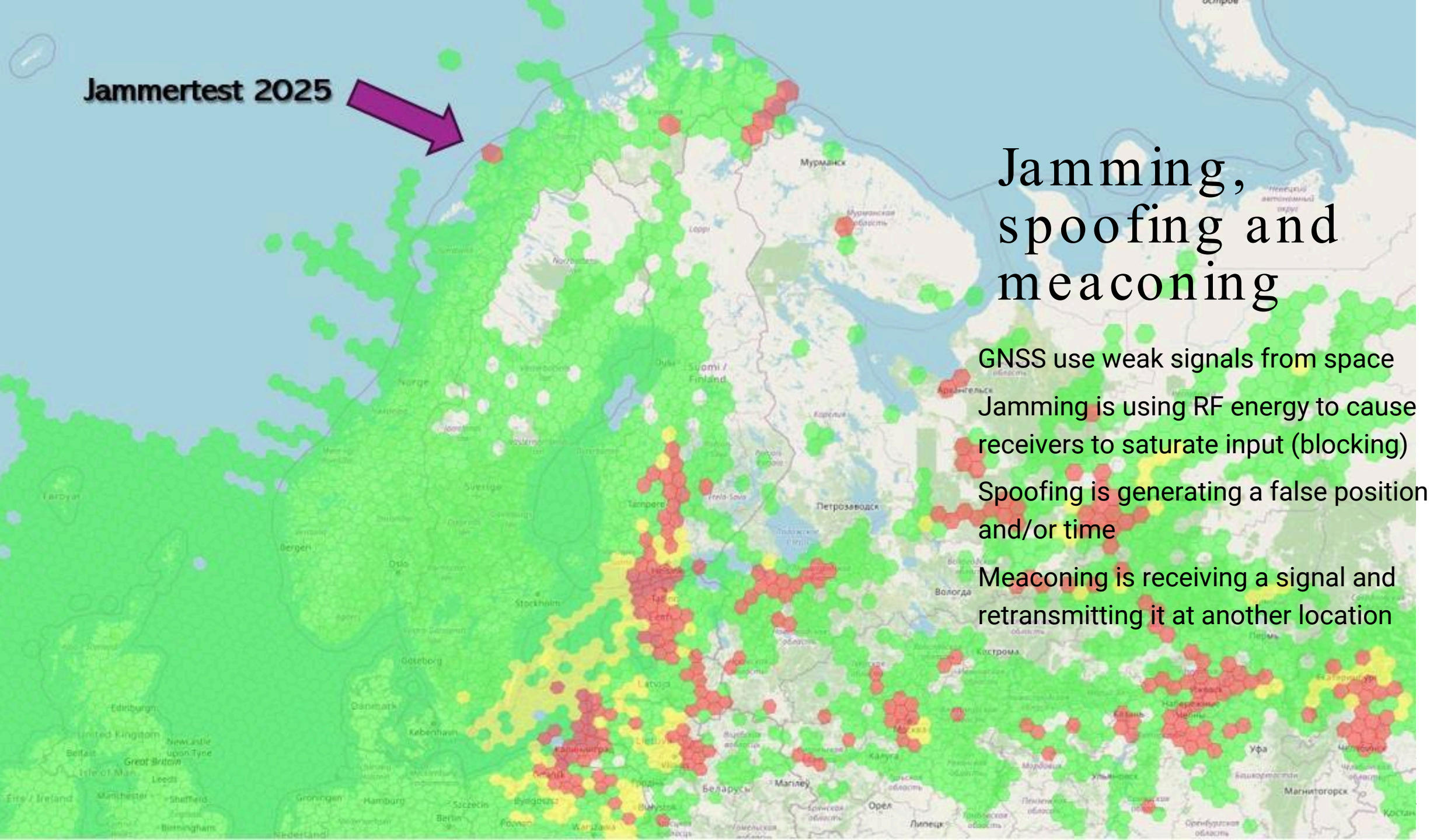
Detecting GNSS spoofing in a hostile environment

Magnus Danielson, Net Insight
Based on presentation done with Erillisverkot at ITSF by Hans Sjöstrand and Simo Hallikainen

netinsight



Jamming, spoofing and meaconing

GNSS use weak signals from space

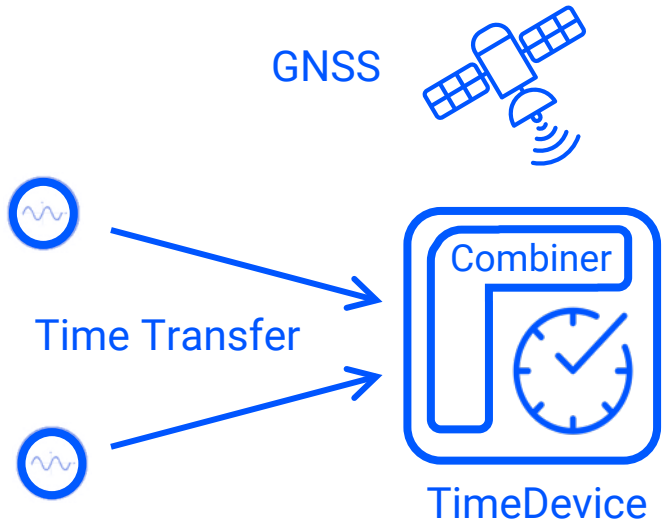
Jamming is using RF energy to cause receivers to saturate input (blocking)

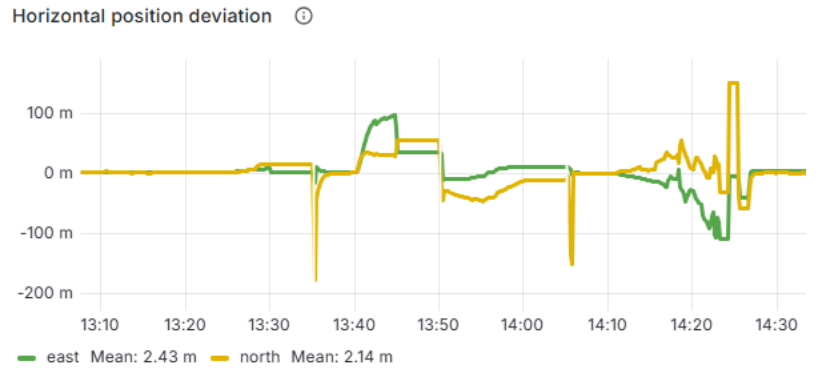
Spoofing is generating a false position and/or time

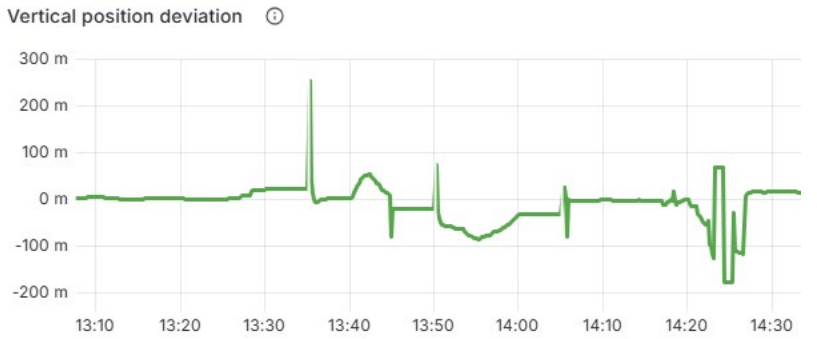
Meaconing is receiving a signal and retransmitting it at another location

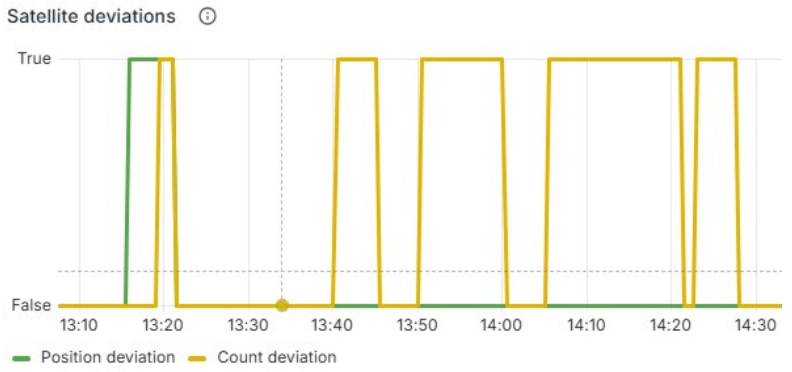
Timing redundancy

Jammertest case 2.3.12-15 : Time spoofing Flying ”drone scenario”







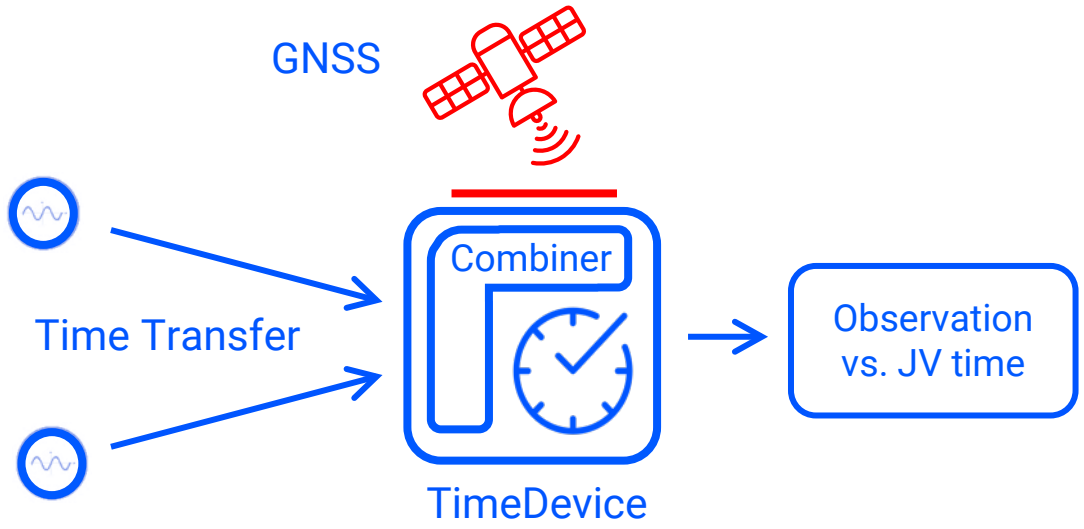


- The TimeDevice uses a combiner function:
  - GNSS time = primary source
  - network source time = backup

- The TimeDevice GNSS receiver has reasons to be suspicious
  - Location on a very stationary device comes and goes,
  - Satellites appear out of nowhere …

Timing redundancy

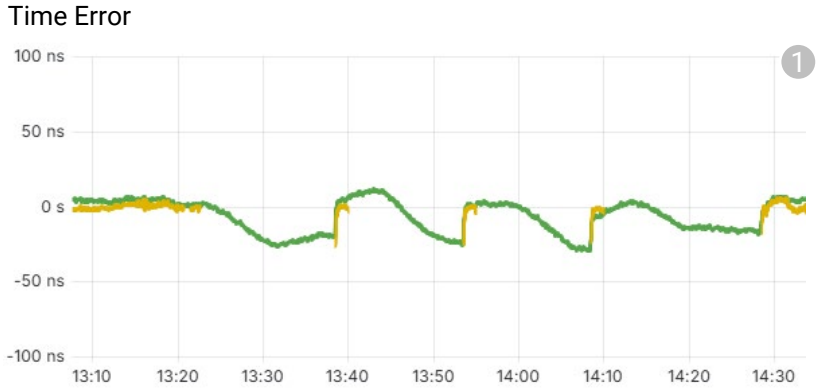
Jammertest case 2.3.12-15 : Time spoofing Flying ”drone scenario”



- The TimeDevice:
  - Abandons GNSS time before it gets compromised
  - Goes back to GNSS time when it’s considered as a primary source

- The TimeDevice maintains better than 30 ns accuracy also in disturbed circumstances.

Timing redundancy is already mandatory for Swedish mobile and critical networks



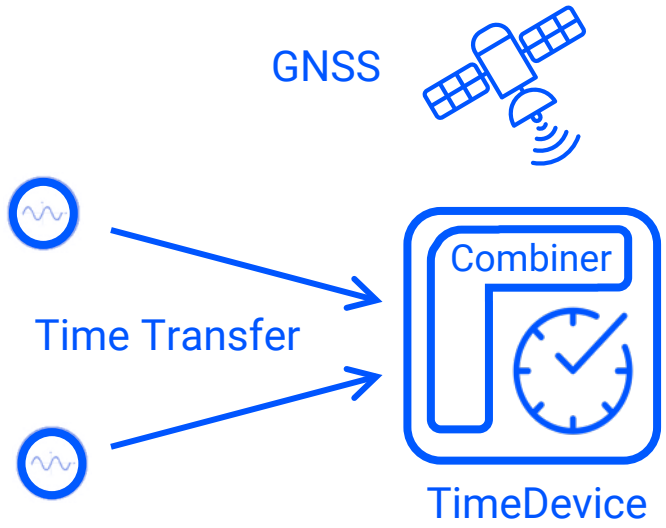
1 Network time was actually offset
20ns to better follow events.

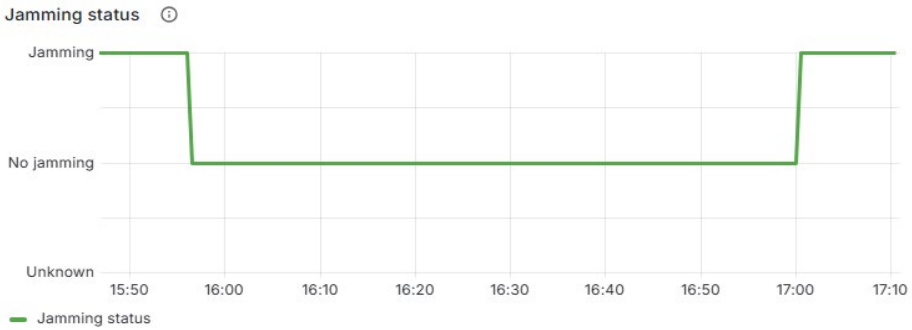
2 Extremely stressed circumstances, a few minutes between testcases etc.

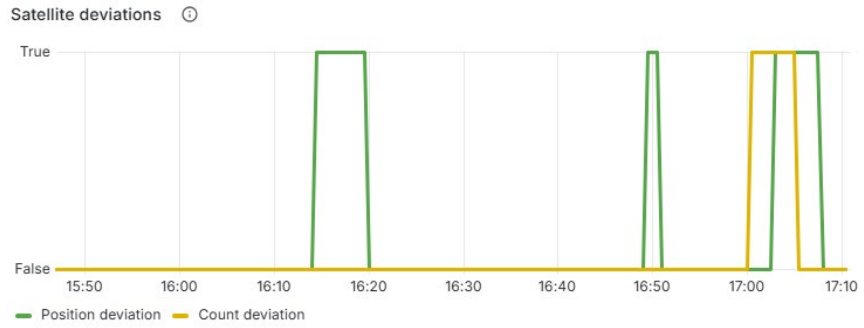
(JV) Justervesenet - Norwegian Metrology Service, where supplying an undisturbed PPS

Spoofing resilience

Jammertest case 2.3.17 : Longer period with drifting position and time spoofing

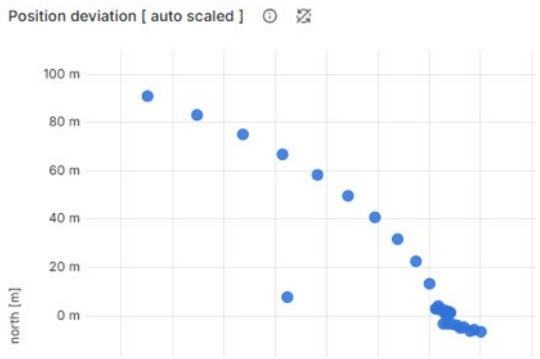






- The TimeDevice uses:
  - GNSS time = primary source
  - Network source time = backup

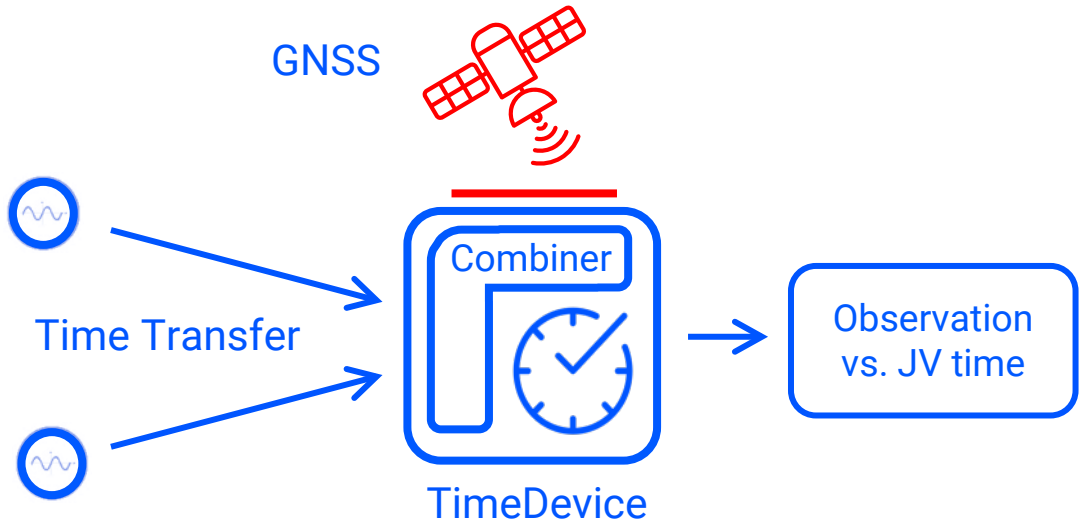
- The GNSS receiver function is now fairly comfortable
  - no major cause for alarm
  - Jamming situation is gone and GNSS seems reasonably trustworthy …



And we actually decreased spoofing sensitivity to get better data.

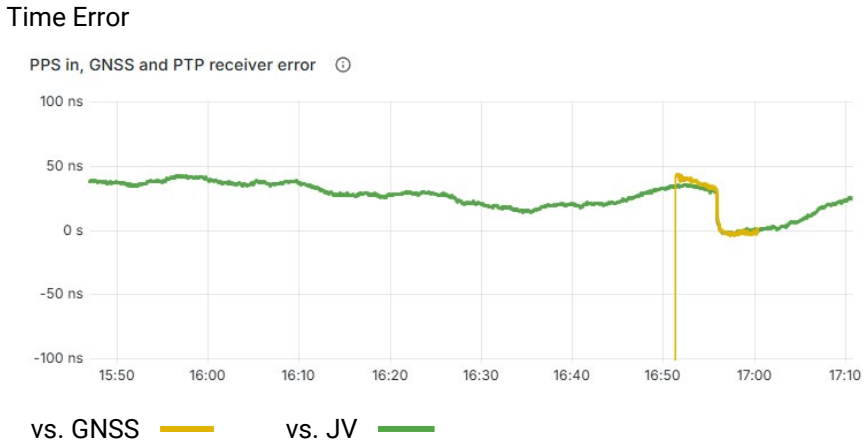
Spoofing resilience

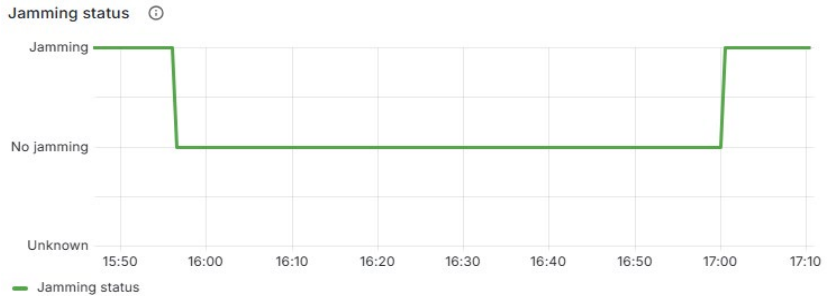
Jammertest case 2.3.17 : Longer period with drifting position and time spoofing

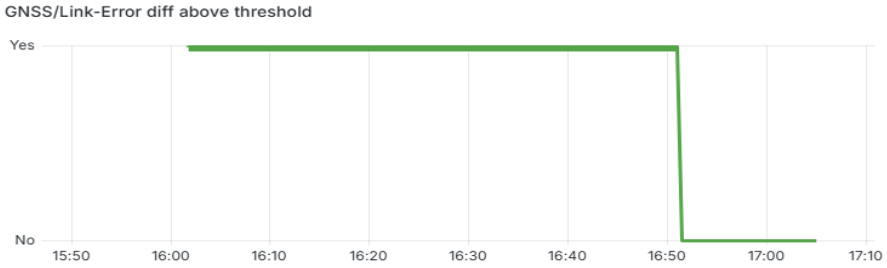


- The TimeDevice combiner performs a constant analysis of the time behavior of incoming sources
  - How is GNSS behaving?
  - How is the network time behaving?
- The network time-based spoofing analysis disqualifies the GNSS time and maintains better than 30 ns accuracy despite very sophisticated spoofing

Several sources are not only required for timing redundancy, but also for increased resiliency







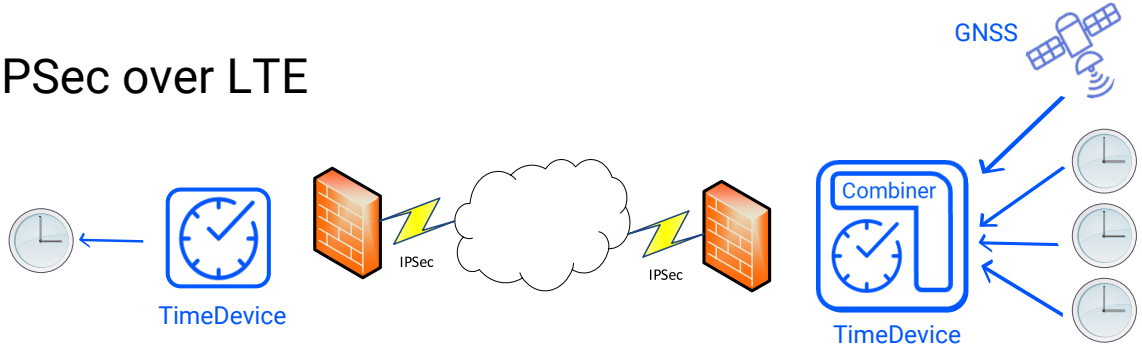
Multiple ways of detecting spoofed time received from GNSS

- Monitor several sources of time, detect suspicious changes and drop unreliable sources
- Spoofing detection algorithms in GNSS receiver chips can provide significant help when they work reliably.
- When all the GNSS-based time sources are untrusted, use either local holdover time or time transferred over network, compare those to GNSS-based sources to detect recovery from the situation and make decisions on reuse of the GNSS-based sources based on need and situation

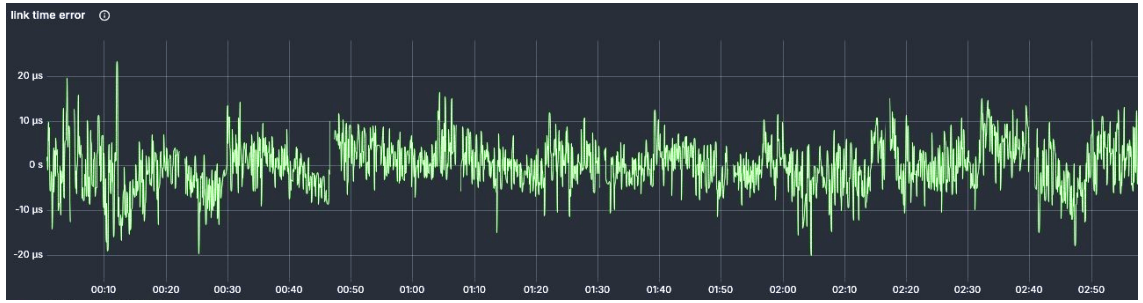
Rapid deployable time over …

± 2 ms

IPSec over LTE

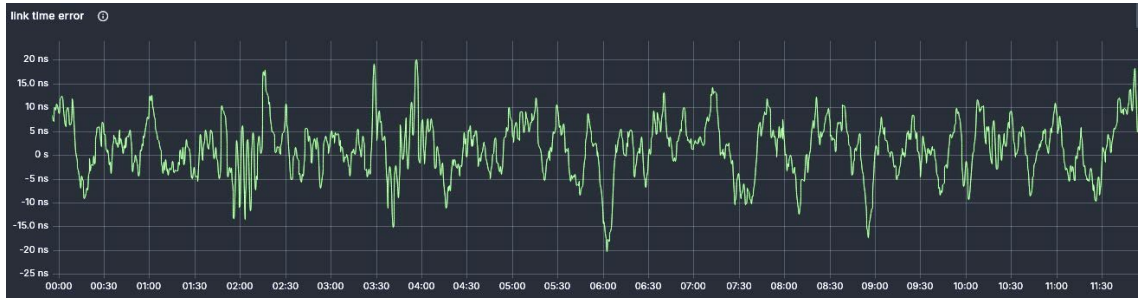


± 20 µs



IPSec over Fixed Internet

± 20 ns



L1 Quantum Key Distribution (QKD) encrypted DWDM

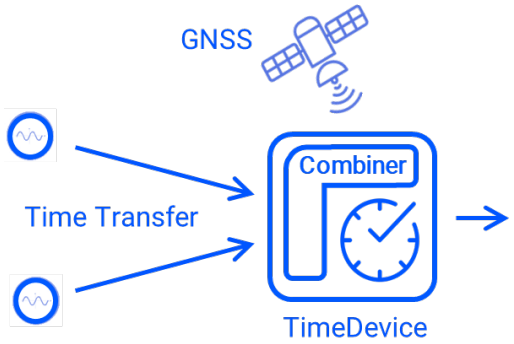
Use case: Quantum secure time transfer

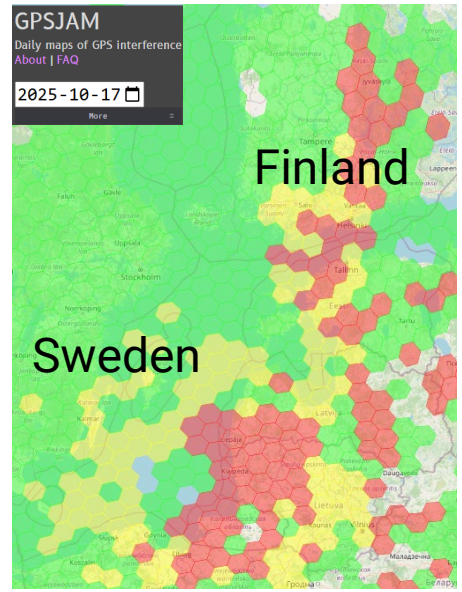
Time itself is not secret by definition, but if you include additional data like coordinates or fiber lengths, correction factors etc, then you might end up exposing locations!

Erillisverkot is a part of the NaQCI.fi consortium in the EuroQCI project, focusing on governmental use cases. Long-distance QKD links will be key to the future deployment of the actual national QCI backbone. Testing activities cover QKD devices and their integration with classical security components part of traditional communication networks.

One of our pilot use cases involve using QKD on dark submarine fibers and using a hybrid of QKD&PQC to form an L1 encrypted 400+km Zyntai based timelink in the Baltic Sea region. This setup has proven to be usable for multiple scenarios, including GNSS independent sync.

Lessons learned





Multiple sources of time are always required.

This was evaluated during Jammertest 2024 and Jammertest 2025 to handle also the most harsh circumstances

Get outside the lab, test your equipment on the field!

Spoofing & jamming affects PNT services daily in many countries, getting more technically sophisticated all the time.

Be prepared, choose your time sources wisely!

netinsight

Erillisverkot

ITSF 2025