Single Antenna GPS Spoof Detection that is Simple, Static, Instantaneous and Backwards Compatible for Aerial Applications

Emily McMilin, David S. De Lorenzo, Todd Walter, Thomas H. Lee, Per Enge
Stanford University, USA

BIOGRAPHY

Emily McMilin is a Ph.D. candidate under Professor Per Enge in the Stanford GPS Research Laboratory. She completed her B.S. at Stanford in Symbolic Systems and her M.S. in Electrical and Computer Engineering at the University of Victoria in British Columbia. Prior to returning to Stanford for her Ph.D. in Electrical Engineering, Emily was an Antenna Engineer at Apple for 2.5 years. In addition to GPS antennas, Emily is interested in GPS applications for developing regions.

David S. De Lorenzo is a Principal Research Engineer at Polaris Wireless and a consulting Research Associate to the Stanford GPS Laboratory. His current research is in adaptive signal processing, software-defined radios, and navigation system security and integrity. He received the Ph.D. degree in Aeronautics and Astronautics from Stanford University and previously has worked for Lockheed Martin and for the Intel Corporation.

Todd Walter is a Senior Research Engineer in the Department of Aeronautics and Astronautics at Stanford University. He received his Ph.D. in 1993 from Stanford University. His current activities include defining future architectures to provide aircraft guidance and working with the FAA on the implementation of dual-frequency WAAS. Key early contributions include: prototype development proving the feasibility of WAAS, significant contribution to WAAS MOPS, and design of integrity algorithms for WAAS. He is a fellow of the ION and served as its president.

Thomas H. Lee received the S.B., S.M. and Sc.D. degrees in electrical engineering, all from the Massachusetts Institute of Technology in 1983, 1985, and 1990, respectively. Since 1994, he has been at Stanford University. He served for a decade as an IEEE Distinguished Lecturer of the Solid-State Circuits Society, and has been a DL of the IEEE Microwave Society as well. He holds over 60 U.S. patents and authored The Design of CMOS Radio-Frequency Integrated Circuits, and Planar Microwave Engineering. He is a co-author of four additional books on RF circuit design, and also cofounded Matrix Semiconductor (acquired by Sandisk in 2006). He is the founder of ZeroG Wireless, a cofounder of Ayla Networks, and is a past Director of the Microsystems Technology Office at DARPA. In early April of 2011 he was awarded the Ho-Am Prize in Engineering (colloquially known as the "Korean Nobel") for his work on CMOS wireless.

Per Enge is a Professor of Aeronautics and Astronautics at Stanford University, where he is the Kleiner-Perkins Professor in the School of Engineering. He directs the GPS Research Laboratory, which develops satellite navigation systems based on the Global Positioning System (GPS). He has been involved in the development of WAAS and LAAS for the FAA. He has received the Kepler, Thurlow and Burka Awards from the ION for his work. He is also a member of the National Academy of Engineering and a Fellow of the IEEE and the ION. He received his Ph.D. from the University of Illinois in 1983.

ABSTRACT

Despite the antenna's privileged position as the first line of defense against interferers, jammers and spoofers, most detection and mitigation techniques are realized in the receiver's backend signal processing blocks. Nonetheless, these solutions often require considerable additional hardware added to the receiver's frontend and antenna design. For example, multi-antenna arrays replace a single antenna design for the purpose of detection/mitigation of interference, jamming [1] and spoofing [2] [3]. Among the single antenna detection/mitigation designs, some form of antenna movement over time is required. For example, the use of a synthetic aperture [4] and the generation of high frequency antenna motion [5] has been proposed for spoof

detection/mitigation. All of the aforementioned innovations utilize additional signal processing blocks in the backend, in conjunction with the supplemented frontend hardware, to achieve their intended goals.

A primary technique for achieving this type of adaptability in sub-wavelength single antenna systems is the use of discrete circuit components on or near the antenna element [6]. Circuit components manipulating signals in the RF domain can achieve analog "signal processing" directly on the antenna, essentially eliminating additional computational complexity. However, signal processing in the digital domain often affords far more flexibility and applicability. The primary limitation of this design is that the spoof-detection technique is most effective when spoofed signals are originating from a source below the antenna, thus limiting its applicability to predominantly aerial implementations. Nonetheless, we feel this solution is well suited to the form-factor and payload constraints that aerial applications such as commercial aviation and UAVs demand. Additionally, we introduce some techniques for extending the applicability of this design.

In our design we simply add an electronic switch inside the radome of the antenna that permits high speed switching from the default radiation pattern that is predominantly right-hand circularly polarized (RHCP) to one that is predominantly left-hand circularly polarized (LHCP), in the upper hemisphere of the antenna. However, at very low angles of elevation and generally below the antenna, the radiation pattern is neither predominantly RHCP or LHCP [7], so the switching has little effect on the radiation pattern at all. We can exploit this expected telltale drop in the received SNR or C/N_0 to identify if the signal is originating from above the antenna or from below it, and thus, if the signal is genuine or spoofed.

INTRODUCTION

Direct signals from GPS/GNSS satellites RHCP and arrive in the upper hemisphere of a standard GPS/GNSS receive antenna on earth. Thus, GPS/GNSS receive antennas are designed for sensitivity to only RHCP signals and only in the upper hemisphere. In practice, all antennas have some sensitivity to LHCP signals. The total sensitivity of the antenna is sum of the RHCP and LHCP sensitivities. A performance metric measuring the antenna's ability to distinguish the RHCP energy from the total energy it receives is called "cross-polarization discrimination" (XPD), and is defined as

$$\frac{\text{RHCP gain or sensitivity}}{\text{LHCP gain or sensitivity}} \tag{1}$$

for each potential signal direction of arrival (DoA). GPS antennas are designed to maximize XPD in the upper hemisphere, because the presence of any upper hemispheric LHCP sensitivity proportionately reduces the antenna's sensitivity to the satellite's RHCP signals. However, there is no design constraint to maximize XPD in the lower hemisphere. Rather, standard GPS antennas are also designed to minimize all lower hemispheric sensitivity, without regard to polarization. Not only does lower hemisphere sensitivity correspondingly reduce upper hemisphere sensitivity, but it also exposes the antenna to detrimental multipath and other harmful signals. This lower hemisphere sensitivity is called back-lobe radiation. A standard metric for quantifying the back-lobe sensitivity of GPS antennas is called the "multipath rejection" (MPR) ratio, defined as:

$$\frac{\text{RHCP gain in upper hemisphere}}{(\text{LHCP gain} + \text{RHCP gain}) \text{ in lower hemisphere}} \tag{2}$$

Note that electromagnetic radiation is elliptically polarized (EP) in its most general form, where EP radiation is any combination of RHCP and LHCP radiation, so we could replace the denominator in Equation 2 with "EP gain in lower hemisphere".

The antenna we introduce in this paper exploits this "nuisance" back-lobe radiation for the detection of GPS spoofers. Specifically, the technique utilizes the fact that most GPS antennas have a large XPD ratio in the upper hemisphere, and a relatively small XPD ratio in the lower hemisphere. Thus, this often derided, yet unavoidable back-lobe radiation becomes our ally.

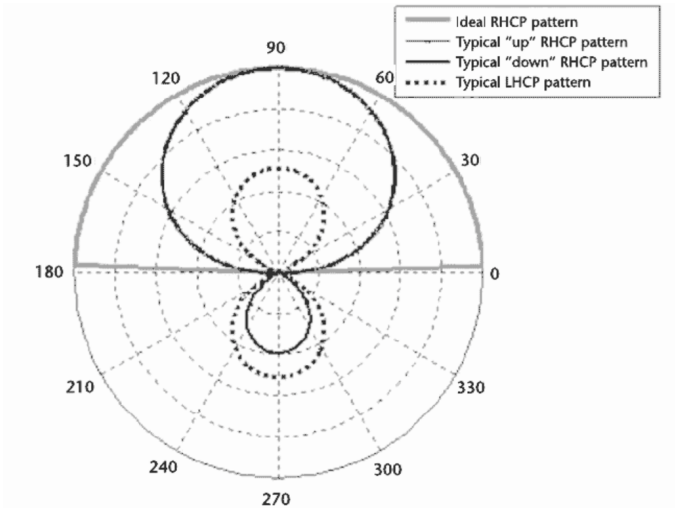

Fig. 1: Typical RHCP (solid line) and LHCP (dashed line) radiation patterns. Source: [7].

Typical relative values for RHCP and LHPC radiation patterns in both lobes are shown in Figure 1 [7]. Note that while RHCP sensitivity is much greater than LHCP sensitivity in the upper hemisphere (in other words the XPD ratio is many dB), in the lower hemisphere the RHCP sensitivity is approaching that of the LHCP sensitivity (the XPD ratio is usually just several dB).

Generally, little attention is afforded to the back-lobe's characteristics, other than the desire that its total sensitivity be as small as possible. Often radiation pattern plots exclude the back-lobe entirely. In part, this is because it is difficult for antenna manufacturers to provide meaningful metrics about the back-lobe's performance in practice. Unlike the antenna's front-lobe, the environment around the antenna's back-lobe is far from pristine, and the random nature of these disturbances cause any polarization purity to also be disturbed. For example, the presence of conductive objects such as mounting fixtures or an airplane fuselage that are co-planar or below the antenna's ground plane, will have a significant effect on the back-lobe's sensitivity and polarization. We will discuss this phenomenon further in a later section. Figure 2 show RHCP and LHCP patterns on the fuselage of a scaled-down F-16 jet [8]. Note the very small values for the back-lobe XPD ratio.

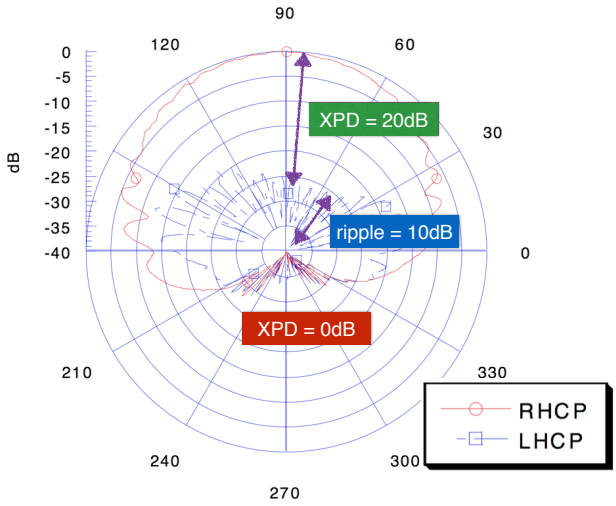

Fig. 2: Measured radiation patterns on an F-16 scale model of a single element on airplane fuselage. Source: [8].

While the total back-lobe radiation could be sufficiently minimized to ameliorate most multipath concerns, it could never ameliorate spoofing concerns. In the face of even very low back-lobe sensitivity, for example an MPR ratio of 30 dB, a spoofer need simply increase their transmit gain such that the signal power incident on the back-lobe of the antenna is only several nano-watts, in order to reasonably overcome the GPS satellite signals.

In this paper it is our preference to defer to measurement data from existing typical GPS antenna designs. We want to exploit only the existing qualities of standard GPS antennas, in our effort to achieve a backwards-compatible design. This is in recognition of the fact that even simple GPS antennas are optimized for performance given an existing body of constrains, and the introduction of any new constraint will inevitably require trade-offs and a resulting performance degradation.

FRONTEND DESIGN AND SIMULATION

RHCP signals are generated by exciting two linearly polarized electromagnetic fields that are separated by 90° both in space and in time. Despite the single feed between the radio and the antenna, GPS antennas may in-fact have several ports inside of the antenna radome. Typical GPS antennas including patch antennas, quadrifilar helix antennas, and crossed bow tie antennas may all have multiple internal ports, and thus will be compatible with the design proposed in this paper. A 3-D CAD of a basic patch antenna is shown in Figure 3. The 90° separation in space is achieved with two orthogonal ports and the associated electromagnetic fields, indicated as the "x-axis" and "y-axis" ports and fields.

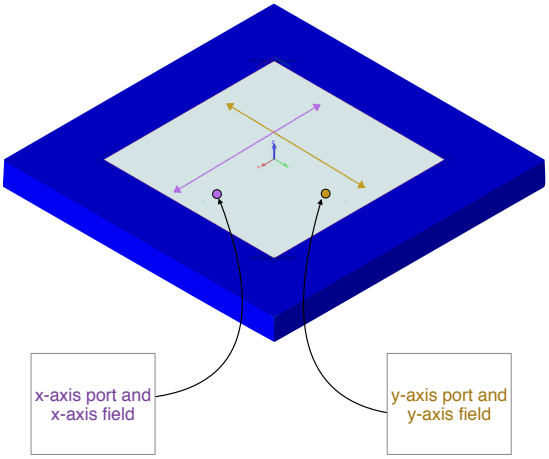

Fig. 3: 3-D CAD of a basic patch antenna with two orthogonal feed ports.

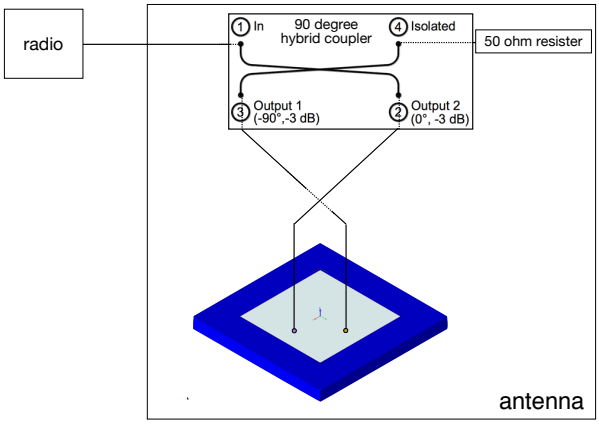

Fig. 4: Block diagram for a standard two port GPS patch antenna.

The 90° separation in time can be achieved by various techniques including the insertion of a 90° hybrid coupler in the signal path. These couplers are available as commercial off the shelf (COTS) parts, several square mm in dimension

and could be included inside the antenna radome as shown schematically in Figure 4. The single transmission line entering the antenna's radome is fed to a 90° coupler which splits the signal into two transmission line feeds, with equal magnitude but differing phase by 90°. One feed is attached to the y-axis port and the other feed is attached to the x-axis port of the antenna. In the nominal set up, the y-axis field lags the x-axis field by 90°, due to the insertion of the coupler in the signal path. This 90° lag in the antenna's y-axis field results in sensitivity to predominantly RHCP radiation in the upper hemisphere. For example, given a good XPD ratio of 20 dB, the antenna is 100 times more sensitive to RHCP signals than LHCP signals.

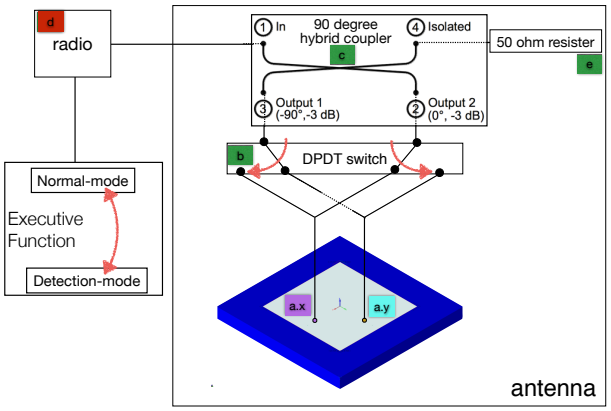

Fig. 5: Block diagram for our GPS spoof detection patch antenna.

In our design we only add a switch in the signal path (as shown in Figure 5) and some "executive function" to control the switch. The elements of interest have been labeled with markers from a to e, and those of most interest are marked with unique colors, specifically, $a.x$ and $a.y$ which are the two ports feeding the linearly polarized fields of the antenna, and d which is the port feeding the radio.

As we detail later, the switch can be implemented with cell phone industry COTS components and the executive function can implemented as a human operator or a simple control algorithm. The switch serves to dynamically change the upper hemisphere radiation from predominantly RHCP to predominantly LHCP. Specifically, when the switch is flipped from "normal-mode" to "detection-mode" the 90° phase lag is now inserted in the x-axis signal path. Now, with the x-axis field lagging the y-axis field by 90°, and the antenna is predominantly sensitive to LHCP radiation in the upper hemisphere. Figure 6 shows a rough depiction of radiation patterns with normal-mode on the left and detection-mode on the right. The figure shows that in detection-mode, the RHCP signal is swapped with the LHCP one, so we'd now find the antenna is 100 times less sensitive to RHCP signals than LHCP signals, assuming an XPD of 20 dB. Thus, when the antenna is flipped to detection-mode, we'd expect the SNR or C/N_0 reported by the receiver to reduce by 20 dB for genuine GPS signals.

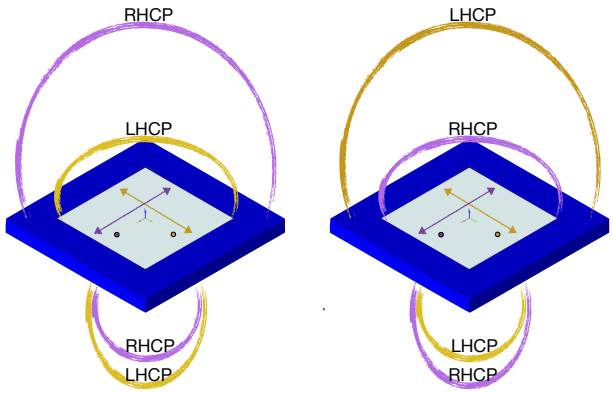

Fig. 6: Rough depiction of radiation patterns with normal-mode on the left and detection-mode on the right.

Alternatively, as Figure 6 indicates, the RHCP and LHCP back-lobe radiation patterns do not change drastically when switching between normal-mode and detection-mode due to the smaller XPD ratio in the back-lobe. For optimal spoof-detection, we would prefer a XPD in the back-lobe that is approaching 0 dB. As noted ealier, as more conductive objects are placed near or below the antenna, the XPD ratio does in fact tend toward 0 dB. This phenomenon can be due to random scattering energy off these nearby objects [8]. Additionally, at low angles of elevation, one of the two orthogonal fields (what we called the x-axis field or the y-axis field at boresight) will tend toward vertically polarized while the other tends toward horizontally polarized, relative to the patch. If the patch is located on a large ground plane, such as the body of an airplane, the horizontal field component will now be parallel to the conductive body of the airplane and will quickly dissipate, resulting in an XPD ratio equal to 0 dB [7]. Thus, when the antenna is flipped to detection-mode, we'd expect the SNR or C/N_0 reported by the receiver to remain largely unchanged for spoofed signals, regardless of the spoofer's choice of signal polarity (RHCP, LHCP, linearly polarized or EP), as long as the signal is originating from below the antenna.

Figure 7 is a schematic representation of the block diagram we saw in Figure 5, shown Agilent's Advanced Design System (ADS) software environment. ADS can simulate the high frequency response of this schematic, and generate S-parameter data at each exposed port. Again we see markers from a to e, representing the components of the schematic, consistent with Figure 5, where the two ports feeding the antenna are $a.x$ and $a.y$, and the port feeding the radio is d. This schematic uses manufacturer measured S-parameter data for the switch (Skyworks SKY13381-374LF) and 90° hybrid coupler (Anaren C1517J5003AHF). Both parts are a couple mm in size and cost less than one dollar for small

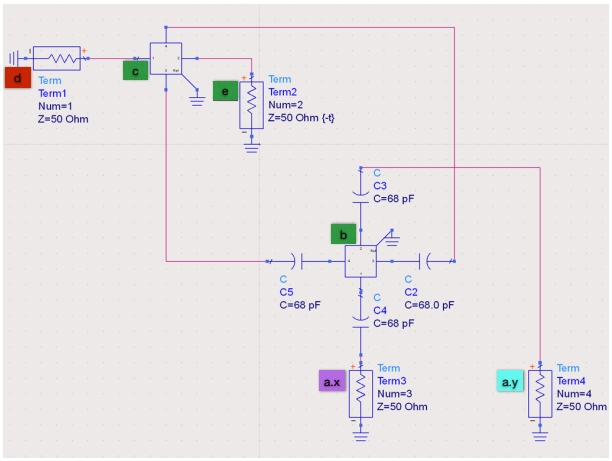

Fig. 7: ADS schematic representation of the block diagram from Figure 5.

quantity purchases.

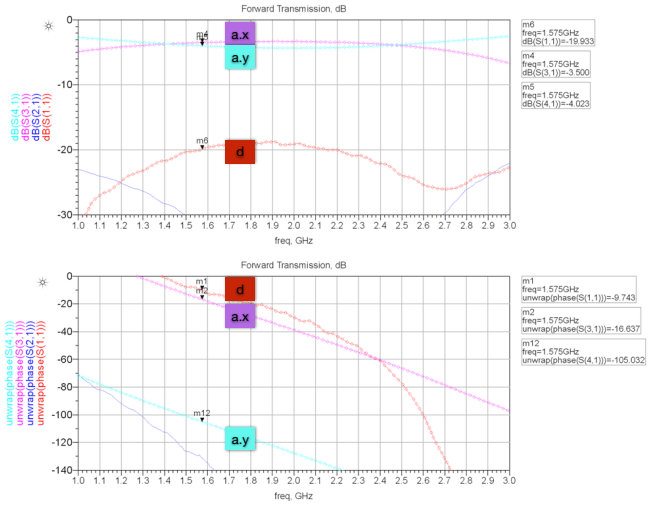

Fig. 8: S-parameter data (magnitude on top and phase on bottom) from ADS simulation of schematic in Figure 7 with switch in normal-mode.

Figure 8 and Figure 9 shows the simulated measurement results for the schematic, when the circuit is switched to normal-mode and detection-mode, respectively. The upper diagrams show the magnitude response of ports $a.x$, $a.y$ and d (x-axis port, y-axis port, and radio port) and the lower diagrams show the phase response of these ports. Note that the relative magnitudes of port $a.x$ and port $a.y$ are similar and essentially unchanged when switching between normal-mode and to detection-mode; however the relative phase differences change by 180°. Of importance, both the phase and the magnitude seen at port d (the GPS receiver) remain essentially unchanged while switching between modes. Additionally, inspection of the magnitude response at 1.575 GHz for ports $a.x$ and $a.y$ show that the insertion loss for the switch and hybrid coupler combined

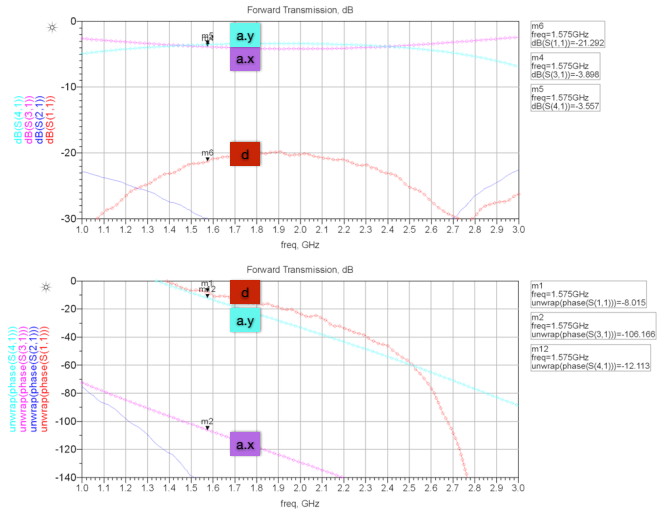

Fig. 9: S-parameter data (magnitude on top and phase on bottom) from ADS simulation of schematic in Figure 7 with switch in detection-mode. Note that when compared to Figure 8 the phases of $a.x$, $a.y$ swap but their magnitude stay the same, and that the phase of the radio (port d) is the same despite switching.

is only about 0.7 dB.

ANTENNA DESIGN AND MEASUREMENT

In order to test the spoof detection concept for various signal direction of arrivals (DoAs), we needed "typical" antenna radiation pattern measurement data, including both RHCP and LHCP full back lobe patterns. It was not easy to find high resolution data to this detail, so we decided to try to make our own typical GPS patch antenna and conduct our own measurements. Specifically, we strived to achieve typical upper/lower hemisphere gain patterns, typical XPD, and typical size (ARINC 743 compatible). As we noted before, a simple and typical antenna design was desirable because we are interested in a general solution that is consistent with the existing requirements for simple GPS antennas.

The antenna we constructed, shown in Figure 10, was built on a 73 mm by 73 mm by 5 mm block of Rogers TMM4 ceramic with a dielectric constant of 4.7. The x-axis and y-axis feed are connected to an external 90° hybrid coupler, which we intend to replace with a smaller internal component (Anaren C1517J5003AHF). We then performed anechoic chamber measurement with facilities and support donated by Space Systems/Loral. The measured radiation pattern in normal-mode is shown in Figure 11 with worst-case upper and lower hemisphere XPD annotated. Additionally the radiation pattern in detection-mode is shown in Figure 12 without annotation, where we have performed an ideal 180° switch in post-processing.

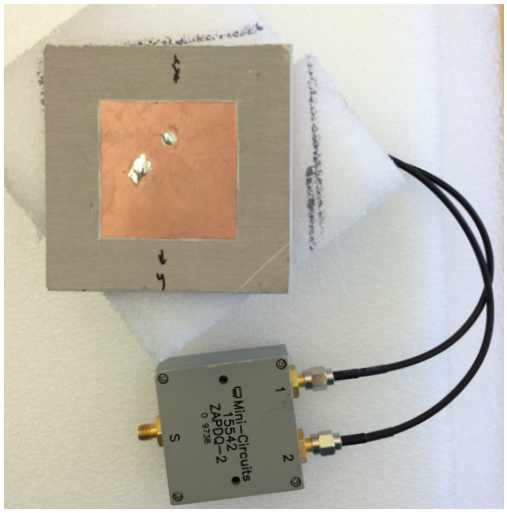

Fig. 10: Two port antenna we built on a 73 mm x 73 mm x 5 mm block of Rogers TMM4 ceramic with a dielectric constant of 4.7, attached to external 90° hybrid coupler for measurement.

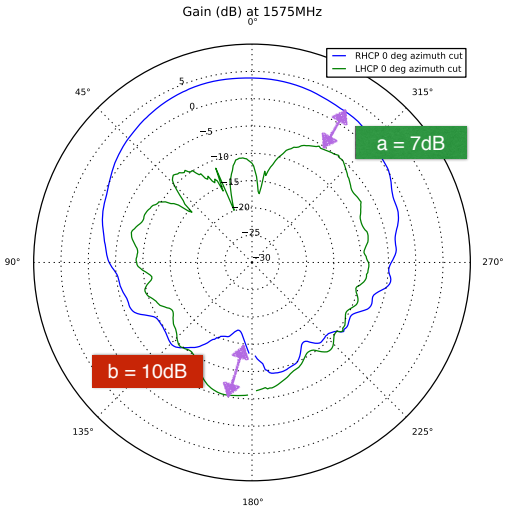

Fig. 11: Measured radiation pattern in normal-mode.

As can be inferred from our measured data, we found that building a typical, simple GPS antenna is not very simple at all. Particularly the poor XPD ratio of 7 dB at a high elevation in the upper hemisphere was disappointing, as typical antennas can often out perform that value by 8 dB to 13 dB. However, our prototyping tools consisted of a scalpel and copper tape, and surely lacked the precision desirable for improved performance.

SYSTEM SIMULATION AND RESULTS

Having obtained a form-factor compatible antenna design, we now desired integration with a GPS receiver in a backward compatible fashion. Our ideal integration process would be only the connection of the existing GPS receiver

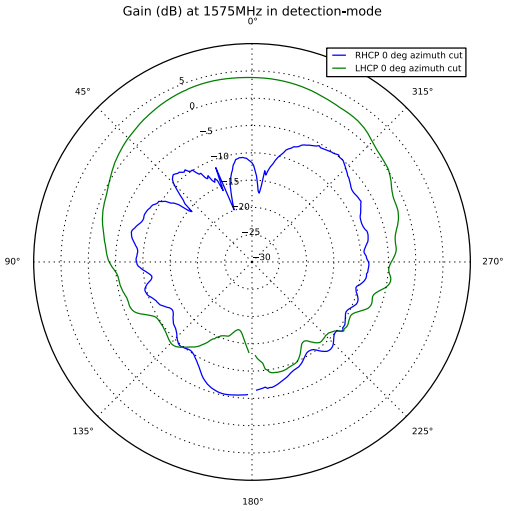

Fig. 12: Measured radiation pattern in detection-mode, achieved in post processing with the insertion of an ideal 180° phase delay.

to this new antenna. As we discuss later in this section, an additional simple circuit must be inserted between the RF cable and the radio for remote control of the antenna. However other than this simple circuit and the simple antenna, our method requires no further additions to the receiver systems. Instead we exploit only a minimum required set of existing functionality blocks in the receiver. This requires our design to report spoof-detection results using the existing reporting framework inherent to the receiver such as C/N_0 or SNR.

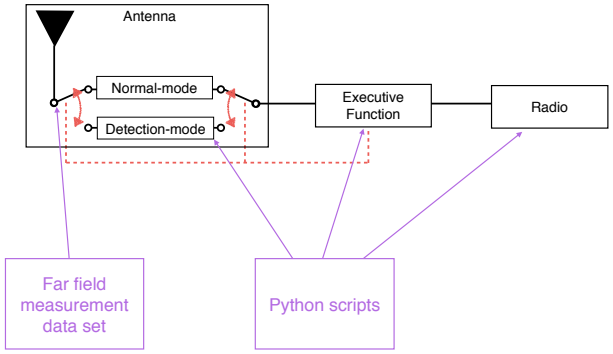

Fig. 13: High-level block diagram representation of system simulation and implementation method.

Figure 13 shows a high-level block diagram representation of the system simulation with the hybrid coupler and switch abstracted into a single switching block. The executive function block includes a control line carrying a DC voltage, to trigger the different modes of the switch. The DC voltage switching logic can be multiplexed onto the RF cable connecting the radio to the antenna, and thus no additional cables are needed between antenna and ra-

dio receiver. Unlike the schematic representation in Figure 5, here we see the executive function block in between the radio and the antenna. In this case the executive function can be implemented with a simple circuit, ideally not much larger than an RF barrel connector. This added circuit is for the purposes of placing the DC voltage onto the inner conductor of the RF coaxial cable and would consist of a small battery, an exposed switch or dial, an RF choke and DC blocking capacitor. For additional control functionality the dial must be connected to a basic logic circuit that translates the dial's setting to the percentage of time the switch remains in detection-mode. At this time, the receiver, executive function and switching blocks are implemented with python scripts and the antenna block is implemented with the data set from our radiated pattern measurement.

All signals are simulated by looking up the measured antenna gain value for a given DoA. If the DoA is above the horizon, then we label the associated signal as a GPS signal. If the DoA is below the horizon, we label it as a spoofed signal. We have assumed an intelligent spoofer that has selected a transmit power level that reasonably over powers the signals coming from GPS satellites. We use two polarizations for the spoofer, as all other polarizations are a combination of RHCP and LHCP, and try various DoAs.

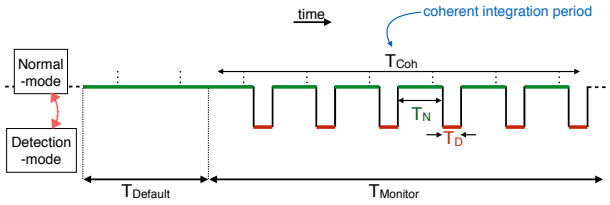

Fig. 14: Time-domain representation of an example switching scenario between normal-mode and detection-mode.

Figure 14 shows a time-domain representation of how the executive function may implement switching between the two modes. Initially, Figure 14 shows the system in a default-state that lasts a duration of $T_{Default}$ seconds, during which the antenna remains in normal-mode. Next, the system enters a monitor-state where the antenna switches between normal-mode and detection-mode for a duration of $T_{Monitor}$ seconds. For the particular monitoring duration show in Figure 14, the antenna has a normal-mode integration period (T_N) that is larger than the detection-mode integration period (T_D), and also note that $T_N + T_D$ is much smaller than the total coherent integration period (T_{Coh}). However $T_N + T_D$ can also be about equal to T_{Coh}, because $T_{Monitor}$ can last for many cycles of T_{Coh}, thus averaging out any potential timing mis-alignment between the switching states of $T_N + T_D$, and T_{Coh}. There can also be the case where $T_N + T_D$ is much larger than T_{Coh}. This last scenario should only be used when the operator is not concerned about cycle slips.

In general, if there is concern of losing carrier lock for some satellites, the ratio of $\frac{T_D}{T_N+T_D}$ should be set conservatively. Of course, if a response characteristic of a spoofer is initially detected with a conservative $\frac{T_D}{T_N+T_D}$ ratio, the operator may decide that potential cycle slips is a reasonable trade-off for improved confidence in spoof detection. Finally, the operator can choose how often to check for spoofing, but it is quite likely that in most use cases the antenna will remain in the $T_{Default}$ state the majority of the time and only enter $T_{Monitor}$ for brief periods of time.

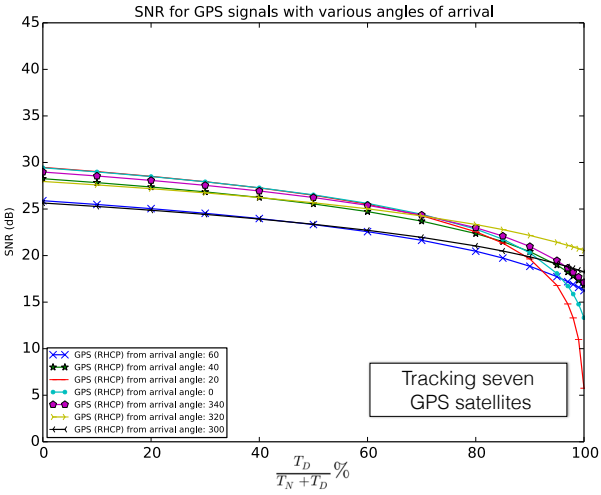

Fig. 15: Reduction in SNR reported by our simulated GPS receiver as percentage of time allocated to detection-mode (T_D) increases, for seven signals with DoAs in the upper hemisphere (from 60° - 300°).

As explained above, due to the antenna's decreased sensitivity in the upper hemisphere during detection-mode, we would expect the magnitude of the SNR or reported C/N_0 to drop linearly as the amount of time spent in detection-mode increases. Thus, when there is no spoofer present, the values for the SNR or C/N_0 (in dB) will drop logarithmically as $\frac{T_D}{T_N+T_D}$ increases. This response can be seen for seven signals with DoAs in the upper hemisphere (from 60° to 300°) in Figure 15. The y-axis of this plot shows the SNR values that we would expect the GPS receiver to report at any given time, for each satellite. The x-axis shows the percentage of time that the antenna is in detection-mode. To improve the confidence in the reported value, an exposed dial in the executive function module can allow the operator (or algorithm) to increase this percentage, thereby further increasing the measurable difference between a spoofer's presence and absence. The trade-off for increased spoof-detection confidence is a reduction in SNR during $T_{Monitor}$. Finally, note that it is only because the signals are originating from the upper hemisphere, that we label them as genuine GPS signals in the legend.

If a spoofer is present, the SNR will stay relatively flats as $\frac{T_D}{T_N+T_D}$ increases, as can be seen in Figure 16. In this

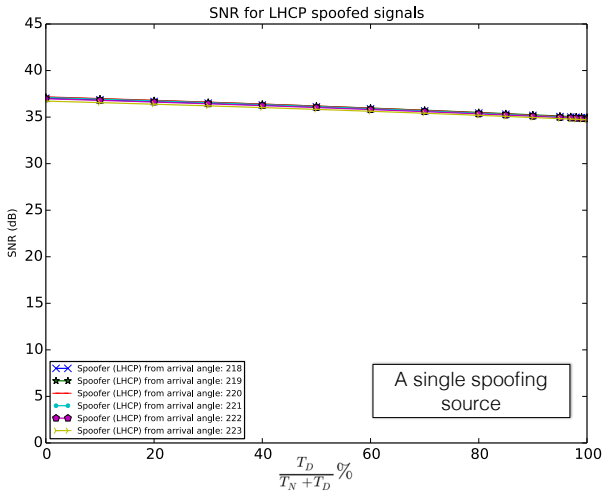

Fig. 16: Flat response in SNR reported by our simulated GPS receiver as percentage of time allocated to detection-mode (T_D) increases for a spoofer transmitting seven LHCP signals from a single DoA around 220°.

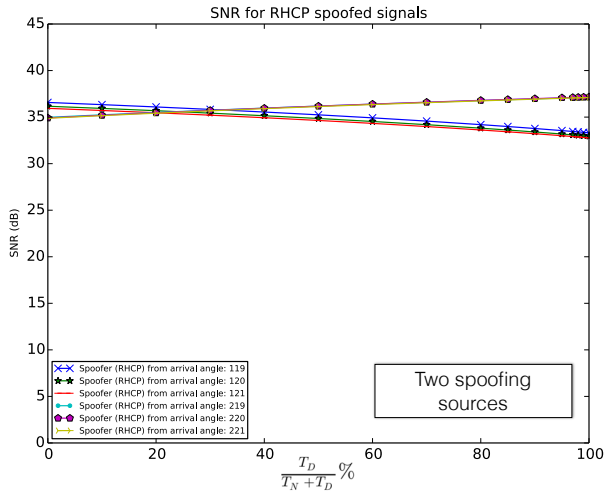

Fig. 17: Flat responses in SNR reported by GPS our simulated receiver as percentage of time allocated to detection-mode (T_D) increases for a spoofer transmitting seven RHCP signals from two DoAs around 120° and 220°.

case, seven signals are originating from about the same DoA of 220°. Because the signals are originating from the lower hemisphere, we indicate them as spoofed signals in the legend, however, their SNR response alone exposes them as non-genuine signals to the operator of the GPS receiver. Specifically, as a first order effect, we note that the SNR is not rapidly decreasing as $\frac{T_D}{T_N+T_D}$ increases, and we use this response to correctly label these signals as originating from a spoofer. Figure 17 shows the case of two spoofed sources, which are originating from DoAs below the horizon at about 120° and 220°, and as expected the SNR stays relatively unchanged as $\frac{T_D}{T_N+T_D}$ increases, detecting the spoofed origin of these signals. Also note Figure 17 shows the scenario where the spoofer happens to use a RHCP source, whereas Figure 16 assumes a LHCP source. This spoof detection technique is effective for all polarities of spoofed signals that originate from DoAs below the horizon.

However, we can also see that in the case of the solitary (or several) spoofer(s), we can rely on other signatures specific to authentic GPS signals that are not present due to a single spoofed source. As we saw in Figure 15, there is a distinct trace that exhibits a unique response for each satellite that is coming from a different DoA (for which we see unique XPD and antenna gain values). On the contrary, for the single (or several) spoofed source, we expect to see non-unique responses for multiple satellites, as was shown in Figure 16 and Figure 17. This technique will work regardless of whether the spoofed signal is originating in the upper hemisphere or the lower hemisphere and expands the possible applicability of this design to beyond aerial applications alone.

MODIFIED SYSTEM SIMULATION AND RESULTS

In the prior section we saw that spoof detection can be achieved by observing the unique characteristics of how each signal's SNR drops as the percentage of time allocated to detection-mode increases. However, we advertised this solution as instantaneous and simple, which the above method is not.

For true backwards compatibility, we would prefer that an operator or algorithm just quickly look at the GPS receiver's reported SNR's or $C/N_0's$, and instantly detect whether or not spoofing is taking place. Specifically, the operator (or algorithm) conducts a monitoring session, and immediately the receiver should report SNR's or $C/N_0's$ that have dropped by about 15 dB to 20 dB (equivalent to the XPD ratio for each satellite's DoA). If there is concern about losing carrier lock, the ratio of $\frac{T_D}{T_N+T_D}$ can be adjusted to a lower percentage, and the magnitude of the SNR decrease will only drop by that percentage. However, because our home-built antenna has an XPD ratio of only 7 dB at some high elevation angles, this technique will not achieve the compelling drop in SNR performance required for easy spoof identification.

To show the expected simplicity of this detection technique, we look back toward the earlier antenna radiation patterns we saw in Figure 2. We seek to compensate our poorly performing home-built antenna by modifying its radiation patterns to more closely resemble this one. Specifically, we reduce the LHCP pattern of our measured data (from Figure 11) by 5 dB, as shown in Figure 18, such that the upper hemisphere XPD becomes 13 dB at 320° and the

lower hemisphere XPD begins to approach 0 dB in some locations. We again repeat the simulations of the above section, but this time look at seven spoofed sources with DoAs ranging from 120° to 240° .

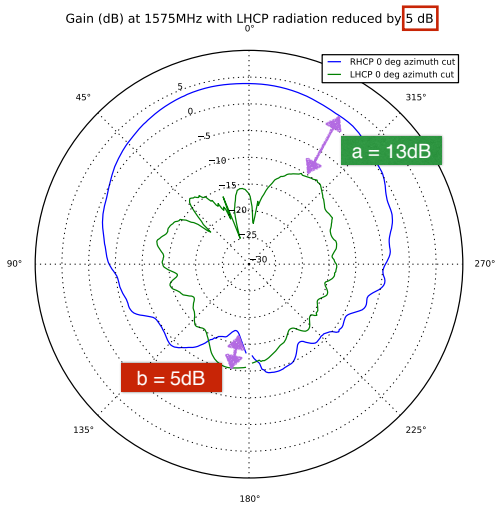

Fig. 18: To emulate professional GPS antennas, we artificially reduce the LHCP pattern of our home-built antenna (measurement in Figure 11) by 5 dB.

Figures 19 and 20 show results we would expect to observe in SNR or C/N_0, with our artificially modified spoof detection antenna, as the percentage of time allocated to detection-mode increases. The seven spoofers are assumed to use LHCP and RHCP radiation, for Figures 19 and 20, respectively. The plots show that the SNR or C/N_0 values clearly diverge, separating the spoofed signals from the genuine GPS signals as $\frac{T_D}{T_N+T_D}$ tends toward 100%. This divergence would permit an operator or algorithm to take a quick look at the receiver's reported SNR or C/N_0 values, and immediately detect the presence of a sophisticated spoofing attack originating from below the antenna.

SUMMARY AND CONCLUSIONS

In this paper we have introduced a static single antenna design that can instantly detect spoofed GPS signals originating from below the horizon, without requiring any additional backend signal processing steps. During the normal operation of this dynamic antenna, the additional insertion loss caused by the detection components is less than a dB. This detection antenna can be achieved within a standard GPS antenna form-factor. If used in replacement of an existing standard GPS antenna, neither the existing antenna footprint, nor existing GPS receiver require any changes. We stress the backward compatibility of this design not necessarily as the realization of its most practical implementation, but instead as documentation of its simplicity

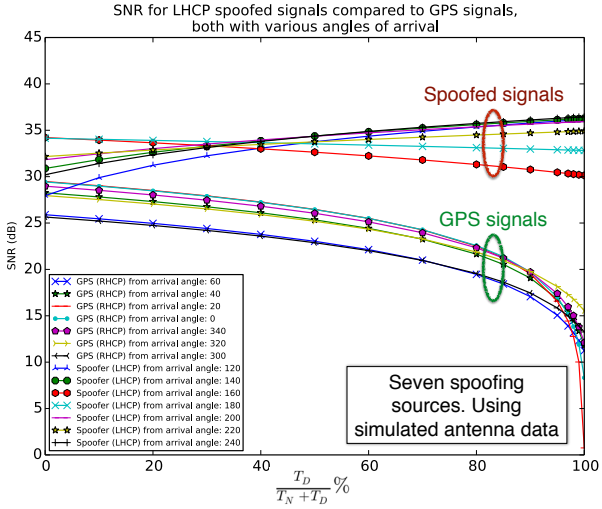

Fig. 19: SNR reported by our simulated GPS receiver with our artificially modified spoof detection antenna, as percentage of time allocated to detection-mode (T_D) increases for spoofers transmitting LHCP signals from seven DoAs linearly spaced at angles 30° below the horizon, as compared to seven authentic GPS signals with seven DoAs linearly spaced for angles 30° above the horizon.

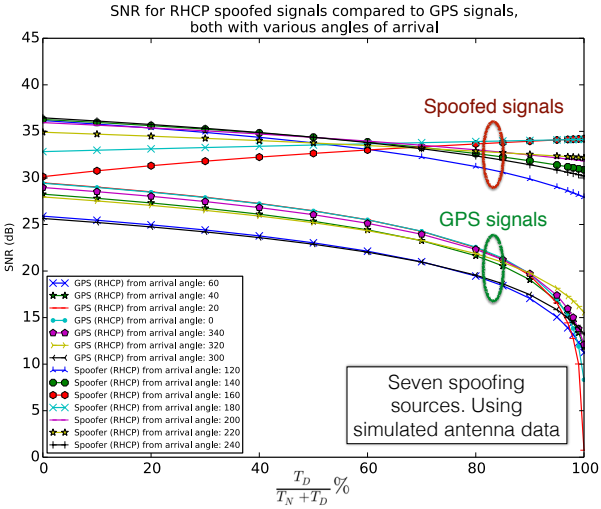

Fig. 20: SNR reported by our simulated GPS receiver with our artificially modified spoof detection antenna, as percentage of time allocated to detection-mode (T_D) increases for spoofers transmitting RHCP signals from seven DoAs linearly spaced at angles 30° below the horizon, as compared to seven authentic GPS signals with seven DoAs linearly spaced for angles 30° above the horizon.

and consistency within the current constraints of GPS receiver systems and antenna form-factors.

We have also identified the general requirements for detection. If we can assume GPS satellites are above and spoofers are below, then we require the XPD in the upper hemisphere be much greater than the "cross-polarization

discrimination" (XPD) in the lower hemisphere for at least several satellite signal DoAs. If we can not assume satellites are above and spoofers are below, we can exploit characteristics unique to each genuine GPS signal such as the antenna's XPD ripple and gain for a given DoA. Future work will include use of an antenna with improved XPD for better qualification of these requirements and associated confidence metrics.

ACKNOWLEDGMENTS

The research conducted for this paper took place at the Stanford University Global Positioning System Research Laboratory with funding from the WAAS program office under FAA Cooperative Agreement 12-G-003. The anechoic chamber measurements were conducted at Space Systems/Loral, with special thanks to Paul Miller, Sunali Chokshi, Martin McBride, Larry Arnett, Claudia Lam and Chris Hoeber. Also special thanks to Dennis Akos for his insightful consultations.

REFERENCES

[1] Chen, Yu-Hsuan, Lo, Sherman, Akos, Dennis M., De Lorenzo, David S., Enge, Per, "Validation of a Controlled Reception Pattern Antenna (CRPA) Receiver Built From Inexpensive General-purpose Elements During Several Live-jamming Test Campaigns,"Proceedings of the 2013 International Technical Meeting of The Institute of Navigation, San Diego, California, January 2013, pp. 154-163.

[2] P. Montgomery and T. E. Humphreys, "A Multi-Antenna Defense: Receiver-Autonomous GPS Spoofing Detection," Inside GNSS, no. March/April, pp. 40-46, 2009.

[3] Konovaltsev, Andriy, Cuntz, Manuel, Haettich, Christian, Meurer, Michael, "Performance Analysis of Joint Multi-Antenna Spoofing Detection and Attitude Estimation," Proceedings of the 2013 International Technical Meeting of The Institute of Navigation, San Diego, California, January 2013, pp. 864-872.

[4] Nielsen, John, Broumandan, Ali, Lachapelle, Gerard, "GNSS Spoofing Detection for Single Antenna Handheld Receivers", NAVIGATION, Journal of The Institute of Navigation, Vol. 58, No. 4, Winter 2011-2012, pp. 335-344.

[5] Psiaki, M.L., Powell, S.P., O'Hanlon, B.W., "GNSS Spoofing Detection using High-Frequency Antenna Motion and Carrier-Phase Data," Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, September 2013, pp. 2949-2991.

[6] Bauregger, Frank N., Walter, Todd, Akos, Dennis, Enge, Per, "A Novel Dual Patch Anti Jam GPS Antenna," Proceedings of the 58th Annual Meeting of The Institute of Navigation and CIGTF 21st Guidance Test Symposium, Albuquerque, NM, June 2002, pp. 516-522.

[7] Rao, B. Rama, Kunysz, W., Fante, R., and McDonald, K., "GPS/GNSS Antennas", Artech House, 2012

[8] Rao, B. Rama, Williams, Jonathan H., "Measurements on a GPS Adaptive Antenna Array Mounted on a 1/8-Scale F-16 Aircraft," Proceedings of the 11th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1998), Nashville, TN, September 1998, pp. 241-250.