SHORT-PAPER

Universal Spoofing of Real-World Aircraft Multilateration

OLIVER SENN, Swiss Federal Institute of Technology, Zurich, Zurich, ZH, Switzerland

GIORGIO TRESOLDI

DANIEL MOSER, Armasuisse, Switzerland, Bern, BE, Switzerland

VINCENT LENDERS, Armasuisse, Switzerland, Bern, BE, Switzerland

MARTIN STROHMEIER, Armasuisse, Switzerland, Bern, BE, Switzerland

Open Access Support provided by:

Armasuisse, Switzerland

Swiss Federal Institute of Technology, Zurich

Published: 30 June 2025

Citation in BibTeX format

WiSec 2025: 18th ACM Conference on Security and Privacy in Wireless and Mobile Networks
June 30 - July 3, 2025
VA, Arlington, USA

Conference Sponsors:
SIGSAC

Universal Spoofing of Real-World Aircraft Multilateration

Oliver Senn
ETH Zurich
Zurich, Switzerland
oli.senn@bluewin.ch

Giorgio Tresoldi
OpenSky Network
Burgdorf, Switzerland
tresoldi@opensky-network.org

Daniel Moser
Cyber-Defence Campus, armasuisse
Thun, Switzerland
daniel.moser@armasuisse.ch

Vincent Lenders
Cyber-Defence Campus, armasuisse
Thun, Switzerland
vincent.lenders@armasuisse.ch

Martin Strohmeier
Cyber-Defence Campus, armasuisse
Thun, Switzerland
martin.strohmeier@armasuisse.ch

Abstract

As spoofing attacks on GNSS-based aircraft navigation systems become more common in commercial aviation, independent localization methods such as ground-based distributed multilateration are increasingly being adopted for enhanced safety. While previous work has suggested these systems may be susceptible to multi-device spoofing, no successful real-world multilateration spoofing attacks have been documented so far. In this study, we examined the feasibility and potential impact of wireless spoofing on two deployed commercial multilateration systems. Our findings reveal that these systems share vulnerabilities with GNSS-based solutions such as ADS-B, although considerably greater effort is required for a successful attack. Using a testbed with a reception range exceeding 300 km, we evaluated the requirements and constraints for executing such attacks and compared the efficacy of ghost injection, flooding, and trajectory manipulation tactics. These insights can help inform measures to secure existing multilateration systems.

CCS Concepts

• **Networks** → **Mobile and wireless security**.

Keywords

wireless spoofing, multilateration, real-world systems, aviation

ACM Reference Format:
Oliver Senn, Giorgio Tresoldi, Daniel Moser, Vincent Lenders, and Martin Strohmeier. 2025. Universal Spoofing of Real-World Aircraft Multilateration. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2025), June 30-July 3, 2025, Arlington, VA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3734477.3734720

1 Introduction

Accurate live tracking of aircraft is essential for safe navigation and collision avoidance. Modern digital air traffic control (ATC) systems all rely on unauthenticated wireless signals inherently vulnerable to spoofing [5]. To mitigate these vulnerabilities, multilateration (MLAT) techniques based on time-difference-of-arrival (TDoA) have been proposed as a physical-layer backup and are currently on the way to replacing traditional radar systems in many countries [6].

The literature suggests that MLAT systems, although more challenging to attack, may inherit the same vulnerabilities as classical ATC systems [11]. However, up to now, such attacks have only been analyzed in lab settings with non-commercial systems.

In this work, we deploy and investigate the spoofing resistance of two commercial MLAT systems that are used in operational environments. Our findings and contributions are as follows:

- We deploy and test two commercial MLAT systems covering several hundred square miles and demonstrate that previous lab-based attacks are insufficient to successfully spoof real-world commercial systems.
- We develop a novel robust, transferable and universal spoofing attack which works against both real-world deployments.
- We report on novel flooding and trajectory modification attacks on multilaterated aircraft whereas these attacks have previously only been considered in classical GNSS-based ATC settings.

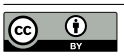
Our findings highlight the gap between theoretical, laboratory-based attacks and their practical applicability, underlining the need for more robust security testing and measures in modern aviation.

2 Background on ADS-B

ADS-B allows aircraft to broadcast their state, including GNSS position, periodically without interrogation from the ground. ADS-B messages are 112 bits long and split into 5 parts. ADS-B is based on the older Mode S downlink, with a dedicated downlink format (DF) of 17. It has 3 bits for the transponder capabilities, and a unique 24-bit transponder code assigned by the International Civil Aviation Organization (ICAO). Lastly, there is a 56-bit payload and 24-bit parity. ADS-B messages contain a Type Code, which is located in the first 5 bits of the payload and indicated the message type. The most common messages are the airborne position and velocity, which are sent at 2 Hz. The aircraft identification message is sent at 0.2 Hz as is the aircraft status. Finally, the target state and status information is sent at 0.8 Hz and the operational status at 0.4 Hz.

Security of ADS-B. There is no authentication or encryption in ADS-B and its datalinks, allowing a variety of attacks, including location spoofing [5]. For example, an attacker can inject ghost aircraft or spoof the location of real aircraft by sending false positions. Such attacks are easy to launch on real ADS-B systems [12].

ADS-B spoofing remains a relevant open problem as surveys and expert interviews with the aviation community demonstrate [15].



WiSec 2025, Arlington, VA, USA

ACM ISBN 979-8-4007-1530-3/2025/06
https://doi.org/10.1145/3734477.3734720

For an overview of the security issues in ADS-B, see [18]. There, many approaches are outlined, including MLAT, Kalman filters, or cryptographic methods. Notable among these is data fusion, e.g., the combination of traditional primary radar and ADS-B to verify the latter [1]. However, the basic use of MLAT has been the most popular and practical verification solution for ADS-B and ATC, both in the literature and in commercial products deployed [2–4, 10, 13].

3 System and Threat Model

3.1 Aircraft Multilateration

Our system model considers an aircraft multilateration system (MLAT). MLAT has been widely presented as a solution to spoofing attacks on ADS-B by independently verifying the origin of ADS-B messages [2, 3, 10]. It is replacing traditional radar systems across the Western world [6]. MLAT requires 4 or more ground receivers providing timestamps for each received aircraft message with very high precision of a few nanoseconds. To achieve this precision, it is necessary to synchronize their clocks, e.g. using GPS.

In hyperbolic localization, multilateration is achieved in two different steps, the ranging and the lateration step. The range R can be calculated as follows: $R = v \cdot T$, where v is the wave speed (close to the speed of light in air) and T is the wave propagation time. We can then estimate the ranges based on the time-difference-of-arrival (TDoA) $\Delta_{i,j}$ of a signal at sensors i and j as

$$\Delta_{i,j} = T_i - T_j = \frac{R_i - R_j}{v}$$

The second step is lateration. Given the above equation and known sensor positions (x_i, y_i, z_i), the position (x, y, z) of the aircraft to be localized can be estimated by calculating $(\hat{x}, \hat{y}, \hat{z})$ such that

$$(\hat{x}, \hat{y}, \hat{z}) = \arg\min_{x,y,z} \sum_{i=1}^{n} [|\vec{p}_i - \vec{p}| - R_i]^2$$

with

$$|\vec{p}_i - \vec{p}| = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2}$$

Here, n is the number of receivers. The resulting set of equations is nonlinear and must be solved numerically in real time. The calculations can done for example using linear least squares [7].

3.2 Threat Model

We assume a motivated threat actor attacking a deployed MLAT system used for ATC to disrupt it with one or more spoofed aircraft. The attacker has knowledge of the locations of at least a subset of MLAT ground stations and the ability to send wireless signals over a line of sight channel to them using a software-defined radio (SDR). These assumptions are reasonable: ground stations are typically in exposed positions for maximum coverage, SDRs cheaply available, and the structure of aviation protocols widely known.

We assume that the attacker is controlling multiple devices synchronized in time at multiple locations. The attacker injects consecutive time-synchronized messages, resulting in a legitimate path calculated by the MLAT system. As radio signals travel at the speed of light, a delay of 1 μs equals nearly 300 m error. This implies the need for nanosecond-level synchronization precision between the attacking devices to spoof locations to a few meters accuracy. We assume that the attacker synchronizes the clocks of the multiple devices using GPS such as proposed in [11]. This assumes a higher hardware cost (around 1500 USD per targeted receiver in our case) and additional skill and effort in strict site selection and synchronization compared to basic ADS-B spoofing. It is similar to more complex GNSS spoofing scenarios [16].

Table 1: Capabilities of the two real-world MLAT systems.

	Receive ADS-B	Receive Mode S	Receive FLARM	MLAT Mode S	MLAT ADS-B	Verify Positions
Man. A	✓	✓	✓	✓	✗	✗
Man. B	✓	✓	✗	✓	✓	✓

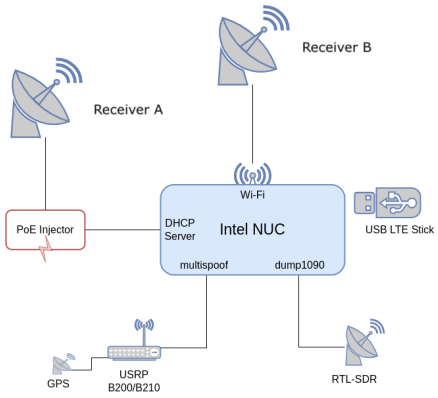


Figure 1: Complete experimental setup.

4 Experimental System Deployment

To test wireless spoofing attacks in the real world, we set up two commercial MLAT systems with 9 ground stations spread at five locations covering an area of several hundred square miles. We anonymize the systems at this stage; both companies have acknowledged the attack but fixing it will take time, as the issue is fundamental to MLAT and not specific to their systems.

4.1 MLAT Systems

We use two commercially available MLAT systems in their September 2023 versions, henceforth called Manufacturer A and Manufacturer B. We deployed five receivers from Man. A and four from Man. B. at five suitable locations on premises of universities. Table 1 details the two systems' capabilities, which include several different ATC technologies. The MLAT receivers are connected via internet to a central station performing the calculations.

4.2 Attacker Setup

4.2.1 Hardware. For each MLAT receiver, we deploy a dedicated attacker device: a PC and a USRP with GPS. All devices are controlled by a Master PC, enabling each USRP to send synced messages to the target receivers. We use cost-effective Intel NUC 11 Pro Minis with an Ubuntu OS, LTE connectivity, and remote restart capabilities. We use the USRP B200 and B210 from Ettus Research with GPSDOs for accurate timing. The two commercial systems are connected to the NUC for an efficient test setup (see Figure 1).

To perform attacks over-the-air, we consider the legal and safety implications, as the 1090MHz channel is licensed only for certified

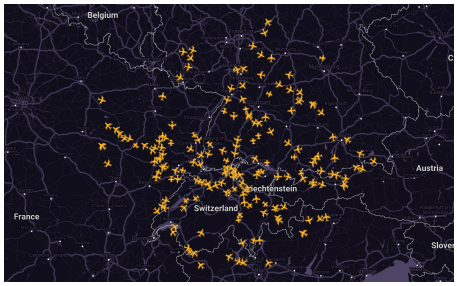


Figure 2: Full range of our setup of System A.

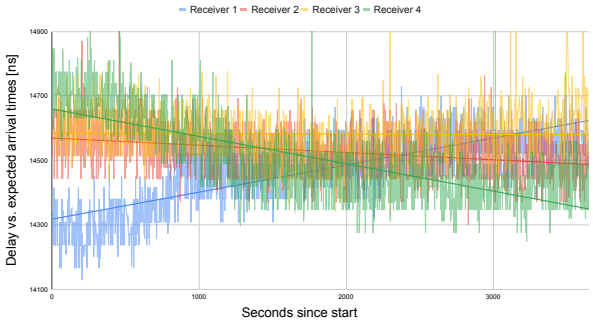


Figure 3: Timing delay of messages sent to four receivers.

transponders. We use Faraday cages, inside which the attack device is sending. The receiver has an antenna inside and outside the box, connected with a splitter. This setup allows us to receive both the spoofed and real signals at the same time. We use the STE3000 RF shielded test enclosures from Ramsey Electronics.

4.2.2 Software. To control the synchronized experiments, we write glue code using Python, shell scripting and autossh. To generate the spoofing targets, we kindly received the original code from the authors of [11], which for safety reasons is not openly available.

4.3 System and Attack Setup Validation

More generally, MLAT capabilities depend on three parameters:

(1) The **number of receivers** who receive the same message. If we need to calculate the aircraft's altitude, 4 receivers are required, otherwise 3 suffice.
(2) The **position of the aircraft in relation to the receivers**. The closer an aircraft is to the center of the cluster of receivers, the better the expected result, assuming that the aircraft is within line of sight of the receivers.
(3) The **geometry of the receivers**. The cluster of receivers should be distributed over a plane. If receivers are in line, it will lead to poor results.

Considering these parameters, we first establish a good operating performance of both systems in a realistic, i.e. large-scale, setting in an urban area around an airport. Figure 2 shows the range of visible aircraft with System A. We receive aircraft in a range of approx 300 km around our deployment. Aircraft crossing the center of the setup are multilaterated. For System B, the overall reception range is slightly reduced as its smaller antennas were less effective with our setup and four instead of five receivers were deployed.

We also validate the tight time synchronization and precision necessary to perform the attack. For this analysis, we received access to nanosecond-level timestamps for each message from Man. A. We compare the time at which the message arrived at the receiver to the time that we calculate as the correct sending time, which is given to the USRP. We find a standard deviation of about 64 *ns*, which is in line with 60 *ns* observed by [11].

We then compare the measured timings of several targeted receivers to see how much they individually vary from their expected timings. In Figure 3 we can see the results of this experiment, which we let run over 60 minutes. We observe that the timing between different receivers is generally accurate, but there is clock drift that we can only see over a longer time-frame, illustrated by receiver 1. Overall, we see that the combined clock drift of the attacker device and receivers remains within 150 *ns*, which at the speed of light results in about 45 meters of error in the worst-case scenario, which is well within the requirements for MLAT systems.

5 Towards a Universal MLAT Spoofing Attack

Equipped with two working MLAT systems and a distributed attacker setup, we went on to assess the success rate of different spoofing attack scenarios. The most fundamental attack against a MLAT system is to inject a ghost aircraft in the recognized air picture. However, to our surprise, despite our fully synchronized and validated attacker setup, we initially failed against both System A and B to inject a ghost aircraft. This result implies that commercial MLAT systems exhibit additional checks or different algorithms than what is typically assumed in the literature [11].

5.1 Why Classical Multi-Device Spoofing Attacks Fail in Practice

To understand why a classical multi-device spoofing attack fails in practice, we need to better understand the behavior of the MLAT systems. Unfortunately, as we were dealing with black-box systems, we received no feedback on the actual MLAT calculations and algorithms themselves. Therefore, we had to reverse engineer the behavior of both systems to identify why the ghost aircraft injection attack fails. We came to the following conclusion for each system:

System A. In System A, ADS-B messages were not used for MLAT calculations at all. Instead, the MLAT system relies purely on Mode S messages transmitted by aircraft as responses to ground radar interrogations, which were never considered in previous research [11].

System B. While System B did actually conduct MLAT on ADS-B messages, it also required higher rate Mode S messages for timely initial target acquisition, explaining why our attack failed.

5.2 Universal MLAT Spoofing Requirements

Based on the failed attack and our reverse engineering work, we identify the requirements for a working MLAT attack, that is *robust* and *universal*, i.e., *transferable* between different real-world systems:

(1) **Synchronization**: The TDoA $\Delta_{i,j}$ of a message must for all receivers appear as if the signal was transmitted from the spoofed location.

Table 2: Necessary messages of the universal MLAT attack.

DF	Bits	Type	This work	[11]
0	56	Short air-air surveillance (ACAS)	✓	✗
4	56	Surveillance, altitude reply	✓	✗
5	56	Surveillance, identity reply	✓	✗
11	56	All-Call reply	✓	✗
17	112	Position (ADS-B)	✓	✓
17	112	Identification (ADS-B)	✓	✓
17	112	Velocity (ADS-B)	✓	✓

(2) **Isolation**: Each receiver only receives signals from the intended attack device. This is not an issue in practice as typically receivers are not close.
(3) **Completeness**: All aircraft messages (not just ADS-B position messages) used by the MLAT system must be correctly produced, providing plausible semantics and trajectory (speed, heading and altitude).
(4) **Geometry**: MLAT systems are subject to strict geometric conditions. These must be taken into account by the attacker.

Requirements (1) and (2) were explicitly or implicitly discussed in prior work on MLAT attacks. However, completeness and geometry have so far been ignored, leading to the observed failures of attacking MLAT systems in practice.

5.3 Design of a Universal MLAT Spoofer

As mentioned in requirement (3), commercial MLAT systems do not, or not exclusively, rely on ADS-B as assumed by prior work. Instead, the older Mode S technology, which uses interrogation pulses and replies, is still widely used in ATC and also the examined MLAT systems. In addition to the three long ADS-B message types (*position*, *velocity* and *identification*) used by [11], we additionally identify four short Mode S message types that need to be accurately provided to successfully spoof a commercial MLAT system: *short air-air surveillance*, *altitude reply*, *identity reply*, and *all-call reply*. We list all necessary messages in Table 2.

Requirement (4) of the universal MLAT attack concerns the so-called geometric dilution of precision (GDOP), which roughly describes the area where MLAT — and a potential attack – is effective [14]. GDOP relates the relationship between errors from TDoA measurements and errors of the actual localization estimate, as follows (a concrete description is found in [8]):

$$\Delta Location\ Estimate = \Delta TDoA\ Measurements \cdot GDOP$$

We calculate the geometric attack boundaries for our five receiver locations, by separating the area into a grid and calculating the GDOP for individual points, assuming an altitude of 10,000 m, the typical cruising altitude of aircraft. For GPS, which uses GDOP as a metric, areas with values above 20 are considered poor quality. Thus, we target our universal attack in areas of 15 and below.

5.4 Universal Spoofer Verification

Finally, we verify the effectiveness of our new universal spoofer. With System A, a ghost aircraft spoofing now succeeds in under five seconds from sending the first message until we see the first MLAT result in the target location. Indeed, the very first message is already successfully multilaterated, illustrating the accuracy of the setup. Figure 4 shows the result of this preliminary evaluation against a pre-calculated GDOP map. Red triangles show points, where we were able to successfully spoof a multilaterated aircraft and blue dots show unsuccessful locations. We see that theoretical and practical boundaries align but are not fully congruent.

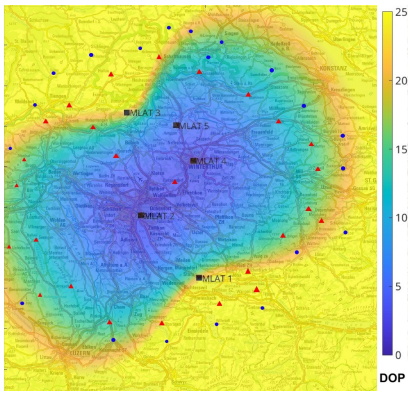


Figure 4: GDOP map (100x100 km) for our MLAT setup, with overlay of MLAT attack boundaries. Red triangles denote successful attacks, blue dots unsuccessful attacks.

6 MLAT Attack Evaluation

We examine the performance and boundaries of the universal MLAT spoofer on the two targeted systems for (i) a ghost aircraft attack, (ii) a flooding attack, and (iii) a trajectory modification attack.

6.1 Ghost Aircraft Attack

We first focus on the ghost aircraft attack referred to in the literature [5]. MLAT has been widely touted as the main defense against such ADS-B spoofing [2–4, 10, 13]. We test both *point spoofing*, where an aircraft is simply stationary, and the more complex *track spoofing* of a complete aircraft trajectory across the MLAT coverage.

We calculate the *localization error* to measure precision. That is, we inject a ghost aircraft and compare its intended position at the time a message is sent with the position that MLAT is calculated from that message. We use the planar or 2D localization error, as the altitude calculations from MLAT are prone to errors in typical setups where the receivers on the ground are all on a similar altitude. Secondly, we examine how precise the synchronization between attacker devices needs to be to attack real-world MLAT systems. We artificially add delays to several receivers, thus making their synchronization worse and measure the outcome.

6.1.1 Attack Accuracy. To analyze our attack accuracy, we use a single track between two points in the accurate GDOP area. We run the experiment for 13 minutes and around 3,000 messages, which resulted in about 650 positions calculated by System A. The ECDF of this experiment results in 80% errors below 200 meters.

When performing the same experiment on System B, out of the 3,000 messages, around 2,600 are seen by three or more receivers. The resulting ECDF shows that the error of about 90% of received messages is below 200 m. Interestingly, the MLAT uncertainty on the System B's website during this experiment, which may take

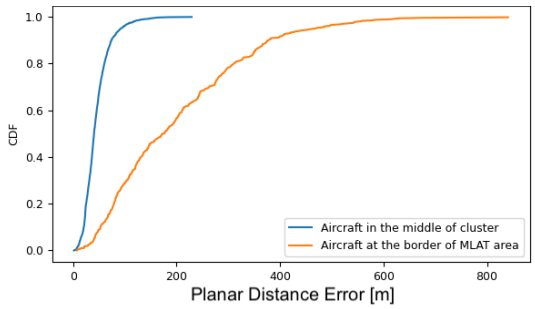


Figure 5: Distribution of planar localization error when spoofing in the center of the cluster vs. at the border.

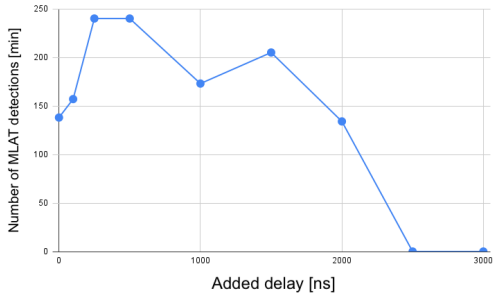


Figure 6: Number of MLAT results successfully calculated by System B when delay is added to two senders

into account additional receivers not controlled by us, showed 300 - 500 meters of uncertainty, while in actuality, the displayed results were highly accurate compared to our ground truth.

Notably, both manufacturers confirmed that they could not distinguish spoofed from real messages in their systems using TDoA.

6.1.2 GDOP Influence. To examine the GDOP influence, we choose a set of two coordinates: one in the system's center with low GDOP and one close to the attack border, where we still get MLAT results, with higher GDOP. We perform point spoofing for both locations on System A. Both tests ran for 11 minutes, during which about 2,600 messages were sent. For lower GDOP, 1,263 messages were seen by at least 4 receivers and multilaterated. In the high GDOP test this number dropped to 461 messages, indicating that many messages were dropped due to an error above the system's tolerance. Figure 5 shows the ECDF of the two experiments, illustrating the importance of positioning the spoofing targets in an attack.

6.1.3 Synchronization Error Tolerance. To test the synchronization limits, we vary the delay added and send 240 Mode S messages per minute and test case. Surprisingly, for System A, we still get MLAT results, even if the added delay is very high (up to 75,000 ns, which equals a distance of 22 km).

We then perform the same attack on System B (see Figure 6). Once the added delay reaches 1,500 ns, the verification feature flags the aircraft's position as faulty. After 2,500 ns, the MLAT results are discarded. At the speed of light, these 1,500 ns translate to a difference of around 450 m, where the system recognizes that the timings do not add up with the broadcast ADS-B position.

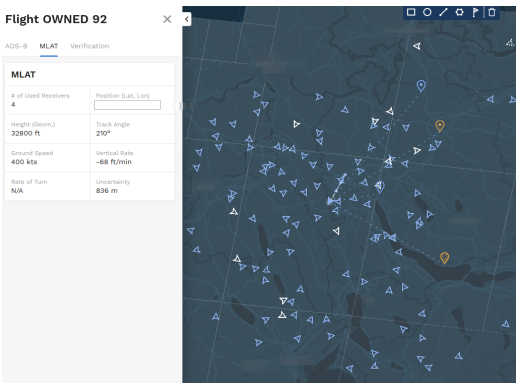


Figure 7: Flooding attack against MLAT System B.

6.2 Flooding Attack

The flooding attack consists of spoofing as many ghost aircraft as possible at the same time. This attack represents a general threat to commercial aviation [9], in particular near airports where air traffic control could lose situational awareness due to the mass of false information. In the following, we investigate the feasibility of flooding the MLAT system with ghost aircraft.

6.2.1 Theoretical Limits. We first consider the physical channel limits. ADS-B messages consist of an 8 μs preamble and 112 μs of data, resulting in a total message length of 120 μs. If we consider a 100 km distance for a MLAT attack, we must add a delay of about 300 μs. Thus, if we want to make sure that none of the messages overlap, we should have about 500 μs between each message. This implies that we are limited to 2,000 messages per second. If we want to make all aircraft look as close to real aircraft as possible, we must further transmit all relevant ADS-B message types, which means sending roughly 5 per aircraft and second (see Section 2). This results in a theoretical limit of at most 400 aircraft we can spoof simultaneously. If we add the four Mode S message types required for initial acquisition, this is lowered even further.

6.2.2 Proof of Concept. The flooding attack works as intended for both point and track spoofing on both systems. As Manufacturer A's map uses exclusively ADS-B messages for display if available (and not multilaterated messages), the visualization is the same as in a traditional ADS-B-only flooding attack. Flooding Man. B's system offers a better visualization. Fig. 7 shows the map during the attack. An air traffic controller, who is faced with such a situation and only the information given in this radar picture, would have a very difficult time separating the real from fake aircraft.

6.3 Trajectory Modification

We now modify the trajectory of a legitimate multilaterated aircraft track. As the legitimate aircraft moves along its intended actual trajectory, the spoofed attack track slowly moves into a different direction. We aim to perform a smooth takeover of the original track and modify it by diverting the spoofed track by 15 degrees. First, we attack our own spoofed aircraft, to control both the existing and attack trajectories of the aircraft. We use a modified version of the ghost aircraft attack and specify two aircraft with the same

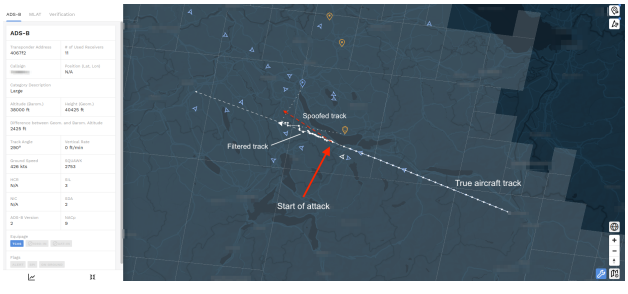


Figure 8: Trajectory modification attack on a real aircraft.

identifiers and starting location. We specifically do this to imitate a real attack, where the receiver would suddenly see twice the amount of messages from the targeted aircraft. The MLAT track displayed moves back and forth between the two different tracks and is not verified. While that serves as evidence of an attack, the system cannot identify the problem and separate the tracks.

Next, we perform this attack against a real aircraft track. We pick an aircraft at the border of the MLAT area and send messages using its ICAO code with a modified position diverting the track by 15 degrees. For simplicity, we can only spoof the airborne position messages as all other messages are provided by the real aircraft.

First, we use a single device to send the wrong ADS-B position. Here, the aircraft moves along its legitimate trajectory, and the true MLAT position is correctly calculated. However, the system does not mark the aircraft as verified, enabling a simple global attack on the verification feature. Next, we send a wrong position for a real aircraft using the synchronized multi-device attack. Figure 8 shows the result of this attack. As before, the verification is removed as soon as the spoofed track is seen by the receivers, and we see a jittery mix of both MLAT tracks on the map.

Challenges and Future Improvements. While not an MLAT issue (but one of radar systems generally), filtering of the aircraft tracks can impact the spoofing success in this scenario as two tracks are competing. Man. A did not use a filter during our experiments, hence the displayed track effectively jumps to the last received position. This means it fully oscillates between both tracks, leading to potentially strong "jitter" depending on the two track distances.

Man. B employed a Kalman filter, which is a black-box setting for our attacker. Here, the track behaves less predictable as illustrated in Fig. 8. The jitter depends (non-exhaustively) on a) update rates and sliding windows used the tracks, b) the frequency and distance of spoofed and real messages, c) the measurement-noise standard deviation that the Kalman filter assumes for each position reading, and d) the process-noise variance that the Kalman filter assumes for the motion model between updates. In our experiment, with similar frequency and growing distance between the laterated tracks, the displayed track oscillates towards their average.

Independent of the settings and the filtering used, the attack can easily be detected by the system – although identifying the true track may still be difficult. For full stealth, the attacker must effectively suppress the real track, using reactive jamming [17] at all MLAT receivers, i.e. identify all Mode S and ADS-B messages with the aircraft identifier and destroy the applied parity check through targeted interference. This raises the difficulty significantly and makes the trajectory modification attack less attractive compared to ghost aircraft and flooding attacks.

7 Conclusion

We deploy two commercial MLAT systems in a real-world setup and show that naive multi-device MLAT spoofing attacks fail to generalize in practice. Instead, an attacker must fulfill geometric and completeness requirements in order to successfully attack such MLAT systems. Based on these insights, we develop a novel robust, universal, and transferable spoofer and successfully use it against both systems. We disclosed our findings to both manufacturers. Manufacturer A plans to use positions from multilaterated Mode S replies and ADS-B positions to cross-validate each other in a future update to improve availability. Other measures are currently not considered. In discussion with Manufacturer B, we found that the attack still looks different compared to real aircraft on the physical layer (beyond timing), which they were subsequently able to identify. We are planning a collaborative effort to design and implement countermeasures to our attack in the future.

References

[1] O. Baud, N. Honore, and O. Taupin. 2006. Radar / ADS-B data fusion architecture for experimentation purpose. 1 – 6.
[2] S. Capkun and J.-P. Hubaux. 2005. Secure positioning of wireless devices with application to sensor networks. In *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, Vol. 3. 1917–1928 vol. 3.
[3] Y. Chen, W. Trappe, and R. P. Martin. 2007. Attack Detection in Wireless Localization. In *IEEE International Conference on Computer Communications (INFOCOM).*
[4] Jerry Chiang, Jason Haas, Jihyuk Choi, and Yih-Chun Hu. 2012. Secure Location Verification Using Simultaneous Multilateration. *Trans. on Wireless Communications* 11 (02 2012), 584–591.
[5] Andrei Costin and Aurélien Francillon. 2012. Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices.
[6] Federal Office for Civil Aviation. 2020. *100 Jahre BAZL.* Technical Report. https://www.bazl.admin.ch/dam/bazl/de/dokumente/Das_BAZL/Studien_Berichte_und_Projekte/broschure_100_jahre.pdf
[7] Mantilla Gaviria and Iván Antonio. 2013. New Strategies to Improve Multilateration Systems in the Air Traffic Control.
[8] R. B. Langely. 1999. Dilution of Precision. In *GPS World*, Vol. 10. 52–59.
[9] Donald McCallie, Jonathan Butts, and Robert Mills. 2011. Security analysis of the ADS-B implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection* 4, 2 (2011), 78–87.
[10] Márcio Monteiro, Alexandre Barreto, Research Division, Thabet Kacem, Jeronymo Carvalho, Duminda Wijesekera, and Paulo Costa. 2015. Detecting malicious ADS-B broadcasts using wide area multilateration. In *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC).*
[11] Daniel Moser, Patrick Leu, Vincent Lenders, Aanjhan Ranganathan, Fabio Ricciato, and Srdjan Capkun. 2016. Investigation of Multi-Device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking.*
[12] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. 2013. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. In *Applied Cryptography and Network Security (ACNS).* 253–271.
[13] Matthias Schäfer, Vincent Lenders, and Jens Schmitt. 2015. Secure Track Verification. In *2015 IEEE Symposium on Security and Privacy.* 199–213.
[14] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2015. Lightweight Location Verification in Air Traffic Surveillance Networks *(CPSS '15).* Association for Computing Machinery, New York, NY, USA, 49–60.
[15] Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. 2017. On Perception and Reality in Wireless Air Traffic Communication Security. *IEEE Trans. on Intelligent Transportation Systems* 18, 6 (2017).
[16] Christopher Tibaldo, Harshad Sathaye, Giovanni Camurati, and Srdjan Capkun. 2025. GNSS-WASP: GNSS Wide Area SPoofing. In *USENIX Security 2025.*
[17] Matthias Wilhelm, Ivan Martinovic, Jens B Schmitt, and Vincent Lenders. 2011. Short paper: Reactive jamming in wireless networks: How realistic is the threat?. In *Proceedings of the fourth ACM conference on Wireless network security.* 47–52.
[18] Zhijun Wu, Tong Shang, and Anxin Guo. 2020. Security Issues in Automatic Dependent Surveillance - Broadcast (ADS-B): A Survey. *IEEE Access* 8 (2020).