TEXBAT DATA SETS 7 AND 8

TODD HUMPHREYS

Abstract. The Texas Spoofing Test Battery, or TEXBAT, is a set of recorded spoofing scenarios that has been compiled for evaluating civil Global Positioning System (GPS) signal authentication techniques. The battery can be considered the data component of an evolving standard meant to define the notion of spoof resistance for commercial GPS receivers. The original TEXBAT set, published in September 2012, contained 6 data sets, with binary file names `ds1.bin` through `ds6.bin`. Two additional data sets, `ds7.bin` and `ds8.bin` were added to TEXBAT in August 2015. This document briefly describes `ds7.bin` and `ds8.bin`.

1. Background

Authentication of civil Global Positioning System (GPS) signals is increasingly a concern. Spoofing attacks, in which counterfeit GPS signals are generated for the purpose of manipulating a target receiver's reported position and time, have been demonstrated with low-cost commercial equipment against a wide variety of GPS receivers [1–4]. Such attacks threaten the integrity of financial transactions, communications, and power grid monitoring operations that depend on GPS signals for accurate positioning and timing [5–7].

Whereas the military GPS waveform was originally designed to be unpredictable and therefore resistant to spoofing [8], the civil GPS waveforms are precisely specified in publicly-available documents [9]. Also, although not entirely constrained by the signal specifications, the navigation data messages modulated onto the civil waveforms are highly predictable. Known signal structure and data bit predictability make civil GPS signals susceptible to spoofing attacks.

Several researchers have proposed techniques for overlaying unpredictable but verifiable modulations on existing and future civil GPS signals [10–14]. These space-segment-side cryptographic techniques offer the promise of effective globally-available signal authentication without requiring additional hardware such as multiple antennas [15] or inertial measurement equipment [16], which would be impractical in cost-sensitive applications.

Unfortunately, even while many of the technical challenges of implementing space-segment-side cryptographic civil GPS authentication have been overcome, daunting procedural and financial hurdles remain. This sobering reality has lead several researchers to conclude that efforts to authenticate civil GPS signals over the next decade should focus on strategies that do not require support from the GPS space segment. Examples of such space-segment-independent authentication strategies can be categorized as (1) receiver-autonomous signal-processing-oriented

Date: March 16, 2016.

techniques, which require no antenna motion or specialized antenna hardware [17–19]; (2) receiver-autonomous antenna-oriented techniques, which require antenna motion or specialized antenna hardware [15, 20, 21]; and (3) techniques that exploit the existing encrypted military signals to offer civil GPS signal authentication for networked GPS receivers [22–25].

All existing or proposed civil GPS signal authentication schemes are premised on hypothesis tests involving statistical models for the authentic and counterfeit GPS signals. These models make simplifying assumptions that permit tractable analytical treatment of the detection problem. In general, the statistics of the null hypothesis (only authentic signals present) are readily verifiable by laboratory experiment but the statistics of the alternative hypothesis (spoofing attack underway) are not easily verified. This is because sophisticated signal generation hardware capable of code- and carrier-phase-aligned spoofing attacks is neither commercially available nor straightforward to construct. Thus, for example, experimental validation of the authentication technique proposed in [22] was limited to the null hypothesis.

A testbed capable of simulating realistic spoofing attacks is needed so that the efficacy of proposed civil GPS signal authentication techniques can be experimentally evaluated. A generic testbed capable of evaluating all known authentication techniques would be prohibitively expensive (e.g., it would require a large anechoic chamber for evaluating receiver-autonomous antenna-oriented techniques). But if the scope of evaluation is limited to receiver-autonomous signal-processing-oriented techniques and networked techniques (categories (1) and (3) above), then it is possible not only to develop an inexpensive testbed but to share the testbed's data component so that the tests can be replicated in laboratories across the globe.

2. TEXBAT

The Texas Spoofing Test Battery, or TEXBAT, is a set of high-fidelity digital recordings of live static and dynamic GPS L1 C/A spoofing tests conducted by the Radionavigation Laboratory of the University of Texas at Austin. The battery can be considered the data component of an evolving standard meant to define the notion of spoof resistance for civil GPS receivers. According to this standard, successful detection of or imperviousness to all spoofing attacks in TEXBAT could be considered sufficient to certify a civil GPS receiver as spoof resistant, as suggested in Humphreys' 2012 congressional testimony [26]. The original 6 data sets were released in September, 2012, and are described in [27,28]. The current document briefly describes two new data sets that have been added to TEXBAT.

As of September 2014, over 130 users have downloaded some of all of the first 6 data sets in TEXBAT. The list of users includes the following:

- University of Calgary, Position, Location, and Navigation Group
- Stanford University, GPS Lab
- University of New South Wales
- Dr. Bruno Sinopoli's research group at Carnegie Mellon University
- Logan Scott Consulting

- NovAtel Inc.
- Aerospace Corp
- URS Corporation, Systems Engineering & Information Solutions Group
- Purdue AAE 575: Introduction to Satellite Navigation and Positioning (taught by Prof. James Garrison)
- Schweitzer Engineering Laboratories
- Oak Ridge National Laboratory
- Vahid Dehghanian at Mount Royal University, Calgary, Canada
- NavSAS group at Istituto Superiore Mario Boella and Politecnico di Torino
- NAVIS Centre, Hanoi University of Science and Technology
- Dynetics
- Air Force Institute of Technology (AFIT)
- u-blox
- U.S. Air Force
- Texas A&M University
- MITRE
- Booz Allen Hamilton Engineering Services
- University of Cincinnati
- Coherent Navigation
- Lockheed Martin

3. Improvements in Spoofing Data Set Generation

The testbed used to develop TEXBAT data sets and apply them for receiver spoofing resistance evaluation is described in [29]. From October 2014 to July 2015, this testbed was significantly improved compared to the earlier version used to generate TEXBAT data sets `ds1.bin` through `ds6.bin`:

(1) The software-defined spoofer was modified to generate four-level (two-bit) output data samples. The earlier software-defined spoofer was only capable of outputting two-level (one-bit) data samples. The improved quantization resolution of the new spoofer substantially reduces noise due to quantization error in the output data sets.
(2) An error was corrected in the software-defined spoofer that caused the spoofing signals' Doppler frequency to be slightly different from the authentic signals' Doppler.
(3) A high-quality digital combination technique was developed that allows an original 16-bit, 25 Msps (complex) recording of authentic GNSS signals to be combined with a 2-bit, 50 Msps (real) output file from the software-defined spoofer in such a way that the combined file replicates the signal that would be recorded from an antenna receiving the authentic signals and a high-quality spoofer. A spoofing amplitude profile modulates the amplitude of the spoofing signals in this combination so that the output file can either be spoofing free (spoofing amplitude zero) or dominated by the spoofing signal (large spoofing-to-authentic relative amplitude).

Binary data sets `ds7.bin` and `ds8.bin` benefit from these improvements.

4. Description of `ds7.bin`

The `ds7.bin` spoofing scenario is based on the `cleanStatic.bin` data set. It is a *power-matched time push* scenario much like `ds3.bin` but more subtle because it employs carrier phase alignment between the spoofing and authentic signals. The scenario proceeds as follows, where each segment is labeled with its time interval in seconds:

0-110 No spoofing present. During this interval, data are identical to data from 0 to 110 seconds in `cleanStatic.bin`.

110-130 A spoofing signal is injected for each GPS L1 C/A signal present. Let $P_a(t)$ be the phasor representing the amplitude and phase of a particular GPS L1 C/A signal at time t. For simplicity, assume that P_a is real (all power in the in-phase component) with constant amplitude A_a. Thus, $P_a(t) = A_a$. The injected spoofing signal's phasor $P_s(t)$ is given by $P_s(t) = A_s(t)\exp[j\theta(t)]$, where the relative phasor angle $\theta(t)$ starts at $\pi/2$ and increases linearly in time over the interval until reaching π at $t = 130$ seconds: $\theta(t) = \pi/2 + (t - 110)(\pi/2)/20, t \in (110, 130]$.

The spoofing signal's amplitude $A_s(t)$ also increases over the interval, but does so nonlinearly according to $A_s(t) = -2A_a\cos[\theta(t)], t \in (110, 130]$. Thus, $A_s(t)$ starts at 0 at $t = 110$ and ends at $-2A_a$ at $t = 130$.

Due to the particular choice of the functions $\theta(t)$ and $A_s(t)$, the combined phasor $P_{as}(t) = P_a(t) + P_s(t) = A_a + A_s(t)\exp[j\theta(t)]$ maintains a constant amplitude over the interval while its phase angle changes from 0 to π. At the end of the interval ($t = 130$ seconds), each spoofing signal is twice as long as, and antipodally aligned with, its counterpart authentic signal. This allows the spoofer to smoothly take over the carrier and code tracking loops without the need to synchronize the spoofing attack with the navigation data bits.

130-150 Each spoofing signal's phasor $P_s(t)$ remains just as it did at $t = 130$ seconds. During this interval, the target receiver's tracking loops are controlled by the spoofer but the victim receiver's observables (C/N_0, pseudorange, beat carrier phase) are not significantly different from the values they would take on during the same interval of `cleanStatic.bin` except that the carrier phase is greater by π. During this 20-second interval of antipodal phase alignment, the spoofer could mount a navigation data bit attack by setting $A_s(t) = 0$ whenever the navigation data bit of the authentic signal is the spoofer's desired bit value and $A_s(t) = -2A_a$ whenever the spoofer wants to inject the opposite data bit value. No such data bit manipulation takes place in `ds7.bin`, but a receiver's failure to detect the spoofing attack between $t = 110$ and $t = 150$ indicates that it could have been fooled by such a data-bit manipulation attack.

150-400 Each spoofing signal's relative phase $\theta(t)$ is held constant at $\theta(t = 130) = \pi$ but its amplitude ramps linearly from $-2A_s$ to $-A_s$ over the 250-second interval: $A_s(t) = -2A_a + (t - 150)A_a/250, t \in (150, 400]$. Meanwhile, the code phase of all spoofing signals relative to their counterpart authentic increases from 0 at a rate of 1.2 meters per second. This common code phase error induces a clock offset in the target receiver. Note that the Doppler frequency of the spoofing signals remains exactly as the Doppler

frequency of the authentic signals (since $\theta(t) = \text{const}, t \in (150, 400]$); thus, in the language of [29], this is a *frequency-locked* attack.

400-468 Each spoofing signal's relative phase $\theta(t)$ is held constant at $\theta(t = 130) = \pi$ and amplitude is held constant at $A_s(t = 400) = -A_s$, but the relative code phase of each spoofing signal continues to increase at 1.2 meters per second. At $t = 468$, the common relative code phase between spoofing and authentic signals is 381.6 meters, which causes a 1.273 us clock offset in the target receiver.

5. Description of `ds8.bin`

The `ds8.bin` spoofing scenario is identical to the `ds7.bin` scenario except that the spoofer treats every received navigation data bit as if it were an unpredictable low-rate security code and attempts to guess the value of the data bit in real time. This is a zero-delay security code estimation and replay (SCER) attack [14]. Approximately 50 us after each navigation data bit transition boundary, the spoofer's guess of the data bit value is correct to a very high probability. Thus, receivers attempting to detect a SCER spoofing attack need only pay attention to the first 50 us after each data bit boundary.

References

[1] T. E. Humphreys, 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," in *Proceedings of the ION GNSS Meeting*, (Savannah, GA), Institute of Navigation, 2008.

[2] D. Shepard and T. E. Humphreys, "Characterization of receiver response to a spoofing attack," in *Proceedings of the ION GNSS Meeting*, (Portland, Oregon), Institute of Navigation, 2011.

[3] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks," in *Proceedings of the ION GNSS Meeting*, 2012.

[4] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.

[5] John A. Volpe National Transportation Systems Center, "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," 2001.

[6] N. S. W. Center, "Global positioning system impact to critical civil infrastructure (GICCI)," tech. rep., Mission Assurance Division, Naval Surface Warfare Center, 2009.

[7] U. Kroener and F. Dimc, "Hardening of civilian GNSS trackers," in *Proceedings of the 3rd GNSS Vulnerabilities and Solutions Conference*, (Krk Island, Croatia), Royal Institute of Navigation, Sept. 2010.

[8] J. J. Spilker, Jr., *Global Positioning System: Theory and Applications*, ch. 3: GPS Signal Structure and Theoretical Performance, pp. 57–119. Washington, D.C.: American Institute of Aeronautics and Astronautics, 1996.

[9] GPS Directorate, "Systems engineering and integration Interface Specification IS-GPS-200G," 2012. `http://www.gps.gov/technical/icwg/`.

[10] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proceedings of the ION GNSS Meeting*, pp. 1542–1552, 2003.

[11] G. Hein, F. Kneissl, J.-A. Avila-Rodriguez, and S. Wallner, "Authenticating GNSS: Proofs against spoofs, Part 2," *Inside GNSS*, pp. 71–78, September/October 2007.

[12] O. Pozzobon, "Keeping the spoofs out: Signal authentication services for future GNSS," *Inside GNSS*, vol. 6, pp. 48–55, May/June 2011.

[13] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation, Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2012.
[14] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013.
[15] 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.
[16] N. White, P. Maybeck, and S. DeVilbiss, "Detection of interference/jamming and spoofing in a DGPS-aided inertial system," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 34, no. 4, pp. 1208–1217, 1998.
[17] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing module for legacy civil GPS receivers," in *Proceedings of the ION International Technical Meeting*, (San Diego, CA), Jan. 2010.
[18] K. D. Wesson, D. P. Shepard, J. A. 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, OR), 2011.
[19] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/N_0 estimates," in *Proceedings of the ION GNSS Meeting*, (Nashville, Tennessee), Institute of Navigation, 2012.
[20] D. S. D. Lorenzo, J. Gautier, J. Rife, P. Enge, and D. Akos, "Adaptive array processing for GPS interference rejection," in *Proceedings of the ION GNSS Meeting*, (Long Beach, CA), Institute of Navigation, Sept. 2005.
[21] A. Broumandan, A. Jafarnia-Jahromi, V. Dehgahanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in *Proceedings of the IEEE/ION PLANS Meeting*, (Myrtle Beach, SC), Institute of Navigation, April 2012.
[22] S. Lo, D. DeLorenzo, P. Enge, D. Akos, and P. Bradley, "Signal authentication," *Inside GNSS*, vol. 0, pp. 30–39, Sept. 2009.
[23] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, and T. E. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *Proceedings of the ION GNSS Meeting*, (Portland, Oregon), Institute of Navigation, 2011.
[24] 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*, vol. 49, no. 4, pp. 2250–2267, 2013.
[25] B. O'Hanlon, M. Psiaki, J. Bhatti, and T. Humphreys, "Real-time spoofing detection using correlation between two civil GPS receiver," in *Proceedings of the ION GNSS Meeting*, (Nashville, Tennessee), Institute of Navigation, 2012.
[26] T. E. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing." `http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Humphreys.pdf`, July 2012.
[27] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas Spoofing Test Battery: Toward a standard for evaluating GNSS signal authentication techniques," in *Proceedings of the ION GNSS Meeting*, 2012. `http://radionavlab.ae.utexas.edu/texbat`.
[28] T. R. Laboratory, "Texas Spoofing Test Battery (TEXBAT)," July 2014. `http://radionavlab.ae.utexas.edu/texbat`.
[29] T. E. Humphreys, D. P. Shepard, J. A. Bhatti, and K. D. Wesson, "A testbed for developing and evaluating GNSS signal authentication techniques," in *Proceedings of the International Symposium on Certification of GNSS Systems and Services (CERGAL)*, (Dresden, Germany), July 2014. (available at `http://radionavlab.ae.utexas.edu/testbed`).

The University of Texas at Austin

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