Spoofing Android GNSS measurements

Alessandro Mulassano s330263, Manuel Firrera s329226, Iacopo Epinot s333998
Politecnico di Torino

1 INTRODUCTION

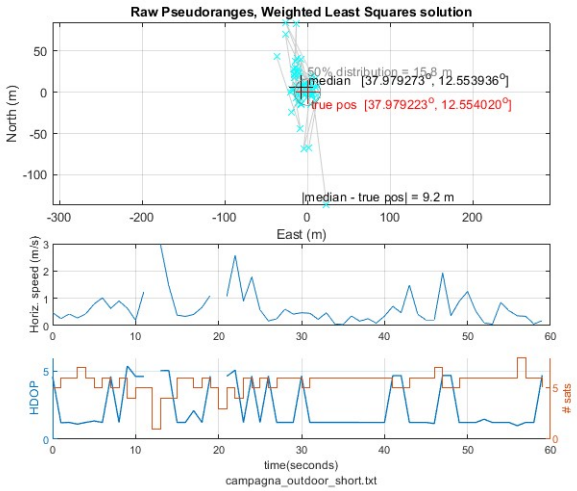
The main goal of this laboratory is to perform the analysis of raw measurements and PVT solution by collecting data in different conditions using the GNSS logger app and computing different spoofed positions.

2 COUNTRYSIDE GNSS ANALYSIS

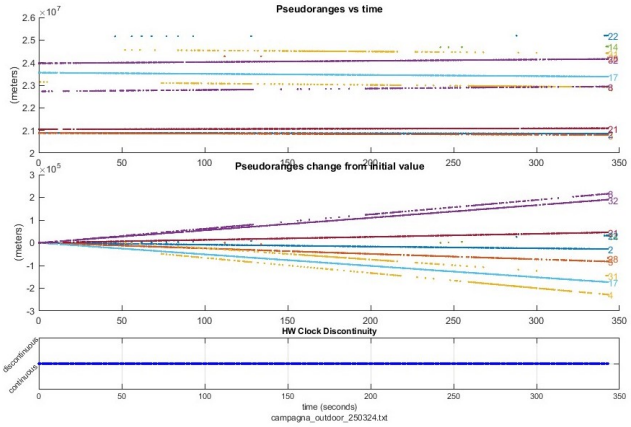
The first analysis performed is about data collected in a countryside location where there should be no interferences.

2.1 PVT analysis

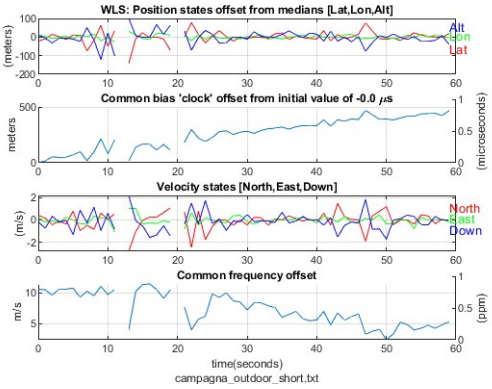
All the logs retrieved from our Android devices were analyzed using a MatLab tool developed by Google.



The first section of the image above represents the median of the positions received by the GNSS module. The median is within the 10-meter radius from the true position, which is on par with the GPS specifications. In the second section, we can see the estimated speed of the stationary device, which is calculated between an acceptable range of 3 m/s. In the third, the red curve represents the number of satellites present in a time slot and the blue curve represents the geometric dilution of precision. It's interesting to note that when the number of satellites decreases in x=11/12s, there is a spike in the hor. speed and the HDOP because of the position miscalculation.



In the figure above, we computed the distance between the receiver and the satellite respectively vs time and the initial value. It's observable that some satellites are getting closer and others are moving away. The third section represents the device clock with no discontinuity.



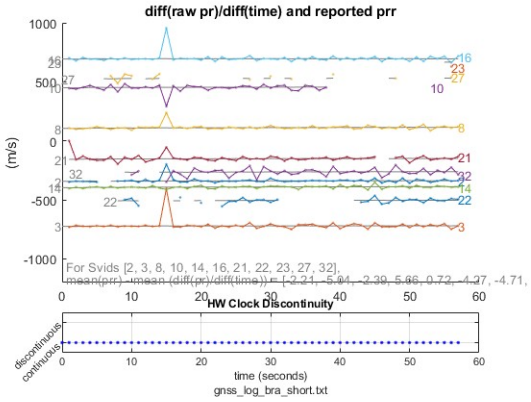
The last figure gives us a deeper insight into:

- The WLS position offset of the calculated position from the median. In this case, we can see an almost linear behavior around 0 with some spikes caused by uncertainty error.
- The common bias clock offset represents an offset between the clock of the device and the timekeeping received by the system. It's monotonically growing because the device is slowly synchronizing with the GNSS system timestamp and is adjusting the clock bias.
- This represents the offset of the velocity in the 3 directions (North, East, and Down), again, correctly centered around 0.
- The frequency offset represents the difference between the nominal frequency of the GNSS system transmission and

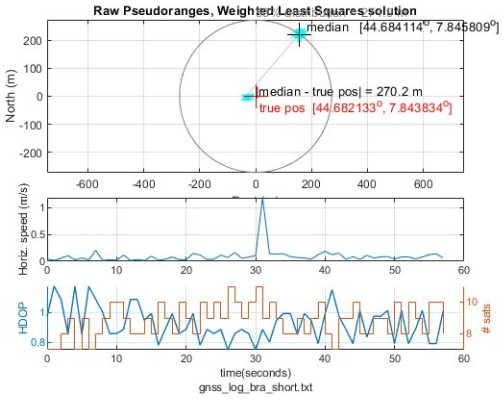
the actual received frequency. This is normally decreasing due to Doppler effects.

2.2 Spoofed position

In this section we have two different spoofed positions, the first one is starting from the real position, while the second one is taking the position from a point near the original one. Regarding the first one, we took our real position through Google Maps, then we added $2*10^{-3}$ centesimal degrees.

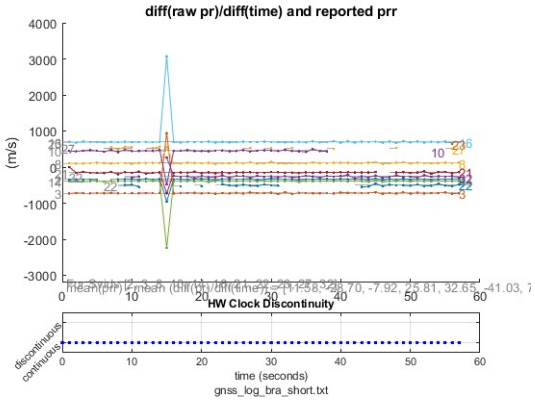


From the figure above, which represents the differential of the pseudorange over time, we can see some spikes around the 15-second mark due to sudden position shifts.

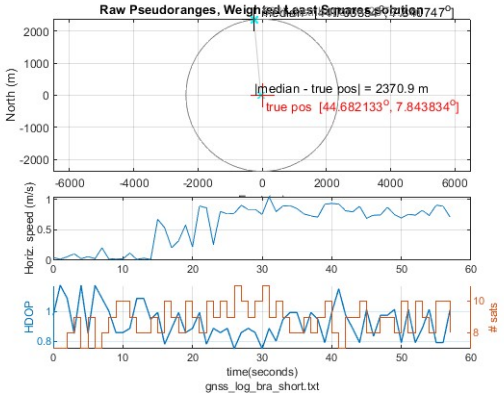


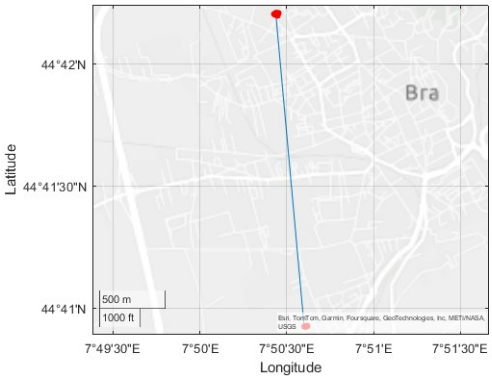
With the spoofing active the median is shifting considerably from the true position.

Regarding the second spoofing attack simulation, we took a position about 2500 m away from the original one.



In the graph, we can observe significant spikes, both positive and negative, at around 15 seconds. This is due to the start of spoofing, which causes the satellites to appear as though they are moving closer or further away. At that instant, their speed undergoes a semi-instantaneous change from approximately 0 to around 3000 m/s and -2000 m/s.





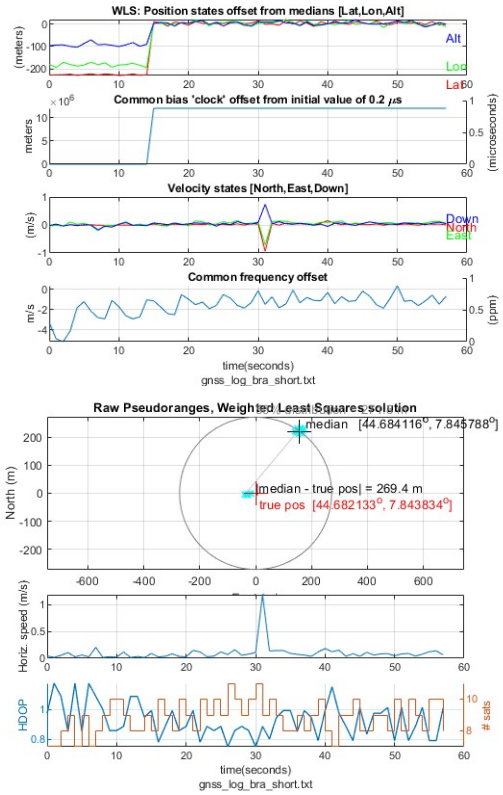
In the figures above, we can observe that the initial position was accurate, but once the spoofing began at the 15-second mark, the position became altered, resulting in a spoofed position.

One way to detect spoofing is to use a device that inspects retrieved

data for anomalies such as spikes, which occur when spoofing is activated.

2.3 Spoofing delay

Adding a 40.212e-3 delay to the spoofer doesn't produce significant results if the user is stationary. As we can see in the figure below, the position didn't change compared to the image with only the spoofed position.

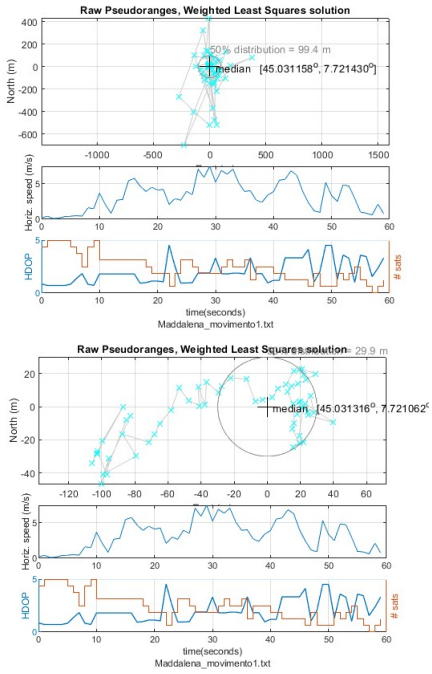


However, in the figure above, we can see an anomaly in the common bias clock offset. At first, before the spoof, the device tries to sync to the system's clock but when the spoofer becomes active the delay applied on the signal desynchronizes the device's clock. This is deadly for the position calculation. We can also notice a peculiar pattern in the common frequency offset. This is caused by the stationary spoofing device, whose transmission frequency is not affected by Doppler effects. If the delay is variable, the device may give up calculating its position, particularly if it is in motion. This led us to experiment with delay on a moving device.

2.4 Non-stationary position

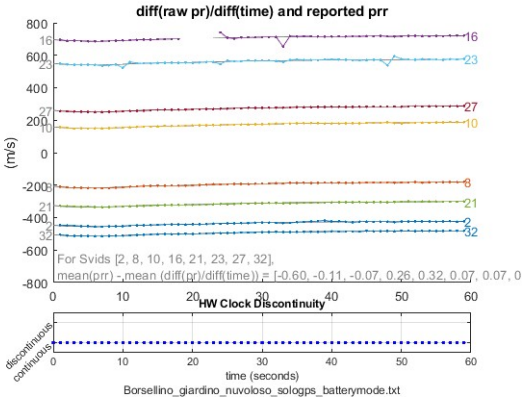
The unnoticeable effect caused by the spoof delay on a stationary device prompted us to experiment with the delay on a moving device. While the spoofing device is stationary, the user is moving away from it. The spoofer sends delayed signals that interfere with the PVT calculations resulting in a successful attack. By looking at the figures below we can see the median centered around the spoofer location.

The horizontal speed jumps at 15 seconds and then swings semi-periodically. That's because the device, due to the spoofer delay, sees continuous fake jumps in the estimated position.



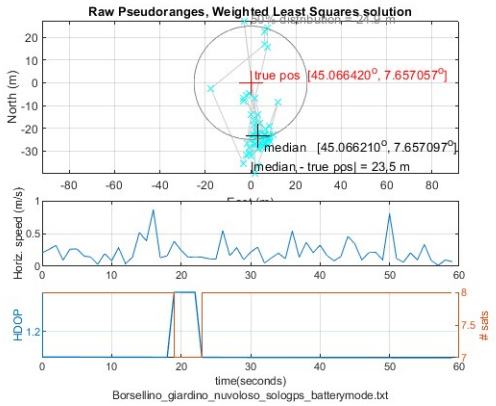
3 CITY GNSS ANALYSIS

In this section, we took the same experiment in Turin, in a place enclosed by buildings, with a cloudy weather condition. The aim is to see the differences between this scenario and the previous one. We took the logs in battery-saving mode but due to the technologies implemented in newer devices, we didn't see any discontinuity in the clock (figure below). This is just an assumption because GNSS chips and algorithms are protected by intellectual property.

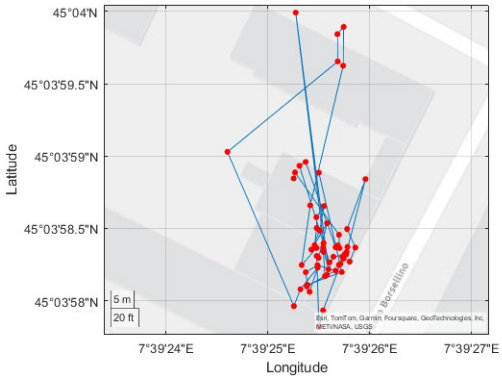


The main differences with the previous section can be seen in the figure below where the taken position is 23.5 m away from the real one, against the 9.2 m of the scenario in the countryside, which is

less than half. This can be attributed to the presence of disturbance sources, a not-so-ideal opensky condition, and the cloudy weather. These phenomena also lower the detected satellites.

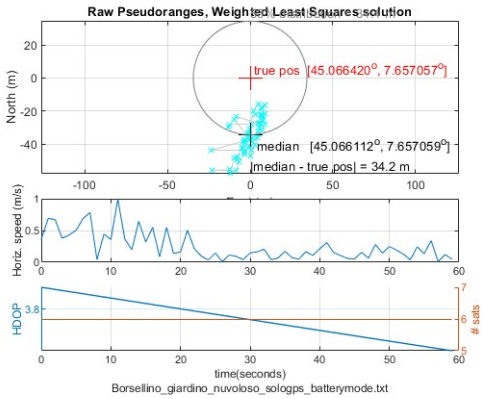


In this last image, we can notice a signal multipath around the buildings and it's not stable, therefore covering a longer trajectory thus increasing the pseudorange.



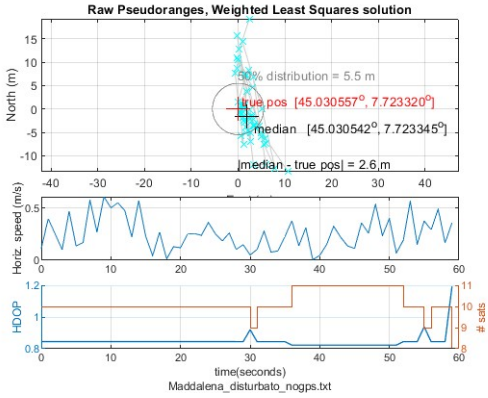
3.1 Filters

We tried then to experiment with the use of some filters to decrease the median-true position difference, so by looking at the various graphs we decided to filter out the signals coming from satellites 16 and 23 that seemed to have some disturbances: the pseudorange vs time was unstable with frequent jumps and low Carrier over noise ratio. The result was worse than before, since the distance from the real position and the estimated one increased by around 10 m. This led us to believe that having a higher number of satellites is always better than filtering them out.



4 BROADCASTING TV ANTENNAS

In this last section, we wanted to see what happens near potential interference sources, in this case the broadcasting TV antennas located on the Maddalena hill. We can notice the difference with the real position is low, just 2.6 m, but data have a bigger dispersion since we have a lot of points out of the distribution of the 50%, represented by the circle in the figure below.



Another interesting fact is that the interference detection and mitigation systems work appropriately since, even near a signal disruption source, we receive clear signals and PVT calculations are on par, if not better, with the countryside measurements.