Journal of Open Aviation Science (2023), Vol.**1**
doi:10.59490/joas.2023.7495

JOAS

EDITORIAL

Reviews and Responses for Scaling the Timing-Based Detection of Anomalies in Real-World Aircraft Trajectories

Authors: Lukas Baege, Patrick Schaller, Vincent Lenders, and Martin Strohmeier

Reviewers: Vishwanath Bulusu, Andrei Gurtov, and David Lovell

Editor: Tatiana Polishchuk

1. Original paper

DOI for the original paper: https://doi.org/10.59490/joas.2023.7205

2. Review - round 1

2.1 Reviewer 1

The paper addresses an interesting issue of detecting attacks and sensor errors in broadcast ADS-B messages. Statistical analysis is a very early-stage introductory work. It was not clear how certain aspects were narrowed down; for example, what were the different thresholds used, and how were their values decided? Using the median value for sensor spoofing distinction is also arbitrary.

The paper does a good job of explaining the results and identifying its own limitations.

Here are a few errors to fix:

- Line 24 - It also enables (use enables or facilitates instead of both).
- Line 35 - "gnssoofing" Looks like a typo.

2.2 Reviewer 2

The paper addresses an important topic: attack detection in ADS-B messages. A fast dataset from OpenSky is used. Technical errors so far represent the major source of anomalies and need to be filtered out first. Effects from GNSS distortions are visible, too. However, it appears no deliberate attacks have been found in the messages so far. Overall, the paper is interesting and well-written.

The weakest side of the paper is the lack of comparison with prior work and missing references.

For ADS-B attack demonstration, it is worth mentioning the paper below, as it also was the first to demonstrate SDR attacks on CPDLC datalink.

S. Eskilsson, H. Gustafsson, S. Khan, A. Gurtov, Demonstrating ADS-B And CPDLC Attacks With Software-Defined Radio, in Proc. of Integrated Communications Navigation and Surveillance Conference (ICNS), 2020.

To raise awareness of ATC about attacks, there is an ADS-B simulator that can model different kinds of attacks (unresponsive aircraft, stationary, wrong speed and altitude, jumping, flooding, etc). Also, it can be used to generate an artificial attack dataset that can be mixed with real-world ADS-B traces.

A. Blaberg, G. Lindahl, A. Gurtov, B. Josefsson, Simulating ADS-B Attacks in Air Traffic Management, in Proc. of IEEE/AIAA 39th Digital Avionics Systems Conference (DASC), 2020.

Most importantly, the paper does not compare the proposed AI model to detect ADS-B attacks in datasets. I suggest that a revision of the paper should compare several attack detection methods using real OpenSki and generated datasets from the paper below.

S. Khan, J. Thorn, A. Wahlgren, A. Gurtov, Intrusion Detection in Automatic Dependent Surveillance-Broadcast (ADS-B) with Machine Learning, in Proc. of IEEE DASC'21, 2021.

About the future, the paper concludes that no ADS-B replacement is coming soon. What about the ADS-C effect? Also, the LDACS data communication system should provide built-in security.

Some nits:

- To deviate from its intended course and transmit incorrect location data over ADS-B. [gnssoofing] 35
- Large margin (see Figure 7, left). This behaviour could indicate a GNSS jamming attack, where the 321

2.3 Reviewer 3

This paper presents a statistical algorithm for detecting flawed trajectory data within crowd-sourced samples of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. This is a very relevant topic, and the paper adds to the growing literature dealing with potential security breaches and other vulnerabilities that this technology possesses. Overall, the paper is very well-written, and the methodology is sound, given the various constraints and assumptions that the authors impose. The largest potential improvement to the paper would come from tightening the exposition of the introductory material. Specific comments are as follows:

Introduction, 2nd paragraph:

- "enables facilitiates": choose one of these words
- "transmit valid" - "transmit seemingly valid"
- "or modify" - "or appear to modify"
- The paragraph ends with a claim that one could spoof ADS-B with a cheap software-defined radio (SDR). That would be by far the cheapest part of the process. Much more expensive would be the broadcasting equipment, with enough transmission power to be useful. Furthermore, such a strong signal would be easy to triangulate and could thus be pursued by law enforcement. While the risks posed by the technology are real, it is not a good idea to over-simplify the ease of hacking it.

Introduction, 3rd paragraph: The paragraph ends with an unfinished citation.

Introduction, 5th paragraph:

- "register own sensors" - "register their own sensors"
- The paragraph highlights external actors and malicious data injection as the reasons for erroneous data to exist. However, properly transmitted data can end up being erroneously received due to message collisions, multipath, etc.

Introduction, 6th paragraph: By itself, statistics on the size of the data sample are not that compelling. It would be more interesting to hear how many flights were included, the average number of sample points per flight, etc., to give the statistics context.

Background, 1st paragraph: The fact that one can display real-time air traffic data using a feed from OpenSky is not relevant. Those data are extensively filtered and consolidated in order to enhance accuracy and make efficient use of real-time bandwidth. Much more important, particularly for this study, is the archive of historical data.

Background, 2nd paragraph: The timestamp generated by the sensor does not really represent the time the message was received, but rather the time that processing of the message was complete after it had passed through a sequence of FIFO queues in both the SDR and the sensor's software. Particularly, the Raspberry Pi-based sensors are not fast processors. You might see "Debuffering Timestamped ADS-B Records for Kinematic Applications" by Cuo et al. in ATM 2023 for more information.

Background, 3rd paragraph: Most of this is redundant.

Background, last paragraph: Again, the authors are making light of the effort required to spoof GPS signals. The occasions they cite are situations where a government actor was purposefully spoofing the signal as a defence against guided missile attacks. This is not very likely in parts of the world where the vast majority of ADS-B traffic is generated. Again, if non-state actors were doing such things against the wishes of the local government, they could be easily detected.

Problem Constraints, 4th paragraph: Again, the authors ignore more common sources of non-malicious error. Are they assuming that the parity information is sufficient to guard against decoding mistakes from message collisions, multipath, etc.? It is not.

Methods, 3rd paragraph: "report more precise timestamps": this needs a citation.

Methods, paragraph after equation (10): "sensor pairs with sufficient distance": what is the threshold used here?

Discussion: Aren't there cases where more than four sensors saw the same flight, particularly in densely populated areas? In this case, one possible improvement, while sticking with the paired sensor paradigm chosen for this paper, would be to test multiple independent pairs of sensors, thereby gaining confidence in a prediction when multiple pairs produced the same outcome.

3. Response - round 1

3.1 Response to reviewers

Response

We have now revised the paper according to the reviews and helpful comments. We believe we have addressed all points with the exception of one requiring extensive additional analysis and computational efforts, i.e. the comment about running the scheme with non-Radarcape sensors and quantifying how much worse it would get. This is a very interesting question, but unfortunately, from our point of view out of the possible scope of this revision/paper.

4. Review - round 2

4.1 Reviewer 1

The authors have adequately addressed all comments. This is a very good paper on applications of ADS-B data, and I recommend its publication.

4.2 Reviewer 2

The authors made some minor changes and added a few references, which is good. No detailed comparison with prior work was added, but hopefully, it will be included in future publications.