GNSS Test Vector Distribution Methodology

Brady O'Hanlon, Christian Keefer-Moomaw

CGSIC 2024

Baltimore, MD

Approved for public release, case #24-2543

Homeland Security Systems Engineering & Development Institute

Acknowledgements

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the U.S. Department of Homeland Security (DHS), acting through the DHS Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. MITRE Corporation operates the Homeland Security Systems Engineering and Development Institute (HSSEDI) as an FFRDC for DHS S&T under contract 70RSAT20D00000001.

The HSSEDI FFRDC provides the government with the necessary systems engineering and development expertise to conduct complex acquisition planning and development; concept exploration, experimentation and evaluation; information technology, communications and cyber security processes, standards, methodologies and protocols; systems architecture and integration; quality and performance review, best practices and performance measures and metrics; and independent test and evaluation activities. The HSSEDI FFRDC also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The HSSEDI FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under:

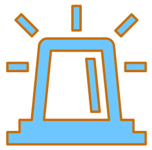
Task Order 70RSAT20FR0000062
DHS S&T Next Generation Resilient PNT
The results presented in this report do not necessarily reflect official DHS opinion or policy.

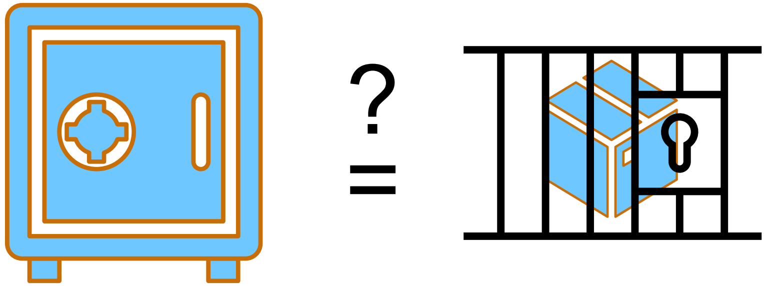
Case Number 24-2543 / 70RSAT20FR-062-19

HSSEDI
Homeland Security Systems Engineering & Development Institute

Background

- **Resilient and robust Positioning, Navigation, and Timing is ever more important**
- **Testing PNT systems against threats has historically been challenging**
  - How does system X respond to threats?
  - How do we compare systems X and Y?
  - What happens when a threat is (un)detected?
  - How can I test without being an expert at generating threats?
- **This tool intended to help answer these questions**

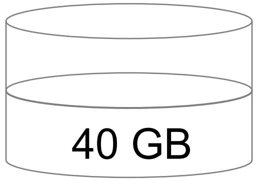




Current Approaches

- **GNSS Simulator plus expert**
- **Custom receiver / simulator**
- **Government run field tests**
- **Pre-generated scenarios (e.g., Texas Spoofing Test Battery)**
- **Avoid testing?**

Test #1 of 75

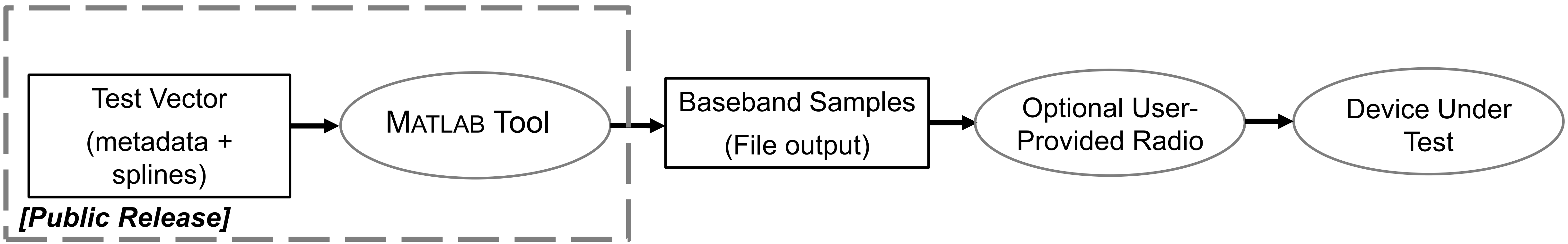


Tool Development Approach

- **Desire a solution that enables threat testing that:**
  - Does not require specialized hardware
  - Does not enable attacks synchronized to the world
  - Is highly flexible
  - Limits infrastructure needed for distribution
  - Can realize realistic and representative threats
  - Doesn’t require user expertise
- **Solution: software tool ingests small (provided) metadata files, generates baseband samples**

P1952, CASC, Field test prep, R&D

Test Vector Distribution Methodology Overview



- **Test vectors are processed by the HSSEDI-provided tool to convert the compact test vector into samples that represent the radiofrequency (RF) signals modeled by the test vector**
- **These samples are then converted to RF by the user-provided tool of choice (e.g., a universal software radio peripheral [USRP])**
- **The resultant RF signals are input to the device under test**

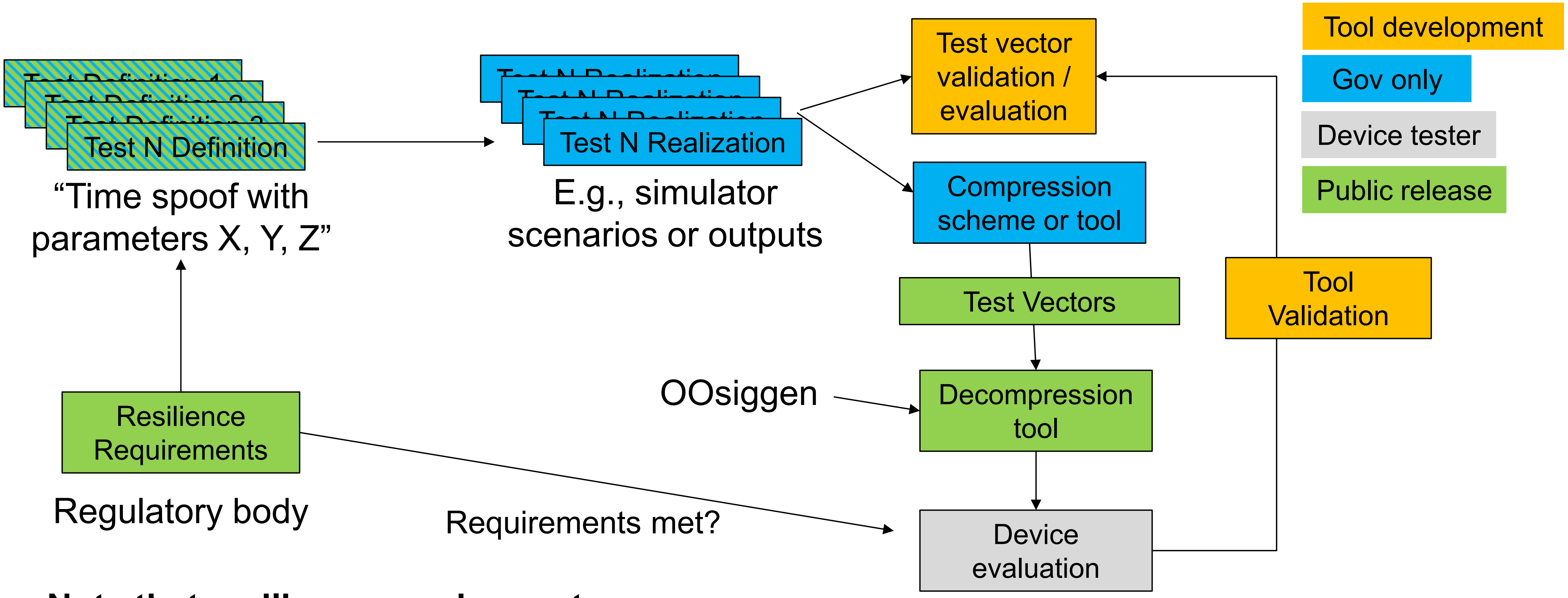
HSSEDI
Homeland Security Systems Engineering & Development Institute

Test Vector Format Overview

A complete test vector as defined for use with these tools comprises various files:

- A JSON file defining the signals that are present in the test vector and various constant parameters for each signal - center frequency, pseudorandom noise code (PRN), etc.
- A set of splines (piecewise polynomials) for each signal defining signal parameters that may change over time:
  - Signal power
  - Pseudorange
  - Doppler Shift
  - Data symbols (supports bi- and quadrature phase shift keying)
  - Noise power

Test Vector Example Use Case



Note that resilience requirements are not part of this task

HSSEDI
Homeland Security Systems Engineering & Development Institute

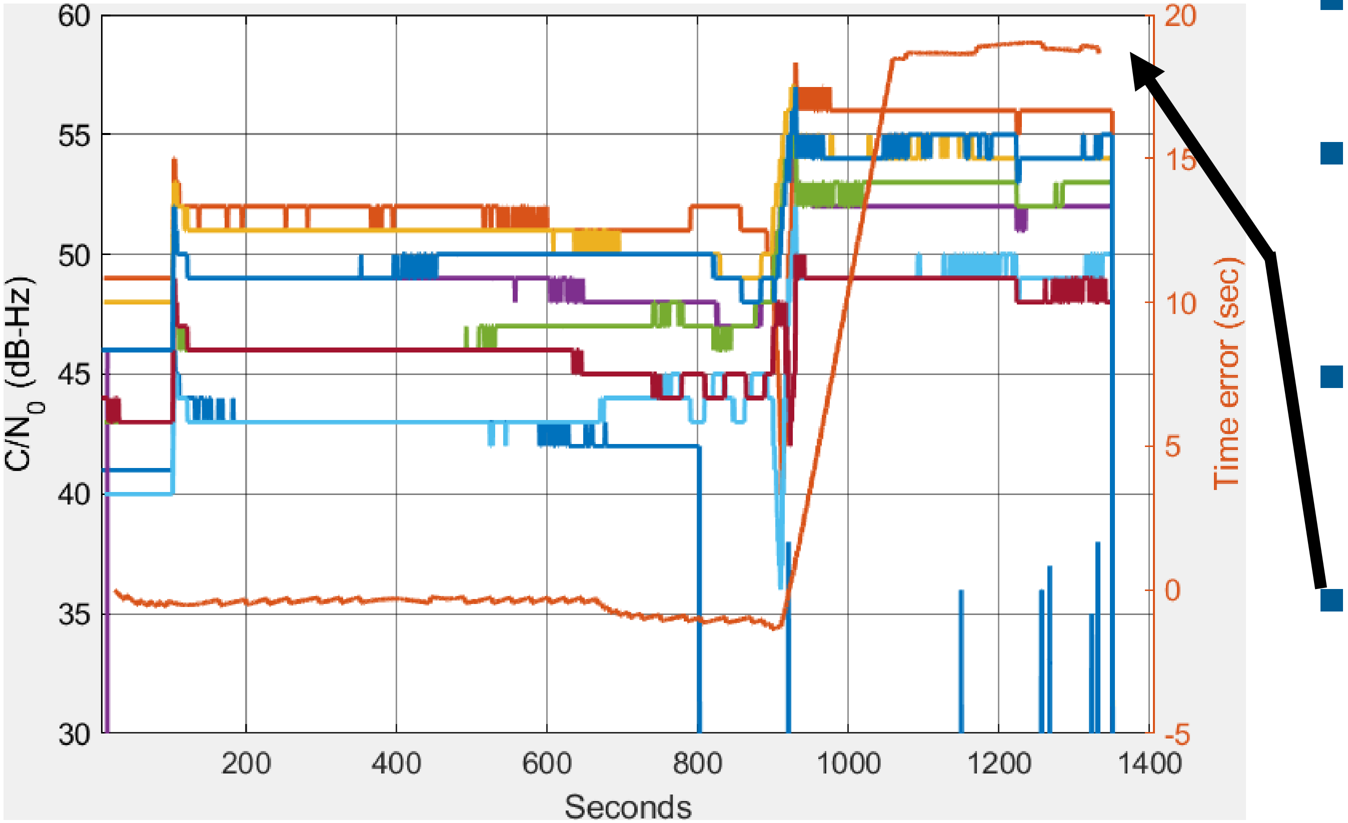
Test Vector Distribution Methodology Capabilities

- **At the time of delivery, the software tool OOsiggen which converts the test vectors into baseband samples supports the following:**
  - GPS C/A, L1C, L5; Glonass L1OF, Galileo E1OS (although only GPS C/A and E1OS are currently supported by the internal test vector creation tool)
  - Broadband noise
  - Any number of signals and constellations
  - Any spoofing scenario that can be created by modifying pseudoranges, carrier phases, signal powers, data bits, or noise power for the support signals
  - Baseband data generated with user-specified sample rate as 16-bit complex interleaved samples

Exemplary Test Vectors

- **Similar to previous sets, for comparison:**
  - TV1: Stationary overpowered time walk
  - TV2: Stationary matched power time walk, freq. lock mode
  - TV3: Stationary matched power position walk, freq. lock mode
  - TV4: Dynamic overpowered position walk
- **Excursions from previous sets**
  - TV5: Stationary overpowered time walk with added noise to maintain C/N0 and Galileo E1OS
  - TV6: Stationary overpowered constant acceleration time walk
  - TV7: Dynamic overpowered position walk with 2 signals unspoofed
- **New tests**
  - TV8: 1 ms time jump with knockoff jamming (demonstrates extended effect duration)
  - TV9: Data compliance check (only one signal set present, subset of satellites with non-compliant data)
- **Scenario details: chose time / location to be generally uninteresting to minimize chance of nefarious use**

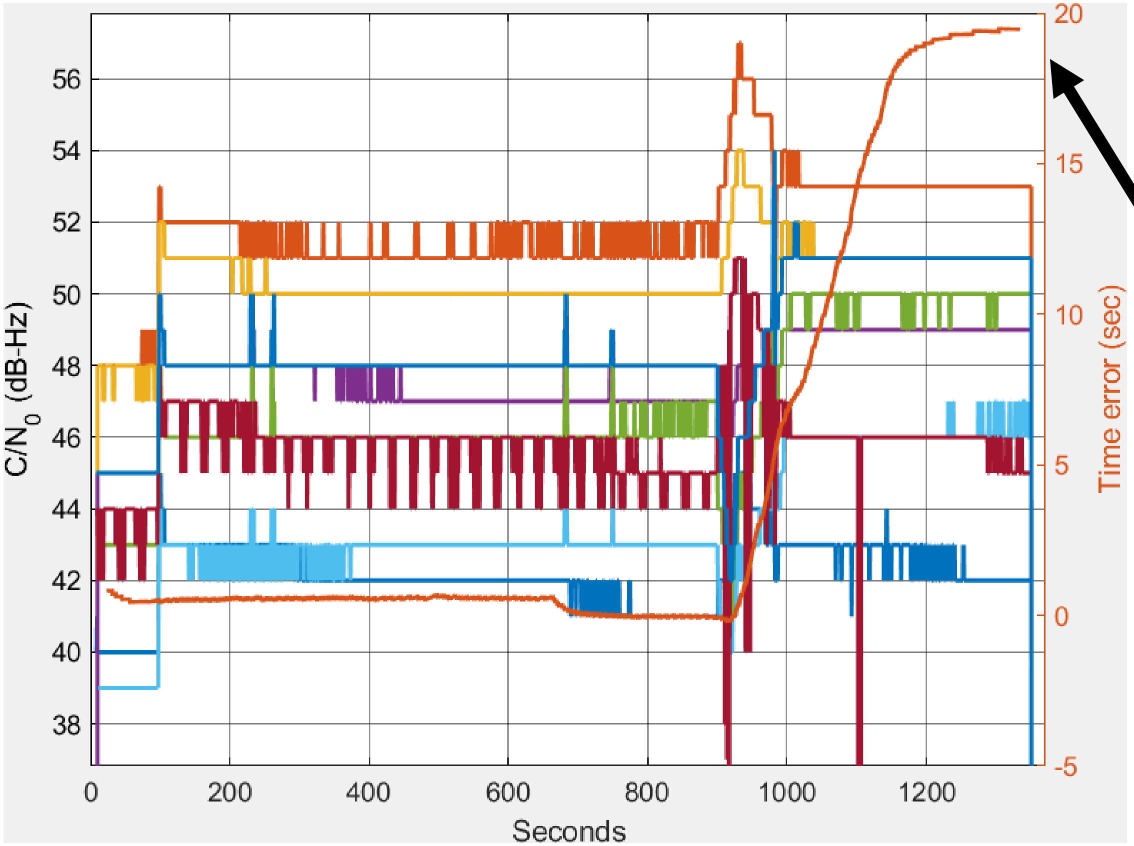
Test Vector 1 Design and Impact



- Scenario includes only GPS C/A signals
- Victim is stationary, attacker has very good knowledge of victim antenna location
- Spoof signals have a 10 decibel (dB) power advantage over authentic
- Observed time error very close to intended time error of 2 microseconds (uS) at scenario end

HSSEDI
Homeland Security Systems Engineering & Development Institute

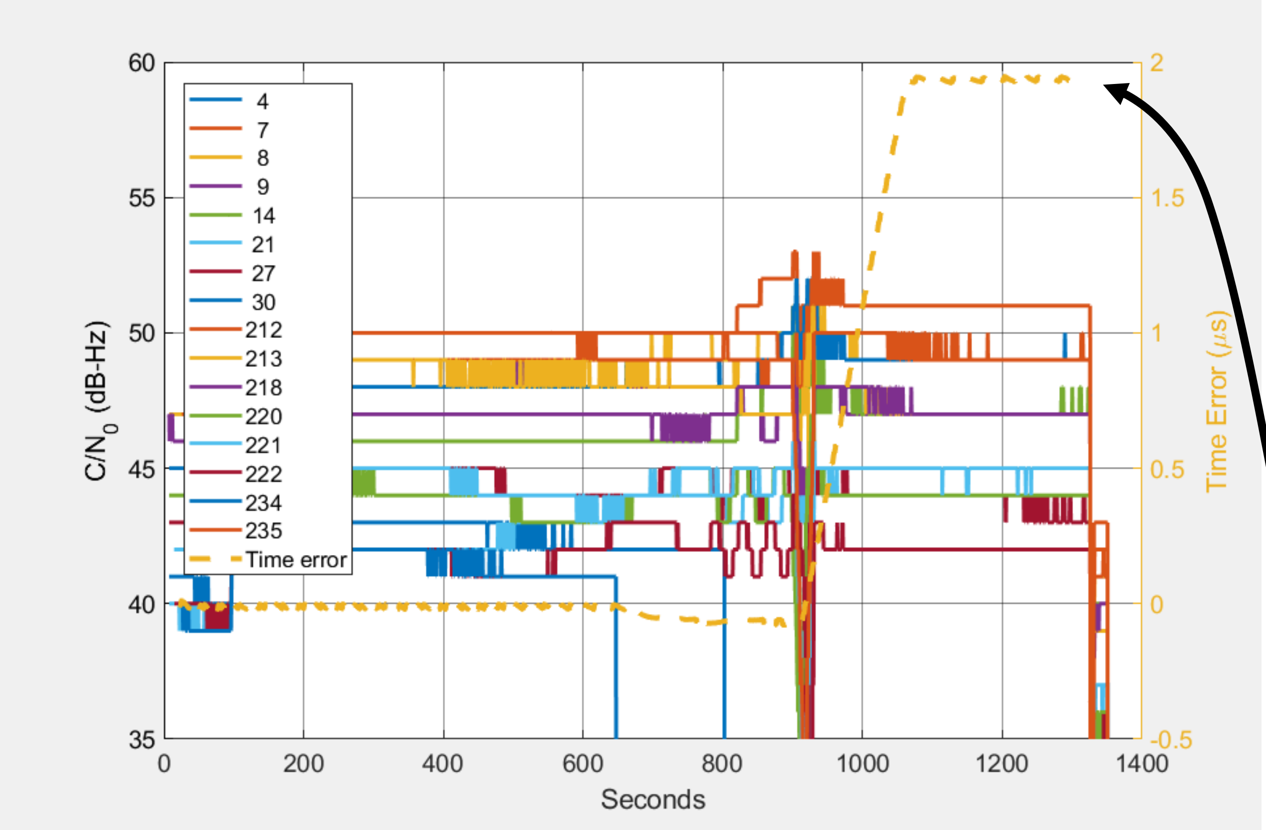
Test Vector 2 Design and Impact



- **This scenario is identical to TV1 except that**
  - Spoofer power advantage is 2 dB
  - Spoofer uses so-called “frequency lock mode” to mitigate beating between true and spoofed signals with small power advantage
- **Observed time error very close to intended time error of 2 uS at end of scenario**

HSSEDI
Homeland Security Systems Engineering & Development Institute

Test Vector 5 Design and Impact

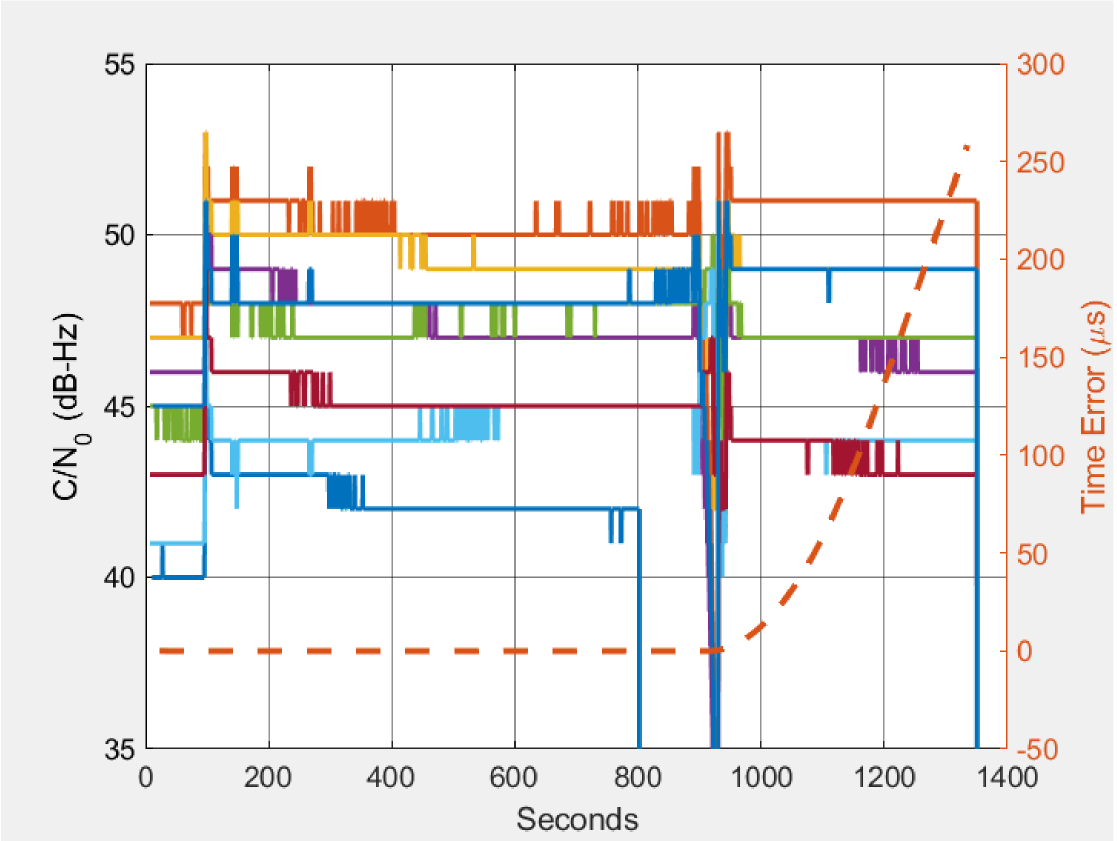


- **Stationary target**
- **Noise is added as spoof power is increased to hold victim C/N0 constant.**
- **Also include Galileo E1OS signals spoofed in the same manner.**
- **Note that Galileo PRNs are (PRN + 210) in plot legend**
- **Induced time error matches intended spoof**

Test Vector 6 Design and Impact

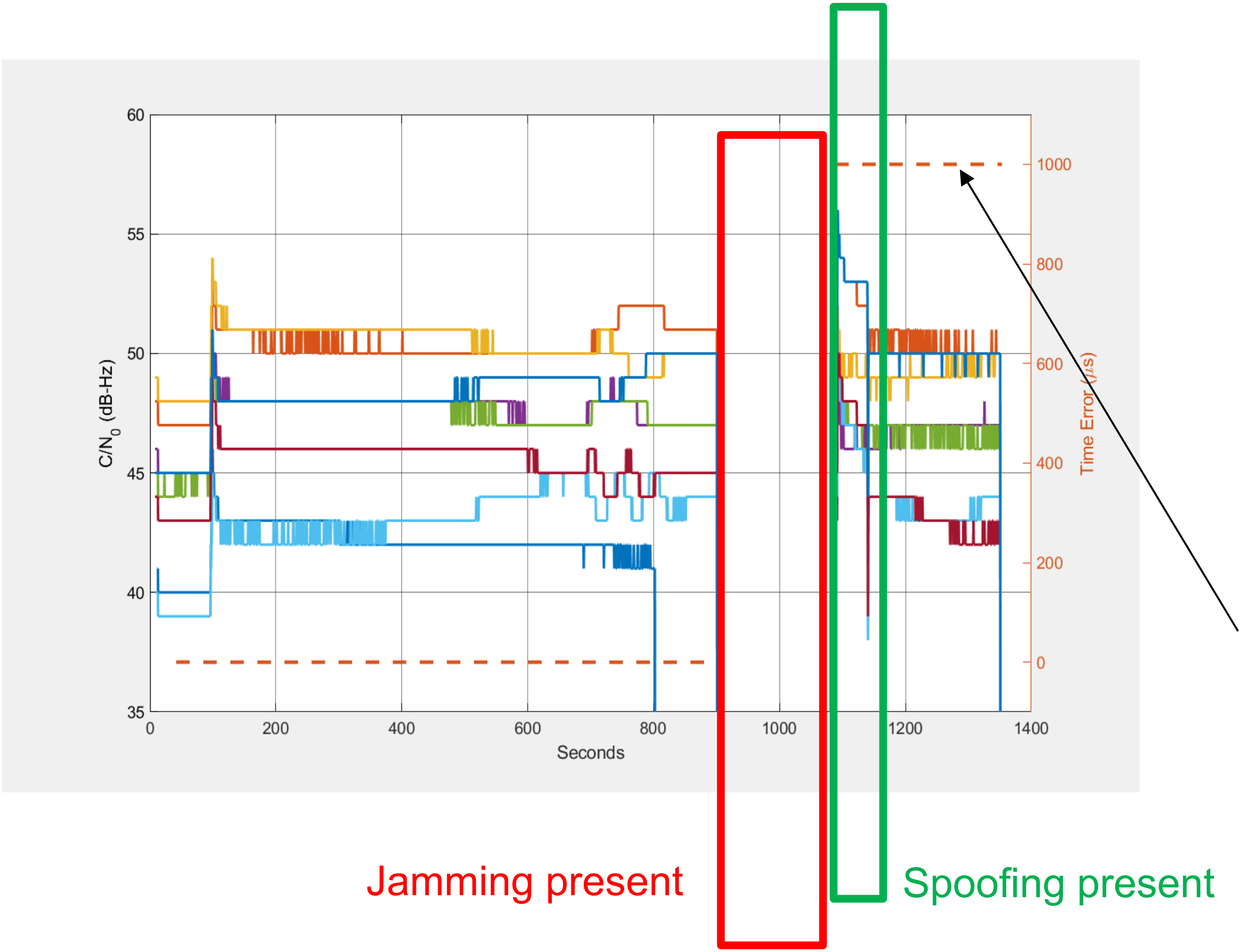
- **Stationary target**
- **GPS C/A only**
- **Time spoof has constant acceleration of 1 m/s^2 from 930-1200 seconds, then constant velocity after that**
- **1.3 dB spoof power advantage with commensurate added noise**
- **Receiver time error very closely matches intended spoof, reaching 250 µs at scenario end**

C/N0 and Time Error from Device Under Test



HSSEDI
Homeland Security Systems Engineering & Development Institute

Test Vector 8 Design and Impact



- Scenario location and other parameters identical to TV1
- Jamming present from 900-1080 seconds
- Spoofing w/ 1 ms time advance present from 1080-1140 seconds
- Returns to truth-only after that
- Receiver time remains 1 ms off even after removal of spoofing signals

HSSEDI
Homeland Security Systems Engineering & Development Institute

Summary

- **A software tool for generating GNSS receiver test vectors has been developed**
  - The test vectors used by this system are compact and easy to distribute
  - This tool greatly lowers barriers to GNSS receiver testing
- **A set of exemplary GNSS spoofing test vectors has been created, and results from one example test receiver processing these test vectors are shown**
  - Additional test vectors are easy to create and distribute
- **The software tool and exemplary test vectors are approved for public released**
  - Hosting location is yet TBD, but stay tuned!

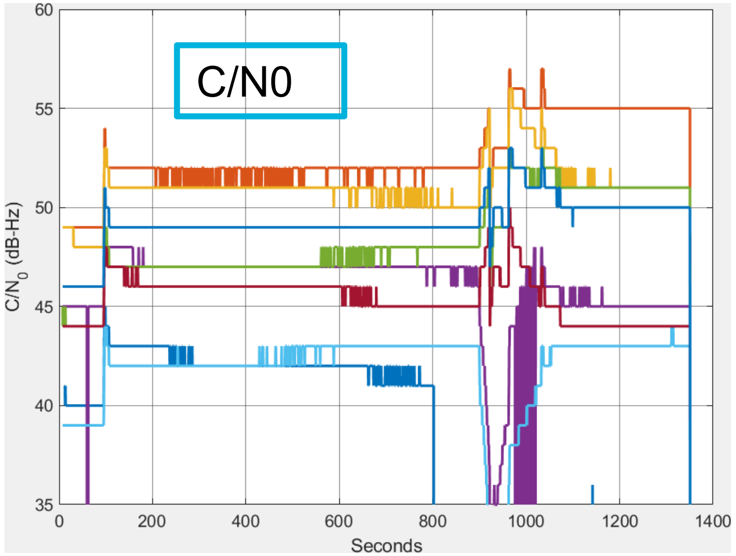
Backup – Additional Exemplary Results

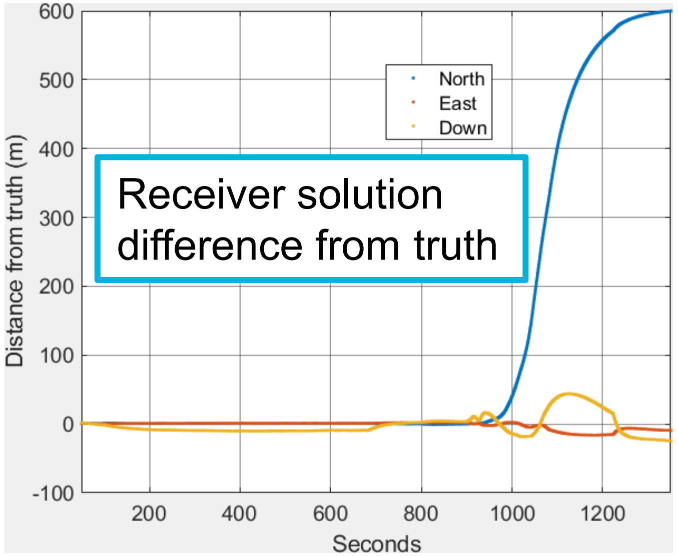
Common Test Vector Details

- Victim Receiver location fixed at 39.833333 North 98.58333333 West, 0 meters height above ellipsoid (static scenarios)
- Start time 2023-Jan-03 21:20:00
- 10-degree elevation mask applied
- Ephemeris reference time is ~2200
- Data bits all set to true (or true-like) at actual scenario time

Test Vector 3 Design and Impact

- **Receiver is stationary at same location as TV1**
- **Spoofer power advantage is 3 dB, frequency lock mode**
- **Intended position spoof moves victim 600m due north over 150 seconds starting at 930 seconds**
- **Spoofed position eventually arrives at intended position; receiver filtering / tracking loop design results in delayed response**

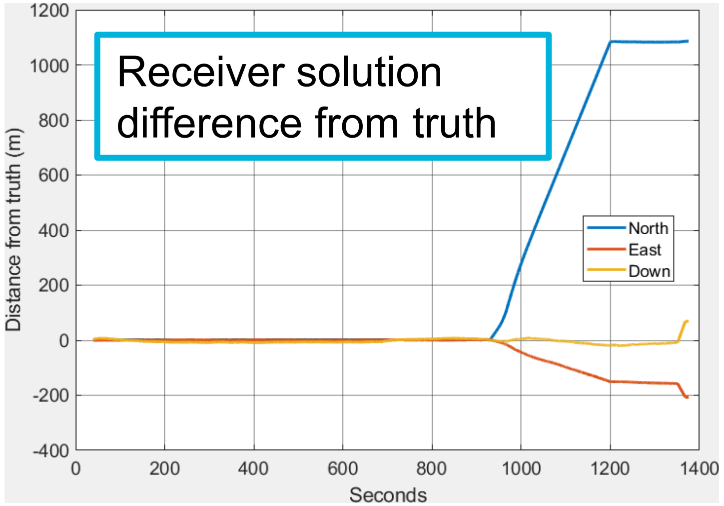


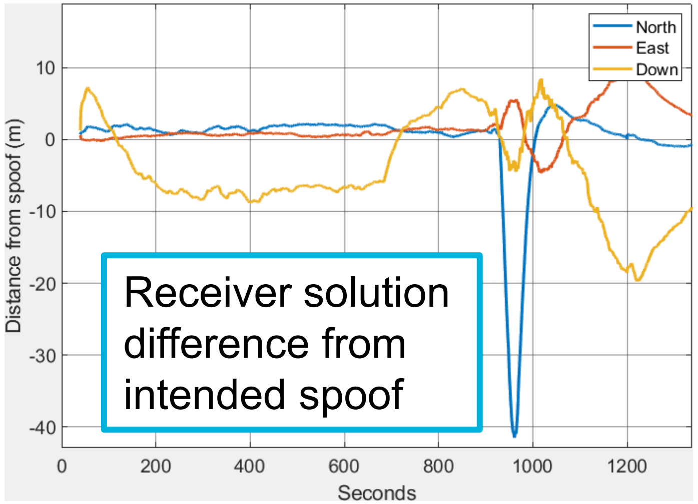


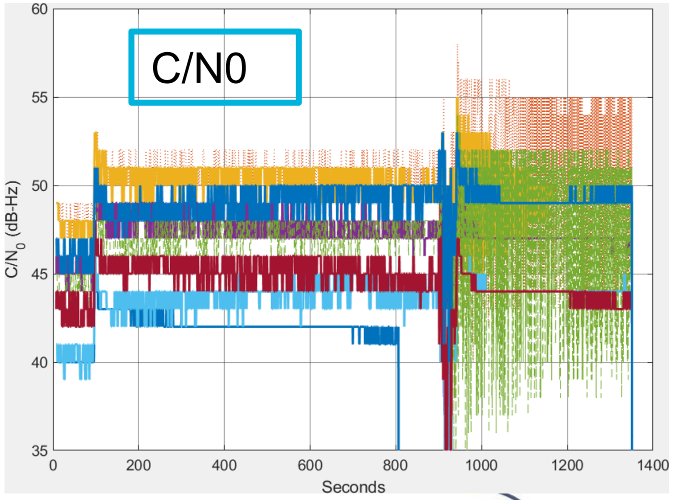
HSSEDI
Homeland Security Systems Engineering & Development Institute

Test Vector 4 Design and Impact

- **Receiver location starts at 39.833333 N 98.58333333 W, 0m HAE**
  - Receiver moves due East at 13 m/s
- **Spoof signals appear at 15:00 and ramp up to +2.3 dB over 30 seconds; noise added to maintain C/N0 at un-spoofed level**
- **Position spoof begins at 15:30, intended spoof would result in receiver turning 17.9 degrees to the north and maintaining 13 m/s speed**
- **Observed C/N0 for 2 signals oscillate significantly due to satellite geometry**
- **Receiver trajectory fairly closely matches intended spoof trajectory**







Test Vector 7 Design and Impact

- **Scenario exactly as TV4: moving victim with position spoof**
  - Except that PRNs 9 and 14 are un-spoofed
  - Intended to emulate an imperfect spoofing scenario or fault in spoofing system
  - Scenario primary utility is in testing spoofing detection algorithms under inconsistent spoofing, thus position response of unprotected receiver (as shown in TV4 plots) is not relevant
- **Note C/N0 for PRNs 9 and 14 decrease due to increased noise and AGC action**