Assessment of GPS Spoofing Detection via Radio Power and Signal Quality Monitoring for Aviation Safety Operations.

Damian Miralles, Aurélie Bornot, Paul Rouquette, Nathan Levigne, Dennis M Akos, Yu-Hsuan Cheng, Sherman C. Lo, Todd Walter,

Assessment of GPS Spoofing Detection via Radio Power and Signal Quality Monitoring for Aviation Safety Operations

Damian Miralles[1], Aurélie Bornot[2], Paul Rouquette[2], Nathan Levigne[1], Dennis M. Akos[1,3], Yu-Hsuan Chen[3], Sherman Lo[3], and Todd Walter[3]

***Abstract*—Due to the ever growing threat of Global Positioning System (GPS) spoofing, it has become necessary for the aviation sector to develop an effective means of detection. This paper focuses on two complementary spoofing detection techniques that are available on commercial GPS receivers and thus require no additional hardware to operate. The primary methodology for detection is using this combination of: Radio Power Monitoring (RPM) metrics, levering both Automatic Gain Control (AGC) and C/N_0 measurements, along with multiple correlations for signal distortion to provide a best practices spoofing detection algorithm which is able to distinguish between interference and spoofing. The paper first assess nominal statistics for both metrics compiled from over 250 hours of nominal data collected from multiple Wide Area Augmentation System (WAAS) stations. This data is compared to previous collections to validate the thresholds and false alarms rates and establish a complete testing methodology. These test and thresholds are then assessed with the Texas Spoofing Test Battery (TEXBAT) series of GPS spoofing data sets to confirm detection capabilities. Finally, these test and thresholds are applied to assess the GPS signal of six extended flights over the United States to assess the performance on an aircraft.**

***Index Terms*—GPS, AGC, signal spoofing detection, RFI, aviation safety.**

I. Introduction

THE number of GPS applications has steadily increased over the last decade. Application domains are many fold: banking, personal navigation, gaming, farming, defense, etc. All of these applications rely on an accurate and trust worthy signal, especially in the aviation sector, where airlines need the guarantee of a service with sufficient precision to reliably determine the position of aircraft. This knowledge is paramount to maintaining a sufficient level of safety in an increasingly crowded airspace.

Due to the nature of GPS signals, receivers are inherently vulnerable to multiple Radio Frequency Interference (RFI) sources, both unintentional, such as radio and TV stations, or intentional, including jamming and spoofing attacks. In the past, interference was the biggest threat to GPS receivers because of its simplicity of operation. In essence, interference consists of the transmission of a signal in the Global Navigation Satellite Systems (GNSS) spectrum that overpowers the signals coming from the satellites. On the other hand, a spoofing attack is more sophisticated and requires a greater knowledge of the GPS protocols involved. A GPS spoofing attack attempts to mislead the receiver by transmitting a false GPS-like signal, which causes the victim's receiver to estimate its position or time erroneously. Recently, researchers proposed an attack in a road navigation scenario using $300 worth of equipment that was capable of spoofing GPS signals. Zeng et al. [1] implemented a "ghost" map that navigates the victim to a false location but also, simultaneously, changes the navigation map to mimic the victim's surroundings (e.g. street names) thus evading suspicion. It brings to the forefront the need for protection from GPS spoofing. Nowadays, it can no longer be thought of as a potential hazard but a real threat to all GPS users, notably after recent episodes of spoofing in the Black Sea, which are considered by experts as the first mass use of GPS misdirection [2].

The aviation sector needs to be prepared to face any kind of hazardous situations, and with the realization of the GPS spoofing threat, they have to think about how to handle such attacks. An inexpensive protection that can be quickly implemented would be the best solution for this field where security needs to be maintained at a maximum level without increasing production cost. Various techniques have been developed in previous literature to detect the presence of GPS spoofing [3]. A combination of detection methods using metrics that are contained inside a GPS receiver and do not require additional hardware in order to detect a spoofing attack would be an effective option for this particular case. As proposed in [4], the combined use of Signal Quality Monitoring (SQM) and RPM measurements allows the user to detect certain types of GPS spoofing attacks. The algorithm is based on metrics that can be obtained from components in commercial GPS receivers, which reduces the costs of implementation in multiple sectors.

The purpose of this paper is to formalize the computation techniques for RPM methods (combination of AGC and C/N_0, use additional field data to reassess the thresholds metrics of the SQM parameters used by the aforementioned publications, and apply the new thresholds and algorithms against collected flight data. In terms of validation, the changes proposed are then evaluated using new nominal data that includes (1) WAAS data collections, (2) in flight data collections, and (3) spoofed data collections.

II. Previous Work

Interest in GPS spoofing has intensified since the initial years of radio navigation technologies. Spoofing countermea-

1-University of Colorado at Boulder
2-ENAC
3-Stanford University

sures have multiple steps. First they attempt to detect whether or not a signal is being spoofed, and if so, they warn the victim's receiver that its position solution is unreliable. Next, they try to recover the true signal, which can be hard or even impossible depending on the type of spoofing attack. According to Psiaki and Humphreys [3], there are various kind of spoofing assaults that can be performed, and these vary greatly in sophistication. From the simplistic approaches, such as meaconning or repeaters, to advanced forms of spoofing, such as nulling attacks. Thus, knowing the different kinds of attacks and how offenders perform them allow us to create effective counter measures. Several spoofing detection methods have been presented before. Among them, approaches based on Kalman filters [5] and Receiver Autonomous Integrity Monitoring (RAIM) [6] operate by using prior knowledge of the position solution and apply filtering logic to determine obvious unrealistic changes in position that the less sophisticated spoofing attacks provide. However, because of the wide variety and complexity of spoofing attacks, at this moment there isn't an effective method of spoofing detection that covers the majority of attacks. Each of the methods described can protect from specific attacks; thus, a combination of methods could be employed to inherit the strengths of each one. Moreover, there are two types of indicators: static and transient. A static indicator is able to detect the presence of spoofing from the moment it is turned on; whereas a transient indicator is only able to detect a spoofing attack when the spoofed signal is modifying the signal parameters of the receiver. It makes sense that the best solution for the aviation sector is to protect from the greatest number of attack modes using the least expensive methods of detection.

An adequate first static indicator is based on RPM throughout the combination of AGC and C/N_0 functionality. In nature, the AGC tries to optimize the dynamic range of the front end of the receiver to that of the Analog to Digital Converter (ADC), by adjusting its gain with respect to the magnitude of the incoming signal of the channel as shown in Fig. 1. Consequently, it was assessed to be a useful metric for detecting overpowered interference [7]. Going further, monitoring the combination of AGC and C/N_0 has proved to be a powerful spoofing detection tool, especially for the most simplistic attacks, such as overpowering [8]. It should also be noted that AGC measurements are becoming more predominant in multi-bit GNSS front-end designs, even now, low cost and mass market receivers are giving access to such measurements to the users, as shown by the new raw GNSS measurements supported by some Android smart-phones [9]. Given that the gain coming from the AGC is dependent on the condition of the signal it can vary depending on the effective temperature of the antenna. Therefore, it is possible that the AGC value by itself may not be stable enough to define a precise threshold for detection. This represents a problem for spoofing detection when under matched power attacks. Moreover, all receivers may not have the same level of sensitivity within their AGC circuitry. Consequently, the AGC values wouldn't be capable of detecting spoofing attacks that are close to matching the power of the true signal with any given receiver.

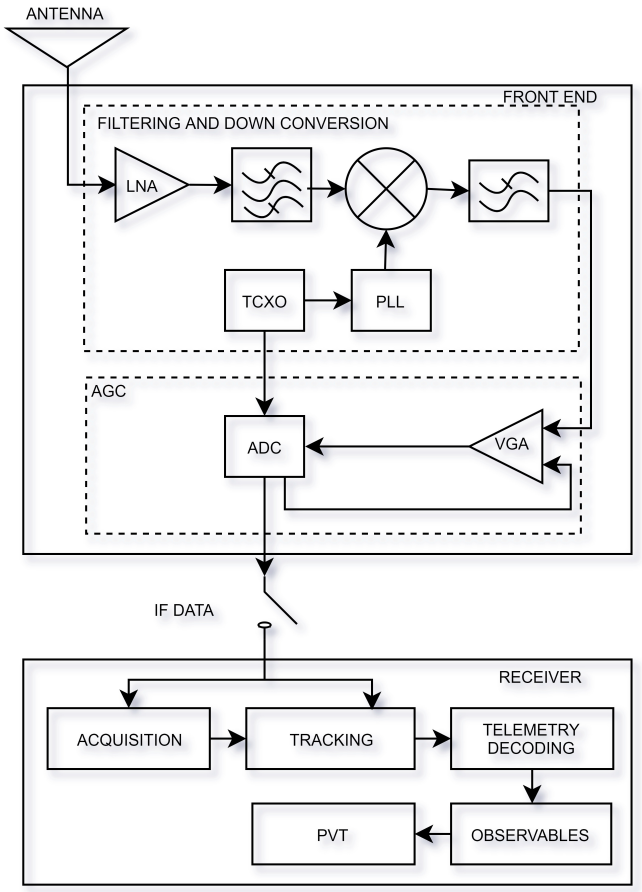


Fig. 1. Conceptual design of the typical GPS receiver architecture.

A solution to cover both overpowered and matched power attacks is to use AGC values with another metric in order to be able to detect matched power attacks. A method based on SQM identifies asymmetries in the correlation function and could be able to fulfill this requirement [10]. The method first establishes thresholds using the Neyman Pearson test, then it compares the current value of the metric of the receiver to the previous metric in order to decide whether a spoofing attack is occurring. Nevertheless, this approach has difficulties detecting attacks where the power of the spoofing signal is far greater than the true signal's power, due to the high power of energy within the channel that mask the signal under the noise floor. The method is a transient indicator, detecting the spoofing attack at the very moment of the change of the signal parameters of the receiver. The combination of these methods are complementary and sufficient enough to solve the needs of the aviation sector concerning the protection of the most common types of spoofing attacks in the most efficient way.

III. WAAS DATA COLLECTION

This work uses more than 250 hours of data collected from several stations across the world divided into two sets: (1) `wdc0814` (120 hours of data from six WAAS stations) and (2) `wdc0218` (168 hours of data from 38 WAAS stations). Both data sets were done using a NovAtel GIII receiver. Although a

set of spoofing and interference threshold were already established for wdc0814 in [4], this work reassess those metrics, and proposes new values based on the combined collection results of wdc0814 and wdc0218. Before establishing any thresholds, we will compare the two sets of data in order to see differences in the reporting spoofing detection metrics based on RPM and SQM.

The AGC metric in the NovAtel GIII receiver uses Pulse Width (PW) units. As reported by [11], these dimensionless units range from 800 [u] in the absence of signal to 350 [u] when AGC saturation is achieved. Work developed by [11] also developed a method to map the dimensionless PW measurements into dB units by inserting controlled amounts of noise (in dB units) into the receiver and recording its output. Although the experiment created an extrapolation tool for unit conversions, work presented here used the original PW measurement due to convenience. The SQM metric is based on the particularity of the shape of the correlation function. In a nominal case, the function is symmetrical, but if any additional signal is present in the L1 frequency band, the shape will be distorted. The metric proposed is made of a linear combination of 9 correlators of the receiver from -0.1016 chips to +0.1016 chips, as shown in Table I. The metric is then normalized by the value at zero delay. Mathematically, work in [4] defined it as:

$$SQM(t) = \frac{1}{N}\sum_{i=1}^{N}\frac{L_x^i - E_x^i}{P_0^i}, \quad (1)$$

where $SQM(t)$ is the computed SQM metric, N is the number of satellites at time t, $L_x^i = (L_{0.10}^i + L_{0.07}^i + L_{0.05}^i + L_{0.02}^i)$ and $E_x^i = (E_{0.10}^i + E_{0.07}^i + E_{0.05}^i + E_{0.02}^i)$ represents the linear combination of the late and early correlators for each satellite, and P_0^i is the prompt correlator at zero delay for each satellite. The thresholds for the metric, were defined in [4], but the analysis for its computation is outside the scope of this material.

TABLE I
GIII LINEAR CORRELATORS AND RESPECTIVE SPACING USED FOR SQM TESTING.

Spacing	Lin.Comb	Spacing	Lin.Comb
-0.1016	-1	-0.0766	-1
-0.0516	-1	-0.025	-1
0	0	0.025	1
0.0516	1	0.0766	1
0.1016	1		

To improve the quality of the datasets' comparison, WAAS stations shared by both collections (wdc0814 and wdc0218) were used. Table II reports the mean value and the standard deviation of the AGC for the common six stations labeled as: FAI, HNL, ZAU, ZBW, ZMA, and ZSE. While Tab. III does the same for the SQM metric.

A closer study of the AGC metric shows that the data for the two sets behaved in similar fashions. Stations who presented drops in the AGC values, because of RFI events, still had those kind of drops in the new datasets. Although both the wdc0814 and wdc0218 data sets logged data for six common stations, an analysis on only two cases is presented here for simplicity. The ZMA station (Miami, FL) was exposed to high levels of RFI. While, the ZSE station (Auburn, WA) was barely exposed to RFI, which was the case for the majority of provided WAAS stations. Data collected for the WAAS stations used in the analysis of [4] (wdc0814), and the ones used in this paper (wdc0218) were not taken at the same time. However, a

TABLE II
MEAN AND STANDARD DEVIATION OF THE AGC METRICS FOR THE RECORDED DATASETS

	Mean AGC (PW)		STD AGC (PW)	
WAAS	wdc0814	wdc0218	wdc0814	wdc0218
FAI	621	538	3.1	3.6
HNL	583	567	2.5	1.0
ZAU	574	561	3.3	2.9
ZBW	628	570	4.0	2.9
ZMA	673	563	4.7	4.9
ZSE	594	562	2.7	3.0

TABLE III
MEAN AND STANDARD DEVIATION OF THE SQM METRICS FOR THE RECORDED DATASETS

	Mean SQM		STD SQM	
WAAS	wdc0814	wdc0218	wdc0814	wdc0218
FAI	0.0009	-0.0003	0.0043	0.0054
HNL	-0.0017	-0.0017	0.0051	0.0051
ZAU	0.0020	-0.0021	0.0055	0.0053
ZBW	-0.0024	-0.0019	0.0048	0.0051
ZMA	0.0006	-0.0017	0.0056	0.0053
ZSE	-0.0007	-0.0009	0.0058	0.0059

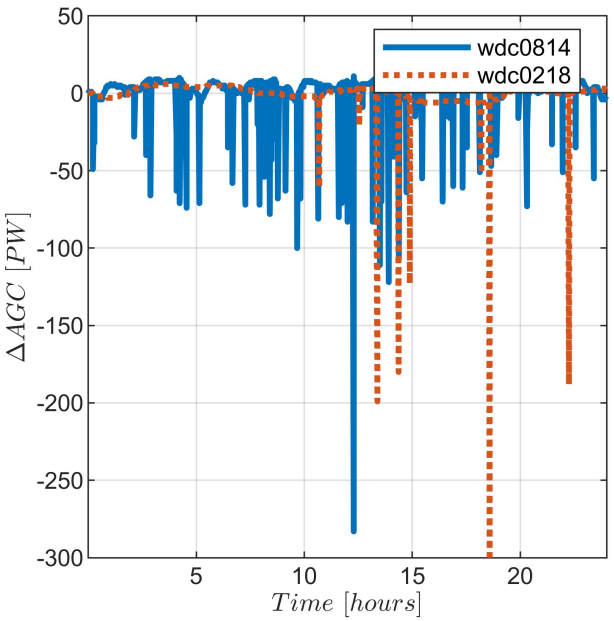


Fig. 2. AGC values upon 24 hours for ZMA WAAS for the two data sets.

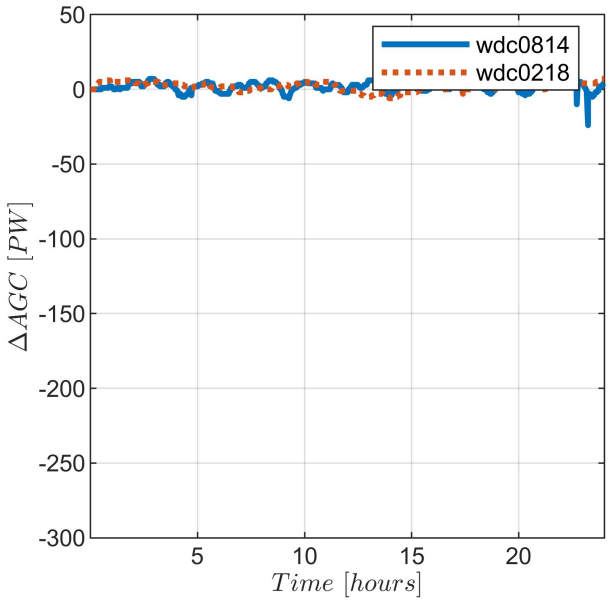


Fig. 3. AGC values upon 24 hours for ZSE WAAS for the two data sets.

consistency in the measurements appears across the stations. Fig. 2 shows a decrease in the AGC values for the ZMA station regardless of the dataset used, this as explained before is an indication of the RFI experienced by the station in its heavily dense urban canyon environment. In a similar way, in the ZSE station, the AGC values are rather stable for both datasets, as shown in Fig. 3, which is expected given that the ZSE station is located in a rural area with negligible sources of RFI. Given the similarities in the results shown before, it is safe to assume that this phenomenon shows the coherence within the collection of the data and the integrity of the WAAS station. As mentioned before, the AGC values are sensitive to the temperature of the antenna, which leads to slightly high variations of its gain [8]. In the WAAS stations framework gain stability is high, thus these variations are generally low and work well for assessing the nominal behavior.

IV. New thresholds and test on the flight data

The spoofing and jamming thresholds proposed in [4] were evaluated thanks to a battery of recorded spoofing scenarios from the TEXBAT datasets. Humphreys et al. [12] compiled these records to define the notion of spoof resistance for commercial GPS receivers . A description of these scenarios is shown in Table IV as per the study of [13], but without loosing the sense of generality, the scenarios on the TEXBAT dataset are divided by (1) power of transmission, and (2) receiver dynamics. The challenge with the dynamic attacks is to differentiate between spoofing effects and similar variations that happen naturally on a platform such as multipath. However, from the perspective of the RPM method, the metric proposed here, only inspects the power change in the band. Thus, the nature of multiple datasets (static or dynamics) do not lead to significant changes in the detection outcome of the RPM method. As a result, multiple scenarios are categorized in the same groups regardless of its dynamics, and a new distinction is used to differentiate over-power and matched-power attacks. For example, the `ds5` scenarios behaves similarly to the static case `ds2`, while `ds6` is similar to `ds4` and `ds4`. Only on the cases of matched powered scenarios, the irregularities in the correlation function will come to play significantly and the SQM techniques will be more relevant in the detection capabilities such as for the `ds3` and `ds4` matched power scenarios.

TABLE IV
TEXBAT SCENARIOS DESCRIPTION.

Name	Scenario	Description
static	Clean datasets	Clean data, no spoofing
ds2	Static overpowered time push	+10dB of power
ds3	Static matched power time push	+1.3dB of power
ds4	Static matched power with position push	+0.9dB of power
ds5	Dynamic overpowered time push	+9.9dB of power
ds6	Dynamic matched power position push	+0.8 dB of power

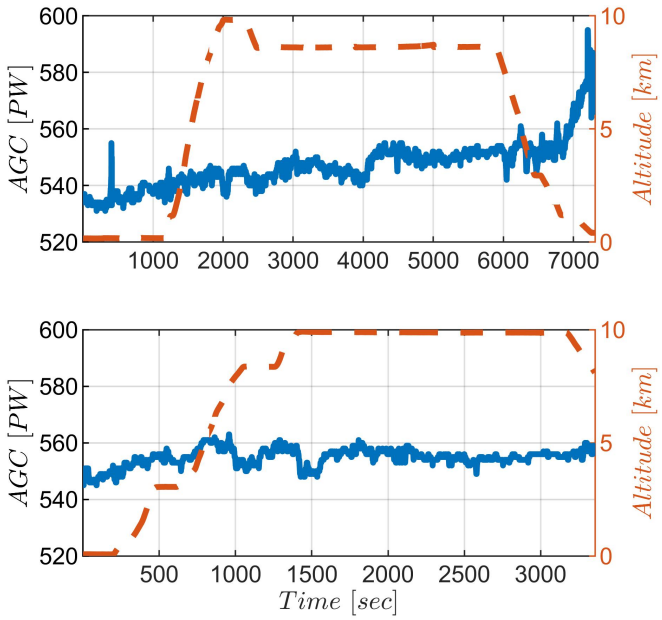


Fig. 4. AGC values vs spacecraft height for the BNA to OKC (top) and NQA to OKC(bottom) flights.

Table IV does not list the latest scenarios added to the TEXBAT datasets, namely `ds7` and `ds8`. The `ds7` spoofing scenario is a power matched time push scenario much like `ds3`, but is more subtle because it employs carrier phase alignment between the spoofed and authentic signals. The `ds8` spoofing scenario is identical to the `ds7` scenario except that the spoofer treats every received navigation data bit as if it were an unpredictable low-rate security code and attempts to guess the value of the data bit in real time [13]. The thresholds proposed in [4] were not evaluated on these

scenarios. A similar situation happens with this work. The authors worked under the assumption that adding a phase alignment or knowing the value of data bit in real time does not change the detection outcome as long as we are only working in a detection of power change or asymmetries in the correlation function. Hence, we consider these scenarios similar in nature to `ds3` and `ds4` and we did not test our thresholds on them.

Another point is that the `wdc0814` thresholds introduced in [4] are in dB, but the AGC metric reported by NovAtel receivers, including those deployed in WAAS stations such as the NovAtel GIII are provided in PW units. Although, the authors recognize that the PW units are not standardized for reporting AGC measurements, a trade-off is done to increase the accuracy of detection and to avoid potential errors in the mapping translation proposed in [4]. In addition, the further refinement of the detection thresholds discussed in the paper, will also be of value to other models within the brand, and the nature of the double difference "sliding window" concept in the detection explained in section V. We will then use this unit for all of our AGC analysis and a mapping will be provided in order to convert to the previous thresholds. Thanks to the consistency within the two sets of WAAS data, and as long as the newly proposed thresholds were validated on the TEXBAT datasets, the new set of thresholds can also be validated.

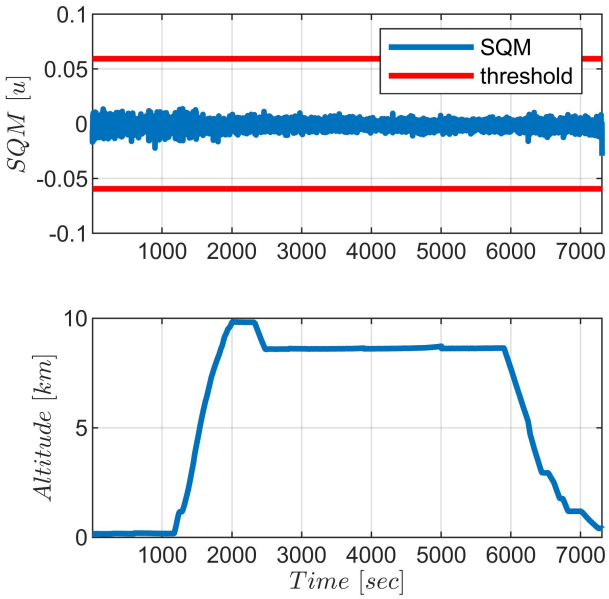


Fig. 5. SQM metric vs altitude for the BNA to OKC flight

In addition to the WAAS data, recorded flight test data (see Table V) was replayed into the NovAtel GIII receiver. The flights took place over six different airports: Nashville International Airport (BNA), Will Rogers World Airport (OKC), Sacramento International Airport (SMF), Atlantic City Airport (ACY), Millington Regional Jetport (NQA), and William J. Hughes Technical Center (WHJTC). The recorded flight data is presumed to have no spoofing during the collection of the measurements.

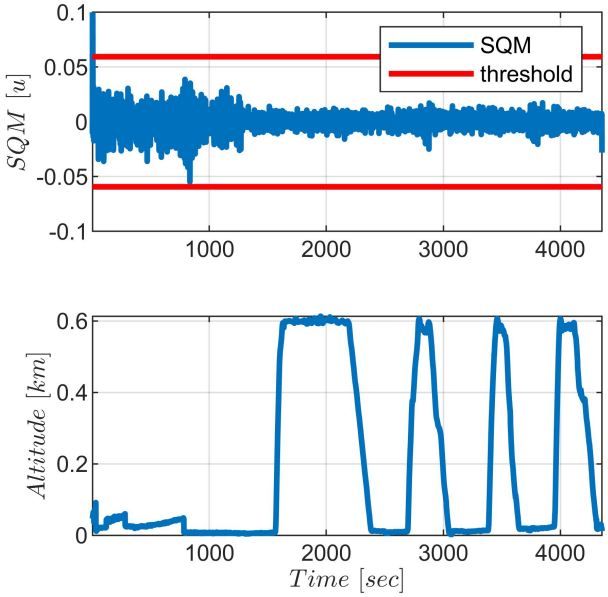


Fig. 6. SQM metric vs altitude for the WJHTC to WJHTC flight

Fig. 4 shows the AGC metrics results for the flights BNA to OKC and NQA to OKC. Although only displaying a subset of all the flights, the AGC is stable during the period of collection and only shows minimal changes in its ranges when the plane is taking off or landing due to it experiencing significant changes in its environment.

TABLE V
SQM STANDARD DEVIATION DURING TOTAL FLIGHT DURATION (σ_{total}), ON THE GROUND (σ_{ground}), AND IN THE AIR (σ_{air}) FOR THE SIX RECORDED FLIGHTS

Flights	Time(min)	σ_{total}	σ_{ground}	σ_{air}
SMF-ACY	289.6	0.0032	0.0052	0.0030
ACY-SMF	355.9	0.0033	0.0057	0.0029
WJHTC-WJHTC	72.5	0.0083	0.0097	0.0050
BNA-OKC	121.8	0.0034	0.0050	0.0030
NQA-OKC	55.9	0.0039	0.0071	0.0036
BNA-BNA	143.9	0.0039	0.0045	0.0038

The same behavior is observed regarding the SQM metric, upon the flights data, the metric never raises any alarm. For all the flights except the WJHTC to WJHTC, the SQM is very similar to the BNA to OKC flight shown in Fig. 5. This is also highlighted by the close standard deviation for all the flights reported in the Table V. Fig. 5 and 6 represent the SQM metric versus altitude computed for the flights BNA to OKC and WJHTC to WJHTC. The SQM has higher variations while the aircraft is on the ground than when the aircraft is flying, as confirmed by Table V (considering that the aircraft is in flight at an altitude higher than 200m). Regarding the flight profile of WJHTC to WJHTC in Fig. 6, the numerous returns of this aircraft to the ground during the flight explain the higher standard deviation, even if it is still close to the other standard deviation values. This highlights the sensitivity

of SQM to multi-paths scenarios, which are more common on the ground. Future work defining different thresholds for the SQM metric while in flight and on the ground can help to a further adjust for the detection of spoofing attacks.

V. Combination of AGC and C/N_0

As mentioned in section II, the AGC was first used as an attempt to detect RFI and spoofing attacks into the GPS band. Regardless of their nature (intentional or unintentional), they both add power to the band, and thus they both have a similar impact on the AGC measurements value. However, the AGC readings are not enough to distinguish both kinds of attacks and in order to lower the probability of false alarm, a criteria to distinguish between RFI and spoofing was considered. A process based upon the observation of both the AGC and C/N_0 value is discussed in [4]. Even if the interference (unintentional RFI, jamming or spoofing) leads 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 an overpowered 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. On the contrary, during an overpowered spoofing attack, the signal is generated to look like a GPS signal. Thus, it increases the power of the carrier signal, leading to a rise in the C/N_0 value.

The new collected data helps validate this premise by creating a differential moving average of the AGC and C/N_0 values respectively. The method, hereafter called a "sliding window" in this paper, is defined by:

$$\vec{\Delta}\psi_i = \psi_i - \frac{1}{N}\sum_{j=1}^{N}\psi_j \tag{2}$$

where $\vec{\Delta}\psi_i$ is the sliding window metric, ψ_i is the instantaneous reading, and $\frac{1}{N}\sum_{j=1}^{N}\psi_j$ is the moving average for the readings with N being the size of the sliding window length selected. The formula from (2) is applied to both the AGC or C/N_0 measurements in order to compute the desired difference. In the case of the C/N_0 measurements, it is important to note that (2) was applied on the metrics of the strongest satellite (highest C/N_0 value).

A result of the sliding window metric for the C/N_0 and AGC measurements of the station ZDC, flight SMF to ACY, and TEXBAT scenario `ds2` is plotted in Fig. 7, 8, and 9, respectively. Assuming that the WAAS station and the flight data were not spoofed during the data collection, the drops of the AGC and C/N_0 values shown in Fig. 7 and 8 are only due to unintentional RFI. On the contrary, Fig. 9 represents the nominally spoofed `ds2` scenario, where a drop of the AGC values is not associated with a drop of the C/N_0 values, indicating, as such, a potential clue for the detection of the overpowered spoofing attack.

Plotting the AGC versus the C/N_0 sliding window metrics, of the WAAS stations, flights collections, and `ds2` scenario causes two distinct sections to appear as shown in Fig. 10. The flights and WAAS stations data, which are nominal operational cases of RFI interference i.e. no spoofing, tend to stay left of the threshold line (red). The spoofing attacks, however, tend

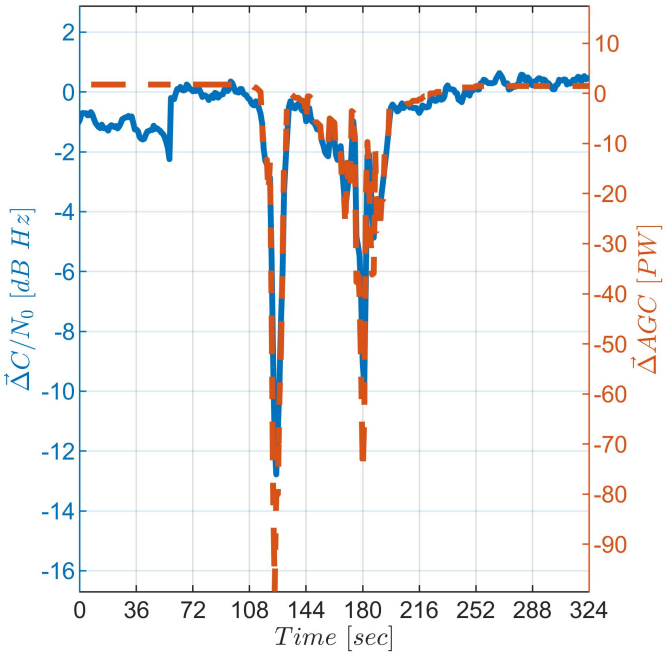


Fig. 7. $\vec{\Delta}C/N_0$ and $\vec{\Delta}AGC$ metrics for ZDC station.

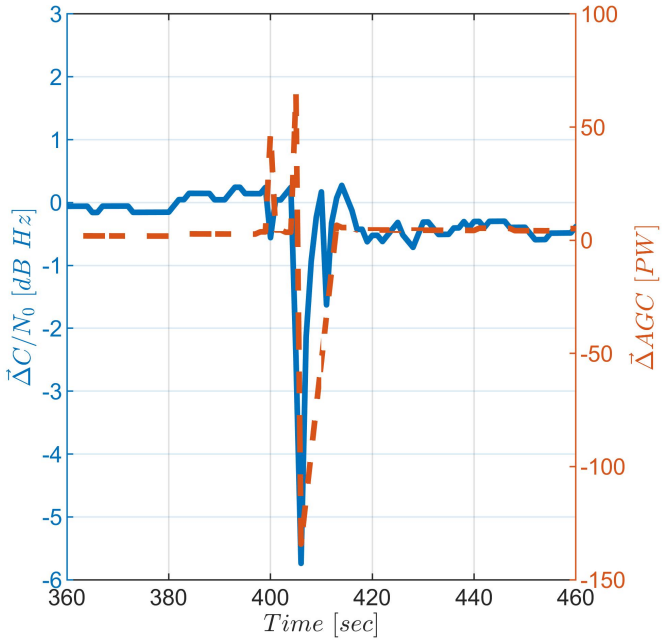


Fig. 8. $\vec{\Delta}C/N_0$ and $\vec{\Delta}AGC$ metrics for SMF to AYC flight.

to be right of the threshold line of the plot. Ideally, a threshold can be defined in order to contain all interference cases to the left section, whereas spoofing attempts will be contained to the right in the diagram.

Fig. 10 was generated by combining the sliding window metric from (2) for the AGC and C/N_0 measurements respectively. Depending on the chosen sliding window length, the two zones on each side of the threshold line can be more clearly detected, and in order to define a threshold with the lowest false alarm probabilities, the spacing between the zones

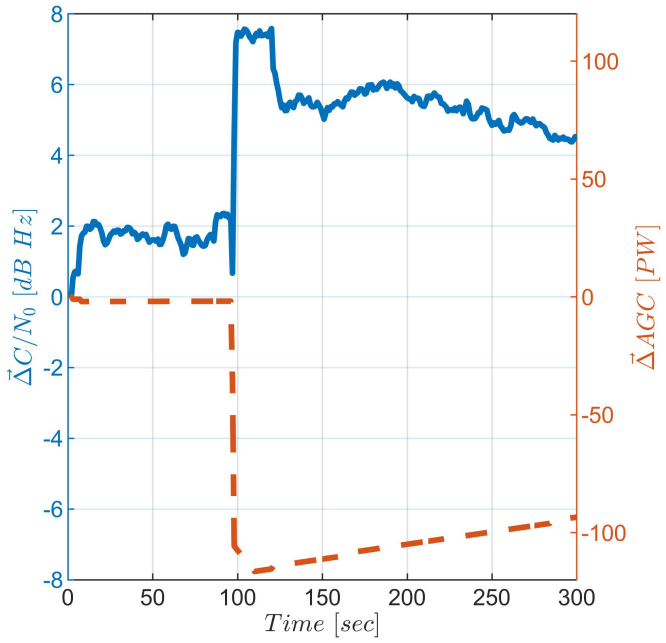


Fig. 9. $\vec{\Delta}C/N_0$ and $\vec{\Delta}AGC$ metrics for the `ds2` spoofing scenario.

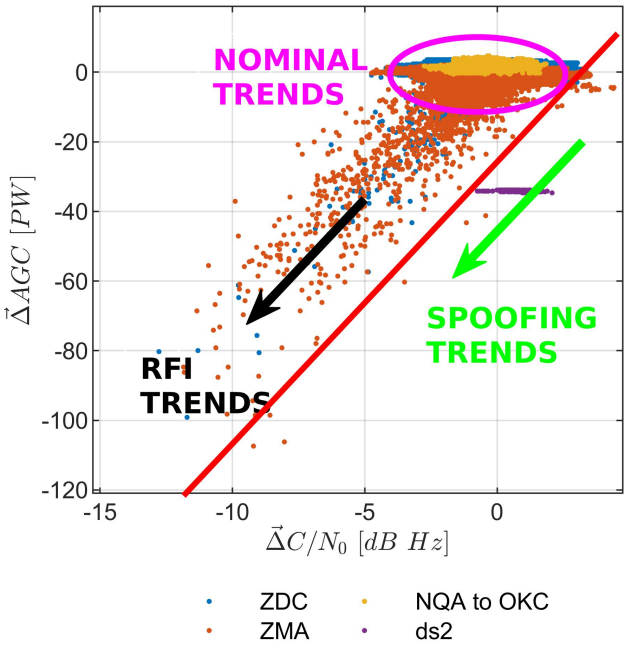


Fig. 10. $\vec{\Delta}C/N_0$ and $\vec{\Delta}AGC$ metrics for different WAAS stations, recorded flight trajectories, and TEXBAT scenarios.

must be maximized. Fig. 11 shows the relationship between the window length and the separation area width. The optimal area width, relative to its window size, happens when using a window length of 1100 seconds, which translates into an area width of 3.15 units. This criteria can be evaluated by plotting data from the collections at hand, which includes the WAAS station ZMA, flight SMF to ACY, and TEXBAT scenario `ds2`.

The width of the area is dependent on the sliding window

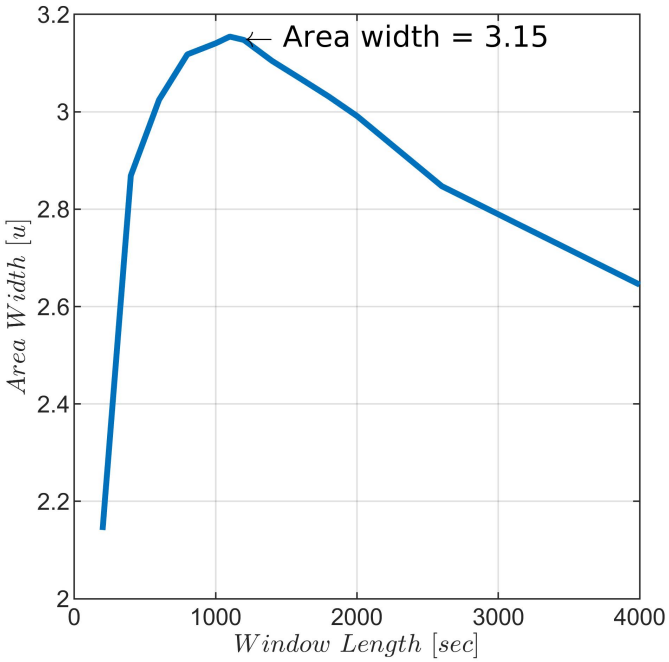


Fig. 11. Size of the area depending on the sliding window size

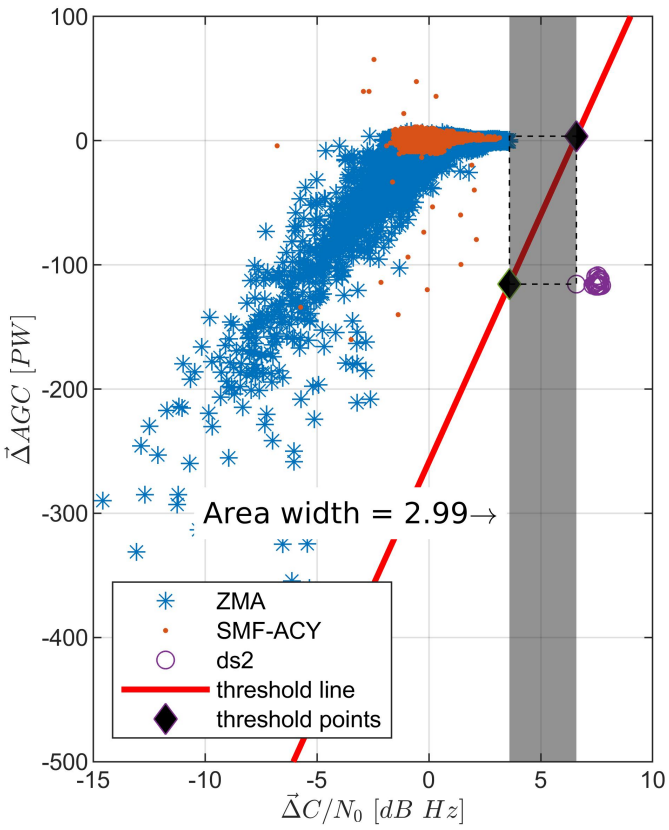


Fig. 12. $\vec{\Delta}C/N_0$ and $\vec{\Delta}AGC$ metrics for sliding window of 2000 seconds in nominal data

length, as shown in Fig. 11 and 12. The computed area is based on the C/N_0 parameter of the data and is defined as the worst C/N_0 for the WAAS/flight data and the best C/N_0 value for the `ds2` set. Notice that when using a window length of 2000

seconds (see Fig. 12) the resulting width is 2.99 units, which is lower than the resulting area width of 3.15 units when using the optimal window size is of 1100 seconds discussed before.

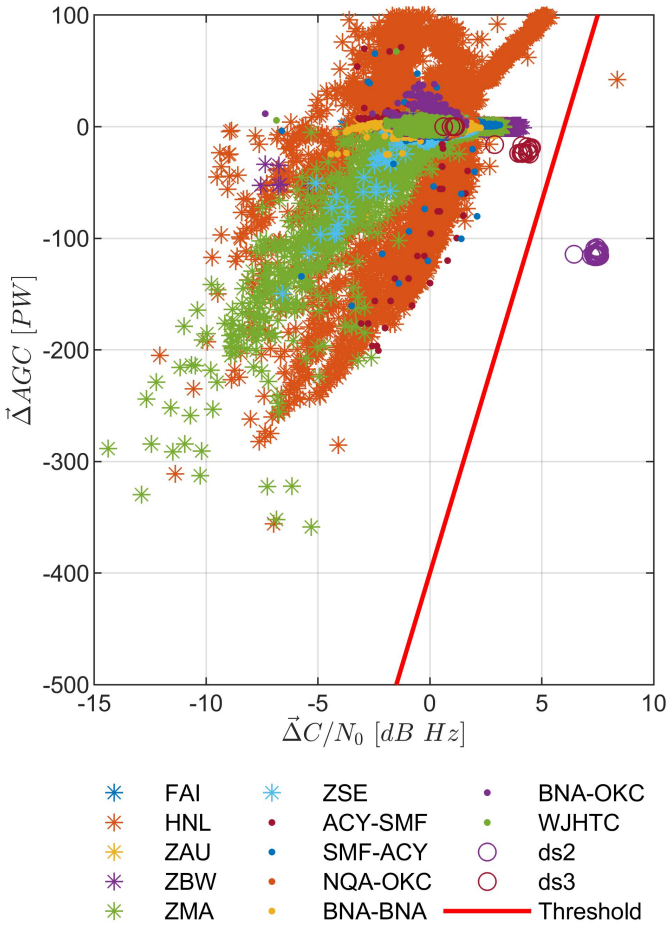


Fig. 13. $\vec{\Delta}C/N_0$ and $\vec{\Delta}AGC$ metrics using a 1100 sec window length for recorded data

Fig. 11 and 12 also offer the methodology used to define the threshold metric that will lower the probabilities of false alarm detection when processing data with the receiver. The threshold line shown is formed by computing the slope created by the threshold points, which will effectively be equivalent to the diagonal of an imaginary square formed by the edges of the operational regions as shown. A diagonal threshold is preferred over a vertical one, because the vertical one would have only taken C/N_0 into account and not the effect of both metrics as the diagonal threshold does. Determining which side of the threshold line a new metric is located can be accomplished by computing the cross product between the vectors formed by the threshold points (Υ_1, Υ_2), and the target measurement point (Γ) as:

$$\begin{aligned} RPM(t) &= \vec{\Upsilon_1\Upsilon_2} \times \vec{\Upsilon_1\Gamma} \\ &= x_{\Upsilon_1\Upsilon_2} \cdot y_{\Upsilon_1\Gamma} - x_{\Upsilon_1\Gamma} \cdot y_{\Upsilon_1\Upsilon_2} \end{aligned} \tag{3}$$

where the threshold points, shown in Fig. 12, have coordinates $\Upsilon_{1,2} = [\Delta C/N_0^*, \Delta AGC^*]$, $\Gamma = [\Delta C/N_0, \Delta AGC]$, and $RPM(t)$ indicates the position of the point in the diagram with $RPM(t) > 0$ indicating the right side and $RPM(t) < 0$ indicating the left side. All the points right of this threshold

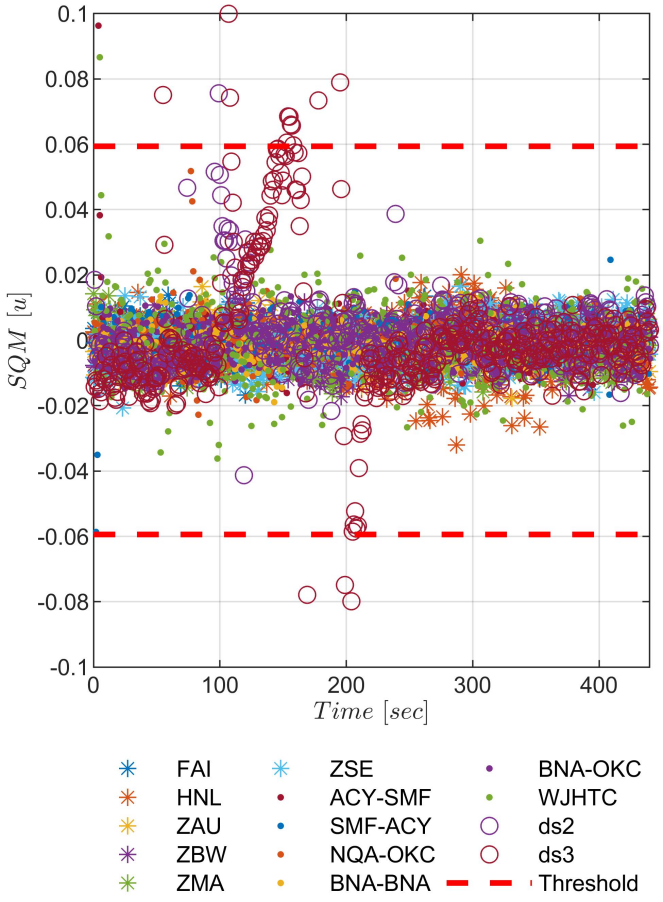


Fig. 14. SQM metrics for the common WAAS stations, flights data and TEXBAT scenarios `ds2` and `ds3`.

line are considered to be spoofing attacks, while points left of this line are RFI or nominal events, see Fig. 13. Of relevance is the `ds3` scenario, which is not detected by this threshold. Nevertheless, this scenario is a power matched attack, as shown in Table IV, and the usage of the SQM metric will result in a more reliable detection method. This is shown by Fig. 14, where the correlation inconsistencies generated by the matched power spoofing attacks are detectable by the predefined thresholds in the metric. The final combination of the discussed metrics is described mathematically in (4) as:

$$\begin{aligned} &Spoofing\ if\ : \\ &RPM(t) > 0, \\ &or \\ &SQM(t) > |0.0594|, \end{aligned} \tag{4}$$

where $RPM(t)$ is the metric defined in (3) and $SQM(t)$ is the metric defined in (1). The association shown in (4) between SQM and AGC+C/N_0 allows us to detect the two different types of spoofing attacks.

VI. Conclusion

This paper presented the use of a more sophisticated spoofing detection technique based on two complementary

methods previously developed. The algorithms developed, and the refinement of the previously established thresholds were performed using an extensive collection of nominal data from WAAS stations. The method is composed of RPM control through the AGC and C/N_0 measurements in association with the monitoring of asymmetries within the correlation function via SQM. Results presented were tested on nominal and spoofed data (using the TEXBAT dataset)that was replayed or collected using the same receiver type to achieve consistency in the measurements. The application of these methodologies and corresponding thresholds were finally evaluated against flight data to create a tool against interference detection in the aviation sector.

The paper also presented a new metric for the SQM, which would require additional correlators but would expand the "zone" of investigation. It would also highlight the sensitivity of the SQM regarding multipath scenarios. Finally, an experiment using a modified version of the work presented by [11] for differentiating between RFI and spoofing was further calibrated with new data, including `wdc0218` and flight data, in order to improve the accuracy of the previously defined metric. The proposed algorithm was tested using a variety of collections that included collections `wdc0218` and `wdc0814`, flight data, and the spoofed scenarios from the TEXBAT datasets. It demonstrated how using a combination of AGC, C/N_0, and SQM allow us to identify more precisely RFI and spoofing in a variety of interference attacks.

The association of those measurements provides an effective means of spoofing detection for the aviation sector due to the simplicity of the methods, the re-usability of measurements provided by some commercial receivers, and computational cost of the methods. To refine this this assessment, it would be important to perform the same test with flight data under spoofing attacks but the authors recognize the difficulty of the task given the strict enforcement of the L1 band, and the limitations of cost of spoofing software in the radio navigation community. Finally, because the methodology proposed, is capable to detect interference and multiple types of spoofing attacks, it should present an improvement for aviation safety operations in such environments.

ACKNOWLEDGMENT

The authors would like to thank Karl Shallberg, John T. Flake, and Roger Ishimoto, from Zeta Associates, for helping with the data collection system and providing the NovAtel G-III receiver and required equipment. In addition, we thank Scott F. Holman from the CU Boulder Writing Center for his feedback and support during the writing process.

REFERENCES

[1] Kexiong Curtis Zeng, Yuanchao Shu, Shinan Liu, Yanzhi Dou, and Yaling Yang. 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, pages 85–90, New York, NY, USA, 2017. ACM.

[2] Inside GNSS. Reports of Mass GPS Spoofing Attack in the Black Sea Strengthen Calls for PNT Backup, July 2017.

[3] M. L. Psiaki and T. E. Humphreys. GNSS Spoofing and Detection. *Proceedings of the IEEE*, 104(6):1258–1270, June 2016.

[4] Esteban Garbin Manfredini, Dennis M Akos, Yu-Hsuan Chen, Sherman Lo, Todd Walter, and Per Enge. Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers. In *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, pages 672–689, Reston, Virginia, January 2018.

[5] K Deergha Rao, MNS Swamy, and EI Plotkin. Anti-Spoofing Filter for Accurate GPS Navigation. In *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, pages 1536–1541, Salt Lake City, UT, September 2000.

[6] Hengqing Wen, Peter Yih-Ru Huang, John Dyer, Andy Archinal, and John Fagan. Countermeasures for GPS Signal Spoofing. In *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*, pages 1285–1290, Long Beach, CA, September 2005.

[7] F. Bastide, Dennis M. Akos, C. Macabiau, and B. Roturier. Automatic Gain Control (AGC) as an Interference Assessment Tool. In *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, pages 2042–2053, Portland, OR, September 2003.

[8] Dennis M Akos. Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *Navigation: Journal of the Institute of Navigation*, 59(4):281–290, Winter 2012.

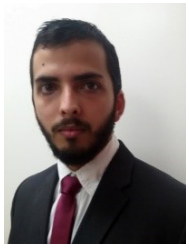
[9] Damian Miralles, Nathan Levigne, Dennis M. Akos, Juan Blanch, and Sherman Lo. Android Raw GNSS Measurements as the New Anti-Spoofing and Anti-Jamming Solution. In *Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, pages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

[10] K. Ali, E. G. Manfredini, and F. Dovis. Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics. In *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, pages 1240–1247, May 2014.

[11] Esteban Garbin Manfredini. *Signal processing techniques for GNSS anti-spoofing algorithms*. Phd, Politecnico di Torino, 2017.

[12] Todd E Humphreys, Jahshan A Bhatti, Daniel Shepard, and Kyle Wesson. The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques. In *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, pages 3569–3583, Nashville, TN, September 2012.

[13] Adam Lemmenes, Phillip Corbell, and Sanjeev Gunawardena. Detailed Analysis of the TEXBAT Datasets Using a High Fidelity Software GPS Receiver. In *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, pages 3027–3032, Portland, OR, September 2016.



Damian Miralles is a PhD 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, software defined radio and digital signal processing.

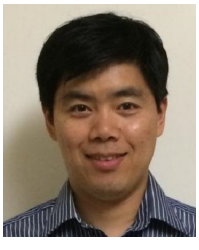
Aurélie Bornot is a master student following the engineering curses at the ENAC, the French university of civil aviation, Toulouse. She specialized in space telecommunication and more specifically in Aerospace Radio Frequency Engineering. Her research interests are in GNSS receiver technologies, integrity control and signal processing.

Paul Rouquette is a master student following the engineering curses at the ENAC, the French university of civil aviation, Toulouse. He specialized in space telecommunication and more specifically in Aerospace Radio Frequency Engineering. His research interests are in GNSS receiver technologies, integrity control and signal processing.

Nathan Levigne is a MS graduate student in the Department of Aerospace Engineering Sciences at the University of Colorado Boulder. He received a B.S. in Aerospace Engineering from the University of Colorado Boulder. His research interests are in GNSS receiver technologies, software defined radio 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 Lule 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 Lule Technical University.

Yu-Hsuan Chen is a research associate at the Stanford GPS Laboratory. He received his Ph.D. in electrical engineering from National Cheng Kung University, Taiwan.



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.

Todd Walter received his B.S. in physics from Rensselaer Polytechnic Institute and his Ph.D. in 1993 from Stanford University. He is currently a senior research engineer at Stanford University. He is a cochair of the WAAS Integrity Performance Panel (WIPP) focused on the implementation of WAAS and the development of its later stages. Key contributions include early prototype development proving the feasibility of WAAS, significant contribution to MOPS design and validation, coediting of the Institute of Navigations book of papers about WAAS and its European and Japanese counterparts, and design of ionospheric algorithms for WAAS. He is the corecipient of the 2001 ION early achievement award, and he is a fellow of the ION.