Adding Resilience and Accuracy to GNSS (Updated)

Heiko Gerstung
Managing Director , Meinberg
heiko.gerstung@meinberg.de

WSTS 2023
Vancouver, Canada

MEINBERG
The Synchronization Experts.

ITSF 2022

Agenda

GNSS Today

New Approach to Secure and Enhance GNSS

State of Test Campaigns

UTC Traceability

First Commercial Implementation

GNSS Today

Weaknesses and Vulnerabilities

GNSS Weaknesses

- Civil GNSS signals: unencrypted and vulnerable
- Widely used to synchronize critical infrastructure
  (power grids, telecom networks, financial markets, media broadcasts)

Jamming and Spoofing

- Jamming relatively easy to detect (you will notice it) and mitigate (holdover is your friend)
  - Holdover protects against Short Term Jamming and is required also for unintended GNSS reception outages
  - Long Term Jamming (e.g. in war zones) requires a different strategy

- Spoofing much more problematic unless detected (detected spoofing = jamming)

New Approach

Adding Resilience and Accuracy to GNSS

New Approach to Secure and Enhance GNSS

- Enhance GNSS resilience and performance using data aquired by a large number of reference stations which is securely transmitted via geostationary satellites to end-user-devices.
- Collect, combine and compute GNSS data from all four major constellations and all satellites
- Transmit correction values and integrity information via a secure channel (one way communication)
- Global coverage and very robust and reliable infrastructure both in space and on the ground.

Reference Stations

- Continuous reception of GNSS satellite signals at ~100 locations all around the world
- Own independent timescale used to verify/measure timing parameters of satellites
- All Reference stations together allow to collect data from every single GNSS satellite of the four constellations in real time
- Anomalies and failures (e.g. SV clock misbehaving) can be detected immediately

Control Centers

- Each Control Center runs two independent software/firmware versions and operates 24/7 in a highly redundant configuration
- Real time data of reference stations is collected, stored and analyzed in real-time
- Precise orbit and clock corrections as well as timescale computed based on the received data
- Correction values and state information for each SV of all four constellations are sent via Inmarsat to all end user devices

End User Devices

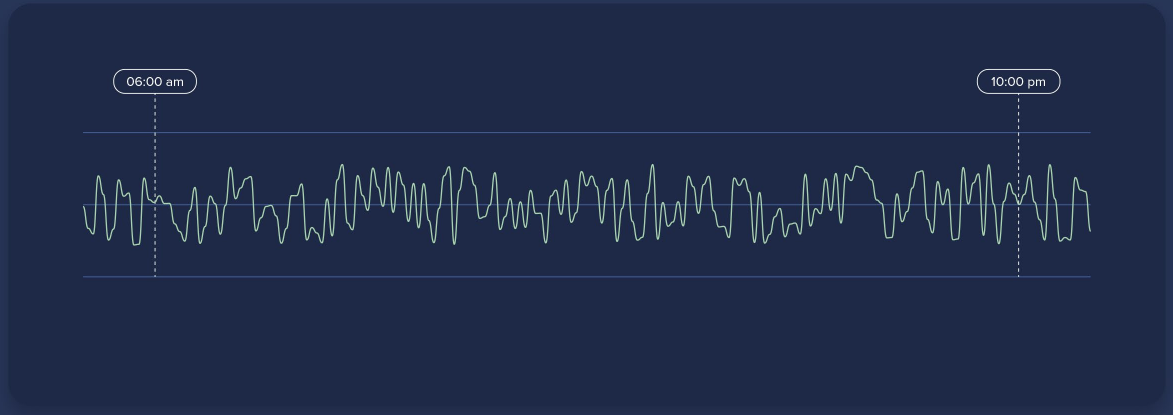
- Receiving GNSS signals for all four constellations
- In addition, L-Band transmissions from geostationary satellites received (cryptographically protected)
- Verification of integrity of received GNSS SV data to detect spoofing attacks
- Applies correction values for enhanced positioning and timing

L-Band Satellite Transmission

- GEO Satellite constellation (geostationary satellites)
- Covers almost the whole planet, only exception is the pole regions
- “Out of band” data transmission (independent of the GNSS signals)
- Proven technology used widely for global satcom applications for decades
- Data transmission protected by asymmetric cryptography (private/public keys)

State of the Tests

Spoofing Protection and
High -accuracy Measurements



Spoofing Protection

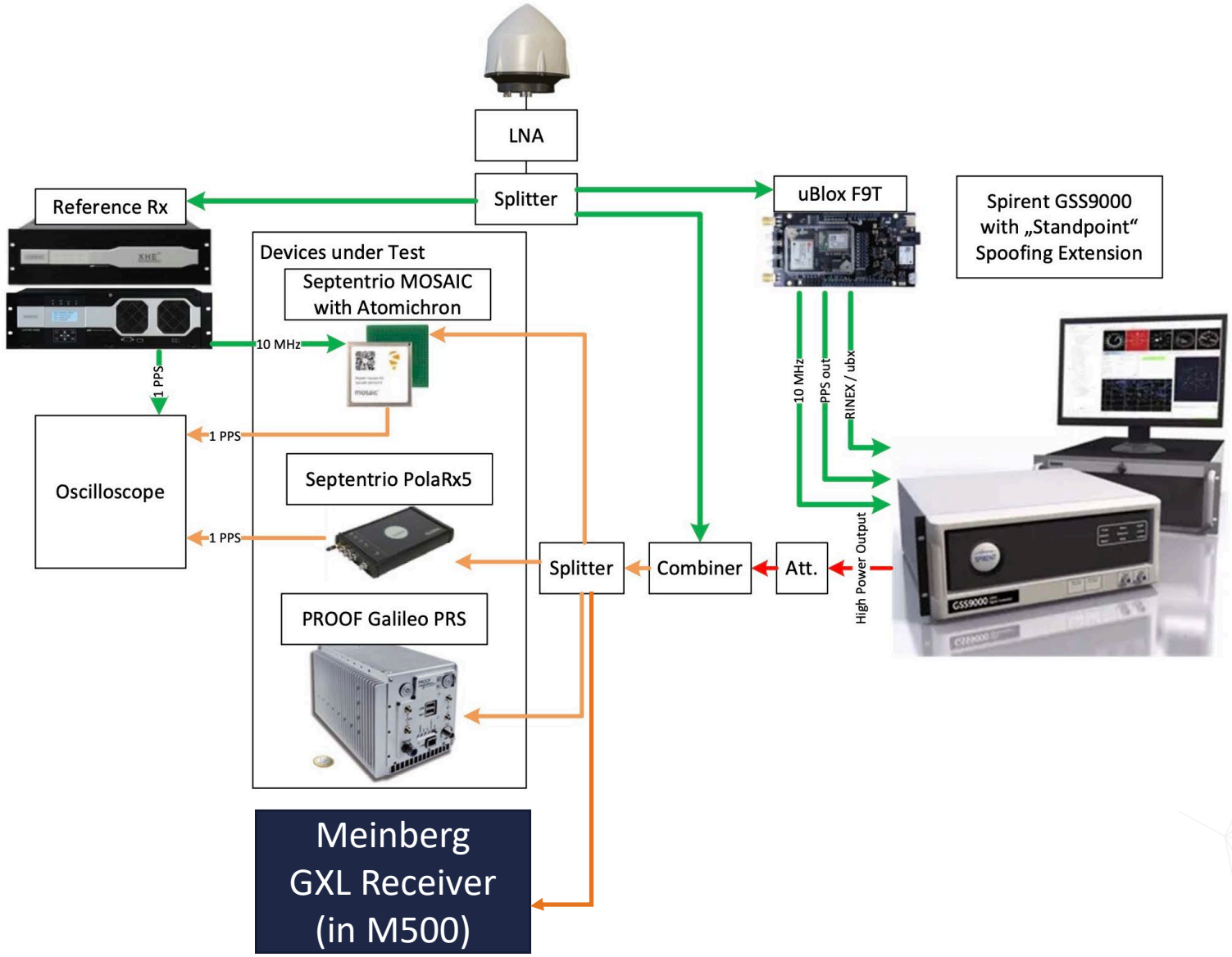
- Tests carried out in January 2023 at Fraunhofer Institute in Nuremberg
- Not easy to test
  - Most spoofing tests use GNSS simulator directly connected to antenna path
  - L-Band signal needs to be added
- Combining „real sky“ antenna with simulator output and feeding real world RINEX into simulator to synchronize it with reality
- Then starting to change things:
  - Moving position
  - Changing time

Spoofing Test Setup

Test Plan:

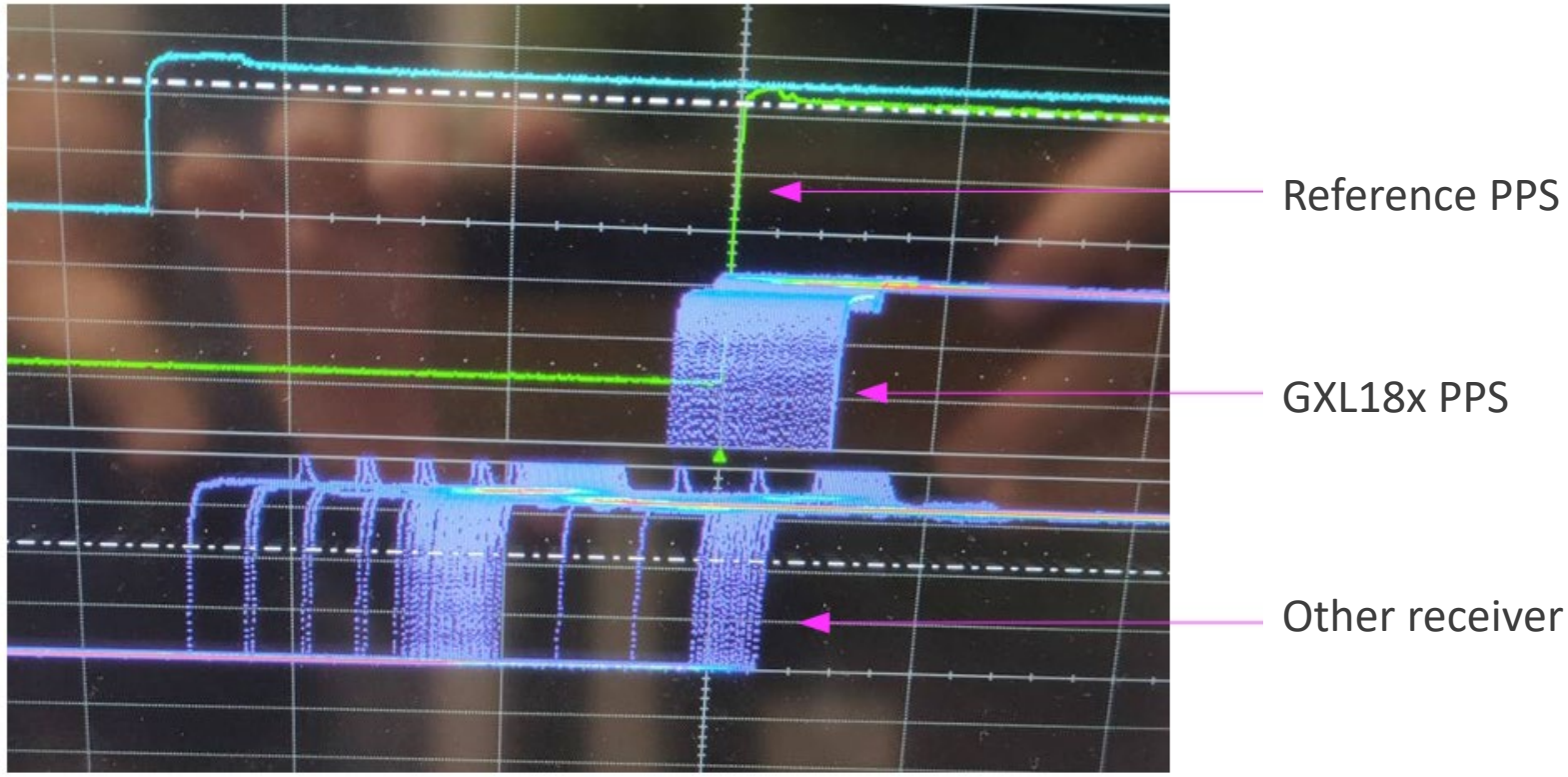
1. “Synchronize” Simulator with real world RINEX data
2. Start Simulator Output once synchronization has been established
3. Wait 60 seconds while Simulator transmitting unmodified data
4. Start to change simulator signal output for all four constellations and multiple frequencies:
    1. Move position @ 50 km/h
    2. Change time (ramp of ~3:30min until 300ns offset achieved)

Compare PPS output of GXL receiver with reference receiver (receiving real world signals only) and other receivers (receiving mixed real world / simulator signals)



Spoofing Protection - Test Results

- Meinberg RXL Receiver (uses Mosaic-T with Atomichron Features) detects spoofing attacks within 30-60 seconds after they start
- Meinberg spoofing mitigation is limiting the „damage“ to 15 ns before going into holdover:



Spoofing Protection - Test Results

- Other findings:
  - Mosaic-T built-in spoofing detection already worked well, but slower than Atomichron (e.g. RAIM, heuristic spoofing detection algorithms and OS-NMA)
  - Receivers picked up a mix of „real world“ signals and spoofed (simulator) signals → realistic scenario
  - Ignoring spoofed satellites while continuing to use unspoofed ones allows to continue to operate without having to go into holdover (and alert the user at the same time)

- Atomichron advantages:
  - Secures all four major constellations
  - will speed up detection of spoofing attacks (30s vs. 240s for OS-NMA for example)
    - Modification underway to further increase the update rate
  - allows to mitigate an attack by ignoring the spoofed satellites
  - Enables the receiver to cold start when under attack

First Commercial Implementation

Securing and Hardening GNSS for Timing

First Implementation in 2023

- Commercial Service with SLAs and Customer Support

- Multiconstellation + Multiband GNSS receiver module based on commercially available GNSS module
  - Already included protection against spoofing and jamming in its base version
  - Special Firmware developed by GNSS module manufacturer to receive and decode L-Band Transmissions
  - Receiver Module verifies status of NMA and takes correction data into account to improve timing

Thank You!

MEINBERG

The Synchronization Experts.

Heiko Gerstung

Managing Director, Meinberg

heiko.gerstung@meinberg.de