GPSPATRON

Real-Time GNSS Jamming and Spoofing Detection

GNSS Signal Quality Analysis

Maksim Barodzka

CEO @ GPSPATRON

www.gpspatron.com www.youtube.com/c/GPSPATRON twitter.com/gpspatron

Presentation Agenda:

1.System Overview

- PowerPoint presentation of our system for GNSS interference detection.

2.Current Results: Jammer Test 2024

- A live update showcasing the latest data and results from ongoing JammerTest 2024.

3.Interference Event: Kaliningrad

- A detailed look at the interference detected in Kaliningrad, including analysis and insights.

4.Live Experiment

- We will perform a live experiment, demonstrating real-time interference detection and system response.

About GPSPATRON

•Who we are:
A pure engineering startup based in Poland. Since 2019, we have been focused on tackling the challenges of GNSS spoofing and jamming.

•Our focus:
We specialize in developing cutting-edge, enterprise-grade solutions for protecting critical infrastructure against GNSS threats.

•What we offer:

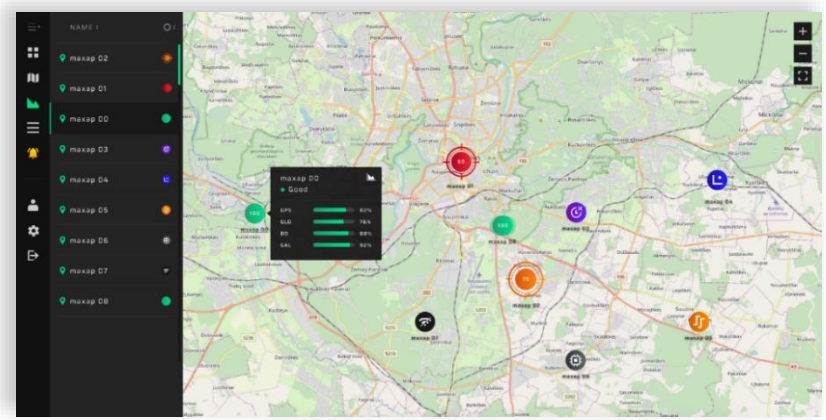
- GNSS interference detectors: GP-Probe TG2 and GP-Probe DIN L1
- GP-Cloud: Cloud-based platform for real-time GNSS signal quality analysis and interference detection
- Software-defined jammer and spoofer

- Our Clients:
  - Industrial drone & drone show operators
  - Airports
  - Telecom operators
  - Smart power gride operators
  - Data centers
  - Radio spectrum monitoring authority

GNSS Interference Detection. Concept of Operation

GPSPATRON is a distributed system for GNSS interference detection and classification. The system consists of GNSS interference detectors and web application:

GP-Cloud



Statistics
User notification
API for integration

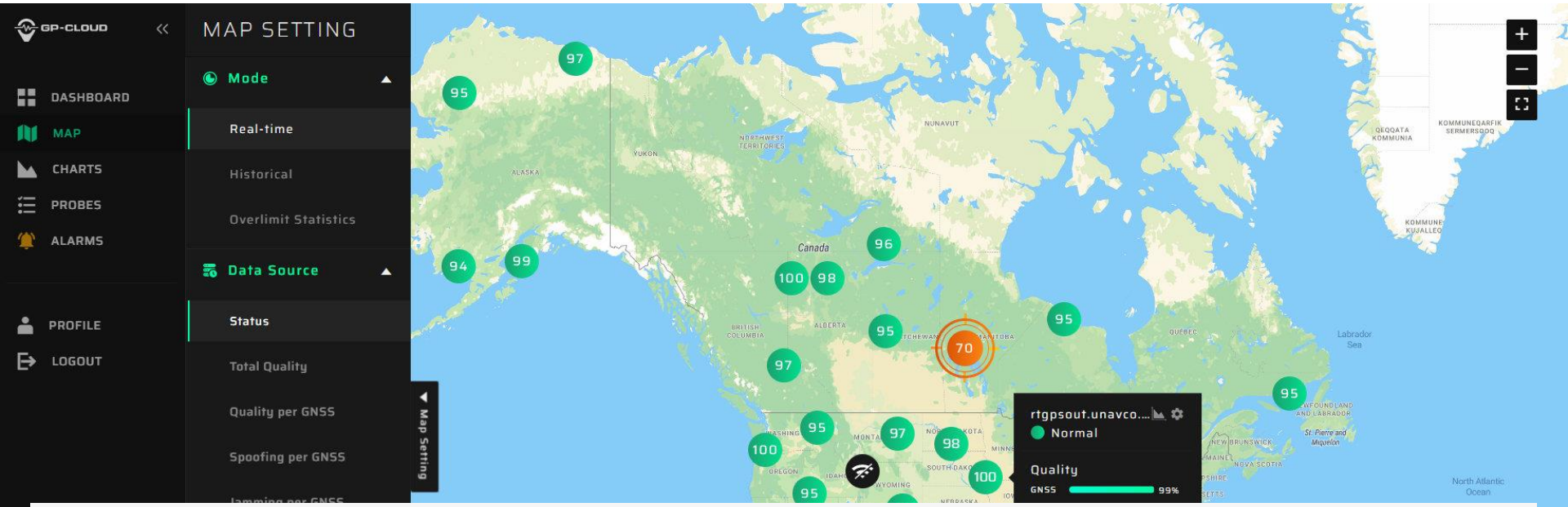
High-performance 3-channel probe

Data streams

One-channel probe

The GP-Probe measures GNSS signals using three RF channels to estimate spatial signal parameters and transmits raw data to GP-Cloud for real-time processing. GP-Cloud uses advanced anomaly detection and classification algorithms.

GP-Cloud

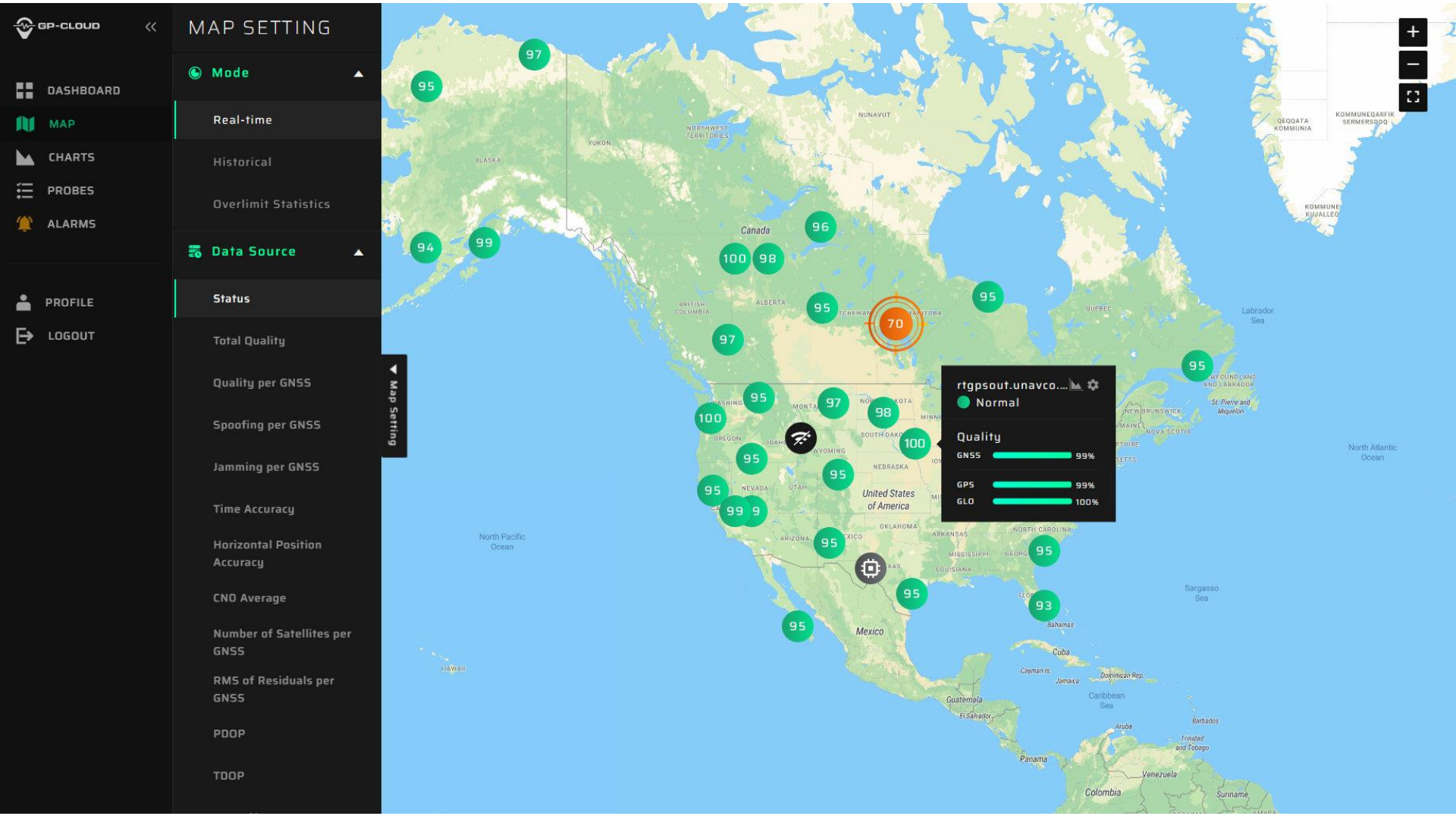


- The application processes raw GNSS data from connected GP-Probes or any other GNSS receivers in real-time, estimates GNSS signal quality/accuracy, detects spoofing/jamming, and saves all results in the database.
- GP-Cloud supports 1-Hz GNSS data from RTK base stations or other GNSS probes\receivers using the RTCM, NMEA, Septentrio SBF protocols over NTRIP.
- GP-Cloud is available as a service or as an on-premises.
- Enterprise-grade application with limitless horizontal scaling.
- REST API for integration.

GP-Cloud User Interface. Dashboard

On the dashboard you can monitor the status of GNSS signals in real-time and evaluate the statistics: how many events occurred, the duration, and what constellations were affected.

GP-Cloud User Interface. Map



On the map, you can monitor the status of all your GNSS-dependent infrastructure in real-time. You can stream data from your existing GNSS receivers to GP-Cloud.

GP-Cloud User Interface. Charts

The system is capable of detecting and classifying the most sophisticated attack scenarios.

GP-Cloud - Detailed Interference Assessment and Its Impact on GNSS Signal Quality

GP-Cloud tools enable detailed interference analysis and assessment of its impact on the quality of GNSS signal reception

GP-Cloud User Interface. Events

The system logs all recorded events for further investigation.

GP-Probe TGE2

- Three RF channels for intentional, synchronous, multiple-TX GNSS spoofing detection.
- Form factor: 19-inch rack, half-size.
- Double power module: 110 – 220 AC, 18 – 75 DC.
- GNSS signal quality measurements: pseudorange errors, carrier phase, SNR, etc.
- PPS input for the external time server health checking.
- 4G modem and 100BASE-TX Ethernet for data transferring to the GP-Cloud.
- Web interface for configuration (HTTP or HTTPS).
- Embedded LUA scripting language to create a custom scenario

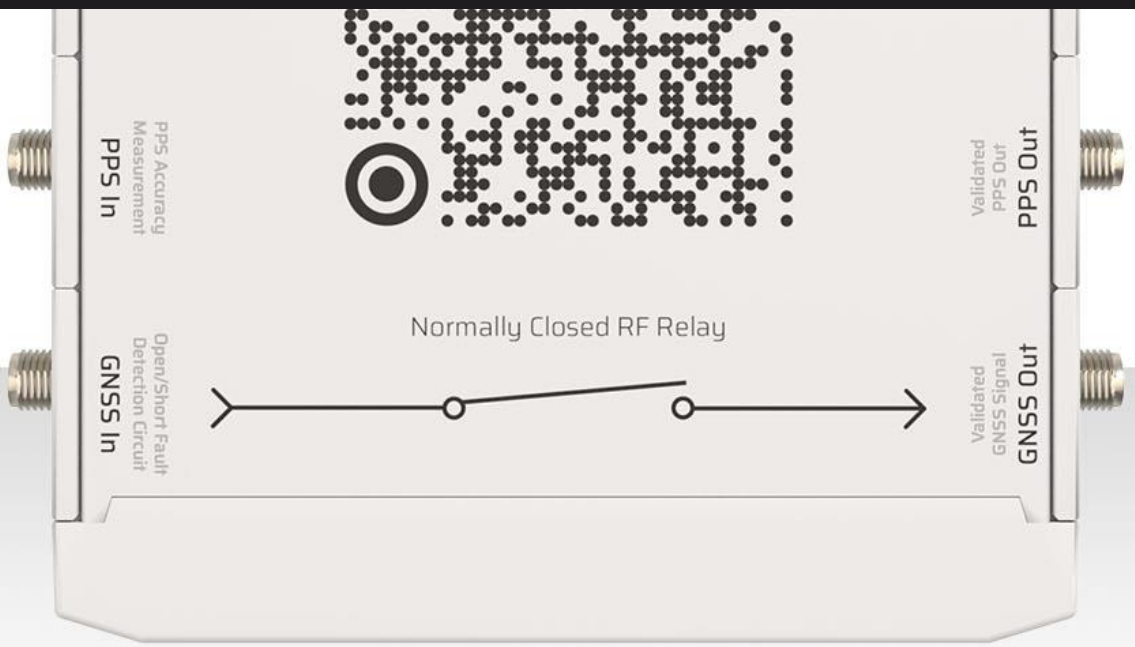
GP-Probe DIN L1

Designed for telecom to monitor GNSS interference and synchronization quality

Cost-effective GNSS probe with built-in RF blocker, onboard GNSS spoofing/jamming detection and LUA scripting. Compatible with GP-Cloud.

GP-Probe DIN L1 covers three primary applications: GNSS interference detection and classification, PPS accuracy monitoring, GNSS signal quality analysis, and logging. The device is easily installed between a GNSS antenna and a receiver or time server. When an event is detected, the GNSS and PPS outputs are immediately disabled, preventing any counterfeit signals from reaching your systems.

Time Server Protection with GP-Probe DIN L1



Built-in RF Blocker

GP-Probe DIN L1 is connected between GNSS antenna and receiver
Built-in RF blocker disables GNSS output when spoofing or signal quality degradation is detected

This in-line device seamlessly integrates between your GNSS antenna and time server, providing real-time monitoring and defense.
Just connect the probe in between a time server and a GNSS antenna.
If there is no anomaly or interference, the GNSS signal passes from input to output. If something is detected, the output is disabled.

PPS Phase Accuracy Monitoring

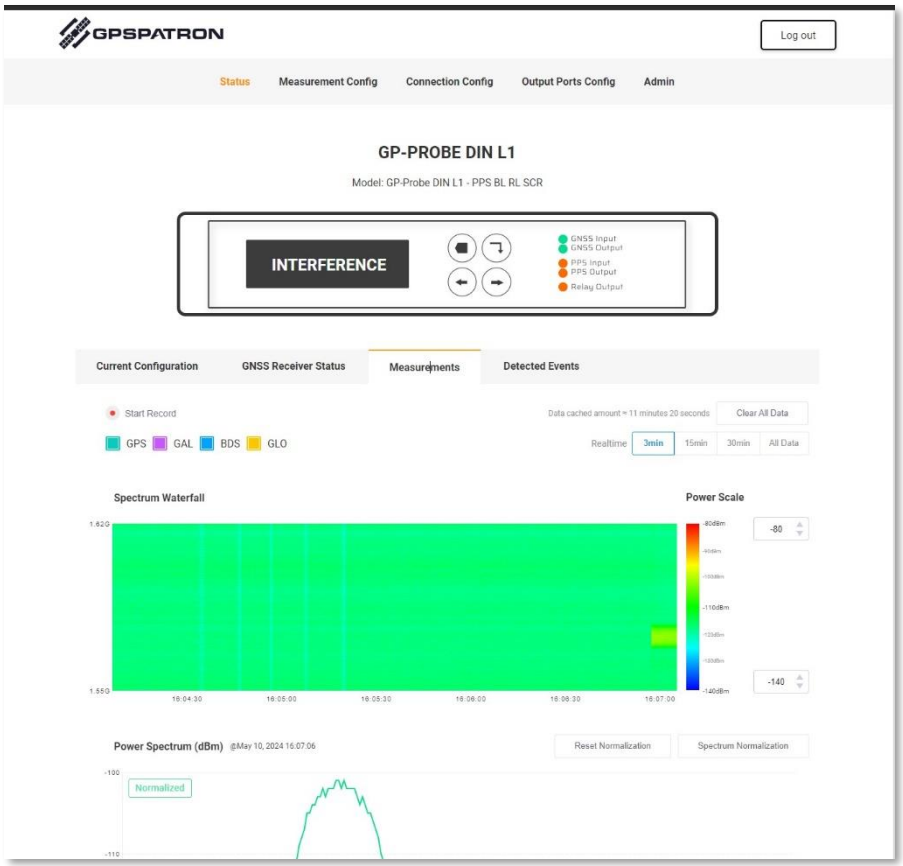
PPS Accuracy Measurement

The synergy of GP-Probe DIN L1 and GP-Cloud delivers a comprehensive solution for:

- time synchronization quality monitoring and logging
- GNSS accuracy degradation detection
- GNSS spoofing/jamming detection

GP-Probe DIN1 measures the time offset between internal and external PPS and streams the data to GP-Cloud for real-time monitoring, statistical analysis, and user notifications.

GP-Probe DIN L1 – Onboard Signal Processing



Onboard signal processing software option for interference and anomaly detection in GNSS signals without connecting to the GP-Cloud servers. The probe operates completely independently.

Demonstration of GPS spoofing detection: https://youtu.be/L9nUqtOLbPM

GP-Probe Case

IP67 Rated Protective Case for Outdoor use of GP-Probe TGE2

With built-in LiPo battery, you can be sure that your GP-Probe TGE2 will stay powered and operational for up to 7 days no matter where you take it, in all weather conditions.

- # GP-Probe Box

IP66 Rated Protective Box for Outdoor Use of GP-Probe TGE2 . Designed for Wall or Pole Mounting

Mounting Kit

The GP-Probe Box features a comprehensive mounting kit designed for secure attachment to both round and square poles, ensuring easy installation on a variety of surfaces.

The enclosure is engineered to house and protect the GP-Probe TGE2 GNSS interference detector in demanding environments. It ensures reliable operation in extreme conditions, withstanding temperatures from -40°C to +50°C. Its user-friendly design allows for easy installation & de-installation of the detector. The comprehensive mounting kit enables secure mounting on various surfaces and walls, ensuring versatile deployment options.

JAMMERTEST 2022, 2023, 2024….

The system was validated during JammerTest2022 & 2023.

The latest test report: https://gpspatron.com/jammertest2023-test-report/

System Applications

- Monitoring and classification of GNSS interference over large areas
- Protection of time servers from intentional GNSS spoofing
- Synchronization accuracy monitoring/logging combined with GNSS signal quality analysis for 5G telecoms
- GNSS interference monitoring and logging of GNSS signal quality during drone operations
- Anomaly detection in raw RTK observations
- GNSS signal integrity validation at airports/seaports
- Detection of car jammers on roads on behalf of public roads administration and police
- Defense

GPSPATRON

Contacts

Maksim Barodzka

CEO @ GPSPATRON

www.gpspatron.com

mb@gpspatron.com

www.youtube.com/c/GPSPATRON

twitter.com/gpspatron