

**STATEMENT ON THE VULNERABILITY OF
CIVIL UNMANNED AERIAL VEHICLES AND OTHER SYSTEMS
TO CIVIL GPS SPOOFING**

TODD HUMPHREYS
THE UNIVERSITY OF TEXAS AT AUSTIN

Submitted to the Subcommittee on Oversight, Investigations, and Management of the
House Committee on Homeland Security

1. SUMMARY

Military Global Positioning System (GPS) signals have long been encrypted to prevent counterfeiting and unauthorized use. Civil GPS signals, on the other hand, were designed as an open standard, freely-accessible to all. These virtues have made civil GPS enormously popular, but the transparency and predictability of its signals give rise to a dangerous weakness: they can be easily counterfeited, or spoofed. Like Monopoly money, civil GPS signals have a detailed structure but no built-in protection against counterfeiting. Civil GPS is the most popular unauthenticated protocol in the world.

The vulnerability of civil GPS to spoofing has serious implications for civil unmanned aerial vehicles (UAVs), as was recently illustrated by a dramatic remote hijacking of a UAV at White Sands Missile Range. The demonstration was conducted by the University of Texas Radionavigation Laboratory at the behest of the Department of Homeland Security (DHS). From a standoff range of a half mile, the University spoofer commandeered the UAV and induced it to plummet toward the desert floor. The results of this demonstration will no doubt factor into the Federal Aviation Administration's (FAA's) plans for integrating UAVs into the national airspace.

Hacking a UAV by GPS spoofing is but one expression of a larger problem: insecure civil GPS technology has over the last two decades been absorbed deeply into critical systems within our national infrastructure. Besides UAVs, civil GPS spoofing also presents a danger to manned aircraft, maritime craft, communications systems, banking and finance institutions, and the national power grid.

Constructing from scratch a sophisticated GPS spoofer like the one developed by the University of Texas is not easy. It is not within the capability of the average person on the street, or even the average Anonymous hacker. But the emerging tools of software-defined radio and the availability of GPS signal simulators are putting spoofers within reach of ordinary malefactors.

There is no quick, easy, and cheap fix for the civil GPS spoofing problem. What is more, not even the most effective GPS spoofing defenses are foolproof. But reasonable, cost-effective spoofing defenses exist which, if implemented, will make successful spoofing much harder.

I recommend that for non-recreational operation in the national airspace civil UAVs exceeding 18 lbs be required to employ navigation systems that are spoof-resistant.

More broadly, I recommend that GPS-based timing or navigation systems having a non-trivial role in systems designated by DHS as national critical infrastructure be required to be spoof resistant.

Finally, I recommend that the DHS commit to funding development and implementation of a cryptographic authentication signature in one of the existing or forthcoming civil GPS signals

2. BACKGROUND

The design of the Global Positioning System came together over Labor Day weekend in 1973. A group of hard-working engineers, mostly Air Force officers, decided over that weekend that the GPS satellites would broadcast two different types of signals, a precise military signal and a so-called clear access or C/A signal. The military signal would later be encrypted to prevent unauthorized use and imitation.

But the clear access signal, true to its name, would be freely accessible to all. Detailed and accurate specifications for the clear access signal were later distributed to encourage its use.

The early designers of the GPS system, for whose tireless efforts we are all indebted, knew the GPS was going to be valuable for civilians across the globe, but they never could have imagined just how valuable. An intentional degradation of the C/A signals called selective availability was discontinued by presidential order in 2000. Instantaneously, every GPS receiver across the globe went from errors the size of a football field to errors the size of a small room. It is hard to overstate the impact of this improvement in accuracy. Before selective availability was turned off, there were no in-car navigation systems giving turn-by-turn directions, because back then civilian GPS couldn't tell you what block you were on, let alone what street. For geolocation, accuracy matters.

Things have only improved over the last decade. With more ground stations, better algorithms, more open-access signals, and better receivers, civil GPS—the family of open-access signals to which all civilians have access—can now tell you not only what street you are on, but what part of the street.

The accuracy, transparency, and low cost of civil GPS have enabled a firestorm of innovation. After 2000, any engineer designing a system for which accurate timing or location was important found GPS to be an almost irresistible option. As a result, civil GPS receivers are built deeply into our national infrastructure: from our smartphones to our cars to the Internet to the power grid to our banking and finance institutions. Some call GPS the invisible utility: it works silently, and for the most part perfectly reliably, in devices all around us—devices of which we are scarcely aware.

Nearly forty years after the GPS design was put together we can look back and marvel at its designers' foresight. The GPS that we all depend on today is nearly identical to their original design. But with forty years of hindsight, many of us in the GPS community, if we could be transported back to those seminal meetings over Labor Day weekend in 1973, would suggest that one crucial change be made to the clear access signal.

The problem is that the same transparency and predictability that have made civil GPS signals so wildly popular all across the globe give rise to a dangerous vulnerability. Transparency and predictability make the civil GPS signals easy to imitate—to counterfeit. The fact is that civil GPS signals are like Monopoly money: they have a detailed structure but no built-in protection against forgery.

That civil GPS is so easy to counterfeit, or “spoof,” would not be a problem if GPS were not so popular, its use so widespread. But such is not the case.

For the past few years my students and I at the University of Texas Radionavigation Laboratory, and several others in the GPS community, have had two goals with regard to GPS security. First, we aim to alert GPS device manufacturers, the public, and public officials that civil GPS—notwithstanding its spectacular utility and historical reliability—is inherently insecure and shouldn't be trusted blindly. Second, we endeavor to develop practical and effective techniques to fix the problem, to make GPS secure and trustworthy for civilian users. The remainder of this statement is a brief summary of our major findings and recommendations to date.

3. EXAMPLE CASE: HIJACKING A UAV BY CIVIL GPS SPOOFING

What implications follow from the lack of authentication on civil GPS signals? Consider unmanned aerial vehicles (UAVs). In February 2012 the U.S. Congress passed the FAA Modernization and Reform Act, which gives the FAA until 2015 to develop a “comprehensive plan for safely accelerating the integration of civil UAVs into the national airspace system.” The Modernization Act has spurred a great deal of discussion. Hobbyists, public safety officials, academics, UAV manufacturers, and many in the general public envision myriad beneficial applications of civil UAVs. Others, less sanguine, point out that UAVs threaten to invade our privacy. Still others question whether UAVs can be integrated safely into the national airspace.

The connection between civil UAVs and civil GPS is straightforward: the vast majority of civil UAVs depend on civil GPS for navigation. It is true that the navigation sensor suite of a typical civil UAV also includes inertial sensors (accelerometers and rate sensors), magnetometers, altimeters, and in some cases a camera; even so, GPS is fundamental to the sensor suite because, unlike the other navigation sensors, it works in all weather conditions and does not drift.

Does the dependence of UAVs on civil GPS make them susceptible to hijacking via GPS spoofing? In February 2012 the University of Texas Radionavigation Laboratory posed this question to the DHS. DHS considered the question seriously. At the time, DHS was moving forward with plans to offer universities and other interested civilian groups a chance to test their proposed techniques for addressing civil GPS vulnerabilities in a series of realistic over-the-air tests at White Sands Missile Range. My students and I proposed to DHS an experiment whereby we would attempt to commandeer a civilian UAV by GPS spoofing. DHS agreed to the test on the condition that the University of Texas furnish all the necessary manpower and equipment—including the target UAV.

Our group selected a Hornet Mini from Adaptive Flight as the target UAV. This sophisticated \$80k rotorcraft, used by law enforcement, has a navigation system built around an extended Kalman filter that draws measurements from an altimeter, a magnetometer, an inertial measurement unit, and a civil L1 C/A GPS receiver. The Hornet Mini’s sensor suite and flight control system are representative of those in much larger commercial UAVs.

It is important to note that the Hornet Mini’s GPS receiver was equipped with a standard technology called Receiver Autonomous Integrity Monitoring (RAIM), which is designed to identify and discard GPS signals that appear to be outliers. Standard RAIM is ineffective against GPS spoofing because a spooper generates a fully self-consistent ensemble of spoofing signals; there are no outliers.

After a dry run on the University of Texas campus, our research group traveled to White Sands for the test of record. The test was conducted as follows: A sophisticated civil GPS spoofer developed in our laboratory was placed on a hilltop about a half mile from the designated test site where the UAV would be flying. The UAV was commanded by its ground control operator to hover 50 feet above the ground at the test site. On command, our spoofer began transmitting weak counterfeit GPS signals toward the hovering UAV, achieving meter-level alignment with the counterpart authentic signals at the location of the UAV’s GPS antenna. The spoofer then rapidly increased its counterfeit signal power, bringing the UAV under its control. By inducing a false upward drift in the UAV’s perceived location, the spoofer fooled the UAV’s flight controller into commanding a dive. At about 10 feet above ground level a human safety pilot assumed manual control of the UAV to prevent it from crashing.

Between this and other tests, the spoofer demonstrated short-term three-dimensional control of the UAV. Thus, we conclude that it is indeed possible to hijack a civil UAV—in this case, a fairly sophisticated one—by civil GPS spoofing.

4. THE LARGER PROBLEM

The vulnerability of civil UAVs to GPS spoofing is but one expression of a more fundamental problem: the insecurity of civil GPS signals. If a UAV can be hijacked by GPS spoofing, what else could go wrong within our GPS-dependent national infrastructure? In what follows, the potential vulnerabilities of our national transportation, communications, banking and finance, and energy distribution infrastructure are discussed briefly.

4.1. Transportation. In 2001, the U.S. Department of Transportation issued a report assessing the vulnerability of the U.S. transportation infrastructure to disruption of civil GPS [1]. Known as the Volpe report, it highlighted the threats posed by civil GPS spoofing attacks. At the time, the open literature contained little research on such attacks and possible countermeasures. Accordingly, the report recommended further study of GPS spoofing and development of civil GPS anti-spoofing techniques. Unfortunately, despite a flurry of GPS security research over the past decade, brought about in part by the Volpe report, no dedicated spoofing defenses have been built into any commercially-available GPS receivers so far as I am aware. This means that the GPS receivers used in commercial and general aviation aircraft, in maritime vessels, and in surface vehicle transport are vulnerable to GPS spoofing just as was the GPS receiver on the UAV tested at White Sands.

4.1.1. Manned Aviation. Manned civil aircraft increasingly depend on civil GPS for navigation. Nonetheless, they are currently somewhat less vulnerable than civil UAVs to GPS spoofing for two reasons:

- (1) All commercial aircraft and many general aviation aircraft continue to operate legacy VOR/DME navigation equipment along with newer GPS equipment. Because of their higher power, VOR/DME signals are less vulnerable to spoofing than GPS signals. Legacy VOR/DME equipment can provide pilots a valuable cross-check against which to compare GPS-produced position and velocity data.
- (2) Manned aircraft are typically equipped with higher-quality (lower drift) inertial measurement units (IMUs) than those used in small UAVs, which means that the GPS navigation solution can be more effectively cross-checked against the IMU. Whereas a spoofer might be able to induce a fictitious acceleration of 0.5 m/s^2 in a small UAV without being detected in a cross-check against the (relatively poor) IMU, an attack against a larger craft with a higher-quality IMU might be limited to an induced acceleration of 0.1 m/s^2 . However, it should be noted that the benefit of a higher-quality IMU is only realized if the navigation system is designed to be on the lookout for suspicious accelerations in the GPS solution.

Despite these advantages, GPS spoofing remains a significant risk to civil manned aircraft. When the aircraft's autopilot is engaged, the course it commands depends primarily on the aircraft's IMU. However, GPS plays a role in estimating the bias drift in each of the IMU's axes. Thus, neither the autopilot nor the human pilot(s) may notice a spoofer-induced navigation error that builds up gradually over time. Pilots are trained to continually monitor the autopilot for errant behavior, and disengage it if necessary, but they rely on anomaly alerts provided by the aircraft's navigation system

itself. I have reason to believe that the resilience of commercial aircraft navigation systems to civil GPS spoofing has not been sufficiently tested. Roll-out of the FAA's NextGen air traffic control system, which will further increase the reliance of commercial and general aviation on civil GPS, would seem to demand even greater scrutiny as regards vulnerability to GPS spoofing.

4.1.2. Maritime. Many of the adverse effects of GPS spoofing in maritime applications follow the pattern of those in aviation applications. As with aircraft, marine craft rely on civil GPS to estimate the bias drift in their inertial sensors. This reliance opens up an indirect vulnerability to GPS spoofing. Marine vessels may in fact be more vulnerable than aircraft to spoofing because the discontinuation of LORAN in the U.S. two years ago left them with fewer radionavigation backups to GPS. It should be noted that differential GPS, often used for improved navigation accuracy on marine craft, is not a defense against GPS spoofing.

Many marine craft autopilot systems could likely be induced by GPS spoofing to veer gradually off course, which could be especially dangerous in constricted waterways. And whereas formal trials have been conducted to evaluate the effect of GPS jamming on commercial marine craft (with alarming results—see the tests conducted in the North Sea by the U.K. Lighthouse Authority), to my knowledge no such tests have been performed to evaluate the effects of GPS spoofing.

4.1.3. Surface Transportation. The reliance of surface transportation on civil GPS is collectively greater than that of aviation or maritime transportation, but the nature of the reliance is different, being attached to far less worrisome consequences. A spoofing attack against an automobile could induce the in-car navigation system to display a false position, which may confuse the driver, but would be unlikely to result in an accident. In the case of autonomous vehicles such as the Google autonomous car, a substantial suspicion of GPS is built into the navigation system. GPS measurements are used to estimate the biases in inertial sensors, but LIDAR, RADAR, and optical sensors are also used for this purpose and their measurements are constantly cross-checked against GPS. The robustness of the Google autonomous car to loss of GPS or GPS spoofing is a good model for all autonomous systems in their use of GPS.

Rail transport employing so-called Positive Train Control (PTC) systems, which automatically locate a train on a digital map in the on-board and control center computers, may be susceptible to civil GPS spoofing. A GPS spoofing attack mounted against a PTC-enabled train at a railway switch may be able to deceive the train operator and the control center monitors into thinking that the train is moving along a different track.

4.2. Communications. Many communications networks, including cellular networks and the Internet, rely on civil GPS for precise timing. The discussion here will focus on cellular networks because these have stringent synchronization requirements.

Code division multiple access (CDMA) cell-phone towers rely on GPS timing for tower-to-tower synchronization. Synchronization prevents towers from interfering with one another and enables call hand-off between towers. If a particular tower's time estimate deviates more than $10\ \mu s$ from GPS time, hand-off to and from that tower is disrupted. In laboratory tests conducted at the University of Texas we have demonstrated that a spoofing device can induce a $10\text{-}\mu s$ time deviation in less than 30 minutes when acting against a typical CDMA tower setup. A spoofing network, or spoofing network, could also cause multiple neighboring towers to interfere with one another. This is possible because CDMA cell-phone

towers all employ the same spreading code, distinguishing themselves only by the phasing (that is, the relative time offset) of their spreading codes. Furthermore, it appears that aspoof could impair CDMA-based E911 user-location

4.3. Banking and Finance. All global financial exchanges, including the New York Stock Exchange (NYSE) and the Nasdaq, have gone digital. Large data centers hold the exchanges' matching engines, the modern-day equivalent of the historic trading floor, in racks of interconnected servers. The DHS considers these data centers critical national infrastructure. Private security personnel, tall fences, and the best network security money can buy protect the integrity of the thousands of high-stakes trades executed every second within these data centers.

But there is one input port that the network firewalls leave entirely unprotected. An unassuming set of antennas on the roof of these data centers carry unsecured civil GPS signals directly into the core of the matching engine network. Slaved to a once-per-second synchronization pulse from a GPS-disciplined clock, the individual servers in the network apply time stamps to the trades they execute. A decade ago, a tenth of a second was an acceptable time stamp resolution. High frequency traders now demand nanoseconds.

I believe that all major financial exchanges across the globe are aware of the GPS spoofing threat. I have been in indirect contact with network service managers at the NYSE, BATS, and London exchanges; they have each taken precautions against GPS spoofing. For example, system time at the NYSE is ultimately traced to civil GPS, but a spoofing attack that shifted the apparent GPS time by more than 0.05 nanoseconds per second would fail a timing consistency check against redundant local atomic clocks. This would limit a spoof to shifting the exchange's system time by less than 5 microseconds per day, making the NYSE system time an attractive target only for the most patient of spoofers.

High frequency traders whose servers are co-located with the matching engines at major exchanges may be more vulnerable to GPS spoofing. In the NYSE and some other exchanges, these co-located customers are offered either a timing feed from the exchange's system time or a direct feed from GPS antennas on the roof. Many co-located customers, distrustful of the exchange's system time, opt for the direct GPS feed. In laboratory tests conducted at the University of Texas we have shown that a popular model of GPS-disciplined oscillator used by these co-located customers is incapable of detecting GPS spoofing attacks that shift timing by less than 100 nanoseconds per second—or 2000 times faster than the maximum undetectable rate when targeting NYSE system time.

Why could this be a problem? Automated transactions initiated by co-located servers account for 50 to 70 percent of the trading volume on major exchanges. The high-frequency traders who own the servers do not like inexplicable market behavior, and unlike old-fashioned traders who are obligated to stay in the market no matter its behavior, high-frequency traders can pull the plug at any moment. In the aftermath of the May 6, 2010 flash crash, it was revealed that automatic data integrity checks in trading algorithms were configured to trigger on unusual latency in the exchanges data feeds. In other words, if transaction time stamps do not look right, algorithmic traders flee the marketplace. A spoofing attack that aggressively manipulated the timing in a large number of co-located servers could therefore cause a partial market vacuum—what traders call a loss of liquidity—with the result being increased price volatility and damage to market confidence.

4.4. Energy Distribution. In a recent study, our laboratory examined the vulnerability of a particular type of smart grid equipment, the phasor measurement unit (PMU), to a timing attack [2]. If a spooper manipulates a PMU’s time stamps, it could cause spurious variations in measured phase angles. These variations could distort power flow or stability estimates in such a way that grid operators or automatic response systems would take incorrect or unnecessary control actions, including powering up or shutting down generators, potentially causing blackouts or damage to power-grid equipment. Under normal circumstances, a changing separation in the phase angle between two PMUs indicates changes in power flow between the regions measured by each PMU. Thus, a spoofing attack could create the false indications of power flow across the grid.

Under controlled experimental conditions at a Department of Energy national laboratory, we demonstrated last December that a GPS-spoofed-induced timing offset does indeed create a proportional offset in the voltage phase angle measured by a PMU. In a brief examination of the consequences of such an offset, we found that future smart grids will likely employ advanced PMUs in automated closed-loop grid control [3] and that such closed-loop control has already been implemented in at least one network [4]. We have reason to believe that timing manipulation would cause generators to trip in this network and in future automated closed-loop grid control networks [2].

5. ASSESSING THE RISK

A thorough assessment of the spoofing risk would investigate two factors, (1) the probability, and (2) the consequences of an attack. The foregoing section presented various consequences, though certainly not a thorough listing, related to critical national infrastructure. The probability of a spoofing attack is a function of the incentives that would prompt an attack and the difficulty of mounting one. As an investigation of incentives is necessarily subjective and, in any case, outside my expertise, I will leave this to others, focusing here on assessing the difficulty of mounting a spoofing attack.

5.1. What Does it Take to Build a Spoof? Constructing from scratch a sophisticated GPS spoofing like the one developed by the University of Texas is not easy. It is not within the capability of the average person on the street, or even the average Anonymous hacker. It is orders of magnitude harder than developing a GPS jammer. Nonetheless, the trend toward software-defined GNSS receivers for research and development, where receiver functionality is defined entirely in software downstream of the A/D converter, has, in recent years, significantly lowered the bar to developing a spoofing.

5.1.1. Cost of Hardware. The University of Texas spoofing was constructed almost entirely from commercial off-the-shelf components. The total hardware cost was between \$1k and \$2k. Universal software radio platforms that rival the capability of our hardware system can be purchased for less than \$2k.

5.1.2. Required Skill and Effort. As a point of reference, I estimate that there are more than 100 researchers in universities across the globe who are well-enough versed in software-defined GPS that they could develop a sophisticated spoofing from scratch with a year of dedicated effort. Spoofing development is likely outside the capability of organized crime or terrorist organizations without access to advanced training, but is well within the capability of near-peer nation states.

5.2. Can One Buy a Spoof? Unlike GPS jammers, marketed by overseas firms as “personal privacy devices” and sold by the thousands on the Internet, sophisticated GPS spoofers such as the one developed by the University of Texas Radionavigation Laboratory cannot currently be obtained in any market of which I am aware. However, a GPS signal simulator, a piece of test equipment that is readily obtainable from various vendors, can serve as an unsophisticated yet effective GPS spoof. A sophisticated spoof is only different from a GPS signal simulator in the following respects:

- (1) It is capable of predicting, with nearly 100% accuracy, the navigation data sequence that modulates the GPS signals—not just the implied orbital and clock data, but the exact sequence. This same effect can be realized on a standard GPS signal simulator only by developing a secondary system that generates blocks of predicted navigation data and uploads these to the signal simulator.
- (2) A sophisticated spoof is capable of precisely aligning (within a few meters equivalent) the codes in its counterfeit signals with the corresponding codes of the authentic signals at the location of the target receiver’s antenna. The University of Texas spoof is capable of achieving this alignment from a standoff distance of several kilometers. An off-the-shelf GPS signal simulator would have to be substantially modified to achieve such alignment.

These differences are only important if one wishes to carry out a stealthy spoofing attack, that is, one that effects a near-seamless transition from authentic to counterfeit signals and is therefore difficult to detect by simple timing and signal checks within the target system. But this is hardly necessary for a successful attack against most targets at present, given that few GPS-based systems perform even these rudimentary checks. Indeed, a vulnerability assessment team from Los Alamos National Lab convincingly demonstrated over a decade ago that an off-the-shelf GPS signal simulator is sufficient to mount a spoofing attack [5], and spoofing defenses in commercial receivers have hardly progressed since that time.

High-end commercial GPS signal simulators cost several hundred thousand dollars, but these can be leased for a few hundred dollars on a weekly basis. Moreover, within the past few years much less expensive (less than \$40k) single-frequency GPS signal simulators have emerged on the market. GPS signal record-and-playback devices, which can be purchased for a few thousand dollars, can also be used effectively as unsophisticated spoofers.

5.3. Range and Required Knowledge of Target. Assuming one could build or otherwise obtain a spoofing device, a successful spoofing attack further requires proximity to and knowledge of the target system.

5.3.1. At What Standoff Range Can a Spoof Be Effective? The University of Texas Radionavigation Laboratory demonstrated a successful spoofing attack from a 0.62-km standoff range in our over-the-air test at White Sands. Our spoof’s maximum standoff range is fundamentally limited only by the spoof’s need to track all or nearly all of the authentic GPS signals seen by the target receiver, which implies an operational range of several tens of kilometers. A spoof’s broadcast power requirement, even at a standoff range of several kilometers, is quite modest because the authentic GPS signals are themselves extremely weak.

5.3.2. What Must the Spoof Know about the Target to Be Effective? For a near-seamless transition from authentic to counterfeit signals, and, in the case of UAV spoofing, for fine-grained control of the

UAV after capture, a spoofing must be furnished with real-time estimates of the target system's location and velocity accurate to within a few meters and meters per second, respectively. This represents a substantial challenge for a would-be spoofing operator. In the case of UAV spoofing it implies that the UAV is being accurately tracked by a RADAR or LIDAR system. However, if a spoofing operator's goal is simply to confuse the target's navigation or timing system, and the operator is unconcerned about possible detection, then knowledge of the target's position and velocity is unnecessary.

6. FIXING THE PROBLEM: WHAT CAN BE DONE TO DEFEND AGAINST GPS SPOOFING?

There is no quick, easy, and cheap fix for the civil GPS spoofing problem. Moreover, not even the most effective GPS spoofing defenses are foolproof. In contrast to message authentication, such as is used to sign data transmitted across the Internet, the security of GPS signal authentication is much weaker and demands a probabilistic model. Nonetheless, there are many possible remedies to the spoofing problem that, while not foolproof, would vastly improve civil GPS security. For discussion, it is convenient to categorize spoofing defenses along two axes: (1) cryptographic or non-cryptographic, and (2) networked or stand-alone. A cryptographic spoofing defense relies on secret keys that encrypt or digitally sign components of the broadcast signals, whereas a non-cryptographic defense does not depend on encryption or digital signatures. A networked defense requires a (possibly intermittent) link to a communications network whereas a stand-alone defense operates in isolation of a network.

Our laboratory has been engaged in developing civil GPS spoofing defenses over the past several years. In addition, a number of other researchers have proposed civil GPS spoofing defenses in the open literature or have otherwise disclosed their ideas to me. In what follows, I examine each of the proposed techniques of which I am aware. More promising techniques approach the ideal spoofing defense, which (1) would reliably detect a sophisticated spoofing attack such as the one conducted at White Sands with a low probability of false alarm, (2) could be implemented in the short term, (3) would not significantly increase the cost of a GPS-based navigation system, and (4) would be applicable to a broad range of GPS dependent systems.

It should be noted at the outset that a military-style spoofing defense, in which the transmitted signals are fully encrypted, is not appropriate for the civilian sector as it denies free and open access. All techniques discussed below permit signal authentication without denying access. Likewise, I do not believe that widespread civilian use of military-grade SAASM receivers is practical or likely. The constraints on manufacture of SAASM receivers makes them significantly more bulky and expensive than standard civil GPS receivers. Furthermore, even though SAASM receivers can be operated in an unclassified setting and can be re-keyed with unclassified "black" keys, use of SAASM receivers is currently restricted to military personnel and to other select and authorized end-users, and initial keying logistics would likely present a headache for civil users. Therefore, civilian use of SAASM-type receivers is not considered here as a viable option.

6.1. Jamming-to-Noise Sensing Defense. Perhaps the simplest and most readily-implementable defense against GPS spoofing is to monitor the total received power near the GPS band(s) of interest (e.g., GPS L1). This can be done with a jamming-to-noise (J/N) sensor within the radio frequency (RF) front-end of a GPS receiver. The presence of in-band spoofing signals tends to increase the total in-band received power. In the case of the White Sands demonstration, to ensure a clean capture of the UAV GPS receiver, the spoofing signal ensemble was configured to be at least 10 times as

powerful as the authentic signal ensemble. The presence of these spoofing signals would have been readily detectable with a J/N sensor.

This is a stand-alone non-cryptographic defense.

6.1.1. *Benefits.*

- (1) Simple and inexpensive. At least one mass-market GPS receiver, the uBlox GPS.G6-SW-10018, already provides a crude J/N output indicator.
- (2) Immediately implementable.
- (3) Forces spoofer to maintain received signal power below threshold.

6.1.2. *Drawbacks.*

- (1) For threshold corresponding to a reasonable false alarm rate, a J/N sensor will not typically detect a spoofing attack in which the spoofed signals are only slightly more powerful than their authentic counterparts.

6.2. Defense Based on SSSC or NMA on WAAS Signals. The SSSC- or NMA-based defenses described below could be implemented on the geostationary wide-area augmentation system (WAAS) satellites even if they are never implemented on the GPS satellites themselves.

6.2.1. *Benefits.*

- (1) WAAS is a civil program and thus could be seen as a proper avenue for implementation of civil signal authentication.
- (2) WAAS signals are generated on the ground, not on the satellite, so an SSSC or NMA overlay is readily implementable.
- (3) A single WAAS authenticated WAAS signal would be sufficient to secure pre-surveyed timing receivers.

6.2.2. *Drawbacks.*

- (1) Implementation of SSSC or NMA on WAAS satellites alone would only provide users with one, or possibly two, authenticated GPS signals. While this would constrain a spoofer significantly, it would not be sufficient to authenticate a full three-dimensional navigation solution.

6.3. Multi-System Multi-Frequency Defense. The GPS receiver on the UAV that was spoofed in the White Sands demonstration was a simple single-frequency GPS L1 C/A receiver. The UAV's navigation system could immediately be made much more secure by incorporating a multi-system or multi-frequency receiver that performs proper cross-checks among separate signal ensembles. The improvement in security is one of degree, not of kind because the new signals accessible with such a receiver would not necessarily have any better inherent security than the GPS L1 C/A signals. Nonetheless, the improvement in security can be significant because, from a spoofer's perspective, it is much more challenging to simultaneously spoof signals at multiple frequencies and from multiple systems than to spoof the popular single-frequency single-system GPS L1 C/A signals.

Satellite navigation systems other than GPS include the Russian GLONASS system (fully operational), the European Galileo system (undergoing in-orbit validation of early spacecraft; may be operational by 2019), and the Chinese Compass system (global system in preliminary test phase). Small, low-power, inexpensive GPS + GLONASS receivers are now available off-the-shelf. These appear to be an excellent option for immediately improving navigation security in existing systems.

As a result of GPS modernization, new civil GPS signals are now being broadcast at the L2 and L5 frequencies in addition to the legacy civil signal on L1. These signals are not yet modulated with proper navigation data, but they can nonetheless already be used for consistency checks against the GPS L1 C/A signals. Similarly, the Galileo system will offer open-access signals at three separate frequencies. Off-the-shelf multi-frequency receivers are currently available, but these are currently several times more expensive than single-frequency GPS receivers or GPS + GLONASS receivers.

The multi-system multi-frequency defense is non-cryptographic and stand-alone.

6.3.1. *Benefits.*

- (1) Small, low-power, inexpensive GPS + GALILEO receivers are available today.
- (2) Increases the difficulty of mounting a spoofing attack by forcing a would-be spoofer to generate other signal ensembles besides GPS L1 C/A.

6.3.2. *Drawbacks.*

- (1) Difficulty of mounting a spoofing attack only increases linearly with the number of new signal ensembles.
- (2) Multi-system, multi-frequency capability must be combined with supervisory software that performs proper consistency checks among observables from all signals. Currently available multi-system, multi-frequency receivers do not perform this supervisory function.
- (3) Multi-frequency receivers will likely remain significantly more expensive than legacy single-frequency GPS L1 C/A receivers.

6.4. Single-Antenna Defense. A stand-alone non-cryptographic single-antenna spoofing defense developed by Cornell University was tested against the University of Texas spoofer during the June White Sands trials. The technique is still under development but initial results indicate that it offers reliable spoofing detection with a low probability of false alarm. Without false alarms, it successfully detected each spoofing trial in which it was invoked at White Sands. The Cornell single-antenna defense is an extension of the signal spatial correlation technique developed by the University of Calgary PLAN group. [6].

6.4.1. *Benefits.*

- (1) Rapid (sub-second), reliable spoofing detection with a low probability of false alarm.
- (2) Stand-alone, compact.

6.4.2. Drawbacks.

- (1) Specialized receiver will likely be several times more expensive than current GPS L1 C/A receivers.
- (2) Uncertain availability.

6.5. Defense Based on Spread-Spectrum Security Codes on L1C. In 2003, Logan Scott proposed a cryptographic anti-spoofing technique based on spread spectrum security codes (SSSCs) [7]. The most recent proposed version of this technique targets the L1C signal, which will be broadcast on GPS Block III satellites. Logan has briefed his proposal to the GPS Independent Review Team and the GPS Directorate is aware of it.

6.5.1. Benefits.

- (1) SSSC are an example of a high-rate security code. As shown in [8], such codes offer an excellent defense against spoofing.
- (2) Because the signal modification is targeted to L1C, whose center frequency coincides with that of the legacy GPS L1 C/A signal, even single-frequency receivers would have access to an authenticated signal.
- (3) The SSSC defense would offer global civil GPS authentication for all users of GPS.

6.5.2. Drawbacks.

- (1) It appears that the first 8 Block III satellites are under design lockdown. There may still be time to modify the remaining satellites to incorporate hardware to support SSSC, but time is quickly running out.
- (2) Even if funds materialized to implement Scott's SSSC proposal, the formal design and validation process would take several years.
- (3) In stand-alone operation, the keys required to verify each SSSC would be released up to 5 minutes after the SSSC was transmitted. For 10 satellites in view, this equates to more than 30 seconds between authentication events on any signal. This would be far too long for use in aviation, where integrity alerts within 2 seconds of an event are required. The time-to-authentication could be reduced to less than 2 seconds in a networked architecture. For example, the keys could be sent over a UAVs command and control link. But if the command and control link were somehow compromised, then short-horizon authentication would again become impossible.

6.6. Defense Based on Navigation Message Authentication on L1C, L2C, or L5. A spoofing defense based on navigation message authentication (NMA) embeds public-key digital signatures into the flexible GPS civil navigation (CNAV) message, which offers a convenient conveyance for such signatures. A detailed proposal for NMA-based authentication is given in [9].

6.6.1. Benefits.

- (1) NMA-based authentication is easier to implement than SSSC because the CNAV format is extensible by design so that new messages can be defined within the framework of the GPS

Interference Specification (IS). The current GPS IS defines only 15 of 64 CNAV messages, reserving the undefined 49 CNAV messages for future use.

- (2) Could be implemented post-launch on Block IIR-M, Block II-F, and Block III satellites.
- (3) Like SSSC, the NMA-based defense would offer global civil GPS authentication for all users of GPS.

6.6.2. *Drawbacks.*

- (1) Inherently less secure than SSSC because its security codes are low rate.
- (2) As with SSSC, in stand-alone operation there is an up-to 5-minute delay between authentication events for any particular signal. The discussion in Drawback 3 of the SSSC technique applies here in full.

6.7. Correlation Profile Anomaly Defense. This stand-alone non-cryptographic defense relies on the difficulty of (1) suppressing the true GPS signals during a spoofing attack, and (2) exactly duplicating the correlation profile of the authentic GPS signals. A preliminary description of this defense is given in [10].

6.7.1. *Benefits.*

- (1) Immediately implementable, low-cost defense.
- (2) No additional hardware required.
- (3) Effective for stationary GPS receivers such as are used for timing applications.

6.7.2. *Drawbacks.*

- (1) Can get confused by multipath when implemented on moving receivers.

6.8. Multi-Antenna Defense. This stand-alone non-cryptographic defense is based on the premise that a spoofer will have great difficulty in mimicking the relative carrier phase of the authentic signals as seen by two or more spatially-separated antennas. The technique is detailed in [11].

6.8.1. *Benefits.*

- (1) Extremely effective spoofing defense when combined with physical security of the antenna array.
- (2) Immediately implementable.

6.8.2. *Drawbacks.*

- (1) Additional antenna(s) and RF front-ends required add cost and weight to the defended receiver.

6.9. Defense Based on Cross-Correlation with Military Signals. This networked cryptographic defense correlates the unknown encrypted military P(Y) code between two civil GPS receivers, exploiting known carrier-phase and code-phase relationships. It is similar to the dual-frequency codeless and semicodeless techniques that civil GPS receivers apply to track the P(Y) code on L2. Originally developed by researchers at Stanford University, the technique has been refined and tested by researchers at Cornell University and the University of Texas [12].

6.9.1. Benefits.

- (1) Strong defense.
- (2) Immediately implementable.
- (3) Less than two second time to detection.

6.9.2. Drawbacks.

- (1) Requires a persistent network connection.
- (2) Computationally expensive.

7. RECOMMENDATIONS

- (1) I recommend that for non-recreational operation in the national airspace, civil unmanned aerial vehicles exceeding 18 lbs be required to employ navigation systems that are spoof-resistant. Spoof resistance will be defined through a series of four canned attack scenarios that can be recreated in a laboratory setting. A navigation system is declared spoof resistant if, for each attack scenario, the system is
 - (a) unaffected by the spoofing attack, or
 - (b) able to detect the spoofing attack.
- (2) More broadly, I recommend that GPS-based timing or navigation systems having a non-trivial role in systems designated by DHS as national critical infrastructure be required to be spoof resistant.
- (3) I recommend that the Department of Homeland Security commit to funding development and implementation of a cryptographic authentication signature in one of the existing or forthcoming civil GPS signals. The signature should at minimum take the form of a digital signature interleaved into the navigation message stream of the WAAS signals. Better would be to interleave the signature into the CNAV or CNAV2 GPS navigation message stream. Best would be to implement the signature as a spread spectrum security code interleaved into the spreading code of the L1C data channel.

REFERENCES

- [1] Anon., “Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System,” tech. rep., John A. Volpe National Transportation Systems Center, 2001.
- [2] D. Shepard, T. Humphreys, and A. Fansler, “Evaluation of the vulnerability of Phasor Measurement Units to GPS spoofing,” in *Sixth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, (Washington, DC), 2012.
- [3] J. Giri, D. Sun, and R. Avila-Rosales, “Wanted: A more intelligent grid,” *IEEE Power & Energy*, pp. 34–40, April 2009.

- [4] E. O. Schweitzer, A. Guzman, H. J. Altuve, and D. A. Tziouvaras, "Real-time synchrophasor applications for wide-area protection, control, and monitoring," tech. rep., Schweitzer Eng. Laboratories, 2009.
- [5] J. S. Warner and R. G. Johnston, "A simple demonstration that the gps is vulnerable to spoofing," *The Journal of Security Administration*, vol. 25, pp. 19–28, 2002.
- [6] J. Nielsen, A. Broumandan, and G. LaChapelle, "Method and system for detecting GNSS spoofing signals," May 31 2011. US Patent 7,952,519.
- [7] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proceedings of the ION GNSS Meeting*, (Portland, Oregon), pp. 1542–1552, Institute of Navigation, 2003.
- [8] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, 2011. to be published; available at <http://radionavlab.ae.utexas.edu/detstrat>.
- [9] K. Wesson, M. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION, Journal of the Institute of Navigation*, 2012. to be published; available at <http://radionavlab.ae.utexas.edu/nma>.
- [10] K. Wesson, D. Shepard, J. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proceedings of the ION GNSS Meeting*, (Portland, Oregon), Institute of Navigation, 2011.
- [11] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "A multi-antenna defense: Receiver-autonomous GPS spoofing detection," *Inside GNSS*, vol. 4, pp. 40–46, April 2009.
- [12] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, 2012. submitted for review; available at <http://web.mae.cornell.edu/psiaki/>.

THE UNIVERSITY OF TEXAS AT AUSTIN

E-mail address: todd.humphreys@mail.utexas.edu