Journal of Open Aviation Science (2023), Vol.**1**
doi:10.59490/joas.2023.7733

JOAS

EDITORIAL

Reviews and Responses for
Securing the Sky: Detecting Aircraft Location Drifting through Cross-Checking Receiver-Based Estimated and Received ADS-B Trajectories

Authors: Ala Darabseh, Syed Khandker, and Christina Pöpper

Reviewers: Vincent Lenders, Matthias Schäfer, Martin Strohmeier

Editor: Tatiana Polishchuk

1. Original paper

DOI for the original paper: https://doi.org/10.59490/joas.2023.7504

2. Review - round 1

2.1 Reviewer 1

General Comments

This paper looks at the problem of identifying ADS-B trajectories that divert from the real trajectory of the transmitting aircraft. This work is relevant because ADS-B does not offer any protection against these kinds of attacks, and it is fairly trivial to launch such attacks in the current system. The problem has been known for more than a decade and many researchers have been developing countermeasures in the past. However, this work addresses the problem from a new angle: by not using the exact position of the ground receivers and not relying on a precise time-of-arrival information. This make the solution appealing for the crowdsourced ADS-B networks such as OpenSky Network in which the owners of the receivers may not want to disclose their precise location. On the downside, the precision of the approach is much worse that other methods that exploit this information. Yet, the authors show that a precision of less than 20 km may be achieved, which could be sufficient to detect attacks in which the attacker tries to diverge the trajectory significantly in one direction that is far from the real position of the aircraft.

Detailed comments to the authors

The threat model is not very clear. The abstract refers to aircraft hijacking, but hijacking attacks may not necessarily involve ADS-B spoofing. The paper later considers further threat models such attackers on the ground, driving in a vehicle, etc. The paper should have a well-defined threat model to make this clearer. The lack of threat model becomes particularly problematic in the discussion in Section 5.

I missed a few relevant references

- when citing [4,5,6] on line 23, you should as well cite "Experimental Analysis of Attacks on Next Generation Air Traffic Communication, ACNS 2013" as it has been the first scientific paper on this

topic.

- on line 34 and 74, you should cite other works, e.g., Secure Track Verification (IEEE S&P 2015), Lightweight Location Verification in Air Traffic Surveillance Networks (ACM CPSS 2015), Secure Motion Verification using the Doppler Effect (ACM WiSec 2016), Investigation of Multi-device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures (ACM MobiCom 2016), A k-NN-based Localization Approach for Crowdsourced Air Traffic Communication Networks (IEEE TAES 2018), In Pursuit of Aviation Cybersecurity: Experiences and Lessons from a Competitive Approach (IEEE S&P 2023)
- Line 76: the idea of using a grid to train a kNN regression model was first presented in "A k-NN-based Localization Approach for Crowdsourced Air Traffic Communication Networks (IEEE TAES 2018)". You should always cite the original papers and not "only" the derivations that appeared later.
- The same applies to ref [14] on line 84. The first approach to lightweight verification was from 2015: "The Lightweight Location Verification in Air Traffic Surveillance Networks (ACM CPSS 2015)"
- The same applies on ref [15] on line 86. The idea of using a timestamp in the ADS-B message for location verification was first proposed in "Secure Track Verification (IEEE S&P 2015)"

In section 3 on line 102, you mention that you have the arrival time in your dataset, but it is not clear if you use it and how? If you don't use it, it is also not clear why? This should be better explained.

A significant part of the paper is dedicated to the problem of not having the exact position of the receivers. This problem can be however solved with self-positioning techniques such as "SkyPos: Real-World Evaluation of Self-Positioning with Aircraft Signals for IoT Devices, JSAC 2023). Using this technique, you can localize the receivers with a precision in the order of meters. You should at least mention these techniques and elaborate more clearly on why not using them.

Figure 2 is hard to interpret. Not sure how useful it is. what are the axis representing? what are the units?

From the paper description, it is not really clear how the method works that you refer to on line 172. There is a lack of a formal description of the method/algorithm. As such it would not be possible to the reader to reproduce your results. It is also not possible from the paper to assess the novelty of the "method" as the details are missing.

Figure 3 is a bit a waste of space. It should be sufficient to plot the error statistics between the reported and the computed locations for all locations in a single graph instead of showing each location in a single graph. The caption seems also misleading. What do you mean with "observed" sensor location? Do you mean "reported" sensor location?

The results on lines 211-231 lack a description of the underlying data being used to obtaining them. How much data was used and how was the data used to produce these performance numbers? Also how representative are the results. You should also give confidence intervals or a standard deviation to make this clear.

Minor things:

Line 46: You should mention that you also use the aircraft signals for the trajectory derivation and not only the coordinates of the receivers.

Line 62: I would remove the word "rapidely" as the transition to ADS-B has been a long multi-decade endeavor.

Line 264: you write that the owners of ADS-B receivers regard their location as private information. This is true for only a few of the OpenSky receivers, and should be relaxed in the text

2.2 Reviewer 2

The paper presents a new method for detecting location drift attacks in ADS-B data, gathered from a crowdsourced network of receivers such as the OpenSky Network. Such attacks involve the injection of erroneous location data into the ADS-B wireless link, misleading about the aircraft's actual trajectory. The proposed method leverages the simultaneous tracking of a single aircraft by multiple sensors, learning each sensor's coverage to perform a plausibility check on the reported positions.

I appreciate the approach's simplicity, its compatibility with existing ADS-B infrastructure, and its independence from time synchronization between sensors. These features make it especially relevant for networks like the OpenSky Network, where unsynchronized data and varied sensor coverage have the potential to enhance the method's security and accuracy.

However, the paper has significant gaps that should be tackled by the authors:

1. Attacker Model: The paper lacks a clearly defined attacker model, which is only briefly touched upon in Section 5.1. This omission leads to questions throughout the paper since the assumptions made regarding the attacker's capabilities and behavior are unclear.

2. Evaluation Results: While the method is proposed as a security measure, the evaluation focuses predominantly on the accuracy of localization rather than on security. Also, the provided metrics are insufficiently detailed. For example, the maximum error in trajectory-based evaluation lacks context (e.g., units and the number of trajectories assessed), and the point-based evaluation omits confidence intervals and other information about the error distribution.

3. Interpretation of Results: The conclusion in Section 5.1 that attacks causing more than 20km offset can be detected is misleading. The paper should focus more on location verification including using data from sensors that did not report seeing the aircraft, which might detect mismatches more effectively than the localization approach. Especially given the ground-based attacker's limited reach.

Additional areas for improvement include:

1. Sensor Location Relevance: The relevance of sensor location is unclear, as the method uses sensor coverage data not the sensor location. Clarification on whether and how physical sensor locations impact the analysis would be beneficial.

2. Weighted Localization Method Details: More information is needed on how weights are assigned in the weighted centroid calculation for localization. Details on signal strength calibration across sensors and the incorporation of sensor-aircraft distances into weight calculations are missing so it is difficult for the reader to assess the validity of the method.

3. Calculation of Sensor Coverage: The methodology for determining sensor coverage, such as geographical binning or other techniques, should be detailed. Consideration of potential coverage data manipulation by attackers would also strengthen the security analysis.

2.3 Reviewer 3

Abstract and Intro:

- "instances of aircraft hijacking" It is clear to me what you mean, but I'd suggest to prefix it with "virtual" or call it "aircraft trajectory hijacking" to distinguish it properly from actual hijacking of a plane by people on board.

- "Such an attack holds the potential to deviate other aircraft from their intended trajectory and could even lead to dangerous collisions between aircraft. " This should be referenced and/or the mechanism outlined. It is not likely that this would happen directly via ADS-B spoofing against another aircraft, as that still has TCAS which has primacy. If ADS-B directly affects a controller (which is not likely now but maybe in the future) then they could direct other aircraft to change course, but more likely they will first use other means, ie call the aircraft or even scramble jets.
- The intro should state what the novel contributions of this paper are.
- I'm missing a threat model for a security paper. That said, the focus of the content beyond the motivation seems to be entirely on the localization (sensor & aircraft) so far, not on, say, spoofing detection. Maybe it would be sensible to position the paper accordingly.
- It would also be good to have a step-by-step end-to-end description of the localization process and the proposed verification method early on for better understanding. Ideally with a picture.

Related work:

- This is a bit short. There has been so much work in this area over the past decade, it is crucial that any additional one positions itself properly in particular against the more recent work, otherwise we risk adding more noise. I would not expect a detailed comparative evaluation of these methods in a Symposium paper but there should be a good overview and a discussion/table of pros and cons and what gap the present paper's approach is closing.
- These are sentences from the introduction that aim to do this but they do not include references to those methods: "Conversely, many current location verification methods, such as MLAT [10], necessitate the reception of messages by four or more sensors, a condition that proves challenging to meet. While alternative verification methods have been suggested, they often fall short of providing a comprehensive predictive solution that addresses challenges like the number of receptions, altitude considerations, and other pertinent factors "
- The choices for [13-15] as representative for secure location verification strike me as a bit arbitrary. There's a long list of methods in [4].

Methods:

- It would be good to define the drifting attack upfront, in slightly more detail outside the intro (maybe methodology), as these terms are AFAIK not used in the literature.
- "We process and assess approximately 3 million messages extracted from OpenSky data " There should be more information about the dataset: time, location, sensor locations, coverage, how it was extracted, cleaned etc. After all JOAS requires the dataset to be open and it should be well described.
- "ultimately create the coverage for each sensor. " Maybe describe the concrete here, rather than in the results/Section 4.
- "Revealing Sensor Locations" What were the difficulties in the sensor locations? I guess the self-reporting may be inaccurate for some many? Please describe this more as it is useful for the community. Second, it is also necessary to describe the self-localization process you've been using. There are some references, e.g. [1,2] but there are more just in aircraft verification, certainly more in indoor/outdoor localization. Importantly, there's also a difference beween radarcapes and dump1090 sensors. The former do report their location quite accurately with GPS, though outliers/errors do exist.
- Why can you not use LocaRDS, which was created specifically for this type or research (testing and comparing of algorithms)? [3] It has verified sensor locations, too.

- It would be good to illustrate central and weighted localization with a figure. Here, again, are likely many references available in the existing literature.
- "These factors play a critical role in determining the suitability and likelihood of a specific location. The ToA allows us to assess the time it takes for a message to reach each receiver, while the RSS measures the signal strength at each receiver. " This needs a cocnrete explanation how exactly these two characteristics do this.

Results:

- Could you explain the importance of Fig. 2? 2a illustrates how far the 45 sensors are from each other? What is the utility of this for the verification? 2b) shows the accuracy of the sensor localization? Why do you use this method instead of, say, a CDF? I also don't really understand if you know treat the reported data as ground truth or not? Again, there have been a few sensor localization attempts in the literature.
- Do the user-reported results work worse for the verification? This would be interesting to see.

Nitpicks:

- It is called both drifter attack, or drifting attack. This should be used consistently.

[1] SkyPos: Real-world evaluation of self-positioning with aircraft signals for IoT devices
Y Lizarribar, D Giustiniano, G Bovet, V Lenders
IEEE Journal on Selected Areas in Communications

[2] Alexander Canals, Pascal Josephy, Simon Tanner and Roger Wattenhofer.
Robust indoor localization with ADS-B.
In Proceedings of the 27th Annual International Conference on Mobile Computing and Networking.
October 2021, 505–516.

[3] LocaRDS: A localization reference data set
M Schäfer, M Strohmeier, M Leonardi, V Lenders
Sensors 21 (16), 5516

[4] Securing the air–ground link in aviation
M Strohmeier, I Martinovic, V Lenders
The Security of Critical Infrastructures: Risk, Resilience and Defense, 131-154

3. Response - round 1

3.1 Response to reviewer 1

1. Threat Model:

Reviewer Comment: Threat model is not clear.

Response

Added a detailed threat model in Section 3.1 and adjusted references to aircraft location drifting not hijacking in the paper.

2. Relevant References:

Reviewer Comment: Missing relevant references in several sections.

Response

Added the missing references throughout the paper as indicated.

3. Arrival Time Data:

Reviewer Comment: Unclear if arrival time data is used.

Response

Explained usage of arrival time data in Section 3.1 in the weighted localization method.

4. Self-Positioning Techniques:

Reviewer Comment: Did not consider self-positioning techniques for localizing receivers.

Response

Explained the relevance of SkyPos technique in Section 4.2.

5. Figure 2 Interpretation:

Reviewer Comment: Figure 2 is hard to interpret.

Response

Justification and explanation provided in Section 4.2 and figure caption.

6. Method Description:

Reviewer Comment: Lack of formal description of the method.

Response

Added detailed explanations and formal description through the whole paper and more specifically in

Section 4.2. 7. Results Data Description:

Reviewer Comment: Lack of description of underlying data and representativeness.

Response

Added detailed data description and justifications in Section 4.4.

8. Minor Comments:

Reviewer Comment: Various minor corrections and improvements needed.

Response

Made all necessary corrections as suggested.

Additional Areas for Improvement and Responses

Clarification on Aircraft Signal Usage

Response

Mentioned the use of aircraft signals for trajectory derivation.

Removal of Unnecessary Terms

Response

Removed terms like "rapidly" to better reflect the transition to ADS-B.

Relaxation of Privacy Concern Statements:

Response

Adjusted statements regarding the privacy of receiver locations.

3.2 Response to reviewer 2

Main Points and Responses

1. Attacker Model:

Reviewer Comment: The paper lacks a clearly defined attacker model, leading to unclear assumptions about the attacker's capabilities.

Response

Incorporated a detailed threat model in Section 3.1.

2. Evaluation Results:

Reviewer Comment: Evaluation focuses on localization accuracy rather than security, and provided metrics lack detail.

Response

Clarified the focus on the prediction phase in the current study. Added detailed metrics in Section 4.4 (Table 1 and Figure 6), including context for maximum error and error distribution.

3. Interpretation of Results:

Reviewer Comment: Misleading conclusion about detecting attacks causing more than 20km offset.

Response

Adjusted abstract and introduction to clarify current focus on location prediction accuracy. Future work will address attack detection in more detail.

4. Sensor Location Relevance:

Reviewer Comment: The relevance of sensor location is unclear.

Response

Explained use of sensor locations in Weighted Localization approach in Section 3.2.

5. Weighted Localization Method Details:

Reviewer Comment: Lack of detail on weight assignment in weighted centroid calculation.

Response

Added details on weight assignment in Section 3.2.

6. Calculation of Sensor Coverage:

Reviewer Comment: Methodology for determining sensor coverage is not detailed.

Response

Added details in Section 3.2.