Real-Time AI-Based Intrusion Detection and Explainable Threat Interpretation for ADS-B Systems

Background & Motivation

Automatic Dependent Surveillance–Broadcast (ADS-B) underpins modern air-traffic surveillance but has no built-in authentication or encryption. This makes it vulnerable to threats such as identity spoofing, false altitude/speed broadcasts, transponder code manipulation, and virtual trajectory changes. A real-time, trustworthy intrusion-detection capability paired with Explainable AI (XAI) can help operators recognize and understand abnormal behavior quickly, improving safety and confidence in AI-assisted decisions.

Project Aim

Design and implement a real-time IDS for live ADS-B streams that:

- Detects anomalies/attacks as they occur, and
- Explains each alert (e.g., via SHAP/LIME/attention) so human operators understand why something was flagged.

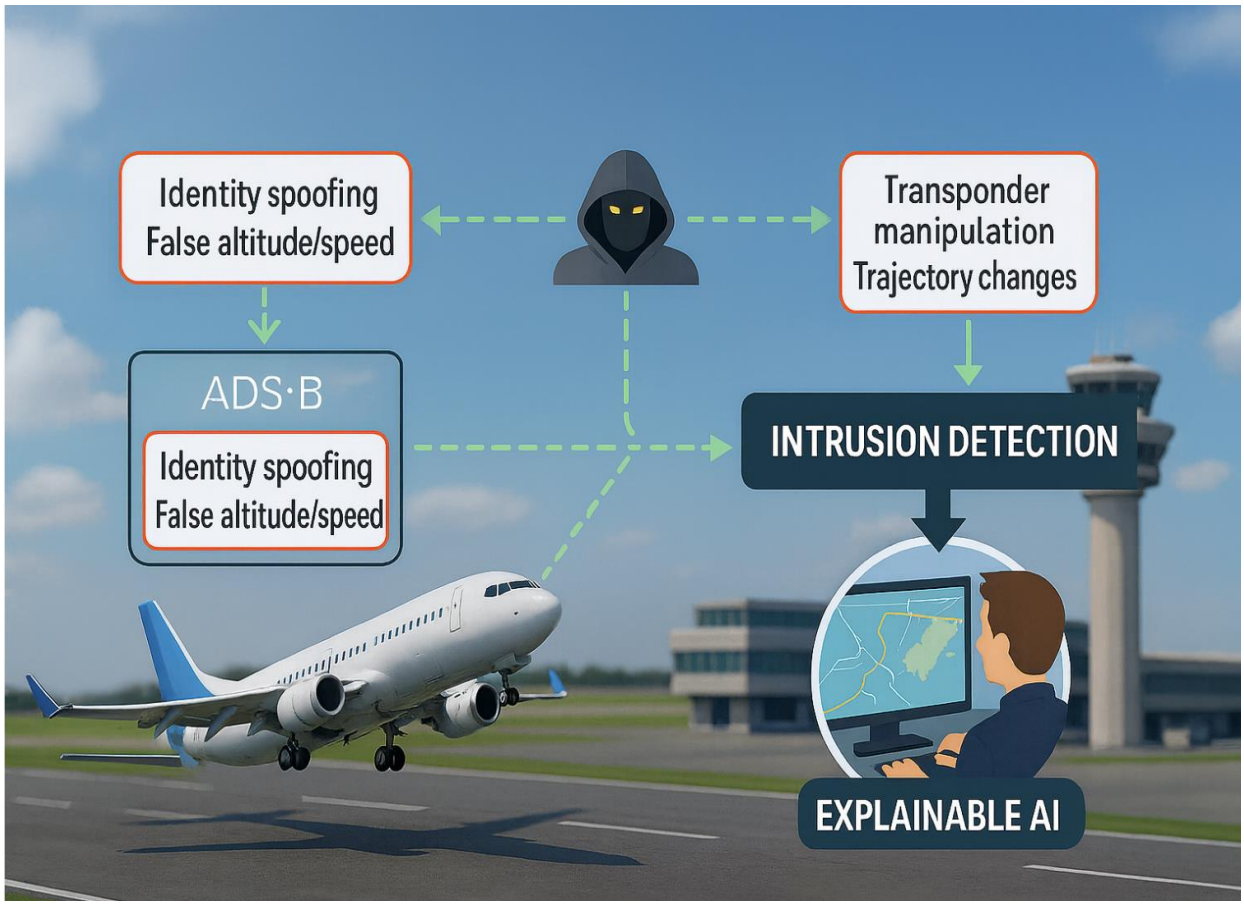
Scope & Key Features

- Live data ingestion: Stream ADS-B messages from OpenSky or local SDR captures.
- Models: Start with strong baselines (e.g., LSTM Autoencoders). Optionally explore Graph Neural Networks or lightweight Transformers.
- Targets (aspirational): ≥95% detection accuracy with ≤5% false positives on curated test scenarios.
- Explainability: Per-alert attributions and visualizations (feature contributions, trajectory highlights on map).
- Integration: Optional display in BlueSky or a lightweight web dashboard.

- Validation: Simulated or replayed attack traces (e.g., openScope scenarios) + held-out real traffic segments.

Learning Goals

- Build an end-to-end streaming ML pipeline (data → model → decision → visualization).
- Compare anomaly-detection approaches (reconstruction vs. prediction vs. one-class baselines).
- Apply explainable AI (XAI) to make alerts interpretable and operator friendly.
- Evaluate models with rigorous metrics and clearly communicate limitations.



Deliverables

- Working system (real-time or near-real-time pipeline) with operator UI.
- Model & XAI report (metrics, ablations, example explanations).
- Attack scenario pack (scripts/traces for replay in openScope/BlueSky).
- Final report

Prerequisite Knowledge (required/recommended)

No prior experience with aviation security or advanced AI is required. All essential ADS-B background and starter code will be provided, and concepts will be introduced step by step.

Required (practical):

- Basic Python skills (read/write/debug scripts; use common libraries).
- Experience with data handling (files/streams) and git for collaboration.

Recommended (nice to have, not mandatory):

- Intro to machine learning concepts (classification, anomaly detection, neural nets).
- Basic cybersecurity notions (spoofing, integrity, replay).
- Prior coursework, such as TDDE01 (Machine Learning) can help but is not required.

This project is designed so that motivated students can learn the necessary ADS-B, ML, and XAI concepts during the course of the work. Guidance, examples, and templates will be provided.

References

- **Identifying anomalies in Automatic Dependent Surveillance–Broadcast with Explainable AI (BSc, 2025).** Linköping University DiVA record: https://liu.diva-portal.org/smash/record.jsf?pid=diva2:1989406. (PDF: https://liu.diva-portal.org/smash/get/diva2:1989406/FULLTEXT01.pdf)
- **Detecting ADS-B spoofing attacks: using collected and simulated data (BSc, 2021).** Linköping University DiVA record: https://liu.diva-portal.org/smash/record.jsf?pid=diva2:1592064. (PDF: https://www.diva-portal.org/smash/get/diva2:1592064/FULLTEXT01.pdf)
- **Simulating ADS-B vulnerabilities by imitating aircrafts (BSc, 2022).** Linköping University DiVA record: https://liu.diva-portal.org/smash/record.jsf?pid=diva2:1671360.
- **Enhancing the openScope ADS-B Attack Simulator (BSc, 2024).** Linköping University DiVA record: https://liu.diva-portal.org/smash/record.jsf?pid=diva2:1874217.
- **Simulating ADS-B Attacks in Air Traffic Management (LiU, IDA paper).** PDF: https://zebroid.ida.liu.se/sims/paper.pdf. (Related DiVA record: https://liu.diva-portal.org/smash/record.jsf?pid=diva2:1452531 — PDF: https://www.diva-portal.org/smash/get/diva2:1452531/FULLTEXT01.pdf)
- **Code – openScope Attack Simulator (LiU GitLab).** https://gitlab.liu.se/openscope/openscope-attack-simulator
- **Code – openScope-attacks (LiU GitLab).** https://gitlab.liu.se/gusli687/openscope-attacks