# Straight Talk on Anti-Spoofing

## Securing the Future of PNT

Disruption created by intentional generation of fake GPS signals could have serious economic consequences. This article discusses how typical civil GPS receivers respond to an advanced civil GPS spoofing attack, and four techniques to counter such attacks: spread-spectrum security codes, navigation message authentication, dual-receiver correlation of military signals, and vestigial signal defense. Unfortunately, any kind of anti-spoofing, however necessary, is a tough sell.

Kyle Wesson, Daniel Shepard, and Todd Humphreys

GPS spoofing has become a hot topic. At the 2011 Institute of Navigation (ION) GNSS conference, 18 papers discussed spoofing, compared with the same number over the past decade. ION-GNSS also featured its first panel session on anti-spoofing, called "Improving Security of GNSS Receivers," which offered six security experts a forum to debate the most promising anti-spoofing technologies.

The spoofing threat has also drawn renewed U.S. government scrutiny since the initial findings of the 2001 Volpe Report. In November 2010, the U.S. Position Navigation and Timing National Executive Committee requested that the U.S. Department of Homeland Security (DHS) conduct a comprehensive risk assessment on the use of civil GPS. In February 2011, the DHS Homeland Infrastructure Threat and Risk Analysis Center began its investigation in conjunction with subject-matter experts in academia, finance, power, and telecommunications, among others. Their findings will be summarized in two forthcoming reports, one on the spoofing and jamming threat and the other on possible mitigation techniques. The reports are anticipated to show that GPS disruption due to spoofing or jamming could have serious economic consequences.

Effective techniques exist to defend receivers against spoofing attacks. This article summarizes state-of-the-art anti-spoofing techniques and suggests a path forward to equip civil GPS receivers with these defenses. We start with an analysis of a typical civil GPS receiver's response to our laboratory's powerful spoofing device. This will illustrate the range of freedom a spoofer has when commandeering a victim receiver's tracking loops. We will then provide an overview of promising cryptographic and non-cryptographic anti-spoofing techniques and highlight the obstacles that impede their widespread adoption.

## The Spoofing Threat

Spoofing is the transmission of matched-GPS-signal-structure interference in an attempt to commandeer the tracking loops of a victim receiver and thereby manipulate the receiver's timing or navigation solution. A spoofer can transmit its counterfeit signals from a stand-off distance of several hundred meters or it can be co-located with its victim.

Spoofing attacks can be classified as simple, intermediate, or sophisticated in terms of their effectiveness and subtlety. In 2003, the Vulnerability Assessment Team at Argonne National Laboratory carried off a successful simple attack in which they programmed a GPS signal simulator to broadcast high-powered counterfeit GPS signals toward a victim receiver. Although such a simple attack is easy to mount, the equipment is expensive, and the attack is readily detected because the counterfeit signals are not synchronized to their authentic counterparts.

In an intermediate spoofing attack, a spoofer synchronizes its counterfeit signals with the authentic GPS signals so they are code-phase-aligned at the target receiver. This method requires a spoofer to determine the position and velocity of the victim receiver, but it affords the spoofer a serious advantage: the attack is difficult to detect and mitigate.

The sophisticated attack involves a network of coordinated intermediate-type spoofers that replicate not only the content and mutual alignment of visible GPS signals but also their spatial distribution, thus fooling even multi-antenna spoofing defenses.

▲ **SPOOFING TESTBED** at the University of Texas Radionavigation Laboratory, an advanced and powerful suite for anti-spoofing research. On the right are several of the civil GPS receivers tested and the radio-frequency test enclosure, and on the left are the phasor measurement unit and the civil GPS spoofer.

**Lab Attack.** So far, no open literature has reported development or research into the sophisticated attack. This is likely because of the success of the intermediate-type attack: to date, no civil GPS receiver tested in our laboratory has fended off an intermediate-type spoofing attack. The spoofing attacks, which are always conducted via coaxial cable or in radio-frequency test enclosures, are performed with our laboratory's receiver-spoofer, an advanced version of the one introduced at the 2008 ION-GNSS conference (see "Assessing the Spoofing Threat," *GPS World*, January 2009).

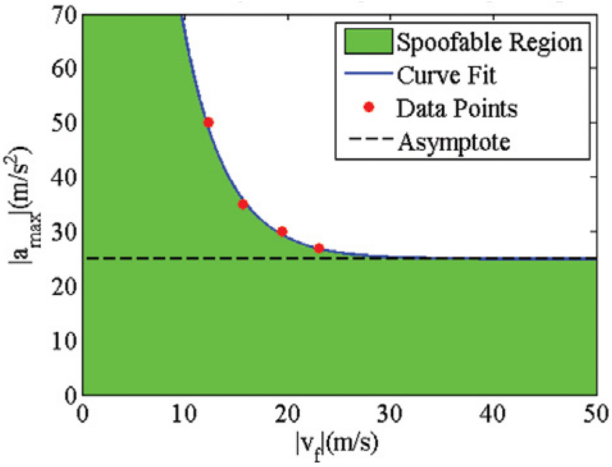
To commence the attack, the spoofer transmits its counterfeit signals in code-phase alignment with the authentic signals but at power level below the noise floor. The spoofer then increases the power of the spoofed signals so that they are slightly greater than the power of the authentic signals. At 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. Once the spoofed signals have moved more than 600 meters in position or 2 microseconds in time away from the authentic signals, the receiver can be considered completely owned by the spoofer.

Although our spoofer fooled all of the receivers tested in our laboratory, there are significant differences between receivers' dynamic responses to spoofing attacks. It is important to understand the types of dynamics that a spoofer can induce in a target receiver to gain insight into the actual dangers that a spoofing attack poses rather than rely on unrealistic assumptions or models of a spoofing attack. For example, a recent paper on time-stamp manipulation of the U.S. power grid assumed that there was no limit to the rate of change that a spoofer could impose on a victim receiver's position and timing solution, which led to unrealistic conclusions.

Experiments performed in our laboratory sought to answer three specific questions regarding spoofer-induced dynamics:

- How quickly can a timing or position bias be introduced?
- What kinds of oscillations can a spoofer cause in a receiver's position and timing?
- How different are receiver responses to spoofing?

These questions were answered by determining the maximum spoofer-induced pseudorange acceleration that can be used to reach a certain final velocity when starting from a velocity of zero, without raising any alarms or causing the target receiver



▲ **FIGURE 1** Theoretical and experimental test results for a high-quality handheld receiver's dynamic response to a spoofing attack. Although not shown here, the maximum attainable velocity is around 1,300 meters/second.

to lose satellite lock. The curve in the velocity-acceleration plane created by connecting these points defines the upper bound of a region within which the spoofer can safely manipulate the target receiver. These data points can be obtained empirically and fit to an exponential curve. Alarms on the receiver may cause some deviations from this curve depending on the particular receiver.

**FIGURE 1** shows an example of the velocity-acceleration curve for a high-quality handheld receiver, whose position and timing solution can be manipulated quite aggressively during a spoofing attack. These results suggest that the receiver's robustness — its ability to provide navigation and timing solutions despite extreme signal dynamics — is actually a liability in regard to spoofing. The receiver's ability to track high accelerations and velocities allows a spoofer to aggressively manipulate its navigation solution.

The relative ease with which a spoofer can manipulate some GPS receivers suggests that GPS-dependent infrastructure is vulnerable. For example, the telecommunications network and the power grid both rely on GPS time-reference receivers for accurate timing. Our laboratory has performed tests on such receivers to determine the disruptions that a successful spoofing attack could cause. The remainder of this section highlights threats to these two sectors of critical national infrastructure.

**Cell-Phone Vulnerability.** 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 microseconds from GPS time, hand-off to and from that tower is disrupted. Our tests indicate that a spoofer could induce a 10-microsecond time deviation within about 30 minutes for a typical CDMA tower setup. A spoofer, or spoofer network, could also cause multiple neighboring towers to interfere with one another. This is possible because CDMA cell-phone towers all use the same spreading code and distinguish themselves only by the phasing (that is, time offset) of their spreading codes. Furthermore, it appears that a spoofer could impair CDMA-based E911 user-location.

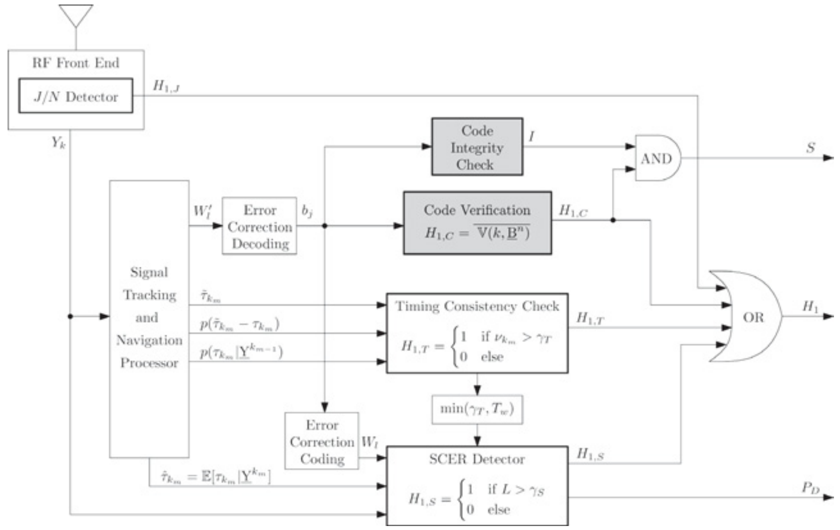
**Power-Grid Vulnerability.** Like the cellular network, the power grid of the future will rely on accurate GPS time-stamps. The efficiency of power distribution across the grid can be improved with real-time measurements of the voltage and current phasors. Phasor measurement units (PMUs) have been proposed as a smart-grid technology for precisely this purpose. PMUs rely on GPS to time-stamp their measurements, which are sent back to a central monitoring station for processing. Currently, PMUs are used for closed-loop grid control in only a few applications, but power-grid modernization efforts will likely rely more heavily on PMUs for control. If a spoofer 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 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. Tests demonstrate that a spoofer could cause variations in a PMU's measured voltage phase angle at a rate of 1.73 degrees per minute. Thus, a spoofing attack could create the false indications of power flow across the grid. The tests results also reveal, however, that it is impossible for a spoofer to cause changes in small-signal grid stability estimates, which would require the spoofer to induce rapid (for example, 0.1–3 Hz) microsecond-amplitude oscillations in timing. Such oscillations correspond to spoofing dynamics well outside the region of freedom of all receivers we have tested. A spoofer might also be able to affect fault-location estimates obtained through time-difference-of-arrival techniques using PMU measurements. This could cause large errors in fault-location estimates and hamper repair efforts.

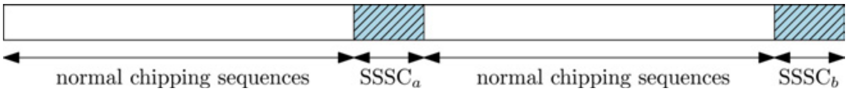
**What Can Be Done?** Despite the success of the intermediate-type spoofing attack against a wide variety of civil GPS receivers and the known vulnerabilities of GPS-dependent critical infrastructure to spoofing attacks, anti-spoofing techniques exist that would enable receivers to successfully defend themselves against such attacks. We now turn to four promising anti-spoofing techniques.

## Cryptographic Methods

These techniques enable a receiver to differentiate authentic GPS signals from counterfeit signals with high likelihood.


RF Front End
$J/N$ Detector
$H_{1,J}$
$Y_k$
Code Integrity Check
$I$
AND
$S$
Signal Tracking and Navigation Processor
$W_l'$
Error Correction Decoding
$b_j$
Code Verification
$H_{1,C} = \overline{\mathbb{V}(k, \underline{B}^n)}$
$H_{1,C}$
OR
$H_1$
$\tilde{\tau}_{k_m}$
$p(\tilde{\tau}_{k_m} - \tau_{k_m})$
$p(\tau_{k_m} | \underline{Y}^{k_{m-1}})$
Timing Consistency Check
$H_{1,T} = \begin{cases} 1 & \text{if } \nu_{k_m} > \gamma_T \\ 0 & \text{else} \end{cases}$
$H_{1,T}$
$\min(\gamma_T, T_w)$
Error Correction Coding
$W_l$
SCER Detector
$H_{1,S} = \begin{cases} 1 & \text{if } L > \gamma_S \\ 0 & \text{else} \end{cases}$
$H_{1,S}$
$\hat{\tau}_{k_m} = \mathbb{E}[\tau_{k_m} | \underline{Y}^{k_m}]$
$P_D$

▲ **FIGURE 2** GNSS receiver components required for GNSS signal authentication. Components that support code origin authentication are outlined in bold and have a gray fill, whereas components that support code timing authentication are outlined in bold and have no fill. The schematic assumes a security code based on navigation message authentication.



▲ **FIGURE 3** Placement of the periodically unpredictable spread spectrum security codes in the GPS L1C data channel spreading sequence.

Cryptographic strategies rely on the unpredictability of so-called security codes that modulate the GPS signal. An unpredictable code forces a spoofer who wishes to mount a successful spoofing attack to either

- estimate the unpredictable chips on-the-fly, or
- record and play back authentic GPS spectrum (a meaconing attack).

To avoid unrealistic expectations, it should be noted that no anti-spoofing technique is completely impervious to spoofing. GPS signal authentication is inherently probabilistic, even when rooted in cryptography. Many separate detectors and cross-checks, each with its own probability of false alarm, are involved in cryptographic spoofing detection. **FIGURE 2** illustrates how the jammer-to-noise ratio detector, timing consistency check, security-code estimation and replay attack (SCER) detector, and cryptographic verification block all work together. This hybrid combination of statistical hypothesis tests and Boolean logic demonstrates the complexities and subtleties behind a comprehensive, probabilistic GPS signal authentication strategy for security-enhanced signals.

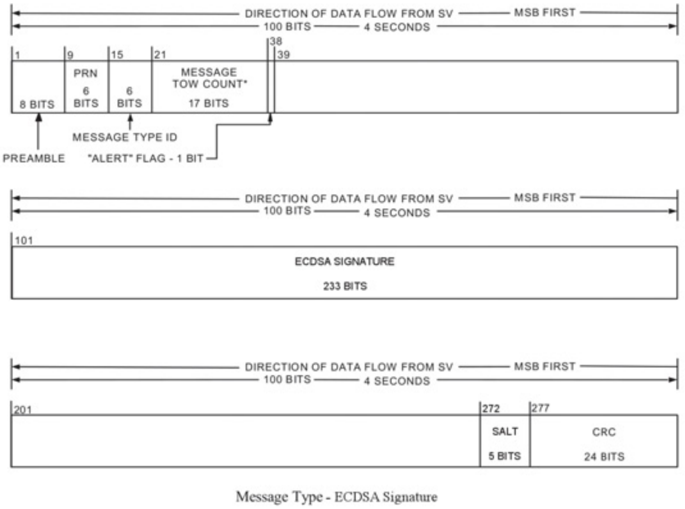
**Spread Spectrum Security Codes.** In 2003, Logan Scott proposed a cryptographic anti-spoofing technique based on spread spectrum security codes (SSSCs). The most recent proposed version of this technique targets the L1C signal, which will be broadcast on GPS Block III satellites, because the L1C waveform is not yet finalized. Unpredictable SSSCs could be interleaved with the L1C spreading code on the L1C data channel, as illustrated in **FIGURE 3**. Since L1C acquisition and tracking occurs on the pilot channel, the presence of the SSSCs has negligible impact on receivers. Once tracking L1C, a receiver can predict when the next SSSC will be broadcast but not its exact sequence. Upon reception of an SSSC, the receiver stores the front-end samples corresponding to the SSSC interval in memory. Sometime later, the cryptographic digital key that generated the SSSC is transmitted over the navigation message. With knowledge of the digital key, the receiver generates a copy of the actual transmitted SSSC and correlates it with the previously-recorded digital samples. Spoofing is declared if the correlation power falls below a pre-determined threshold.

When the security-code chip interval is short (high chipping rate), it is difficult for a spoofer to estimate and replay the security code in real time. Thus, the SSSC technique on L1C offers a strong spoofing defense since the L1C chipping rate is high (that is, 1.023 MChips/second). Furthermore, the SSSC technique does not rely on the receiver obtaining additional information from a side channel; all the relevant codes and keys are broadcast over the secured GPS signals. Of course a disadvantage for SSSC is that it requires a fairly fundamental change to the currently-proposed L1C definition: the L1C spreading codes must be altered.

Implementation of the SSSC technique faces long odds, partly because it is late in the L1C planning schedule to introduce a change to the spreading codes. Nonetheless, in September 2011, Logan Scott and Phillip Ward advocated for SSSC at the Public Interface Control Working Group meeting, passing the first of many wickets. The proposal and associated Request for Change document will now proceed to the Lower Level GPS Engineering Requirements Branch for further technical review. If approved there, it passes to the Joint Change Review Board for additional review and, if again approved, to the Technical Interchange Meeting for further consideration. The chances that the SSSC proposal will survive this gauntlet would be much improved if some government agency made a formal request to the GPS Directorate to include SSSCs in L1C — and provided the funding to do so. The DHS seems to us a logical sponsoring agency.

**Navigation Message Authentication.** If an L1C SSSC implementation proves unworkable, an alternative, less-invasive cryptographic authentication scheme based on navigation message authentication (NMA) represents a strong fall-back option. In the same 2003 ION-GNSS paper that he proposed SSSC, Logan Scott also proposed NMA. His paper was preceded by an internal study at MITRE and followed by other publications in the open literature, all of which found merit in the NMA approach. The NMA technique embeds public-key digital signatures into the flexible GPS civil navigation (CNAV) message, which offers a convenient conveyance for such signatures. The CNAV format was designed to be extensible 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.

Our lab recently demonstrated that NMA works to authenticate not only the navigation message but also the underlying signal. In other words, NMA can be the basis of comprehensive signal authentication. We have proposed a specific implementation of NMA that is packaged for immediate adoption. Our proposal defines two new CNAV messages that deliver a standardized public-key elliptic-curve digital algorithm (ECDSA) signature via the message format in **FIGURE 4**.



▲ **FIGURE 4** Format of the proposed CNAV ECDSA signature message, which delivers the first or second half of the 466-bit ECDSA signature and a 5-bit salt in the 238-bit payload field.

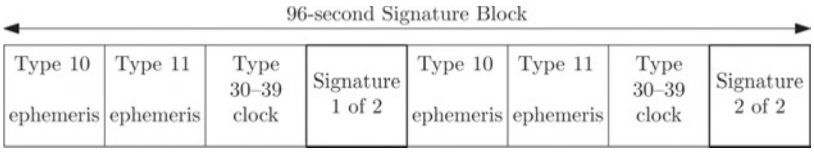
Although the CNAV message format is flexible, it is not without constraints. The shortest block of data in which a complete signature can be embedded is a 96-second signature block such as the one shown in **FIGURE 5**. In this structure, the two CNAV signature messages are interleaved between the ephemeris and clock data to meet the broadcast requirements.

The choice of the duration between signature blocks is a tradeoff between offering frequent authentication and maintaining a low percentage of the CNAV message reserved for the digital signature. In our proposal, signature blocks are transmitted roughly every five minutes (**FIGURE 6**) so that only 7.5 percent of the navigation message is devoted to the digital signature. Across the GPS constellation, the signature block could be offset so that a receiver could authenticate at least one channel approximately every 30 seconds. Like SSSC, our proposed version of NMA does not require a receiver's getting additional information from a side channel, provided the receiver obtains public key updates on a yearly basis.

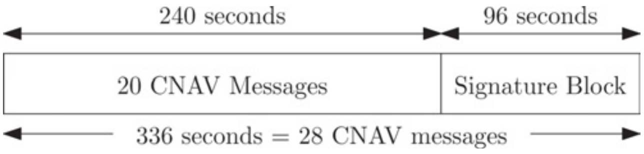
NMA is inherently less secure than SSSC. A NMA security code chip interval (that is, 20 milliseconds) is longer than a SSSC chip interval, thereby allowing the spoofer more time to estimate the digital signature on-the-fly. That is not to say, however, that NMA is ineffective. In fact, tests with our laboratory's spoofing testbed demonstrated the NMA-based signal authentication structure described earlier offered a receiver a better-than 95 percent probability of detecting a spoofing attack for a 0.01 percent probability of false alarm under a challenging spoofing-attack scenario.

NMA is best viewed as a hedge. If the SSSC approach does not gain traction, then NMA might, since it only requires defining two new CNAV messages in the GPS IS — a relatively minor modification. CNAV-based NMA could defend receivers tracking L2C and L5. A new CNAV2 message will eventually be broadcast on L1 via L1C, so a repackaged CNAV2-based NMA technique could offer even single-frequency L1 receivers a signal-side anti-spoofing defense.

**P(Y) Code Dual-Receiver Correlation.** This approach avoids entirely the issue of GPS IS modifications. The technique 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 semi-codeless techniques that civil GPS receivers apply to track the P(Y) code on L2. Peter Levin and others filed a patent on the codeless-based signal



▲ **FIGURE 5** The shortest broadcast signature block that does not violate the CNAV ephemeris and timing broadcast requirements. To meet the required broadcast interval of 48 seconds for message types 10, 11, and one of 30–39, the ECDSA signature is broadcast over a 96-second signature block that is composed of eight CNAV messages.



▲ **FIGURE 6** A signed 336-second broadcast. The proposed strategy signs every 28 CNAV messages with a signature broadcast over two CNAV messages on each broadcast channel.

authentication technique in 2008; Mark Psiaki extended the approach to semicodeless correlation and narrowband receivers in a 2011 ION-GNSS paper.

In the dual-receiver technique, one receiver, stationed in a secure location, tracks the authentic L1 C/A codes while receiving the encrypted P(Y) code. The secure receiver exploits the known timing and phase relationships between the C/A code and P(Y) code to isolate the P(Y) code, of which it sends raw samples (codeless technique) or estimates of the encrypting W-code chips (semi-codeless technique) over a secure network to the defending receiver. The defending receiver correlates its locally-extracted P(Y) with the samples or W-code estimates from the secure receiver. If a spoofing attack is underway, the correlation power will drop below a statistical threshold, thereby causing the defending receiver to declare a spoofing attack. Although the P(Y) code is 20 MHz wide, a narrowband civil GPS receiver with 2.6 MHz bandwidth can still perform the statistical hypothesis tests even with the resulting 5.5 dB attenuation of the P(Y) code. Because the dual-receiver method can run continuously in the background as part of a receiver's standard GPS signal processing, it can declare a spoofing attack within seconds — a valuable feature for many applications.

Two considerations about the dual-receiver technique are worth noting. First, the secure receiver must be protected from spoofing for the technique to succeed. Second, the technique requires a secure communication link between the two receivers. Although the first requirement is easily achieved by locating secure receivers in secure locations, the second requirement makes the technique impractical for some applications that cannot support a continuous communication link.

Of all the proposed cryptographic anti-spoofing techniques, only the dual-receiver method could be implemented today. Unfortunately the P(Y) code will no longer exist after 2021, meaning that systems that make use of the P(Y)-based dual-receiver technique will be rendered unprotected, although a similar M-code-based technique could be an effective replacement.

@ ION 2011
"This is not the end...
It is not even the beginning of the end.
But it is, perhaps, the end of the beginning."
Winston Churchill describing Locata's finest hour.
HISTORY REPEATS ITSELF – GPS REBORN
ON ▸ NO ATOMIC CLOCKS ▸ NO DATA LINKS ▸ NO SATELLITES ▸ THE LOCA
YOUR OWN GPS
The Local Constellation is launched – ION 2011
Locata
www.locatacorp.com

The dual-receiver method, therefore, is best thought of as a stop-gap: it can provide civil GPS receivers with an effective anti-spoofing technique today until a signal-side civil GPS authentication technique is approved and implemented in the future This sentiment was the consensus of the panel experts at the 2011 ION-GNSS session on civil GPS receiver security.

## Non-Cryptographic Methods

Non-cryptographic techniques are enticing because they can be made receiver-autonomous, requiring neither security-enhanced civil GPS signals nor a side-channel communication link. The literature contains a number of proposed non-cryptographic anti-spoofing techniques. Frequently, however, these techniques rely on additional hardware, such as accelerometers or inertial measurements units, which may exceed the cost, size, or weight requirements in many applications. This motivates research to develop software-based, receiver-autonomous anti-spoofing methods.

**Vestigial Signal Defense (VSD).** This software-based, receiver-autonomous anti-spoofing technique relies on the difficulty of suppressing the true GPS signal during a spoofing attack. Unless the spoofer generates a phase-aligned nulling signal at the phase center of the victim GPS receiver's antenna, a vestige of the authentic signal remains and manifests as a distortion of the complex correlation function. VSD monitors distortion in the complex correlation domain to determine if a spoofing attack is underway.

To be an effective defense, the VSD must overcome a significant challenge: it must distinguish between spoofing and multipath. The interaction of the authentic and spoofed GPS signals is similar to the interaction of direct-path and multipath GPS signals. Our most recent work on the VSD suggests that differentiating spoofing from multipath is enough of a challenge that the goal of the VSD should only be to reduce the degrees-of-freedom available to a spoofer, forcing the spoofer to act in a way that makes the spoofing signal or vestige of the authentic GPS signal mimic multipath. In other words, the VSD seeks to corner the spoofer and reduce its space of possible dynamics.

Among other options, two potential effective VSD techniques are

- a maximum-likelihood bistatic-radar-based approach and
- a phase-pseudorange consistency check.

The first approach examines the spatial and temporal consistency of the received signals to detect inconsistencies between the instantaneous received multipath and the typical multipath background environment. The second approach, which is similar to receiver autonomous integrity monitoring (RAIM) techniques, monitors phase and pseudorange observables to detect inconsistencies potentially caused by spoofing. Again, a spoofer can act like multipath to avoid detection, but this means that the VSD would have achieved its modest goal.

| | SSSC | NMA | Dual-Receiver | VSD |
|---|---|---|---|---|
| **Cryptographic Method** | Yes | Yes | Yes | No |
| **Communication Link** | No | Yearly | Continuously | No |
| **Extra Hardware (IMU, Accelerometer, Antenna)** | No | No | Communication Link | No |
| **Time Between Authentications** | 30 seconds (possible) | 30 seconds (possible) | About 1 second | Seconds |
| **Receiver Autonomous** | No | No | No | Yes |
| **Time to Implementation** | Years | Years | Months | Months |
| **Requires Changes to GPS Interface Specification** | Yes, L1C Data Channel Spreading Code | Yes, 2 New CNAV Messages | No, Uses P(Y) Code | No |

▲ **TABLE 1** Comparison of anti-spoofing techniques discussed in this article.

## Anti-Spoofing Reality Check

Security is a tough sell. Although promising anti-spoofing techniques exist, the reality is that no anti-spoofing techniques currently defend civil GPS receivers. All anti-spoofing techniques face hurdles. A primary challenge for any technique that proposes modifying current or proposed GPS signals is the tremendous inertia behind GPS signal definitions. Given the several review boards whose approval an SSSC or NMA approach would have to gain, the most feasible near-term cryptographic anti-spoofing technique is the dual-receiver method. A receiver-autonomous, non-cryptographic approach, such as the VSD, also warrants further development. But ultimately, the SSSC or NMA techniques should be implemented: a signal-side civil GPS cryptographic anti-spoofing technique would be of great benefit in protecting civil GPS receivers from spoofing attacks.

## Manufacturers

The high-quality handheld receiver cited in Figure 1 was a **Trimble** *Juno SB*. Testbed equipment shown: **Schweitzer Engineering Laboratories** *SEL-421* synchrophasor measurement unit; **Ramsey** *STE 3000* radio-frequency test chamber; **Ettus Research** *USRP N200* universal software radio peripheral; Schweitzer *SEL-2401* satellite-synchronized clock (blue); Trimble

## Grant

*Continued from page 17.*

military sectors. We take pride in providing extremely accurate PNT services to billions of users worldwide.

And we are spending considerable resources to modernize the GPS constellation to provide even better service in the future. The continued fielding of new GPS IIF satellites and GPS control segment software updates are key to current modernization efforts. GPS III satellites and the Next Generation Control System (OCX) will further enhance GPS capabilities. Fully compliant user equipment is essential as modernization efforts continue.

We'll continue to improve our constellation with the launches of new satellites; the next GPS IIF is scheduled to launch in September of 2012 and the first GPS III should be available for launch in FY 2014. And OCX remains on-track for a Ready-To-Operate (RTO) date in 2015.

**DJ:** Finally, if you were Queen for a Day, what would you like to see changed?

**JG:** For operators, there is always an interest in and a desire for greater capability, faster processing...and for us it is in pushing the envelope for even greater accuracy with precision timing, position and navigation.

There is also an interest in expanding application of our NAVWAR (Navigation Warfare) knowledge, application and operations — having an even greater number of people trained and embedded with warfighters as NAVWAR experts. This is where I think we will see some real growth in the future.

*Note from Don Jewell:* I have visited the 2SOPS more than 20 times in the past five years, and I have known and visited every 2SOPS commander since that organization began to include then Lt. Col. and now General William Shelton, the four-star AFSPC/CC. I have never seen a more motivated GPS crew force than the one I saw during my last visit with Lt. Col. Grant. Squadrons tend to reflect the work ethic, mores and integrity of their commander, and my hat is off to Lt. Col. Jennifer Grant because her crews are obviously very motivated to support the warfighter, and they seem very happy in their jobs. The atmosphere in 2SOPS these days is positive, upbeat and very customer (that's you and me) oriented. Plus, many of the crewmembers are just back from tours in Afghanistan and Iraq, so they know the needs of the warfighter and they are working hard to fulfill them.

*Resolution SMT* receiver (silver); **HP** GPS time and frequency reference receiver.

### References, Further Information

University of Texas Radionavigation Laboratory, *http://radionavlab.ae.utexas.edu.*

Full results of Figure 1 experiment are given in Shepard, D.P. and T.E. Humphreys, "Characterization of Receiver Response to Spoofing Attacks," *Proceedings of ION-GNSS* 2011.

NMA can be the basis of comprehensive signal authentication: Wesson, K.D., M. Rothlisberger, T. E. Humphreys (2011), "Practical cryptographic civil GPS signal authentication," *Navigation, Journal of the ION,* submitted for review; available at *http://radionavlab.ae.utexas.edu/nma*

Humphreys, T.E, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems,* 2011, submitted for review; available at *http://radionavlab.ae.utexas.edu/detstrat*

**KYLE WESSON** is pursuing his M.S. and Ph.D. degrees in electrical and computer engineering at the University of Texas at Austin. He is a member of the Radionavigation Laboratory. He received his B.S. from Cornell University.

**DANIEL SHEPARD** is pursuing his M.S. and Ph.D. degrees in aerospace engineering at the University of Texas at Austin, where he also received his B.S. He is a member of the Radionavigation Laboratory.

**TODD HUMPHREYS** is an assistant professor in the department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin and director of the Radionavigation Laboratory. He received a Ph.D. in aerospace engineering from Cornell University.