GNSS lab report

Giorgia Moscato, Angelo Barbera, Alessandro Genova

ABSTRACT

This report aims to explore the Global Navigation Satellite System (GNSS), potential attacks (spoofing) and weaknesses (interferences). We performed our measurement in different conditions and then we analysed those data collections and discussed about the output plots highlighting the significant results and differences.

1 INTRODUCTION

Knowing the position is a need that also our ancestors had. It evolved through time and now we have sophisticated and technological methods to obtain our position.

2 METHODOLOGY

The GNSS data have been collected using the GNSSLogger analysis app [2] on Android smartphones under different conditions (e.g. open sky, indoor, walking, car, airplane, interference) and processed using the GNSS Analysis MATLAB code [3]. To perform a measurement, all you need to do is open the GNSSLogger app, toggle on the measurements flag (in Home tab) and the measurement time (in Log tab via Timed Logging button) and press the Start log button. You can analyze the measurement using the GNSS Analysis MATLAB code just by editing the input data part of `ProcessGnssMeasScript.m` with the relative path of the log measurement. The spoofing is also simulated in software using the MATLAB code.

3 FILTERS

Using the MATLAB code is possible to specify different types of filters to select only the data that satisfy a specified constraint. We can do this by modifying `SetDataFilter.m` file.

3.1 Multi-path indicator

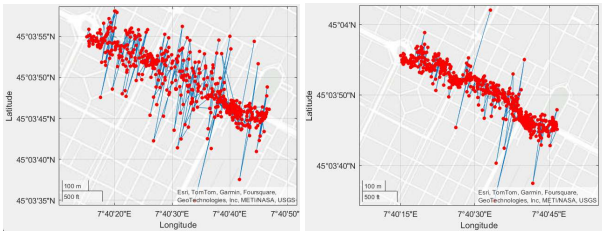
This filter allows to select the signals based on the presence of multi-path propagation, so it is possible to detect whether the signal of satellites has been reflected or refracted, causing erroneous pseudorange measurements. We tried to apply this filter to different dataset but, in all the collected data, the value is always equal to 0 which means that the presence of multi-path signals is unknown [1]. This is due to the architecture of smartphone antennas, which most often do not allow line-of-sight signals to be distinguished from multi-path signals [4].

3.2 Carrier to Noise density ratio

This filter can be used to select the satellites with the specified Carrier to Noise density ratio (C/N0). This can be useful because we can remove the satellites with a too low C/N0 value which reduces the measurements accuracy. However in some cases, reducing the number of satellites used decreases the accuracy of the estimated position, like in our example.

```
dataFilter{end+1,1} = 'Cn0DbHz';
dataFilter{end,2} = 'Cn0DbHz>20';
```

We used this filter in a measurement performed walking in the street, so with line-of-sight partially obstructed. We obtained the plot in figure 1a while without applying the filter we obtained the plot in figure 1b. It is possible to observe that the measurement precision is better considering also the weakest signals (less then 20 dB.Hz) then filtering them, because with the filter the number of satellites used is lower, so in this case the estimated position is less precise. Of course, the results may vary depending on the scenario.



(a) Filter enabled **(b)** Filter disabled

Figure 1: Positioning solution on map

3.3 Constellation type

This filter can be used to select specific GNSS satellite constellations. For instance, we might choose to rely only on the GPS constellation or opt to utilize multiple constellations. Here we activate only GPS and Galileo:

```
dataFilter{end+1,1} = 'ConstellationType';
dataFilter{end,2}   = '(ConstellationType==1)
    | (ConstellationType==6)';
```

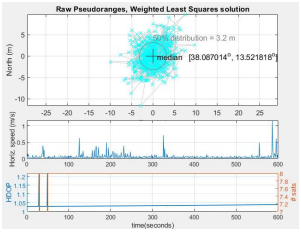
However, we found out that in all our measurements the only one working constellation is the GPS, so we used only this one. This depends on the software implementation of the GNSS Analysis MATLAB code.

4 ANALYSIS

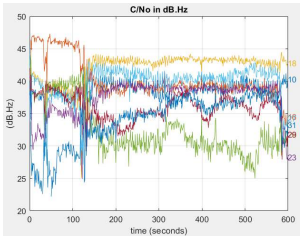
4.1 Open sky

This is the ideal condition measurement. The receiver is far from obstacles, it is not moving and the satellites are in line of sight so the signals are received directly. As we can see in figure 2a the best 50% estimates are contained inside the circumference of a 3.2 meters radius, the number of satellites in view is stable at 8. The horizontal speed variation is at most 1 meter and the Horizontal Geometric Dilution of Precision (HDOP), which measures how the satellite geometry affects the accuracy of the horizontal position, is mostly stable at 1.03 (the lower the better).

GNSS lab report, Torino, 2024
2024. ACM ISBN .
https://doi.org/



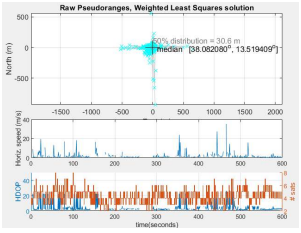
(a) Position estimate, Horizontal speed, HDOP



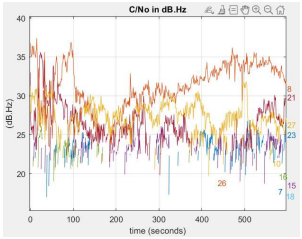
(b) C/N0 in dB.Hz

4.2 Indoor

This measurement was performed inside a building, so the satellites line of sigh is very limited. In figure 3a we observe that the 50% of the position estimates are contained in a circle with a radius of 30 meters, this result, as expected, is worse than the one in open sky condition. Moreover, the horizontal speed has 20 m/s peaks even if the receiver is not moving. The number of satellites in sight varies mostly between 3 and 6 and the HDOP is unstable and it's even 20 times higher with respect to open sky measurement, meaning a very bad satellite geometrical distribution. According to the figure 3b the C/N0 has a mean value of 26.15 dB.Hz and a standard deviation of 4.31 dB.Hz so the signals of some satellites are not very stable. Overall the C/N0 is 30% lower then the ideal condition measurement.



(a) Position estimate, Horizontal speed, HDOP



(b) C/N0 in dB.Hz

4.3 Walking

For this measurement the receiver is moving and the line-of-sight is obstructed in certain moments, this depends on the chosen route because the receiver is not static, and if it's near obstacles, the signals may bounce around. The horizontal speed has some oscillations, which is expected due to the movement of the receiver, but there are some spikes around 14 m/s (but better than 4.2) and this is an indicator of the accuracy of the measurement because it's not plausible for a human walking. As we can see in figure 4 the number of satellites in sight is not stable, in certain instants it's even 1, this means that the position in those cases is not reliable because in order to obtain a correct position we need at least 4 satellites. HDOP has a mean value of 2.91 with a standard deviation of 3.92, and these elevated values contribute to increased errors in the estimated position. In figure 5a the carrier to noise density ratio has a mean value of 24.39 dB.Hz and a standard deviation of 5.87 dB.Hz, which is worse than the previous scenarios.

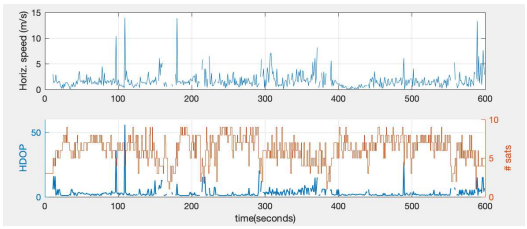
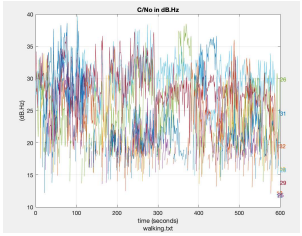
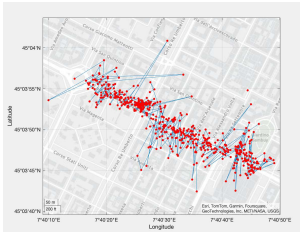


Figure 4: Horizontal speed and HDOP



(a) C/N0 in dB.Hz



(b) Positioning solution on map

4.4 Car

For this measurement the receiver is located inside a moving car, so the line of sight is partially obstructed. The figure 6 shows the receiver's position and we can notice that when the car is inside a tunnel the position is not detected because we cannot get the signals from the satellites. The HDOP value is as good as the open sky measurement. In figure 7, we observe the highest number of satellites in view, which is likely fortuitous, possibly resulting from better satellite geometry at that particular time of measurement. The horizontal speed is mainly distributed between 29 and 31 m/s (about 108 km/h), which is coherent to the speed we had in car since the measurement was performed in highway.

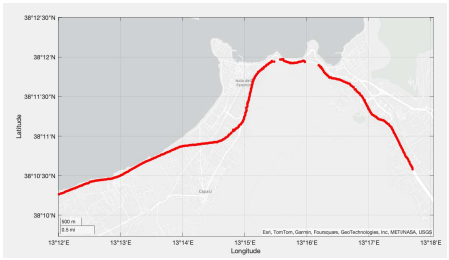


Figure 6: Positioning solution on map

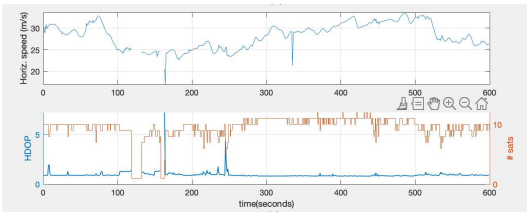


Figure 7: Horizontal speed and HDOP

4.5 Airplane

For this measurement, since the plane can be seen as a Faraday cage, it's fundamental to notice that the only way we can be sure to get signals from satellites is by placing receiver near the window of the airplane. If we are not in the sit near window, we get almost nothing. The figure 8 shows the rectilinear trajectory of the airplane. We can also notice that in correspondence of a drop of the number of received satellites, we get a spike in HDOP plot. This horizontal speed plot is also useful to understand the speed of the airplane in that moment, which is in a range of 215-240 m/s, and it's plausible because cruise speed of a Boeing 737-800 is about 271 m/s. The figure 9 shows us that the received signals are quite high, with a C/N0 mean of 29.95 dB.Hz, this may be due to the fact that we have less inferences and obstacles.

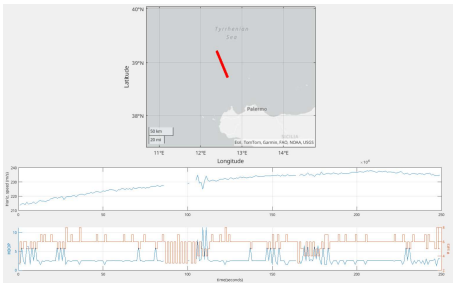


Figure 8: Positioning solution on map, Horizontal speed, HDOP

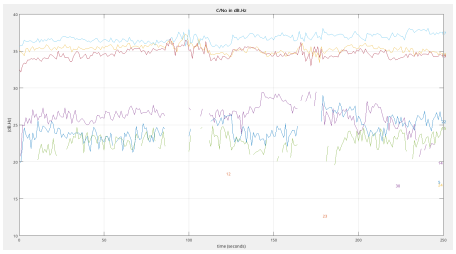


Figure 9: C/N0 in dB.Hz

5 SPOOFING

The spoofing was tested using different spoofing delay and positions, starting it after 300 seconds.

5.1 Spoofing without delay

We simulated spoofing using open sky measurement and a spoof position far from the receiver one.

```
spoof.active = 1;
spoof.delay = 0;
spoof.t_start = 300;
spoof.position=[41.889515,12.491858,100]+1e-3;
```

If we look at the pseudoranges values over time in figure 10 we can observe a significant change and this is caused by the high distance between the spoofed position and the receiver's one.

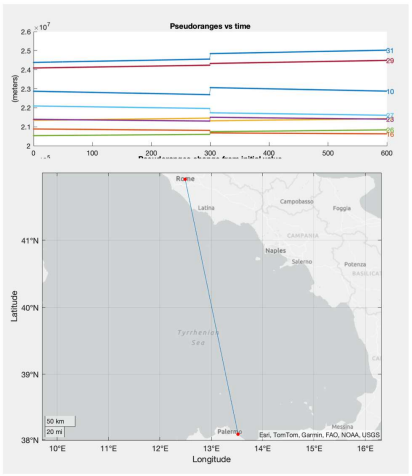


Figure 10: Pseudoranges, positioning solution on map

5.2 Spoofing position near receiver

In this case the spoofed position is near the receiver's one (the offset is 10^{-3}). In figure 11, we can observe that the change in pseudoranges over time is negligible. This is because the scale of the plot, which is on the order of 10^7, makes it difficult to detect small changes, especially when compared to scenarios where the spoofed position is distant from the receiver's actual position (5.1). The position estimate plot shows the real position estimated before spoofing and the fake one estimated after spoofing.

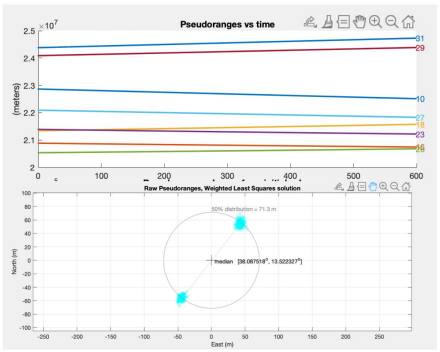


Figure 11: Pseudoranges, position estimate

5.3 Spoofing with delay

In this case, we introduce a spoof delay of 5 milliseconds, which differs from the previous scenario. Figure 12 illustrates that the pseudoranges exhibit a peak due to our introduced spoof delay. The peak occurs because the pseudoranges are calculated based on the time of flight (the time it takes for the signal sent by the satellite to reach us), which is influenced by the receiving timestamp that is modified by our introduced delay. However, it's important to note that this delay does not impact the position estimation directly, as it is perceived as an additional clock bias. This bias is estimated by the receiver as part of its clock offset estimation process. In figure 13, we compare the user clock bias with and without the spoof delay and we can notice that in the former case there is a peak corresponding to the initiation of the spoofing.

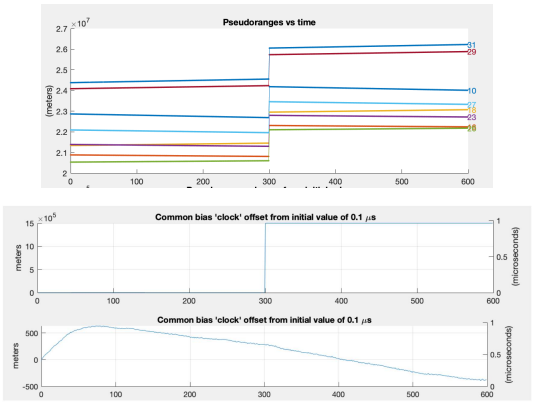


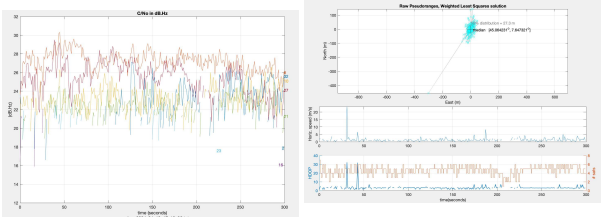
Figure 13: Clock bias difference between delayed and non-delayed

5.4 Spoofing detection

One way to detect spoofing attack is to observe the pseudoranges variation over time because, as we have previously seen, if the spoofed position is far from the real receiver one, or if the spoofer transmit the signals with a delay, the pseudoranges changes rapidly. If this change is greater than a reasonable threshold we can assume that the attack is underway. Another possible detection method is based on the carrier to noise ratio: if the spoofer does not transmit the signals with a power similar to a real satellite, then it's possible to detect that it is a fake signal. Moreover, it is possible to verify if the received signals originates from satellites that are really in view of the receiver or they are just fake signal generated by the spoofer for example by using cryptographic techniques or by analyzing the receiving direction (this can be done if we have an antenna which is able to tell you the signal direction of arrival).

6 INTERFERENCE

We also conducted measurements outdoor near an interference source transmitting on the same frequency band as GPS. As we can see from the figure 14a the signal to noise ratio has a mean value of 23.9 dB.Hz which are values comparable with the ones obtained during the indoor measurement. While if we analyze the figure 14b we notice that the 50% distribution of the measurements are inside a radius of 27.3 meters. The interference from external sources negatively affects the accuracy of the position estimate due to errors in the measured pseudoranges. This interference can occur because satellite signals are relatively weak, making them susceptible to degradation by other signals, such as those generated by television repeaters or other sources. Interferences can be detected and be mitigated at receiver level through the use of antenna shaping, frequency filtering, time domain blanking, etc.



(a) C/N0 in dB.Hz

(b) Position estimate, Horizontal speed, HDOP

7 CONCLUSION

In conclusion we saw the differences in the estimation of the position varying the environmental conditions. We also performed the previous measurements with the power saver turned on, which could potentially cause discontinuities in the smartphone hardware clock to save battery. However, each device exhibited varying behavior, and the same device displayed different behaviors at different times. Therefore, the effects of power saving mode on smartphone measurements are difficult to predict. This variability depends on its implementation, which is specific to each device and not described by the device producers. Additionally, we found no discernible differences between measurements taken with or without battery saver enabled. After analyzing the different values of mean and standard deviation (std) of Horizontal Dilution of Precision (HDOP) and Carrier-to-Noise Ratio (C/N0) in the specific scenarios, we group them in Table 1 to have a complete picture on measurements. It is evident that the highest mean C/N0 value is observed in the open sky measurement, as anticipated, while the lowest values occur in indoor, walking, and interference scenarios. As for HDOP, optimal values are achieved in open sky and car scenarios, due to the unobstructed view of the sky (this holds true even for the car scenario, as we traveled on a highway with minimal obstacles, avoiding densely built-up areas). On the other hand, the poorest HDOP value is recorded in indoor and interference scenarios. Furthermore, the greatest standard deviation in C/N0 is observed during car, airplane, and walking scenarios, which is expected particularly due to the movement among buildings or at high speeds. For HDOP, the indoor scenario exhibits the highest standard deviation, reflecting the challenges posed by obstructed line of sight conditions.

	HDOP		C/N0	
	MEAN	STD	MEAN	STD
Open sky	1.03	0.01	37.56	4.18
Indoor	4.66	6.31	26.15	4.31
Walking	2.91	3.92	24.39	5.87
Car	1.01	0.46	28.86	6.27
Airplane	2.82	1.47	29.95	6.16
Interference	3.32	2.72	23.9	2.83

Table 1: HDOP and C/N0

REFERENCES

[1] Google Inc. 2016. GNSS measurements API. (2016). developer.android.com/reference/android/location/GnssMeasurement

[2] Google Inc. 2016. GPS logger. (2016). github.com/google/gps-measurement-tools/releases/tag/2.0.0.1

[3] Google Inc. 2016. GPS Measurement Tools. (2016). github.com/google/gps-measurement-tools

[4] Samin Nasr-Azadani, Mahdi Alizadeh, and H. Schuh. 2023. DETECTING MULTIPATH EFFECTS ON SMARTPHONE GNSS MEASUREMENTS USING CMCD AND ELEVATION-DEPENDENT SNR SELECTION TECHNIQUE. *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences* X-4/W1-2022 (01 2023), 595–602. https://doi.org/10.5194/isprs-annals-X-4-W1-2022-595-2023