ӘУЕ КӨЛІГІ ЖӘНЕ ТЕХНОЛОГИЯЛАР
ВОЗДУШНЫЙ ТРАНСПОРТ И ТЕХНОЛОГИИ
AIR TRANSPORT AND TECHNOLOGY

**IRSTI 47.49.31**
**UDC 629.7.05**
**https://doi.org/10.53364/24138614_2025_39_4_3**

**I.A. Isgandarov**[1], **S.Z.Amirbayli**[1]

[1]Azerbaijan Airlines CJSC.National Aviation Academy, Azerbaijan, Baku

[*]*E-mail: sakhavat.amirbeyli@naa.edu.az*

# RADIOMETRIC–DNN HYBRID MODEL FOR AUTHENTICATING ADS-B SIGNALS

***Annotation.*** *This article explores the perspective opportunities for securely broadcasting the pulse signals emitted by the ADS-B (Automatic Dependent Surveillance–Broadcast) system, which is currently used in modern aviation systems, against external cyber threats. The objective is to enhance the security level of the existing infrastructure, optimize frequency assessment, and improve traffic management through predictive modeling, thereby enabling more efficient and proactive control. The proposed integration architecture employs deep learning algorithms to analyze aircraft signals and provides functionalities such as signal congestion management, real-time risk forecasting, and proactive prediction of weather and traffic changes. Furthermore, the article presents a performance evaluation of the system operating at 1090 MHz and 978 MHz frequencies and proposes methods for frequency optimization. Research results indicate that incorporating the recognition of device identification via radiometric fingerprints into the ADS-B platform not only enhances security and operational efficiency but also significantly improves the system's adaptability and responsiveness. This approach opens new avenues for the development of smarter and more predictable future aviation networks.*

***Keywords:*** *ADS-B technology, aviation safety, frequency optimization, real-time data processing, air traffic control.*

## Introduction.

Over the past ten years, the aviation industry has witnessed a transformative shift driven by rapid advancements in digital technologies and the integration of artificial intelligence. These innovations have significantly enhanced airspace surveillance, flight safety, and operational efficiency. Among these technologies, ADS-B [9] has emerged as a critical component of modern air traffic management, enabling the real-time broadcasting of an aircraft's position, speed, and other telemetry data using onboard GPS and transponder systems. However, as global air traffic density continues to increase, traditional ADS-B systems face growing challenges in managing frequency congestion, detecting anomalies, and predicting potential risks in dynamic flight environments. To overcome these limitations, researchers and industry experts are exploring the integration of artificial intelligence and machine learning (ML) models into ADS-B frameworks, thereby unlocking new analytical and predictive capabilities.

This paper introduces a next-generation ADS-B platform enhanced with algorithms designed to improve data processing accuracy, strengthen security outcomes, and support proactive airspace management strategies. The proposed system aims to provide a comprehensive solution for intelligent air traffic monitoring and forecasting by combining ML-based trajectory analysis, deep learning methods for anomaly detection, and frequency optimization techniques to mitigate cyber

threats during pulse broadcasting, utilizing both local computers and other aircraft in real time. The approach enables authentication of the signal source and more accurate detection of potential spoofing and anomalies by learning the RF fingerprint of the transmitter. The passive collection of radiometric data and its integration with the DNN architecture introduce an additional layer of security to the ADS-B system while remaining fully compatible with the existing infrastructure. This represents a new and innovative approach that significantly increases the resilience of the traditional ADS-B mechanism against external interference.

**Materials and Research Methods.**

ADS-B, or Automatic Dependent Surveillance-Broadcast, is an advanced surveillance technology that enhances air traffic control and situational awareness for pilots. It works by having aircraft automatically broadcast their GPS position, altitude, and other data to both air traffic control and other equipped aircraft, without requiring pilot or operator input. This information is transmitted using a digital data link, typically on 1090 MHz, and can be received by both ground stations and other aircraft equipped with ADS-B in capabilities.ADS-B refers to the Automatic Dependent Surveillance–Broadcast system. This technology functions automatically, meaning that the aircraft continuously transmits data without any intervention from the pilot or operator. The term dependent signifies that the system relies on navigation tools such as GPS or the Flight Management System (FMS) to determine the aircraft's position and velocity. The surveillance aspect reflects the system's ability to monitor and identify aircraft and other objects in three-dimensional space. The transmitted information includes parameters such as the aircraft's position, altitude, velocity, and call sign. These data are accessible to any individual equipped with suitable receiving equipment.

Due to this feature, ADS-B serves as a valuable tool for aircraft operators and air traffic controllers, contributing to safer and more efficient navigation especially within increasingly congested global airspace (Spire global. (n.d)). Let's take a look at the general operating principles of this system (Figure 1).

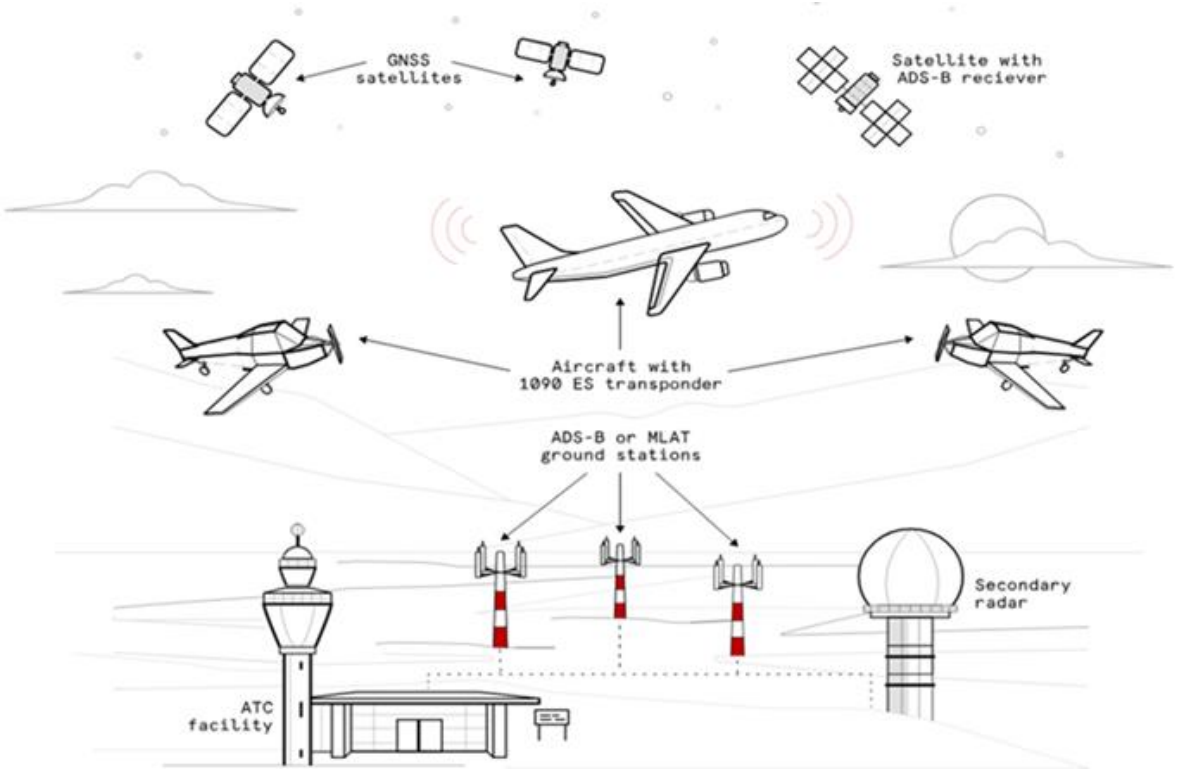


Figure 1 – General operating principles of this system (Spire global. (n.d))

ADS-B (Automatic Dependent Surveillance Broadcast) is an avionic system that enables aircraft to periodically transmit their navigation status without requiring interrogation (Spire global. (n.d)). It has evolved from the ATCRBS (Air Traffic Control Remote Beacon System) – Mode A, Mode C, and Mode S, and is specifically a variation of Mode S. Prior to the introduction of Mode A/C/S, the only method for detecting aircraft was the PSR (Primary Surveillance Radar), which could only provide slant distance and azimuth data [3]. ADS-B "In" enables aircraft to receive TIS-B (traffic data) and FIS-B (weather data), along with direct communication between aircraft (Figure 2).

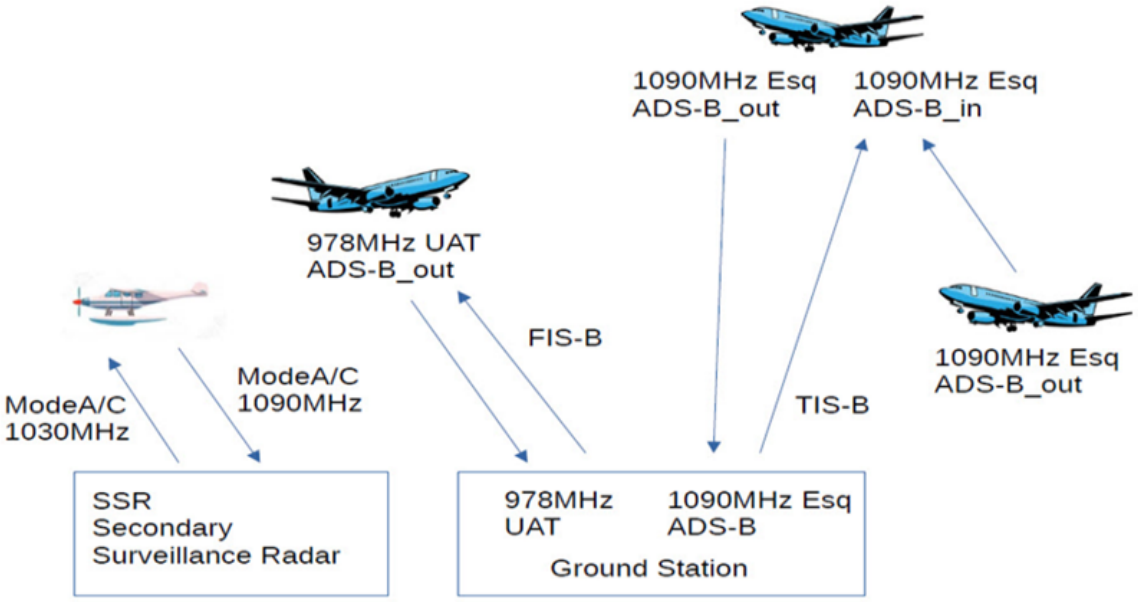


Figure 2 – ADS-B block diagram [2]

Figure 2 illustrates the block diagram of an ADS-B system. Traditional Mode A/C SSR (Secondary Surveillance Radar) systems operate by sending interrogation signals to aircraft on a frequency of 1030 MHz and receiving their responses at 1090 MHz. In contrast, aircraft fitted with ADS-B technology automatically transmit status data at regular intervals over the 1090 MHz frequency, and when appropriately equipped, they are also capable of receiving transmissions on the same frequency [3]. In order to utilize the ADS-B system, aircraft must be equipped with a Mode-S transponder or a beacon featuring ADS-B OUT functionality. To receive data from external sources, the aircraft must also be fitted with ADS-B IN capability. Aircraft equipped with ADS-B autonomously transmit their location data, which is received by both ground stations and satellite systems, ensuring reliable and efficient coverage regardless of environmental constraints [7].

Subsequently, the aircraft continuously transmits this positional data along with identification, flight altitude, velocity, and other relevant parameters. Specialized ADS-B ground stations, designed to receive these signals, collect the transmitted information and relay it to air traffic control authorities, thereby enabling precise tracking of the aircraft [6]. ADS-B data is transmitted every 0.5 seconds via a digital data link operating at a frequency of 1090 MHz, and similar to radar technology, its functionality is constrained by line-of-sight limitations. The ability of a ground station to receive these signals is influenced by the aircraft's altitude, its distance from the station, and the presence of obstructive terrain. The maximum surveillance range of an individual ground station may exceed 250 nautical miles [4]. Within the airspace surrounding each ground station, coverage typically extends to near ground level.

**Results and discussion.**

As noted, the Extended Squitter mode is generally a component of the ADS-B (Automatic Dependent Surveillance–Broadcast) system and operates at a frequency of 1090 MHz. These

signals are transmitted by Mode S transponders and automatically broadcast the aircraft's position, velocity, altitude, and other flight-related information. This technology is employed for radar-independent tracking and management of air traffic, thereby enhancing both the safety and efficiency of air navigation [2]. The Secondary Surveillance Radar (SSR) system consists of airborne transponders and ground-based interrogators/receivers (Figure 3). Mode A responses transmit the target's identification (Code 3/A), allowing the use of up to 4096 discrete codes [5]. Mode C responses, on the other hand, convey barometric altitude information.

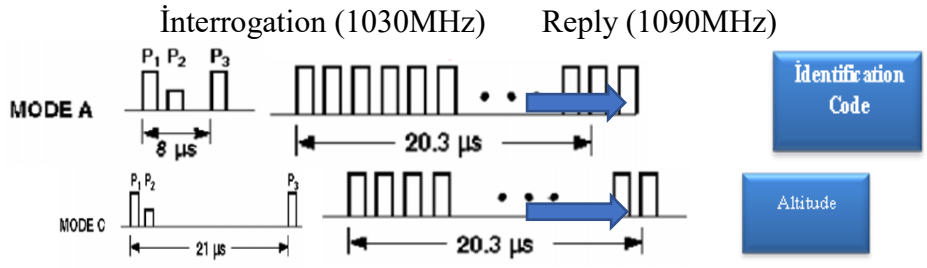


Figure 3 – Interrogation/Reception Pulse Modulation of the Secondary Surveillance Radar System in Mode A/C Operations [5]

- Data transmission rate: 1 Mbit/s
- Modulation method: PPM (Pulse Position Modulation)

Principle of Pulse Position Modulation:

Each bit interval is 1 microsecond in duration. The value of the bit is determined by the position of the pulse within this interval. If the pulse is transmitted in the first half of the interval (the initial 0.5 microseconds), it represents a binary "1"; [5] if the pulse is transmitted in the second half (the latter 0.5 microseconds), it represents a binary "0".

| Initiation Signal (Preamble) – 8 µs |
|---|
| 0 µs \| 1 µs \| 3.5 µs \| 4.5 µs |
| ↑ ↑ ↑ ↑ |
| Bits (1 µs each ) |
| Bit 1 \| Bit 2 \| Bit 3 \| ... |
| "1" → [↑ -] → pulse → pause |
| "0" → [- ↑] → pause → pulse |

Figure 4 – Bit Encoding Method

The preamble signal serves a critical role in the identification and synchronization of signal packets. These pulses act as a system-level alert, indicating the initiation of a transmission sequence. The encoding of bits is implemented using Pulse Position Modulation (PPM) [1] a technique in which the temporal placement of each pulse encodes the corresponding bit value (Figure 4). These signals are transmitted by aircraft transponders and received by radar systems [8] to facilitate the determination of the aircraft's spatial position, velocity, and unique identification.

Managing the identity of sending devices is considered one of the most important issues encountered in any network security system [10]. Because the source MAC address displayed on the display can be easily spoofed, network administrators must resort to additional authentication mechanisms to determine the real source of frames. The proposed approach aims to achieve physical-layer identification of the transmitter and relies on the utilization of unique, benign hardware imperfections (radio-frequency — RF artifacts) inherent to each Network Interface Card (NIC) and observable in the emitted signals. These RF artifacts appear in every transmitted pulse and serve as a distinctive "signature" of the corresponding transmitter; thus, by comparing them with a set of pre-recorded signatures, it becomes possible to accurately determine the identity of the transmitter [10].

Channel-specific features, on the other hand, are primarily used to identify the communication channel between the transmitter and the receiver (Figure 5). Consequently, radiometric identification can be regarded as a more specific and specialized form of the RF fingerprinting technique.

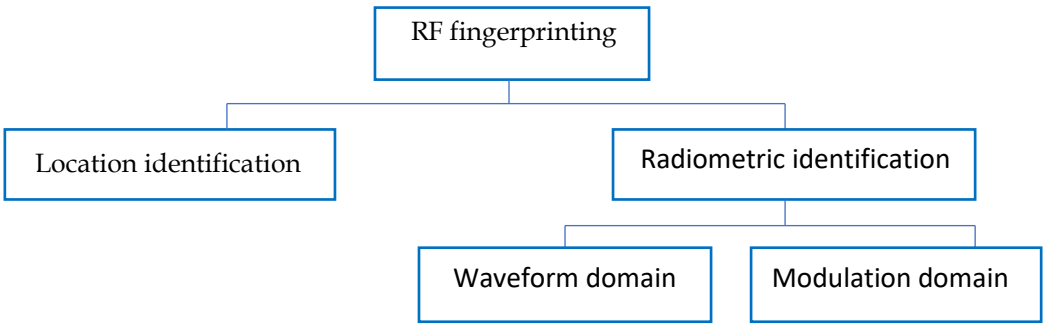


Figure 5 – Structural bases of radiometric identification (Brik V., Banerjee S., 2008)

Radiometric identification is based on the presence of benign hardware imperfections, also known as transmitter impairments, within transmitters. These impairments usually arise during the manufacturing and assembly stages of the analog components in the transmitter's RF front-end. The term "benign" indicates that these imperfections do not negatively affect communication quality and remain within the quality limits specified by impulse transmission standards. All analog components located in the transmission path of the NIC (Network Interface Card) — from interconnects to antennas — cause certain deviations in the emitted signal compared to the ideal one [10]. The main sources of these deviations are illustrated in Figure 6. In practice, although network interface cards produced using the same manufacturing and assembly processes may appear identical, each one is microscopically unique. While it is theoretically possible to eliminate such hardware imperfections through more precise manufacturing and quality control, this would significantly increase the overall cost of the devices. In fact, many technological standards require different NICs to tolerate a certain range of RF variations in received signals to ensure seamless interoperability. Therefore, the RF artifacts generated by these minor hardware imperfections specific to each transmitter can be effectively used to determine the unique identity of that particular transmitter.

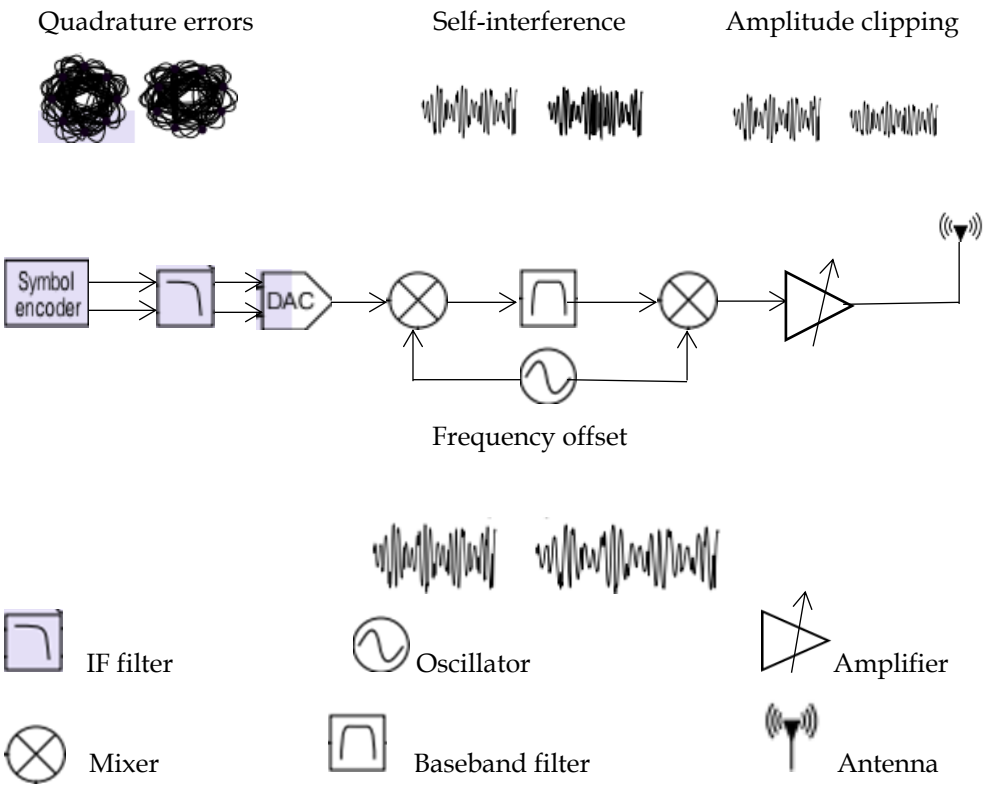


Figure 6 – Frequent transmitter malfunctions and their sources [10]

It should be noted that the foundation of a defined radiometric identification technique lies in the specific artifacts (unique signal characteristics) used to distinguish transmitters from one another. The selection of optimal artifacts for the differentiation process depends on several factors in particular, on the hardware and transmitter design, as well as the underlying communication technology. The concept of radiometric identification itself is not new. Since that time, similar systems have also been implemented by cellular networks, aiming to verify the authenticity of cellular transmitters and to prevent fraud. As such systems possess both commercial and military significance, very limited technical details about their implementation have been publicly disclosed [10]. Nevertheless, further evidence suggests that these systems utilize transient signal characteristics and waveform-level parameters for identification purposes.

The former was specifically developed for aviation services such as ADS-B and requires new hardware, whereas the latter integrates the ADS-B functionality into conventional Mode S transponders. Figure 7 illustrates the ADS-B message structure. Each message consists of an 8 μs preamble for synchronization and a 56-bit (short) or 112-bit (extended) data block. The first 5 bits of the data block indicate the downlink format (i.e., the message type). The subsequent 3-bit capability field serves as an additional identifier. The 24-bit ICAO address is a unique identifier assigned to each aircraft by the ICAO. The 56-bit extended ADS-B data field conveys surveillance information, including identification, position, velocity, and emergency codes [11].

The final field in the ADS-B message consists of a 24-bit parity check, which allows receivers to confirm the integrity of the preceding data. Within the 56-bit data section, the initial 5 bits indicate the Type Code (TC), defining the nature of the information carried in the remaining bits. Out of the 31 possible Type Codes, particular attention is given to messages conveying airborne position with barometric altitude (TCs 9–18) and airborne velocity data (TC 19). Transmission of ADS-B messages occurs approximately every 0.5 seconds, employing the Pulse Position Modulation (PPM) method. At a data rate of 1 Mbps, the total transmission time for an extended ADS-B message, including the preamble, is 120 microseconds [11].

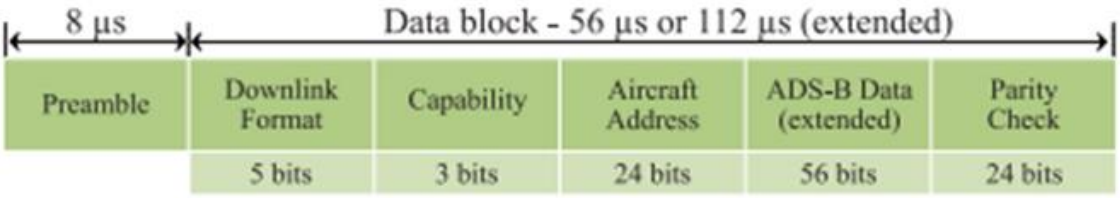


Figure 7 - The schematic representation of the ADS-B message structure demonstrates that each message contains an 8-µs preamble, succeeded by a data field of either 56 µs or 112 µs, according to the specific transmission format [11]

DNNs operate based on the principles of supervised learning, which require a substantial amount of labeled training data for effective performance. A typical DNN architecture consists of input, hidden, and output layers, where each layer comprises a specific number of neurons (nodes). The number of neurons in the input layer corresponds to the number of features in the dataset, while the number of output neurons typically matches the number of classes or labels. The number of hidden layers and the neurons within each layer are considered tunable hyperparameters that define the network's capacity and complexity [11]. In a feed-forward DNN with j hidden neurons, each neuron transforms its input signal, denoted as $x_j$, into an output state $y_j$ through an activation function. This relationship can be mathematically expressed as:

$$x_j = b_j + \sum_i y_i w_{ij} \quad (1)$$

where $b_j$ represents the bias of the j-th neuron, $y_i$ denotes the output value of the i-th neuron in the preceding layer, and $w_{ij}$ is the weight coefficient (equation 1) connecting neuron i to neuron j. The activation function allows the model to learn nonlinear relationships within data, thereby enhancing the network's ability to recognize complex patterns. ADS-B operates as a wireless communication protocol in which messages are transmitted without inherent security mechanisms such as encryption or authentication, rendering the system susceptible to multiple attack vectors [9]. Key threats to ADS-B include eavesdropping, message tampering, signal jamming, and identity spoofing (Figure 8).

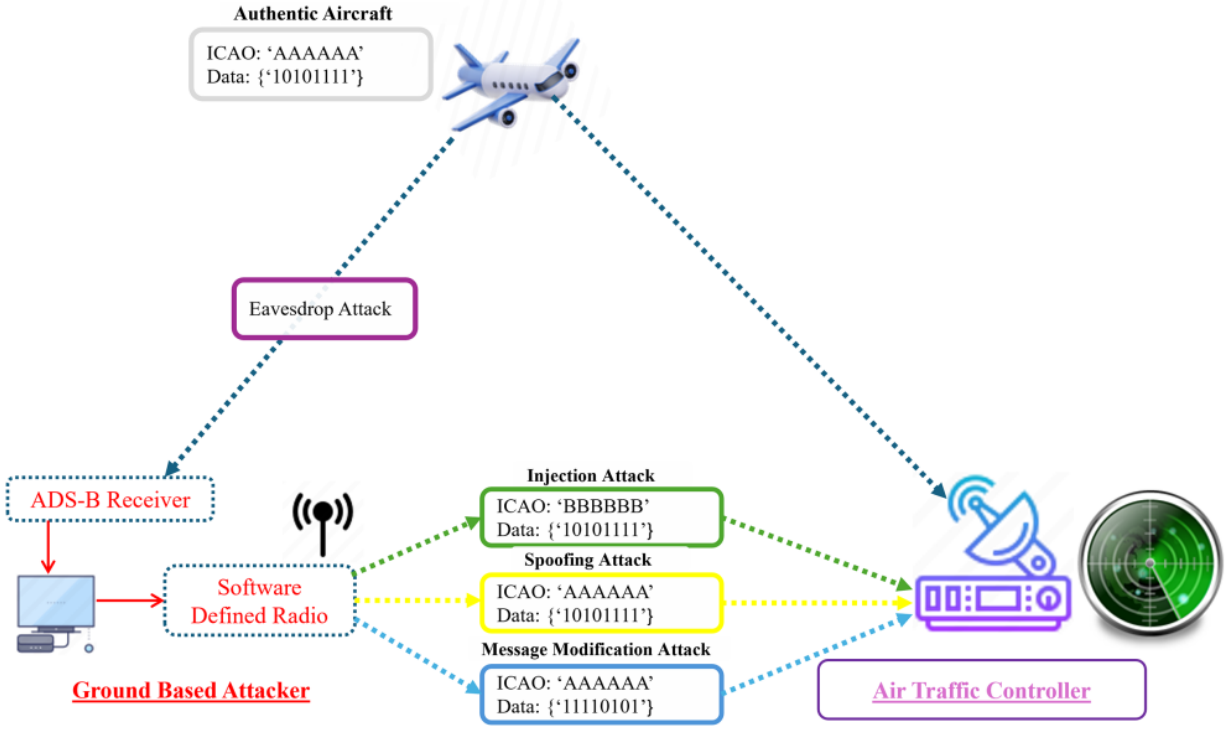


Figure 8 – Conceptual illustration of ADS-B security threats executed by a terrestrial adversary, including signal interception, message manipulation, message injection, and identity spoofing [9]

In contrast to traditional message classification methods, the proposed aircraft classifier does not employ IQ samples or their magnitude values, which directly encode the ICAO address, during the feature extraction stage. This design choice is intended to prevent the classifier from being misled by falsified or manipulated ICAO address information. Instead, the model utilizes phase components that are independent of the claimed ICAO address as the primary discriminative features. Consequently, the phase value of the k-th pair of IQ samples is computed as follows:

$$\phi_k = tan^{-1}(Q_k / I_k) \quad (2)$$

where Ik and Qk denote the in-phase (I) and quadrature (Q) components of the k-th IQ sample, respectively (equation 2). From communication theory, it is well established that the phase components encode information related to the transmitter (TX) and receiver (RX) carrier frequency offsets, as well as the Doppler shift. To illustrate this relationship more clearly, the passband ADS-B signal can be represented as follows:

$$x_p(t) = Re\{\sqrt{2}x(t)c^{j2\pi f_c t}\} \quad (3)$$

This expression (equation 3) illustrates the generation of the real passband signal xp(t) based on the complex baseband signal x(t).

In this context, x(t)=xi(t)+jxq(t) represents the complex baseband signal, while fc denotes the carrier frequency, which is 1090 MHz in ADS-B systems.

Due to the presence of a carrier frequency offset Δf and a phase offset Δϕ the overall form of the signal is modified as follows:

$$\overline{X_p}(t) = Re\{\sqrt{2}x(t)c^{j2\pi(f_c+\Delta f)t+\Delta\varphi}\} = Re\{\sqrt{2}\left(x(t)c^{j\varphi(t)}\right)c^{j2\pi f_c t}\} \quad (4)$$

Here, $\phi(t)=2\pi\Delta ft+\Delta\phi$ is expressed accordingly.Thus, the rate of change of the phase reflects the carrier frequency offset, which is determined by the combined effect of the transmitter (TX) and receiver (RX) frequency mismatches (equation 4), as well as the Doppler shift, and may also be influenced by the propagation channel.

Consequently, the phase components carry valuable information about the dynamic characteristics of the signal, making them a rich source of features that can be effectively utilized in classification models (Ying X., Mazer J., Bernieriy G., 2019).

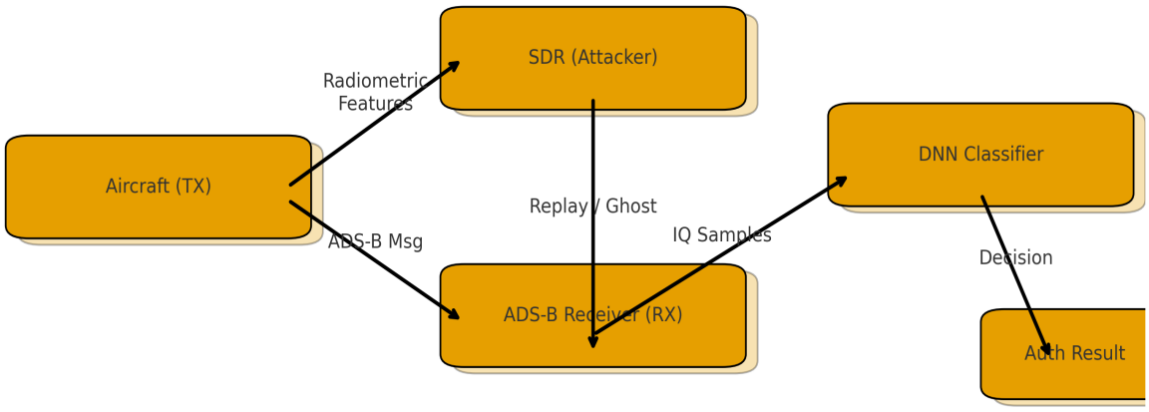


Figure 9 – Radiometric combined with DNN ensures ADS-B message authenticity (Wikipedia, n.d)

This model (Figure 9-10) combines radiometric identification (unique RF traits) with DNN-based learning to ensure ADS-B message authenticity, thereby enhancing cybersecurity in air traffic communication systems.

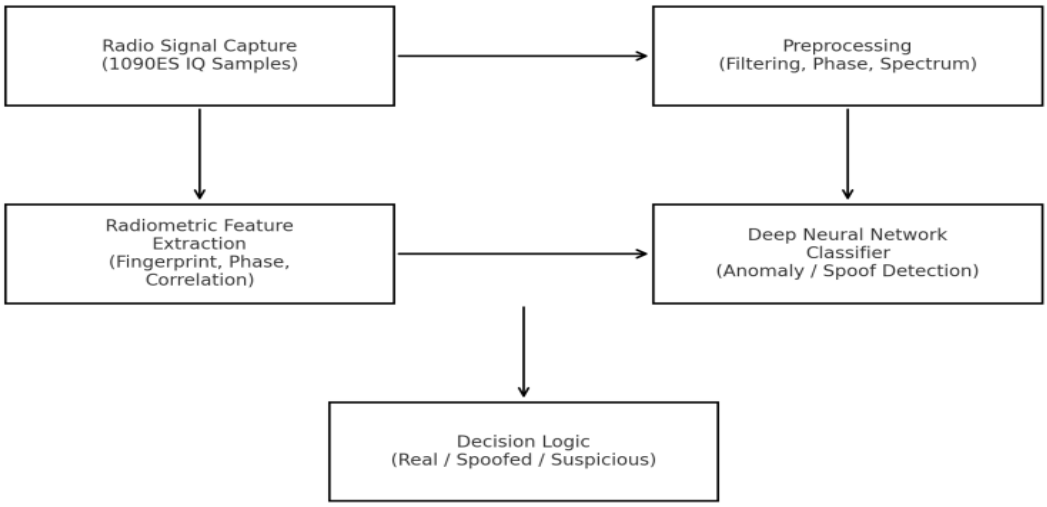


Figure 10 – Radiometric-DNN Hybrid ADS-B Protection Model

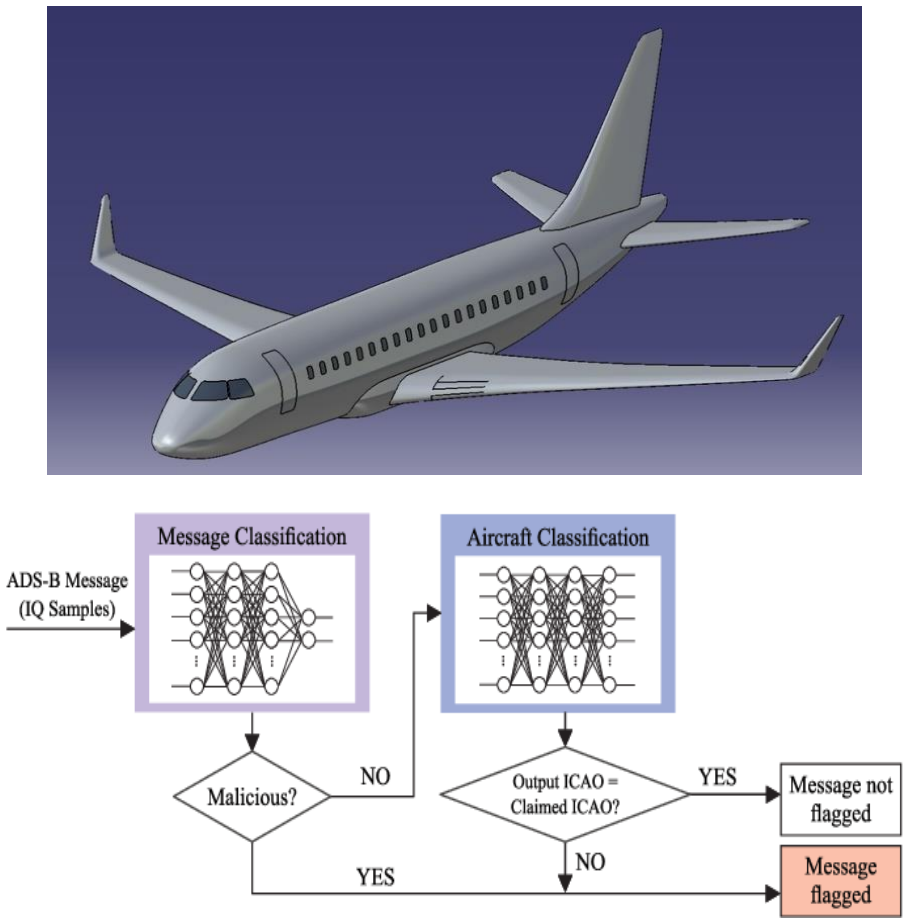


Figure 11 – Illustration of DNN-based detection of ADS-B signal spoofing [11]

The DNN-based approach for detecting ADS-B signal spoofing enables automatic modeling of the multidimensional statistics of signal and trajectory data. The core idea of the method is that the DNN learns normal behavioral patterns characteristic of genuine flights (such as position sequence consistency, speed-distance correlation, altitude variation trends, message interval stability, etc.) and then compares the incoming ADS-B packets against these learned patterns (Figure 11). During spoofing, physically impossible deviations, spatio-temporal inconsistencies, trajectory discontinuities, and signal-level anomalies emerge within these patterns, allowing the DNN to identify such irregularities as anomalies. Consequently, the model accurately detects falsified ADS-B messages based on flight dynamics and signal features, thereby enhancing the reliability of the air traffic surveillance system.

Table 1 – Comparative performance of radiometric fingerprinting and DNN in ADS-B signal authentication (Author's work)

| Metric / Aspect | Radiometric Fingerprint | Deep Neural Network (DNN) | Hybrid (Radiometric+ DNN) |
|---|---|---|---|
| Authentication Accuracy (%) | 89.6 ± 1.8 | 93.4 ± 1.2 | 98.1 ± 0.7 |
| False Positive Rate (FPR) | $3.7 \times 10^{2}$ | $2.1 \times 10^{2}$ | $7.9 \times 10^{3}$ |
| False Negative Rate (FNR) | $5.8 \times 10^{2}$ | $4.4 \times 10^{2}$ | $1.6 \times 10^{2}$ |

| | | | |
|---|---|---|---|
| Average Detection Latency (ms) | 320 ± 25 | 180 ± 20 | 240 ± 22 |
| Model Size (MB) | 1.3 | 54.7 | 56.2 |
| Training Data Required (samples) | $2 \times 10^3$ | $4 \times 10^3$ | $8 \times 10^3$ |
| Robustness vs. SNR (down to dB) | 8 | 5 | 3 |
| Replay Attack Detection (%) | 91.2 | 96.8 | 99.1 |
| UniqueTransmitter Identification Precision (%) | 92.7 | 94.3 | 98.5 |
| Inference Time (per packet, ms) | 65 ± 5 | 18 ± 3 | 22 ± 4 |
| Explainability (1–5) | 5 | 3 | 4 |
| Computational Cost (relative units) | 1.0× | 3.7× | 2.4× |
| Overall Security Gain (%) | - | - | +22.3 |

This table compares three different approaches for ADS-B signal authentication: Radiometric Fingerprinting, Deep Neural Network (DNN), and the Hybrid Radiometric–DNN model. The results indicate that the hybrid model achieves the highest accuracy (98.1 %) while maintaining the lowest false positive and false negative rates ($0.79 \times 10^{-2}$ and $1.6 \times 10^{-2}$, respectively). Radiometric fingerprinting offers the highest explainability (5/5) with minimal computational cost, whereas the DNN model provides faster signal detection but at the expense of larger model size and higher computational requirements. The hybrid model optimizes both accuracy and security gains (+22.3 %), and it more effectively detects replay attacks and identifies unique transmitters. Additionally, the table presents each method's training data requirements, detection latency, and robustness under varying SNR conditions.

**Conclusion.**

In this article, we present a tested conceptual and methodological framework that combines deep neural networks (DNNs) with radiometric fingerprinting and frequency characteristics to detect and mitigate cyber-attacks on ADS-B systems, including threats originating from ground stations and other aircraft. Radiometric fingerprints capture unique patterns arising from the physical, electromagnetic, and frequency properties of transmitter hardware, enabling identification independently of message content, protocol compliance, or frequency variations. DNNs provide a powerful tool to learn these high-dimensional and complex patterns: they can accurately distinguish spoofed or replayed messages by learning both observed signal variations and frequency offsets, while maintaining generalization under varying signal-to-noise ratios, channel conditions, flight dynamics, and frequency fluctuations. The proposed methodology enhances both early attack detection and system resilience in practical deployment. A two-tier verification process based on radiometric and frequency features—protocol and frequency compliance checking at the first level, followed by transmitter fingerprint confirmation at the second level—reduces false positives and false negatives, thereby adding robust defense layers to air traffic security. Future research should focus on expanding datasets across diverse hardware, optimizing workload distribution between edge and cloud computing, and enhancing DNN interpretability and robustness through uncertainty estimation and adversarial defense mechanisms. A DNN-based approach reinforced with radiometric and frequency fingerprinting offers a promising and practically implementable solution for defending ADS-B infrastructure against cyber threats. It complements existing protocol and frequency checks to improve detection sensitivity, while laying the foundation for adaptive and scalable security mechanisms. Reliable

operation requires ongoing experimental validation, regulatory compliance, and careful management of technical and ethical considerations.

## References

1. Carey, B. (2014). India Completes ADS-B Ground Network Installation. https://www.ainonline.com/aviation-news/air-transport/2014-06-13/india-completes-ads-b-ground-network-installation

2. ComSoft ComSoft. (2009, March). Further ADS-B installations in Abu Dhabi through COMSOFT. Retrieved May 13, 2010. https://www.atc-network.com/atc-news/further-ads-b-installations-in-abu-dhabi-through-comsoft

3. Clark J. (2021). E-Books on Telecommunications, Navigation & Electronics.

4. Airservices Australia. (2010). ADS-B Flight Operations Information PackageV4.0. https://www.airservicesaustralia.com/wpcontent/uploads/UAP_Flight_Ops_Info_Package_V4.0.pdf

5. European Organisation for the Safety of Air Navigation. (2019). ADS-B for Dummies 1090MHz Extended Squitter.https://www.sigidwiki.com/images/1/15/ADS-B_for_dummies

6. Mozdzanowska, Aleksandra, Weibel, R., Lester, E., Hansman, R., Weigel, A. & Marais, K. (18–20 September 2007). Dynamics of Air Transportation System Transition and Implications for ADS-B Equipage. Belfast, Northern Ireland: AIAA. https://dspace.mit.edu/bitstream/handle/1721.1/39093/ATIO-ADS-B-transition-2007.pdf?sequence=1

7. Spire global. (n.d). ADS-B systems and technologies in aviation,more internet resource https://spire.com/wiki/how-does-ads-b-work

8. Tong Z. (6 January 2024). China targets devices it says are used to send flight data to foreign entities. South China Morning Post. http: //China targets devices it says are used to send flight data to foreign entities

9. Ahmed, W., Masood, A., Manzoor, J., & Akleylek, S. (2025, June 9). Automatic dependent surveillance-broadcast (ADS-B) anomalous messages and attack type detection: deep learning-based architecture. PeerJ Computer Science. https://doi.org/10.7717/peerj-cs.2886

10. Brik, V., Banerjee, S., Gruteser, M. & Oh, S. (2008). Wireless device identification. Proceedings of the 14th ACM international on Mobile computing and networking,116 – 127. https://wings.cs.wisc.edu/publications/wireless-device-identification-with-radiometric-signatures/

11. Ying, X., Mazer, J., Bernieriy, G., Contiy, M., Bushnell, L. & Poovendran R. (2019). Detecting ADS-B Spoofing. 2019. IEEE Conference on CommunicationsandNetworkSecurity(CNS),187-195https://doi.org/10.48550/arXiv.1904.09969

## ADS-B СИГНАЛДАРЫН АУТЕНТИФИКАЦИЯЛАУҒА АРНАЛҒАН РАДИОМЕТРИЯЛЫҚ–DNN ГИБРИДТІ МОДЕЛІ

***Аңдатпа***. *Бұл мақалада қазіргі заманғы авиация жүйелерінде қолданылатын ADS-B (Автоматты тәуелді бақылау-тарату) жүйесі шығаратын импульстік сигналдарды сыртқы киберқауіптерге қарсы қауіпсіз таратудың перспективалық мүмкіндіктері қарастырылады. Мақсат - қолданыстағы инфрақұрылымның қауіпсіздік деңгейін арттыру, жиілікті бағалауды оңтайландыру және болжамды модельдеу арқылы трафикті басқаруды жақсарту, осылайша тиімдірек және белсенді бақылауды қамтамасыз ету. Ұсынылған интеграция архитектурасы әуе кемелерінің сигналдарын талдау үшін терең оқыту алгоритмдерін пайдаланады және сигналдың кептелісін басқару, нақты уақыт режимінде тәуекелдерді болжау және ауа райы мен трафиктің өзгеруін белсенді түрде болжау сияқты функцияларды қамтамасыз етеді. Сонымен қатар, мақалада 1090 МГц және 978 МГц жиіліктерінде жұмыс істейтін жүйенің өнімділігін*

*бағалау және жиілікті оңтайландыру әдістері ұсынылады. Зерттеу нәтижелері ADS-B платформасына радиометриялық саусақ іздері арқылы құрылғыны сәйкестендіруді тануды енгізу қауіпсіздік пен пайдалану тиімділігін арттырып қана қоймай, сонымен қатар жүйенің бейімделуі мен жауап беру қабілетін айтарлықтай жақсартатынын көрсетеді. Бұл тәсіл ақылды және болжамды болашақ авиация желілерін дамыту үшін жаңа жолдар ашады.*

***Түйін сөздер**: ADS-B технологиясы, авиациялық қауіпсіздік, жиілікті оңтайландыру, нақты уақыт режимінде деректерді өңдеу, әуе қозғалысын басқару.*

## ГИБРИДНАЯ РАДИОМЕТРИЧЕСКИ-DNN-МОДЕЛЬ ДЛЯ АУТЕНТИФИКАЦИИ СИГНАЛОВ ADS-B

***Аннотация.** В данной статье рассматриваются перспективные возможности безопасной трансляции импульсных сигналов, излучаемых системой ADS-B (автоматическое зависимое наблюдение – вещание), которая в настоящее время используется в современных авиационных системах, для защиты от внешних киберугроз. Целью является повышение уровня безопасности существующей инфраструктуры, оптимизация оценки частот и улучшение управления дорожным движением посредством предиктивного моделирования, что обеспечивает более эффективное и проактивное управление. Предлагаемая архитектура интеграции использует алгоритмы глубокого обучения для анализа сигналов воздушных судов и обеспечивает такие функции, как управление перегрузкой сигналов, прогнозирование рисков в реальном времени и проактивное прогнозирование изменений погоды и дорожного движения. Кроме того, в статье представлена оценка производительности системы, работающей на частотах 1090 МГц и 978 МГц, и предлагаются методы оптимизации частот. Результаты исследований показывают, что включение распознавания идентификационных данных устройств по радиометрическим отпечаткам в платформу ADS-B не только повышает безопасность и эксплуатационную эффективность, но и значительно улучшает адаптивность и скорость реагирования системы. Такой подход открывает новые возможности для разработки более интеллектуальных и предсказуемых будущих авиационных сетей.*

***Ключевые слова:** Технология ADS-B, безопасность полетов, оптимизация частоты, обработка данных в реальном времени, управление воздушным движением.*

**Сведение об авторах**



| | |
|---|---|
| Ислам Искендеров | Доктор технических наук, профессор, заведующий кафедрой Национальной авиационной академии, Азербайджан, Баку E-mail: iisgandarov@naa.edu.az |
| Сахават Амирбейли | Магистр, главный лаборант и преподаватель кафедры Национальной авиационной академии, Азербайджан, Баку Электронная почта: sakhavat.amirbeyli@naa.edu.az |



**Авторлар туралы мәлімет**



| | |
|---|---|
| Ислам Исгандаров | PhD, профессор, Ұлттық авиация академиясының кафедра меңгерушісі, Әзербайжан, Баку E-mail: iisgandarov@naa.edu.az |
| Сахават Амирбейли | Ұлттық авиация академиясының магистрі, кафедраның бас лаборанты және оқытушысы, Әзербайжан, Баку Электронная почта: sakhavat.amirbeyli@naa.edu.az |



**Information about the authors**



| | |
|---|---|
| Islam Isgandarov | PhD,Professor,Head of Department at the National Aviation Academy, Azerbaijan, Baku E-mail: iisgandarov@naa.edu.az |
| Sakhavat Amirbayli | Master, Senior laboratory assistant and Lecturer of Department at the National Aviation Academy, Azerbaijan, Baku E-mail: sakhavat.amirbeyli@naa.edu.az |