ADS-B vulnerability to low cost jammers: risk assessment and possible solutions

Mauro Leonardi, Emilio Piracci, Gaspare Galati
Tor Vergata University, Department of Electronic Engineering
Via del politecnico 1, 00133 Rome, Italy
mauro.leonardi@uniroma2.it; piracci@ing.uniroma2.it; gaspare.galati@uniroma2.it

***Abstract*— Automatic Dependent Surveillance-Broadcast (ADS-B) systems provide to the air traffic control centers flight and status information of the cooperating targets. Problems due to jamming and/or spoofing of the ADS-B channel are under study, as well as verification and validation techniques. In this paper, we show how a low cost jammer can affect an ADS-B receiver. Three types of threats were evaluated. A multichannel receiver permitted to evaluate the received signal stream with and without jammer. The measurements were carried out coupling the receiver antenna with the in-cable jammer radio frequency (1090 MHz) signal. The results show the detection loss as a function of jammer range and jammer type. Finally, possible solutions are proposed to mitigate the effects. Some trials to evaluate their effectiveness are described.**

Keywords—ADS-B; jammer; spoofer; SSR signals separation; Air Traffic Control.

I. Introduction to ADS-B system and its vulnerability to jamming

Automatic Dependent Surveillance-Broadcast systems are becoming of widespread use in modern Air Traffic Management. These systems use the SSR Mode S channel and the messages from the aircraft to locate and identify the cooperating targets in their coverage area [1]-[2]. In the ADS-B operation the aircraft (targets) positions are derived from the on-board navigation subsystem (usually GPS-based). These kind of systems have various advantages as compared with the classical radar surveillance. The biggest one is the easy implementation and, then, the low cost of the hardware and the a very high accuracy of position data.

The ADS-B disadvantages are related to the dependency on the navigation satellite system (that could be corrupted, or damaged) and also on the very simple protocol "free to air", based upon the Mode S squitter emitted from the aircraft on the 1090 MHz aeronautic band. Every aircraft emits a 56 or 112 bits message made up by a preamble followed by a data block without any cryptography or authentication. An example of a Mode S Reply is shown in Figure 1 evidentiating the simple pulse-position modulation.

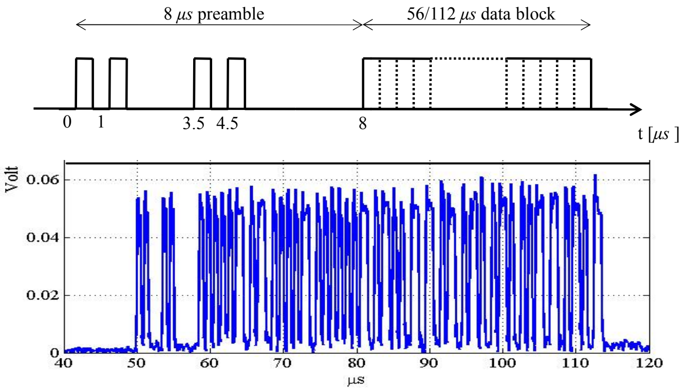

Figure 1 - A Mode S reply signal envelope

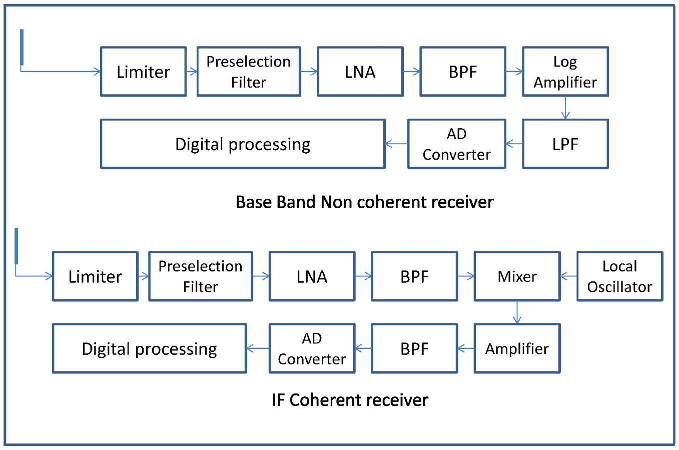

Figure 2 - ADS-B receivers block-diagram (LNA: Low Noise Amplifier, BPF: Band Pass Filter, LPF: Low Pass Filter)

ADS-B receivers follow the standard reported in [1]-[2]. In Figure 2 two possible implementations are shown. The first one is a non-coherent receiver that typically uses a logarithmic receiver that convert directly the RF signal into a voltage level, to be digitized and processed according to the signal specifications and receiver logics as defined in [2]. The second implementation uses an IF coherent receiver with a digitizer at the intermediate frequency. Then the samples of the received

978-1-4799-3094-4/14/$31.00 ©2014 IEEE

signals are processed with Hilbert filtering (or equivalent) to extract the I and Q components to be processed according to the standards, as in the first case.

ADS-B systems can suffer by any corruption of the navigation subsystem that provides the position data. Moreover, a system malfunction can be caused by an in band (1090 MHz) jammer that creates voluntary interferences to the receivers. Note that the ADS-B information can be indirectly corrupted also by a GPS jammer; the related problems and the mitigation are addressed in [3], not in this paper.

All main blocks of an ADS-B receiver (figure 2) can be affected by unwanted interference or jamming and spoofing signals, as follows.

- High power jammers cause saturation of an amplification stage (or of the limiter).
- Unwanted signals in the Mode S band change the SNR/SIR (Signal to Noise Ratio/Signal to Interference Ratio) and produce false alarms (if the threshold is fixed), or missed detections (if the threshold is varying as in the case of Constant False Alarm Rate threshold).
- ADS-B receivers usually implements validation logics to be sure that, for example, a valid message is received (preamble identification) and that the message is not corrupted by other messages. However, validation logics are prone to "smart" jamming signals, mimicking the Mode S/ADS-B ones. In fact, the receiver typically is looking for the preamble. If the jammer send a train of preambles these function of the receiver will be denied. Moreover, jamming signals composed by a train of pulses, formatted as Mode S signals but without any operational meaning, can stress the receiver till the saturation of its computational power.
- Spoofing i.e. intentional harmful signal with the same characteristics of the valid signals, create false targets or saturate the processing.

Considering these scenarios it is important to evaluate how much a standard or an enhanced receiver can be prone to jamming. In fact, it is very easy to develop (or buy) a transmitter on the L band able to produce PPM modulated signal [4], as shown in the following Section.

II. Jammer implementation and Test Bed Description

A jammer device has been implemented in the Tor Vergata "RadarLab" with the NI USRP 2920 a Software Defined Radio (SDR) device with Rx/Tx capabilities in the 50-2200 MHz band [5]-[6]. Three possible jamming-waveforms were analyzed (figure 3):

(a) an ADS-B message with a random data-block, repeated with an inter-message time equal to 10 µs;

(b) a stream of ICAO standard preambles;

(c) a random binary sequence with PPM modulation.

These waveforms were selected in order to stress as much as possible the receiver (in particular pulse validation logics and preamble detection logics).

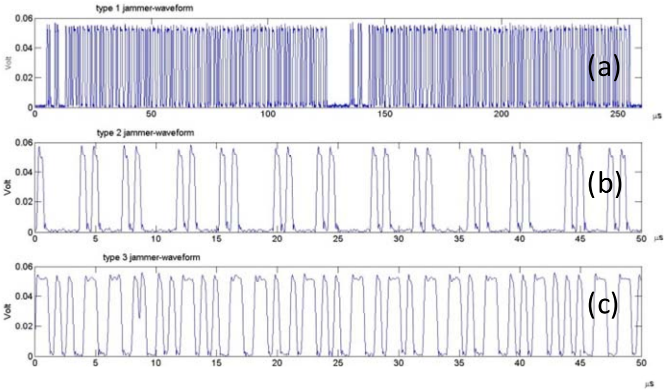

Figure 3 - Jammer-waveforms

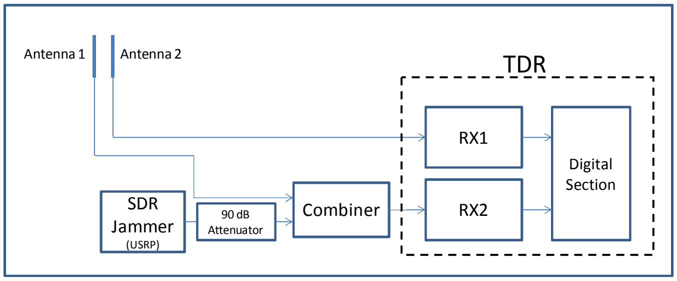

Figure 4 Test-bed block diagram

The RF (1090 MHz) output of the USRP 2920 is coupled to the antenna signal by a combiner. The output of the combiner is fed into a 1090 MHz multichannel receiver. Figure 4 shows the deployment of the test bed. The multichannel receiver, called TDR (Transponder Data Recorder), designed and developed at Tor Vergata University [7], is composed by the antenna, the analog section and the digital section. The antenna (Figure 5) is an array of six patch elements placed on the Engineering Faculty roof; the analog section is a dedicated front-end for RF signal reception and down conversion with five channels: four independent linear channels and one 'logarithmic' channel. The four linear channels, connected to the four central array elements, downconvert the signals to intermediate frequency (IF) at 21.5 MHz. The logarithmic channel, connected to one side array element, is based on the Analog Devices AD8313 [8] log receiver, with a base-band output.

The TDR digital section is based on a NI platform composed by the controller NI PXIe 8135, three acquisition cards NI PXIe 5122 and a FPGA card NI FlexRio PXIe7966. Each acquisition card NI PXIe 5122 has two input channels, and a sample rate up to 100 Msamples/s. These devices (Figure 6) are controlled by software in LabView programming environment.

Varying the USRP output gain/attenuation it is possible to simulate the variation of range between the antenna receiver and the jammer source. Figure 7 shows the same signal as shown in Figure 1, corrupted by a high power type (c) jammer.

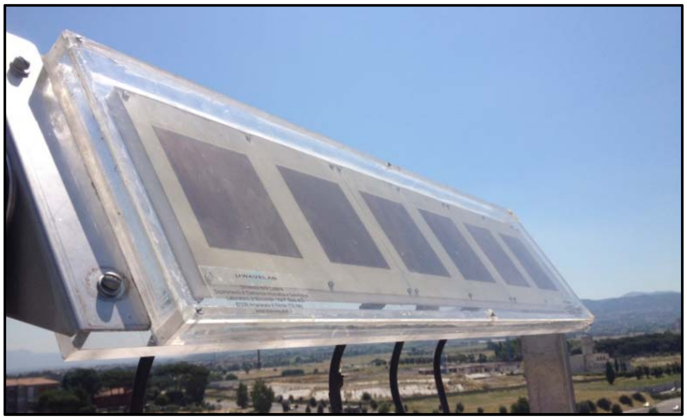

Figure 5 - TDR Antenna

Analyzing the received traffic with two parallel receiving channels it is possible to evaluate the effect of the interferences in terms of missed detection, as a function of the jammer-source range and for a variety of waveform types.

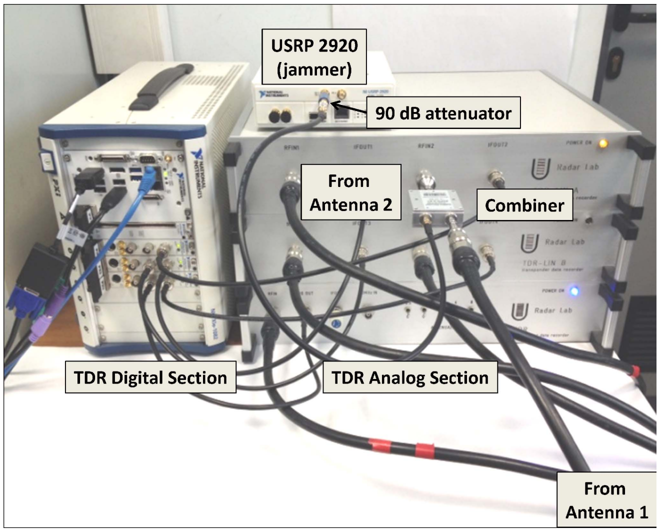

Figure 6 - System setup

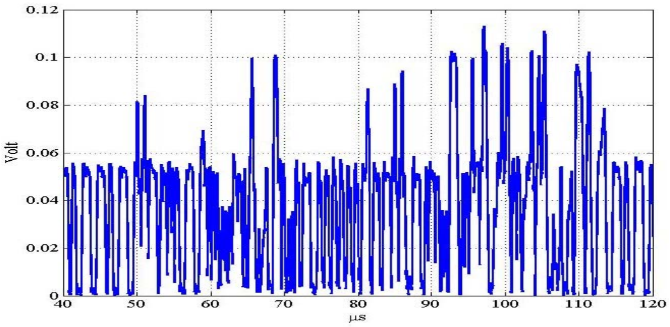

Figure 7 - Mode S signal (figure 1) with jamming interference

III. Jamming trials and Results

The 90 dB attenuator between the USRP and the TDR as shown in figure 4 permits to emulate an attenuation due to ca. 1 Km of distance between the jammer and the ADS-B receiver. In addition, the output power of the USRP can be regulated via software. In this way it is possible to emulate a jammer range between ca. 1 Km and 7 Km (the output power of the USRP can vary between -11 dBm and 20 dBm).
In table I the jammer signal power at the receiver input and the corresponding emulated jammer-receiver range (considering a jammer with a maximum peak power of 20 dBm) are reported. The last column shows the maximum estimated range of an avionic Mode S transponder, in order to have a Signal-to-Interference-Ratio greater than, or equal to 3 dB. These values are obtained considering an EIRP of 53 dBm for the avionic transponder. This particular value of SIR (≥ 3 dB) was chosen since in a standard receiver an occurrence of pulses 3 dB or more stronger than the signal under decoding, causes a re-triggering event (i.e. a decoding procedure stop). Then, the last column of table I can be interpreted as the theoretical coverage of an ADS-B receiver, when a jammer with a 20 dBm EIRP is placed at the distance indicated in the second column.

TABLE I. Received jammer power, Receiver Range and expected coverage of the reeceiver under attack for a +20 dBm jammer

Prx (dBm)	Simulated range of the jammer (Km)	Maximum range with jammer (Km)
-90	6.92	218.78
-87	4.90	154.88
-83	3.09	97.72
-80	2.19	69.18
-77	1.55	48.98
-74	1.10	34.67

Theoretically the NI USRP used as a 1090 MHz, 20 dBm jammer at 1 km can reduce the coverage of the ADS-B receiver to 35 km from the original, > 400 Km, typical coverage of a stand-alone ADS-B station (depending on the receiver sensitivity).

Thinking to a possible real implementation of a 1090 MHz jammer, it should be also possible to use low cost RF power amplifier of 20 dB to achieve better jamming performance i.e. a reduction of the coverage to 3 Km with a very low additional cost.

In these computations multipath, reflection or side lobe receiving of the jammer signal are not considered.

Using the USRP to generate the interfering signal and the TDR receiver with the DO-260A [2] algorithms for ADS-B signal detection and decoding, the different interfering waveform and range combination was analyzed.

To perform the analysis, real signals were recorded for six seconds intervals varying the jammer range. Figure 8 and Figure 9 shows the results obtained decoding only the Airborne Position Messages DF17 (APM-DF17). The APM-DF17's contain the identity (ICAO address) and the 3D position data of the sources. The identity permit to perform a Cyclic Redundancy Check (CRC) to count the number of decoded bit errors. Figure 8 shows the maximum coverage of the station with or without jamming (that is the distance of the farther airplane detected) for different possible jammer-ADS-B station simulated distances. Figure 9 shows the number of DF17 detected and decoded with no error (i.e. with CRC OK) with or without the jammer.

It results that for any type of jammer the capability to produce harmful interference is very high. The three types of jammer produce a reduction of the coverage depending on the relative range. The coverage is limited to 160-200 km by a jammer at 6.92 km, and in the worst case the coverage is reduced at 30-40 km by a jammer at 1.10 km. The results from the measurements are quite similar to the theoretical one.

Figure 10 shows an example of this harmful effect: the upper-side of the figure shows jammer-free extracted plots, the bottom-side of the figure shows the plots extracted by the same signal corrupted by the jammer. Figure 11 is a zoom of figure 10 area close to the coast. It shows that apart from the coverage reduction, the jammer also causes the loss of some plots of a near airborne target. It is also visible the loss of the two messages emitted by the aircraft on the runway.

The coverage and detected signals reduction due to reduced SIR, are the consequence of two main effects in the receiver :

- the probability of detection of a valid pulse is reduced
- the extraction of the information is corrupted and the CRC test is not passed.

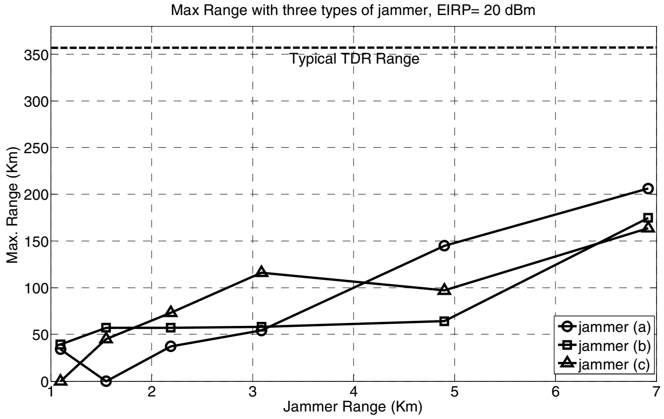

Figure 8 - Max range with three types of jammer, EIRP = 20 dBm

Another important effect is the overhead of the processor that can cause the service interruption or the loss of data (the receiver operates in real-time).

For example it results that the jammer type (a) and jammer type (c) produce in the worst case up to ca. 50000 detection events (using RTCA DO 260A algorithms [2]) in six seconds (the real detection number without jamming is ca. 2000 in six seconds considering all Mode S signals).

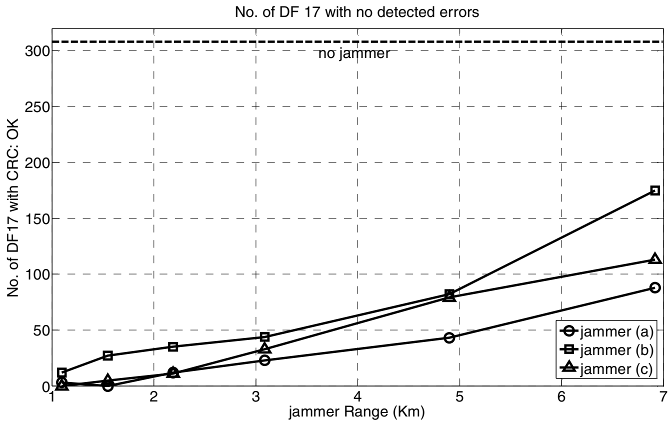

Figure 9 - No. of DF 17 with no detected errors versus the jammer range

The receiving station has to execute (for any detection) all the algorithms to validate the replies and, only after these controls, can declare that they are false alarms.

Therefore jammers and spoofers cannot be mitigated by decoding algorithms or by system level validation (i.e. MLAT check [20]), but must be mitigated at the signal level, i.e. before the detection and decoding procedures.

IV. MITIGATION AND POSSIBLE SOLUTIONS

Different methods for ADS-B protection and security assessment have been proposed [14]-[15]. In [9] a survey of risk mitigation methods is reported. The state of the art is based on the implementation of "high level" solutions. Typically, these solutions need system up-dating or the implementation of new system functionalities. For example: an ADS-B multilateration-based position data check need the up-date of the high-level software to implement the related operations, operator control to enable-disable the function. Here, we propose to add a "low level" solution to be implemented in the receiver, in particular in the "digital processing" block of figure 2. The "digital processing" block, performs the following operations: 1) pulses extraction, 2) preamble detection, 3) bit sequence decoding, 4) message information decoding. The proposed method consists on the use of ad-hoc signal processing algorithms useful for detection and separation of overlapping signals. These methods have been implemented for non-directive antenna equipped receiver (such as the ADS-B ground station), in high traffic density area where the probability to receive overlapping signals from many sources is not negligible. Considering the jammer as source, the mitigation problem can be treated as a signal overlapping problem. The signal separation methods have to be implemented in the "digital processing" block, between the 'pulses extraction' and the 'preamble detection'.

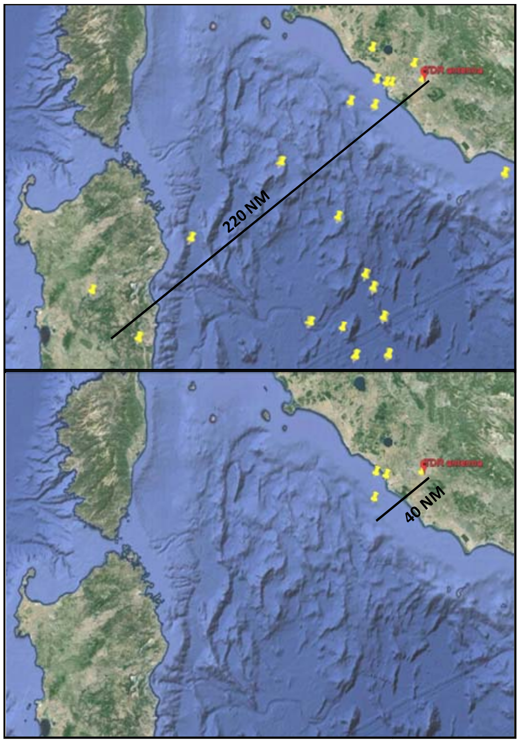

Figure 10 - Comparison of the ADS-B plot, free and jammed channel

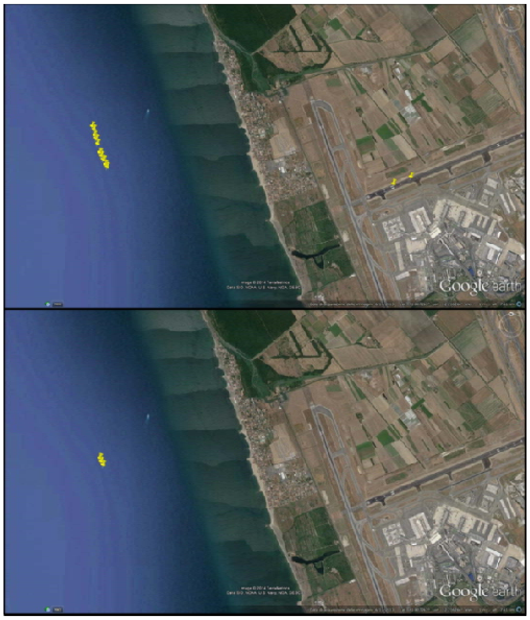

Figure 11- Comparison of a ADS-B track, free and jammed channel

The benefit from the usage of these methods relies on the possibility to 'remove' the jammer signal by the valid one, thus restoring the receiver coverage and reducing the processor computational load. Moreover, also in the case of separation failure, the knowledge about the number of sources is available. The stand-alone receiver has the capability to detect a suspicious signals rate increase, then a warning alert to for high level control should be set up, implementing a self-integrity-monitoring.

We proposed a separation method, the Projection Algorithm for Single Antenna (PASA) [10], a single channel receiver, and array processing based methods [11]-[12], Projection Algorithm (PA) and Extended PA (EPA), for a multi-channel receiver. In [13] a survey of other array processing methods is reported. The PASA can be implemented in the present ADS-B ground stations, as they are normally equipped with a single channel receiver. PA and EPA need an array antenna and a multi-channel receiver to be implemented, a more expensive solution although they don't need a calibrated array. These algorithms derive the sources beamformers by algebraic operations on the received data, arranged in a matrix. The algebraic method perform the sources beamformers estimation exploiting the sources diversity. In PA and EPA the diversity is represented by the different direction of arrival of the impinging signals, while in PASA the signal diversity relies on the signals frequency shift. PA and PASA need a free-interference time support for each source that has to be extracted, meanwhile EPA is a recursive algorithm able to extract also sources completely mixed each other. According to the considered jammer waveforms, the superimposition in time with an airborne signal doesn't provide a consistent signal time support with only one source. Under this condition the best candidate appears to be the EPA. In [11] the EPA performance has been evaluated: with a mixture of 2 signals the algorithm has a success rate of 90%. It is intended that, a case is success if the replies are detected and sent to the decoding block. Other separation methods based on array processing are [16] and [17] only useful for a very high traffic.

Note that the use of signal separation algorithms in conjunction with enhanced decoding techniques [18] add also a benefit in terms of channel capacity improvement [19].

V. CONCLUSION

The effects of a jammer on an ADS-B receiver has been analyzed using a 1090 MHz multichannel receiver and a Software Defined Radio (SDR) source to generate the jammer waveforms. The results obtained by the decoding of the interference-free channel compared to the jammed one show reduced coverage and reduced detection probability. The jammer risk mitigation has been addressed by several papers. The proposed solutions are addressing high level methods, that need the implementation of new system concepts or the up-date of the actual systems functions. We propose a ‘low level’ method based on the implementation of a signal separation method in the ADS-B receiver, to be implemented upstream the detection and decoding procedures. The benefits of this solution relies on: i) the ADS-B station has the capabilities of a self integrity monitoring, ii) the implementation has not legacy problem and doesn’t need the use of new system concepts, but it is easy realized by a detection/decoding receiver software up-date. Ongoing research activities are related to the performance study and analysis of the separation methods for ADS-B ground systems, and on the improvement of signal separation algorithms to better fit the jammer problem.

REFERENCES

[1] ICAO: ‘Annex 10 to the convention on international civil aviation, Aeronautical Telecommunications, Vol. IV Surveillance Radar and Collision Avoidance systems’, 2002.

[2] RTCA DO-260A: ‘MOPS for 1090 MHz ES ADS-B and TIS-B’, 2003

[3] Di Fonzo, A., Leonardi, M., Galati, G. *et al.*: “GNSS software defined anti-jammer equipment receiver for in car navigation”, in Proc. Of IEEE MetroAeroSpace, Benevento, Italy, 29-30 May, ISBN 978-1-4799-2070-9, pp. 320-325.

[4] Costin, A., Francillon, A.: ‘Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices’, Black Hat USA 2012, available on EURECOM web site at https://www.eurecom.fr/fr/publication/3788/download/rs-publi-3788.pdf.

[5] Piracci, E., Galati, G., Pagnini, M.: “ADS-B signals reception: a Software Defined Radio approach”, in Proc. Of IEEE MetroAeroSpace, Benevento, Italy, 29-30 May, ISBN 978-1-4799-2070-9, pp. 543-548.

[6] NI website: USRP datasheet http://sine.ni.com/ds/app/doc/p/id/ds-355/lang/it.

[7] Galati, G., Leonardi, M., Petrochilos, N., Piracci, E.G., Samanta, S.: ‘Trasponder Data Recorder: final implementation and first results’ IEEE Aerospace and Electronic Systems Magazine, Vol. 29, I. 2, pp. 6-13.

[8] Analog Device AD8313 website datasheet: http://www.analog.com/static/imported-files/data_sheets/AD8313.pdf.

[9] Sampigethaya, K., Poovendran, R.: ‘Visualization & assessment of ADS-B security for green ATM’, Proceedings of IEEE DASC, October 2012 , pp. 3.A.3.1-3.A.3.16.

[10] Piracci, E.G., Petrochilos, N., Galati, G.: ‘Single antenna projection algorithm for Mode S based airport traffic surveillance’, Proc. European Microwave Week, 4th Radar Conference EuRad 2007, Munich, Germany, October 2007.

[11] Petrochilos, N., Galati, G., Piracci, E.G.: ‘Separation of SSR signals by array processing in multilateration systems’, IEEE Transactions on Aerospace and Electronic Systems, 2009, Vol. 45, No. 3, pp. 965-982.

[12] Piracci, E.G., Petrochilos, N., Galati, G.: ‘Mixed SSR sources exploiting sparsity: a geometrical approach’, Proc. European Microwave Conference, 6th Radar Conference EuRad, Rome, Italy, September-October 2009, pp. 85-88.

[13] Petrochilos, N., Galati, G., Piracci, E.G.: “Array processing of SSR signals in the multilateration context, a decade survey”, in proc. Of ESAV 2008, Italy, Rome, September 2008, pp. 60-64, ISBN 978-88-903482-0-4

[14] Sampigethaya, K., Poovendran, R., Bushnell, L.: ‘Secure operation, control, and maintenance of future e-Enabled airplanes’, Proceedings of IEEE, Vol. 96 n. 12 2008, pp. 1992-2007.

[15] Krozel, J., Andrisani, I.: “Independent ADS-B verification and validation” in Proc. AIAA 5th Aviation, Technol., Integr., Oper. Conf (ATIO), 2005, pp. 1-11.

[16] N. Petrochilos and A.-J. van der Veen, "Algebraic algorithms to separate overlapping secondary surveillance radar replies," IEEE Trans. Signal Process., vol. 55, no. 7, pp. 3746-3759, Jul. 2007.

[17] M. Zhou and A. van der Veen, "Improved blind separation algorithm for overlapping secondary surveillance radar replies," in Proc. IEEE CAMSAP, San Juan, Puerto Rico, Dec. 2011, pp. 181-184.

[18] Galati, G., Gasbarra, M., Piracci, E.G.: “Decoding techniques for SSR Mode S signals in high traffic environment”, in Proc. of European Microwave Week EuRad 2005, Paris, France, October 2005.

[19] Piracci, E.G, Galati, G., Petrochilos, N., Fiori, F.: ‘1090 MHz channel capacity improvement in the air traffic control context”, International Journal of Microwave and Wireless Technologies, 2009, 1 (3), pp. 193-199.

[20] G. Galati, M. Leonardi, P. Magarò, V. Paciucci “Wide Area surveillance using SSR Mode S multilateration: advantages and limitations”, Proceeding of European Radar Conference, EURAD, 2005, pp 225-229.