

GNSS Spoofing: an increasing threat – how to detect, test and mitigate

Karen von Hünerbein¹,

¹ Lange-Electronic GmbH, Rudolf-Diesel-Str. 29A, 82216 Gernlinden, Germany
kvh@lange-electronic.com

Abstract

GPS/GNSS (GPS is Global Positioning System) is a widely used technology in all areas of navigation and timing, enabling a great variety of applications. As the GPS/GNSS signals are very weak they are easy to jam and can be faked. Faking is called spoofing, and has become increasingly easier with the advent of Software Defined Radios (SDR), which can generate many different types of RF signals, including false GPS/GNSS signals. Jamming and spoofing attacks have increased over time, especially in the context of recent military conflicts. Most receivers are not protected against jamming and spoofing attacks. But for many applications, especially safety of life ones, it is crucial to ensure secure operation, good accuracy and high integrity. In this paper we will show recent examples of real life spoofing events, and describe a method to detect spoofing with a professional GNSS interference detection and monitoring system. We will also present means of testing GNSS receivers and navigation systems spoofing enabling repeatable, controlled and extensive testing. The most efficient test method is dedicated and sophisticated GNSS test equipment: e.g. GPS/GNSS RF simulators with embedded Jamming and Spoofing signal generation. We would like to present an example of a sophisticated RF signal generator and its functionality. Lastly, we would like to show one way of mitigating the issue of spoofing with advanced CRPA antennas.

Key words: GPS/GNSS Spoofing, CRPA antennas, detection, controlled testing, RF simulation

Introduction

GNSS (Global Navigation Satellite Systems) is a widely used technology in all areas of PNT: positioning, navigation and timing, enabling a great variety of applications, both civilian, and military, for transportation, control instruments, sensors, synchronization of power grids and base stations in communication and television/broadcast and timing. As the GPS/GNSS signals are very weak, even below the thermal noise floor, they are easy to jam and can be faked. Faking is called spoofing, with signals almost identical to real GPS/GNSS signals, but containing wrong and misleading information, so that the user will obtain a false position, velocity or time, if relying on the spoofed signals. Spoofing used to be rare and has become increasingly easier with the advent of Software defined radios (SDRs) which can generate many different types of RF signals, including false GPS/GNSS signals. Jamming and spoofing attacks have increased over time, especially in the context of recent military conflicts. Most receivers are not protected against jamming and spoofing attacks. For many applications, especially safety of life ones like aviation and

autonomous driving it is crucial to ensure secure operation, good or high accuracy and a high integrity. [1,2,3,4,7]

Impacts of Spoofing on Aviation have been described in detail by the GPS Spoofing Working Group in their report published in September 2024: "GPS spoofing began to severely impact civil aviation in September 2023. While GPS interference is not a new phenomenon, the scale and effects of the current wave of spoofing are unprecedented. In the first few months, relatively few aircraft were affected, but in January 2024, an average of 300 flights a day were being spoofed. By August 2024, this had grown to around 1500 flights per day. Most recently, for the one-month period from July 15 – August 15, 2024, a total of 41,000 flights experienced spoofing." [3]. Flight Data Exchange has also reported a massive rise in GNSS Interference incidents, with more than 580.000 flights losing their GPS signal over the last 3 years.

"Overall, the Workgroup assessed that the impact of GPS Spoofing on flight safety, aircraft operation and handling, and ATC operations, is extremely significant." [citation from 3]

"The workgroup is very concerned about the overall impact of GPS Spoofing on flight safety. A total of 8 overall safety concerns, and a further 33 specific concerns were raised, including: Aircraft operation and handling (11 concerns), EGPWS (8 concerns), Procedures and training (4 concerns), Human factors and CRM (6 concerns), Air Traffic Control (4 concerns)." [3]

"Warning System (GPWS). The system does not operate correctly after spoofing, even if GPS coverage is restored. The number of false alerts is astounding. There is an increasing normalization of risk. As a result, there was widespread apprehension in the Workgroup that the decades-long work to reduce Controlled Flight Into Terrain (CFIT) accidents is at great risk of being undone." [citation from 3]

"A similar concern is the significant possibility of the GPS Receiver appearing normal to flight crew after spoofing, but in reality being contaminated with false data. This places doubt on the use of GPS at any point after spoofing, especially RNP approaches, and RNP enroute use." [3]

"This year" [2024], "a 500% increase in spoofing has been observed. On average 1500 flights per day are now spoofed, versus 300 in Q1/Q2 of 2024. This is coincident with the summer months in spoofing affected areas. With winter approaching, the operating environment changes from predominantly good weather and VMC conditions, to poor weather, icing, and IMC conditions. This change will increase the risk factors significantly." [citation from 3]

Improving receivers' performance under spoofing attacks can be achieved with mitigation methods and extensive testing. In order to test efficiently and within a reasonable amount of time, there is a need to use simulation tools in the laboratory, such as GPS/GNSS RF (Radio Frequency) simulators.

There are many different mitigation methods, in this paper we would like to present one of them, a Controlled Reception Pattern Antenna (CRPA) based approach, developed by DLR (Deutsche Luft- und Raumfahrt).

In addition, we would like to presents methods and systems for spoofing detection and testing tools and functionality.

Examples of Real-Life Spoofing

Spoofing used to be a rare event, because it was expensive and difficult to carry out [14]. This has changed in the last few years, as cheap SDR (Software Defined Radios) and open source code have become available [14, 15]. In 2017, a

massive interference and spoofing event was observed by more than 1300 commercial ships in the Black Sea. [13, 14] The affected ships often had their position shifted by as much as 20 nautical miles, sometimes even to positions on land. The positions corresponded to location of an Airport. All affected ships were reporting same false position at airport. Some ships found position solutions "jumping around between real and fake location" [15, 17]. In 2019, a special phenomenon was observed in ships near Shanghai, where positions were spoofed in mysterious ways to form rings on nearby river banks [14]. Circle spoofing has also been observed in other parts of the world. As the GPS Spoofing Working Group and the RIN have described: Spoofing Events have multiplied in recent years, especially with the military conflicts in Europe and the Middle East. [3,4]



Fig. 1. Graph of spoofed trajectory in the water (yellow) and true trajectory (orange) along a coastal road. Source SBG Newsletter May 2026

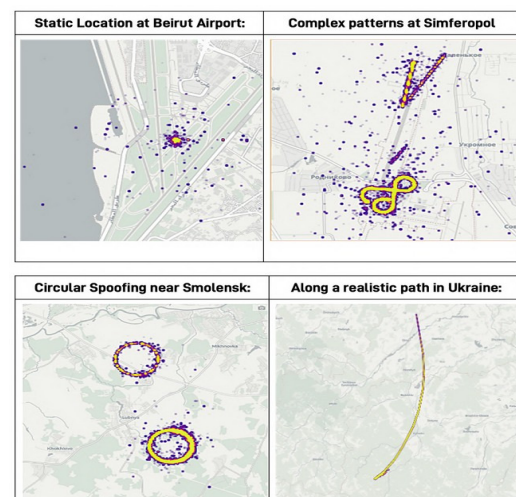


Fig. 2. Spoofing Examples from Ukraine War published by the 2024 GPS Spoofing Workgroup

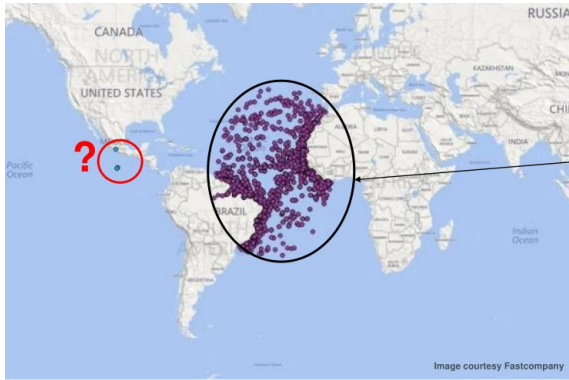


Fig. 3. AIS Spoofing: satellite footprint in black, spoofed positions inside red circle on the left side [14, 17]

GIDAS Monitoring the signal environment

The interference and spoofing monitoring system, which we would like to present in this paper is the GIDAS System: GNSS Interference Detection and Analysis System by OHB Austria in Austria [2,5]. This system is based on a set of algorithms and has been implemented in three different versions:

- as a stationary system, which can be useful for permanent monitoring in industrial areas and harbours, or other critical infrastructure
- as a portable system in a suitcase for field testing in various locations
- as an embedded system, where the software detector algorithms are integrated into GPS/GNSS receivers or other third party electronic systems.

The algorithms use a set of different detector parameters, which are combined and weighted to allow a secure and clear detection of both spoofing and jamming. [2]

The detector parameters are:

1. Power Spectral Density Detector
2. Received Power Detector
3. Carrier to Noise Ratio
4. Pseudorange
5. Correlation Peak Detector
6. Clock Detector
7. Position solution
8. Spatial Correlation
9. Doppler Shift detector
10. RAIM / ARAIM detector
11. PVT detector

“The **power spectral density (PSD)** of the signal describes the power present in the signal as a function of frequency, per unit frequency.” [8]. In GIDAS, it is possible to define different thresholds to optimize the interference detection to the jamming types relevant to the use, e.g. narrow-band thresholds, wide-band thresholds or the ICAO mask (for civil aviation), see figure 7 for an example. [7]

The **received power detector** measures the absolute received signal power within the monitored frequency band. In case of interference, the received power is usually significantly stronger and thus overwhelms the GPS/GNSS receiver frontend.

Carrier to noise ratio (C/No), is the signal to noise ratio. In case of interference, a strong drop of the carrier to noise ratio is observed, while in case of spoofing there usually is an increase in C/No, because the fake signals add to the signal strength of the original GPS/GNSS signals. Also the spoofer can try to take over the receiver tracking loops by transmitting the fake signals with a slightly increased signal strength.

The **Pseudorange Detector** evaluates the variations of standard deviations of pseudorange Measurements from GPS/GNSS satellites, which tend to be quite stable, in an interference free situation [9] and tend to fluctuate a lot, when interference is present. In case of position spoofing, the pseudorange values will move away from the real, expected pseudorange observables, which can be calculated from the almanac. Thus a comparison between the measured and the expected pseudorange values can reveal the presence of a spoofer [9], when the deviations exceed a certain threshold.

Doppler shift is high with signals from real satellites, as they orbit the Earth with a high speed, and tends to be much lower or even zero when spoofing signals are transmitted by ground stations and ground vehicles. However, RF simulators are capable of generating signals with realistic Doppler shift, if they know the positions of the satellite and the victim receiver and the velocity of the victim receiver. Even if the spoofer generates realistic Doppler shift, it is usually not perfect and slight differences can be detected. Eventually the spoofer will pull the fake GNSS signals away from the truth ones, in order to convey a fake position, and then the Doppler shift will deviate from the respective values of the truth signals. This difference can be detected and used to identify spoofing. [9]

The PVT Detector indicates spoofing, when the Position deviates significantly from a reference position, which is known in case of a static application, and which needs to be measured by a reference navigation system in case of a moving application. In case of a static application also the velocity should be zero, and in case of a moving application the velocity of the vehicle is known to the user, so it can be compared to the GPS/GNSS PVT fix. With advanced statistical analysis also interference and jamming can be detected. [9]

A combination of these six parameters PSD, C/No, overall received power and Pseudo Range, Doppler Detector and PVT Detector are used to detect interference in GIDAS. The combination of many different parameters is advantageous for a low false alarm rate. When the interference is strong there will also be a failure of the receiver to fix a position solution. This results in a denial of GPS/GNSS service. Sometimes the receiver carries on providing position outputs to the user, however, in the presence of medium strength interference, these position fixes can become inaccurate and unreliable.

“The **clock-based spoofing detector** operates on the assumption of non-perfect synchronization of the spoofed signals with respect to their authentic counterparts. A GNSS receiver continually estimates its own clock bias relative to the system time within the PVT solution. After receiver initialization, large jumps in the estimated clock bias are typically not expected due to the clock steering algorithm. In case of spoofing takeover, however, such a jump is expected (it is the combined effect of non-perfect time synchronization of the spoofer and non-perfect spoofer as well as victim receiver position estimation)” [2,7]

Correlation Peak Detector: In case of spoofing there are two correlation peaks for each satellite signal: the true signals are still present and in addition there is a fake spoofing signal for each satellite. Thus a determination of the amount of correlation peaks for each satellite is a good indication of the presence of a Spoofer.

Spatial Correlation Detector: Even if the spoofer transmits fake GNSS signals with perfectly realistic Doppler values, there are anomalies compared to the real signals' Doppler values, as soon as the victim GNSS receiver moves. When it moves all Doppler values will change: a) differently with relation to the real GNSS satellite signals, and the same with relation to the spoofer signals. This difference can be exploited to detect spoofing. [9]

RAIM / ARAIM Detector: The spoofer usually tries to spoof all visible GNSS satellite signals in the victim's view. [9] But in some cases the receiver tracks and uses a mix of spoofed and truth signals. In such a case a RAIM (receiver autonomous integrity monitoring) or ARAIM (advanced RAIM) algorithm can detect anomalies and outliers as an indication for spoofing. [9]

In summary a weighted combination of several detectors is used to detect spoofing: Doppler Shift, Clock, A/RAIM, Pseudorange, Spatial Correlation, PVT and Correlation Peak Detector.

The **number of tracked satellites** shows whether the GPS/GNSS receiver has enough satellites in view to be able to calculate a PVT solution: position, velocity and timing. A GPS receiver needs at least four satellites to do so. If the number of tracked satellites is low, there can be various reasons. Lack of sufficient amount of satellites can be caused by interference, or it can also be caused by high structures obscuring satellite view. Lack of sufficient number of satellites is thus a reason for alert and countermeasures, even if no spoofing or jamming is detected.

Overall Functionality of the GIDAS System

The GIDAS system uses the above mentioned detector algorithms and provides a real-time 24/7 monitoring of jamming and spoofing signals for all GNSS systems on L1, and for GPS on L1,L2,L5, Galileo E1, E5a, E5b and E6, GLONASS L1 and L2, Beidou B1, SBAS on L1: EGNOS, WAAS, GAGAN, MSAS on L1 with a maximum bandwidth of 81 MHz. The events are classified and saved for later analysis. They are also listed in the GUI and stored in a database with time of occurrence and duration. The direction of arrival of the interference systems can be determined, with an antenna with two or more antenna elements. The GIDAS system is hardware agnostic, thus different antennas can be attached. Users are alerted via E-Mail or via a custom alert interface. Information can be viewed remotely via a web-based graphical user interface. The graphical user interface displays a map and detailed information about the interference events, all detector parameters are displayed. “Since GIDAS automatically captures and stores raw baseband signal snapshots for every interference event, it is even possible to gather more detailed insights on the jamming signals by post processing analyses.” [7]

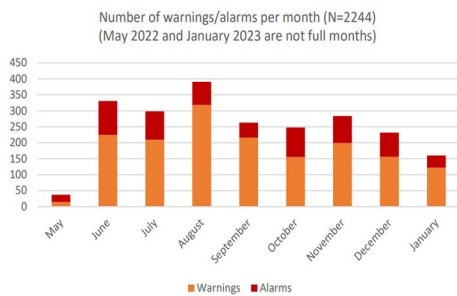


Fig. 4. Number of warnings alarms per month

Longterm results of a fully operational stationary GIDAS system with three monitoring stations at 3 locations around an airport are described in a whitepaper from 2023 [7]: “Since May 2022 we operate a permanent GIDAS installation at a European airport, together with the local air navigation service provider. The goal of the commonly operated GNSS quality assurance system is to gather data-based evidence for future decision-making and strategy definition on how to handle GNSS interference, inflicting air traffic surrounding the airport premises. The first eight months of operation show, that especially along motorways and construction sites, the quantity of interference signals in the restricted GNSS bands is even higher than expected. Between the 17th of May 2022 and the 18th of January 2023 (246 days of operation), the system detected 630 interference events with a severity classified as an alarm (which means that there was an actual degradation of the GNSS measurement quality). During this period an additional number of 1614 interference events with a severity classified as a warning has been captured.” [7]

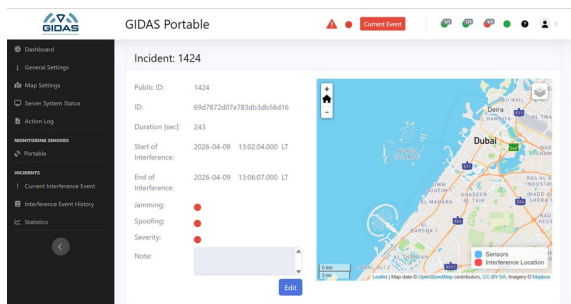


Fig. 5. A severe recorded interference event on the L1 frequency, both Jamming and spoofing in April 2026, courtesy OHB-Austria

In their results they found that interference events occur on a daily basis, especially along motor ways and that a significant amount of such events correlate with daily rush hours and working hours. [7]

Recently measured real Spoofing Events

Since the beginning of wars in eastern Europe and the Middle East there has been an dramatic rise both in Jamming and in Spoofing Events.[4]. Poland has been heavily affected by GNSS jamming and spoofing in the last few years, since it has 3 borders with countries involved in the Russian-Ukrainian war. Since January 2025 more than 3000 interferences have been detected and multiple spoofing events observed on most days (e.g. 9th and 20th April 2026), see figure 9.

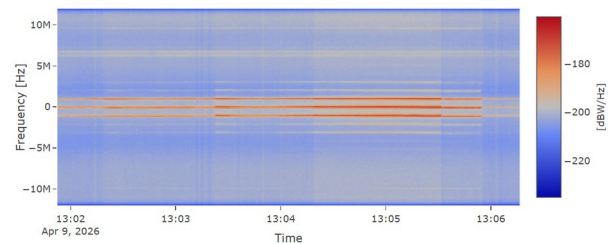


Fig. 6. Waterfall Diagram of the Spoofing Event, red stripes on the GPS CF and near the CF are caused by the fake signal, courtesy OHB Austria

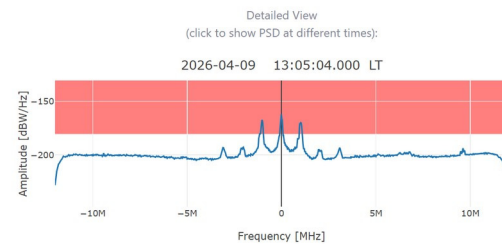


Fig. 7. Power Spectral Density of the Spoofing Event in Figure 5, with high power peaks on the GNSS Center frequency, courtesy OHB Austria,

Another example of a spoofing event in April 2026 can be seen in figures 5-7. This events is seen as a red alert on the map page of the GIDAS GUI and clearly visible in both the waterfall diagram in figure 6 and the power spectral density in figure 7. In figure 7 the peaks of the spoofing signals are prominently visible both on the Center frequency (CF) of the GNSS signal and to the left and right with a higher power than the truth signal to trick the receiver into accepting the false signals.

Effects of Monitoring

Even though monitoring does not eliminate unintentional interference, jamming or spoofing, it increases situational awareness and provides alerts. Alerted operators can pass this information on to all human users, pilots and automated vehicles allow them to switch over to other sensors, such as inertial sensors and to

disregard the GPS/GNSS information for a certain period of time.

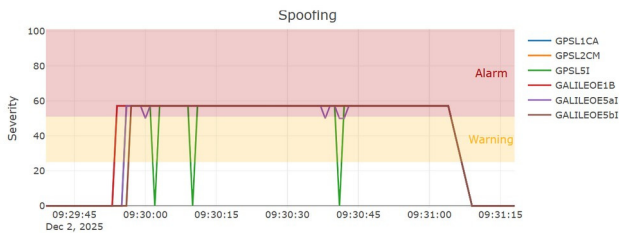


Fig. 8. Spoofing event in Dec 2025 detected by GIDAS -- affected GNSS frequency: E5 and L5

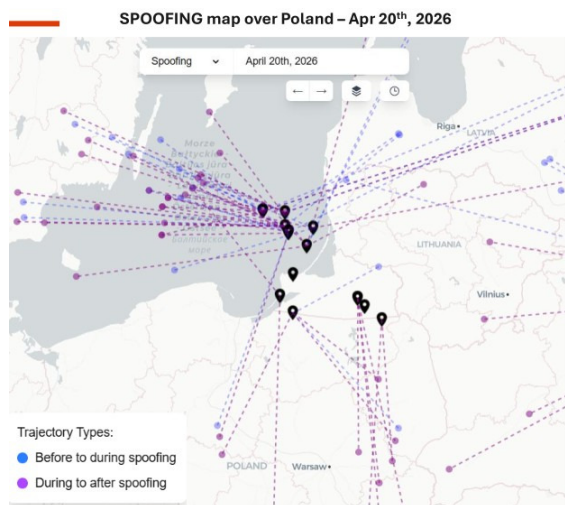


Fig. 9. Spoofing map over Poland. Source <https://rfi.stanford.edu>

In addition operators can decide to stop the automated vehicles and freeze their position, while the GPS/GNSS outage lasts, which can help to prevent accidents, due to false PNT solutions and thus save loss of material and damage. Other countermeasures can be a hand over to remote control steering of the automated vehicle. Since GIDAS also allows to localize interference sources, it is possible to search for them and to remove the interference transmitters. This contributes to overall smoothness of operation and thus better sustainability.

Testing to Improve Resilience

“In order to protect safety critical infrastructure and all sorts of vehicle traffic on land, in the air and at sea, GPS GNSS receivers and navigation systems, need to be hardened and improved, to detect and mitigate spoofing and to resort to other position and Timing sources, when under attack.” [1] “Different detection methods of spoofing can be tested in the laboratory, with the help of GPS/GNSS signal generators. Controlled and repeated tests allow to assess the behavior

of the receivers, and to check different algorithms

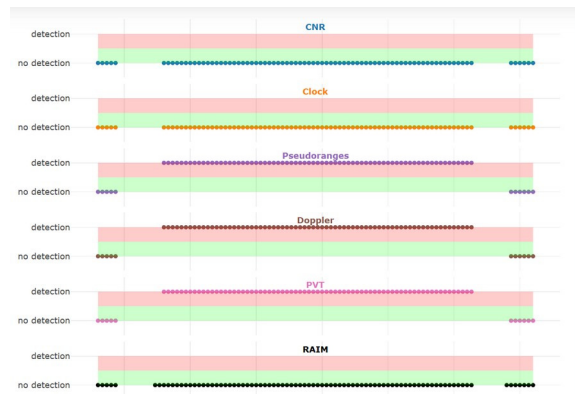


Fig. 10. Spoofing event in Dec 2025 detected by GIDAS: several detectors show an alert, (but not all of them), courtesy OHB-Austria

and mitigation methods in order to achieve a more robust behavior of the GPS/GNSS based navigation solutions, and enhance their ability to detect and mitigate the impact of interference and spoofing signals.” [1]

“Another reason for lab testing is that testing of spoofing attacks outdoor is hardly feasible, except on special test ranges, as it will impair normal operation of other users’ GPS/GNSS equipment. New test functions and test methods for spoofing have been developed recently, for GPS/Galileo RF signal generators capable of simulating all GNSS RF signals and Galileo PRS. For realistic tests with live-sky signals it is important to synchronize the simulated spoofing attack to NTP server time, so that the spoofing signals can be aligned and synchronized with real live sky GPS/GNSS signals, available in the outdoor environment.” [1] The method to achieve this synchronization is the Standpoint Synchronisation Tool.

Here we would like to present the PNT-X by Spirent Communications as an example of a GNSS RF simulator capable of simulating complex spoofing scenarios.[18]



Fig. 11. PNT-X GNSS RF Simulator, source Spirent Communications

The PNT-X is a high end RF simulator generating realistic GNSS (Global navigation Satellite Signals) signals of all GNSS (GPS, Galileo, GLONASS, Beidou) on all GNSS L-band frequencies, SBAS (Satellite Based Augmentation Systems) and regional systems, satellite S-Band signals, and allowing replay of recorded IQ files in the L-band, simulation of jamming and spoofing and LEO navigation signals, including XONA's signals. The aim is to achieve high test coverage and realism. [18]

It can generate up to 640 signals (GNSS/band) on 10 SDR cards, with 1,2 or 10 RF Outputs. There are a lot of different options for spoofing simulation: "... such as meaconing, code/carrier attacks, navigation data attacks, application-level spoofing and multi-method attacks. It can simulate up to 4 independent spoofers in a given scenario, allowing user definition of the following parameters for each spoofer [18]:

- Number of transmitters (up to 64) and their dynamics.
- Power level model.
- False vehicle position (spoofed position).
- Spoofing signal content selection, including navigation data and errors.
- Independent and uncorrelated noise patterns with a fixed 90 MHz (3 dB bandwidth) noise source to simulate the unique wide-band thermal noise of each transmitter 15." [18].

In this way, very complex spoofing scenarios can be programmed and executed, with multiple spoof transmitters, which can move relative to the spoofed vehicle, generating multiple spoof trajectories and multiple constellation copies of any GNSS constellation inside the simulation. The latter allows to modify and falsify navigation data content. Spoofing signals can also be output with a time delay to the actual simulation time, generating a time difference between truth signals and spoof signals, which can shift the time tag inside the receiver, if the receiver accepts the false, spoofed signals for its PNT (position, navigation and timing solution).

Mitigation with CRPA-Guard

In addition to detection and testing there is a strong need for mitigation of interference signals and fake signals during normal operation in the field and on the move, on the ground, at sea and in flight. This can be achieved with many different methods, e.g. CRPA (Controlled Reception pattern antenna) technology based on multi-element antennas in combination with an embedded receiver capable

of active signal processing resulting in spatial signal analysis, null forming of interference signals and beam forming to amplify the true GNSS signals.

CRPA-GUARD is based on this technology consisting of a 4-element CRPA antenna plus a multi-frequency, multi-GNSS receiver, which provides PVT (Position, Velocity and Timing) and comprehensive signal data including DoA Direction of Arrival of the incoming of L1/E1 and L5/E5 signals, both GNSS truth signals and interference. It has been developed by DLR [19,20,21,22], and will now be commercialized by Lange-Electronic. Direction of Arrival in itself is already a strong indicator, whether the signals are true ones or fake ones, since true GNSS signals arrive from different directions across the sky, while fake ones are usually transmitted from 1 or 2 transmitter stations on the ground, thus arriving at the receiver from a low elevation, and only one or two directions.

Null forming is achieved in the pre-correlation stage for all signals combined by the means of covariance matrix and filtering, so that nulls can be formed for a maximum of 3 jammers simultaneously, thereby significantly attenuating their impact on the receiver.

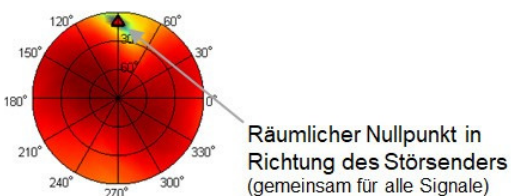


Fig. 12. Null forming, a null is created in the direction of a jammer (for all signals combined) image by DLR

Beam forming takes place in the correlation stage for each satellite signal individually, so that beams are steered towards the expected direction of arrival of GNSS satellites, thus amplifying the desired truth signals from the GPS/GNSS satellites.

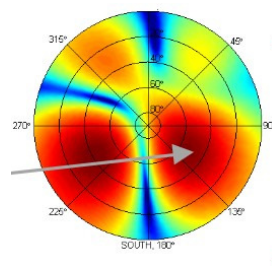


Fig. 13. Beam forming, grey arrow pointing to one beam (for each signal individually) image by DLR

In the case that CRPA-Guard simply replaces the original antenna, the user can use Null Forming only, to eliminate up to three jamming signals. In order to take advantage of the beam forming, various data from the embedded receiver need to be used and feedback in addition to the user's primary receiver.

In contrast to conventional CRPA antennas, the integrated multi-antenna GNSS receiver allows to control the antenna phase center with sophisticated calibration techniques.

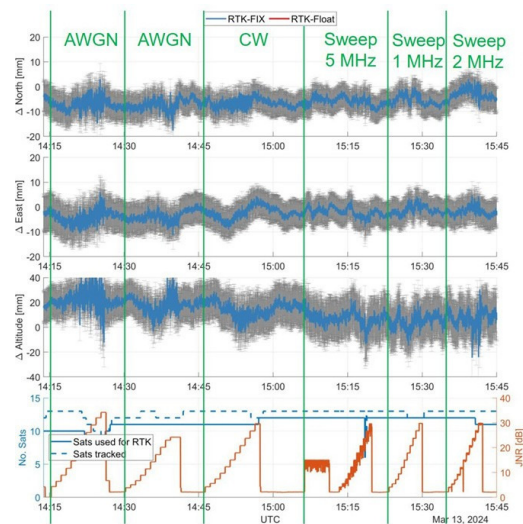


Fig. 14. results of field tests with DLR's prototype predecessor of CRPA-Guard showing position accuracy in the first 3 rows, static test

Operating modes:

CRPA-GUARD can be used to replace an existing antenna, to enable full GNSS reception plus spatial filtering and thus suppression of up to 3 jamming signals – jammer cancellation, and can thus be integrated into existing systems without significant hardware modification or architectural redesign.

References

- [1] K. Hünnerbein, W. Lange. "Efficient testing of Spoofing of GPS/GNSS signals." Conference Proceedings of ETTC 2021, Toulouse, June 2021.
- [2] S. Bartl, M. Kadletz et al. "Mitigating the Threat of Jamming and Spoofing to Aeronautics." Inside GNSS Sep/Oct 2022, vol. 17, no. 5: 46-55.
- [3] Report of the 2024 GPS Spoofing Workgroup
- [4] Royal Institute of Navigation. Impacts of GNSS interference on maritime Safety. A special report by the RIN Maritime GNSS Interference Working Group. January 2026

In standalone mode it provides resilient PNT data with RTK accuracy, which is maintained even in the presence of jamming, and provides output, storage and analysis of all signal observables enabling an in depth interference and spoof signal analysis.

Conclusion:

Spoofing has occurred and been measured in the field and in real flights in the last few years, especially in regions with military conflict. The numbers of events have risen sharply. The GPS Spoofing Working group and the Royal Institute of Navigation from the UK are very concerned about the impact of spoofing on marine and flight safety. [3, 4] In this paper we have presented several real life examples of spoofing and a technical system for mitigation: CRPA-GUARD, based on a CRPA antenna with an integrated multi antenna GNSS receiver, which filters up to 3 Jamming signals by null forming, and also allows beam steering, which will be launched soon. We have also presented another technical system GIDAS for measurement, detection, monitoring, classification, localization and analysis of jamming and spoofing signals. In addition, we introduced one way to develop and test more resilient hardware and software solutions, with the help of RF Signal generators such as PNT-X Multi-GNSS multi-frequency and LEO satellite constellation simulator.

Acknowledgements

I appreciate the support and the possibility to include unpublished data from Sascha Bartl and Benedikt Stingl, from OHB-Austria and to Manuel Cuntz and Stefano Caizzone from DLR and would like to thank them for their support and cooperation.

- [5] K. von Hünnerbein. Detection and Monitoring of Jamming and Spoofing of GPS/GNSS Signals in Harbours and Industrial Areas. In *The European Test and Telemetry Conference* (pp. 11-13) (2024). <https://doi.org/10.5162/ettc2024/a3.2>
- [6] A. Konovaltsev, E.P. Marcos, M. Cuntz, M., Meurer, R. Wong, G. Buesnel, W. Lange. "Development of array receivers with anti-jamming and anti-spoofing capabilities with help of multi-antenna GNSS signal simulators." In *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)* (pp. 953-966). <https://doi.org/10.33012/2019.16988>

- [7] M. Kadletz. "Jamming and Spoofing of Safety Critical Infrastructure." January 2023. Whitepaper by OHB-Digital
- [8] https://en.wikipedia.org/wiki/Spectral_density#Power_spectral_density
- [9] OHB-Austria. Personal communication and proprietary, internal report. Nov 2025
- [10] M. Stanisak, K. Hünnerbein K, U. Bestmann, W. Lange, "Measured GNSS Jamming Events at German Motorways", Proc. of POSNAV ITS, DGON Conference, Berlin, Germany, 5th-6th July, 2016.
- [11] K. Hünnerbein, W. Lange "Real Life Evidence for Spoofing and Jamming of GNSS Receivers", Conf. Proc. of CerGal, DGON Conference, Darmstadt, Germany, 7th-8th July, 2015.
- [12] D. Shephard, J. Bhatti, T. Humphreys, "Drone Hack: Spoofing Attack Demonstration On a Civilian Unmanned Aerial Vehicle", GPS World, Aug 2012, vol. 23, no. 8, pp. 30-33.
- [13] M. Jones, "The Civilian Battlefield", Inside GNSS, March/April 2011, vol. 6, no. 2, pp. 40-49.
- [14] M. Hunter, F. Fillipi, G. Buesnel: "An Assessment of GNSS Receiver Behaviour in Laboratory Conditions When Subject to GPS Meaconing or Spoofing Scenarios," Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), September 2020, pp. 1533-1555. <https://doi.org/10.33012/2020.17735>
- [15] P. Crampton: "Spoofing and Other Threats" March 2021, Online Presentation, Training by Spirent Federal
- [16] Spirent Communication: "Spoofing for Commercial Applications", Presentation, 2020
- [17] G. Buesnel: "Vulnerability and Security in Global Satellite Navigation Systems", In *Proceedings of the European Test and Telemetry Conference 2021*, Toulouse
- [18] Spirent Communications: Datasheet PNT-X. 2025
- [19] M. Cuntz, A. Konovaltsev, & M. Meurer, (2016). Concepts, development, and validation of multiantenna GNSS receivers for resilient navigation. *Proceedings of the IEEE*, 104(6), 1288-1301. <https://doi.org/10.1109/jproc.2016.2525764>
- [20] M. Cuntz, A. Konovaltsev, et al. "Field test: jamming the DLR adaptive antenna receiver." In *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)* (pp. 384-392).
- [21] A. Konovaltsev, M. Cuntz, C. Haettich, M. Meurer, "Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array," *Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, September 2013, pp. 2937-2948.
- [22] A. Konovaltsev, S. Caizzzone, M. Cuntz, M. Meurer, "Autonomous Spoofing Detection and Mitigation with a Miniaturized Adaptive Antenna Array" *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014)*, Tampa, Florida, September 2014, pp. 2853-2861.