GNSS Spoofing Experiments

Christian Coduri, Eliana De Giuseppe and Giovanni Lombardi
Politecnico di Torino

1 INTRODUCTION

GNSS spoofing and jamming are significant issues in today's geopolitical conflicts. In May 2024, experts reported that Russia was causing disruptions to satellite navigation systems, affecting thousands of civilian flights. While the problem existed before the Russian invasion of Ukraine in February 2022, it has been worsening.

Given the importance of addressing these challenges, this report presents two analyses of GNSS data, acquired using the *GnssLogger* app by *Google*.

The initial part of the report provides a detailed analysis of the first acquisition at *Monte dei Cappuccini (TO)*. Then, the focus will shift to different experiments applied to the same data-log, which involve spoofed positions and signal delay. Following that, the report will analyze another case study, obtained in proximity of a Space Centre in the province of *Como*.

2 ANALYSIS

The first data acquisition occurred at *Monte dei Cappuccini (TO)*, with coordinates 45.0598793° N latitude and 7.6974950° E longitude, at an altitude of 270 meters above sea level. The acquisition took place on the 27th of March 2024, starting at 17:17:27 for a duration of 10 minutes without movement under cloudy weather conditions.

2.1 Pseudoranges

By analyzing the pseudorange measurements corresponding to each tracked satellite (Figure 1), it can be observed that satellites 10, 16, 23, and 27 are moving away, as highlighted by the increasing distance between them and the receiver. On the contrary, satellites 2, 8, 21, and 32 show a decreasing distance, indicating that they are approaching the receiver.

As shown in Figure 2, satellites 27 and 10 are those positioned most directly overhead, hence the distances between them and the observer vary the least, as confirmed in Figure 1.

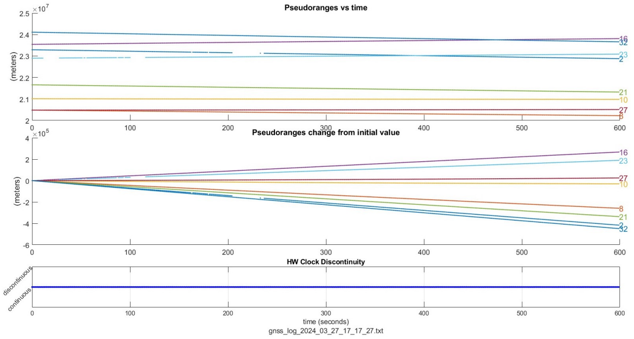

Figure 1: Pseudoranges (*Monte dei Cappuccini*)

In the third graph in Figure 1, a hardware clock discontinuity would suggest a problem in the receiver; however, in the studied case it is shown continuous hardware clock without any discontinuity.

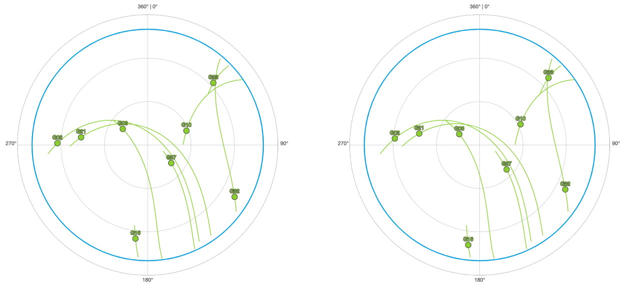

Figure 2: GPS constellation at 17:20 and 17:30 (*Monte dei Cappuccini*)

2.2 Interference

The pseudorange (PR) represents the distance between a receiver and a satellite. In Figure 3 it is observable how the pseudorange varies over time (rate of change of a pseudorange).

Given that the receiver is stationary, if there were no interference, the PR's variation would be equal to the satellite's movement in meters per second. This movement would be linear, increasing or decreasing depending on whether it is gaining distance or not.

However, in the study case, it can be observed that the lines are not linear, which is due to the influence of biases and external factors on the received signal.

The graph displays multiple gray straight lines, each representing the average pseudorange rate of a specific satellite. It can be seen how the pseudorange rate oscillates around these lines without sudden jumps, indicating minimal and contained interference.

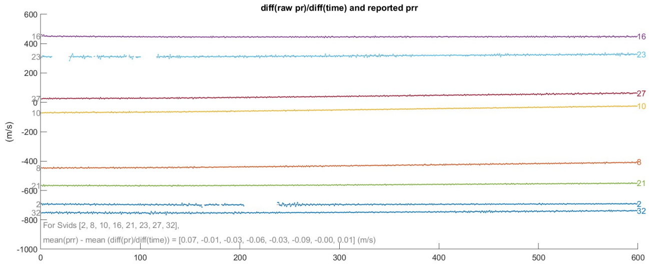

Figure 3: Pseudoranges Rates (*Monte dei Cappuccini*)

Furthermore, it is observed that satellites 2, 23, and 32 are subject to more significant fluctuations. In addition, Figure 4 illustrates the Carrier-to-Noise Ratio (C/N_0), indicating that these same satellites are the weakest GNSS signal in certain periods of time.

The acquisition location was situated close to a church positioned to the southeast. The directional information provided in the Figure 2, shows that the trajectory of satellite 32 closely aligned with the direction of the church, potentially contributing to the observed phenomena.

The presence of interference affecting the satellite 23, positioned to northeast, could potentially be attributed to environmental factors such as cloud cover or obstruction from nearby trees.

Finally, satellite 2, situated to the northwest, experiences both a weak signal and interference, likely attributed to the presence of a nearby building positioned in that direction.

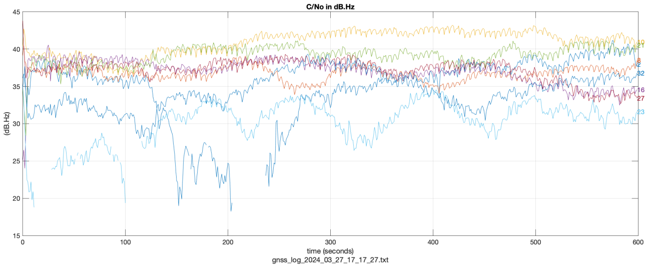

Figure 4: Carrier-to-noise Density Ratio (*Monte dei Cappuccini*)

2.3 Common Bias Clock

Furthermore the common bias clock offset and common frequency offset decrease simultaneously, meaning that the clock signal is becoming more accurate and stable overall.

2.4 Median and HDOP

Using the data obtained, the median is found to be 45.059906° N and 7.697464° E, which is accurate as the variance from the original position is $8.36 \cdot 10^{-11}$ (acquired from *Google Maps*). Additionally, the number of satellites used for the calculation is mainly equal to 8 (total number of observed GPS satellites) with an HDOP consistently below 2, indicating that the error due to satellite geometry is not high (Figure 5).

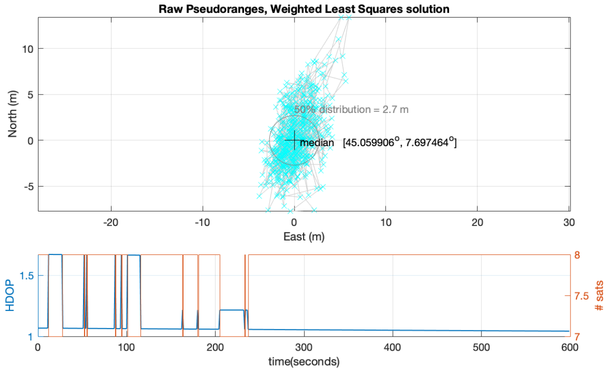

Figure 5: Median, HDOP and Number of Satellites (*Monte dei Cappuccini*)

For a more accurate analysis, a filter was applied, removing satellites 2, 23 and 32 (which were previously identified as affected by possible interference). In this case, the median is found to be 45.059927° N and 7.697455° E, with a variance from the actual position of $1.21 \cdot 10^{-8}$.

This variance is higher compared to the previous one, because of the fact that the removed satellites are peripheral (as shown in Figure 2) and therefore allowed a more accurate position calculation. This deduction is confirmed by the HDOP (error due to satellite geometry) that after the application of the filter has increased.

3 SIMULATION OF SPOOFING: POSITION

In a spoofing attack, false signals are transmitted to emulate authentic GNSS signals, potentially with altered timing, strength, or content. These signals are usually transmitted with a power higher than the original ones, to confuse victim navigation. In this experiment, however, spoofing was introduced via software. This was done by modifying the reception time to emulate spoofing behavior. Given this, there was no effect on the signals' power, and the C/N_0 plots remained unchanged in all the simulations.

3.1 Spoofed Position: Median plus an Offset

In this experiment, the median obtained from the previous analysis (Figure 5) with an added offset of 10^{-3} on longitude, latitude, and altitude, was chosen as the spoofed position.

As a result, the median shifted minimally (coordinates: 45.060905°, 7.698471°) due to the minimal spoofing offset. Additionally, the distribution's 50% range appears to be more dispersed, within a radius of 7m, compared to the 2.7m range presented in the not-spoofed case. Naturally, this also had repercussions on the graph representing the difference in latitude, longitude, and altitude from the median across all the estimated positions.

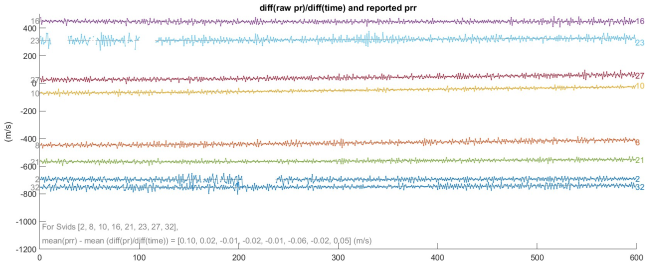

Figure 6: Spoofed Pseudoranges Rates (Median plus an Offset)

The greatest difference is visible in the graph in Figure 6. The non-linear lines, representing the pseudorange rate (PRR) after the spoofing, show wider variations compared to those in the non-spoofed case in Figure 3.

It can be observed how the PRR of each satellite (colored lines) has deviated from the average PRR of the non-spoofed measurements (gray lines). If one were to calculate the mean over the spoofed PRR, it would result in a line parallel to grey one. The distance between these two lines would define how much the PRR has changed after the spoofing.

3.2 Spoofed Position: Over the River

In this experiment, the spoofed position was selected using a point on Google Maps, situated not far from the location of data collection (coordinates: 45.061494°, 7.693911°). Consequently, the situation appears to be similar to the previous one: the median shifts slightly (45.061498°, 7.6939079), resulting with the 50% distribution within a radius of 6.8m.

The graph of PRR also appears to be similar, with contained oscillations attributed to the interference.

3.2.1 *Spoofing Detection Strategy.*

In a real scenario, the first method of spoofing detection is monitoring the power of the received GPS signals, for example considering signal to noise ratio

(C/N0). Alternatively, in the case of a device that receives only some of the spoofed signals and not all, a cross-check could be performed between different groups of antennas to assess the variation in the estimated position.

However in the analyzed scenario, since it is simulated via software and the mentioned checks cannot be performed, it could be considered that since the acquisition was done while stationary, finding a distribution of 50% of the estimated positions within a too wide radius (above a certain threshold) could indicate spoofing.

3.3 Spoofed Position: *Isla de Pascua*

In this last example of position spoofing, the selected spoofed position was *Isla de Pascua* (coordinates: -27.114410, -109.425270).

Due to the fact that this island is on the opposite side of the globe, the satellites that were approaching the receiver's position during the acquisition, after spoofing, tend to move away and vice-versa (Figure 7).

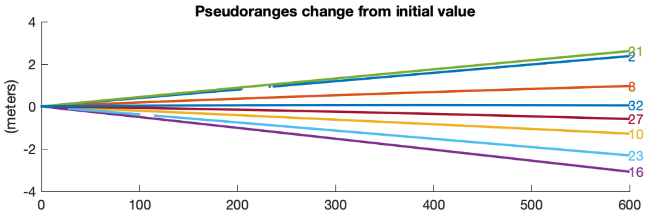

Figure 7: Spoofed Pseudoranges (*Isla de Pascua*)

Of course, the median was altered, and as a result, 50% of the distribution fell within a radius of 16.2 meters.

Finally, regarding the PRR (shown in Figure 8), the issue observed in the first experiment remained the same but more exaggerated, resulting in a significant difference between the average PRR of raw measurements and the PRR after spoofing.

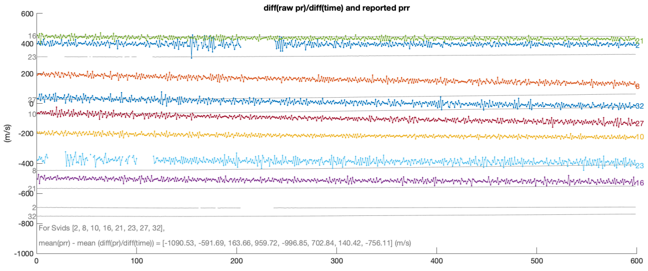

Figure 8: Spoofed Pseudoranges Rates (*Isla de Pascua*)

4 SIMULATION OF SPOOFING: DELAY

An attacker can manipulate a receiver's position estimation by introducing a delay in the spoofed GNSS signals.

The GNSS signal received includes the start time and coordinates of the satellite, which are used to calculate the pseudorange. If a delay is introduced in one or more, but not all, satellites, the receiver will compute an incorrect position.

However, in the following case all the GNSS signals are retransmitted with the same delay. Introducing a common additional delay to all measurements creates a situation analogous to having a clock that is more biased compared to the GNSS clock. The added delay acts like a constant clock offset for all received signals. Consequently, it is compensated in the user's clock bias estimation, effectively nullifying its impact on the calculated position. As a result, the estimated position remains accurate.

To confirm this, a delay of 0.001 seconds was introduced at the 100th second of acquisition. The same position where the acquisition was performed is used as the spoofed position (coordinates: 45.0598793, 7.6974950).

As expected, it can be seen from the median, in Figure 9, how the estimated position remains unchanged despite the introduced delay. However, the radius which includes half of the distribution has slightly widened.

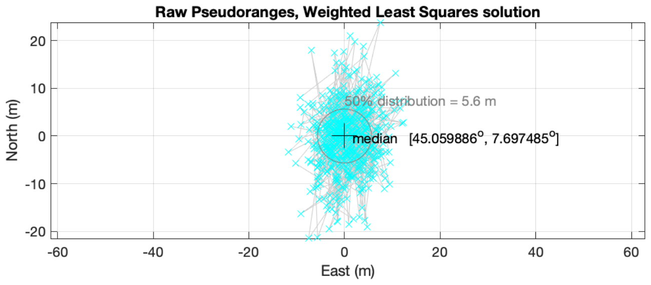

Figure 9: Distribution of Estimated Positions (Delay case)

Regarding the variation of the clock bias, it can be observed that from the 100th second, when the spoofing begins, the bias is brought to a higher value, but as time progresses, it decreases and approaches zero. Therefore, the clock bias is correctly approximating the error introduced by the delay.

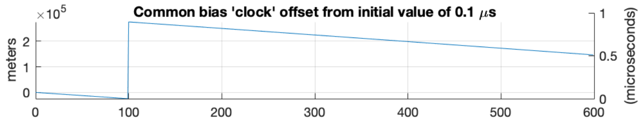

Figure 10: Clock Bias (Delay case)

While the position estimation is not affected by the delay, the computed pseudoranges change because the delay alters the perceived time of signal transmission from the satellites to the receiver. As a result, the pseudoranges, which are derived from the time difference between the signal transmission and reception, are influenced by the spoofing. The increase in all distances caused by the delay is illustrated in Figure 11.

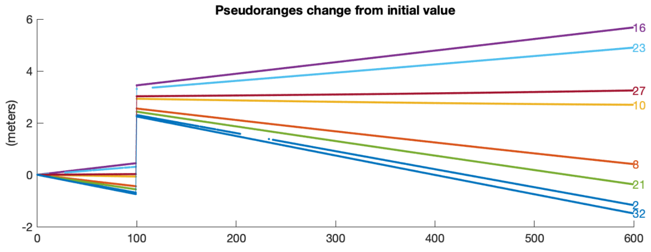

Figure 11: Pseudoranges (Delay case)

5 ANALYSIS OF AN ACQUISITION NEAR TO AN INTERFERENCE SOURCE

For this conclusive experiment, an acquisition of 5 minutes took place near the *Lario Space Centre* (coordinates: 46.158549, 9.409049), located in the province of *Como*, at a distance of approximately 500 meters from the antennas. According to information from "*telespazio.com*", the Center includes over 60 antennas capable of managing satellite services, including those used for broadcasting.

Figure 12: *Lario Space Centre* - sourced from *telespazio.com*

In the carrier-to-noise ratio graph (Figure 13), the satellites 3 and 27 consistently exhibit power levels below the 33dBHz. This indicates that the signals from these satellites are more dominated by noise, probably due to the interference near the acquisition site.

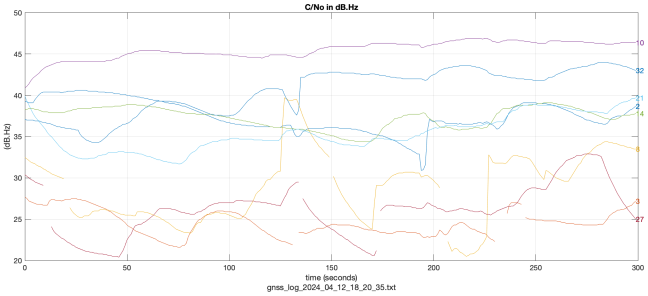

Figure 13: Carrier-to-noise Density Ratio (*Lario Space Centre*)

Furthermore, within the same graph, it is observable that all signals, with the exception of satellite 10 which demonstrates a relatively stable trend, show oscillations with rapid peaks and troughs, indicating that the source of noise is not constant. For instance, the broadcasting signals from nearby towers could intermittently interfere with the reception of GNSS signals, causing these fluctuations.

In the pseudorange rates, satellites 3, 8, and 27, which have weaker signals and more variation, exhibit pronounced oscillations. On the contrary, satellite 10 maintains consistency closest to the PRR average, reflecting its accuracy.

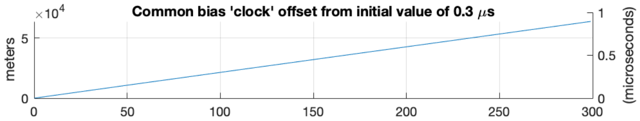

Figure 14: Clock Bias (*Lario Space Centre*)

Electromagnetic interference from the near station can disrupt GNSS signal reception, causing delays. These delays might be seen as increased clock bias by the receiver, reducing location accuracy (Figure 14).

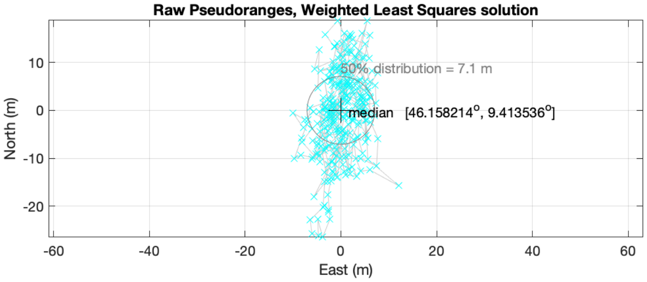

Figure 15: Distribution of Estimated Positions (*Lario Space Centre*)

In conclusion, the 50% distribution radius, measuring 7.1 meters in Figure 15, indicates a remarkable degree of inaccuracy, particularly significant as the acquisition was conducted from a stationary position. This value is similar to the results observed in the case study of spoofing over the river, suggesting a similarly compromised positioning accuracy in both scenarios.