Tests of Crowdsourced Smartphones Measurements to Detect GNSS Spoofing and Other Disruptions

Sherman Lo, *Stanford University*, Yu Hsuan Chen, *Stanford University*, Dennis Akos *Stanford University and University of Colorado Boulder*, Brandon Cotts, *University of Colorado Boulder*, and Damian Miralles *University of Colorado Boulder*

BIOGRAPHY (IES)

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. He was awarded the ION Early Achievement Award.

Yu-Hsuan Chen is a research engineer at the Stanford GPS Laboratory. He received his Ph.D. in Electrical Engineering from National Cheng Kung University, Taiwan in 2011.

Brandon Cotts is a graduate of the Department of Aerospace Engineering Sciences at the University of Colorado Boulder. He received a B.S.

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.

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.

ABSTRACT

GNSS spoofing is a growing concern due to the increasing use of GNSS in safety and economically important applications. The widespread use of GNSS in these tasks means that GNSS needs to be protected from spoofing in many location. Even with the most basic task of GNSS spoof detection, it is generally difficult and costly to have a rapid and widespread response. An attractive way of addressing the challenge is to harness the most widespread and lowest cost GNSS receivers, those found in smartphones, to help with spoof detection. Further enhancing this potential are the raw GNSS measurements enabled by the latest versions of Android (7.0 and above). The capability and ubiquity of these GNSS receivers along with the connectivity and alternative navigation sources found in smartphone makes a crowdsourced network both powerful and reasonable. This paper examines the potential of these crowdsourced, networked smartphone measurements for spoof detection. Specifically, it focuses on tests of the crowdsourced detection concept using different smartphone measurements and multiple smartphones. It examines several available measurements: 1) position, 2) acceleration (from GNSS and accelerometer), 3) automatic gain control (AGC) and carrier to noise (C/No) levels and 4) pseudo ranges. These are examined on both a standalone and a networked, cross receiver basis. These are examined using measurements taken from laboratory and field tests, including an on air spoofing test.

INTRODUCTION

GPS and GNSS is well integrated into our society. This integration is only going to increase in the future. It is part of our critical infrastructure for timing communications, power grids and financial transactions. It is critical for aircraft navigation. Its use as a safety of life navigation source in railway control and autonomous vehicles is increasing. It also supports hobbies and location based games such as Pokémon Go. But its popularity and ubiquity is also makes it a target for many. The widespread use of position in many consumer applications (i.e. Uber) also creates financial incentives for spoofing GNSS [1][2][3]. Deliberate disruption of GNSS, either jamming or spoofing, can have wide ranging effects making it a potential target for malicious individuals. Even people without malicious intent, looking to only disrupt GNSS due to privacy concerns or gaming advantage, may inadvertently affect safety and economically critical uses of GNSS. Hence it is important for safety and economic considerations that such these deliberate disruptions and degradations be identified and terminated as soon as possible. An attractive idea is to use crowd-source GNSS information from smartphones to provide rapid detection and localization of degradation events.

Many characteristics of smartphones make them a good building block for a responsive GNSS interference detection system. Their ubiquity helps with detection even on a small scale and where disruption may have the worst effect. Indeed, as these devices are carried by people, they are most densely located where people are most densely located. Since there is a high density of devices in many areas, even a small, localized disruption may be observed by some devices. Hence, they may be useful to detect smaller interference events. Second, they have many sensors and outputs that can aid in detection. Inertial sensors can help detect outlier positions. Recent versions (as of 2017) of Android will support outputs such as carrier phase, pseudo ranges, and automatic gain control (AGC) levels. These can also be used to discriminate between natural sources of degradation such as multipath, shadowing or being indoors and deliberate sources. Third, they are networked which means we can leveraged the power of many such devices to do cross checking and localization.

This paper discusses and examines our preliminary developments and testing with using smartphones to perform crowd-sourced detection and localization of interference, focused on spoofing. A smartphone app capable of capturing GPS observables from Android smartphones was developed to support this endeavor [4]. It can obtained and upload all GNSS observables provided by the smartphone including satellite or pseudo random number (PRN), carrier to noise ratio (C/No), position as well as network location and other location information. It is built to capture data that are supported in Android version 7 and 8 such as pseudo range, carrier phase, and AGC levels if they are provided. It can push this data to a server and stores a local copy as a backup. Using this application, we examine three aspects of using crowd-sourced measurements to detect jamming and spoofing: 1) network comparison of GNSS positions and C/No, 2) networked acceleration comparisons and 3) AGC to minimize false alerts from natural causes of signal degradation. These results are based on field data collect in government sponsored interference exercises conducted in 2017.

Our prior papers covered crowdsourced interference detection [4] and single receiver detection methods [5] so this paper will focus primarily on spoof detection via crowdsourced, networked based solutions. Specifically it examines comparison of positions, measurement discrepancies, inertial and continuity. It outlines the performance and challenges of crowd-source smartphone measurements for GNSS spoof detection. It utilizes on-air data to show some of the different behaviors found and examines means of managing these behaviors to create a robust detection system.

2. BACKGROUND

GNSS Localization

An important step to mitigating radiofrequency interference (RFI), be it jamming or spoofing, is detection and localization. How can the detection and localization be accomplished? In the past, such as the interference event at Moss Landing (2003) and Newark (2009, 2012), it took a directional antenna and hours, days or even months of manual effort to localize due to several factors [6][7]. As the interference is intermittent, detection equipment needs to be in place and ready for operations. In the early incidents, even a simple directional antenna with a detector took time to get. To expedite detection, we proposed using an unmanned aerial vehicle, known as Jammer Acquisition with GPS Exploration and Reconnaissance or JAGER, to find the interferers. JAGER could fly a find jammers though it was. Another possible rapid response is to use dedicated infrastructure. An example is the Signal Sentry system built by Exelis (now Harris) which was test deployed at the Superbowl held in the Meadowlands, New Jersey, shown in Figure 1, as well as a few other venues [8]. This system has demonstrated its capabilities in several field tests [8] and can work well but it would be costly to scale up. To cover the couple square miles, it has many fixed stations with communications infrastructure.

Another approach proposed is to use mobile assets to crowdsourced measurements. First, this approach can offers many observers and observables – especially with recent Android additions. Furthermore, it is potentially low cost and easy to deploy and scale as it only requires an app download to add another observer. There are several drawbacks to the approach relative to fixed, dedicated assets. The system is not homogeneous with less controlled and noisier measurements. While smartphones GNSS receivers are powerful receivers, they are not reference or survey grade receivers nor have the high quality antennas that would be employed in a dedicated detection system. Furthermore, smartphones may be moving and inside purses and pockets making their GNSS measurements both more difficult to use for some detection techniques (i.e. acceleration comparison) and weaker relative to fixed assets. It is also ad hoc and its deployment may not be ideal to provide guaranteed protection of specific sites. That being said, existing Android cellphone users can provided useful measurements and additional units can be fielded with relatively low costs. As the old saw goes, "quantity has a quality all its own."

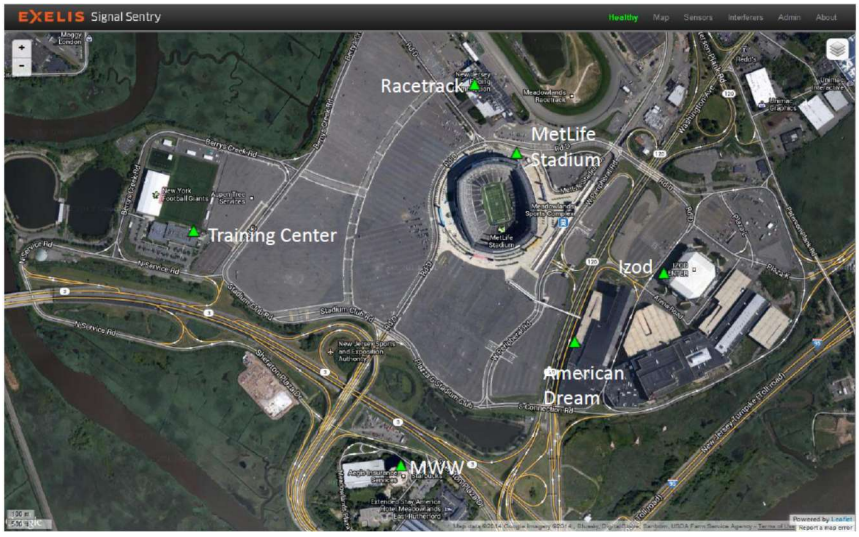

Figure 1. Exelis Signal Sentry 1000 deployed in Meadowlands, NJ [8]

Android App and Observables

While the idea of using smartphones for crowdsourced GNSS interference detection has been around [4][9], new developments in the Android operating system (OS), since Android 7.0 or Nougat, has allowed users to access many GNSS related observables that were previously unavailable. It provides additional powerful means for spoof detection. Prior to Android 7.0, position, the most relevant available observables for detection are position, velocity, C/No and satellite available. Android 7.0 offers pseudo range, pseudo range rates, carrier phase measurements and others. Android 8.0 added AGC measurements. This is shown in Table 1. These observations make the smartphone an even more powerful interference detector and provides stronger capabilities to identify and distinguish between spoofing and jamming. It is important to note that the observables available from the phone depends not just on the version of Android operating system but also on what the phone original equipment manufacturer (OEM) and the GNSS chipset maker provides. For example, while there are many phones operating on Android 8.0, only the Google Pixel 2 and 3 smartphone series currently provide AGC measurements enabled by this OS version. Available measurements on specific models are provided in https://developer.android.com/guide/topics/sensors/gnss.

Table 1. Android OS version and potential available observable for GNSS interference and spoof detection

Android Version	Benefits	GNSS observables
6 "Marshmallow" and earlier	Basic GNSS measurements	Position, Velocity C/No, satellite/constellation
7 "Nougat"	Raw GNSS measurements	Pseudo range and pseudo range rate, Navigation messages. Accumulated delta range or carrier. Hardware (HW) clock.
8 "Oreo"	Automatic Gain Control	AGC

Each generation provides even more possibilities. Soon all US phones will have access to Galileo measurements. On November 15, 2018, the US Federal Communication Commission (FCC) has approved a waiver allowing the use of Galileo signals on non-federal US GNSS devices [10][11]. While this has been built into chipsets for many years and available around the world, this decision finally allows US smartphones access which provides us the use of these signals to aid RFI detection. In fact, the Google Pixel phones, as of January 2019, are now able to use Galileo in the US. Additionally, Android has built into the protocol access to these observables on multiple frequencies and the first multi-frequency mass market smartphone, the Xiaomi Mi 8, is now available and utilizes L5.

The most basic processed measurements provided by all receivers are position, velocity, and, by extension, acceleration. These measures can be used for detection of jamming or spoofing in a standalone receiver, however, it may be hard to have confidence in the detection and discrimination from a single receiver given the variety of conditions it may experience. This is particularly true for smartphones that are constantly moving around in different orientations and environments. For example, a jump in position or velocity may be due to spoofing or it may be due to multipath. Loss of signal may be due to jamming but it may also be due to blockage from foliage, tunnel, buildings or going indoors. Pseudo ranges and pseudo range rates can provide a more precise look based on individual satellites but this measure suffers from the similar limitations. Acceleration comparison is another possibility as practically all smartphones, including the cheapest, utilize three axis microelectromechanical systems (MEMS) accelerometers to manage screen orientation. Comparison between GNSS- and accelerometer-derived accelerations is another potential measure for standalone and networked based spoof detection. As we shall see later, individual discrepancies between GNSS and accelerometer acceleration, even if large, does not guarantee that there is spoofing.

Another useful set of measurements are receiver signal parameters such as AGC and C/No [12][13]. As discussed later, AGC and C/No can be a good indicator of jamming and spoofing for a standalone receiver. Ideally, they are used together as this combination can differentiate between jamming and spoofing. AGC gain is set to keep the power entering the receiver relatively constant. Hence decreased gain indicates more power is entering the antenna. Thus it can be used to determine the relative amount of energy entering the antenna. If we use C/No, then it can help tell whether the increased energy is due jamming or spoofing or something else.

The utility of crowdsourced, networked detection is the fact that we can compare across multiple receivers to see if something is systematic. The effects of many natural events depend on individual locations and times and generally will befall different receivers at different times. However, deliberate interference or spoofing should manifest in all affected receivers almost simultaneously. For example, if all local receiver simultaneously lose positions or have position jumps, this is a strong indication of interference or spoofing. This paper focuses on the crowdsourced aspect of spoof detection.

The networked approach can also enhance several desirable features of spoof detection. The first is that it can allow for more steady state detection tests – tests that detect spoofing even well after it has been initiated and has captured the receiver. Some tests, such as range, position or acceleration consistency tests, only can detect on the initial onset of spoofing where the receiver is transition from the genuine to the spoof signals. These tests are termed transient tests and do not work once the receiver has been completely captured. But, across multiple receivers, indications of spoofing that may be equivocal during after capture, such as a slightly lower AGC value or C/No changes may still provide useful detection when examined across multiple affected receivers. The network approach can also help with other important metrics such as low missed detection and false alert rates. Very low false alert rates are vital as any alert reduces system availability. False alerts are a tax on the user, especially since spoofing is currently exceptionally rare. Too high a false alert may make the user distrust the receiver warnings or even dislike the spoof detection feature. Measurement and spatial diversity provided by the crowdsourced networked approach should help develop robust, meaning low missed detection and false alert, GNSS spoof detection. Finally, smartphones are attractive for GNSS spoof detection because of the many measurements available and the relative ease of fielding and crowdsourcing these measurements.

3. EXPERIMENTAL SET UP & TESTING OVERVIEW

While we can conceive of many means to use crowdsourced receiver measurements for RFI detection and localization, real receivers and scenarios often do not conform to our idealized conception of their behavior. To test some of the concepts we acquired several smartphones and develop an app to capture available GNSS data from the device [4]. The bespoke app,

termed GNSSLogger like the Google developed app it was based on, was used to gather available GNSS, network and hybrid position data. Additionally, it can gather raw GNSS measurements if available. The app can be set to store locally or send to server. Additionally other apps were used to collect sensor data. Specifically, the now unavailable "sensor track" app was used to collect accelerometer, orientation and GNSS data. Similar apps for sensor data collection such as Sense-It are available on the Android store.

Equipment

The smartphones used for most field tests with on air jamming or spoofing were low cost Alcatel Ideal (ALC). Also available were Samsung Galaxy Note 3 (GN3), LG Aristo (LGA). These phones were generally on Android version 6 or earlier which means they only had access to position, satellites, and C/No. After these field tests, we obtain a Google Pixel 2 and Pixel 3 XL which are on Android 8.0 or higher which allowed us access to additional measurements such as pseudo ranges and AGC. All phones used could support our GNSSLogger app and sensor data app. These apps can detect the measurements available on the phone and collect only those supported measurements. Table 2 shows the phones used, the Android version installed at the time of testing and available measurements.

Table 2. Smartphones used and their available measurements at time of field tests

Smartphone	Android Version	Available Measurements
Alcatel Ideal	6	Position (GNSS, Network, Hybrid), C/No, Accelerometer
Samsung Galaxy Note 3	5	Position (GNSS, Network, Hybrid), C/No, Accelerometer, Gyroscope, Magnetometer, Barometer
LG Aristo	6	Position (GNSS, Network, Hybrid), C/No, Accelerometer
Google Pixel 2	8	Position (GNSS, Network, Hybrid), C/No, Accelerometer, Gyroscope, Magnetometer, Barometer, GNSS Raw Measurements, AGC

Field Testing

Empirical tests were conducted at several different locales with various smartphones. Laboratory and field experiments were conducted with the Google Pixel 2 and 3 to examine AGC performance. Interference tests were conducted in a small anechoic box. Field tests under nominal conditions were conducted in 2016 and 2017 in the San Francisco Bay area with measurements taken onboard the local commuter train, Caltrain, used for comparing smartphone GNSS and accelerometer accelerations. A modified Samsung Galaxy Note 3 was used with an example set up shown in Figure 2.

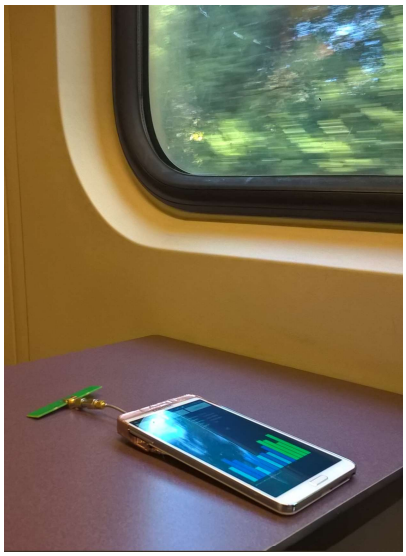

Figure 2. Samsung Galaxy Note 5 data collection on Caltrain

On air spoofing tests were conducted at government sponsored interference exercises in 2017. In the spoofing exercise, a spoofed signal was transmitted into a targeted area to minimize effect on other parties. The equipment under test operated in the targeted area. Many different spoofing scenarios were conducted affecting either position or time. GPS was spoofed, but other signals such as the Wide Area Augmentation System (WAAS) or GLONASS were typically not. Jamming sometimes occurred prior to spoofing. Furthermore, since our victim receivers are in spoofed zone, their locations are roughly known.

These smartphones were fielded statically at several locations in the spoofed zone as seen in Figure 3. Our bespoke app was operated on each phone with the app and was set to store data locally as our test area did not have cellular connectivity. While five phones were fielded, different Android phones have different implementations and settings for sleep mode. The Alcatels are basic phones that generally did well recording continuously however other phones would stop recording after one hour presumably due to their power management systems.

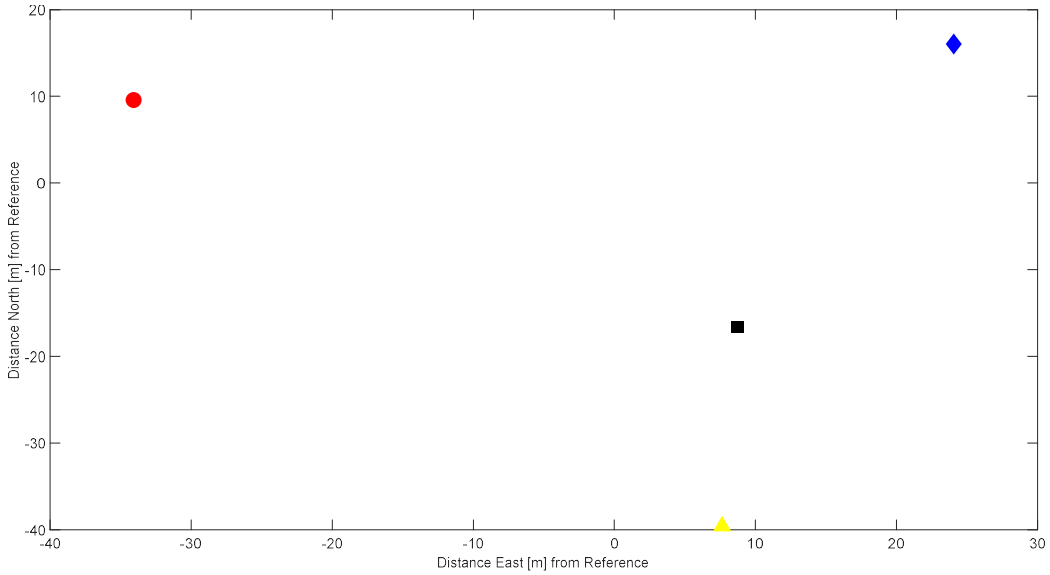

Figure 3. Static relative positions of static Alcatel smartphones during spoofing scenarios presented

4. RESULTS

We examined some of the possible measures for spoof detection previously discussed using the various data collection efforts. First, we examine GNSS position and position comparisons across several affected smartphones. We will see that this method has some utility but has significant limitations by itself. Next, we examine comparison of acceleration derived from GNSS and MEMS accelerometer to provide a way of getting additional information. Receiver measures such as AGC and C/No provides independent metrics for interference and spoofing detection. These can be utilized together or individually across multiple smartphones. A fourth possibility is to use pseudo range measurements allows us to overcome one of the issues with position comparisons.

Position

Position, and by extension velocity, is a measurement available on all smartphone GNSS as that is their raison d'etre. Examining GNSS position on a standalone receiver cannot provide robust spoof detection. While some spoofing may cause position jumps, such jumps may also be caused by natural sources. Smartphones are often moving in urban areas which can satellite ranges to have come in and out and have multipath resulting in position jumps. Smart spoofers may be surreptitious enough not to cause jumps. But we can use comparisons of positions across many smartphones to help detect spoofing.

A simple approach is to compare smartphone positions. One may expect to see receivers experiencing the same spoofing signals to output the same position. However, this phenomena generally does not occur, even if the receivers are exactly the same and are experiencing the same spoof signal. Figure 4 shows the calculated positions of three Alcatel Ideal smartphones

experiencing the same set of spoofing scenarios over the course of several hours. The figure is zoomed out of the area where the phones are actually deployed so locations outside of the exact center are spoofed location. The figure shows that the phones often do not report the same spoofed position. There are many reasons for the difference. The same jamming and spoofing can affect smartphones differently based on their relative location, hardware and even the internal operating state of the receiver, such as the state of the positioning engine. Each receiver may weigh of each signal differently depending on past history. For example, GLONASS is not spoofed or knocked out during the scenarios shown in the figure. So one potential contributor to the difference seen in the figure is that each receiver weighs the genuine GLONASS pseudo ranges differently relative to the spoofed GPS signals. So we need to be more sophisticated about the comparisons to have robust detection techniques.

Rather than expecting positions to converge, another metric may be to look for position changes that occur near simultaneously. Figure 5 shows a plot of the position changes over time for the set of spoofing scenarios that resulted in the previous figure. The red overlay blocks indicate the approximate periods when there is on air spoofing with each block representing a scenario. Looking at the scenarios sequentially, scenarios 1, 2, 4, 6, 7 and 11 are position spoofing scenarios whereas the others aim to affect time only. Scenarios 4 and 6 are position jumps while the others position spoofing scenarios walked off the position. Note Scenario 0 was a calibration or synchronization scenario with a spoofed signal that did not try to change position or time. Scenarios 1, 2, 3, 4, and 6 had some jamming prior to the start of spoofing. From this figure, we can see near simultaneous position jumps or drift. However, this comparison does not seem adequate by itself. The information from these three phones would not have capture the spoofing in scenarios 4, and maybe 7 and 11. We may utilize velocity, this is essentially the gradient of the plot in Figure 5, acceleration or other measurements to enhance confidence in spoof determination.

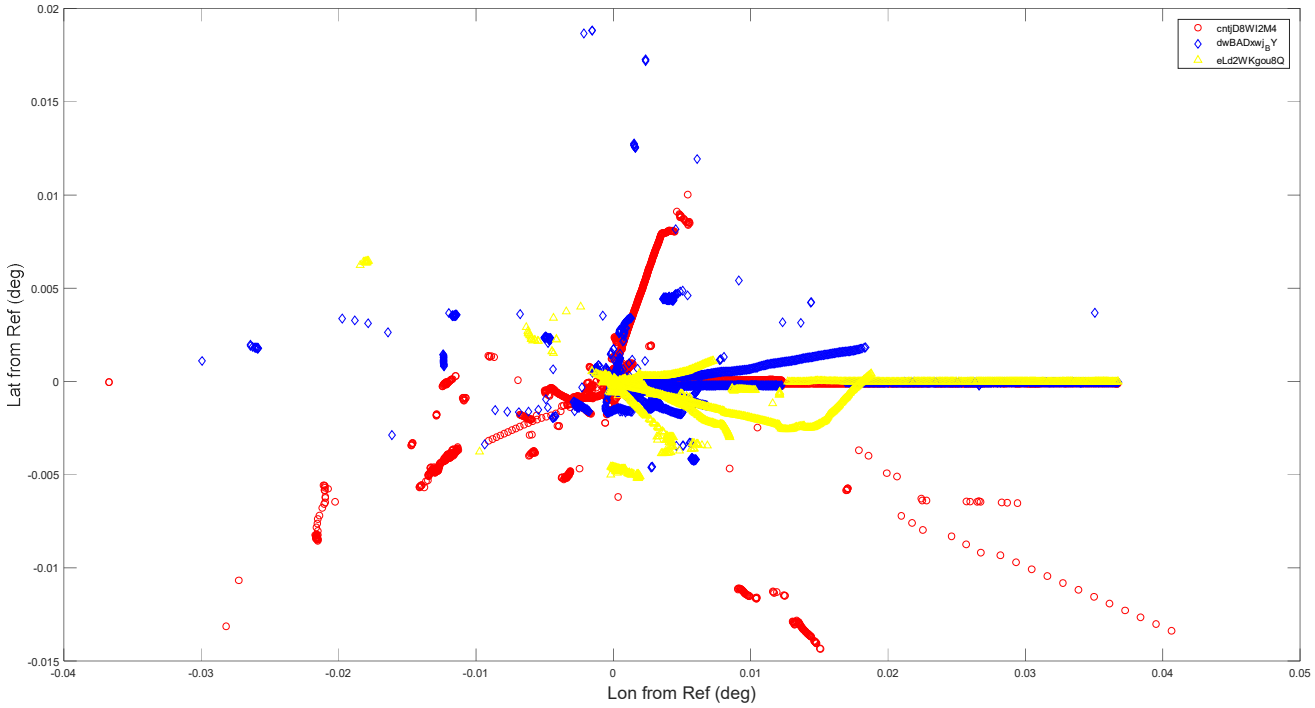

Figure 4. Reported GNSS positions of three static Alcatel smartphones over 11 different spoofing scenarios

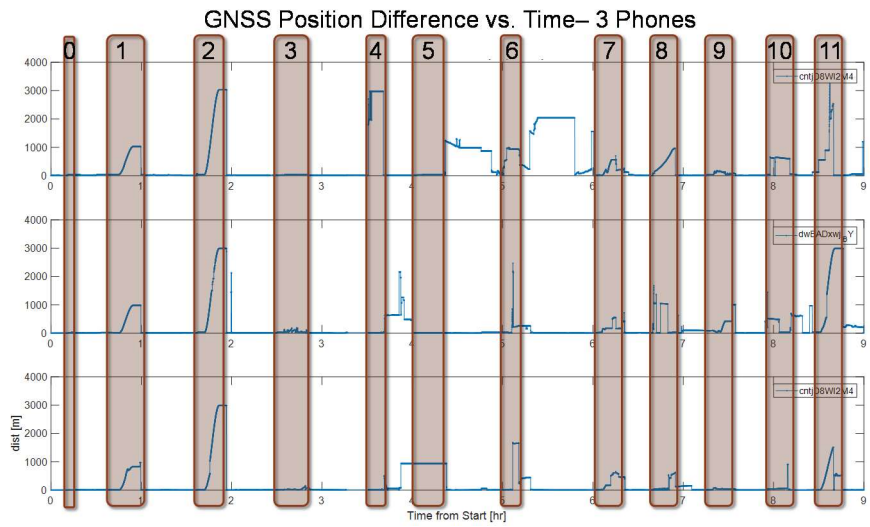

Figure 5. Difference in position of three static Alcatel smartphones over 11 different spoofing scenarios (approximate spoof periods indicated in red)

Accelerometer Comparison

A more efficacious way to use GNSS accelerations for spoof detection is to combine it with accelerations derived from smartphone accelerometers. To compare and utilize GNSS and accelerometer accelerations for spoof detection, we have to manage some important issues. First, the comparison is not straight-forward as GNSS and accelerator accelerations are measured in two different frames. We typically cannot align these two frames as we generally do not know the orientation of the smartphone. So the comparison is made on an absolute basis rather than along each axes. Second, GNSS accelerations can be very noisy due to several natural factors as well as the double differencing of position. Natural factors such as multipath and blockage can result in large calculated accelerations from GNSS due to positon jumps. Using GNSS velocity helps reduce the noise from the latter source as GNSS velocity is derived from carrier tracking. Additionally, the timing of GNSS measurements and low update rate creates a challenge, as will be discussed later. Because of these issues, standalone smartphone receiver-based detection using the comparison may only identify significant discrepancies between the accelerometers and GNSS-derived accelerations. As discrepancies can also result from natural effects, a high threshold may need to be set to prevent too many false alerts. However, if this information is examined across receivers, then we should gain a greater ability to discriminate between natural occurrences and spoofing. For multiple receivers in a scattered in given area, naturally occurring errors should generally be induced at different times in each receiver whereas, the effect of spoofing should be near simultaneous across the affected receivers.

For the acceleration comparison on a smartphone, a comparison of absolute acceleration is made rather than using individual axes as may be possible on other platforms [14]. This also allows us to somewhat account for the effect of gravity on the accelerometer. Figure 6 shows the nominal accelerations from static accelerometers. It so happens that this data was taken during a series of spoofing scenarios where location was displaced. If we subtract gravity, residual is less than 0.2 m/s^2 with standard deviation less than 0.1 m/s^2. The important point verified by this test is that we can get raw accelerometer measurements that are not calibrated by GNSS or affect by GNSS spoofing.

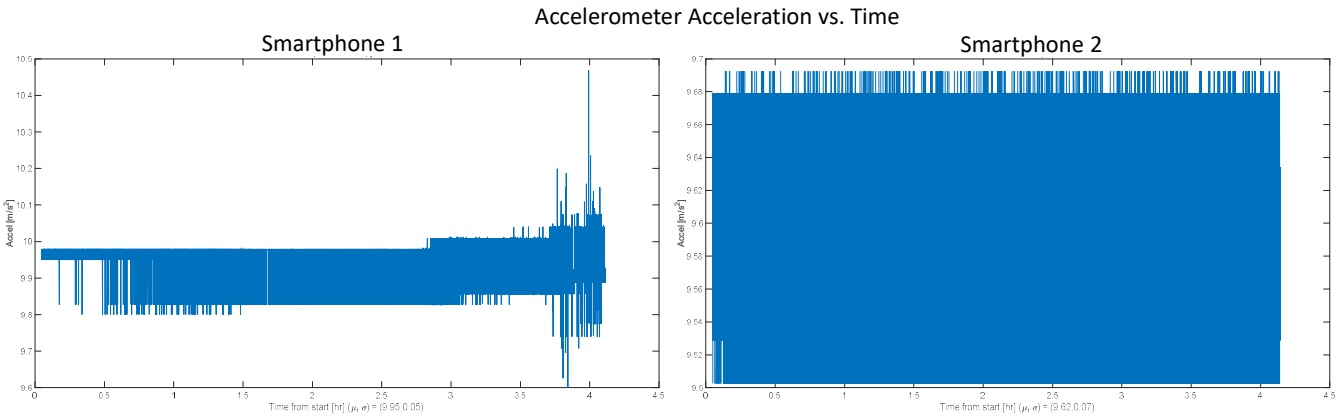

Figure 6. Acceleration of two static Alcatel smartphones over different spoofing scenarios as measured by MEMS accelerometers (gravity also measured)

To see typical differences, we examine the performance of the acceleration comparison under nominal conditions. Figure 7 shows a mostly mobile test of smartphone GNSS and accelerometer acceleration measurement on a commuter train, Caltrain with no spoofing. Additionally, there are two instances of static measurements, around 0.075 and 0.15 hours in the figure, when the train is stopped at a station. GNSS data is typically available at a much lower rate, 1 Hertz (Hz), than accelerometer. To compensate for the noise and update rate, the data is smoothed using 10 second exponential averaging which translates to 80 and 10 data points, respectively, for the 8 Hz accelerometer and 1 Hz GNSS data. From the static data, the noise on both accelerometer and GNSS acceleration can be seen. Generally the discrepancy between the two sources, as seen in the right of the figure, is below 1 m/s^2. There are a few instances where the discrepancy is greater and these are worth discussing. First, there are three instances where GNSS acceleration spikes much higher than accelerometer acceleration. Each instance occurs as the train is starting to accelerate out of the station. This may be due to the low GNSS update rate and perhaps some memory in the position filter. There is one instance, at the end of the collection, where accelerometer acceleration is much larger. This is because the smartphone was picked up by the user prior to getting off the train. Hence the accelerometer is measuring acceleration due to more rapid and smaller human motion which may not be picked up by a 1 Hz GNSS position estimate. This is a common occurrence and needs to be considered in the overall monitor design. These results indicate that our monitor would be better served by higher GNSS update rates. Smartphones will duty cycle GNSS, sometimes to 10%, to preserve battery. Recently, Google provided a version of Android that can prevent such duty cycling.

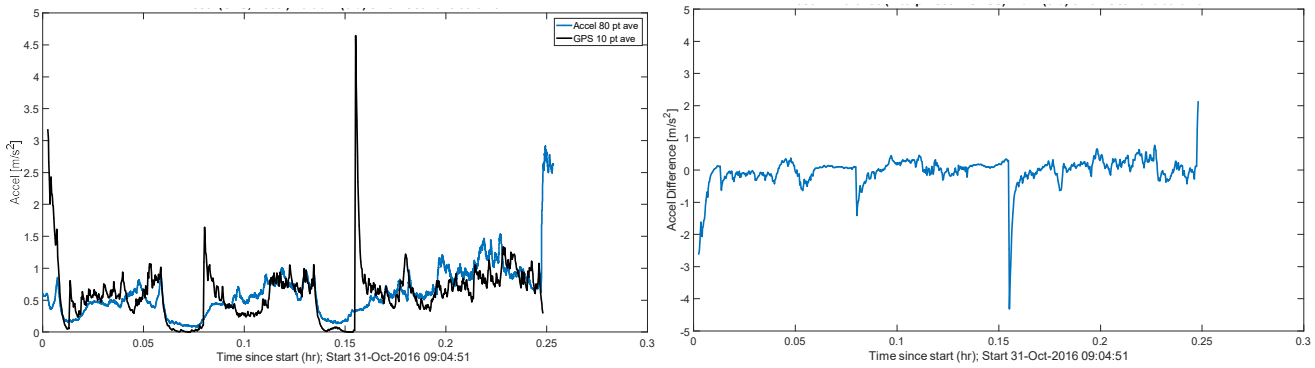

Figure 7. Magnitude of smartphone GNSS and Accelerometer derived acceleration from a Train (Left), Difference of acceleration (Right) using 10 second exponential smoothing

Now examine the GNSS derived accelerations during the spoofing tests. These are calculated by differencing the position change (i.e. double difference of position over time) as velocity results were not collected. Velocity, derived from GNSS Doppler pseudo range rates, should provider better GNSS acceleration measurements. Figure 8 shows the GNS derived acceleration for the same spoofing scenarios as in Figure 5. Again, the red highlighted areas are the approximate periods where spoofing is on. As the phones are static, one would expect zero acceleration and so the measured GNSS acceleration is

also the ideal acceleration difference. Hence, were we to compare the acceleration with that from the accelerometers, the difference, based on Figure 6, would be roughly that seen in the figure with the accelerometer contributing approximately 0.2 m/s^2. Based on the prior results, 1 m/s^2 seems like a reasonable threshold to flag unusual acceleration differences (i.e. potential spoofing). Scenarios 1, 2, 4, 6, 7 and 11 are position spoofing scenarios whereas the other aim to affect time without significant effect on position. Large GNSS accelerations across all receivers are seen in many of the position spoof periods. However, they are also found during non-spoofing periods. Some periods where large GNSS accelerations are seen across all phones occurs during the recovery from spoofing. The fact that this can last for minutes after spoofing is off may indicate there is some memory to the receiver position filter. The effect is another factor to consider when designing the monitor. There are still other times where there are significant acceleration. Some may be attributed to jamming which did not knock out GLONASS so the phones still could have a position and acceleration solution. Regardless, while we can see large accelerations across multiple phones during spoofing, there are also many non-spoofing periods where this is seen. Hence, acceleration comparison, even across multiple phones, should be supplemented to limit false alerts.

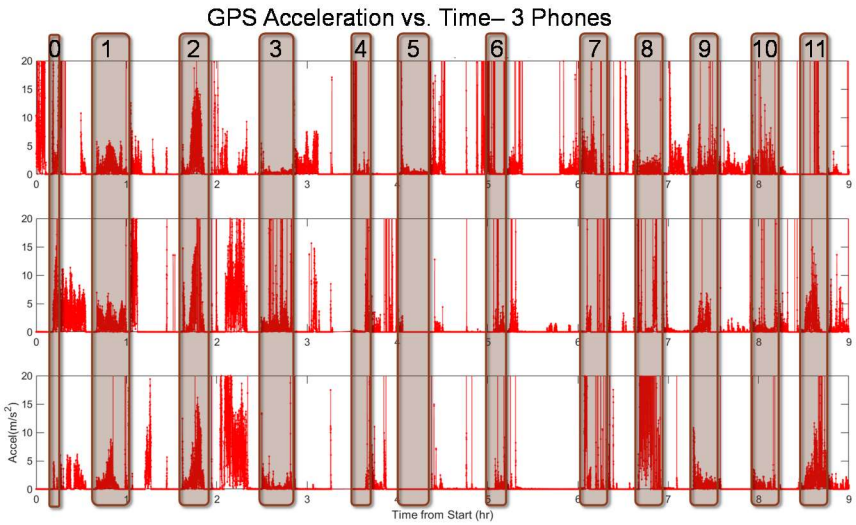

Figure 8. Acceleration (double difference of position) of three static Alcatel smartphones over 11 different spoofing scenarios (approximate spoof periods indicated in red)

AGC and C/No

Standalone interference and spoof detection using AGC and C/No have been long proposed [15][16]. Using these two metrics together not only can help to more robustly detect RFI but also to identify the type of interference. Jamming interference will place more energy into the antenna, causing AGC gain to reduce. This increased noise also reduces the signal to noise ratio (SNR) or C/No on the received GNSS signal. Spoofing also introduces additional energy unto the antenna, also reducing AGC gain. This energy is necessary to induce the receiver to track the spoofed signals rather than the genuine signals. However, unlike a jammer, a spoofer will generally not try to change C/No as reducing the relative signal to noise ratio makes the spoof signal harder to track, defeating the purpose of spoofing. Jamming and spoofing will generally affect both AGC and C/No but have different profiles when examined on an AGC versus C/No plot. Thus, these two metrics are useful for both detection and identification of the RFI.

Figure 9 shows AGC and C/No results from field data and different tests taken by Novatel WAAS GIII receivers [17]. In the figure, the C/No shown is the average of the C/No of the top four satellites. Many of the measurements are from different WAAS reference stations (WRS). These stations experienced different amounts of interference from personal protection devices (PPDs). Some stations commonly experienced PPD interference and this is seen in some of WRS data points with both lower (below zero) AGC gain and C/No. Other stations have relatively clean measurements with AGC and C/No near their nominal zero values. Also shown on the plot are scenarios from the TEXBAT spoof battery [18] played back into the receiver. From the figure, one can see that while spoofing can also lower AGC and C/No, its characteristic C/No versus AGC relationship is different than that of jamming due their different goals.

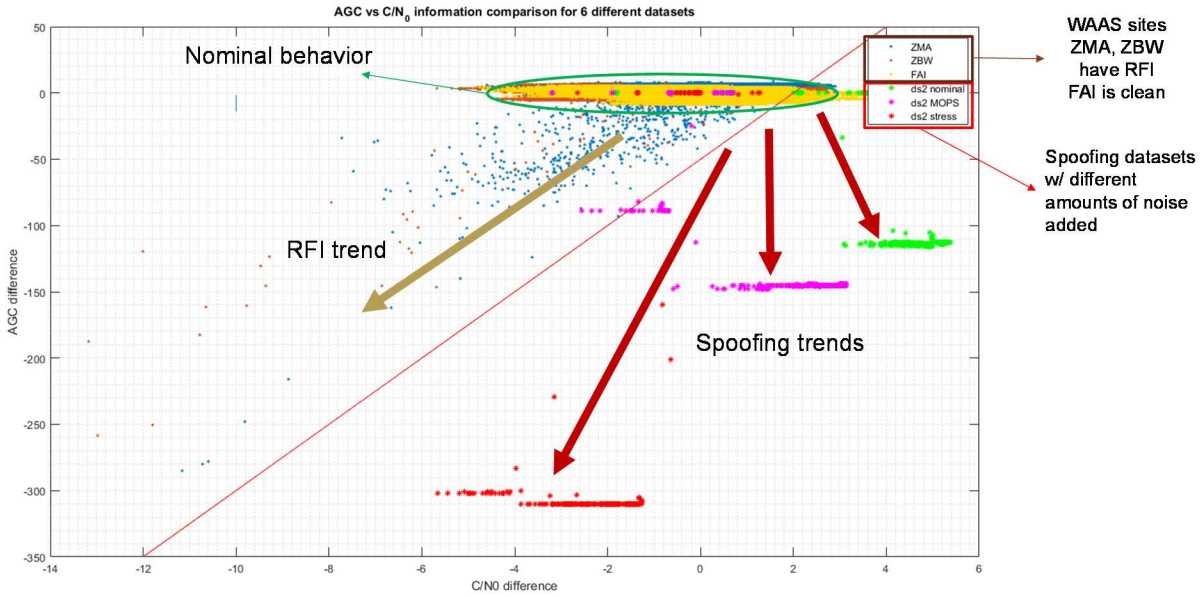

Figure 9 AGC and C/No of Novatel GIII receivers under different field and laboratory conditions [19]. Field data are from fielded WRS receivers while spoofing was conducted in controlled laboratory conditions to test its effects

We were unable to field test the full AGC and C/No capability in a smartphone in 2017 as, unfortunately, there were no smartphones with AGC output available at the time of the spoofing exercise. But even without AGC, crowdsourced C/No measurement can provide useful information about interference. If the spoofer cannot match C/No in all receivers, then we should see similar simultaneous step changes across receivers in the network. Figure 10 shows the average C/No of the top four satellites for three Alcatel Ideal smartphones over the spoofing scenarios previously discussed. Both jamming and spoofing can be identified in the plot. With jamming, all receivers being jammed will experience a near simultaneous drop in C/No. Spoof detection is less obvious but still discernable. Without spoofing, different receivers should have some variations in C/No for each satellite. Under spoofing, once the satellite tracking loop has been captured by the spoofed signal, each receiver will have the roughly the same C/No for this satellite. This is because the spoofing signal will generally dictate both the noise and signal power. Hence, a statistical approach may be used to discover spoofing due to this effect. It can be seen in the data in the figure that the average C/No varies more across receivers during nominal situations than during spoofing periods. A C/No variation or consistency test across receivers can be done on a satellite by satellite basis. While this method identifies all spoofing instances in the scenarios seen in the figure, it is not foolproof. Local effects may cause spoofed C/No to differ from receiver to receiver. For example, if the receiver is tracking a mixture of the spoofed and genuine signal or the spoofed signal with multipath, this may result in a C/No that is significantly different than that from the pure spoofed signal. Additionally, a spoofer, with some work, may be able to weaken this test, especially if GNSS C/No not measured at the same time or similarly. A similar conclusion may be drawn about AGC.

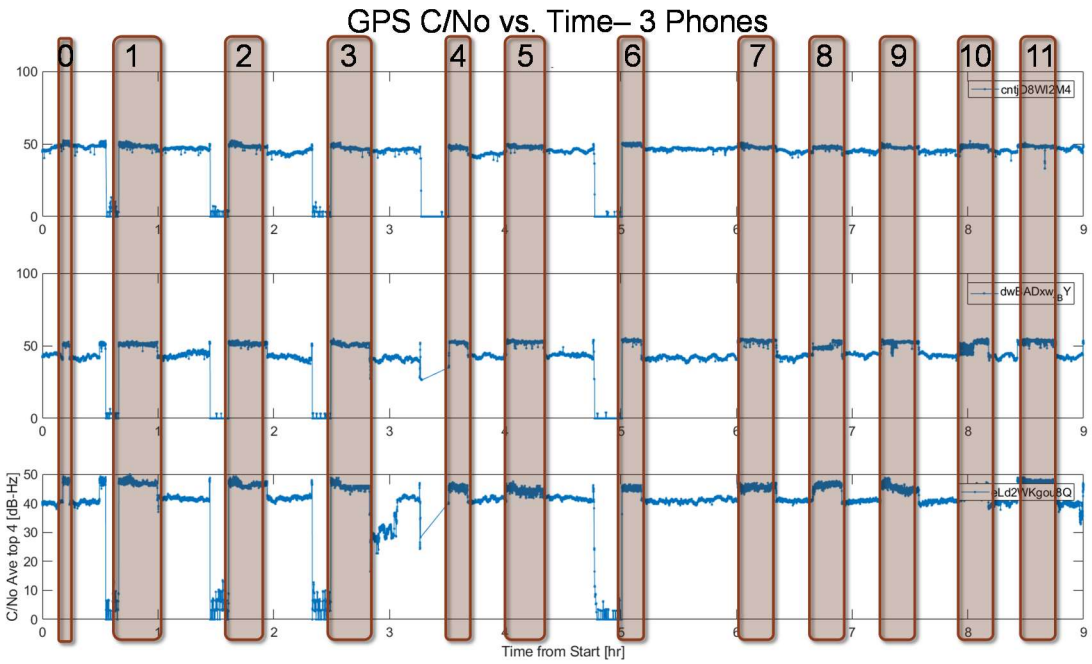

Figure 10. Average C/No of top four tracked satellites for three static Alcatel smartphones over 11 different spoofing scenarios

While we had no smartphones with AGC at the spoofing field exercise, we had other receivers that acted as proxies for smartphone AGC to identify and detect spoofing. AGC data was collected in the field exercise using different radiofrequency front ends. Figure 11 shows an example collected using a SiGe front end during a jamming, then spoofing scenario. Here the reduction in AGC voltage due to jamming is clearly seen. However, spoofing does not cause a significant change in AGC as due to the transmitted spoofing power and our proximity. For a real spoofer, this means having knowledge of the location of the victim receivers and understanding of the transmitted power and gain pattern of the spoofing antenna. While there is a difference, it may not be enough to declare spoofing with a single receiver. If multiple receivers indicated similar decreases simultaneously, this would provide much more evidence.

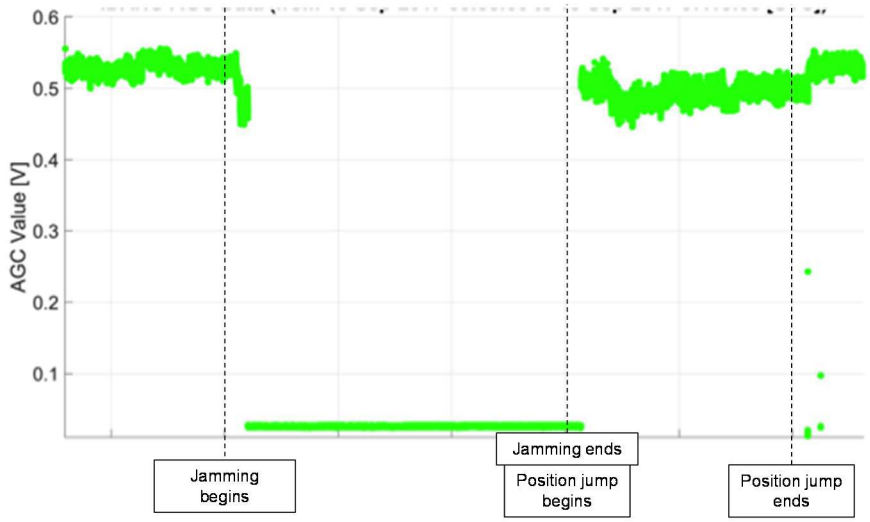

Figure 11. SiGe AGC value during an on air interference test with jamming then spoofing (position jump)

We also collected AGC measurements from Google Pixel phones output under nominal and interference conditions to see the performance of AGC on a smartphone. Figure 12 shows the variation of AGC in a Pixel 3 XL under nominal static outdoor operations – in this case in purely passive operations without human interaction. The figure shows some significant variation

in AGC with variations of almost 5 dB over a very short period (< 30 seconds). This variation may be due to many conditions, such as temperatures or other transmissions and automatic smartphone operations. AGC can also change due to natural or man-made noise such as emissions from a microwave oven. One can imagine even greater fluctuations with smartphone use. We also examined the performance during GNSS interference in an anechoic chamber. The overall AGC and C/No performance of a Pixel 2 under different conditions is shown in Figure 13. The Pixel 2 had different resolution levels to AGC and was generally coarser. The figures illustrate some of the challenges of using AGC in a smartphone. The potentially large allowable variation in AGC in smartphones means that smartphone based AGC + C/No detection may not catch weak jamming or spoofing that is within 5 dB of nominal.

Steady state detection requires knowing the nominal range for AGC. As seen before, this range would likely be large and may differ for each type of smartphone. Using a single smartphone for AGC based detection is thus challenging due to the range of variation that need to be accepted. However, with multiple smartphones, a greater confidence can be developed. For example, one phone having a low, but within nominal range, value of AGC is inconclusive. However, if many smartphones in an area has such low results, this could indicate a systematic cause of increased energy into the antenna, such as spoofing.

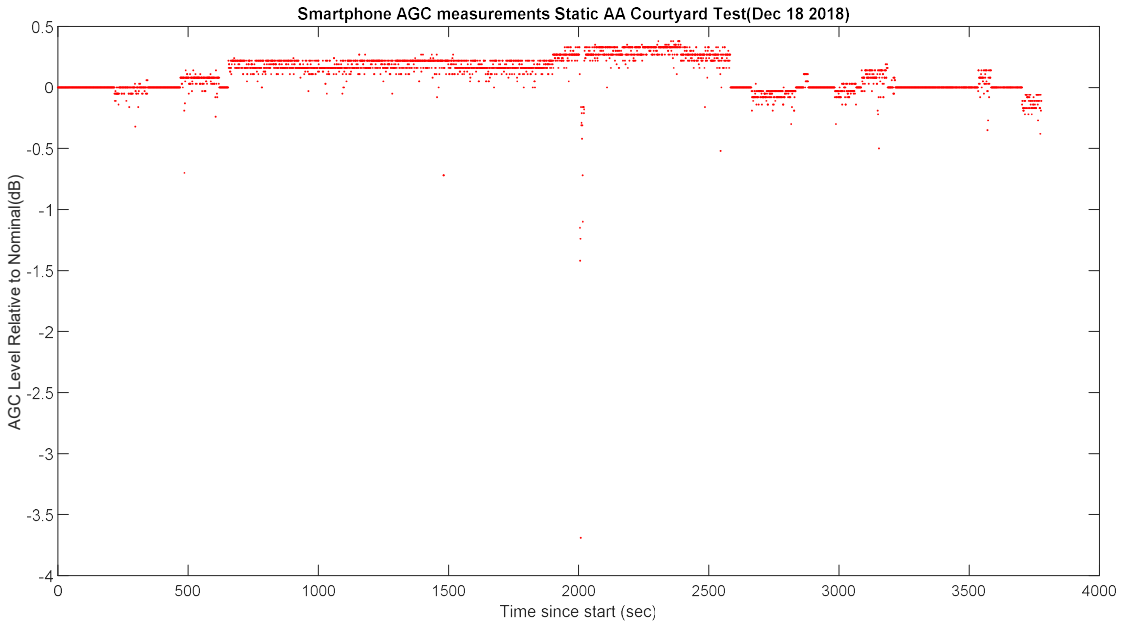

Figure 12. AGC Measured from Google Pixel 3 XL during Static Outdoor Test with No User Interaction

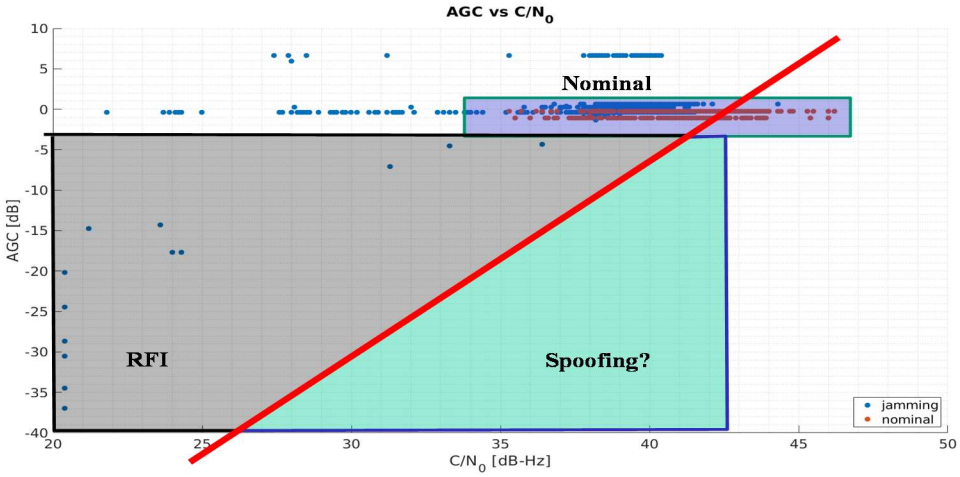

Figure 13. AGC and C/No Measured from Google Pixel 2 under Nominal and Jamming Conditions (Jamming tested inside Anechoic box) [5]

Pseudo ranges and Pseudo range rate

Pseudo ranges provide several possibilities for spoof detection. First, they can allow for stand-alone test of range consistency, such as using receiver autonomous integrity monitoring (RAIM), which may be able to detect disagreements associated with a mixture of spoofed and genuine signals. These consistency checks are usually thought of as a good complement to AGC + C/No spoof detection. This is because power-based spoof detection means that spoof signals cannot overwhelm the genuine signal making the mixture of spoofed and genuine signals more likely.

Second, use of pseudo ranges across receivers may allow us to overcome some of the issues with position comparison across receivers. As shown, receivers spoofed by the same signal may not converge to the same solution as they may have different mixed of spoofed or genuine signals. Rather, we can compare pseudo ranges from receivers for each satellite. For each given satellite, a spoofed range from one receiver should show consistency with spoofed ranges with other smartphones minus a time offset between the individual phones. This time offset should be essentially the same across all compared spoofed signals and is essentially the difference in time between each receiver clock as the spoof satellite clock bias cancel out. If the various pseudo ranges from the spoofer are self-consistent, then an even stronger check may be possible. Certainly, the spoofer has incentive to make this so as it would make its signals more likely to be used. Similarly pseudo range rate may also provide be used to provide a consistency check across receivers. Unfortunately, none of our smartphones could provide pseudo ranges at the time of the spoofing test. More testing on this concept will be done in the future.

5. SUMMARY & OBSERVATIONS

Crowdsourced smartphone measurements present a great opportunity for GNSS spoof detection but also poses several challenges. They can be used as their own detection network or to supplement and improve the measurements of dedicated spoof detection assets. Their use also comes with several challenges not encountered with dedicated monitor receivers. Special care in must be taken with the design of detection using measurements from smartphones as they are noisier, generally dynamic, and subject to greater variation in natural disturbances. Additionally, as they are not dedicated GNSS receivers, they suffer from some important limitations such as update rate and duty cycle. Understanding these limitations is critical to designing robust detectors using crowdsourced smartphone measurements.

This paper examined several different methods of spoof, and other RFI, detection with smartphones, particularly in a networked way. Network approaches are particularly useful with crowdsourced smartphone measurements because they are both subject to more noise (due to user movement and local RFI from within and outside the device) and come from potentially unknown and unverified sources. Power measurements, such as with AGC and C/No, was shown to provide good means of detecting jamming and spoofing. Field test results showed C/No consistencies across smartphone receivers under spoofing. Other measures such as acceleration comparisons, either with accelerometers or other smartphones, and position comparisons can give some indication but not conclusive spoof detection by themselves. Measurements now being made available such as pseudo range, pseudo range rate, carrier phase will help deal with some of the issues seen with acceleration and position comparisons. Even more, AGC, dual frequency measurements and even dual frequency AGC will provide further metrics to aid robust spoof detection. But with each addition, we must be sure to test and test thoroughly in the field. An important caveat, as shown in field tests, one must understand the behavior of smartphone receivers to design a robust detector. A misconception is that spoofing signal will not affect each receiver, even if they are the same model, identically. The spoofing tests did not move all the smartphones' positions to the same location simultaneously. Each smartphone under test, despite having the same receiver, has different states resulting in different behavior when experiencing an attack.

ACKNOWLEDGMENTS AND DISCLAIMERS

The authors thank the Federal Aviation Administration (FAA) and the Stanford Center for Position Navigation and Time (SCPNT) for sponsoring this research. The authors also thank the US Government providing us with an opportunity to test under live GPS spoofing and jamming

The views expressed herein are those of the authors only and are not to be construed as official or those of any other person or organization.

REFERENCES

[1] Yemisi Adegoke, “Uber drivers in Lagos are using a fake GPS app to inflate rider fares,” Quartz Africa, November 13 2017, https://qz.com/1127853/uber-drivers-in-lagos-nigeria-use-fake-lockito-app-to-boost-fares/

[2] “GPS Spoofing A Growing Problem for Uber,” Solid Driver, June 9, 2017, http://soliddriver.com/GPS-Spoofing-A-Growing-Problem-for-Uber

[3] “2.7 million shop visits points to false GPS reports and leads arrest of man on charge of fraud” https://www.nikkei.com/article/DGXMZO37667540121120 18ACYZ00/

[4] Strizic, Luka , Akos, Dennis M., and Lo, Sherman, “Crowdsourcing GNSS Jamming Detection and Localization,” Proceedings of the Institute of Navigation International Technical Meeting, Reston, VA, January 2018

[5] Miralles, Damian, Levigne, Nathan, Akos, Dennis M., Blanch, Juan, Lo, Sherman, "Android Raw GNSS Measurements as the New Anti-Spoofing and Anti-Jamming Solution," Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, Florida, September 2018, pp. 334-344.

[6] James R. Clynch, Andrrew A. Parker, Richard W. Adler, and Wilbur R. Vincent, Naval Postgraduate School; Paul McGill and George Badger, Monterey Bay Aquarium Research Institute, “The Hunt for RFI: Unjamming a Coast Harbor,” GPS World, January 1 2003, https://www.gpsworld.com/the-hunt-rfi/

[7] “FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS,” InsideGNSS, August 31, 2013

[8] Joe Rolli, “Signal Sentry GPS Interference Detection & Geolocation Technology,” 55th Meeting of the Civil GPS Service Interface Committee (CGSIC), Tampa Bay, FL 14-15 September 2015 https://www.gps.gov/cgsic/meetings/2015/rolli.pdf

[9] Logan Scott, “J911: The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches,” Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation GNSS (ION GNSS 2011), Portland OR, September 2011

[10] Sean Barbeau “Why Galileo is not seen in United States?,” https://galieognss.eu/why-galileo-is-not-seen-in-united-states/

[11] FCC News, “FCC Approves Use of Galileo Global Navigation Satellite System in the United States,” November 15, 2018, https://docs.fcc.gov/public/attachments/DOC-355098A1.pdf

[12] H. Borowski, O. Isoz, F. M. Eklöf, S. Lo, D. Akos, “Detection of False GNSS Signals using AGC,” GPS World, April 2012

[13] Gross, Jason N., Humphreys, Todd E., "GNSS Spoofing, Jamming, and Multipath Interference Classification using a Maximum-Likelihood Multi-Tap Multipath Estimator," Proceedings of the 2017 International Technical Meeting of The Institute of Navigation, Monterey, California, January 2017, pp. 662-670.

[14] Sherman Lo, Yu Hsuan Chen, Tyler Reid, Adrien Perkins, Todd Walter, Per Enge, "The Benefits of Low Cost Accelerometers for GNSS Anti-Spoofing," Proceedings of ION Pacific PNT, Honolulu, HI, May 2017

[15] 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.

[16] Akos, Dennis 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, Winter 2012, pp. 281-290.

[17] Brandon Cotts, Sherman Lo, Dennis Akos, “Leveraging GPS/GNSS Automatic Gain Control (AGC) and Unique IF Data Processing to Detect GNSS Disruptions," Proceedings of the Institute of Navigation Joint Navigation Conference, Newport Beach, CA, July 2018

[18] 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.

[19] Esteban Garbin Manfredini, Dennis Akos, Yu-Hsuan Chen, Sherman Lo, Todd Walter Per Enge, “Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers,” Proceedings of the Institute of Navigation International Technical Meeting, Reston, VA, January 2018