GPS Patron GNSS Quality Monitoring System

With a world that is heavily dependent on Global Navigational Satellite Systems (GNSS), it is important that the integrity of the signals, especially location and time accuracy, remain uncompromised. There are 4 billion of GNSS receivers in various applications around the world that are highly susceptible to GNSS signals quality degradation. This includes:

Financial Services

Spoofing attacks can cause a timestamp shift that influences the security and integrity of banking transactions and can lead to data manipulations.

Transport Infrastructure

The distribution of autonomous machines requires uncompromised accuracy of coordinates. Coordinates manipulations can lead to undesired damages, and even human loses.

Power Grid System

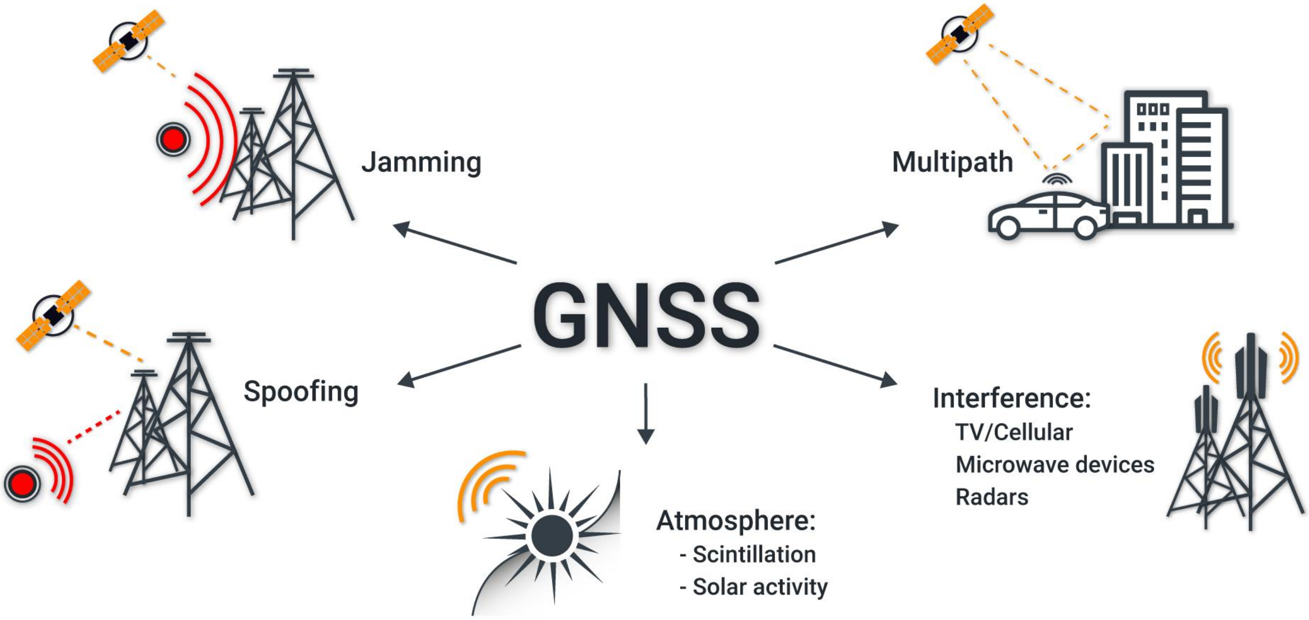
Time synchronization distortion of a Phasor Measurement Units can lead to cascading faults and large-scale power blackouts.

Cellular Communication Networks

Modern communication systems such as 5G require high precision PPS. Poor satellite signal quality or intentional spoofing attacks can leave whole regions and even cities without communication.

GNSS RF signals received power levels are typically 20dB below the ambient noise floor. Therefore, they are highly susceptible to various interferences. With the introduction of more and more wireless technologies, the RF spectrum is becoming more crowded. In densely populated cities with tall buildings and a large number of communications systems, receiving high-quality GNSS signals can be a big problem.

Factors that impair GNSS signals quality:

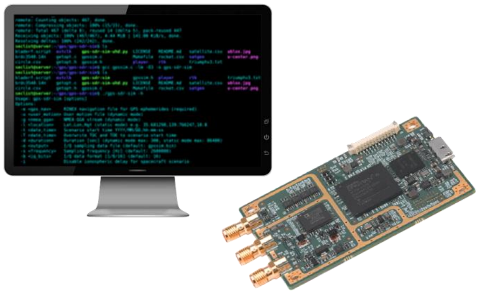


GNSS Spoofing

More and more facts of GNSS spoofing are detected around the world. A new report from C4ADS, a non-profit organization focusing on conflict and security, found 9,883 cases of GNSS spoofing. Such a widespread use of spoofers is explained by the fact that GNSS spoofing is used for:

- VIP and mass events protection (Counter-UAV)
- Deception of vehicle tracking systems
- Military exercise

In many countries, security guards have begun to use GNSS spoofing to protect against Unmanned Aerial Vehicle. Unscrupulous drivers of cars and trucks use spoofing and jamming to trick vehicle tracking systems. If GNSS spoofing is used in a densely populated city, then banks, cellular operators, TV broadcasting are experiencing problems with time synchronization of PNT servers with GNSS receiver. An unintended spoofing attack leads to time and coordinates shift and cause unpredictable heavy damages to businesses.



5 years ago, GPS spoofing used to require considerable technical skills and financial expenses. Now it can be done with low-cost commercial hardware (SDRs like HackRF) and software downloaded from the GitHub (e.e., osqzss/gps-sdr-sim).

So now, any student can organize a spoofing attack on a bank's processing center in 15 minutes.

GNSS Signal Quality

Not all GNSS receivers have access to multiple satellite signals needed for accurate timing. Obstacles like trees, tall buildings, construction cranes, billboards, etc., block satellite's signals, especially in densely populated urban areas, precisely were more GNSS-depended equipment is needed. This problem can be solved by placing a receiver on a rooftop, above the obstacles, but that is not feasible in every case. Additionally, the quality of the GNSS signals are affected by: atmospheric interference, multi-path from reflected signals, radiation from the cellular base stations or broadcasting station.

These vulnerabilities are not acceptable for the time-critical applications like 5G, power grid system, financial sector. Especially taking into account that in 2018, regulators in Europe and the US introduced clock synchronization regulations for financial services firms. In Europe, ESMA's MiFID II requires investment firms and venues to timestamp trading events accurately to Coordinated Universal Time (UTC) and to an appropriate level of granularity such as microseconds for High Frequency Trading (HFT). Since February 2018, US firms have been timestamping to the National Institute of Standards and Technology (NIST) atomic clock in order to meet SEC 613 requirements. Accurate timestamping is a high priority for the regulators in all jurisdictions and we expect to see requirements become more onerous over time.

All the above-mentioned facts underpin the necessity to implement more complex GNSS signal quality monitoring systems that can provide timely notifications of threats and switch time-critical infrastructures to backup synchronization channels. Such monitoring systems should be easily integrated with currently deployed systems and complement them with new functionalities.

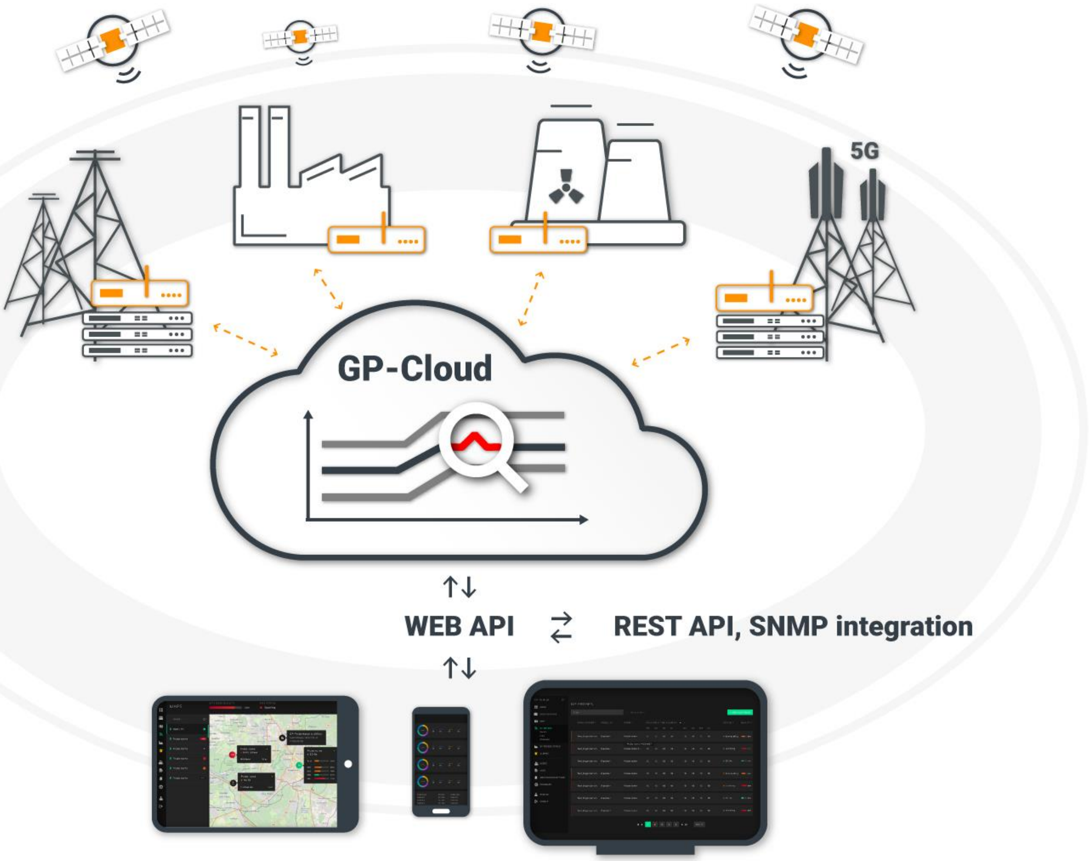
GPS Patron Solution

GPS Patron GNSS Quality Monitoring System is a neural network based distributed system for monitoring and protecting time/coordinates critical infrastructure. It supports: GPS, GLONASS, BeiDou, Galileo.

Applications

- ✓ 24/7 Real-Time Position and Timing Accuracy Monitoring
- ✓ Detection of All Types of Spoofing and Jamming

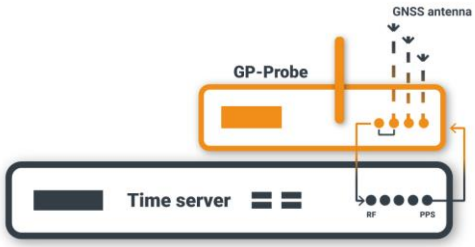
The system consists of affordable three-channel GNSS probes (GP-Probe) and a powerful cloud service (GP-Cloud). GP-Probe conducts GNSS signal measurements using 3 channels with angle-of-arrival estimation and transmits raw data to the GP-Cloud for real-time processing. GP-Cloud uses advanced anomaly detection algorithms for determining any nonlinearities present in the radio frequency signals.



With GPS Patron technologies you are able to control all your GNSS-dependent entities. Just install GP-Probe on your time/coordinates critical infrastructure and fully control it in one web interface.

It’s an ideal solution for the time-critical applications like 5G, financing services, DVB-T, power grid systems.

How it works

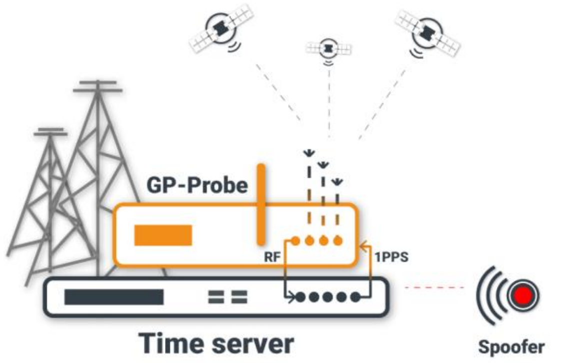


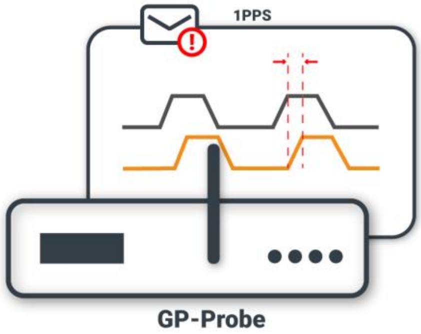
1. Install GP-Probe on your time/coordinates-critical infrastructure, for example, near your time server. The GP-Probe has a transit RF port for transmitting GNSS signals to the protected receiver.

In case of spoofing or low signal quality, GP-Probe disables transit port.

2. To guarantee uncompromised detection of any type of advanced spoofing, GP-Probe uses 3 spaced antennas for measuring GNSS signals.

Every second GP-Probe registers more than 900 parameters for all visible GPS, GLONASS, BeiDou, Galileo satellites.



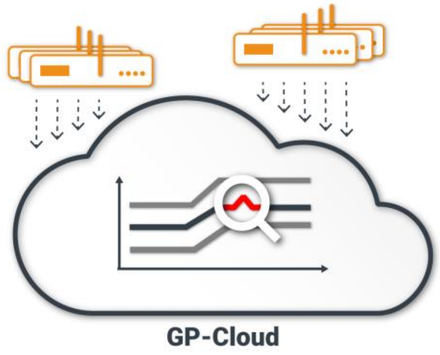


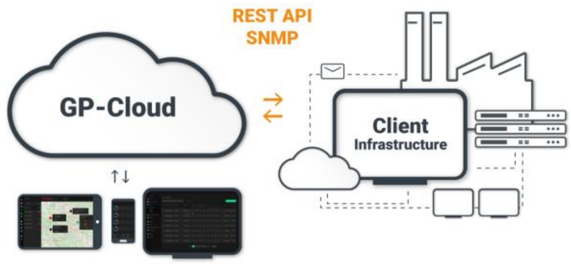
3. For advanced time server protection, the GP-Probe can measure the difference between internal and external PPS. In the case of any major mismatch, GP-Probe instantly sends the corresponding alarm to the GP-Cloud.

This functionality helps to improve the overall reliability of synchronization systems.

4. GP-Probe transmits raw data to the GP-Cloud for real-time processing. GP-Cloud analyzes data and computes the time/coordinates accuracy and probability of spoofing/jamming.

The spoofing detection algorithm is based on the cutting edge Machine Learning Techniques for anomalies detection and classification.





5. Monitor your entire time/coordinates critical infrastructure in a single user-friendly web-interface. If the system detects any type of spoofing or jamming, as well as GNSS parameters degradation, you will receive instant notification.

A powerful REST API allows you to integrate your existing infrastructure to our solution.

GP-Probe

The GNSS Radio Probe for Timing (PNT) & Frequency Reference System Protection

- PPS offset measurement
- 19-inch rack half-size form factor
- dual power module: 110/220 AC; 18 – 75 VDC

GP-Probe Time Guard Edition is specifically designed to monitor and protect time servers (PNT).

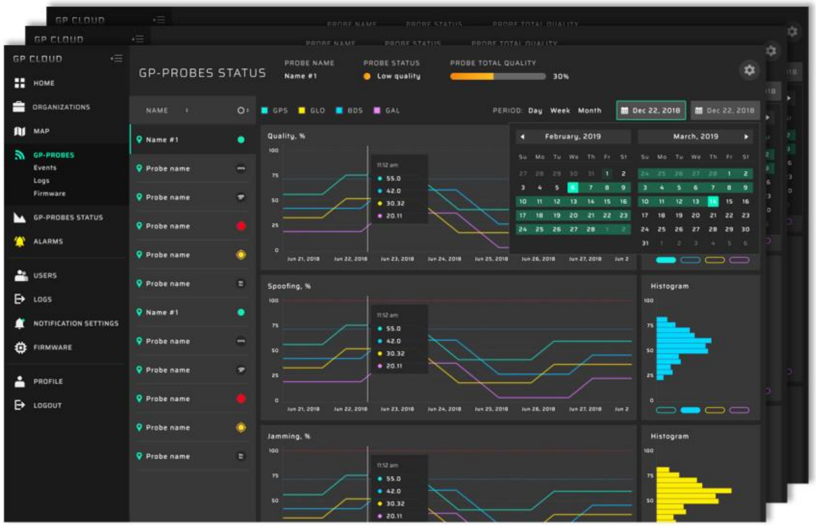
It conducts GNSS satellite signals measurements on 3 channels and transmits raw data to the **GP-Cloud** for real-time processing.

Features

- Three RF channels for advanced GNSS spoofing detection and signal quality estimation.
- Support: GPS/QZSS L1 C/A, GLONASS L10F, BeiDou B1I, Galileo E1B/C, SBAS L1 C/A: WAAS, EGNOS, MSAS, GAGAN.
- PPS input for PNT health checking. GP-Probe measures the time difference between internal and external PPS.
- GNSS transit port to connect the time server. It turns off in case of spoofing or low signal quality.
- Form factor: 19-inch rack half-size.
- Power supply: 110 – 220 AC or 18 – 75 DC.
- RS232 for external devices remote control. GP-Cloud can send a remote control commands to the connected equipment.
- Active/passive GNSS antennae support.
- 3G/4G modem and 100BASE-TX Ethernet for data transferring to the GP-Cloud.
- Web interface for configuration.
- Firmware auto-update engine.

GP-Cloud

The GP-Cloud web user interface allows you to view the health of your entire all the time/coordinates critical infrastructure in real time.



GP-Cloud analyzes RAW data from the **GP-Probe** in real time and estimates:

- coordinates accuracy
- time accuracy
- spoofing probability
- jamming strength

The system is designed to detect any types of spoofing\jamming or other anomalies of the navigation field, resulting in coordinates\time accuracy degradation

Features

- The interactive map that displays locations of all GP-Probes and their health status.
- Dashboard for analyzing the entire infrastructure with all system status Indicators.
- GP-Probe’s measurements history.
- Detailed alarms log.
- Based on machine learning techniques for anomaly detection in measured data.
- Powerful REST API for integration.

GPS Patron Services

✓ Evaluate the Vulnerability of Your GNSS Equipment to Spoofing in GPS Patron's Laboratory

Do you have GNSS dependent time/coordinates-critical infrastructure and you want to evaluate its vulnerability to a new and increasingly common threat of GNSS spoofing attacks?
GPS Patron provides laboratory testing services of you GNSS equipment for identifying vulnerabilities to spoofing attacks. Since we are developing a dedicated system of protection against spoofing and experimenting in the field, we have all necessary empirical knowledge about different types of attacks, their features, as well as their methods of execution. To simulate a spoofing attack, we use our own solution – GP-Simulator. For your specific requirements, we will develop custom test methods and protocol templates.
Typical test objects are the RTK Base Stations and Time Servers.

✓ On-Site Testing of Your Infrastructure for Resistance to GNSS Spoofing

Do you want to evaluate the vulnerability of your entire GNSS-dependent infrastructure to spoofing?

GPS Patron team provides on-site testing services. Our team can conduct all necessary tests on your site in accordance with a pre-approved test schedule. You can check how your existing infrastructure responds to a timestamp shift, PPS shift, and GNSS signal quality degradation.

✓ GNSS Signal Quality Monitoring as a Service

Do you need to select the right site for GNSS equipment like RTK Base Station, Time Server, etc? Or do you want to make sure that the quality of GNSS signals on your current site is proper?
GPS Patron offers its solutions as a service so that you can monitor and protect your time\coordinates-critical infrastructure without investing into new hardware and software. We can rent out the GP-Probe, install it on your site, and conduct the corresponding measurements. GP-Probe registers more than 900 parameters for all visible GPS, GLONASS, BeiDou, Galileo satellites every second. The entire huge volume of data is collected and stored in the GP-Cloud for further analysis. We pose all the necessary methods and tools required for the analysis of that kind of data for calculating GNSS quality indicators. We prepare test reports with further recommendations.
This service is highly suitable for EGNOS and WAAS providers and operators for the right site selection and RFI monitoring.

✓ System installation services

GPS Patron team provides GNSS quality monitoring system as turnkey solutions. Our professional team can install GP-Probe on your infrastructure, set it up and implement its integration.

✓ System integration services

We can effortlessly integrate our solutions into your existing infrastructure. GP-Cloud provides a powerful API for third-party services integration that can be implemented on your own or ordered from us as a service.

✓ GP-Probe Customization

The GP-Probe can be customized to perfectly suit your particular needs.