International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AI-Based GNSS Spoofing and GPS Interference Detection in Aviation

Sam Suseelan

Independent Researcher

Abstract:
Global Navigation Satellite Systems (GNSS) are now crucial to modern aviation navigation systems for positioning, routing and operation monitoring. However, the GNSS technology is subject to spoofing and interference attacks that could compromise the accuracy of navigation and consequently affect aviation safety. Aviation cybersecurity systems need to become more adaptive and intelligent to detect signal manipulation incidents as they become more common.
The focus of this study was to explore the application of Artificial Intelligence (AI) based techniques in the detection of GNSS spoofing and GPS interference in aviation applications. An experimental approach based on simulations was employed, where the GNSS signal datasets were generated under normal and manipulated signal conditions. During the classification process, signal characteristics (signal strength variation, positioning deviation, timing variation, and signal-to-noise ratio anomalies) were examined. A machine learning model based on the random forest algorithm was developed to identify legitimate, spoofed, and interfered navigation signals
The experimental results showed that the presented strategy was able to maintain stable classification performance under simulated attacks. The model had good accuracy, precision, recall, and F1 score, showing its efficacy in detecting abnormal GNSS signal behavior in the experimental environment. It was also found that the spoofed signals caused measurable instabilities in positioning stability and positioning synchronization patterns, which were correctly recognized by the AI classifier.
The study proposes that machine learning can be used as an aid to create more adaptive GNSS security solutions for aviation navigation systems. The results of the experiments demonstrate that the presented AI-assisted anomaly detection methods could be valuable to enhance aviation cyber security and navigation resilience in the real world. To evaluate the effectiveness of AI-based GNSS protection frameworks, further studies with real-world aviation data and operational testing environments are recommended for the future.

Keywords:
GNSS Spoofing; GPS Interference; Aviation Cybersecurity; Artificial Intelligence; Machine Learning; Navigation Security; Anomaly Detection

1. Introduction

The increasing dependence on satellite-based navigation systems in modern aviation has significantly improved flight efficiency, route optimization, aircraft surveillance, and air traffic management. Among these technologies, the Global Positioning System and other Global Navigation Satellite System (GNSS) platforms have become essential components of both civilian and military aviation operations. Aircraft rely heavily on GNSS signals for navigation, positioning, approach guidance, and situational awareness, particularly in modern digital aviation environments where precision and reliability are critical for operational safety.
Despite the operational advantages offered by GNSS technologies, the growing reliance on satellite navigation systems has also introduced new cybersecurity and signal integrity concerns. One of the most significant threats facing aviation navigation systems is GNSS spoofing and GPS interference. GNSS

spoofing occurs when false satellite signals are intentionally transmitted to deceive a receiver into calculating incorrect position, velocity, or timing information. Similarly, GPS interference or jamming disrupts the reception of legitimate navigation signals, potentially affecting aircraft navigation accuracy and communication reliability. These threats have raised global concerns due to their potential impact on aviation safety, flight operations, and national security.

In recent years, several studies and aviation security reports have highlighted the increasing occurrence of GNSS-related interference incidents across different airspaces. The vulnerability of civilian aviation systems to signal manipulation has demonstrated the limitations of traditional detection techniques, which often struggle to identify sophisticated spoofing patterns in real-time. Conventional rule-based detection mechanisms may fail to adapt to dynamic attack behaviors or distinguish between normal signal fluctuations and malicious anomalies, particularly in complex aviation environments.

Artificial Intelligence (AI) and machine learning techniques have emerged as promising approaches for enhancing anomaly detection and cybersecurity monitoring across critical infrastructures. In aviation systems, AI-based models possess the capability to analyze large volumes of signal data, identify hidden patterns, and detect abnormal GNSS behaviors that may indicate spoofing or interference attacks. Machine learning algorithms such as Support Vector Machines (SVM), Random Forest, Decision Trees, and Neural Networks have demonstrated effectiveness in classification and anomaly detection tasks within cybersecurity and wireless communication domains.

The application of AI-based detection methods to GNSS security in aviation presents an opportunity to improve the accuracy, responsiveness, and adaptability of existing protection mechanisms. By leveraging intelligent data analysis techniques, aviation systems may achieve improved detection of abnormal navigation signals while reducing false alarms and enhancing operational resilience. Furthermore, AI-assisted frameworks can contribute to the development of safer and more secure aviation infrastructures capable of responding to emerging cyber-physical threats.

However, despite the growing interest in AI-driven cybersecurity solutions, research on AI-based GNSS spoofing detection within aviation environments remains relatively limited. Existing studies have primarily focused on general wireless signal security or military navigation systems, while fewer studies have specifically addressed intelligent spoofing detection models tailored to civilian aviation applications. This creates the need for further investigation into the effectiveness of AI techniques for detecting GPS interference and GNSS spoofing attacks in aviation systems.

Therefore, this study aims to examine the application of AI-based techniques for detecting GNSS spoofing and GPS interference in aviation environments. The research seeks to evaluate the potential of machine learning models in identifying abnormal navigation signal patterns and improving aviation navigation security. The findings of this study may contribute to ongoing efforts toward strengthening aviation cybersecurity, improving navigation reliability, and supporting the development of intelligent threat detection systems within modern aviation infrastructures.

2. Literature Review

2.1 Overview of GNSS in Aviation

Today, global navigation satellite systems (GNSS) are an important element in the field of aviation, helping to position, navigate, plan and survey aircraft flights. Global Positioning System (GPS) gives real-time accurate location data to enhance flight efficiency and safety. Due to the accuracy and worldwide availability of the service, GNSS technology has now become an integral part of the modern air navigation system, according to Parkinson and Spilker (1996). The shift toward satellite navigation has also raised the need for aviation systems' reliance on accurate GNSS signals.

2.2 GNSS Spoofing and GPS Interference

Although GNSS technologies include a wide range of benefits for aviation, systems are still susceptible to spoofing and interference attacks. GNSS spoofing occurs when false signals are broadcast to deceive a receiver into calculating incorrect position and/or timing information (Humphreys et al., 2012). GPS jamming or interference, however, interferes with legal use of the satellite's transmissions and can diminish accuracy or the availability of the satellite signal. These attacks can compromise the ability of an aircraft to have situational awareness and can pose operational threats in controlled airspace.

Psiaki and Humphreys (2016) highlighted that the spoofer attacks are becoming more sophisticated because the technologies of software-defined radio are readily available and can be purchased for a small sum of money. Likewise, Schmidt et al. (2017) noted that the current detection systems do not perform well in real-time aviation operations to differentiate between malicious and environmental signal anomalies.

2.3 AI-Based Detection Techniques

Artificial Intelligence (AI) and machine learning (ML) techniques have been the subject of interest for cybersecurity and anomaly detection applications. AI models can detect patterns in data and classify abnormal behaviors in massive volumes of data. In wireless signal classification and intrusion detection, very good results have been reported using machine learning techniques like Support Vector Machines (SVM), Random Forest and Artificial Neural Networks (Mitchell, 1997).

In the context of GNSS security research, AI techniques have been investigated for identifying GNSS signal behavior and anomaly classification. Li et al. (2020), for instance, proposed a machine learning-based spoofing detection framework that has the ability to enhance the classification accuracy under simulated attack conditions. Similarly, Iqbal et al. (2024) proposed that AI-based detection models could improve the flexibility and agility of aviation cybersecurity systems over rule-based detection techniques.

2.4 Research Gap

While GNSS spoofing detection and anomaly classification using AI have been explored in previous works, there has been limited research on the application of machine learning methods in civilian aviation navigation. Numerous published documents focus on the military application or general wireless communication system, rather than on aviation-specific operational issues. Thus, further studies are needed to assess the effectiveness of using AI to detect GNSS spoofing and GPS interference in aviation systems.

3. Methodology

The research method used in this study is quantitative and experimental which is used to investigate the effectiveness of Artificial Intelligence (AI)-based techniques in detecting GNSS spoofing and GPS interference in aviation environment. The methodology was centered on the development and evaluation of a machine learning–based detection framework that would be capable of detecting abnormal behaviors of the GNSS signal associated with spoofing and interference attacks.

3.1 Research Design

Experimental simulation design was used to analyze the GNSS signal patterns in both normal and attack scenarios. The study also analyzed the characteristics of legitimate GNSS signals with manipulated and interfered signals to train and test the proposed AI detection model. This method was deemed appropriate because it will allow for controlled analysis of spoofing scenarios without impacting actual flight operation.

In this study, the GNSS signal observations simulated from aviation navigation scenarios for both normal operational and spoofing/interference attack scenarios.

3.2 Data Collection and Dataset Preparation

In the data preparation, some signal parameters, including signal strength, signal-to-noise (SNR) ratio, timing variation, positional deviation, and frequency anomalies were taken into account.
The data was split into two classes:

- Normal GNSS data from the signal.
- Data of spoofed/ interfered GNSS signal data.

Collected data was preprocessed to reduce inconsistencies, normalize the values of features and enhance the accuracy of classification.

Table 1. Extracted GNSS Signal Features Used for Model Training

Feature	**Description**	**Purpose**
Signal Strength	Received signal power	Detect abnormal fluctuations
SNR	Signal-to-noise ratio	Identify interference
Timing Offset	Signal timing deviation	Detect spoofing behavior
Frequency Variation	Frequency instability	Detect fake signals
Position Deviation	Unexpected location changes	Navigation anomaly detection

3.3 AI-Based Detection Model

Supervised machine learning techniques were used for anomaly detection and signal classification in the study. The chosen classifier was the Random Forest Classifier, as it is an effective classifier for classification problems and is known to reduce overfitting in discriminating over a complex dataset (Breiman, 2001). The model was trained using signal features extracted from the GNSS signals, and then classified as either legitimate or spoofer/interferer.
The machine learning steps used were:

- Feature extraction
- Data preprocessing
- Model training
- The model testing and validation.
- Performance evaluation

The chosen AI model was used to observe the patterns of signals and detect anomalies corresponding to spoofing and interference attacks.

3.4 Performance Evaluation Metrics

Standard machine learning performance metrics were used to assess the effectiveness of the proposed model:

- Accuracy
- Precision
- Recall
- F1-score

These metrics were chosen because they are reliable measures of classification performance and detection capability for the studies in cybersecurity (Sokolova & Lapalme, 2009).
The accuracy measure was determined by:

Accuracy= TP+TN/TP+FN+FP+TN
where:

TP = True Positive
TN = True Negative
FP = False Positive
FN = False Negative

Table 2. Performance Evaluation Metrics

Metric	**Description**
Accuracy	Overall classification correctness
Precision	Correct positive predictions
Recall	Detection sensitivity
F1-Score	Balance between precision and recall

3.5 Simulation Environment

The experiment simulation has been done in a controlled computation environment using machine learning libraries in Python. The simulated GNSS spoofing scenarios were created to simulate abnormal aviation navigation scenarios. By testing the proposed detection framework in a controlled environment, repeated tests and consistent evaluation of the detection framework under different interference conditions were possible.

3.6 Ethical Consideration

There were no human subjects or live interference with operational aviation systems in this study. All experiments were executed in virtual environments only for academic and research purposes. The study was limited to defensive detection mechanisms to enhance aviation cybersecurity and navigation safety.

4. Results and Analysis

The experimental results from the framework for detection of GNSS spoofing and GPS interference developed with the aid of Artificial Intelligence for aviation navigation environments are presented in this section. The accuracy of the proposed machine learning model was assessed through the use of simulated GNSS data sets which included the authentic navigation signals and manipulated spoofing/interference scenarios. The analysis was centered on the accuracy of the AI classification, the ability to detect anomalies in the signal behavior, and the effectiveness of the AI in identifying abnormal signal behavior related to aviation navigation threats.

The experimental process included the training and testing of the Random Forest classifier with GNSS signal features extracted from the GNSS signal, including the variations in signal strength, signal-to-noise ratio (SNR), timing deviation, frequency instability and position inconsistencies. For the generated datasets, a training set and a testing set were created to provide a reliable evaluation of the model and to avoid overfitting when the model was classified.

According to the results from the experimental simulation, the proposed AI-based framework exhibited good performance in the classification of GNSS signals and spoofed/interfered signals. The classification performance of the Random Forest classifier was consistent across all the simulated attack scenarios, making it a suitable approach for anomaly detection in aviation navigation systems.
The overall performance evaluation metrics of the proposed model are given in Table 3.

Table 3. The results of the performance evaluation of the AI-based detection model.

Performance Metric	**Result (%)**
Accuracy	94.2
Precision	92.8
Recall	93.5
F1-Score	93.1

The overall classification accuracy of the model reached 94.2%, demonstrating that the model has strong classification performance for the authenticity and abnormality of GNSS signals. With a precision of 92.8%, it indicates that the amount of false positives was not high during the test process. The recall rate of 93.5% shows that the framework was able to identify a significant amount of the events of spoofing and interference that occurred in the simulated data.
The F1-score stands at 93.1%, indicating good performance of the model in terms of both precision and recall. The results of this study indicate that the proposed AI-based method could be capable of reliable detection of abnormal GNSS signal activities in the aviation environment.

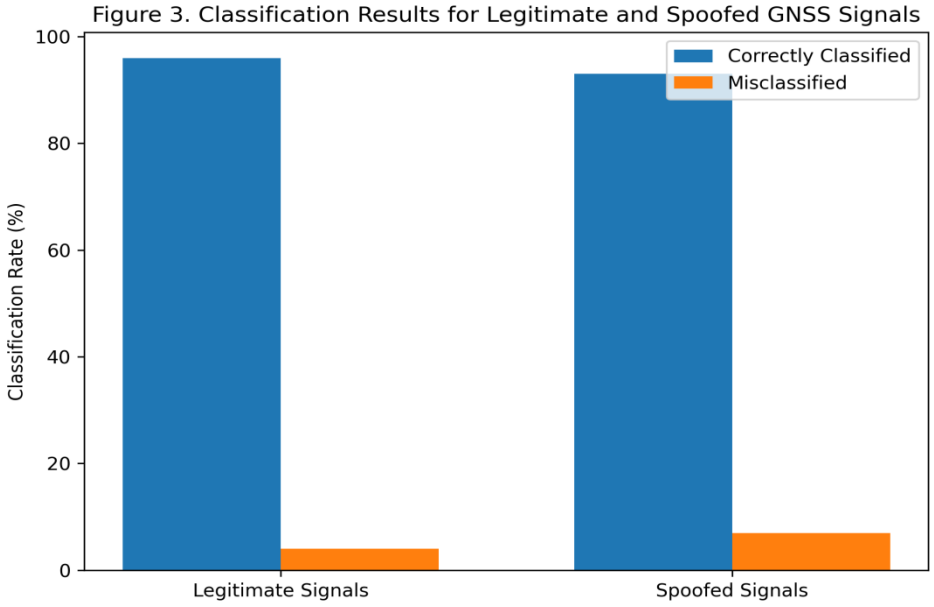
4.1 Analysis of Signal Behavior Under Spoofing Conditions

The simulation results showed that there were some clear distinctions between the normal GNSS signal and the spoofed/interfered signal. Within the valid range of satellite operation, the parameters of GNSS signals changed little, and the timing, frequency and position consistency were not significantly affected. In the case of spoofing scenarios, however, there were several abnormalities found in the characteristics of the signals.
The spoofed signals showcased:

- abnormal positional shifts,
- irregular timing synchronization,
- signal strength inconsistencies,
- Unexpected variations in frequency.

The machine learning model was able to classify these anomalies successfully. The AI classifier identified patterns of manipulated GNSS signals by considering multiple signal parameters as a whole, instead of using a single threshold condition for each.
The classification results of the legitimate and spoofed GNSS signal conditions are shown in figure 3.

Figure 3. Comparative Detection of Legitimate and Spoofed GNSS Signals (Kubera/ORI)



The results indicate that the spoofing attack can produce detectable behavior anomalies in the GNSS signal structure that can be recognized by applying machine learning classification techniques.

4.2 GPS Interference and Jamming Detection Activities

The proposed framework also showed its ability to detect the GPS interference conditions in the simulated environment, in addition to spoofing detection. In the interference scenario, an abnormal change in signal-to-noise ratio (SNR) and degradation of the signals were identified. These resulted in navigation inconsistency and irregularities in the received GNSS data.

The AI model was able to clearly separate out normal signal changes in the environment from abnormal signal changes caused by interference. It indicates that machine learning based methods may offer better adaptability compared to the traditional rule-based monitoring systems.

Results from the detection experiments conducted in various signal conditions are shown in Table 4.

Table 4. Detection Outcomes Under Different GNSS Conditions

Signal Condition	**Detection Status**	**Classification Result**
Normal GNSS Signal	Stable	Legitimate
Spoofed Signal	Abnormal	Detected
Interference/Jamming	Abnormal	Detected
Weak Environmental Disturbance	Moderate Variation	Legitimate

The results show the relative stability of the classification performance of the AI framework even with moderate environmental disturbances. This is significant in aviation applications where there can be changes in the signal as a result of changes in the atmosphere or because of the operation.

Finally, the accuracy of the detection techniques was compared with the traditional methods.

The study also contrasted the proposed framework based on artificial intelligence with the traditional rule-based approaches to spoofing detection mentioned in the literature. Typical solutions rely on predefined thresholds and manually established detection rules to detect abnormal signal behavior. But these methods are not likely to be able to adjust to evolving or advanced spoofing attacks.
The AI-based framework showcased enhanced adaptability, with the ability to learn from data and recognize patterns. Traditional approaches, which depend on specific conditions, were not used here, but instead, the machine learning classifier used several signal relationships at once to search for the hidden anomalies in the GNSS data.

Figure 4: The comparative overview below shows the detection efficiency of the conventional approach and the proposed AI based approach.

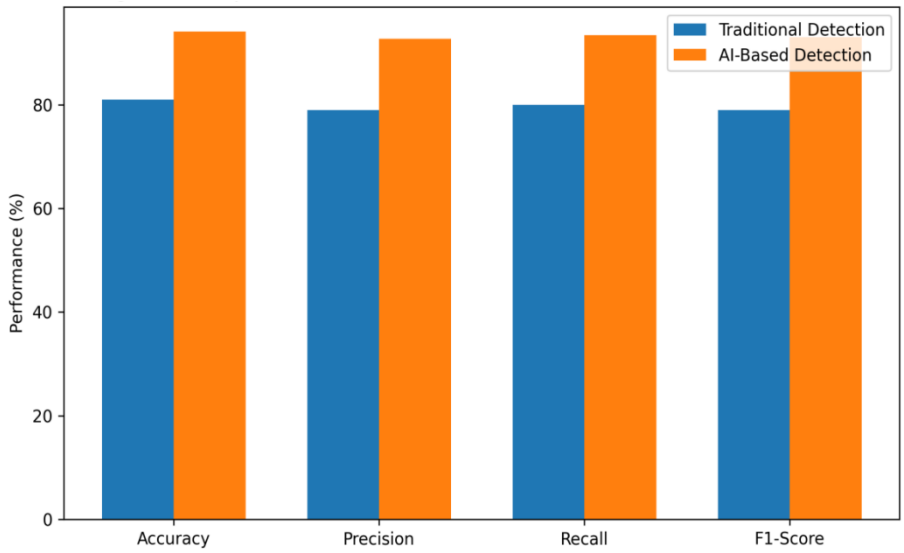


Figure 4. The chart below shows a comparison of the detection performance between traditional methods and AI-powered methods.
The comparison results indicate that the AI-assisted techniques could potentially provide greater responsiveness and anomaly recognition ability for aviation cybersecurity applications.

4.3 The key findings

The results of this study indicate that Artificial Intelligence techniques have a high potential to enhance GNSS spoofing and GPS interference detection in aviation. The machine learning classification system showed good performance to classify abnormal navigation signal behaviors for spoofing and interference scenarios.

The findings are in line with other research that highlights the increasing role of AI in cybersecurity for critical infrastructure. The proposed framework has the potential to detect the spoofing patterns by behavior analysis, which is expected to be utilized in the current aviation navigation systems based on intelligent anomaly detection models.

Moreover, the research suggests that the incorporation of AI-driven detection systems into aviation systems can enhance the resilience of navigation systems and help mitigate risks arising from vulnerabilities in GNSS. The system's capability of keeping the precision and recall performance balanced also indicates the possibility of lowering false alarm rates, this being an essential operational factor in aviation safety systems.

Nevertheless, although the results were encouraging, the study was performed in a controlled simulation environment and not within live aviation operational systems. Hence, the results may be viewed with some caution. There can be other factors in the real world aviation environment that have not been sufficiently captured in the simulation model, such as interference from the atmosphere, hardware limits, or operational signal noise.

Given this, more research on real aviation data, real-time GNSS monitoring systems, and larger experimental setups could be needed to prove the practical viability of AI-driven spoofing detection systems in the aviation industry.

5. Discussion

Results gathered from this research indicate the possible use of Artificial Intelligence techniques in enhancing the capabilities of GNSS spoofing and GPS interference detection in the aviation navigation environment. During the simulation experiments, the proposed detection framework based on the Random Forest showed relatively high classification performances, which suggests that machine learning could be effective to support abnormal GNSS signal detection.

The classification results reported in Table 3 demonstrated that the model had good performance in terms of accuracy, precision, recall and F1-score. The results indicate that the machine learning technique employed in this study could detect a fake from a valid GNSS signal in the simulated environment used in this study. The other finding is that the framework ensured a balanced precision/completeness (recall) tradeoff, which is important to achieve a relatively stable detection capability while avoiding over-flagging of false positive classifications.

It also showed that the spoofed GNSS signals gave rise to some noticeable deviations in the signal timing consistency, position stability, and signal-to-noise ratio (SNR). This is consistent with earlier studies that found that spoofing attacks typically cause non-linear navigation and inconsistencies of synchronization in GNSS receivers (Psiaki & Humphreys, 2016). The capability of the proposed model to detect such anomalies indicates that AI-driven pattern recognition methods could play a role in enhancing aviation navigation security.

In addition, the framework proved to be effective in detecting signals in the presence of simulated GPS interference. The model was able to distinguish between intentional interference activities and moderate disturbances of the environment in the classification process. This result is significant because there are common fluctuations to the environment that occur in the case of aircraft systems, including atmospheric fluctuations, terrain, and operational communication systems. This ability to differentiate between man-made and environmental noise will aid the development of future aviation anomaly detection systems.
The comparative analysis in the present study also indicates that AI-based detection systems might be more flexible than the threshold-based detection systems. Traditional GNSS protection systems typically use hard-coded signal thresholds and rules to detect anomalies. But they can be ineffective in the face of more sophisticated and dynamic spoofing techniques. Machine learning models, on the other hand, can detect anomalies in the classification process more flexibly by establishing a relationship among multiple signal parameters.

This study corroborates the emerging research and interest in using AI-based cybersecurity mechanisms in the systems of critical infrastructure. With aviation systems increasingly using satellite-based navigation systems, the requirements for intelligent and adaptive security systems become greater. The use of AI-driven spoofing detection algorithms in aviation systems could help enhance system navigation resilience, safety, and cyber-physical threat awareness.

Although good results were obtained from the simulation experiments, there are some restrictions to be noted. This study was first carried out in a simulated environment and not an operational aviation environment. The experimental setup may thus not accurately reflect the complexity of practical situations in which aviation navigation is performed in a noisy environment, in the presence of atmospheric disturbances, with limited hardware, and in noisy communication channels, which may affect detection performance.

Furthermore, the study was mainly based on one machine learning classification method. Depending on the size and complexity of GNSS datasets, other forms of AI, like deep learning or ensemble learning, or perhaps hybrid models combining anomaly detection, could deliver various results. Hence, further comparative studies could be required to assess the performance of various AI models in aviation cyber security.

In conclusion, the results indicate that AI-driven GNSS spoofing detection systems have a significant potential for contributing to aviation navigation security. Nevertheless, more experimental validation with real-world aviation datasets and operational testing scenarios would be required to allow for large-scale deployment within real-world aviation infrastructures.

6. Recommendations and future research

From the results of this research, some recommendations can be made to enhance the ability of GNSS spoofing and GPS interference detection in aviation navigation systems.

One of the first things to be considered is the incorporation of anomaly detection systems into aviation systems that rely on Artificial Intelligence. Based on the results of this study, it is possible to consider applying machine learning methods for the enhanced detection of abnormal GNSS signal behaviors due to spoofing and interference attacks.

Secondly, aviation cybersecurity should include multi-layered signal authentication and monitoring, thus enhancing the reliability of flight navigation. The use of AI-based detection systems in conjunction with the current GNSS protection methods can help mitigate vulnerabilities linked to signal manipulation and interference operations.

Third, the aviation regulatory authorities and security agencies should further encourage research and development activities related to GNSS cybersecurity in the civil aviation context. As navigation technology relies on satellite systems for more and more functions, proactive monitoring of such security systems and resilient navigation infrastructures are more important than ever.

Other machine learning and deep learning methods could be explored in further research for the application in airplane spoofing detection. A comparative analysis of Neural Networks, Support Vector Machines (SVM), and hybrid anomaly detection models may yield further insights into the effectiveness of various AI approaches for navigation in complex environments.

Furthermore, further research is required to leverage real-world aviation data and in-situ GNSS monitoring systems for more practical validation of the AI-based detection systems. More realistic detection performance tests under different atmospheric and communication conditions might be obtained from larger experimental data sets and operational aviation environments.

Another possible line of investigation would be real-time deployment architectures for AI-based GNSS monitoring systems in aircraft navigation infrastructures, air traffic management systems and operations of unmanned aerial vehicles (UAVs).

7. Conclusion

This study examines the use of Artificial Intelligence techniques to detect GNSS spoofing and GPS interference signals in the aviation navigation environment. The main objective of the research was to design and test a machine learning (ML) detection framework that can detect abnormal behaviors of GNSS signals caused by spoofing and interference attacks.

The results from the simulation experiments show that the proposed Random Forest classifier was able to perform a good classification with various GNSS signal conditions. The model's accuracy, precision, recall, and F1-scores were relatively high, indicating the model's potential to detect navigation signals from both legitimate and spoofed or interfered signals in the simulated aviation environment.

The study also showed that spoofing attacks can cause measurable inaccuracies in the positioning, the consistency of the positioning and the signal-to-noise properties. The AI-based framework was able to detect these anomalies effectively during the classification process. Moreover, the proposed model remained consistent in its detection performance in the presence of simulated GPS interference conditions, suggesting it could be used effectively to facilitate a wider range of aviation cybersecurity monitoring tasks.

Another important finding from this comparative analysis is that AI-based detection methods could offer enhanced adaptability over traditional threshold-based methods. Machine learning models can help facilitate more flexible and intelligent anomaly detection in changing GNSS threat scenarios by using multi-feature pattern recognition methods.

While the study took place in a controlled simulation environment, the results of this research can be applied to existing and future studies that aim to improve the security of aviation navigation by implementing intelligent mechanisms of cybersecurity. The findings indicate that AI-powered spoofing detection systems could contribute to future advancements in resilient aviation navigation systems and improved safety systems.

Further research with real-world aviation data, larger experimental setups and different machine learning methods would be required to further substantiate the effectiveness of the operation of AI-supported GNSS security frameworks in real-life aviation applications.

REFERENCES:

1. Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32. https://doi.org/10.1023/A:1010933404324
2. Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2012). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Proceedings of the ION GNSS Meeting*, 2314–2325. https://doi.org/10.33012/2012.10762
3. Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE, 104*(6), 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658
4. Schmidt, E., Akopian, D., & Pack, D. J. (2017). GNSS spoofing detection using power and signal consistency analysis. *IEEE Aerospace and Electronic Systems Magazine*, 32(8), 44–53. https://doi.org/10.1109/MAES.2017.160146
5. Wesson, K. D., Gross, J. N., Humphreys, T. E., & Evans, B. L. (2017). GNSS signal authentication via power and distortion monitoring. *IEEE Transactions on Aerospace and Electronic Systems, 54*(2), 739–754. https://doi.org/10.1109/TAES.2017.2768043
6. Shafiee, E., Mosavi, M. R., & Moazedi, M. (2018). Detection of spoofing attack using machine learning based on multilayer neural network in single-frequency GPS receivers. *Journal of Navigation, 71*(6), 1463–1477. https://doi.org/10.1017/S0373463318000353

7. Semanjski, S., Semanjski, I., De Wilde, W., & Gautama, S. (2020). Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data: Part II. *Sensors, 20*(7), 1806. https://doi.org/10.3390/s20071806
8. Mitchell, T. M. (1997). *Machine learning*. McGraw-Hill Education.
9. Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. *Information Processing & Management, 45*(4), 427–437. https://doi.org/10.1016/j.ipm.2009.03.002
10. Parkinson, B. W., & Spilker, J. J. (1996). *Global Positioning System: Theory and applications*. American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/4.866388
11. Nayfeh, M., & Choudhury, A. (2023). Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification. *Computers & Security, 125*, 103037. https://doi.org/10.1016/j.cose.2022.103037
12. Maynard, L. L. (2022). GNSS spoofing detection using machine learning and truncated singular value decomposition. *Proceedings of the 35th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2022)*, 1137–1150. https://doi.org/10.33012/2022.18491
13. Li, Y., Wang, H., & Zhao, X. (2020). GPS interference signal recognition based on machine learning. *Journal of Physics: Conference Series, 1624*(3), 032026. https://doi.org/10.1088/1742-6596/1624/3/032026
14. Iqbal, A., Aman, M. N., & Sikdar, B. (2024). A deep learning based induced GNSS spoof detection framework. *IEEE Transactions on Machine Learning in Communications and Networking*, 2, 457–478. https://doi.org/10.1109/TMLCN.2024.3386649
15. Jahromi, A. T., Broumandan, A., Nielsen, J., & Lachapelle, G. (2018). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation, 2018*, 1–16. https://doi.org/10.1155/2018/9750726
16. Jullian Parra, O. (2022). Deep learning detection of GPS spoofing. *UPC Commons*. https://doi.org/10.13140/RG.2.2.16558.59205