SAND2022-13569C

# Detection and Localization of an Adversarial GPS Interference Source Based on Clock Signatures

Joseph Smith
Joshua Wood
Scott Martin
Connor Brashar (Sandia)

Tuesday, October 04, 2022

AUBURN UNIVERSITY

GPS & Vehicle Dynamics Laboratory

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

# Outline

- Introduction
- Detection using clock signatures
  - Algorithm development
  - Simulation results
  - Hardware validation
- Localization with multiple receivers
  - Range estimation
  - Azimuth and elevation estimate
  - Least squares position solution

# Introduction

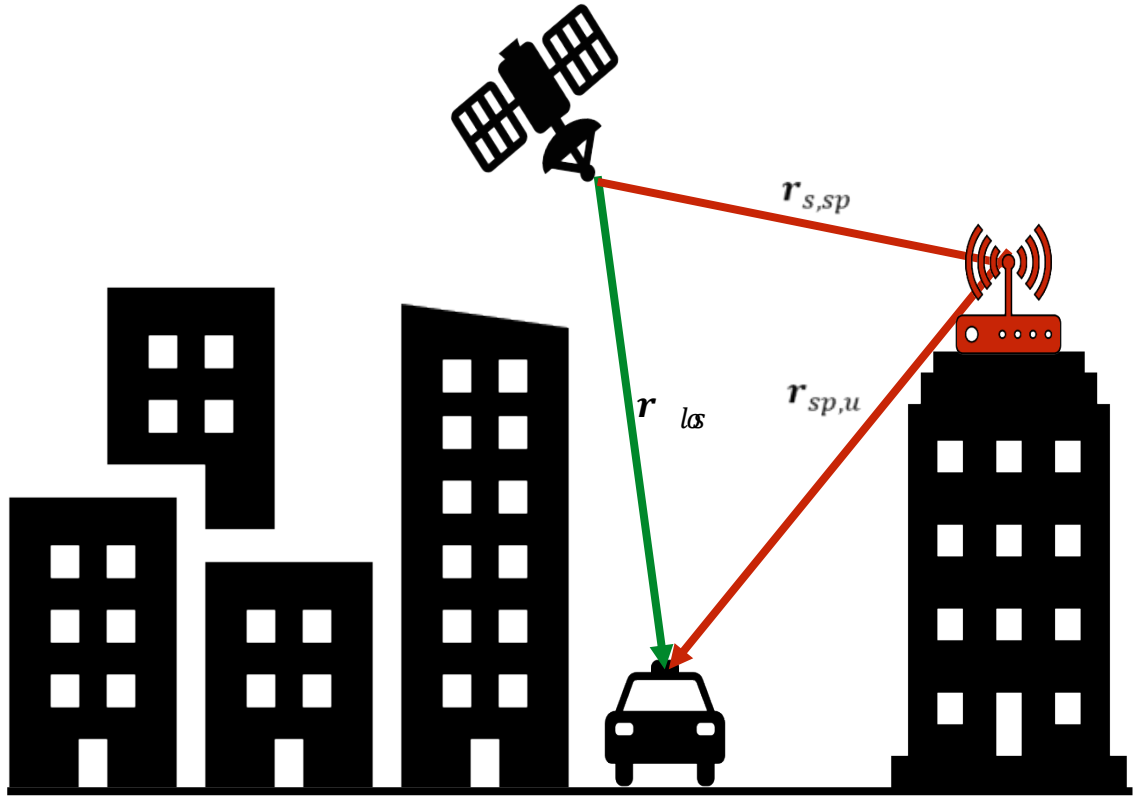
- Detect and localize the source of an inauthentic signal using clock signatures
  - Detection methods are independent of receiver location or signal geometry
  - Detect deviations in clock bias or drift
  - Use deviations to estimate pseudoranges
  - Localize the transmitter of the signal
- Compare results for different types of inauthentic signals
  - Spoofer – time based attack with no change in position

$$\rho_{sp} = r_{s,sp} + r_{sp,u} + cb_u + ct_{proc} + ct_{ctrl} + I + T + \eta$$

  - Meaconer – full position replacement (repeater)

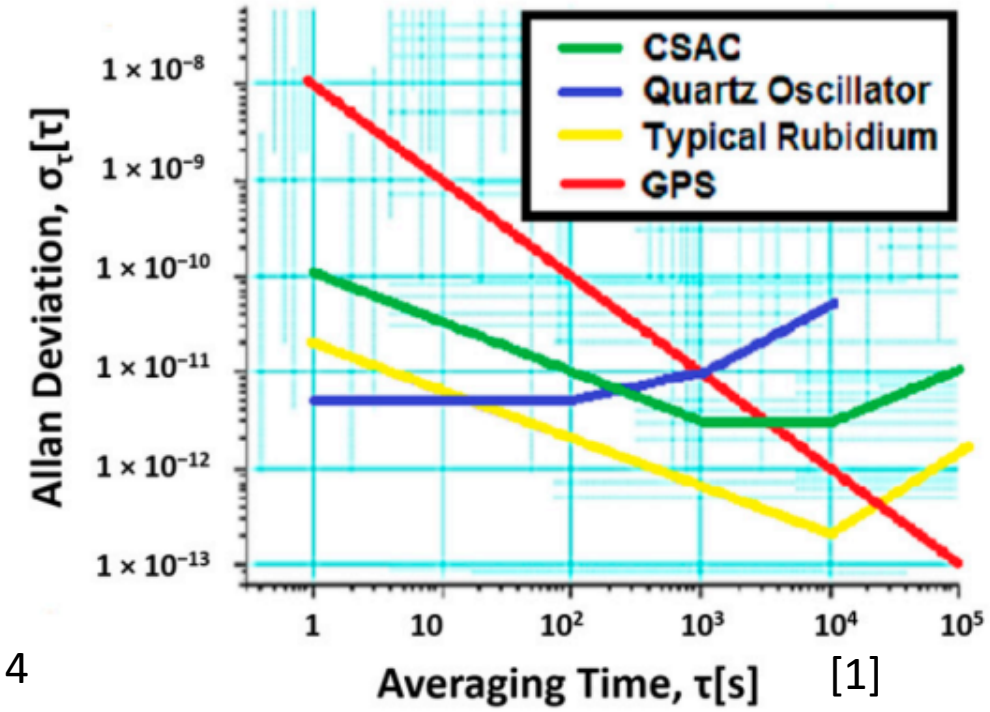
$$\rho_m = r_{s,m} + r_{m,u} + cb_u + ct_{proc} + I + T + \eta$$

  - $t_{proc}$ processing delay
  - $t_{ctrl}$ controlled delay



# Clock Model

- Evaluate algorithms using clocks of various qualities
  - Four clocks tested (two crystal, two atomic)
  - $H_0$ – frequency white noise
  - $H_{-2}$ – frequency random walk



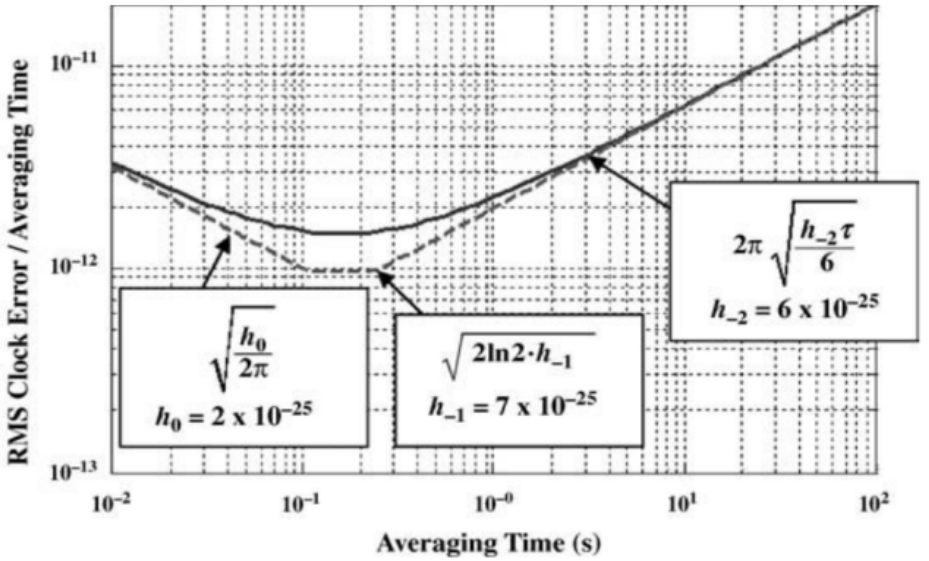

[1]

- Two state Clock Model

$$\begin{bmatrix} \dot{b} \\ \ddot{b} \end{bmatrix}_k = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} b \\ \dot{b} \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} w_b \\ w_r \end{bmatrix}.$$

- Discretized process noise matrix $Q_{clk}$

$$Q_{clk} = \begin{bmatrix} \frac{H_0}{2}\Delta t + \frac{2\pi^2 H_{-2}}{3}\Delta t^3 & \frac{2\pi^2 H_{-2}}{2}\Delta t^2 \\ \frac{2\pi^2 H_{-2}}{2}\Delta t^2 & 2\pi^2 H_{-2}\Delta t \end{bmatrix}$$




[2]

# Clock Parameter Estimation

- Kalman Filter used to estimate clock bias and drift
  - Assume no change in position
  - Assume minimal change in atmospheric effects over short periods
- Clock Drift estimate using pseudorange rate
  - Instantaneous Doppler measurement

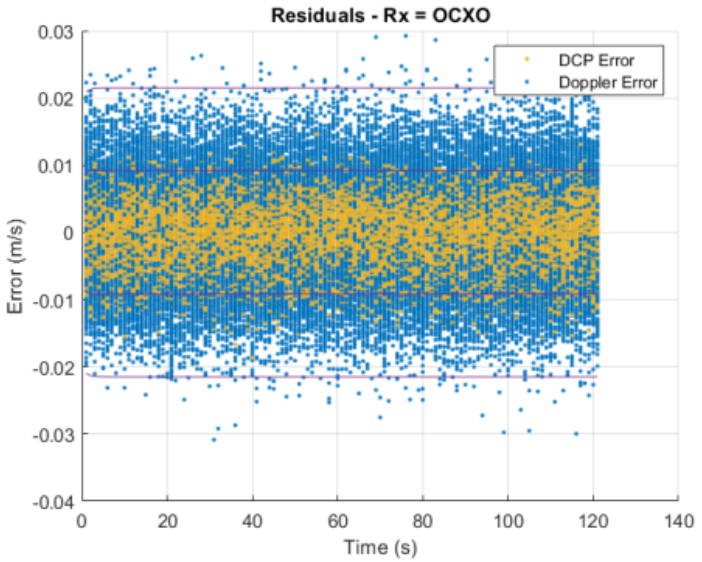
$$\dot{\rho} = D\lambda =$$

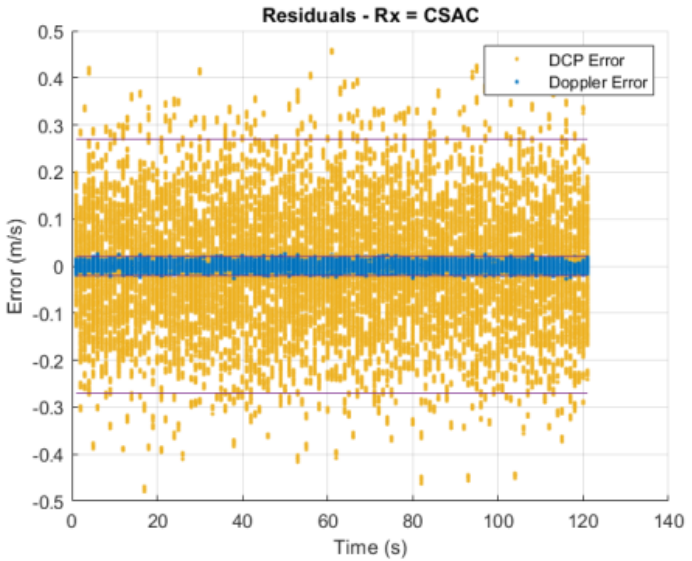
$$c\dot{b} = D\lambda - \frac{\Delta r^i}{\Delta t}$$

  - Delta Carrier Phase measurement

$$\frac{\Delta\phi^i}{\Delta t} = \frac{\Delta r^i + c\Delta b}{\Delta t} = \frac{\Delta r^i}{\Delta t} + c\dot{b}$$

$$c\dot{b} = \frac{\Delta\phi^i}{\Delta t} - \frac{\Delta r^i}{\Delta t}$$

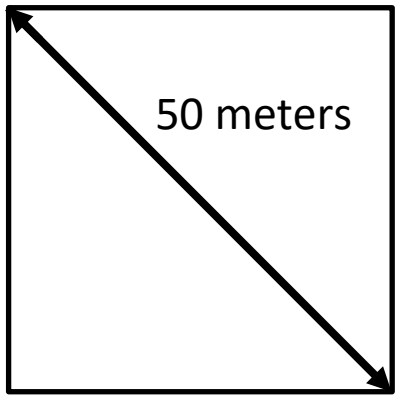


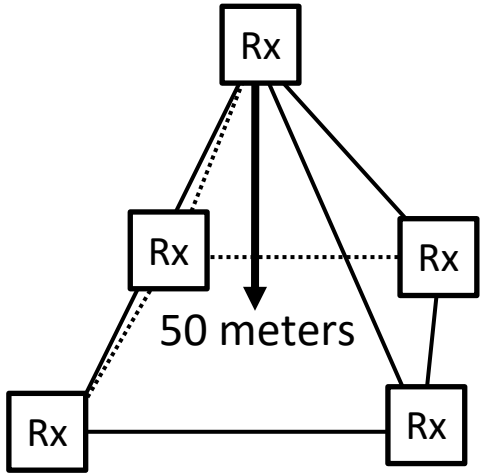



# Test Scenarios

- 50 Monte Carlo runs per simulated test for both scenarios

- Static Simulation
- Five static receivers in a pyramid shape
  - Four at same altitude  meters apart diagonally
  - Fifth in center  meters above others
  - All receivers have same quality of clock




- Dynamic Simulation
- One receiver going in a circle around the emitter
  - 100 Meter radius
  - Completes one rotation every minute
  - Constant altitude

# Single Receiver Detection Methods

- Innovation Filtering
  - Instantaneous error
  - Normalized innovations outside of 3 sigma bounds

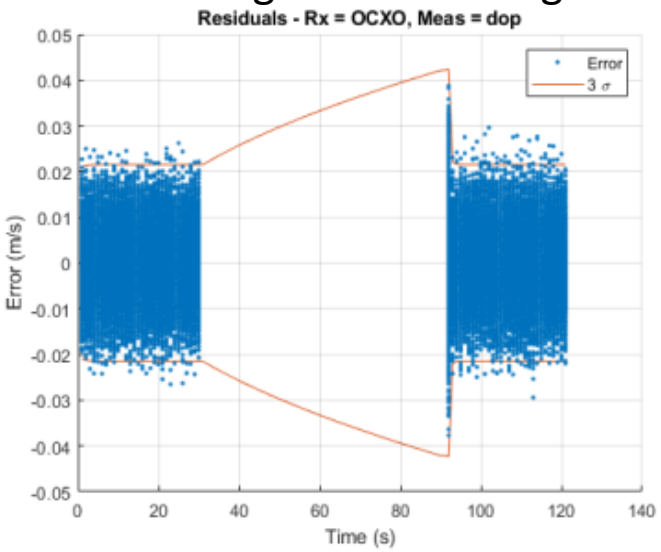
$$y_k = \left| \frac{\delta z_k}{\sqrt{C_{\delta z_k}}} \right| > 3$$

- Innovation sequence monitoring
  - Slow growing errors over time

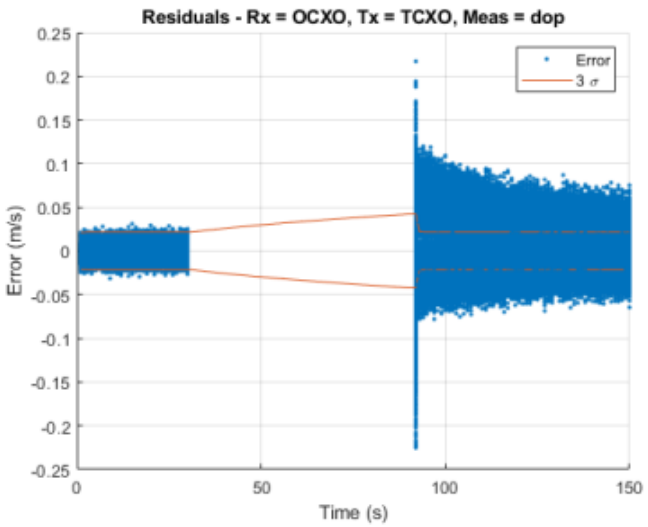
$$\mu_k = \frac{1}{N} \sum_{i=k+1-N}^{k} y_i \qquad |\mu_k| > \frac{T}{\sqrt{N}}$$

Sample results plotted with respect to time

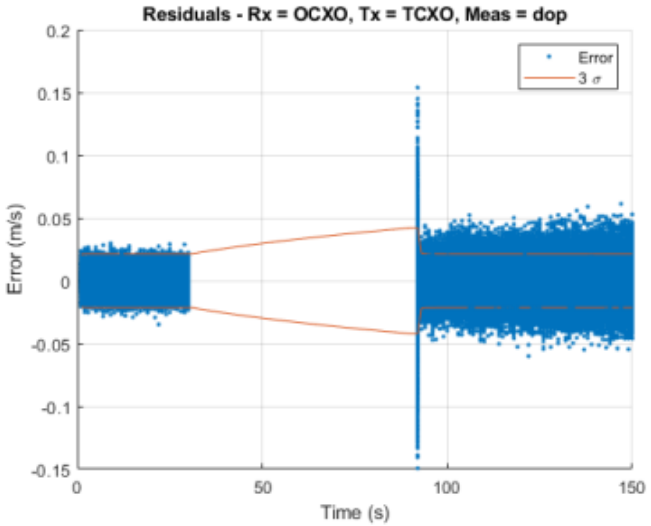
Clean signal after outage




Meaconer after outage




Time spoofing after outage



# Single Receiver Detection Results

- Innovation Filtering detection results and trends:
  1. Higher false alert percentage for clocks with higher frequency noise (CSAC and Rubidium)
  2. Higher detection percentages for atomic clock receivers than crystal oscillators receivers
  3. Easier to detect a transmitter with a higher frequency noise clock (such as CSAC) using a delta carrier phase measurement
- Innovation Sequence Monitoring detection results:
  1. Lowest detection percentage of all methods tested
  2. Higher detection rates for transmitter clocks with larger frequency random walk (TCXO and OCXO) with Doppler measurements
  3. False alerts only occurred when using TCXO which is the worst clock tested

| Innovation Filtering Results with Spoofer | | | | | |
|---|---|---|---|---|---|
| Meas. | Tx | Fault Detection % | | False Alert % | |
| Delta Carrier | Rx = 3 | OCXO | Rubidium | OCXO | Rubidium |
| | TCXO | 100 | 100 | 17.2 | 71.2 |
| | OCXO | 76.4 | 97.2 | 17.6 | 78 |
| | CSAC | 100 | 100 | 15.2 | 73.6 |
| | Rubidium | 100 | 100 | 22.4 | 76.8 |
| Doppler | Rx = 3 | OCXO | Rubidium | OCXO | Rubidium |
| | TCXO | 100 | 100 | 0.4 | 0.4 |
| | OCXO | 80 | 99.6 | 2.4 | 0 |
| | CSAC | 68.8 | 81.2 | 0.4 | 0 |
| | Rubidium | 72.8 | 82.4 | 0.8 | 1.6 |

| Innovation Sequence Monitoring Results with Spoofer | | | | | |
|---|---|---|---|---|---|
| Meas. | Tx | Fault Detection % | | False Alert % | |
| Delta Carrier | Rx = 3 | OCXO | Rubidium | OCXO | Rubidium |
| | TCXO | 100 | 100 | 0 | 0 |
| | OCXO | 8 | 2 | 0 | 0 |
| | CSAC | 100 | 100 | 0 | 0 |
| | Rubidium | 26 | 2 | 0 | 0 |
| Doppler | Rx = 3 | OCXO | Rubidium | OCXO | OCXO |
| | TCXO | 98 | 100 | 0 | 0 |
| | OCXO | 30 | 100 | 0 | 0 |
| | CSAC | 16 | 64 | 0 | 0 |
| | Rubidium | 26 | 60 | 0 | 0 |

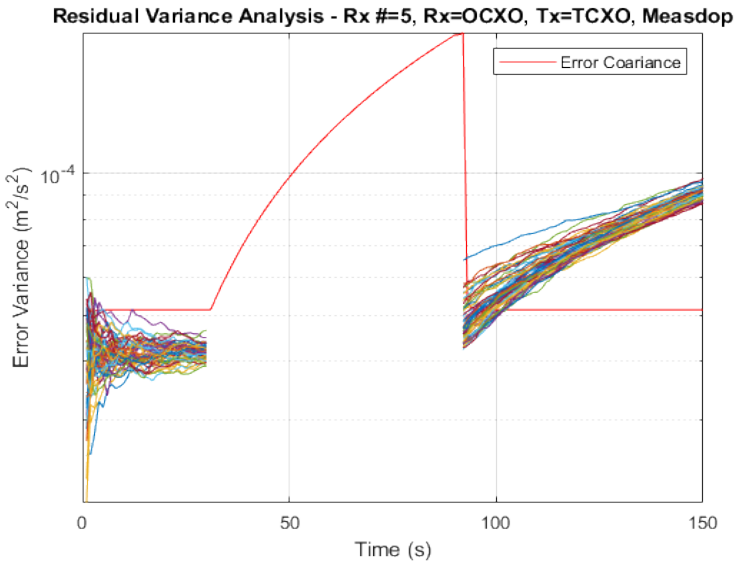
# Multiple Receiver Detection Method

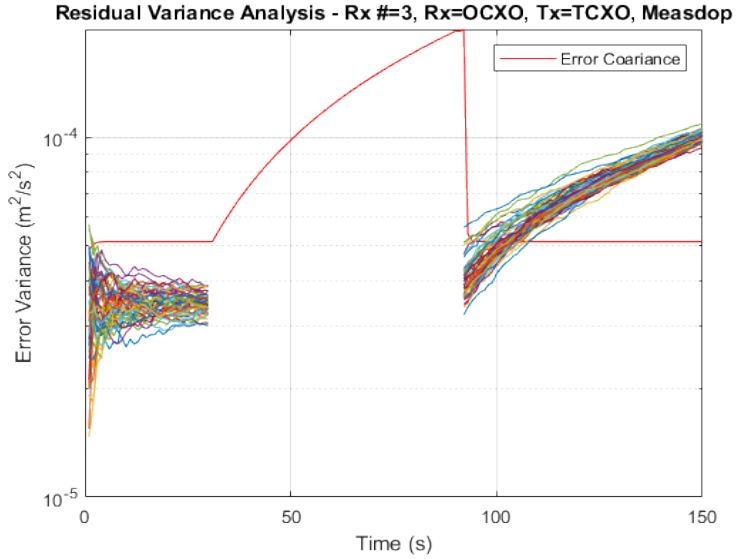
- Multiple receiver variance
  - Variance of all receiver residuals for same channel
  - Mean of all variances
  - Divide by the residual covariance
  - Fault if innovation is greater than arbitrary threshold value TS

$$\sigma^2_{\delta z_{k,rx}} = \frac{1}{k}\sum_{i=1}^{k} E_i\left[\left(\delta z_{i,rx} - \delta \bar{z}_{i,rx}\right)^2\right]$$

$$y_k = \frac{\sigma^2_{\delta z_{k,rx}}}{C_{\delta z_k}} > \mathrm{TS}$$

- Plot shows a moving mean of the variances for all 50 samples



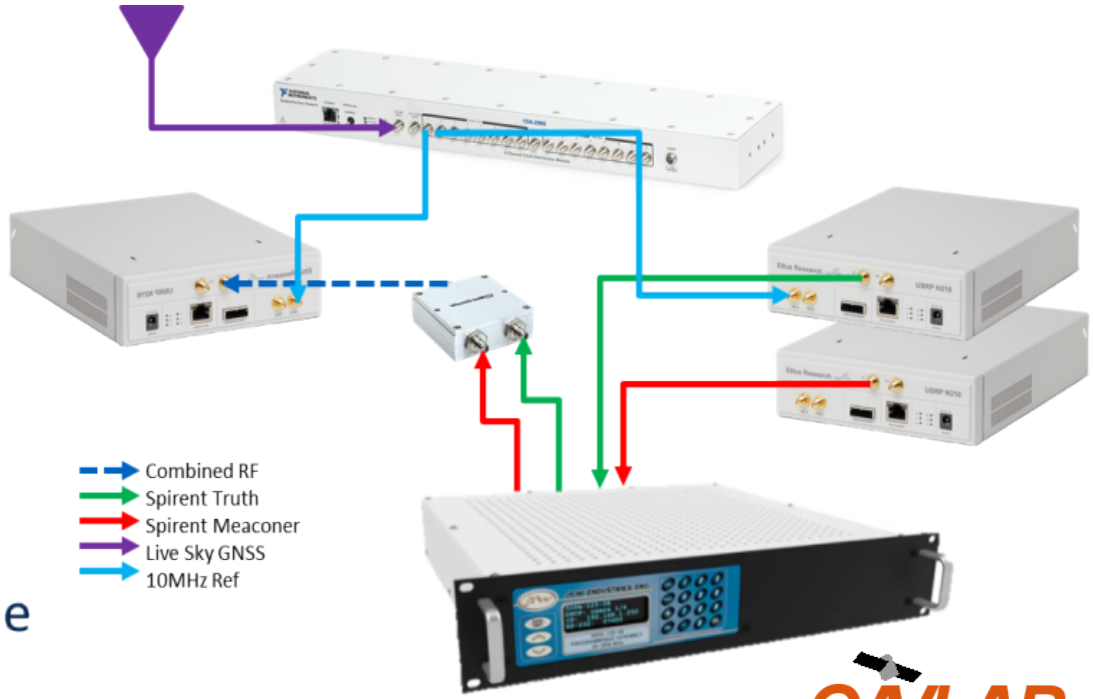
# Multiple Receiver Detection Results

- Full table of results at the end of the presentation
- Threshold value of 2 for all tests
- Notable results and trends:
  1. Higher frequency noise results in higher false alerts with a delta carrier phase measurement
  2. False alerts are minimal for the crystal oscillators that have lower frequency noise
  3. Doppler detection percentages are higher for all clock combinations with minimal false detections

| Multiple Receiver Variance with Spoofer, TS = 2 | | | | | |
|---|---|---|---|---|---|
| Meas. | Tx | Fault Detection % | | False Alert % | |
| Delta Carrier | Rx = 3 | OCXO | Rubidium | OCXO | Rubidium |
| | TCXO | 16 | 100 | 0 | 98 |
| | OCXO | 28 | 100 | 4 | 98 |
| | CSAC | 8 | 98 | 6 | 96 |
| | Rubidium | 14 | 100 | 2 | 98 |
| Doppler | Rx = 3 | OCXO | Rubidium | OCXO | Rubidium |
| | TCXO | 100 | 100 | 0 | 0 |
| | OCXO | 100 | 100 | 0 | 0 |
| | CSAC | 100 | 100 | 0 | 0 |
| | Rubidium | 100 | 100 | 2 | 0 |

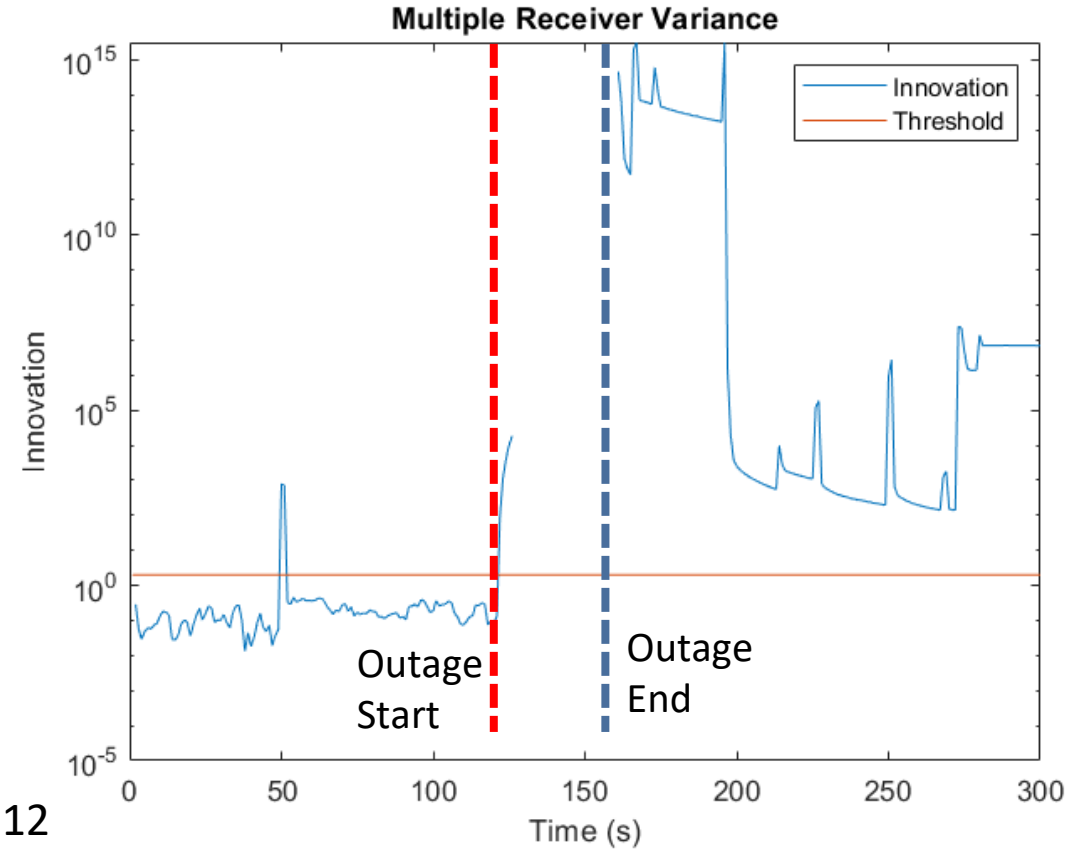
# Hardware Setup

- Spirent GSS9000 was used to generate true receiver signal data and meaconer location data
  - Both truth data and meaconer data was recorded using N210 USRPs – record start time the same for both ($t_{0,GPS} = t_{0,meac}$)
- Playback tests done with three N210s – one receiver, one meaconer transmitter, and one GPS truth transmitter
  - GPS truth and receiver sync'd to same clock
- Signals passed through attenuators to block unwanted signals at given times
  - Since both meaconer and truth were recorded at the same time, both USRPs were started at the same time during replay

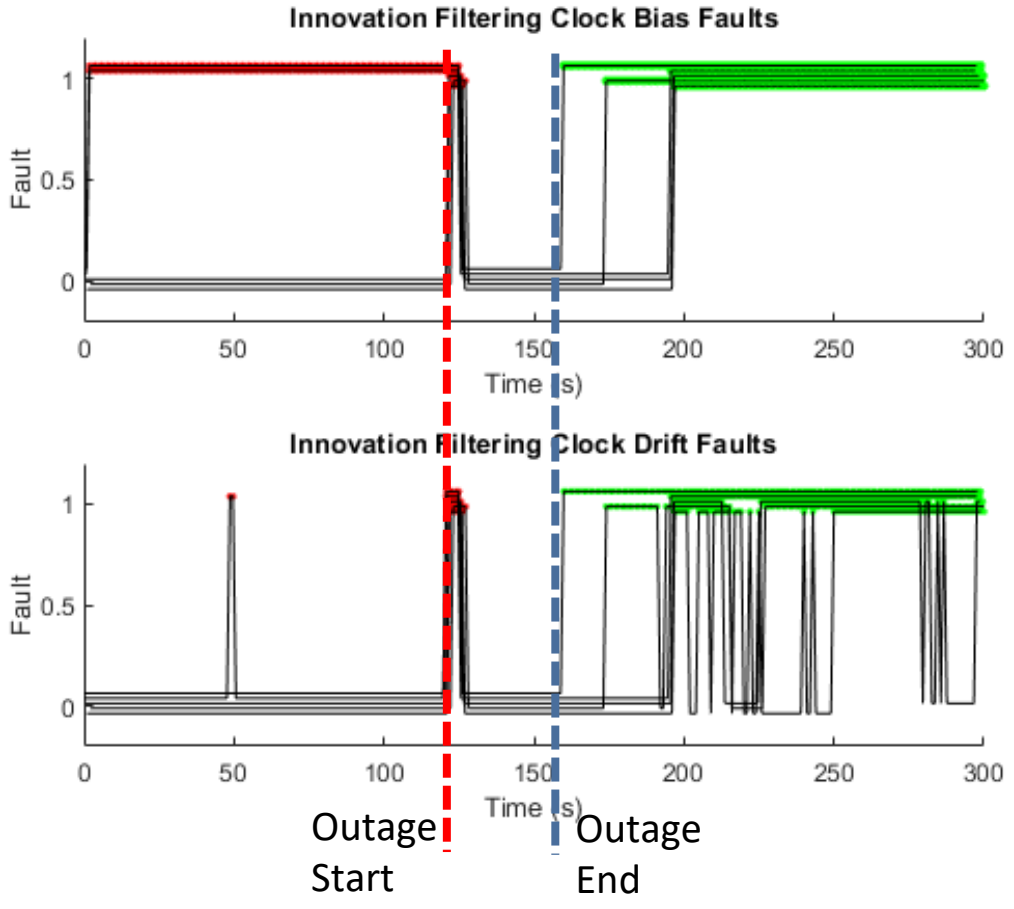


# Hardware Detection Results

- Multiple Receiver Variance results plotted as innovations over time
- Empirically selected threshold value of 2 based on simulation data

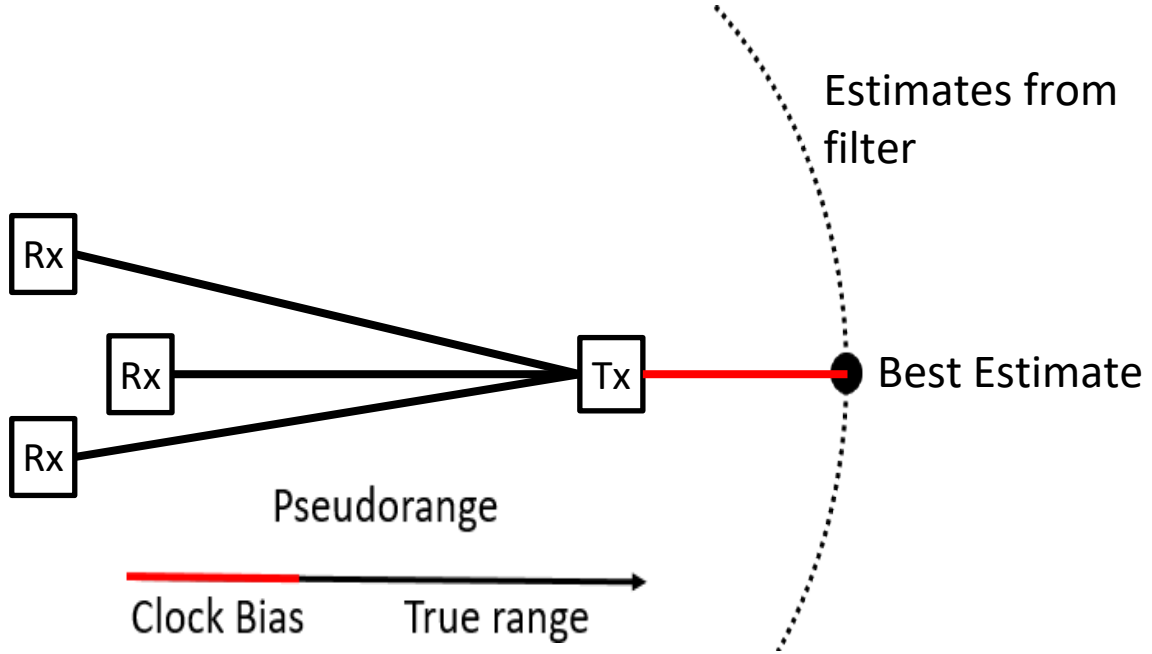



- Innovation filtering results plotted for clock bias and clock drift residuals
- Binary plot (1 is a fault, 0 is no fault)



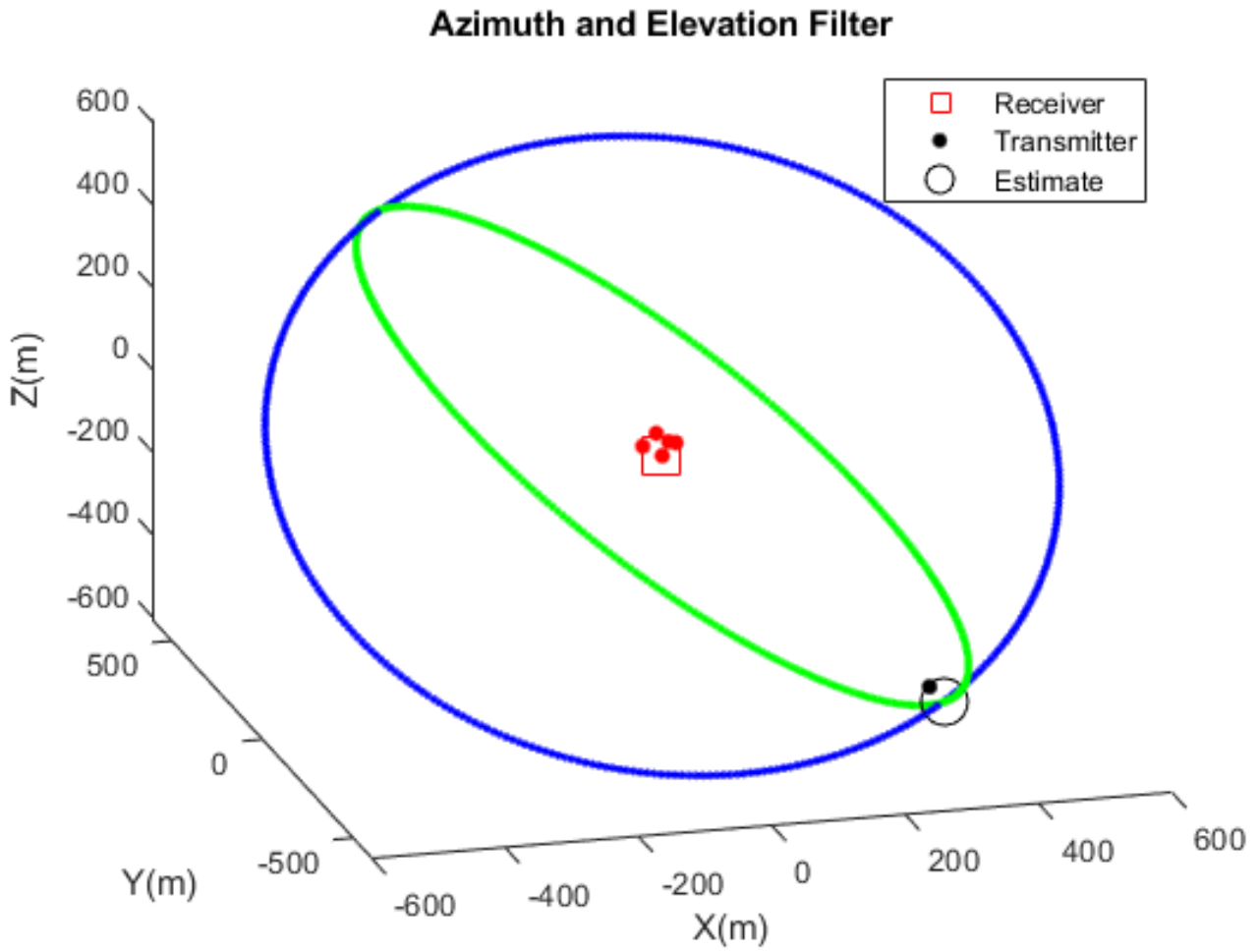
# Transmitter Localizer

- Two large sources of error
  - Inaccurate initial position estimate
  - Geometric dilution of precision (GDOP)
- Three step process
  - Range estimation using clock bias jump
  - Initial estimate filter
    - Azimuth and elevation estimate at the range distance from one receiver
  - Iterative least squares
    - Attempt to remove the transmitter clock bias
    - Address geometric uncertainty by using varying state vectors



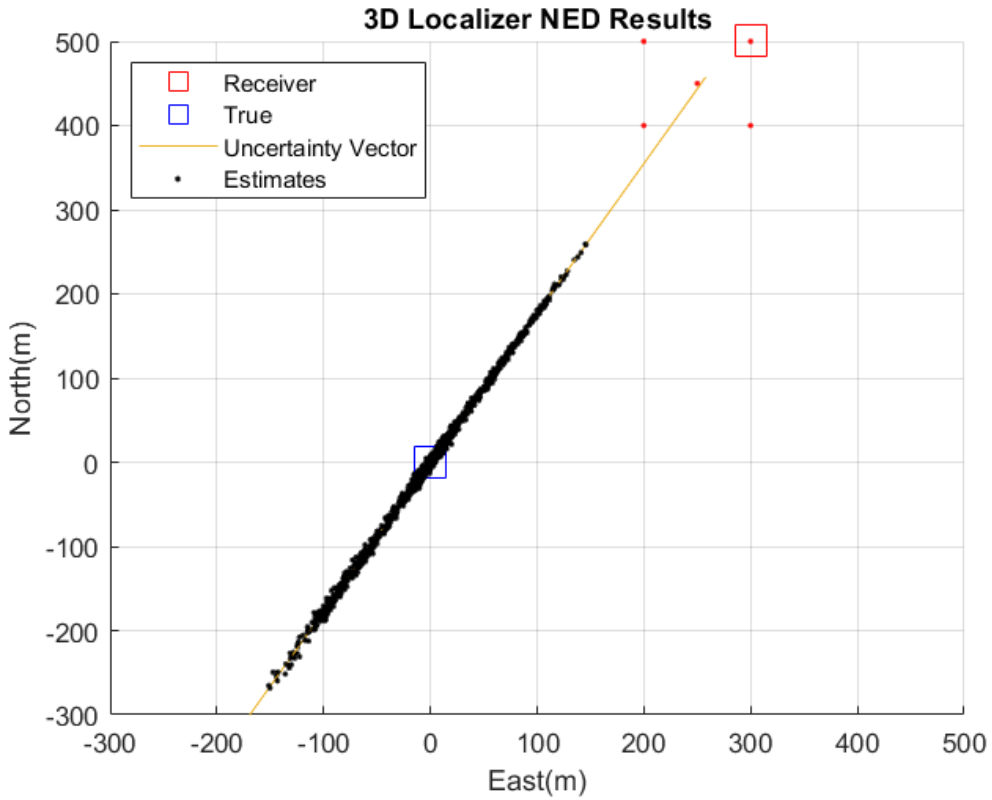
# Initial Estimate Filter

- Initial estimate for least squares
- Samples are at the range estimate distance from one of the receivers
- Deterministically sampled azimuth angles (blue)
- Best azimuth angle is evaluated at different elevation angles (green)

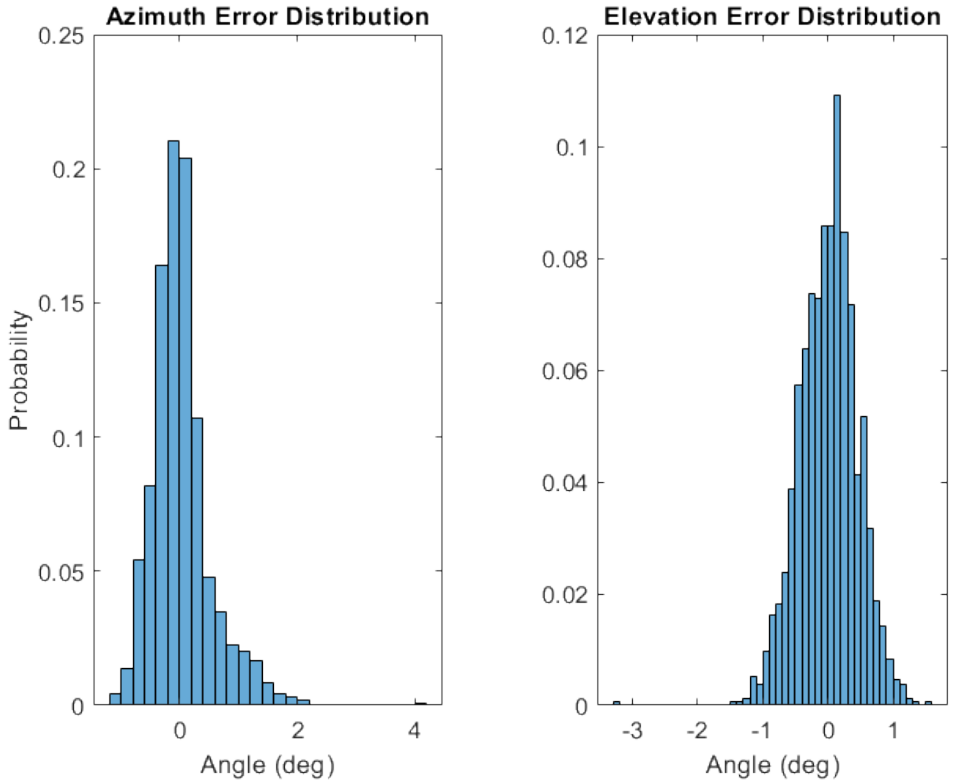


# Simulation Localizer Results – Static Scenario

- 3D Localizer $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$




- Directional error




| Tabulated Results | Rubidium (shown) | | OCXO | |
|---|---|---|---|---|
| | Azimuth | Elevation | Azimuth | Elevation |
| Mean | -0.0318 | 0.0100 | 0.1641 | -0.0482 |
| Std. Dev. | 0.5012 | 0.4441 | 1.5370 | 2.3623 |

# Geometric Uncertainty Improvements

- For certain geometries, the range bias error and position errors scale proportionately in a certain direction
- Results in a vector with all points along vector equally likely to the least squares estimator
  - Each iteration slides along vector and never meets criteria to end the iteration

- Different localizer states to improve Dilution of Precision (DOP)
- 2D localizer
  - Remove altitude uncertainty
- No bias estimate
  - Removes range uncertainty

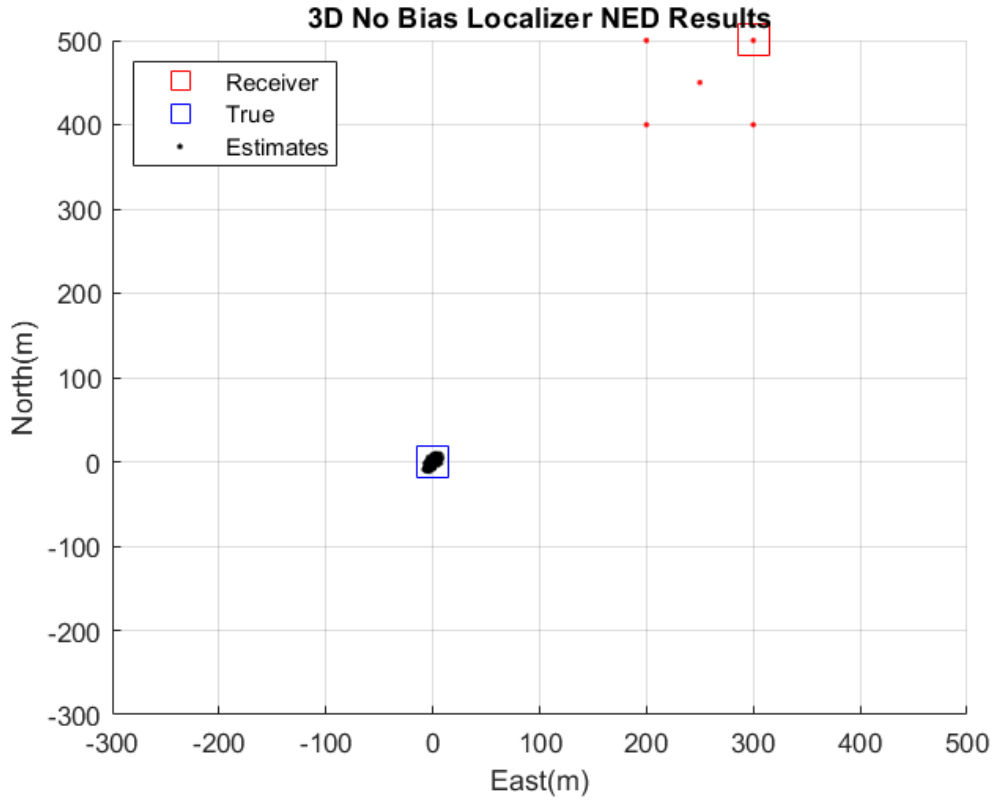
$$H = (G^T G)^{-1} = \begin{bmatrix} \sigma_x^2 & \sigma_{xy}^2 & \sigma_{xz}^2 & \boldsymbol{\sigma_{xb}^2} \\ \sigma_{xy}^2 & \sigma_y^2 & \sigma_{yz}^2 & \boldsymbol{\sigma_{yb}^2} \\ \sigma_{xz}^2 & \sigma_{yz}^2 & \sigma_z^2 & \boldsymbol{\sigma_{zb}^2} \\ \boldsymbol{\sigma_{xb}^2} & \boldsymbol{\sigma_{yb}^2} & \boldsymbol{\sigma_{zb}^2} & \sigma_b^2 \end{bmatrix}$$

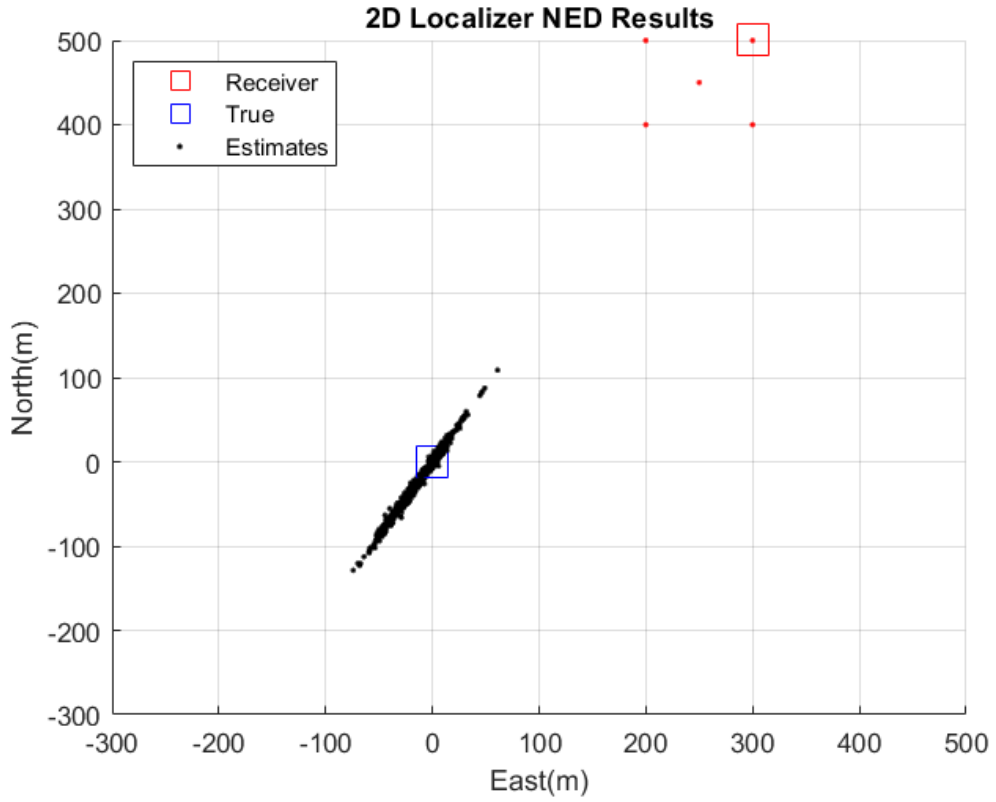
$$uv = \frac{1}{\|\sigma_{xb}^2 + \sigma_{yb}^2 + \sigma_{zb}^2\|} \left[\sigma_{xb}^2, \quad \sigma_{yb}^2, \quad \sigma_{zb}^2\right]^T$$

# Simulation Localizer Results – Other Localizers

- No bias estimate $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$
- Better accuracy than original
- Vulnerable to biased ranges

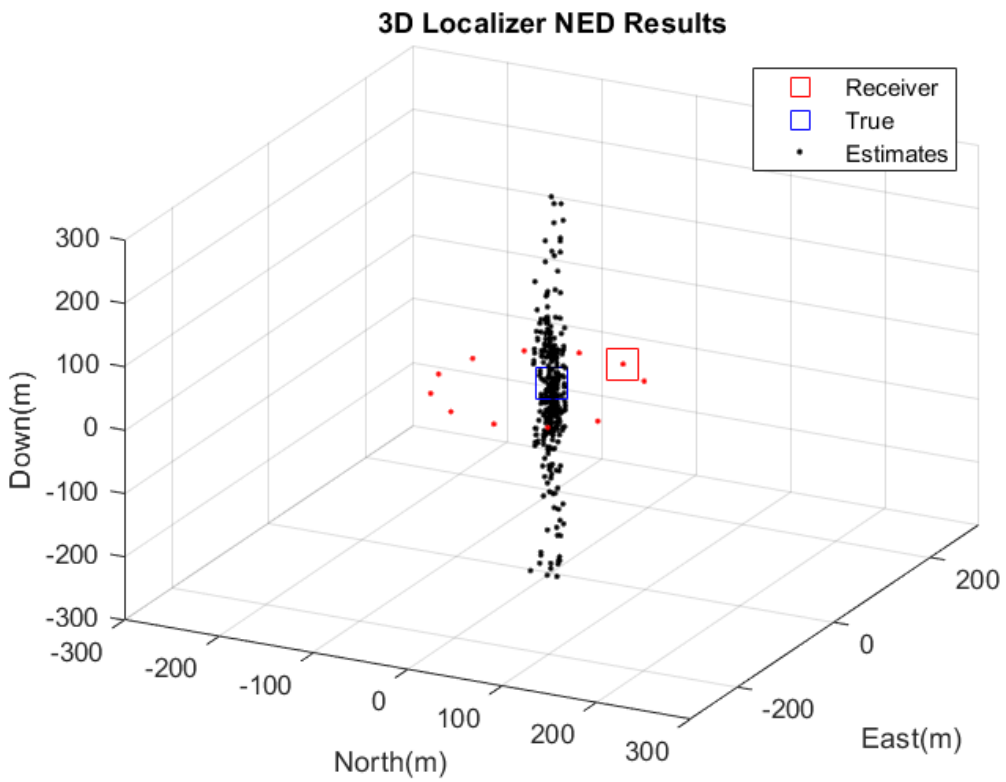
- 2D Localizer $\begin{bmatrix} N \\ E \\ b \end{bmatrix}$
- Slightly more accurate than original



# Simulation Localizer Results – Dynamic Scenario

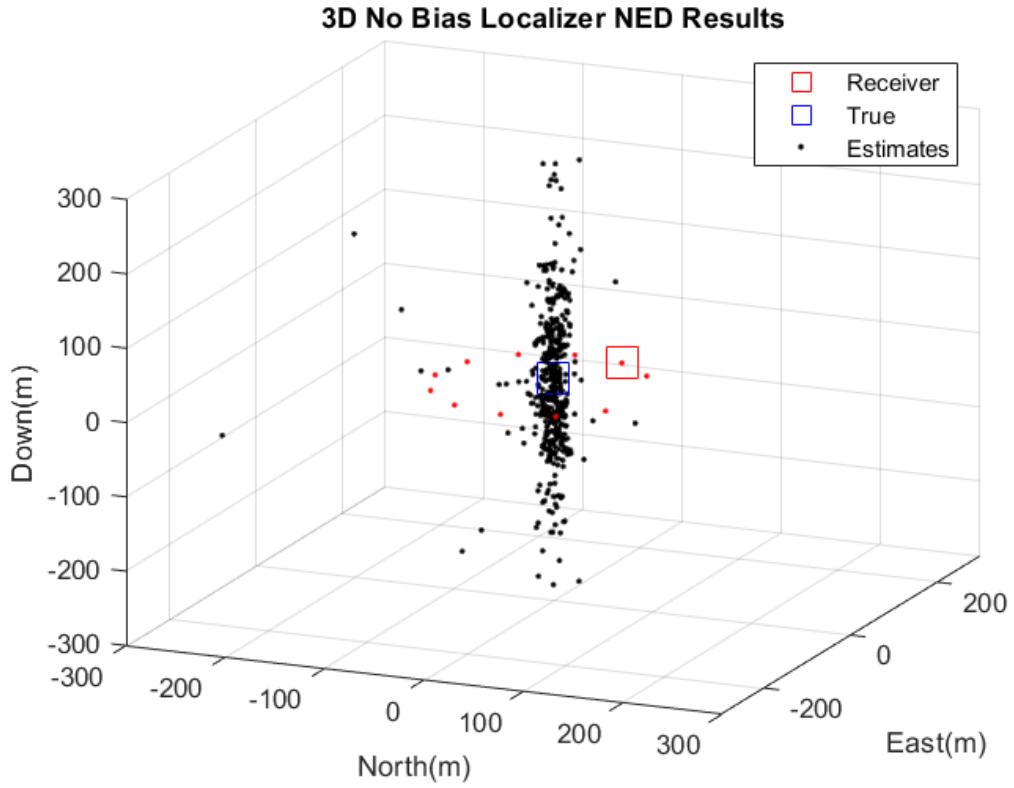
- 3D Localizer



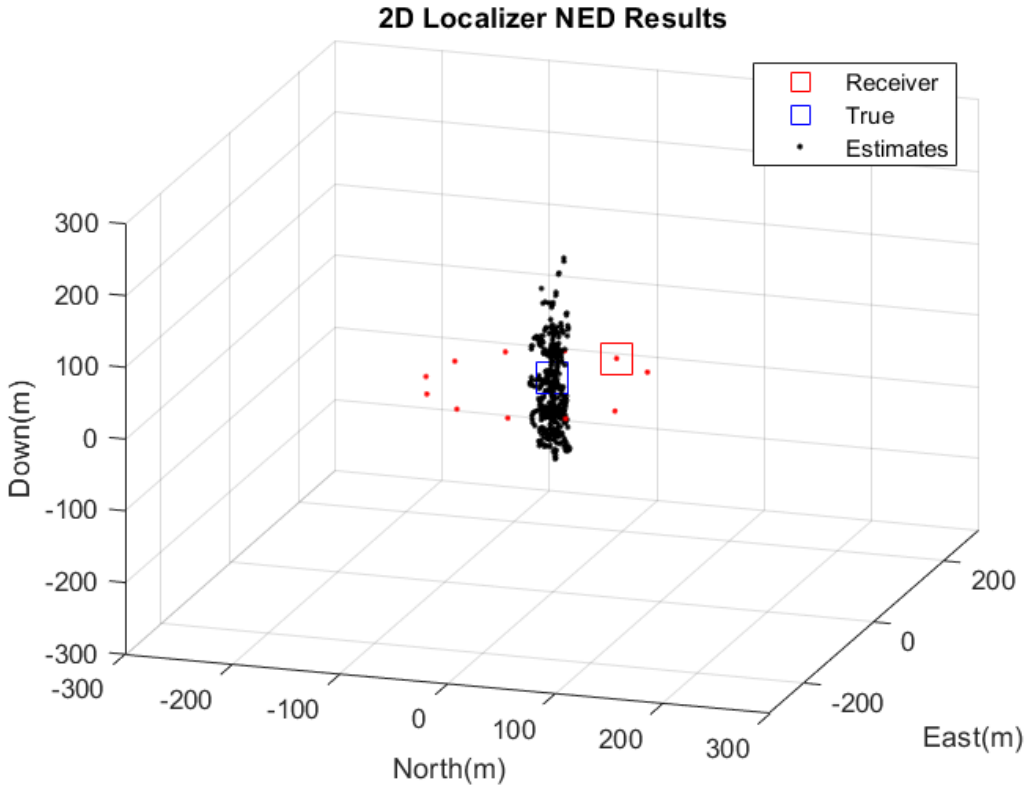

- Uncertainty vector isolated to altitude rather than distance
  - Orthogonal to the plane of receivers
- Converged to a solution with 25% of range measurements

# Simulation Localizer Results – Other Localizers

- No bias estimate $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$
- Converged to an estimate with 100% of estimates




- 2D Localizer $\begin{bmatrix} N \\ E \\ b \end{bmatrix}$
- Altitude error is due to propagation of a biased pitch measurement



# Summary

- Simulations show high detection rates with low false alerts for certain detection methods
- Hardware validation shows it is possible to use the same detection techniques and detect an inauthentic signal
- Localizer algorithm can accurately estimate the transmitters direction
- Localizer accuracy is scenario dependent and a combination of multiple methods may help overcome geometric issues

# References


1. Fernández, Enric et al. “CSAC Characterization and Its Impact on GNSS Clock Augmentation Performance.” *Sensors (Basel, Switzerland)* vol. 17,2 370. 14 Feb. 2017, doi:10.3390/s17020370.
2. Brown, Robert, and Hwang, Patrick. *Introduction to Random Signals and Applied Kalman Filtering.* John Wiley and Sons Inc., Hoboken, NJ, 2012.
3. Groves, Paul D. *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*. Second ed., Artech House, 2013.

# Questions?

Thank You!