Signal Authentication

A Secure Civil GNSS for Today

SHERMAN LO, DAVID DE LORENZO,
AND PER ENGE
STANFORD UNIVERSITY AND ZANIO, INC.

DENNIS AKOS
UNIVERSITY OF COLORADO

PAUL BRADLEY
DAFCA, INC.

Many civil GNSS applications need secure, assured information for asset tracking, fleet management and the like. But there is also a growing demand for geosecurity location-based services such as hardware configuration and management, virtual site licenses, digital rights management and geofencing. Unfortunately, GNSS is vulnerable to malicious intrusion and spoofing. How can users be sure the information they receive is authentic? This article introduces a new method that uses hidden attributes fundamental to the GPS satellite broadcast — and cross-compared between two receivers — to authenticate signals and the location solutions they generate.

Brad Parkinson, first director of the GPS Joint Program Office, once remarked that the NAVSTAR Global Positioning System represents, next to the Internet, perhaps the most successful civilian adoption of military-developed, dual-use technology.

Today, hundreds of millions of people worldwide rely on satellite navigation to deliver accurate position and time information to a host of critical services, including everything from guiding aircraft at night and during inclement weather to synchronization of cellular communication networks. Other applications range from helping emergency dispatchers direct rescue personnel to giving route instructions to touring motorists.

As these and other GNSS-enabled applications become increasingly woven into the fabric of our global 21st-century economic and social infrastructure, the consequences of breach-of-service become greater as well. In this context, service breach encompasses not only system outages (e.g., constellation failures, inadvertent or deliberate interference, and so forth) but also failures of trust in the basic integrity of the position and time broadcast.

Moreover, experience with the Internet shows that as a resource becomes more valuable to our civil infrastructure, criminal or malicious agents will seek to discover and exploit weaknesses in order to disrupt legitimate users or to perpetrate fraud.

Navigation system security is ever more important for two reasons. The first reason is to ensure that the position, navigation, and time (PNT) information upon which we increasingly rely are indeed trustworthy. The second is that secure PNT can serve as a building block for protection of critical data and assets in the global fight against information technology attack. We refer to these features as "security for navigation" and "security from navigation."

Ideally, security would be a built-in feature of civilian GNSS. Unfortunately, as with the Internet, this was not an initial design consideration for civil use of GPS. The European Galileo system, which will employ such features possibly as a fee-based service, still is a number of years from operational capability.

Recently, proposals have been made to incorporate security and authentication signatures directly into the civil GPS signal. However, GPS probably will not incorporate these features, due both to institutional priorities and to long procurement and deployment cycles.

Thus, the GNSS community must work within the existing system to develop civilian navigation security features. In this article, we will present a new technique that can provide such capabilities today for civilian GNSS.

The GNSS Security Threat

Recent experience shows that GNSS security threats exist now and will increase in the future. In a comprehensive study of GPS vulnerabilities, the U.S. Department of Transportation warned in the 2001 Volpe Report that "the GPS signal is subject to degradation and loss through attacks by hostile interests."

Due to the low received power of GNSS signals, the most common attack currently contemplated is denial-of-service by jamming or intentional interference. Of greater concern in the future will be spoofing, where a signal is transmitted so that a GNSS receiver computes an incorrect position. Spoofing represents a more pernicious attack than denial-of-service, because it attempts to misrepresent the user's true location while at the same time avoiding detection of the attack itself.

Concerns about GNSS authenticity are particularly relevant today. For example, several over-the-air spoofing incidents already have been reported. A number of such incidents are mentioned in the article by B. Forssell cited in the Additional Resources section.

Additionally, a U.S. research team has developed and described a portable GPS civilian spoofer capable of several different attack mechanisms (See the article by T. Humphreys et alia in Additional Resources.). This "cookbook on GPS spoofing" expands the attacker threat space to include not only sophisticated foreign powers but also rogue organizations and even moderately skilled domestic groups or individuals.

These developments not only demonstrate intent but also illustrate the ever-increasing attack sophistication. Hacking the satellite-to-receiver signal interface opens GNSS to the same types of attacks that daily plague personal computers, corporate mainframe systems, and the Internet.

An additional attack vector occurs when a supplicant party submits its position to a permission-granting agent. Without an authentication token generated as part of the position computation process, no mechanism exists whereby a party can assure that a position assertion is *bone fide*. Consequently, the navigation security threat space raises these dual concerns for a user: (1) when processing signals that I receive myself, how do I ensure their authenticity? and (2) when receiving an assertion from another party about the signals that they receive, how do I ensure the validity of their assertion?

Current methods of protecting GPS users against system faults or intentional attacks rely on cross-checks against metrics either internal or external to the GNSS subsystem, or on tests of predictable characteristics of the navigation signal. Of course, as the robustness of the defensive countermeasures increases, system complexity and cost go up as well — which can be a barrier in applications where the GNSS hardware bill-of-materials is expected to remain below $1!

And not all countermeasures are secure against every possible attack. For example, even sophisticated direction-of-arrival anti-spoofing methods described in the literature — for example, the article by P. Y. Montgomery et alia in Additional Resources — do not protect the integrity of location assertions made by one party to another.

With these concerns in mind, we

have developed and tested a signal authentication technology that relies not on the predictable characteristics of the GPS signal, but rather makes use of hidden attributes that are fundamental to the satellite broadcast and that can be cross-compared between receivers to ensure the validity of the signals that are received and the location solutions that those signals generate.

Anti-Spoofing for Civil GNSS

Some GNSS signals are specifically designed to prevent spoofing or to deny unauthorized access — encrypted signals such as the GPS P(Y) and M-code and Galileo's Public Regulated Service (PRS), or obscured signals such as the GLONASS P-code.

These signals produce asymmetry, meaning that the service provider has the encryption or generation mechanism while an attacker does not. Consequently, an attacker will not be able to generate the authentic encrypted signal for use in a spoofing broadcast or injection attack. Of course, civil users do not have access to the P(Y), M-code, or PRS, and even authorized military GPS users require Selective Availability/anti-spoofing module (SAASM) hardware, which is both expensive and access-restricted.

Our research has created a method to provide the anti-spoofing benefits of secret codes, without needing access to the codes themselves. This capability is achieved by joint processing of the signal received at one location with a nearly synchronous signal received at a remote (preferably trusted) station; the theory of this joint processing is described in the next section.

A central tenet of this method is that the better the secret codes are protected by the corresponding operating authority, such as the U.S. Department of Defense (for the P(Y) and M-code) or the Galileo operating agency (for the PRS), the better the security of this authentication system. (Security can be expressed in terms of an equivalent cryptographic strength, the brute-force attack time, and so forth.)

The following section and the remainder of the article will use the GPS L1/P(Y) code as the secret code being operated upon. While L1/P(Y) is used as an illustrative example, the technique can be applied to other navigation and communication signals as well.

Processing of Secret Signals for Authentication – Theory

To describe joint processing for signal authentication, we begin with a GPS device receiving satellite signals at the L1 frequency. The signals transmitted by each satellite are composed of a sinusoidal carrier, a satellite-specific pseudorandom spreading code, and a navigation data sequence.

The L1 frequency carries both C/A-code and P(Y)-code signals, transmitted in phase quadrature. Hence, on L1 a GPS receiver has available to it a signal $s_{L1}(t)$ that is composed of the received RF energy $s^i(t)$ from each of N satellites in the visible constellation, plus thermal noise $\eta(t)$:

$$s_{L1}(t)=\sum_{i=1}^{N}\left[s^i_{L1/C/A}(t)+s^i_{L1/P(Y)}(t)\right]+\eta(t) \tag{1}$$

Note that the received signals are well below the thermal noise floor and only detectable after correlation processing with a receiver-generated replica or observation via high-gain steerable antennas.

We now focus on the data and code components of the L1 signal from a specific satellite i while dropping the L1 subscript; at receiver #1 this signal is $s^i_1(t)$:

$$\begin{aligned}s^i_1(t)=&A^i_1D^i\left(\mathrm{t}-\tau^i_{C,1}\right)x_C\left(t-\tau^i_{C,1}\right)\cos\left[2\pi\left(f_{L1}+f^i_{D,1}\right)t+\theta^i_1\right]\ldots\\&+B^i_1D^i\left(t-\tau^i_{P,1}\right)x_P\left(t-\tau^i_{P,1}\right)\sin\left[2\pi\left(f_{L1}+f^i_{D,1}\right)t+\theta^i_1\right]\end{aligned} \tag{2}$$

Here, subscripts C and P denote C/A-code and P(Y)-code respectively, A and B are scaling parameters for the received signal power, D is the navigation data bit sequence (possibly different for C/A and P(Y)), x_C and x_P are the C/A-code and P(Y)-code sequences, τ_C and τ_P are the phases of the respective generating functions, f_D is the satellite-to-receiver Doppler frequency (it may also include a frequency offset between the satellite oscillator and that of the receiver), and θ is the phase of the received RF carrier with respect to the local reference oscillator.

The receiver performs a series of functions on the received signal in space: amplification, mixing and frequency down-conversion, low-pass filtering, and Doppler frequency and carrier-phase estimation to yield a baseband signal suitable for processing, as follows:

$$\begin{aligned}s_1(t)=&A_1D\left(t-\tau_{C,1}\right)x_C\left(t-\tau_{C,1}\right)\left\{\begin{matrix}\cos\left[2\pi\left(f_{D,1}-\hat{f}_{D,1}\right)t+\theta_1-\hat{\theta}_1\right]\ldots\\+i\sin\left[2\pi\left(f_{D,1}-\hat{f}_{D,1}\right)t+\theta_1-\hat{\theta}_1\right]\end{matrix}\right\}\ldots\\&+B_1D\left(t-\tau_{P,1}\right)x_P\left(t-\tau_{P,1}\right)\left\{\begin{matrix}\sin\left[2\pi\left(f_{D,1}-\hat{f}_{D,1}\right)t+\theta_1-\hat{\theta}_1\right]\ldots\\-i\cos\left[2\pi\left(f_{D,1}-\hat{f}_{D,1}\right)t+\theta_1-\hat{\theta}_1\right]\end{matrix}\right\}\end{aligned} \tag{3}$$

Here, the superscript i has been dropped for clarity and the superscript caret '^' indicates estimation. Processing for C/A-code detection and tracking involves multiplication by a replica C/A-code sequence $x_C\left(t-\hat{\tau}_{C,1}\right)$. Since x_C is orthogonal to x_P (meaning their cross-correlation product is nearly zero for all τ_C and τ_P), accumulation (noise-averaging) for an integration interval T_C yields in-phase and quadrature terms:

$$\begin{aligned}S_{I,1}&=\int^{T_C}A_1D\left(t-\tau_{C,1}\right)x_C\left(t-\tau_{C,1}\right)x_C\left(t-\hat{\tau}_{C,1}\right)\cos\left[2\pi\left(f_{D,1}-\hat{f}_{D,1}\right)t+\theta_1-\hat{\theta}_1\right]dt\\S_{Q,1}&=\int^{T_C}A_1D\left(t-\tau_{C,1}\right)x_C\left(t-\tau_{C,1}\right)x_C\left(t-\hat{\tau}_{C,1}\right)\sin\left[2\pi\left(f_{D,1}-\hat{f}_{D,1}\right)t+\theta_1-\hat{\theta}_1\right]dt\end{aligned} \tag{4}$$

Signal tracking seeks to maximize S_I and to minimize S_Q by driving to zero the differences between the received and estimated values of code-phase, Doppler frequency, and carrier-phase. **Figure 1** shows this process for code-phase alignment. A receiver with access to the encrypted P(Y)-code sequence can process that signal component in an analogous manner. (In addition, some codeless and semi-codeless techniques exploit the fact that identical P(Y)-code sequences are broadcast on the L1 and L2 frequencies.)

The foregoing procedure is common, with small variations, to almost all commercial GNSS receivers. The innovation we are introducing is the joint processing of signals received at two separate locations to access the secret code sequence for authentication. This authentication process recognizes and exploits the fact that the P(Y)-code sequence received at a location #1, $x_p(t - \tau_{P,1})$, is identical to the sequence received at a location #2, $x_p(t + \Delta t - \tau_{P,2})$, except for the differential satellite-to-receiver signal travel time Δt.

At this point, accumulation of the product of the Eq. (4) quadrature signals from two receivers (and remembering that x_C is orthogonal to x_P, and that with Doppler frequency and carrier-phase alignment the 'sin' terms go to zero and the 'cos' terms go to one) yields:

$$S_{Q,1:2} = \int^{T_C} B_1 B_2 D\left(t-\tau_{P,1}\right) D\left(t+\Delta t-\tau_{P,2}\right) x_P\left(t-\tau_{P,1}\right) x_P\left(t+\Delta t-\tau_{P,2}\right) dt \tag{5}$$

Observation of a correlation peak, as shown in **Figure 2**, indicates the presence of component $s_{P(Y)}(t)$ in both receiver #1 and receiver #2 signals, and is accomplished by sliding the correlation window until $\Delta t = \tau_{P,2} - \tau_{P,1}$. A peak in the function $S_{Q,1:2}$ establishes signal authenticity (with the trivial caveat that receiver #1 and receiver #2 not be within reception range of the same signal-spoofing attacker).

The value of Δt accounts both for receiver clock offset and for different satellite-to-receiver signal travel times. Consequently, if Δt should be measured on several satellites, then the presence of the correlation peaks serves not only to confirm the authenticity of each receiver's signal observation but also to locate receiver #1 with respect to receiver #2 in a manner analogous to GPS carrier-phase differential positioning.

The strength of the correlation peak depends on many factors such as correlation time duration and the signal-to-noise ratio (SNR) of the measurements. For example, the correlation results will be more evident if the reference station uses a high-gain dish or steered-beam array antenna rather than an omnidirectional patch antenna.

The difference between this joint processing method and having the actual P(Y)-code sequence (which is like having a noiseless measurement) is shown

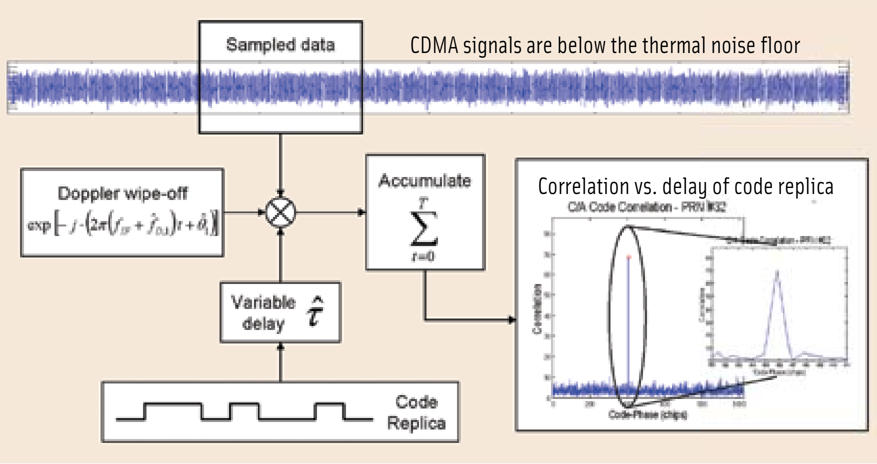
Sampled data
CDMA signals are below the thermal noise floor
Doppler wipe-off
exp[-j·(2π(f_IF + f̂_D,i)t + θ̂_i)]
Accumulate
Σ t=0 T
Correlation vs. delay of code replica
C/A Code Correlation - PRN #32
Variable delay τ̂
Code Replica
Correlation
Code-Phase (chips)

FIGURE 1 GPS signal correlation with known CDMA sequences.

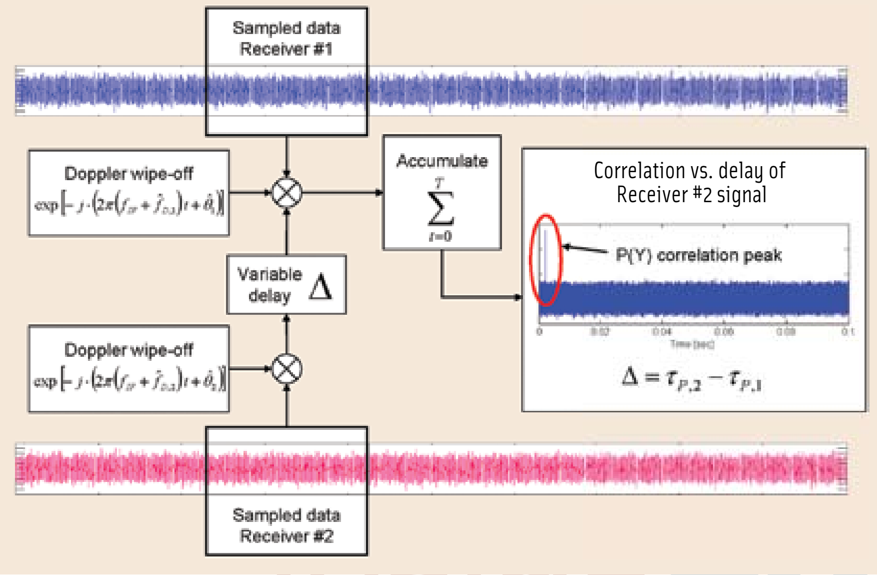

FIGURE 2 Two-receiver correlation with unknown CDMA sequence. The presence of a P(Y)-code correlation peak authenticates the signal. The peak timing for several satellites allows relative positioning (and timing) of receiver #1 vs. receiver #2.

in Equation 6, assuming noise power is $\frac{\sigma^2}{2}$, the receiver #1 signal has amplitude B_1, and the receiver #2 "reference signal" has amplitude $B_2 = \alpha B_1$ (with the same noise); N represents the averaging time. Note that as the gain of the reference station antenna increases, the ratio approaches 1 as expected.

$$\frac{SNR_{jointproc}}{SNR_{PYcode}} = \frac{\sqrt{N}\alpha\, B_1 \Big/ \left[\sigma\sqrt{\left(\frac{\sigma}{B_1}\right)^2 + \alpha^2 + 1}\right]}{\sqrt{N}B_1/\sigma} = \frac{\alpha}{\sqrt{\left(\frac{\sigma}{B_1}\right)^2 + \alpha^2 + 1}} \quad (6)$$

An Authentication Architecture

This joint processing technique enables both signal authentication and position verification because the appearance of the correlation peaks guarantees the presence of the hidden encryption signatures, and the timing of several of these peaks allows computation of a differential position receiver-to-receiver.

A system implementing one possible variant of this authentication architecture is illustrated in Figure 3. In this example, the reference station continuously collects and stores GPS raw data (or it could do so on a published schedule); these archived data are used in the authentication joint processing operation. The steps required for joint processing can be described as follows:

1. Record GPS raw data at location #1 (i.e., the user device) and location #2 (i.e., the reference station).
2. Transmit a data snapshot from the user device to the reference station for processing, along with a time-stamp of the data snapshot.

For each satellite of interest in a data set pair (user device and reference station):

3. Perform Doppler frequency wipe-off.
4. Estimate carrier-phase to allow signal separation into in-phase and quadrature components.
5. Correlate the Q-channel from the user device with the Q-channel from the reference station; slide the correlation window until a peak of sufficient magnitude appears.

The first two steps relate to signal collection and distribution. Note that the signal bandwidth must be sufficient to recover energy from the embedded secret code; for the P(Y)-code, a bandwidth of at least 10-20 megahertz is desirable. Signal processing occurs in the last three steps.

The simplest method of estimating Doppler frequency and carrier-phase, of course, is to acquire and track the C/A-code; this operation is simple for the reference station to perform but could be prohibitive at the user device (due to processor complexity or battery life concerns, for example). If the data snapshot is not sufficiently long for tracking, then a Doppler frequency estimate can come either from signal acquisition or from the satellite ephemeris.

Signal Authentication with Live Satellite Broadcasts

We conducted a validation test shortly after developing the initial signal authentication concept. This test involved near-simultaneous GPS data observation at two widely separated locations, the first in Palo Alto, California, and the second in Boulder, Colorado.

Raw RF data were collected at each site with an RF signal analyzer in a 20 megahertz band about the GPS L1 center frequency using a hemispherical patch antenna (both sites) and a 1.8-meter high-gain steerable dish antenna (Palo Alto only). The dish antenna provides approximately 25 decibels of gain over that of a standard patch. Coarse time synchronization was achieved through cellular communication links, which yielded ~0.25 seconds of timing error.

In analyzing the results of this test, we first sought to validate the basic signal-authentication concept. The correlation between measurements taken with the patch antennas at the two locations was examined. **Figure 4** shows the in-phase (C/A-code) and quadrature (P(Y)-code) correlation with a 100-millisecond observation window, two-bit I/Q data samples, and precise Doppler frequency and carrier-phase alignment (from signal tracking with a GPS software receiver). The repeating peaks in the C/A-code receiver-to-receiver correlation output are an artifact of the one-millisecond C/A-code repeat interval, modulated by the 50-hertz navigation data message.

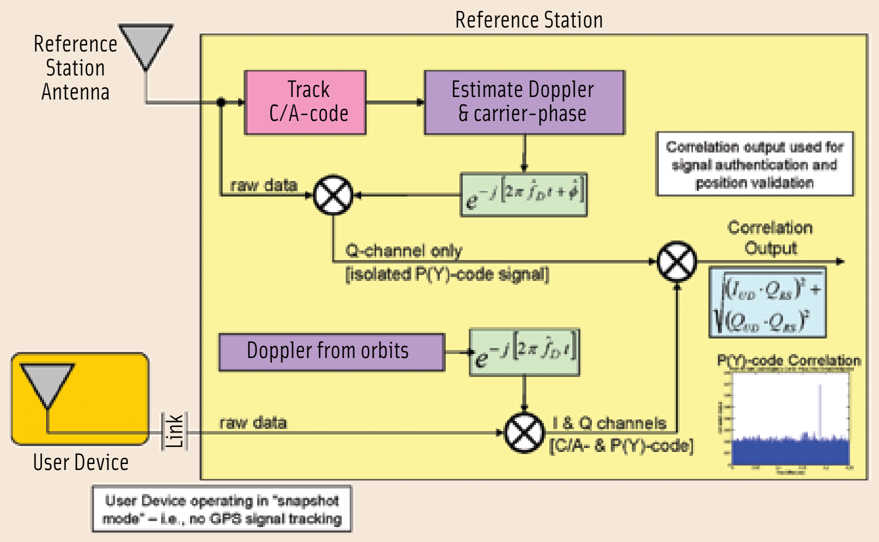
Reference Station
Reference Station Antenna
Track C/A-code
Estimate Doppler & carrier-phase
raw data
$e^{-j\left[2\pi \hat{f}_D t + \hat{\phi}\right]}$
Correlation output used for signal authentication and position validation
Q-channel only
[isolated P(Y)-code signal]
Correlation Output
$\sqrt{(I_{UD}\cdot Q_{RS})^2 + (Q_{UD}\cdot Q_{RS})^2}$
Doppler from orbits
$e^{-j\left[2\pi \hat{f}_D t\right]}$
P(Y)-code Correlation
User Device
Link
raw data
I & Q channels
[C/A- & P(Y)-code]
User Device operating in "snapshot mode" – i.e., no GPS signal tracking

FIGURE 3 Authentication Architecture. A user device records a snapshot containing GPS signals from several satellites and transmits this snapshot to an authentication reference station for processing. This illustrates one simple implementation scheme with minimal signal processing required at the user device.

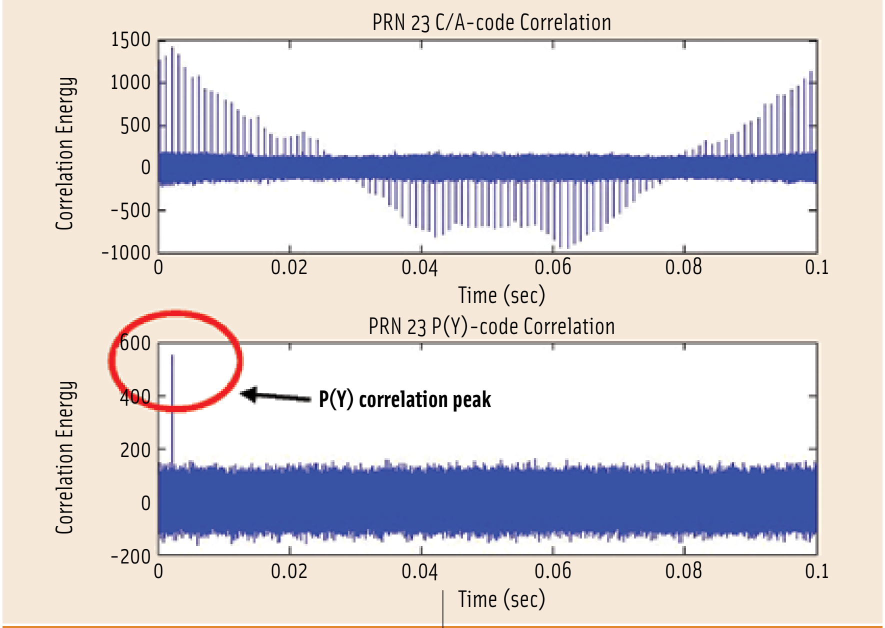

FIGURE 4 Live data validation of receiver-to-receiver P(Y)-code signal authentication: 100 millisecond correlation window; each receiver utilizes a hemispherical patch antenna.

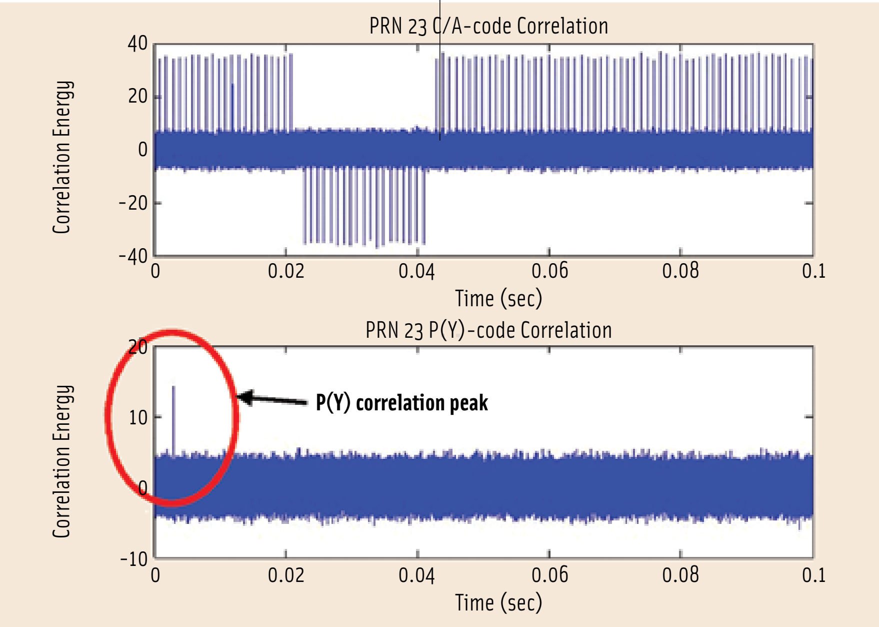

FIGURE 5 Minimal data storage requirements: 1.8-meter high-gain steerable dish antenna on receiver #1, one-bit I/Q samples at receiver #2, one-millisecond correlation, 23.68 MHz sampling frequency, total record size = 4,800 bits. Using a 15 MHz sampling frequency would yield 3,000 bits of data record length.

Another important goal of our analysis seeks to minimize the required memory size of the data snapshot stored at one receiver. This is important in memory- or bandwidth-constrained authentication applications such as integrated circuits, smart cards, or near-real-time challenge-response scenarios.

Using the 1.8-meter high-gain steerable dish antenna for one receiver (i.e., the reference station), one-bit I/Q samples at the other receiver (i.e., the user device), and a one-millisecond correlation window allows recovery of a prominent correlation peak with no more than 4,800 bits of data, as shown in **Figure 5**. Reducing the signal bandwidth to a 15-megahertz sampling frequency could push the data storage requirements below 3,000 bits.

Requirements & Benefits

Three elements are needed to support the authentication technology described herein. The most basic requirement is a supporting infrastructure of trusted reference stations covering the geographic areas of interest. (Regional coverage may require only a single reference station.) The other two elements, receiver technology and communication links, have requirements that vary depending on application.

A reference station network (and the associated authentication servers) is needed to provide the authentication function. We should note that the required number of reference stations is quite modest, because a single reference station can serve a sizable area. For example, the continental U.S. could be covered by two or three such stations with significant redundancy, as the reference station network requirement simply is to observe every satellite that may be seen by any user in the service coverage area. (Peer-to-peer authentication is a slight modification of the above-described architecture and does away with the reference station network entirely.)

The most basic user device, essentially a data capture engine, can make do with less functionality than a typical GNSS receiver, because the entire authentication processing typically is done remotely. Stripping away correlation, tracking, and navigation units leaves only a wide-band front-end, simple analog-to-digital converter (1-1½ bit), storage, and input/output subsystems. Furthermore, remote processing drastically reduces power consumption, which still can be a major concern for GNSS receiver integrators.

Real-time or near real-time receivers also require a secure communications link. With the proliferation of data communication technologies such as Wi-Fi, Wi-Max, and numerous high-speed cellular communication standards, this

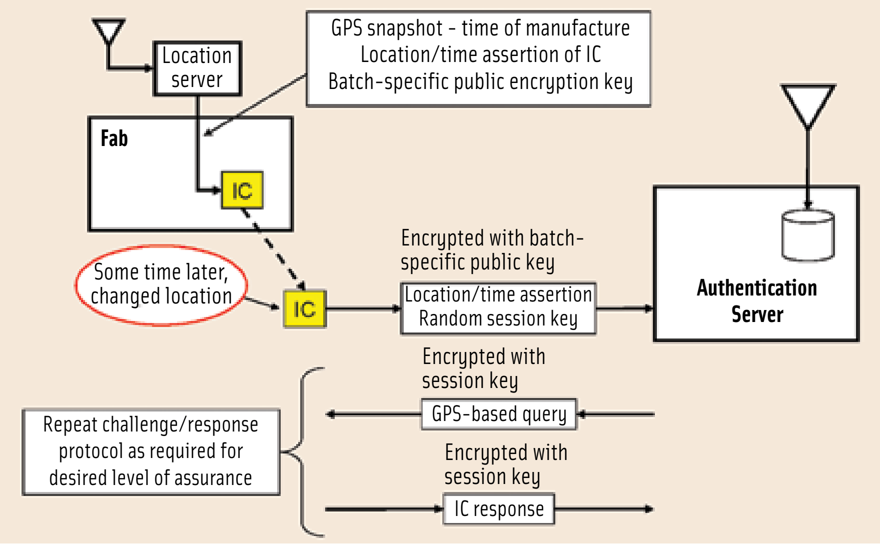
Location server
GPS snapshot - time of manufacture
Location/time assertion of IC
Batch-specific public encryption key
Fab
IC
Some time later, changed location
IC
Encrypted with batch-specific public key
Location/time assertion
Random session key
Authentication Server
Encrypted with session key
GPS-based query
Repeat challenge/response protocol as required for desired level of assurance
Encrypted with session key
IC response

FIGURE 6 Using secure GNSS to provide integrated circuit protection.

requirement is not a major constraint in most of the developed world. Additionally, the hardware needed for these links increasingly is being integrated with GPS in mobile telephony.

In contrast, some applications may find a real-time communications link unnecessary. For example, a receiver designed for route auditing or cargo transit assurance needs only to store GPS snapshots in tamperproof memory, with verification done at intermediate or final destination.

With these required elements, the authentication architecture essentially transfers the security, and possibly the navigation, functionality from the user device to the trusted authentication processor. This reduces costs by moving the main security vulnerability from the distributed users to a few hardened locations.

The sites containing the authentication processor and the GNSS reception equipment can be hardened with features such as physical security barriers, high-gain directional antennas, or steered-beam antenna arrays. The benefit to this centralization is that high-cost security features only are needed in a few locations, with the resulting cost amortized across many users.

The end result is an architecture that can support many PNT security applications at very reasonable cost. These include not only current high-value applications such as asset tracking and fleet management, but also emerging geo-security location-based services such as hardware configuration and management, virtual site licenses, digital rights management and manners policies, and geo-fencing. Moreover, new applications

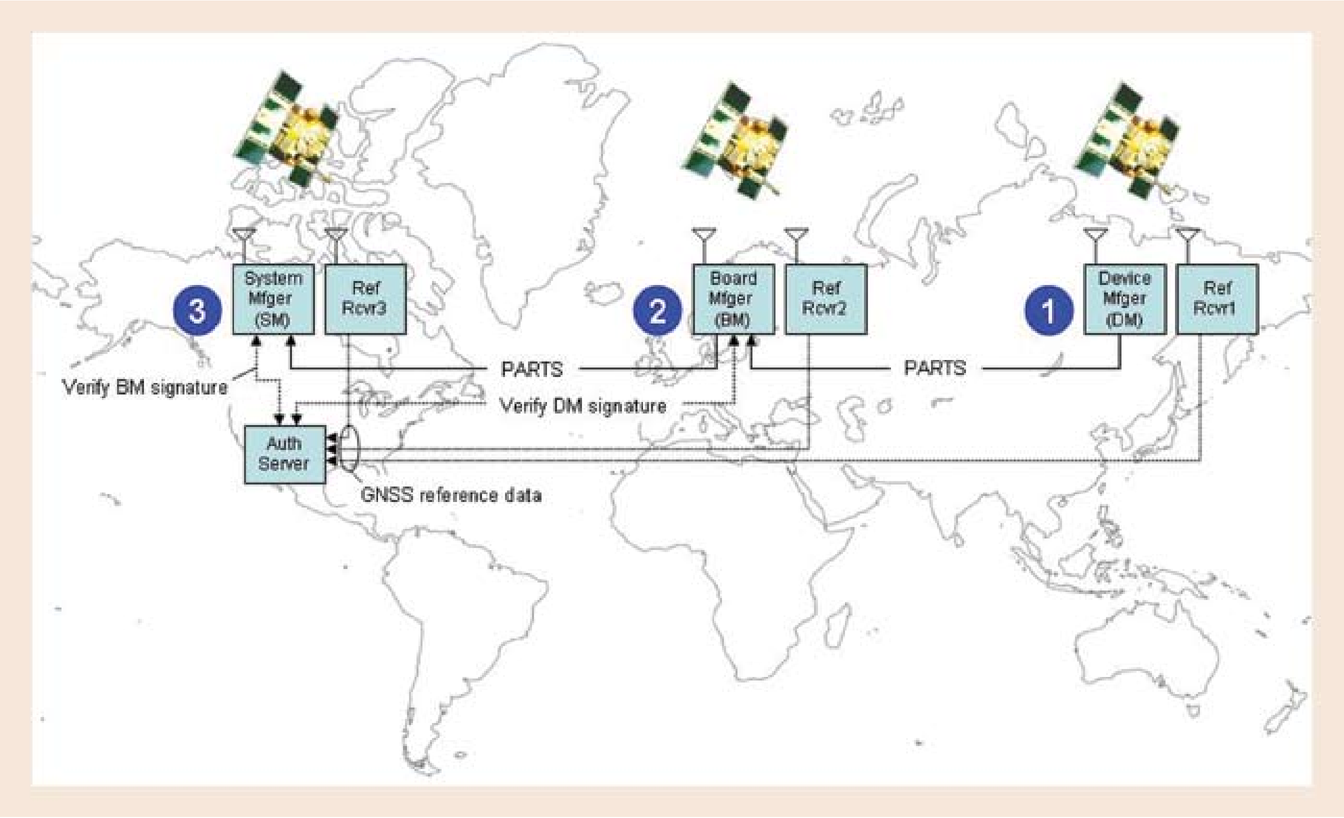

FIGURE 7 Verification of integrated circuit and hardware through stages of production

can be supported, such as the following example of secure location signatures for integrated circuit (IC) assurance.

Location Security for IC Assurance

Numerous security concerns surround the manufacturing of integrated circuits, including counterfeiting, theft, and the introduction of Trojan logic (i.e., a hidden malicious modification to the circuit that triggers for the purposes of compromising security features). Such concerns are growing as a result of the expanding use of third-party intellectual property (IP) and the rapid globalization of device and system manufacturing. The risks to mission-critical systems such as those in avionics, military, and communications applications are significant.

Secure GNSS offers a novel and cost-effective solution to address integrated circuit and supply chain assurance by implanting one or more unique time- and location-based signatures within the IC at the times of fabrication, board level manufacturing, and system assembly. Figure 6 shows one means of using GNSS authentication signatures for IC verification as part of a multi-factor integrated suite of defensive technologies.

However, the IC logic and silicon gate-count devoted to the assurance functionality are severely constrained, as resources allocated to security or validation circuits directly compete with the primary processing features of the die. For example, the on-die and at-speed IP of DAFCA's reconfigurable security product suite have been optimized to minimize the footprint in the final silicon device.

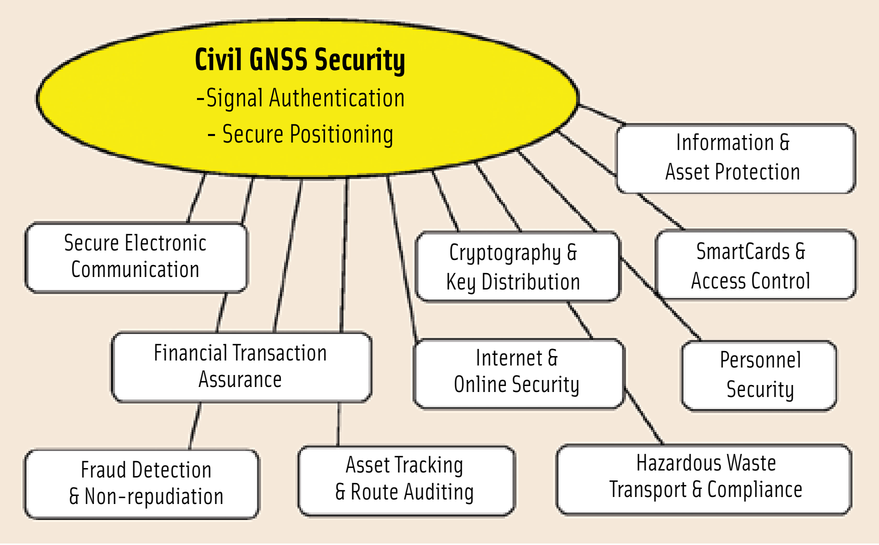
Civil GNSS Security
-Signal Authentication
- Secure Positioning
Information & Asset Protection
Secure Electronic Communication
Cryptography & Key Distribution
SmartCards & Access Control
Financial Transaction Assurance
Internet & Online Security
Personnel Security
Fraud Detection & Non-repudiation
Asset Tracking & Route Auditing
Hazardous Waste Transport & Compliance

FIGURE 8 High-integrity applications of secure GNSS.

We have developed and tested a signal authentication technology that relies not on the predictable characteristics of the GPS signal, but rather makes use of hidden attributes that are fundamental to the satellite broadcast and that can be cross-compared between receivers to ensure the validity of the signals that are received and the location solutions that those signals generate.

For this reason, it is likely that GNSS location and time signatures, and the logic resources required to securely store them in memory, comprise an IC assurance technology that may be most suited to high-value mission-critical devices such as systems on chip (SoCs), central processing units (CPUs), integrated memory controllers, specialized digital signal processors (DSPs), and other system or I/O control chips.

We estimate that the storage requirements of a 400-kByte GNSS signature, along with the associated encryption and tamperproofing circuits, and using existing die-to-system communication channels, becomes feasible for devices containing approximately one million transistors.

Of course, one benefit of combining the circuit validation and IC manufacturing assurance capabilities at the same phase of the design cycle is architectural simplification of shared communication across standardized test access ports. In this way, a system integrator (for example) could validate the functional integrity, manufacturing provenance, and transport chain-of-custody through a common test interface.

Figure 7 illustrates an example process wherein the GNSS security protocol provides an attack-resistant verification of the manufacturing and transport stages within the IC supply chain by requiring that each successive step be dependent on successful authentication during the previous step.

The scheme in Figure 7 can further be extended into a feature activation scheme that integrates the location and time signatures with hardware-based activation logic and software verification. With the addition of tamper-resistant hardware and software, along with hardware countermeasures, a robust security system can be created that extends from logic design and device fabrication, through the supply channel, and into system deployment.

Conclusions

Satellite navigation has emerged as a global infrastructure utility, complementing modern public services such as energy distribution, global transport and travel, and voice and data communications networks. As a ubiquitous and indispensable component of modern life and business, GNSS is vulnerable to malicious intrusion and nefarious misuse. Adversaries can jam, spoof, or manipulate a system to deny service or to obfuscate a reported position. Because GNSS can be used to authorize actions, trust and authenticity are required for proper implementation and enforcement policy.

In this article, we have described a signal-authentication system architecture for single-frequency civil-use GNSS devices that delivers a verifiable position report or confirms a position assertion by a remote agent. We have validated this authentication architecture through live signal tests with hardware in the loop, and have described the implementation of GNSS security signatures for integrated circuit and supply chain assurance.

As the satellite navigation attack threat space and sophistication continue to grow, this and other defensive technologies will become increasingly important to the high-integrity application of GNSS, as illustrated in Figure 8. With this effort, we will realize *security for GNSS* and *security from GNSS.*

Manufacturers

Stanford University and Colorado researchers use an 89600 vector signal analyzer (VSA) from **Agilent Technologies**, Santa Clara California, USA, to collect signals received either from high-gain steerable dish or hemispherical-gain patch antennas. The 1.8-meter dish is part of the Stanford GNSS Monitor Station; the patch antennas are NovAtel GPS Pinwheel Model 702 from **NovAtel, Inc.**, Calgary Alberta, Canada. The software GNSS receiver and the specialized signal authentication codebase are implemented in MATLAB from the **MathWorks, Inc.**, Natick Massachusetts, USA.

Disclosure: The first three authors are members of the Stanford University GPS Laboratory and have formed the start-up company **Zanio** to pursue development of GNSS security and authentication technology.

Additional Resources

[1] Forssell, B., "The Dangers of GPS/GNSS," *Coordinates,* February 2009

[2] Humphreys, T. E., and B. M. Ledvina, M. L. Psiaki, B.W. O'Hanlon, and P.M. Kintner, Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," *Proceedings of the Institute of Navigation GNSS Conference,* pgs. 2314-2325, 2008

[3] John A. Volpe National Transportation Systems Center for the U.S. Department of Transportation, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," *Final Report,* 2001

[4] Kuhn, M. G., "An Asymmetric Security Mechanism for Navigation Signals," *Proceedings of the 6th Information Hiding Workshop,* pgs. 239–252, 2004

[5] Montgomery, P. Y., and T. E. Humphreys and B. M. Ledvina, "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer," *Proceedings of the Institute of Navigation International Technical Meeting,* pgs. 124-130, 2009

[6] Scott, L., "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," *Proceedings of the Institute of Navigation GPS/GNSS Conference,* pgs. 1543-1552, 2003

[7] Stansell, T. A., "Location Assurance Commentary," *GPS World,* July 2007, p. 19

[8] Wullems, C., and O. Pozzobon and K. Kubik, "Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems," *Proceedings of the European Navigation Conference GNSS,* 2005

Authors

Sherman Lo, Ph.D., is a senior research engineer at the Stanford University GPS Research Laboratory where he is the associate investigator for Stanford University's efforts on the technical evaluation of Loran and also works also on a variety of GNSS-related security and integrity topics. He received the Ph.D. degree in aeronautics and astronautics from Stanford University and has received the Institute of Navigation Early Achievement Award and the International Loran Association President's Award.

David De Lorenzo, Ph.D., is a research associate at the Stanford University GPS Research Laboratory where his current research is in GNSS software receivers, adaptive beam-steering antenna arrays, indoor and urban reception of radio signals, and navigation system security and integrity. He received the Ph.D. degree in aeronautics and astronautics from Stanford University and previously has worked for Lockheed Martin and for the Intel Corporation.

Per Enge, Ph.D., is a professor of aeronautics and astronautics at Stanford University, where he directs the GPS Research Laboratory. He has been involved in the development of the Federal Aviation Administration's GPS Wide Area Augmentation System (WAAS) and Local Area Augmentation System (LAAS). Enge received the Ph.D. degree from the University of Illinois and is a member of the National Academy of Engineering and a Fellow of the IEEE and of the Institution of Navigation.

Dennis Akos, Ph.D., is an assistant professor with the Aerospace Engineering Science Department at the University of Colorado at Boulder and holds a visiting professor appointment at Luleå University of Technology, Sweden, and a consulting professor appointment at Stanford University. His research interests include GNSS systems, software-defined radio (SDR), applied/digital signal processing, and radio frequency (RF) design. He received the Ph.D. degree in electrical engineering from Ohio University within the Avionics Engineering Center.

Paul Bradley is chief technical officer of DAFCA, Inc. Bradley has more than 20 years' experience in electronics and systems design and specializes in product development and engineering leadership in emerging technology markets. He has held numerous engineering and technical leadership positions at Motorola, Nortel, CrossComm, Sonoma Systems, and Internet Photonics prior to joining DAFCA. IG