

SOFTWARE ENGINEERING ASSIGNMENT

Suleman Khan

Linkoping University

1 My Project Background

The Next Generation Air Transportation System (NextGen) employs the Automatic Dependent Surveillance-Broadcast (ADS-B) to manage congested airspace and optimize air traffic operations. ADS-B delivers precise aircraft location information through satellite navigation, improving air traffic management. Despite its benefits, the plain-text nature of ADS-B makes it vulnerable to various cyber attacks, including Eavesdropping, Injection, Alteration, Replay, Jamming, and Spoofing. These attacks can mislead aircraft pilots and air traffic control personnel, posing a dangerous threat. To ensure the security of air-ground communication, we are working to propose a cutting-edge anomaly detection framework for ADS-B protocol and develop an open-source simulator to train Swedish ATC people against cyber attacks. In order to detect anomalies, we are proposing a framework that employs a three-stage deep learning approach, which includes Spatial Graph Convolution Networks (GCN) and a Deep auto-regressive generative model. The first stage classifies the data across the operating aircraft airspace as normal or under attack using GCN. In the second stage, the system analyzes the state sequences of airspace to identify anomalies using a generative Wavenet model and outputs the attacked features. The final stage comprises an aircraft (ICAO) classification module that utilizes each aircraft's unique RF transmitter signal characteristics, enabling ground station operators to scrutinize incoming messages. We aim to obtain promising results in terms of False Alarm Rate (FAR) and detection accuracy by training our models on raw and decoded ADS-B data. We are developing an advanced aircraft simulator that mimics the behaviour of a real aircraft in the sky. This tool will serve as a training platform for new air traffic control personnel. Additionally, it will prepare operators to respond more effectively to cyber threats and take decisive actions during such events.

2 Principles from Robert's lectures

We are working to enhance the NextGen Air Transportation System with our ADS-B protocol. We are incorporating vital principles from both Software Engineering and Machine Learning Engineering to achieve this. We begin with strict Version Control, which ensures an accurate history of data and model changes. Our system must be trustworthy and resilient, especially regarding air traffic management. To guarantee this, we use a three-stage deep learning framework that undergoes rigorous Testing. Testing is a cornerstone of SE, and we apply it to our QA process for ML. Our Spatial Graph Convolution Networks and Wavenet model operate on patterns, which requires a deeper dive into intricate decision pathways. Our commitment to Requirements Engineering is also evident. We use raw and decoded ADS-B data to ensure comprehensive Testing, preparing our system and ATC teams to foresee and tackle cyber threats effectively. Our aircraft simulator is an advanced QA tool which helps us achieve this goal. We aim to create an ADS-B security framework that epitomises robustness and reliability in air traffic control by weaving together these SE and ML practices.

3 Principles from Guest Lectures

In our pursuit to improve and optimize the NextGen Air Transportation System, it is critical to acknowledge that our software's accuracy relies heavily on establishing precise boundaries. The ADS-B protocol is responsible for managing busy airspace and air traffic operations, and it requires careful definition and validation of these boundaries. To uncover any discrepancies between the desired and actual system behaviour, software testing must include Boundary Value Exploration. Given the ADS-B system's susceptibility to cyber attacks, such as Evasion, Injection, Alteration, Replay, Jamming, and Spoofing, it is crucial to conduct comprehensive boundary value exploration.

My cutting-edge anomaly detection framework, which utilizes a three-stage deep learning process, heavily relies on these boundaries. Each process step is susceptible to potential vulnerabilities if the boundaries are not well-defined, tested, and refined. To address this, I have created an advanced aircraft simulator as a training platform and a sandbox for rigorous boundary value testing. It is essential to thoroughly explore these boundaries to ensure that the NextGen Air Transportation System is dependable and safe. By doing so, we can ensure that the system performs as intended

and promptly addresses any deviations, thus ensuring efficient air-ground communication.

4 Security and Privacy

Understanding: While exploring software engineering, I realized that Security and Privacy are crucial beyond just protecting data. It is essential to ensure that systems are strong enough to withstand potential vulnerabilities and that user data remains confidential. As I focus on ADS-B, a vital technology for aircraft communication, I understand the significance of ensuring its security. Areas of Opportunity in my ADS-B Research:

4.1 Research Challenges:

Spoofing and Replay Attacks: My research has identified that because ADS-B signals are currently unencrypted, they are susceptible to malicious impersonations, where attackers can "spoof" or mimic genuine aircraft signals.

Jamming: Another dimension I'm exploring is the intentional disruption of ADS-B signals. Such disruptions can prevent the system from functioning correctly, potentially leading to aviation mishaps [1].

Eavesdropping Mitigation: I'm exploring ways to encrypt ADS-B signals to prevent eavesdropping by third parties.

4.2 Commercial Opportunities:

Secure ADS-B Infrastructure Development: I'm considering enhancing ADS-B technology by integrating encryption and anomaly detection.

Security Consultation: I see potential in offering specialized solutions and consultancy in ADS-B security protocols.

4.3 Application of AI/ML:

Anomaly Detection: Using machine learning, I'm working on models that can automatically detect unusual patterns in ADS-B signals. Such anomalies might indicate potential spoofing or other attacks.

Predictive Analysis: My research also encompasses AI-driven tools that can proactively predict and counteract emerging security threats by analyzing global ADS-B traffic patterns.

5 Human-Computer Interaction (HCI)

Understanding: My study into HCI has shown me the importance of intuitive and user-friendly systems. In the context of ADS-B simulator development, I've been focusing on making them as intuitive and realistic as possible. Opportunities in my ADS-B Simulator Development Research:

5.1 Research Challenges:

Interface Design:: It's imperative that the simulator's interface is both realistic (to mirror actual ADS-B systems) and user-friendly. I'm constantly iterating on designs to strike this balance.

Adaptive Learning: Another key aspect I'm delving into is how the simulator can adapt its difficulty and scenarios based on the user's proficiency, offering a tailored learning experience.

5.2 Commercial Opportunities:

Modular ADS-B Simulators: I envision a future where simulators can be easily customized to fit specific training needs for various aviation roles.

Simulator Usability Consultation: Leveraging my expertise in HCI, I see a potential role in collaborating with simulator developers to enhance the user experience.

5.3 Application of AI/ML:

Personalized Training Regimes: I'm experimenting with AI algorithms that can analyze a trainee's performance in real-time, adjusting simulator challenges accordingly.

Enhanced Interactivity: By incorporating AI-driven features like voice and gesture recognition, the simulator experience can be made even more immersive and intuitive [2, 3].

6 Future Trends I foresee in Software Engineering related to ADS-B and AI/ML:

Proactive Security Protocols: With the insights I've gained, I predict a future where ADS-B security doesn't just prevent breaches but uses AI to predict and proactively counteract them.

Emphasis on AI Transparency: In the coming years, any ADS-B solutions integrating AI will need to be transparent in their decision-making, a principle I’m firmly grounding in my research.

AI’s Role in Simulator Training: Beyond adaptive challenges, I believe AI will be utilized in simulators to replicate real-world system failures, offering trainees a comprehensive experience.

For my career path, I’m deeply invested in the intersection of AI and ADS-B security. My goal, whether in academia or industry, is to be at the forefront of ADS-B innovations, ensuring safer skies and better-trained aviation professionals. As AI evolves, I’m committed to continuous learning, ensuring my work remains at the cutting edge of technology and security.

References

- [1] S. Rudys, J. Aleksandravicius, R. Aleksiejunas, A. Konovaltsev, C. Zhu, and L. Greda, “Physical layer protection for ads-b against spoofing and jamming,” *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100555, 2022.
- [2] A. Blåberg, G. Lindahl, A. Gurtov, and B. Josefsson, “Simulating ads-b attacks in air traffic management,” in *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*. IEEE, 2020, pp. 1–10.
- [3] I. Gupta, R. Gupta, A. K. Singh, and R. Buyya, “Mlpam: A machine learning and probabilistic analysis based model for preserving security and privacy in cloud environment,” *IEEE Systems Journal*, vol. 15, no. 3, pp. 4248–4259, 2020.