76th International Astronautical Congress (IAC 2025), Sydney, Australia, 29 Sep-3 Oct 2025.

IAC-25,E9,2,5,x97029

Hijacking the Cosmos: The Impact of GNSS Attacks on Critical Space Systems

Arnold Chan[a]*, **Andrew Savchenko**[b]

[a] *University of South Australia, Mawson Lakes Campus. Mawson Lakes Blvd, Mawson Lakes SA 5095, Australia.*
[b] *University of Technology Sydney, Data Science Institute, Behavioural Data Science Lab. 61 Broadway, Ultimo, NSW 2007, Australia.*
* Corresponding author

Abstract

Satellite navigation systems make geopositioning possible through the use of technology called Global Navigation Satellite System (GNSS), which is vital to numerous civilian, commercial and military applications in positioning, navigation and timing (PNT). However, the reliability and availability of the GNSS signals are under growing threat from jamming and spoofing attacks that pose a significant risk to aviation, maritime navigation, autonomous systems and national security. The adversaries are found to take advantage of the vulnerabilities of these systems and launch sophisticated attacks. These threats reveal the need for new and better countermeasures that can detect, mitigate and defend against GNSS interference. This paper conducts a systematic survey of the state of the art on jamming and spoofing mechanisms in GNSS, their real-life scenarios and countermeasures. We discuss current counterjamming measures and suggest a cybersecurity-oriented approach to GNSS protection. The paper aims to enrich the field of space cybersecurity as well as to systematise technical solutions, policy proposals and strategic countermeasures that address the risks of GNSS jamming and spoofing in an increasingly complex and hostile space environment.

Keywords: GNSS authentication, GNSS defence, GNSS interference, GNSS security, satellite security, space security

Acronyms/Abbreviations

AI	Artificial Intelligence
BDS	BeiDou Navigation Satellite System
CHIMERA	Chips–Message Robust Authentication
CISA	Cybersecurity and Infrastructure Security
CNNs	Convolutional Neural Networks
CRPA	Controlled Reception Pattern Antennas
EASA	European Union Aviation Safety Agency
ECDSA	Elliptic Curve Digital Signature Algorithm
EIRP	Effective Isotropic Radiated Power
EU	European Union
EW	Electromagnetic Warfare
FFT	Fast Fourier Transform
FIR	Finite Impulse Response
FSPL	Free Space Path Loss
GDP	Gross Domestic Product
GLONASS	Globalnaya Navigazionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HEO	Highly Elliptical Orbit
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ICG	International Committee on Global Navigation Satellite Systems
IIR	Infinite Impulse Response
IoT	Internet of Things
IW	Information Warfare
MAC	Message Authentication Code
MEO	Medium Earth Orbit
ML	Machine Learning
MVDR	Minimum Variance Distortionless Response
NIST	National Institute of Standards and Technology
NMA	Navigation Message Authentication
NORAD	North American Aerospace Defense Command

OSNMA	Open Service Navigation Message Authentication
PNT	Positioning, Navigation and Timing
PQC	Post-Quantum Cryptography
PRN	Pseudo-Random Noise number
PVT	Position, Velocity and Time
QZSS	Quasi-Zenith Satellite System
RF	Radio Frequency
RNNs	Recurrent Neural Networks
SBAS	Satellite-Based Augmentation System
SCER	Security Code Estimation and Replay
SDR	Software-Defined Radio
SNR	Signal-to-Noise Ratio
SVM	Support Vector Machines
TESLA	Time Efficient Stream Loss-Tolerant Authentication
UAV	Unmanned Aerial Vehicle
UN	United Nations
USRP	Universal Software Radio Peripheral

1. Introduction

This paper surveys the technical and operational landscape of GNSS security with a focus on non-kinetic threats. It examines methods of interference, including broadband and narrowband jamming, meaconing and spoofing enabled by software-defined radios and analyses documented incidents to illustrate their operational impacts. It then reviews the principal lines of defence: adaptive filtering, directional antennas, spectrum monitoring, and cryptographic techniques such as Galileo's Open Service Navigation Message Authentication (OSNMA). By linking technical countermeasures to real-world disruptions in military [1], commercial and civilian domains, the paper aims to clarify both the vulnerabilities of current systems and the pathways to improved resilience. The scope is deliberately broad, encompassing technical, operational and policy perspectives, highlighting the position of GNSS security as one of the central elements in the space security strategy.

1.1 Importance of GNSS

GNSS systems are critical space systems that are integral to modern societies; they provide PNT capabilities for civilian and military applications alike, serving as virtually irreplaceable instruments to a wide variety of users. The United States' Global Positioning System (GPS), Europe's Galileo, Russia's 'Globalnaya Navigazionnaya Sputnikovaya Sistema' (GLONASS) and China's BeiDou Navigation Satellite System (BDS) are the foundation of current PNT services around the world with GPS being the first and is now the most common. It supports services for synchronising aviation, maritime, telecommunications and financial transactions. Russia runs GLONASS, which has been continuously updated since the 2000s to cover the whole world. It is an important strategic tool for Russia and also works with other constellations [2]. Galileo, which is developed by the European Union, was designed to guarantee the autonomy of Europe in navigation and is widely regarded as the most precise global system [2]. The OSNMA service was introduced to enhance resilience against spoofing. China runs BeiDou, which became fully global in 2020. Its distinct feature is that it offers a hybrid constellation across several orbital regimes and a unique short-message communication feature for particularly remote users. Together, these four major constellations have become interoperable and are used in combination by most modern receivers, with over 80% of devices capable of multi-constellation tracking [3]. Their integration into both civilian infrastructure and military operations makes them indispensable instruments for global security, economic activity and safety-of-life applications. GNSS constellations provide value not only on Earth, but also in the space domain. Modern satellites use GNSS for attitude and orbit determination achieving centimetre-level accuracy [4]. We believe that reliable and trustworthy GNSS will remain crucial for orbital and planetary missions for space exploration, defence applications and the expanding Internet of Things (IoT), as these activities will increasingly depend on resilient space-based assets.

1.2 Growing threats to GNSS security

The GNSS has become a part of the world's critical infrastructure, and disruptions can have cascading impacts. Studies estimate that over 10% of Gross Domestic Product (GDP) in advanced economies relies on GNSS-enabled services; for example, 11.3% of the UK's GDP is supported by GNSS, such that a large-scale outage could cost nearly £2 billion per day [5]. Even tiny timing errors on the order of 0.00001 seconds can halt trading systems, strand ships, disrupt power grids and impair emergency services [5]. Given that GNSS is so vital for many, it is a desirable target for adversaries and makes it more crucial than ever to improve GNSS security. The primary threats to GNSS signals are jamming and spoofing including related techniques like meaconing. Jamming is the deliberate transmission of radio frequency (RF) noise or signals on GNSS frequencies to overwhelm or block the authentic signals [6]. Spoofing is more insidious because it involves transmitting fake GNSS-like signals to deceive receivers into calculating incorrect positions or time [6]. Until recently, executing sophisticated jamming or spoofing required specialised equipment and expertise. However, the proliferation of low-cost, programmable radios and readily available online instructions has dramatically lowered the barrier to entry [6]. Cheap software-defined radios (SDRs) such as HackRF or universal software radio peripheral (USRP) devices that cost only a few hundred dollars can be turned into GNSS interference tools, meaning ‘almost anyone’ can now attempt jamming or spoofing attacks [6]. Indeed, the literature notes a ‘rapid development and increased number of attacks’ in recent years, driven by easy-to-use SDR platforms and widely shared techniques [6].

Our paper presents a survey on the impact of GNSS attacks on critical space systems as well as the recent technological developments in the detection and countermeasures against the non-kinetic attacks. The threats to space assets continue to increase as our reliance on such systems becomes institutionalised and universal. Given the advancements in robotics and uncrewed systems coupled with the increased commercial interest, we foresee ransomware-type attacks happening not only over the public Internet and directed at virtual assets, but well and truly in the operational domains and targeting physical space assets in orbit.

2. GNSS spoofing and jamming techniques

There are different doctrines and ways of categorising jamming techniques. For the purpose of this paper, we split them into two major sections: broad and narrow band. We use this 2-section enumeration, as it broadly aligns with the terminology used within the Information Warfare (IW) and Electronic Warfare (EW) communities.

But before we look more closely at the attacks themselves, let us outline key phases in the GNSS acquisition process. Generally speaking, to obtain a position lock, a receiver needs to know 3 things apart from the frequency:

1. Pseudo-random noise number (PRN), an ID that is unique to a satellite within a given constellation at a specific time. A receiver knows these in advance; however, it does not know which PRNs are currently in its view without recent almanac, ephemeris, time, and own position. PRNs can be pre-configured, cached from previous sessions, obtained via A-GNSS or found via exhaustive search.
2. Code phase. A timing offset of the received PRN compared to the local replica that corresponds to the signal latency and is essential for ‘pseudorange’ estimation.
3. Doppler frequency. Knowing a frequency shift that occurs due to the relative motion between a receiver and transmitter is required to compensate for the Doppler effect and demodulate the signal. For a stationary receiver, maximum search range is about ±5 kHz or ≈10 kHz in total [7]. This can be further increased because of the high orbital speed of the transmitter with respect to the receiver, which can prevent or delay the lock acquisition.

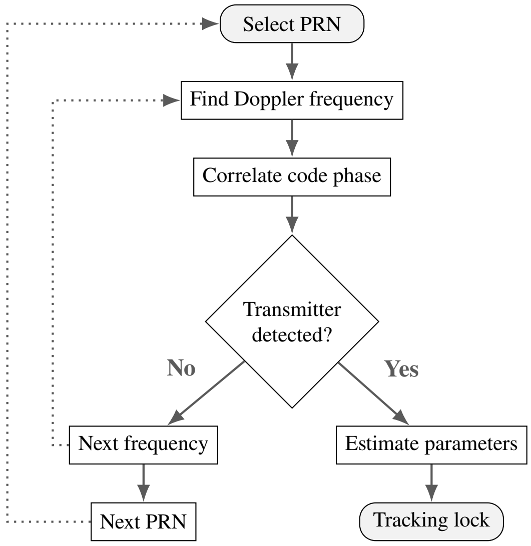

Fig. 1: Simplified GNSS acquisition process flow.

You can refer to the Fig. 1 for a graphical overview of the process. It is worth noting that while GNSS constellations are vulnerable to all of the approaches listed in section 2 and are not too dissimilar from the terrestrial assets, they do have their own idiosyncrasies. Due to their altitude, space-based GNSS receivers on LEO orbit are affected by the ionosphere to a lesser degree and have to deal with a different signal path geometry where atmospheric delays play a lesser role compared to their ground-based counterparts. However, unlike the terrestrial receivers, space-based ones have to account for solar radiation [8], higher Doppler dynamics and a comparatively short window where an individual transmitter is available.

Also, of note would be low power levels exhibited by GNSS signals, normally within the -122 to -133 dBm for Galileo and Beidou respectively [9]; a direct consequence of space assets relying on restricted power packages along with the significant distances between the ground level and satellites, latter reaching as high as $\approx 40,000$ km (QZS-1, NORAD ID 37158). Predictably, such a vast range between transmitters and receivers leads to high latencies making defences that rely on bi-directional communication less practical. Lastly, there are physical limitations to keep in mind. Where ground-based systems can temporarily increase their power output to counter interference and improve SnR, the space domain can rarely afford such luxury due to the limited battery reserves and thermal constraints.

2.1 Broadband attacks

Attacks in this category intend to deny the receiver capability to obtain lock on the transmitter; they use broad-spectrum emissions to increase noise floor in the parts of the spectrum that overlap with the carrier components and ranging information. These are jamming attacks and can be broadly separated into:

1. White noise, also known as random or uniform – a *'noise in which the frequency and power spectrum are constant and independent of frequency'* [10].

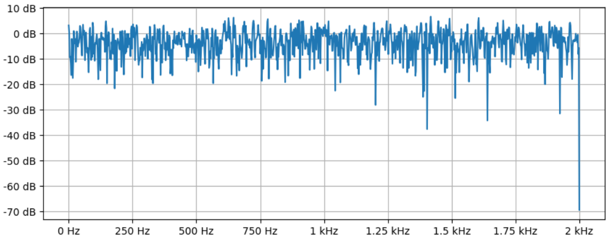

Fig. 2: Illustrative spectrogram of the white noise.

2. Coloured noise – a signal covering broad range of the spectrum where power output is dependent on frequency; includes terms such as 'pink' and 'brown' noise often used in analog electronics [10].

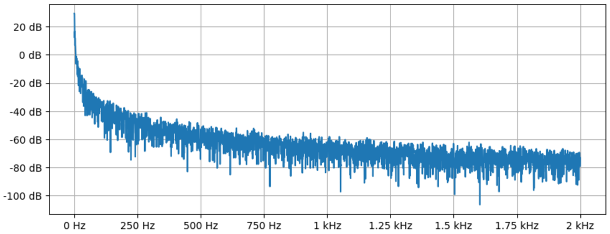

Fig. 3: Illustrative spectrogram of the pink noise.

While jamming attacks can be conducted from either the ground surface or an orbit, power needs range from single-digit kilowatts of effective isotropic radiated power (EIRP) for degradation to tens and hundreds for the complete loss of lock [11]. They can vary greatly based on the orbital position of the target, frequency, antenna design and deployed countermeasures. Either way, achieving such output would present a challenge for most satellites. This is especially true in crisis scenarios when a jamming attack must be sustained for an entire period during which the jammer and its target are not shadowed by their respective masking angles or other astronomical objects.

For example, let us look at the very rough approximation of an attack that requires sustaining 2 kW of output power over 12-hour window at 80% efficiency:

$$Energy_{\mathrm{Wh}} = \frac{2,000\ watts \times 12\ hours}{0.80\ efficiency\ ratio}$$

This gives us 30 kWh required over the 12-hour period, which equals to $30000 \div 12 = 2500\ W/h$. Now, let us find the weight of required battery pack at 100 Wh/kg energy density and solar power generation capacity. We will assume LEO orbit with sunlight fraction 60%, panel area 10m^2, 30% efficiency and use solar constant 1.361 kW/m^2.

$$Power = 1361\ W/m^2 \times 10\ m^2 \times 0.30 = 4083\ W$$

Therefore, a battery for the emitter alone would need to provide anywhere from 0 to 2500 W of power depending on illumination of the solar array. As we have assumed 60% sunlight, time distribution becomes: $0.60 \times 12 = 7.2$ hours illuminated and $0.40 \times 12 = 4.8$ hours shadowed. Then, maximum energy required from the battery is $2500\ W \times 4.8\ h = 12000\ Wh$ and its mass becomes:

$$Battery\ weight = \frac{12000\ Wh}{100\ Wh/kg} = 120\ kg$$

Add to this thick wiring, thermal dissipators, rest of the subsystems and support structures to handle it all – you end up with a satellite that can reach 1000 Kg wet mass. Economic considerations as well as the bus requirements would present significant operational limitations for the launch of such an asset.

However, we also need to consider that achieving even tens of kW EIRP is entirely feasible and more cost-effective on the earth's surface, where a transportable antenna would be sufficient to compensate for the loss caused by the distance. We now verify this and calculate a rough power budget of such an attack.

First, we need to find the free space path loss (FSPL) of common carrier frequencies for data transmission: 1575.42 MHz for Galileo E1 or GPS/QZSS L1 and 1278.75 MHz for E6/L6 at typical MEO altitude of ≈20200 km. We will use the following formula[1]

$$\mathrm{FSPL}_{dB} = 20\log_{10}(d) + 20\log_{10}(f) + 32.45$$

[1] https://ib-lenhardt.com/kb/glossary/fspl

where d is a distance in km and f is a frequency in MHz. This gives us ≈182.5 dB for GPS and ≈180.7 dB for Galileo and QZSS. Complete expanded forms are available in Appendix A as (1) and (2) respectively. While E6/L6 offers approximately 2 dB advantage in the path loss, E1/L1 remains the more attractive target for GNSS interference attacks as numerous receivers still require E1/L1 (and/or E5/L5) in the cold start scenario, and will not be able to utilise E6/L6 until an approximate PVT is obtained.

To achieve reliable loss of lock, our signal must exceed noise floor + processing gain on the receiver. The required transmitter antenna gain becomes: $Jamming\ signal - Transmitter\ signal + FSPL$.

We can calculate the required gain using the minimum signal specification[2] of −160 dBW [12] and the same 2 kW transmitter (which can be expressed as 33 dBW). We begin with L1/E1: $-160-33+182.5 = -10.5$ dB and E6: $-160-33+180.7 = -12.3$ dB. Then, we need to account for the 27 dB C/A code acquisition and 47 dB C/A code lock loss thresholds [13] to overcome the processing gain.

For acquisition disruption:

$$\begin{aligned}\text{L1/E1}_{disruption} &= -10.5 + 27 = 16.5\ dB\\ \text{E6/L6}_{disruption} &= -12.3 + 27 = 14.7\ dB\end{aligned}$$

And for the complete tracking loss:

$$\begin{aligned}\text{L1/E1}_{loss} &= -10.5 + 47 = 36.5\ dB\\ \text{E6/L6}_{loss} &= -12.3 + 47 = 34.7\ dB\end{aligned}$$

Thus, even accounting for imperfect alignment of the antenna and atmospheric effects, adding a 20-40 dB parabolic dish should be sufficient.

We hope that this little comparison contrasts dramatic operational efforts required to achieve broadband jamming from a space asset compared to the relatively affordable capabilities that can be deployed from the land domain. That being said, there is a range of 'narrowband' attacks that do not require such dramatic power outputs and therefore are more attractive to mount from an orbit.

2.2 *Narrowband attacks*

Attacks under this category serve two distinct goals: denial and deception. While jamming aims to simply deny the PNT capability, the end goal of spoofing is to make it inaccurate in a way that is advantageous to the adversary. Here, we will use the following categories:

1. Single frequency jamming, commonly referred to as 'spot jamming' – simple suppression of a particular, narrow carrier frequency [6].

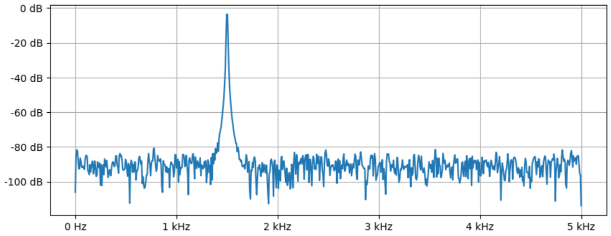

Fig. 4: Illustrative spectrogram of the spot jamming.

2. Sweep frequency jamming – also referred to as the 'chirp jamming'. Similar to the single-frequency, but the carrier frequency changes with time [6].

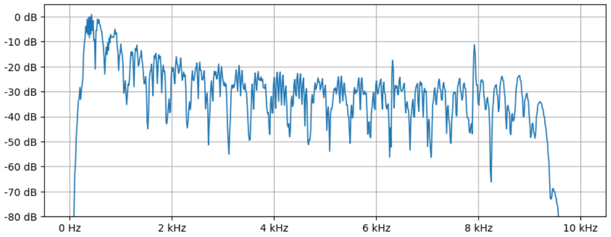

Fig. 5: Illustrative spectrogram of the chirp jamming.

3. Spoofing – transmission of a deceptive signal with the intention of misguiding the receiver. Such a signal often, but not always, has marginally higher power output compared to the authentic source.

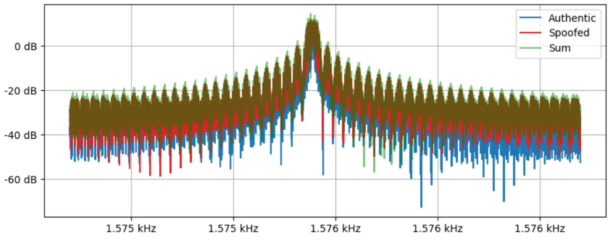

Fig. 6: Illustrative spectrogram of the spoofing showing $authentic\ signal + spoofed\ signal + additive\ noise$ with simulated interference.

As we have already established baseline requirements for jamming attacks, let us focus our attention on spoofing methods. It is important to keep in mind that cryptographic protection of the messages is not deployed as

[2] Further information can be found in Interface Control Documents (ICDs) for the respective constellations.

widely as one might assume. As noted by Eberhard et al., who tested 57 space-capable GNSS receivers, 47 of them (85.5%) show complete absence of any authentication features and 8 (14.0%) support only exclusive P(Y)/M authentication codes [14] that are exclusive to the military[3].

Methods described in this section work on signal level and rely on obscuring the original signal with the forged one, not on attacking cryptographic implementation.

2.2.1 Synchronous and asynchronous spoofing

We will use classification proposed by J. Rossouw van der Merwe et al. [15] and focus on two strategies of forcing the receiver to lock onto the spoofed signal: synchronous and asynchronous.

Synchronous takeover is rather complex; to perform it successfully, an attacker must [16] align spoofed signal within the narrow correlation window on the receiver. For GPS C/A code, this would be approximately 1 ms [12]. Overall, an attacker should ensure that:

1. Spoofed signal has *slight* power advantage over the authentic one, and is in sync with the authentic signal code phase and Doppler.
2. Carrier frequency and phase are closely aligned, navigation data bit timing and content are consistent.
3. There is no loss of lock in the process (in other words, that the transition is transparent to the receiver).

While spoofing attacks can be executed during both acquisition and tracking phases, it is the search across a wide Doppler range and comparatively lengthy code phase traversal that increases the probability of the successful takeover. Such choreography requires delicate balancing of marginally higher power output at around 4 dB [17] along with the precise instrumentation.

In contrast, asynchronous spoofing demands significantly higher power output, approximately 40-50 dB above authentic signal level [15]. Although it can be performed in less time, unless detected by the source (which is not impossible given the $\approx$ 30 dB difference).

One of the most straightforward examples of the asynchronous attack is a basic replay often referred to as 'Meaconing'. In essence, attacker captures authentic GNSS packets and retransmits them with a delay causing Position, Velocity and Time (PVT) drift on the receiver. This is especially problematic in situations when an on-orbit receiver relies on side-lobes of GNSS transmitters to maintain truthful PVT.

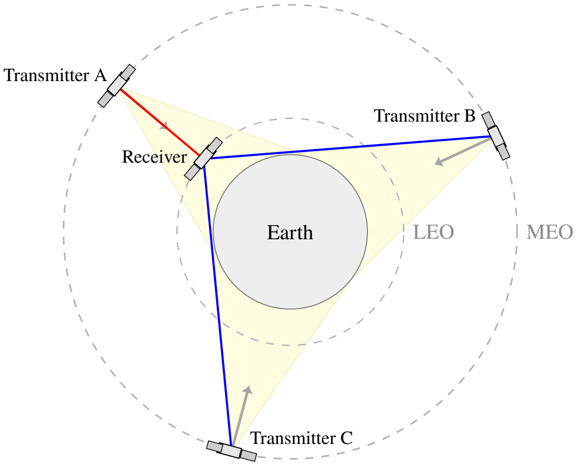

Fig. 7: Receiver on LEO orbit receiving GNSS signals via primary (red) and secondary (blue) lobes from transmitters on MEO orbit.

Consider Figure 7; it would be quite impossible for the receiver to obtain the lock relying exclusively on the strong primary lobe of the transmitter *'A'* directly behind it, therefore it has to count on the other two: *'B'* and *'C'*. This creates an opportunity to mount a successful attack utilising a smaller payload and less powerful transmitter that targets only the secondary lobes, therefore compensating for the higher gain normally required for an asymmetric attack. Given the orbital dynamics, this can introduce PVT error measured in hundreds of kilometres [18] and lead to catastrophic navigation failures during the orbital insertion or cause other manoeuvre errors.

Contrary to jamming, meaconing is harder to detect, especially in situations where power difference is not obvious, highly accurate clock source is not available or if receiver is performing a 'cold start' [18] where previously stored time and location can not be relied on. Even if Navigation Message Authentication (NMA) system (e.g. Galileo OSNMA) is used, meaconing remains an ongoing concern as signal-level timing manipulation does not require breaking cryptography implementation. In fact, attackers who choose to employ these methods are unlikely to care if encryption or signing is even implemented.

Otherwise, an attacker in a favourable electromagnetic environment can try to mount a Security Code Estimation and Replay (SCER) attack to enumerate cryptographic elements and replay them to a receiver that relies on NMA.

3. Contemporary GNSS attacks

GNSS attacks in the recent decades have evolved in both quality and quantity. Threats to the global space infrastruc-

[3] US, UK, Australia, Canada and select NATO members.

ture extend to the orbits as high as ≈1900 km [19] and have potential to disrupt anything from an individual space vehicle to an entire constellation. For example, Starlink[4] has been under systematic attack since February 2022, with its network of >7000 satellites facing coordinated EW operations [20, 21]. From the technical standpoint, we would like to highlight several relatively modern developments:

1. Widespread [22] exposure of space-based assets to public networks. This creates opportunities for attackers to reuse existing ground stations to increase numbers of operationally-viable transmitters under their control.
2. Proliferation of commercial hardware and open-source schematics that lower technical and financial barriers for conducting an attack [6, 23].
3. Creative deployment options such as on uncrewed aerial vehicles to reduce the interference and distance to target [23].

These advancements occurred in parallel with the increase in frequency and geographic expansion where new regional hotspots have emerged across multiple areas. In Myanmar, the military junta has deployed multiple jammer types affecting parts of the coastal border with Bangladesh in addition to some local areas [24]. North Korean activities adversely affected hundreds of ships and aircraft [25, 26] in East Asia. Russian GPS interference operations expanded from the war in Ukraine to the Baltic and Black Sea, affecting civilian aviation [27] and maritime traffic [28] disrupting tens of thousands assets [29] across Europe. We would like to point out that some of the transmitters and antennas currently used for jamming and spoofing on land, sea and in the air have sufficient power and directionality to be repurposed against orbital assets. This can create preconditions for potential cascading failure, where numerous, small-scale PVT disruptions lead to an orbital collision with unpredictable outcomes.

4. Countermeasures and protective strategies

Most of the modern GNSS receivers use a range of techniques to defend against jamming (e.g. intentional interference) and spoofing (e.g. false signal injection) attacks. Below is a literature-backed overview of anti-jamming measures and anti-spoofing strategies [30] [31] [32] and advanced cybersecurity defences that are focused on developments from the past 5 years.

4.1 Anti-jamming techniques

The GNSS has become a critical enabler of PNT and synchronization across both civil and military domains; the vulnerability of its weak satellite signals to intentional interference has driven extensive research into anti-jamming measures. Three major categories of protection are spatial filtering through controlled antennas, adaptive signal-processing methods and front-end hardening combined with spectrum monitoring that form the backbone of modern defense strategies.

4.1.1 Directional antennas and null-Steering

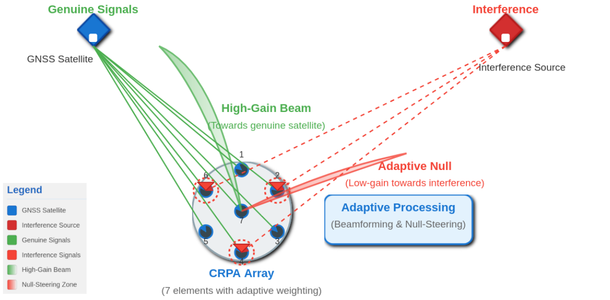

Fig. 8: An effective anti-jamming approach using CRPAs.

Antenna-based defences possess the advantages of being resistant to software attacks, intrinsically resistant to spoofing, and it is capable of enhancing the security of existing receivers. An effective anti-jamming approach is the use of multi-element or phased-array antennas which are often called Controlled Reception Pattern Antennas (CRPAs) that can steer antenna gain patterns as shown in Figure 8, where the antenna array forms a high-gain beam toward the genuine satellite while steering nulls toward interference sources. By adaptively weighting antenna elements, the receiver forms nulls (low-gain directions) toward interferers while maintaining high gain for genuine satellite signals [33, 34]. This spatial filtering is achieved normally via the minimum variance distorionless response (MVDR) or power-inversion algorithms that is significantly attenuates jamming sources, yielding large improvements in interference tolerance (on the order of tens of dB in C/N0 or jamming-to-signal ratio) in recent studies [33].

4.1.2 Adaptive filtering and interference mitigation

Besides spatial filtering, receivers use time and frequency-domain filtering to suppress jammers. For example, pulse blanking can zero out strong interference pulses, and adaptive notch filters that realised with infinite impulse response (IIR) and finite impulse response (FIR)

[4] SATCOM constellation owned and operated by SpaceX.

techniques automatically notch out narrowband jamming in the receiver's passband [33]. These adaptive filters leverage the signal's statistics to minimise impact on GNSS signals, though care is needed to avoid removing parts of the spread-spectrum signal [33]. Advanced transform-domain methods that apply fast fourier transform (FFT) and wavelet transforms as examples that further help separate interference from signal in time-frequency space, enabling removal of chirp or wideband jammers via spectral projection or thresholding [33]. Such adaptive filtering schemes have been widely researched as practical interference mitigation techniques in the last few years.

4.1.3 Shielded receivers and spectrum monitoring

Physical and RF front-end protections can harden GNSS systems against interference. High-quality RF filters and shielding architectures in the antenna or front-end (for example, cavity filters or choke-ring antennas that block low-elevation signals) attenuate out-of-band and off-axis interference [35]. These measures reduce a receiver's susceptibility by limiting the jamming energy that reaches the GPS/GNSS correlators. In addition, continuous spectrum monitoring – either within the receiver or via external sensor networks is used to detect and localise jamming sources in real time [35]. Many countries' national authorities have deployed networks of interference monitors to flag GNSS jamming events, improving situational awareness and enabling prompt counteractions [35]. In brief, an array of front-end protection along with close monitoring makes the receiver less likely to be jammed.

4.2 Anti-spoofing techniques

Spoofing is a highly deceptive vulnerability to GNSS since it produces fake signals that seem like real ones in order to deceive receivers. Unlike jamming, which is overt and results in signal loss, spoofing seeks to subtly alter a user's position or timing solution. To defend against this, modern GNSS systems employ a layered strategy combining signal diversity, cryptographic authentication and anomaly detection that each provides a distinct line of defence against spoofed signals.

4.2.1 Multi-frequency and multi-constellation receivers

When using multiple GNSS frequencies and constellations such as GPS, Galileo, GLONASS or BeiDou, it offers the additional protection and cross-checking that makes it much easier to spot spoofing. A spoofer would need to precisely counterfeit signals on several frequencies and from many satellites consistently, which is significantly more difficult to do without detectable inconsistencies. Receivers can perform integrity checks on measurements, for example, comparing pseudo-ranges from different satellites or constellations to detect anomalies indicative of spoofing [6]. Prior work has shown that differential pseudorange or position consistency checks across constellations can reveal the presence of a fake signal source (since a single spoofer often cannot perfectly align with the geometry of all real satellites) [6]. Overall, multi-constellation and multi-frequency GNSS use not only improves accuracy but also makes the system inherently more robust against single-system attacks.

4.2.2 Navigation Message Authentication (NMA) - Galileo OSNMA

Cryptographic authentication of navigation data is an innovative approach to prevent spoofing that is now being used in GNSS. Notably, Europe's Galileo system has introduced the Open Service Navigation Message Authentication (OSNMA) feature, which embeds cryptographic authentication data into the satellite's broadcast message on the E1 signal. This added data allows a receiver to verify that the navigation message (orbit, clock, etc.) indeed originates from a Galileo satellite and has not been modified in transit [36]. Galileo OSNMA that is officially launching in 2025 uses a public-key scheme: the satellites transmit signed authentication bits and receivers, with the appropriate public keys, that can validate the signatures [36]. This provides a robust layer of defence against spoofing of the navigation message – in effect, the receiver can cryptographically detect false data. Galileo is the first GNSS to offer an open-service authentication of this kind, adding significant spoofing resistance for civil users (though it does not prevent jamming) [36]. Following Galileo, similar navigation message authentication schemes are being planned for other systems; for example, GPS 'CHIMERA' on L1C and Satellite-Based Augmentation System (SBAS) message authentication. There is also ongoing debate within the space industry regarding the extent to which NMA can protect users against SCER-based spoofing attacks [37].

4.2.3 Time-based and Doppler shift anomaly detection

Even without cryptographic aids, receivers can exploit the laws of physics to spot spoofers. One tell-tale sign of a spoofing attack is anomalous Doppler and timing behaviour. Real satellites are in motion relative to the receiver, so each genuine GNSS signal has a distinct Doppler frequency that changes over time. However, a spoofing device is usually at a fixed location relative to the target and often broadcasts all counterfeit signals from one spot, resulting in an identical static Doppler shift on all signals. In other words, the forged satellite signals show the same Doppler (or no Doppler change) across different satellites, which is unrealistic for true GNSS signals [6]. Likewise, the geometry of spoofed signals may imply a constant range or elevation angle to the 'satellites', again reflecting the fixed spoofer location [6]. Receivers can monitor for these red flags: a cluster of signals with the same Doppler or sudden, synchronised jumps in pseudorange or time values (which cannot happen simultaneously on all genuine satellites) indicate a likely spoofing or meaconing attack [6]. Many present spoofing detection algorithms evaluate on things like Doppler consistency, shifts in signal transit time, or modifications to the position solution to automatically convey real signals from fraudulent ones.

4.3 Advanced cybersecurity defences

Current GNSS faces increasingly sophisticated cyber and electronic threats; traditional countermeasures are no longer sufficient. The emerging cybersecurity defences for GNSS have been increasingly combine of intelligence, resilience and trust through methods like AI/ML-based anomaly detection, secure firmware management and cryptographic authentication. These approaches are converging into a layered defence architecture that integrates detection, life cycle security and signal integrity. These measures will be critical to ensuring GNSS reliability and resilience against future jamming, spoofing and cyber attacks.

4.3.1 AI/ML-based GNSS anomaly detection

Due to the complicated spectral signatures of jamming and spoofing, machine learning has become a popular approach to protect GNSS. Recent surveys show that in the last few years, a variety of machine learning (ML) models – from decision trees and support vector machines (SVM) to neural networks – have been applied to classify normal versus attacked GNSS signal conditions [6, 38, 39]. ML algorithms are capable of analysing features including carrier-to-noise ratios, signal quality metrics, position residuals, and spectrum data to identify patterns that suggest interference. High accuracy in spoofing detection has been reported by researchers utilising supervised classifiers with field-tested models. Decision trees and SVM exhibited enhanced efficacy in distinguishing genuine cases versus spoofed signals in multiple studies [6,38,39]. Likewise, neural network approaches (including deep learning on raw signal samples or correlator outputs) have shown promise in detecting subtle or evolving attack strategies [6,38,39]. The advantage of AI/ML methods is their ability to fuse many parameters and adapt to new attack signatures; thus, incorporating AI-based anomaly detection in GNSS receivers is a cutting-edge defense to rapidly flag jamming and spoofing events that might evade traditional thresholds.

4.3.2 Secure GNSS receiver firmware updates

Maintaining safe and current firmware on GNSS devices is a crucial defensive measure. As GNSS receivers become connected devices (e.g., in drones, vehicles, or critical infrastructure), they will encounter cyber vulnerabilities like any other networked equipment. Makers and operators need to use safe ways to upgrade firmware (digital signatures for authenticity and encryption for privacy) and to quickly fix any security holes found in receiver software. Recent policy guidance from the U.S. and others explicitly urges GNSS receiver manufacturers to improve the security, integrity, and resilience of their equipment in the evergrowing cyber threats [40].

4.3.3 Cryptographic methods for GNSS integrity

Researchers are working on a wider range of cryptographic protections to check GNSS signals at several levels, not just for navigation message authentication. The main idea is to put cryptographic markers into GNSS signals or data so that a receiver can use math to check that the signal is real. By adding unpredictable, secret-based features to the signal (whether in the navigation bits or even the spreading code), one can make it infeasible for an adversary to forge the signal without the secret. As a general principle, *'adding cryptographic markers to satellite navigation signals allows the receiver to verify that the signals are from real satellites and have not been tampered with'* [41]. Current implementations and proposals include digital signatures on nav messages (as in OSNMA and similar schemes), symmetric- key sequences or one-time keys for spreading code modulation, and delayed-disclosure protocols like TESLA that authenticate bits after a short delay. For example, a navigation message authentication protocol might use a combination of a public-key digital signature and a hash-based one-time key (TESLA) to sign the data, which ensures both authenticity and timeliness of the signal [41]. Figure 9 shows a high-level illustration of the OSNMA process, which is built on the TESLA protocol, where the authenticating key is broadcast with a delay for all satellites, enabling both auto-authentication and cross-authentication of data across different satellites [42].

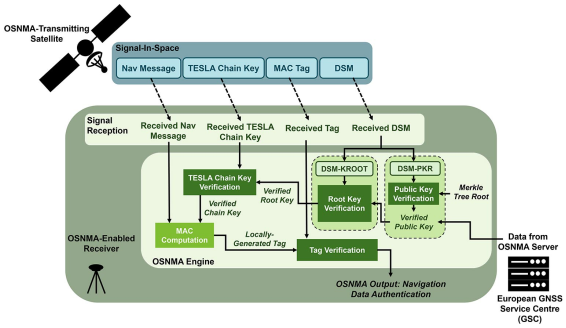

Fig. 9: Illustration of the OSNMA process [42, Fig. 1]

These cryptographic GNSS integrity measures are being standardised – Galileo's OSNMA is pioneering one approach, and GPS is testing the Chips-Message Robust Authentication (CHIMERA) technique for future use. As these technologies mature, they are expected to greatly enhance civilian GNSS integrity by virtually eliminating certain spoofing vectors (since an attacker cannot feasibly fake the cryptographic components of the signal). In summary, adding cryptography into GNSS signals represents a forward-looking strategy to bolster trust in GNSS-provided position, navigation and timing information.

5. Future challenges and research directions

For the future challenges and research directions, we discuss three interconnected developments that are currently shaping the future of GNSS protection. These challenges highlight that the future of GNSS security will depend on sustained innovation, coordinated policies and global cooperation that provides the foundation for the concluding discussion on resilience strategies and their implications for critical space systems.

5.1 Quantum-resistant GNSS authentication

Current open-service authentication schemes, such as the Galileo OSNMA, rely on a hybrid approach combining symmetric TESLA-based message authentication codes and a public-key trust anchor based on elliptic curve digital signatures (ECDSA). While effective against today's adversaries, these primitives are vulnerable to quantum computing advances. In particular, Shor's algorithm compromises the ECDSA trust anchor and Grover's algorithm reduces the effective security of symmetric schemes unless key sizes are substantially increased. This implies that the future GNSS authentication protocols must adopt quantum-resistant cryptography that balances security with the severe bandwidth and latency constraints of satellite navigation signals. Recent studies indicate that lattice-based, hash-based signature schemes or hybrid models; combining TESLA with post-quantum key distribution mechanisms, may provide an achievable option while maintaining acceptable time-to-first-fix and message overheads [43]. Further research has to consider the need for quantum resistance with the strict time and spectrum constraints intrinsic to satellite navigation systems.

5.2 AI-enhanced GNSS security solutions

The development of sophisticated jamming and spoofing attacks requires a shift from traditional rule-based detection systems to machine learning-based solutions [6,38, 39]. Deep learning models including convolutional neural networks (CNNs), recurrent neural networks (RNNs) and transformers show high effectiveness in distinguishing authentic GNSS signals from spoofed signals through detailed analysis of correlator output patterns, carrier-to-noise ratios, Doppler residuals and time-frequency signatures [6, 38, 44]. The AI-based detection methods show better performance than statistical methods by achieving detection success rates exceeding 95% in laboratory tests [45]. The implementation of these neural models proves beneficial for unmanned aerial vehicle (UAV) navigation and connected vehicle systems because they operate on embedded hardware to detect spoofing attacks in real-time [46]. The primary challenges for deploying AI-based GNSS defences in safety-critical aviation and maritime environments involve protecting against adversarial machine learning attacks and creating standardised testing datasets and certification frameworks.

5.3 Space-based GNSS cybersecurity policy and regulations

GNSS security depends on more than technical countermeasures because policy and regulatory frameworks have become equally important. The European Union Aviation Safety Agency (EASA) work together with the International Air Transport Association (IATA) developed coordinated mitigation plans for 2024-2025 to address increasing GNSS jamming and spoofing incidents which require standardised reporting methods and operational flight procedures and receiver performance requirements [47, 48]. The United States has established minimum security requirements for PNT-dependent systems through National Institute of Standards and Technology (NIST)'s PNT Cybersecurity Profile [49] and Cybersecurity and Infrastructure Security (CISA) Resilient PNT Conformance Framework [50] which focus on equipment design security and operational system resilience.

National and supranational policies now align at the strategic level because the European Union (EU) Space Strategy for Security and Defence (2023) and the proposed EU Space Act (2025) enforce enhanced cyber-resilience requirements for space operators while the United States Space Policy Directive-5 established essential cybersecurity principles for space systems that link to post-quantum cryptography while they request states to track and report and enforce regulations against intentional disruptions. The international community currently uses standardised transition plans. The United Nations (UN) International Committee on Global Navigation Satellite Systems (ICG) and the International Civil Aviation Organisation (ICAO) consider GNSS interference a security hazard, instituting cybersecurity regulations for space assets and GNSS systems through international agreements that combine technological innovation with institutional and legal safeguards.

6. Conclusion

As increasing numbers of industries rely on GNSS, while jamming and spoofing attacks become easier to carry out and more advanced, it is clear that space systems require better cybersecurity right away. The evolution of GNSS threats through SDR and AI-based interference methods demands space systems to implement defence systems that combine electronic protection with cybersecurity measures to achieve national security through resilience of the GNSS system. To ensure that GNSS is reliable, resilient and sufficient to support global security, economic activity, and safety-of-life applications, we require a multifaceted approach that includes advanced anti-jamming and anti-spoofing technologies, cryptographic authentication, AI-driven anomaly detection, secure firmware and comprehensive policy frameworks. The future will need constant innovative concepts, especially in quantum-resistant cryptography and powerful AI. Furthermore, international cooperation and rules will need to be improved to boost trust in GNSS-provided position, navigation and timing information.

Acknowledgements

The authors would like to express their heartfelt gratitude to the University of South Australia and University of Technology Sydney for providing library access and all the necessary resources that enabled the successful completion of the paper. The authors would also like to thank A/Prof. Patrick Neumann and William Ferguson for their reading of the manuscript and constructive feedback that substantially improved the clarity of this paper.

Appendix A: Formulas

$$\begin{aligned}\mathrm{FSPL}_{GPS} &= 20\log_{10}(20200) + 20\log_{10}(1575.42) + 32.45\\ &= 20 \times 4.305 + 20 \times 3.197 + 32.45\\ &= 86.10 + 63.94 + 32.45\\ &= 182.49 \text{ dB}\end{aligned} \tag{1}$$

$$\begin{aligned}\mathrm{FSPL}_{QZSS} &= 20\log_{10}(20200) + 20\log_{10}(1278.75) + 32.45\\ &= 20 \times 4.305 + 20 \times 3.107 + 32.45\\ &= 86.10 + 62.14 + 32.45\\ &= 180.69 \text{ dB}\end{aligned} \tag{2}$$

References

[1] Cleo Arya and Australian Department of Defence. Defence strengthens edge against GPS denial, August 2025.

[2] Joseph N. Pelton, Scott Madry, and Sergio Camacho-Lara, editors. *Current and Future GNSS and Their Augmentation Systems*, pages 617–654. Springer New York, New York, NY, 2013.

[3] European GNSS Supervisory Authority. Gnss user technology report. issue 3, 2020. Technical report, European Global Navigation Satellite Systems Agency, 2020.

[4] Duoduo Li, Xuhua Zhou, and Kai Li. Centimeter-level orbit determination of grace-c using igs-rts data. *Remote Sensing*, 15(7), 2023.

[5] Robert Thomas. Russian aggression shows the West's GNSS weakness. *Global Defence Technology*, 1(Issue #137), October 2022. Accessed: 2025-09-01.

[6] Katarina Radoš, Marta Brkić, and Dinko Begušić. Recent advances on jamming and spoofing detection in gnss. *Sensors*, 24(13), 2024.

[7] Stephen Wicker, Mukesh Kothari, and Harish Dhingra. Methods and systems for provisioning a mobile device for secure access to a network, 12 2010. Patent US20100309960 A1.

[8] Yoaz E. Bar-Sever and Kenneth M. Russ. New and Improved Solar Radiation Models for GPS Satellites Based on Flight Data. Technical Report RF-182 / 808

(Task Order Agreement), 80-4193 (Task Plan), Jet Propulsion Laboratory, California Institute of Technology, apr 1997. Final Report prepared for Air Force Materiel Command, Space and Missile Systems Center/CZSF.

[9] Spirent Communications. *Spirent Technical Reference: PosApp, GNSS default power levels*, November 2024. Article ID 000003197.

[10] Ron Mancini. *Op Amps for Everyone, Design Reference*. Texas Instruments, USA, 2nd edition, 2002.

[11] Bandagadde Umesha Sahana, Thomas Kraus, Nikolas Dütsch, Clovis Maia, and Thomas Pany. Navigating the noise: How space receivers could defend against ground-based jamming attacks. *Inside GNSS*, 19(4):44–51, 2024.

[12] Tony Anthony and Mary Kerns. NAVSTAR GPS Space Segment / Navigation User Segment Interfaces. Technical Report IS-GPS-200, Revision N, Space Systems Command (SSC), MilComm and PNT Directorate, United States, August 2022.

[13] Jay R Sklar. Interference mitigation approaches for the global positioning system. *Lincoln laboratory journal*, 14(2):167–179, 2003.

[14] Eberhard Gill, Jade Morton, Penina Axelrad, Dennis M. Akos, Marianna Centrella, and Stefano Speretta. Overview of space-capable global navigation satellite systems receivers: Heritage, status and the trend towards miniaturization. *Sensors*, 23(17), 2023.

[15] J. Rossouw van der Merwe, Xabier Zubizarreta, Ivana Lukčin, Alexander Rügamer, and Wolfgang Felber. Classification of spoofing attack types. In *2018 European Navigation Conference (ENC)*, pages 91–99, 2018.

[16] Mark L. Psiaki and Todd E. Humphreys. GNSS Spoofing and Detection. *Proceedings of the IEEE*, 104(6):1258–1270, 2016.

[17] Long Huang, Zhi cheng Lv, and Fei xue Wang. Spoofing Pattern Research on GNSS Receivers. *Journal of Astronautics*, 33(7):884–890, 2012.

[18] Panagiotis Papadimitratos and Aleksandar Jovanovic. Protection and fundamental vulnerability of gnss. In *2008 IEEE International Workshop on Satellite and Space Communications*, pages 167–171, 2008.

[19] Shaun Waterman. Gps jamming extends to low-earth orbit as pentagon races to bolster constellation. *Air and Space Forces Magazine*, July 2025.

[20] Interpret: China, Center for Strategic and International Studies. Starlink militarization and its impact on global strategic stability. 2024. English translation. Accessed September 2025.

[21] Secure World Foundation. 2025 global counterspace capabilities report: An open source assessment, 04 2025. Accessed September 9, 2025.

[22] Isabel Manjarrez. Internet-exposed GNSS receivers in 2024. *Kaspersky Securelist*, Nov 13 2024.

[23] Adrien Perkins, Yu-Hsuan Chen, Sherman Lo, Chiawei Lee, and J. David Powell. Real-Time Unmanned Aerial System (UAS) Based Interference Localization in a GNSS Denied Environment. In *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, pages 1003–1019, Miami, Florida, September 2019.

[24] GPSJamming.com. Gps jamming report: June 2024, July 2024. Accessed September 2025.

[25] Al Jazeera. South korea military blames north korea for gps signal jamming attack. November 2024. Accessed September 2025.

[26] RNT Foundation. North korea spoofing aircraft and ships, June 2024. Accessed September 2025.

[27] Clayton Swope, Kari A. Bingen, Makena Young, and Kendra LaFave. Space threat assessment 2025. Report, CSIS Aerospace Security Project, April 2025.

[28] C4ADS. Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria. Technical report, C4ADS, Washington, DC, 2019.

[29] Travis Turgeon, Tjaša Pele, and Antoine Cayphas. Gnss interference report: Russia – part 3 of 4: Moscow and major urban zones. *Spire Global*, 8 2025.

[30] Desmond Schmidt, Kenneth Radke, Seyit Camtepe, Ernest Foo, and Michał Ren. A survey and analysis of the gnss spoofing threat and countermeasures. *ACM Comput. Surv.*, 48(4), May 2016.

[31] Zhijun Wu, Yun Zhang, Yiming Yang, Cheng Liang, and Rusen Liu. Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. *IEEE Access*, 8:165444–165496, 2020.

[32] Lianxiao Meng, Lin Yang, Wu Yang, and Long Zhang. A survey of gnss spoofing and anti-spoofing technology. *Remote Sensing*, 14(19), 2022.

[33] Zhongliang Deng, Zhichao Zhang, Xiangchuan Gao, and Peijia Liu. Differentiated gnss baseband jamming suppression method based on classification decision information. *Applied Sciences*, 15(13), 2025.

[34] Annemarie van Zwol, Jan-Joris van Es, Daniel Kappelle, Hein Zelle, Fennanda Doctor, and Yuri Konter. Interference detection, localization, and mitigation capabilities of controlled reception pattern antenna for aviation. *Engineering Proceedings*, 54(1), 2023.

[35] Adnan Malik and Muzaffar Rao. Radio frequency interference, its mitigation and its implications for the civil aviation industry. *Electronics*, 14(12), 2025.

[36] EU Agency for the Space Programme. Galileo open service navigation message authentication adds another layer of protection against gnss interference. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-OS-SDD_v1.3.pdf, July 2025. Accessed: August 25, 2025.

[37] Francisco Gallardo and Antonio Pérez Yuste. Scer spoofing attacks on the galileo open service and machine learning techniques for end-user protection. *IEEE Access*, 8:85515–85532, 2020.

[38] Arul Elango, Sahar Ujan, and Laura Ruotsalainen. Disruptive gnss signal detection and classification at different power levels using advanced deep-learning approach. In *2022 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–7, 2022.

[39] Adyasha Mohanty and Grace Gao. A survey of machine learning techniques for improving global navigation satellite systems. *EURASIP Journal on Advances in Signal Processing*, 2024(1):73, 2024.

[40] The White House. Memorandum on space policy directive 7 – the united states space-based positioning, navigation, and timing policy. https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-7/, jan 2021. Accessed: August 25, 2025.

[41] Xiao Chen, Ruidan Luo, Ting Liu, Hong Yuan, and Haitao Wu. Satellite navigation signal authentication in gnss: A survey on technology evolution, status, and perspective for bds. *Remote Sensing*, 15(5), 2023.

[42] Ali Pirsiavash, Ali Broumandan, and Sandy Kennedy. Osnma: Necessary but not sufficient for gnss security. *Inside GNSS+*, September 2024. Sept/Oct 2024 issue.

[43] Javier Junquera-Sánchez, Carlos Hernando-Ramiro, Oscar Gamallo-Palomares, and José-Antonio Gómez-Sánchez. Assessment of cryptographic approaches for quantum-resistant galileo osnma. *NAVIGATION: Journal of the Institute of Navigation*, 71(2):navi.648, 2024.

[44] Ali Reda and Tamer Mekkawy. Gnss jamming detection using attention-based mutual information feature selection. *Discover Applied Sciences*, 6(4):163, 2024.

[45] Ben Niu, Xuebin Zhuang, Zijian Lin, and Linjie Zhang. Navigation spoofing interference detection based on transformer model. *Advances in Space Research*, 74(10):5156–5171, 2024.

[46] Ahmad Almadhor, Jamel Baili, Shtwai Alsubai, Abdullah Al Hejaili, Rastislav Kulhanek, and Sidra Abbas. Ctdnn-spoof: compact tiny deep learning architecture for detection and multi-label classification of gps spoofing attacks in small uavs. *Scientific Reports*, 15(1):6656, 2025.

[47] European Union Aviation Safety Agency (EASA). Global navigation satellite system (gnss) outages and alterations leading to communication / navigation / surveillance degradation, safety information bulletin sib 2022-02 r3. Safety Information Bulletin 2022-02 R3, European Union Aviation Safety Agency, July 2024. Revision 3; addresses increasing GNSS jamming and spoofing issues; targeted at CAs, ATM/ANS providers, air operators, manufacturers.

[48] International Air Transport Association (IATA) and European Union Aviation Safety Agency (EASA). Easa and iata publish comprehensive plan to mitigate the risks of gnss interference. Press release, June 2025. Workshop held in Cologne on 22–23 May 2025; plan addresses increased GNSS interference through four key public-safety workstreams: reporting/monitoring, prevention/mitigation, infrastructure/airspace, coordination/preparedness.

[49] Michael Bartock, Suzanne Lightman, Ya-Shian Li-Baboud, James McCarthy, Karen Reczek, Joseph Brule, Karri Meldorf, Doug Northrip, Arthur Scholz, and Theresa Suloway. Foundational pnt profile: Applying the cybersecurity framework for the responsible use of positioning, navigation, and timing (pnt) services. Nist interagency/internal report (nistir) 8323 revision 1, National Institute of Standards and Technology, Gaithersburg, MD, January 2023.

[50] Ernest Wong, Benjamin Salazar, William Jackson, Renee Stevens, Yonas Nebiyeloul-Kifle, Dr. Arthur Scholz, Dr. Patricia Larkoski, Dr. William Young, Dr. Bradley Moran, Brian Callahan, P. Stephan Bedrosian, Dr. Steven W. Lewis, Dr. Sai Kalyanaraman, Helmut Imlau, Lannie Herlihy, Andrew F. Bach, Victor Yodaiken, Dr. Steve Guendert, Leigh Whitcomb, Lee Cosart, Rich Foster, Greg Wolff, Dr. Paul E. Black, Ya-Shian Li-Baboud, Magnus Danielson, Dr. Deepak Maragal, Dr. Cristina Seibert, Dr. Stefania Römisch, Charles Swain, Monty Johnson, John Fischer, David Sohn, Jeff Dagle, Lori Ross O'Neil, Dr. Michael O'Connor, Christina Riley, Dan Rippon, Dr. Francisco Girela Lopez, Dr. Marc Weiss, Mitch Narins, Haroon Muhammad, Jeffery Sanders, Dave Howard, Dr. Hadi Wassaf, Dr. Gerard Offermans, and Tyler Reid. Resilient PNT Conformance Framework. Technical report, Cybersecurity & Infrastructure Security Agency (CISA), May 2022. Version 2.0.