3rd URSI AT-AP-RASC, Gran Canaria, 29 May – 3 June 2022

E-Fin: Enabling RF Fingerprinting for Real-world aircraft with Few Labeled ADS-B Signals

Guyue Li[1,3], Jitong Shi [1], Jiabao Yu[3] and Aiqun Hu[2]
(1) School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China
(2) National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China
(3) Purple Mountain Laboratory, Nanjing 210096, China
{guyuelee, jtshi, aqhu}@seu.edu.cn; yujiabao@pmlabs.com.cn

Abstract

Automatic Dependent Surveillance-Broadcast (ADS-B) surveillance faces various security threats on tampering due to the absence of authentication support. The emerging device identification technology of radio frequency fingerprinting (RFF), despite its promising, faces challenges in identifying practical aircraft with few labeled ADS-B signals. To address this issue, we have proposed a novel RF fingerprint identification approach, referred to as E-Fin, which was designed based on zero-padding preprocessing and a CNN classifier. The proposed algorithm provided a solution for aircraft identification with few labeled ADS-B signals. Experiments were conducted on real ADS-B data to compare the proposed method with previous approaches, and the comparison results illustrated its effectiveness and accuracy.

1. Introduction

As a cornerstone of the next-generation digital sky, Auto-Dependent Surveillance-Broadcast (ADS-B) system has been mandated for aircraft tracking and flight management operations in the airspaces of several countries, e.g., U.S and Europe since 2020 [1]. However, ADS-B lacks basic security mechanisms, such as data encryption and message authentication, and thus has been found prone to a large number of attacks, e.g., spoofing, eavesdropping, jamming, replay and message modification [2]. When an attacker interferes or modifies the navigation signal, flight safety is compromised [3].

Although many cryptographic countermeasures have been proposed to secure ADS-B through encryption algorithms, they encounter difficulties of conflicting with the open nature of ADS-B broadcast and complicate key management in large-scale, distributed, and dynamic environments of ADS-B. Therefore, it is extremely desirable for an effective and practical alternative to enhance ADS-B security, considering realistic requirements of privacy, authenticity, performance, and compatibility in air traffic monitoring and control.

Recently, radio frequency (RF) fingerprinting has emerged as a new paradigm that extracts the intrinsic hardware features from a radio signal to identify which device the signal comes from. Specifically, hardware features, e.g., transient phase, modulation error, timing error, frequency offset and power perturbation, extracted from signal waveforms, are regarded as universal, distinctive and permanent, and thus can act as the unique fingerprint for the device [4]. Unlike MAC or IP address, RF fingerprint is difficult to forge, and can hence be employed to identify fake signals sent by rogue devices.

Although a large number of works have recently appeared on the topic of RF fingerprint classification and authentication for various internet of things (IoT) devices, as of yet, only a few works have investigated this promising technique for aircraft identification. Leonardi et.al classified seven kinds of aircraft using ADS-B message's phase pattern, however, they have not realized individual identification [5]. Zha et.al proposed an RF fingerprint recognition method which transforms raw signals into contour stellar images and applies a trained deep learning neural network to classify each aircraft's ADS-B RF emissions [6]. Experimental results showed that when the signal-to-noise ratio (SNR) is greater than 28 dB, their method can achieve a classification accuracy rate higher than 90% on 1090 MHz Extended Squitter (1090ES) ADS-B signals collected by RTL-SDR from five different aircraft. However, their classification accuracy also shows a rapid deterioration at low SNR, e.g., roughly 70% at 10 dB. Unfortunately, regarding the aircraft application, the SNR is usually lower than 20 dB and the interference is severe for 1090ES ADS-B signals. Moreover, these negative effects of noise and interference on RF fingerprint identification accuracy will be more apparent with the reduction of labeled data for neural network training and the rise of the number of classification categories.

On the whole, it is still missing how to enable RF fingerprinting to identify aircraft in practical scenarios. Inspired by the unique waveform of ADS-B signals, we propose a novel RF fingerprint identification approach, referred to as E-Fin, to classify a large number of aircraft with a few labeled signals. The main contributions of this paper are listed as follows:

- We propose a zero-padding based preprocessing algorithm to reduce the negative effect of environments on ADS-B signals. This algorithm enhances the quality of raw signals through detecting the region of interest and wiping out signals that are entirely caused by noise and interference.
- We realize feature extraction through various trained convolutional neural networks (CNNs). To address the problem of insufficient training data, we expand

the dataset using overlapped sliding windows and obtain a robust identification result through a voting taken by all overlapped samples.

- We verify the effectiveness of the proposed approach on over-the-air ADS-B signals from 100 aircraft in the open and real-world scenarios. Experimental results show that compared to the state-of-the-art, the proposed E-Fin approach largely improves the identification accuracy, especially in few-shot scenarios.

2. System Overview

In this section, we overview the proposed RF fingerprint identification approach, E-Fin, which works on the popular ADS-B data link standard of 1090ES. We assumed that raw signals, i.e., I/Q signals, have been obtained through existing signal detection algorithms for ADS-B [7]. Fig. 1 describes the process workflow of E-Fin, which consists of a training stage and an identification stage.

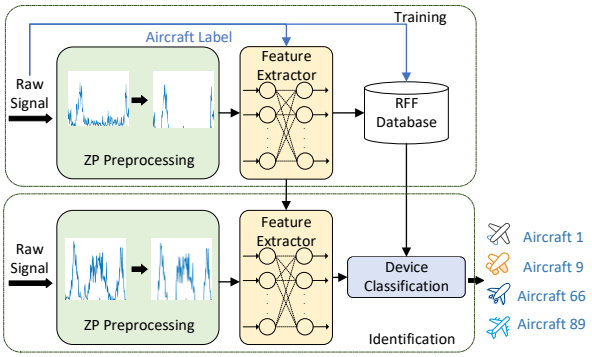


Figure 1. Process workflow of the E-Fin approach

In both stages, raw signals are first pre-processed to enhance the data quality. After that, in the training stage, a feature extractor is trained to select the most representative hardware features from the pre-processed I/Q signals, with the help of some labeled ADS-B signals. These features should be stable for the same aircraft and be distinguishable between different aircraft. At the end of the training stage, an RF fingerprint database will be established. Next, in the identification stage, the RF fingerprint of the unknown aircraft will be extracted from the preprocessed signals through previously trained extractor. Finally, aircraft will be identified through a device classification algorithm, which matches the extracted RF fingerprint with those in the database. The pre-processing algorithm will be represented in Sec. 3, and the feature extraction and device classification algorithm will be elaborated in Sec. 4, respectively.

3. The Pre-processing Algorithm Based on Zero-Padding

Real-world ADS-B signals suffer from environmental noise and interference, making it difficult to extract effective RF fingerprint features from raw signals. Since ADS-B signals use pulse modulation, the transmitting voltage has two levels. When the transmitting voltage is zero, the received signal is entirely made up of additive noise and interference, which has harmful effects on feature extraction. Inspired by this idea, we propose a novel pre-processing algorithm, which improves the data quality by zero-padding these useless signals. To improve the effectiveness of this pre-processing algorithm, we use a coarse synchronization as well as a fine synchronization to detect the accurate region of interest before zero padding. Fig. 2 illustrates the block diagram and waveforms observed at each block of this pre-processing algorithm.

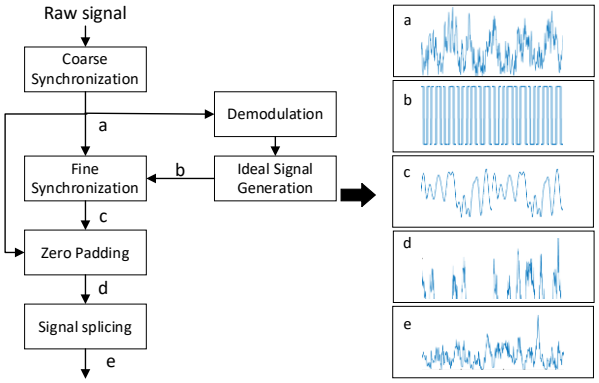


Figure 2. An illustration of the pre-processing algorithm

a. Coarse Synchronization

First, the raw signal s(i) is synchronized coarsely by detecting the fixed preamble. Each ADS-B signal frame consists of two parts: the preamble of 8us and the data block of 112us. According to the modulation format of ADS-B signal based on the 1090ES data link, the 8us preamble contains four pulses, each with a width of 0.5us. The four pulses are positioned at fixed intervals of 1.0us, 3.5us and 4.5us respectively. To align the preamble in the raw signal, we generate a local signal

$$p(i)=\begin{cases}1, & nf_S-\sigma \le i \le \left(n+\dfrac{L}{2}\right)f_S-\sigma \\ 0, & \text{otherwise}\end{cases}, \qquad (1)$$

where $n=0,1,3.5,4.5$ represents the arrival time of pulses, f_S is the sampling rate, L is the width of a pulse and σ is the position bias which indicates the pulse arrives early or late. The position of the preamble is found through a sliding correlation algorithm, whose objective is to find a bias σ that maximize the sum product of the raw signal and the local signal.

b. Fine Synchronization

The actual arrival time of each pulse varies slightly due to many factors during signal transmission such as the channel state and the propagation distance. Therefore, we further use the data part to realize a fine synchronization. Pulse Position Modulation (PPM) coding is utilized in the data block. Specifically, data '1' is transmitted when the pulse arrives in the first half bit, and '0' on the contrary. In actual communication scenarios, the arrival time of each pulse does not exceed 0.05us before and after. Through comparing the average value in the first and second half of each symbol, the symbols in data block will be

demodulated. Next, we generate an ideal pulse signal with the demodulation information. Likewise, we find the exact position of each pulse through a sliding correlation between the raw signal and the ideal pulse signal.

c. Zero-Padding and Signal splicing

After the fine synchronization, we compare the average values of the first and second half pulse and define the half with lower value as the useless part. Finally, the value of the sample point in the useless part is set as zero. Then, we reconstruct the pre-processed signal $s_p(i)$ by splicing the non-zero samples of the preamble and data parts together.

4. Feature Extraction and Device Classification

In this section, we extract representative RF fingerprint features from $s_p(i)$ through various trained CNNs. To address the problem of insufficient training data, we expand the dataset using overlapped sliding windows and obtain a robust identification result through a voting taken by all overlapped samples. The feature extraction and device classification process can be divided into three parts: slicing, feature extraction and voting.

a. Slicing

First, a slicing algorithm is exploited to realize data augmentation. Figure 3 illustrates the slicing operation, which generates k slices from one frame of pre-processed samples. Denote M as the number of samples in one frame and L as the length of a slicing window, respectively. Each adjacent windows have $L-\sigma$ overlapped samples. Then, the number of slices satisfies that $k=\left\lfloor \frac{M-L+1}{\sigma} \right\rfloor$, where $\lfloor \cdot \rfloor$ denotes the floor operation.

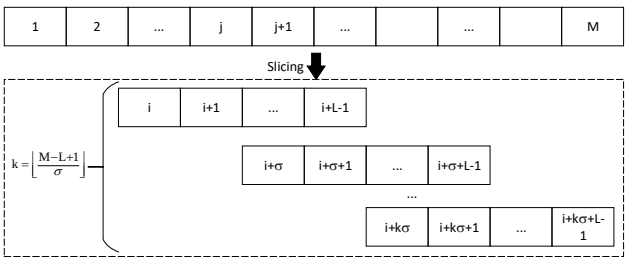


Figure 3. An illustration of the slicing operation

Through the sliding window, each frame of pre-processed signal is transformed into k overlapped slices, which largely expands the dataset.

b. CNN

Due to the excellent classification performance, CNNs are widely utilized for feature extraction and classification. In this paper, we use CNN to extract the RF fingerprint of each slice automatically. Specifically, we consider the classical CNN network structure of VGG16 and ResNet. However, they can not be applied into RF signal feature extraction directly due to the 2D structure of input. Hence, we transform the input structure to 1D in these networks for processing time series signals.

c. Classification and Voting

After feature extraction of each slice in CNN, all the features are sent to a set of fully-connected layers for slice classification. Then we employ voting to integrate the output $\hat{y}$ of the CNN into the final prediction of the frame. The final predicted label of one frame can be obtained by:

$$Y = mode(\hat{y}) \quad (2)$$

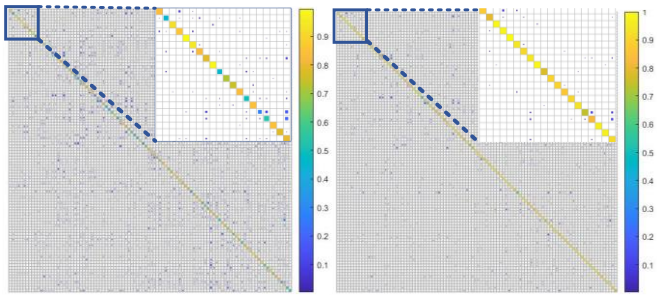
where *mode* is the operation of taking the highest number of labels in the output.

5. Experimental Evaluation

5.1 Experimental Settings

In the experiment, we used the ADS-B signal dataset from real-world aircraft, which was created in [7]. The dataset was collected in a real-world scenario from June 3, 2020 to June 23, 2020 in China Civil Aviation Science and Technology Industrialization Base. After a series of capture processes (which is elaborated in detail in [7]), we selected ADS-B signals from 100 aircraft as our dataset. For each aircraft, we randomly selected about 40 frames of the original baseband I/Q signals. These ADS-B signals are labeled by the International Civil Aviation Organization (ICAO) code decoded from them. Then, the dataset is divided into a training set (80%) and a test set (20%). Since each aircraft only has a few labeled training data, less than 40, it is challenging to identify these aircraft accurately through existing RF fingerprinting approaches.

5.2 Experimental Results



(a) Without (b) With

Figure 4. Confusion Matrix for test data without and with pre-processing

Figure 4 illustrates the confusion matrix on the test dataset without and with pre-processing by the same classification method of VGG16. The image in the upper right corner of each figure magnifies the confusion matrix for the No. 1 - No. 10 aircraft. The color blocks with pre-processing are more concentrated in the diagonal, which means that the possibility of classification error is reduced. This result verifies that the proposed zero-padding pre-processing algorithm can increase the identification accuracy in few-shot scenarios.

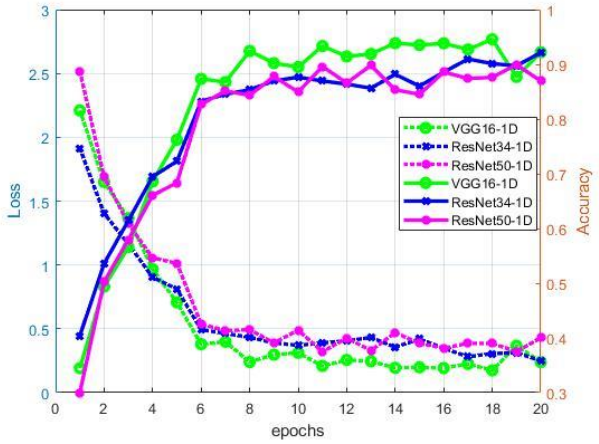


Figure 5. Classification performance of different CNN models

Figure 5 describes the loss and accuracy of different CNN models, including VGG16-1D, ResNet34-1D and ResNet50-1D. The comparison result shows that VGG-1D achieves the highest classification accuracy of 92.21%, while ResNet34-1D and ResNet50-1D have similar performance, fluctuating around 88%.

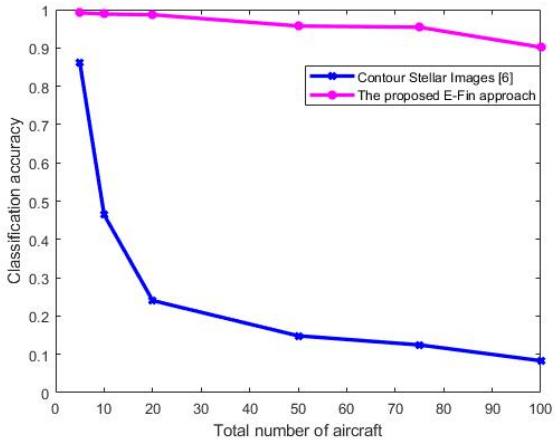


Figure 6. Classification accuracy of different aircraft number

Figure 6 compares the classification accuracy of the proposed E-Fin approach and the Contour Stellar Images-based method proposed in [6], under different number of aircraft. As observed, the Contour Stellar Images-based method achieves a classification accuracy of 90% for 5 aircraft. However, when the number of aircraft increases, the classification accuracy of the Contour Stellar Images-based method has a severe decline, lower than 50% for 10 aircraft. Conversely, the E-Fin approach shows a more robust classification performance for a large number of aircraft. Although the classification accuracy of E-Fin also has slight drop with the increase of aircraft number, it still achieves an accuracy above 92.21% of 100 aircraft. The result in Fig. 6 verifies the effectiveness of E-Fin to identify a large number of aircraft with few labeled training data.

6. Conclusion

This paper studied the aircraft identification problem using RF fingerprint in a practical scenario where the training data is insufficient. Two algorithms were proposed to address this issue. First, a pre-processing algorithm based on zero-padding was applied to raw signals to enhance the data quality for feature extraction. Second, the database was expanded by using overlapped sliding windows, and for these overlapped samples, voting was taken to achieve a robust identification result in the classification phase. Experimental results on over-the-air ADS-B signals from 100 aircraft showed that the proposed E-Fin approach is effective in scenarios with few labeled signals and a large number of aircraft, reaching an identification accuracy above 92.21%.

References

[1] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li and X. Zhang, "A Practical and Compatible Cryptographic Solution to ADS-B Security," *IEEE Internet of Things Journal*, **6**, 2, April 2019, pp. 3322-3334, doi: 10.1109/JIOT.2018.2882633.

[2] S. Khandker, H. Turtiainen, A. Costin and T. Hamalainen, "Cybersecurity attacks on software logic and error handling within ADS-B implementations: Systematic testing of resilience and countermeasures," *IEEE Transactions on Aerospace and Electronic Systems (Early Access)*, doi: 10.1109/TAES.2021.3139559.

[3] Z. Wu, T. Shang and A. Guo, "Security Issues in Automatic Dependent Surveillance - Broadcast (ADS-B): A Survey," *IEEE Access*, **8**, pp. 122147-122167, 2020, doi: 10.1109/ACCESS.2020.3007182.

[4] Q. Xu, R. Zheng, W. Saad and Z. Han, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," *IEEE Communications Surveys & Tutorials*, **18**, 1, First quarter 2016, pp. 94-104, doi: 10.1109/COMST.2015.2476338.

[5] M. Leonardi, L. D. Gregorio, and D. D. Fausto., "Air traffic security: Aircraft classification using ADS-B message's phase-pattern." *Aerospace 4*, **4**, 51, 2017. https://doi.org/10.3390/aerospace4040051.

[6] H. Zha, Q. Tian and Y. Lin, "Real-World ADS-B signal recognition based on Radio Frequency Fingerprinting," *2020 IEEE 28th International Conference on Network Protocols (ICNP)*, 2020, pp. 1-6, doi: 10.1109/ICNP49622.2020.9259404.

[7] Y. Tu, Y. Lin, H. Zha, J. Zhang, Y. Wang, G. Gui, S. Mao, "Large-Scale Real-World Radio Signal Recognition with Deep Learning", *Chinese Journal of Aeronautics*, in press, 2021, doi: 10.1016/j.cja.2021.08.016.