Android GNSS measurements report

Alberto Ameglio 330946, Enrico Di Stasio 323075, Giovanni Luca Di Bella 332088
Polytechnic of Turin class: LM-32 (DM270)
01GYSUV - Wireless Security Lab

Abstract

In this laboratory, we focused on the raw analysis of GNSS signals, conducting various experiments under different conditions with particular attention to security.

1 Introduction

When a cell phone is active and has access to the GPS service, it starts receiving radiofrequency signals transmitted by a constellation of satellites orbiting the Earth. These signals contain timing and position information, allowing the phone to calculate its exact location on the Earth's surface. In 2016, Google made raw GNSS measurements[2] accessible to developers through a specific localization API. In this report, we will present some recent measurements to delve deeper into this technology and better understand its nature. These measurements were conducted using a Samsung device model SM-P613 with Android 14, instead the data logging was facilitated by the free application GnssLogger, developed by Google to continuously record and track the device's GPS position over time. For the analysis of the collected data, we utilized the GPS-Measurement-Tool [1] library written in Java and available for the MATLAB environment.

The main objective of this work is to provide a critical evaluation of the capabilities of these software tools, identifying their potentials and any limitations. Through a series of empirical experiments and comparative analyses, we aim to determine the accuracy of the obtained measurements by comparing and assessing the reliability of the results.

1.1 Project elaboration

The measurements were conducted in different locations and on different days, always using the same device with GnssLogger installed. During the various tests, unless otherwise specified, the device was exclusively used with only the active application running and nothing else in the background, in standard usage mode, and connected to the internet via Wi-Fi networks.

Regarding the settings selected on the "Home" tab page, all the readings were taken with the following features enabled: Location, GNSS Location, Measurements, Fused Location, Network Location. The various recordings were made with variable time intervals managed through "Timed Logging". Additionally, the use of the "Skyplot" tab section was very helpful for recording useful information that was later compared during the analysis phase.

The analyses were based on the result of pseudorange calculations. Pseudorange calculation in GNSS measurements involves determining the signal travel time between a satellite and a receiver, in this case, our device, using the device's local clock bias to compare frequencies and calculate an approximate distance estimate. This estimate, called pseudorange, was used to estimate the receiver's position, which requires corrections to compensate for various factors affecting the signal travel time.

The analyses were conducted using the gps-measurement-tool library, focusing mainly on the GPS constellation. This tool was indispensable for implementing certain filters that allowed us to reflect more on our recordings and to make considerations regarding the consequences of spoofing.

2 Standard conditions Readings

We start from a measurement of the 03/04/2024 done walking in open space with a very clear sky, no surrounding buildings and no sources of interference, only filters used in the Matlab script are the "FullBiasNanos ~= 0" and the "ConstellationType == 1" (limiting our observations to GPS type satellites due to inconsistencies with other constellations caused by either the Matlab script or the android device used for the measurements). During the measurements, which lasted around 10 minutes, the device was in standby and battery saving mode was switched on at the 300 seconds mark. We use this as a baseline from which to start analysing different scenarios and conditions. In the following picture the skyplot from the moment in which the measurements were taken is shown.

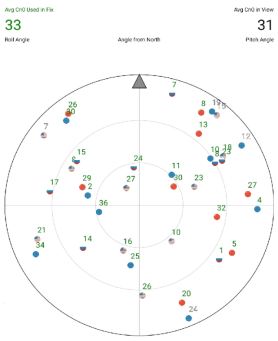

Figure 1: Skyplot of the recording from Asti

A first interesting observation we can make are the pseudoranges measured by satellite 27, which is shown to be the closest to us and also remain very constant in time as shown in "Pseudoranges vs time" and "Pseudoranges changes from initial values" plots, this is consistent with the skyplot which confirms the fact that satellite 27 is the closest to the zenith among the GPS ones. Another significant plot is the HDOP one where we can track the

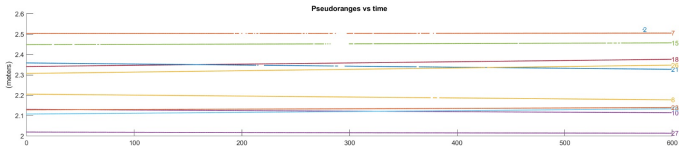

Figure 2: Pseudoranges vs Time graph

geometrical distribution of satellites, there is a clear drop in number of satellites tracked around the 300 seconds mark as shown in the pseudoranges plots discontinuities (in particular Svid: 7,15 and 21)

which leads to a peak of the HDOP and a consequent PVT estimation error, highlighted in the "Velocity States". We link this drop in number of satellites to the activation of the battery saving state that might have messed with the correct receiving of signals, causing the discontinuity. As these were measurements done in open space

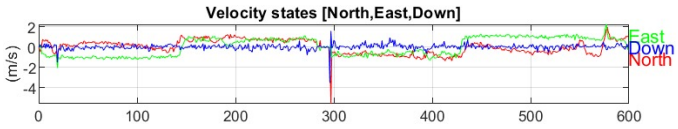

Figure 3: Velocity states

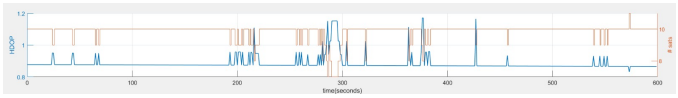

Figure 4: HDOP

without many buildings on which the signal could be reflected, the multipath phenomenon is not very present, this is shown by the fact that re-running the script with the "MultipathIndicator < 1" filter does not improve the pseudoranges at all as shown in this second version of the "Pseudoranges vs time" plot:

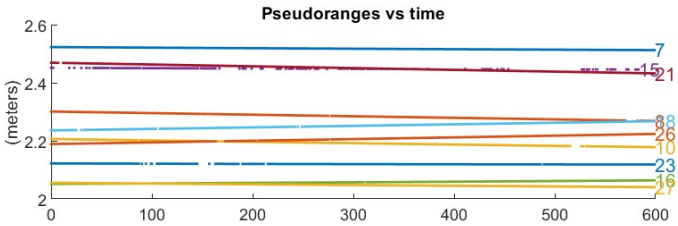

Figure 5: Pseudorange vs time Torino

2.1 Reading with source of Interference

This second set of measurements was instead taken on 07/04/2024 near a source of interference (antenna) and in clear sky conditions, the device wasn't moving and there weren't many buildings around except for the antenna, the measurements lasted 10 minutes with the android device in standby.The antenna was found on the following official list [3] and is the property of RAI. Since we couldn't turn off the antenna we couldn't establish a baseline from which to compare the interfered measurements, still, we are able to make a few observations. The presence of the antenna is evident from the "C/N0 in dB.Hz" plot where we would've expected a better performance without the interferences, in fact the plot shows many peaks in noise contributions: The interference disturbs the pseudoranges measurements which become very much discontinuous as shown in "Pseudoranges vs time" plot (dotted lines instead of continuous ones), without the external interference we would have expected to have less gaps and not for every satellite, more similar to other measurements. Once again, as for the first set of measurements, the "HDOP" plot helps in showing reduced satellite tracking: while in the first set the dip was only around the 300 seconds mark due to the activation on battery saving feature on the tracking device, here the number of tracked satellites tends to decrease very often leading to HDOP peaks which create false pseudoranges reads and

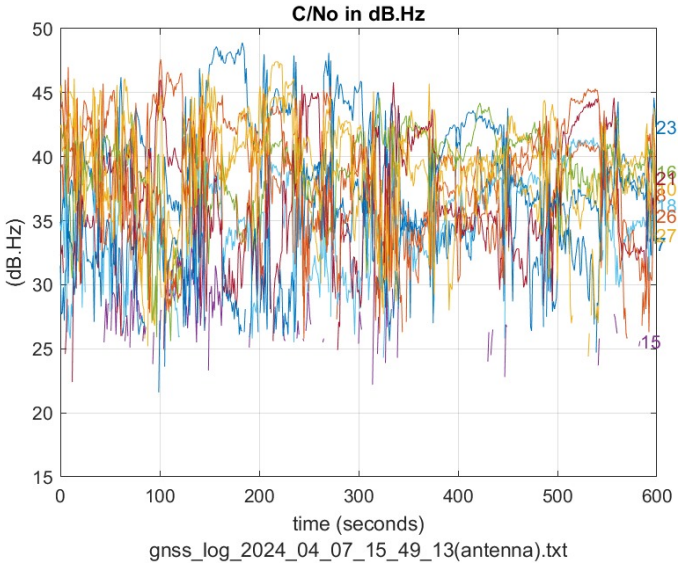

Figure 6: C/No in Db.Hz

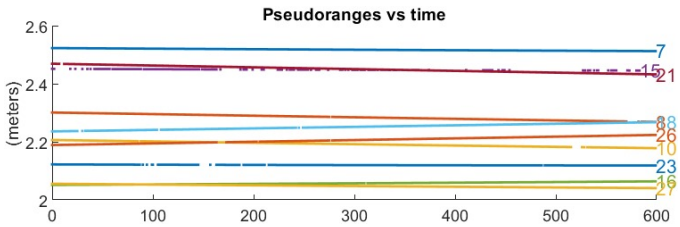

Figure 7: Pseudorange vs time

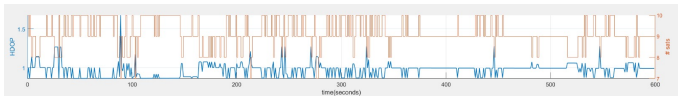

Figure 8: HDOP

therefore incorrect computed position There's a confirmation of this in the "Velocity States" and "WLS" plots which show movement (sometimes even significant) while in reality all the measurements were taken standing still near the antenna.910

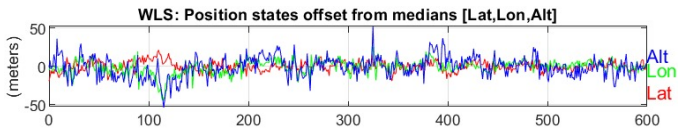

Figure 9: WLS

3 measurement comparing

In this measurement we tried to test the effect of multipath on our measurements, at this purpose we placed on a street surrounded with tall buildings to emphasize the effect as much as possible. With this condition, we took two different measurements: one standing still, while the other moving along the streets to see the change of the effect. There is a clear distinction between the two measurements in the "C/No Db.Hz" plot where:

- In the first scenario, we can clearly define the disparities among the signals from each satellite, each within a different

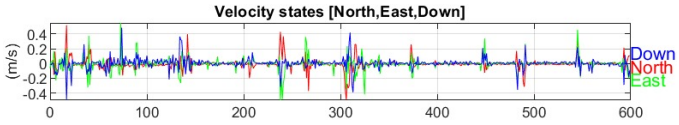

Figure 10: Velocity state

power range. Given this statement, we assume that the multipath interference uniquely affected each signal, generating a very similar behaviour for each satellite but placed in a different range of power.

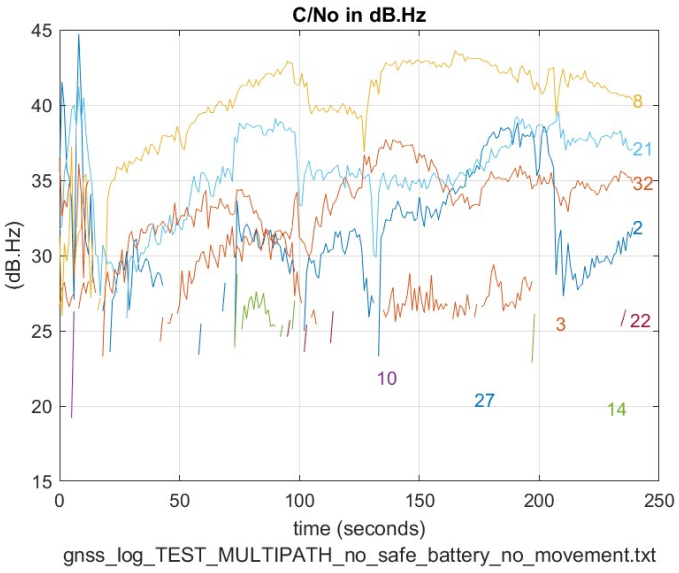

Figure 11: C/No in dB.Hz

- In the second scenario, since the device was moving along the streets each signal, alternatively, could find its own path at different time, creating a fluctuating patter over time, where certain signals increased while others decreased. For instance, signal 2 (dark blue) begins at 40 dB, then decreases gradually to 27 before rising again. Meanwhile, signal 8 (yellow) reaches the top when signal 2 is at its lowest and reaches its lowest point when 2 is at its peak.

Another interesting aspect is that, in the first analysed case, satellites 10, 27 exhibit such a weak signal that they are barely visible from the C/No plot. However, in the second case, due to the device's movement, their power has slightly increased allowing them to give better result. These observations are supported also by the "Pseudoranges vs time" plots where, in the first scenario (first image) the contribution of these satellites is almost zero, while in the second case they participated more in the measurements, evidenced by their increased participation on the plots.15

From the second measurement can be noticed a particular effect of multipath interference from the "Plot Positioning on Map" where appears a 6km outlier, that produces a distortion in the standard deviation computation. As shown in the same image15, applying the "Svid" filter we've been able to identify the satellite that generated the outlier. However, since for most of the time it gave correct measures, removing it would cause a low in the performances in

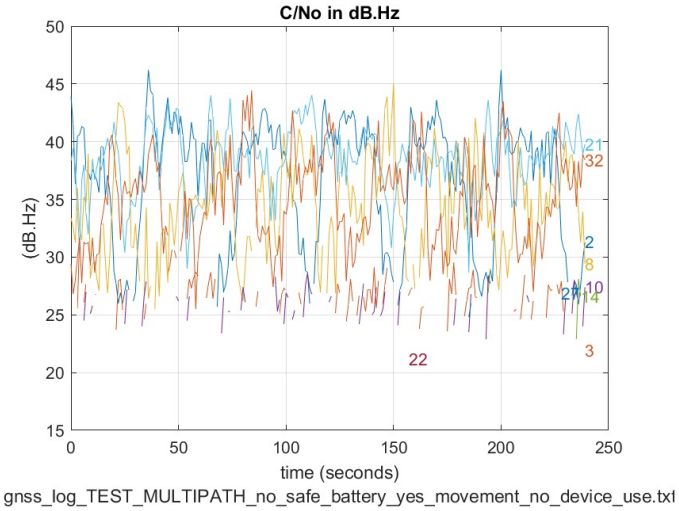

Figure 12: C/No in dB.Hz

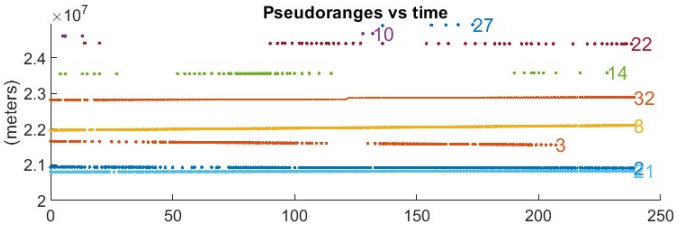

Figure 13: Pseudoranges vs Time

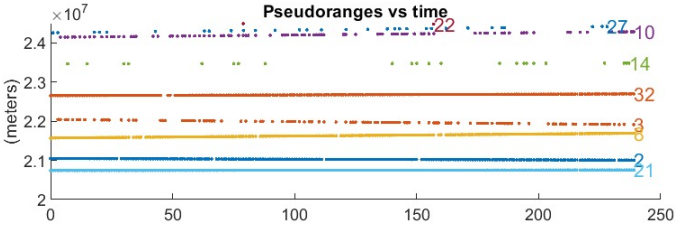

Figure 14: Pseudoranges vs Time

terms of standard deviation (from 17.3m to 22.4m) we decided to keep it.

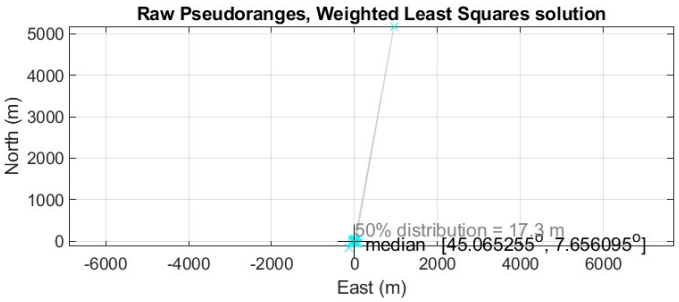

Figure 15: Raw Pseudoranges with outliers

4 jamming

.

Jamming, or intentional interference, is a type of attack in which interference signals are transmitted in the same frequency band as

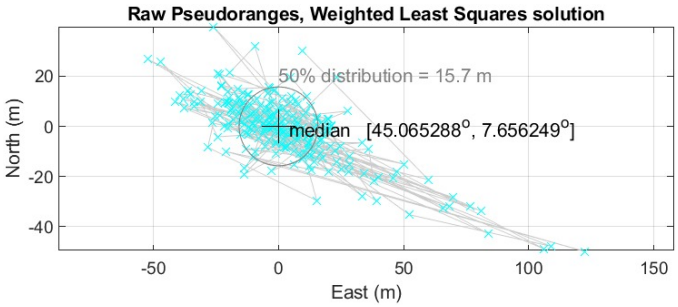

Figure 16: Raw Pseudoranges without outliers

GNSS signals to disrupt or hinder the reception of GNSS signals by receivers. This interference can be deliberately generated for harmful or hostile purposes, such as blocking communications or compromising navigation.

When jamming is present, interference signals are added to the GNSS signal, increasing the overall noise level in the system. This has a direct impact on the C/No measured by the GNSS receiver. Since the carrier signal remains constant while the noise increases, the signal-to-noise ratio decreases.

Therefore, during jamming, a steep decrease in C/No is expected compared to its normal condition without interference. This can negatively affect the performance of the GNSS receiver, reducing its ability to acquire and track satellite signals and compromising the accuracy and reliability of position and time measurements.

The effects of jamming on C/No can vary depending on the power and frequency of the interference, the sensitivity of the GNSS receiver, and other environmental and system factors. In some cases, jamming can be so intense as to render the GNSS signal completely unusable, while in other cases it may be less harmful but still negatively affect the overall performance of the navigation system.

We wanted to test this property without using an actual jammer, but by using a common household appliance, a microwave oven. In fact, a microwave oven operates using high-frequency electromagnetic waves, known as microwaves, to heat and cook food. These microwaves have frequencies ranging from 1 GHz, corresponding to a wavelength of 30 cm, to 300 GHz, or 1 mm wavelength. The waves used by satellite systems are radio waves ranging from 1 GHz to 300 GHz. Therefore, we expect that by placing the detection device sufficiently close to the active microwave, a significant change in the behavior of C/No will be observed.

Our experiment was conducted on April 7, 2024, starting at 5:40 PM for a duration of 10 minutes on a fairly clear day, with the device under standard conditions as described here1. The device was always placed near the front of the microwave , which operated in 2-minute intervals at a power of 800 W.

The graph presented here shows what was expected; sudden peaks can be observed at the 120th and 360th seconds, and abrupt increases at the 240th and 480th seconds, with a difference of 5-10 dBHz between them. This change can be considered the result of the microwave activation at the 120th and 360th seconds and its subsequent deactivation at the 240th and 480th seconds, as previously predicted. The remaining graphs are also significant to observe. The pseudoranges represent several significant jumps for

Figure 17: Experiment conduct

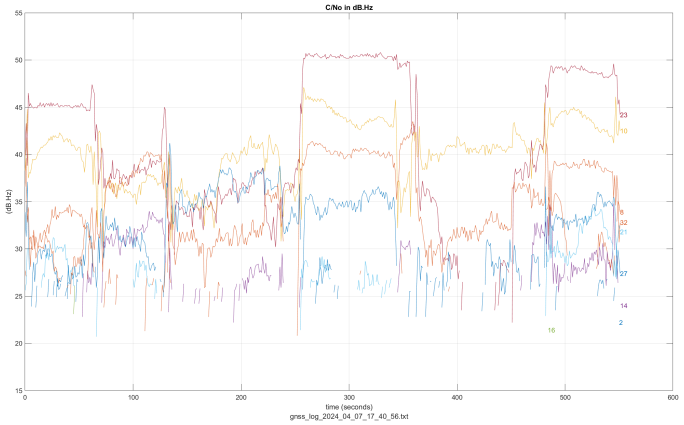

Figure 18: C/No in Db.Hz

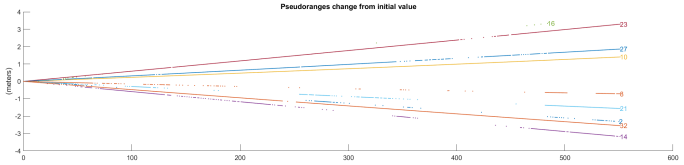

Figure 19: Pseudoranges change form initial value

most of the GPS constellation satellites at that moment, except for satellites 23, 10, and 32. This reinforces the observation made in the graph presented here18, as these satellites precisely show a clear oscillation at the previously described moments. The WLS graph shows movements, and there is also a jump from the 380th second,

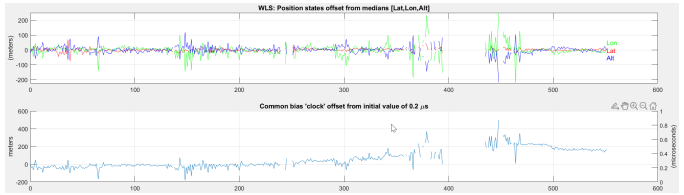

Figure 20: WLS graph

attributable to an inability due to lack of data to estimate the position, also confirmed by the Common bias clock graph. The HDOP

graph ,shows a visible increase, especially when the microwave

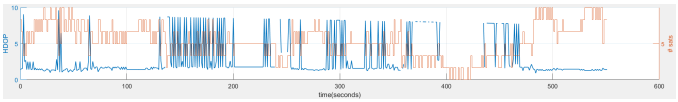

Figure 21: HDOP graph

was active, resulting in a probable error in the PVT estimation. It is even clearer at the 480th second, after the microwave was turned off for the last time, that the HDOP returns to levels that we can consider good for a proper PVT estimation.

The graph presented here ,shows a standard deviation of 14.6

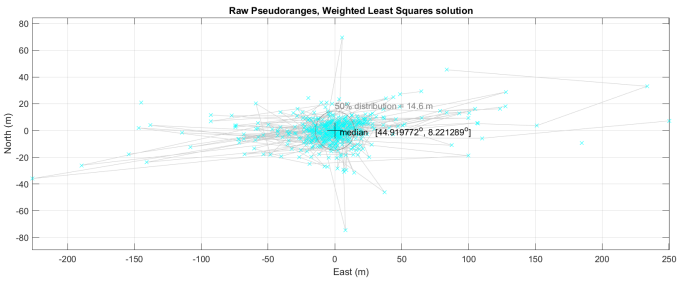

Figure 22: Raw Pseudoranges, Weighted Least sqaures solutions

m with a significant portion of outliers up to 100 meters away from the median. Obviously, being close to the microwave, the test was conducted stationary. We attempted to estimate how this type of jamming would affect the position by conducting further observations. However, we decided not to report them as they were inconclusive. It is indeed impossible to obtain a good reference detection by recording on a third-floor apartment balcony. Having not found a different way to conduct the experiment, we prefer not to make assumptions about the increase in position detection error, but we adhere to the HDOP graph, which shows that an increase is very likely to be expected.

5 Spoofing

We have sought to understand the behavior of spoofing starting from the detection described here. Positioning spoofing emulates the transmission of a false position, in this case [44.919099, 8.219904, 347.48], leading to a completely distorted estimate of positioning. Delay spoofing, on the other hand, introduces artificial delays in GNSS communications, influencing the precision of positioning data and creating potential inconvenience for users. In our test, we observed that by inserting the spoof.position at a plausible position close to the detection,e all estimates made concentrate around the

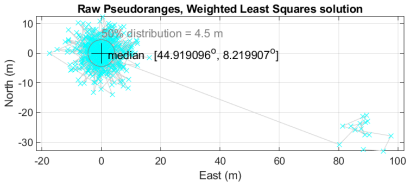

Figure 23: Raw Psuedoranges

indicated point, which also turns out to be similar to the midpoint found. In our experiments, we noted that the estimate of the midpoint and deviation is highly sensitive if the spoof.position is far from the described path and from t-start, which is the second when spoofing begins. This concentration of position estimates is also highlighted by the WLS graph. As for the behavior of spoof.delay, it

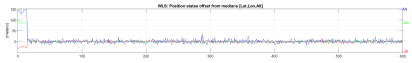

Figure 24: WLS graph

appears to further concentrate positioning estimates. Indeed, with a delay inserted of 40.212e-3 and the same position indicated above, a deviation of 4.7 is observed without the delay and 4.5 with the delay. The delay interacts with clock data, resulting in a flat and constant signal, similarly affecting the Pseudorange vs Time graph

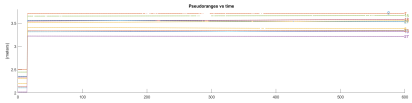

Figure 25: Raw Psuedoranges

and the pseudorange change from init, demonstrating how these three graphs are directly correlated. This type of spoofing is immediately detectable through these graphs. Conversely, spoofing with only the position is not immediately detectable without further information.

References

[1] google. 2023. gps-measurement-tools. (2023). chrome-https://github.com/google/gps-measurement-tools

[2] Office of the European Union. 2017. USING GNSS RAW MEASUREMENTS ON ANDROID DEVICES. (2017). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.euspa.europa.eu/system/files/reports/gnss_raw_measurement_web_0.pdf

[3] otgtv. 2024. otgtv. (2024). https://www.otgtv.it/listapost.php?prov=AT&provincia=Asti