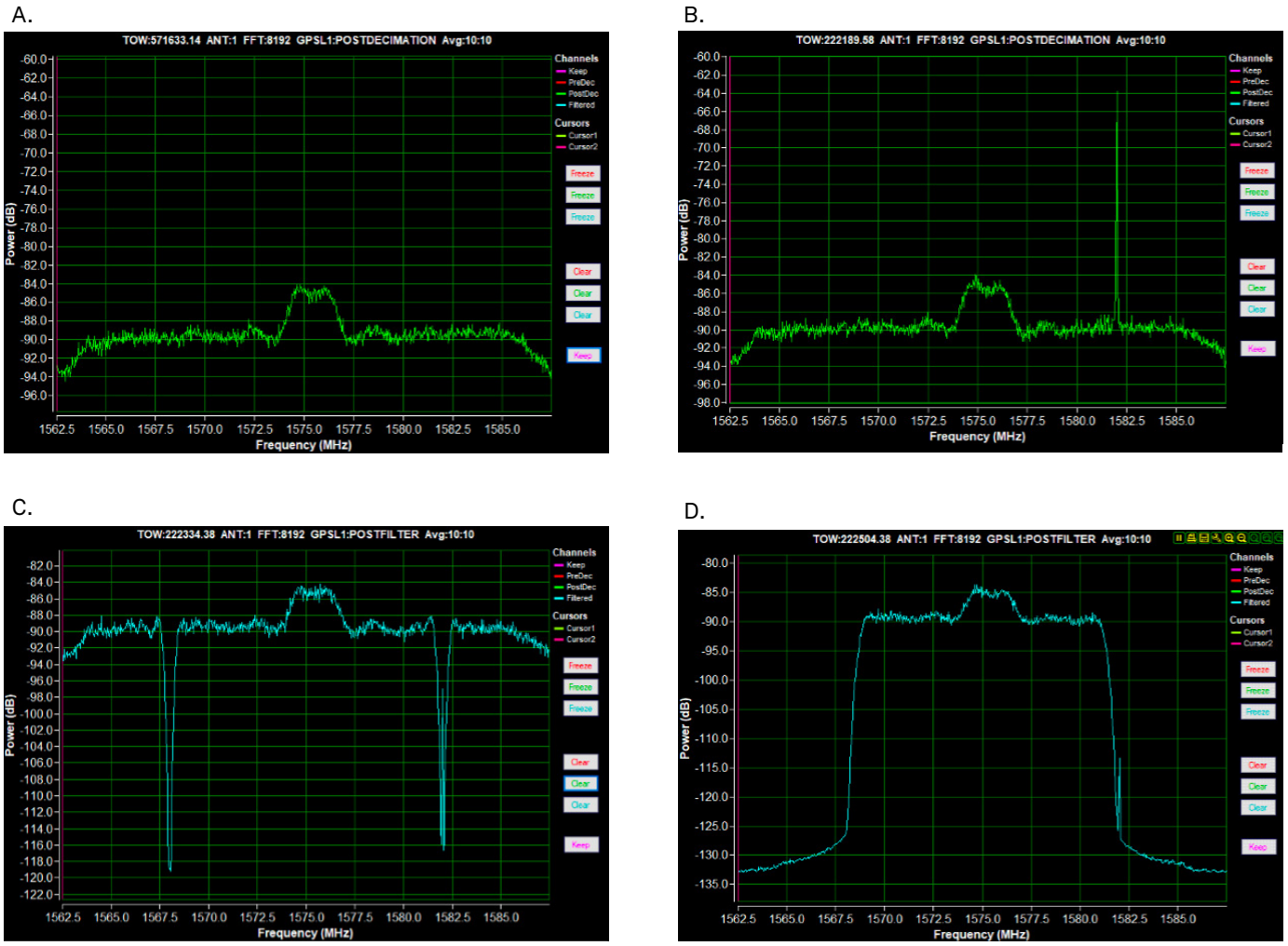

Figure 6. Example spectral plots showing the GPS L1 band spectrum without interference (A), GPS L1 band with interference (B) and the use of notch (C) and bandpass (D) filters to block the interference.

How is anti-jam performance measured?

If you've reviewed specification sheets for anti-jam products, you've likely seen several terms used to express anti-jam performance. Examples of terminology include jammer protection, interference suppression, jamming mitigation/rejection/resistance and jammer-to-signal ratio (J/S). Several of these terms are used interchangeably and the nuances in the meaning of these measurements can be confusing.

As a comparison, two common measurements are interference suppression and J/S, both measured in decibels (dB).

Interference suppression (IS) quantifies an anti-jam antenna system's ability to reduce the level of a jammer signal before it reaches the receiver. It is measured as the difference in jamming power it takes to disrupt a receiver protected by an anti-jam antenna system versus an unprotected receiver. For example, an interference suppression of 40 dB means that a receiver protected by an anti-jam antenna system can withstand 40 dB more jamming power before it is disrupted versus the same unprotected receiver. The metric for disruption of the receiver can be the complete loss of position, a 10-metre position error, or another relevant metric for the integrator's application.

J/S is the ratio of jammer to signal power before a positioning system is disrupted. When operating with a non-CRPA GNSS antenna, the J/S of the positioning system is dominated by that of the receiver, as the GNSS antenna offers limited protection against jamming. However, when paired with an anti-jam antenna system, the J/S of the Total Positioning System **(Figure 7)** is a combination of the IS provided by the anti-jam antenna system and the inherent J/S of the receiver. Additionally, the J/S value is dynamic and depends on the jamming scenario, such as the number of jammers and their signal types, bandwidths and locations, as well as the receiver type and signals tracked (C/A, P(Y) or M-Code).

As discussed in the previous section, the ability of a GNSS solution to suppress jamming depends on the attacking signal, anti-jam antenna system and receiver used. Therefore, any measure of jamming mitigation must take into consideration the individual components. An analogy would be a stereo system with a CD player, receiver and speakers. The audio performance of the systems depends on the quality of all the components individually.

For example, a manufacturer of an anti-jam antenna system may quote a J/S value without specifying that it is for the total positioning system – including the contribution of the receiver. As such, the impression is that the anti-jam antenna system provides all the protection. If a user were to compare this value to the interference suppression stated by another anti-jam antenna system manufacturer, they may assume the latter has a lower performance.

Unfortunately, there is no common test methodology on how to measure anti-jam J/S or improvement factor. Variables that impact these values include: 1) paired receiver, 2) number of jammers, 3) jamming signal, 4) direction of jammer, and 5) antenna. As such, the best way to assess anti-jamming or anti-spoofing capability is to test solutions in your specific application and environment.

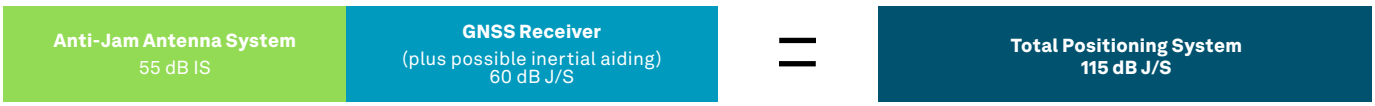

Figure 7. The jammer-to-signal ratio (J/S) capability of a total positioning system is equal to the combined capabilities of the anti-jam antenna system and GNSS receiver.

Is there GNSS equipment that cannot be jammed?

The simple answer is no. With sufficient jammer power and/or quantity of jammers, any GNSS positioning system can be jammed. It's like armour — a tank gives more protection than an SUV but with a big enough weapon, you can defeat a tank. The purpose of a resilient positioning system is to make it robust enough to make the logistics and equipment required to cause the loss of APNT expensive and impractical.

Because interference mitigation depends on the full system capability, the best way to defeat jamming and spoofing is a layered defence using an anti-jam antenna (CRPA) and an INS with deep coupling to the GNSS receiver and alternative sensors. For military users, employing a keyed military encrypted receiver (M-Code) provides an added layer of protection.

The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

References

- A. Broumandan, S. Kennedy and J. Schleppe, "Nobody's Fool: Spoofing Detection in a High-Precision Receiver," Inside GNSS+, July/August 2020, pp 36-42.
- A. Broumandan, S. Kennedy and J. Schleppe, "Demonstration of a Multi-Layer Spoofing Detection Implemented in a High Precision GNSS Receiver," 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 2020, pp. 538-547, doi: 10.1109/PLANS46316.2020.9109842.
- Jafarnia-Jahromi, Ali, Broumandan, Ali, Daneshmand, Saeed, Lachapelle, Gérard, "Vulnerability Analysis of Civilian L1/E1 GNSS Signals Against Different Types of Interference," Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015), Tampa, Florida, September 2015, pp. 3262-3271.
- "Try to spoof us. But fool us? Not a chance. Jamming and spoofing detection and mitigation in a commercial receiver." Hexagon's Autonomy & Positioning division's Velocity MagazineVelocity, 2021, pp 10-15.
- Pirsiavash, A., Broumandan, A., & Kennedy, S. (2024). OSNMA: Necessary But Not Sufficient for GNSS Security. Inside GNSS+, Sept/Oct 2024, pp 20-28.
- Pirsiavash, A., Broumandan, A., & Kennedy, S. (2024). Galileo Open Service Navigation Message Authentication (OSNMA) Benefits, Challenges, and Limitations. Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024), 16-20 September, Baltimore, Maryland.
- Pirsiavash, A., Broumandan, A., & Kennedy, S. (2024). OSNMA: A Step Toward Multi-Layered GNSS Security. Hexagon's Autonomy & Positioning division's Velocity Magazine 2024.

Hexagon is the global leader in precision technologies at any scale. Our digital twins, robotics and AI solutions are transforming the industries that shape our reality.

Hexagon's Autonomy & Positioning division is a global technology leader, pioneering end-to-end solutions for assured positioning for land, sea and air. Its solutions power intelligent positioning ecosystems in vital industries and safety-of-life applications, enabling the advancement of autonomy (cars, UAVs, industrial vehicles, trains, vessels and more). The division includes leading brands NovAtel, Veripos and AutonomouStuff.

Novatel Inc.
Hexagon Calgary Campus | 10921 14th St. NE | Calgary, Alberta, Canada T3K 2L5
US & Canada 1-800-NOVATEL or +1-403-295-4900
China +86-21-68882300 | Europe +44-1993-848-736 | SE Asia & Australia +61-400-883-601
Website: novatel.com | Email: sales.ap@hexagon.com

Version 2
May 2025