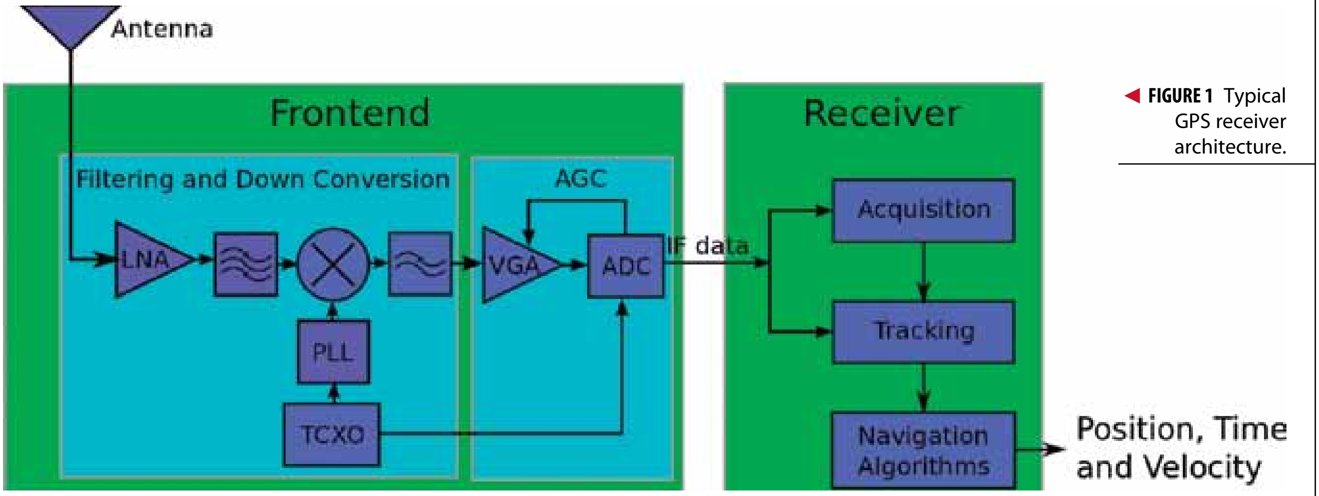


FIGURE 1 Typical GPS receiver architecture.

Detecting False Signals

with Automatic Gain Control

A component of most GPS receiver front-ends, the automatic gain control (AGC) can flag potential jamming and spoofing attacks. The detection method is simple to implement and accessible to most GPS receivers. It may be used alone or as a complement other anti-spoofing architectures. This article presents results from a baseline AGC characterization, develos a simple spoofing detection method, and demonstrate the results of that method on receiver data gathered in the presence of a live spoofing attack.

Holly Borowski, Oscar Isoz, Fredrik Marsten Eklöf, Sherman Lo, and Dennis Akos

Growing reliance on GNSS also creates the need to defend against those with the ability to exploit its weaknesses. Specifically, GNSS signal spoofing is recently a growing concern, as an effective spoofing attack can fool a GNSS receiver into producing erroneous navigation and timing information. Although applicable to many GNSS, GPS will be used as the example.

One example of spoofing seen recently in the popular press was the Iranian claims of bringing down a U.S. unmanned aircraft via a GPS spoofing attack. Although this may be unfounded given the complexity required, spoofing attacks to autonomous vehicles are emerging threats. A second hypothetical example is a fisherman whose location is monitored using GNSS may be motivated to use spoofing, such that illegally fishing in protected waters is not detected, increasing profits.

GPS signals received by a traditional hemispherical antenna are below the thermal noise floor, a physical constant dependent only on temperature. Although multiple signals are transmitted at low power in the same frequency band, they can be acquired and tracked using code-division multiple-access (CDMA). However, low signal power also makes GPS systems vulnerable to intentional radio-frequency interference (RFI) and the more sophisticated spoofing.

Spoofers range from simple to sophisticated. For example, a simple spoofer may be built from a GPS repeater (known as meaconing) by simply using it to rebroadcast signals at a higher power than the authentic GNSS signals. Receivers close enough to these spoofers then acquire and track the stronger spoofed signal, producing an erroneous position/timing solution. In this case, a position jump is likely to occur in the victim receiver's reported solution as it transitions from the true signals to the spoofed signal, alerting the user of a potential spoofing attack. Somewhat more complex than a simple repeater would be to broadcast signals from a GPS simulator, which would enable a threat with more control over the signal-to-noise ratios as well as the resulting position. Finally, a very sophisticated spoofing attack first introduced by Humphreys , et al. in 2008 may be implemented by placing a spoofer near the receiver, so that it can correctly align its transmitted false signals to the authentic ones seen by the victim receiver. The spoofer then gradually increases the power of its transmitted signals, eventually capturing the receiver. After the receiver begins tracking the false signals, the spoofer can gradually deviate its transmitted signals from the authentic ones, causing the victim receiver to produce false navigation and timing information.

Effective methods have been

developed for distinguishing spoofed from authentic GPS signals with a summary most recently presented in a January 2012 GPS World article by Wesson, Shepard, and Humphreys. In short, these methods can be divided into cryptographic and non-cryptographic spoofing detection schemes. Unfortunately the presented methods are not readily available to the majority of current standalone GPS receivers and can be quite computationally expensive.

We suggest a method using the Automatic Gain Control (AGC), a component of most GPS receiver front ends, to flag potential jamming and spoofing attacks. The proposed spoofing detection method is simple to implement and accessible to most GPS receivers as a measure of confidence in the authenticity of received and tracked signals. It may be used by itself on receivers without other spoofing detection capabilities or to complement other anti-spoofing architectures.

AGC Background

GPS receivers consist of an analog portion and a digital portion: the analog signal, comprised nominally of GNSS signals and white Gaussian thermal noise, is received, amplified, down-converted, and filtered, then converted to a digital signal for processing within receiver acquisition and tracking loops. During signal sampling and quantization by the Analog to Digital Converter (ADC), some quantization losses will occur. These losses depend on the ratio between the ADC's maximum quantization threshold, L, the number of bits utilized, and the incoming signal standard deviation, σ.

This is where the AGC comes in. In a typical GPS receiver, it sits between the analog portion of the front end and the ADC, as shown in **FIGURE 1**. The AGC acts as a variable gain amplifier, adjusting the power of the incoming signal to optimize the L/σ ratio, minimizing quantization losses. This assumes the receiver is a multibit design which is the norm for GPS receivers today.

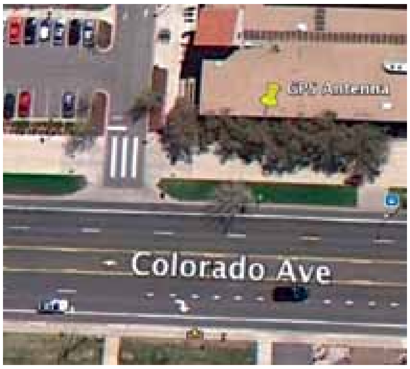
When the GPS band is interference free, which should be the norm due to restrictions on emissions in and near the band, the AGC gain depends almost exclusively on thermal noise, since the received GPS signal power level is below that of the thermal noise floor. Since this thermal noise is a physical constant with minimal fluctuation resulting from the span of temperature variations on earth, the primary role of the AGC is to adjust to different active antenna gain values. However, in the unlikely presence of interference the AGC gain drops in response to increased power in the GPS band. Thus, AGC levels may be used to indicate potential interference. Moreover, AGC levels are expected to respond to the interference before receiver performance is compromised, so useful flags may be established, which could provide a warning before a problem exists.

Baseline AGC Data Gathering

Prior to the spoofer experiment, baseline AGC data were collected for 72 hours using both a survey grade and a mass market receiver. The GPS antenna was located on the roof of the Engineering Center at Colorado University (CU) in Boulder (**FIGURE 2**).

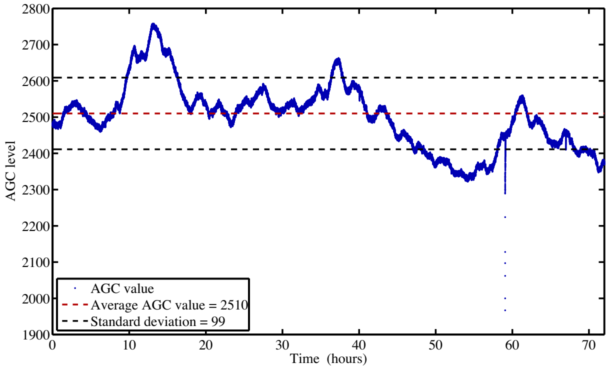
Currently there is no standardization among GPS receivers for AGC reporting units or the measurement itself. Most receivers offer such a metric but it is likely that each needs to be interpreted individually. However, in general this metric provides an indication of the relative gain of the amplifier within the receiver. Should the active antenna be disconnected (loss of gain), the AGC metric will increase showing the increase in internal gain needed to compensate for the loss of the active antenna amplification of the thermal noise floor. Should additional energy be detected in band, the internal gain will decrease accordingly.

Baseline AGC levels from the survey grade and mass market receiver are shown in **FIGURES 3A AND 3B**, respectively. The survey grade receiver AGC measurement was more sensitive to changes in the nominal environment; these results will be discussed later in more detail. The mass market receiver provided a much more consistent measure for the entire test period. Interestingly, there was one brief yet noticeable drop in AGC metric from the survey grade and mass market receivers at approximately hour 59 into the collection. Its magnitude was not overly significant, as it did not have an impact on the availability or accuracy of the position solution measurements from either receiver. It is assumed that this is a brief RFI event that occurred during the collection, perhaps from an illegal personal privacy device (PPD) in a vehicle on the nearby road.

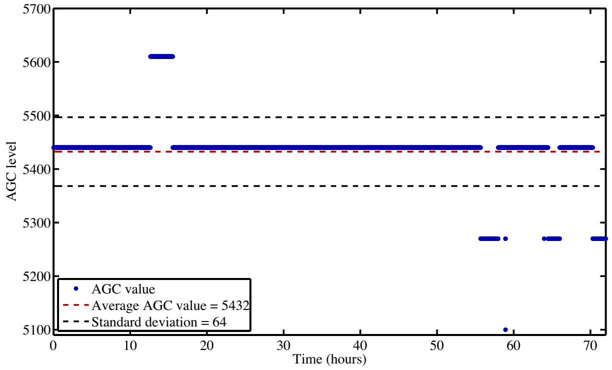


▲ **FIGURE 2** Antenna location for baseline AGC data collection.

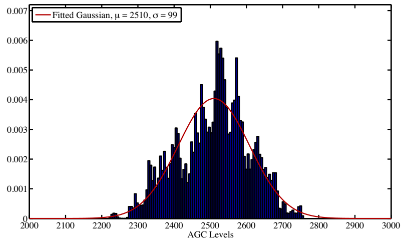
This RFI event outlier was excluded from the computed mean and standard deviation from the receivers' AGC data. As shown in **FIGURE 4A**, the mean reported AGC gain was approximately 2510, and its standard deviation was approximately 99. For the mass market receiver, the data shows clear evidence of quantiztion in **FIGURE 4B**. Here the mean AGC level in this test was approximately 5432, standard deviation was approximately 64. Again, the absolute measures mean little and cannot be compared from various vendors of receivers. It is, of course, possible to calibrate individual receivers and obtain an absolute measure should this be required for



▲ **FIGURE 3A** Nominal AGC values for survey-grade receiver.



▲ **FIGURE 3B** Nominal AGC values for mass-market receiver.



▲ **FIGURE 4A** Histogram of survey-grade AGC data.

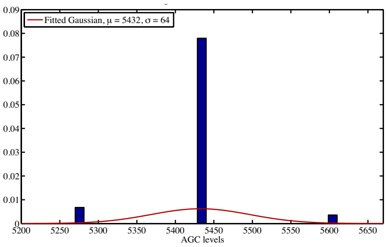
a specific application. During the baseline data collection receiver reported position solutions were nominal, with deviations on the order of 2-3 meters in east and north directions, and 5-6 meters in the vertical direction for both receivers. A Gaussian curve was fit to the AGC data and although the data may not be well modeled by a Gaussian, a 2x standard deviation will be used to establish a quick initial flag to indicate potential spoofing/interference.

AGC Reactions to Live Spoofing

Live RFI or spoofing experiments are quite difficult to conduct due to the global and national legislation protecting the GPS frequency band. Any such experiments tend to be conducted with significant advanced planning and in locations where the testing will have no impact on any system or application which uses GPS outside the test range. Thus, we are grateful to have been able to test the AGC detection of live transmissions in the GPS band. This was done at the Robotförsökplats Norrland test range in Northern Sweden (**FIGURES 5A, 5B, 5C**) with the support of the Swedish Defense Research Agency.

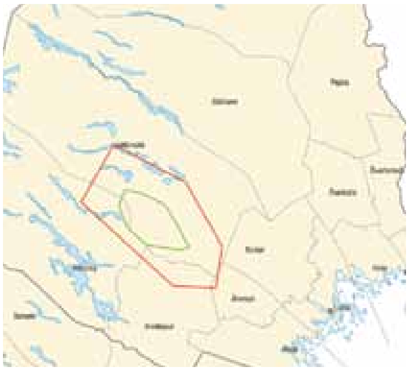
Dynamic GPS receiver measurements (position and AGC) from both the survey grade and mass market receivers were logged in the presence of repeater spoofing. Tests performed involved installing GPS antennas on the rooftop of a vehicle and driving along a 4km stretch of road toward (and away) from a hill top repeater spoofer transmission antenna while logging AGC levels and receiver positions from various GPS receivers. The data from both the survey grade and mass market receivers, used in the baseline collections, will be used here. The repeater spoofer source and transmissions antennas and the road (color shaded by elevation) used to go to/from the spoofer transmission antenna are shown in **FIGURE 6**.

The baseline receiver data was used to establish the change in AGC levels necessary to flag potential jamming, spoofing, or unintentional RFI. In order to implement the AGC flag proposed in this paper, a known fixed RF chain (antenna, cable, and front end) would be calibrated in a known non RFI environment and the mean AGC would be established. Given the baseline data collection, a mean value has been established and a 2σ threshold is set as the RFI/Spoofing flag for each receiver. When the AGC drops below this flag, the resulting position/time solution should not be trusted.

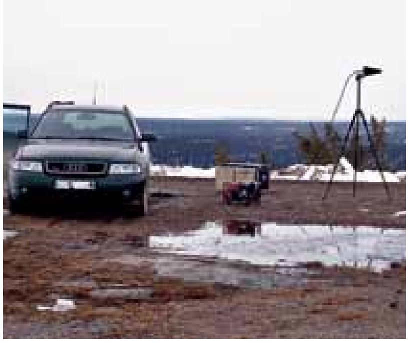


▲ **FIGURE 4B** Histogram of mass-market AGC data.

In **FIGURE 7** the measurements (AGC metric and survey receiver reported position) are shown as a function of time as the receiver is driven toward the spoofer transmission antenna. Under nominal conditions (no RFI or spoofing) one would expect a constant "safe" AGC value as well as a smooth gradual change in the reported XYZ coordinates (as the drive maintained a constant speed on the road for the duration of the test). However, as expected, due to the additional power in the GPS band, the AGC gain drops as the receiver gets closer to the repeater spoofer. At approximately 138 seconds the receiver fails to report a position and this continues for the next 30 seconds as the vehicle progresses toward the spoofer transmission antenna. At approximately 168 seconds, the survey receiver is captured and reports the fixed position of the spoofer source antenna despite continually moving toward the transmission source. Although the loss of lock and position jump could be utilized as a flag for spoofer detection, the AGC metric here clearly shows the additional power



▲ **FIGURE 5A** Robotförsökplats Norrland test range in Northern Sweden (green outline is the test range and red outline is the flight restriction area, approximate 130 x 70 kilometers).



▲ **FIGURE 5B** Repeater spoofer transmission antenna.

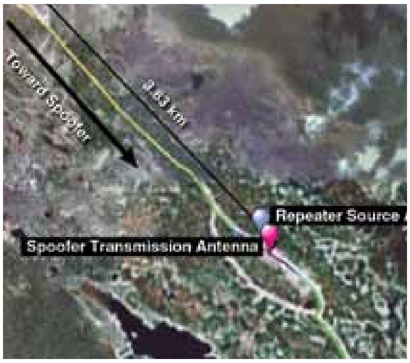
▲ **FIGURE 5C** Test vehicle.

in the band prior to any corruption of the reported GPS receiver position. If the previously computed threshold is used here, the 2σ trigger occurs as the AGC level begins to drop, significantly before any loss of lock or any change in the position solution resulting from the repeater spoofer.

FIGURE 8 shows this same data for the mass market receiver with similar observations. First, and most importantly, the AGC metric can be used here as a flag well before any corruption of the resulting position solution. The resulting position solution as the receiver becomes "captured" by the spoofer is odd, not going directly to the repeater source antenna location but also not maintaining the true position either. Likely a result of the navigation filtering coupled with individual range measurements transitioning from the true satellite measurements to that from the repeater spoofer. Nevertheless, it is clear from the AGC metric that the receiver output should not be trusted , well before any misleading information is provided.

FIGURE 9 shows AGC levels and reported positions for the survey grade receiver as it is driven away from the repeater spoofer. At the beginning, the receiver is already captured by the spoofer and reports a false fixed position solution even while the vehicle is moving. While in close proximity to the spoofer, the AGC levels are low, attempting to compensate for the additional power in the GPS band. This would be an obvious flag that the resulting position cannot be trusted (all measurements to the left of the threshold are considered untrustworthy). As the receiver is driven away and exits the spoofer's region of influence, power levels in the GPS band return to normal, the AGC reacts accordingly by increasing its gain, and the receiver begins to report accurate position solutions.

FIGURE 10 shows this same data for the mass market receiver with similar observations. The AGC metric can be used as a flag indicating the position solution cannot be trusted until the receiver is well outside the range of the repeater spoofer. In this test, the AGC level does not return to a level within the established threshold, indicating that GPS solutions should not yet be trusted. This is likely a result of an overly conservative threshold (perhaps from the poor fit of data which is not well represented by a Gaussian) or perhaps hysteresis or smoothing in the AGC metric for this receiver.



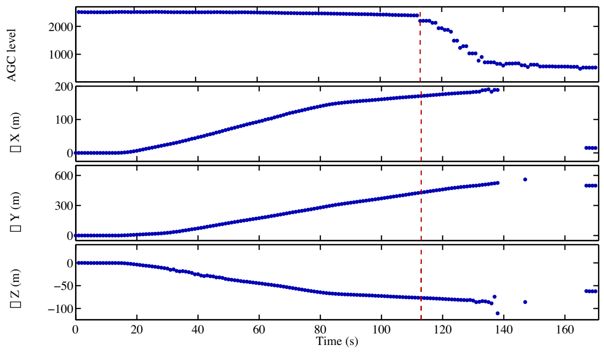
▲ **FIGURE 6** Google Earth vew of testing environment.

These cases are representative of similar repeater spoofing tests we performed: in all cases this trigger identified potential interference well before the receiver reported false positions with the simple triggers established.

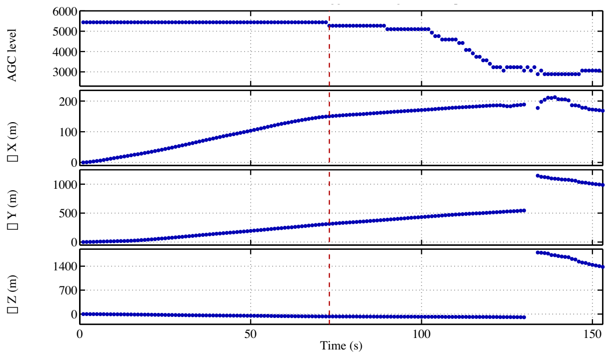
Improvements and Optimizations

These results do demonstrate the power of AGC to detect deception in GPS transmission, rendering these spoofers no more of a threat than the much less sophisticated jammers. However, the spoofer used in this testing was of a simple nature — a repeater spoofer.

The challenge would be to utilize such an approach to detect the most sophisticated spoofing attacks. This should be possible as the underlying thermal noise floor is a physical constant and in order for a receiver to be spoofed additional energy must enter the RF chain which, again, should be detectable. The optimization will come in via establishing thresholds – similar to GPS signal acquisition/detection. One will not want to set such a loose threshold such that frequent false alarms provide little confidence in the resulting position/time solution. Likewise one would not want to establish threshold so loose that the more sophisticated spoofing attacks would be successful. The key is the calibration and assessment of the underlying AGC measurement.



▲ **FIGURE 7** Survey-grade RX AGC/position during drive toward spoofer.



▲ **FIGURE 8** Mass-market RX AGC/position during drive to spoofer.

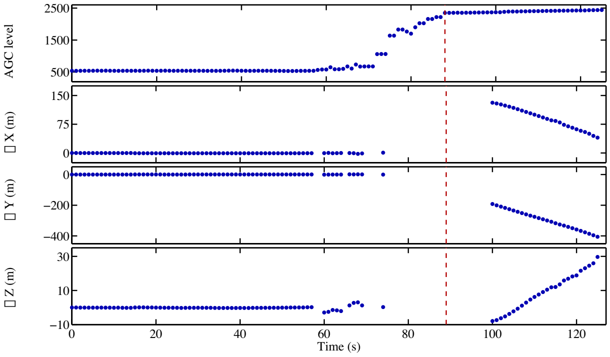
Recall the variation observed in the survey grade receiver data. Was this truly random noise that one must overbound as was done to establish the threshold for the experiments in this paper? And why were the noise levels so different for the baseline AGC collections in the survey grade and mass market receiver? We try to address both of these questions to provide a bit of insight into the advantages and shortcomings of the AGC metric.

First, the AGC measurement across receivers is not equal. In comparing these two receivers, the survey grade receiver has a much higher resolution measurement than that of the mass market receiver. This is obvious from the baseline data which showed little deviation from specific quantized levels in the mass market AGC metric. So although the great majority of GPS receiver already have/report their AGC measurement it may not be of sufficient fidelity for the most sophisticated spoofer detection.

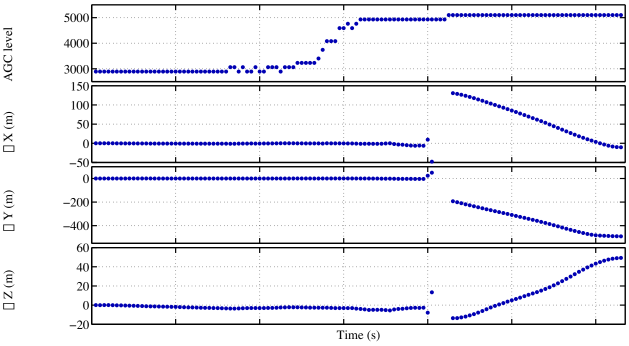
Second, high resolution provides little benefit in a noisy measurement. So there is a pending question if there is a source for the variation in the AGC measurement for the survey grade receiver during the 72 hour baseline data collection – or was it simply a noisy measurement. Past work in this area led to the association of ambient temperature and the AGC measure, but perhaps not in the way one would initially think. Yes, the thermal noise level is dependent on temperature (from kTB), as well as bandwidth and Boltzmann's constant, but this is really antenna temperature and in this case the correlation is with ambient temperature.

The baseline AGC levels were compared to changes in ambient temperatures in Boulder during testing to determine if observed fluctuations were related to temperature. The weather data were gathered in Broomfield, approximately 10 miles from CU; thus plotted temperatures do not exactly reflect the air temperature at the antenna. However, the data do reflect a correlation between approximate ambient temperature and AGC gain, shown in **FIGURE 11A, B, AND C**.

Why does this correlation exist? Why, when the temperature increases, must the gain of the receiver also increase? That may initially appear to be counter intuitive in that one may think higher temperature would result in higher thermal noise. Again, it is important not to confuse antenna temperature and ambient temperature which is the basis for the thermal noise floor. Why then must the receiver provide more gain with higher ambient temperatures? The validated hypothesis is that the antenna is an active design with an internal low noise amplifier. The gain, or really efficiency, of this amplifier is dependent on its temperature (and it is quite small, on the order of a dB). So as the ambient



▲ **FIGURE 9** Survey-grade RX AGC/position during drive from spoofer.



▲ **FIGURE 10** Mass-market RX AGC/position during drive from spoofer.

temperature increases the efficiency of the amplifier in the antenna decrease so the receiver is required to put more gain into the RF chain to accommodate.

This temperature correlation is an attempt to illustrate the power of the AGC metric and its potential sensitivity for detection. Other triggering methods, such as comparing current AGC levels with a moving average of previous values, could be implemented depending on desired performance. If such changes can be incorporated and/or calibrated out, we expect the most sophisticated spoofers could be detected coupled with a low false alarm rate.

Conclusion

A trigger based on the AGC, a measure available in a majority of GPS receivers, has been proposed that indicates the presence of potential signal spoofing prior to a compromise in receiver positioning. This proposed trigger is an effective tool for current GPS receivers to establish a low computational complexity measure of confidence of the reported position solution, and may complement other spoofing detection methods. The triggering mechanism may be adapted according to desired sensitivity in AGC changes, thereby either reducing the false alarm rate, or providing a conservative flag of potential RFI. Upon receiving such a flag, other navigation sources may be consulted to determine position, or the trust in the GPS solution may simply be lowered. Thus spoofing would be no more of a threat to satellite navigation/timing receivers than the much less sophisticated jamming.

Acknowledgments

Our thanks to the Robotförsökplats Norrland test range in Northern Sweden and the Swedish Defense Research Agency, particularly, Peter Johanson and Mickael Alexandersson (provided many of the photographs), for supporting the experiment.

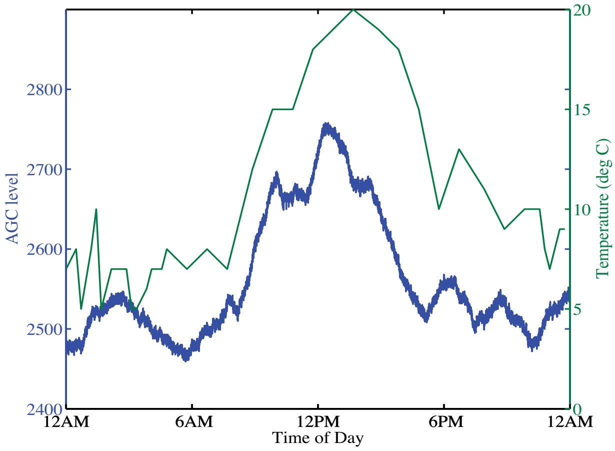
HOLLY BOROWSKI is a Ph.D. student working in the Research and Engineering Center for Unmanned Vehicles at the University of Colorado-Boulder. Her research involves unmanned vehicle path planning for information gathering in uncertain environments.

OSCAR ISOZ is a Ph.D. student at Luleå University of Technology. He has studied GPS interference detection and localization and is now focusing on radio occultation.

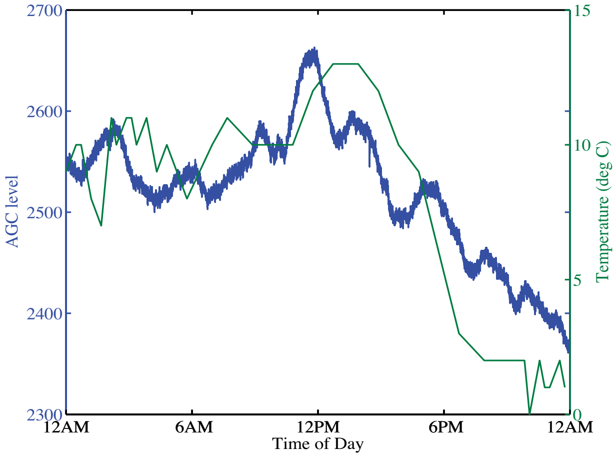
FREDRIK MARSTEN EKLÖF is the project manager for NAVWAR research at the Swedish Defense Research Agency.

SHERMAN LO is a senior research engineer at the Stanford GPS Laboratory. He is the associate investigator for the Stanford University efforts on the FAA evaluation of alternative position navigation and timing (APNT) systems for aviation.

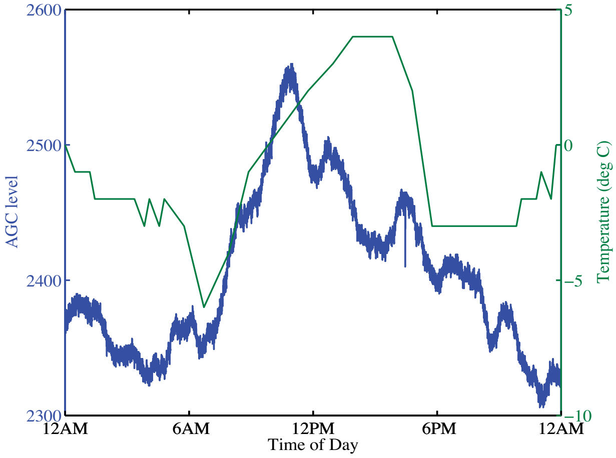
DENNIS AKOS is an associate professor with the Aerospace Engineering Sciences Department at the University of Colorado as well as a consulting associate professor with Stanford University and a visiting professor with Luleå University of Technology.



▲ **FIGURE 11A** AGC measure (survey-grade RX) and ambient temperature, Day 1.



▲ **FIGURE 11B** AGC measure (survey-grade RX) and ambient temperature, Day 2.



▲ **FIGURE 11C** AGC measure (survey-grade RX) and ambient temperature, Day 3.