Global Incidents of Aviation Spoofing in 2024-2025 Detected with Automatic Dependent Surveillance Broadcast

Sherman Lo, Zixi Liu, Lyla Ibrahim, Yu Hsuan Chen, Dennis Akos, Todd Walter, *Stanford University*

Biography (ies)

Sherman Lo is a senior research engineer at the Stanford GPS Laboratory and the executive director of the Stanford Center for Position Navigation and Time. He received his Ph.D. in Aeronautics and Astronautics from Stanford University in 2002. His research focuses on navigation robustness and safety.

Zixi Liu is a Ph.D Candidate in the Stanford GPS Laboratory.

Lyla Ibrahim is an undergraduate majoring in Computer Science at Stanford University.

Yu-Hsuan Chen is a research engineer at the Stanford GPS Laboratory. He received his Ph.D. in Electrical Engineering from National Cheng Kung University, Taiwan in 2011.

Dennis Akos is a Professor in the Department of Aerospace Engineering Sciences at the University of Colorado Boulder.

Todd Walter is professor of research in the Department of Aeronautics & Astronautics. He directs at the Stanford GPS Laboratory. He received his Ph.D. in Applied Physics from Stanford University.

1. INTRODUCTION

Recent events have made it clear that aviation can no longer ignore the issue of GNSS spoofing. While flights are being affected near conflict regions such as Syria, Israel and Russia, these events are not confined to just those regions but are more commonplace. Crowdsourced data from automatic dependent surveillance broadcast (ADS-B) has made clear that there are many other areas being regularly affected by GNSS spoofing. And since the data is derived from ADS-B, this means that aviation GNSS systems are being affected. This paper examines recent GNSS spoofing incidents that we have found around the world using ADS-B. It examines the different types of trajectories seen and some of characteristics of each.

First, the paper will overview the various unique regions and incidents of GNSS spoofing that we have detected. For example, in Russia, there are many regions that exhibit spoofing. One region is around Smolensk where there is a large area of spoofing that results in aircraft showing that it is flying in circles around Smolensk (Lo 2024). There is spoofing in the Black Sea that been results in aircraft appearing to be on approach to airports in Crimea. And in Kaliningrad, there is clear evidence of spoofing with multi-frequency jamming. The eastern Mediterranean is another area with well-known incidents where aircraft are spoofed to either Beirut or Cairo airport. But GNSS spoofing is more widespread than just conflict regions. For example, there are persistent spoofing events in Myanmar and India-Pakistan border.

The paper then examines specific event regions and the characteristics to the spoofing in these areas. From the data, we examine the characteristics, persistence and consistency of the spoofing. The analysis helps address the questions: 1) “What different spoofing patterns are being used?” 2) “Is it always on?” 3) “Does it change over time?” We also examine means of better understanding the impact of the spoofing such as the region and frequencies affected. The data from ADS-B is limited for this purpose due to many factors such as its use of GPS L1 only and gaps in ground coverage. Under spoofing, the reported (i.e. spoofed) positions do not provide the true location of the aircraft. Hence, we use other means and sources to supplement the ADS-B data to better understand the area and frequency of the interference. The paper uses of radiofrequency interference (RFI) events coming from Kaliningrad to demonstrate this.

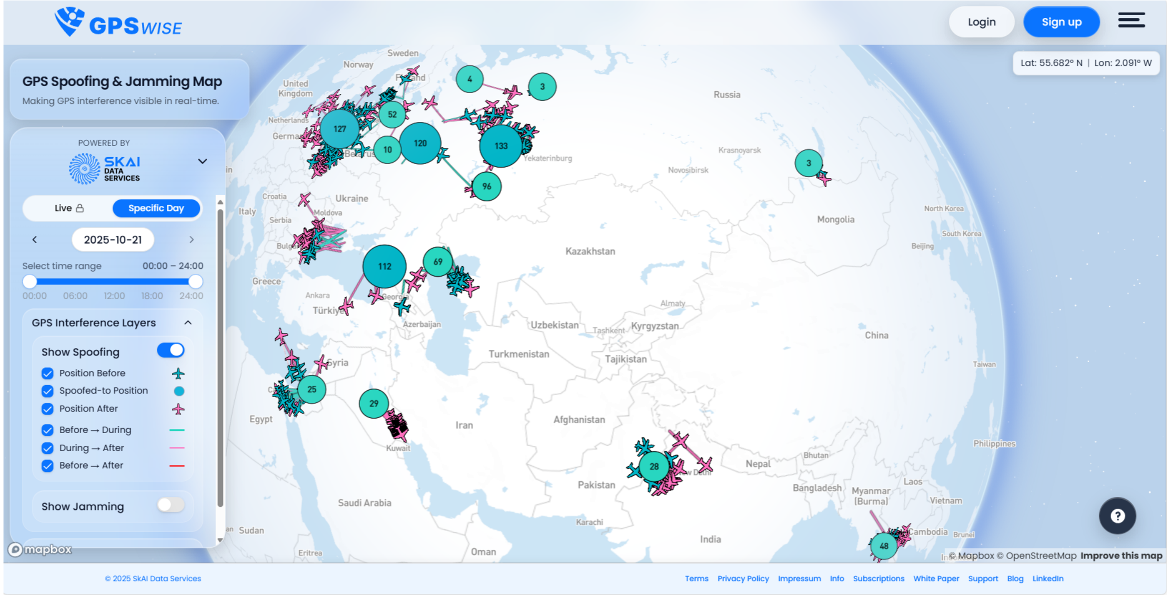
2. BACKGROUND

The widespread use of GNSS has made the ability to detect GNSS RFI more urgent. It has also aided in its detection. This is well reflected in aviation. The widespread use of GNSS in aviation provide many capabilities for efficient operations. At the same time, aircraft broadcast of its GPS derived locations, used for air traffic control and situational awareness, through automatic dependent surveillance broadcast (ADS-B) (RTCA 2003) (RTCA 2004) has provided a very useful means of monitoring GNSS RFI (GPS L1 C/A). ADS-B provides regular broadcast of aircraft GNSS derived positions (2 Hertz), velocity and altitude as well as some basic integrity and accuracy metrics. Because it is broadcast in the clear, it can be received and decoded by anyone and so there are several providers of crowdsourced ADS-B information such as OpenSky, ADSBExchange, AirNav and airplanes.live. Additionally, it has significant coverage since nearly every commercial aircraft broadcast it while operating. As these aircraft are generally at high altitude (above 10000 meters), the GNSS receiver onboard has a large radio horizon for where it may be affected by ground-based GNSS RFI signal. However, there are a few important limitations. ADS-B currently only uses GPS L1 C/A and has very limited information on GPS performance. Note that in this paper, we will often say ADS-B helps detect GNSS spoofing as a shorthand but, more accurately, it can only be used to detect GPS L1 C/A spoofing. Furthermore, coverage, especially for crowdsourced providers, is limited to locations where there are ground stations that receive and share the ADS-B transmissions. Also, crowdsourced providers often provided aggregated and processed, rather than raw, information from the ADS-B messages which can obscure some useful information.

2.1 ADS-B Data for Spoof Detection

ADS-B has been used for both jamming and spoofing detection of GNSS for a few years (P. Lukeš 2020). It gained visibility with gpsjam.org, the first widely used and publically available tool for seeing areas of GPS degradation (interference) using ADS-B. Much work has been done refining techniques using ADS-B for GNSS interference detection. Some means and practices are discussed in (Liu 2023, Liu 2024) and generally uses integrity and accuracy metrics to find areas where performance is degraded. Soon other tools such as gpswise.aero, developed by SkAI data services and the Zurich University of Applied Sciences (ZHAW) (https://spoofing.skai-data-services.com/) (ZHAW 2024) and rfi.stanford.edu, developed by the Stanford GPS Laboratory, were made to detect and display both jamming and spoofing events and regions using ADS-B data. These tools have processing to help improve detection as well as data display. For example, different algorithms and processes used by rfi.stanford.edu for our spoofing and jamming detection have been presented in (Liu 2025B, Liu 2024, Liu 2025A). This section briefly discusses spoof detection using ADS-B.

There are several means of using ADS-B derived data to detect spoofing. One method relies on finding clusters of different aircraft at roughly the same location and time. This approach was initially used by gpswise. Another method is to detect spoofing using position changes (jumps) and/or speed. Reported position changes that significantly exceed a reasonable flight speed of a commercial aircraft should indicate an incorrect or spoofed position. Both gpswise and rfi.stanford.edu use large position jumps from ADS-B data for spoof detection (Liu 2024). Examples are seen in FIGURE 1 and FIGURE 2 which shows spoofing detected by gpswise and rfi.stanford.edu, respectively. As most ADS-B sources are commercial aircraft, the flight speeds at cruise are within a very narrow range – typically about 500 knots (kts) and hence feasible position change rates and speeds are limited. Additionally, landing speeds are around 200 knots providing a minimum speed which should only be seen around airports. Hence too low a speed can be an indication of spoofing for a particular aircraft and condition. For example, the position changes seen in the spoof circle patterns seen in Smolensk translate to a flight speed of about 200 kts. This is too slow for a commercial aircraft en route (Lo 2025). A commercial aircraft only maintains this speed during landing operations. Using low speeds as an indicator requires a deeper understanding and analysis. Aircraft on approach and landing fly much slower and there are aircraft that can fly very slowly or even at zero velocity (e.g. helicopter). Another method that can be used is to compare broadcast barometric and GPS (geometric or height above ellipsoid (HAE)) altitude over time. Usually there is an offset between the two altitudes and this offset may change in time and location but it should be gradual. If there is a large change in that difference, that could be an indication of GPS spoofing as the geometric altitude may be affected but the baro-altitude should not be affected. FIGURE 3 shows an example of this. Note that the reported altitude in ADS-B is usually baro-altitude. GPS altitude may also be provided in some position reports but it is generally derived from the baro-altitude using the velocity report. The velocity report provides the offset between geometric and barometric altitude. Another method is examine changes in ADS-B position accuracy and integrity quality metrics known as navigation accuracy and integrity categories (NAC and NIC), respectively (Lo 2025). These spoof detection methods, using altitude and position quality, are not, to the best of our knowledge, currently implemented in any of the discussed ADS-B based spoofing visualization tools.



GPS Spoofing & Jamming Map

Making GPS interference visible in real-time.

Live | Specific Day

2025-10-21

Select time range 00:00 – 24:00

GPS Interference Layers

Show Spoofing

☑ Position Before

☑ Spoofed-to Position

☑ Position After

☑ Before → During

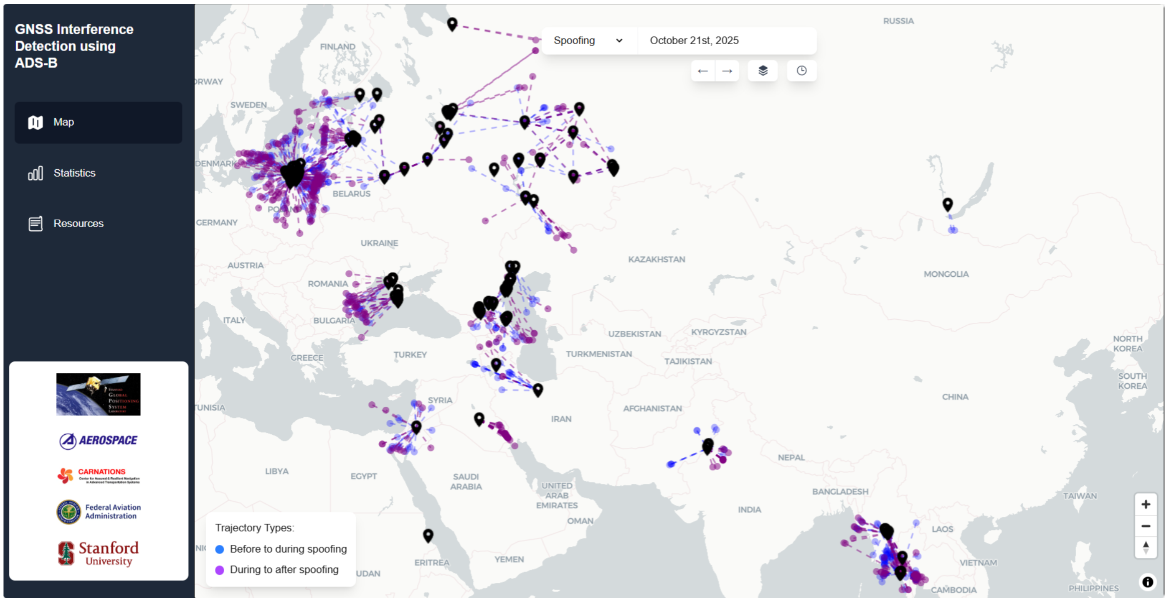
☑ During → After

☑ Before → After

Show Jamming

Lat: 55.682° N | Lon: 2.091° W

FIGURE 1. *GNSS spoofing map with detected spoofed to locations flagged and ADS-B positions before and after jump to spoofed position indicated. October 21 2025, from gpswise.aero*



GNSS Interference Detection using ADS-B

Spoofing | October 21st, 2025

Trajectory Types:

● Before to during spoofing

● During to after spoofing

FIGURE 2. *GNSS spoofing map with detected spoofed to locations flagged and ADS-B positions before and after jump to spoofed position indicated. October 21 2025, from rfi.stanford.edu*

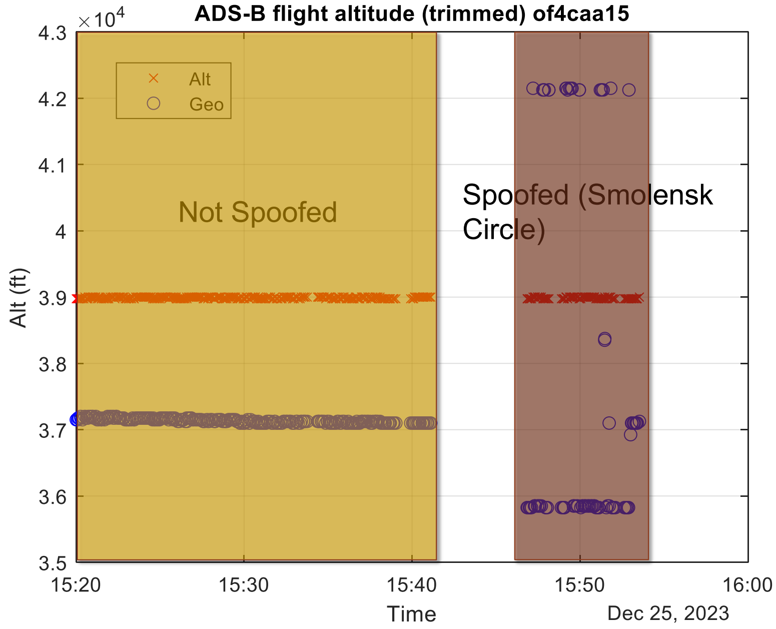


FIGURE 3. *Comparison of barometric altitude (Alt) and GPS altitude (Geo) from ICAO 4CAA15 (Mongolian Airlines 787-9) ADS-B prior to and the aircraft being spoofed to Smolensk on December 25 2023*

2.2 Detected Spoofing using ADS-B

Our automated detection utilized on rfi.stanford.edu has allowed us to use ADS-B data to detect many potential instances of spoofing around the world. From that we can quickly identify spoof regions and events as well as trends over time. For example, rfi.stanford.edu, as seen in FIGURE 2, shows detected events indicated by a location marker, as well as the reported positions of the aircraft prior to and after jumping to the spoof locations. The result shown for October 21 2025 has many regions where spoofing was detected including Russia, Myanmar, India/Pakistan, Iran, etc. with generally multiple events in each region. Going through different dates on rfi.stanford.edu, it is clear that many of these events that are persistent.

Russia has perhaps the longest history of GNSS spoofing events. However, the number, geographic diversity and complexity of the events has grown over time. The figure shows that Russia has multiple separate spoofing events in different areas. There are likely many more events but these are not visible as there is limited availability of ADS-B data in Russia due mostly to not having many ground stations. The detected events range geographically from being in throughout European Russia (Kaliningrad, next to Poland, Smolensk, Moscow, Crimea, Georgia) to southern Asia and Central Asia (Outer Mongolia). rfi.stanford.edu also allowed us to examine past data also to see how the number of events has grown over time.

Additionally, the tool also has helped us find and study other spoofing incidents that were previously not publicly reported. For example, we have seen incidents of spoof circles near the India-Pakistan border as well in Myanmar. These regions have persisted and show multiple distinct events daily. These will be discussed in Section 3. Clearly spoofing is not a problem that is going away.

3. SPOOFING OBSERVED

This section overviews the spoofing found using ADS-B data and rfi.stanford.edu in several regions around the world. Some, like Russia, have had spoofing for many years but this threat has both grown and evolved. Other regions like Myanmar and India-Pakistan only started exhibiting spoofing in around 2024.

3.1 Russia Spoofing

Persistent on-air GNSS spoofing has been seen in Russia since at least 2018 (C4ADS 2019) with the number of events increasing rapidly since the 2023 (Lo 2025). Entering the third year of the Russia-Ukrainian conflict, we are seeing even more spoofing events, particularly deeper inside Russia (central Russia). These events have several different trajectories (patterns) with circles, semi-circles to straight path, hendecagon (11 sided polygon) being commonly seen. FIGURE 5 shows a sample of these incidents from March 2025. Four separate event regions are highlighted with different spoof trajectories shown and the approximate diameter spanning the pattern. Each spoof pattern is reasonably large with diameters from 2 to 11 kilometers (km). The trajectories are tracks that move along the pattern. The size and speed of these trajectories indicates that the spoofing is targeted at larger air vehicles such as cruise missiles or fixed wing drones rather than small consumer drones. For example, the spoofing to Smolensk exhibit a speed of approximately 200 kilometers per hour (kph). This is comparable to the cruise speed of a drone such as the Shahed-136 which cruises at 185 kph and much slower than a commercial aircraft which cruises at about 900 kph. The size contrasts with the smaller spoof trajectories seen in Myanmar or India-Pakistan. In addition to the different spoof trajectories observed in these events, there are some changes in the pattern over time – either in their location or with different trajectories. For example, the spoofing in the lower right corner of FIGURE 5 shows two of the same hendecagon pattern but offset in their center location. However, the patterns, except for Kaliningrad, tends not to change nor does the spoofed locations shift very much over time. We have not analyzed many of these affected areas in depth as we have limited ADS-B information available. Given that there are very few aircraft travel that traverse Russia, in many regions there have significant time gaps in ADS-B observations. So it is not clear if the spoofing and changes are gradual or if they represent the spoofing being turned off and reset to a new position. Additionally, spoofing may be accompanied by jamming which can further obscures the nature of the spoofing by affecting the ADS-B output.

Kaliningrad is an area of interest that we studied further since there is good ADS-B coverage and it is close to GNSS receiver assets (in Poland) that could provide more insight into the nature of the RFI. The Kaliningrad area had, in the last few years, occasional jamming and spoofing. Jamming became more regular and starting around November 9 2024, it also started exhibiting regular spoofing and so we had both types of GNSS RFI. This activity intensified in the month following November and has persisted. The Kaliningrad area, particularly on the western side (Poland), is overflown by many commercial aircraft and many of these aircraft experience jamming with some also experiencing spoofing. FIGURE 4 shows a map from rfi.stanford.edu around Kaliningrad on March 9 2025. It marks the spoofed locations (location indicator) and ADS-B positions before and after the jump to spoofed position indicated of the region. The insert shows a commercial aircraft (ICAO A7-ALH, Qatar Airways, Airbus 350) that flew in the region on that date and its indicated ADS-B locations during the period it was spoofed to Kaliningrad. The spoofed trajectory starts at the top of the circle and goes about 270 degrees before going to a straight line heading northwards. This spoof trajectory is similar to the one seen in Crimea in FIGURE 5 (lower left) and perhaps it is meant to simulate a final to an approach. Other different spoofing events and trajectories were found in the Kaliningrad data from that date. The RFI in this locale is examined more in Section 4.

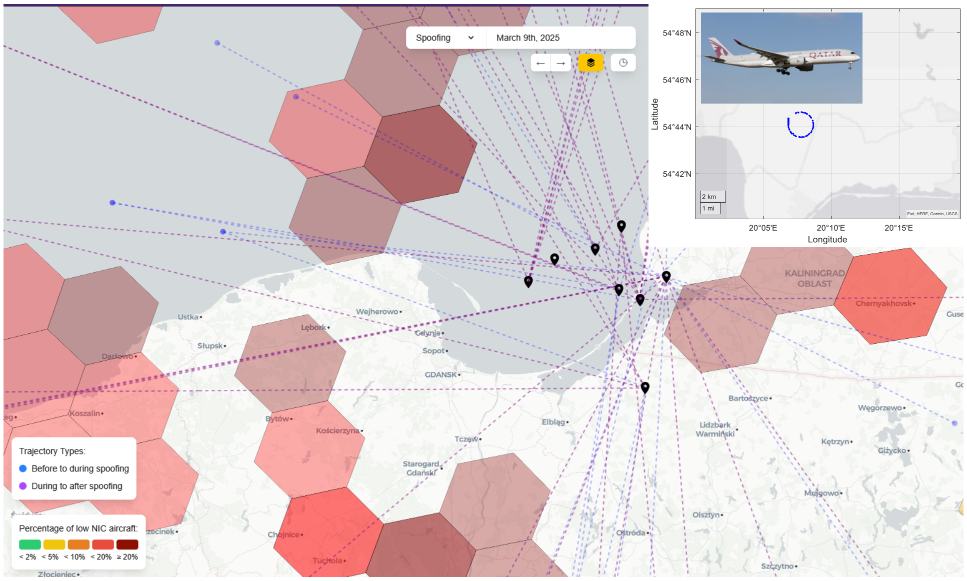


FIGURE 4. *Detected spoofing around Kaliningrad on March 9 2025. Spoofed locations flagged and ADS-B positions before and after jump to spoofed position indicated. (rfi.stanford.edu). Insert shows Qatar A350 and its spoofed locations from ADS-B.*

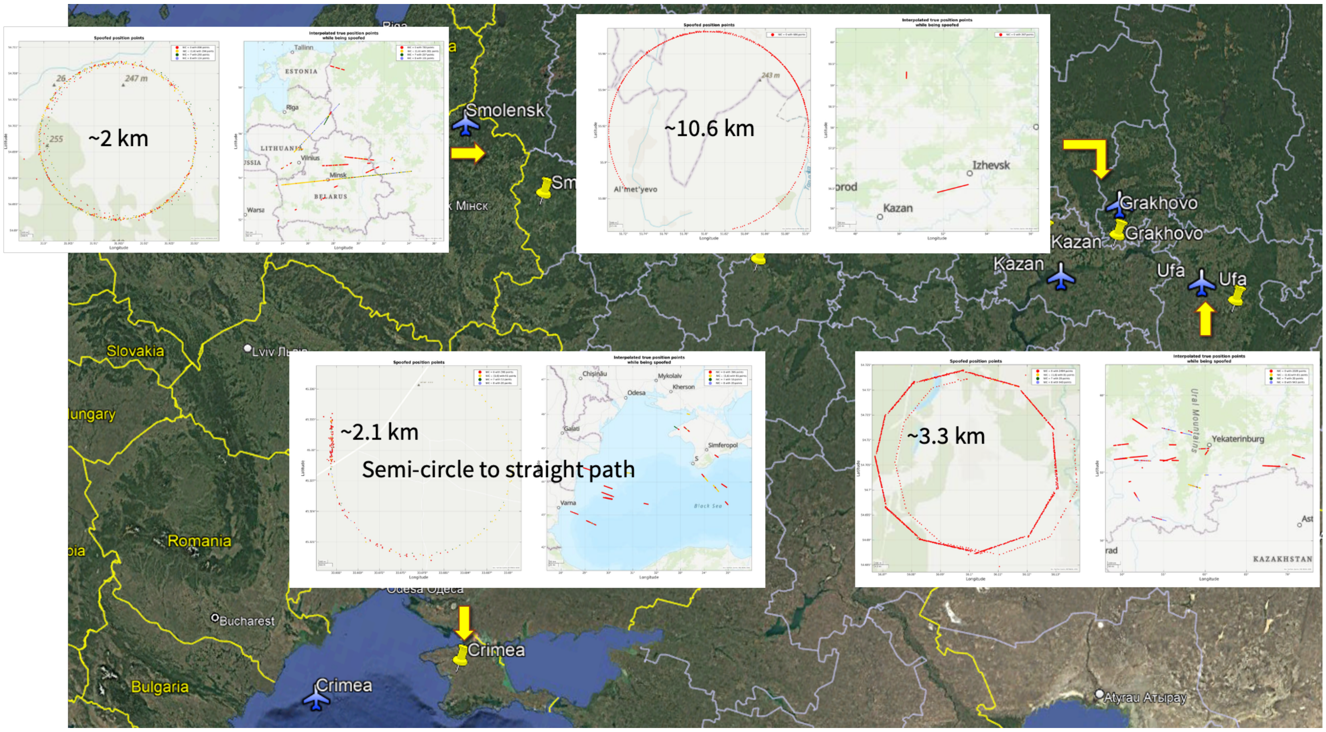


FIGURE 5. *Other spoofing seen in Russia, March 2025. 4 distinct events are shown in the inserts with the rough diameter of the largest spoof "circle" in each event (left plot) and estimated positions during spoof (right plot)*

3.2 Myanmar Spoofing

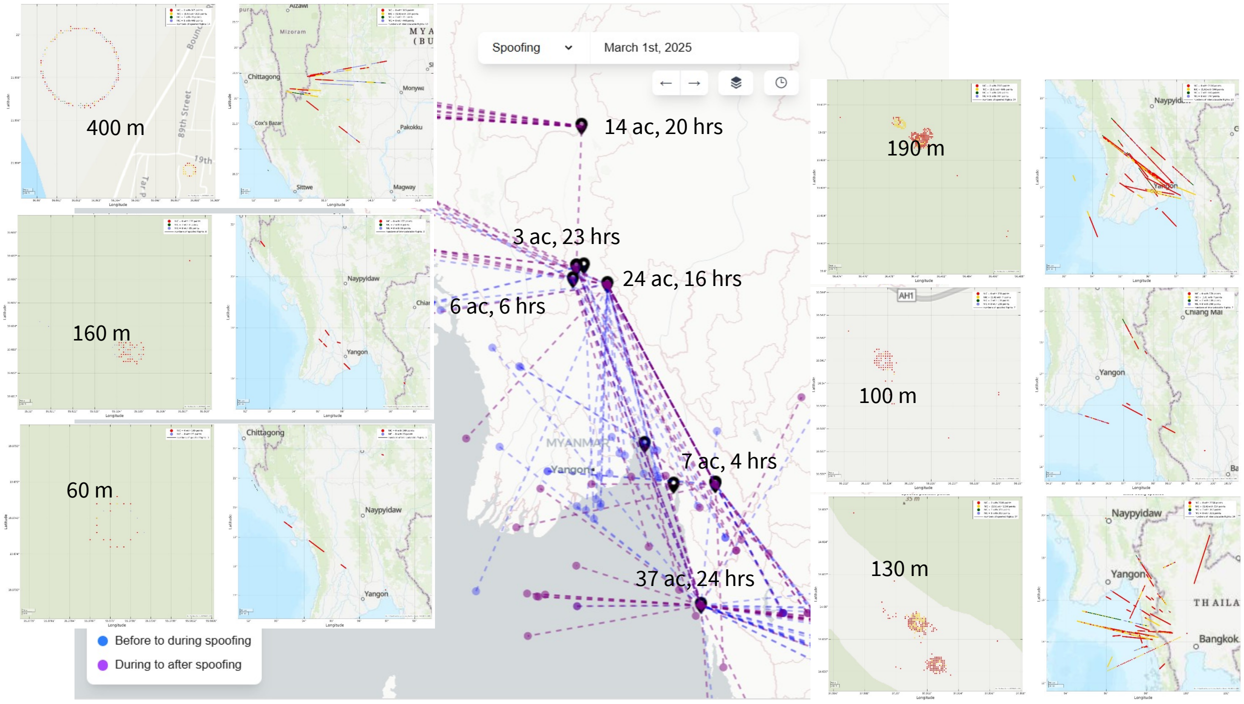


FIGURE 6. *Detected spoofing in Myanmar on March 1 2025. Spoofed locations flagged and ADS-B positions before and after jump to spoofed position indicated. 6 distinct events are shown in the inserts with the rough diameter of the largest spoof "circle" in each event (left plot) and estimated positions during spoof (right plot) (rfi.stanford.edu)*

Data processed by rfi.stanford.edu indicates that spoofing in Myanmar started around August 2024 with one or two distinct events in the south of the country by Yangon. The regularity and number of events have increased since then. FIGURE 6 shows the six distinct spoofing events in Myanmar from March 1 2025 along with the reported ADS-B positions prior to and after the jump to the spoofed location. The six events are generally circles but are small in diameter varying from 60 to 400 m with some events exhibiting multiple circles. Five of the events have spoof circles less than 200 m in diameter. The 400 m spoof trajectory exhibit a speed about 70 kph. The small size of circles, compared to that found in Russia, may indicate that their target is different – perhaps small commercial drones (e.g DJI). These tend to be the type of drones operated by the anti-junta forces in Myanmar. As suggested by the figure, the spoofing also seems widespread with aircraft flying in the country as well as along its western coastline affected. Additionally, when looking over the month and then the year, these events are persistent. They even persisted during and after the 7.9 magnitude earthquake in Myanmar in March 28 2025 despite the need for GNSS to support international rescue and relief efforts in the country. The spoofing seems long lasting with our detection showing the events lasting hours if not nearly the whole day. However, it is hard to be sure that the spoofing is continuous due to not having regularly data in the area throughout the day.

3.3 India-Pakistan Spoofing

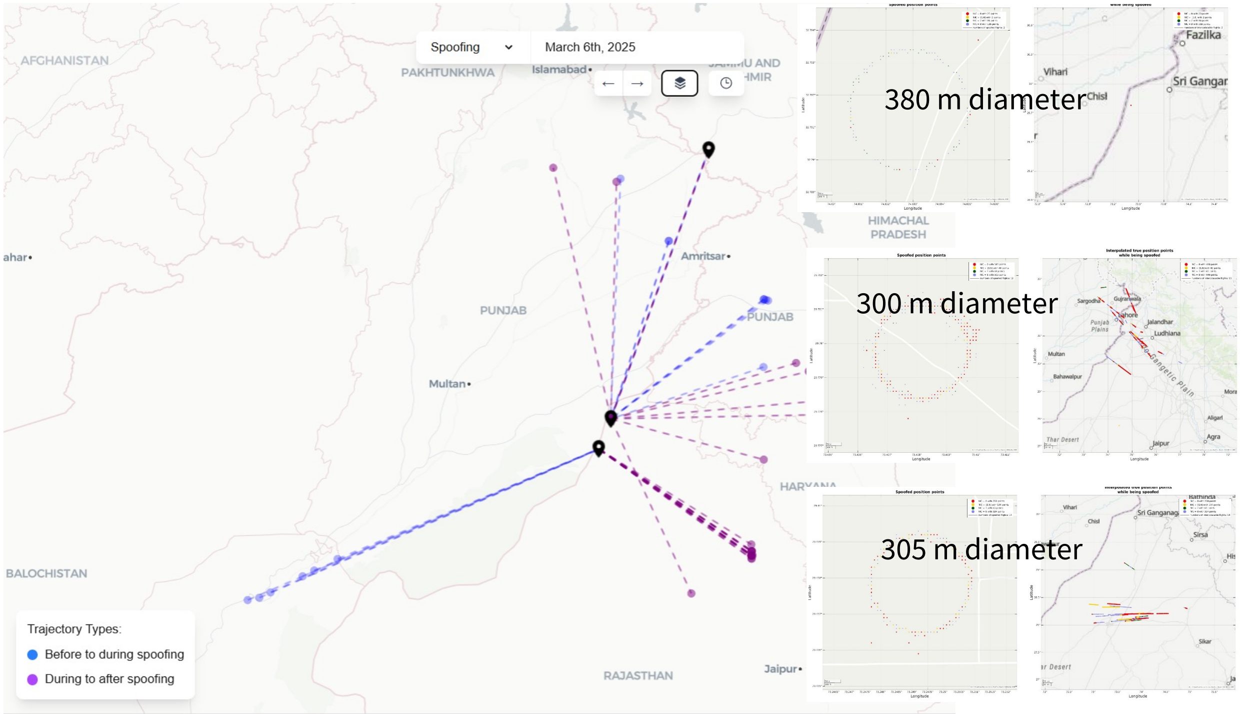


FIGURE 7. *Detected spoofing in India-Pakistan on March 6 2025. Spoofed locations flagged and ADS-B positions before and after jump to spoofed position indicated. 3 distinct events are shown in the inserts with the rough diameter of the largest spoof "circle" in each event (left plot) and estimated positions during spoof (right plot) (rfi.stanford.edu)*

FIGURE 7 shows the three distinct spoofing events on the India/Pakistan border near Jodhpur on March 6 2025 along with the reported ADS-B positions prior to and after the jump to the spoofed location. The three events have spoof circles with roughly the same diameter of around 300 m. The tracks are smaller than what is found in Russia but bigger than most seen in Myanmar. The circular tracks show a speed of approximately 110 kph which is faster than that seen in Myanmar but slower than in Russia. These two differences implies that the spoofing is targeting air vehicles larger than consumer drones – perhaps small military drones. The spoofing may be long lasting with at least one event been seen several times in a 22 hour period. Given the limited data throughout the day so it is hard to be sure that the spoofing is continuous. These spoofing events were seen regularly (daily) starting around May 30 2024. There was one event in May 2024. Other distinct events were then seen a month later. A brief gap spoofing event detection in the region is seen late April to early May 2025. This was during a period of increased tension and air combat between India and Pakistan. Hence, the lack of detection is more likely due to lack of information, i.e. commercial aircraft avoiding hot conflict zones and so no reports are available, rather than the absence of spoofing. This highlights one of the limitations with ADS-B use as we do not get reports from regions where there are no commercial flights nearby. Given that no commercial aircraft will operate nearby, the lack of GNSS RFI situational awareness may not be too detrimental for the civil community.

3.4 Other Spoofing Affected Areas Worldwide (2025)

Russia, Myanmar and India-Pakistan are only three of many regions that have regular GNSS spoofing. They are highlighted as they have many persistent events. However rfi.stanford.edu has identified many other areas of spoofing such as Georgia, Azerbaijan, Eastern Mediterranean, Israel, Iran, Iraq and the Persian Gulf region. These are all potential conflict areas. ADS-B has also identified potential irregular spoofing in Manchuria (October 15 2025) and India that we need to further assess. The power of ADS-B is that it has allowed us to regularly track and quantify the growth of GNSS spoofing events. We can take those events and examine the position and other data in more details to understand some of its characteristics. It also shows the growing use and sophistication of GNSS RFI. And, especially when supplemented with other data, shows the increasing complexity of spoofing such as jamming and spoofing and multi-frequency attacks. This is shown in the next section.

4. SUPPLEMENTRING ADS-B INFORMATION FOR RFI DETECTION & CHARACTERIZATION

ADS-B has limitations for GNSS RFI detection and localization. One issue is that it, for obvious reasons, cannot provide the true aircraft location when it is being jammed or spoofed. In our rfi.stanford.edu tool, we interpolate/extrapolate these locations using ADS-B positions from before and after the RFI. However, this is an estimate that depends the aircraft not changing directions or course during the period where we do not have true positions. Another limitation is to understand if the RFI is on GPS L1 C/A only or other signals and frequencies. Finally, additional coverage can be useful, especially on the ground, to better understand the profile of the RFI and its radio horizon. We examined a mitigation for each of these limitations: 1) using other flight data such as flight plan information and multi-lateration ((MLAT) data to provide aircraft location, 2) ground-based receivers (ground monitors) to examine other signals and 3) broadcast data from ships – Automatic Identification System (AIS) that transmit the ships GPS location.

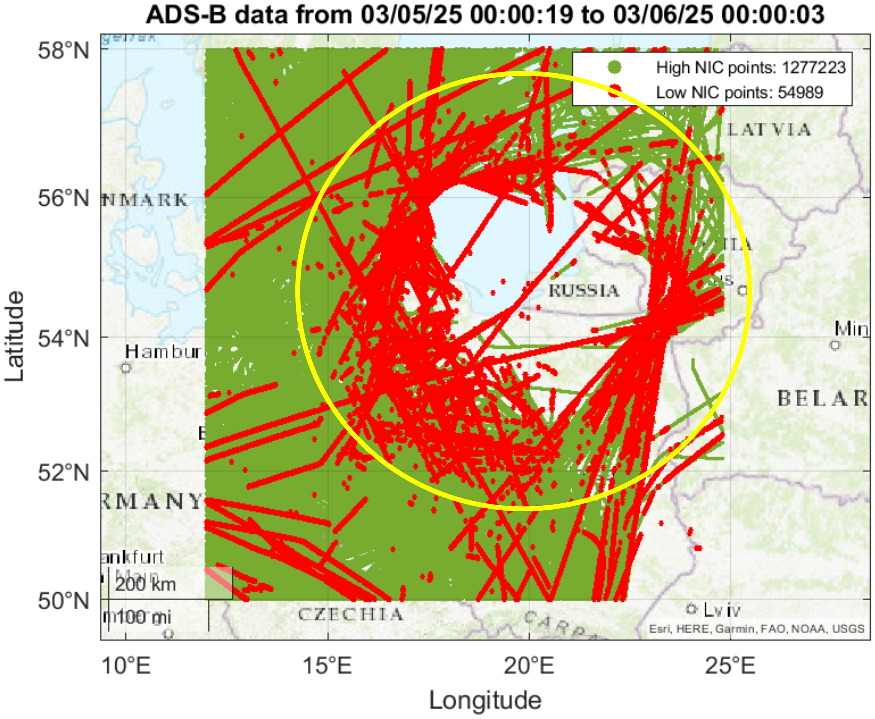


FIGURE 8. *Reported ADS-B positions with yellow circles indicating estimated location of aircraft when spoofed to Kaliningrad (left) and latitude/longitude/altitude (GPS = blue/red, Baro = black) where blue/red are reports with high/low NICs.*

For the study, we use the RFI from Kaliningrad as a test case. Kaliningrad is a good test case as there are many flights and ADS-B ground station in that region (particularly Poland), we have nearby low-cost monitor stations (LCM) in Gdynia and we can get AIS data from ships in the gulf of Poland that covers Kaliningrad to Gdynia. Importantly, there has been increased RFI in the Baltic Sea region, both in Kaliningrad and in the Gulf of Finland. The RFI coming from Kaliningrad started out as occasional jamming starting in about 2022-23. It started small but became more powerful and widespread. The effect of the jamming on ADS-B is seen in FIGURE 8 which shows a plot of the NICs reported by aircraft on March 5 2025. The jamming seems omni-directional and surrounds the Kaliningrad area and extends about 250 kilometers in radius around Kaliningrad.

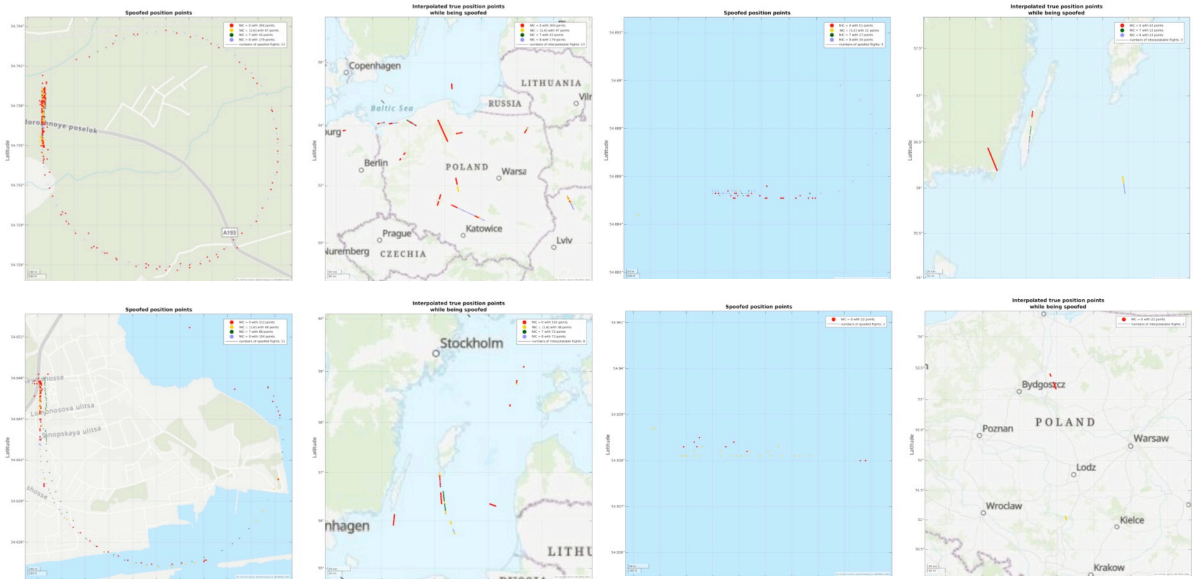


FIGURE 9. *Selected Kaliningrad spoofing events from March 9 2025. 4 distinct events are shown in the inserts with spoofed locations (left plot) and estimated positions during spoof (right plot) (rfi.stanford.edu)*

Regular spoofing from Kaliningrad started around November 9 2024 and became increasingly common in December 2024. We examined several days in early March. On any given day, several different spoofed position trajectories were seen such as point location or a semi-circular track (3/4 circle to a straight line). FIGURE 9 shows several of these patterns from March 9 2025 identified by rfi.stanford.edu. It is unclear whether the spoofing is intermittent or persistent as there is a low volume of aircraft that seem to be affected by the spoofed. We did not find two different spoofed locations at the same time in the days that we examined. However, for some of the patterns, the spoofed areas is in a given direction while for others it is in a different direction or even more omni-directional. Hence it could be one spoofer operated serially or several different spoofing antennas.

4.1 Supplementing with other Flight data

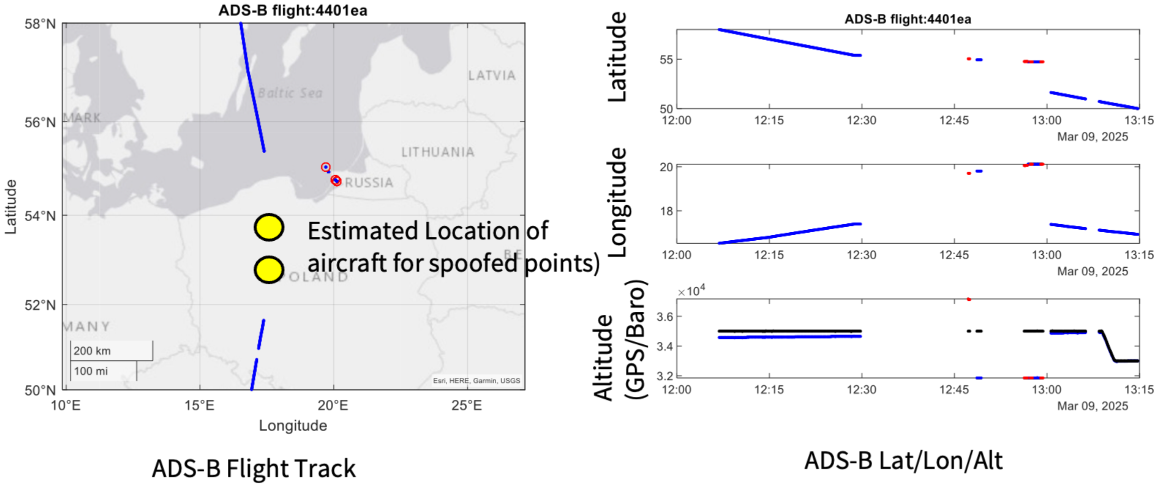
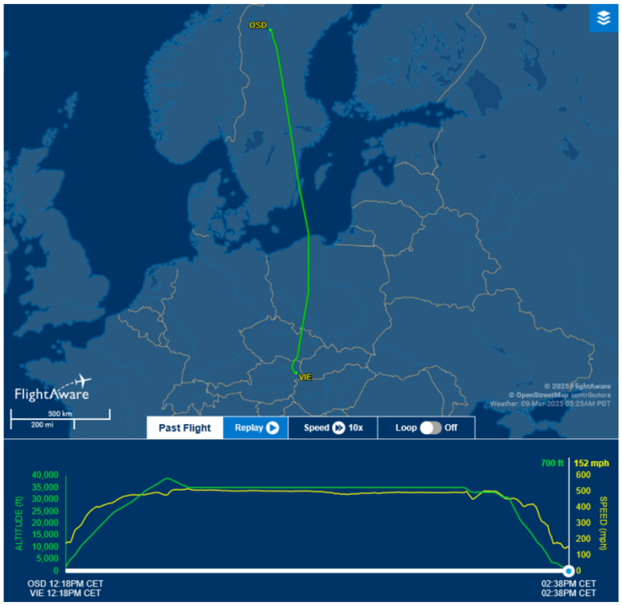
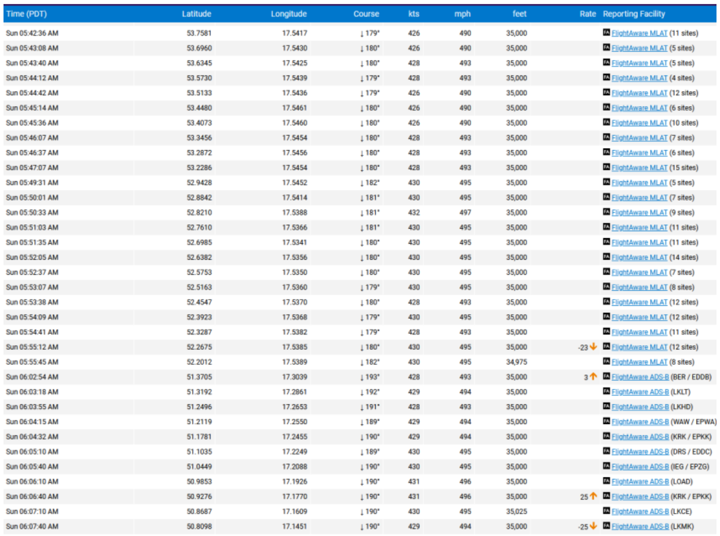


FIGURE 10. *Reported ADS-B positions of Embraer ERJ-135 (OE-LOW) on March 9 2025 with yellow circles indicating estimated location of aircraft when spoofed to Kaliningrad (left) and latitude/longitude/altitude (GPS = blue/red, Baro = black) where blue/red are reports with high/low NICs. Estimated location generated by interpolation and using flightaware tracks generated with multi-lateration.*

The layering of jamming and spoofing from Kaliningrad creates a jam then spoof situation for some aircraft passing through the region as they first experience jamming and then are spoofed. This can be seen in FIGURE 10 which shows the flight path of a Jetology Embraer ERJ-135 (OE-LOW) which first loses position and indicates a jump to spoofed positions in Kaliningrad, then loses the spoofed positions and eventually regain true positions.

rfi.stanford.edu estimates the true location of the aircraft during spoofing by interpolating known locations before and after spoofing. This is challenging for Kaliningrad due to the jamming causing large outages in positions hence the interpolation may have significant errors especially if the aircraft changes course. One option, when available, is to use flight plan information or multi-lateration (MLAT) from providers such as flightaware.com. MLAT determines the position of a transmission source by measuring the (relative) time of arrival (TOA) of the transmission at multiple geographically distributed stations and calculating the position based on those TOAs. FIGURE 11 (left) shows the flight path of the Embraer from flightaware.com along with the position data and its source (right). This flight was chosen as it had significant amount of flightaware MLAT positions during its position outage. It is also a flight that slightly changes directions during the outage of ADS-B positions. When MLAT is not available, flightaware provides estimates presumably based on the aircraft flight path and its flight plan.





Time (PDT)	Latitude	Longitude	Course	kts	mph	feet	Rate	Reporting Facility
Sun 05:42:36 AM	53.7581	17.5417	↓ 179°	426	490	35,000		FlightAware MLAT (11 sites)
Sun 05:43:08 AM	53.6960	17.5430	↓ 180°	426	490	35,000		FlightAware MLAT (5 sites)
Sun 05:43:40 AM	53.6345	17.5425	↓ 180°	428	493	35,000		FlightAware MLAT (5 sites)
Sun 05:44:12 AM	53.5730	17.5439	↓ 179°	428	493	35,000		FlightAware MLAT (4 sites)
Sun 05:44:42 AM	53.5133	17.5436	↓ 179°	426	490	35,000		FlightAware MLAT (12 sites)
Sun 05:45:14 AM	53.4480	17.5461	↓ 180°	426	490	35,000		FlightAware MLAT (6 sites)
Sun 05:45:36 AM	53.4073	17.5460	↓ 180°	426	490	35,000		FlightAware MLAT (10 sites)
Sun 05:46:07 AM	53.3456	17.5454	↓ 180°	428	493	35,000		FlightAware MLAT (7 sites)
Sun 05:46:37 AM	53.2872	17.5456	↓ 180°	428	493	35,000		FlightAware MLAT (6 sites)
Sun 05:47:07 AM	53.2286	17.5454	↓ 180°	428	493	35,000		FlightAware MLAT (15 sites)
Sun 05:49:31 AM	52.9428	17.5452	↓ 182°	430	495	35,000		FlightAware MLAT (5 sites)
Sun 05:50:01 AM	52.8842	17.5414	↓ 181°	430	495	35,000		FlightAware MLAT (7 sites)
Sun 05:50:33 AM	52.8210	17.5388	↓ 181°	432	497	35,000		FlightAware MLAT (9 sites)
Sun 05:51:03 AM	52.7610	17.5366	↓ 181°	430	495	35,000		FlightAware MLAT (11 sites)
Sun 05:51:35 AM	52.6985	17.5341	↓ 180°	430	495	35,000		FlightAware MLAT (11 sites)
Sun 05:52:05 AM	52.6382	17.5356	↓ 180°	430	495	35,000		FlightAware MLAT (14 sites)
Sun 05:52:37 AM	52.5753	17.5350	↓ 180°	430	495	35,000		FlightAware MLAT (7 sites)
Sun 05:53:07 AM	52.5163	17.5360	↓ 179°	430	495	35,000		FlightAware MLAT (8 sites)
Sun 05:53:38 AM	52.4547	17.5370	↓ 180°	428	493	35,000		FlightAware MLAT (12 sites)
Sun 05:54:09 AM	52.3923	17.5368	↓ 179°	430	495	35,000		FlightAware MLAT (12 sites)
Sun 05:54:41 AM	52.3287	17.5382	↓ 179°	428	493	35,000		FlightAware MLAT (11 sites)
Sun 05:55:12 AM	52.2675	17.5385	↓ 180°	430	495	35,000	-23 ↓	FlightAware MLAT (12 sites)
Sun 05:55:45 AM	52.2012	17.5389	↓ 182°	430	495	34,975		FlightAware MLAT (8 sites)
Sun 06:02:54 AM	51.3705	17.3039	↓ 193°	428	493	35,000	3 ↑	FlightAware ADS-B (BER / EDDB)
Sun 06:03:18 AM	51.3192	17.2861	↓ 192°	429	494	35,000		FlightAware ADS-B (LKLT)
Sun 06:03:55 AM	51.2496	17.2653	↓ 191°	428	493	35,000		FlightAware ADS-B (LKHD)
Sun 06:04:15 AM	51.2119	17.2550	↓ 189°	429	494	35,000		FlightAware ADS-B (WAW / EPWA)
Sun 06:04:32 AM	51.1781	17.2455	↓ 190°	429	494	35,000		FlightAware ADS-B (KRK / EPKK)
Sun 06:05:10 AM	51.1035	17.2249	↓ 189°	430	495	35,000		FlightAware ADS-B (DRS / EDDC)
Sun 06:05:40 AM	51.0449	17.2088	↓ 190°	430	495	35,000		FlightAware ADS-B (IEG / EPZG)
Sun 06:06:10 AM	50.9853	17.1926	↓ 190°	431	496	35,000		FlightAware ADS-B (LOAD)
Sun 06:06:40 AM	50.9276	17.1770	↓ 190°	431	496	35,000	25 ↑	FlightAware ADS-B (KRK / EPKK)
Sun 06:07:10 AM	50.8687	17.1609	↓ 190°	430	495	35,025		FlightAware ADS-B (LKCE)
Sun 06:07:40 AM	50.8098	17.1451	↓ 190°	429	494	35,000	-25 ↓	FlightAware ADS-B (LKMK)

FIGURE 11. *Flight track (left) and data for flight track with its reporting source (right) for Embraer ERJ-135 (OE-LOW) on March 9 2025. (flightaware.com)*

4.2 Low Cost Monitor Data

Another way to further assess the Kaliningrad RFI is to use multi-frequency GNSS receivers that we can get observables from. We examined data from our low cost monitor (LCM) that we had installed in the port city Gdynia, Poland (Kriezis 2025). This LCM is located at sea level about 90 kilometers across the Gulf of Poland from Kaliningrad and based on traditional 4/3rd earth model for radio horizon, we would not expect to experience any transmission from Kaliningrad unless it was transmitted from a very high tower. However, because of atmospheric factors such as inversion which can extend the radio horizon, we occasionally can receive the interference. FIGURE 12 shows an example of the measurement from the LCM on L1 and L5 from May 18 2025. It shows the automatic gain control (AGC) which relates to the power of the receiver and the maximum carrier to noise ratio (C/No) observed for GPS. It shows that the RFI is on both L1 and L5 (it also affected Galileo, Beidou and GLONASS on these frequencies). There is some but not severe degradation on the max C/No on both frequencies. However we did not experience spoofing indicating the jamming is perhaps a separate transmission. Or it may mean that the spoofing is not directed as far out as the jamming.

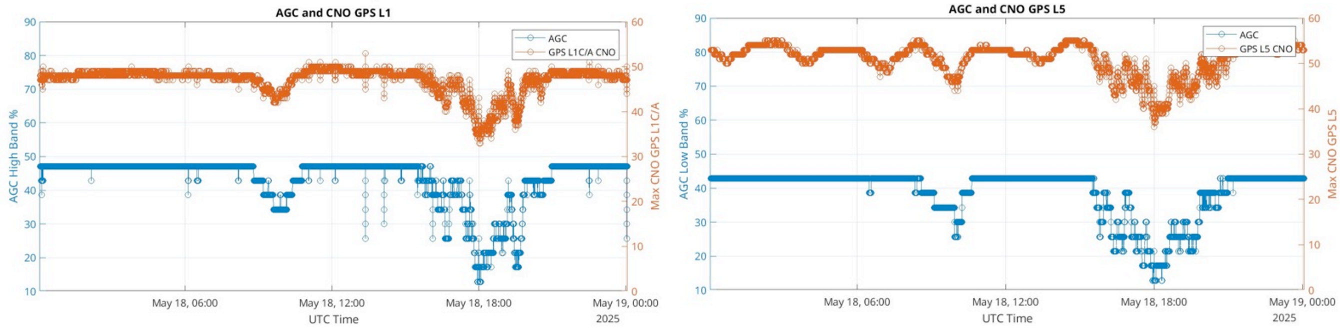


FIGURE 12. *Automatic gain control (AGC) and maximum carrier to noise ratio (C/No) on tracked GPS satellites for L1 (left) and L5 (right) from the ublox monitor stationed in Gdynia, Poland on May 18 2025.*

4.3 AIS Ship data

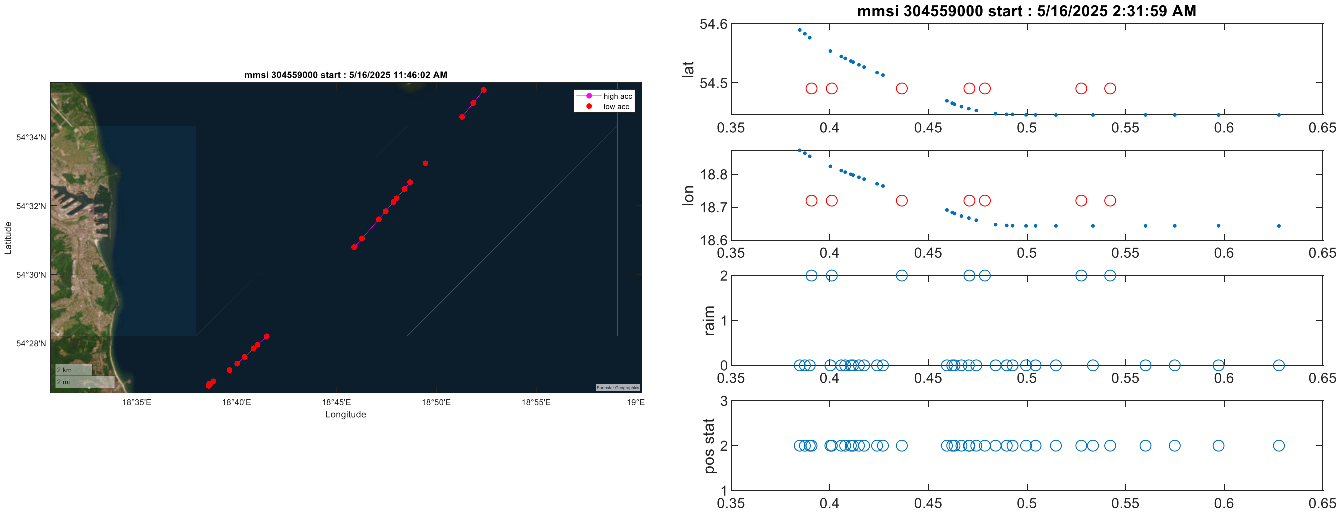


FIGURE 13. *AIS derived positions for ship (left) and latitude longitude, RAIM indicator and position status flag (right) over time (day) on Gdynia, Poland on May 16 2025.*

AIS broadcast from ships was also used to examine and supplement our analysis of Kaliningrad RFI. We collected AIS from May 16 2025 to see to what extent GNSS RFI from Kaliningrad could be seen. One can think of AIS is being the equivalent of ADS-B for maritime vessels. Another way that GNSS based AIS data is like ADS-B is that there is little information on the receiver performance. Indeed, usually the only GNSS related information available are position and speed (speed over ground or sog) which a 1-bit indicator of performance level (high vs low accuracy). An example is seen in FIGURE 13 which shows the ships trajectory (left) along with a plot of its latitude, longitude and receiver autonomous integrity monitoring (RAIM) status over time. The red circles on the latitude and longitude plots indicate times we have non-position AIS messages suggesting the AIS data channel is functional during that time. Furthermore, unlike ADS-B, these position reports are not as frequent (can be minutes between transmissions) or regular for AIS. The result is that we must infer when GNSS is unavailable. To do this, we want to be able to distinguish between the two possible causes of not having AIS positions: 1) GPS not operating (due most likely to jamming) and 2) lack of reception of AIS transmissions. One way is to examine the reception of non-positon related AIS messages to verify that the transmission is getting through. Another way is to see if we have received AIS messages from that location in other instances. FIGURE 14 shows another ship trajectory. This example has a period where we do not have position messages, but we receive other AIS messages (red circles in latitude and longitude plots) suggesting the lack of GNSS positions from AIS is due to a receiver issue. Another way, given that we have fixed AIS ground stations, is to map the coverage area and see if we are missing positions while the ship is in an area with coverage. This is seen FIGURE 15. The left side shows a ship transiting an area into the port of Gdynia while providing its positions along the entire route. The right side shows another ship at a different time making the same transit but without position reports for half of the route. It shows many position reports near the same area before quickly jumping to being in port. This suggest that the position report was coasting (perhaps because its GPS was jammed) and not really providing the true positions for part of the time. Hence, the AIS may not actually provide the true position even when not being spoofed. These issues illustrate some of the challenges of using AIS for GNSS RFI detection and analysis.

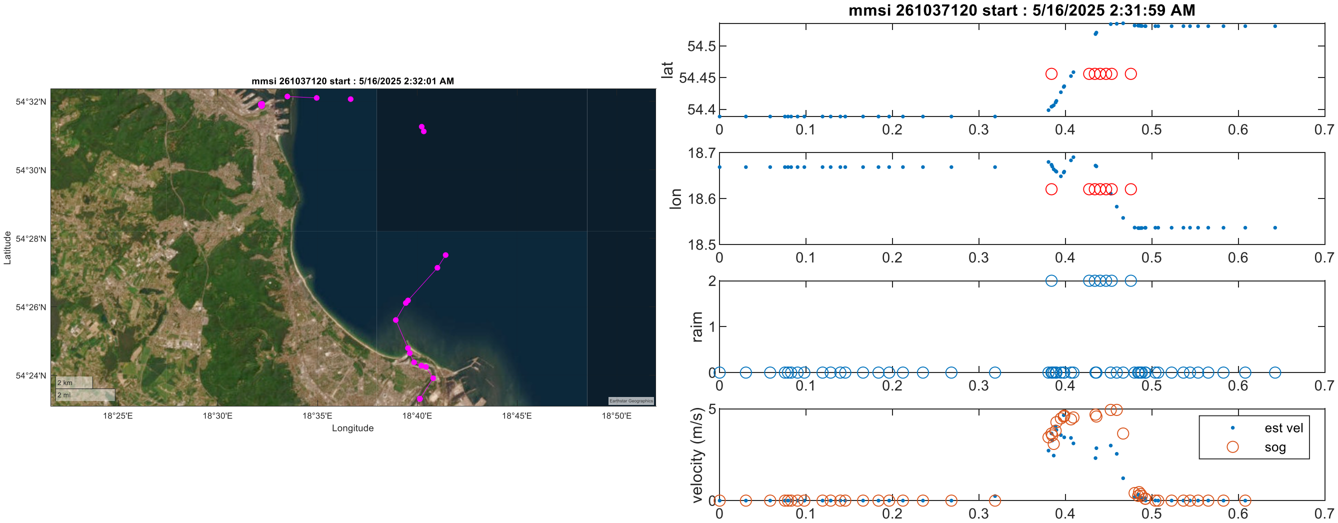


FIGURE 14. *AIS derived positions for ship (left) and latitude longitude, RAIM indicator and velocity (speed over ground and differential position) (right) over time (day) on Gdynia, Poland on May 16 2025.*

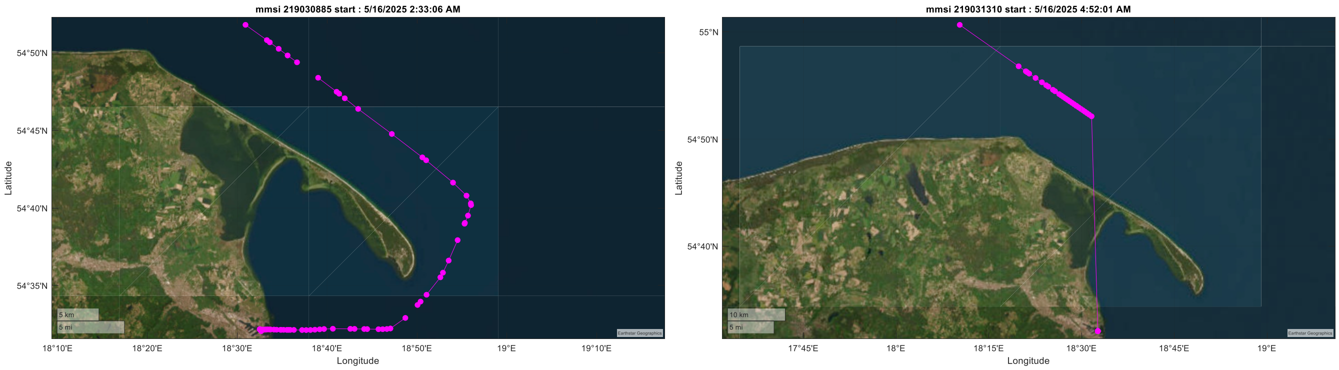


FIGURE 15. *AIS derived positions for two different ship transiting the same region in Gdynia, Poland on May 16 2025.*

5. SUMMARY

This paper uses ADS-B data to show how widespread GNSS spoofing has become and the different regions where aircraft have been clearly affected. The data also shows the different characteristics of the spoofing patterns seen in various regions and how persistent the spoofing has become with many of the discussed regions having incidents daily. Finally, it shows how we can supplement ADS-B data with other information to better understand the spoofing and RFI.

ADS-B data processed by rfi.stanford.edu has allowed us to identify and examine many hotspots with multiple spoofing events around the world. The paper examines the widespread spoofing in Russia. It highlights two other areas that are not as commonly discussed: 1) Myanmar and 2) India/Pakistan border. Both are in areas with some military conflicts (Myanmar civil war and India/Pakistan disputes) and there are multiple events that started in 2024. The spoofing in both areas are persistent and generally spoofed to a circle rather than a fixed point. The spoofed circles and patterns are smaller than that in Russia and do not exhibit as much diversity in shapes. The spoofed trajectories also exhibit different speeds. The combination of these factors implies the different types of vehicles they may be targeting. The data also helped us assess the persistence of the events. For example, spoofing events in all three region had aircraft being spoofed throughout the day suggesting that they may be continuously on.

ADS-B is a great tool but it has limitation and other data source can be used to supplement ADS-B. Ground stations are especially useful for monitoring more details about the RFI. Other aircraft data (MLAT, flight plans) give a better sense of where the aircraft was when it reported its spoof location.

ACKNOWLEDGMENTS

The authors would like to acknowledge the support of Federal Aviation Administration (FAA) Navigation Services, The Aerospace Corporation, and Department of Transportation CARNATIONS University Transportation Center (UTC) for this work.

REFERENCES

Liu, Zixi, Lo, Sherman, Blanch, Juan, Walter, Todd, "GNSS Spoofing Detection and Localization Using ADS-B Data," Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024), Baltimore, Maryland, September 2024, pp. 796-803. https://doi.org/10.33012/2024.19749

C4ADS (2019), “Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria,” March 26 2019

Gault, Matthew (2025), “Ukraine Is Jamming Russia’s ‘Superweapon’ With a Song,” November 20 2025, 404Media https://www.404media.co/ukraine-is-jamming-russias-superweapon-with-a-song/

Kazmierczak, J., Joseph, A., and Cook, G., (2021). Aviation gnss interference analysis based on ads-b out data. In Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), pages1108–1121.

Kriezis, Argyris, Chen, Yu-Hsuan, Akos, Dennis, Lo, Sherman, Walter, Todd, (2025) "Real-World Spoofing Detection and Characterization Using Low-Cost Receivers," *Proceedings of the 2025 International Technical Meeting of The Institute of Navigation*, Long Beach, California, January 2025, pp. 414-424. https://doi.org/10.33012/2025.19997

Li, Jinqi, Wang, Hongxia, Dan, Zhiqiang, Xu, Jiahao, Wang, Zhipeng, Zhu, Yanbo, (2023) "Civil Aviation GNSS Interference Detection and Location Based on Genetic Algorithm Using ADS-B Data," *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, Denver, Colorado, September 2023, pp. 4168-4182. https://doi.org/10.33012/2023.19392

Liu, Z., Lo, S., Blanch, J., Walter, T., (2024) "GNSS Spoofing Detection and Localization Using ADS-B Data," *Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024)*, Baltimore, Maryland, September 2024, pp. 796-803. https://doi.org/10.33012/2024.19749

Liu, Z., Blanch, J., Lo, S., Walter, T., (2023) "Investigation of GPS Interference Events with Refinement on the Localization Algorithm," *Proceedings of the 2023 International Technical Meeting of The Institute of Navigation*, Long Beach, California, January 2023, pp. 327-338. https://doi.org/10.33012/2023.18627

Liu, Zixi, Lo, Sherman, Chen, Yu-Hsuan, Walter, Todd, (2025A)"A Scalable Pipeline for Real-Time Global Detection and Localization of GNSS Interference Using ADS-B," *Proceedings of the 38th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2025)*, Baltimore, Maryland, September 2025, pp. 446-456. https://doi.org/10.33012/2025.20358

Liu, Zixi, Lo, Sherman, Blanch, Juan, Chen, Yu-Hsuan, and Walter, Todd, (2025B) “Locating GNSS Interference Sources using ADS-B with Non-linear Least Squares,” Published in *NAVIGATION*, Vol. 72 No. 3, Fall 2025, DOI 10.33012/navi.71

Lo, Sherman, Liu, Zixi, Ibrahim, Lyla, Chen, Yu Hsuan, Walter, Todd, (2025) "Observations of GNSS Spoofing in Russia in 2023-2024," *Proceedings of the 2025 International Technical Meeting of The Institute of Navigation*, Long Beach, California, January 2025, pp. 425-442. https://doi.org/10.33012/2025.19985

Lukeš, P., Topková, T., Vlček, T., and Pleninger, S., (2020) "Recognition of GNSS Jamming Patterns in ADS-B Data," *2020 New Trends in Civil Aviation (NTCA)*, Prague, Czech Republic 2020, pp. 9-15, doi: 10.23919/NTCA50409.2020.9291039.

RTCA Special Committee-186 (2002), "Minimum Aviation System Performance Standards For Automatic Dependent Surveillance Broadcast (ADS-B)," RTCA/DO-242, June 2002

RTCA Special Committee-186 (2003), "Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services Broadcast (TIS-B)," RTCA/DO-260A, April 2003

RTCA Special Committee-186 (2020), "Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services Broadcast (TIS-B)," RTCA/DO-260C, December 2020

Warner, J. and Johnston, R., (2003), "A simple demonstration that the Global Positioning System (GPS) is vulnerable to spoofing," Journal of Security Administration, In Press (2003)

Warner, J.S. and Johnston, R.G., (2004) "Think GPS Offers High Security? Think Again!", Talk for the Business Contingency Planning Conference, May 23-27, 2004 (Las Vegas, NV)

Zurich University of Applied Sciences (ZHAW) (2024), Live GPS Spoofing Tracker, 12 April 2024, https://www.zhaw.ch/en/about-us/news/news-releases/news-detail/event-news/live-gps-spoofing-tracker

Stanford University, rfi.stanford.edu