# ADS-B Message Authentication Using Features of Signal in Transition Regions

Nan Jiang[1], Shutong Qi[1], Feixiang Luo[1*], Wang Jun[1], Wenfeng Wang[1],
[1]School of Electronic and Information Engineering of Beihang University, Beijing, China
[*]Email address: (luofeixiang@buaa.edu.cn)

**Automatic Dependent Surveillance - Broadcast (ADS-B) is an essential communication protocol used in modern air traffic control. However, lacking security measures such as authentication and encryption, ADS-B messages can be forged and modified easily by malicious attackers. This paper addresses the problem of authenticating an ADS-B message by means of specific emitter identification (SEI), employing the unintentional modulation on pulse (UMOP). A complete identification system is presented, including data acquisition, feature extraction and classification. In order to create the feature vector for classification, the transition region in a pulse is first delimited and then used for extraction of UMOP features through Hilbert-Huang Transform. The performance of the method is tested by real signal from 30 ADS-B transmitters. Our proposed method is shown to achieve an recognition ratio of over 94%, and performs better under low SNR compared with two previous techniques. It is demonstrated that the SEI technique proposed can be used as an additional tool to enhance the security of ADS-B protocol.**

***Index Terms*—ADS-B, security, specific emitter identification, transition region, classification**

## I. Introduction

The automatic dependent surveillance broadcast (ADS-B), as an Air Traffic Management and Control (ATM/ATC) Surveillance system, is intended to replace traditional secondary surveillance radar (SSR) and become a key component of next-generation air transportation system, holding the promise of reducing infrastructure costs and increasing localization accuracy. However, since ADS-B messages are all broadcast without encryption and authentication, illegal but correctly modulated ADS-B massages can be injected into the ATC system through simple and cheap technological means [1]. As a result, creating ghost aircrafts, formed by the forged signals from malicious attackers, will become a means of destruction by interfering normal operation of both air traffic controller and aircrafts [2]. Nonetheless, ADS-B support will be mandatory in a growing number of airspaces in the world, which leads to a widespread concern about the security of the system.

Specific emitter identification (SEI) is an approach of identifying individual emitter based on unintentional modulation on pulse (UMOP) generated by hardware or software imperfections in the emitter. SEI-based ADS-B authentication system works without large-scale modification or infrastructure construction, as ADS-B signal sources can be classified simply by collecting the UMOP features of specific ADS-B transponders and implementing machine learning techniques. A great many methods of UMOP feature extraction have been proven to be feasible in the identification of radar emitters. Features from intra-pulse data are proposed and studied in [3]. A feature vector extracted from instantaneous amplitude, phase and frequency was utilized for classification in [4].The second order Power Spectral Density function is used in [5] for feature extraction. [6] provided an overview of identifying emitters based on The empirical mode decomposition (EMD) method. Fractal features were used in [7] to recognize different copies of radar.

The classification methods proposed in previous works have achieved satisfactory results. However, considering the reality when SEI is applied to authenticate ADS-B messages, there is still room for improvement. Firstly, although previous work regarding the Mods S reply signal has confirmed that UMOP mainly appears at the leading and trailing edges (transition regions) [8], specific methods for extracting optimum regions of signal have not yet been proposed. Secondly, prior studies lack the evaluation of the method under variant signal quality. Although acceptable results have been derived, the approaches may fail to distinguish emitters under low SNR.

In this paper, a SEI-based method using transition signal for ADS-B message verification is proposed. The first difference of pulse is applied for transition detection, while Hilbert-Huang transform (HHT), having displayed its advantage as a means of SEI [9], is utilized to extract exhaustive UMOP features. The performance of the method is tested by real signals broadcast by the ADS-B transponders equipped on planes. Experimental results demonstrate that transition detection using the method proposed is effective, and that the method is insensitive to the decrease of signal quality.

The rest of this paper is organized as follows. Section II illustrates the way ADS-B signals are collected. In section III, the method of feature extraction based on the transition region of signal is proposed. Experimental results and conclusion are respectively discussed in Sections IV and V.

## II. Data Acquisition

Fig. 1 shows the equipment used for signal acquisition, classification and processing as well as specific experimental process. The signal to be collected is Mode S reply signal operating in the Aeronautical Radio Navigation Services (ANRS) band from 960 to 1215 MHz [11]. The Mode S reply signal is sampled directly at Radio Frequencies (RF), using a technique known as Direct RF Sampling (DRFS) [10]. DRFS can be

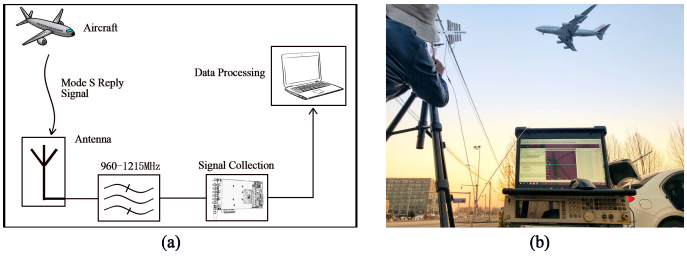



Fig. 1. (a) The block diagram of the system for data acquisition. (b) The field and deployment of the data acquisition experiment.

implemented either through Nyquist sampling, by sampling at least at twice the highest frequency (at least 2430 MHz), or through bandpass sampling. Here bandpass sampling is applied, in which case the sample rate $f_s$ for the ARNS band should be no less than 607.5 MHz [11].

Signal acquisition is carried out near an airport. Our system comprises a Yagi-Uda antenna with a center frequency of 1090MHz and a gain of 11.5 dB for receiving Mode S reply signals, a Spectrum data acquisition card operating with a $f_s$ of 1.25GHz for sampling and a personal computer for follow-up data processing. The acquisition card is set to trigger mode. Once the signal amplitude is greater than the threshold set beforehand, the acquisition card automatically records 125$\mu$s of data. The whole record starts at 2$\mu$s before the trigger point and ends at 123$\mu$s after the trigger point. Thus, messages with both two possible lengths specified in Mode S can be completely recorded.

The signals collected need to be categorized according to the transmitter to which they belong. From the information acquired after decoding a signal, the 24-bit International Civil Aviation Organization (ICAO) aircraft address could be picked out for source identification. Signals with the same ICAO aircraft address are emitted by the same transmitter. They are associated together and labeled with the corresponding address.

Mode S reply signals from 30 airplanes are received and sampled with more than 100 messages. Each message (56-/112-bit) contains 30 to 80 pulses (0.5/1.0 $\mu$s) . Signal in one Mode S packet is denoted as $s(t)$.

## III. Methodology

Fig. 2 is the block diagram of the method proposed in this paper targeting the Mode S reply signal. The method consists of three parts: pulse segmentation, transition detection and feature extraction. Firstly, given the structure characteristics of Mode S reply signal and the 56 or 112-bit message it carries, a series of pulses in a data block can be separated into individual ones. Next, first-order difference of the signal is used to determine the exact start and end points of two transition regions (positive-going and negative going) to be characterized in a pulse. The frame of signal between two transition regions is used for normalization that lowers the impact of variant signal quality. Finally, features based on the transition regions are extracted using HHT.

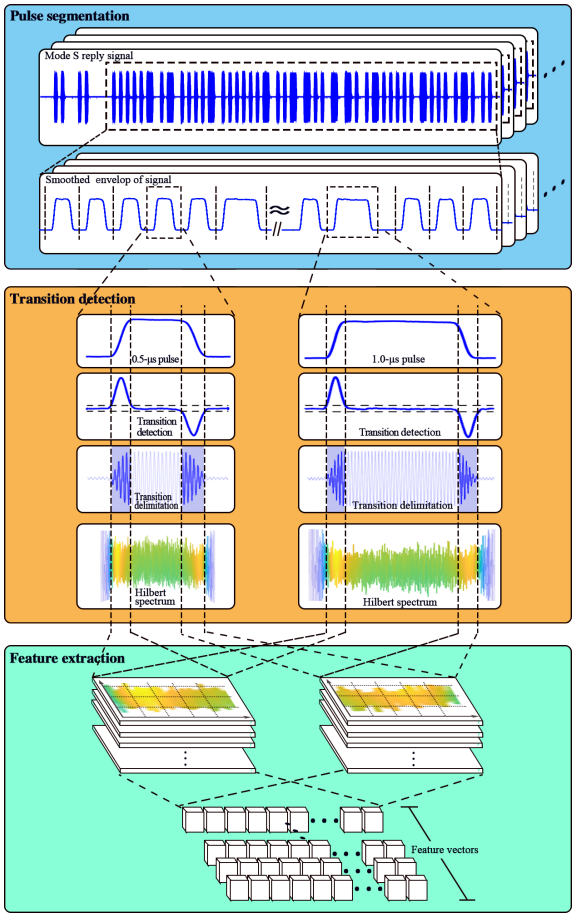



Fig. 2. Data processing for feature extraction

### A. Data Block Segmentation

Fig. 3 provides a graphical view of the Mode S reply signal. The way a packet is segmented depends on the time of arrival (TOA) of each pulse. TOA can be easily estimated according to the 56-or 112-bit massage contained in the data block. Firstly, the message is acquired by detecting the preamble and then decoding the signal received. The related methods have been widely applied in ADS-B receivers [12].Then, given the length of a pulse and its position relative to the starting point of the preamble, the exact positions of leading and trailing edges can be obtained. In order to extract features from the transition signal, the leading and trailing edges should remain intact after segmentation. Therefore, the cut points (start and end points) of each section should be as far from the edges as possible. Considering the fact that equal section length

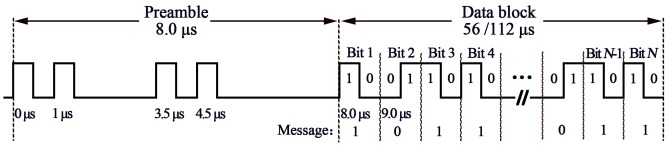



Fig. 3. ADS-B Mode S Packet

facilitates subsequent data processing, the start point of $i^{th}$ section, denoted as $l_i$, is located on 0.25$\mu$s before the leading edge and the end point $t_i$ is located on 0.25$\mu$s after the trailing edge. Raw signal in $i^{th}$ section is represented as $p_i(t)$. Subscript $i$ is omitted in subsequent chapters for simplicity.

### B. Transition Detection

This section illustrates the method of detecting the start and the end point of transition regions. Since UMOP features will be extracted from transition signal in pulses, imprecise detection could affect the performance of features extracted afterwards, which is evaluated in section IV.

Fig. 4 shows how the transition region is detected. As can be seen, each pulse contains a positive-going transition region (PTR) and a negative-going transition region (NTR). Here the range of transition region is determined by the first difference of pulse. Firstly, we need to get the envelope of $p(t)$, denoted as $a(t)$, using techniques such as Hilbert transform and a median filter to get the envelope smoothed. Then the first difference of $a(t)$, represented as $d(t)$, is obtained. As fig.4 shows, at PTR, the amplitude of the signal does not rise with a fixed slope. Instead, the slope increases at first and decreases after the peak. The slope changes in the opposite direction at NTR. Therefore, PTR(NTR) can be considered as a region where $d(t)$ is greater(lower) than a threshold set beforehand. Exceptional cases in which $d(t)$ fluctuates greatly and accidently exceeds the threshold should be eliminated. Thus, only the longest continuum that satisfies the definition is considered. For PTR, the start point $t_{rb}$ and the end point $t_{re}$ are defined as

$$\arg\max_{t_{rb},t_{re}} |t_{rb} - t_{re}|, s.t. \forall t_{rb} \le t \le t_{re}, d(t) > d_{th} \times \max d(t) \tag{1}$$

$\max d(t)$ corresponds to the upper boundary in fig.4, while $d_{th} \times \max d(t)$ corresponds to the upper reference. Here the threshold $d_{th}$ is set to 0.2. For NTR, the starting point $t_{fb}$ and the ending point $t_{fe}$ are defined in a similar way:

$$\arg\max_{t_{fb},t_{fe}} |t_{fb} - t_{fe}|, s.t. \forall t_{fb} \le t \le t_{fe}, d(t) < d_{th} \times \min d(t) \tag{2}$$

Since the quality of signals varies with the distance from aircrafts and channel condition, signals of different pulses should be standardized using the constant frame between PTR and NTR.

$$\hat{p}(t) = p(t) \Big/ \frac{1}{t_{fb} - t_{re} + 1} \sum_{n=t_{re}}^{t_{fb}} p(n) \tag{3}$$

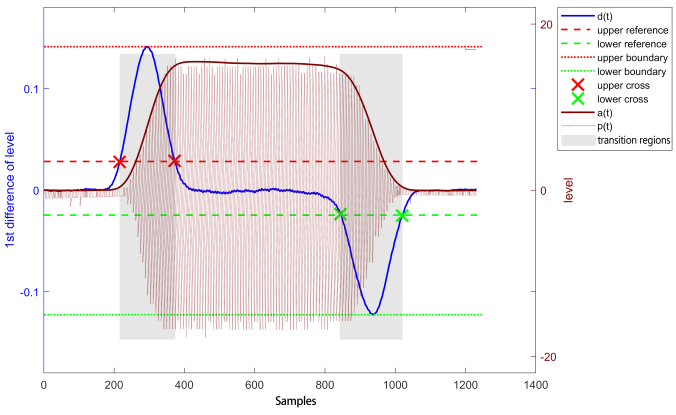



Fig. 4. Transition detection based on the $1^{st}$ difference of pulse envelope

### C. Feature extraction

In this section, UMOP features are generated based on the Hilbert Spectrum of transition regions of $\hat{p}(t)$. All other features in [9]except *Sum of energy* and *Duration of the maximum energy point* are applied to rising and falling edge of the signal respectively, generating a vector with $2 \times 11 = 22$ features. The purpose of feature extraction is to generate unique fingerprint to distinctly differentiate an emitter from the rest. Principal component analysis (PCA) is used for reducing the dimensionality of the UMOP feature space [13]. In the classification test, the number of principal components left was set to 10.

### D. Classification

Classification is performed by machine learning techniques to recognize an ADS-B signal as an original one based on their UMOP features. A deep neural network is trained as classifier, which consists of six layers in total, with 3 trainable neural layers and 3 dropout layers. Each trainable neural layer has a Rectified Linear Unit to accelerate the convergence speed and help to increase the nonlinearity of the model. The input of the model is the feature vector of each emitter, and after 5 hidden layers comes the output, which is the predicted category among all the emitters learned before.

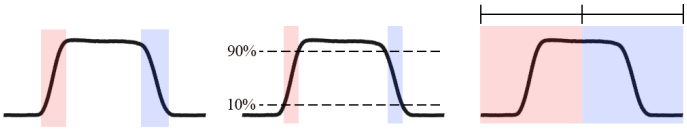
## IV. Performance Evaluation

In this section, the performance of the method proposed in this paper is evaluated using real Mode S reply signal. The process of data acquisition has been illustrated in section II.

Two tests, named transition feature test and robustness test respectively, are performed to evaluate the method proposed in this article. The first test aims to prove the reasonability of the transition detection in the method, while the second measures the recognition ability of the method under different signal qualities(SNR).

### A. Feature Uniqueness Test

Feature uniqueness test compares the performance of features extracted from transition regions with different lengths. Fig. 5 shows the three ways the transition signal, marked with colored background, is delimitated in this test. Here the method proposed in this paper based on transition signal delimitated by the first difference is denoted as TS-D. Two other




(a) TS-D (b) TS-C (c) ED

Fig. 5. Delimitation of transition signal in (a)TS-D, (b)TS-C and (c)ED

comparative experiments, using the same HHT-based feature extraction method as TS-D but based on different regions of signal, are performed to study the effect of target regions on the uniqueness of features. The first comparative experiment separates the target regions in accordance to the conventional definition of transition duration [14], which are the intervals between the 10%- and 90%- amplitude points on the leading and trailing edge, while the second experiment simply divides $\hat{p}(t)$ into two equal parts. The two comparative experiments are called transition signal delimitated by conventional definition (TS-C) and equal division(ED) respectively.

1,200 pulses from Emitter 22 and 26 (E22, E26) respectively, with particularly similar waveforms, are picked out for performance evaluation of ED, TS-C and TS-D. The 22 features derived from three different regions of signal are calculated, normalized and shown in box-plots in figs. 6-8. On each box, the horizontal line inside the box marks the median; the upper and lower borders of the box are the 25th and 75th percentiles; the two vertical dotted lines represent the parts near the extreme values; outliers are plotted individually.

As can be seen from fig. 6, all pairs of feature box are partially overlapped, indicating a poor performance of ED in distinguish E22 from E26. As can be seen from fig. 7, for TS-T, the feature F17 can partly distinguish E22 from E26 but not completely, since the feature boxes of F17 are completely separable but an overlapping area exists in the outliers. Similarly, features F3 and F5 can partly distinguish E22 from E26, even though the feature boxes of both F3 and F5 overlap a little. Accordingly, although features of TS-T perform better than ED, high recognition ration could not be achieved by TS-T. As can be seen from fig. 8, the features

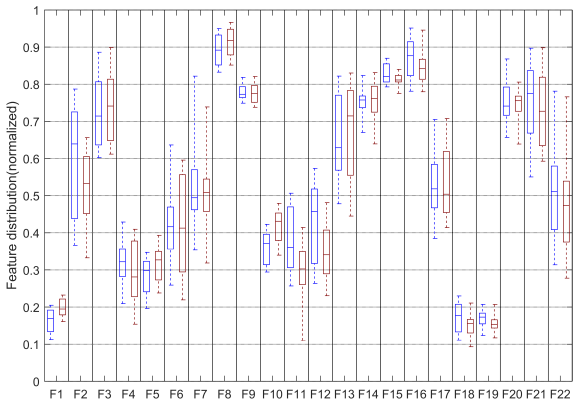



Fig. 6. Features acquired by ED

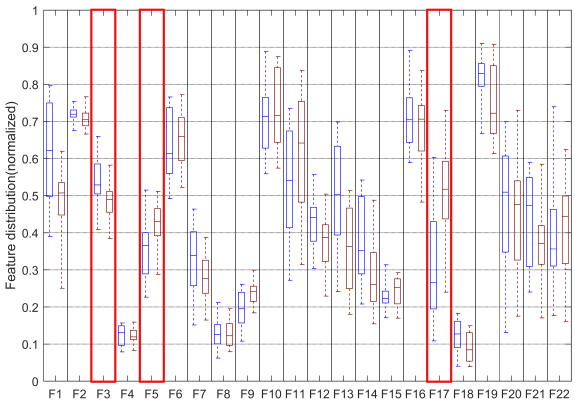



Fig. 7. Features acquired by TS-C

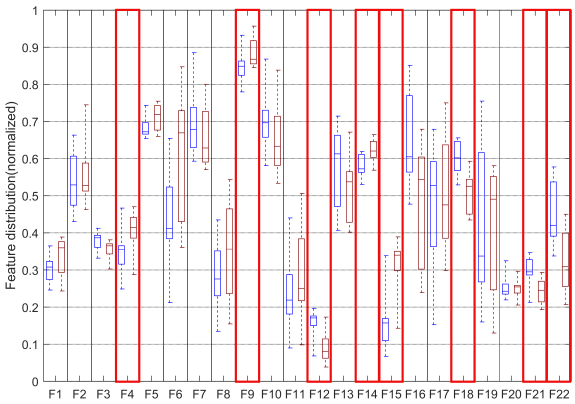



Fig. 8. Features acquired by TS-D

F4,F12,F15,F18 and F21 can partly distinguish E22 from E26 with totally separate boxes. Features F9, F14 and F22 also contribute to the recognition. Through comparison, it can be found that more effective features are derived from TS-D, which proves that the approach of transition detection in this paper generates appropriate sections for feature extraction and identification.

### *B. Noise sensitivity test*

This test judges the performance of a method under various signal qualities. For each transponder, 1200 pulses are chosen randomly to create a training set and another 300 pulses are used as a test set. The method proposed in this paper (TS-D) is compared with two other techniques proposed in [3] and in [4]. The former is based on features in the time and the frequency domain of intra-pulse data (IPD) while the latter is based on transient instantaneous amplitude, phase and frequency (APF). Besides, the classification results of TS-C and ED are also included.

Results of noise sensitivity test are shown in fig. 9 and table 1. In fig. 9, the whole range of SNR is divided into six parts For each method the identification accuracy in a single part is represented by a point in the line chart. In table 1, the overall recognition ratio takes into account classification

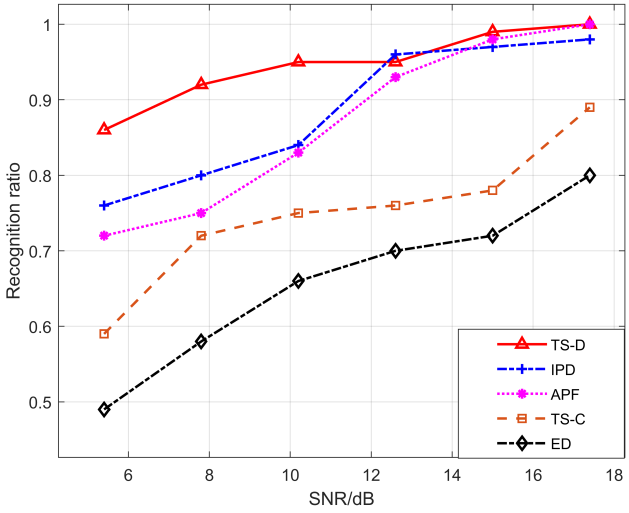



Fig. 9. The identification performance under various SNR

TABLE I
RECOGNITION CAPABILITIES AND NOISE SENSITIVITIES OF THE FIVE METHODS.

| **Measurements** | **Methods** | | | | |
|---|---|---|---|---|---|
| | ***TS-D*** | ***IPD*** | ***APF*** | ***TS-C*** | ***ED*** |
| Overall recognition ratio | **94.9%** | 89.1% | 87.2% | 72.7% | 65.5% |
| Noise sensitivity | **10.8** | 20.6 | 26.1 | 18.0 | 21.8 |

results within the whole SNR range, and the noise sensitivity refers to the slope of the regression line through the points of the corresponding method in fig. 9. Generally, the method proposed in this paper stands out with a recognition ratio of 94.9%. TS-D and two techniques from previous works all achieve high identification accuracies (>95%) when SNR is higher than 14dB, while the performance of TS-C and ED are relatively worse even under high signal quality, which results from the ineffectiveness of features studied in the feature uniqueness test. Identification accuracies of all methods decline with the reducing of SNR. However, as can be seen from table 1, the decline rate of TS-D is apparently lower than that of other tests. For TS-D, the accuracy keeps above 85% even when SNR drops to 4dB, while the accuracies of IPD and APF fall below 70% at low SNR. The test results demonstrate that the proposed method is effective and relatively insensitive to the noise.

## V. CONCLUSION

In this paper, a SEI-based system for ADS-B message verification is proposed. We designed an ADS-B signal acquisition system and proposed a method for feature extraction. A novel approach to extract the transition as the target region of signal by using the first difference of envelope is developed. The approach is proved to be effective under experiments using real data. Firstly, pulses from two transponders with particularly similar waveforms are used to evaluate the features extracted from different parts of the signal. Results demonstrate that the method of transition limitation proposed in this paper enhances the uniqueness of features. Then, classification experiments are performed using signals with various SNR from 30 ADS-B transponders. The classification result shows that the method is effective with an recognition ratio of 94.9% and that the effect of noise on the proposed method is relatively small compared with two previous techniques, which could be of advantage to the practical application in ADS-B message verification.

## REFERENCES

[1] A. Costin and A. Francillon, “Ghost in the Air (Traffic):On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices,”Black Hat, July 2012.
[2] M. Strohmeier, M. Schafer, V. Lenders and I. Martinovic, “Realities and challenges of nextgen air traffic management: the case of ADS-B,” in IEEE Communications Magazine, vol. 52, no. 5, pp. 111-118, May 2014.
[3] A. Kawalec and R. Owczarek, “Radar emitter recognition using intra-pulse data,” 15th International Conference on Microwaves, Radar and Wireless Communications (IEEE Cat. No.04EX824), Warsaw, Poland, 2004, pp. 435-438 Vol.2.
[4] M. Conning and F. Potgieter, “Analysis of measured radar data for specific emitter identification,” in Proc. IEEE Radar Conference, Washington, D.C., USA, Mar 2010, pp. 35-38.
[5] T.W. Chen, W.D. Jin, and J. Li, “Feature extraction using surroundingline integral bispectrum for radar emitter signal,” in Proc. IEEE IJCNN, Hong Kong, 2008, pp. 294-298.
[6] Chunyun Song, Jianmin Xu and Yi Zhan, “A method for specific emitter identification based on empirical mode decomposition,” 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, Beijing, 2010, pp. 54-57.
[7] J. Dudczyk and A. Kawalec, “Fractal features of specific emitter identification,” Acta Physica Polonica A, vol. 124, no. 3, pp. 406-409, 2013.
[8] X. Ru, H. Ye, Z. Liu, Z. Huang, F. Wang and W. Jiang, “An experimental study on secondary radar transponder UMOP characteristics,” 2016 European Radar Conference (EuRAD), London, 2016, pp. 314-317.
[9] Y. Yuan, Z. Huang, H. Wu and X. Wang, “Specific emitter identification based on Hilbert-Huang transform-based time-frequency-energy distribution features,” in IET Communications, vol. 8, no. 13, pp. 2404-2412, 5 September 2014.
[10] O. A. Yeste-Ojeda, J. Zambrano and R. Landry, ”Design of integrated Mode S Transponder, ADS-B and Distance Measuring Equipment transceivers,” 2016 Integrated Communications Navigation and Surveillance (ICNS), Herndon, VA, 2016, pp. 4E1-1-4E1-8.
[11] O. A. Yeste-Ojeda and R. Landry, ”Integrated direct RF sampling front-end for VHF avionics systems,” 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), Herdon, VA, 2015, pp. L1-1-L1-11.
[12] RTCA Inc.Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent SurveillancełBroadcast (ADS-B) and Traffic Information ServicesłBroadcast (TIS-B); DO-260B with Corrigendum 1; RTCA Inc.: Washington, DC, USA, 2011.
[13] R. Duda, P. Hart, and D. Stork, Pattern Classification, 2nd ed., New York: John Wiley & Sons, 2001, pp. 115C117.
[14] “IEEE Standard Pulse Terms and Definitions,” in IEEE Std 194-1977, 1977.