Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)

DENNIS M. AKOS
University of Colorado

Received March 2012; Revised August 2012

ABSTRACT: *The idea of Global Positioning System (GPS)/Global Navigation Satellite System (GNSS) "spoofing," or the ability to mislead a satellite navigation receiver into establishing a position or time fix which is incorrect, has been gaining attention as spoofing has become more sophisticated. Various techniques have been proposed to enable detection if a receiver is being spoofed – with varying degrees of success and computational complexity. In this paper, a monitor in the Radio Frequency (RF) front end using the automatic gain control (AGC) mechanism is outlined. It has low computational complexity and is an extremely powerful means to detect spoofing, making spoofing no more of a threat than the much less sophisticated radio frequency interference/jamming. The technique is validated using live testing. Copyright © 2012 Institute of Navigation.*

INTRODUCTION

The output of a satellite navigation receiver is often considered truth for both time and position information. However, it is possible to trick such a receiver into outputting false estimates of time and position. This is the problem addressed herein. The consequences are obvious but also quite dire for vehicle navigation as well as reference stations. The discussion within this paper will focus on the GPS L1 frequency, although it can be extended to all satellite navigation signals and systems.

The most simplistic approach to trick a receiver into a false position/time solution is using a GPS repeater, known as meaconing. These devices typically leverage an outdoor antenna, pass that reception signal through a cable, and then into an amplifier and transmission antenna at the same frequency as GPS. Receivers in close proximity to this transmission antenna receive this stronger broadcast and decode the position of the original reception antenna rather than their own position. Such a technique is effective, and can be productive, in initializing a GPS receiver which is denied an open sky view, but the operational scenario demands immediate signal tracking once the receiver is given access to sky view (such as a parachute about to exit an aircraft). However, these can be misused, as was the case when a GPS repeater was utilized in an airport hangar to enable technicians to test equipment indoors – the high repeater power caused aircraft on the runway to output the position of the original repeater antenna as opposed to their own true position [1].

A GPS simulator can be considered a spoofer as well. A simulator is quite effective in doing just what it is designed for – to test a receiver by processing an input RF data stream such that the receiver provides an output which corresponds to an artificial simulation. For the purpose of receiver testing this is fine as it is hard wired testing and the operators know what to expect from the receiver under test. However, if this same GPS simulator signal is broadcast and its power level is greater than that of the received true GPS signal, then these receivers in close proximity can unknowingly provide an output determined by the GPS simulator.

Potentially the most sophisticated/diabolical approach was presented in 2008 [2] which involves a methodology to intentionally spoof a satellite navigation receiver. This spoofer design is placed near the antenna of the victim receiver, obtaining a similar GPS signal profile. Once established, the spoofer powers on its transmitter, gradually increasing its power above the thermal noise floor, capturing the victim receiver, and then generating a transmission which emulates a position deviating from truth. Such an approach, which is quite powerful, would be more challenging to apply to a moving object where the spoofer could not be collocated – such as an automobile or aircraft.

Radio frequency interference is detrimental to satellite navigation, denying a position solution. But spoofing moves beyond that, providing an incorrect time or position solution, either intentional or unintentional

NAVIGATION: *Journal of The Institute of Navigation*
Vol. 59, No. 4, Winter 2012
Printed in the U.S.A.

(with intentional typically employing the more deceptive tactics). Consider the fisherman whose position is being monitored via GPS to ensure he does not violate restricted waters. Likewise, consider the truck driver trying to hide the true amount of driving done to avoid GPS-based road tolling charges and/or required rest breaks. These scenarios provide motivation for individuals to risk illegal action for financial gain.

Ideally one could trust the resulting GPS measurements of time and position and have confidence the resulting solution was not a result of GPS spoofing. The following sections of this paper will discuss previous approaches/countermeasures for spoofing, introduce the concept of automatic gain control (AGC) for GPS, discuss how AGC can be applied for spoofer detection, show the results of field trials testing the effectiveness of AGC for spoofer detection, discuss possible improvements, and provide conclusions.

PREVIOUS WORK ON SPOOFING DETECTION/ COUNTERMEASURES

Early in the history of GPS, the potential of spoofing was recognized and a unique component, Y-code, was added to the military P-code signal to provide an antispoofing transmission [3, 4]. Researchers have found novel means to leverage these military specific signals as a spoofing countermeasure, despite not knowing their exact properties/contents in civil receivers via cross correlation [5]. However it does require a secure communications link and a second receiver to use for correlation. Yet it is one of the more effective, low computational methodologies proposed to date and leverages the existing military signals.

One can also consider civil signal design constructs which would add an antispoofing capability. These have been investigated and candidates proposed [6]. However the signal design cycle is extremely long and, at least for the near future, these signals do not look like they will be incorporated in GPS and it is uncertain regarding their place in other GNSS.

Fairly obvious tests can be employed which can easily identify the less sophisticated spoofing attacks, one in which the user's position or time estimate take an unrealistic time/position jump as determined by the navigation Kalman filter. Examples are presented in [7, 8]. A similar approach would be through the use of receiver autonomous integrity monitoring (RAIM). These techniques are quite effective for the less sophisticated attacks and are not overly computationally expensive though the mechanism for detection is a single epoch change and is quite sensitive to the jump magnitude/filter tuning.

If one looks beyond the core single antenna GPS receiver, augmentations can be leveraged to provide spoofing detection. One of the simplest approaches leverages a well-known/researched technique of adding inertial sensors and cross comparing the resulting dynamics; one such example is documented in [9]. Given the availability/low cost of multi-axis MEMS accelerometers, even the inclusion of these should be quite effective to include and cross compare reported movement and raise a confidence flag when they do not agree. However, the great multitude of GPS receivers available today do not contain such sensors. If one considers the antenna, it too can be used for spoofing detection. The typical GPS antenna is either omnidirectional (for mobile phones) or hemispherical (for fixed locations) and receives signals from all directions. An antenna array is quite effective to steer beams toward the known direction of the satellites and nulls toward power sources. Thus the antenna array is one of the few technologies that can not only flag a potential spoofing condition but also attempt to operate in the presence of it. Researchers have also proposed using a synthetic array, applicable for a single antenna dynamic receiver, to determine the presence of a spoofing source – which is functional but requires additional complexity and is only applicable for a stationary spoofing source [10].

Lastly, there have been a number of attempts to enable the detection of GPS spoofing, even the most sophisticated approaches, in the signal processing domain. The majority of these operate in the correlation domain, which is computationally expensive, applying signal quality monitoring type approaches to look for additional, perhaps weaker, correlation peaks which would show evidence of additional signals and potential spoofing [11–13]. The downside of such an approach is the computational complexity to obtain the additional correlation measurements and then also the challenge of distinguishing spoofing signals from multipath in the secondary correlation measures.

Thus to date, there is no single readily available detection methodology published in the open literature that could be applicable to the bulk of the existing receiver base, or incorporated easily in forthcoming receivers, to determine with minimal computational complexity and/or infrastructure if a satellite navigation receiver is under a spoofing attack.

RECEIVED GPS SIGNAL CHARACTERISTICS AND AUTOMATIC GAIN CONTROL (AGC)

The metric proposed in this paper for spoofer detection is based on AGC functionality. Prior to describing the specific spoofer detection implementation, this section provides the background on this front end component within the receiver.

The received GPS signal power on Earth by a traditional hemispherical RHCP antenna is below that of the thermal noise floor power, P_N, given by Equation (1).

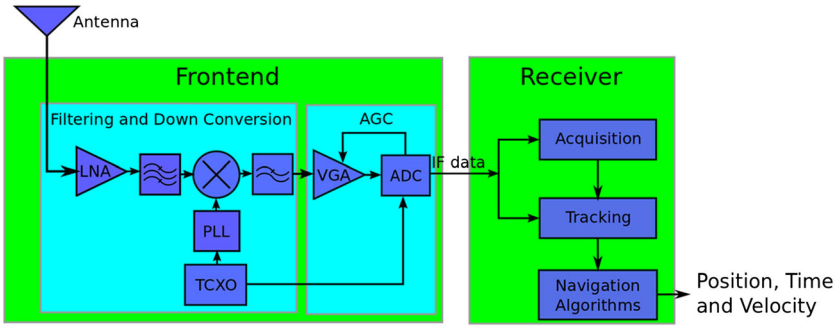

Fig. 1–Typical GPS receiver architecture with AGC shown

$$P_N = k\,T_A BW \tag{1}$$

where k is Boltzmann's constant, T_A is the effective antenna temperature, and BW is the bandwidth.

This coupled with the additive noise from the first stage front end components, as expanded in Equation (2), implies that noise is the dominant source in the capture of raw intermediate frequency (IF) GPS data samples [12].

$$P_{Ntotal} = k\,(T_A + T_R)BW \tag{2}$$

where T_R is the receiver noise temperature derived from Friis formula and the cascade of the front end components.

Any GPS receiver which utilizes more than single bit sampling, which is the great majority of GPS receivers, relies on AGC to optimize the gain of the front end to that of the analog-to-digital converter (ADC) input range as illustrated in Figure 1. However, these two statements are somewhat contradictory. If receiver noise, a stable value dependent on the established antenna and receiver noise temperatures, is the primary component in a GPS data capture, why is AGC needed? Two primary reasons; first, to enable a GPS front end to adapt to varying levels of gain provided by different active antenna designs as well as the additive noise from the early stage front end components; and second, to adjust the gain in the presence of RF interference or RFI. An underlying premise here is that these early stage front end components are stable and have little to no impact on the AGC. With this premise, this second component (adjusting the gain in the presence of RFI) has been explored initially in [12, 13] and then in more detail in [14] as an interference detector and it is the same mechanism proposed in this paper as an effective computationally efficient spoofer detector.

Given that the expected signal to be captured is thermal noise, a Gaussian distribution of samples is expected within the captured data. Thus, the AGC circuitry for a multi-bit works to adjust the gain in the receiver's front end to achieve this distribution to minimize digitization losses. This is illustrated for a 2 bit analog-to-digital converter (ADC) in Figure 2. Given a sigma, σ, for the Gaussian distribution of the incoming signal or thermal noise the loss associated with non-optimal quantization is depicted in Figure 3. Various algorithms, both digital and analog, can be utilized for the AGC implementation. One digital-based approach is to continuously monitor the distributions of the samples and raise/decrease the gain if the distribution does not match the expected Gaussian, as shown in Figure 4 for a 2 bit ADC.

Although any multi-bit receiver will implement AGC, all receivers may not have the same level of sensitivity within their AGC circuitry. A test of this AGC sensitivity for three different GPS front ends was presented in [15] and that setup and result are shown in Figures 5 and 6, respectively. Of course, the more sensitive the AGC mechanism, the better RFI/spoofer detection it will provide.

AGC DETECTION OF LIVE REPEATER SPOOFING

An experiment was conducted to assess the ability of the AGC measurement to detect the presence of a spoofing signal provided by a GPS repeater. Since live broadcast within the GPS frequency band is difficult due to national and global protection of the GPS frequency band, such a test was conducted with appropriate permission at a test range with the support of the Swedish Defense Research Agency (FOI).

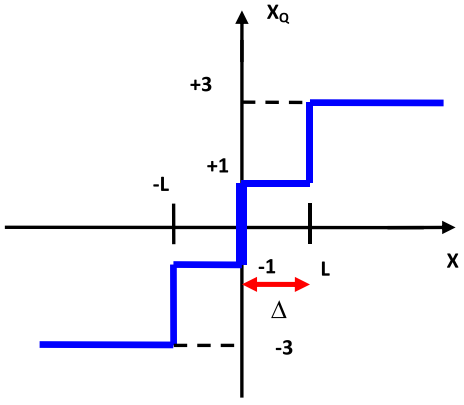

Fig. 2–Quantization Representation for 2 Bit Sampling

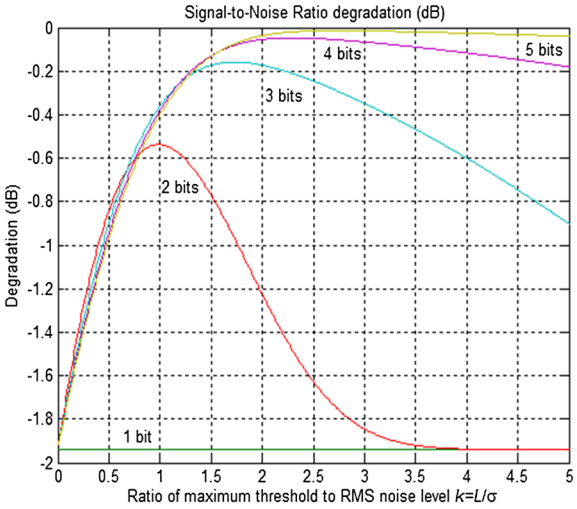

Fig. 3–Digitization Degradation as a Function of Quantization Level (from [14])

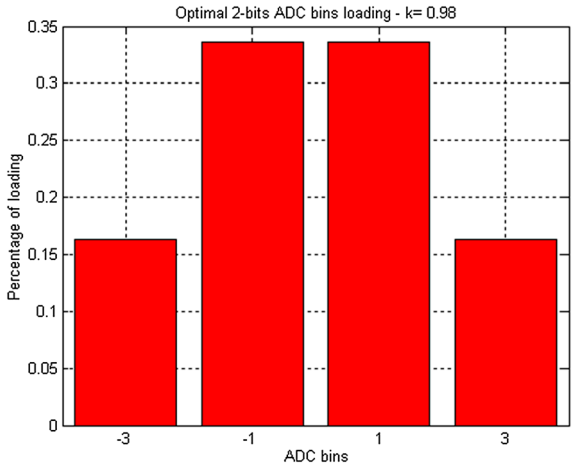

Fig. 4–Optimal AGC Bin Distibutions for a 2 Bit ADC

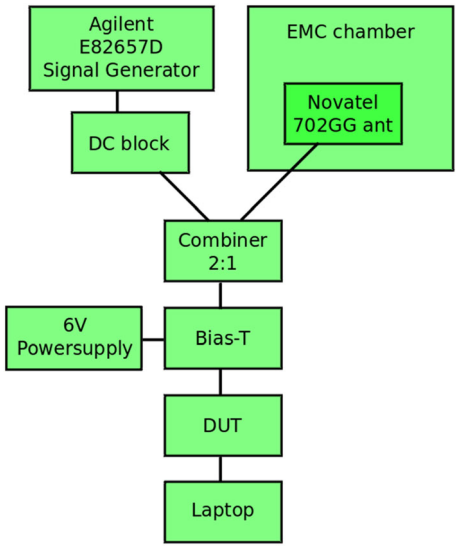

Fig. 5–AGC Sensitivity Testing Block Diagram

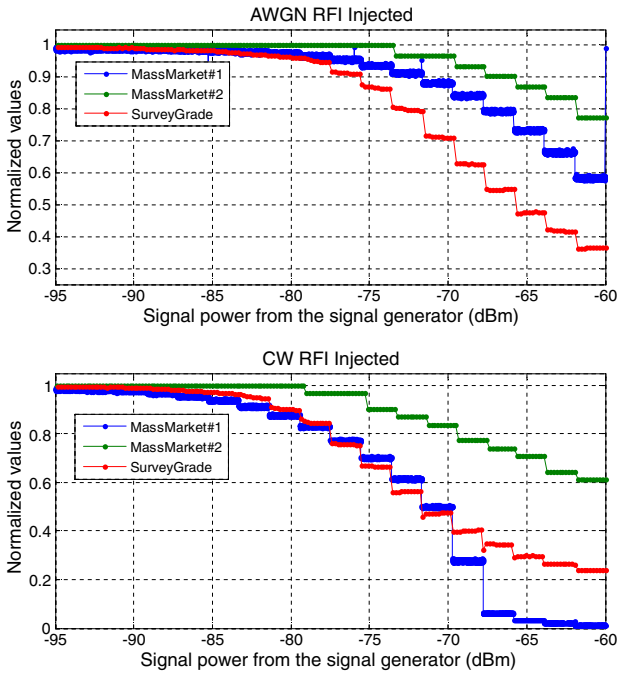

Fig. 6–Normalized AGC Metrics from the RFI Injection Testing for White Noise and CW RFI

Repeater spoofing is a more simplistic level of GPS spoofing as one can watch for the "position jump" from the true receiver position to that of the repeater source antenna and use this as a detection metric as was described earlier. Ideally the more sophisticated spoofing attack could have been used in such a test, yet such equipment was not available. Nevertheless, it is interesting to use a repeater and conduct such testing to assess the performance of the AGC as a spoofer detection metric, compare that to the position jump approach, and discuss the extension to more sophisticated spoofing detection.

Prior to conducting the spoofing test, a calibration run was conducted over a period of three days at the University of Colorado in an outdoor environment. The AGC measurement for the survey grade receiver used in this test is shown in Figure 7. Some interesting elements can be gathered from this data. First, the AGC does appear to have some level of noise associated with the measurement as it is not constant for the duration of the test. Second, it is clear that at approximately 59 hours into the collection the receiver antenna was exposed to an RFI event as the AGC measure quickly dropped for a period of tens of seconds, indicating the internal amplifier needed to provide less gain (implying additional RF energy in the band). Finally, the mean and standard deviation of the data, excluding the RFI event, has been computed and indicated on the plot.

After the calibration, the actual testing was done. A Google Earth sky view of the repeater spoofing experiment conducted in Sweden is depicted in Figure 8. Shown are the position of the repeater

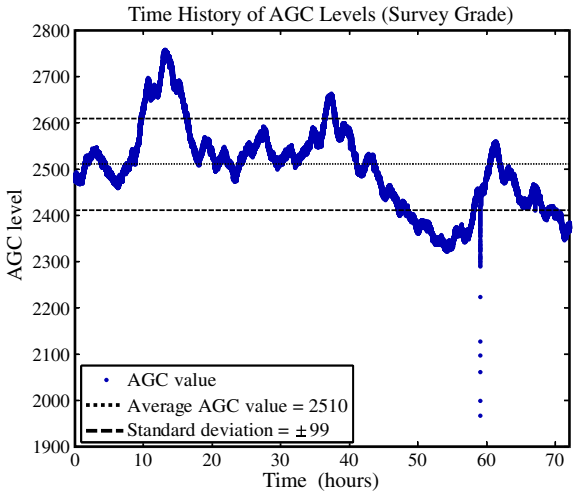

Fig. 7–Time History of 72 Hours of Nominal AGC for a Survey Grade GPS Receiver

source antenna, the repeater transmission antenna, and then a road on which a vehicle drove to/from the repeater transmission antenna. The vehicle had a roof mounted GPS antenna and various GPS receivers. Two tests were conducted. First, the vehicle started outside the range of the repeater spoofer, the GPS equipment was powered on and logging was initiated once a position fix had been established, and then the vehicle drove toward the transmission antenna. Second, while in close proximity to the repeater spoofer transmission antenna, the GPS equipment was powered on and logging was initiated for a second collection once a position fix had been established. Then logging continued as the vehicle drove away from the transmission antenna. The position solution was logged along with the AGC measurement, both at a 1 Hz rate. The focus here will be on the survey grade GPS receiver used in the early calibration as prior testing showed it to be the most sensitive to wideband interference although additional receivers and GPS front ends were connected to the antenna.

The data of interest are plotted in Figures 9 and 10, showing the drive to the spoofer transmission antenna and then the drive away from the spoofer transmission antenna, respectively. The metrics are the AGC value and then the x, y, z position provided by the GPS receiver as a function of time. Also shown on this plot is a threshold when the AGC measurement crosses a two sigma threshold established from the calibration data.

For the drive to the spoofer, shown in Figure 9, the vehicle is moving with approximately constant speed toward the spoofer transmission antenna and one can observe the coordinates changing as the vehicle is moving. At approximately 135 s into the drive toward the antenna, the position solution seems to diverge and then no position is available until approximately 170 s into the drive when the receiver outputs the position of the spoofer source antenna as the receiver has been captured by the repeater spoofer. Other metrics, such as the lock on the individual channels, were investigated and analyzed but the resulting position solution provided the most broad/clear depiction of the events. As flagged earlier, the loss of the position output followed by a position jump could likely be used as a potential spoofing detection metric. However, plotted in parallel with the position is the AGC data for the survey grade receiver. The measure has a negative slope as the vehicle moves toward the spoofer transmission antenna. At approximately 115 s the AGC measure crosses the two sigma threshold and then begins to change rapidly – well in advance of any distortion in the position domain

Fig. 8–Google Earth Image of Repeater Spoofer Layout and Driving Route

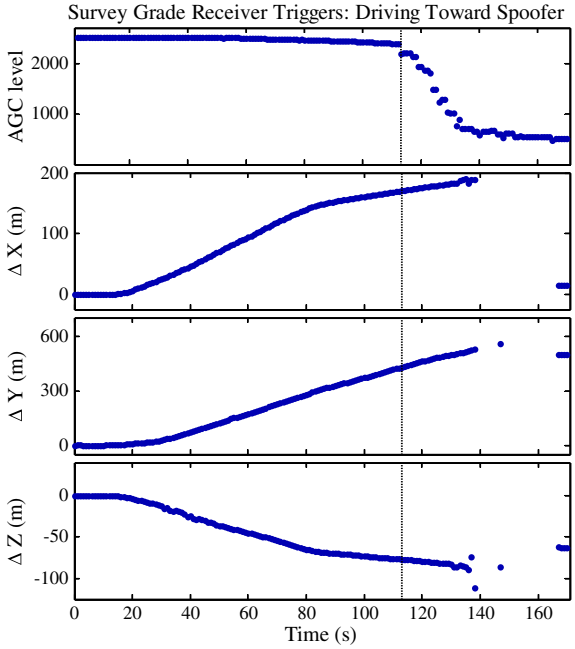

Fig. 9–Experimental Results – Survey Grade Receiver Drive to Spoofer Transmission Antenna

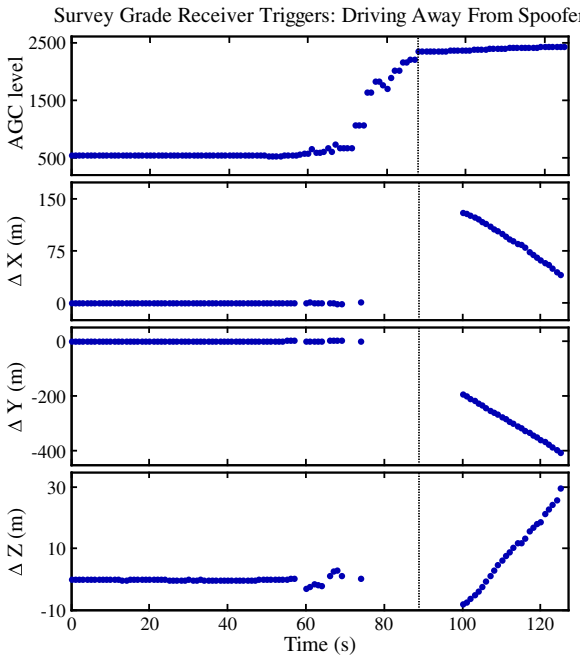

Fig. 10–Experimental Results – Survey Grade Receiver Drive from Spoofer Transmission Antenna

results – and thus appears to be a solid indicator of the confidence one can have in the receiver output.

For the drive from the spoofer, shown in Figure 10, the GPS equipment is powered on in close proximity to the spoofer and the vehicle is driven away from the spoofer transmission antenna. Despite the dynamics, the receiver reported position remains fixed on that of the repeater source antenna for a majority of the drive. At approximately 60 s into the drive, the position fix becomes intermittent as the spoofer power begins to decrease and eventually the receiver loses the position fix. No position is available until approximately 100 s into the collection when the receiver acquired live GPS signals and its reported position is true. In terms of the AGC measure for this case, it again clearly protects the user from misleading information. When the receiver is powered on, the AGC metric is well outside the nominal range determined from calibration – thus any receiver reported measurements should not be trusted as it is clear there is excessive additional RF energy in the frequency band. As the vehicle leaves the region of influence of the spoofer repeater, the AGC metric shows decreasing energy in the band. Eventually when within the established two sigma threshold, at approximately 90 s, the receiver output can be trusted. When this happens the receiver does not provide a position output as it is in an acquisition mode, having lost the signals from the repeater spoofer and is attempting to acquire the live GPS signals. The live GPS signals are acquired at approximately 100 s and, based on the AGC measure, can be trusted for navigation/operation.

Other GPS front ends and receivers were also tested in parallel with the survey grade receiver. In all cases the AGC metric demonstrated the ability to detect the spoofing environment well in advance of any corruption/distortion of the reported position domain results [16].

REFINING AGC DETECTION

The previous experiment showed the power of the AGC metric for assessing the validity of the output/trustworthiness of a satellite navigation receiver. However, the test used a very basic spoofer design. Thus the question remains as to the effectiveness of AGC against a more sophisticated spoofing attack such as that presented in [2].

It is important to recognize that a sophisticated spoofing attack can be quite difficult. If the spoofer transmission antenna cannot be collocated with that of the victim GPS antenna, then significant transmission power must be utilized to capture the victim receiver and detection/localization techniques are available for high power signals in the GPS band [17]. Further, if colocation is not possible for a dynamic GPS antenna it can be quite challenging to use the "lift and carry" approach used by the more sophisticated spoofers, as an accurate dynamic position of the target platform is required by the spoofer. Again, recall that inertial sensors, often employed on high value dynamic platforms, can also be used to test for potential discrepancies in GPS versus INS measurements.

For a stationary receiver whose antenna is accessible (perhaps used for timing applications), the attack is more problematic as the transmission antenna can be placed in close proximity and leverage low power. Perhaps more challenging of a threat is the use case where GPS, often coupled with a wireless modem, serves as a monitor for the position of a vehicle or person. In such a case there may significant motivation for spoofing of this receiver such that the reported/relayed position solution is incorrect.

Would the AGC metric, even the most sensitive as that in the survey grade receiver, be capable of flagging potential spoofing in these more problematic attacks? In such cases the added power to the band will be as minimal as possible, simply enough to "lift" the receiver off the true measurements and then "carry off the receiver" to the measurements/location specified by the spoofer.

The challenge, as shown in Figure 7, is this variability of the AGC measurement under normal operating conditions. Although it was shown to be quite effective in the spoofer repeater experiment, increased sensitivity could improve the detection capabilities. In order to have the most sensitive measure possible, to detect any additional energy in the band, it would be desirable to have a very stable AGC measure under nominal conditions reflecting the constant which is the thermal noise floor. So why do we see this variability? Recall that the thermal noise floor is not quite a constant, but dependent on temperature as expressed in Equation (1). In Figures 11–13 the AGC calibration measurement has been plotted (with the RFI event removed) along with the ambient temperature measured in Boulder, CO, USA. Although this is not the exact temperature at the antenna (rather a generic measure within the city), a strong correlation is obvious. However, two things must be flagged. First, within the equation T_A refers to the effective antenna temperature (which experiences little change on the Kelvin scale), not the ambient temperature. Second, the effect observed does not agree with Equation (1) – when the temperature increases then gain of the front end actually increases (implying the thermal noise has gone down, not up). Further investigation revealed the main factor in this AGC change results from the change in temperature of the amplifier in the antenna itself whose performance varies with temperature. As the amplifier increases in temperature, its efficiency and resulting gain decrease. Thus the AGC, or internal amplification within the receiver, increases to compensate for this. Calibration efforts computed the change in the gain to be approximate 2 dB as a result of this temperature effect. Given this insight, it would be possible to further calibrate the AGC as a function of ambient temperature (or thermally isolate the first stage amplifiers), further increasing the sensitivity, should that be required.

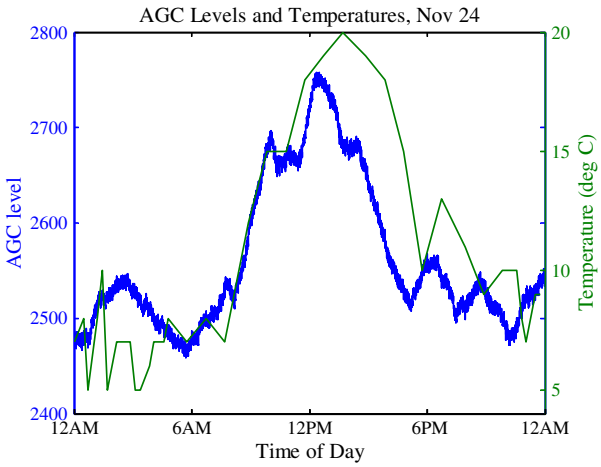

Fig. 11–AGC Level and Ambient Temperature – Day 1

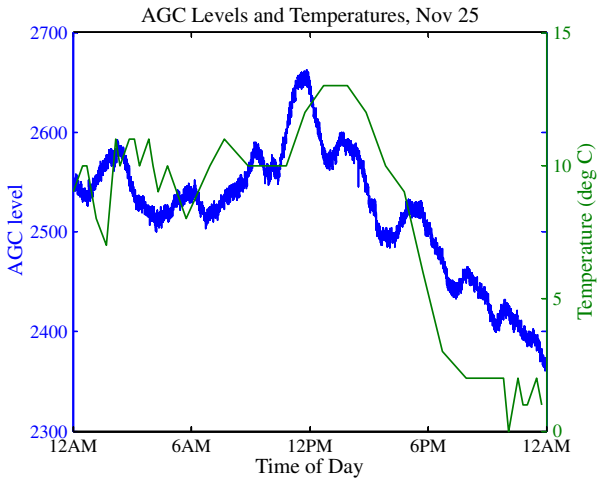

Fig. 12–AGC Level and Ambient Temperature – Day 2

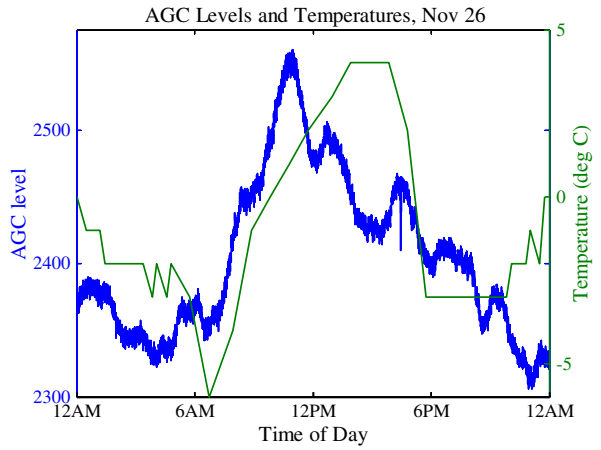

Fig. 13–AGC Level and Ambient Temperature – Day 3

In the more devious cases, those in which an informed individual may attempt to spoof an installed receiver for illegal gains, one could envision additional measures being employed. One possible idea would be to block/shield the true GPS signals such that the spoofer transmit power would not need to overcome the existing signal power to capture the receiver. Experimental work has shown that the AGC metric can be used to effectively combat such an attack as this as well as those previously described. In this case, the AGC metric can provide insight into the operational environment of the antenna/GPS receiver. In order to demonstrate this concept a simple experiment was conducted. In this case, AGC and C/No measurements were logged from a rooftop antenna after a brief snowfall. Procedures for the experiment are shown in Table 1.

The test revealed interesting results shown in Figures 14 and 15 for the C/No for PRN06 (a high elevation angle satellite) and AGC for the receiver, respectively. The primary mechanism under investigation is the effective antenna temperature. A stationary GPS antenna is hemispherical in nature, focusing most of its gain skyward, but also has some sidelobes/backlobes which contribute to the overall pattern. The effective temperature of such an antenna is estimated at 130 K [18], mapping temperature over the antenna pattern. This value is the temperature used in Equation (1) to determine noise power which drives the underlying AGC measurement.

During the first 20 min of the test, a light cover of snow sits atop the antenna which has a double effect. First, the snow slightly attenuates the GPS signal power reaching the antenna as can be seen within the C/No plot. After the snow is cleared (which results in a short antenna blockage), the C/No increases slightly. Even more interesting is that this light snow covering also has an impact on the AGC measurement. While it is covering the antenna, it changes the effective temperature of the antenna as the antenna no longer has a clear view of cold space, raising the effective temperature of the antenna. This can be seen in the AGC data.

Next a plastic radome is placed over the antenna. This structure covers the antenna completely but is electrically transparent and thus no change in the C/No or AGC is expected nor observed in the data.

Table 1—Procedures for experiment following light snowfall

Time (minutes)	*Action*
0	AGC and C/No data logging initiated
20	Light snowfall cleared off the top of the antenna
24	Plastic radome placed over the antenna
27	Plastic radome removed
31	Metal trash can placed over the antenna
34	Metal trash can removed
36	Test complete, logging terminated

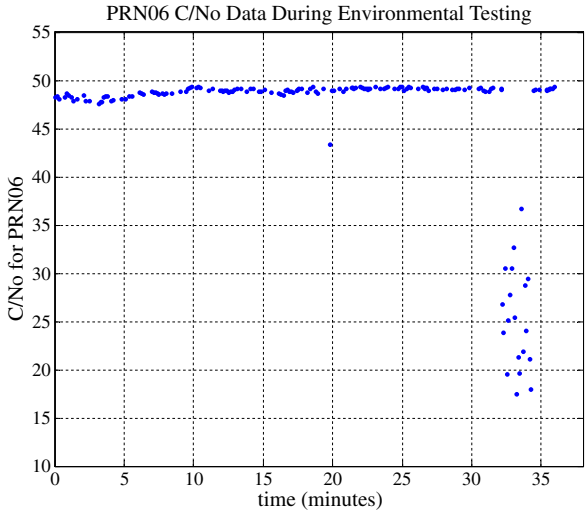

Fig. 14–C/No for PRN06 during the Environmental Testing

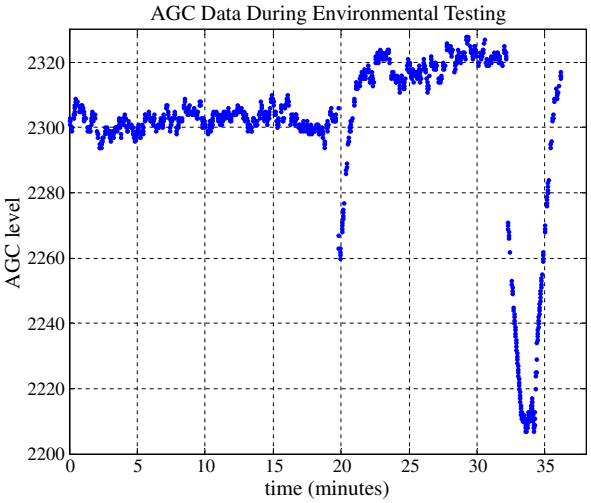

Fig. 15–AGC Data for the GPS Receiver During the Environmental Testing

Finally, a metal trash can is placed over the antenna. Now the GPS signals are attenuated significantly to the point where tracking is lost. A potential spoofer could now be introduced at a minimal power level. However, the AGC metric drops as the effective temperature of the antenna changes from 130 K to the 273 K ambient temperature, clearly showing a change in the operational environment. With this higher effective temperature, almost 3 dB more noise (from Eq. (1)) is now entering the front end chain, thus the AGC lowers its internal gain to compensate. As the trash can is removed to complete the test, the measurements return to their nominal state.

This experiment shows that the AGC can provide a good deal of insight into the operational environment of a GPS receiver. For example, in the devious

case where one might want to block all GPS signals to introduce the lowest possible power spoofer, it should be possible to detect if the receiver is operating in open sky conditions or is blocked. Again, sensitivity and a proper calibration will be critical in such a case.

CONCLUSION

This paper presents the use of the AGC measure within a GPS L1 receiver as a low computational complexity means to detect and flag potential spoofers, rendering them no more harmful than the much less sophisticated jammers.

The experiment used to validate this approach clearly showed the danger of spoofing, as a receiver powered on in the presence of a spoofer will lock onto the signal and provide erroneous measurements. However, using the AGC, it was clearly evident that those resulting measurements could not be trusted as a consequence of the additional frequency energy in the band.

AGC is available in all multibit GPS and GNSS front end designs, with varying levels of sensitivity, and thus offers a means to provide a confidence or trust metric to the satellite navigation receiver. It is likely this could be leveraged in the existing base of deployed GPS receivers with minimal modification.

The typical trade off of higher sensitivity/potential false alarms can be explored as the AGC measure itself can be calibrated to provide significant insight into the operational environment of the receiver and maximize spoofer detection capability.

AGC should not be considered the single "silver bullet" to prevent spoofing attacks. But, again, it is simplistic and can complement other methodologies to detect such an attack. Using AGC does rely on the nature of the GPS L1 frequency band in that it is a protected band and other transmission sources, which would impact a receiver's AGC measurement, are not allowed. Spurious emissions and radio frequency leakage, such as that allowed by the US Federal Communication Commission (FCC) Part 15 ruling, may increase the noise floor resulting in potential false alarms. Also front end components, prior to AGC, which provided additive noise need to be stable over their operating parameters. Similarly the GPS L5 band has other, legal, transmission sources so protection there may be more difficult.

Further, although the title of this paper somewhat facetiously implies that spoofers need not be considered a threat, the appropriate modifications must be incorporated to leverage AGC, or other mechanisms for detection, and then this premise should very much hold. The much more simplistic RFI will remain problematic for GNSS even with such modifications.

The combination of accelerometers (or other possible sensors to be used as an integrity check) and AGC should provide a very effective means of spoofer detection. And AGC alone provides significant insight into the operating environment of the GPS/GNSS receiver.

ACKNOWLEDGEMENTS

The author thanks the Swedish Defense Research Agency (FOI) who served as host of the live spoofer experiment documented in this paper, particularly the assistance from Fredrik Marsten Eklöf, Peter Johanson and Mickael Alexandersson. Oscar Isoz was a tremendous asset in the data collection during the testing. Holly Borowski, Sherman Lo, Frank van Graas, and Juyong Do assisted with the experimentation and/or data interpretation.

References

1. Dunkel, W., *11th International GBAS Working Group (IGWG)*, Osaka International Convention Center, Osaka, Japan, February 2011.
2. Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., and Kintner, P. M., Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, GA, September 2008, pp. 2314–2325.
3. GLOBAL POSITIONING SYSTEM WING (GPSW) SYSTEMS ENGINEERING & INTEGRATION, Navstar GPS Space Segment/Navigation User Interfaces INTERFACE SPECIFICATION - IS-GPS-200 Revision E, 8 June 2010.
4. Ward, P., "Monograph on GPS Antispoofing," *Proceedings of the 8th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1995)*, Palm Springs, Ca, September 1995, pp. 1563–1571.
5. Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., and Humphreys, T. E., "Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, OR, September 2011, pp. 2619–2645.
6. Scott, L., "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, Portland, OR, September 2003, pp. 1543–1552.
7. Rao, K. D., Swamy, M. N., and Plotkin, E. I., "Anti-Spoofing Filter for Accurate GPS Navigation," *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, Salt Lake City, UT, September 2000, pp. 1536–1541.

8. Wen, H., Huang, P. Y.-R., Dyer, J., Archinal, A., and Fagan, J., "Countermeasures for GPS Signal Spoofing," *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*, Long Beach, CA, September 2005, pp. 1285–1290.
9. White, N. A., Maybeck, P. S., and DeVilbiss, S. L., "MMAE Detection of Interference/Jamming and Spoofing in a DGPS-Aided Inertial System," *Proceedings of the 11th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1998)*, Nashville, TN, September 1998, pp. 905–914.
10. Nielsen, J., Broumandan, A., and Lachapelle, G., "GNSS Spoofing Detection for Single Antenna Handheld Receivers," *NAVIGATION*, Vol. 58, No. 4, Winter 2011–2012, pp. 335–344.
11. Wesson, K. D., Shepard, D. P., Bhatti, J. A., and Humphreys, T. E., "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, OR, September 2011, pp. 2646–2656.
12. Van Dierendonck, A. J., "GPS Receivers," *Global Positioning System: Theory and Application*, B. Parkinson and J. J. Spilker, Jr., Eds., Washington, D.C.: AIAA, Inc., 1996.
13. Ndili, A., and Enge, P., "Receiver Autonomous Interference Detection," *Proceedings of the 53rd Annual Meeting of The Institute of Navigation*, Albuquerque, NM, June, 1997, pp. 79–88.
14. Bastide, F., Akos, D., Macabiau, C., and Roturier, B., "Automatic Gain Control (AGC) as an Interference Assessment Tool," *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, Portland, OR, September 2003, pp. 2042–2053.
15. Isoz, O., Akos, D., Lindgren, T., Sun, C.C., and Jan, S.-S., "Assessment of GPS L1/Galileo E1 Interference Monitoring System for the Airport Environment," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, OR, September 2011, pp. 1920–1930.
16. Borowski, H., Isoz, O., Eklöf, F. M., Lo, S., and Akos, D., "Detecting False Signals with Automatic Gain Control," *GPS World*, Vol. 23, No. 4, April 2012, pp. 38–43.
17. Isoz, O., Balaei, A. T., and Akos, D., "Interference Detection and Localization in the GPS L1 Band," *Proceedings of the 2010 International Technical Meeting of The Institute of Navigation*, San Diego, CA, January 2010, pp. 925–929.
18. van Diggelen, F., *A-GPS: Assisted GPS, GNSS, and SBAS*, Artech House, ISBN-13:978-1-59693-374-3, 2009.