Drone Hack

Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle

A radio signal sent from a half-mile away deceived the GPS receiver of a UAV into thinking that it was rising straight up. In this way, the UAV's dependence on civil GPS allowed the spoofer operator to force the UAV vertically downward in dramatic fashion as part of multiple capture demonstrations.

Daniel P. Shepard,
Jahshan A. Bhatti,
and Todd E. Humphreys

In December 2011, Iran captured a U.S. Central Intelligence Agency (CIA) surveillance drone with only minor damage to the undercarriage of the drone, likely due to a rough landing when captured. An Iranian engineer claimed in an interview that "Iran managed to jam the drone's communication links to American operators" causing the drone to shift into an autopilot mode that relies solely on GPS to guide itself back to its home base in Afghanistan. With the drone in this state, the Iranian engineer claimed that "Iran spoofed the drone's GPS system with false coordinates, fooling it into thinking it was close to home and landing into Iran's clutches."

Although the Iranian claims are highly questionable, this incident left many unanswered questions as to the security of GPS systems on unmanned aerial vehicles (UAVs). The CIA drone should have been guiding itself based on the encrypted military GPS signals, which would be incredibly difficult to spoof. However, some experts have conjectured that simultaneous jamming of the military signals and spoofing of the civilian signals might have worked if the drone had been programmed to fall back on the civilian GPS signals in the event that the military signals were jammed. This raises the question: How difficult would it be to spoof a UAV guiding itself based on civilian GPS signals?

▲ **UNMANNED AERIAL VEHICLE (UAV)** used in the spoofing tests; owned by the University of Texas.

FAA Modernization Act

In February of this year, Congress passed the FAA Modernization and Reform Act of 2012. According to the Library of Congress summary, this act "requires the Secretary [of Transportation] to develop a plan to accelerate safely the integration by September 30, 2015, of civil unmanned aircraft systems (UASes, or drones) into the national airspace system … [and] determine if certain drones may operate safely in the national airspace system before completion of the plan."

Such civilian UAVs would be primarily guided by civil GPS, which has been shown to be readily spoofable in the lab. This would create a significant potential hazard in the national airspace if the problem of civil GPS spoofing is not fixed. Thousands of civilian UAVs (operated by postal services, police departments, research institutions, and others) could populate the skies in only a few years while still being vulnerable to remote hijacking via GPS spoofing. The passing of the FAA Modernization Act further emphasizes the need to examine the vulnerability of UAVs to GPS spoofing.

Test

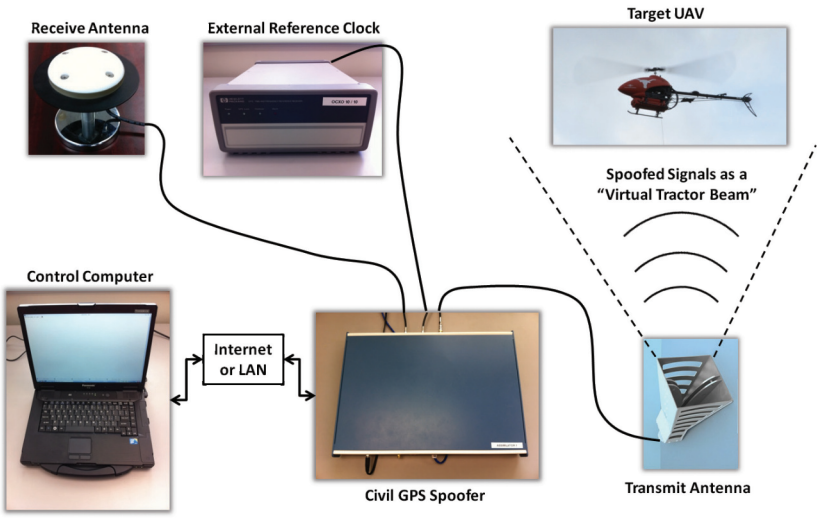
On invitation of the Department of Homeland Security (DHS), unclassified spoofing tests against a UAV were performed at White Sands Missile Range (WSMR) on June 19, 2012 during the DHS GYPSY test exercise. These tests demonstrated the capability of a spoofer, built by the University of Texas (UT) Radionavigation Lab, to commandeer a civilian UAV by

influencing the position-velocity-time (PVT) solution of the UAV's GPS receiver.

The Spoofer. The civil GPS spoofer used for these tests is an advanced version of the spoofer reported in "Assessing the Spoofing Threat," GPS World, January 2009. A schematic representation of the spoofer is shown on PAGE 34. It is the only spoofer reported in open literature to date that is capable of precisely aligning the spreading codes and navigation data of its counterfeit signals with those of the authentic GPS signals. Such alignment capability allows the spoofer to carry out a sophisticated spoofing attack in which no obvious clues remain to suggest that an attack is underway. The spoofer is implemented on a portable software-defined radio platform with a digital signal processor (DSP) at its core. This platform comprises:

- A radio frequency (RF) front-end that down-mixes and digitizes GPS L1 and L2 frequencies
- A DSP board that performs acquisition and tracking of GPS L1 C/A, calculates a navigation solution, predicts the L1 C/A databits, and produces a consistent set of up to 14 spoofed GPS L1 C/A signals with a user-controlled fictitious implied navigation and timing solution.
- An RF back-end with a digital attenuator that converts the digital samples of the spoofed signals from the DSP to analog output at the GPS L1 frequency with a user-controlled broadcast power.
- A single-board computer that handles communication between the spoofer and a remote computer over the Internet.

The spoofer works by first acquiring and tracking GPS L1 C/A and L2C signals to obtain a navigation solution. It then enters its "feedback" mode, in which it produces a counterfeit, data-free feedback GPS signal that is summed with its own antenna input. The feedback signal is tracked by the spoofer and used to calibrate the delay between production of the digitized spoofed signal and output of the analog spoofed signal. This is necessary because the delay is non-deterministic on start-up of the receiver, although it stays constant thereafter.



▲ **FIGURE 1** Schematic of the test setup.

After feedback calibration is complete and enough time has elapsed to build up a navigation data bit library, the spoofer is ready to begin an attack. Initially, it produces signals that are aligned to within a few meters with the authentic signals at the location of the target antenna but have low enough power that they remain far below the target receiver's noise floor. The spoofer then raises the power of the spoofed signals slightly above that of the authentic signals. At this point, the spoofer has taken control of the victim receiver's tracking loops and can slowly lead the spoofed signals away from the authentic signals, carrying the receiver's tracking loops with it. The target receiver can be considered completely captured when either of the following are true:

- each spoofed signal has shifted by 2 μs relative to the authentic signals, or
- each spoofed signal is at least 10 dB more powerful than the corresponding authentic signal.

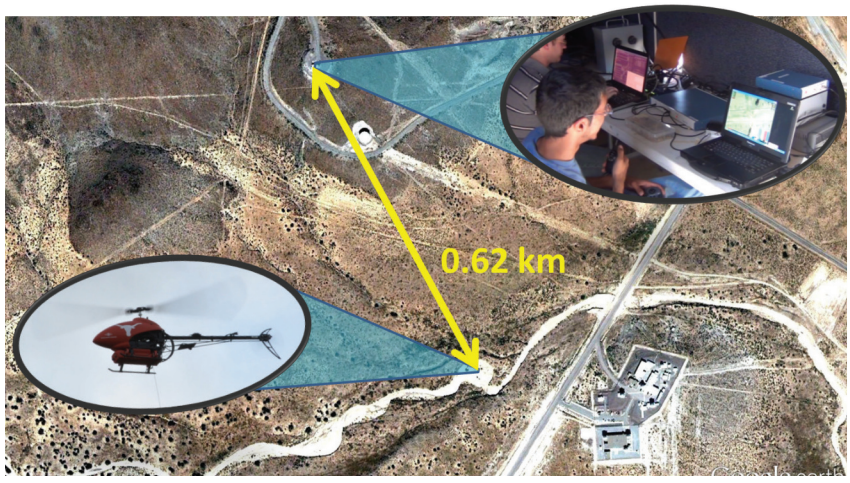
The latter option ensures that there is no significant interaction between authentic and spoofed signals by simultaneously jamming and spoofing.

The UT spoofer and attack strategy have been tested against a wide variety of civil GPS receivers and have always been successful in commandeering the target receiver.

Test UAV. The spoofing tests targeted a University-of-Texas-owned Hornet Mini UAV supplied by Adaptive Flight, which is shown in the OPENING PHOTO. The Hornet Mini is roughly five feet long and weighs about 10 pounds when fully loaded. The Mini's sophisticated avionics package loosely couples an altimeter, magnetometer, and a MEMS IMU package to a GPS receiver via an extended Kalman filter.

The Hornet Mini is representative of UAVs used by law enforcement. Thus, the results of the spoofing tests with the Mini also apply to other similarly-designed UAVs, including those used in most civil applications, whose navigation systems are centered on civil GPS. It should be noted that no special alterations were made to the Hornet Mini for this test – it was in its "as sold" or "stock" configuration.

Setup. A schematic of the setup used for the spoofing tests against the civil UAV at WSMR appears in FIGURE 1. The spoofer was located on a hilltop with the receive antenna on the far side of the hilltop from the transmit antenna as shown in FIGURE 2. The UAV site was located in a sandy basin approximately



▲ **FIGURE 2** Aerial view of the test site showing the spoofer location on a hilltop and the UAV site 0.62 kilometers away.

620 meters from the transmit antenna.

Procedure. The UAV was commanded by its ground controller to hover approximately 60 feet above ground level at the UAV site. After the initial ground control command was sent, the UAV maintained its hovering position automatically based on the navigation solution of its extended Kalman filter, which is based in part on GPS. At this point in the test procedure, the spoofed signals were not being broadcast: the UAV was only under the influence of the authentic GPS signals.

The spoofer was then commanded to begin transmitting spoofed signals. To ensure seamless capture of the UAV's GPS unit, the code phases of the spoofed signals were aligned to within meters of the authentic signals at the location of the UAV's GPS antenna. The spoofed signals overpowered their authentic counterparts and instantly captured the tracking loops within the UAV's GPS receiver.

Immediately after capture, the spoofer induced a false velocity and corresponding position change in the UAV's GPS receiver, drawing the position reported by the UAV's extended Kalman filter away from the UAV's commanded hover position. To compensate, the UAV's flight controller responded by moving in the opposite direction. A safety pilot was on hand to prevent the UAV from drifting out of control. This was necessary because by commandeering the UAV's GPS receiver, the spoofer operator effectively breaks the UAV autopilot's feedback control loop. The spoofer operator must now act as an operator-in-the-loop, which requires real-time, meter-level knowledge of the UAV's true location.

Results. Between tests WSMR and UT, the spoofer demonstrated short-term 3-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.

Interestingly, the Hornet Mini relies only on its altimeter for direct measurements of its vertical position; the GPS-measured vertical position is ignored. This can be done with reasonable accuracy because of the Hornet Mini's short flight endurance (~20 minutes). However, the GPS vertical velocity does affect the extended Kalman filter's vertical coordinate estimate because the filter propagates GPS velocity measurements through a UAV dynamics model to form an a priori vertical estimate that gets updated with the altimeter measurements. This dependence on GPS velocity allowed the spoofer operator to force the UAV vertically downward in dramatic fashion in the final three capture demonstrations.

Developing a full spoofer-based control system for a UAV is a difficult problem that, in addition to the requirement for real-time true position feedback, requires the spoofer to model the UAV's feedback control behavior and to estimate the UAV's desired path. Causing a UAV to spin out of control and crash is not difficult with a spoofer, but fine-grained control certainly is.

Implications

These tests have demonstrated that civilian UAVs will be vulnerable to control by malefactors with a civil GPS spoofer looking to hijack or crash these UAVs unless their vulnerability to GPS spoofing is addressed. There are several reasons why someone may want to spoof a drone including fear over drones invading people's privacy. This poses a significant safety concern that could result in mid-air collisions with other aerial vehicles or buildings, not to mention loss of property.

Constructing from scratch a sophisticated GPS spoofer like the one developed by UT is not easy, nor is it within the capability of the average anonymous hacker. It is orders of magnitude harder than developing a GNSS 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 significantly lowered the bar to spoofer development in recent years.

As a point of reference, we estimate that there are more than 100 researchers in universities around the globe who are well-enough versed in software-defined GPS that they could develop a sophisticated spoofer from scratch with a year of dedicated effort. More worrisome is the fact that one does not have to build a sophisticated spoofer like ours, capable of aligning its signals precisely with authentic signals at the location of a chosen target, to spoof a civil GPS receiver. A low-cost off-the-shelf GPS signal simulator would not permit the kind of seamless attack we carried out, but would be adequate to confuse and disrupt the navigation system of a commercial UAV.

Fixing the Problem

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. Nonetheless, there are many possible remedies to the spoofing problem that, while not foolproof, would vastly improve civil GPS security. These defenses can be broken up into two categories: cryptographic and non-cryptographic defenses.

Cryptographic defenses come primarily in two forms, spread-spectrum security codes (SSSC) and navigation message authentication (NMA), depending on whether the unpredictable digital signature is placed on the spread-spectrum code or the navigation data. These cryptographic signatures could be placed on WAAS signals or existing or future GPS signals to provide authentication of the source of the WAAS or GPS signals. A cryptographic defense implemented with appropriate checks to protect against certain variants of spoofing attacks, described in "Straight Talk on Anti-Spoofing," GPS World, January 2012, would significantly raise the bar for a would-be spoofer. Several proposals for cryptographic methods are currently on the table including a proposal by Logan Scott to place SSSC signatures on GPS L1C signals that will be broadcast by GPS Block III satellites. However, the current proposals for civil GPS cryptographic authentication schemes are still at least several years away from implementation and have a 5-minute window between authentications of each individual GPS signal. These proposals have currently gained no ground in being implemented because of a lack of dedicated funds for development and implementation.

There are also a number of promising non-cryptographic techniques for civil GPS spoofing detection that include jamming-to-noise power detectors (J/N meters), correlation profile anomaly defenses, and antenna-based defenses. J/N meters are simple and easily-implementable and would prevent a spoofer from simultaneous jamming and spoofing. However, 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. The inclusion of a J/N meter does ensure that the authentic signals will also be visible as a corruption to the correlation curve during a spoofing attack, due to the difficulty of nulling out the authentic signal. This allows correlation profile anomaly defenses to be viable. However, these methods suffer from the difficulty of distinguishing multipath effects from a spoofing attack, particularly in mobile receivers. Antenna-based defenses also present an attractive option for anti-spoofing, but most of these methods require additional hardware (multiple antennas) and cost. One promising new antenna-based defense is currently under development at Cornell University that does not require multiple antennas. This defense involves an extension of the signal spatial correlation technque developed by the University of Calgary PLAN group. However, this technique is still under development, and receivers implementing this technique would likely be several times more expensive than current receivers.

For details on potential spoofing defenses, see Todd Humphrey's Congressional testimony on page 14.

Recommendations

We recommend that for non-recreational operation in the national airspace, civil UAVs exceeding 18 pounds 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 either unaffected by or able to detect the spoofing attack. Spoofing detection combined with an appropriate GPS-denied mode for the UAV to fall back on will significantly increase the difficulty of mounting a successful spoofing attack.

Additionally, civil GPS receivers in many critical infrastructures (communications networks, financial trade centers, and the power grid) are also vulnerable to civil GPS spoofing. These critical infrastructures primarily rely on GPS for timing, which is also susceptible to manipulation with varying consequences depending on the application. A discussion of power grid vulnerabilities to GPS spoofing is given in "Going Up Against Time" in this issue of the magazine on page 34. We also 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, we recommend that funding be committed for 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. A better plan would be to interleave the signature into the CNAV or CNAV2 GPS navigation message stream. The best plan for implementing a cryptographic authentication signature would be to implement the signature as an SSSC interleaved into the spreading code of the L1C data channel. Inclusion of a cryptographic signature would greatly aid manufacturers in developing receivers that are spoof-resistant.

Manufacturers

The Hornet Mini UAV carries a **µBlox** GPS receiver.

DANIEL P. SHEPARD is pursuing M.S. and Ph.D. degrees in aerospace engineering at the University of Texas (UT) at Austin. He is a member of the Radionavigation Laboratory.

JAHSHAN A. BHATTI is pursuing a Ph.D. in aerospace engineering and engineering mechanics at UT and is a member of the Radionavigation Laboratory.

TODD E. HUMPHREYS is an assistant professor of aerospace engineering and engineering mechanics at UT and director of the Radionavigation Laboratory. He received a Ph.D. in aerospace engineering from Cornell University.