Android Raw GNSS Measurements as a New Anti-Spoofing and Anti-Jamming Solution

Damian Miralles, Nathan Levigne, Dennis M. Akos
University of Colorado at Boulder
Juan Blanch, Sherman Lo
Stanford University

BIOGRAPHIES

Damian Miralles is a graduate student in the Department of Aerospace Engineering Sciences at the University of Colorado Boulder. He received a B.S. in Electrical and Computer Engineering from the Polytechnic University of Puerto Rico. His research interests are in GNSS receiver technologies, SDR and digital signal processing.

Nathan Levigne is a MS graduate student in the Department of Aerospace Engineering Sciences at the University of Colorado Boulder specializing in GNSS applications, astrodynamics, and satellite navigation. He received a B.S. in Aerospace Engineering from the University of Colorado Boulder and is currently employed there as a research assistant for the Colorado Center for Astrodynamics Research. His research interests are in GNSS RFI detection, localization, and mitigation.

Dennis M. Akos completed the Ph.D. degree in Electrical Engineering at Ohio University within the Avionics Engineering Center. He has since served as a faculty member with Luleå Technical University, Sweden, and then as a researcher with the GPS Laboratory at Stanford University. Currently he is a faculty member with the Aerospace Engineering Sciences Department at the University of Colorado, Boulder and maintains a visiting appointments at Stanford University and an affiliation with Luleå Technical University.

Juan Blanch is a senior research engineer at Stanford University, where he works on integrity algorithms for Space-based Augmentation Systems and on Receiver Autonomous Integrity Monitoring. A graduate of Ecole Polytechnique in France, he holds an MS in Electrical Engineering and a Ph.D. in Aeronautics and Astronautics from Stanford University. He received the 2004 Parkinson Award for his doctoral dissertation and the 2010 Early Achievement Award from the Institute of Navigation.

Sherman Lo is a senior research engineer at the Stanford GPS Laboratory. He received his Ph.D. in Aeronautics and Astronautics from Stanford University in 2002. He has and continues to work on navigation robustness and safety, often supporting the FAA. He has conducted research on Loran, alternative navigation, SBAS, ARAIM, GNSS for railways and automobile. He also works on spoof and interference mitigation for navigation. He has published over 100 research papers and articles.

ABSTRACT

Reliable radio navigation signals are of extreme importance. Nowadays we rely on Global Navigation Satellite System (GNSS) related technologies for a range of uses ranging from agricultural, financial, transportation and military applications. As such, providing existing systems with the tools to combat the threat presented by malicious spoofing or jamming attacks is critical. The paper explores the properties of the different sensors available on a smartphones and evaluates their potential for spoofing and jamming detection. By properly assessing key sensor properties, this work will detect spoofing or jamming by monitoring alarm triggers set by a combination of sensors including but not limited to: (1) network location provider, (2) combined Automatic Gain Control (AGC) and C/N_0 engine, (3) inertial sensor data, and (4) pseudorange residual metrics. In addition, we investigate the existence of the solution on the smartphone and further discuss the sensors with potential in the identification if any type of interference attack. Combining all together is GNSSAlarm, an Android application (still under development) that creates a tool, based on resources already in the pocket of millions of individuals and develops an effective anti-spoofing, anti-jamming tool that will allow proper functionality when in the presence of spoofing attacks and will notify the user when under jamming attacks.

INTRODUCTION

The GNSS industry has been revolutionized with the plan by several countries to launch satellites transmitting new signals in dedicated bands with the idea of an international GNSS system that allows for cross-compatibility and reduced expenses in receiver design. The concept started with the transmission of the Global Positioning System (GPS) L1 C/A signal, which became short after the gold standard of radio navigation. Globalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS) satellites followed and the constellation reached maturity during the Soviet Union era, but degraded after its collapse. However, in early 2000s efforts by the Russian Federation government were focused in the restoration of the constellation which is now fully functional. The Galileo constellation finally cemented this idea with the addition of the E1 open service signals. Most recently, we had the addition of the Beidou constellation and its B1 signals. It is also true that the existing and new constellations offer signals in frequencies other than the L1 band, but the design for multiple constellation receiver at the smallest cost/ power consumption benefits from this single frequency approach.

With the technological advantages of our era, GNSS receivers have been drastically reduced in price and size. This allows for smaller single frequency chipsets that use multiple constellations to compute the position solution to be used in day to day devices such as wrist watches, smart-phones, etc. Moving multiple signals from different constellation into a single band makes this design paradigm stronger since there is significant hardware reutilization and software techniques can be used to do the low level signal processing. The release of GNSS chips like the Broadcom BCM47755, first chip with support for dual frequency capabilities ready for consumer market applications like phones, add another level of capabilities. However, the widespread deployment is still years from being fully integrated into these devices, and most wearables receivers rely in this single frequency approach. Hence, with the community moving towards this direction, it is worth asking, Is there a threat in the signal processing for single band receivers? What are the advantages of navigation system with rich frequency diversity?

Previous research highlights [1] [2] feasibility and effectiveness of cheap Personal Privacy Devices (PPD and their impact on the radio navigation signals. It can be speculated then that a system moving toward the single band navigation system by means of the Code Division Multiple Access (CDMA) exploitation is also extremely susceptible to Radio Frequency Interference (RFI)) attacks that can easily null the band usage with the press of a single button. An analysis of commercial off the shelves PPD showed how these devices can turn a wide range of CDMA signals completely unusable in its presence [2].

Another interesting case recently reported episodes of Global Positioning System (GPS) spoofing happening in the Black Sea [3]. Given the resources available, receivers can no longer simply rely in one single constellation or the other, the future relies in the design of receivers capable of mixing solutions from multiple constellations in a wide range of frequencies. Although, not the ultimate solution, it does make the work harder for malicious attack on the band. Perhaps the presence of a GLONASS capable receiver would have avoided this by allowing the system to eliminate the compromised GPS measurements and perform navigation with the aid of the GLONASS Frequency Division Multiple Access (FDMA) signals, assuming off course that the latest were not also spoofed in the area during those episodes.

Research also suggest that there are many motivations to spoof, even outside the military environments. Work developed in [4] showed that a quick search on the Google Play store shows multiple pages of applications attempting to fake GPS measurements. The first app, “Fake GPS Go Location Spoofer Free”, alone has over 91,241 reviews as of September, 2018. In addition, work developed in [5] showed how easy is to spoof the navigation solution in the phone using software radios and additional equipment totaling to less than $300 USD. The most concerning episode of spoofing in the Android domain accounts for the work developed by [6] which presents a practical spoofing of navigation services in a combination of false navigation signals transmitted and fake maps integration. This work account for the first time spoofing does not only happens in the location engine but also in the navigation engine of the device. As such, with millions of devices nowadays relying in the legacy GPS signal, a more practical solution needs to be applied. Modern Android devices with lower level GNSS measurements may have a solution to this conundrum.

In 2016 the Android framework Application Programming Interface (API) allowed access to raw GNSS measurements. Released originally under Android API 7.0, the framework gave access to multiple raw measurements including navigation messages, pseudo-ranges, pseudo-range rates, Doppler frequency, constellation status, etc. More recently and with the release of Android API 8.0, the Google framework is now also providing AGC measurements in its android.location modules. However, it is worth mentioning, that even though the Android API supports all these measurements, phone manufacturers are not forced to comply with providing those and availability of some of the measurements will vary by device.

In this paper, we develop and examine GNSSAlarm, an Android app to perform RFI and spoofing detection via a combination of methods that take advantage of native hardware inside the phone to increase the integrity of the positioning system. We initially consider the AGC measurements in the device. This set of measurements are extremely useful when detecting high power jamming and spoofing attacks and have been used in the past for detecting such kind of faulty signals [7]. In the detection process the receiver will stop providing a position solution in the affected bands, at which time the AGC could be used to detect the nature of the problem. This will then trigger a safe mode operation in the app in which the subsequent measurements will be used with the knowledge that in the presence of jamming or spoofing attacks. We will also examine the raw GNSS measurements generated by the phone and combine those into a solution that explores the potential of the sum of

squares residuals, which will add protection levels for the GNSS navigation solution. In addition, we will also look into the fused position algorithm of the framework and use those in the aid of the spoofing detection attack when cellular connection or Wi-Fi access points are available. Finally, we perform a direct comparison of the inertial sensors available inside the phone (accelerometers and gyroscopes) and use this as another set of measurements helping in the spoofing or RFI detection. This design allows for a robust and reliable system that could be used as a tool in the detection and removal of corrupted measurements in a position solution.

A series of testing exercises, where the GPS signal was either jammed or spoofed were used to validate the claims presented in this paper. Most of the experiments performed were done simulating isolated locations where cell phone service was not available and as such the device will only rely in its internal hardware sensors and its raw GNSS measurements. Exposing the phone to this environment as well as hours of nominal data that illuminate typical day to day activities will help catalog the performance of the device under such conditions and will help examine the proper level of thresholding for alarm identification when in the presence of jamming or spoofing.

PHONE MEASUREMENTS

Smartphones nowadays host a wide variety of sensors to satisfy the demands of growing market needs or applications. The multi-purpose usage of the device is cumbersome and its use is no longer limited to the telephony domain. Sensors in smartphones today include cameras, GNSS sensors, motion sensors, temperature, pressure, etc. In the same way that developers make use of those features to solve a user need, this work uses a set of sensors on the device to provide a solution for spoofing and jamming detection. Previous sections showcased documented episodes of malicious attacks, and in most cases the targeted sensors were corrupted by the fake signals. However, given that smartphones are such powerful tools, we investigate the existence of the solution on the smartphone and further discuss the sensors with potential in the identification if any type of interference attack.

Raw GNSS Measurements

Probably the most relevant set of measurements for spoofing detection in a smartphone belongs to this group. The raw GNSS engine provides a plethora of measurements ranging from AGC to code and carrier phase. Even though not all cellphone manufactures provide the whole set of measurements supported by the Android API, an increasing number of new phones seems to be providing at least pseudoranges and pseudorange rates. In conjunction with the navigation data (obtained either by parsing navigation messages or from external sources like the Receiver Independent Exchange Format (RINEX)), it can be used to generate metrics that could alert the user of anomalies with the position solution when computed in a multi-constellation scenario. Ideally will combine the raw GNSS measurements with the ephemerides data to generate pseudorange residuals (Equation 1) and pseudorange residual sum of squares (RSS) metrics (Equation 2). Figure 1 shows such metric when the receiver is operating in nominal circumstances.

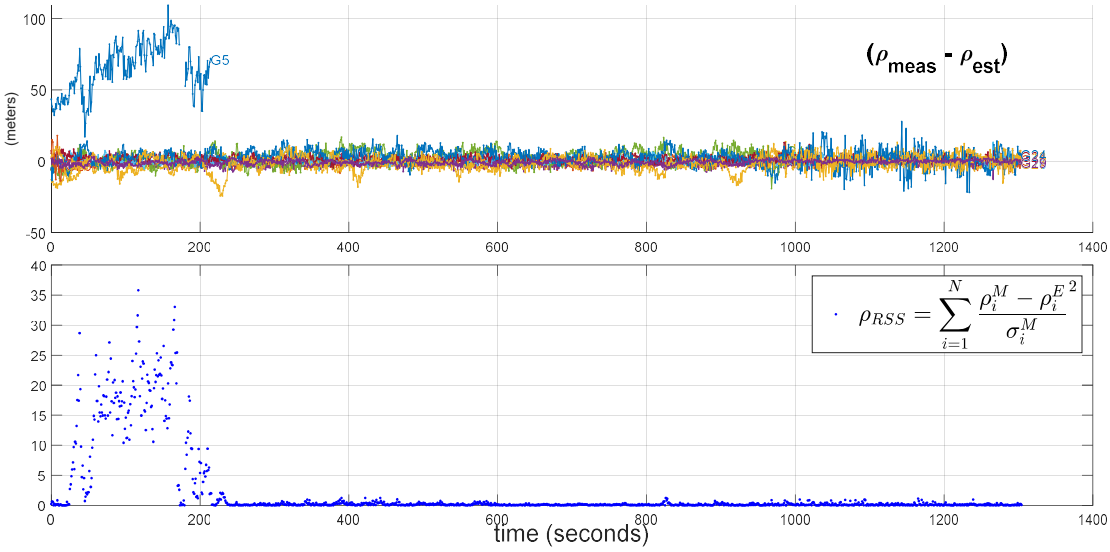


Figure 1 Sample pseudorange metric generated by GPS measurements using Pixel 2 smartphone

$$\Delta\rho_i = \rho_i^M - \rho_i^E \quad (1)$$

$$\rho_{\{RSS\}} = \sum_{0}^{N} \left(\left(\frac{\rho_i^M - \rho_i^E}{\sigma_i^M} \right)^2 \right) \quad (2)$$

where:

- » σ_i : Standard deviations of the expected pseudorange error
- » ρ_i^M : Measured pseudorange from receiver
- » ρ_i^E : Estimated pseudorange using satellite and receiver positions
- » $\Delta\rho_i$: Pseudorange residual metric.
- » $\rho_{\{RSS\}}$: Pseudorange residual sum of squares

Inertial Measurements

Nowadays Inertial Measurements Units (IMU) are present in most smartphone and wearables devices. Technological advancements on the field have allowed for a reduced cost, power, and size of the chips, translating into its insertion of mass market devices. One key component of all IMU are accelerometers, which measures the external specific force acting on the sensor. The specific force consists of both the sensor's acceleration and the earth's gravity. The low cost of the sensor in most mass market devices is bounded to the use of low accuracy devices that easily drift off the real trajectory. However, when combined with GPS measurements the solution tends to improve. The sensor measurements are commonly used for detection of motion and acceleration and as such serve as a potential trigger of spoofing detection when position walks attacks are present.

The Android API offers support for accelerometer readings in two forms: (1) raw acceleration and (2) linear acceleration. The latter is just a further processed reading where the Android OS removes the gravity components to deliver a "true" linear acceleration. Figure 2 shows the axis orientation inside typical smartphones as seen by Android. This is key to properly compute the device acceleration and direction.

Combined AGC and C/N_0 Measurements

In order to optimize the gain of the front end of the receiver to that of the analog-to-digital converter (ADC) the AGC adjusts its gain with respect to the present interference power in the channel. Consequently, it was first assessed as a useful interference detection device [7]. Monitoring the AGC has been proved to be a powerful spoofer detection tool, especially for the simplest attacks such as the overpowered approach [8]. Even though the AGC is available in all multibit GNSS front end designs, inherently to its nature, the AGC can vary depending on the effective temperature of the antenna. Then it is not sufficiently stable to define thresholds and a low false alarm probability, which is a problem when in matched power attacks.

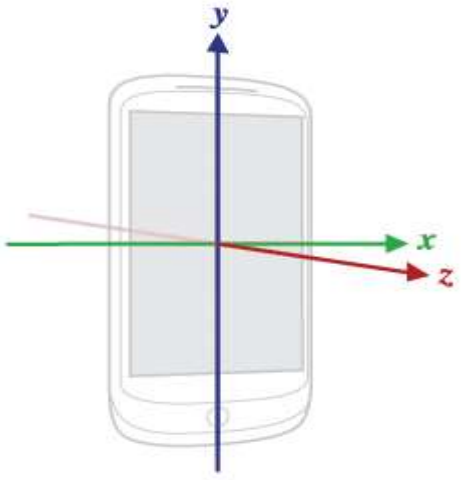


Figure 2 Accelerometer orientation axis on smartphones

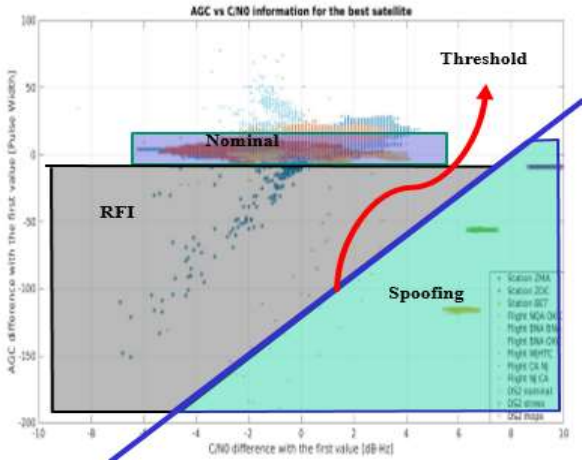


Figure 3 Combined AGC and C/N_0 detection zones

When combined with other measurements like the C/N_0, the efficiency of the detection algorithm is increased, since it will not false alarm during matched power attacks for spoofing when only RFI is present. RFI attacks, regardless of their

nature (intentional or by accident), share the common point to add additional power within the band, and so they both have a similar impact on the AGC value. The AGC is really sensitive to these RFI attacks and in order to lower the probability of false alarm a criteria to distinguish between these two forms of interference was considered. A process based upon the observation of both AGC and C/N_0 value is discussed in [7]. Indeed, even if both types of RFI lead to a drop of the AGC when they appear within the band, the way they are generated are different because of their respective nature. For a non-intentional RFI attack, the signal is not consistent with the satellite and noise is added to the GPS band, which leads to a drop of the C/N_0 of the tracked signal. Conversely, during a spoofing attack the signal is generated to look like a GPS signal. Thus, it increases the power of the carrier signal and so, it leads to a raise of the C/N_0 value.

Fused Position Engine

Android location services provides GPS and Android's Network Location Provider (NLP) to acquire the user location at any given time. Of the two sources GPS is most accurate, but it only works outdoors when visibility of GNSS satellites is available. Given the challenges offered by the urban canyon geometry, less than ideal antenna, and multipath signal reception, positioning with this source is challenging for multiple users. As an alternative Android's NLP determines user location using cell tower and Wi-Fi signals, providing location information in a way that works indoors and outdoors, responds faster, and uses less battery power. NLP although not as accurate as its GPS counterpart offers a good estimate of the location of the device even in the challenging environments mentioned before.

Location services in Android can be challenging because measurements are exposed to a multiplicity of error sources that include: (1) Multitude of location sources, (2) User movement and (3) varying accuracy [9]. The multitude of location sources is given by measurements from GPS, Cell-ID, and Wi-Fi, where each provide a clue to user's location with varying levels of accuracy, speed and battery efficiency. The user movement also impacts the solution because the user location changes, and algorithms must account for movement by re-estimating user location every so often. Finally, the accuracy of each measurement varies depending on the source and the time of last update. *Figure 4* shows the location algorithm used by Android for position estimation.

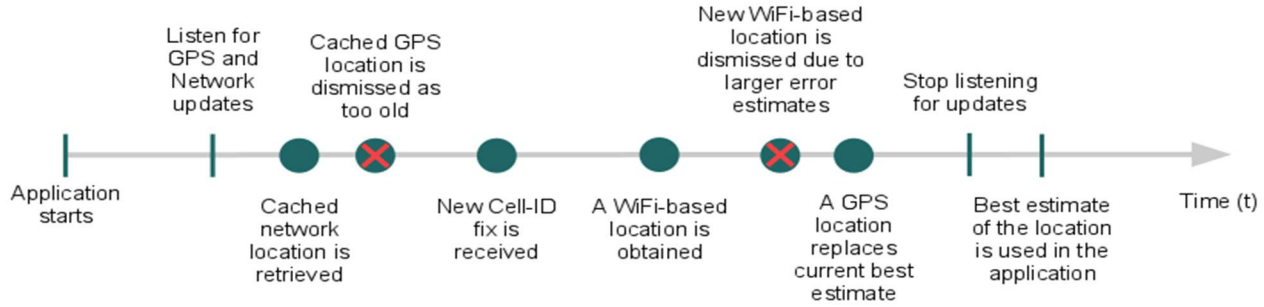


Figure 4 Android's fused location engine with a combination of sources including GPS and NLP.

EXPERIMENTAL SETUP

Multiple scenarios were designed to test the system targeting specific group of sensors. In order to expose the cellphone to the wireless data transmitted a radio frequency shielded box was used, and inside it a cellphone supporting raw measurements logging and a UBlox receiver were placed. After multiple scenarios, as listed in Table 1 were tested. The phones used in the experiment included the Google Pixel 2 and the Huawei P10. Each phone has a set of features lacking its counterpart, for example Google Pixel 2 is the only phone in the market to support AGC measurements, while Huawei P10 offers multiple measurements across the full set of GNSS constellations, including ephemeris data.

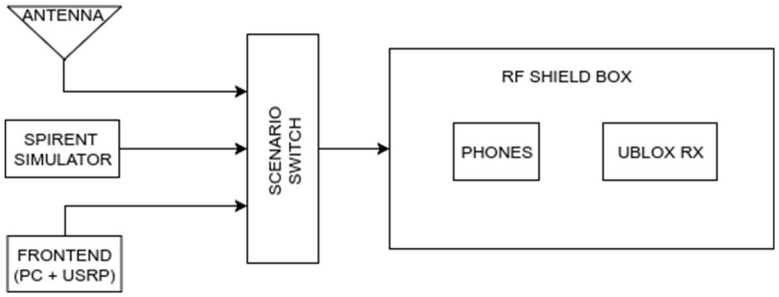


Figure 5 Experimental setup to validate test cases scenarios described below

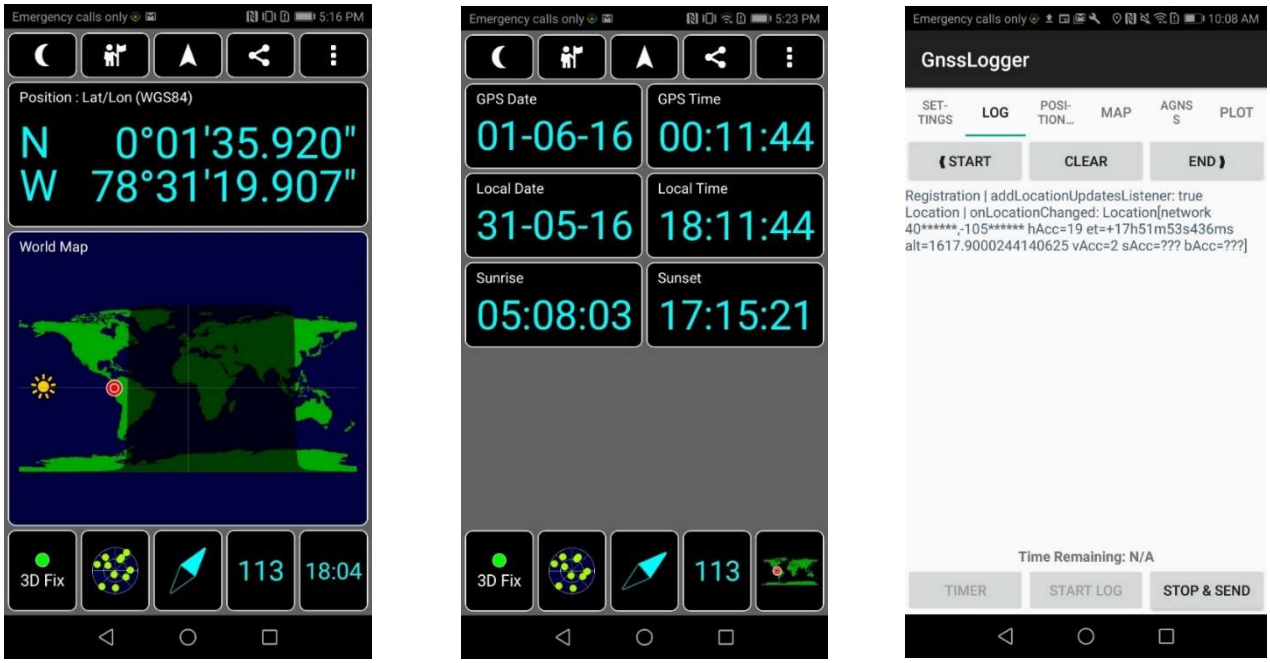
Table 1Test scenarios description stressing different triggers reporting spoofing or jamming attacks

Scenario	Target	Observations
Network-Spoof	Network and Location Engine	Phone spoofed with simulated driving scenario. Time regression and position jump
AGC-C/N_0-Spoof	AGC and CN_0 measurements	Phone collected data during nominal performance and controlled RFI attacks
Residual-Spoof	Raw GNSS measurements (nav. data, pseudoranges, etc)	Used replayed Texas Spoofing Test Battery (TEXBAT) data sets [10], focusing in scenarios **ds2** and **static clean**. UBlox receiver used for measurement generation as Pixel 2 and Huawei P10 phone did not support SBAS measurements.
Accelerometer-Spoof	Accelerometers	Replay driving scenario to phone in box while also collection accelerometer measurements internally.

RESULTS

Network Position

The location engine in the Android Operating System (OS) gives a higher level of priority to measurements from the GPS chipset on the phone. GPS offers a more accurate position solution than what the network engine can offer. However, under spoofing attacks, the GPS position quickly becomes compromised and measurements from time and position are invalid. Figure 6 (a) and (b) show the reported position and time of a phone that has been spoofed by a fake signal transmitted in a controlled scenario. In case (a), the phone does not have access to any type of network connection, i.e. airplane mode, and the only source for positioning and timing comes from the GPS engine. However, in case (b), when the phone is exposed to the same signal as in (a), and have access to a Wi-Fi connection we also notice the spoofed position and time. When this happens, the network connection still shows a rough estimate of the true position of the phone (c). Although a rough estimate, the network position on the phone is an effective trigger of anomaly when time and position information from both sources diverge.



(a) No network connection (Airplane mode enabled)

(b) Network connection (Wi-Fi enabled)

(c) Network positioning with Wi-Fi connection

Figure 6 GPS and Network location provided under multiple connectivity modes and spoofing attacks.

Combined AGC and C/N_0 Measurements

The combination of AGC and C/N_0 measurements worked as a RFI detector under the test cases evaluated. Nominal data collected was used to assess the typical operational zone of the phone's AGC under daily use activities. Then, the data was compared to the readings obtained during a jamming scenario. Figure 7 shows the results of this operation, as shown, when the jamming attack happens the AGC measurements of the phone are increased drastically while a drop on the C/N_0 is also seen. Those symptoms will trigger immediately the alarm on the app as a clear indicator of a problematic behavior. The case for the spoofer detector was more difficult to test because reproducing the adequate signal levels in the phone through the RF shielded box is a difficult task given the limited gain in place for the cellphone antennas. Testing the spoofer detector levels under open sky conditions with the phone remains an important future addition to this work.

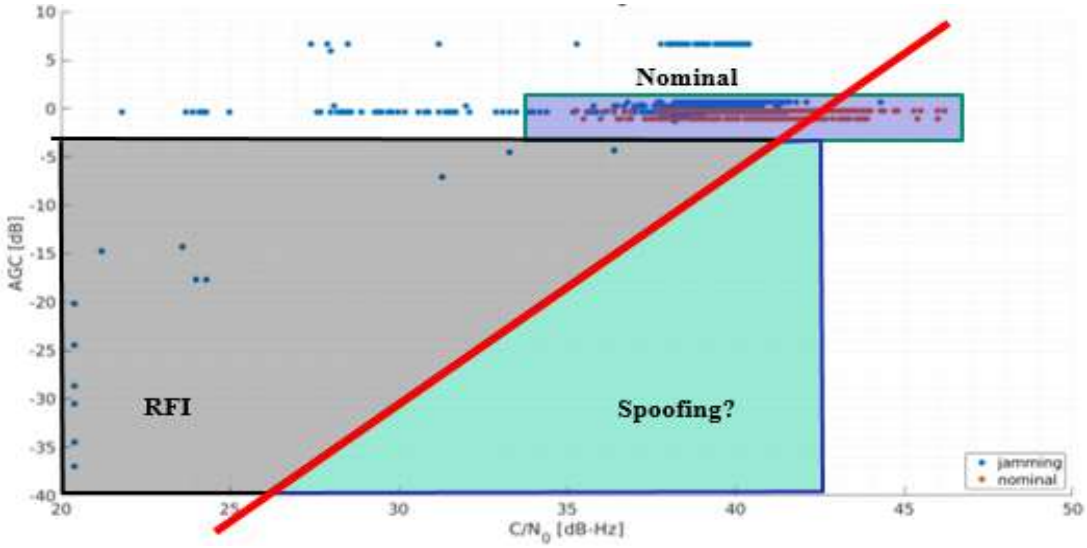


Figure 7 Combined AGC and C/N_0 metric for jamming and overpowered spoofing detection

Pseudorange Residuals

Testing of the pseudorange residuals was done using the TEXBAT datasets and a multi-constellation Ublox receiver. This scenario was designed to take advantage of the nature of the TEXBAT datasets where spoofing only happens in the GPS L1 C/A signal. The situation is a common deficiency of most spoofers in use in the sense that only the GPS signal is spoofed. Since spoofing the full set of signals in the radio navigation band is more challenging, this simple approach proposes a residual cross check across constellations.

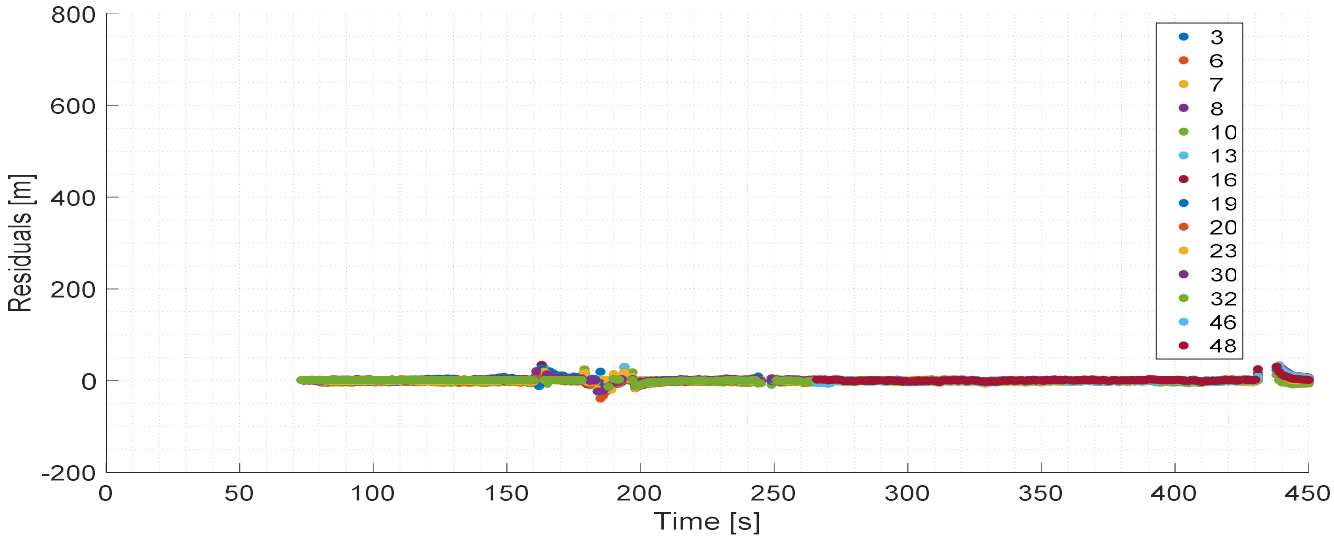


Figure 8 Pseudorange residual metric for static clean dataset in TEXBAT when using a solution of GPS and SBAS satellites

Figure 8 showcases the pseudorange residual metric for the static clean set in TEXBAT. Of relevance I the fact that the residuals test is done using the GPS and SBAS constellation. Pseudorange residuals in this case and for a combine solution do not show significant discrepancies as expected since the replayed dataset is the one for a clean collection. However, Figure 9 shows the results of the same metric but when the receiver is exposed to the ds2 scenario (overpowered spoofed attack). If only looking at the residuals from GPS, it can be seen that because the spoofer was acting on the L1 C/A signal alone no discrepancies happened between the estimated and measured pseudoranges. Nevertheless, the SBAS satellites immediately showed a discrepancy between measured and estimated pseudoranges as the spoofed signal did not manipulated this constellation.

The results from this test are intended to show the richness of this simple approach in which a simple cross constellation check can alert the user of dubious operation. The method was not tested in a smartphone because at the moment of this writing there was not Android device supporting measurements from SBAS constellation. Regardless of it, the Android Hardware Abstraction Layer (HAL) has fields supporting SBAS measurements and as such will end up gaining support in the future. In addition, the method can also be applied to other constellation combination including Galileo, GLONASS or Beidou.

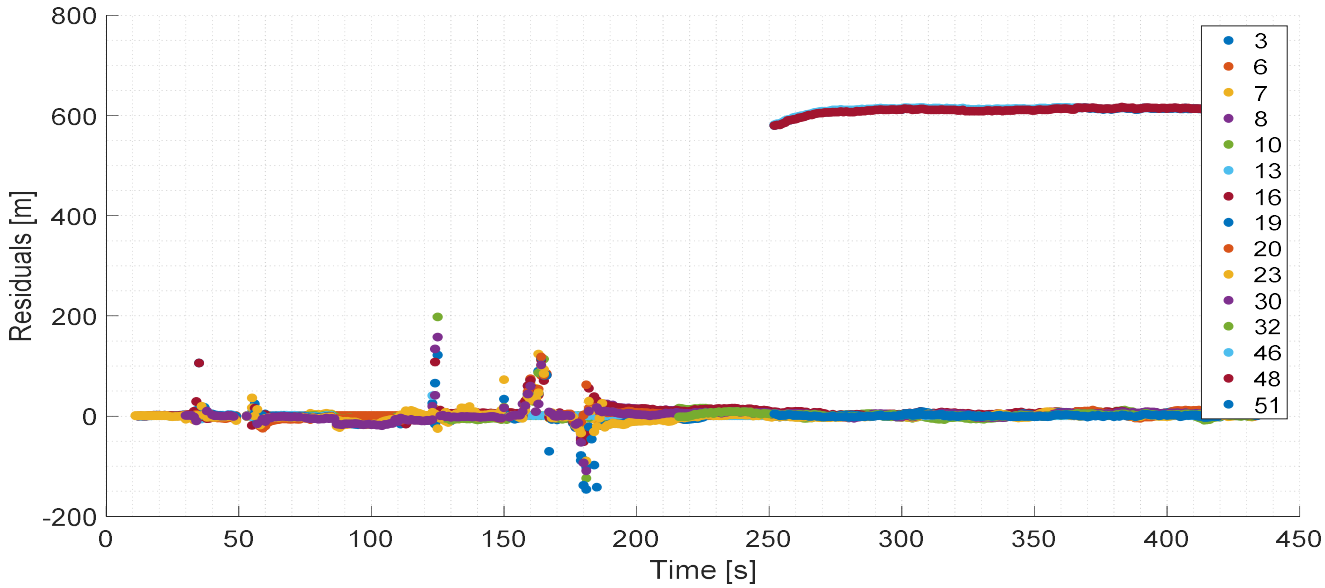


Figure 9 Pseudorange residual metric for ds2 dataset in TEXBAT when using a combined solution of GPS and SBAS satellites

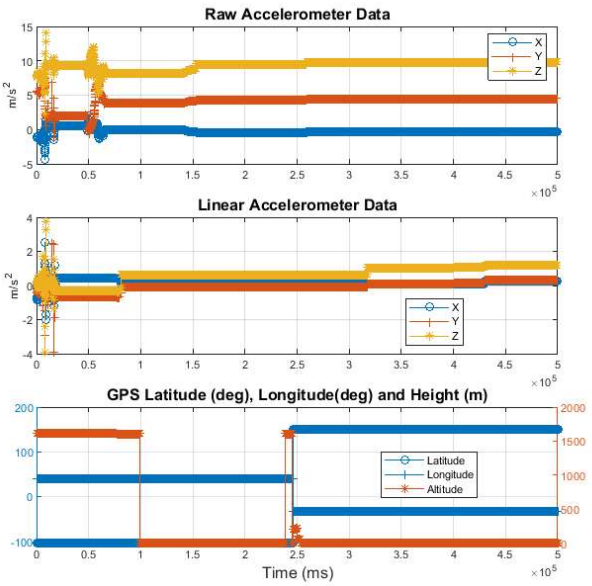
Accelerometer Data

Another potential alarm trigger for the app comes from the accelerometer data from the device. Under position walk attacks, the receiver reports movement that deviates it from its true position. Accelerometer data can then be used to detect changes in the acceleration and then report that to the receiver as a trigger of false movement. Figure 10 shows the accelerometer readings (raw and linear acceleration), and GPS position reported by the device. The difference between the two plots is that (a) shows data collected when smartphone was being spoofed and a driving simulation was running. The change in speed and acceleration will be shown in the GPS position but not in the change on acceleration seen by the device. On the other case (b) shows the case when collected data was in a real driving scenario and the change in position and acceleration is shown by both sensors GPS and accelerometers. Although the results from these tests are not as promising given the quality of the accelerometers which requires higher dynamics, as per the previous cases they still represent a significant source of malicious positioning reporting. Further development on the analysis of these measurements needs to be considered as to avoid reporting on false alarms based on this set.

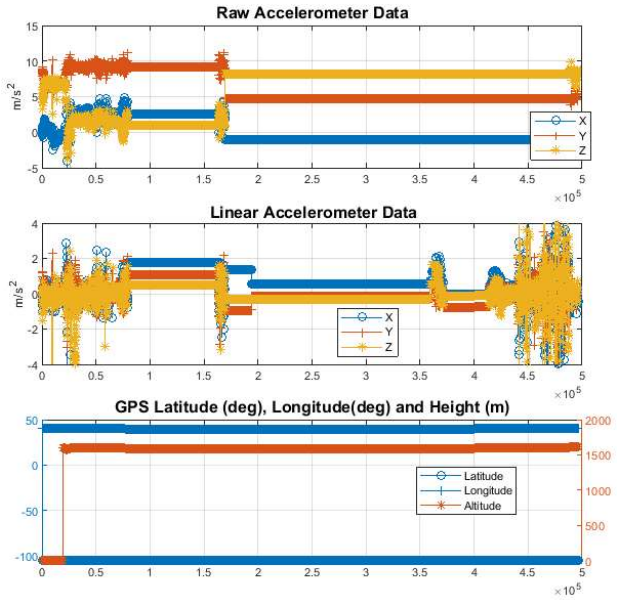
GNSSALARM APPLICATION

At the moment of this writing the GNSSAlarm app was still under development. However, key components of the app are illustrated in Figure 11. Part (a) shows the graphical interface of the app where the four trigger trends previously discussed are shown. In addition, part (a) will display an alarm indicator with lamps that will activate depending on the type of interference detected and the certainty on the reported metric. Part (b) shows a push notification type message that will also alert the user if the app is running in the background. This push notification alert will also serve to disregard false alarms notification by the

app. Finally, part (c) shows the crowdsource RFI localization feature when multiple devices in the area under interference are connected and sending information to a processing server that will notify on the location of the emitting source. This feature builds upon the work developed in [12], which used smartphones for localization purposes, and integration of the technology is underway.

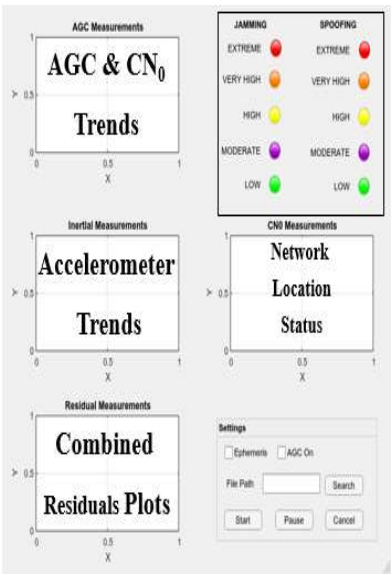


(a) Accelerometer and GPS logs in a simulated driving scenario. Linear and raw acceleration logged.

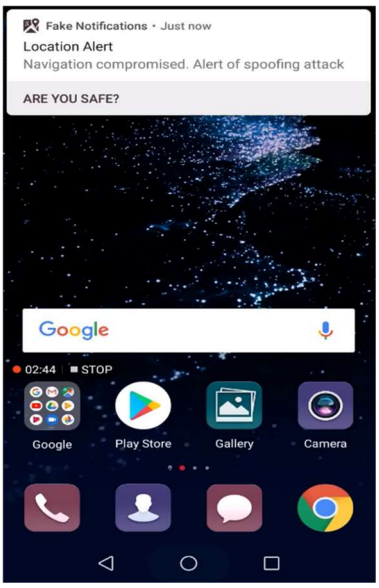


(b) Accelerometer and GPS logs in a real driving scenario. Linear and raw acceleration logged.

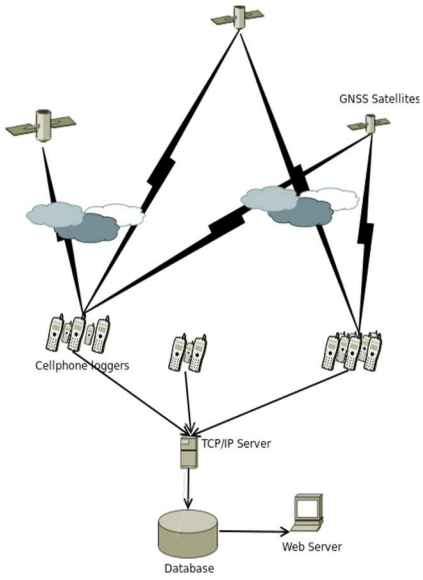
Figure 10 Acceleration measurements reported by smartphone during simulated and experimental driving scenarios



(a) Graphical interface monitoring alarm trigger and interference type status



(b) Push notification alert when jamming or spoofing is happening



(c) Crowdsource RFI localization using multiple smartphone devices

Figure 11 GNSSAlarm main features and components under development

CONCLUSIONS

The sensors considered during this study, showed the potential they have as a tool for spoofing and jamming detection. Inertial sensors on the phone like accelerometers are ideal for monitoring acceleration and as such serve as a trigger alarm against position walks attacks. The combined metric of AGC and C/N_0 is ideal for detection of strong RFI interference, but a more detailed study of the AGC measurements per phone is required so that effective thresholds could be defined. Position and timing though Android's NLP should play a more essential role in the overall device solution computation as if offers a coarse yet accurate measure of the location of the device. The assurance provided by the NLP is an excellent resource against position or time jumps. Finally, the biggest potential resides in the raw measurements supported by the latest Android devices, the simple pseudorange residual metric showed its potential against the standard spoofing datasets used in the community. In addition, these set of measurements could also be integrated into more complex solutions like Advanced Receiver autonomous integrity monitoring (ARAIM) solutions or serve as a secondary source for receiver positioning when legacy constellations are compromised.

There have been multiple documented cases showing the ease of spoofing the cell phone navigation engine within Android OS. Upon the new threat imposed by these types of attacks, the use of a "black box" ASIC GNSS engine delivering only a position fix or National Marine Electronics Association (NMEA) 0183 messages is limited in providing the needed GNSS integrity. The current set of messages are only limited to the use of the GPS L1 C/A signal and do not consider into the position solution the measurements from any of the other constellations available worldwide. As such, a simple attack on the GPS signal could null out the reliable position to thousands of users in the area. Google moves to incorporate raw GNSS measurements adds significant value to GNSS integrity because the new set of measurements can be combined with other sensors within the Android OS for integrity but also for localization and detection via crowdsourcing. Although under still under development at the moment of this writing GNSSAlarm will offer the first of its kind app capable of detecting spoofing and jamming attacks. We expect that, in multiple scenarios, it will eventually be capable of secure navigation even under the presence of compromise signals in the band.

ACKNOWLEDGMENTS

This material is based upon work partially supported by the National Science Foundation Graduate Research Fellowship under Grant No. DGE 1144083

REFERENCES

1. Fonzo, A. D., Leonardi, M., Galati, G., Madonna, P., and Sfarzo, L., "Software-Defined-Radio techniques against jammers for in car GNSS navigation," *2014 IEEE Metrology for Aerospace (MetroAeroSpace)*, 2014, pp. 320–325. doi:10.1109/MetroAeroSpace.2014.6865942.
2. Kraus, T., Bauernfeind, R., and Eissfeller, B., "Survey of In-Car Jammers - Analysis and Modeling of the RF Signals and IF Samples (Suitable for Active Signal Cancelation)," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, OR, 2011, pp. 430–435.
3. Stan Goff, "Reports of Mass GPS Spoofing Attack in the Black Sea Strengthen Calls for PNT Backup | Inside GNSS News,", 2017. URL http://www.insidegnss.com/node/5555.
4. Lo, S., and Yu, H. C., "The Benefit of Low Cost Accelerometers for GNSS Anti-Spoofing," *Tech. rep., Stanford University, Palo ALto, CA, 2015.*
5. K. Wang, S. Chen, and A. Pan, "Time and Position Spoofing with Open Source Projects," *in Black Hat Europe, 2015, vol. 148.*
6. Zeng, K. C., Shu, Y., Liu, S., Dou, Y., and Yang, Y., 2017. "A practical GPS location spoofing attack in road navigation scenario". *In Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications, HotMobile '17, ACM, pp. 85–90*.
7. Bastide, F., Akos, D., Macabiau, C., Roturier, B., "Automatic Gain Control (AGC) as an Interference Assessment Tool," *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, Portland, OR, September 2003, pp. 2042-2053.
8. Akos, D. M., "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)," *NAVIGATION, Journal of the Institute of Navigation*, Vol. 59, No. 4, 2012, pp. 281–290.
9. Android Developers, "Location Strategies." [Online]. Available: https://developer.android.com/guide/topics/location/strategies.html. [Accessed: 05-Apr-2018].

10. Humphreys, Todd, Bhatti, Jahshan, Shepard, Daniel, Wesson, Kyle, "The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques," *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 2012, pp. 3569-3583.
11. Lemmenes, Adam, Corbell, Phillip, Gunawardena, Sanjeev, "Detailed Analysis of the TEXBAT Datasets Using a High Fidelity Software GPS Receiver," *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, Portland, Oregon, September 2016, pp. 3027-3032.
12. Strizic, Luka, Akos, Dennis M., Lo, Sherman, "Crowdsourcing GNSS Jammer Detection and Localization," *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, Reston, Virginia, January 2018, pp. 626-641.