XXII SITRAER 2025
Simpósio de Transporte Aéreo

Leveraging Open Data and Machine Learning to Minimize the Risks of Aviation Satellite Navigation Interference

Celso Ferreira de Moura[1], João S D Garcia[1], Andrei Piccinini Legg[2]

2. Embry-Riddle Aeronautical University
2. Universidade Federal de Santa Maria

* **Corresponding author e-mail address**: souzadij@erau.edu

PAPER ID: SIT1239773

ABSTRACT

Global Navigation Satellite Systems (GNSS) are essential for modern aviation and provide crucial safety information in support of aircraft operations like timing, positioning, and navigation support. In recent years, the reliability of such systems has been tested by a significant increase in the cases of unintentional and intentional interference, commonly referred to as jamming and spoofing. Some progress has been made in detecting GNSS interference, but practical challenges remain. Existing approaches based on broadcast low Navigation Integrity Category (NIC) reports show promise but can sometimes miss smaller, localized, or intermittent jamming events that do not produce overt disruptions in satellite navigation systems, potentially leaving threats undetected in some operational environments. This research explores a machine learning framework to enhance the detection of GPS interference in aviation, particularly leveraging open Automatic Dependent Surveillance-Broadcast (ADS-B) to identify new reliable predictors of these events. The project also explores logistic regression with L1 regularization and LightGBM algorithms. The authors examine various predictors, including NIC-based metrics, aircraft movement variations, and detailed altitude bin distributions. Beyond commonly used variables like the percent of low NIC values, this study introduces spatial neighbor features to capture additional anomalies in regional traffic patterns and other metrics. Data from actual 2024 GNSS disruption events collected from official investigation reports by aviation and telecommunications authorities support the current analysis. The most promising results came from LightGBM models enhanced with spatial neighbor statistics, trained on a dataset that included two confirmed interference events. These models had a F1-score of 79.67% alongside an ROC AUC of 0.9582. Key predictors included mean altitude neighbor statistics and positional jump metrics. These findings show that, while existing methods provide valuable insights, there is room for refinement in detecting intermittent and more localized jamming events. The research suggests a new approach that leverages novel variables and advanced machine learning techniques, contributing to the ongoing effort to enhance aviation safety and resilience against GNSS interference.

Keywords: Aviation safety, GNSS interference, Machine Learning, ADS-B, GPS jamming detection.

ACKNOWLEDGEMENTS

This research was supported by the Office of Undergraduate Research at Embry-Riddle Aeronautical University through the Summer Undergraduate Research Fellowship (SURF) program.

GENERATIVE AI USAGE STATEMENT

The authors declare that the use of generative AI tools was limited to the creation and optimization of the code while ensuring methodological rigor and academic integrity. *ChatGPT* was the tool used for the code refinement and was not involved in the generation of content, analysis, or conclusion of the work.

PAPER ID: SIT1239773
Leveraging Open Data and Machine Learning to Minimize the Risks of Aviation Satellite Navigation Interference

1 INTRODUCTION

Global Navigation Satellite Systems (GNSS), such as the Global Positioning System (GPS), have become foundational to modern aviation, providing essential navigation, positioning, and timing support. One of the systems leveraging GNSS data is Automatic Dependent Surveillance–Broadcast (ADS-B), which enables aircraft to continuously broadcast position, speed, and other flight information to ground stations and nearby aircraft. This technology plays a central role in air traffic safety by supporting pilots' and controllers situational awareness and preventing collisions.

In recent years, however, the reliability of GNSS in aviation has come under increasing scrutiny due to a growing number of interference incidents. Growing cases of GNSS radio frequency interference, including jamming and spoofing, pose serious challenges to aviation safety and operations (International Civil Aviation Organization, 2022; European Union Aviation Safety Agency, 2024). Unintentional and intentional disruptions commonly referred to as jamming have been linked to flight delays and cancellations, diversions, and loss of navigational capability (Goward, 2024; McCollum, 2024; Bureau of Transportation Statistics, 2024). Issues impacting GNSS precision or reliability can affect critical aviation systems such as ADS-B, Controller-Pilot Data Link Communications (CPDLC), and Enhanced Ground Proximity Warning Systems (EGPWS) (GPS Spoofing Workgroup, 2024). Figure 1 provides a simplified diagram of how ADS-B works and how jamming devices can affect the aircraft systems, interfering with the incoming signals and affecting the information relayed to other aircraft and air traffic control. Implications go beyond safety concerns, with events invariably leading to changes in flight routes or canceling flights, with direct consequences for sustainability and passenger well-being. While such events have made headlines more and more frequently, industry stakeholders indicate that feasible technical solutions are still "years away" (Carey, 2025; Thurber, 2024). As a result, aviation and telecommunications authorities have worked on the development of reliable detection mechanisms for identifying GNSS interference in real time.

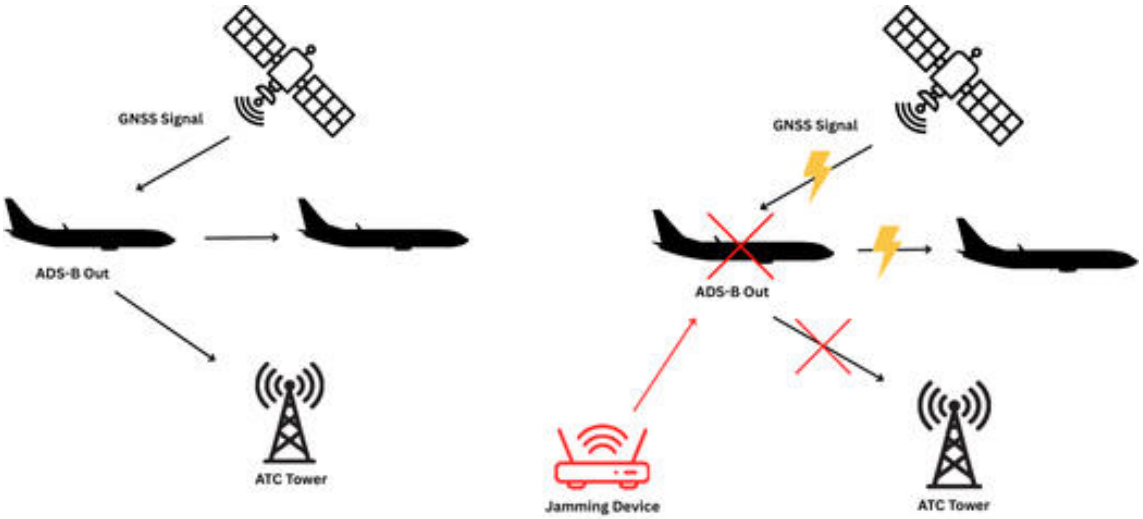


Figure 1: ADS-B broadcasts fail when GPS jamming disrupts position data.

One prominent example of such interference occurred in 2024 near Brazil's Guarulhos Airport (GRU), the busiest airport in Brazil (CAPA — Center for Aviation, 2025; CNN Brasil, 2024). On September 3, 2024, several flights were canceled due to GPS anomalies (Benevides, 2024). According to a technical report by the National Telecommunications Agency (ANATEL), aircraft flying in and out of the area experienced GNSS disruptions both on the ground and during initial climb. Pilots reported that GNSS reception typically normalized after surpassing 6000 feet (Agência Nacional de Telecomunicações, 2024). A field investigation deployed specialized equipment to trace the interference source, ultimately identifying a cell phone tower as a possible cause. Figure 2 shows the recorded frequency spectrum from the site, indicating an anomalous signal activity in the GNSS band.

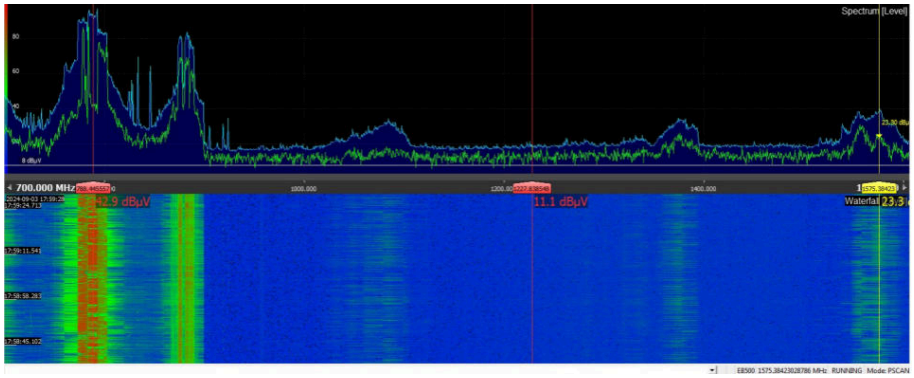


Figure 2: Frequency spectrum of a signal recorded near Guarulhos Airport, Brazil (Agência Nacional de Telecomunicações, 2024).

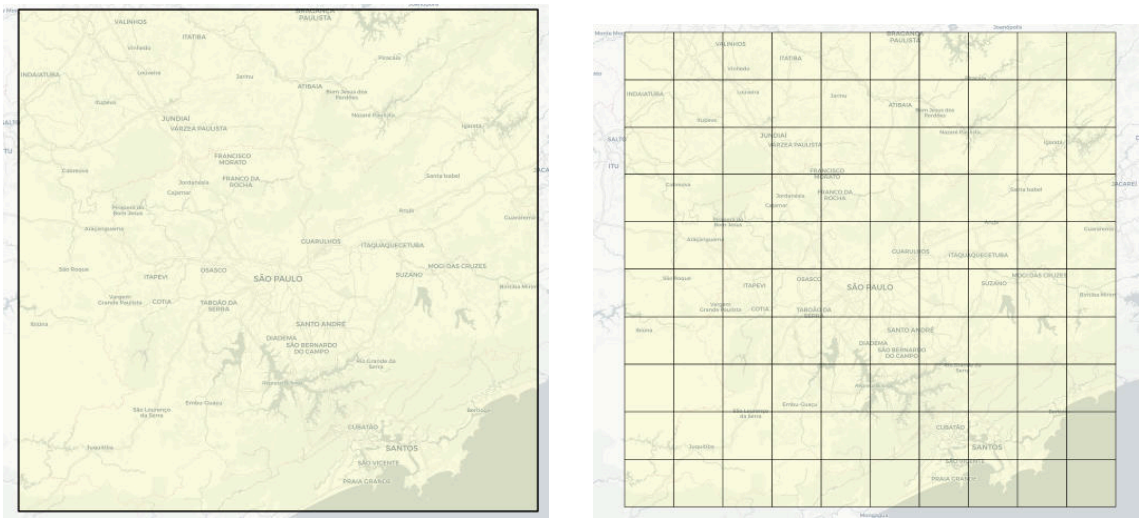
Existing detection methods often rely on metrics derived from ADS-B data, particularly the Navigation Integrity Category (NIC). A high percentage of ADS-B messages reporting low NIC values is typically used as an indicator of possible interference. However, this approach has limitations. Not all forms of interference manifest as low NIC, and localized or short-duration jamming events may not be detected by these methods.

Previous research has attempted to expand the understanding of the factors associated with GPS interference. Pik et al. (2025) explored several variables potentially associated with GNSS anomalies and found indications of issues in areas with heavy aircraft traffic and low-traffic areas associated with potential conflicts. Other studies have explored methods for detecting GPS anomalies, primarily relying on signal characteristics analysis, position references checks, and multi-sensor techniques (Tariq e Tariq, 2025; Stanisak et al., 2024; Zhang et al., 2015). Some studies suggested that ADS-B data can help locate jamming sources (Schäfer et al., 2023). Liu et al. (2022) propose a method for interference source localization using ADS-B data and the development of a simulator to generate ADS-B data from affected simulated flight tracks. Other sources suggest using Inertial Navigation System (INS) positions to detect spoofed trajectories (Kujur et al., 2020).

This study builds upon those insights by introducing a machine learning framework that leverages ADS-B data to improve the detection of GNSS interference events. In addition to traditional NIC-based metrics, the proposed models incorporate spatial neighbor features, altitude distributions, and movement anomalies. By evaluating the performance of logistic regression and LightGBM models for a confirmed 2024 jamming incident, this research aims to help understand the value of different variables in predicting interference events.

2 METHOD

ADS-B data were obtained from the OpenSky Network, an open-source platform providing real-time and historical aircraft surveillance data (Strohmeier, 2020). The dataset included position, velocity, NIC, and timestamped data for flights recorded during periods of known and suspected GNSS interference in 2024. The study area was divided into a fixed-resolution grid based on latitude and longitude indices. Each grid cell represented a $0.25^\circ \times 0.25^\circ$ spatial region, and data were aggregated every 60 seconds to capture temporal trends in GNSS performance. The 60-second window was chosen as a balance between computational efficiency and statistical reliability: shorter intervals would increase processing demands while often leaving cells sparsely populated, whereas longer intervals risked obscuring subtle jamming events.



(a) Area of Study **(b)** 10×10 Grid of Area

Figure 3: Region over GRU Airport segmented into a 10×10 grid for interference analysis: (a) overall area of study and (b) grid segmentation.

Flights below 12,000 ft were selected to increase the likelihood of capturing GPS interference while minimizing altitude-related noise in spatial patterns. Messages with incomplete or corrupted data, such as those missing position or NIC values, were discarded. To ensure reliable metric calculation, only aircraft with consistent message frequency and continuity were retained. A set of initial metrics was then defined using a purpose-built Python code to capture potential indicators of GNSS degradation or jamming. These included the percentage of ADS-B messages reporting NIC values below 6 (indicating degraded integrity), variations in altitude consistency across short time windows, deviations from expected message rates per aircraft and other 21 variables. These features formed the core of the baseline detection strategy and were computed for each hour–grid cell combination, though it is important to note that the reliance on a fixed set of features and grid-based aggregation imposes certain limitations on the scope of the analysis.

To enhance the sensitivity of the detection approach to subtle disruptions, additional secondary features were added to the dataset. These included the rate of change of NIC values and velocities, which could highlight abrupt shifts in position, potentially signaling spoofing or interruptions. One variable also binned altitudes in 2000 ft increments, with recalculated metrics such as the percentage of low NIC and jump counts, to better capture

the vertical distribution of anomalies. All features were normalized and centered using z-score scaling before model training.

Another refinement was the incorporation of spatial neighbor features to account for localized and regional effects. For each grid cell, statistics from up to eight adjacent neighbors were integrated into the feature set, including the mean and standard deviation of low NIC percentages, the number of aircraft with positional or speed anomalies, and measures of regional altitude variation and traffic density. This addition allowed the models to consider geospatial context and identify clusters of degraded GNSS performance, adapting the approach on jammer localization proposed by Liu et al. (2022).

With the features established, two classes of machine learning models were trained to detect potential jamming activity. Logistic Regression with L1 regularization (Lasso) was chosen for its simplicity and ability to enforce sparsity, and consider the most relevant predictors. Light Gradient Boosting Machine (LightGBM) was also employed, offering strong performance on imbalanced datasets and the ability to capture complex interactions among features. A binary outcome variable indicated whether a given hour–grid combination overlapped with a confirmed 2024 jamming event or represented normal operation.

Model evaluation accounted for the rarity of jamming events by using stratified sampling to preserve class proportions when splitting the dataset into training (80%) and validation (20%) sets. Performance was assessed using Accuracy, Precision, Recall, F1-score, and ROC AUC, with feature importance evaluated through model-specific methods such as SHAP values for LightGBM. This process ensured that the models were both accurate and interpretable, while also providing insights into which predictors contributed most strongly to the detection of GNSS interference.

3 RESULTS

The study evaluated multiple models for detecting GPS jamming events using aviation-derived predictors from ADS-B data. Three primary modeling approaches were tested: L1-regularized logistic regression, LightGBM with altitude bins, and LightGBM with spatial neighbor features. Overall, the introduction of neighboring feature statistics significantly improved detection accuracy and alignment with real-world interference patterns.

Initial models using L1 regularization offered modest performance, capturing general trends but with limited precision. For the single-day disruption case, the logistic regression model achieved an accuracy of 64%, a recall of 48%, and a precision of only 23%. The top predictors: medium quality NIC and percentage of low NIC were expected, as degraded NIC has been a commonly used indicator in prior literature and official reports. However, the model's limited sensitivity to more subtle or intermittent disruptions reduced its overall usefulness. When tested on a two-day disruption dataset, recall improved to 77%, but at the expense of overall accuracy (56%) and precision (24%). This highlighted a key limitation of NIC-centric metrics: while they may signal severe degradation, they often miss short-duration or spatially localized jamming activity.

Significant gains were observed with gradient-boosted models incorporating altitude bin statistics in the LightGBM with Altitude-Based Features. For a single confirmed jamming day, the LightGBM model reached 85.67% accuracy, 79% recall, and 55% precision, a notable improvement over the logistic baseline. Performance improved further with the two-day dataset, achieving 87% accuracy, 81% recall, and 59% precision, with an F1-score of 68.15% and ROC AUC of 0.9143. Top features included mean altitude, number of unique aircraft, and percentage of position jump per flight, all of which are consistent with expected behaviors during GNSS interference events. For example, sudden position jumps

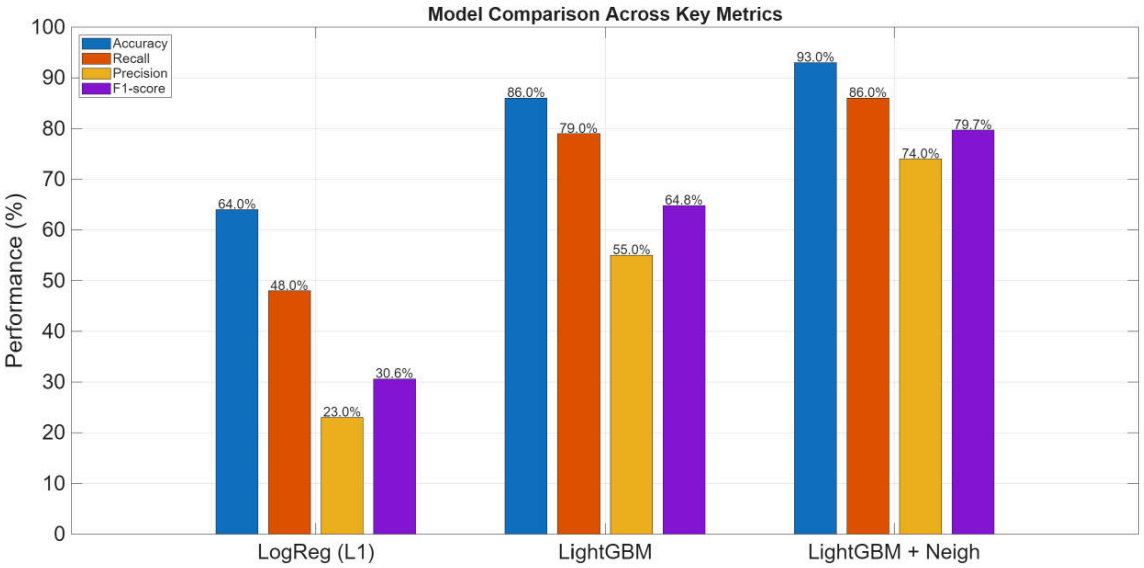


Figure 4: Model performance comparison using accuracy, jamming precision, jamming recall, and F1 score.

and irregular altitude distributions have been frequently noted in 2024 GNSS disruption investigations (GPS Spoofing Workgroup, 2024).

The best-performing model was the LightGBM with Neighboring Feature Statistics incorporating spatial neighbor features, capturing mean, min, max, and standard deviation values of select metrics from surrounding grid cells. On the one-day jamming dataset, this model achieved 89% accuracy, 75% recall, and 63% precision. When applied to the two-day dataset, it reached a peak performance of 93% accuracy, 86% recall, and 74% precision.

To further evaluate model discrimination capability, Receiver Operating Characteristic (ROC) curves were generated for all models. The ROC AUC scores confirmed that incorporating altitude and neighboring features led to significantly better separation between jamming and non-jamming cases. The spatially aware LightGBM model achieved the highest ROC AUC of 0.9585, reflecting excellent predictive quality.

To interpret which features most influenced model predictions, SHAP (Shapley Additive explanations) values were computed for the best-performing LightGBM model, as seen in figure 6. The SHAP summary plot revealed that features such as mean neighbor altitude, standard deviation of neighbor position jumps, and percentage of position jump per flight contributed most to classification decisions. These align with operational expectations during GNSS interference, where clustered anomalies in altitude and positioning behavior often emerge.

Key predictors such as mean altitude of neighbors, minimum altitude of neighbors, and standard deviation of position jumps of neighbors reflect localized disruptions that align with clustered effects reported in real-world GNSS interference scenarios. These spatial-context features supported the model's ability to detect anomalies even when flight data from individual bins alone were insufficient.

In summary, the progressive improvement in performance from NIC-only metrics to altitude-informed models, and finally to spatially aware LightGBM models, demonstrates the value of incorporating regional context into jamming detection. The final model not only achieved the best metrics across all evaluated criteria but also highlighted predictor variables that match patterns observed in official aviation incident reports, validating both

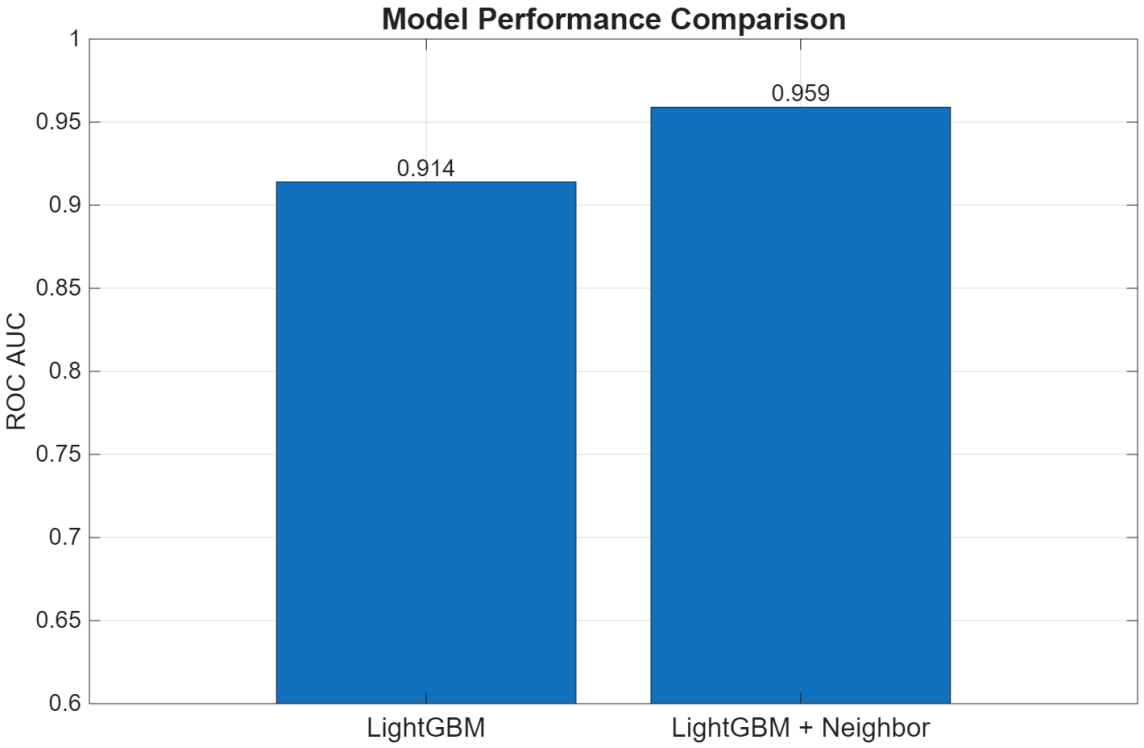


Figure 5: Graph comparing F1-Scores for the best models.

the methodological and practical relevance of the approach.

4 CONCLUSION

This study presents a novel approach to detecting GPS jamming in aviation surveillance data by leveraging machine learning models enriched with engineered features and spatial context. Initial models using traditional NIC-based metrics provided limited precision and recall, particularly for brief or localized interference events. However, by incorporating altitude-distributed predictors and regional neighbor statistics, the detection performance improved significantly, resulting in a LightGBM model with over 93% accuracy, 86% recall, 74% precision and F1-score of 79.67%.

A key advancement in this work is the use of spatial neighbor features, which capture localized disruptions that are often missed by single-aircraft indicators. This regional perspective aligns with patterns observed in confirmed 2024 GNSS jamming incidents and provides a scalable framework for operational deployment.

Moreover, the flexibility of the feature engineering process, combining NIC quality, altitude variations, aircraft movement irregularities, and spatial relationships, demonstrates that varied sets of predictors may better support detection. This opens the door to further innovation in jamming detection by introducing additional time-based features, weather and other atmospheric variables, or aircraft-type dependencies.

Nonetheless, the reliance on ADS-B data and grid-based aggregation may under represent short-lived or low-traffic events, and model performance is still constrained by the specific features engineered in this work. Future research should expand feature engineering process to include other interference events, explore finer temporal resolution, and optimize feature selection for real-time implementation. Importantly, this framework has potential

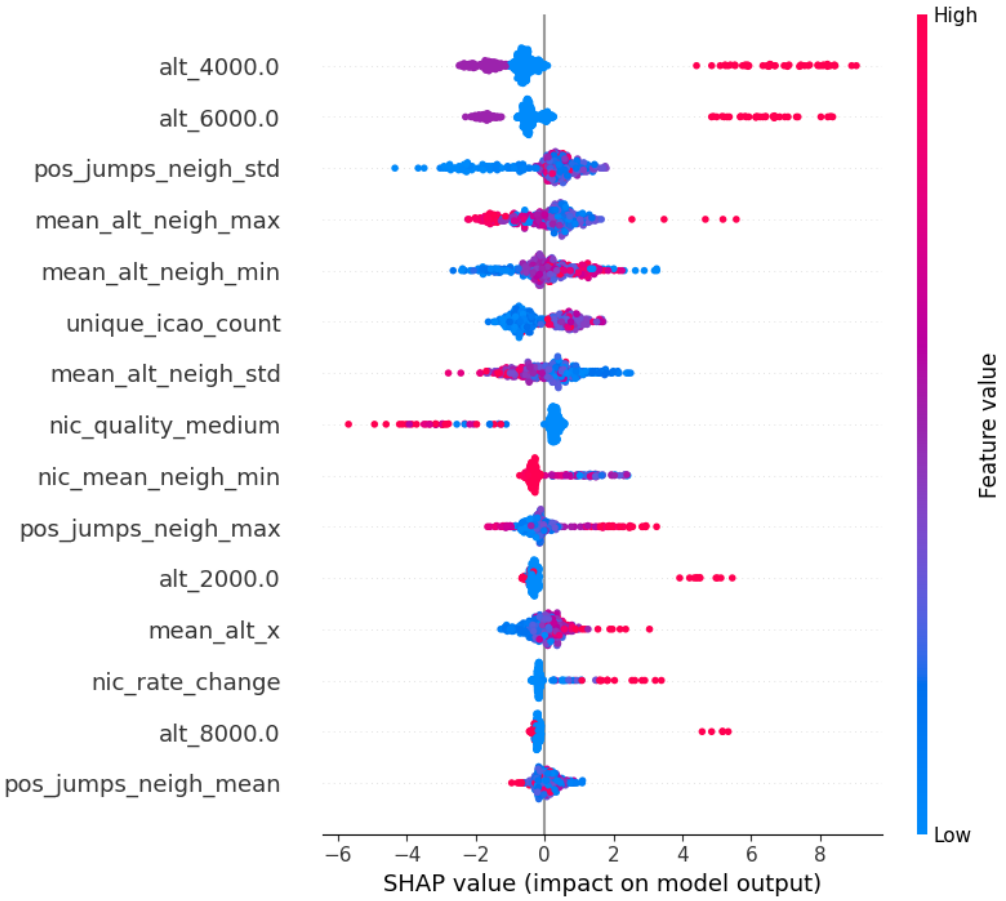


Figure 6: SHAP summary plot showing the most influential features in the best-performing LightGBM model.

applications for oversight organizations and air navigation service providers, who could use it to monitor regional traffic for GNSS disruptions and respond more proactively to operational risks. By refining the methodology and validating it across diverse conditions, the approach could evolve into a practical tool for safeguarding aviation against navigation signal interference, ensuring safer and more resilient air traffic management. Taken together, these findings illustrate how machine learning can transform GNSS interference detection from a reactive process into a proactive safeguard for the future of air traffic management.

References

Agência Nacional de Telecomunicações (2024). Relatório de fiscalização nº 389/2024/gr01fi2/gr01/sfi: Interferência no sinal GPS nas imediações do aeroporto de guarulhos. Relatório Técnico SEI 53504.007401/2024-61, Agência Nacional de Telecomunicações (Anatel), São Paulo, Brasil. Available at:`https://sei.anatel.gov.br/sei/publicacoes/controlador_publicacoes.php?acao=publicacao_visualizar&id_documento=1907066&id_orgao_publicacao=0`. Ação de Inspeção #153678.

Benevides, G. (2024). Tower suspected of interfering with GPS signal at guarulhos airport is shut down. *AeroFlap*. Available at:https://www.aeroflap.com.br/en/.

Bureau of Transportation Statistics (2024). Understanding the reporting of causes of flight delays and cancellations. U.S. Department of Transportation. Available at:https://www.bts.gov/topics/airlines-and-airports/understanding-reporting-causes-flight-delays-and-cancellations. Retrieved April 15, 2024.

CAPA — Center for Aviation (2025). Gru airport — são paulo guarulhos international airport (gru) — airport profile. CAPA Centre for Aviation. Available at:https://centreforaviation.com/data/profiles/airports/gru-airport-sao-paulo-guarulhos-international-airport-gru. Retrieved September 27, 2025.

Carey, B. (2025). GPS jamming, spoofing fixes still 'years away'. *Aviation Week Network*. Available at:https://aviationweek.com/business-aviation/flight-deck/gps-jamming-spoofing-fixes-still-years-away.

CNN Brasil (2024). Problemas em GPS voltam a provocar cancelamento de voos em guarulhos. CNN Brasil. Available at:https://www.cnnbrasil.com.br/nacional/problemas-em-gps-voltam-a-provocar-cancelamento-de-voos-em-guarulhos/. Published September 3, 2024.

European Union Aviation Safety Agency (2024). EASA partners with IATA to counter aviation safety threat from GNSS spoofing and jamming. European Union Aviation Safety Agency. Available at:https://www.easa.europa.eu/en/newsroom-and-events/press-releases/easa-partners-iata-counter-aviation-safety-threat-gnss-spoofing. Press Release.

Goward, D. (2024). GPS disruptions in aviation show importance of backups. GPS World. Available at:https://www.gpsworld.com/study-gps-disruptions-in-aviation-show-importance-of-backups/. Published June 12, 2024.

GPS Spoofing Workgroup (2024). GPS spoofing final report of the GPS spoofing workgroup. *OPS GROUP*.

International Civil Aviation Organization (2022). Cybersecurity in civil aviation: Threats to GNSS. Working Paper A40-WP/108, International Civil Aviation Organization, Montréal, Canada. Available at:https://www.icao.int/sites/default/files/Meetings/a42/Documents/WP/wp_108_en.pdf. Presented at the 40th Session of the ICAO Assembly.

Kujur, B., Khanafseh, S., & Pervan, B. (2020). Detecting GNSS spoofing of ADS–B equipped aircraft using INS plans. Institute of Electrical and Electronics Engineers. DOI: 10.1109/PLANS46316.2020.9109966.

Liu, Z., Lo, S., & Walter, T. (2022). GNSS interference source localization using ADS–B data. In: *Proceedings of the 2022 International Technical Meeting of The Institute of Navigation*, pages 158–167. DOI: 10.33012/2022.18241.

McCollum, M. (2024). Maintaining air traffic efficiency when GPS signals degrade. MITRE. Available at:https://www.mitre.org/news-insights/impact-story/maintaining-air-traffic-efficiency-when-gps-signals-degrade. Published June 11, 2024.

Pik, E., Berra, M., Yearwood, J., & Garcia, J. S. D. (2025). GPS anomalies in aviation: Preliminary insights from automatic dependent surveillance–broadcast data. *Journal of Aerospace Information Systems*, 22. DOI: 10.2514/1.I011527. Available at:https://doi.org/10.2514/1.I011527.

Schäfer, M., Sõeruer, S., Kippak, T., & Sadrak, E. (2023). Jammer on the horizon: A robust method for GPS jammer localization using ADS–B data. In: *Proceedings of the 36th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2023*, pages 4183–4196. Institute of Navigation. DOI: 10.33012/2023.19393.

Stanisak, M., Wilkens, C.-S., & Musmann, F. (2024). High-precision reference positioning in case of GNSS jamming. In: *Proceedings of the International Conference on Aerospace Science & Communication (ICASC)*, pages 1–8. Available at:https://icasc.co/wp-content/uploads/2024/08/High_Precision-Reference-Positioning-in-Case-of-GNSS-Jamming.pdf.

Strohmeier, M. (2020). Research usage and social impact of crowdsourced air traffic data. *Proceedings*, 59. DOI: 10.3390/proceedings2020059001.

Tariq, U. & Tariq, B. (2025). Signal characteristic analysis and anomaly detection for GPS spoofing mitigation. *Ubiquitous Technology Journal*, 1(1):10–22. DOI: 10.71346/utj.v1i1.7. Available at:https://www.researchgate.net/publication/388797302_Signal_Characteristic_Analysis_and_Anomaly_Detection_for_GPS_Spoofing_Mitigation.

Thurber, M. (2024). GPS spoofing still a problem for business aircraft operators. *Aviation International News*. Available at:https://www.ainonline.com/aviation-news/air-transport/2024-12-08/gps-spoofing-still-problem-middle-east-operators.

Zhang, Y. D., Wang, B., & Amin, M. G. (2015). Multi-sensor excision of sparsely sampled nonstationary jammers for GPS receivers. In: *Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, pages 3307–3313, Tampa, Florida. Institute of Navigation.