



GNSS SPOOFING FILTER

Hardware GPS anti-spoofing for drones

8 detection signals · 4g weight · 0-100 confidence score · Combat-tested

The Problem

GPS spoofing is the #1 electronic warfare threat to UAV operations.



Hijacked Navigation

Spoofed GPS signals redirect drones to enemy-controlled coordinates — causing mission failure, asset loss, or capture of the aircraft and its payload.



Undetected Position Drift

Slow-drift spoofing gradually shifts the drone's position without triggering any alarm. The aircraft silently deviates from its planned route.



No Smart Recovery

When jamming ends, standard flight controllers accept the first GPS fix available — even if it's still spoofed. This leads to cascading failures.



Zero EW Forensics

Standard autopilots don't log spoofing or jamming events. Operators have no data to understand what went wrong or improve future flights.

The Solution

AirDroper GNSS Spoofing Filter

A lightweight hardware module between your GPS receiver and flight controller. It analyzes raw GNSS data using 8 independent physics-based detection signals, computes a real-time confidence score, and blocks spoofed fixes — automatically switching to dead reckoning when needed.

8

Detection
Signals

4g

Total
Weight

20+

EW Systems
Tested

0-100

Confidence
Score

Detection is physics-based, not signature-based — works against any EW system, including those not yet deployed.

8 Detection Signals

Each signal is independently weighted. Together they produce a 0-100 confidence score.

1

SNR Anomalies

Abnormal signal-to-noise spikes from ground-based spoofing transmitters.

5

GDOP Changes

Abnormal shifts in satellite geometry dilution of precision.

2

Pseudorange Residuals

Inconsistencies in measured vs. expected satellite distance.

6

GPS Time Drift

Clock deviation from expected GNSS time references.

3

SNR Temporal Correlation

Unnatural signal uniformity over time — real satellites vary.

7

Velocity-Position Mismatch

Reported speed doesn't match actual position changes.

4

Heading Reversals

Sudden 180° heading flips without corresponding maneuver.

8

Clock Bias

Receiver clock offset exceeding normal operational bounds.

+ South-hemisphere satellite hard block for additional protection

Core Features

Built for the battlefield, tested in the field



Spoofing Confidence Score

0-100 score from all active signals in real time — not just a binary alarm. Know exactly how suspicious the GNSS data is.



Auto-Recovery & Geo-Fence

Hot/cold restart watchdog with configurable geo-fence up to 2,000 km. Smart rejoin validates signal quality before restoring GPS.



Real-Time MAVLink Telemetry

Streams NAMED_VALUE_INT confidence score and detection reasons to your GCS. Monitor live in Mission Planner.



Tamper-Proof Firmware

Encrypted firmware unique per board hardware ID. Read-protected flash (RDP1) triggers mass erase on extraction.



Wide Receiver Support

u-blox M8/M9/M10/F9/F10 and Unicore UM980/UM981/UM982. Auto-configures u-blox at boot.



ArduPilot-Native Logging

Spoofing events logged as STATUSTEXT in SD-card dataflash. Review alongside your regular flight logs.

With Filter vs Without

What happens when GPS spoofing hits your drone

| SCENARIO | WITHOUT FILTER | WITH AIRDROPER |
|----------------------------------|------------------------------------|--|
| GPS spoofing attack | Flies to wrong location | Blocks spoofed data, holds position |
| GNSS jamming | Loses GPS, drifts or crashes | Switches to dead-reckoning (DR1) |
| Slow position drift | Undetected — flies off course | Geo-fence detects drift, triggers DR1 |
| GPS recovery after attack | Accepts first fix (may be spoofed) | Validates signal quality before rejoin |
| Post-flight analysis | No spoofing data recorded | Full event log in SD-card dataflash |



Battle-Tested Against Real EW

Tested against 20+ electronic warfare systems in real combat conditions.

UKRAINIAN EW

GPS Spoofing:

Lima, Patelnia, Pokrova

GNSS Jamming:

Bukovel, Nota, Damba, Enclave,
Enclave-Malyuk

Drone Suppression:

Dandelion, PARASOL, Piranha AVD
360

RUSSIAN EW

GPS Spoofing:

Pole-21 (Field-21), Shipovnik-Aero

GNSS Jamming:

R-330Zh Zhitel, Borisoglebsk-2

Other:

Krasukha-2/4, Leer-3, Murmansk-
BN, Repellent-1, Infauna

OTHER / FUTURE

Belarusian:

Groza (KB Radar)

**Detection is physics-based,
not signature-based.**

Works against any EW system that
affects GNSS signals — including
systems not yet deployed.

How It Works

From unboxing to protection in minutes

1

Buy & Activate

Purchase the filter board. Enter your license key in the Windows provisioning app and flash the encrypted firmware via ST-Link V2 / SWD.

2

Install

Wire the filter between your GPS receiver and flight controller. Power on — the filter is transparent to normal operations until spoofing is detected.

3

Fly Protected

The filter continuously analyzes GNSS signals across all 8 detection channels. When spoofing is detected, it blocks the bad data and triggers dead reckoning.

4

Analyze

Open your ArduPilot SD-card dataflash log in Mission Planner. Spoofing events appear as STATUSTEXT entries with reason, confidence, and duration.



Hardware & Integration

| | |
|--------------------------|--|
| Processor | STM32F401CCU6 (BlackPill) |
| Dimensions | 53 × 23 mm · 4 grams — fits any airframe |
| Power | Low-power, USB or board supply |
| Protocol | MAVLink2 @ 115200 baud — ArduPilot 4.6.1+ |
| GPS Receivers | u-blox M8/M9/M10/F9/F10, Unicore UM980/UM981/UM982 |
| Firmware Security | Encrypted per-board unique ID, RDP1 flash protection |
| Configuration | Tunable via Mission Planner MAVLink parameters |
| Provisioning | Windows app + ST-Link V2 / SWD programmer |
| Telemetry | NAMED_VALUE_INT + STATUSTEXT to GCS in real time |

Why AirDroper



Only Physics-Based Solution

Not signature-based. Detects spoofing from any EW system, including those not yet deployed. No database updates needed.



Combat-Proven

Tested against 20+ real EW systems across Ukrainian and Russian electronic warfare platforms in active conflict zones.



Ultra-Lightweight

4 grams total. No additional processing load on the flight controller. Transparent when GPS is clean.



Widest Receiver Support

Works with u-blox and Unicore receivers — the broadest GPS compatibility of any anti-spoofing filter on the market.



Unclonable Hardware

Each board has a unique encrypted firmware tied to its hardware ID. RDP1 protection means it can't be reverse-engineered.



Full Observability

Real-time MAVLink telemetry, confidence scoring, and post-flight log analysis — complete EW situational awareness.

Market Opportunity



Military & Defense

Armed forces worldwide need GPS anti-spoofing for reconnaissance, logistics, and strike UAVs. The growing EW threat drives immediate procurement urgency.



Commercial Drone Operators

Delivery, surveying, agriculture, and inspection fleets are vulnerable to GPS interference near conflict zones and urban centers.



Humanitarian & NGO

Aid delivery drones in conflict zones face active EW. Reliable navigation under EW conditions directly impacts mission success.



OEM / Drone Manufacturers

Embedded anti-spoofing as a factory feature for new drone platforms. Hardware-level GPS protection as a product differentiator.

\$ Pricing & Business Model

GPS Spoofing Filter Board

\$200

per board · license included

STM32F401CC BlackPill · 4g · 53x23 mm
Encrypted firmware · License key activation



Hardware Sales

Direct B2C and B2B board sales via airdroper.org. Volume pricing for fleet operators and defense procurement.



Firmware Licensing

Each board requires a unique encrypted license key. Per-unit provisioning creates recurring customer touchpoint.



OEM Integration

White-label and embedded licensing for drone manufacturers. Factory-integrated anti-spoofing at scale.



PROTECT YOUR FLEET

Hardware GPS anti-spoofing
combat-proven, plug-and-play.



gps.airdroper.org

Scan to visit product page

airdroper.org

gps.airdroper.org · Product & Documentation
+380 97 256 3273 · info@airdroper.org