

A Review of GNSS Interference and Mitigation Strategies

Global Navigation Satellite Systems (GNSS)—including GPS, GLONASS, Galileo, and BeiDou—are essential for modern navigation and timing. However, their signals arrive at the Earth's surface extremely weak (around -130 dBm), making them highly susceptible to radio frequency interference. Such interference, whether intentional or unintentional, is increasingly threatening GNSS reliability due to

the widespread use of RF devices and the availability of low-cost jammers. Figure 1 depicts the GPS jamming occurrences over Europe on June 3rd, 2025 [1].

This review outlines the sources and effects of GNSS interference, explores mitigation techniques, and highlights how Controlled Reception Pattern Antennas (CRPAs) enhance receiver resilience.

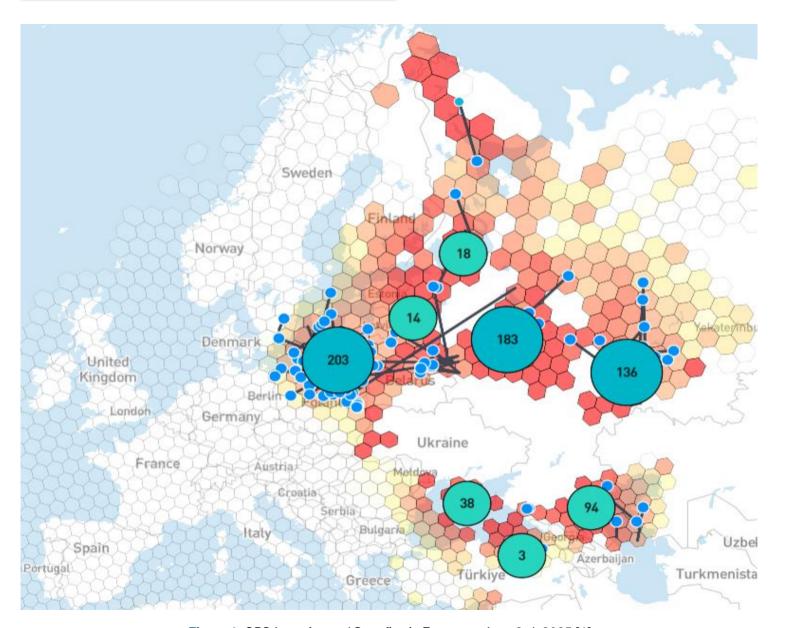


Figure 1. GPS Jamming and Spoofing in Europe on June 3rd, 2025 [1].



1. Nature and Causes of GNSS Interference

GNSS interference can arise from unintentional sources or deliberate attacks [2]. It can also be characterized by its signal properties, such as spectral and temporal behavior. We first classify interference by intent and then by technical characteristics.

1.1. Unintentional Interference

This arises from systems that emit RF energy in the vicinity of GNSS bands, including aviation beacons (DME/TACAN), broadcast transmitters, radars, and UWB devices. Such signals do not target GNSS but can still overwhelm or confuse GNSS receivers if sufficiently robust. For DME/TACAN pulses aeronautical band, which overlap with Galileo E5, have been shown to severely degrade receiver performance if left unmitigated. Unintentional interference can be narrowband (occupying a small frequency range) wideband. Narrowband examples continuous wave carriers or narrow spurious emissions (e.g., a sinusoidal tone or an intermodulation product). At the same time, wideband interference spans a broad frequency range (comparable to or wider than the GNSS signal itself). An ultra-wideband (UWB) transmitter is example of wideband an interference, emitting low-power noise over a large bandwidth. Generally, traditional time- or frequency-domain filtering can effectively mitigate many narrowband interferers. Wideband interference presents greater challenges, often reducing the effectiveness of standard mitigation methods and necessitating additional techniques or spatial antenna strategies to address it.

1.2. Intentional Interference

Intentional threats include jamming, spoofing, and meaconing. Jammers raise the noise floor by using noise, chirps, or continuous wave (CW) signals; spoofers transmit fake GNSS-like signals to mislead receivers; and meaconers

replay genuine signals with a delay. These jammers are readily available on the market as personal privacy devices, showcasing their growing accessibility and importance in safeguarding individual privacy, as illustrated in Figure 2.



Figure 2. On-market GPS Jammers [3].

Jamming has been a significant issue not only for the military but also for civilian sectors. For instance, in 2010, a truck-mounted jammer near Newark Airport disrupted aviation navigation. North Korean jammers interfered with South Korean GPS receivers, and maritime GPS disruptions occurred during UK trials [4]. These attacks can disrupt GNSS tracking or produce false position estimates. CRPA technology is especially effective here, enabling adaptive beamforming and null steering to suppress interference sources directionally. This makes CRPAs a key component in defending critical GNSS applications such as the security of civilian aviation, UAVs, naval platforms, and both civilian and military receivers.

2. Impact of Interference on Applications

GNSS interference can lead to effects ranging from reduced positioning accuracy to total service loss. This section outlines the impact across three key domains: civilian systems (including transportation and critical infrastructure), uncrewed aerial vehicles (UAVs), and maritime/naval platforms.



2.1. Civilian Applications

In civilian contexts, GNSS interference typically causes degraded positioning or timing accuracy. For everyday users, this may result in lost navigation on smartphones or in-car GPS. While inconvenient, the consequences are far more severe in safety-critical systems, such as civil aviation.

A 2022 DLR flight test over the Eastern Mediterranean demonstrated that intentional jamming completely disabled satellite navigation on an Airbus A320, thereby forcing the aircraft to rely on backup systems. If such outages occur during landing or approach, they pose clear safety risks [5]. The GPS faults, which cause Aided Mode operation, as described in [5], are illustrated in Figure 3.



(a



(b)

Figure 3. (a) GPS 1 and GPS 2 faults indicate loss of usable GPS signals on the two independent MMR receivers in the A320 avionics, though the receivers remain operational. (b) When fewer than four satellites are available, the receiver switches to Aided Mode, relying on the inertial platform for navigation [5].

In a recent study of maritime GNSS interference, researchers observed that ports, telecom providers, and emergency services all rely on GNSS, and undetected jamming can lead to cascading failures across these sectors [6]. Beyond aviation, GNSS-based timing underpins key infrastructure—telecom networks, power grids, and emergency services all depend on precise time synchronization. Interference in these sectors can lead to service outages or cascading failures. Even a localized jammer can disrupt operations at ports, airports, communication hubs, underscoring the broad vulnerability of civilian infrastructure to GNSS disruption.

2.2. Uncrewed Aerial Vehicles (UAVs)

UAVs—ranging from commercial drones to military platforms—are highly vulnerable to GNSS interference because they rely on satellite navigation for autonomous flight. In a GNSS-denied environment, a UAV may lose the ability to maintain its course or navigate, notably if it lacks a robust fallback system [7].

Navigation systems are essential for Unmanned platforms and typically combine multiple sensors, such as GNSS receivers and Inertial Navigation Systems (INS), to provide accurate position, velocity, and orientation data. A variety of sensors on a UAV are used to gather diverse navigation inputs, as shown in Figure 4.

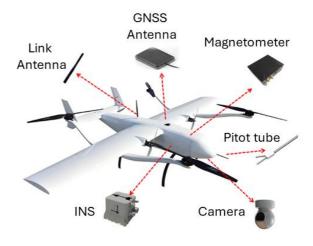


Figure 4. Navigation sensor on a UAV [7].



While small drones used in agriculture, surveying, or delivery often rely solely on GNSS for waypoint tracking and hovering, sudden signal loss can cause instability or crashes if the autopilot cannot compensate for it. Military UAVs operating in contested environments face deliberate jamming aimed at disabling or misleading them, and without robust inertial or visual navigation alternatives, they effectively lose situational awareness. Even with INS, drones experience position drift without GNSS updates, leading to increasing navigational errors over time. Additionally, spoofing attacks that feed false GPS signals can redirect drones into restricted areas or result in their capture and control. Overall, GNSS interference whether from jamming or spoofing—poses serious threats to UAV safety and mission success, underscoring the importance of antijamming technologies, such as CRPAs and integrated backup navigation systems, for both civilian and military applications.

2.3. Maritime and Naval Applications

Modern ships and naval vessels heavily rely on GNSS for navigation, charting, docking, and timing. Interference at sea—whether from coastal jammers, other vessels, or airborne sources—can jeopardize safe operations, especially in congested or hazardous waters. A well-known incident occurred in the Black Sea in 2017 when numerous ships reported GPS anomalies that were later linked to intentional spoofing (See Figure 5) [8].

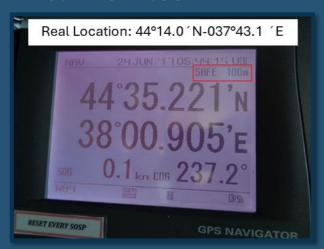


Figure 5. Interference in the Black Sea [8].

Reference [8] reports that near Novorossiysk, Russia, some GPS equipment experienced intermittent signal loss. Although the device showed an HDOP of 0.8 and claimed accuracy within 100 meters, the actual position was off by 25 nautical miles, as documented by the U.S. Coast Guard Navigation Center via the RNT Foundation.

More recently, monitoring in the Baltic Sea revealed over 84 hours of GNSS jamming within six months, with some single events lasting over seven hours [6]. Such an incident has been reported in [9] as given in Figure 6.

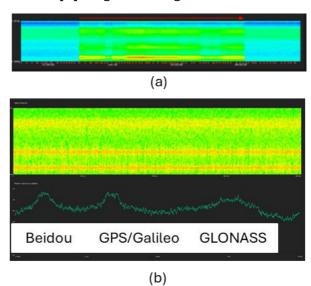


Figure 6. (a) GNSS interference event lasting 7 hours, 43 minutes, and 53 seconds from 22:25:42 CET on June 27 to 06:09:35 CET on June 28. (b) Spectral analysis and jamming structure [9].

These extended outages disrupt not only ship navigation and positioning but also port operations and vessel tracking, which depend on precise GNSS timing. In naval defense, GNSS jamming is a known tactic used to degrade a fleet's situational awareness, weapons synchronization, or fleet coordination. Many jamming signals in recent events have shown signs of frequency-agile, multi-constellation jammers, likely of military-grade.

During prolonged outages, ships must revert to inertial or dead-reckoning methods, which quickly lose accuracy.



These risks underscore the need for robust antijam systems, such as CRPA-equipped GNSS receivers, and resilient Positioning, Navigation, and Timing (PNT) architectures, particularly in defense and high-traffic maritime environments

3. GNSS Interference Mitigation Techniques

A wide range of mitigation techniques has been developed to protect **GNSS** receivers, categorized by their location in the signal chain. Pre-correlation methods processing operate on the raw RF or IF signals before the tracking loops to suppress interference early. At the same time, post-correlation techniques analyze derived data (e.g., pseudoranges, SNR, or position) to detect or reject corrupted measurements. Figure 7 summarizes some interference mitigation methods.

In practice, a layered defense that combines both approaches is most effective [10]. Standard methods include adaptive filtering, blanking, robust tracking loops, multiconstellation support, measurement screening, and RAIM (Receiver Autonomous Integrity Monitoring), each offering complementary protection.

3.1. Pre-Correlation Mitigation Techniques

These techniques attempt to eliminate or attenuate interference at the signal processing level before it can corrupt the GNSS correlation process. By cleaning up the signal early, the GNSS receiver's chances of maintaining lock on satellites are greatly improved even under jamming.

3.1.1. Adaptive Notch Filtering (Frequency-Domain Filtering)

A foundational pre-correlation method is the notch filter, which suppresses power at interference frequencies. While fixed notches can target static tones, Adaptive Notch Filters (ANFs) are crucial for tracking dynamic threats, such as chirp jammers, which sweep across GNSS bands. ANFs utilize frequency-tracking algorithms or frequency-locked loops to track and suppress the jammer in real-time [11].

However, traditional ANFs face trade-offs: they must be fast enough to track frequency changes but stable enough to avoid distorting GNSS signals. If the filter is too slow, it lags the chirp; too fast, and it may attenuate parts of the GNSS band.

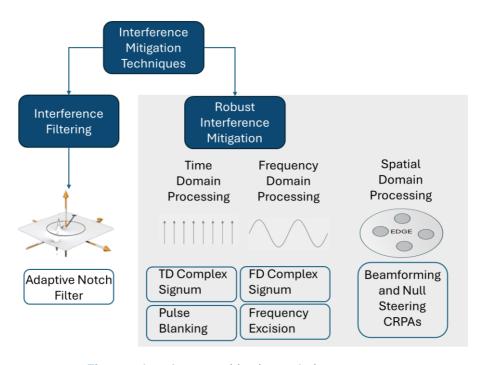


Figure 7. Interference mitigation techniques.



To improve agility and robustness, van der Merwe et al. proposed the Multi-Parameter ANF (MPANF), which adds adaptive controls over notch width, depth, and loop bandwidth [11]. design allows quick adaptation to frequency changes while maintaining precision when the jammer is steady. MPANF outperformed basic ANFs in tests, offering better suppression and faster convergence to interference frequency jumps.

In general, frequency-domain excision works best for narrowband interferers (continuous-wave tones or slowly varying signals). It has been shown that using an adaptive notch or frequency-domain "zeroing" method can tolerate interferers up to ~10-15 dB stronger than the GNSS signal with minimal performance loss [2]. However, designers must be cautious: filtering out part of the GNSS band can distort the correlation of genuine signals. For example, an aggressive notch filter slightly delays GNSS code phases, introducing a bias in pseudorange measurements [12].

Recent findings [12] indicate that although ANFs introduce small biases can pseudoranges due to code delays, these are typically consistent across satellites, making the impact on position negligible. However, the same study showed that the ANF-induced delay modulation-dependent and can affect intersystem biases when the signals have differing spectral characteristics. In contrast, several robust interference mitigation (RIM) techniques, when properly configured, do not introduce measurable biases in clock time series, clock drift, or intersystem timing. RIM approaches have been shown to reduce shortterm clock noise, as quantified by Allan deviation (ADEV), and preserve GNSS timing performance [13].

This suggests that while ANFs are effective for suppressing dynamic interference, their side effects on timing and pseudorange biases must be managed carefully. RIM methods, by contrast, offer a bias-resilient alternative for interference mitigation, particularly in applications where timing integrity is critical.

3.1.2. Time-Domain Pulse Blanking (Temporal Filtering)

Pulse blanking is a time-domain pre-correlation technique that suppresses bursty or pulsed interference [2, 12]. When the input signal's instantaneous power exceeds a set threshold, indicating a strong pulse such as from radar or DME, the receiver briefly "blanks" or zeroes the signal to prevent front-end overload.

Blanking is most effective when the duty cycle of interference is low, as only small portions of the GNSS signal are lost. For example, DME pulses (3.5 μ s long, 12 μ s apart, up to 3000 per second) can be mitigated by momentary blanking windows. In tests on the Galileo E5 band, pulse blanking proved more effective than notch filtering for DME-like interference, while the reverse held for continuous tones [2].

The trade-off is that blanking also removes a proper GNSS signal. If applied too frequently or with a low threshold, it can degrade tracking. Thus, threshold tuning is critical. Adaptive blanking schemes address this by dynamically adjusting thresholds or using interpolation to fill in lost data.

Overall, pulse blanking is a simple yet powerful tool against pulsed interferers, particularly in radar-rich or aviation environments, and complements spectral filtering in a robust GNSS defense strategy.

3.1.3. Kalman Filter-Based Tracking and Aiding

While not a traditional interference filter, Kalman filtering plays a key role in enhancing GNSS robustness under interference. It can be used within tracking loops or as an external estimator to suppress or bypass interference effects.

One application involves using a Kalman filter to track the frequency of a dynamic interferer, such as a chirp jammer. For example, in [14], Kang et al. demonstrated that modeling the chirp frequency as a time-varying state enables real-time frequency estimation, thereby improving notch placement beyond what basic adaptive noise filters (ANFs) can achieve.



More advanced approaches have combined multiple notch filters with Cardinalized Probability Hypothesis Density (CPHD) filters to handle numerous simultaneous jammers, although these require greater computational resources and careful tuning [14, 15].

A more common and practical use is in vector tracking and GNSS/INS integration. Traditional scalar tracking processes each satellite channel independently, which makes it vulnerable when several channels are jammed. Vector tracking, by contrast, uses a Kalman filter to estimate the receiver's position, velocity, and clock bias from all channels collectively. This allows healthy signals to support tracking on jammed ones, improving robustness during partial signal loss.

Further resilience is achieved by integrating inertial measurement units (IMUs) with Global Navigation Satellite Systems (GNSS) using tightly coupled Kalman filters. During GNSS outages, the INS provides an independent motion estimate, allowing the receiver to narrow loop bandwidths or freeze carrier tracking while maintaining navigation accuracy [16]. This "coasting" ability enables GNSS receivers to maintain lock or quickly recover after interference subsides.

Kalman-based architectures, particularly tightly coupled GNSS/INS fusion techniques, have become foundational in modern anti-jamming systems used in aerospace, defense, and highend UAV applications. These architectures enhance robustness by maintaining navigation continuity during GNSS outages and interference events through inertial aiding and dynamic filtering [17,18].

3.2. Post-Correlation Mitigation Techniques

If interference is not completely removed at the signal level, its effects may still show up in the GNSS measurements. Post-correlation techniques focus on identifying and handling compromised measurements or navigation solutions. These fall under measurement domain screening and position domain integrity monitoring.

Additionally, using more satellites and frequencies (when available) is a fundamental strategy to dilute the effect of interference.

3.2.1. Multi-Constellation and Multi-Frequency Utilization

A highly effective passive mitigation strategy is to exploit multi-constellation (GPS, Galileo, GLONASS, BeiDou) and multi-frequency (L1, L5/E5) capabilities. Since interference is often frequency-specific or spatially localized, it may only affect specific signals. For instance, a jammer targeting GPS L1 C/A may leave Galileo E5 or GPS L5 unaffected.

By combining signals from multiple constellations, receivers gain diversity—even if some satellites or bands are jammed, others may remain usable. In [10], Gioia and Borio showed that receivers using GPS, Galileo, and BeiDou together maintained position fixes under jamming conditions that would have disabled single-constellation receivers.

Similarly, multi-frequency receivers can fall back to unjammed bands. If L1 is compromised, L5 or E5 signals may still support navigation, albeit with reduced accuracy due to the absence of ionospheric correction. Since many jammers target the widely used L1 band, dual-frequency support offers resilience in many practical scenarios.

However, sophisticated or wideband jammers may affect multiple bands and constellations. Even then, having access to a broader set of satellites increases the chance of tracking at least a subset of signals. In summary, multiconstellation, multi-frequency processing enhances robustness by providing redundancy, enabling GNSS receivers to maintain service during partial interference events.

3.2.2. Measurement Quality Monitoring

Once GNSS measurements (e.g., pseudorange, carrier phase, C/N_0) are obtained, measurement screening and integrity monitoring can help detect and mitigate interference effects. Common indicators of interference include:



- Drop in C/N_0 across one or more satellites
- Rise in Automatic Gain Control (AGC) levels, indicating a surge in RF power
- Pseudorange residuals or code/phase jumps

Several recent studies have investigated GNSS disruptions caused by radio frequency interference (RFI) [19-24]. Bartl et al. [19] employed a combination of power spectral density (PSD), received power, and carrier-tonoise ratio (C/N_0) to identify and flag events. interference Fors et al.N[21] implemented two detection methods based on received power and average C/No, identifying approximately 50 interference cases across Swedish CORS stations. Gerrard et al. [22] focused on GNSS RFI along Norwegian highways, utilizing automatic gain control (AGC) and C/N_0 as indicators. Similarly, Jada et al. [23] applied C/N_o and its temporal variations to monitor interference events on U.S. highways. Collectively, these studies highlight C/No and AGC as effective metrics for detecting and flagging GNSS interference [25].

3.2.3. Receiver Autonomous Integrity Monitoring

A formal method for measurement validation is the Receiver Autonomous Integrity Monitoring (RAIM) technique. RAIM uses redundant satellite signals to detect and exclude outliers. The receiver compares position solutions using different satellite subsets—if one satellite's data is inconsistent, it's excluded (Fault Detection and Exclusion, or FDE).

RAIM is especially valuable in spoofing or localized jamming scenarios. If one channel is corrupted, RAIM can detect inconsistency and isolate the fault. More advanced variants, like Robust RAIM (RRAIM) and RAIM+INS integration, enhance reliability in high-interference environments.

In the 2023 JRC multi-layer study, combining pre-correlation filtering with RAIM yielded highly reliable position solutions even at high jamming levels [10]. However, RAIM requires sufficient satellite redundancy (5 for detection, six or more for exclusion), reinforcing the value of multi-constellation use.

In summary, RAIM does not suppress interference; instead, it serves as a critical safeguard, ensuring that corrupted measurements are excluded and alerting users when reliability is compromised. A feasibility study conducted in 2024 demonstrated that integrating an INS with RAIM on the airport surface could detect and tolerate interference or multipath events more effectively than RAIM alone [25].

4. The Role of CRPA Technology in Mitigation

While techniques like filtering, blanking, and screening enhance GNSS receiver robustness, single-antenna systems remain limited in the face of sophisticated or powerful jammers. Controlled Reception Pattern Antennas (CRPAs) address this gap through spatial filtering, which utilizes multiple antenna elements to shape the reception pattern and suppress interference dynamically.

A CRPA can place nulls toward jammers and beams toward satellites, offering directional selectivity unmatched by other methods. Since satellites arrive from known sky locations and jammers often sit near the horizon, the system can exploit angle-of-arrival differences to isolate legitimate signals.

4.1. Key Advantages of CRPAs

Spatial signal processing using antenna arrays has demonstrated superior effectiveness in addressing key challenges in GNSS, including suppressing radio frequency interference [26], countering spoofing threats [27], and mitigating errors caused by multipath propagation [28]. The advantages of CRPAs can be listed as follows:

- Multi-Source Suppression: M elements, a CRPA can place up to M-1 independent nulls, enabling the simultaneous mitigation of multiple or broadband interferers, far beyond the capability of spectral or temporal filtering.
- Preserved GNSS Signal Integrity: Spatial nulls reduce jammer power without



cutting into GNSS bandwidth. For example, a two-panel CRPA successfully mitigated a strong jammer without degrading other satellite signals, preserving signal continuity and navigation accuracy.

 Resilience Against Wideband and Adaptive Threats: Unlike notch filters, CRPAs are modulation- and bandwidth-agnostic. They are effective against CW, chirp, pulsed, and spoofing attacks—any signal that arrives from an off-axis direction.

Additionally, advanced array processing techniques, such as Space-Time Adaptive Processing (STAP), enhance the capability of CRPA. STAP combines spatial and temporal filtering to correct for array element separation and handle high-band signals (e.g., L5). For instance, Brachvogel et al. demonstrated robust CRPA jamming protection on vehicles with physically separated subarrays by employing STAP, maintaining effective nulling even under adverse array geometries [29].

4.2 .CRPA in a Multi-Layer Protection Strategy

CRPAs serve as the first and most effective line of defense, attenuating interference at the RF front end. This dramatically eases the burden on subsequent processing layers:

- Pre-correlation techniques (e.g., notch filters, blanking) become more effective or even redundant.
- Post-correlation methods (e.g., RAIM, C/N_o screening) benefit from cleaner measurements and more tracked satellites.
- Multi-constellation receivers retain more signals across all bands since spatial nulling protects them collectively.

A 2023 multi-layer interference study confirmed this strategy: CRPAs increased signal availability under jamming, and RAIM used these signals to ensure solution integrity. Together, they formed a complementary mitigation architecture that was both robust and verifiable.

4.3. Emerging Trends and Strategic Value

Historically confined to military platforms, CRPA technology is becoming more accessible due to advances in:

- Compact arrays for UAVs or automotive platforms,
- · Digital beamforming ASICs,
- Integration with GNSS/INS fusion.

These developments are pushing CRPAs into civil aviation, autonomous vehicles, maritime systems, offering previously unavailable anti-jam protection. For these reasons, CRPAs are indispensable for resilient Positioning, Navigation, and Timing (PNT) in contested radio frequency (RF) environments. They work synergistically with traditional techniques to provide a layered, scalable defense against GNSS interference. interference threats continue to grow, CRPAs stand as the core enabler of robust and secure navigation across civilian, commercial, and defense applications.

To facilitate this transition, our proposed HEDGE 8008 system provides a cost-effective, compact, and highly integrated CRPA package that features low-power digital beamforming, seamless GNSS/INS fusion, and scalable array architecture. HEDGE-8008 is specifically designed to retrofit existing aerial, automotive, and maritime platforms. By minimizing SWaP and manufacturing costs, HEDGE 8008 makes resilient, anti-jam PNT protection viable for commercial and civil applications, promoting widespread adoption of CRPA-enabled navigation in contested RF environments.



CONCLUSION

GNSS interference is a significant and growing threat to navigation and timing across various systems. While techniques like adaptive filtering and signal screening are essential for mitigation, they often fall short in high-power or complex environments. Controlled Reception Pattern Antennas (CRPAs) enhance GNSS receivers by rejecting interference at the antenna level, providing superior performance compared to single-antenna methods. When combined with other strategies, such as multi-constellation tracking and integrity monitoring, CRPAs offer a robust defense against jamming and spoofing. As RF threats evolve, CRPA technology is maintaining essential for secure performance for military and civilian users. Investing in CRPA systems now ensures reliable navigation in increasingly contested electromagnetic environments.

Recent peer-reviewed studies and experimental reports were referenced throughout, including Borio & Gioia on interference biases [12, 13], Gioia & Borio on multi-layer mitigation and RAIM [10], van der Merwe et al. on advanced adaptive notch filtering [11], and Osechas et al. on aviation RFI impacts [5]. Jiang et al. on UAV interference challenges [7], Baltic Sea interference monitoring results [8], and Brachvogel et al. on CRPA/STAP performance [29], among others. These studies underscore the urgency of GNSS interference issues, and the effectiveness of the mitigation techniques discussed.

To learn more, visit www.edgemicrowave.com and follow us on LinkedIn for the latest updates.

FURTHER READING

- [1] SKAI Data Services, "GNSS Spoofing Detection and Monitoring," [Online]. Available: https://spoofing.skai-data-services.com/. [Accessed: Jun. 3, 2025].
- [2] D. A. de Diego, N. G. Ferrara, J. Nurmi, and E. S. Lohan, "Interference Mitigation in the E5a Galileo Band Using an Open-Source Simulator," Inside GNSS, vol. 11, no. 4, pp. 55–60, 2016.
- [3] L. Eldredge, 2010, "Alternative Position, Navigation and Time," briefing to the FACA on Space Based Position, Navigation and Time, October 2010
- [4] National PNT Advisory Board, "White Paper on GPS Jamming," Nov. 2010. [Online]. Available: http://gps.gov/governance/advisory/recommendations/2010-11-jammingwhitepaper.pdf
- [5] O. Osechas, F. Fohlmeister, T. Dautermann, and M. Felux, "Impact of GNSS-band radio interference on operational avionics," NAVIGATION, vol. 69, no. 2, pp. 1–13, 2022.
- [6] M. Barodzka, "GNSS Disruption at Sea Level: An Interference Study in the Baltic Sea," GPS World, Feb. 18, 2025.
- [7] P. Jiang, X. Geng, G. Pan, B. Li, Z. Ning, Y. Guo, and H. Wei, "GNSS Anti-Interference Technologies for Unmanned Systems: A Brief Review," Drones, vol. 9, no. 5, p. 349, 2025. [Online]. Available: https://doi.org/10.3390/drones9050349
- [8] Inside GNSS, "Reports of Mass GPS Spoofing Attack in the Black Sea Strengthen Calls for PNT Backup," Inside GNSS, Jul. 24, 2017.
- [9] GPSPATRON and Gdynia Maritime University, Report on GNSS Interference in the Baltic Sea: Analysis Using a Terrestrial Monitoring System and Comparison with ADS-B Data, Observation period: 02 Jun. 2024 28 Nov. 2024, Doc. revision 2.1, Feb. 11, 2025. GPSPATRON, Poland, Gdynia Maritime University, Poland. [Online]. Available: https://gpspatron.com/gnss-interference-in-the-baltic-sea-a-collaborative-study-by-gpspatron-and-gdynia-maritime-university/
- [10] C. Gioia and D. Borio, "Multi-layered Multi-Constellation Global Navigation Satellite System Interference Mitigation," NAVIGATION: Journal of the Institute of Navigation, vol. 70, no. 4, 2023.
- [11] J. R. van der Merwe, I. Cortés, F. Garzia, A. Rügamer, and W. Felber, "Multi-Parameter Adaptive Notch Filter (MPANF) for Enhanced Interference Mitigation," NAVIGATION: Journal of the Institute of Navigation, vol. 70, no. 2, Art. no. navi.570, Jun. 2023.



[12] D. Borio and C. Gioia, "GNSS Interference Mitigation: A Measurement and Position Domain Assessment," NAVIGATION: Journal of the Institute of Navigation, vol. 68, no. 1, pp. 93–114, 2021.

[13] D. Borio and C. Gioia, "Interference mitigation: impact on GNSS timing," GPS Solutions, vol. 25, no. 37, pp. 1–13, 2021.

[14] C. H. Kang, S. Y. Kim, and C. G. Park, "An adaptive Kalman filtering approach to Fourier analysis for estimating various chirp-type GNSS interference frequencies," NAVIGATION: Journal of the Institute of Navigation, vol. 65, no. 1, pp. 53–68, 2018.

[15] S. Y. Kim, C. H. Kang, and C. G. Park, "Frequency tracking and mitigation method based on CPHD filter and adaptive multiple linear Kalman notch filter for multiple GNSS interference," NAVIGATION: Journal of the Institute of Navigation, vol. 66, no. 4, pp. 803–830, 2019.

[16] P. D. Groves and D. C. Long, "Combating GNSS interference with advanced inertial integration," Journal of Navigation, vol. 58, no. 3, pp. 419–432, 2005.

[17] C. H. Kang, S. Y. Kim, and C. G. Park, "An adaptive Kalman filtering approach to Fourier analysis for estimating various chirp-type GNSS interference frequencies," NAVIGATION: Journal of the Institute of Navigation, vol. 65, no. 1, pp. 3–13, 2018.

[18] P. Dong, J. Cheng, and L. Liu, "A novel anti-jamming technique for INS/GNSS integration based on black box variational inference," Applied Sciences, vol. 11, no. 8, p. 3664, 2021.

[19] S. Bartl, M. Kadletz, P. Berglez, and T. Duša, "Findings from interference monitoring at a European airport," in Proc. 34th Int. Tech. Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), 2021, pp. 3683–3697.

[20] A. Raghuvanshi, S. Bisnath, and J. Bond, "Preliminary analysis of GNSS radio frequency interference events detected in Canada and impacts on GNSS-based applications," in Proc. 36th Int. Tech. Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023), 2023, pp. 4130–4144.

[[21] K. Fors, N. Stenberg, and T. Nilsson, "Using the Swedish CORS network SWEPOS for GNSS interference detection," in Proc. 34th Int. Tech. Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), 2021, pp. 4323–4333.

22] N. Gerrard, A. Rødningsby, A. Morrison, N. Sokolova, and C. Rost, "GNSS RFI monitoring and classification on Norwegian highways—An authority perspective," in Proc. 34th Int. Tech. Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), 2021, pp. 864–878.

[23] S. Jada, J. Bowman, M. Psiaki, C. Fan, and M. Joerger, "Time-frequency analysis of GNSS jamming events detected on U.S. highways," in Proc. 35th Int. Tech. Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022), 2022, pp. 933–946.

[24] F. Bastide, D. Akos, C. Macabiau, and B. Roturier, "Automatic gain control (AGC) as an interference assessment tool," in Proc. 16th Int. Tech. Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003), 2003.

[25] J. Song, C. Milner, and H. No, "Feasibility study of GBAS/INS and RRAIM for airport surface movement under low-visibility conditions," NAVIGATION: Journal of the Institute of Navigation, vol. 71, no. 4, Art. no. navi.673, 2024.

[26] S. Pullen and G. Gao, "GNSS jamming in the name of

privacy," Inside GNSS, Mar./Apr. 2012. [Online]. Available: https://insidegnss.com/gnss-jamming-in-the-name-of-privacy/ [27] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in Proc. 21st Int. Tech. Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, 2008, pp. 2314-

[28] S. Zorn, B. Saadi, M. Niestroj, M. Brachvogel, and M. Meurer, "Accurate position and attitude determination in a multipath environment using an uncalibrated multi-antenna system," in Proc. 31st Int. Tech. Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018), Miami, FL, 2018, pp. 4027–4039.

[29] M. Brachvogel, M. Niestroj, M. Meurer, S. N. Hasnain, R. Stephan, and M. A. Hein, "Space-Time Adaptive Processing as a Solution for Mitigating Interference Using Spatially-Distributed Antenna Arrays," NAVIGATION, vol. 70, no. 3, pp. 1–17, 2023.