Spoofing Detection for Airborne GNSS Equipment*

Christopher Hegarty, Ali Odeh, *The MITRE Corporation*
Karl Shallberg, Kyle Wesson, *Zeta Associates*
Todd Walter, *Stanford University*
Ken Alexander, *Federal Aviation Administration*

BIOGRAPHIES

Christopher Hegarty is a Technical Fellow with The MITRE Corporation, where he has worked mainly on aviation applications of GNSS since 1992. He received B.S. and M.S. degrees in electrical engineering from WPI and a D.Sc. degree in EE from GWU. He is currently the Chair of the Program Management Committee of RTCA, Inc., and co-chairs RTCA Special Committee 159 (GNSS). He is a Fellow of the ION and IEEE, and co-editor/co-author of the textbook *Understanding GPS/GNSS: Principles and Applications*, 3rd Ed.

Ali Odeh is a Senior Engineer at The MITRE Corporation. He received a B.S. and M.S. degree from North Carolina State University, both in electrical engineering. He has over 6 years' experience designing, developing, and analyzing digital signal processing algorithms for GPS receivers, GPS anti-jam systems and wireless communications systems.

Karl Shallberg is a Senior Associate with Zeta Associates Inc. and since 2013 has been the Project Lead for the Zeta FAA GNSS Program Support effort as well as the Project Lead for the Zeta Volpe PNT Spectrum Engineering effort. He has supported the FAA GNSS program on areas such as GPS receiver performance, interference assessments and system engineering issues since 1996. He previously was President of Grass Roots Enterprises Inc. and started his career with the US Government. He received his B.S. in physics from Norwich University.

Kyle Wesson works at Zeta Associates and supports the FAA's WAAS Program Office. He received his Ph.D. in electrical and computer engineering at the University of Texas at Austin in 2014 focusing on GPS security.

Todd Walter is a senior research engineer in the GPS Research Laboratory in the Department of Aeronautics and Astronautics at Stanford University. He received his Ph.D. from Stanford in 1993 and has worked extensively on the Wide Area Augmentation System (WAAS). He has received the Thurlow and Kepler awards from the Institute of Navigation (ION). In addition, he is a fellow of the ION and has served as its president.

Ken Alexander is the FAA Chief Scientist for Satellite Navigation Systems and Civil Co-chair of the National PNT Engineering Forum. Ken received his BS and MSEE from the University of Louisville and has over 40 years of aviation experience in aircraft and avionics development, systems engineering, flight test, flight operations and international cooperation. He has over 3500 flight hours as a USAF Transport Pilot. Ken also serves as the ICAO Navigation Systems Panel (NSP) member nominated by the U.S. and co-chairs the U.S. and European Union working group on GNSS Modernization.

ABSTRACT

Standards for the next-generation of civilian airborne GNSS equipment are now in development by RTCA and the European Organisation for Civil Aviation Equipment (EUROCAE). An initial version (for verification and validation) of Minimum Operational Performance Standards (MOPS) for dual-frequency multi-constellation (DFMC) GNSS airborne equipment is planned to be completed by 2020 and a final version by 2022. One objective for the next-generation airborne equipment is for improved resiliency in the presence of GNSS threats including spoofing. The current direction within RTCA and EUROCAE is for the threat of spoofing to be addressed primarily through the introduction of new requirements to detect the presence of

* The contents of this document reflect the views of the authors and do not necessarily reflect the views of the Federal Aviation Administration (FAA) or the Department of Transportation (DOT). Neither the FAA nor the DOT makes any warranty or guarantee, expressed or implied, concerning the content or accuracy of these views.

false GNSS signals within the airborne equipment so that so that an alternative means of navigation can be employed without a significant reduction in safety.

This paper postulates a set of minimum high-level spoofing detection requirements for airborne GNSS equipment and assesses various methods against these requirements. One objective of this paper is to identify a number of issues for spoofing detection that are unique to certified airborne equipment for the purpose of fostering research to address these issues.

INTRODUCTION

Standards for the next-generation of civilian airborne GNSS equipment are now in development by RTCA and the European Organisation for Civil Aviation Equipment (EUROCAE) [1]. An initial version (for verification and validation) of Minimum Operational Performance Standards (MOPS) for dual-frequency multi-constellation (DFMC) GNSS airborne equipment is planned to be completed by 2020 and a final version by 2022 [2]. One objective for the next-generation airborne equipment is improved resiliency in the presence of GNSS threats including spoofing. For instance, the RTCA Special Committee 159 (SC-159) Terms of Reference [2] states that the new standards will address spoofing "to the extent practicable". The current direction within RTCA and EUROCAE is for the threat of spoofing to be addressed primarily through the introduction of new requirements to detect the presence of false GNSS signals within the airborne equipment so that so that an alternative means of navigation can be employed without a significant reduction in safety.

This paper postulates a set of minimum high-level spoofing detection requirements for airborne GNSS equipment and assesses various methods against these requirements. The high-level requirements on spoofing detection include that: (1) the method will not prevent the equipment from meeting very stringent availability and continuity of service requirements established for each phase of flight when no spoofing threat is present, (2) the method will work for all equipment modes including single-frequency (L1-only or L5-only) reversionary modes, (3) the method will function satisfactorily in conditions regularly experienced in the airborne environment (e.g., nominal levels of interference, dynamics). For the first high-level requirement, an upper bound on an acceptable spoofing detection false alarm rate is derived. To help characterize some aspects of the airborne equipment environment, Zeta Associates has developed a GNSS signal data recorder and gathered digitized GNSS signal data onboard various Federal Aviation Administration (FAA) aircraft flights.

The paper describes the results of preliminary assessments of various spoofing detection methods that may be suitable for implementation within airborne GNSS receivers. Although numerous spoofing detection methods have been identified and assessed in previous research, the performance of these methods in the airborne operational environment is largely unknown. Although it is unlikely that RTCA or EUROCAE would require any specific method to be utilized in lieu of performance requirements, the establishment of such performance requirements will be greatly facilitated if there is at least one known method to achieve them. The preliminary assessments include consideration of the performance of each method in the anticipated operational environment as well as their "practicality".

SPOOFING DETECTION REQUIREMENTS

"Do No Harm"

Airborne equipment is most often expected to operate when a spoofing threat is not present. The inclusion of a spoofing detection capability must address concerns with potential false alerts, i.e., indications that the pseudoranges and/or position estimate may be unsafe to use in the absence of any signal corruption. Such false alerts are tolerable provided they are sufficiently rare so as to have negligible impact on pilot and controller workloads.

The International Civil Aviation Organization (ICAO) has established tolerable ranges of GNSS signal-in-space (SIS) continuity interruptions in [3] that depend upon the intended operation, traffic density, complexity of airspace and availability of alternative conventional navigation aids. The ICAO SIS continuity risk range is 10^{-4} per hour (for areas with low traffic density and airspace complexity) to 10^{-8} per hour (for areas with high traffic density/complexity) for operations utilizing GNSS for horizontal guidance. The continuity risk is 8×10^{-6} per 15 seconds for operations with vertical guidance, including Category I precision approaches, although [3] notes that a more stringent requirement may be appropriate in some circumstances (e.g., when the system failure may affect multiple aircraft such as for closely-spaced parallel runway operations).

The horizontal continuity risk values above translate to an average of 10,000 to 100 million hours between interruptions in service per aircraft and the vertical value to an average of approximately 500 hours between interruptions per aircraft. Because the specified discontinuity rates are evaluated on a per aircraft basis, any source of a false alert that could affect more than one aircraft at a time should be subject to an even smaller upper bound. That is, if a regional event could cause *N* aircraft to falsely declare that satellite navigation is unsafe, then that false alert mechanism should have a rate no greater than the ICAO values divided by *N*. As an example, sources such as thermal noise or local multipath typically only trigger an alert for one aircraft and therefore can use the full ICAO allocation. A source that could trigger simultaneous alerts for ten aircraft should be ten times less likely to do so.

The impact of an alert must also be better understood. In general, an alert can have varying degrees of impact, for example:

i) a reduction in the GNSS supported service level at the aircraft;
ii) a loss of all GNSS based guidance at the aircraft; or
iii) a loss of GNSS based guidance for a majority of aircraft within a sector or multiple sectors (with a subsequent investigation regarding the source of the alert).

Many threats to GNSS continuity do not harm all ranging sources. Many threats only somewhat degrade accuracy and therefore fall into the first category. However, the threat of spoofing (or failure to authenticate the signal source) creates an opportunity for an unbounded position error. It may not be possible to verify that the position solution is accurate to within even the loosest horizontal requirements. Therefore, such a false alert would fall into the second or third category. The horizontal continuity requirement should be maintained at all times since the loss of horizontal guidance could in some instances preclude missed approach guidance.

Given that there are approximately 25,000 scheduled commercial landings per day in the United States, an 8×10^{-6} per 15 seconds discontinuity rate would result in an average of two approach interruptions per day (assuming a 150 second approach segment, the least demanding GNSS SIS continuity risk, and one aircraft affected at a time). This number is small compared to the current total number of actual missed approaches that occur per day in the United States. It remains to be seen if such an increase would be acceptable or not. The perceived benefit of spoofing protection measures will be influenced by threat perceptions and real-world events. The 10^{-4} per hour discontinuity rate results in an average of 0.1 approach interruptions per day across the United States national airspace. There are approximately 50,000 commercial aircraft flight hours per day on average in the United States (~ 25,000 scheduled flights with an average duration about two hours). The 10^{-4} per hour discontinuity rate therefore would result in an average of total 5 GNSS flight interruptions per day. This may be an acceptable level provided that the occurrences are spread across locations and suitable backup navigation is available to preclude almost all operational diversions to an alternate airport.

As a starting point, the ICAO horizontal rate of 10^{-4} per hour is proposed as an upper bound on the acceptable false alert rate with the understanding that the specific number should be revisited as the false alert threats are better identified.

Detection Performance

Once it is established that a spoofing detection method yields an acceptable false alert rate in the absence of spoofing, the next category of requirements to be developed should address the performance of the method when spoofing is present. Very little progress has been made on this category of requirements to date for the next generation GNSS avionics for several reasons:

1. The threat space has not yet been agreed upon. The FAA has postulated a set of potential GNSS threats including four spoofing threats in [4]. These are identified in [4] as “unintentional reradiator”, “pinpoint spoofing attack”, “coordinated spoofing attack”, and “coordinated interference and spoofing attack”. The FAA has informed RTCA that the “unintentional reradiator” spoofing threat is currently viewed as the minimum threat space for future standards since it alone has been observed by civil aircraft to date (on several occasions, see, e.g., [4]). Additional threats to aviation are anticipated in the future, but the complete set of threats that needs to be mitigated will remain subjective until specific threats are observed by aircraft.
2. Achievable performance of a spoofing detection method against an agreed-upon set of threats within the airborne environment cannot be evaluated until the threat space is established.

For the purposes of this paper, “satisfactory” performance of a spoofing detection function is considered to the combination of an acceptably low false alert rate and a reasonable detection probability. The function should be worth the investment in the

subjective view of the aviation community including airspace users, civil aviation authorities, and air navigation service providers.

OPERATIONAL ENVIRONMENT

Airborne equipment is expected to reliably operate in environmental conditions that are described within this section. The information in this section was derived from two primary sources: (1) RTCA standards, and (2) a data collection effort that is described in the following subsection.

Flight Data Collection

To gather information on typical (vs specified worst-case) environmental conditions, a flight data collection package was developed by Zeta Associates and flown onboard FAA aircraft. Flight data collections were initiated to support spoofing mitigation efforts with the realization that gathering a repository of different flight conditions would be beneficial in testing individual and combined mitigation techniques. These flight collections were assisted with relatively frequent access to aircraft outfitted with L1/L5 capable GNSS antennas and a data collection capability that could be easily integrated on these aircraft. Flight access arrangements were made with the FAA flight inspection group in Oklahoma City, OK and the FAA test group in Atlantic City, NJ. The aircraft type at Oklahoma City was the Bombardier Challenger 605 and at the Atlantic City Technical Center was a Bombardier Global 5000. These aircraft were outfitted with ANTCOM G8Ant-743A4T1-A2 antennas which were top-mounted towards the front of the aircraft as would be expected for operational GNSS antenna installations. The Oklahoma City flight tests were generally regional flights at lower altitude and focused on approach procedure verification, and therefore, were generally of greater interest to the work pertaining to this paper. An example ground track from one such flight is shown in Figure 1. The numeric labels along the ground track are GPS seconds of week (SOW) divided by 1000. Receiver outputs for this flight for GPS L1 and L5 signals for pseudorange noise ranging code (PRN) 10, including C/N_0, pulse blanking duty cycle, automatic gain control (AGC) value, and time of continuous track are shown in Figure 2.

Figure 1. Flight Example from Oklahoma City, OK to Nashville TN

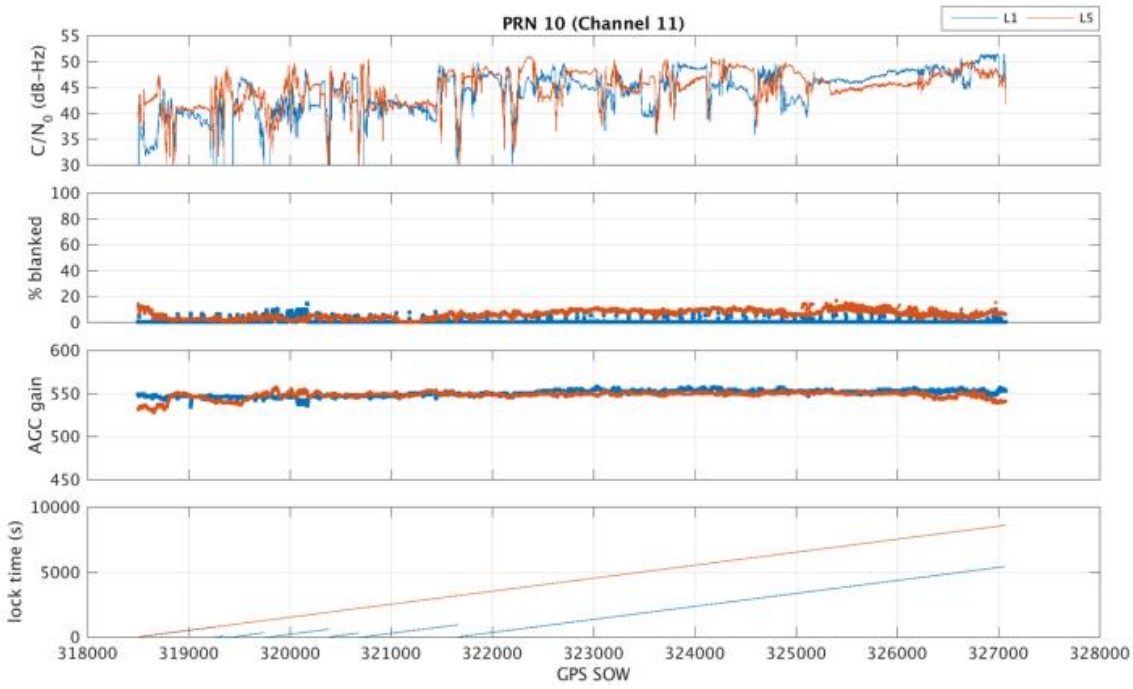

Figure 2. Airborne GPS Equipment L1 and L5 Data Outputs

The primary data collection for these flights was digitized L1 and L5 RF data from the GNSS antenna. The core component of this collection system is the ICEPOD-6.5, which is configured with two L-band digital tuners and high-speed I/O to write samples to the 3 TB solid state memory. RF data recording for these tests was configured for L1 and L5 with a 30 MHz span and 8-bit complex digitization. A more complete description of the collection system and its performance is provided in [5]. The important aspect for these data collections was the capability to replay the recorded data with fidelity comparable to the original signal reception. This capability supports replay of flight collections into multiple aviation receivers in a laboratory setting and offers the ability to augment the recorded data with the introduction of interference and other scenarios of interest such as replaying the recorded data on the same frequency while introducing different relative time delays and amplitudes.

Signal-to-noise Ratios

RTCA SC-159 is currently preparing updated L1 and L5 interference reports that will inform the normative interference environments for the future DFMC MOPS and associated antenna MOPS. Until these interference reports are completed, the current RTCA assessments of the L1 and L5 interference environments should be assumed. Per RTCA documents DO-235B [6] and DO-292 [7], the L1 interference environment is assumed to yield a carrier-to-noise density ratio, C/N_0, as low as 30 dB-Hz and L5 C/N_0 as low as 27 dB-Hz.

An example of typical C/N_0 values is provided in Figure 2. For both L1 C/A-code and L5, note that C/N_0 values vary significantly and can change rapidly ranging from above 50 dB-Hz to below 30 dB-Hz. Although some of these variations may be due to changing interference levels, they are influenced more by aircraft maneuvers as can be determined by comparing the C/N_0 plots with the time-tagged flight profile in Figure 1. Banking in particular can result in diminished antenna gain when the antenna is pointing away from a particular satellite or obstructed by aircraft surfaces (e.g., wings, tail).

Dynamics

Airborne GNSS receivers are typically specified to meet all performance requirements in the presence of ground speeds up to 800 kts, horizontal accelerations up to 0.58 g, vertical accelerations up to 0.5 g, and jerks up to 0.25 g/s [8]. These levels of dynamics are not much of a challenge for modern GNSS receivers. More challenging for some spoofing detection methods

(such as C/N_0 monitors) are the changes in attitude that civilian aircraft can undertake. Bank angles for commercial aircraft are typically less than 30 degrees for passenger comfort, but other types of aircraft may frequently bank beyond 30 degrees.

Multipath

The presence of multipath can make it more difficult to detect the presence of a spoofed GNSS signal, since both multipath and spoofing result in the presence of a second version of the desired GNSS signal. However, unlike a spoofed GNSS signal, a multipath signal always arrives after the desired signal and has a similar Doppler frequency. Multipath experienced by airborne GNSS equipment can arise from reflection sources on the aircraft (e.g., fuselage, wings, tail) or from the surrounding environment (ground, water, buildings, etc.). Short-delay multipath (i.e., echoes that arrive within ~1.5 microseconds of the direct GNSS signal) has been well-studied by the aviation GNSS community (see, e.g., [9 – 13]). The reason that this community has focused only on short-delay multipath, is that a GNSS receiver's pseudorange and carrier phase measurements are only perturbed by echoes of the desired signal that arrive within 1.5 chips (~1.5 microseconds for the GPS C/A-code) of the direct signal. For the above reasons, long delay multipath has been mostly ignored by the navigation community but is important for some spoofing detection methods (e.g., complex ambiguity function monitoring). Fortunately, long delay multipath is of great interest to the GNSS reflectometry community (see, e.g., [14 – 16]) and some well-known characteristics are discussed in the following.

Figure 3 shows the geometry underlying specular multipath for an aircraft in flight. From the geometry, the reflected signal path can be determined to be larger than the direct signal path by an amount given in meters by:

$$\Delta d = 2h\sin(\phi)$$

where ϕ is the elevation angle of the GNSS satellite and h is the height of the aircraft in meters above the reflecting surface. The multipath echo thus arrives later in time than the direct signal with a relative delay (in seconds) of:

$$\Delta\tau = \frac{2h}{c}\sin(\phi)$$

where c is the speed of light. Figure 4 shows the expected multipath delay vs aircraft height for several elevation angles.

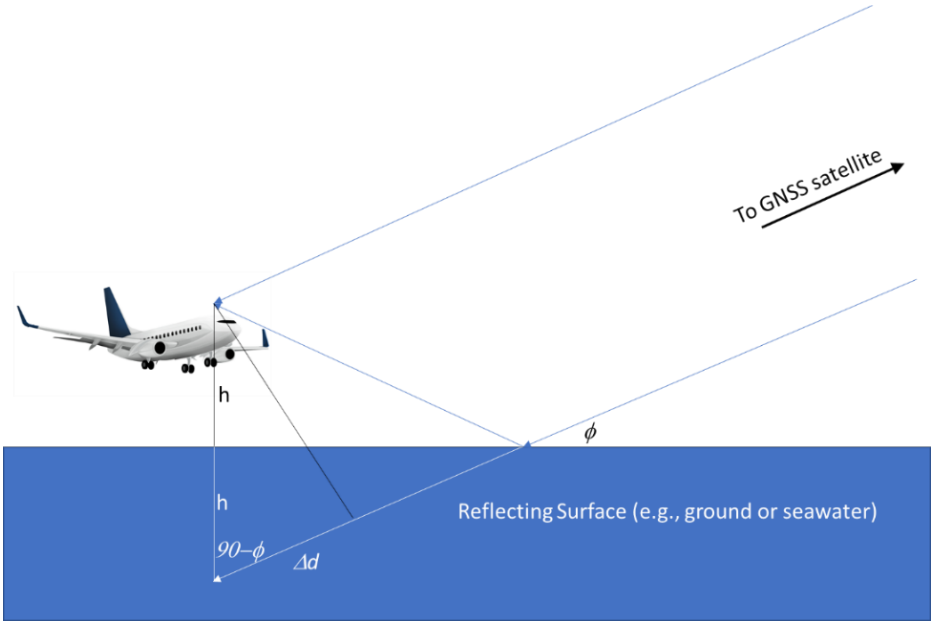

Figure 3. Airborne Specular Multipath Geometry

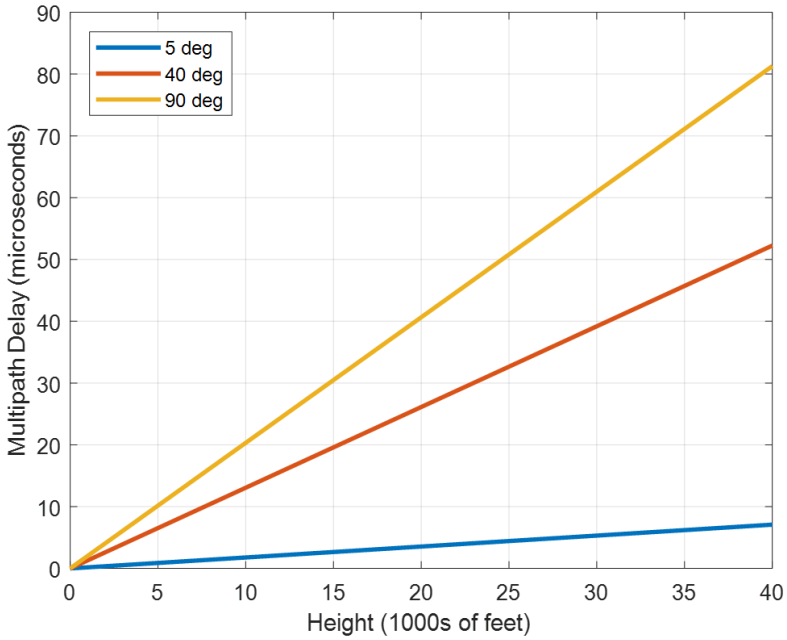

Figure 4. Multipath Delay vs Aircraft Height

The Doppler of the multipath signal relative to the direct is

$$\begin{aligned}\Delta f &= \frac{d}{dt}\left(\Delta d / \lambda\right) \\ &= \frac{2}{\lambda}\frac{d}{dt}\left(h\sin(\phi)\right) \\ &= \frac{2}{\lambda}\left[\frac{dh}{dt}\sin(\phi) + h\cos(\phi)\frac{d\phi}{dt}\right]\end{aligned}$$

The first term on the right-hand-side is due to the vertical velocity of the aircraft relative to the reflecting surface (either due to descent/ascent of the aircraft or rising/falling terrain). Aircraft climb/descent rates from 500 – 1500 fpm (2.5 – 7.5 m/s) are typical, but in some circumstances (e.g., descent in mountainous areas or in emergency) much higher values can be encountered. A 1500 fpm climb/descent rate over a flat surface would result in specular multipath with a relative Doppler frequency of less than 80 Hz at L1 and less than 60 Hz at L5. The largest magnitude of relative Dopplers correspond to high-elevation angle satellites, for which the echo amplitudes are typically smallest.

The amplitude of reflected signals can theoretically approach unity with respect to the direct signal for low-elevation angle satellites when the reflecting surface is flat. At low elevation angles, this characteristic is true for many types of material for the reflecting surface (e.g., seawater, concrete, earth). Although right-hand circularly polarized GNSS signals can become left-hand circularly polarized when they reflect from some surfaces in some conditions, for low-elevation angles this is not consequential for typical airborne antennas that are dominantly vertically polarized at the horizon. Typical reflected signal amplitudes diminish with increasing elevation angle and surface roughness.

To assess typical long-delay characteristics for airborne equipment, digitized received signal data at L1 from one low-altitude flight over sea water was processed. The flight was approximately 4 hours long and the aircraft never exceeded an altitude of around 8500 feet over its duration. Significant echoes were observed with relative delays up to 10 microseconds. In general, the observed delays of the echoes were consistent with Figure 4. The amplitude of the echoes was greatest for low-elevation angle satellites as shown in Figure 5, also consistent with expectations.

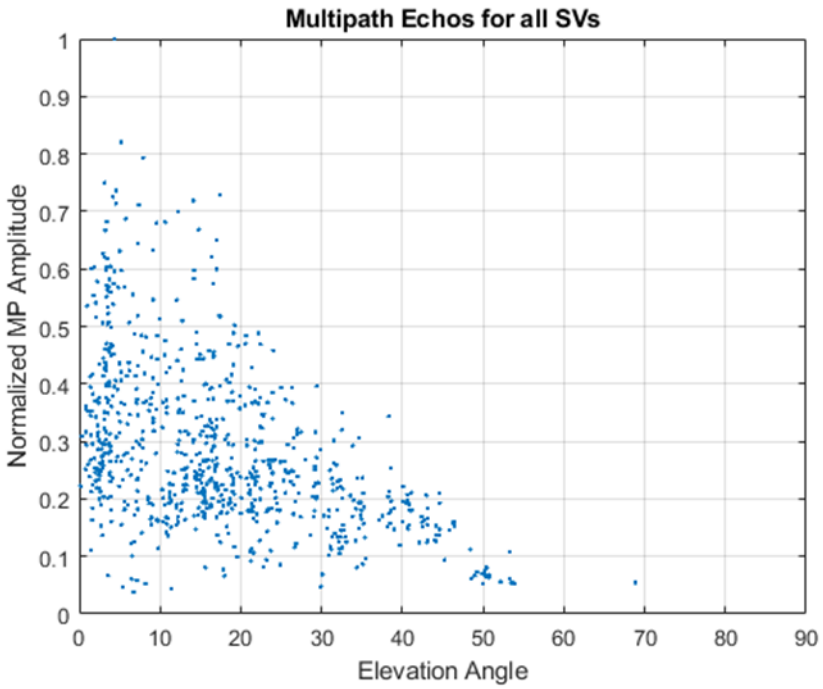

Figure 5. Estimated Multipath Amplitude vs Elevation Angle from Low-altitude Over-ocean Flight Data

Ionospheric Scintillation

Ionospheric scintillation can make spoofing detection more difficult in at least two important ways. First, it can result in rapid variations in received signal-to-noise levels, which complicates spoofing detection methods that rely on monitoring C/N_0. Second, there is an objective for future GNSS avionics standards to require that airborne equipment recover more quickly after losing lock on GNSS signals due to strong amplitude fades. This feature may make future equipment more susceptible to certain spoofing threats that can provide similar conditions.

Miscellaneous

Airborne equipment is required to work in extreme temperature, vibration, pressure and other conditions that are experienced by aircraft. These requirements are contained within portions of RTCA document DO-160 [17] that are invoked by GNSS airborne equipment MOPS. As just one example, an active airborne GNSS antenna on a typical commercial aircraft is required to work at temperatures ranging from -55° to +70° C and may experience the ambient temperature changing rapidly from extreme to the other. As discussed later in this paper, these environmental conditions provide challenges certain spoofing detection techniques such as automatic gain control (AGC) monitoring.

DETECTION METHODS

This section identifies and assesses various spoofing detection methods that may be suitable for implementation within airborne GNSS receivers. Although it is unlikely that RTCA or EUROCAE would require any specific method to be utilized in lieu of performance requirements, the establishment of such performance requirements will be greatly facilitated if there is at least one

known method to achieve them. The high-level assessments include consideration of the performance of each method in the anticipated operational environment as well as their "practicality". Practicality encompasses the following considerations:

- Size, weight, power, and cost.
- Can the method be expected to be provide some utility over the typical lifetime of airborne equipment, which historically can be 25 years or more?
- Is the method export-restricted, e.g., on the U.S. Munitions List (USML) and controlled by International Tariff in Arms Regulations (ITAR) or Export Administration Regulations (EAR) such as the Commerce Control List (CCL)?
- Are there intellectual property use concerns?

Importantly, the performance weaknesses of many of the methods discussed below when they are operating alone can be overcome through the concept of an *executive monitor*, i.e., logic within a GNSS receiver to declare the presence of spoofing based upon monitoring multiple conditions rather than just one. There are also the open issues of how best to alert pilots during operations, if at all, and what steps should be taken by the equipment/pilot after an alert/detection.

Automatic Gain Control (AGC)

Many GNSS receivers use AGC [18] to regulate the power in the signal that is digitized by the analog to digital converter. AGC monitoring has been identified by many researchers as a means to detect GNSS spoofing (see, e.g., [19]). This technique is very simple, but as will be illustrated below, cannot detect spoofed signals unless their received power levels are significantly greater than those of the authentic GNSS signals, which may not be representative of all threats.

In benign environments, AGC is driven mostly by thermal noise power within a GNSS receiver front end. For example, assuming that there are 10 visible GPS satellites with an average antenna gain of 0 dBic at maximum expected power levels (-153 dBW for C/A and -155 for P/Y), the signals produce approximately -143 dBW + (-145 dBW) = -140.9 dBW at the antenna port. In contrast, noise power referenced to the same point will be somewhere between -138.5 dBW and -125.5 dBW for the range of bandwidths (2–20 MHz) permitted within current RTCA MOPS. Thus, noise power dominates GNSS signal power. This inequality holds even for newer GPS satellites that are broadcasting M-code signals, or that will additionally broadcast the L1C signal.

Since noise power dominates GNSS signal power, spoofed signals can be present without reliable AGC detection when the received spoofing power is between the total GNSS power and the noise power. This limitation is exacerbated when the noise background includes man-made interference within the required operational envelope of the avionics as specified by the technical standard order (TSO) for modern avionics. This limitation is detailed below for the following two cases: signal generator C/A code spoofing and analog repeater spoofing.

Figure 6 shows the total received power (that drives the AGC) in the presence of true GPS signals (C/A, P/Y, M), spoofed GPS signals (C/A-code only) produced by a signal generator (assumed to be devoid of noise), and thermal noise. For the curves labeled with "I0," broadband interference at -200.5 dBW/Hz is also included. This interference level is the maximum external interference level for which certified GPS avionics need to continue to meet all applicable performance requirements.

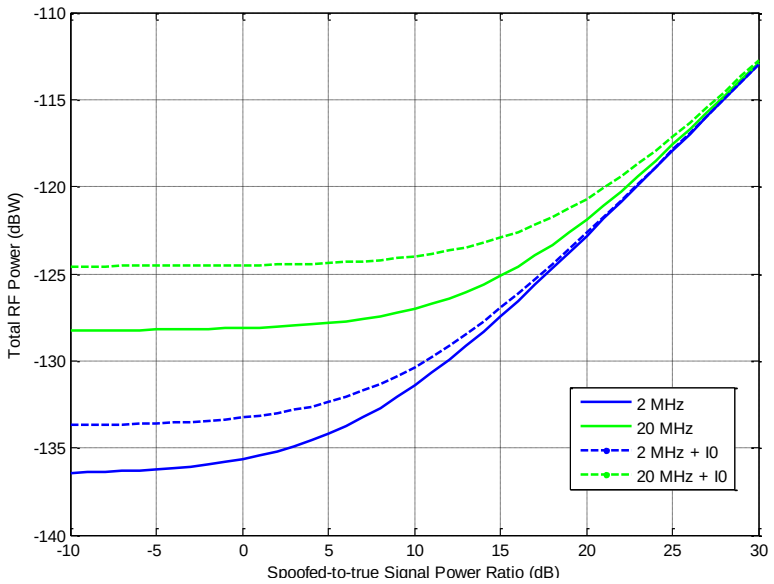

Figure 6. Impact on AGC of C/A-code Spoofing Produced by Signal Generator

The following observations are based on Figure 6:

- For either GPS receiver bandwidth examined, AGC values in the absence of spoofing can change by three to four dB for interference conditions ranging from no interference to maximum tolerable.
- Use of AGC to detect spoofing is easier for a narrowband receiver. In the absence of external interference, the presence of spoofed signals 0.6 dB stronger than the true signals will result in AGC gain decreasing by one dB. With maximum tolerable external interference, the presence of spoofed signals 3.4 dB stronger than the true signals will result in the same one-dB gain decrease.
- For a wideband receiver in the absence of external interference, the presence of spoofed signals 8.9 dB stronger than the true signals will result in AGC gain decreasing by one dB. With maximum tolerable external interference, the presence of spoofed signals 12.5 dB stronger than the true signals will result in the same one-dB gain decrease.
- Gain and other variations in the amplifiers prior to the AGC circuitry due to environmental conditions can lead to AGC gain variations even without any changes in the antenna output levels. For instance, most low noise amplifiers (LNAs) experience a decrease in gain (typically less than one dB over a 120ºC temperature swing) and increase in noise figure (typically on the order of one dB over 120ºC) with increasing temperature. Also, in the absence of interference or spoofing, aircraft attitude changes can result in significant variations in received GNSS signal levels and antenna (noise) temperature. These two factors can result in dB-level variations in AGC gain. For these reasons, one should use caution in setting thresholds for "abnormal" AGC variations.

Considering the above, it is likely that only spoofed C/A-code signals produced by a signal generator that are on the order of 20 dB stronger than the true GPS C/A-code signals could be robustly detected using AGC in a wideband receiver.

For an analog re-radiator (repeater) spoofer, the situation is different for two primary reasons:

1. The repeater will broadcast spoofed versions of all visible L1-band signals.
2. The repeater does not just broadcast the GNSS signals. Since the repeater uses the same type of front end as a GNSS receiver, within its front end the GNSS signals are buried by noise. So, the L1 repeater output is all visible L1 GNSS signals plus noise. If the repeater is assumed to use the exact same front end as the victim receiver, the ratio of received C/A-code signal power received from the spoofer to noise received from the spoofer will be approximately the same as the victim receiver's observed ratio of true C/A-code signal power to the victim receiver's noise floor.

Figure 7 shows the total RF power (that drives the AGC) in the presence of true GNSS L1 signals, repeater spoofed GNSS L1 signals, receiver noise, and spoofer broadcast noise. For the curves labeled with "I0," broadband interference at -200.5 dBW/Hz is also included. As compared with the signal generator spoofer (Figure 6) results, the repeater spoofer is slightly easier to detect using AGC because of the presence of noise in the spoofer transmitted signal. Still, it is likely that only repeater-spoofed C/A-code signals that are on the order of 15 dB stronger than the true GPS C/A-code signals could be robustly detected using AGC in a wideband receiver.

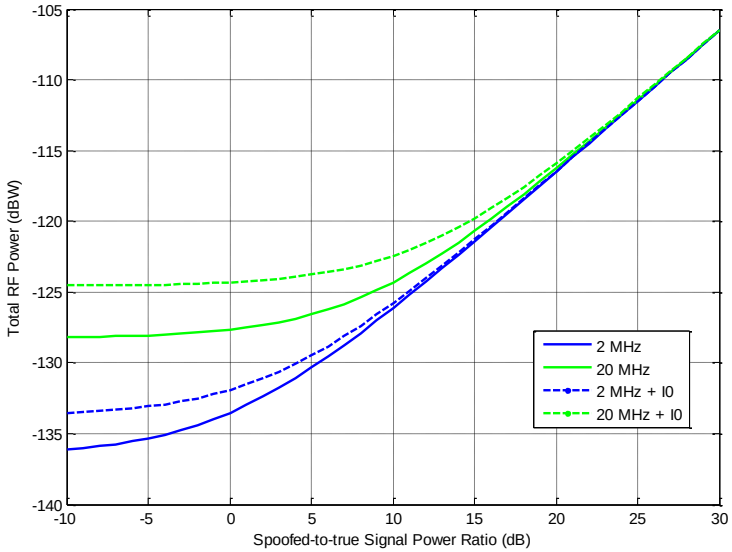

Figure 7. Impact on AGC of Repeater Spoofing

In summary, AGC detection of spoofing by itself will not be effective unless the spoofing signal(s) are 15 to 20 dB stronger than the received C/A-code signals. However, AGC detection may be among the easiest mitigations to implement. Moreover, the control of spoofing signal power is not simple for an aircraft attack. Thus, the AGC alternative retains value for detecting a spoofing attack that is high powered or does not have careful power control.

Signal-to-noise Monitoring

A signal-to-noise ratio (SNR) monitor could prove effective in the case where all of the spoofed signals exhibit an unusually high carrier-to-noise ratio (e.g., 55+ dB-Hz). In general, an SNR monitor on its own would have a steep challenge discerning between a spoofed signal and signal-to-noise ratio fluctuations, degradations, and outages that occur naturally due to the dynamics of aircraft flight (see, e.g., Figure 2). An executive monitor that utilizes both AGC and SNR inputs is described in [20].

Measurement, Navigation Data, and Position/Velocity/Time (PVT) Estimate Consistency Checks

Current-generation GNSS avionics (e.g., those meeting the requirements in [8]) employ several consistency checks on measurements, navigation data, and their PVT solutions. These include:

- Step detector – if a pseudorange measurement changes by more than 700 m over a measurement epoch, the receiver is required to exclude this measurement from the position solution.
- Receiver autonomous integrity monitoring (RAIM) – a well-known method to determine the consistency of the measurements in producing the position solution. New standards will include the evolution of RAIM methods for multiconstellation receivers, which is referred to as Advanced RAIM (ARAIM).
- Cross-check on satellite ephemeris and almanac data – included for current-generation equipment to preclude inadvertent tracking of the incorrect satellite due to the GPS C/A-code cross-correlation.

These checks were not designed to detect spoofing but could be reformulated for future standards to do so. Additional checks could also be implemented. Navigation data checks are recommended in [21, 22]. Examples of PVT consistency checks may be found in [21, 23]. A general limitation for consistency checks built into standalone GNSS receivers is that they can detect some but not all spoofing threats. For example, a GNSS receiver that is turned on just prior to departure on an aircraft that is from the onset captured by a reradiator may have all consistency checks pass even though it is being (perhaps unintentionally) spoofed.

Complex Ambiguity Function (CAF) Monitoring

Except for the most sophisticated spoofing attacks (those in which the spoofer generates a phase-aligned nulling signal that completely cancels out the authentic GNSS signal), the authentic signal remains present during a spoofing attack. At certain times during an attack, particularly when the powers between the authentic and spoofing signal are similar and the relative delay is short, their interaction causes distortions in the complex correlation function (or complex ambiguity function). These distortions can be readily monitored by receivers using the early/prompt/late correlators that drive the code tracking loops (and perhaps additional correlators as well). The largest obstacle to overcome in this approach is differentiating between spoofing and short-delay multipath since multipath causes distortions that are similar to spoofing. One approach to differentiate spoofing and short-delay multipath is documented in [24], which examines the correlation distortion coupled with a measurement of total in-band power.

Spoofed GNSS signals that vary significantly in either time-of-arrival or Doppler from true GNSS signals can be detected by monitoring the complex ambiguity function (CAF) for each desired signal. The CAF can be monitored either in serial or parallel in a similar fashion to the way that most GNSS receivers perform acquisition, i.e., by correlating the received signal against the product of a replica of the PRN code and a complex exponential with varied delay and frequency. Figure 8 depicts the CAF for C/A-code PRN 3 in the presence of a spoofer; two peaks are clearly visible in the CAF.

CAF monitoring has several limitations:

- As discussed above, it is difficult to detect a spoofed signal that has a time-of-arrival and Doppler close to the true signal. In that case, it appears that the CAF only has one peak as would be expected in the absence of spoofing.
- Long-delay multipath can be confused with a spoofed signal since they can both result in two discernable peaks in the CAF. Importantly, a long-delay multipath CAF peak will always be later than the peak for the true signal, and for airborne equipment, there are only certain relative delays, relative Dopplers, and relative amplitudes that are expected for long-delay multipath (discussed earlier in this paper).
- The true signal peak in the CAF can be obscured if the spoofed signal includes strong noise. This occurs naturally for reradiated GNSS signals. This condition could be detected using an executive monitor that uses both CAF and AGC data as inputs.

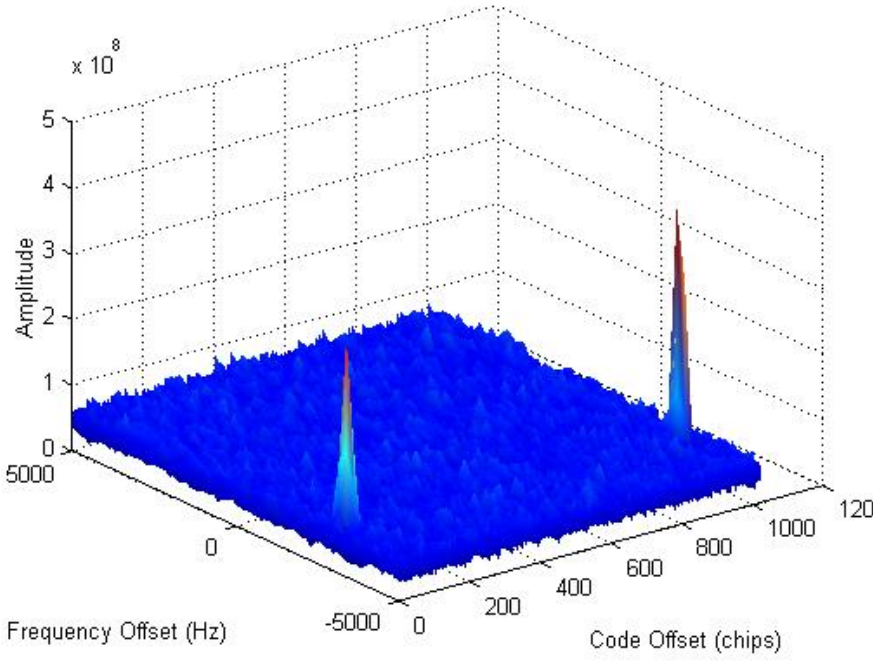

Figure 8. CAF for C/A-code PRN 3 in the Presence of Spoofing

Cryptography

The addition of cryptographic features to GNSS signal navigation messages or spreading codes can be used as a mitigation against spoofing threats. One promising cryptographic method is navigation message authentication (NMA), which has been considered for GNSS signals since at least 1994 [25]. NMA involves incorporating digital signatures into the broadcast navigation data [25 – 31]. These signatures allow the user to determine whether the data bits were generated by the expected source. The signature is generated through use of a secure private key that only the GNSS service provider has controlled access to. The signature is a function of the broadcast data and this private key. The user is provided access to a public key that is associated with the private one and they also receive the regular broadcast navigation data. The public key is used to determine whether or not the signature was created by the private key (without using or revealing the contents of the private key). This process allows the user to determine whether or not the navigation data that they are receiving was generated by the GNSS service provider. Therefore, an attacker would be unable to fool the user with a spoofed signal containing arbitrary navigation data, as they would be unable to create valid signatures without access to the private key. However, a spoofer could listen to the true signal and repeat the true navigation data including the valid signatures. Thus, they would not be able to trick the user into calculating erroneous satellite clock and orbital locations, but the threat remains for erroneous user position and/or clock estimates introduced by varying the amount of delay on each satellite signal. This delayed threat attack could be prevented if the user had access to very precise time, independent of GNSS. However, to be effective, this alternate timing source would need to be accurate to on the order of microseconds. One potential is to leverage a highly stable onboard oscillator.

The user algorithm needs to invalidate its position output (or at least the navigation data) whenever the signatures fail to confirm the navigation data. In addition to spoofing, such failures could be caused by message loss (e.g., similar to those that would cause loss of parity) or inability to obtain and validate the current public key. The NMA algorithm must be designed to have tolerance against message loss and the key distribution method must be extremely reliable. NMA also needs to support a Time-To-Alert (TTA) that may be as short as six seconds, but ultimately depends on how long it is tolerable to have a spoofed signal present at the receiver input before the position output can be intolerably corrupted. The time between signature messages will have to be no longer than this required TTA. Unfortunately, the TTA requirement and the continuity requirement compete against each other and it will be challenging to meet both.

The paired private and public keys need to be periodically updated in order to ensure security. Therefore, there must be a process to get public key updates to the user in a way that they can be certain that it originated form the GNSS provider. This rekeying process may be performed over the air with another set of messages or through a side channel such as from a secure website [31]. The processes for generating and confirming digital signatures require non-trivial computational effort compared to the other receiver processes. Further, some cryptographic techniques are potentially vulnerable to future advances in quantum computing. There is a risk that the currently standardized authentication algorithms will become vulnerable to attack within the next twenty to thirty years. Best cryptographic practices allow for updating or replacing the signature scheme on timescales much shorter than the expected thirty-year aviation receiver lifecycle.

Authentication offers powerful protection against independently created counterfeit signals. However, it cannot protect against all spoofing threats. Repeated/delayed GNSS signals carrying the true navigation data can still be used to spoof the user's position while passing the authentication checks if NMA is used alone. The spoofing threats need to be evaluated, along with the performance of the other spoof-detection algorithms, to understand where authentication fits into the complete package of mitigations.

As noted above, NMA provides *data authentication*, i.e., unless the keys or algorithm have been compromised it assures the receiver that the navigation data bits originated with the GNSS service provider and that no other party altered the bits between generation and reception. *Timing authentication* is more challenging and is intended to permit the receiver to confidently estimate or assess that the time of transmission of the navigation signal has not been delayed or altered by forces other than those that are expected (e.g., time of flight, receiver processing time). Proposals to provide timing authentication through embedded features in the spreading codes of GNSS signals may be found in [26, 29]. Although promising, these proposals have some challenges:

- Altering the spreading codes for established satellite navigation systems will likely take considerable time. For instance, for GPS the most likely injection point would be for the 11th GPS III satellite that is anticipated to be available for launch no earlier than 2025.
- They require increased user equipment complexity.
- Further work is necessary to verify their utility for airborne equipment that needs to operate in the environmental conditions described earlier in this paper.

For civil users relying on unencrypted navigation signals, there is a broad consensus that the following guidelines apply:

- Any technique should not harm legacy users (e.g., no changes to the L1 C/A signal).
- Any technique must rely on public-key cryptographic techniques such as digital signatures since private-key management makes private-key cryptographic techniques infeasible for civil aviation.
- Cryptographic schemes must be as bit-efficient as possible, meaning that any solution cannot take up more of the broadcast message than necessary. Since many navigation messages have low data rates (50 bps) or small message sizes (250 bits), digital signature techniques like elliptic curve cryptography, the Schnorr algorithm, or variants of the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol are generally proposed.
- More frequent digital signatures of new/updated navigation data offer more security, since the receiver can more often deduce if the received signal is authentic (both in time and data).
- Whatever technique is implemented, it should be secure for the next 25 years or longer, or updateable, to support the long lifetime of aviation products and receivers. As computing power increases, longer key lengths are necessary to offer the same level of protection. In addition, cryptographic techniques that are thought to be secure today may fail against future cryptographic attacks based on quantum security. Schemes that allow for longer digital signatures or updatable signature algorithms should be favored.
- The intellectual property landscape needs to be favorable for receiver manufacturers to implement.

For GNSS, the most practical and effective approaches for incorporating NMA either through an elliptic curve technique or through a TESLA variant [27, 28]. In either case, new navigation message types would need to be defined and broadcast at a set repetition interval that provide the digital signatures. Public keys are offered over the air as well and are updated at a rate consistent with the presumed threat to deduce a key. Some techniques are amenable to future updates that could change the signature should a current cryptographic method be shown to be quantum resistant.

When considering specific authentication techniques for satellite-based augmentation systems (SBAS) including the FAA's Wide Area Augmentation System (WAAS), additional considerations apply:

- The technique needs to maintain the WAAS 10E-3 word error rate (WER).
- The technique needs to meet link budget assumptions for the 5° elevation user specified in the MOPS.
- The technique should incorporate protections for both the L1-only, L5 only, and L1+L5 user.
- The technique needs to be able to me DO-178 Level B software requirements in the Ground Uplink Station (GUS) safety computers.
- Key updates need to be scheduled ahead of time so that aircraft do not lose the ability to authenticate during flight.
- Key management needs to be internationally coordinated and secure.

Candidate architectures for SBAS include an inphase-only and an inphase/quadrature approach. The inphase/quadrature approach is illustrated in Figure 9. As an exemplar of this approach, the inphase power of an SBAS signal be reduced by as little as 1/5 (1 dB) and converted to quadrature power. This would support an elliptic curve digital signature technique based on a 256-bit key based on the following assumptions for L5:

- L5 minimum EIRP: +32.1 dBW
- Received signal strength at 5° elevation user: -157.0 dBW
- Noise: -200 dBW/Hz
- FEC enabled with soft Viterbi decoding (+5.5 dB coding gain)
- $E_b/N_0 > 10$ dB for WER 10E-3
- Inphase data rate of 250 bps (500 sps) and quadrature data rate of 512 bps (1024 sps)

To meet the more constrained link budget requirements for L1, some of these parameters would need to change (or an entirely different approach would be needed for L1 such as TESLA). Possibilities include: modifying the power split (increase EIRP), reducing the symbol rate on quadrature, reducing the symmetric key strength, and/or modifying the FEC type and parameters.

Despite their cryptographic features, NMA techniques can still fall victim to a reradiator or simple replay type attack unless additional measures are used. NMA is not a panacea but can provide a useful layer of security.

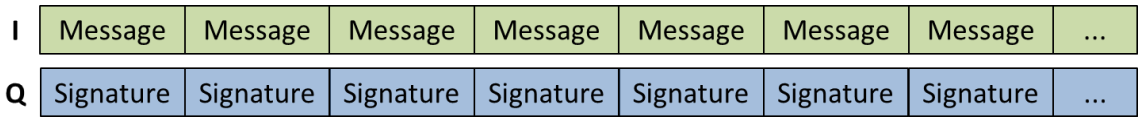

Figure 9. Example Inphase/Quadrature WAAS Broadcast with Digital Signatures.

Crosschecks with Other Navigation Sensors

Aircraft equipped for navigation in instrument meteorological conditions typically carry many other navigation sensors. These can include equipment for distance measuring equipment (DME), very high frequency omnirange (VOR), baro-altimeters, radio-altimeters, air data inertial reference units (ADIRUs), marker beacons, magnetometers, non-directional beacons, and instrument landing system (ILS). Cross-checks of GNSS equipment with these other sensors, e.g., within a flight management system (FMS), can be used to detect spoofing (see, e.g., [21, 32]). A general limitation is that only GNSS position errors that exceed the accuracy of the other sensors can be reliably detected.

Antenna Techniques

Adaptive antennas can be used to both detect and mitigate spoofing (see, e.g., [21, 33]), but unfortunately are severely export restricted within the United States. After being updated in 2016, the U.S. Munitions List (USML) continues to include most adaptive GNSS antennas [34]. Specifically, Category XII (Fire Control, Laser, Imaging, and Guidance and Control Equipment) includes "GNSS receiving equipment specifically designed for use with an antenna described in Category XI(c)(10)" and "GNSS anti-jam systems specifically designed for use with an antenna described in Category XI(c)(10)". Category XI ("Military Electronics")(c)(10) reads:

> (c)(10) Antenna, and specially designed parts and components thereof, that:
> (i) Employ four or more elements, electronically steer angular beams, independently steer angular nulls, create angular nulls with a null depth greater than 20dB, and achieve a beam switching speed faster than 50 milliseconds;
> (ii) Form adaptive null attenuation greater than 35 dB with convergence time less than 1 second;
> (iii) Detect signals across multiple RF bands with matched left hand and right hand spiral antenna elements for determination of signal polarization;
> (iv) Determine signal angle of arrival less than two degrees (e.g., interferometer antenna)

Other countries have export controls on GNSS adaptive antennas that are less restrictive than in the United States. For instance, Canada and the European Union have export controls on GNSS adaptive antennas, but both of these entities do not control such "equipment designed for commercial, civil, or 'Safety of Life' (e.g., data integrity, flight safety) GNSS services."

Use of dual antennas is a promising method for spoofing detection. Many commercial and general aviation aircraft are equipped with two GNSS antennas for reliability with typical separations from 20 cm to 1 m. As an example, Figure 10 shows a JetBlue Airbus A320. Two ARINC-743 form-factor GPS antennas (approximately $12 \times 7.5 \times 1.9$ cm^3) are visible atop the fuselage just behind the cockpit and fore of a VHF blade antenna. Robust methods of detecting spoofing using dual antennas have been demonstrated, for instance in [35] using the standard outputs of independently operating commercial receivers.

A single antenna with dual-polarization feeds is proposed in [36] for spoof detection and mitigation of jamming. This proposal offers similar benefits to low-end adaptive antennas but with reduced size and without the export control constraint. One drawback is that it requires a non-standard interface with the receiver.

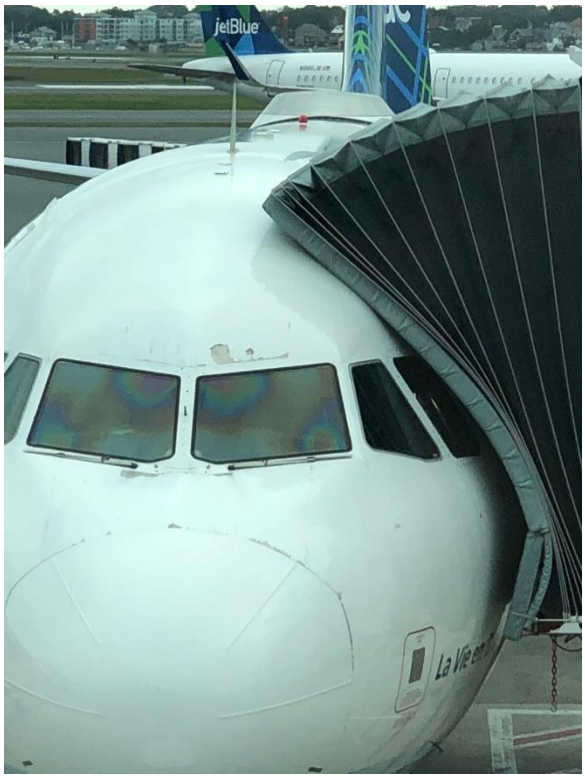

Figure 10. Airbus A320 with Two GPS Antennas Visible atop Fuselage

OPEN ISSUES

There are many open issues regarding spoofing detection for airborne equipment, and this topic is a fertile area for future research. Some of the more challenging open issues are identified in the subsequent subsections.

Threat Space

As discussed above, the FAA has postulated that the unintentional reradiator is the minimum threat to consider in developing standards for next-generation airborne equipment but additional threats may be added to the threat space if they are observed by civil aviation. What spoofing threats should be included in the DFMC MOPS that is scheduled to be published in 2020/2022?

Persistence in Rejecting Measurements

Current-generation GNSS airborne equipment includes consistency checks including RAIM and a pseudorange step detector. These checks can in some circumstances prevent spoofed satellites from being incorporated in the position solution, especially during partial capture (i.e., the condition where only some tracking loops are locked onto the spoofed rather than true GNSS signals). However, currently fielded equipment will reincorporate the measurements when RAIM indicates that the position solution is consistent. A consistent set of measurements is often what is observed when a receiver is completely captured by a spoofer. What philosophy should be used for next-generation equipment regarding persistence of rejecting measurements? There is a tradeoff between allowing some spoofing attacks to succeed vs the desire for a quick recovery due to some other receiver failure conditions.

Indeed, several ground-based tests on unmanned aerial vehicles demonstrated that RAIM had limited effectiveness against a spoofing attack especially in times when the spoofed signals were more plentiful and exhibited a higher C/N_0 when compared to the authentic signals. In such cases, the RAIM technique could flag all of the authentic signals as being anomalous while keeping the spoofed signals.

Requirement Specification

Aviation organizations including RTCA typically favor performance-based standards rather than prescriptive standards. For spoofing detection, the likely objective will be for the standard to require an acceptably low false-alarm rate and a reasonable detection probability in the presence of spoofing without prescribing a specific detection technique. This presents challenges related to the "Threat Space" open issue above. How should the detection requirement be specified in a testable manner? One possible solution includes specifying one or more test conditions, i.e., the use of a signal generator that produces a mixture of "true" and "spoofed" signals with prescribed power levels, Dopplers, and delays and requiring that the airborne equipment provide an alert within a specified time period. An alternative solution would be to actually provide synthesized recordings of spoofing threats.

It is also possible that spoofing detection requirements may involve a mix of performance-based and prescriptive requirements. For instance, a pseudorange step detector and RAIM are already required in current-generation standards (e.g., [8]). Reformulated monitors (ARAIM and step detectors) will likely be included in the DFMC MOPS and can be designed to be more effective at detecting spoofing.

Another open issue regarding requirement specification is what is the desired receiver behavior when spoofing is detected? Some engineers have recommended providing a visual and/or audible alert to the pilot. Human factors experts favor not doing so to avoid causing confusion in the cockpit. A spoofing detection alert should result in the GNSS sensor position output being discontinued and possibly an output flag to be sent via a communications path to the air navigation service provider.

One final open issue in this category is whether spoofing detection/alerting is sufficient or whether there should be requirements for equipment to "operate through". While spoofing mitigation includes the process of first detecting and alerting the pilot to an attack, it is not clear that spoofing mitigation is a reasonable goal during flight for several reasons. First, mitigation techniques may be more expensive, both monetarily and computationally, than detection techniques. Second, there are many backups to GNSS for aircraft navigation such as DME or magnetic compass (with air traffic control heading vectors) that the pilot can quickly switch to once notified of a spoofing attack. Third, the wide-variety of receiver manufacturers, equipment, and airframes suggest that there would be no one-size fits all mitigation solutions.

Navigation Message Authentication

Navigation message authentication offers some practical benefits but also needs a through cost-benefit analysis prior to civil aviation endorsement or adoption. Open issues include:

- What is the key management and distribution platform? How will this fit into civil aviation flight operations?
- What will be the cost to pilots, receiver vendors, and aircraft manufacturers?
- How will the system update and remain secure for 25+ years?
- What is the intellectual property landscape nationally as well as internationally?
- What is the threat of quantum computing and does a technique need to be quantum secure prior to implementation? If not, is there a potential alternative cryptographic technique that could take its place if the current implementation is broken or too weak to defeat future countermeasures?
- Can quadrature L1 and L5 SBAS channels be implemented given the tight L1 C/A-code C/N_0 budget [6] and constraints on aggregated GNSS signal power flux density in the 1164 – 1215 MHz band to protect DME [38]?
- Does NMA meet the "do no harm" requirement?

Future Direction of U.S. Export Control Laws

It is unclear how tightly adaptive GNSS antennas will be export controlled in the United States in the future as applicable regulations are updated. In addition to their utility to detect and mitigate GNSS spoofing, such technology is necessary to support myriad other civilian commercial applications including: 5G cellular, vehicular collision control radars, and advanced weather radars where their use continues to become commonplace and the applications have eclipsed potential enforcement actions. Various entities have provided inputs to the Department of State to consider removing or at least modifying the XI(c)(10) paragraph described above from the USML [39].

SUMMARY

This paper has postulated a set of minimum high-level spoofing detection requirements for airborne GNSS equipment: (1) the method will not prevent the equipment from meeting very stringent availability and continuity of service requirements established for each phase of flight when no spoofing threat is present, (2) the method will work for all equipment modes including single-frequency (L1-only or L5-only) reversionary modes, (3) the method will function satisfactorily in conditions regularly experienced in the airborne environment. A 10^{-4} per hour upper bound on spoof detection false alert rate has been derived for the first high-level requirement. For the third requirement, the paper provided an overview of worst-case specified and typical environmental conditions.

The paper has also described the results of preliminary assessments of various spoofing detection methods that may be suitable for implementation within airborne GNSS receivers. Open issues have also been identified that require closure before next-generation airborne equipment can be finalized.

ACKNOWLEDGMENTS

The authors would like to thank Barbara Clark, FAA, for her contribution towards developing the continuity requirement proposed in this paper.

REFERENCES

1. Hegarty, Christopher J., Ligler, George T., Alexander, Ken, Chesto, Larry, Moses, Harol, Wichgers, Joel M., Enge, Per, Erlandson, Bob, Van Dierendonck, A.J., Azoulai, Laurent, Kalyanaraman, Sai, Heppe, Steve, Lee, Young C., Wesson, Kyle, Studenny, John, "RTCA SC-159: 30 Years of Aviation GPS Standards," *Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, Tampa, Florida, September 2015, pp. 877-896.
2. https://www.rtca.org/sites/default/files/sc-159_june_2018_tor.pdf
3. ICAO, *Annex 10 to the Convention on International Civil Aviation*, Amendment 91, International Civil Aviation Organization, Montreal, Canada, applicable November 2018.
4. Alexander, K., and D. Lawrence, "GNSS Intentional Interference and Spoofing," presentation to RTCA Special Committee 159, Washington, D.C., October 2015.
5. Shallberg, K., J. Flake, D. Baraban, and C. Hegarty, "Updated Aviation Assessment of Interference in the L5/E5A Bands from Distance Measuring Equipment," *Proceedings of ION GNSS+ 2018*, Miami, FL, September 2018.
6. SC-159, *Assessment of Radio Frequency Interference Relevant to the GPS L1 Frequency Band*, DO-235B, RTCA, Inc., Washington, D.C., March 2008.
7. SC-159, *Assessment of Radio Frequency Interference Relevant to the GNSS L5/E5a Frequency Band*, DO-292, RTCA, Inc., Washington, D.C., July 2004.
8. SC-159, *MOPS for GPS/Wide Area Augmentation System (WAAS) Airborne Equipment*, DO-229E, RTCA, Inc., Washington, D.C., December 2016.
9. Murphy, Tim, Snow, Robert, Braasch, Michael, "GPS Multipath on Large Commercial Air Transport Airframes", *NAVIGATION, Journal of The Institute of Navigation*, Vol. 43, No. 4, Winter 1996-1997, pp. 397-406.
10. Murphy, Tim, Harris, Matt, Booth, Janet, Geren, Preston, Pankaskie, Tom, Clark, Barbara, Burns, Jason, Urda, Ted, "Results from the Program for the Investigation of Airborne Multipath Errors," *Proceedings of the 2005 National Technical Meeting of The Institute of Navigation*, San Diego, CA, January 2005, pp. 153-169.
11. Murphy, Tim, Harris, Matt, Geren, Preston, Pankaskie, Tom, Clark, Barbara, Burns, Jason, "More Results from the Investigation of Airborne Multipath Errors," *Proceedings of ION GNSS 2005*, Long Beach, CA, September 2005, pp. 2670-2687
12. Steingass, Alexander, Lehner, Andreas, Pérez-Fontán, Fernando, Kubista, Erwin, Martín, Maria Jesús, Arbesser-Rastburg, Bertram, "The High Resolution Aeronautical Multipath Navigation Channel," *Proceedings of the 2004 National Technical Meeting of The Institute of Navigation*, San Diego, CA, January 2004, pp. 793-804.
13. Amielh, Capucine, Chabory, Alexandre, Macabiau, Christophe, Azoulai, Laurent, "Validation of Existing GNSS Multipath Model," *Proceedings of ION GNSS+ 2017*, Portland, Oregon, September 2017, pp. 1772-1789.
14. K.M. Larson, E.E. Small, J.J. Braun, and V.U. Zavorotny "Environmental Sensing: A Revolution in GNSS Applications," *Inside GNSS*, Vol. 9, No. 4, July/August 2014, pp. 36–46.

15. V. U. Zavorotny and A. G. Voronovich, “Scattering of GPS signals from the ocean with wind remote sensing application,” *IEEE Transactions on Geoscience and.Remote Sensing*, vol. 35, no. 3, pp. 951–964, Mar. 2000.
16. Lin, B., S. Katzberg, J. Garrison, and B. Wielicki, “Relationship between GPS signals reflected from sea surfaces and surface winds: Modeling results and comparisons with aircraft measurements,” *Journal of Geophysical Research*, Vol. 104, No. C9, September 15, 1999.
17. SC-135, *Environmental Conditions and Test Procedures for Airborne Equipment*, DO-160G, RTCA, Inc., December 2010.
18. Van Dierendonck, A.J., “GPS Receivers,” in *Global Positioning System: Theory and Applications*, B. Parkinson and J.J. Spilker, Eds., American Institute of Aeronautics and Astronautics, Washington, D.C., 1996.
19. 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.
20. Manfredini, Esteban Garbin, Akos, Dennis M., Chen, Yu-Hsuan, Lo, Sherman, Walter, Todd, Enge, Per, "Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers," *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, Reston, Virginia, January 2018, pp. 672-689.
21. Günther, Christoph, "A Survey of Spoofing and Counter-Measures", *NAVIGATION, Journal of The Institute of Navigation*, Vol. 61, No. 3, Fall 2014, pp. 159-177.
22. DHS, Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure, January 2017. https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf
23. Chu, Fengkui, Li, Hong, Lu, Mingquan, "A GNSS Spoofing Detection Method Based on the Consistency of Measured and Calculated Carrier Dopplers," *Proceedings of the ION 2017 Pacific PNT Meeting*, Honolulu, Hawaii, May 2017, pp. 832-841.
24. Wesson, K., J. Gross, T. Humphreys, and B. Evans, “GNSS Signal Authentication Via Power and Distortion Monitoring,” *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 54, No. 2, April 2018.
25. Enge, P., and M. Hellman, “Authenticating the WAAS Message,” presentation to FAA, October 31, 1994.
26. Scott, L., "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," *Proceedings of ION GPS/GNSS 2003*, Portland, OR, September 2003, pp. 1543-1552.
27. Kerns, A.J., Wesson, K.D., Humphreys, T.E., "A Blueprint for Civil GPS Navigation Message Authentication," *Proceedings of IEEE/ION PLANS 2014*, Monterey, CA, May 2014, pp. 262-269.
28. Fernández-Hernández, Ignacio, Rijmen, Vincent, Seco-Granados, Gonzalo, Simon, Javier, Rodríguez, Irma, Calle, J. David, "A Navigation Message Authentication Proposal for the Galileo Open Service", *NAVIGATION, Journal of The Institute of Navigation*, Vol. 63, No. 1, Spring 2016, pp. 85-102.
29. Anderson, Jon M., Carroll, Katherine L., DeVilbiss, Nathan P., Gillis, James T., Hinks, Joanna C., O’Hanlon, Brady W., Rushanan, Joseph J., Scott, Logan, Yazdi, Renee A., "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," *Proceedings of ION GNSS+ 2017*, Portland, Oregon, September 2017, pp. 2388-2416.
30. Neish, Andrew, Walter, Todd, Enge, Per, "Quantum Resistant Authentication Algorithms for Satellite-Based Augmentation Systems," *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, Reston, Virginia, January 2018, pp. 365-379.
31. Cogdell, K., and P. Reddan, “Australia/New Zealand DFMC SBAS Navigation Message Authentication,” *Proceedings of ION GNSS+ 2018*, Miami, FL, September 2018.
32. Tanil, C., S. Khanafseh, M. Joerger, and B. Pervan, “An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position,” *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 54, No. 1, February 2018.
33. Daneshmand, Saeed, Jafarnia-Jahromi, Ali, Broumandon, Ali, Lachapelle, Gérard, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 2012, pp. 1233-1243.
34. Department of State, “Amendment to the International Traffic in Arms Regulations: Revision of U.S. Munitions List Category XII,” *Federal Register*, Vol. 81, No. 197, October 12, 2016.
35. Borio, Daniele, Gioia, Ciro, "A Dual-antenna Spoofing Detection System Using GNSS Commercial Receivers," Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015), Tampa, Florida, September 2015, pp. 325-330.
36. McMilin, E., *Single Antenna Null-steering for GPS & GNSS Aerial Applications*, PhD Dissertation, Stanford University, March 2016.
37. https://www.itu.int/ITU-R/go/space-resolution609/en
38. https://www.pmddtc.state.gov/sys_attachment.do?sys_id=9ea00fe3dba653003b1272131f961917