ADS-B Signal Signature Extraction for Intrusion Detection in the Air Traffic Surveillance System

1st Mauro Leonardi
Department of Electronic Engineering
University of Rome "Tor Vergata"
Rome, Italy
mauro.leonardi@uniroma2.it

2nd Davide Di Fausto
Department of Electronic Engineering
University of Rome "Tor Vergata"
Rome, Italy
ddifausto@gmail.com

***Abstract*—Automatic Dependent Surveillance-Broadcast (ADS-B) is a surveillance system used in Air Traffic Control. In this system aircraft transmit their own information (identity, position, velocity etc.) to any equipped listener for surveillance scope. ADS-B is based on a very simple protocol and doesn't provide any kind of authentication and encryption, making it vulnerable to many types of cyber-attacks. In the paper, it is proposed the use of airplane/transmitter RF level features to perform a test to distinguish legitimate messages from fake ones. The received signal features extraction process is described and an intrusion detection algorithm is proposed and evaluated by the use of real data. The results show that by a simple signal processing add-on on a classical (and low cost) ADS-B receivers, it is possible to detect if the ADS-B messages are sent using the expected hardware or not in the 85% of the case.**

***Index Terms*—ADS-B; Security; Classification; Air Traffic Control; Fingerprinting**

I. Introduction

The Automatic Dependent Surveillance-Broadcast (ADS-B) system is one of the pillars of the Future Air Traffic Systems [1] [2]; it is a dependent and cooperative surveillance system used in Air Traffic Control (ATC) in which aircraft periodically transmit their own information such as identity, position, velocity etc. to any equipped listener for surveillance scope [3].

Equipped aircraft utilizes on-board navigation system (i.e. the GPS unit) to calculate its position and its velocity and then to broadcast this information on a common RF channel using an on board emitter called $transponder$. Ground-based receivers are used by the ATC centers to produce an image of the traffic on the controller's display.

ADS-B system has various advantages compared to the classical radar surveillance: the biggest ones are the easy implementation, the low cost of the hardware and the very high accuracy of data position. It also has some important disadvantages that are the dependency on the Satellite Navigation System (that could be corrupted, damaged or interfered) and the simple "free to air" protocol.

In commercial applications, the ADS-B system uses a data-link protocol called *"1090 Extended Squitter (1090ES)"* that is an evolution of the old Identification Friend or Foe (IFF) Secondary Surveillance Radar (SSR) signals [4] [3]: each aircraft periodically transmits messages PPM modulated on L-band (1090 MHz) with random access to the channel. Each message is composed of a preamble of four pulses and a data-block of 112 pulses where the information are coded with a 24-bit CRC [3] [5]. Every message also contains a 24-bit unique transponder identifier (i.e. the unique identifier of the aircraft) called *ICAO address* [3]; in Fig. 1 the format of the ADS-B message is reported. Various types of messages, with different data rates, can be coded and sent, such as: Aircraft Identification, Surface Position, Airborne Position, Airborne Velocities etc. and their transmission rate ranges from 2 msg/sec to 0.2 msg/sec depending on the message type.

The ADS-B protocol does not offer any encryption and authentication method and may be subjected to various cyber-attacks [6] [7] [8]. Different techniques to mitigates these risks are proposed in literature such as, encryption, Multilateration or Anti-Jamming [9] [10] [11] [12] [13].

In this work, we will focus on False Aircraft Injection Attack: injecting false messages on the channel, it is possible to emulate the presence of non-existing aircraft. We propose a method to contrast this attack based on the identification/classification of legacy transmitters. We propose to identify the wireless devices by extracting unique features embedded in the electromagnetic waves emitted by the transmitter. These features arise from randomness in the manufacturing process such as, for example the presence of analog components in the transmission chain, different HW and SW implementation, transmitter clock stability etc.

Once particular features of the transmitter are discovered, it is possible to create a Database of trusted aircraft/transponders containing these particular features and then check if the received signal from a particular airplane has the expected features (i.e. it is generated from the same transmitter as the one recorded in the Database) and, if not, raise an alarm.

We propose to use three different features for the ADS-B transmitter: carrier phase along the ADS-B message; carrier frequency of the transmitted message, and time distance between same-aircraft/same-type consecutive messages.

In the next section we will describe the signal processing needed for the extraction of these features; in Section III, the proposed intruder detection algorithm is reported and evaluated with real data.

ISBN 978-90-827970-1-5

II. ADS-B Signal Signature extraction

Consider the *1090ES* data link format reported in Fig. 1: the PPM modulation implies that, neglecting the preamble, the Data-Block is always composed of $m = 112$ pulses with different time positions to encode the information to be transmitted (i.e. Manchester coding) [3] [14].

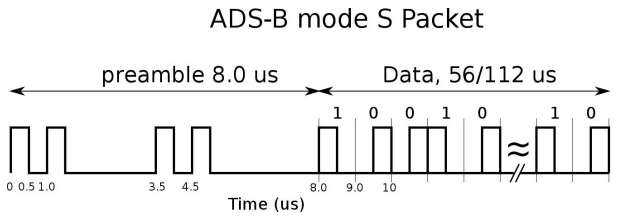

Fig. 1. ADS-B/Mode S reply format.

ICAO standards [3] [14] allow the manufacturers to develop transmitting devices with some tolerances on the various parameters. For the ones of interest in this work we have:

- central frequency f_C should be $1090 \pm 1MHz$;
- no restrictions exist concerning the carrier phase due to the fact that all the information is coded in the amplitude of the signal;
- repetition time for the same type of message is fixed, but has a tolerance; DF17 message with the position information has, for example, a repetition time of 0.5 sec with a tolerance of ± 0.1 sec.

The transmitted signal (considering only the data-block) $s_t(t)$ can be represented as follows:

$$s_t(t) = C(t) \cdot \sin\left[2\pi\left(f_C + \delta f\right)t + \phi(t)\right] \tag{1}$$

where $C(t)$ represents the transmitted 112 pulses sequence, f_C is the carrier frequency equal to 1090 MHz, δf is the allowed jitter of the carrier frequency, and, finally, $\phi(t)$ is the phase of the carrier. Assume to use a 1090 MHz coherent receiver, the presence of Additive White Gaussian Noise (AWGN) and a sampling on the received base band signal, (1) becomes:

$$s_r(k) = s_r(kT_s) = C(kT_s)\sin\left[2\pi\delta f k T_s + \phi(kT_s)\right] + n(kT_s) \tag{2}$$

where $n(kT_s)$ represents the noise and T_s is the sampling time. We have assumed equal to zero the propagation delay from the transmitter to the receiver only to simplify the notation.

Using the samples of the received signal it is possible to:

1) estimate the central frequency of the transmitter;
2) estimate the carrier phase behavior along the message;
3) time-stamping received signals, estimate the Time Difference of Arrival of the signals coming from the same aircraft and then estimate the Time Distance between messages of the same type.

The estimation of the carrier frequency of the message $f_C + \delta f$ can be done using any kind of frequency estimator such as finding the maximum value of the Discrete Fourier Transform of the received signal:

$$\hat{\delta f} = argmax\left\{\left|DFT\left(s_r(k)\right)\right|\right\} \tag{3}$$

The time of arrival of the signal can be estimated using the preamble detection algorithm of the classical ADS-B receiver, and time-tagging the first pulse with a local clock time-stamp.

Finally, concerning the carrier phase behavior, it is possible to estimate 112 different phase values $\hat{\phi}_m$, one for each pulse of the ADS-B message using the following Maximum Likelihood Estimator for the phase [15]:

$$\hat{\phi}_m = \arctan\left[\frac{\sum_K s_r(kT_S)\sin(2\pi\delta f k T_S)}{\sum_K s_r(kT_S)\cos(2\pi\delta f k T_S)}\right] \tag{4}$$

where m identifies the pulse and K the relative pulse's samples; to perform this computation it is mandatory to know the time position of each pulse: it can be easily determined decoding the envelope of the received signal, as done by any ADS-B receiver [3],

Without loss of generality, we can refer all the phases to the first pulse and apply a phase unwrapping procedure to prevent phase ambiguity and to obtain the phase sequence $\left\{\hat{\phi}_m\right\}$.

Considering the Time-Distance between ADS-B message coming from the same receiver, every received message is time-tagged and the distribution of Time Distance can be evaluated using N consecutive messages.

A preliminary measurement campaign to evaluate these features was done in November 2016 using the Transponder Data Recorder. See [16] for details on the campaign and [17] for details on the TDR.

The antenna has been installed on the Engineering Faculty roof receiving 660182 messages sent by 676 different aircraft.

Examples of measured phase patterns, $\left\{\hat{\phi}_m\right\}$, carrier frequency distribution and time distance distribution are reported in Fig. 2, Fig. 3 and Fig. 4.

In Fig. 2, for each graph, the phase patterns obtained from different messages coming from the same aircraft, are plotted. As expected, many airplanes don't have a particular phase pattern and different messages are uncorrelated each other (see Figure 2.(c)), but many others have very particular patterns (see Figure 2.(a-b-d-e)).

Concerning the Central Frequency of the messages, example of distribution over different messages of the same airplane are reported in Fig. 3. It can be noted that, first of all, the transmitted carrier frequency is not always the same but may change inside the available tolerance range, and, secondly, different airplanes may have different carrier frequency distribution.

Finally concerning the Time distance between messages, as expected, it is distributed between 0.4 s and 0.6 s but different aircraft may have different types of distribution, as also shown in [18], see Fig. 4. In particular the distribution between 0.4 and 0.6 s is not uniform but the transmitted frequencies are grouped in bins. We found, at least, four different type of transmitters that differ each other for number and distance of the bins and specific bins presence or absence.

ISBN 978-90-827970-1-5

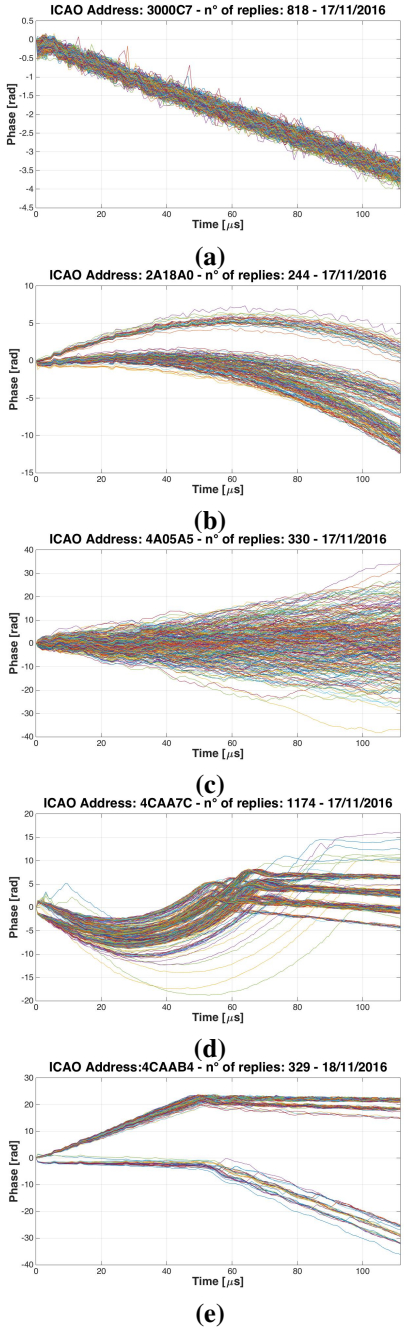

Fig. 2. Phase patterns examples of five different aircraft: (a) Linear, (b) Quadratic, (c) Non-Coherent, (d) Mixed: quadratic+linear, (e) Mixed: linear+linear

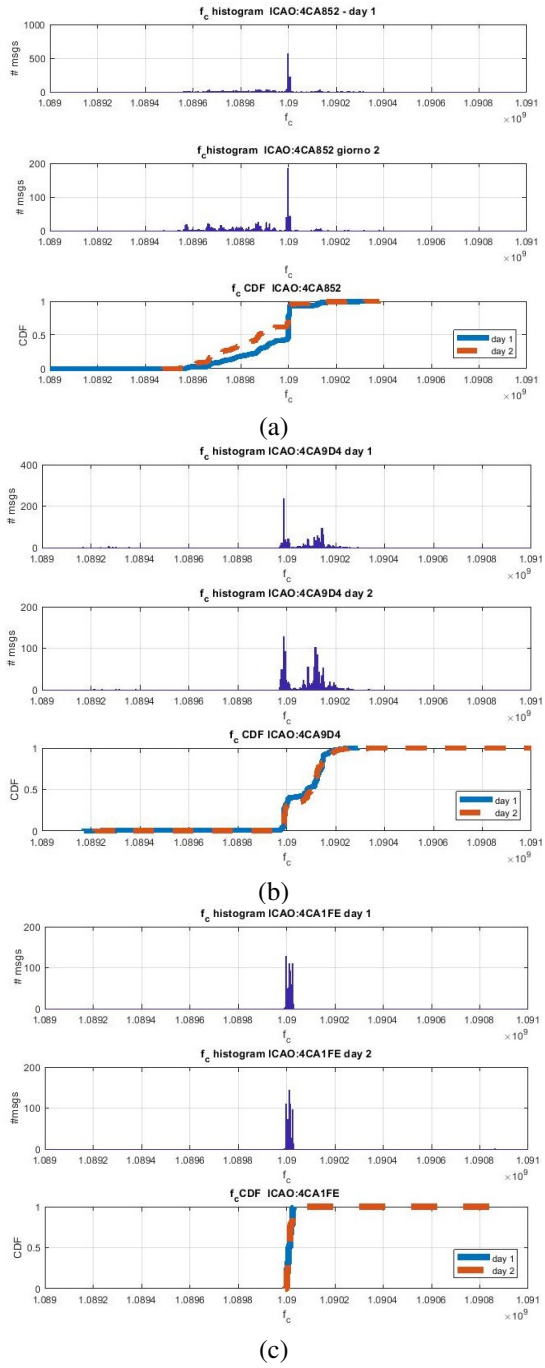

Fig. 3. Example of different Frequency distribution for different Transmitters

Having these measured parameters for each received message, they can be grouped by Aircraft (using the ICAO address contained in the message). On a group of N messages from the same aircraft, signatures related to phase pattern, frequency distribution and Time distance can be extracted. This allows performing the intrusion test every N replies received from the same aircraft. A block diagram of the processing chain in reported in Fig. 5.

Concerning the phase signature a second grade best-fitting polynomial, $y = ax^2 + bx + c$, is used to represent each message phase sequence and, for every group of N consecutive messages, the following six parameters are extracted : $E(a)$, $E(b)$, $E(c)$, $std(a)$, $std(b)$ and $std(c)$.

To describe the carrier frequency distribution, the following features are extracted from the group of N consecutive messages: $E(f)$, $max(f)$, $min(f)$, $std(f)$, $mode(f)$.

Finally, concerning the time distance, the following parameters are extracted from the time distance distribution on N consecutive messages: n_{bins}, number of bins composing the

ISBN 978-90-827970-1-5 © EURASIP 2018

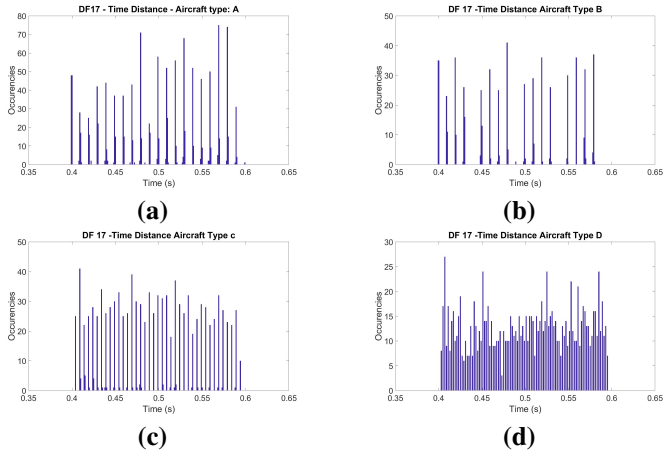

Fig. 4. Example of different distribution of Time Distance between DF-17 Airborn position messages

distribution, d_{bins} mean distance between consecutive bins, n_0, number of selected bins with zero/not zero occurrences.

At the end, it is possible to identify three different vectors usable to classify the group of messages coming from the same aircraft:

$$\begin{aligned}\mathbf{T_1} &= [E(a), E(b), E(c), std(a), std(b), std(c)]' \\ \mathbf{T_2} &= [E(f), min(f), max(f), std(f), mode(f)]' \\ \mathbf{T_3} &= [n_{bin}, d_{bin}, n_0]'\end{aligned} \tag{5}$$

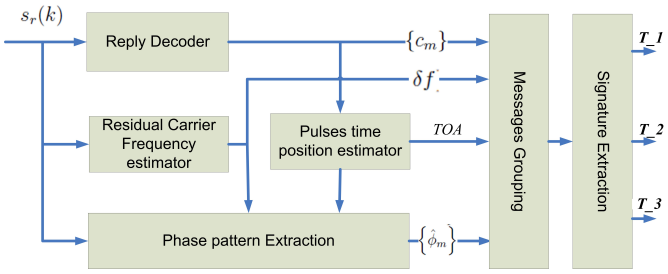

Fig. 5. ADS-B signal features extraction block diagram

III. Intrusion detection test and real data evaluation

The three previously described vectors can be used to perform three different tests and to check the veracity of the transmitter. Here we propose to use the magnitude of these vectors to perform the test.

Making the (strong) hypothesis that the aircraft don't change their signatures in the time, we expect for each entry of $\mathbf{T_i}$ a Gaussian distribution with a given mean value (that is the signature of the transmitters) and with a standard deviation related to entities of the measurement noise.

If a data-base containing (the last) $\mathbf{M}$ signatures of the aircraft is populated for each aircraft, the expected values ($E(\mathbf{T_i})$) and the covariance matrix ($cov(\mathbf{T_i})$) can be estimated using of sample average ($\mathbf{M_i}$) and the sample variance ($\mathbf{C_i}$) and for each incoming signature a new test variable can be defined as:

$$t = (\mathbf{T_i} - \mathbf{M_i})'\mathbf{C^{-1}}(\mathbf{T_i} - \mathbf{M_i}) \tag{6}$$

having the following proprieties:

- it is a non-negative scalar quantity, this allows a simple decision rule: a failure is detected whenever the magnitude of the vector is larger than a defined threshold;
- in the H_0 hypothesis, i.e. the signature is not changed, all the elements of the vector are Independent Identically Zero-Mean Gaussian Distributed, t has a chi-square distribution with given degrees of freedom [19];
- in the H_1 hypothesis, i.e. the signature of the aircraft is changed, all the elements of the vector are independent Non-Zero Mean Gaussian Distributed, t has a Non Central Chi-Square distribution with N-1 degrees of freedom [19].

Finally, a threshold for the test can be fixed using the Neyman Pearson Criterion [19], fixing the Probability of False Alarm (e.g. $P_{FA} = 10^{-6}$).

Summing up, the intrusion detection algorithm extracts the mean values and the covariation matrix for the aircraft signals by the use of the past observations and then use these estimations to calculate the test variable t. If the test variable is larger than the fixed threshold, an alarm is raised.

To evaluate the proposed method, about 22 millions of ADS-B messages from 961 aircraft was received in two days using a very simple and cheap receiver composed by a Software Defined Receiver running over a Raspberry Pi equipped with a DVB-T dongle and an omnidirectional ADS-B antenna (see Fig. 6) [20] [21] [22]. The first days is used only to populate the database and the second one to perform the test. A total number of about 28000 tests was performed. Two kinds of test were performed to compute the Probability of Detection and the Probability of False Alarm. In the first case, the incoming message is arbitrarily manipulated, changing its ICAO Address, in this case the message is declaring to be a different airplane. The algorithm should raise an alarm. Without manipulation, the algorithm should not declare alarm (if an alarm is raised, in this case, it is a False Alarm). Results for computed Probability of Detection and Probability of False Alarm are reported in Table I. The probabilities are computed for each test (phase, frequency and time) and also on the union of the three tests (i.e. at least one alarm on any of the three tests). The α parameter is introduced as a margin on the accuracy of the mean and covariance estimation. In practice, to compute the test variables as defined in (6) the covariance matrix $\mathbf{C}$ is substituted by $\alpha \cdot \mathbf{C}$

As can be seen in the Table, the most performing test is the one on the carrier phase, that can reach a $P_D = 78.66\%$ maintaining the P_{FA} equal to 1.24%. The overall performance can reach a probability of detection of about 84% with a false alarm rate lower than 2% using the one over three logic. These are promising results if compared with previous ADS-B fingerprinting studies: [16] and [18].

ISBN 978-90-827970-1-5 © EURASIP 2018

TABLE I
INTRUSION DETECTION P_D AND P_{FA} FOR DIFFERENT VALUES OF α. THE LAST COLUMN IS FOR THE COMBINATION OF THE THREE TESTS: AT LEAST ONE THEM OVER THE THRESHOLD.

	Phase (T_1)		Freq. (T_2)		Time T_3)		All (1 over 3)	
α	P_D	P_{FA}	P_D	P_{FA}	P_D	P_{FA}	P_D	P_{FA}
1	85.18	2.89	60.56	1.45	30.48	1.09	89.70	3.93
1.5	78.66	1.24	54.87	1.05	26.87	0.51	84.29	1.80
2	72.23	0.77	51.33	0.81	24.21	0.33	78.35	1.19
4	56.17	0.30	43.12	0.47	17.26	0.21	63.72	0.53

Fig. 6. Picures of ADS-B SDR Hardware

Concerning the value of false alarm probability, it cannot be low as expected due to the fact that some aircraft change their signatures in the time (this aspect was confirmed also by visual inspection). In the authors opinion the results can be improved also:

- using a more complex non-linear confirmation logic (e.g. an alarm must be confirmed from another one in the following test);
- by the use of a black-list (list of airplanes for which the test cannot be used) for the airplanes that usually change signatures;
- improving the proposed statistic model, verifying and, if needed, removing the strong hypothesis of Stationary Processes for the airplane features.

IV. CONCLUSION

This work shows that it is possible to identify an intrusion on ADS-B surveillance network by the use of features extracted from the signal transmitted by ADS-B transmitter. Among the three type of proposed features the best one was the carrier phase feature, but, using all the features together a probability of detection of an intruder of about 85% can be reached. This result is important because, by a simple signal processing add-on (extracting the proposed features) on ADS-B receivers, it is possible to detect if ADS-B messages are sent using the expected hardware or not.

REFERENCES

[1] SESAR, "http://www.sesarju.eu/."
[2] NEXTGEN, "https://www.faa.gov/nextgen/."
[3] *Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance Broadcast (ADS-B) and Traffic Information Services Broadcast (TIS-B). DO-260B with Corrigendum 1*, RTCA Inc., Dec. 2011.
[4] M. Strohmeier, "Large-scale analysis of aircraft transponder data," *IEEE Aerospace and Electronic Systems Magazine*, vol. vol. 32, pp. pp. 42–44, 2017.
[5] M. Stevens, *Secondary Surveillance Radar*. Artech House, 1988.
[6] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.
[7] M. Leonardi, E. Piracci, and G. Galati, "Ads-b vulnerability to low cost jammers: Risk assessment and possible solutions," *2014 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)*, pp. pp. 41–46, 2014.
[8] J. Butts, D. McCallie, and R. Mills, "Security analysis of the ads-b implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78–87, 08 2011.
[9] K. Sampigethaya and R. Poovendran, "Visualization & assessment of ads-b security for green atm." in *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, 2010.
[10] M. Strohmeier, "Security in next generation air traffic communication networks," Ph.D. dissertation, University of Oxford, 2016.
[11] I. Mantilla-Gaviria, M. Leonardi, G. Galati, and J. Balbastre-tejodor, "Localization algorithms for multilateration (mlat) systems in airport surface surveillance," *Signal, Image and Video Processing*, vol. 9, no. 7, pp. 1549–1558, 10 2015.
[12] M. Leonardi, G. Galati, and M. Gasbarra, "Multiple faults integrity algorithm for mode s multilateration systems," in *Tyrrhenian International Workshop on Digital Communications - Proceedings of Enhanced Surveillance of Aircraft and Vehicles, TIWDC/ESAV 2008*, Capri, Italy, 09 2008.
[13] G. Galati, M. Leonardi, and V. Paciucci, "Wide area surveillance using ssr mode s multilateration: Advantages and limitations," in *EURAD 2005 Conference Proceedings - 2nd European Radar Conference*, Paris, France, 10 2005, pp. 225–229.
[14] *Annex 10 to the Convention on International Civil Aviation Aeronautical Telecommunication*, ICAO, 1998.
[15] A. Goldsmith, "Wireless communication," *Cambridge University Press*, 2005.
[16] M. Leonardi, L. Di Gregorio, and D. Di Fausto, "Air traffic security: Aircraft classification using ads-b messages phase-pattern," *Aerospace*, 10 2017.
[17] G. Galati, M. Leonardi, E. Piracci, N. Petrochilos, and S. Samanta, "The transponder data recorder: Implementation and first results," *IEEE Aerospace and Electronic Systems Magazine*, vol. 29, no. 2, pp. 6–13, 02 2014.
[18] M. Strohmeier and I. Martinovic, "On passive data link layer fingerprinting of aircraft transponders," in *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, A. N. York, Ed., Denver, Colorado,USA, 10 2015.
[19] A. Papoulis, *Probability and Statistics*, A. Papoulis, Ed. Prentice Hall, 1990.
[20] *www.rtl-sdr.com*.
[21] *https://www.raspberrypi.org/*.
[22] "https://github.com/antirez/dump1090."

ISBN 978-90-827970-1-5