Over-the-Air Jamming and Spoofing Tests of GNSS Timing Devices

Thomas Rødningen and Harald Hauglin
Justervesenet – Norwegian Metrology Service
Kjeller, Norway
hha@justervesenet.no

Anders Rødningsby
Norwegian Defence Research Establishment (FFI)
Kjeller, Norway

***Summary*—We present results of over-the-air jamming and spoofing interference tests against two types of commercial GNSS timing devices: a stand-alone GNSS timing receiver chip and a multi-source timeserver with an integrated GNSS disciplined (OCXO) clock. During jamming, the receiver chip showed poor and fluctuating timing, while the timeserver was protected by a high stability oscillator and eventually switched over to the external PPS input as the active sync source. During GPS L1 spoofing both devices maintained good timing as long as GLONASS signals were in use. With GLONASS disabled, the timeserver switched over to the spoofed time and position instead of selecting the available alternative sync source.**

Keywords—GNSS interference;GNSS jamming;GNSS spoofing

I. INTRODUCTION

Accurate timing signals from GNSS clocks are crucial to basic infrastructure in e.g telecommunication, finance and the power grid. Genuine GNSS signals from satellites may be overpowered by inadvertent or advertent noise (jamming) or false GNSS signals (spoofing). Here we show results from an open air GNSS jamming/spoofing exercise in September 2021 in Skibotn, Norway.

II. METHODS

A. Monitoring setup

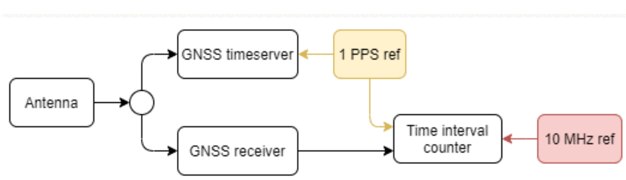

Fig. 1. Setup for monitoring timing disturbances during GNSS interference. Reference time (PPS) and frequency is provided by a chip-scale Cesium clock (CSAC) in holdover. Timing (pulse output) from the GNSS receiver is measured with a time interval counter. The GNSS timeserver has an internal measurement system that measures the timing offset between the internal timescale, GNSS timing input and external PPS input. Both GNSS devices use GPS L1 and GLONASS G1.

The monitoring setup, as displayed in fig. 1, displays how the units were connected, including the connection of reference signals, during the tests. The signal from the antenna is split using a simple GNSS signal splitter to provide both the GNSS receiver and the timeserver with RF-signals. Reference signals were generated from a chipscale atomic clock (CSAC) which was disciplined to GNSS while the real signal were available and undisturbed (this was done in the morning before the start of the tests and during the lunch break). The unit in question was a Chronos Timeport which is capable of providing 1-pulse per second (PPS) and 10 MHz as well as a few other option for time distribution. Timing performance of the GNSS receiver was monitored using a time interval counter (TIC) to compare the PPS generated from the unit to our reference signal. For the timeserver we utilised the measurement capabilities of the internal multi-reference system, which is capable of measuring the alternative timing sources against the "master"-source. Data

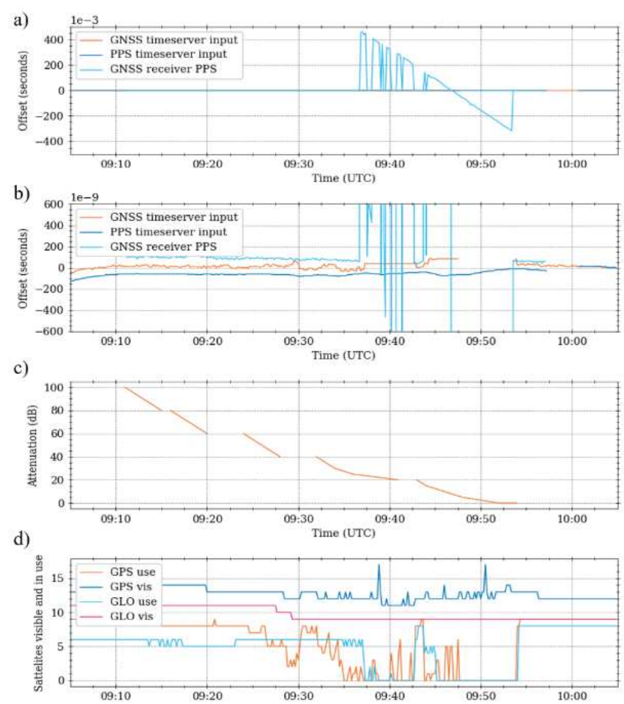

Fig. 2. Time series of timing offsets and satellite signal usage during jamming power ramp. Coarse timing offsets in a) and detailed in b) show the external reference PPS timeserver input (dark blue) and GNSS timeserver input (orange) against the timeserver internal timescale, and the stand-alone GNSS receiver PPS against the external reference PPS (light blue). Jamming transmission power attenuation is shown in panel c). Breaks in the attenuation data indicate pause in jamming signal transmission. Timeserver satellite visibility and usage for GPS/GLONASS is shown in panel d).

is collected from the two units through the available mechanisms and logs and later analysed using python scripts.

Fig. 3. Timeserver change of position during jamming represented on map. The signal degradation experienced by the timeserver during the jamming scenario caused the position reported by the timeserver to change by several hundred meters for as long as the interference persisted.

B. *Jamming interference ramp-up*

The generated jamming interference signal, covering GPS L1, L2, L5 and GLONASS G1, was transmitted with a gradually increasing signal strength over a range of 100 dB up to a maximum of 0.1 W. The applied attenuation can be seen in figure 2c, the gaps in the plot indicate pauses in the interference transmissions due to swapping of attenuators in the transmission chain.

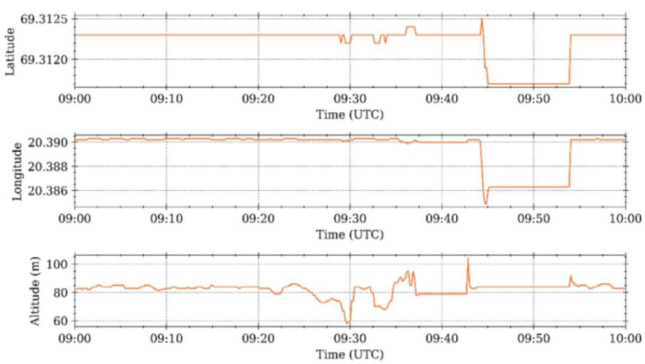

Fig. 4. Timeserver change of position during jamming. The signal degradation experienced by the timeserver during the jamming scenario caused the position reported by the timeserver to change by several hundred meters for as long as the interference persisted.

C. *Incoherent GPS L1 spoofing*

A GPS L1 spoofing signal was generated in advance using easily available software and replayed using a software defined radio (SDR). The spoofing signal did not use GPS clock and ephemeris parameters matching the actual live-sky constellation, making an incoherent spoofing scenario. The transmitted spoofing signal corresponded to a position jump of approx. 400 km and roughly two weeks backwards in time from the time of the spoofing event.

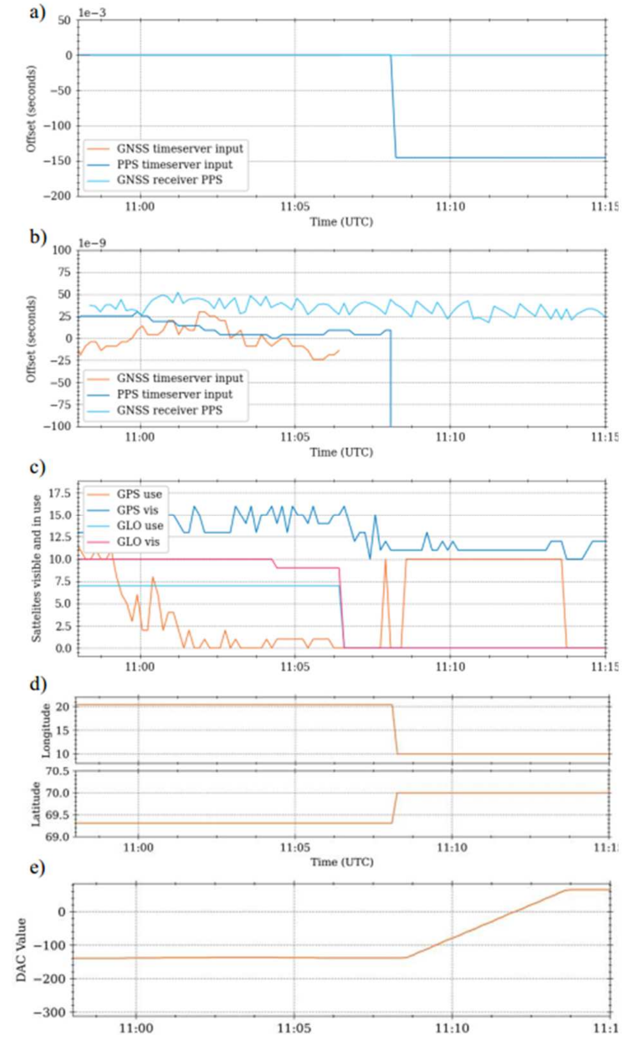

Fig. 5. Timing offsets, position change, satellite signal usage and oscillator steering during incoherent GPS L1 spoofing. Coarse timing offsets in a) and detailed in b) show the external reference PPS timeserver input (dark blue) and GNSS timeserver input (orange) against the timeserver internal timescale, and the stand-alone GNSS receiver PPS against the external reference PPS (light blue). Timeserver satellite visibility and usage for GPS/GLONASS is shown in panel c). GLONASS tracking was disabled at 11:06. Panel d) shows the logged coordinates of the GNSS timeserver. Panel e) shows OCXO oscillator DAC steering values.

III. RESULTS

A. *Jamming*

Timing disturbances during jamming are shown in fig. 2. Note that the ‘simple’ GNSS receiver chip has timing errors in the 100s of milliseconds and an internal clock with a relative rate error of 10^{-3}. The timeserver switched to external PPS input as the selected external sync source at 09:38 and back again to GNSS at 09:52 when jamming was switched off. Both units recovered gracefully within a few minutes after the interference ended. Even though jamming is usually considered a bit of an on/off-problem (the signal is available or blocked) our observations indicate that the biggest problem occurs when the jamming signal is transmitted at such a level as to severely degrade the available signals, but not completely block them.

Fig. 6. Position change during spoofing. The position change that occurred during the spoofing scenario displayed on a map. The change in position is approximately 400 km.

B. Spoofing

Timing disturbances, signal/satellite usage and logged positions during GPS L1 spoofing are shown in fig. 3. Note that both the simple GNSS receiver chip and the GNSS timeserver were initially configured to use both GPS and GLONASS. The GNSS receiver maintained its timing and position during GPS spoofing. When the GNSS timeserver was reconfigured to only use GPS (at 11:06) it accepted the spoofed position and timescale within a couple of minutes. The approximately 150 ms jump in the external PPS timeserver input against the timeserver timescale (at 11:08) is likely an arbitrary offset (modulo an integer number of seconds) between correct GNSS timing and the free running SDR spoofer clock. This time the timeserver did not recover gracefully from the spoofing interference and required a cold-start of the internal GNSS receiver to restore normal operation after end of spoofing signal transmission.

IV. Conclusions

Both the tested units have proven to be vulnerable to GNSS interference in the form of both jamming and spoofing. Both units recovers gracefully from the jamming scenario, while for the spoofing it was necessary to perform a cold-boot to bring the timeserver back to normal operation. The timeserver might possibly have recovered gracefully given enough time, but due to the limited time between tests during the event did not leave enough time to do this (as a worst case it might take a unit 1-2 hours to recover from such problems as experienced by the timeserver). The most important takeaway from this work is how it highlights how even advanced units, with the option of using multiple reference signals can still be vulnerable to such simple forms of interference as these jamming and spoofing attacks represent. It is also important to note that a complex multi-reference system might not protect reliably without operator intervention during interference events. The unit simply seems to lack robust functionality to detect/switch to secondary references when problems occur. It would be beneficial to further explore techniques for interference detection capable of detecting anomalies before a performance degradation occurs and identifying parameters that can be used effectively to decide when to switch to a secondary reference source.

References

[1] T. Rødningen, GPS timing interference – Building a system for testing the effect of jamming and spoofing of GPS based timing devices, University of Oslo, 2022 (unpublished)