Jamming against GNSS receivers: attacks and mitigation techniques

by Marco Lisi

Jamming interference to GNSS receivers is a growing threat as more systems and devices rely on GNSS for Positioning, Navigation, and timing (PNT). The European GNSS Agency (GSA today EAASA) estimated there were 6.4 billion GNSS-enabled devices in use worldwide in 2019, and forecasts this will rise to 9.5 billion by 2029 — equivalent to 1.1 devices for every person in the world.

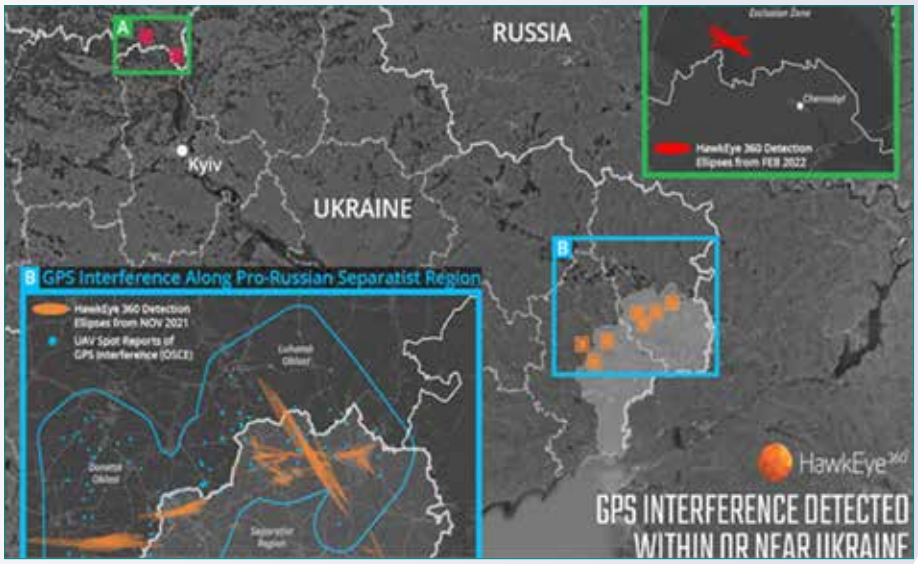

Figure 1: jamming of GPS signals detected by Hawkeye 360 satellite in Ukraine

Many of GNSS receivers are used in safety-critical and liability-critical systems. In the US, 13 of the 16 sectors of critical national infrastructure rely on GNSS, according to the Department of Homeland Security. The more the world relies on GNSS, the greater the threat presented by RF interference — whether intentional GNSS frequency jamming by malicious or mischievous actors or unintentional interference from radio transmissions in bands close to the GNSS frequencies. The impact of jamming is being felt worldwide. In the maritime sector, jamming traced to the Syrian conflict has been disrupting shipping in the Eastern Mediterranean since 2018. In aviation, the number of reports of suspected GPS signal jamming made to NASA's Aviation Safety Reporting System (ASRS) has been steadily rising. In road transport and logistics, illegal jammers are widely used to disrupt employer telematics, as well as for criminal activities. The war in Ukraine has shown in all its evidence that security concerns must be extended to all space assets, since cyberattacks, often combined with physical ones, target all digital infrastructures, on ground and in space, well knowing their interdependencies.
As far as satellite positioning systems are concerned, European aviation authorities reported a sudden increase of interferences against GPS signals in places as far away as Finland, the Mediterranean and Iraq since Russia invaded Ukraine, forcing aircraft to reroute or change destination (Fig. 1).

Definition and impact of GNSS jamming

GNSS (Global Navigation Satellite System) jamming refers to intentional interference with the signals of satellite navigation systems like GPS (Global Positioning System) or Galileo. These jamming techniques aim to disrupt or disable the operation of GNSS receivers, preventing accurate positioning, navigation, and timing information.
GNSS jamming can have various effects depending on the severity and duration of the interference. Some common effects include

degraded accuracy in positioning, navigation, and timing information, loss of signal lock or signal dropouts, incorrect positioning or velocity estimates, and increased vulnerability to spoofing attacks. These effects can impact critical infrastructure, such as aviation, maritime navigation, transportation systems, and military operations.
The effectiveness of jamming signals can vary depending on factors such as the power level of the jammer, the proximity to the targeted GNSS receivers, and the specific techniques employed.
Figure 2, however, gives an immediate feeling of how destructive jamming can be.
A very simple and inexpensive jammer transmitting a tiny 10 mW signal can cause the loss of the GPS L1 signal in receivers in a radius of 1 km and prevent its acquisition in a radius of 10 km.

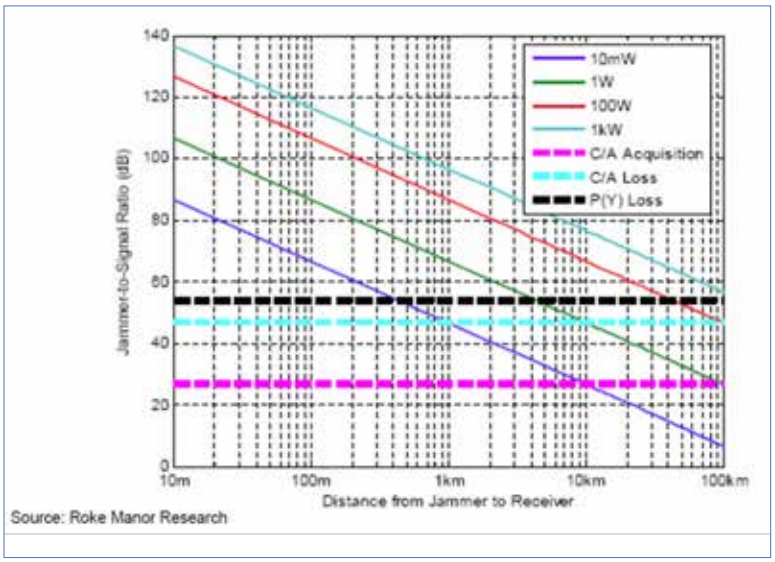

Figure 2: Susceptibility to Interference/Jamming

GNSS Jamming Techniques

Before addressing the various GNSS jamming techniques most adopted, it is worth looking at the present allocation of the RF spectrum to the main GNSS systems (fig.3)
As state-of-the-art receivers, even for commercial and consumer applications (e.g., smartphones), operates in dual frequency mode (e.g.: L1 and L2 for GPS) and even in multi-frequency, multi-constellation mode, it is evident that to be effective a GNSS jammer should operate over a quite large spectrum, generating multiple interfering signals or, otherwise, very broadband signals.
Depending on the sophistication of the jammer and its target receiver, various jamming techniques are adopted:

• Continuous Wave (CW) Jamming: this technique involves transmitting a continuous, high-power radio signal on the frequency band used by GNSS satellites. The jammer emits a powerful and persistent signal that can overpower the relatively weak GNSS signals, making it difficult for receivers to accurately acquire and track satellite signals;
• Narrowband Jamming: in this technique, jammers transmit signals that occupy a narrow frequency band within the GNSS frequency range. The jammer's signal may have similar characteristics to the GNSS signals, making it harder for receivers to distinguish between the genuine satellite signals and the jamming signals;
• Pulsed Jamming, involving the transmission of intermittent bursts of jamming signals. These bursts can be synchronized with the GNSS signal structure, mimicking the normal GNSS transmissions;
• Broadband Jamming: broadband jammers transmit a wide range of frequencies that encompass the GNSS frequency bands. These jammers can interfere with multiple GNSS systems simultaneously, such as GPS, GLONASS, Galileo, and BeiDou, increasing the chances of disrupting GNSS-based positioning and navigation.

GNSS Jamming Devices

GNSS jammers come in various forms, ranging from

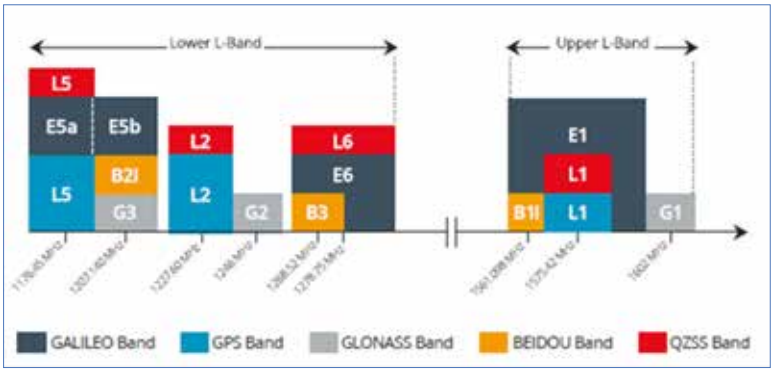

Figure 3: GNSS signals spectrum allocation

Figure 4: Commercial GNSS (GPS) Jammers

small portable devices to more powerful and sophisticated equipment. Portable jammers can have a limited range and may be used for personal privacy reasons or illicit activities. Higher-power jammers can cover larger areas and have a more significant impact on GNSS signals.
There is a huge selection of commercial jammers available on the Internet for less than $100 (fig.4).
What used to be expensive military technology a few decades ago is nowadays easily available, rather cheap, off-the-shelf products. Studies of many of these jammers have been performed, and they were categorized into the following three categories:
a. Jammers that are designed to plug into a 12 Volt car cigarette lighter socket power supply outlet. This category of jammers usually has rather low transmit power(below 100 mW) and the possibility to connect an external antenna. An example of a jammer from this category is shown in Figure 5.
b. Jammers that have an internal battery and an external antenna connected via an SMA connector. Some of these jammers transmit at both the L1 and L2 frequency bands and additional frequency bands for other types of communication (e.g. WiFi and GSM). The transmit power is up to 1 W. An example of a jammer in this category is shown in Figure 6.
c. Jammers disguised as harmless electronic devices, such as cell phones. The jammers in this group have internal batteries but no possibility of connecting an external antenna. All jammers in this group transmit power in L1, L2, and additional frequency bands, with up to 100 mW power.
Commercially available jammers often transmit chirp-like signals (i.e. frequency modulated continuous waves (FMCWs)) and operate across the band 1565-1585 MHz. The jammer changes frequency rapidly over time and sweeps across the frequency, overpowering the GNSS signal. The use of frequency sweeping means that a narrowband jammer can be used to overpower a frequency range which would otherwise have required a broadband jammer.
In conclusion, a recent and more sophisticated approach to jamming, named systematic or systemic jamming, is presented. A systematic GNSS jammer refers to a jamming device designed and deployed with

Figure 5: car GNSS jammer (10 US$ on eBay)

Figure 6: dual frequency, medium power jammer

a methodical or organized approach to disrupt Global Navigation Satellite System (GNSS) signals intentionally. The concept of systematic jamming is the following: a simple jammer might be equipped with some information of the GNSS signals and can use this to perform more sophisticated jamming. For example, it is suggested that the jammer may be equipped with a simple low-cost commercial GNSS receiver, such that it would then have access to accurate position and time, and to satellite ephemerides.
With some very basic integration of this information, it might be possible to trigger short and sparse bursts of interference at specific times, such as to deny GNSS to a nearby receiver, and to do so with a very low average power. In this manner, a receiver might be unable to: reliably detect that a jamming attack was ongoing; to effectively mitigate the jamming attack or to identify or localize the jamming source. Figure 7 shows a possible block diagram of a systemic GNSS receiver.
Just for completeness, Figure 8 shows some very high-power military jammers, like those utilized in these days in the Ukrainian war.
Depending on the type and sophistication of the jammer equipment used, the effects of jamming on the GNSS receiver can be of basically three types:

• No effect at all, if the jammer is out of range, or its centre frequency is not aligned with the target GNSS frequency;
• Degradation of GNSS signals; as the carrier-to-noise (C/N0) ratio of received signals drops, affecting the dilution of precision (DOP) value (often lower-elevation signals are affected first);
• Complete loss of tracking of GNSS signals and saturation of the receiver front end, meaning the receiver will need to re-acquire the signals.

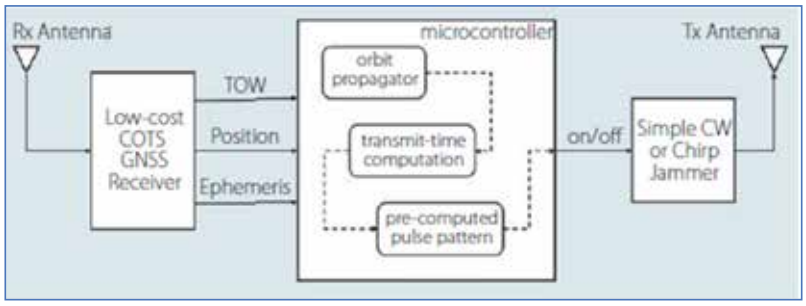

Figure 7: Systematic GNSS jammer

GNSS Anti-Jamming Techniques

To enhance the resilience of GNSS systems against jamming, researchers and engineers are developing anti-jamming techniques. These techniques include advanced signal processing algorithms, anti-spoofing techniques, secure signal authentication methods, and the use of more robust and interference-resistant receiver designs.
Interferences that are sparse in the time or frequency domain are straightforward to mitigate: pulsed jammers can simply be blanked in the time domain, and stationary continuous wave (CW) jammers can be efficiently mitigated by applying a notch-filter. FMCW jammers (commonly perceived and referred to as chirps) are more difficult to mitigate, due to the constant transmission (i.e., no time domain blanking possible) and changing frequency (i.e., notch filter must be adaptive if used). This leads to the high complexity of the interference mitigation implementation, with often only limited mitigation success.
GNSS anti-jamming techniques can be broadly classified into pre-correlation and post-correlation methods based on when they are applied in the signal processing chain of a GNSS receiver (figure 9).

Figure 8: Very High-Power, Military Vehicle-Mounted GPS Jammers

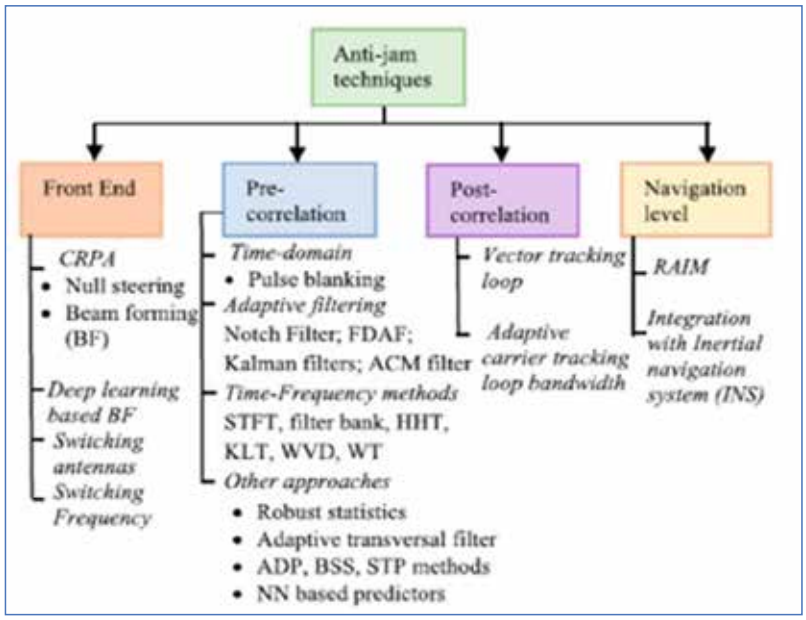

Figure 9: Categorization of anti-jam techniques

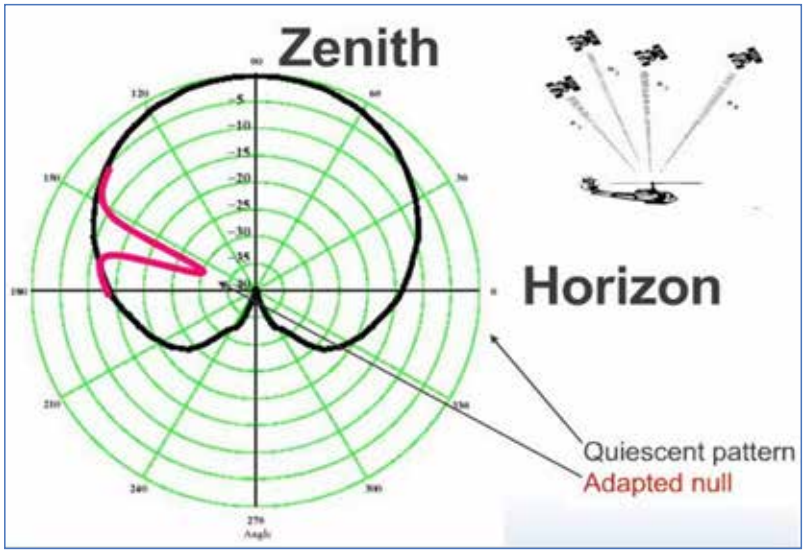

Figure 10: Principle of Spatial Nulling and Beamforming

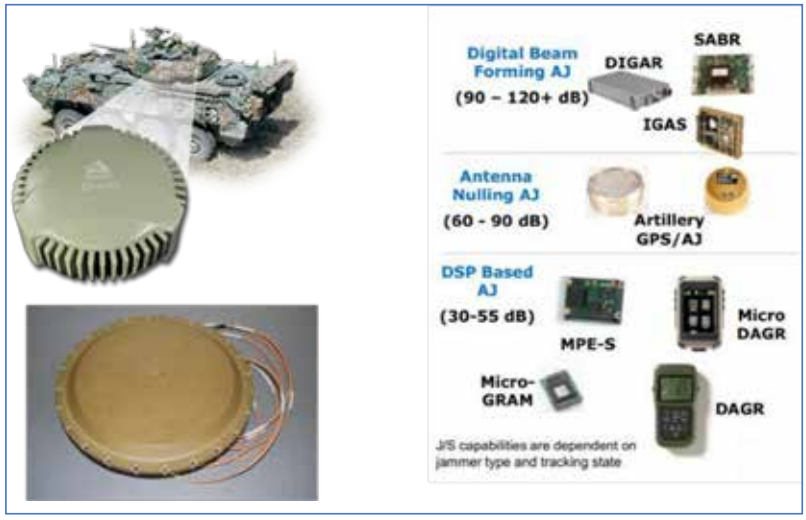

Figure 11: GPS Controlled Reception Pattern Antennas (CRPAs) with Anti-Jamming Capabilities

These techniques aim to mitigate the effects of jamming signals before or after the correlation process, which is the fundamental step in extracting timing and positioning information from the received GNSS signals.
Pre-correlation techniques can be implemented either at Rf or at IF/baseband, after analog-to-digital conversion.
Post-correlation techniques necessarily operate at baseband.
Both pre-correlation at baseband and post-correlation level mitigation techniques require access to raw GNSS signals and unless you are a GNSS receiver developer this is almost impossible.
Among the Pre-correlation techniques it is worth mentioning the Automatic Gain Control Technique and the Antenna Nulling and Beamforming.
The first is a very simple front-end level technique, operating at RF, based on the Automatic Gain Control (AGC)(either built into the external LNA or derived from the following GNSS receiver, if available), where the gain of a receiving GNSS antenna is automatically adjusted to prevent stronger jamming signals to reach the receiver. This technique provides some protection against jamming but not the continued operation under persistent jamming.
The Antenna Nulling method involves using an array of antennas to create nulls in the direction of jamming sources, reducing the strength of the interfering signals before they enter the correlation process. These antennas are named Adaptive Antenna Arrays.
By adjusting the phase and amplitude of the antenna elements, the receiver can create

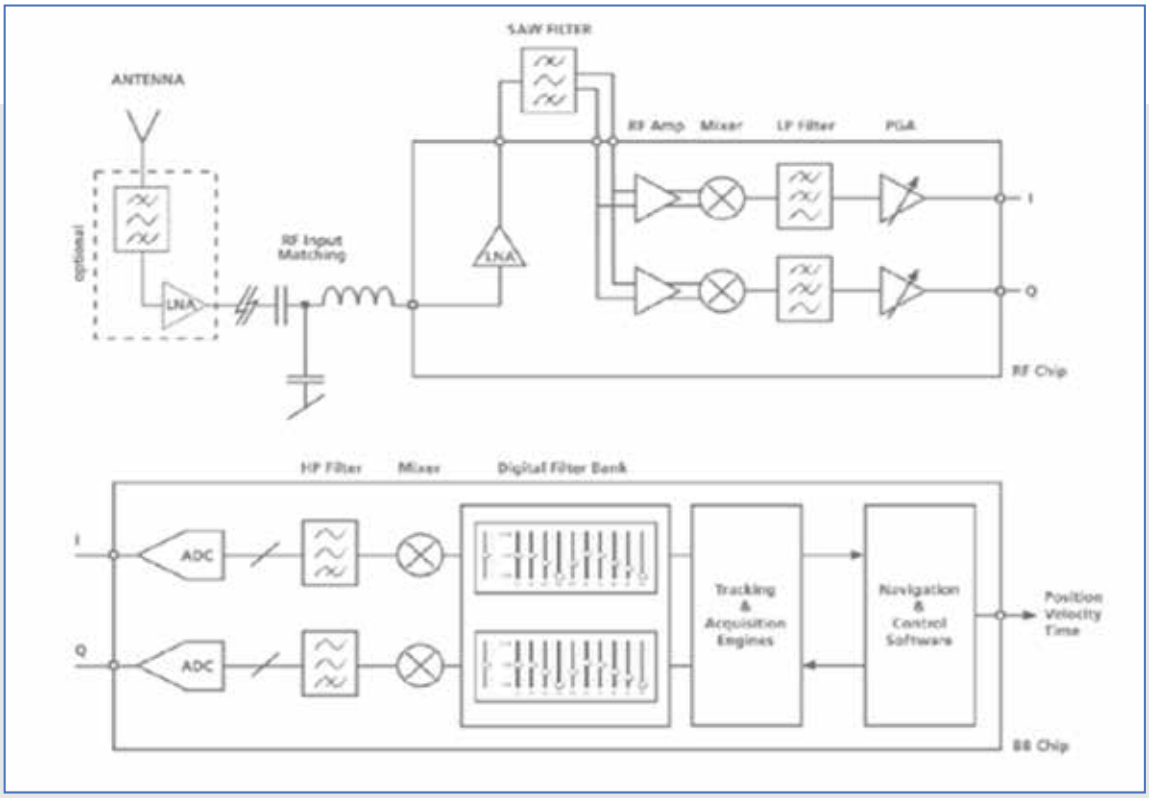

Figure 12: GPS Anti-Jamming Receiver (U-blox)

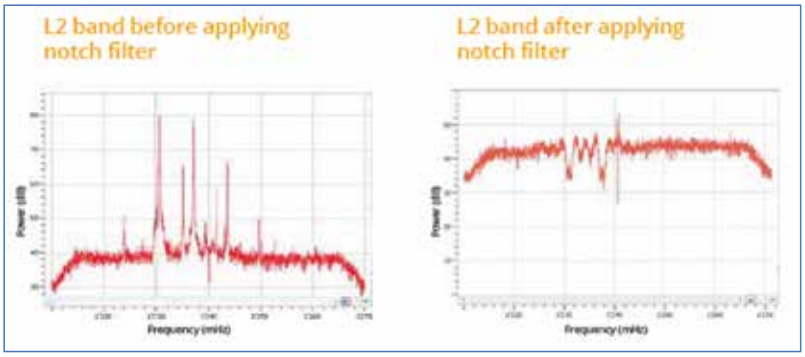

Figure 13: effect of active notch filtering

nulls in the direction of the jammer, reducing its impact on the received GNSS signals (Figure 10).
In their practical and commercial implementation, nulling anti-jamming antennas are called Controlled Radiation Pattern Antennas (CRPA).
CRPAs are widely used with digital beamforming techniques that quickly detect the jamming direction and nulls the reception in that direction to provide resilient anti-jamming capability to GNSS receivers.
Figure 11 shows some commercially available CRPAs and their anti-jamming capabilities.
Another pre-correlation technique widely adopted is based on active notch filtering.
Notch filters can be configured in the receiver firmware or by the user to filter out signals in narrow frequency bands that are susceptible to interference.
Figure 12 shows an implementation of active notch filtering in the form of digital filters for the "I" and "Q" components of the signal, before correlation and processing.
Figure 13 shows the effect of digital notch filtering on the GNSS signal (GPS L2 in this case).

KEYWORDS
GNSS; JAMMING; ANTI-JAMMING

ABSTRACT
Attacks and mitigation techniques for the jamming against GNSS receivers are described according to the fact that many of GNSS receivers are used in safety-critical and liability-critical systems.

AUTHOR
MARCO LISI
INGMARCOLISI@GMAIL.COM
MEMBER OF THE ITALIAN SPACE AGENCY BOARD OF DIRECTORS