GaaS 02

s322918, s331461, s333996

ACM Reference Format:
s322918, s331461, s333996. 2025. GaaS 02. In *Proceedings of Wireless Security Report*. ACM, New York, NY, USA, 4 pages.

1 ABSTRACT

During this laboratory, we performed GNSS raw measurements on our Android smartphones, using the GnssLogger app, in different data collection conditions, subsequently, we analyzed the results through a MATLAB script. After we introduced spoofing into our measurements to evaluate its effects. Spoofing involves sending fake signals that imitate GNSS signals, causing the receiver to calculate incorrect positions.

2 RAW MEASUREMENT ANALYSIS

We conducted stationary measurements in the inner courtyard of the Polytechnic under three specific conditions: open sky, beneath the emergency stairs, and open sky with battery-saving mode enabled.

2.1 Open sky Condition

In the courtyard of Politecnico, we conducted a recent outdoor GNSS measurement. Upon analyzing the collected data, observations emerge: FIGURE 1 illustrates that our measurements exhibit some degree of imprecision. Upon thorough analysis of the graphs, noteworthy observations support our thesis. Firstly, it's observed that 50% of the positions fall within a circumference of 12.1 meters (FIGURE 2), indicating a relatively wide margin of error. This discrepancy could be attributed to various factors such as multipath effects, atmospheric disturbances, or receiver inaccuracies commonly encountered in GNSS measurements.

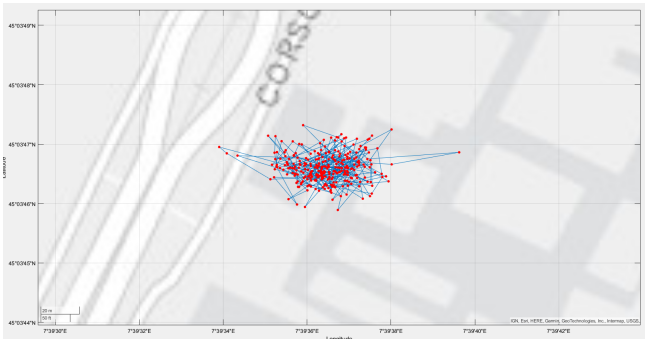


Figure 1: Plot positioning solutions on map

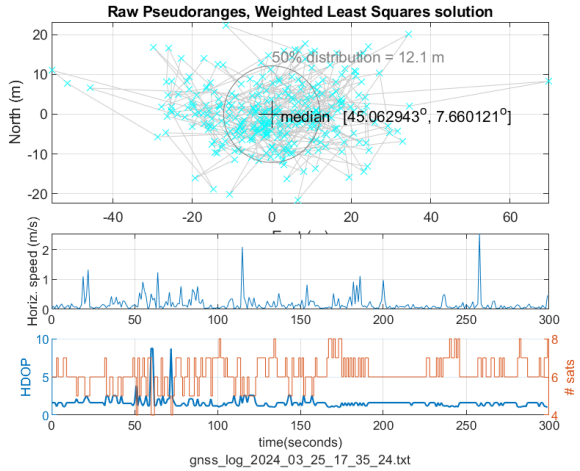


Figure 2

Moreover, as shown in FIGURE 3, numerous signals fall below the 30 dBHz mark, with satellite 21 consistently maintaining levels below the 25 dBHz threshold. This persistent low signal strength may compromise the accuracy and reliability of positioning solutions. C/No, the Carrier-to-Noise density ratio, serves as a crucial metric for assessing signal quality in GNSS, comparing the power of the carrier signal to the background noise density.

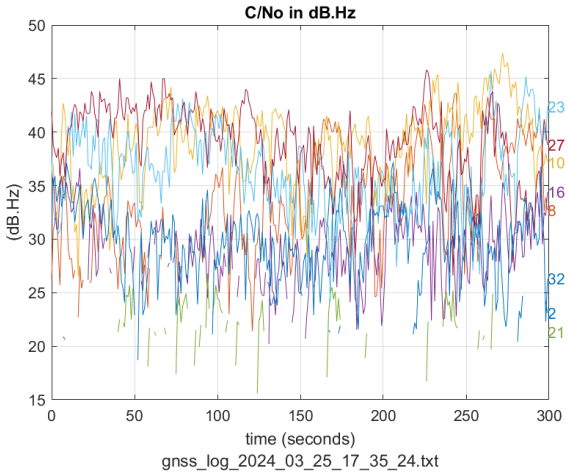


Figure 3

Also, it's noteworthy that horizontal velocity often exhibits peaks at 1 m/s and two at 2 m/s, accompanied by corresponding reflections (FIGURE 2). These sudden variations in velocity could be indicative of dynamic environmental conditions or multipath interference, where signals reflect off surfaces before reaching the receiver. Such reflections introduce errors in velocity estimation, emphasizing

the importance of mitigating multipath effects for accurate GNSS measurements.

2.2 Battery Saving mode

While Android 7 doesn't directly provide GNSS time, once the receiver has estimated GPS time, applications or services on the device can calculate GPS time by adjusting the device's internal hardware clock time according to the receiver clock bias.

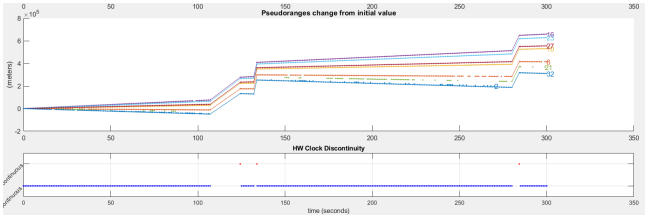


Figure 4

Using battery saving mode results in an internal clock discontinuity, affecting the computation of the absolute timestamp and consequently the reception time, a parameter involved in the pseudorange measurements.

FIGURE 5 depicts the user clock bias increasing at the times when FIGURE 4 shows hardware clock discontinuities (at 120 and 280 seconds), moreover the jumps in the graph concerning the change in pseudorange are directly linked to the jumps in the user clock bias.

Figure 5

2.3 Obstructed reception

We have also conducted an experiment by placing our smartphone under emergency stairs between two buildings, creating suboptimal conditions for signal reception. Upon analyzing the data, we can affirm our hypothesis that under such conditions, accuracy is lacking. This is evident in FIGURE 6, which displays various outliers, including one notably significant outlier.

Figure 6

FIGURE 7 illustrates that the radius encompassing 50% of the positions is larger compared to the "opensky" dataset (16.2 m). Additionally, the graphs representing horizontal speed and HDOP reveal peak around 180 seconds, coinciding with the instance where position is notably distant from others. These peak occur with a lower number of satellites (4), indicating either a poor geometric distribution of received satellites or more likely, multipath issues given the measurement location.

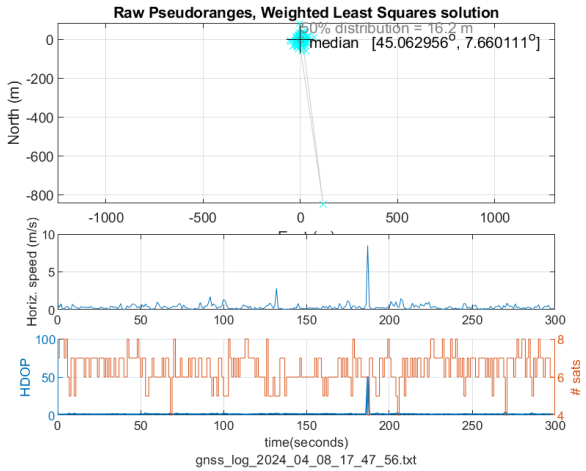


Figure 7

Further confirmation arises from FIGURE 8, where at the same instant, the common bias peak at 0, or from the position states offset from medians or velocity states, which show strong variations at the same instant.

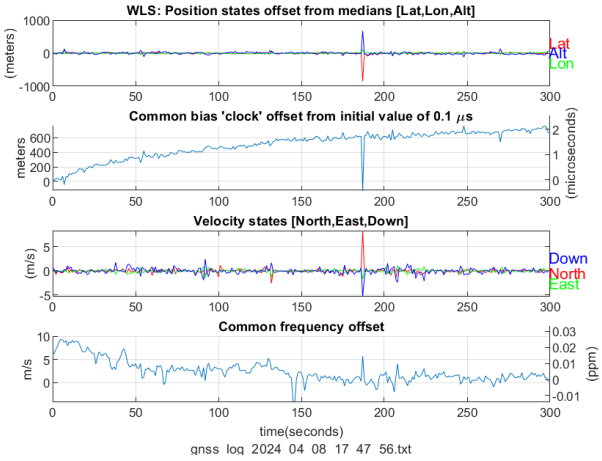


Figure 8

2.4 Custom filters

In this section, we aim to enhance the precision of the "opensky" dataset by applying specific filters. Firstly, we retained satellites with nearly linear differentials (PR/Time), resulting in the preservation of satellites 23, 27, 10, and 8. Secondly, we implemented a filter based on C/No values exceeding 30 dB-Hz, as it is indicative of a strong signal quality

The application of these filters yielded a slight improvement, evident in the reduced presence of outliers in FIGURE 9. Furthermore, this enhancement is confirmed by a decrease in horizontal velocity compared to the unfiltered dataset, as well as less variation in longitude. However, despite these improvement, 50 percent of the positions still fall within a circumference with a slightly larger radius compared to the unfiltered dataset , FIGURE 10 (12.9 instead of 12.1).

Finally, it's important to acknowledge that while these filters led to a noticeable improvement, they also introduce trade-offs. For instance, by selectively retaining satellites based on their PR/Time differentials, we may inadvertently exclude potentially valuable data from other satellites. Similarly, setting a threshold for C/NO values may result in the exclusion of satellites that could contribute to positioning solutions, through with slightly lower signal strengths.

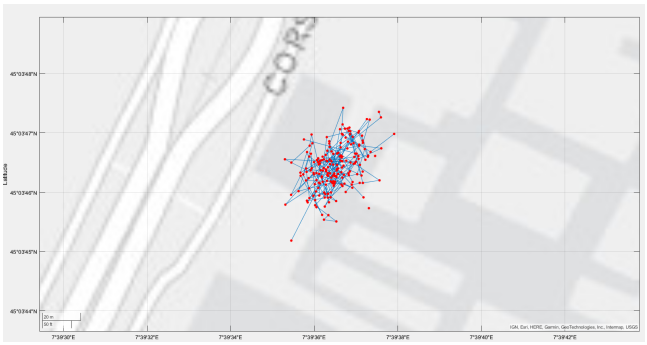


Figure 9: Plot positioning solutions on map

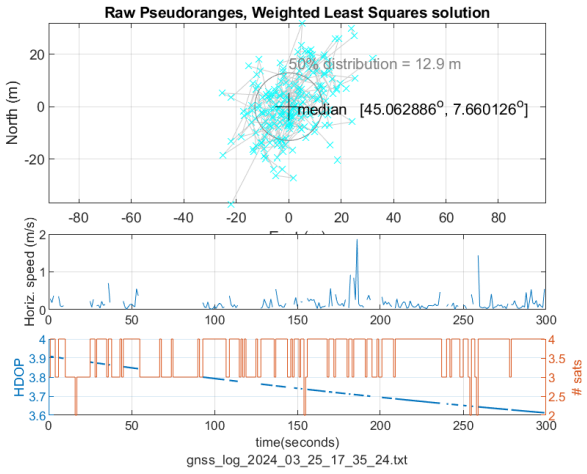


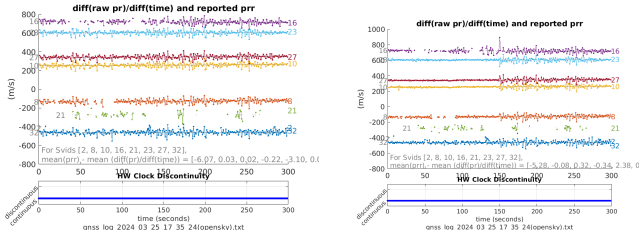
Figure 10

3 ENABLING SPOOFING

In this section, we conducted experiments using OpenSky measurements, where we simulated spoofing attacks by manipulating parameters such as the spoofer's position(spoofer.position), start time(spoofer.time), and delay(spoofer.delay).

3.1 Spoofing position

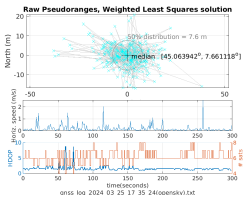
In this subsection, we analyzed the opensky measurements using a near spoof position and two different values of spoofing start time, 0 and 150. Firstly, in FIGURE 11 we noticed a sudden peak at the moment of delayed spoofing activation due to the postponed spoofing attack. In contrary,when the starting time of spoofing correspond to initial time of the measurement, we can't observe this change.



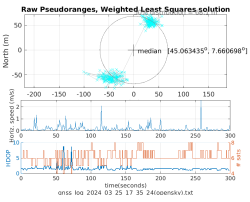
(a) Start time = 0 **(b) Start time = 150**

Figure 11

Consequently, in FIGURE 12 we cannot clearly highligth the spoofed position and the real one and the radius, which represents the spread of 50% of the points derived from the WLS (Weighted Least Squares) solution, is approximately 8 meters. Conversely, in the scenario where the start time is set at 150, we observe a clear separation between the calculated positions attributed to the spoofer and those representing the actual positions. This leads to a significant increase in the radius, up to 60.7 meters.



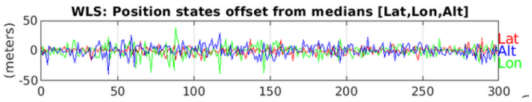
(a) Start time = 0



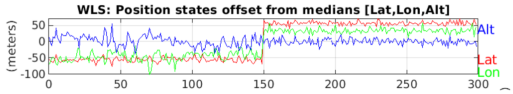
(b) Start time = 150

Figure 12

In the above image, the variation of coordinates can be observed clearly in FIGURE 13, as it illustrates the sudden change in latitude and longitude coordinates in terms of meters, with a spike of approximately 100 meters.



(a) Start time = 0



(b) Start time = 150

Figure 13

3.2 Adding Spoofing delay

Finally, we added a spoofing delay, that is a common delay to all measurements, not distinguishable against an error of synchronization.

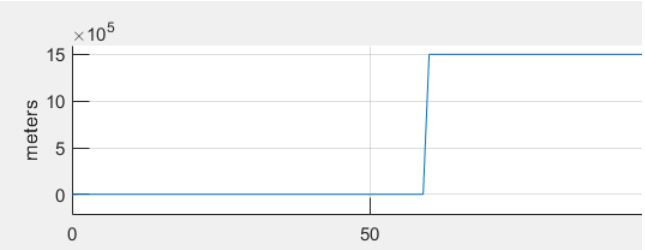


Figure 14: Common bias 'clock' offset from initial value

Correctly the receiver estimates this additional delay a further component of user clock bias, in fact we see a jump in the clock bias estimation, as it can be seen from (FIGURE 14), that has the value we defined in the Matlab script.

The receiver clock bias is a variable in the pseudorange computation, the effects of a significant change of the first can be observed in these figures (FIGURE 15 and 16). In this configuration, the position estimation is not affected, because it would change if each measurement had a different delay, which would correspond to a different position.

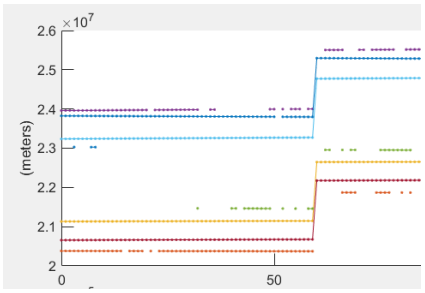


Figure 15: Pseudoranges vs Time

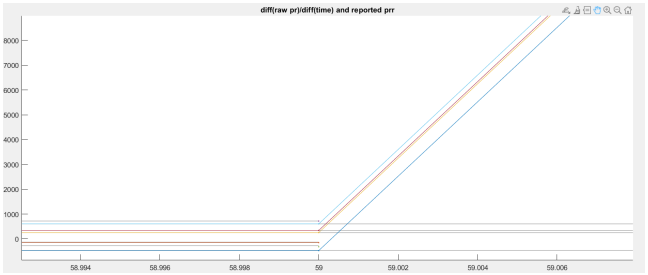


Figure 16: diff(raw pr)/diff(time)

4 CONCLUSION

The quality and characteristics of the signals received from GNSS depend greatly on the location and the receiving device. It becomes relatively easy to conduct attacks like spoofing, which, as demonstrated by the results obtained, lead the victim to display an incorrect position and can also compromise time synchronization services, disrupting various applications. Therefore, it is important to design countermeasures based on the detection of significant changes in parameter values such as user clock bias and pseudoranges, to be integrated with other systems such as authentication and encryption.