Spoofing Android GNSS Measurements

Antonello Di Pede

1 EXPERIMENT'S PURPOSE

Since Android 7, access to raw GNSS measurements on everyday smartphones has ushered in a new era of advanced positioning, marrying affordable COTS hardware with powerful onboard sensors. In this study, we probe how raw pseudoranges, Doppler-derived pseudorange rates, and carrier-to-noise ratios (C/N_0) shape the accuracy of Position–Velocity–Time (PVT) solutions across a range of real-world conditions. Before each session, we confirmed at least ten satellites in view and median C/N_0 around 30dB-Hz to guarantee robust data quality. We begin with a baseline "open-sky" data collection, then introduce a subtle spoofing offset to the receiver's true location, follow with a controlled signal delay, and finally examine an indoor interference scenario. By carefully inspecting the MATLAB-generated plots for each case—and applying targeted filters and integrity checks—we aim to illuminate the capabilities, limitations, and potential vulnerabilities of smartphone-based GNSS.

2 METHODS

In our work, we use an Honor 200 Lite (MediaTek Dimensity 6080) running Android 14 and the GNSS Logger app to capture five-minute sessions of pseudoranges, Doppler rates and C/N_0 in each scenario. Before logging, we ensure at least 10 satellites are in view via the Skyplot tab and observe typical C/N_0 values around 30 dB-Hz to guarantee high-quality data.

2.1 Data Collection Scenarios

We recorded .txt logs in the dataset folder under the following conditions:

(1) *Stationary, standard mode* in Piazza Carlo Alberto della Chiesa.
(2) *Stationary, power-saving mode* in Piazza Carlo Alberto della Chiesa.
(3) *Stationary, indoor apartment* at Corso Montevecchio 36.
(4) *Stationary, inside a microwave oven* at Corso Montevecchio 36.

In the first phase, we process each of our five baseline scenarios through `ProcessGnssMeasScript.m` and critically examine the following figures:

- **Figure 1: Pseudoranges & Clock Reset** Raw satellite–receiver ranges over time, with any clock discontinuities flagged.
- **Figure 2: Pseudorange Rates** Numerical range derivatives compared to the chipset's reported PRR to check consistency.
- **Figure 3: C/N_0** Carrier-to-noise density traces per satellite, serving as a signal-quality indicator.
- **Figure 4: PVT Solutions** Weighted least squares fixes, horizontal speed trends, and HDOP vs. satellite count.
- **Figure 5: State Offsets & Clock Drift** Position errors from the median, clock-bias/drift time series, and NED velocity components.
- **Figure 6: Geographical Trajectory** Sequential receiver fixes plotted over a basemap, showing the actual path traveled.

Once these baseline plots are fully analyzed, we proceed to the core experiments requested by the professor:

(1) **Position Spoofing:** inject a spoofed location a few hundred meters from the true site, re-run the script, and measure the resulting PVT shift and any anomalous HDOP or PRR behavior to propose detection strategies.
(2) **Spoofing Delay:** apply a millisecond-scale rebroadcast delay (Δt), observe the clock-bias jump ($\Delta_{\text{bias}} = c\,\Delta t$) and geometric distortion, and evaluate the impact on time-sensitive applications.
(3) **Indoor/Interference Analysis:** compare a five-minute log recorded inside an apartment—where multipath and attenuation dominate—and an extreme case with the device placed inside a microwave oven—to the open-sky baseline, highlighting expected degradations in C/N_0, HDOP, and position accuracy.

3 RESULTS

3.1 Stationary-Standard Mode

In this experiment, we collected raw GNSS measurements from a smartphone placed stationary for 300 seconds in Piazza Carlo Alberto della Chiesa **(Figure 1)**. The square is open to the sky, so no light-of-sight signal obstruction, with surrounding buildings about 10 meters away, far enough to avoid any direct obstruction to satellite signals. The GNSS chipset operated in standard mode, with no power-saving features or artificial disturbances enabled.
Under these conditions we expect stable signal quality (C/N_0), smooth and continuous pseudoranges, and no clock resets. Position estimates should gather tightly around the true point, with low HDOP and low velocity noise. The data should show general great stability and clear signal tracking overall. In other words, the setup should reveal a best-case scenario for GNSS signal tracking and receiver behavior.
As shown in **Figure 2**, the pseudorange measurements from all tracked satellites are smooth and continuous throughout the entire observation window. Most satellites maintain a strong and uninterrupted lock, indicating consistent visibility and minimal signal degradation. While a few brief data gaps appear, for example with some signals around the midpoint, these are minor and likely due to transient measurement noise or temporary signal weakening. The bottom subplot confirms that the hardware clock remained continuous for the entire session, indicating no resets or clock anomalies.
Figure 3 compares two independent estimates of pseudorange rate: one computed by taking the time derivative of the raw ranges, and the other reported directly by the chipset. The reported rates are clean and filtered, while the numerically computed ones show a bit more variation, capturing slight fluctuations and short jumps. The close alignment between the two confirms the reliability of the logger and suggests that no spoofing or major anomalies are present in the raw data.
Turning to signal quality, **Figure 4** plots the C/N_0 values across all satellites. Most signals hover between 25 and 40 dB-Hz, which is consistent with a clear-sky, low-multipath environment. Some satellites do show brief dips below 25 dB-Hz, particularly SV 27 and

SV 10, which might be caused by reflections or subtle obstructions. Overall, the signal strength remains robust, supporting the tracking quality observed in the previous figures.

Figure 5 shows how the GNSS receiver performed while remaining completely still during the test. In the top plot, each blue cross represents a position estimated from raw pseudoranges using a weighted least squares method. These points cluster closely around the reference location, with a median error of about 16.8 meters. Most of the estimates fall well within the 50% confidence circle, and there are no major outliers, which is a good sign of consistency. Looking at the middle plot, the horizontal speed stays near zero, just as expected for a stationary device. The few brief peaks likely reflect noise in the signal or small adjustments in the filter, rather than any real motion. The bottom panel tracks HDOP and the number of satellites used throughout the test. HDOP values remain low (under 1.5), indicating a solid satellite geometry. The receiver also maintains lock on at least 7 satellites at all times, often more, which supports the stability and accuracy seen in the position results.

Overall, this baseline test confirms the excellent performance of the GNSS receiver under static open-sky conditions. The tracking is stable, the satellite geometry is good (as confirmed by low HDOP values), and the signal strength is high.

3.2 Stationary-Power Saving Mode

In this experiment, we collected raw GNSS measurements from the smartphone in Power Saving Mode for 300 seconds in Piazza Carlo Alberto della Chiesa **(Figure 6)**. As before the open sky ensures no significant obstructions to satellite signals, and the surrounding buildings are far enough to avoid direct interference. This mode prioritizes power conservation by reducing the frequency of GNSS measurements, which may lead to less accurate or more fluctuating data compared to normal.

As expected, the Power Saving Mode shows notable differences when compared to the other cases. First, the pseudorange measurements from all tracked satellites exhibit significant fluctuations **(Figure 7)**. The values are less stable compared to the other modes, and large jumps can be observed, particularly in the first few seconds. Specifically, the change in pseudorange varies significantly between satellites, with some deviations reaching as high as ±4 meters. This indicates reduced precision and irregular tracking quality, likely due to the reduced frequency of measurements.

The C/N0 values **(Figure 8)** show that there are no significant differences between Power Saving Mode and Standard Mode in terms of signal quality. Despite the phone being set to Power Saving Mode, the operating system appears to have maintained a similar GNSS measurement frequency to that of Standard Mode. As a result, the C/N0 values remain relatively stable across both modes, fluctuating between 15 and 45 dB-Hz. While minor variations in signal strength are present, these differences are not significant enough to attribute them solely to the power-saving settings. This suggests that, although Power Saving Mode is activated, the system may not have enforced a reduction in GNSS measurement frequency, leading to similar performance between the two modes in terms of C/N0. Therefore, any small fluctuations observed in the C/N0 graph are likely due to natural signal variations rather than the mode selected.

When analyzing the PVT solutions **(Figure 9)**, we observe that the GNSS receiver's position estimates are more dispersed, with a median error of around 19.0 meters compared to 16.8 meters in Standard Mode. The receiver's position, as shown in the plot, is less consistent, with some points drifting significantly, indicating that the receiver's accuracy suffers in Power Saving Mode. The horizontal speed in the middle plot also shows slight fluctuations, suggesting that the GNSS measurements may not be providing accurate updates as frequently as in other modes.

In conclusion, the Power Saving Mode significantly impacts the accuracy and stability of GNSS measurements. The pseudoranges and ADR residuals show increased deviations, and the C/N0 values are bit lower, consequently they do not affect the measurements. Positioning accuracy is also impacted, with a higher median error in PVT solutions, and overall, this mode demonstrates that while power conservation is achieved, it comes at the cost of substantial degradation in GNSS performance.

3.3 Position Spoofing

This experiment replicates the static outdoor scenario illustrated in subsection 3.1, introducing spoofing effects through software manipulation of the GNSS log. The spoofing mechanism is activated by setting `spoof.active = 1`, while the spoof delay parameter (`spoof.delay`) is set to zero. This means no common timing offset is introduced across all satellites, thereby avoiding changes in the receiver clock bias, and the spoofing effect is entirely due to satellite-specific pseudorange shifts derived from the difference between the real and spoofed receiver positions.

The spoofed location is configured near Porta Nuova, while the receiver remains physically stationary in the original location. Spoofing begins at $t = 15$ seconds and is implemented in the `emulateSpoofing` function, which modifies the reception time of each satellite measurement using the precomputed spoofed pseudorange differences (`spoof.spSv_ranges_diff_zeros`). These corrections emulate the measurements that a receiver would observe if it were located at the spoofed coordinates, without introducing uniform clock bias that could otherwise be absorbed by the WLS solver.

In **Figure10** we do not notice any changes since every pseudorange is shifted by about 1112 m, the distance from our real position to Porta Nuova, and the y-axis covers tens of thousands of kilometers, so a one-kilometer shift is not detectable.

Figure 11 perfectly shows the effects of spoofing. The top subplot illustrates, for each satellite, two lines: the smooth one is the PRR (pseudorange-rate), the value that comes straight out of the GNSS chipset, while the irregular trace, made of short almost vertical line segments is the range-rate reconstructed by time-differencing the raw pseudoranges, which are affected by spoofing. During the first fifteen seconds, during which spoofing is not enabled yet, the two estimates lie almost on top of one another, so each color appears as a single line. The moment spoofing is switched on, however, the trace derived from the raw pseudorange goes up and down, while the receiver-reported PRR continues to evolve smoothly. The size of each sudden jump depends on how the one-kilometer spoof offset projects onto the line of sight of a specific satellite. If that satellite happens to lie almost perpendicular to the direction of the spoof shift, only a small fraction of the kilometer shows up, so the

corresponding step is small. Satellites which view lines are more closely aligned with the spoof vector inherit a larger slice of the offset and therefore produce bigger peaks.

Figure 12 shows the carrier-to-noise density ratio (C/N_0), which remains generally consistent with typical values, indicating that spoofed signals do not inherently exhibit degraded signal quality from the receiver's point of view. This confirms that spoofing can be subtle and not easily detectable through signal strength alone.

In **Figure 13**, the weighted least squares solution visibly diverges from the true location. The final position estimate drifts towards the spoofed location, with a median offset exceeding 1.2 km. The map in **Figure 15** illustrates this spatial shift clearly, showing the receiver's estimated position being pulled away from the true coordinates and toward the spoofed point.

Finally, **Figure 14** presents the state estimation metrics. The HDOP and satellite count remain within reasonable bounds, and no clock discontinuities are reported. However, the velocity and frequency offset estimations display anomalies consistent with the injection of manipulated timing data.

These results demonstrate how a geometrically consistent spoofing attack can significantly alter position estimates without the need to introduce a uniform timing delay. In order to detect this kind of attack the receiver should analyze when the graph showing derivatives and check if they do not match PRR. If that gap shows up on several satellites at the same time, it is a strong hint of spoofing.

3.4 Spoofing with Delay

In this experiment, spoofing was simulated by injecting both satellite-dependent pseudorange biases and a common time delay of 5 ms (`spoof.delay`) into the GNSS measurement stream. Unlike the previous case, where the delay was set to zero, this configuration emulates a more realistic spoofing attack, such as meaconing or coordinated spoofers, in which a uniform delay is introduced alongside pseudorange manipulation. The presence of a non-zero delay not only alters the measurement stream but significantly affects the internal state estimation of the receiver.

The most notable change introduced by the spoofing delay is visible in the clock bias estimate. As shown in the middle plot of **Figure 18**, the receiver interprets the uniform pseudorange increase as a temporal offset, resulting in a sharp jump in the estimated clock bias. This response is expected, as GNSS positioning algorithms rely on the relative geometry of the satellites: when all pseudoranges are shifted by the same amount, the system adjusts the receiver's internal clock to compensate, without modifying its perceived spatial location.

Interestingly, despite this abrupt change in timing, the estimated position **(Figure 19)** does not significantly change with respect to the delay-free spoofing case. The reason lies in the geometric nature of the position solution: since the spoofing delay is common to all satellites, it does not distort the relative spatial geometry necessary for position estimation. Instead, it introduces a systematic timing error. As a result, the spatial solution remains consistent, while the timing solution (i.e., the receiver clock estimate) absorbs the spoofing effect.

From a practical standpoint, this has important consequences for GNSS receiver performance. Systems that rely on precise time synchronization, such as those used in telecommunications, finance, or power grid monitoring, would be directly impacted, as their internal clock would be misaligned. At the same time, the spoofed position appears geometrically valid, and the number of tracked satellites and HDOP **(Figure 17)** remain within acceptable operational ranges. This makes such spoofing attacks particularly dangerous and harder to detect, as they can silently degrade the integrity of time-sensitive systems without raising immediate alarms.

Moreover, **Figure 16** shows a clear step and divergence in the pseudorange evolution at the spoofing onset, confirming the artificial range manipulation.

In summary, this experiment demonstrates that even a simple spoofing strategy involving a static pseudorange bias and a uniform delay can effectively mislead a GNSS receiver. While the position estimate may remain stable, the timing solution is corrupted, leading to subtle but critical performance degradations. These results underscore the importance of detecting spoofing through signal-level or consistency-based checks, rather than relying solely on positional accuracy.

3.5 Indoor Analysis

The measurements used for this scenario were taken indoors, specifically inside a residential building near the original reference point. This setting was chosen to evaluate the impact of typical indoor conditions, such as walls, ceilings, and multipath effects, on the quality of GNSS signals and positioning accuracy. The pseudorange trends over time and their relative variations **(Figure 20)** show a higher level of fragmentation and discontinuity compared to the open-sky scenario. Several satellites report intermittent reception, and the pseudorange values frequently reset or jump, a clear indication of signal degradation due to obstruction and multipath effects caused by the indoor environment.

The pseudorange rate comparison **(Figure 21)** further confirms the instability of the signal tracking. Unlike in open-sky conditions, where the variation in pseudorange over time closely follows the receiver-reported rate, in this case, significant gaps appear. This behavior reflects the difficulty in maintaining continuous lock on satellite signals indoors.

Figure 22 shows the C/N_0 values recorded during the session. Most satellites exhibit relatively low signal-to-noise ratios, fluctuating between 20 and 25 dB-Hz,sometimes going down to 14 dB-Hz . These values are below the commonly accepted threshold of 30 dB-Hz for reliable pseudorange estimation. Additionally, frequent dropouts in the C/N_0 traces indicate intermittent loss of signal tracking. This is consistent with the expectation in indoor environments, where satellite signals reach the receiver only after significant attenuation or reflection.

The horizontal positioning results in **Figure 23** show an evident degradation of accuracy. The estimated positions form a scattered cloud extending over several hundred meters, despite the receiver being stationary. The computed median is significantly offset from the known true position, with a positioning error exceeding 200 m. This error is consistent with the geometric dilution of precision (HDOP) and number of visible satellites reported in the bottom

panels of the same figure. For a large portion of the test duration, fewer than four satellites are tracked, and the HDOP frequently exceeds 5, indicating poor satellite geometry and high uncertainty in the solution.
Overall, the results of the indoor test highlight the challenges of GNSS signal processing in non-line-of-sight environments. Signal attenuation, multipath, and reduced satellite visibility significantly impair both the availability and the accuracy of the positioning solution.

3.6 Microwave Analysis

In this scenario, the smartphone was placed inside a microwave, and the GNSS logs were collected. As shown in the figures **(Figure 24**, **Figure 25)**, the phone was able to capture only one satellite signal (SV 14), with poor quality and irregular pseudorange measurements. The microwave, which acts as a Faraday cage, effectively blocked the majority of the GPS signal. A Faraday cage works by preventing electromagnetic waves, including GPS signals, from entering or exiting the enclosed space. This is due to its metal walls that reflect and absorb electromagnetic radiation, including radio frequencies used by GPS satellites. With nearly all the signals blocked, the receiver couldn't hold a steady lock—catching only brief glimpses of a single satellite, far short of the four it needs to calculate position. This experiment underscores how effective the Faraday cage effect of a microwave is at blocking GPS signals, rendering the receiver incapable of obtaining accurate positioning data. The microwave's structure was able to block GPS signals entirely except for the occasional lock on a single satellite, as the device was unable to interact with enough satellites to generate a valid solution.

4 CONCLUSION

The conducted experiments provide a comprehensive overview of GNSS signal behavior under various operational and adversarial conditions. In open-sky static scenarios, the receiver achieves stable tracking with strong signal quality and a positioning error of less than 17 meters, as expected in ideal conditions. Conversely, indoor and microwave environments significantly degrade reception: while indoor measurements still allow intermittent tracking, yielding a degraded but plausible PVT solution, the microwave shielding effectively prevents signal acquisition, confirming the impact of Faraday cage effects.
Spoofing experiments reveal the vulnerability of standard GNSS receivers to adversarial manipulation. In the spoofing scenario without delay, the attacker modifies pseudorange values while maintaining time consistency. This results in spatial errors in the estimated position (over 1 km) but with relatively unperturbed clock bias. However, when a spoofing delay is introduced, the deception becomes more convincing: both the position and the receiver clock estimation are altered, with a consistent drift observed in the clock bias. This demonstrates that even simple spoofing schemes with added delay can produce highly credible but entirely false navigation solutions.
Overall, the results underline the importance of multi-parameter consistency checks in GNSS security. Signal strength alone is insufficient to detect spoofing, as spoofed signals can present high C/N_0 values and maintain satellite visibility. Advanced detection must leverage cross-validation between position, velocity, timing, and residual analysis to flag inconsistencies indicative of malicious interference.

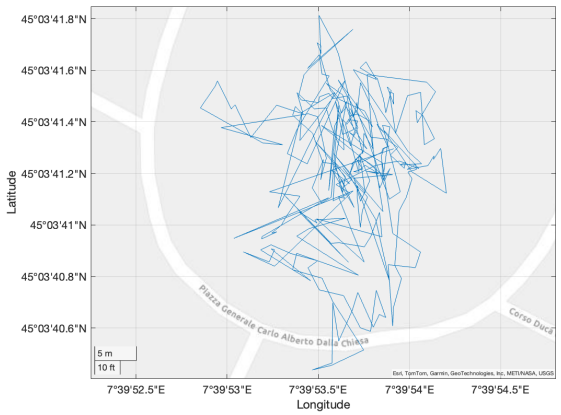

Figure 1: Map Plot Standard Mode

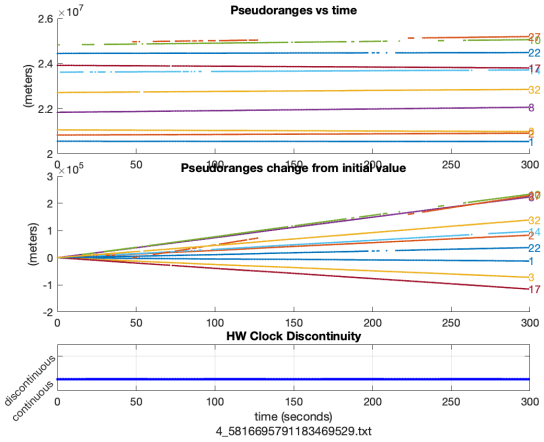

Figure 2: Pseudoranges Standard Mode

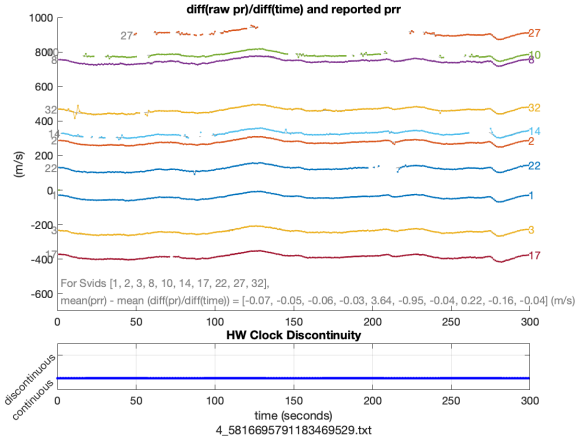

Figure 3: Pseudoranges Rates Standard Mode

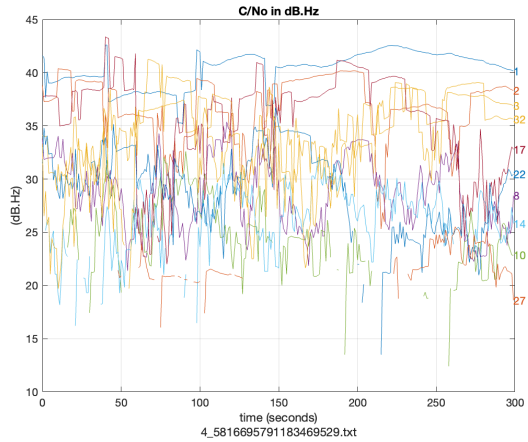

Figure 4: C/N0 Values Standard Mode

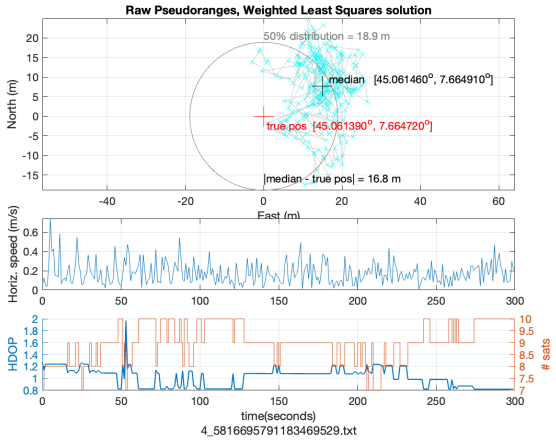

Figure 5: PVT Solution Standard Mode

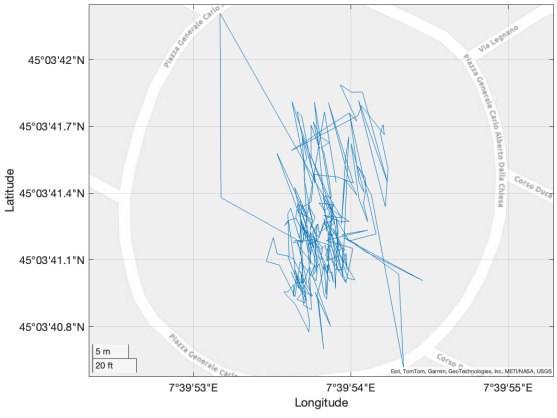

Figure 6: Map Plot Power Saving

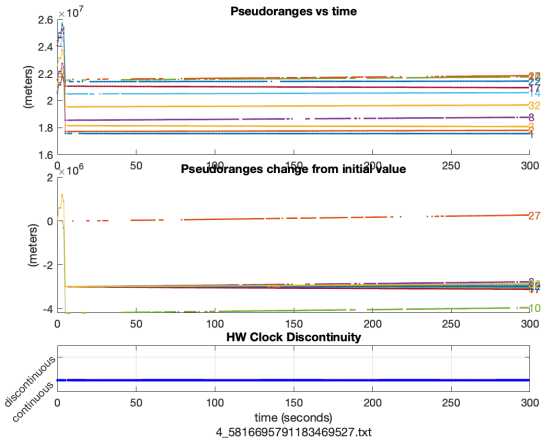

Figure 7: Pseudoranges Power Saving

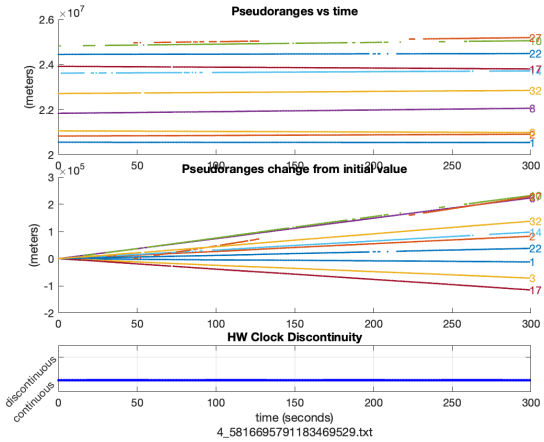

Figure 10: Psuedoranges Spoofing Position

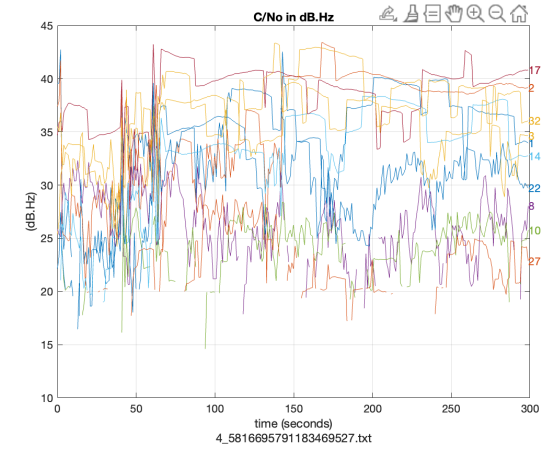

Figure 8: C/N0 Values Power Saving

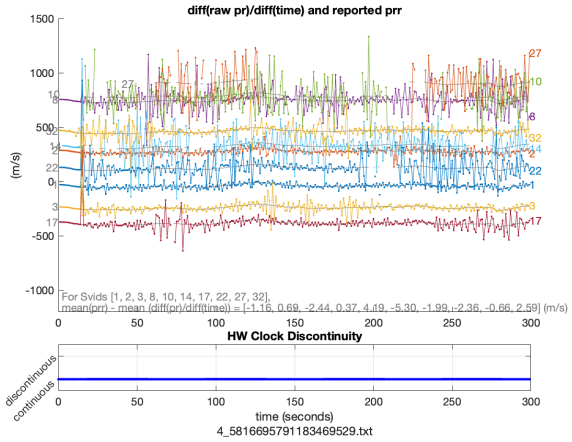

Figure 11: Psuedoranges Rates Spoofing Position

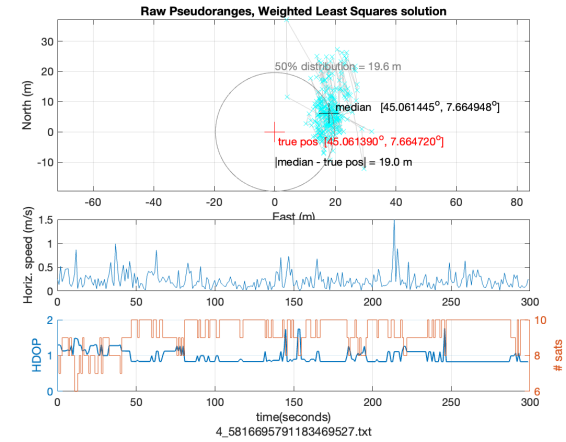

Figure 9: PVT Solution Power Saving

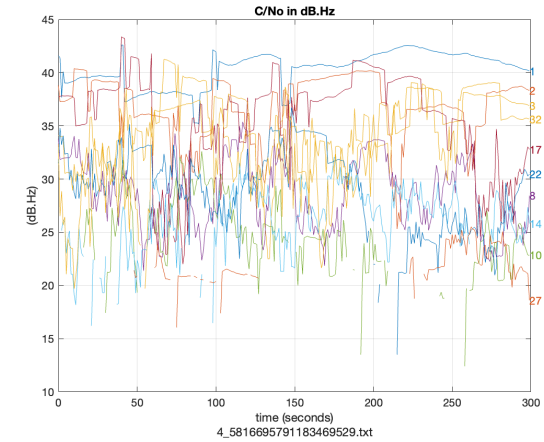

Figure 12: C/N0 Values Spoofing Position

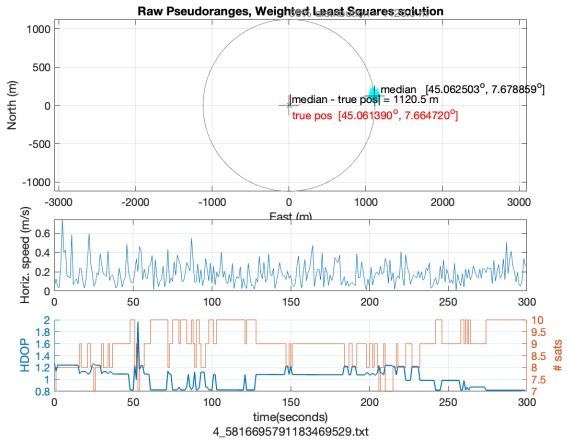

Figure 13: PVT Solution Spoofing Position

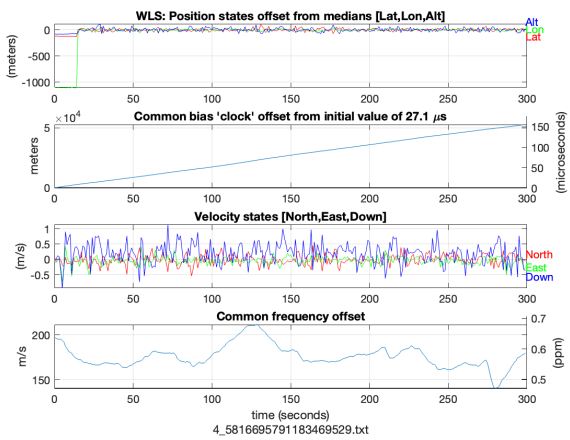

Figure 14: PVT States Spoofing Position

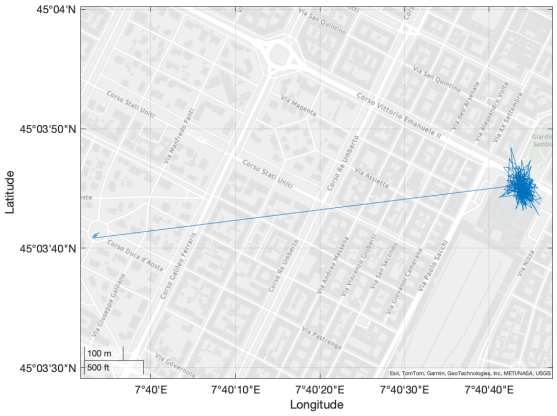

Figure 15: Map Plot Spoofing Position

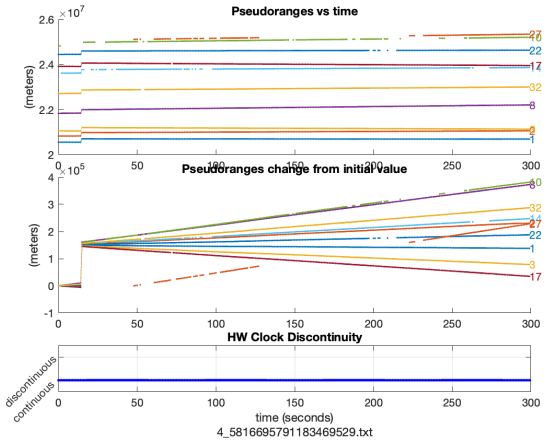

Figure 16: Psudeoranges Spoofing Delay

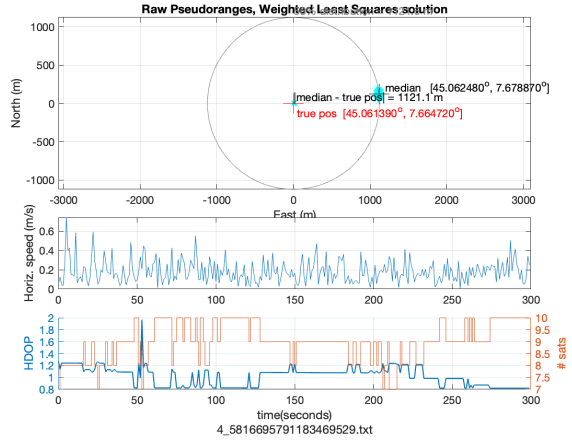

Figure 17: PVT Solution Spoofing Delay

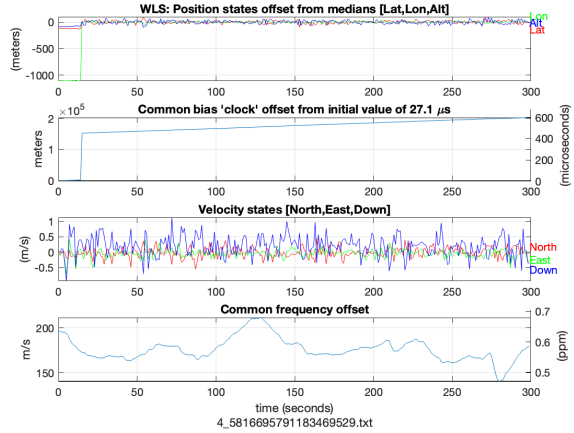

Figure 18: PVT States Spoofing Delay

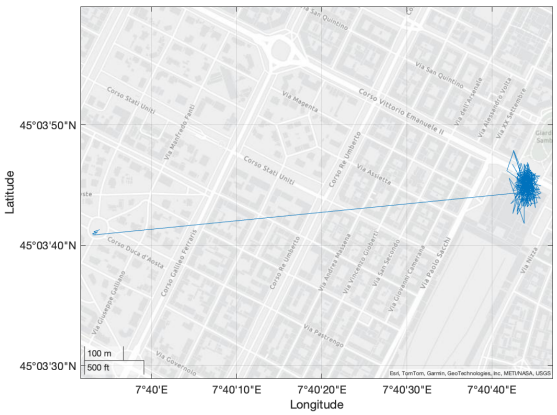

Figure 19: Map Plot Spoofing Delay

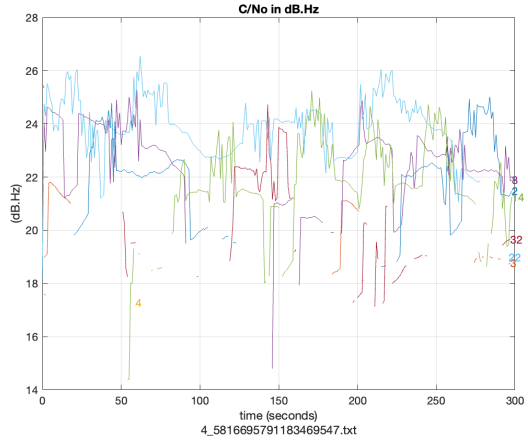

Figure 22: C/N0 Values Indoor

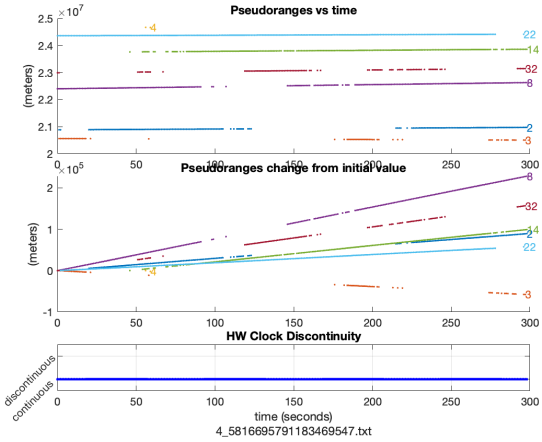

Figure 20: Psuedoranges Indoor

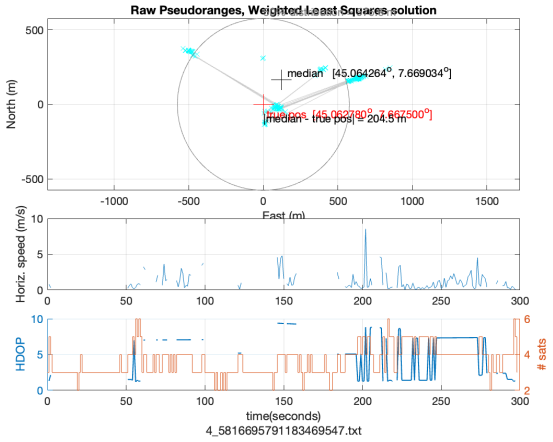

Figure 23: PVT Solution Indoor

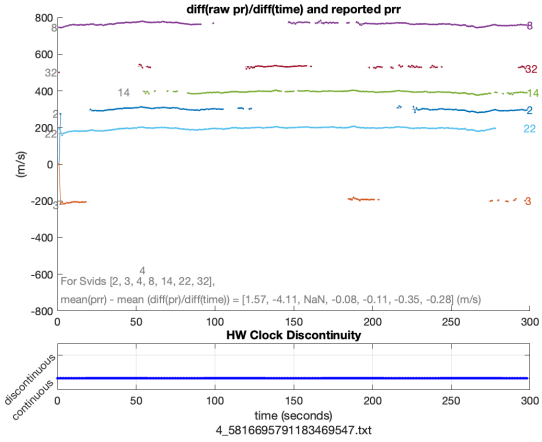

Figure 21: Psuedoranges Rates Indoor

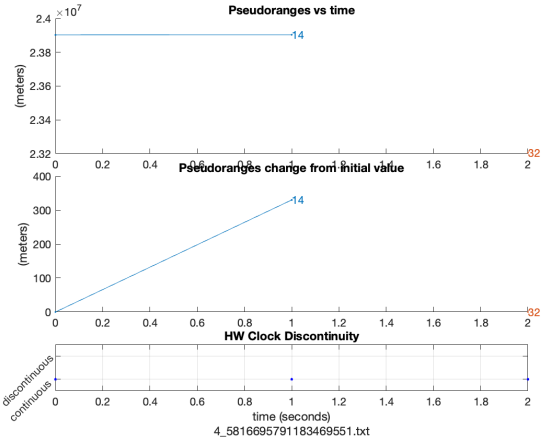

Figure 24: Psudeoranges Microwave

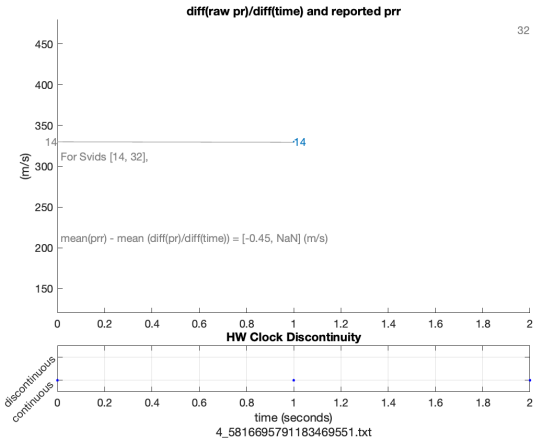

Figure 25: Psudeoranges Rates Microwave