SAND2022-7660C

Sandia National Laboratories

(U) A Novel Motion Correlator for GNSS Spoofer Survivability

Tucker Haydon, Connor Brashar

2022 ION Joint Navigation Conference

Distribution Statement A
Approved for public release: distribution unlimited

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

Patent Pending

U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration

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.

TODO

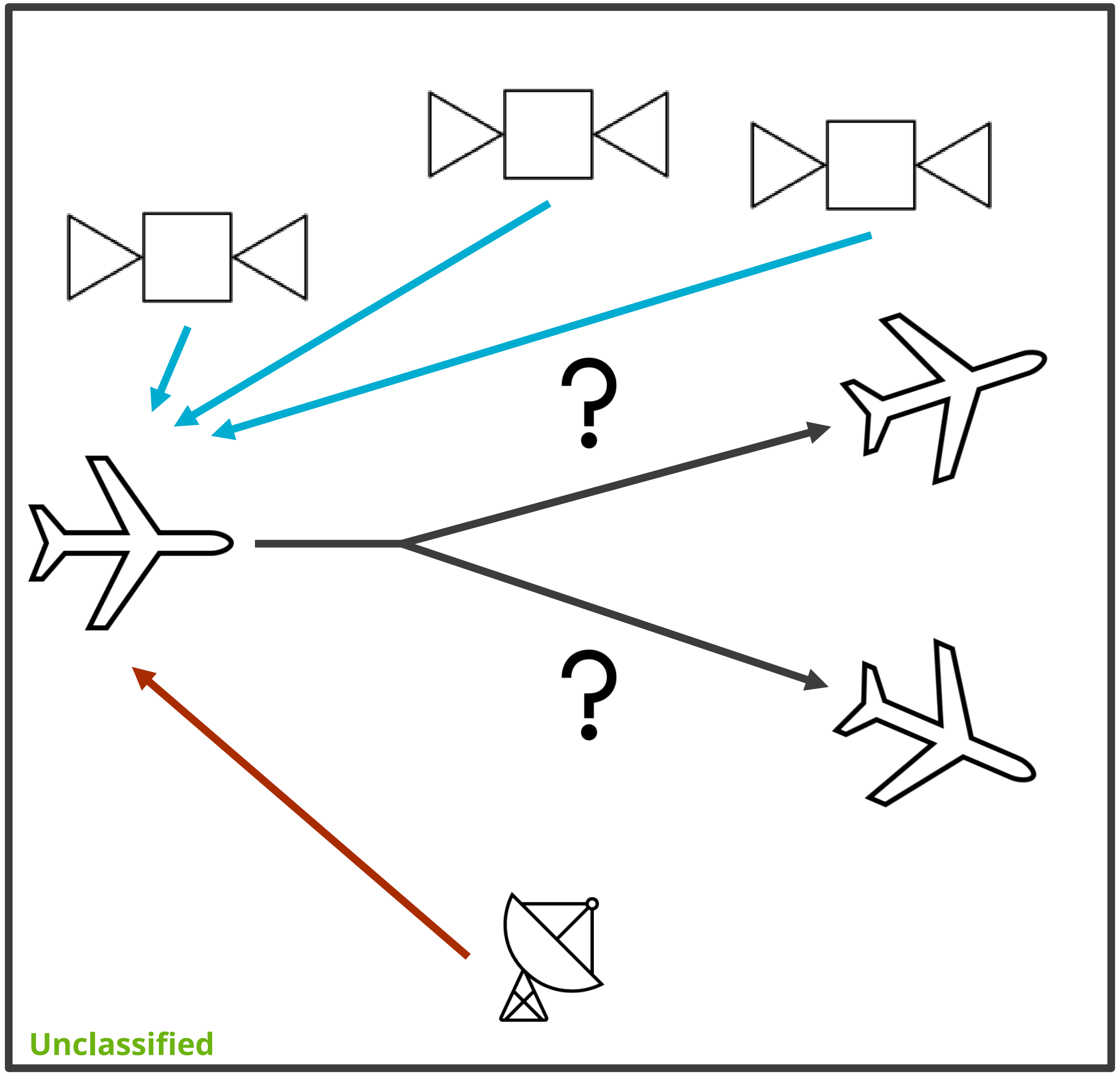
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

(U) Goals

1. (U) Survive a GNSS spoofing attack.

2. (U) Only use:
   (1) (U) A single GNSS antenna element.
   (2) (U) An inertial measurement unit.
   (3) (U) A local clock.

3. (U) Determine the angle-of-arrival of the spoofed GNSS signals.



(U) High-Level Strategy

(U) Constellation Binner

1. (U) Acquire and track several candidate correlation peaks within the correlator’s time-frequency search space.
2. (U) Evaluate all possible combinations of pseudorange measurements and create a set of candidate GNSS least-squares solutions.
3. (U) Employ a hypothesis test to determine the two least-squares solutions that are *consistent*.

(U) Produces two consistent measurement sets whose credibility is uncertain.

(U) Jitter Detection

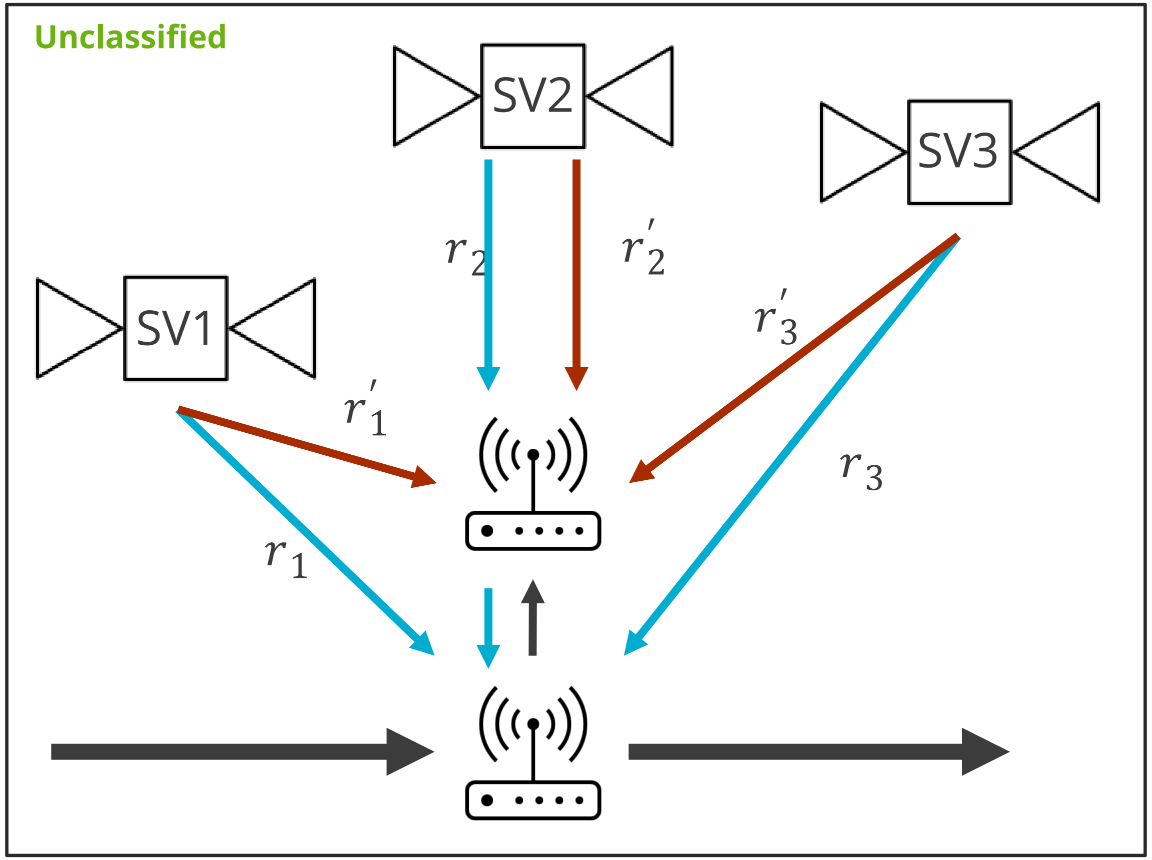
1. (U) Create a model for both the true and spoofed GNSS signals.
2. (U) Jointly estimate all the model parameters (including the angle-of-arrival).
3. (U) Employ a Kalman filter innovations hypothesis test to assign each of the two measurement sets to either the true or spoofed models.

(U) Determines which of the two consistent measurement sets is valid.

(U) Key Observation

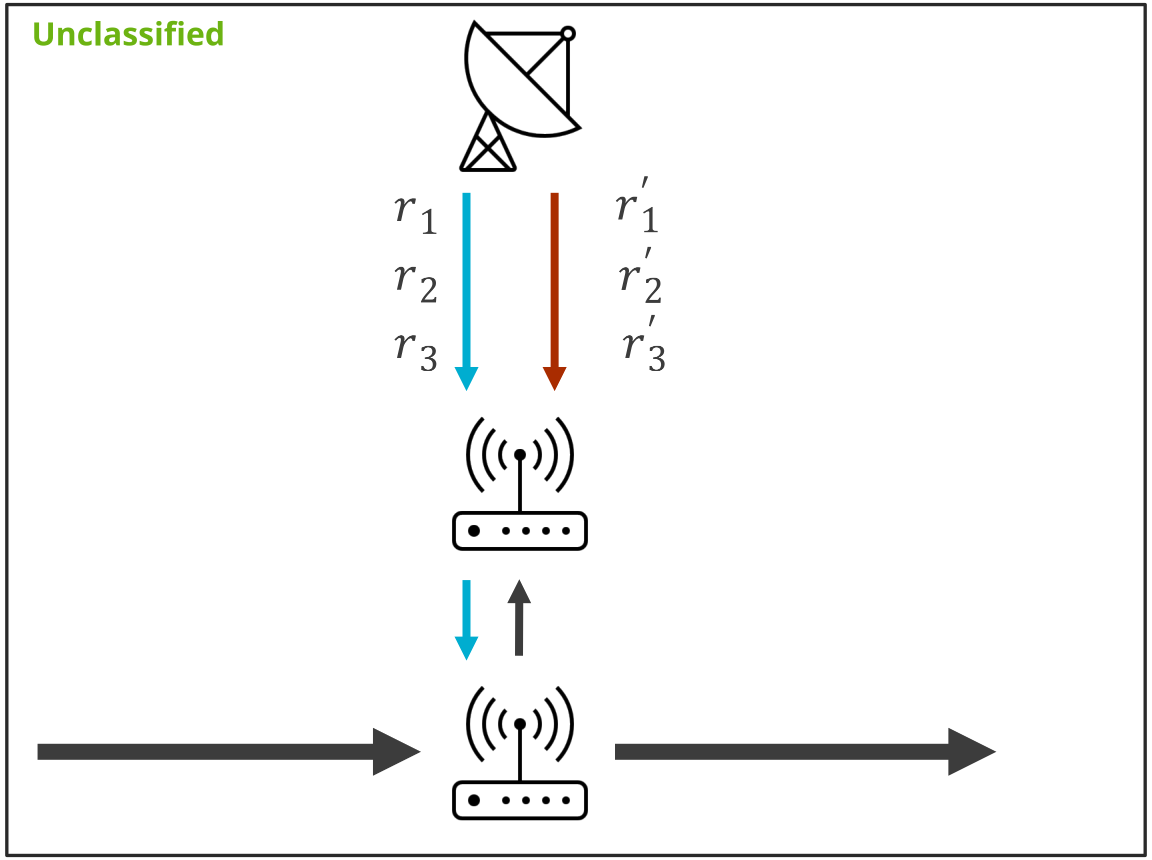
(U) Measurements from Satellite Vehicles

(U) An impulse in the receiver's position creates a different response in each pseudorange measurement channel.



(U) Measurements from Theoretical Spoofer

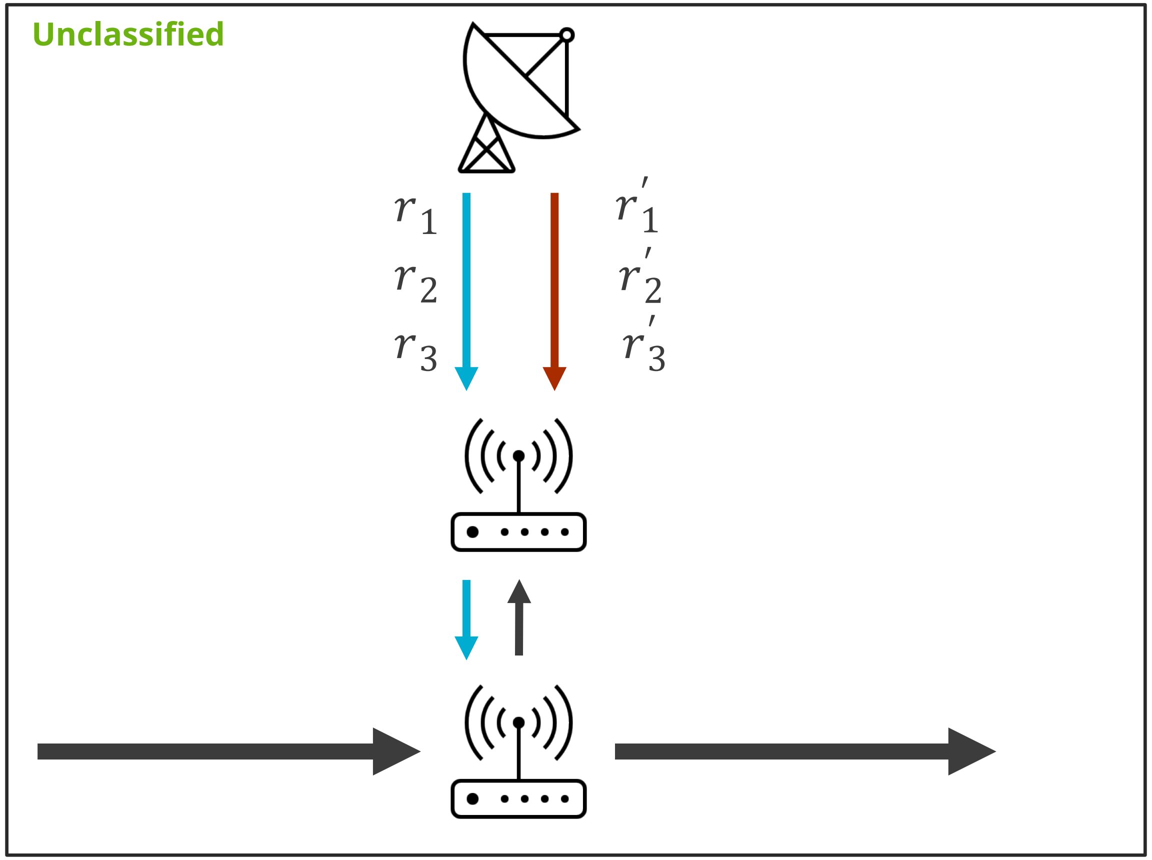
(U) An impulse in the receiver's position creates the same response in each pseudorange measurement channel.



(U) Key Assumption

(U) In our theoretical spoofer model, we *assume* that the spoofer cannot compensate for high-frequency, low -amplitude receiver motion.

(U) We term this motion *Jitter*.



(U) Measurement Models

Nominal Pseudorange Measurement Model

$$\mathbf{z}^{(i)} = \left\|\mathbf{p} - \mathbf{p}_{sv}^{(i)}\right\| + c \cdot \delta t + \boldsymbol{\epsilon}^{(i)}$$

Where

$\mathbf{z}^{(i)}$ is the pseudorange measurement to the ith satellite.

$\mathbf{p}$ is the true position of the receiver.

$\mathbf{p}_{sv}^{(i)}$ is the position of the ith satellite.

c is the speed of light.

δt is the receiver's clock bias.

$\boldsymbol{\epsilon}^{(i)}$ is independent gaussian noise on the measurement.

Unclassified

Theoretical Spoofed Pseudorange Measurement Model

$$\tilde{\mathbf{z}}^{(i)} = \left\|\tilde{\mathbf{p}} - \mathbf{p}_{sv}^{(i)}\right\| + c \cdot \delta\tilde{t} - \hat{\mathbf{r}}^{T}\delta\tilde{\mathbf{p}} + \tilde{\boldsymbol{\epsilon}}^{(i)}$$

Where

$\tilde{\mathbf{z}}^{(i)}$ is the ith spoofed pseudorange measurement.

$\tilde{\mathbf{p}}$ is the spoofed position of the receiver.

$\mathbf{p}_{sv}^{(i)}$ is the position of the ith satellite.

c is the speed of light.

$\delta\tilde{t}$ is the combined receiver-spoofer clock bias.

$\delta\tilde{\mathbf{p}}$ is the receiver's jitter motion.

$\hat{\mathbf{r}}$ is the unit vector from the receiver to the spoofer.

$\tilde{\boldsymbol{\epsilon}}^{(i)}$ is independent gaussian noise on the measurement.

Unclassified

(U) Motion Models

(U) Nominal Motion

(U) Let an accelerometer measure a biased and noisy version of the receiver's acceleration:

(U) $$\boldsymbol{a_m} = \boldsymbol{\ddot{p}} + \boldsymbol{b} + \boldsymbol{\epsilon_a}$$

(U) where

(U) $\boldsymbol{a_m}$ is accelerometer measurement.

(U) $\boldsymbol{\ddot{p}}$ is the true acceleration of the receiver.

(U) $\boldsymbol{b}$ is the accelerometer's constant bias.

(U) $\boldsymbol{\epsilon_a}$ is Gaussian white noise.

(U) The accelerometer bias is assumed constant, although it could be modeled as time-varying without loss of generality.

(U) Jitter Motion

(U) *Jitter* is defined as the high-pass component of the receiver's position. Model this motion with a linear high-pass filter on the receiver's true position states:

(U) $$\frac{d}{dt}(\boldsymbol{\alpha}) = \boldsymbol{A\alpha} + \boldsymbol{Bp}$$

(U) $$\boldsymbol{\delta\tilde{p}} = \boldsymbol{C\alpha} + \boldsymbol{Dp}$$

(U) where

(U) $\boldsymbol{p}$ is the receiver's true position.

(U) $\boldsymbol{\delta\tilde{p}}$ is the receiver's jitter motion.

(U) $\boldsymbol{\alpha}$ is the high-pass model parameter.

(U) $\boldsymbol{A, B, C, D}$ are the high-pass system matrices.

(U) In the following simulation, a second-order high-pass Butterworth filter is applied.

(U) Motion Models

(U) Nominal States

(U) The nominal states are driven by the accelerometer measurement and a two-state clock model.

(U) $\frac{d}{dt}(\boldsymbol{p}) = \dot{\boldsymbol{p}}$

(U) $\frac{d}{dt}(\dot{\boldsymbol{p}}) = \boldsymbol{a}_{\boldsymbol{m}} - \boldsymbol{b} + \boldsymbol{\epsilon}_{\boldsymbol{a}}$

(U) $\frac{d}{dt}(\delta t) = \delta\dot{t} + \epsilon_{\delta t}$

(U) $\frac{d}{dt}(\delta\dot{t}) = \epsilon_{\delta\dot{t}}$

(U) $\frac{d}{dt}(\boldsymbol{b}) = \boldsymbol{\epsilon}_{\boldsymbol{b}}$

(U) Jitter States

(U) The jitter states are driven by a constant-velocity spoofed position motion model, a high-pass filter model for the jitter motion, and a two-state clock model.

(U) $\frac{d}{dt}(\tilde{\boldsymbol{p}}) = \dot{\boldsymbol{p}}$

(U) $\frac{d}{dt}(\dot{\tilde{\boldsymbol{p}}}) = \boldsymbol{\epsilon}_{\dot{\tilde{\boldsymbol{p}}}}$

(U) $\frac{d}{dt}(\delta\tilde{t}) = \delta\dot{\tilde{t}} + \epsilon_{\delta\tilde{t}}$

(U) $\frac{d}{dt}(\delta\dot{\tilde{t}}) = \epsilon_{\delta\dot{\tilde{t}}}$

(U) $\frac{d}{dt}(\hat{\boldsymbol{r}}) = \boldsymbol{0}$

(U) $\frac{d}{dt}(\boldsymbol{\alpha}) = \boldsymbol{A}\boldsymbol{\alpha} + \boldsymbol{B}\boldsymbol{p}$

(U) Kalman Filter States

- (U) Jointly estimate the nominal and jitter states in a single Kalman filter and take advantage of *both* sets of pseudorange measurements.

- (U) The current problem is that we do not know which set of pseudorange measurements is true and which is produced by the theoretical spoofer – i.e. what states to assign the measurements to.

(U) Standard GNSS Kalman Filter States

(U) $$\boldsymbol{x} = \begin{bmatrix} \boldsymbol{p} \\ \dot{\boldsymbol{p}} \\ \delta t \\ \delta \dot{t} \\ \boldsymbol{b} \\ - \\ \tilde{\boldsymbol{p}} \\ \dot{\tilde{\boldsymbol{p}}} \\ \delta \tilde{t} \\ \delta \dot{\tilde{t}} \\ \boldsymbol{\alpha} \\ \hat{\boldsymbol{r}} \end{bmatrix} = \begin{bmatrix} \text{True Receiver's Position} \\ \text{True Receiver's Velocity} \\ \text{Receiver Clock Bias} \\ \text{Receiver Clock Drift} \\ \text{Accelerometer Bias} \\ --------------- \\ \text{Spoofed Receiver's Position} \\ \text{Spoofed Receiver's Velocity} \\ \text{Spoofer Clock Bias} \\ \text{Spoofer Clock Drift} \\ \text{High-Pass Filter Parameters} \\ \text{Angle-of-Arrival} \end{bmatrix}$$

(U) New Jitter Kalman Filter States

(U) Hypothesis Test

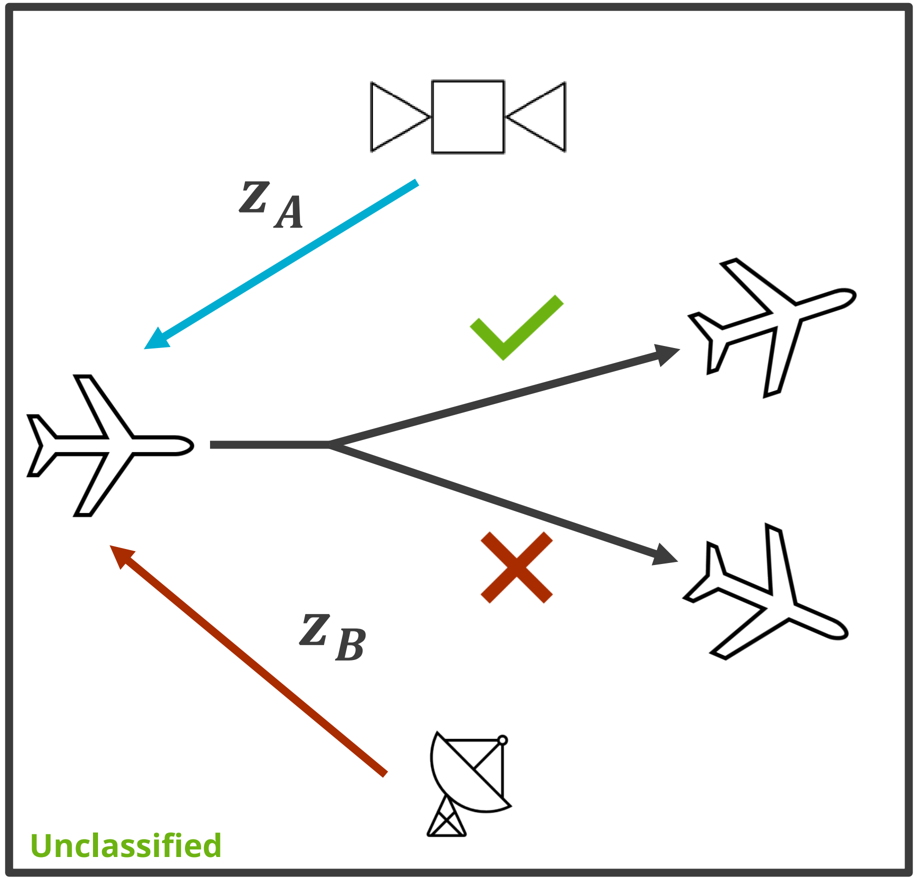
- (U) A set of two Kalman filters is initialized with the two competing hypotheses.
- (U) Each Kalman filter is run in parallel and their measurement innovations are accumulated over a finite horizon.
- (U) After a configured finite horizon, the accumulated measurement innovations are compared against a chi-squared distribution to determine which Kalman filter is operating on the true hypothesis.

- (U) Let $\boldsymbol{z_A}$ and $\boldsymbol{z_B}$ be the two sets of consistent pseudorange measurements produced by the Constellation Binner.
- (U) Under the null hypothesis H_0, assume that $\boldsymbol{z_A}$ are the true pseudorange measurements and $\boldsymbol{z_B}$ are the spoofed pseudorange measurements.
- (U) Under the alternate hypothesis H_A, assume that $\boldsymbol{z_A}$ are the spoofed pseudorange measurements and $\boldsymbol{z_B}$ are the true pseudorange measurements.

(U) Hypothesis Test

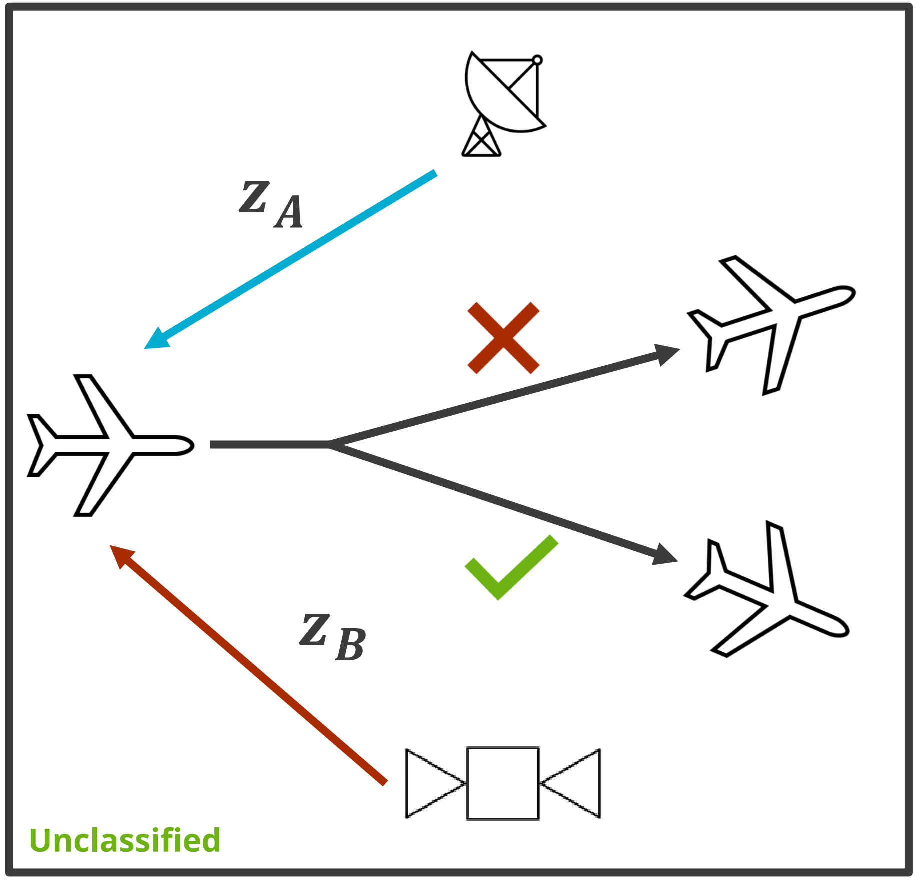
(U) Null Hypothesis

(U) Assume that $\boldsymbol{z_A}$ is from the satellite vehicles and $\boldsymbol{z_B}$ is from the theoretical spoofer.



(U) Alternate Hypothesis

(U) Assume that $\boldsymbol{z_A}$ is from the theoretical spoofer and $\boldsymbol{z_B}$ is from the satellite vehicles.



(U) Simulation

- (U) A receiver was simulated in an inertial 3D space with nine “satellite vehicles” uniformly distributed above it.

- (U) The receiver oscillates with a high frequency and low amplitude around the origin – the *jitter*. This jitter motion is assumed to be undetected and uncompensated by the theoretical spoofer.

- (U) A Cubature Kalman Filter jointly estimates the nominal and jitter states.

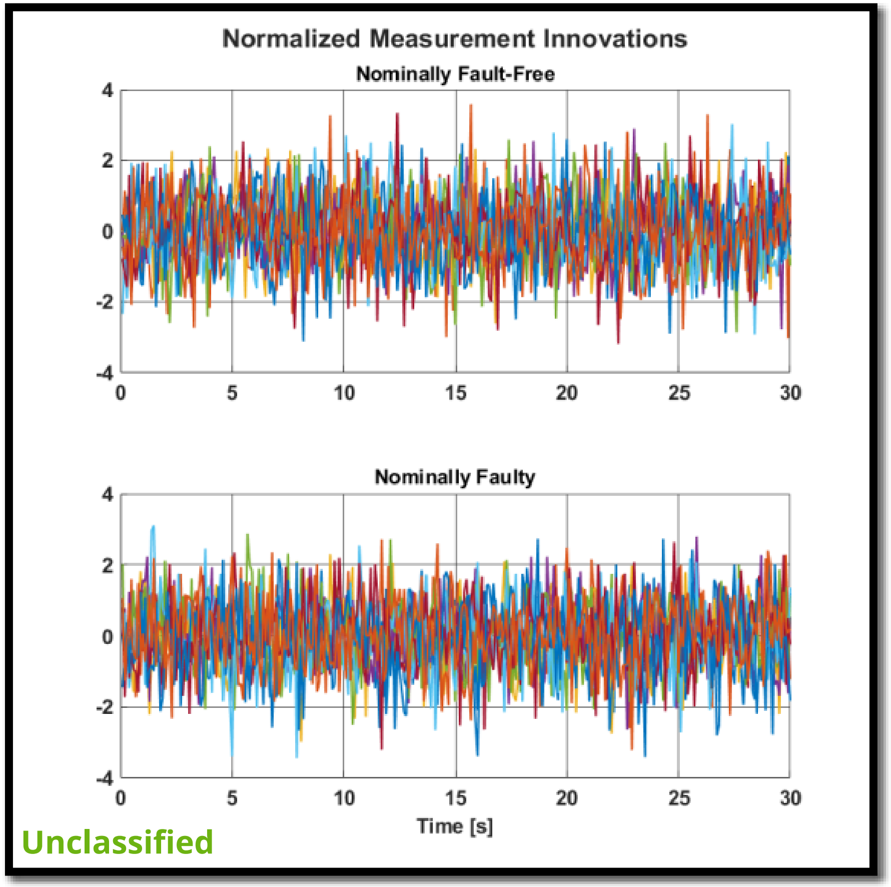
Parameter	Value
Accelerometer Quality	Navigation Grade
Receiver Clock Quality	OCXO
Spoofer Clock Quality	OCXO
Jitter Frequency	3 Hz
Pseudorange Measurement Noise	2 cm (assuming carrier-phase-like measurements)
Innovation Accumulation Horizon	5 - 15 s

Unclassified

(U) Extreme Motion – 10 cm Oscillation

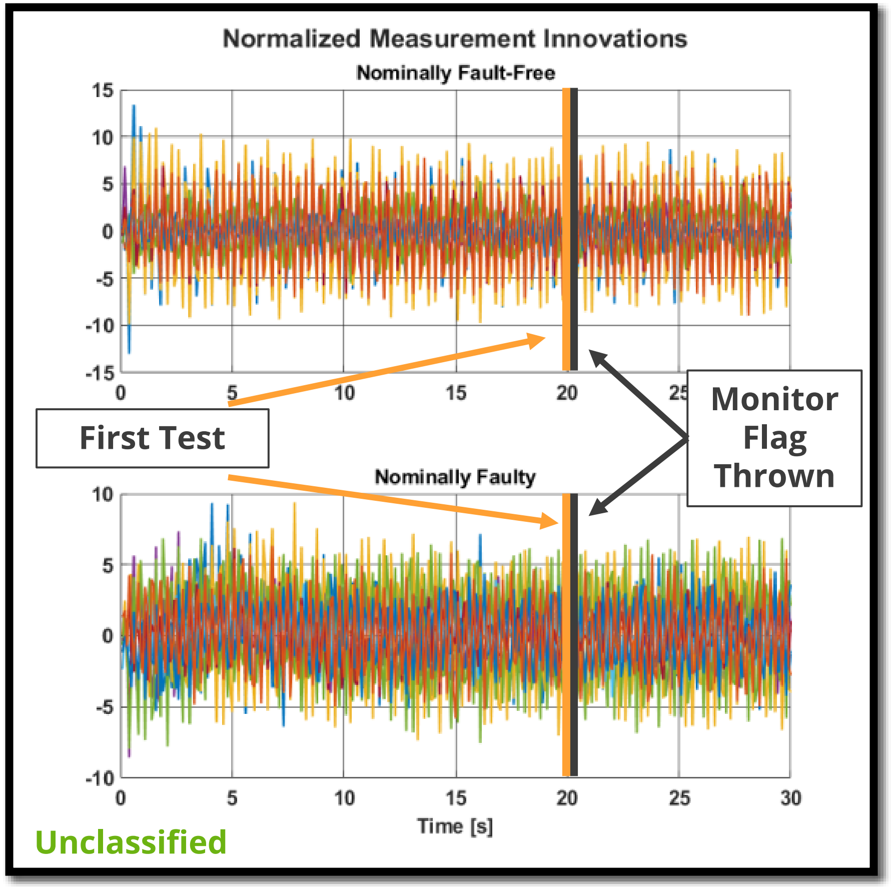
(U) Correct Hypothesis

- (U) The measurement innovations are approximately distributed like a unit Gaussian distribution.
- (U) No innovation monitor flags are thrown.



(U) Incorrect Hypothesis

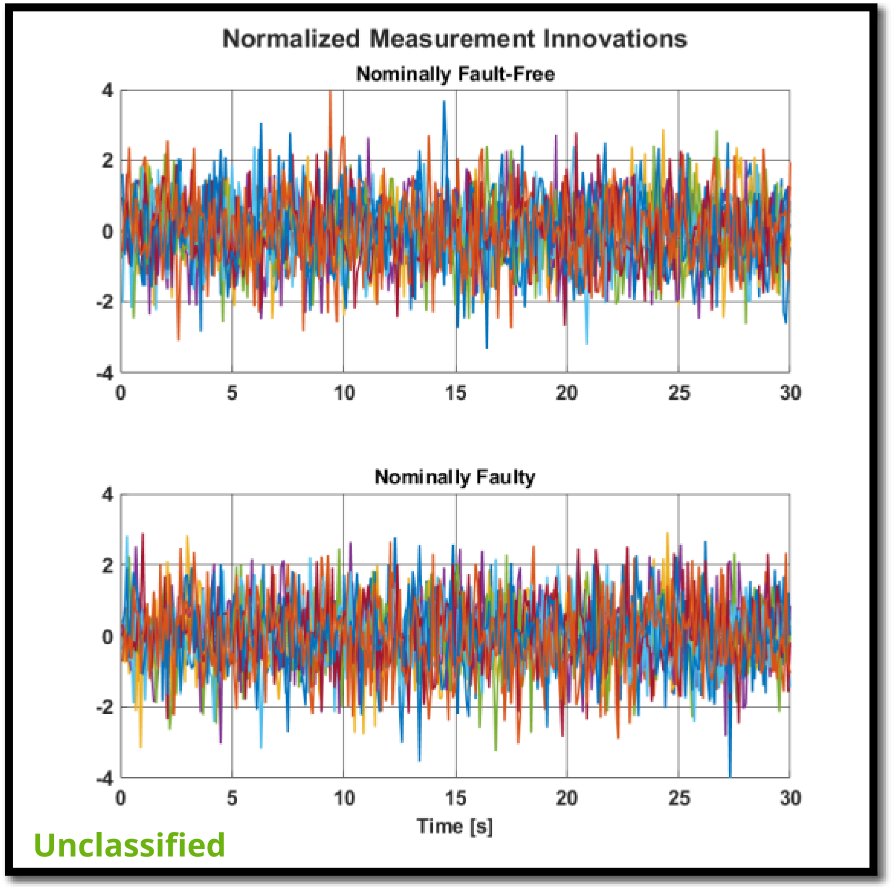
- (U) The measurement innovations are clearly not distributed like a unit Gaussian distribution.
- (U) An innovation monitor flag is immediately thrown.



(U) "Jitter" Motion – 1 cm Oscillation

(U) Correct Hypothesis

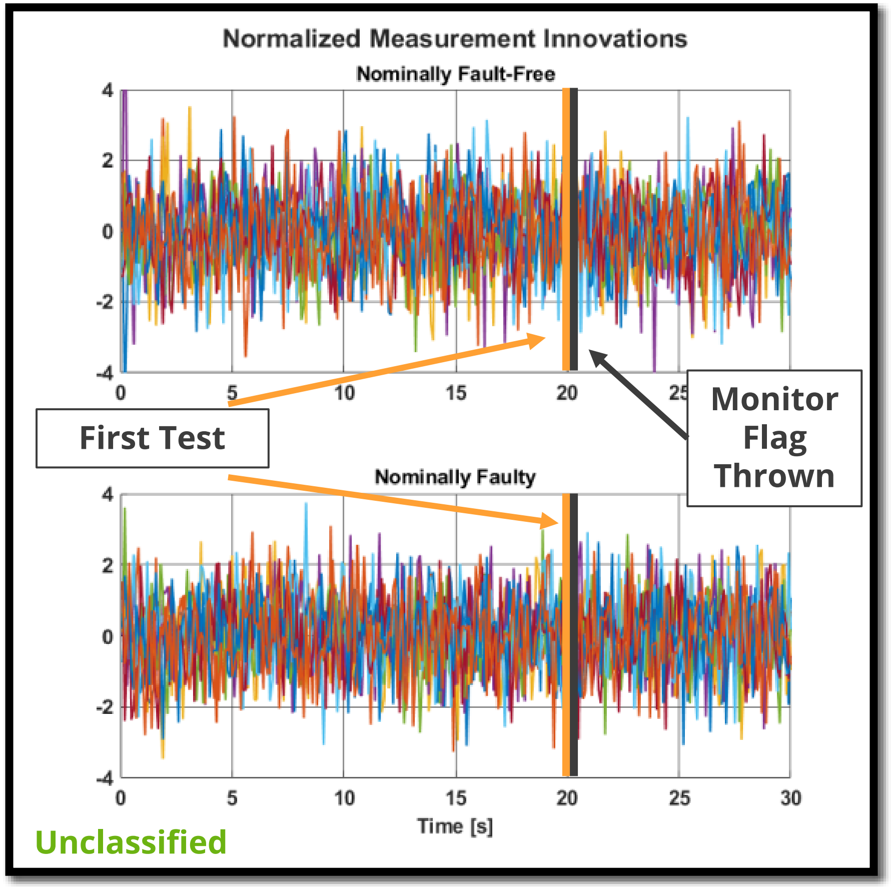
- (U) The measurement innovations are approximately distributed like a unit Gaussian distribution.
- (U) No innovation monitor flags are thrown.



Unclassified

(U) Incorrect Hypothesis

- (U) The measurement innovations are slightly correlated and <u>not</u> distributed like a unit Gaussian.
- (U) An innovation monitor flag is immediately thrown.



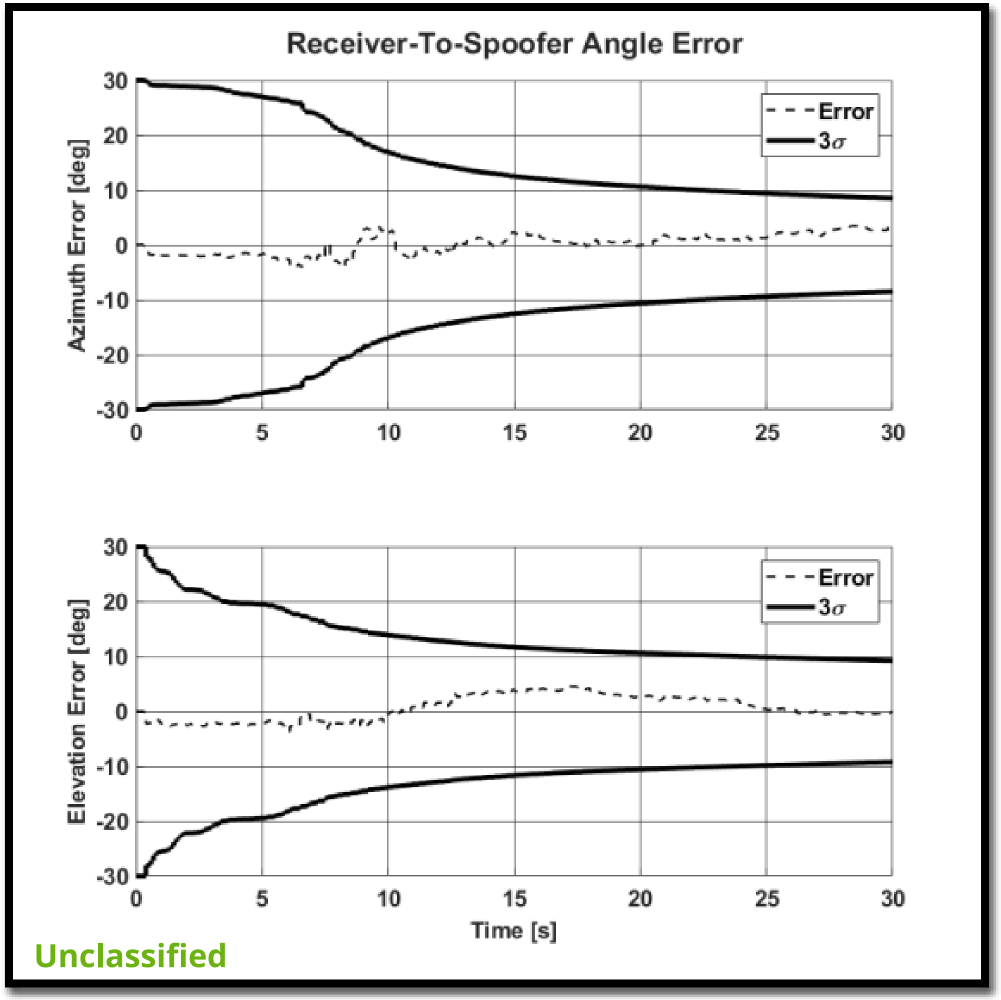
First Test

Monitor Flag Thrown

Unclassified

(U) Angle-Of-Arrival Estimation

- (U) With the “jitter” simulation and under the correct hypothesis, the angle-of-arrival was indeed observable.
- (U) The 3σ covariance bounds degreased from [30, 30] degrees in azimuth and elevation to ~ [10, 10] degrees.
- (U) Further simulations have indicated that the angle-of-arrival estimate can be improved with larger “jitter”.



Unclassified

(U) Caveats & Conclusions

- (U) Purely an academic exercise.
  - (U) Severely limited our available resources.
    - (U) Use only one antenna element, a clock, and an accelerometer.
  - (U) Tried to estimate the angle-of-arrival.
- (U) Many, many assumptions.
  - (U) Spoofed trajectory is constant-velocity.
  - (U) Theoretical spoofer cannot compensate for vehicle motion beyond a fixed frequency.
  - (U) Carrier-phase-like quality pseudorange measurements.
  - (U) No other sources of error (atmosphere).
- (U) These caveats aside, we believe that the Constellation Binner + Jitter Detection framework opens several new doors and possible paths for anti-spoofing algorithms.

Thank You!
Tucker Haydon
tchaydo@sandia.gov

(U) References

(U) 1. Givhan, Anderson, Brashar, Connor, Walker, Mike, Haydon, Tucker, and Esterly, Elizabeth. " A Novel Fault Correlator for GNSS Spoofer Survivability." *Institute of Navigation Joint Navigation Conference (ION JNC 2021)*. 2021.

(U) 2. Shapiro, Jerome M. "Signal Clustering Using Bayesian Inference (SCUBI): A Bayesian Approach to Choosing Consistent GNSS Signals." *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*. 2021.

(U) 3. Psiaki, Mark L., Steven P. Powell, and Brady W. O'Hanlon. "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data." *proceedings of the 26th international technical meeting of the satellite division of the Institute of Navigation (ION GNSS+ 2013)*. 2013.