GNSS Smartphone Spoofing

Francesco Rosucci, Niccolò Bedini, Fabrizio Perna

ABSTRACT

This report aims to analyze GNSS measurements acquired through the GNSS Logger app, available for Android, to depict how GNSS signals are influenced by external factors (such as measurements indoor compared to measurements outdoor) and to assess the effects of potential spoofing actions through software simulation, evaluating potential countermeasures.

1 INTRODUCTION

The widespread integration of GNSS systems into various aspects of daily life has made them essential across multiple sectors, including transportation, agriculture, emergency response, and telecommunications. These systems not only enable accurate navigation but also facilitate precise timing, synchronization of critical infrastructure, and monitoring of environmental changes. Despite their widespread use and significant impact on modern society, there is often limited awareness of the physical limitations inherent in GNSS technology. Furthermore, there is a lack of understanding regarding the complex algorithms and methodologies employed to calculate our position with remarkable accuracy. Thus, this report, through various assigned tasks, seeks to shed light on the fundamental aspects of GNSS technology. By testing various usage scenarios and examining the influence of external factors on the accuracy of calculations, it aims to elucidate the complexities involved in GNSS positioning. Moreover, the project endeavors to underscore the vulnerability of GNSS signals to spoofing attacks, such as those performed using a meaconer via software. Through exploring these aspects, it intends to deepen our understanding of GNSS systems and their crucial role in modern life, while also addressing potential security concerns

2 BACKGROUND AND RELATED WORK

In order to conduct our analysis effectively, we utilized a MATLAB script provided by Google. This script is designed to analyze measurements and generate various plots that highlight the most pertinent data. Our focus on these plots is intended to comprehend and accentuate the differences arising from various measurements:

- Pseudorange vs. Time and Pseudoranges change from initial value: These plots play a crucial role in depicting the fluctuations in the distance between satellites and the receiver. They are particularly valuable for identifying signal interruptions, which could signify potential attacks or interferences, especially when they are notably large and sudden. However, given that these distances typically span tens of kilometers, these plots may not be optimal for detecting attacks characterized by minor distance variations
- Differential Pseudorange over Time (Derivative): This derivative plot highlights peaks in sudden variations of pseudorange, thereby simplifying the detection of abnormal satellite behaviors and potential spoofing attempts. Ideally, a constant trend for each satellite would indicate correct and precise measurements.
- C/N0 Signal Strength: By examining the Carrier-to-Noise ratio, we can assess the power of GNSS signals and potentially apply a filter to select the best signals. This aids in inspecting the differences and optimistically achieving more accurate positioning.
- Visual Representation of Estimated Position Over Time: Another graph displays the estimated position over time, along with data on the coordinates of the median derived from various positions. This median is then used in subsequent graphs that are fundamental for detecting interferences or spoofing attacks, and for comparing the estimated (median) position with the true position input.
- Position States Offset from Medians: This plot shows how coordinates vary over time relative to the estimated median position. It is extremely useful in inspecting peaks or characteristic behaviors, which could help in detecting spoofing.
- Common Bias 'Clock' Offset: This graph displays variations in clock bias over time relative to an initial value. Although typically, changes in clock bias are not very explanatory, certain attacks (e.g., those performed with meaconing) may present jumps or discontinuities that assist in tracing these types of attacks.
- Geometrical Distribution of Satellites: This is useful because it provides a general indication of the "quality" of the satellite positions in estimating your location. Generally, a fewer number of satellites results in less accurate measurements because they may not be favorably positioned relative to the receiver, and this is less likely to occur with a larger number of satellites.

These analyses and visualizations are fundamental for understanding our measurement data and deriving final conclusions in our report. By focusing on these specific plots, we enhance our ability to accurately interpret and respond to the data.

3 METHODOLOGY/DESIGN

We conducted measurements using the GSSLogger app under various conditions. Specifically, we performed two collections indoors, with the device stationary in Puglia. One collection was conducted with the device in normal operating conditions, while the other had battery-saving mode activated, aiming to assess its potential impact on performance. Additionally, we conducted one further collection in Lazio, performed outdoors, while the device was in motion. Initially, we analyzed the collected data using a MATLAB script to perform basic analyses. Subsequently, we delved into more detailed analyses. The script facilitated the application of filters to refine

Wireless Security Report, Torino, 2024
2024. ACM ISBN .
https://doi.org/

the measurements based on various criteria, such as C/N_0 (signal-to-noise ratio) to include only signals above a specified threshold or constellation type to focus solely on signals from particular constellations. Furthermore, the script enabled us to simulate spoofing attacks with a meaconer via software. Parameters such as spoofed position, start time, and delay could be adjusted accordingly. We leveraged these capabilities to firsthand experience the effects of signal alterations on computed positions and to draw conclusions regarding the potential detection of spoofing attacks. Additionally, we investigated how various factors impact position accuracy even in the absence of a simulated attack.

4 EVALUATION

4.1 Measurements analysis

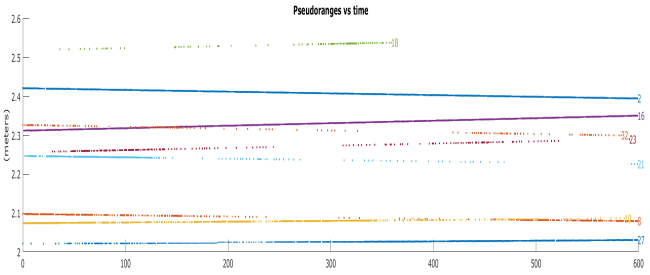

Figure 1

Inside home measureament: The first measurement was conducted indoors and in a stationary position. From the initial graph presented in the figure **1**, we detected significant discontinuities in the signals, attributable to the typical issues encountered with wireless signals in the presence of obstacles, as is common indoors. Subsequent graphs related to the pseudorange differences over time confirmed this observation, which was further supported by the high values observed in the geometrical position. From the signal-to-noise ratio graph, it is evident that although most satellites exhibited fluctuating signal quality, three specific satellites were notably stable and consistent. However, the average C/N0 value was generally low. Despite various signal discontinuities, these initial graphs did not show any particular peaks suggesting the presence of artificial interferences or attacks.

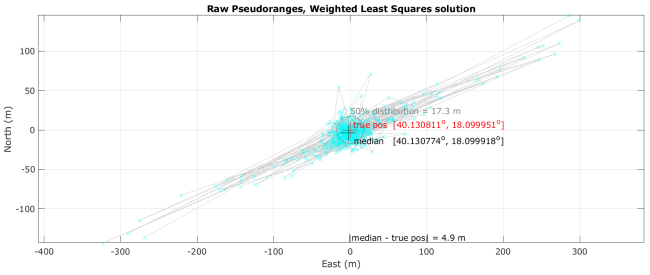

Figure 2

The figure **2** reveals that, despite the challenging conditions and signal discontinuities, the computed median position was quite accurate, deviating only by 5 meters from the true position. Further analysis of subsequent graphs, which tracked the distance of the coordinates from the median over time, identified several peaks. These peaks correspond to the most erratic points consistently present in the map shown in the figure **2**, attributable to the issue of multipath interference, which is characteristic of indoor environments. Despite the estimated position being close to the true position, upon examining the differences in signal strengths, we attempted to apply a filter that would only include signals with a C/N0 above a certain threshold, to see if this would yield improvements. Contrary to expectations, by eliminating the more discontinuous signals, the estimated position worsened slightly by about one meter. We attribute this to the reduction in the number of satellites available for computation, as only three were consistently stable and continuous. Thus, in this specific case, applying such a filter proved to be disadvantageous.

Battery save mode measurement: Analyzing the measurements conducted with the device in battery-saving mode, we did not observe any significant alterations. Despite the implementation of battery-saving measures, there were no noticeable clock discontinuities, and the quality of the received signals generally improved, owing to the increased visibility of satellites at that moment. In summary, constraining the computational capacity of the device did not appear to impact the determination of its position in any discernible manner.

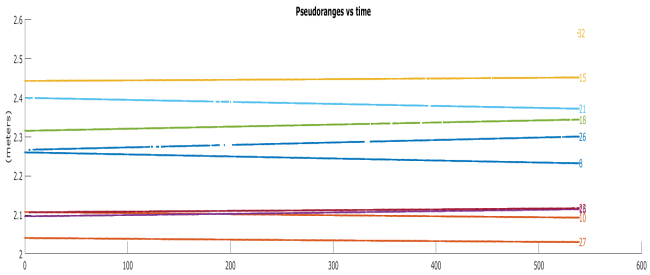

Figure 3

Outside measureament: Building on these initial data, we conducted an outdoor measurement to identify potential differences and enable a beneficial comparison. The graph pertaining to pseudorange in figure **3** and $C/N0$ reveals a marked improvement in signal stability outdoors, showing neither discontinuities nor the significant signal attenuation observed indoors.

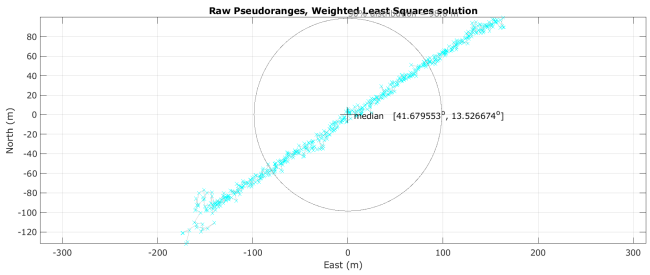

Figure 4

Since conducted on the move, the relevance of the median, or estimated position, diminishes; however, the path accuracy derived from all individual positions was confirmed by the map in figure **4**

to be highly accurate. Additionally, the horizontal velocity remained constant with minimal fluctuations around 1.5 m/s. Notably, this graph also captured the final period when the receiver ceased moving. An intriguing difference we observed was that the map from the moving measurement displayed fewer deviations from the actual path compared to the stationary indoor measurement, which showed some estimated points significantly distant from the true position. This underscores the profound impact of the environment (indoor vs. outdoor) on the measurements, more so than whether the device is stationary or in motion. This outcome is not only a consequence of the inherent nature of wireless signals but is also significantly influenced by GNSS technology itself. The quality of the results depends largely on the number of satellites received, which is typically higher outdoors as confirmed by the graph of the geometrical distribution. Phenomena such as reflection and multipath interference are critical in indoor environments, further complicating the accuracy of GNSS signals.

4.2 Spoofing

Spoofing shifting the real position: The subsequent step involved conducting a simulated spoofing action during the previous outdoor movement measurement, emulating a meaconer that activates after 15 seconds to retransmit signals with zero delay. This was intended to shift the estimated position of the receiver coordinates by a value of $(10^{-3})°$. However, the pseudoranges vs time graphs do not show significant variations from the previous measurements. Although we believe that all signals experience a shift at 15 seconds, this is not evident because the shift of $(10^{-3})°$ is negligible on the scale of 10^6 used in the graphs.

Figure 5

This assumption is further supported by the subsequent graph, also shown in figure **5**, where, at 15 seconds, all signals in the Differential pseudorange over time plot exhibit a simultaneous peak before stabilizing. This peak occurs due to the sudden change in the pseudoranges consequent to the spoofing and, once the position is spoofed, the distance from the satellites begins to change linearly again. This phenomenon, detectable on the scale of meters per second, suggests an increase or decrease in distances by several hundred meters, consistent with the difference in coordinates from the true position to the spoofed position. This characteristic behavior, which was not observed in previous measurements, clearly reflects the positional shift resulting from the meaconer's spoofing action. The graph displaying the map, as shown in figure **6**, is highly illustrative and highlights the success of the experiment. It depicts the points calculated during the first 15 seconds, representing the

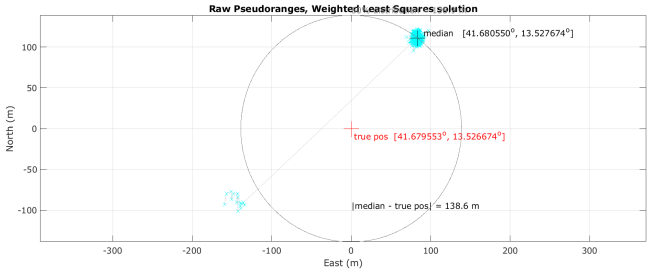

Figure 6

starting point of the measurement (which does not coincide with the true position because the latter is referred as the median point of the outdoor measurement analyzed before), and then shows the immediate shift of 300 meters to the spoofed position. Given the duration of the test, approximately 10 minutes, the median ultimately aligns with the spoofed position.

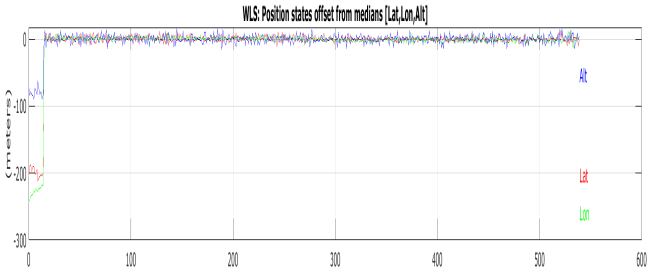

Figure 7

In final analysis, it is particularly interesting to focus on the graphs in figure **7** showing the shift in coordinates from the median (which, we recall, nearly coincides with the spoofing position). Unlike previous measurements, where there were sporadic peaks against a constant behavior, here the coordinates from 0 to 15 seconds are relatively constant but with a visible offset from the zero level (median coordinates). After the fifteenth second, there is a single peak for all coordinates bringing them to level zero. Unlike other measurements, after this peak, the various coordinates remain constant at zero and do not return to the position prior to the peak. This behavior marks the difference between normal interference or computational errors, where peaks are sporadic and eventually return the signals to their pre-peak trend, and a spoofing action where there is a simultaneous peak for all coordinates, which not only shifts the coordinates to new values but also maintains them at these new positions.

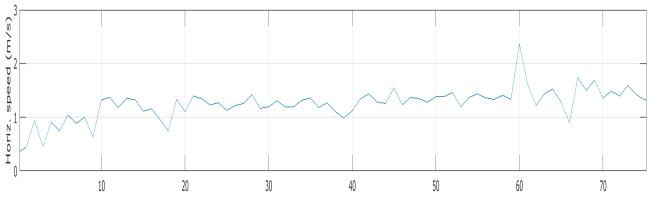

Figure 8

Spoofing with a selected position: In the subsequent spoofing simulation, a position relatively close to the actual median was selected. Similarly to the prior case, in this instance, it's evident that

following the initiation of spoofing, the newly calculated points cluster around the designated false position. Moreover, we observe in the figure **8** the persistence of the same phenomenon wherein, despite an evident peak post-activation, the horizontal velocity does not demonstrate a pronounced shift as might be expected probably due some compensation or automatic correction in the positioning system.

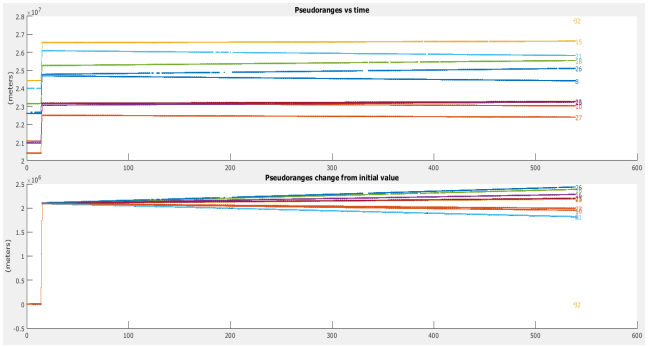

Figure 9

Spoofing with delay: In the final analysis, we recreated a more realistic scenario by introducing a delay in the spoofed signals. Consequently, we observed several anomalies in the plots. Firstly, with the addition of even a few milliseconds of delay -since these delays are multiplied by the speed of light and incorporated into the clock bias of the receiver in the pseudorange formula- we observed a significant jump in the plots in figure **9** depicting the variation of pseudoranges over time. This is a critical difference compared to the same graph from the spoofing without delay. In the latter scenario, no discontinuities were noticed because the shifting was only by a few meters, which were negligible in the computation of the pseudorange formula. However, with the addition of a few milliseconds of delay, the component of the speed of light is maintained in the formula, introducing a non-negligible variation in the computation of the pseudorange. This change manifests as a discontinuity in the graph; indeed, with a delay of 7 milliseconds, there was a jump of approximately $2.1 \cdot 10^6$ meters. These peaks were also conspicuous in the plot of differential pseudorange over time, exhibiting a very high peak for each signal at the same point in time. These peaks were also conspicuous in the plot of differential pseudorange over time, exhibiting a very high peak for each signal at the same point in time.

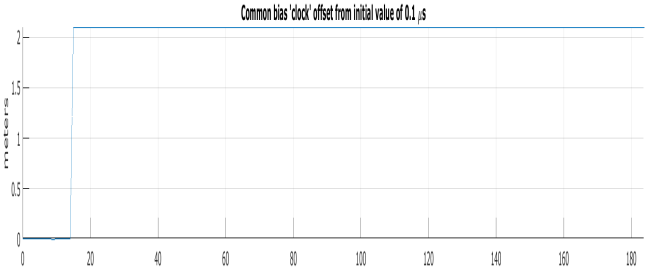

Figure 10

Another notable difference from the scenario of spoofing without delay was the emergence of anomalies in the plot shown in figure **10** representing how the clock bias changes relative to the starting point. After 15 seconds, when the spoofing was activated, we could observe (insert graph) the significant jump in bias on the plot, which was consistent with the introduced delay values. However, introducing a delay doesn't seem to affect the computation of the spoofed position, as it remains largely unchanged. Regarding detection, some plots, such as the variation of latitude, longitude, and altitude with respect to the median or differential pseudorange over time, provide strong indications, but they are computed post facto. The most useful plots derived from real-time data that could be computed and monitored are the variation of pseudorange over time, both in terms of difference from the starting point value and general variation over time, as well as the common bias clock offset.

5 CONCLUSION

The comprehensive analysis conducted in this report sheds light on various aspects of GNSS technology and its applications. Through a series of measurements and simulations, we have gained valuable insights into the performance, vulnerabilities, and limitations of GNSS systems. The evaluation of GNSS measurements conducted under different conditions provides a nuanced understanding of the technology's behavior. Indoors, where signal obstructions and multipath interference are prevalent, we observed significant signal discontinuities and fluctuations in signal quality. Despite these challenges, the computed positions remained relatively accurate, showcasing the resilience of GNSS systems in adverse conditions. However, the impact of environmental factors on signal quality was evident, with outdoor measurements exhibiting improved stability and accuracy due to unobstructed line-of-sight to satellites. Moreover, the simulation of spoofing attacks using a meaconer software revealed critical insights into the susceptibility of GNSS signals to manipulation. By spoofing the receiver's position and introducing delays in signal transmission, we demonstrated the potential for malicious actors to deceive GNSS receivers and manipulate computed positions. The analysis of spoofing simulations highlighted detectable anomalies in pseudorange variations and clock bias offsets, underscoring the importance of vigilance against spoofing attacks. Overall, this report underscores the intricate interplay between environmental factors, signal integrity, and security considerations in GNSS technology. By elucidating these complexities, we contribute to a deeper understanding of GNSS systems' role in modern society and advocate for robust measures to mitigate security risks. Through continued research and awareness, we can ensure the reliability and integrity of GNSS technology in diverse applications, safeguarding its essential contributions to transportation, agriculture, emergency response, telecommunications, and beyond.