Detailed Analysis of the TEXBAT Datasets Using a High Fidelity Software GPS Receiver

Capt Adam Lemmenes, M.S., *USAF GPS Program Office*
Lt Col Phillip Corbell, Ph.D., *Air Force Institute of Technology*
Dr. Sanjeev Gunawardena, *Air Force Institute of Technology*

Biographies

Capt Adam Lemmenes received his Master's of Science in Electrical Engineering in 2016 from The Air Force Institute of Technology (AFIT). His thesis research focused on the detection of counterfeit GPS signals using Radio Frequency-Distinct Native Attributes (RF-DNA). He has Bachelor's of Science degrees in Engineering Physics and Electrical Engineering from the University of Wisconsin-Platteville. He has worked at the Air Force Technical Applications Center working on seismic systems for nuclear detonation monitoring, and is currently assigned to the GPS Directorate.

Lt Col Phil Corbell is an Assistant Professor at AFIT in Dayton, Ohio. Lt Col Corbell received his Masters and PhD degrees from AFIT in 2000 and 2006, respectively, and has 19 publications in topics including GPS simulation and adaptive radar signal processing. Previous assignments include the 746th Test Squadron, AFRL Sensors Directorate, AWACS Block 40/45 program office, and the NRO. His current research interests are electronic warfare, navigation warfare, radar, and disruptive technologies.

Dr. Sanjeev Gunawardena is a Research Assistant Professor with the Autonomy & Navigation Technology (ANT) Center at AFIT. His research interests include RF design, digital systems design, reconfigurable computing, software defined radio, and all aspects of GNSS receivers and associated signal processing.

Abstract

Capable and inexpensive Global Positioning System (GPS) spoofers are more likely to threaten our world today due to increased public awareness, advancement of computing power, and the advent of software defined radio technology. Just recently, the introduction of GNSS enabled augmented reality games such as Pokemon Go, has also contributed significantly to the global interest in GPS spoofing [1]. To combat this threat, several researchers are developing methods of detecting spoofing attacks [2]. Integral to these efforts are the use of pre-recorded spoofing datasets in order to test the methods being developed.

The University of Texas at Austin has published datasets for evaluating spoofing mitigation techniques. These datasets, known as the Texas Spoofing Test Battery (TEXBAT), include eight separate spoofing scenarios. This paper endeavors to offer an addendum to [3, 4] with independent results, observations, and additional commentary regarding the static TEXBAT scenarios as an aid to the community of researchers utilizing this dataset. It is not the intended purpose of this paper to suggest or evaluate anti-spoofing techniques, but rather to inform the community of our observations derived from working with the TEXBAT datasets.

This paper leverages an AFIT-developed high-fidelity software-based GPS receiver known as the GNSS Educational Adjustable Receiver Software (GEARS) to process and investigate the TEXBAT spoofing scenarios. This highly flexible and customizable receiver can be used to very quickly explore many different receiver observables. It is capable of sub-sample sized correlator spacing with carrier-aided code tracking, and utilizes a programmable state machine that dynamically reconfigures the tracking loop parameters to achieve a high degree of flexibility and accuracy [5].

Observations include the characterization of power biases and time offsets between scenarios, the discovery of a "global" code and carrier range rate divergence in some scenarios, and an accurate tabulation of the onset of spoofing in each scenario. Artifacts in the RF spectrum are also described.

Introduction

The TEXBAT dataset consists of eight different spoofing scenarios, six using a static antenna and two using a moving antenna, and two "clean" reference scenarios. Characteristics of each scenario are given in [3]. This paper focuses exclusively on the static scenarios. The results presented in the TEXBAT white paper [3] are compared to similar plots produced by the software receiver used in this research. This serves to validate our software receiver and independently report on the

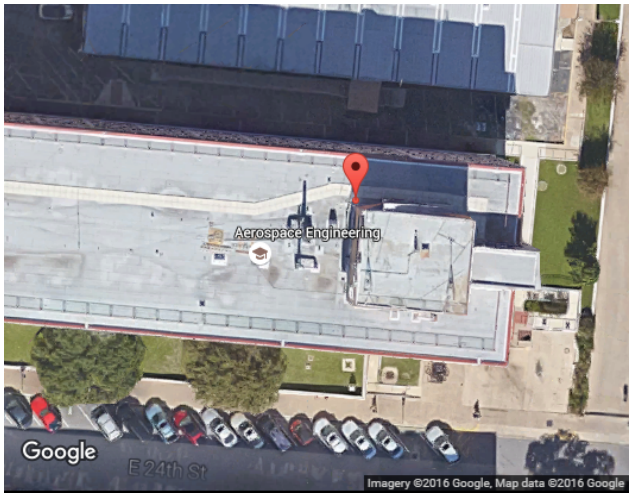

Figure 1. (U) Mapped average position solution (30°17′15.068”N, 97°44′08.642”W) of TEXBAT clean static data on top of the University of Texas at Austin Aerospace Engineering building. Imagery and map data from Google.

spoofing activity as measured by our software receiver in each static spoofing scenario.

Figure 1 shows the software receiver's position solution obtained from the clean scenario plotted on Google Maps. The location of the clean data recording was on the roof of the University of Texas at Austin Aerospace Engineering Building.

As can be seen in Figure 2, the clean data position solution only varies by two meters horizontally and three meters vertically over the seven minute recording using the new software receiver used in this research. The receiver clock error stays within 10 nanoseconds of the mean as seen in Figure 3. These plots show that the software receiver used in this research is at least as accurate as the receiver used in [3]. The zero time used in this paper's plots occurs at 477,882.37 week-seconds GPS time on 14 September 2012 which corresponds to the start of scenario two.

Time and Power Differences

Analysis of the TEXBAT data sets downloaded from [6, 7] revealed apparent offsets in the time alignments and relative powers of the scenarios. Researchers utilizing the TEXBAT data may find it useful to align the scenarios in time. To find the sample-accurate offsets, a piece of each scenario before spoofing was correlated with a piece of the appropriate clean scenario. Table 1 lists the offsets for each static scenario in samples and seconds. The clean dataset predated each of the scenarios with the exception of the new scenarios, 7 and 8, which were already perfectly aligned because they had the spoofing signals digitally added to the clean dataset [4].

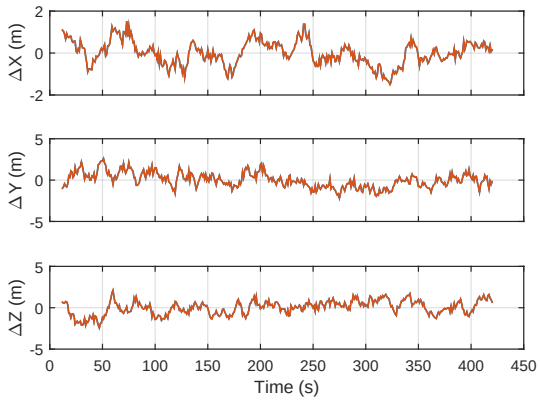

Figure 2. (U) Calculated position errors over time for the clean static scenario. The zero positions are the means of the calculated clean scenario positions (-741992.74, -5462240.48, 3198027.11).

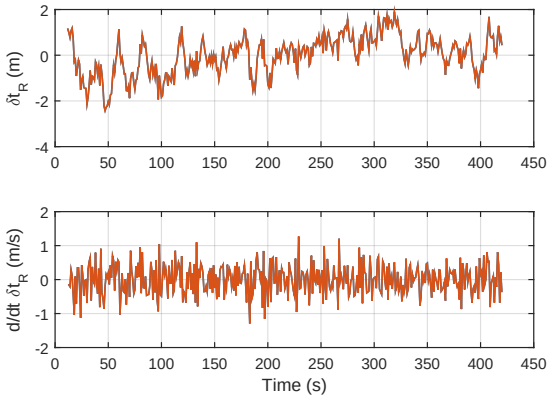

Figure 3. (U) Receiver clock error of the solution over time for the clean static scenario.

The overall power of the clean static scenario was also found to be 8.6 dB higher than the pre-spoofing part of the spoofed scenarios. An amplitude correction factor was found empirically to be 0.373. Multiplication of the clean static scenario by this factor will scale the raw signal and noise power in the sampled data to match that recorded in the spoofing scenario files. Scenarios seven, eight, and the clean static scenario should be multiplied by this correction factor to eliminate the increased signal and noise power relative to Scenarios 1-4.

Carrier and Code Rate Offset

A small constant offset between the code and carrier range rates was observed in scenarios one through four. This discrepancy could be caused by a uniform shift in all retransmitted carrier frequencies, as was done to

Table 1. TEXBAT static scenario sample and time offsets.

Scenario	Samples Offset from Clean	Time Offset (seconds)
1	62,561,438	2.50245752
2	74,922,938	2.99691752
3	55,083,021	2.20332084
4	69,344,725	2.77378900
7	0	0
8	0	0

create Scenarios 1-4. This causes a drift of the code minus carrier (CmC) range which was calculated to be approximately 0.0702 m/s, and translates to a carrier offset of 0.369 Hz as seen in Figure 4. By running the receiver with this value subtracted from the local replica carrier frequency, the drift was zeroed for all PRNs in scenarios 1-4. Because this drift is common to all PRNs in spoofing Scenarios 1-4, but not present in the clean static data or Scenarios 7-8, it is believed that the oscillator of the vector signal generator re-broadcasting the previously recorded clean RF data into the spoofer while re-recording the spoofed scenarios was offset by approximately 0.369 Hz relative to the clean data recording. It will be important for researchers using the TEXBAT datasets to account for this carrier offset in Scenarios 1-4. Otherwise, a potential spoofing detector could be biased by the drift in code and carrier ranges.

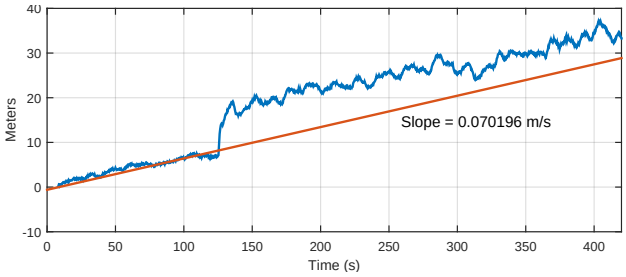

Figure 4. Drift rate of the PRN 23 carrier and code range difference in Scenario 1. This drift rate was found to be common with all PRNs in Scenarios 1-4.

Spectrum Artifacts

Some features in the RF spectrum present during the simulated spoofing attacks are also noteworthy. For example, a double side-band spectrum of the spoofer's signal is visible in some scenarios after the spoofer is turned on. This can be clearly seen in Scenario 2, depicted in the spectrogram shown in Figure 5. These features could be easily spotted by a simple detector looking at the raw RF spectrum, but such features are likely to be minimized with different radio hardware or better filtering. Any spoofing detection techniques based on these RF features will also fail on scenarios seven and eight since the spoofer is digitally added to the clean signal.

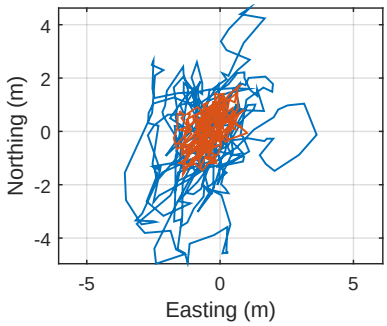

Figure 6. Scenario 1 (blue) horizontal position track overlayed on the clean scenario's track (orange) as calculated by the software receiver. The origin is located at 30°17′15.068″N, 97°44′08.642″W.

Solution Comparisons

The software receiver's tracking loops used in this research were configured with a correlator spacing of 0.1 chips and was carrier-aided with a phase-lock loop bandwidth of 10 Hz. With these tight tracking tolerances, not all of the tracking loops were captured by the spoofer in all scenarios. This caused some of the spoofer induced solution errors to differ from that shown in the TEXBAT white paper [3]. In TEXBAT Scenario 1, the receiver was switched from live-sky GPS signals to spoofer signals with the live-sky signals removed, so all tracking loops were successfully captured by the spoofer. The significant ∼10 dB power advantage in Scenario 2 enabled the spoofer to capture all tracking loops. However, only PRN 7 was captured in Scenario 3, which employed a 1.3 dB power advantage. While Scenario 4 only employed a 0.4 dB power advantage, it successfully captured PRNs 3, 10, and 23. The spoofing signals in Scenarios 7 and 8 successfully captured all tracking loops. Figures 6 through 10 show the software receiver's calculated position tracks from scenarios 1, 2, 3, 4, and 7 respectively, as well as the clean scenario track. The timing errors induced by the spoofer in Scenarios 1-4 and 7 are shown in Figures 11 through 15. Figures 8, 9, 13, and 14 exhibit a deviation from the intended spoofing profile shown in [3] due to the partial tracking loop capture experienced in Scenarios 3 and 4. All tracking loops in Scenarios 1, 2, and 7 are successfully spoofed and therefore the position and timing error plots shown here match very closely to the solution plots in [3].

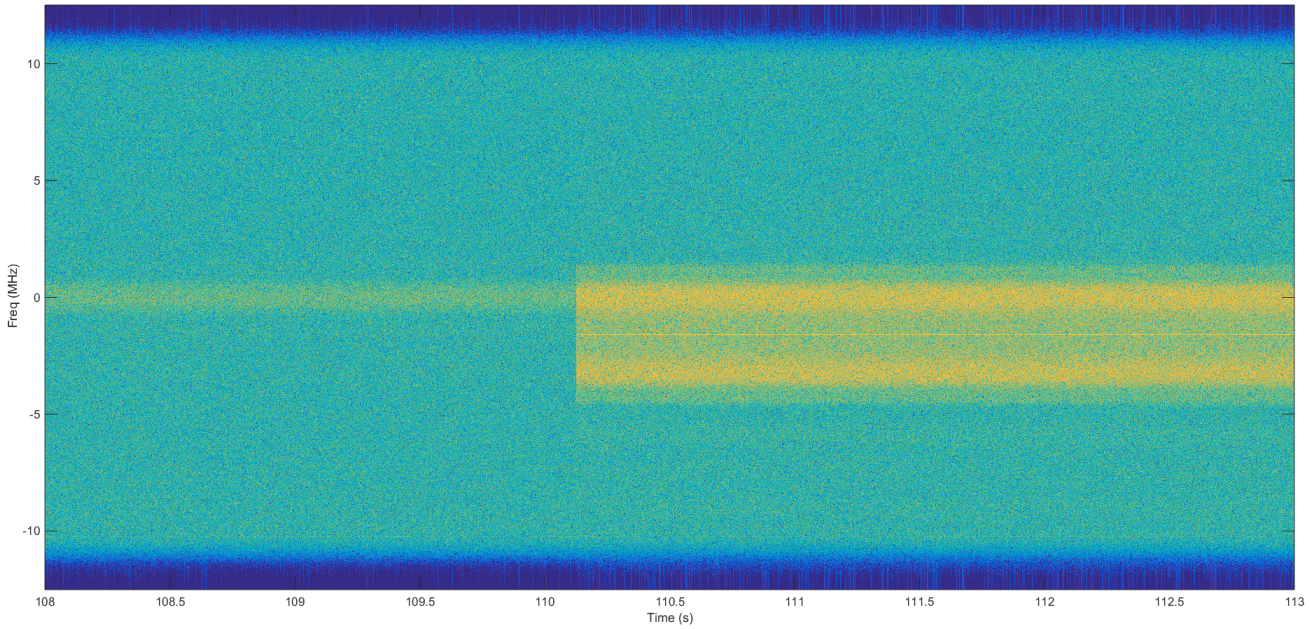

Figure 5. Spectrogram of the raw RF at the onset of spoofing in Scenario 2.

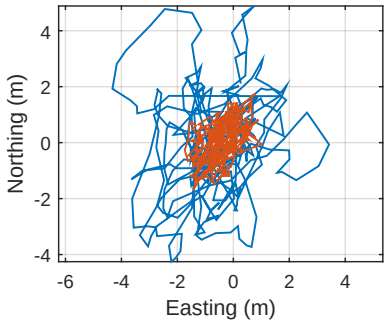

Figure 7. Scenario 2 (blue) horizontal position track overlayed on the clean scenario's track (orange) as calculated by the software receiver. The origin is located at 30°17′15.068″N, 97°44′08.642″W.

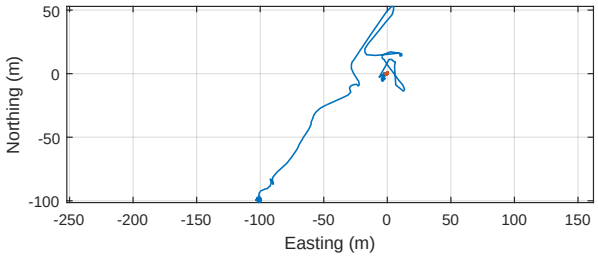

Figure 9. Scenario 4 (blue) horizontal position track overlayed on the clean scenario's track (orange) as calculated by the software receiver. The origin is located at 30°17′15.068″N, 97°44′08.642″W.

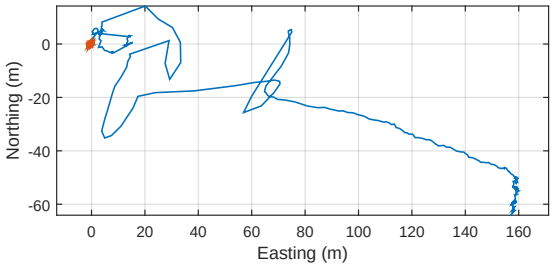

Figure 8. Scenario 3 (blue) horizontal position track overlayed on the clean scenario's track (orange) as calculated by the software receiver. The origin is located at 30°17′15.068″N, 97°44′08.642″W.

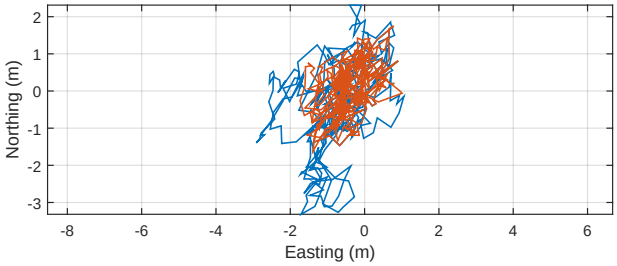

Figure 10. Scenario 7 (blue) horizontal position track overlayed on the clean scenario's track (orange) as calculated by the software receiver. The origin is located at 30°17′15.068″N, 97°44′08.642″W.

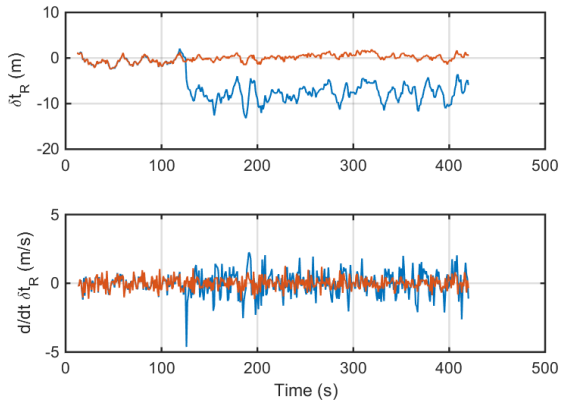

Figure 11. Top panel showing the Scenario 1 solution's time history of the receiver clock error overlayed on the clean scenario's (orange). Bottom panel showing the clock error rate of the solution of the clean (orange) and Scenario 1 (blue) datasets.

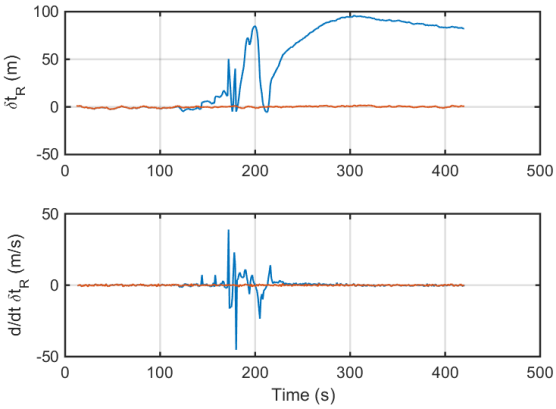

Figure 13. Top panel showing the Scenario 3 solution's time history of the receiver clock error overlayed on the clean scenario's (orange). Bottom panel showing the clock error rate of the solution of the clean (orange) and Scenario 3 (blue) datasets.

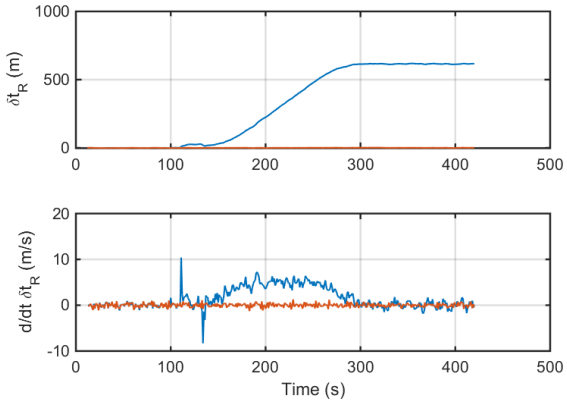

Figure 12. Top panel showing the Scenario 2 solution's time history of the receiver clock error overlayed on the clean scenario's (orange). Bottom panel showing the clock error rate of the solution of the clean (orange) and Scenario 2 (blue) datasets.

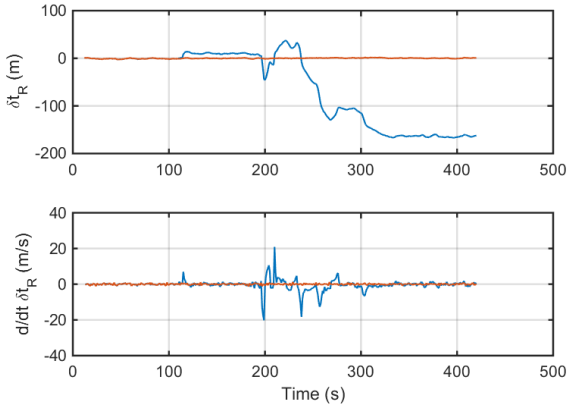

Figure 14. Top panel showing the Scenario 4 solution's time history of the receiver clock error overlayed on the clean scenario's (orange). Bottom panel showing the clock error rate of the solution of the clean (orange) and Scenario 4 (blue) datasets.

Revised Timing of Spoofing Events

From these and other receiver tracking observables, the onset time of major spoofing state transitions were preceisely determined. Table 2 shows the onset times of three separate spoofing events which are denoted as the activation signature, the spoofing signal onset, and the pull-off start. All times are given in seconds after the start of scenario two, incorporating the offsets in Table 1. The "activation signature" is a perceptible disturbance that can be ascertained from a correlator discontinuity as well as changes in the signal spectrum. The spoofing signal onset is determined by jumps in multiple observables, including the C/N_0 estimator, phase tracking error, and the output of the correlators. Pull-off start was estimated from the start of the position or timing solution deviation, and/or the CmC observable. These start times were found to differ slightly across scenarios and with the spoofing start times given in [3]. Figure 16 shows the correlator tap history from [3] for Scenario 3 lined up visually with the tap history produced by GEARS. The correlator responses are visibly aligned, where the time axis on the GEARS plot has its zero reference as the start time of Scenario 2.

Conclusion

These observations of the TEXBAT datasets highlight important signatures and biases for researchers to be aware of when using these datasets to advance the field of GPS signal authentication. It is hoped that this paper will aid researchers to correct the observed time

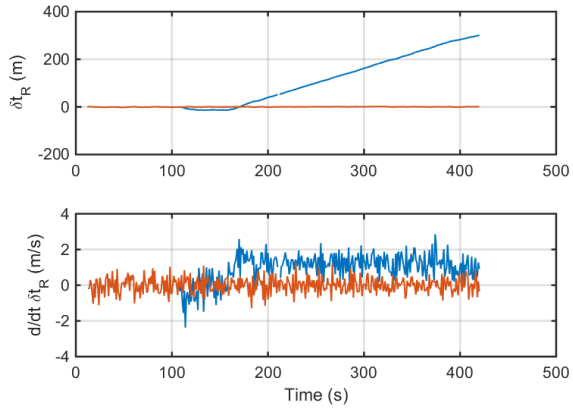

Figure 15. Top panel showing the Scenario 7 solution's time history of the receiver clock error overlayed on the clean scenario's (orange). Bottom panel showing the clock error rate of the solution of the clean (orange) and Scenario 7 (blue) datasets.

Table 2. (U) TEXBAT spoofing event times in seconds after start of scenario two.

Scenario	Activation Signature	Spoofing Signal Onset	Pull-off Start
1	117.5	125	N/A
2	99.4	110.1	133
3	114.1	118.9	195
4	109.9	113.8	225
7	N/A	110	136
8	N/A	110	136

offsets, range rate offset, and power differences.

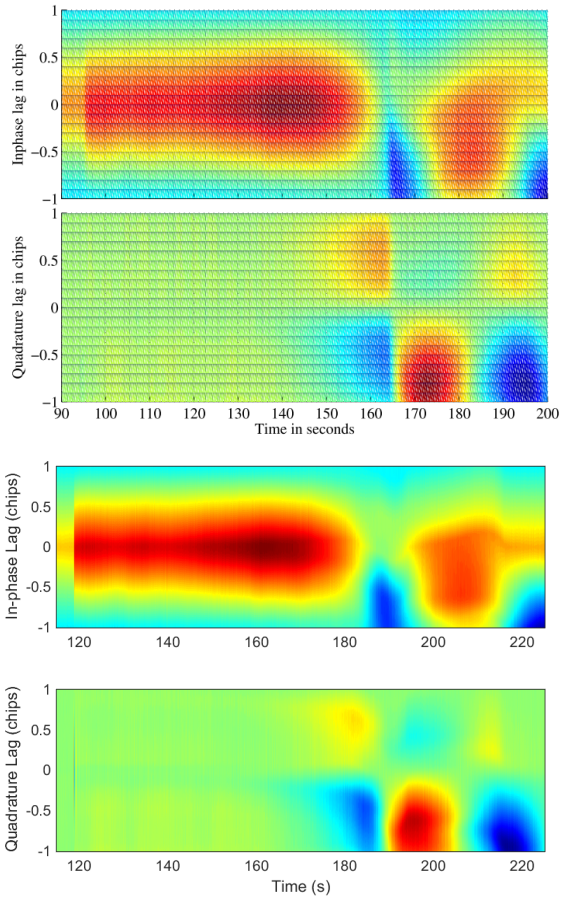

Figure 16. Top two figures show the in-phase and quadrature correlation space history of Scenario 3 from [3] with 21 correlator taps. The bottom two figures show the PRN 23 in-phase and quadrature correlation space history from the software receiver using 61 correlator taps and 50 millisecond accumulation time.

References

[1] S. Kiese, "Gotta Catch Em All! WORLDWIDE! (or how to spoof GPS to cheat at Pokmon GO)." https://www.insinuator.net/2016/07/gotta-catch-em-all-worldwide-or-how-to-spoof-gps-to-cheat-at-pokemon-go/, 2016. Accessed: 29 Aug 2016.

[2] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*, 2016.

[3] T. E. Humphreys, J. a. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas Spoofing Test Battery : Toward a Standard for Evaluating GPS Signal Authentication Techniques," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012) September 17 - 21, 2012 Nashville Convention Center, Nashville, TN*, no. 1, pp. 3569 – 3583, 2012.

[4] T. E. Humphreys, "Texbat Data Sets 7 and 8," tech. rep., 2015. http://radionavlab.ae.utexas.edu/datastore/texbat/texbat_ds7_and_ds8.pdf.

[5] S. Gunawardena, "Class Notes, EENG 633 - Global Navigation Satellite System Receiver Design," 2015. https://www.afit.edu/docs/2015-2017%20AFIT%20Graduate%20Catalog.pdf.

[6] T. E. Humphreys, "http://www.ni.com/landing/119/en/," 2012.

[7] T. E. Humphreys, "http://radionavlab.ae.utexas.edu/datastore/texbat/," 2015.