Selecting Optimal Anti-Spoofing and Anti-Jamming Techniques for Resilient GNSS

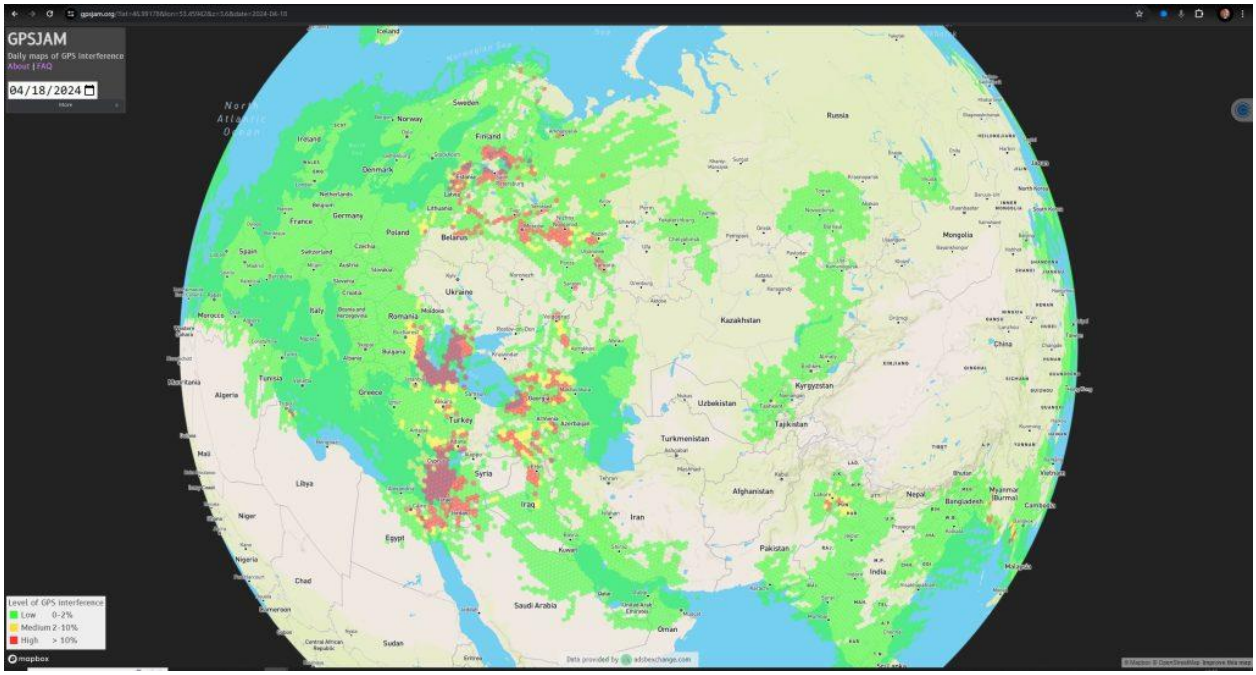
Know your enemy and know yourself, and you will be invincible in a hundred battles – Sun Tzu, The Art of War

For those who don't want to read the whole article:
To develop an optimal GNSS interference mitigation solution, you should analyze the GNSS interference prevalent in your area. You have to know what you're dealing with. Spoofing? Coherent or non-coherent? How long does it usually last, a few minutes or a few days? What constellations are being attacked?
There are a lot of questions and you should know them to choose the optimal countermeasures.

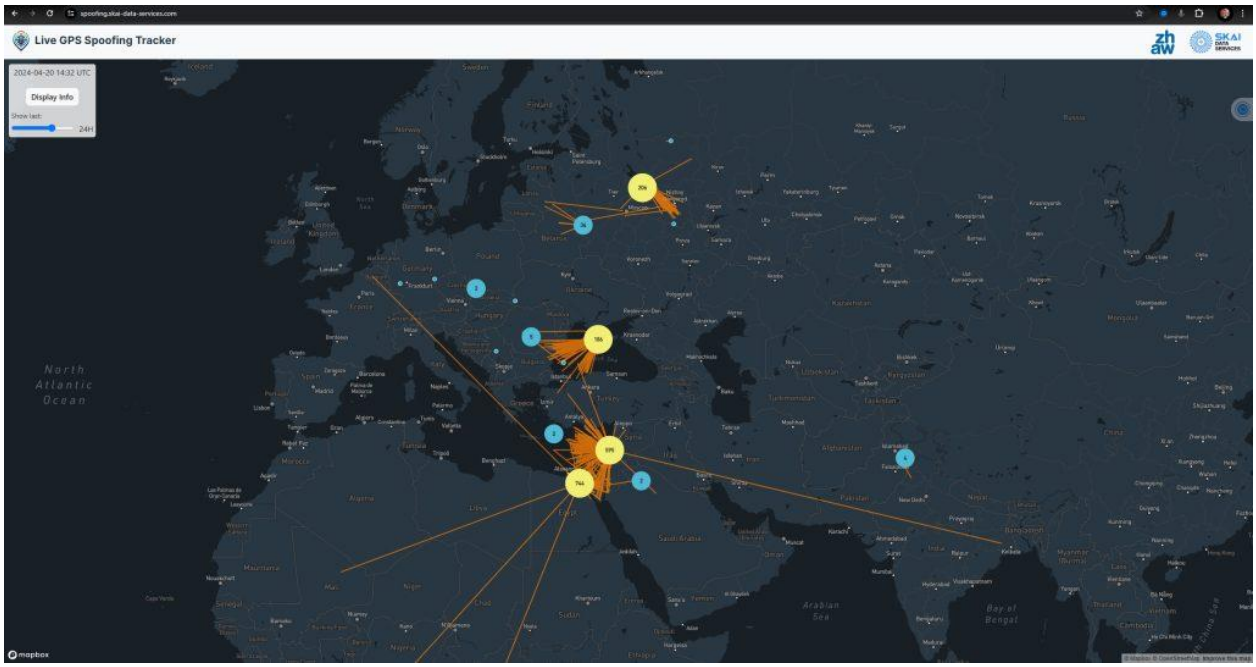
Introduction

The sophistication and frequency of GNSS jamming and spoofing activities have surged, manifesting across a spectrum of scenarios from military operations to the use of Uber drivers.

The following map visualizes GNSS jamming incidents based on ADS-B data from gpsjam.org on April 18:

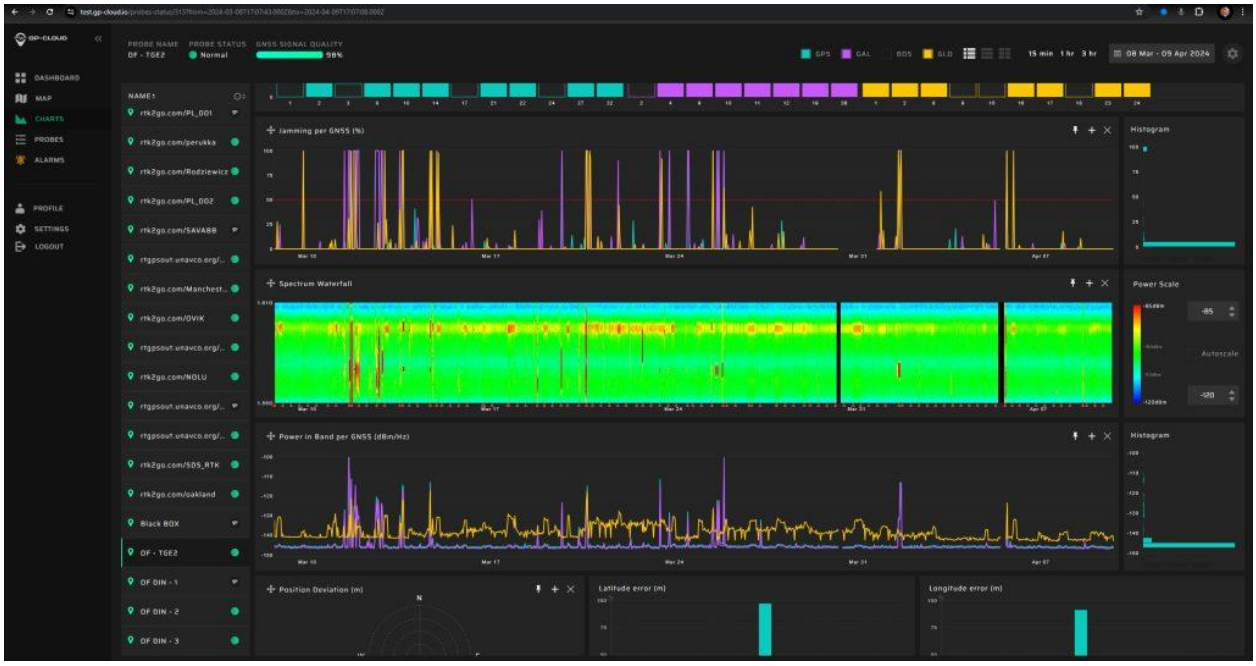


This screenshot shows a map with the number of registered GNSS spoofing cases:



Source: spoofing.skai-data-services.com. April 20, 2024.

As you can see, GNSS interference, with power enough to affect aircraft at an altitude of 10 km, is plentiful. But on the surface, it's even worse. Here is another visual from Warsaw, depicting a month's worth of interference:

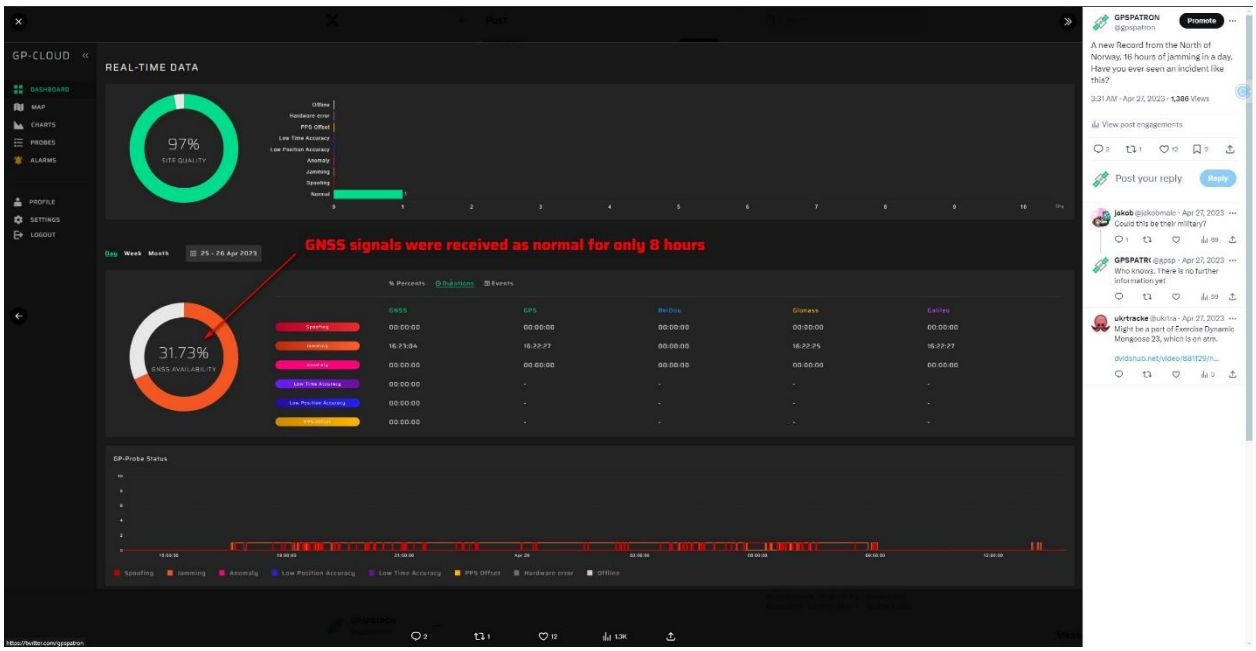


GNSS Spoofing and Jamming Use Cases

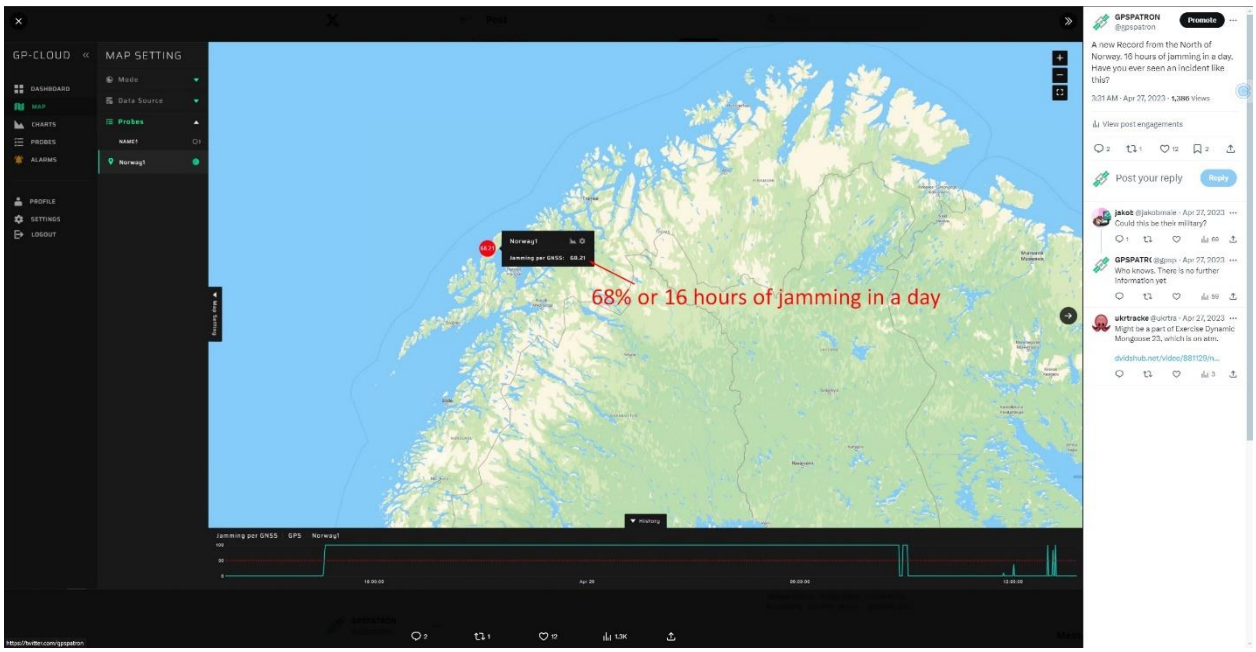
GNSS spoofing is no longer a theoretical problem from scientific papers. We have highlighted the most frequent reasons for use:

1. **Military Use in Conflict Zones**: In regions of military conflict, GNSS spoofing is used to misdirect or neutralize the enemy's navigational capabilities, often integrated into broader electronic warfare strategies. High-powered spoofers cover extensive areas to disrupt enemy UAV operations or mislead navigation systems.
2. **Infrastructure Protection**: Anti-drone systems may employ GNSS spoofing to create no-fly zones or manipulate UAV navigation, preventing unauthorized access or attacks on critical installations. These systems can be activated temporarily during drone detection or operate continuously as a deterrent.
3. **Civilian Misuse on Roads**: Truck and taxi drivers frequently use portable jammers to avoid real-time location tracking by employers or law enforcement, impacting GNSS reliability along major transport routes. This misuse often results in brief but frequent signal disruptions, especially near highways and parking lots.
4. **Maritime Navigation Fraud**: Ships, especially those from nations facing international sanctions, use GNSS spoofing to mask their true locations to enter restricted waters or engage in unauthorized fishing and goods transportation. These operations often involve sophisticated methods to consistently deceive tracking systems over long periods. Learn more about what it's used for: https://www.nytimes.com/interactive/2023/05/30/world/asia/russia-oil-ships-sanctions.html
5. **Evasion of Toll Systems**: In several countries, drivers use GNSS jammers to bypass toll collection systems, causing financial losses to infrastructure and complicating traffic management.
6. **Recreational Cheating**: Enthusiasts of augmented reality games like Pokémon GO manipulate their location data to access geo-specific game features without physically traveling, which can affect the integrity of online community experiences. This article will reveal how many repositories are available on GitHub intended for GPS spoofing: https://gpspatron.com/680-forks-on-github-for-gps-signal-simulation/

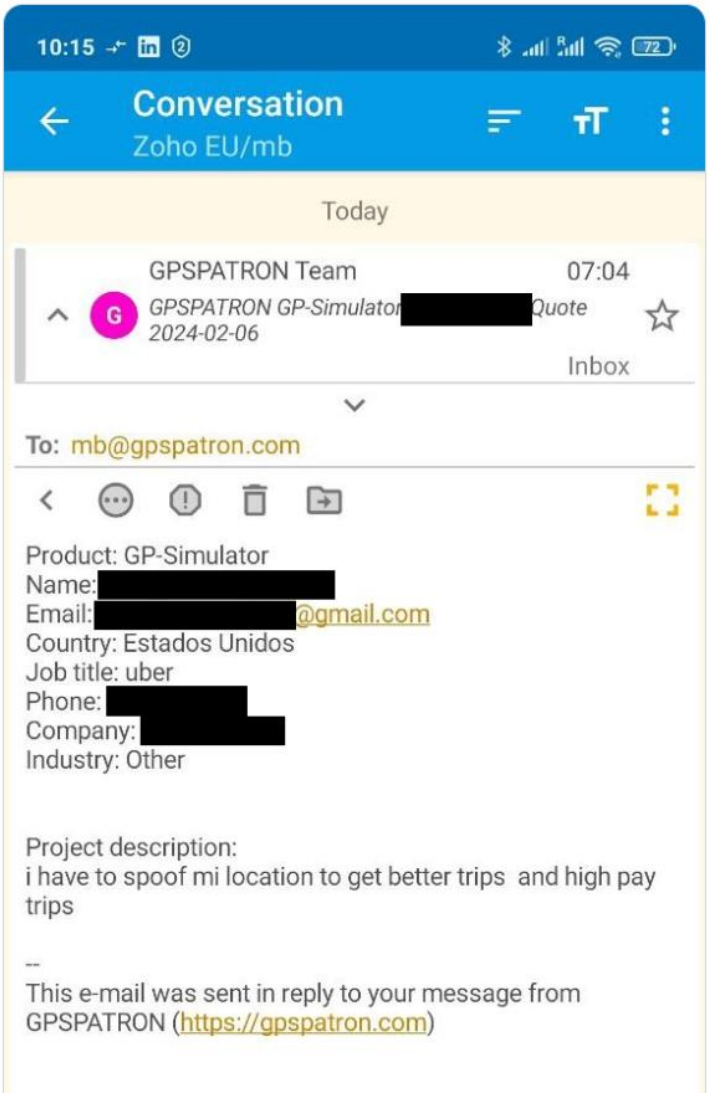
Each scenario reveals different characteristics and impacts, necessitating a strategic approach to GNSS protection tailored to specific threats and operational contexts. In the screenshots below you can see GNSS jamming coming from an unidentified vessel in northern Norway:


GP-CLOUD
DASHBOARD
MAP
CHARTS
PROBES
ALARMS
PROFILE
SETTINGS
LOGOUT
REAL-TIME DATA
97%
SITE QUALITY
Offline
Hardware error
PPS Offset
Low Time Accuracy
Low Position Accuracy
Anomaly
Jamming
Spoofing
Normal
GNSS signals were received as normal for only 8 hours
31.73%
GNSS AVAILABILITY
GP-Probe Status
Spoofing
Jamming
Anomaly
Low Position Accuracy
Low Time Accuracy
PPS Offset
Hardware error
Offline
GPSPATRON
@gpspatron
Promote
A new Record from the North of Norway. 16 hours of jamming in a day. Have you ever seen an incident like this?
3:31 AM · Apr 27, 2023 · 1,386 Views
Post your reply
Reply
jakob @jakobmale · Apr 27, 2023
Could this be their military?
GPSPATR(@gpsp · Apr 23, 2023
Who knows. There is no further information yet
ukrtracke @ukrtra · Apr 27, 2023
Might be a part of Exercise Dynamic Mongoose 23, which is on atm.
dvidshub.net/video/881129/n...


GP-CLOUD
DASHBOARD
MAP
CHARTS
PROBES
ALARMS
PROFILE
SETTINGS
LOGOUT
Number of Satellites per GNSS
Spectrum Waterfall
16 hours
Power in Band per GNSS (dBm/Hz)
Jamming per GNSS (%)
Spoofing per GNSS (%)
Histogram
Power Scale
Autoscale
GPSPATRON
@gpspatron
Promote
A new Record from the North of Norway. 16 hours of jamming in a day. Have you ever seen an incident like this?
3:31 AM · Apr 27, 2023 · 1,386 Views
Post your reply
Reply
jakob @jakobmale · Apr 27, 2023
Could this be their military?
GPSPATR(@gpsp · Apr 23, 2023
Who knows. There is no further information yet
ukrtracke @ukrtra · Apr 27, 2023
Might be a part of Exercise Dynamic Mongoose 23, which is on atm.
dvidshub.net/video/881129/n...



We get funny requests like this on our website on a regular basis. And that explains why spoofing is used not only by the military but also by ordinary people. Check out this post on Twitter:



Challenges in Selecting an Optimal GNSS Anti-Spoofing and Anti-Jamming

Operators of critical infrastructure that relies on GNSS are considering various options for protection against spoofing and jamming. The available countermeasures vary depending on the specific application requirements:

For time synchronization systems:

- GNSS time servers equipped with anti-jamming CRPA antennas.
- Time transmission using protocols such as PTP, NTP, or WhiteRabbit.
- A combination of GNSS time servers with a cesium reference oscillator and GNSS signal authentication systems.
- Various integrated approach combinations.

For applications requiring reliable navigation and positioning, such as aviation, maritime and ground transport, UAV auto-piloting, industrial drones, and drone shows:

- Inertial navigation systems.
- Alternative navigation systems, such as Loran-E or LEO constellations.
- A combination of inertial navigation systems and GNSS receivers.
- Multi-element CRPA antenna systems implementing null-steering and beam-forming technologies.
- Various integrated approach combinations.

However, choosing the optimal protection system is challenging due to multiple constraints:

- Cost.
- Size and weight.
- Power consumption.
- Export restrictions.

We recommend starting with an analysis of the adversary, as the interference scenario varies significantly across different regions. It is also crucial to understand how your infrastructure behaves under spoofing and jamming attacks.

1. In some locations, you might encounter only simple car jammers used by truck drivers and taxi drivers. If your infrastructure is located along roads, you might experience brief, low-power episodes of interference as a vehicle with a jammer passes by. In

parking areas, you could face prolonged episodes of interference since drivers do not always turn off their GNSS jammers.

2. In some countries, different government agencies may use anti-drone systems that employ spoofing, like in Turkey. There are two scenarios here:
    - An automatic anti-drone system that activates for a few minutes after detecting a drone. Often, multi-element antenna systems are used to generate interference only in the necessary sector to avoid significant impact on the infrastructure.
    - A continuously active system that generates a fake signal continuously or quasi-continuously. In such cases, spoofing may be activated only during certain events.
3. In conflict zones, GNSS spoofing is extensively used to protect against UAVs. These scenarios can vary widely, but they commonly feature enormous output power covering large spaces within the line of sight.
4. The prevalence of GNSS jamming and even spoofing to evade road toll systems in certain countries.
5. If your region has an extensive coastline, you may face prolonged spoofing from ships used to evade monitoring systems for illegal entry into territorial waters or to circumvent sanctions.

We believe the ideal protection involves the use of a 16-element CRPA antenna system in combination with a high-quality inertial navigation system and a GNSS receiver with spoofing detection algorithms. However, such a system may not always be suitable due to high costs, large dimensions, and significant energy consumption. As with any engineering system, compromises are necessary to find the optimal solution for your specific case.

Type of Interference	Protection for Navigation & Positioning Applications	Protection for Time Applications
Short-Term Jamming *Examples:* • Passing car with low-power GNSS jammer • Powerful jamming from automatic anti-drone system	**Inertial Navigation System (INS):** Combines inertial measurements with a GNSS receiver to maintain navigation continuity and stability during short-term interference. Utilize inertial data to quickly exit the jamming zone.	**Rubidium Reference Oscillator:** Provides a stable clock source to maintain time accuracy during brief GNSS jamming periods. **Cesium Atomic Clock:** Offers exceptional long-term stability and accuracy, maintaining high-precision time synchronization during prolonged periods of long-term jamming. **Time Transmission Protocols:** • **PTP (Precision Time Protocol):** Provides highly accurate time synchronization over Ethernet networks, offering resilience against jamming by relying on network-based time sources instead of GNSS signals. • **WhiteRabbit:** Combines sub-nanosecond accuracy with Ethernet-based communication to provide an alternative time source independent of GNSS, ensuring precise time synchronization during jamming incidents. **Alternative Navigation Systems: Loran-E and LEO Constellations** • **Loran-E:** o Offers a reliable, low-frequency navigation system that operates independently of GNSS, providing a robust alternative for time synchronization. o By leveraging ground-based transmitters, Loran-E ensures continuous timing accuracy and resilience against jamming by utilizing highly stable, long-range signals.
Low-Power, Long-Term Jamming *Example:* Parked car with GNSS jammer near infrastructure	**4-Channel CRPA Null-Steering Antenna:** Adaptive antenna system suppresses interference signals by >40 dB, effectively reducing the impact of low-power jammers. **High-Stability Inertial Navigation System (INS):** Offers navigation integrity and stability during prolonged GNSS signal disruptions **Alternative PNT Sources:** Utilize signals of opportunity or other non-GNSS navigation aids.	
High-Power, Long-Term Jamming *Example:* Government jamming to protect VIPs	**8-Channel CRPA Null-Steering Antenna:** Typically, the more channels you have, the more interference cancellation you can expect. But it all depends on many factors. **Alternative PNT Sources:** Machine vision for navigation, INS, Terrestrial navigation systems, Celestial navigation	
Multiple Sources of High-Power Jamming *Example:* Military exercises or combat operations	**Ultra Multi-channel CRPA:** The more interference sources to be suppressed, the more CRPA system channels are required. Systems up to 16 channels are commercially	

Type of Interference	Protection for Navigation & Positioning Applications	Protection for Time Applications

	available, providing interference suppression from 15 directions.	• **LEO Constellations:**
		  ○ Low Earth Orbit (LEO) satellite constellations like Starlink, OneWeb, Orbcomm, and Iridium provide accurate timing through signals of opportunity, offering a strong alternative when GNSS signals are unavailable.
		  ○ These constellations deliver resilient and precise timing services by:
		  ▪ **Higher Signal Strength:** Their proximity to Earth provides stronger signals that can reach challenging environments like urban canyons and polar regions.
		  ▪ **Novel Frequencies and Geometry:** Transmission on novel frequencies enhances resilience against jamming, and the unique geometry improves availability.
		  ▪ **Combining with GNSS Systems:** They work alongside GNSS (e.g., Galileo) to provide exceptional resilience, ensuring continuous timing services even in contested environments.

Non-Coherent, Short-Term Spoofing	**GNSS Receiver + INS:** Combination of GNSS receiver with basic spoofing detection algorithm and inertial system. Possible algorithms for detecting non-coherent spoofing:	**Basic Spoofing Detection Algorithms + Stable Reference Oscillator:** Combination of basic spoofing detection techniques and a Rubidium Reference Oscillator or Cesium Atomic Clock.

Type of Interference	Protection for Navigation & Positioning Applications	Protection for Time Applications

Example: Automatic anti-drone system with spoofing	anomalies in GNSS signals such as jumps in coordinates that are inconsistent with INS data.	• **Detection Algorithms:**
		  ○ Detect time inconsistencies between GNSS receiver and alternative sources.
		  ○ Identify anomalies in raw GNSS data.

Non-Coherent, Long-Term Spoofing
Example: Protecting critical infrastructure from UAVs with spoofing
	GNSS Receiver + Alternative PNT Sources: Combination of GNSS receiver with basic spoofing detection algorithm and machine vision/INS/ Terrestrial navigation systems/Celestial navigation. Possible algorithms for detecting non-coherent spoofing: anomalies in GNSS signals such as jumps in coordinates that are inconsistent with INS data.	**Basic Spoofing Detection Algorithms + Alternative Time Sources:** Combination of basic spoofing detection techniques and alternative time sources like PTP, WhiteRabbit, Loran-E, or LEO constellations.
		• **Detection Algorithms:**
		  ○ Identify time inconsistencies between GNSS and alternative sources.
		  ○ Detect anomalies in raw GNSS data.

Coherent, Deliberate Spoofing
Example: Cyberattack on GNSS infrastructure
	Advanced Spoofing Detection System + Alternative PNT Sources: Combination of spoofing detector with multi-element antenna system and alternative PNT. Possible algorithms for detecting coherent spoofing: spatial signal analysis, angle of arrival estimation.	**Advanced Spoofing Detection Algorithms + Alternative Time Sources:**
		Combination of advanced spoofing detection algorithms with multi-element antenna systems and alternative time sources like PTP, WhiteRabbit, Loran-E, or LEO constellations.
		• **Detection Algorithms:**
		  ○ Spatial signal analysis to detect coherent spoofing.
		  ○ Angle of arrival estimation to identify the direction of spoofed signals.

The methods in this table offer potential strategies for countering spoofing and jamming, but they are not a one-size-fits-all solution. Each situation demands careful analysis and tailored protection methods to address specific attack techniques. We've simply highlighted the types of interference you might encounter and possible ways to tackle them.

When selecting the right technology to combat GNSS spoofing and jamming, consider the following steps:

1. **Study GNSS Interferences in Your Region**: Investigate the types and frequencies of GNSS disruptions that occur in your area. This could include understanding patterns of jamming and spoofing activities and identifying the main sources of these interferences.
2. **Assess the Impact on Your Infrastructure**: Evaluate how these GNSS disruptions affect your specific infrastructure. Consider the criticality of GNSS services in your operations and determine the potential risks and consequences of interference.
3. **Make an Informed Decision**: After analyzing the regional GNSS interferences and their impact on your infrastructure, carefully weigh the pros and cons of various countermeasures. Choose the most effective solution that meets your needs while considering cost, complexity, and long-term sustainability.

Researching GNSS Interference with the GPSPATRON System

The GPSPATRON system provides a comprehensive suite of tools for analyzing GNSS interference, essential for protecting navigation and timing systems. The system comprises two main components: the GNSS interference detector, known as the GP-Probe, and a web application, GP-Cloud. The GP-Probe measures various parameters of GNSS signals and sends the raw data to GP-Cloud in real-time. GP-Cloud utilizes sophisticated algorithms to promptly analyze this data, detecting and categorizing anomalies/interferences. This process enables the identification of complex GNSS spoofing and jamming attacks.

The combination of GP-CLoud and GP-Probe allows you to explore interference in depth:

1. **Type of Interference:**
   The combination of GP-Cloud and GP-Probe TGE2 allows real-time differentiation between GNSS spoofing and jamming, ensuring accurate identification of interference types.

2. **Constellation-Specific Analysis:**
   GP-Cloud identifies the specific GNSS constellation targeted (GPS, GLONASS, Galileo, BeiDou), measuring each individually. This enables users to see exactly which constellation was attacked and adjust their defenses accordingly.

3. **Interference Strength & Coverage Area:**
   Several dozen GP-Probes distributed over an area, combined with centralized monitoring via GP-Cloud, estimate the interference zone, providing insight into interference power and coverage.

4. **Duration Analysis:**
   To develop effective countermeasures, understanding interference duration is crucial. GP-Cloud's built-in event detection mechanism collects statistical data on interference timing, providing meaningful insights into the temporal parameters of the interference action.

5. **Source Identification:**
   Using TDOA (Time Difference of Arrival) localization techniques, GP-Cloud and GP-Probe TGE2 with RFSA and TDOA options identify the location and likely source of interference. This information is critical for precise countermeasures and system resilience enhancement.

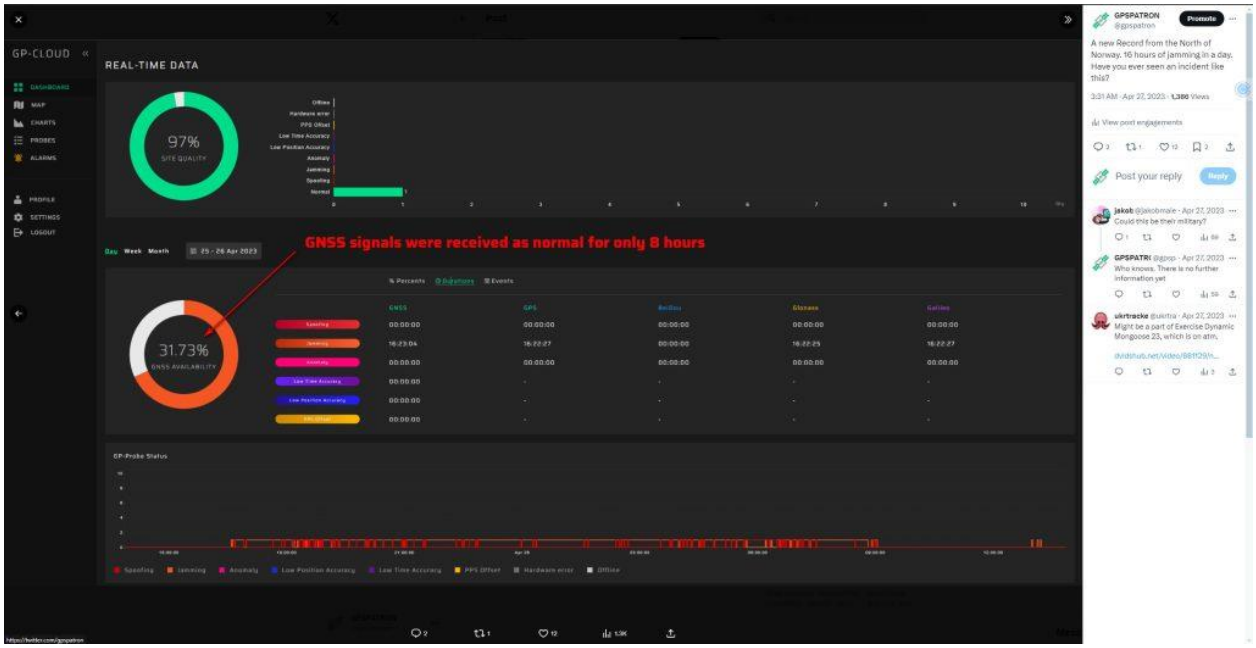
6. **Modulation Analysis:**
   The embedded RF signal analyzer in GP-Probe TGE2 provides power spectrum, waterfall, and spectrogram analysis of interference signals. This reveals the types of signal modulation used, offering insights into the tactics employed by attackers.

Detailed Signal Analysis and Attack Visualization with the GPSPATRON System

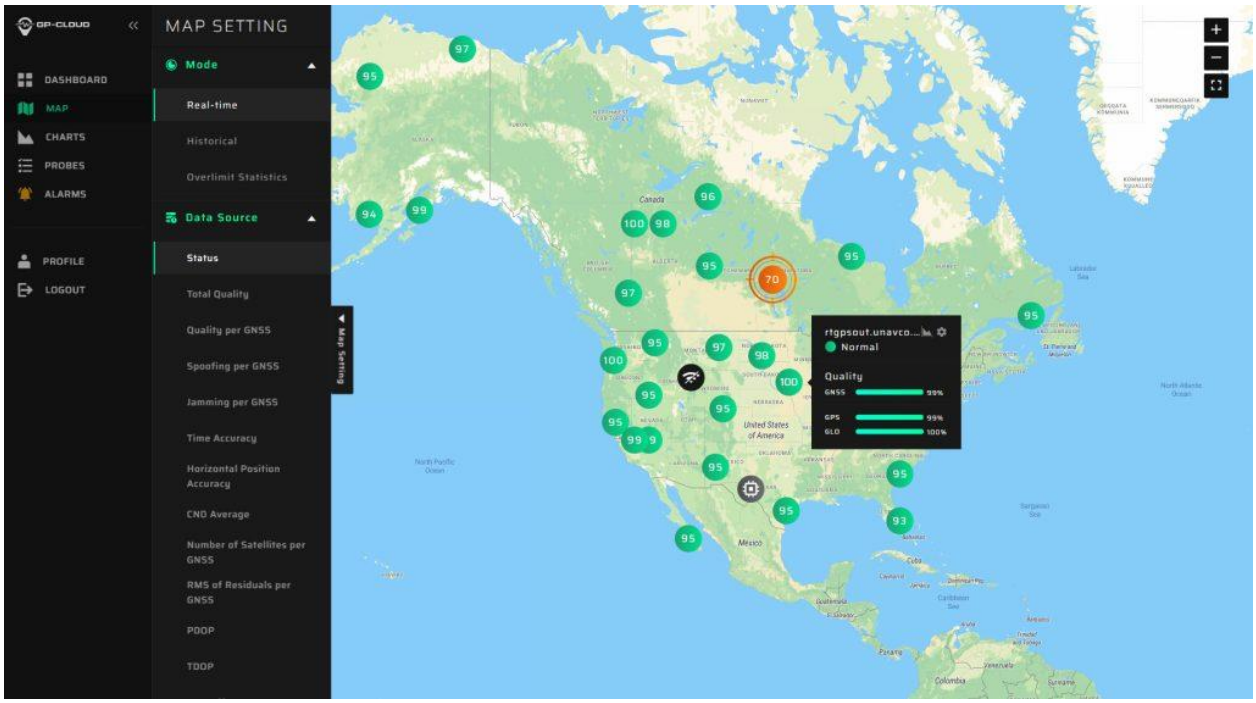
Below are screenshots showing the detailed data provided by the GPSPATRON system.

Complex Attack Scenario: A screenshot depicts a sophisticated attack scenario starting with jamming of all constellations followed by spoofing of the GPS and Galileo systems, while simultaneously jamming the GLONASS system. This visual helps users understand the sequence and complexity of multi-pronged interference strategies.

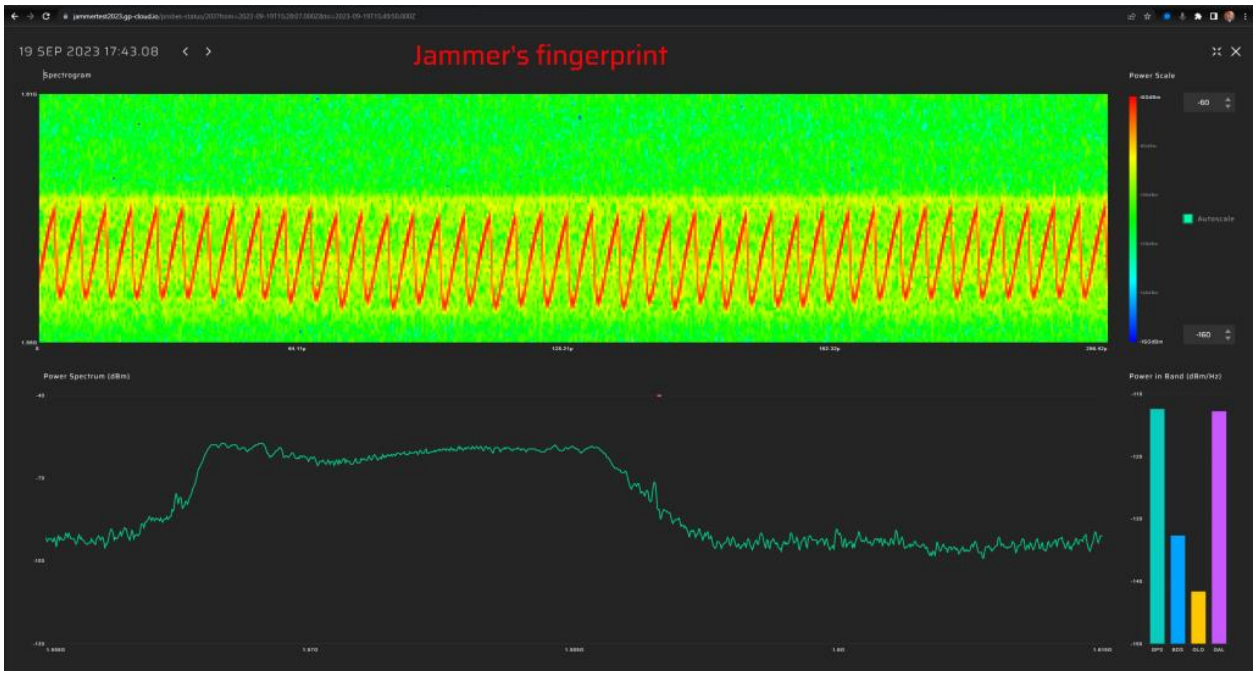
Statistical Dashboard: A display provides statistical data on the frequency, duration, and types of interference detected over time. This dashboard allows for quick assessment and trend analysis, helping users make informed decisions on potential threats.



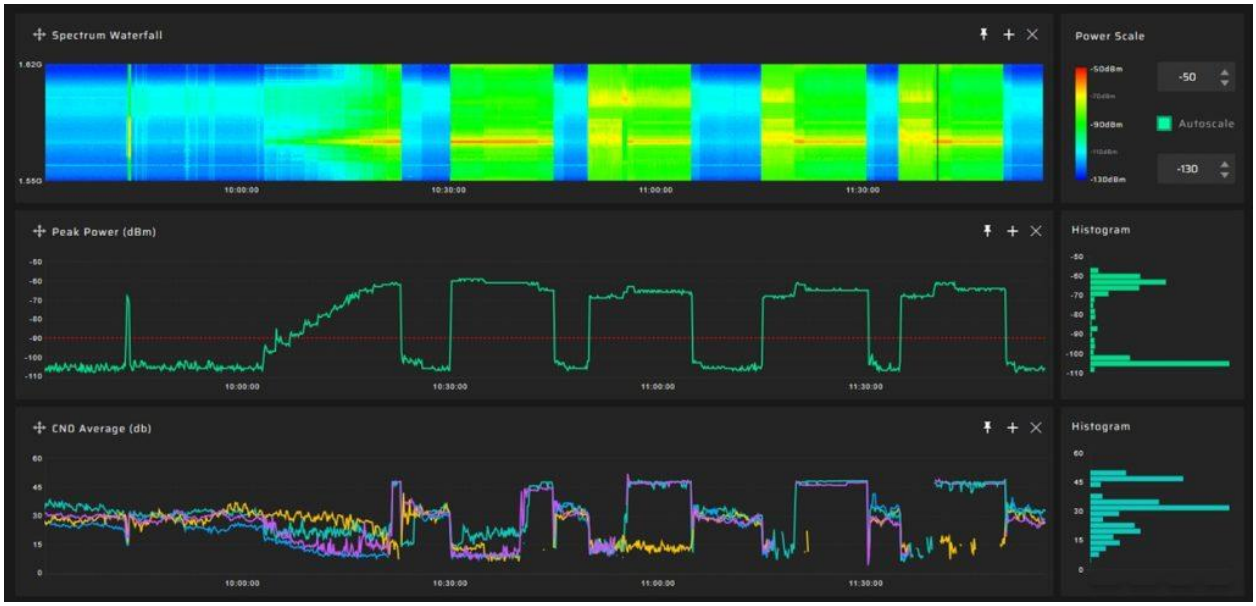
Interactive Map: A screenshot of the GP-Cloud map displays your entire infrastructure with GP-Probe installations, highlighting interference zones and offering a comprehensive understanding of areas impacted by GNSS signal disruptions.



Interference Spectrogram: A screenshot displays a spectrogram of RF interference, revealing the frequency-modulated signal of a jammer. This visualization enables users to analyze interference patterns, identify the jammer's characteristics, and better understand the attack's impact on GNSS signal reception.

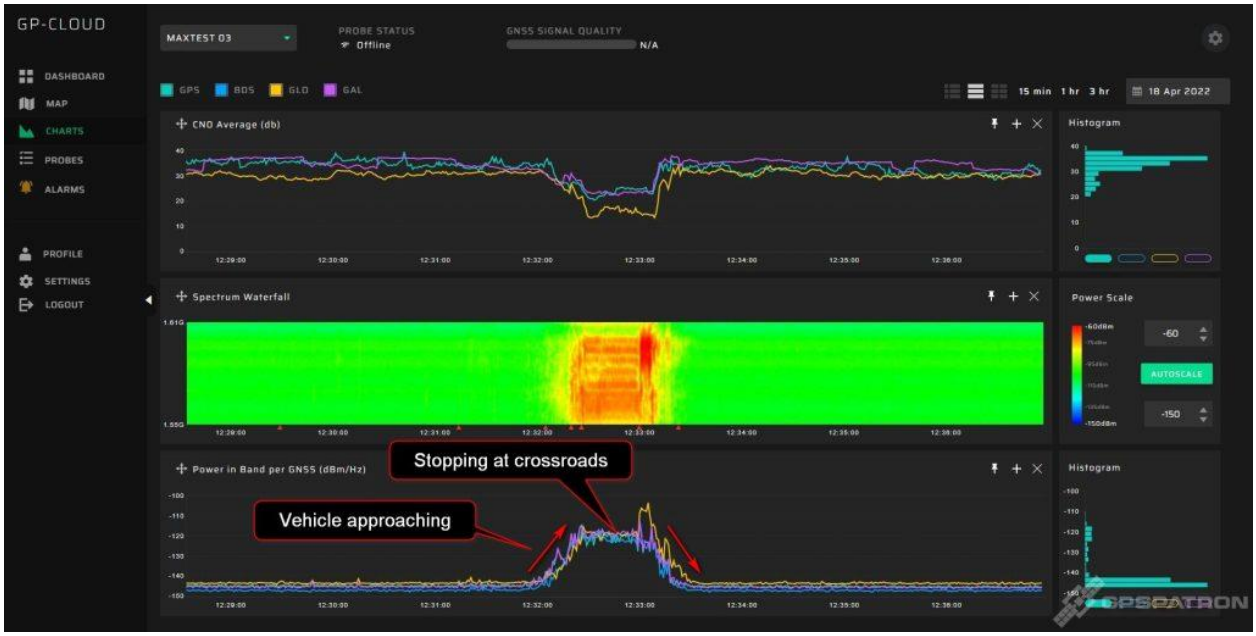


Assessment of Interference Timing Parameters: A screenshot illustrates a series of GNSS spoofing attacks, helping users evaluate the attack tactics used and analyze their timing parameters.

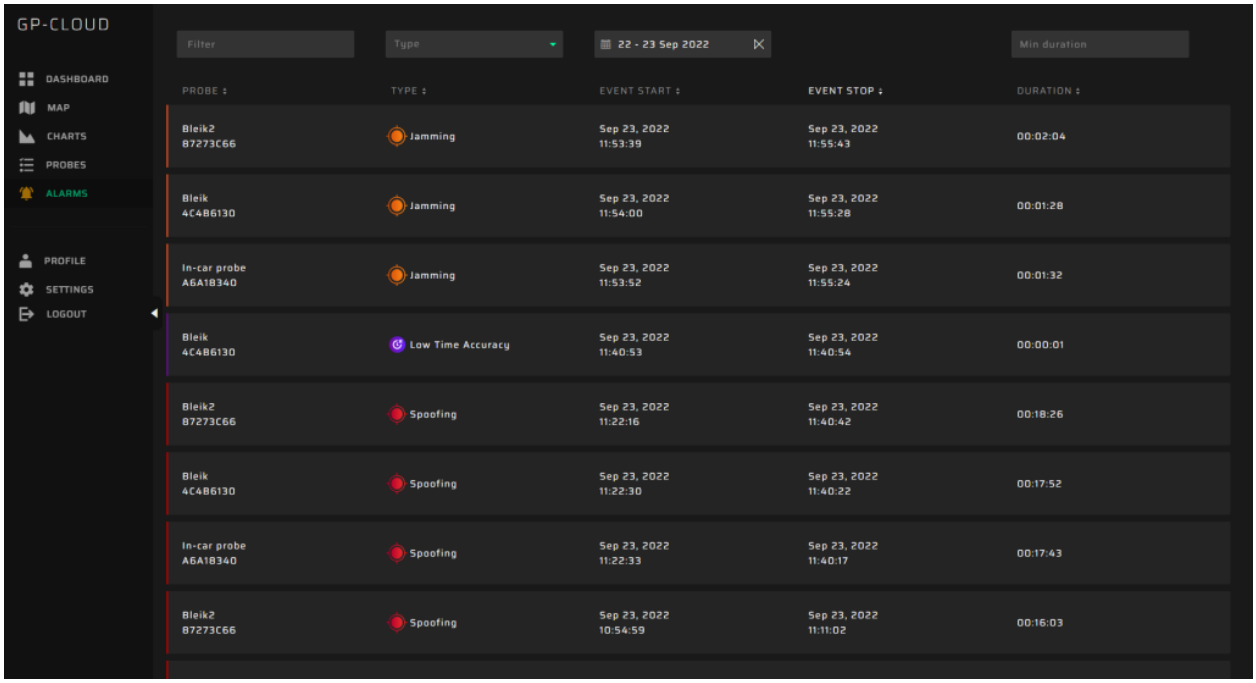


Non-Coherent Spoofing Detection: A screenshot displays a non-coherent GNSS spoofing attack scenario, where the receiver suddenly shifts its coordinates. This visualization helps users distinguish between coherent and non-coherent spoofing. Keep in mind that coherent spoofing is always deliberate and specifically targeted at you.

Interference Power Profile Analysis: A screenshot displays a GNSS jamming scenario likely originating from a passing vehicle. The jamming signal's power profile rises as the vehicle approaches and declines as it moves away, helping users clearly identify the mobile interference source.



Detected Interference List: A screenshot displays a list of detected interference events, complete with their classification and key parameters.



Conclusion

The GPSPATRON system provides comprehensive and in-depth data on GNSS interference that is essential for effectively developing and implementing protection methods against spoofing and jamming. Without full knowledge of these threats, choosing the optimal solution becomes challenging. The insights gained from the GPSPATRON system empower you to make informed decisions and tailor your defense strategies to best meet your specific needs.