Developing a Practical GNSS Spoofing Detection Thresholds for Receiver Power Monitoring

Sherman Lo, *Stanford University*, Fabian Rothmaier, *Stanford University*, Damian Miralles, *University of Colorado, Boulder*, Dennis Akos, *University of Colorado, Boulder*, Todd Walter, *Stanford University*

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.

Fabian Rothmaier is a Ph.D. candidate at the GPS Laboratory at Stanford University. He received his B. Engr. degree from the University of Applied Sciences Bremen, Germany in 2015 and his M. Sc. degree from Stanford University in 2017.

Damian Miralles completed his Ph.D. in the Department of Aerospace Engineering Sciences at the University of Colorado Boulder in 2021. 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 is a faculty member with the Aerospace Engineering Sciences Department at the University of Colorado, Boulder

Todd Walter is a research professor in the Department of Aeronautics and Astronautics at Stanford University

ABSTRACT

Robust GNSS interference and spoof detection is a desirable feature to have in many receivers, particularly those used for safety or economically critical activities. Using the combination of automatic gain control (AGC) and carrier to noise ratio (C/No) measurements, collectively termed receiver power monitoring (RPM) is attractive as these metrics are both generally readily available and complimentary. However, detection tests need to be developed that can robustly utilize these measurements to provide detection of spoofing. This paper details the development of our RPM detection method. This method uses snapshot measurement of changes in RPM measures from nominal to identify spoofing from jamming and nominal conditions. A detection threshold line in the 2-D space of ΔAGC and ΔC/No is found to differentiate the cases. The paper discusses the challenges to using these measurements. It shows that the nominal value and variations in this metric is affected by many factors such as aircraft state (i.e. take-off, climb, in flight and approach). The paper outlines the specific steps to calculate the threshold line from empirical data. It shows a metric to quantify the strength of the detection in terms of distance from the threshold line. This provides a single quantitative detection output that allows the technique to integrate with other detection techniques. The threshold calculation is modified to develop a more practical threshold detection that incorporates uncertainty and known relationships between the RPM metrics. One practical improvement is that the technique may not need as much empirical data.

I. INTRODUCTION

GNSS radiofrequency interference (RFI) in the form of spoofing and jamming pose a significant challenge to its reliable use as safety and economically critical PNT infrastructure. There have been numerous documented cases of inadvertent and deliberate jamming events. Even more troubling is the increasing number of spoofing events - from repeaters or GNSS signal generator being accidentally left on and broadcasting over the air to deliberate spoofing such as those seen in the Black Sea, Moscow and more recently, with so-called spoofing circles, in Shanghai and Iran [1][2][3]. Given the different size and scope possible events, a low cost, readily available GNSS interference detection and characterization capability will be useful to protect receiver operations. Just as important, this capability may also provide authorities with information needed to rapidly identify and even localize events

Receiver power monitoring (RPM), particularly using a combination of automatic gain control (AGC) and carrier to noise ratio (C/No), has been proposed as an attractive method of identifying GNSS spoofing and jamming [4][5][6]. These measures, AGC and C/No, are attractive as they are commonly available in receivers with little to no hardware modifications. Together, these two metrics are powerful as they can be used to detect and differentiate between jamming and spoofing attacks. Additionally, they are well complemented by other commonly proposed detection methods such as receiver autonomous integrity monitoring (RAIM) or cross ambiguity function (CAF) [7] which can give more conclusive determinations in conditions, such as weak or near power matched radio frequency interference (RFI), that are more challenging for RPM.

Our past work on RPM examined its utility and developed snapshot detection based on a threshold line derived from empirical receiver C/No and AGC measurements under many conditions [8]. The developed threshold line represents the demarcation between events that may be classified as spoofing versus interference/normal conditions. The goal of the current effort is to clarify and build upon this concept and provide a more flexible and more practical means of deriving a detection threshold line. This paper examines developing a practical means of implementing RPM detection in a receiver. This paper covers three areas: 1) enumeration and examination of sources of error for RPM detection, 2) derivation of RPM spoof detection threshold line using empirical measurements, 3) enhancement of the threshold technique using combination of empirical measurement and modeling targeted for more practical receiver implementation.

II. BACKGROUND

Overview of C/No & AGC Detection

AGC and C/No are readily available measures that can be useful for RFI identification and detection. C/No is a measure of the tracked GNSS signal power relative to the noise in the measurement and is a common and ideally standard measurement made by all receivers to assess signal reception quality. It is measured for each tracked satellite signal. AGC is circuitry that provides the receiver analog gain such that received measurements being processed the GNSS receiver, after the front-end processing, has relatively constant power levels. The gain from the AGC circuit is applied prior to analog to digital converter (ADC) of GNSS receiver. Thus, if more signal and noise energy enter into the antenna, the AGC decreases the gain to maintain the same overall power level. Hence, the AGC level provides a measure of overall input power of each frequency band used. In this paper, we will use the term AGC or AGC level to refer to the AGC gain level and AGC circuit to refer to the physical equipment providing the gain. Figure 1 shows the AGC levels from a Novatel GIII receiver, given in pulse widths (PW), in the L1 and L5 band during a flight. Sporadic interference on L1 results in abrupt spikes of lower AGC levels. L5, since it is in the distance measuring equipment (DME) band, experiences interference from DME throughout flight which can be seen by the consistently lower AGC during the flight portion. As will be discussed next, these two metrics are ideally used together as they complement each other's blind spots

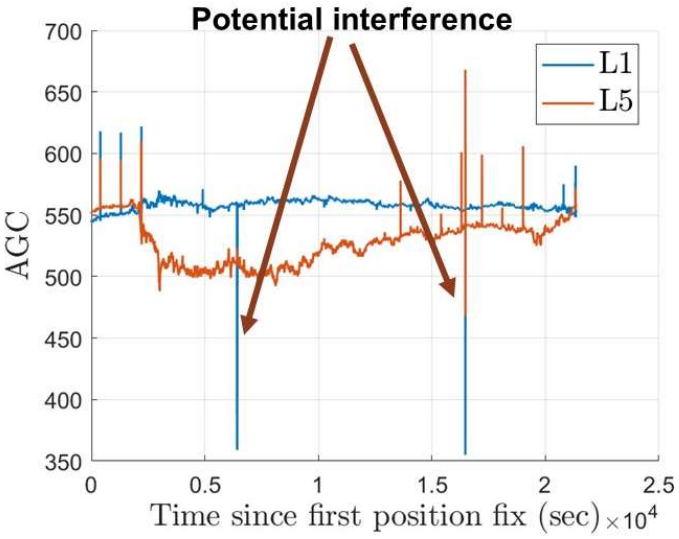

Figure 1. Novatel GIII L1 and L5 AGC measurements from cross country (New Jersey – California) flight on Global 5000

Attack Scenarios & Consideration

To see how AGC and C/No are useful for spoof/interference detection, examine two common spoofing attack: jamming then spoofing and (correlator) lift off spoofing. The first attack seeks to overpower the genuine signal and capture the receiver tracking loop with spoofed signals by employing either jamming followed by a strong spoofing signal or a highly overpowered spoofing signal. The goal of the jamming is to knock down the genuine signal correlation peak relative to noise and interference such that the tracking loop becomes unlocked. Then a spoof signal is sent such that it can capture the receiver tracking loop or correlators by being (much) stronger, and hence more preferred, than the genuine signal. A very powerful spoof only attack may have a similar effect. The sequence of this attack is seen in Figure 2 showing the tracked segment of the correlation function. The first (left most) plot shows the correlation function and tracking points in nominal conditions – i.e. genuine signal only. The middle shows the effect of jamming and the third shows the correlation function combining the genuine signal and the much higher power spoofing signal. Due to the much higher correlation peak, a receiver should track the correlation peak of the spoofing signal. The attacker can match the typical C/No of the satellites so as to not cause an unusual change in C/No which means the receiver may not notice any unusual C/No, other the temporary loss of signal due to jamming. However, the attack will cause an increased power, at least for a short time, which should get noticed by the AGC. Thus this attack is easily noticed AGC but not as discernable by C/No. The second case is a relatively power matched (i.e. matched to nominal GNSS plus thermal noise power level) attack often termed lift off spoofing. Figure 3 shows the stages of this attack on the correlation function. To capture the tracking loops, the attacker conducts a spoofing attack where it matches the genuine signal code offset. At first, it starts at low power, below the power of the genuine signal (second plot from left in Figure 3). It then carefully raises (lift off) its power to become slightly more powerful that the genuine signal (third plot from left in Figure 3). In doing this, it can cause constructive or destructive interference before finally capturing the receiver tracking loop with a (slightly) higher power signal and pulling it off the genuine correlation peak (leftmost plot of Figure 3). The second and third plots in Figure 3 shows this as constructive interference but because of changing phase offsets, it will generally fluctuate a lot between constructive and destructive interference. For this attack, the goal is to minimize increased power and hence there may only be a slight decrease in the AGC level. The C/No may vary significantly during the lift off phase (due to the combination of the genuine and spoofed signal) and should be slightly higher during the final pull off. This case is hard to discern with the AGC but leaves telltale indicators in the C/No.

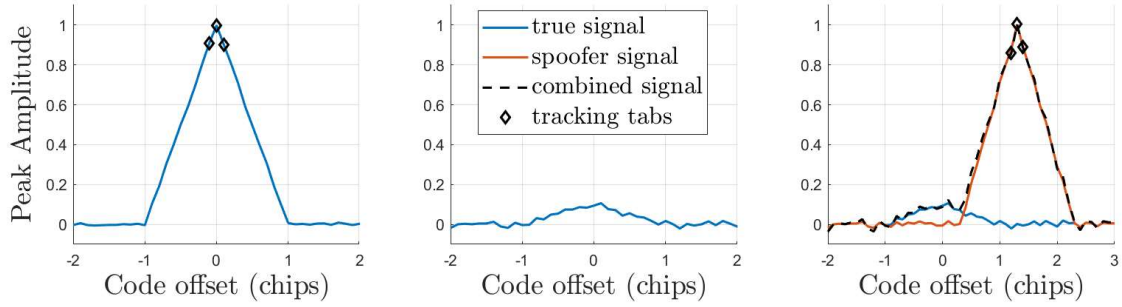

Figure 2. Overpower spoof attack (jam then spoof) as seen by receiver correlator

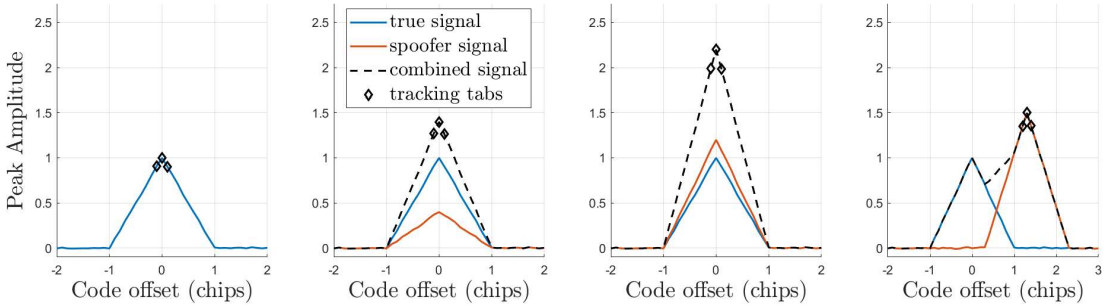

Figure 3. Surreptitious spoof attack (lift off spoof) as seen by receiver correlator

As seen from the spoof attack scenario descriptions, AGC and C/No have different individual blind spots in identifying spoofing. However, their complementary nature can mitigate their individual blind spots and these metrics are best used together. So they are often used together and this combination is commonly termed receiver power monitoring (RPM). Figure 4 shows a plot of AGC and C/No from different scenarios relative to nominal reference value, denoted as ΔAGC and ΔC/No, as seen by a Novatel GIII receiver. One set (red) is from a flight under nominal conditions. A second set (blue) is from a static Wide Area Augmentation System (WAAS) reference station Miami (ZMA) which occasionally experiences jamming from personal privacy devices (PPD) being used by vehicles on a nearby highway. The final set (circle) is the spoofing scenario TEXBAT DS2 [9] which is played back into the receiver. These represent nominal, nominal and jamming, and spoofing results. From the figure, it is clear that nominal, jamming and spoofing tend to occupy different regions in this 2-D space of AGC and C/No. Given this result, our goal is to determine the demarcation or threshold line between these conditions (nominal, jamming and spoofing). Of particular importance is finding a reliable threshold line between spoofing and nominal/jamming conditions as that can be used to detect spoofing. This idea is illustrated in Figure 5.

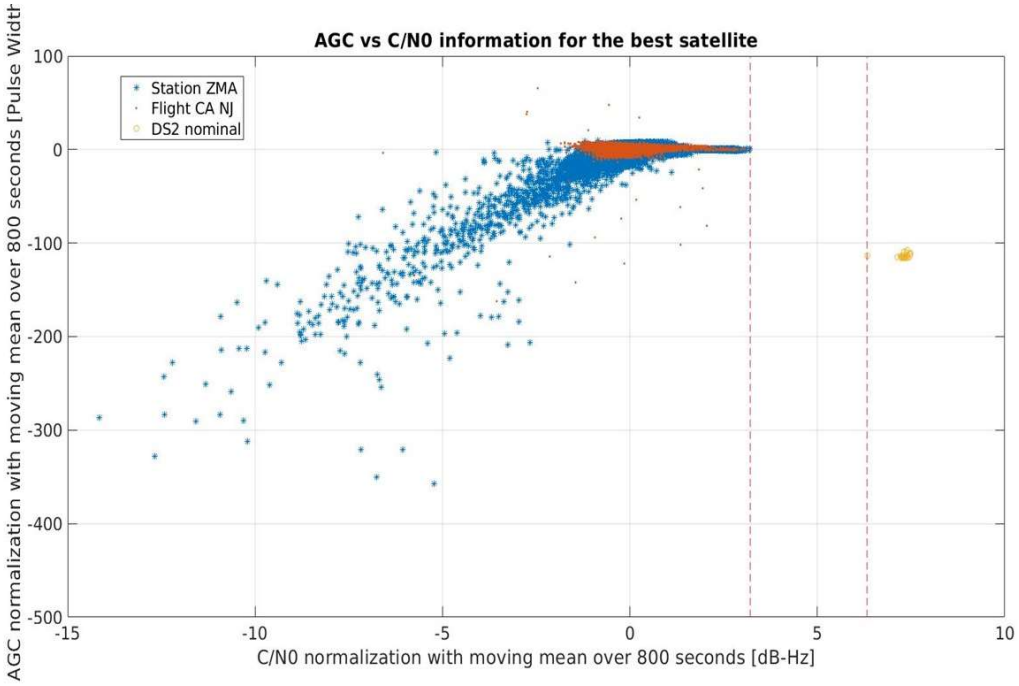

Figure 4. Plot of ΔC/No vs. ΔAGC for several scenarios

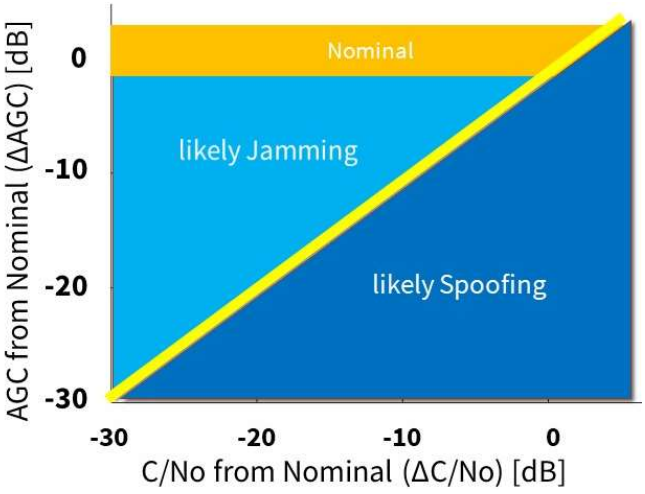

Figure 5. Representation of RPM Spoof vs. Jam Detection Threshold Line

III. CHALLENGES TO USING AGC AND C/NO

Developing the threshold/detection line is practically challenging due to various factors. One factor comes from measurement and calculation error. A second factor is that there is no single constant nominal or reference condition – nominal values can change over time due to changing conditions. For example, in aviation, nominal values of AGC and C/No can vary due to flight operations and conditions. A third factor is having consistent use and definitions for AGC and C/No. All these can lead to errors in the estimated factors of interest (ΔAGC and ΔC/No). All this means that we may need to have some tolerances in the calculation and use of the developed threshold. This section will examine the second and third factor as they are less commonly explored.

Nominal AGC and C/No values and statistics can vary over time. To illustrate this, we use data from a cross country flight from Tennessee to Oklahoma, whose flight path is shown in Figure 6. Figure 7 shows the AGC values on L1 and L5 during flight. One can see increase in L1 AGC during the flight indicating a decrease in noise whereas L5 AGC level stays the same or decreases indicating there is more noise in flight (likely due to DME). The decrease in L1 noise may be due to several factors such as lower overall air and aircraft temperatures due to being in flight at altitude. The L5 AGC likely has this decrease noise offset but also likely experiences increased L5 noise due to DME interference in flight. The change seen in L1 corresponds to about 1.2 dB which, while not huge, is a significant amount.

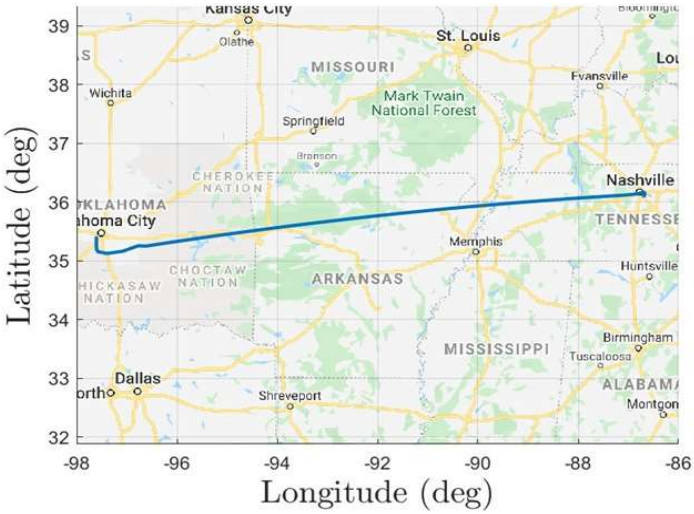

Figure 6. Path of measurement flight from Tennessee to Oklahoma on Global 5000

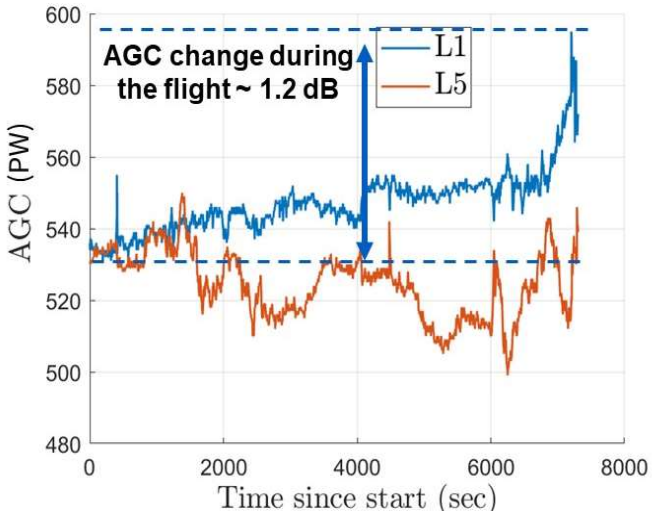

Figure 7. Novatel GIII L1 and L5 AGC measurements from Tennessee to Oklahoma flight on Global 5000

Similarly, nominal C/No also varies with conditions. For example, C/No can vary with satellite elevation angle relative to the antenna to the gain pattern of both the satellite transmit and the receive antenna. Additionally, the flight operations such as take off and landings may also result in greater variation of C/No. Figure 8 shows the C/No of various GPS satellite L1 C/A signals. At around 400 to 1000 seconds into the data, there is a large fluctuation in C/No. This is while the aircraft is still at the airport and due perhaps to multipath as well as aircraft vibration. In flight, C/No is more constant though there are some longer period fluctuations. Finally, on approach and landing, around 6200 seconds into the data, there is increased rapid fluctuations. This is seen more clearly when examining the single time difference of C/No ($\Delta C/No = C/No_i - C/No_{i-1}$) which is shown in Figure 9.

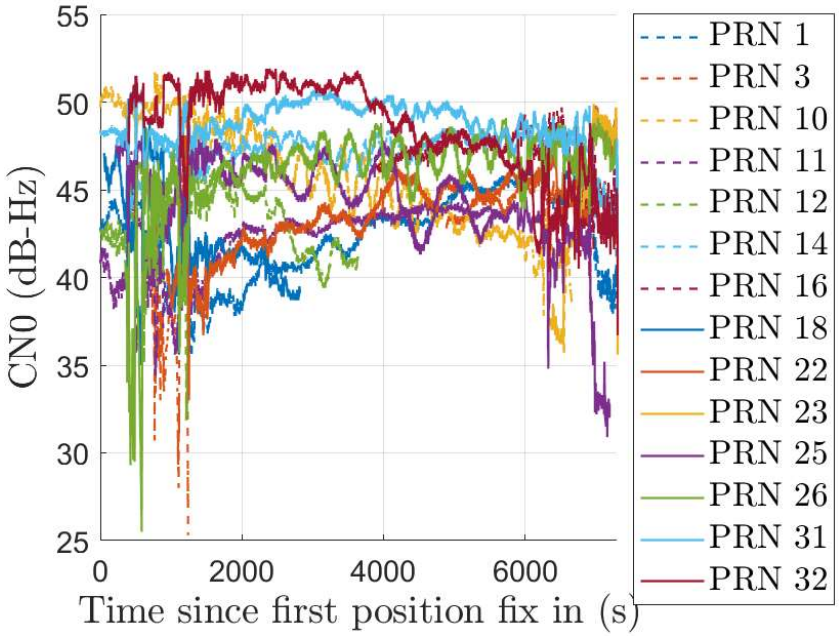

Figure 8. GPS L1 C/No on Novatel GIII from Tennessee to Oklahoma flight on Global 5000

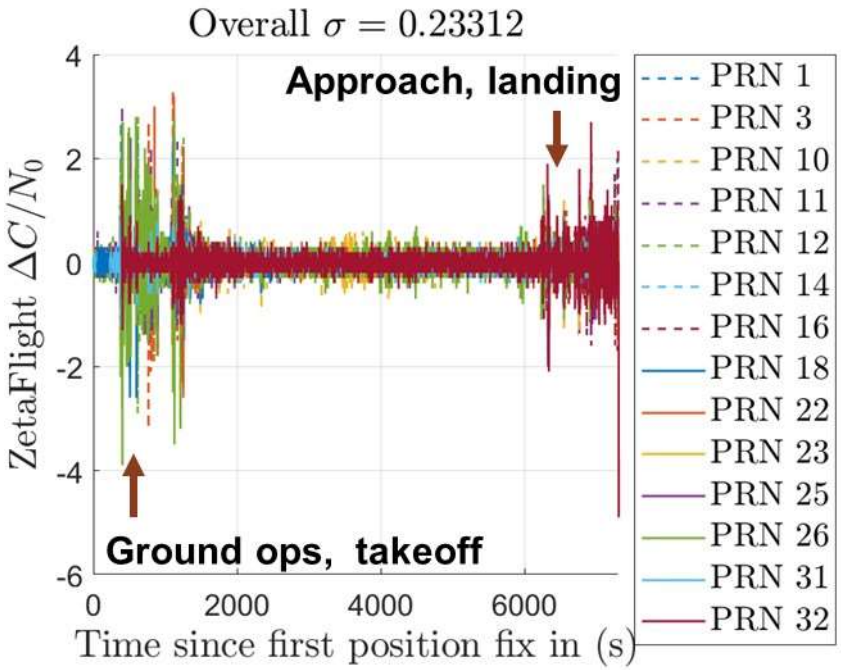

Figure 9. Difference in GPS L1 C/No ($\Delta C/No = C/No_i - C/No_{i-1}$) on Novatel GIII from Tennessee to Oklahoma flight on Global 5000

Another important factor to consider is the variation due to the calculation of the metrics. There is no generally agreed upon definition for receiver AGC outputs and indeed each receiver outputs its own metric. In the Novatel GIII, AGC level is expressed in units of pulse width (PW). To convert PW to a gain value in deciBel (dB), empirical testing was conducted with noise is injected to see AGC output [10]. From the testing, it was found that the GIII AGC changed about 18 dB per 1000 PW. In [10], it was also shown that different types of interference (continuous wave (CW), swept CW, etc.), while having similar slopes have different input power levels where the interference starts to affect the AGC level. This may be due to many factors such as the front-end bandwidth. There are other problems even if there is a seemingly clearly defined presentation such as in Android raw measurements which uses decibel (dB) to quantify the AGC level. The problem seen with this is that each manufacturer has chosen to interpret the meaning of this and do not present AGCs uniformly [11]. Some present an absolute AGC, others a relative AGC and others present an AGC level relative to a time varying level. Some present positive AGC as an increase in AGC level (decrease in input power) while this is a negative AGC value in others.

C/No can be calculated in multiple ways which are generally similar at typical C/No levels but can diverge greatly at higher levels (above 50 dB-Hz) [12]. These higher levels may be important as they may be experienced under spoofing. [12] documents the major methods of calculating such as Real Signal Complex Noise (RSCN), Beaulieu's method (BL), Signal to Noise Variance (SNV), Moment Method (MM), Narrowband-Wideband Power Ratio (NWPR). In Figure 2 and 4 of [12], the C/No calculated using these methods are plotted against true C/No and Signal power, respectively.

In developing the detection threshold line for spoofing, examine ways to incorporate uncertainty and errors.

IV. DEVELOPING AND DETERMINING RPM THRESHOLD

The determination of the empirical RPM threshold line for spoofing, as seen in [8], starts with three steps. The first step is to determine the nominal or reference C/No and AGC to use for calculating ΔC/No and ΔAGC. The second step is to gather data from a sufficient set of scenarios (nominal, interference and spoofing) to calculate and plot that ΔC/No and ΔAGC. Finally, those data points are used to generate threshold line based on looking at extreme points in the scenarios.

Determining the nominal values of C/No and AGC is not as straight-forward as it may seem. Performance can change under nominal (no RFI) conditions, due to natural variations, change external conditions (i.e. temperature changes) as well as errors due to quantization, noise, multipath. We examined two ways to calculate nominal values. One way is to use a nominal determined from historical data or calibration conducted at the factory. Having a stored value is useful as it can be used immediately. However, the value may not easily account for changing nominal situations. A second way is to derive a nominal value based on recent past measurements. For this approach, we used a moving average of recent past values as the nominal reference. This is seen in Equation (1) for parameter μ (C/No or AGC) at time i. The limitation is that this moving average may incorporate non-nominal situations if these are not detected and excluded from the averaging.

$$\Delta\mu_i = \mu_i - \frac{1}{N}\sum_{j=1}^{N}\mu_{i-j} = \mu_i - \mu_{nom} \qquad (1)$$

The next step to determining the empirical threshold line is to calculate ΔC/No and ΔAGC from measured C/No and AGC data from various scenarios. The measured AGC is the AGC level for the frequency of interest while the C/No used is the max C/No over all satellites. A moving average window is used to calculate the nominal value with the size of moving average window, N from Equations (2) or (3), determined *a priori* from a parametric study such as that conducted in [8]. The results are then plotted.

Next, two points are determined to calculating a quantity we term adjusted ΔC/No, $\Delta C/No_{adj}$. The calculation is given in Equation (4). The adjusted C/No accounts for the noise level, as indicated by the AGC. The assumption made is that each decrease in AGC level of 1 dB, which should correspond to an increase of input noise by 1 dB, should result in a 1 dB decrease of C/No. Hence, by subtracting off the AGC level in dB, we get a measure of signal power or equivalent C/No at nominal AGC (ΔAGC = 0). Thus $\Delta C/No_{adj}$ should be proportional to actual signal power less some offset. This assumption is ideally true – if the AGC indicates that one dB more noise is added, then C/No should decrease by one dB. A corollary to the assumption is that the relationship between ΔAGC and ΔC/No, i.e. the slope of ΔAGC per ΔC/No, should be 1 dB/dB-Hz slope for constant signal level (i.e. nominal and interference conditions). There may be some factors that may change this such as filtering after

the AGC circuit. Of course, spoofing could also violate this relationship. However, since spoofing is trying to capture the receiver, likely differences to the ideal relationship should only move in the direction of increased signal power (larger ΔC/No for a given ΔAGC). This is acceptable as it would push a data point further to the right of the plot and more into the spoof detection region. We will use this corollary in the next section to enhance the threshold line determination.

The first point we find is the maximum $\Delta C/No_{adj}$ under nominal conditions. Since this is roughly zero ΔAGC, it is about the same as finding the maximum nominal ΔC/No. By using $\Delta C/No_{adj}$, we can also use points from jamming condition. This is essentially the most extreme (i.e. closest to looking like spoofing) nominal or non-spoof point on the AGC-C/No plot. This is the point "Max C/No at nominal" in Figure 10 which corresponds to (x_1, y_1) in Figure 11. The next point to determine is the spoofing point where the $\Delta C/No_{adj}$ is the lowest spoof. Qualitatively, this should be the most nominal-like spoof point. This is the point "Min C/No at spoofing" in Figure 10 which corresponds to (x_2, y_2) in Figure 11.

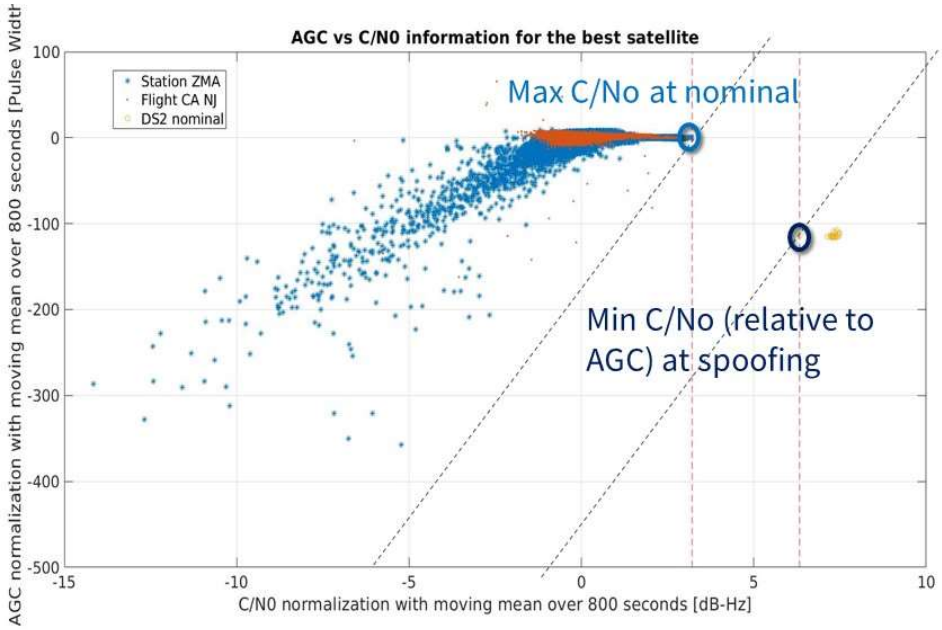

Figure 10. Determination of defining points for developing the spoof/no spoof detection threshold line on ΔC/No vs. ΔAGC plot of several scenarios

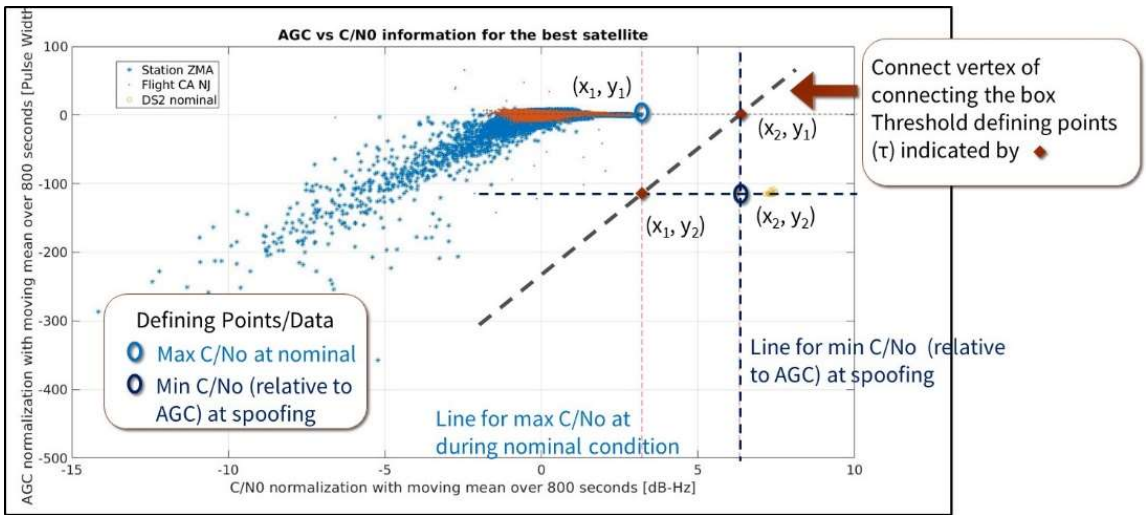

Figure 11. Determining the empirical threshold line using highest adjusted C/No nominal point (x_1, y_1) and lowest adjusted C/No(x_2, y_2) as seen on ΔC/No vs. ΔAGC plot of several scenarios

$$\Delta AGC_i = AGC_i - \frac{1}{N}\sum_{j=1}^{N} AGC_{i-j} \quad (2)$$

$$\Delta C/No_i = C/No_i - \frac{1}{N}\sum_{j=1}^{N} C/No_{i-j} \quad (3)$$

$$\Delta C/No_{adj} = \Delta C/No - \Delta AGC_{dB} \quad (4)$$

These two points, (x_1, y_1) and (x_2, y_2) as seen in Figure 10, define two opposing corners of a rectangle. From that we get the other two corners, (x_1, y_2) and (x_2, y_1). The empirical threshold line we developed is found by pass a line through these two other corners, (x_1, y_2) and (x_2, y_1) [8]. The line lies in between the most spoof-like nominal point (x_1, y_1) and most nominal-like spoof point (x_2, y_2). This empirical threshold determination has some limitations. One limitation is the threshold line is not fixed or constrained by the theoretical relationship between ΔAGC and ΔC/No indicated previous (1 dB/dB-Hz slope). The next section addresses this limitation.

Constraining Threshold Slope

We use the prior development to produce a threshold line with a proscribed slope *m*. Ideally, the slope should theoretically be 1 dB/dB-Hz. For this derivation, we will use a generic slope of *m* which is useful if the relationship is different or if the units of AGC used is not in dB.

To develop the threshold, we use the points, the most spoof-like nominal point (x_1, y_1) and most nominal-like spoof point (x_2, y_2), found using $\Delta C/No_{adj}$. The line with desired slope *m* passing through each point is found. This is shown in Figure 12 as line 1 and line 2. We can then choose a parallel line in between line 1 and line 2 and the threshold line. This line will have the same slope *m*. Nominally, the threshold line can be exactly in between line 1 and line 2. This will be termed the center threshold line for this paper and can be found by calculating d_{min}, the distance between line 1 and line 2 and then finding a line that is ½ d_{min} away from line 1 or line 2. d_{min} can be calculated using the equation in the next section by taking line 1 and point (x_2, y_2). A more convenient way to determine the threshold line, especially if ΔC/No error statistics is utilized, is to the use the horizontal distance between the two defining lines, d_{hor}. The horizontal distance is given in Equation (5) as a function of the slope *m* and the minimum distance between the two lines.

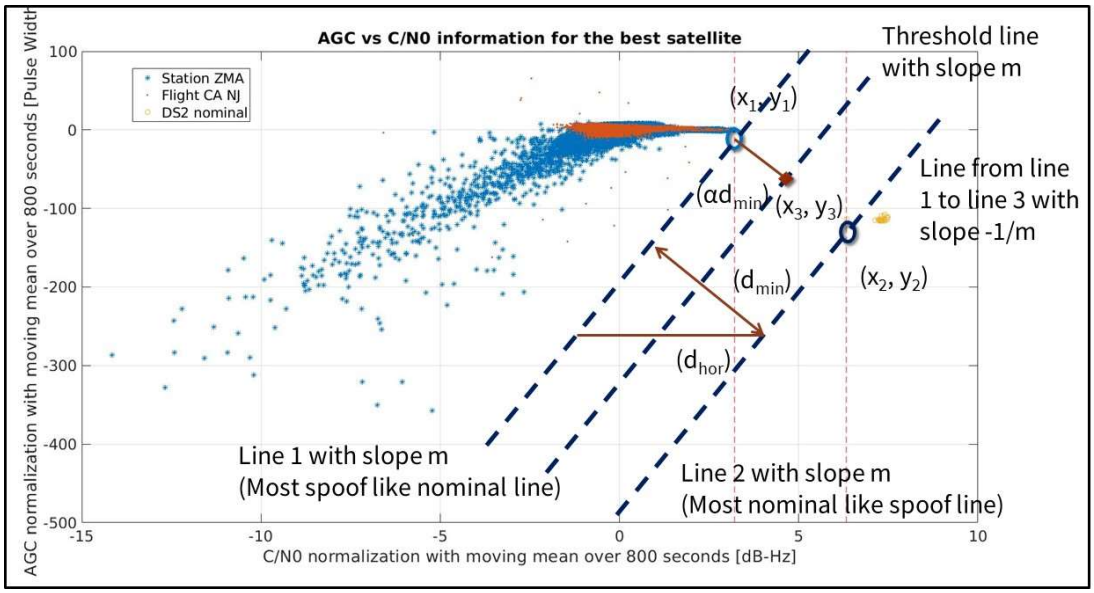

Figure 12. Determining the slope constrained threshold line using highest adjusted C/No nominal point (x_1, y_1) and lowest adjusted C/No(x_2, y_2) as seen on ΔC/No vs. ΔAGC plot of several scenarios

Provided the slope relationship is correct, the threshold line has desirable spoof detection properties. Any points that are further to the left of the line will have weaker received signal power relative to a point on the threshold line with the same AGC level. This is not desirable for a spoofer as it wants to be more attractive (more powerful) than the genuine signal to capture receiver tracking. In other words, if the detection line represents the limits of nominal operating conditions for a genuine signal without spoofing, operating at a point that further in the no spoof detected region would require that the spoofing signal have less signal power which reduces it chance of successfully capturing the receiver tracking loops. This is still possible partly as genuine signals have variations in C/No values under nominal conditions. This can be accommodated, as seen in the next section.

The more desirable operating point for a spoofer to have more signal power. This means operating at a point in the ΔAGC-ΔC/No space that is further to the right than a nominal point and hence further to the right of our threshold line. This is the desired outcome. Any point to the right of the line would have a stronger received signal power, something desirable to spoofers, but this puts the point more in the spoof detected region.

$$d_{hor} = d_{min}\left(\frac{\sqrt{m^2+1}}{m}\right) \quad (5)$$

Accounting for Variations, Errors & Uncertainties

$$C/N_{0_{meas}} = C/N_{0_{true}} + \varepsilon_{C/N_0};\ C/N_{0_{ref}} = C/N_{0_{ref,true}} + \varepsilon_{C/N_{0_{ref}}} \quad (6)$$

$$\Delta\, C/N_{0_{meas}} = C/N_{0_{meas}} - C/N_{0_{ref}}\,(AGC,\ elev,\ sat) \quad (7)$$

$$\Delta\, C/N_{0_{meas}} = \Delta\, C/N_{0_{true}} - \left(\varepsilon_{C/N_0} - \varepsilon_{C/N_{0_{ref}}}\right) \quad (8)$$

$$\varepsilon_{\Delta C/N_{0_{meas}}} = \left(\varepsilon_{C/N_0} - \varepsilon_{C/N_{0_{ref}}}\right) \qquad \Delta\, C/N_{0_{meas}} \sim N\left(\Delta\, C/N_{0_{true}}, \sigma_{\varepsilon_{\Delta C/N_{0_{meas}}}}\right) \quad (9)$$

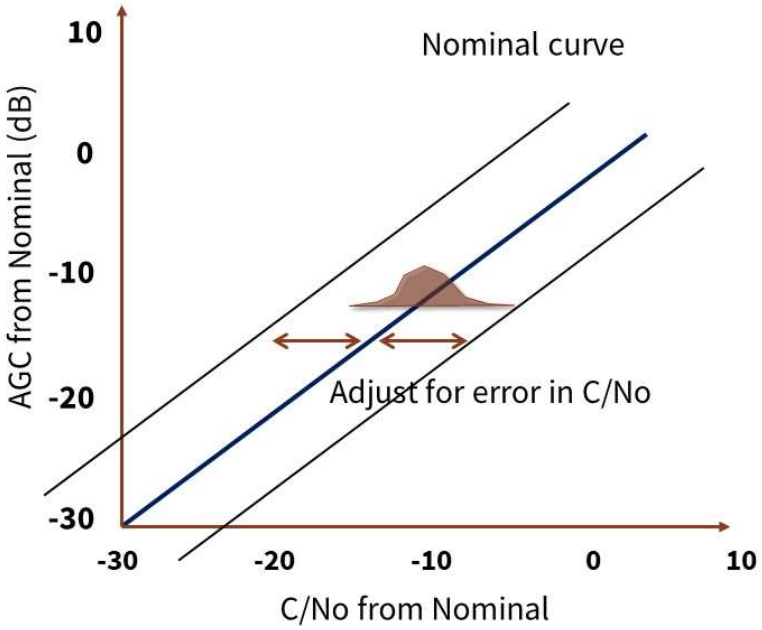

Figure 13. Adjusting the threshold line from the center threshold line to account for uncertainty in ΔC/No

The threshold line determination methodology also allows for handling uncertainty in our measurement. The uncertainty can come from measurement and calculation errors, bias in nominal reference value, and other phenomena. Equations (6)-(9) show the modeling of the uncertainties from both the measurement and nominal/reference value and how that affects the calculated ΔC/No used, $\Delta C/No_{meas,used}$. Using such calculations to determine the error statistics on $\Delta C/No_{meas,used}$, these statistics can be

incorporated into the threshold line determination to accommodate uncertainty. We outline two ways to incorporate uncertainty information into the developed RPM based detection. The first way is to adjust the location of the threshold line. The developed statistics can be used to adjust where the detection threshold line relative to the initially determined center threshold line to manage the uncertainty. This is depicted in Figure 13. For example, it can be moved horizontally towards left to increase the probability of spoof detection and hence have a lower probability of missed detection (P_{MD}). This comes with a commensurate increase in probability of false alert (P_{FA}) of spoofing. The error statistic can be used to quantify the probabilities as we can calculate the likelihood of a spoof point being on the no spoof side of the threshold line. The second to incorporate uncertainty is to define a zone of uncertainty where no decision is made. With this approach, we define as boundaries lines that are $k*\sigma_{\Delta C/No}$ horizontally from the center threshold line, with one to right and the other to the left. The zone or region in between these two new lines is the no decision region. The selection of the number of standard deviations, k, to define the zone depends on the confidence levels, such as P_{FA}, desired. This approach is graphically shown in Figure 14. The approach makes sense if the user has other spoof detection techniques available such as signal quality monitoring or CAF – cross ambiguity function which would work well in this uncertain region where spoofing and genuine signals are similar in power. As detection in the no decision region will be based on other means, the statistics is used to set the line and manage the probability of false alerts.

This formulation also suggests a potentially more practical way of developing the threshold line. A limitation of the empirical threshold line calculation is that it requires data from many scenarios including jamming, spoofing and nominal situations for each receiver set up. This makes its implementation challenging. We can use only nominal and jamming data to develop line 1 with slope m, as shown in Figure 12. A detection threshold line with the same slope that is some distance to the right of line 1. The desired distance is defined by our uncertainty as determined by our statistic. Alternatively, the region between line 1 error statistics can be used to define an uncertain zone where no decision is made. The benefit of this formulation is that we do not utilize a line 2, which requires spoofing data. This method is potentially could be more practical as it does not require spoofing data.

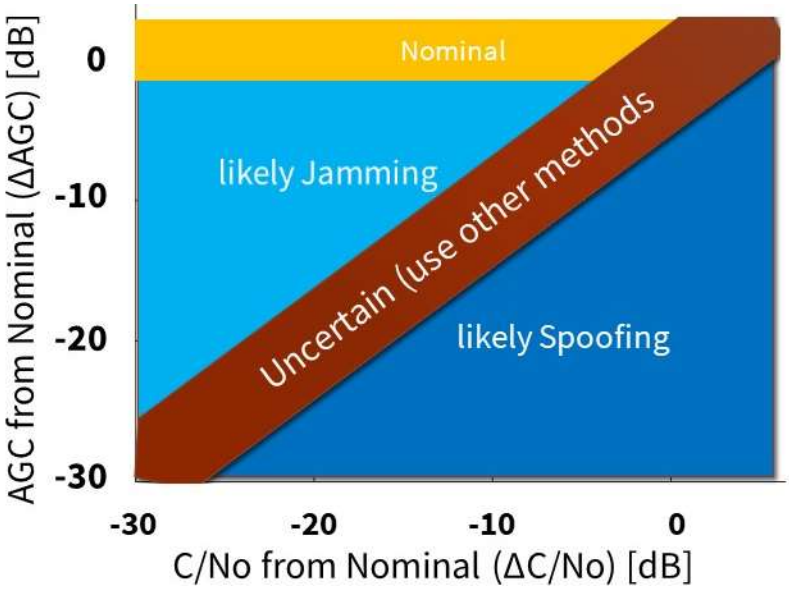

Figure 14. Using error statistics in ΔC/No to determine an uncertain zone about the center threshold line where RPM cannot make a decision on spoof/no spoof.

Decision Metric

With the detection threshold line, the confidence of the detection can be quantified by calculating the shortest distance to the threshold line. This is shown in Figure 15 and given in Equation (10). So, for a given data point (ΔC/No, ΔAGC), we get its location on the plot (i.e. which detection region it is in) which indicates the current state (spoofed or not). We then calculate the distance of that point to the detection line using Equation (10). There is greater confidence in a detection decision when the point is further from the threshold line. As seen earlier, this distance can be related to the error statistics on the ΔC/No, ΔAGC measurements.

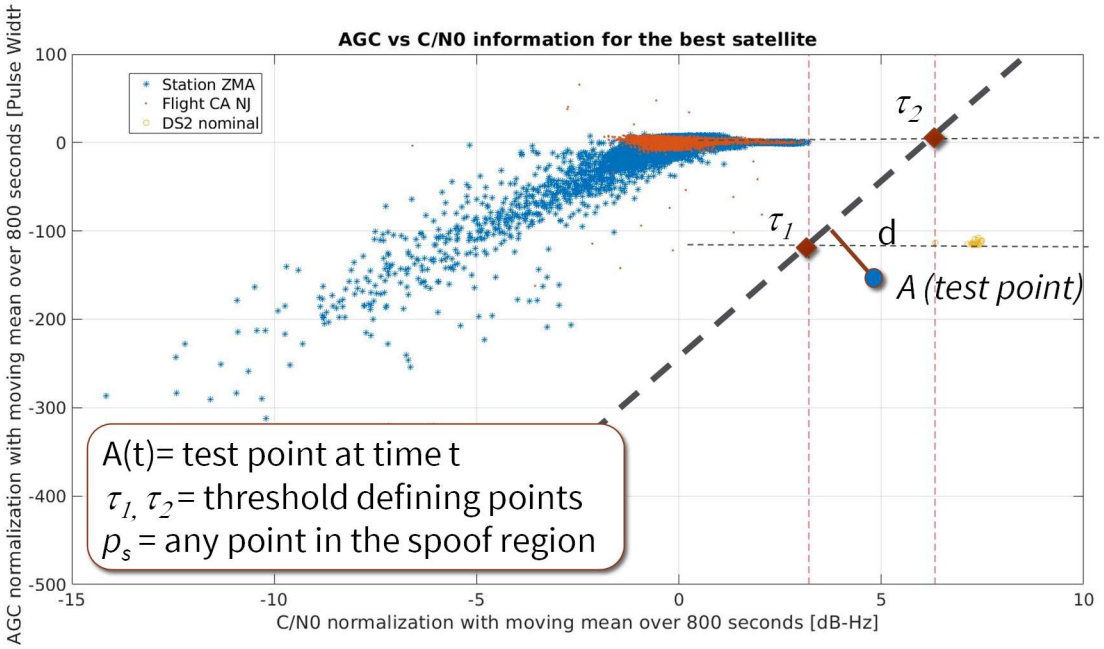

Figure 15. Empirical Detection Threshold Line with plotted data and detection metric based on distance to line

$$d = \frac{\left\| \overrightarrow{\tau_1 A(t)} \times \overrightarrow{\tau_1 \tau_2} \right\|}{\left\| \overrightarrow{\tau_1 \tau_2} \right\|} \tag{10}$$

V. LIMITATIONS AND FUTURE WORK

There are several limitations to the developed RPM technique. These limitations also suggest future directions for this work. The detection test developed is a snapshot technique and does not use any past values or time histories. As discussed, different spoofing attacks have different time signatures. It would be useful to utilize this information as part of the detection and can strengthen the detection confidence. Another limitation in the implementation is that it only utilizes one C/No measurement, the maximum over all satellites, per epoch. The other information is thrown out and it would be useful to adapt the technique to utilize the other C/No.

VI. CONCLUSION

This paper provides an overview of current state of our developed RPM test. It describes the challenges involving in using C/No and AGC measurements for spoof detection. It details the calculation of decision threshold lines to determine the spoof/no spoof detected regions in the two-dimensional ΔC/No vs ΔAGC space. The calculation of the baseline threshold line which has been shown in previous papers is described in detail. A modified means of determining a threshold line is developed that incorporates the relationship between ΔC/No vs ΔAGC. Finally, the paper describes and enumeration ways of incorporating error uncertainties in the detection test.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the support of the FAA Navigation Programs.

REFERENCES

[1] Harris, M., "Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai," *MIT Technology Review*, November 15, 2019

[2] C4ADS, "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria," 2019

[3] Goward, D., "GPS circle spoofing discovered in Iran," GPSWorld, April 21, 2020

[4] Akos, D. M., "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)," *Navigation: The Journal of the Institute of Navigation*, Winter 2012, Volume 59, Issue 4, pp 281-290. https://doi.org/10.1002/navi.19

[5] Wesson, K. D., Gross, J. N., Humphreys, T. E., & Evans, B. L. (2018), "GNSS Signal Authentication Via Power and Distortion Monitoring," *Institute of Electrical and Electronics Engineers (IEEE) Transactions on Aerospace and Electronic Systems*, 54(2), 739–754. https://doi.org/10.1109/TAES.2017.2765258

[6] Miralles, D., Levigne, N., Akos, D. M., Blanch, J., Lo, S., "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. https://doi.org/10.33012/2018.15883

[7] Hegarty, C., O'Hanlon, B., Odeh, A., Shallberg, K., Flake, J., "Spoofing Detection in GNSS Receivers through Cross-Ambiguity Function Monitoring," *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, Florida, September 2019, pp. 920-942. https://doi.org/10.33012/2019.16986

[8] Miralles, D., Bornot, A., Rouquette, P., Levigne, N., Akos, D., Chen, Y.-H., Lo, S., Walter, T., "Assessment of GPS Spoofing Detection via Radio Power and Signal Quality Monitoring for Aviation Safety Operations," *Special Issue on GNSS for Intelligent Transportation System, Institute of Electrical and Electronics Engineers (IEEE) Intelligent Transportation Systems Magazine*, Fall 2020; Volume 12, Issue 3, pp 136-146

[9] Humphreys, T., Bhatti, J., Shepard, D., Wesson, K., "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.

[10] Manfredini, E. G., *Signal processing techniques for GNSS anti-spoofing algorithms*. PhD Dissertation, Politecnico di Torino, 2017.

[11] Lee, D.-K., Spens, N., Gattis, B., Akos, D., "AGC on Android Devices for GNSS", *Proceedings of the of The Institute of Navigation International Technical Meeting (ION ITM 2021)*, January 2021

[12] Falletti, E., Pini, M., Lo Presti, L., "GNSS Solutions: Carrier-to-Noise Algorithms," *InsideGNSS* January/February 2010