IIT Armour College of Engineering
ILLINOIS INSTITUTE OF TECHNOLOGY

IIT NavLab

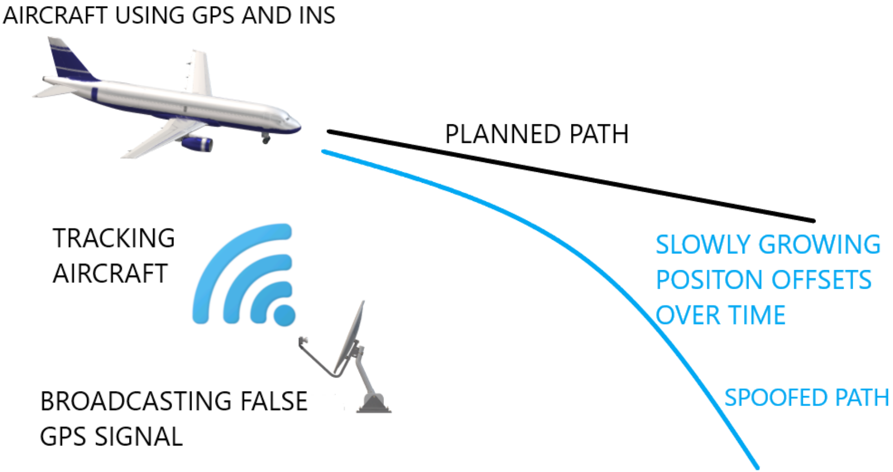
Detecting GNSS spoofing of ADS-B equipped aircraft using INS

Birendra Kujur, Samer Khanafseh, Boris Pervan

Illinois Institute of Technology

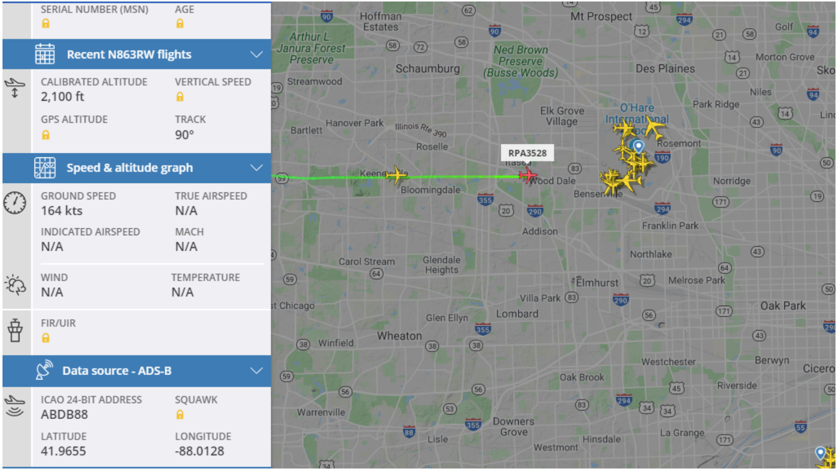
10th ICG Workshop on GNSS Spectrum Protection and Interference Detection and Mitigation
United Nations Vienna International Center
Vienna, Austria and Online
December 6, 2022

What is spoofing?



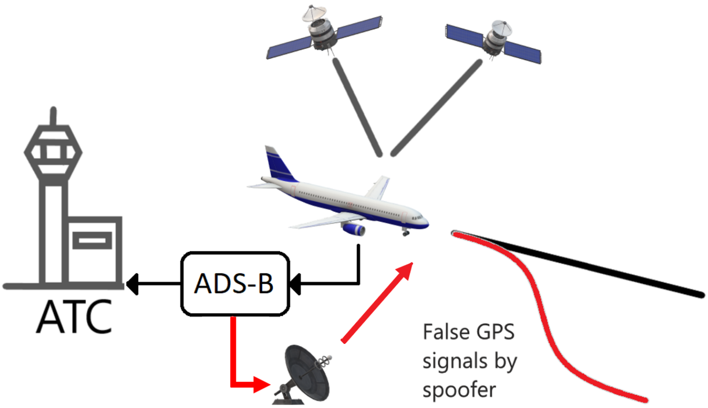
Background

Aircraft tracking using Automatic Dependent Surveillance-Broadcast (ADS-B)[1]



[1] Live Air Traffic. Retrieved from https://www.flightradar24.com/

How ADS-B can aid a spoofer?



Availability of low-cost ADS-B tracker[2]

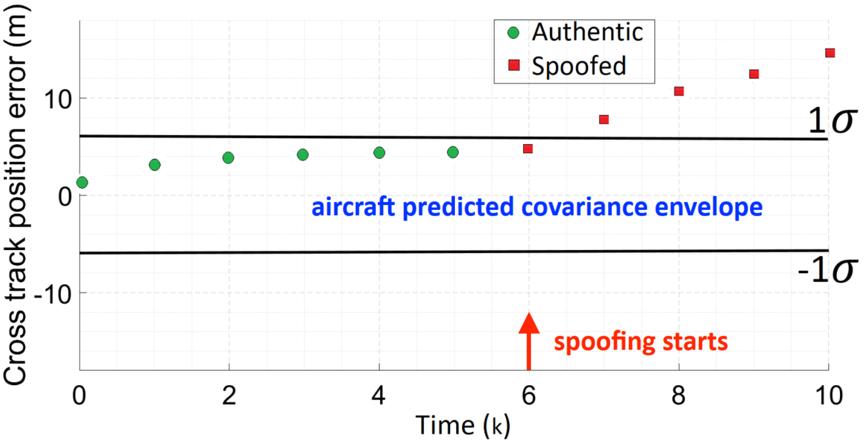
2 Share your ADS-B data. Retrieved from https://www.flightradar24.com/

Example: En route aircraft

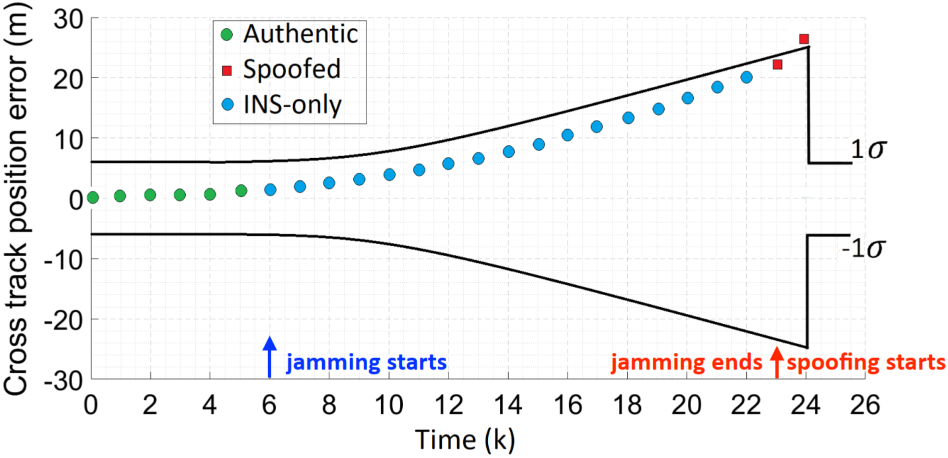
- Aircraft on level flight with constant cruising speed
- Inertial-aided GNSS in Kalman Filter (KF) for navigation and ADS-B Out
- Receives single frequency code and carrier measurements
- Idea also applicable to dual frequency multi-constellation GNSS, terminal and precision approach scenarios

Example: En route aircraft

How can spoofer deviate an aircraft?



GNSS outage (jamming) and re-acquisition



Spoofing scenario

- Position and velocity states from KF are used for ADS-B as $\hat{\mathbf{r}}_{k_{ADS-B}}$ and $\hat{\mathbf{v}}_{k_{ADS-B}}$.
- Spoofer receives ADS-B and predicts the future aircraft position

$$\bar{\mathbf{r}}_{k+1_s} = \hat{\mathbf{r}}_{k_{ADS-B}} + (\hat{\mathbf{v}}_{k_{ADS-B}} \times \Delta t)$$

- Compensating reasonably for other GNSS error states, spoofer creates signal corresponding to range measurements

$$\mathbf{z}_{k+1_s} = \mathbf{H}_{k+1}\bar{\mathbf{x}}_{k+1_s}$$

- Finally, the aircraft observes the measurements as

$$\mathbf{z}_{k+1_{s(A/C)}} = \mathbf{z}_{k+1_s} + \mathbf{m}' + \boldsymbol{\nu}_{th}$$

where, $\mathbf{H}$ is the observation matrix, $\mathbf{m}'$ is the multipath error and $\boldsymbol{\nu}_{th}$ is the receiver thermal noise.

ADS-B modulation

- Spoofer can predict the aircraft's position using accurate ADS-B information.
- No need to implement an active tracking device (e.g., Lidar).
- To deny potential spoofers such easy access, aircraft can "modulate" ADS-B Out positions (within FAA AC 20-165 standards)

$$\hat{\mathbf{r}}_{k_{ADS-B}} = \hat{\mathbf{r}}_k + \mathbf{b}_k$$

- This will cause subsequent spoofed measurement to have an inherent offset which can be detected using a monitor.

Position domain-innovation monitor

- Spoofing is detected by comparing position obtained from GNSS measurement and INS propagation.

- At any time k, the KF measurement update is

$$\hat{\mathbf{x}}_k = \bar{\mathbf{x}}_k + \mathbf{L}_k(\mathbf{z}_k - \mathbf{H}_k\bar{\mathbf{x}}_k)$$

  where, $\mathbf{L}$ is the Kalman gain, and $\bar{\mathbf{x}}_k$ is state obtained after INS propagation.

- Before using the measurement, we check the test statistic in one position direction

$$q_k = \mathbf{u}^T\mathbf{L}_k(\mathbf{z}_k - \mathbf{H}_k\bar{\mathbf{x}}_k)$$

  where, $\mathbf{u}$ is a single column vector that extracts the desired position state.

Position domain-innovation monitor

- If the measurement is authentic, this test statistic will have distribution with zero mean and variance,

$$\mathrm{var}(q_k) = \mathbf{u}^T \mathbf{L}_k \mathbf{S}_k \mathbf{L}_k^T \mathbf{u}$$

where, $\mathbf{S}$ is the innovation covariance matrix.

- The threshold for false alarm allocation can be chosen using the appropriate multiple of the standard deviation

$$T_k = k_{FA} \times \sqrt{\mathbf{u}^T \mathbf{L}_k \mathbf{S}_k \mathbf{L}_k^T \mathbf{u}}$$

- When the spoofer utilizes the modulated ADS-B and returns a spoofed signal, the bias sent out at previous time epoch appears in the current measurement.

$$\hat{\mathbf{r}}_{k_{ADS-B}} = \hat{\mathbf{r}}_k + \mathbf{b}_k \qquad \rightarrow \qquad \text{sent by aircraft}$$

$$\bar{\mathbf{r}}_{k+1_s} = \hat{\mathbf{r}}_{k_{ADS-B}} + (\hat{\mathbf{v}}_{k_{ADS-B}} \times \Delta t) \qquad \rightarrow \qquad \text{prediction by spoofer}$$

Position domain-innovation monitor

- If the spoofed measurement is received at time $k+1$ the test statistic is

$$q_{k+1} = \mathbf{u}^T \mathbf{L}_{k+1}(\mathbf{H}_{k+1}\bar{\mathbf{b}}_k + \mathbf{m}^{'} + \boldsymbol{\nu}_{th})$$

where, $\bar{\mathbf{b}}_k$ is $[\ \mathbf{b}_k \quad \mathbf{0}\ ]^T$.

- The test statistic has now a shifted mean of

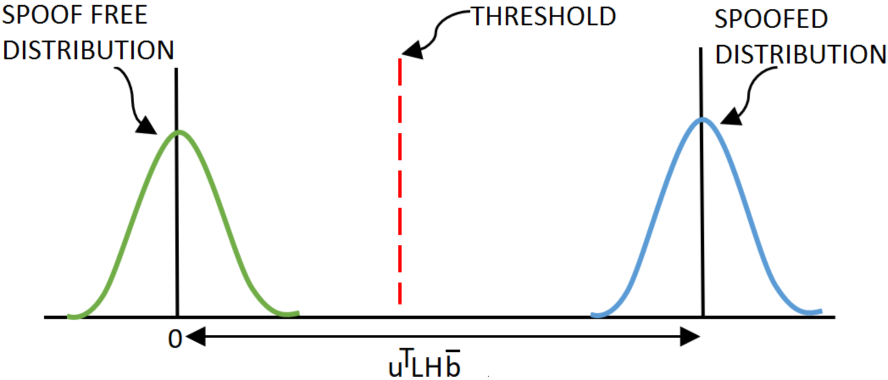
$$\mathbf{u}^T \mathbf{L}_{k+1}\mathbf{H}_{k+1}\bar{\mathbf{b}}_k$$

- The distribution of the test statistic due to spoofed measurement has variance,

$$\mathrm{var}(q_{k+1}) = \mathbf{u}^T \mathbf{L}_{\mathbf{k+1}}\mathbf{M}^{'}\mathbf{L}_{k+1}^T\mathbf{u}$$

where, $\mathbf{M}^{'}$ is the diagonal matrix with the multipath and thermal noise variances for the spoofed signal.

Test statistic distribution change



The ADS-B offset $\bar{\mathbf{b}}$ at any instant k can be chosen as

$$\mathbf{u}^T \mathbf{L}_{k+1} \mathbf{H}_{k+1} \bar{\mathbf{b}}_k = k_{FA} \times \boxed{\sigma_{\bar{x}_{k+1}}} + k_{MD} \times \boxed{\sigma_{m'_{k+1}}}$$

Position domain-innovation monitor

- where,

$$\sigma_{\bar{x}_{k+1}} = \sqrt{\mathbf{u}^T \mathbf{L}_{k+1} \mathbf{S}_{k+1} \mathbf{L}_{k+1}^T \mathbf{u}}$$

$$\sigma_{m'_{k+1}} = \sqrt{\mathbf{u}^T \mathbf{L}_{k+1} \mathbf{M}' \mathbf{L}_{\mathbf{k+1}}^{\mathbf{T}} \mathbf{u}}$$

  k_{MD} is chosen such that the desired missed detection probability is met using the threshold.

- The current ADS-B offset is chosen using predicted position covariances, since the offset will be appearing in the subsequent spoofed measurement set.

ADS-B accuracy and integrity

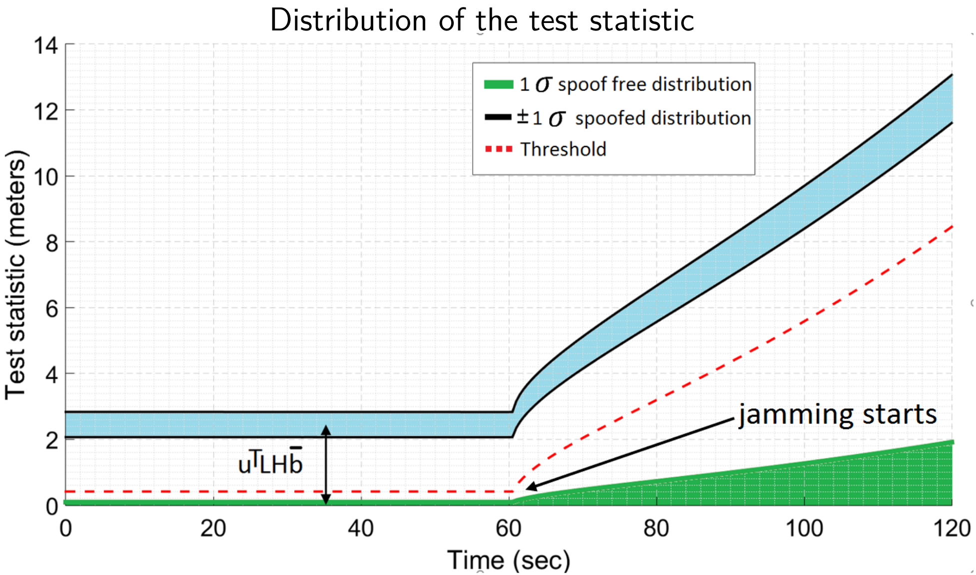
- Within ADS-B, aircraft sends out
  - Navigation Accuracy Category for Position (NAC_P)
  - Navigation Integrity Containment (NIC)
- NAC_P specifies with 95% probability bound on the reported ADS-B position error.
- To operate in civil airspace a minimum nominal NAC_P level of 8 is required, which corresponds to 92.6 m. ($NAC_P(8)$).[3] So the aircraft needs to ensure that,

$$\mathbf{u}^T \bar{\mathbf{b}}_k + 2\sqrt{\mathbf{u}^T \hat{\mathbf{P}}_k \mathbf{u}} \leq NAC_P(8)$$

- While coasting during jamming NIC and NAC_P values will need to be updated to account for increasing position covariances, and ADS-B position offsets.

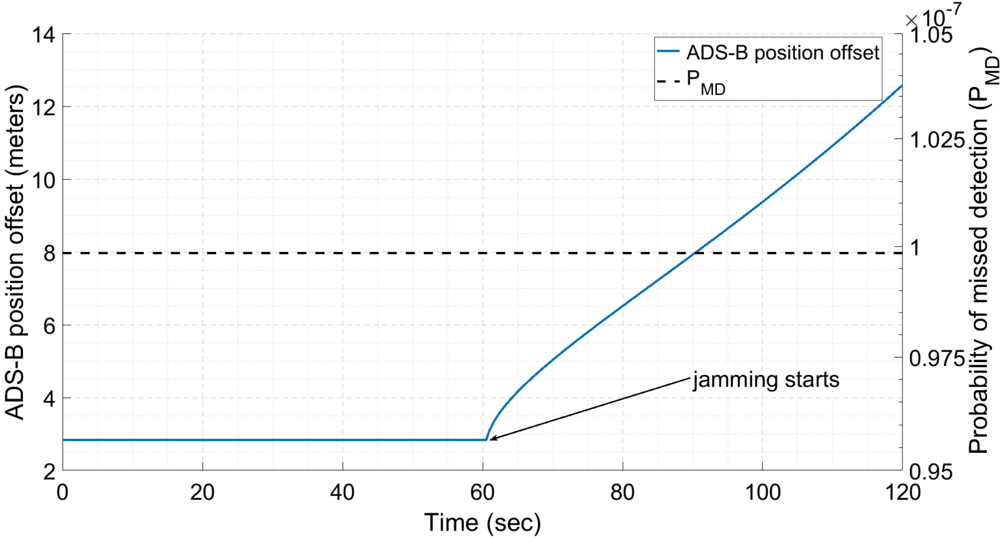
[3] Advisory Circular, Department of Transportation, Federal Aviation Administration: Subject: Airworthiness Approval of Automatic Dependent Surveillance - Broadcast (ADS-B) Out Systems: AC-20-165.

Example Results

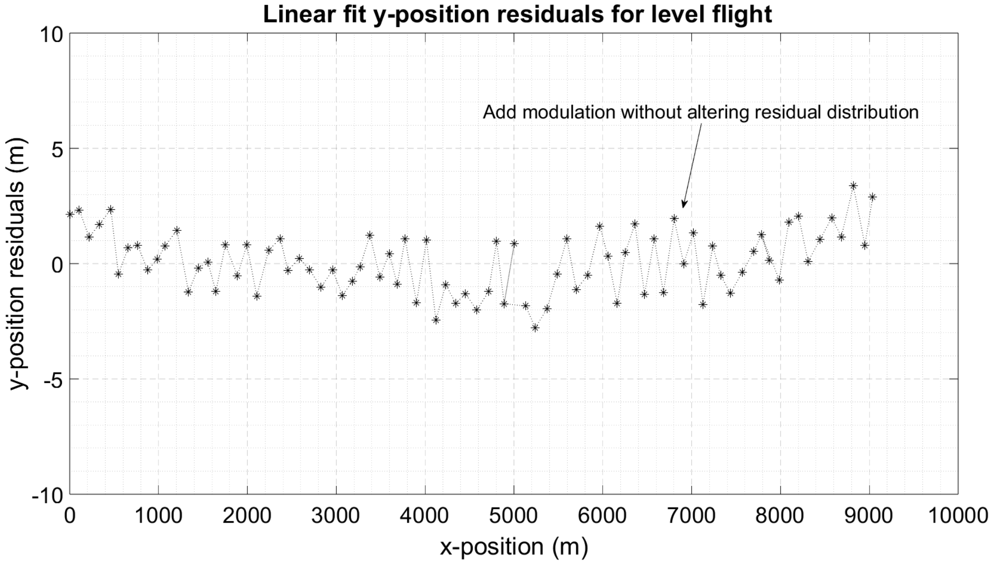


Example results

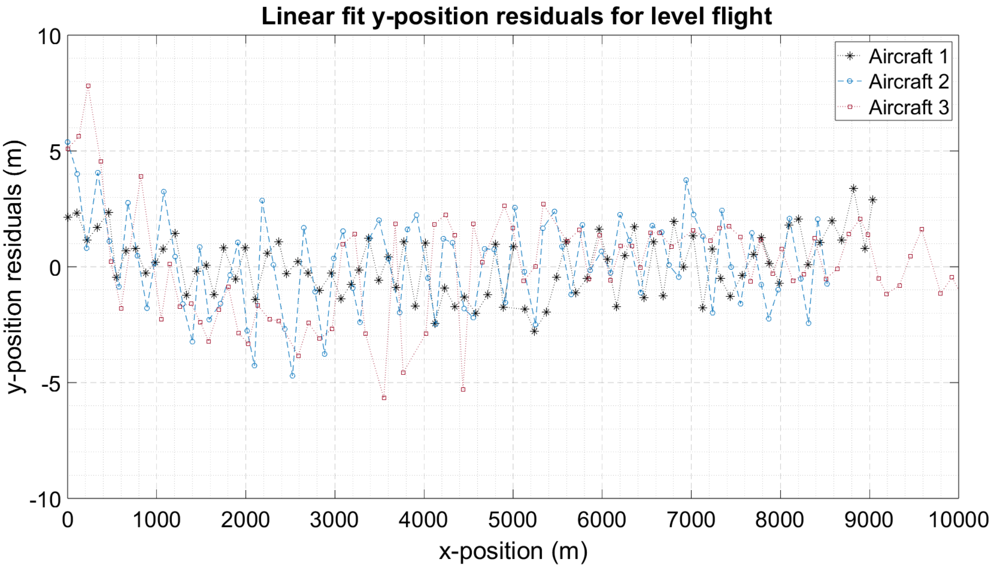
Probability of missed detection and ADS-B position offset



Future work - ADS-B variable modulation



Future work - ADS-B variable modulation



Summary

- ADS-B increases **spoofing vulnerability** of an aircraft.
- Spoofers with access to ADS-B can easily and accurately track aircraft, enabling generation of **false GNSS trajectories that can go undetected** at aircraft even with INS aiding.
- **Adding modulated offsets to ADS-B Out position** reports can be highly effective anti-spoofing measure for INS-equipped aircraft.
- A **position domain-innovation monitor** can detect spoofed GNSS signals created using the offset ADS-B.
- The **jamming-then-spoofing** scenario is also addressed by ADS-B modulation
- Future work includes evaluating and protecting against potential spoofer countermeasures-e.g., attempts to “de-bias” using random counter-offsets.