International Journal of Mechanical, Industrial and Aerospace Sciences
ISSN: 2517-9950
Vol:12, No:3, 2018

Application of PSK Modulation in ADS-B 1090 Extended Squitter Authentication

A-Q. Nguyen. A. Amrhar, J. Zambrano, G. Brown, O.A. Yeste-Ojeda, R. Jr. Landry

***Abstract*—**Since the presence of Next Generation Air Transportation System (NextGen), Automatic Dependent Surveillance-Broadcast (ADS-B) has raised specific concerns related to the privacy and security, due to its vulnerable, low-level of security and limited payload. In this paper, the authors introduce and analyze the combination of Pulse Amplitude Modulation (PAM) and Phase Shift Keying (PSK) Modulation in conventional ADS-B, forming Secure ADS-B (SADS-B) avionics. In order to demonstrate the potential of this combination, Hardware-in-the-loop (HIL) simulation was used. The tests' results show that, on the one hand, SADS-B can offer five times the payload as its predecessor. This additional payload of SADS-B can be used in various applications, therefore enhancing the ability and efficiency of the current ADS-B. On the other hand, by using the extra phase modulated bits as a digital signature to authenticate ADS-B messages, SADS-B can increase the security of ADS-B, thus ensure a more secure aviation as well. More importantly, SADS-B is compatible with the current ADS-B In and Out. Hence, no significant modifications will be needed to implement this idea. As a result, SADS-B can be considered the most promising approach to enhance the capability and security of ADS-B.

***Keywords*—**ADS-B authentication, ADS-B security, NextGen ADS-B, PSK signature, secure ADS-B.

I. Introduction

IN order to respond to the increasing concerns of security level and airspace capacity, Federal Aviation Administration (FAA), in the 2000s, launched the Next Generation Air Transportation System, NextGen. In this new architecture, Automatic Dependent Surveillance-Broadcast (ADS-B) is defined as one of the backbone systems and will become a mandatory avionics for any class A commercial aircraft since January 2020 [1]. Fig. 1 shows an overview of the use of ADS-B in the NextGen, adapted from FAA.

Right after the announcement by the FAA of the new ADS-B system, experts and researchers have shown their concerns about the vulnerable and insecurity of this avionics. As discussed in a presentation at Defcon 20 by Haines ("RenderMan") [2], an intentional attacker can add false targets into the receivers (airplane, air traffic control, etc.) via ADS-B. A few years later, in a graduate research project, McCallie summarized, categorized, and evaluated the risk related to these novel standard avionics [3]. Each type of target, namely airplane (air-to-air transmission) and ground station (air-to-ground transmission), can suffer from aircraft detection, flood denial, and ghost injection. Furthermore, since ADS-B broadcasts periodically data containing ICAO 24-bit address, position, speed, amateur radio enthusiasts can sniff these data and follow the track of the airplane. Even though this kind of surveillance has been done for decades via other avionics such as Aircraft Communications Addressing and Reporting System (ACARS) or VHF Radios, the presence of ADS-B has made it more serious, since now it is easier for the eavesdroppers to track and follow the position of the airplane.

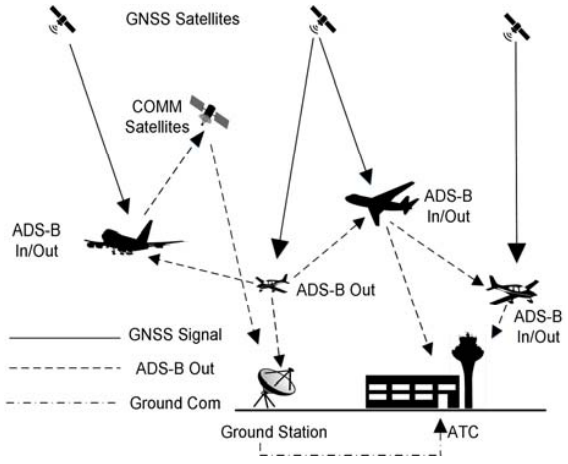

Fig. 1 ADS-B principles

Being attracted by the challenges of this new avionics, many studies have concentrated on finding the answer for these issues. One of the well-known proposals to increase the security level of ADS-B is embedding an authentication. This solution was first mentioned in the work of McCallie [3] and then was implemented using different approaches. For example, Valovage proposed a solution with encryption/ decryption technique applying to ADS-B data in [4], or recently, Baek et al. discussed the application of Identity-Based Encryption in [5]. In case of privacy, various techniques have also been studied, even by FAA themselves, such as protecting FAA's Aircraft Registry or anonymous mode for 1090 ES message [6]. Each of these proposals has their advantages and drawbacks. However, some of them require modifying the current message format, spectrum, and the current-in-use infrastructure. These solutions are, therefore, not feasible, in particular when the deadline of January 2020 is fast approaching.

Recently, in a publication in 2015, Yeste-Ojeda and Landry suggested the using of Differential 16 Phase Shift Keying

A-Q. Nguyen, A. Amrhar, J. Zambrano, G. Brown, and R. Jr. Landry are from Laboratory of Space Technologies, Embedded Systems, Navigation and Avionic (LASSENA), École de Technologie Supérieure (ÉTS), Montreal, QC, Canada (e-mail: renejr.landry@etsmtl.ca, phone: 514 396-8506)

O. A. Yeste-Ojeda is with the National Radio Astronomy Observatory. The NRAO is an NSF facility operated under cooperative agreement by AUI..

(D16PSK) modulation in the ADS-B 1090 Extended Squitter (ES) message to embed a digital signature [7]. As demonstrated in their studies, this approach is compatible with the current-in-use ADS-B. Therefore, no significant modification is required for the installed system. Moreover, with a digital signature, ADS-B message is authenticated in the receiver, hence increases the security level and protects the ADS-B system against harmful activities such as relay attack or ghost injection. The fusing together of Pulse Amplitude Modulation (PAM) and PSK in this Secure ADS-B (SADS-B), as proposed by them, will be one of the most promising solutions to solve the security issues and limited payload of the conventional ADS-B.

In this paper, the authors will continue the work, concentrating on implementing their digital signature idea, developing a hardware prototype and analyzing its performance and capabilities. Furthermore, this work also shows the unlimited potential of embedded payload in the phase of the SADS-B, via two simple applications with Unmanned Aerial Vehicle (UAV) and compress mode ADS-B. To evaluate and demonstrate the functionality as well as the promise of SADS-B, hardware-in-the-loop (HIL) simulation was used. The results of these scenarios confirm firstly the feasibility of the PSK bits of SADS-B in supporting future avionics with different utilizations. On the other hand, they also show that this system meets the requirements for a standard ADS-B 1090 ES Out/In system, as specified in the documents of RTCA [8].

The rest of this paper is organized as follows. The next section will focus on summarizing the principles of ADS-B, along with the type of attacks related to these avionics. After that, in Section III, an overview of the proposed SADS-B can be found, including data format, encryption solution, and hardware architecture. Section IV will demonstrate the HIL simulation, the scenarios, and the related results. Based on these data, Section V will show the conclusions of the authors about this innovative modification of ADS-B, as well as the perspectives and suggestion for further studies.

II. Overview

A. Principle of ADS-B and ADS-B 1090 ES

In general, ADS-B can be separated by different categories. In case of transmitter (TX) and receiver (RX), ADS-B includes ADS-B Out (TX) and ADS-B In (RX). These two systems can be developed and installed independently, and only ADS-B Out will become the mandatory avionics from 2020. In case of carrier, spectrum, and modulation standard, ADS-B NextGen contains two distinguished avionics, ADS-B 1090 MHz Mode-S Extended Squitter (ADS-B 1090 ES) and Universal Access Transceiver (UAT). Table I summarizes some main characteristics of the two types of avionics.

Depending on the airspace utilization, the airplane can install the suitable system. Fig. 2 illustrates these options, as adopted by the documents of FAA [1]. Since this paper only concentrates on the ADS-B 1090 ES, in the scope of this work, ADS-B and ADS-B 1090 ES should be considered as one. Fig. 3 shows the standard message format of an ADS-B message, along with the number of bits, pulses shape, and spacing.

B. Security Issue, Privacy Risks, and Limited Payload

From the characteristics mentioned in Table I, as well as the message format in Fig. 3, it can be seen that ADS-B does not include any solution regarding security and privacy. In fact, as discussed in the report of FAA in 2009 [9], *"encryption of any ADS–B data would unnecessarily limit its use internationally"*. This explanation was understandable at that time, however, unacceptable for some applications in reality, for example, private or non-commercial flights. Recently, acknowledging the rapid development of Software Defined Radio (SDR) technologies, which can be used to establish a sniffing station with a budget of less than $100 US, FAA started to find the solutions for this privacy issue [6]. However, solving the problem of privacy could not increase the robustness of the system against harmful actions, as described in previous works, for example [2], [3], [10].

Based on the previous studies in [3], [7], [10], as well as the authors' point of view, attacks related to ADS-B infrastructure can be categorized as in Table II.

TABLE I
PRINCIPLE OF ADS-B 1090 ES AND UAT [8], [11]

	ADS-B 1090 ES	UAT
Center Frequency	1090 ± 1 MHz	978 MHz ± 20 kHz
Bandwidth	−40 dBc at >23 MHz from center	−60 dBc at >3.25 MHz from center
Bit Rate	1 Msps	1.041667 Msps
Modulation	Pulse Amplitude Modulation (PAM)	Continuous Phase Frequency Shift Keying (CPFSK)
Message Length	112 bits (120 μs with Preamble)	Basic: 276 bits Long: 420 bits
Type of System	Broadcast, In and Out separated	Transceiver, RX and TX together
Transmission Rate	~ 4 Hz	1 Hz

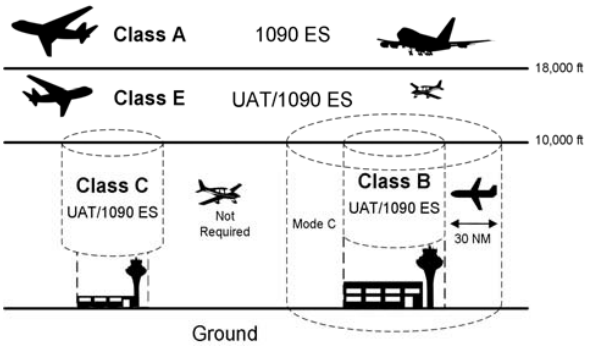

Fig. 2 ADS-B requirements in US airspaces

Moreover, Fig. 3 also illustrates the second problem within ADS-B 1090 ES, which is the limitation of payload. In fact, in trade-off the robust modulation for low requirements of transmitter and receiver, ADS-B 1090 ES uses a relatively wide bandwidth compared to other avionics sharing a similar data rate. In order to support its 112-bit message, ADS-B

occupies up to 50 MHz (20 dB attenuation from peak) [8]. With the increasing number of transmitters from now to 2020 and beyond, expanding the payload of the current ADS-B via increasing the number of bit in the message is unacceptable and unfeasible.

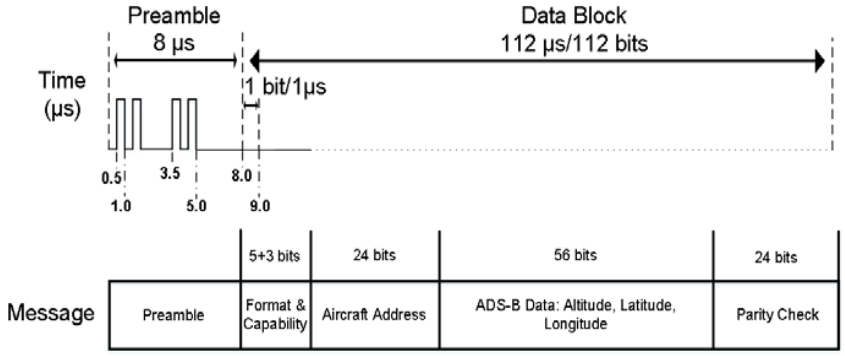

Fig. 3 ADS-B 1090 ES signal and message format

TABLE II
ATTACKS AND RISKS RELATED TO ADS-B

Type of Attack	Description	Complexity	Risk
Eavesdropping	Sniffing Tracking	Low	Low in Security High in Privacy
Jamming	Jam the channel completely with high power transmitter	High for Air, Moderate for Ground System	Moderate in Security
Hazardously Misleading Information (HMI)	Spoofing, Relay Attack, Message Manipulation	High for Air, Moderate for Ground System	High in Security

III. SECURE ADS-B APPROACH

A. Overview

As discussed and analyzed in [7], Secure ADS-B 1090 ES will carry separated information in amplitude (PAM) and phase (PSK), and therefore, no modification needs to be made in the structure of the current ADS-B message, as well as the assigned spectrum. Because of the requirements in bit rate and spectrum of the conventional system (Table I), D16PSK is the optimal option for the embedded signature, results in a capability of 448 useful bits in the phase for a 112-bit ADS-B 1090 ES message. Hence, SADS-B increases the number of bits significantly from 112 to 560 for each message, without increasing the bandwidth. However, because D16PSK is sensitive to noise and other distortion compared to PAM, some consideration needs to be given to increase the robustness of the signature. For this application, Forward Error Correction (FEC), or Reed-Solomon to be precise, is a good solution. Fig. 4 shows the theory Bit Error Rate – Signal-to-Noise (BER-SNR) in a White Gauss Noise Channel (AGWN) of PAM (black line), D16PSK without RS (dash line), D16PSK with RS(255,247) (dash line with diamond marker), and D16PSK with RS(255,233) (dash line with x marker). As it can be seen, without RS, the BER of D16PSK is high, even at an SNR above 16 dB. The implementation of RS(255,247) improves the performance of this signature, particularly when with the SNR above 14 dB. The higher order of RS, the better this improvement, nevertheless, one needs to consider also the trade-off between this improvement and the loss of useful bit. With a RS(255,233), the in-phase bits will lose 176 bits, meaning nearly 40% of the capacity, just for correcting the bit error. Therefore, at this stage of the study, authors propose using only RS(255,247) for the PSK bits in the SADS-B.

After reserving 64 bits at the end of the message for the RS, different approaches can be made to optimize the use of the 384-bit payload. In general, the more bits we have with the digital signature, the harder it is for the attacker to crack the code, get the key, and attack the system. For example, as mentioned in [12], increasing the number of bits from 50 to 75 can increase 650 times the number of iteration needed to break the encryption method. However, it is also true that using all of the payloads in the phase as a signature, as proposed in [7], will waste the potentials of SADS-B to compensate for the limited spectrum issue in aviation. A balance between the digital signature and payload for other applications needs to be decided. In this work, the authors will present all three options, 448-bit digital signature SADS-B, no digital signature and a mix between the two as a reference for the studies in the future.

Fig. 5 presents the format and the utilization of SADS-B as the first option aforementioned. Meanwhile, Fig. 6 demonstrates the procedure to establish the SADS-B Out and In as well as the requirements in transmitter and receivers. In general, every airplane before take-off will receive a key from the authorities, which will be used to encrypt the [ADS-B message + UTC] field in real time during the flight, forming a dynamic digital signature. In this work, in order to adapt the signature with the available 384 bits, Advanced Encryption Standard (AES) is used. Along with 64 RS bits, this signature will be embedded in the PSK modulation part of the SADS-B and transmitted to the air. In RX, with a standard ADS-B In, no difference would be noticed, and standard PAM section will be decoded, together with the low ability to detect HMI attacks.

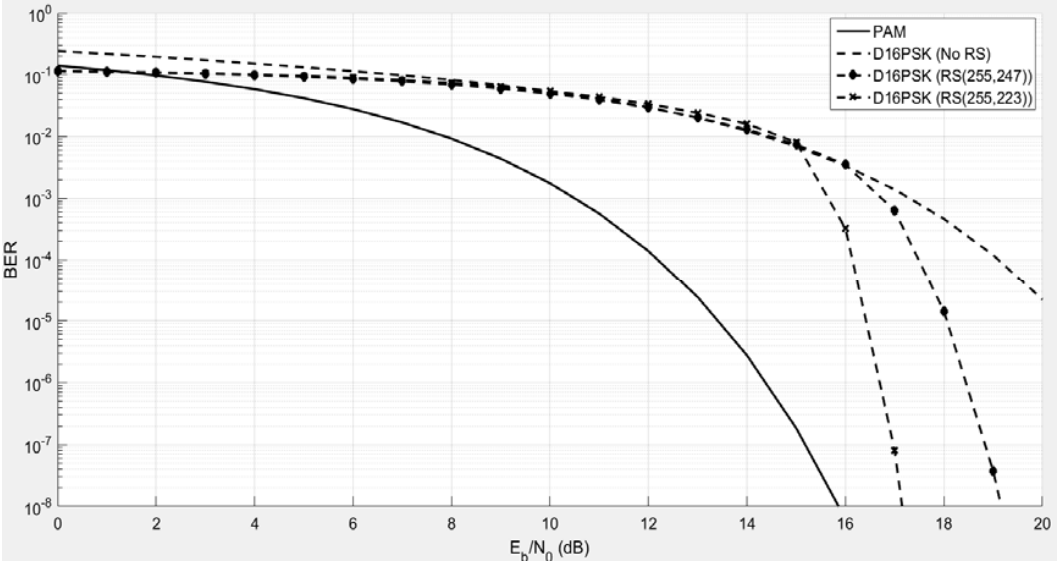

Fig. 4 BER-SNR theory curves for SADS-B, with and without RS (from MATLAB BER Analysis Tool)

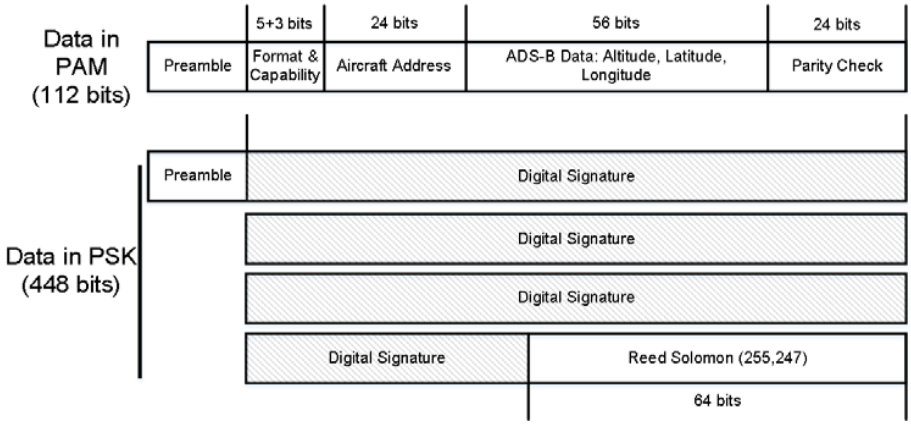

Fig. 5 Structure of the digital signature in SADS-B

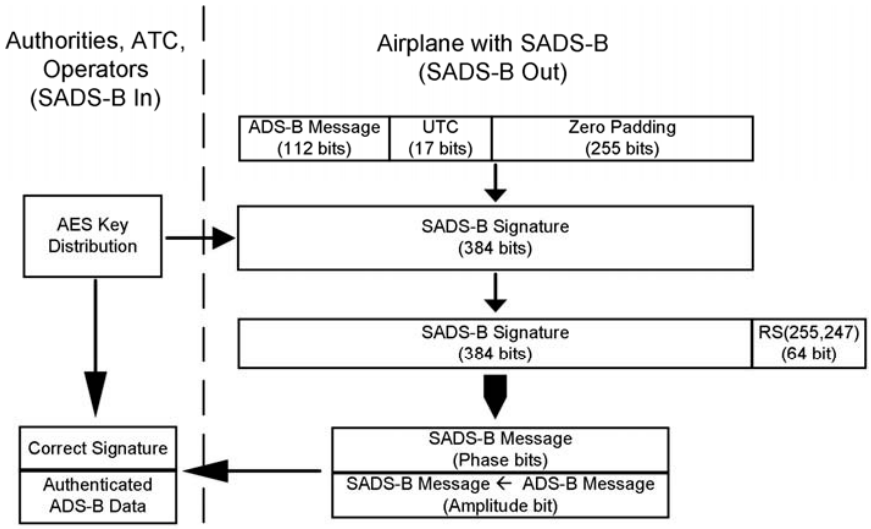

Fig. 6 Fully embedded digital signature in SADS-B option

The SADS-B in receiver, meanwhile, detects the PSK bits along with the PAM data, and will filter out any invalid message, reducing significantly the chance of being attacked, hence increases the integrity of the system in general. To crack this signature, the attacker not only needs to break through the AES key but also the way the zero-padding is implemented. With the number of unknown variables and the limited repetition of data, this could be considered as nearly impossible. Furthermore, to maximize the embedded data in the digital signature and even further increase the robustness of the signature, the zero-padding bits can be later replaced by any additional data, for example MAC address of the transmitter or real-time airplane conditions, or transmitted signal timestamp.

The second option of using these bits, as discussed, will concentrate only on increasing the capability and payload of the conventional ADS-B. By quintupling the payload, many applications can benefit this feature, and hence increase the air-ground communication rate with reasonable expenses. A good example for this utilization is the satellite service supporting NextGen ADS-B. As a part of this future air transportation system, and as shown in Fig. 1, the airplane far from the tower, such as in the middle of the ocean, will transmit ADS-B signal to the ground station via satellites. These satellites in turn will act as a repeater, passing these messages through space to the nearest ground station. The point is that, with the rapid increase in number of ADS-B Out, more satellites, as well as higher work rate will be required to support this system. SADS-B, with the phase modulated bits, can be the solution for this issue. The 384-bit payload of PSK modulation can support up to three ADS-B 1090 ES messages at a time. In the other words, any SADS-B Out signal can carry the ADS-B data of up to four airplanes, reducing the work rate of the satellites by a factor of four. This idea is summarized and illustrated in Fig. 7.

According to the two options above, with one maximizing security and the other optimizing the payload bandwidth, a compromise can be made. Fig. 8 presents the architecture of the in-phase bits for this option. By reducing the zero-padding and compressing the [ADS-B data +UTC] field into 192 bits, this approach offers a 136-bit payload, which carries any auxiliary data, as decided by the user. A scenario for the utilization of these bits will be discussed later, at the end of this paper.

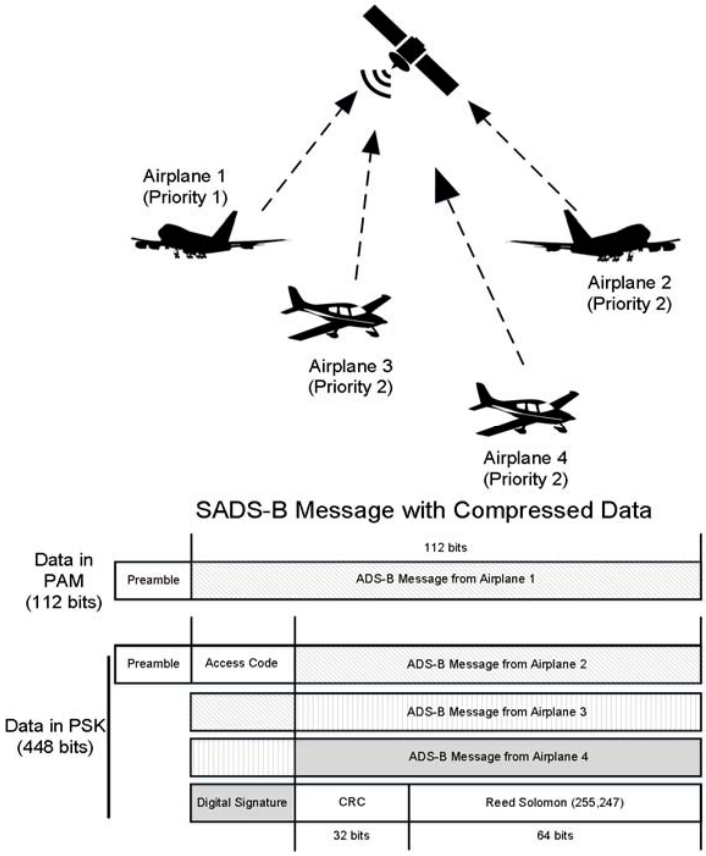

Fig. 7 SADS-B in compressed data mode for satellites

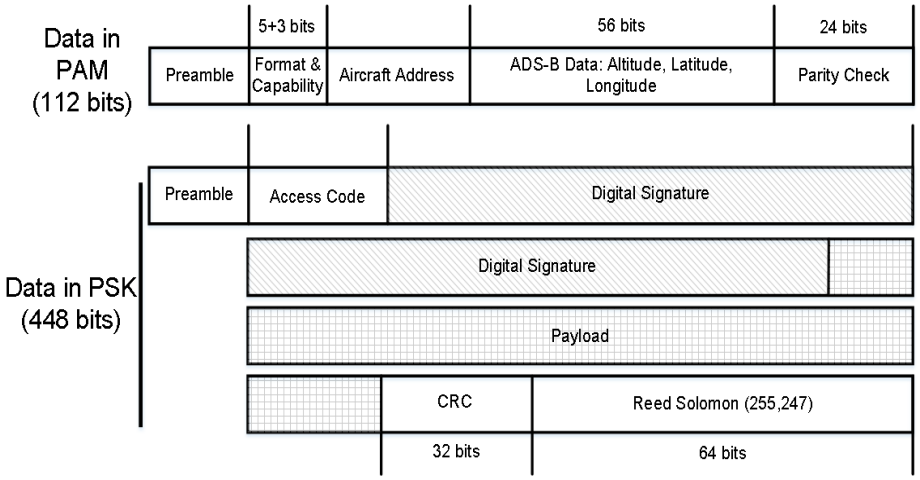

Fig. 8 SADS-B with digital signature and additional payload in PSK bits

With any options of the phase-modulated bits, SADS-B always embeds 560 bits, 112 bits with PAM and 448 bits with PSK. Using a Mixed Domain Oscilloscope (MDO), Figs. 9 and 10 can be obtained. Fig. 9 illustrates the phase, amplitude and spectrum (respectively from top to bottom) of the conventional ADS-B signal, meanwhile, the latter shows the SADS-B results for the same transmitting message from both figures, it can be concluded that:

- There is no difference in PAM between the two messages, which means an ADS-B In would output the same results for both messages.
- The phase of the SADS-B synchronized correctly with the PAM pulses, and carrying the modulated data, unlike the random phase output of conventional ADS-B.
- Both spectrums meet the requirements specified in [8], as analyzed in [7].

B. Architecture and Implementation

The implementation of the SADS-B is separated into two systems, namely SADS-B Out and SADS-B In, as same as its precedent ADS-B. Fig. 11 shows the principle components included in each system, as well as their connection and functionalities. In general, this modified ADS-B has the same primary sub-components as MM-SDAR, namely Analog Sections, Software Defined Radio (SDR) Platform, and General Purpose Processor (GPP).

In this work, the heart of the GPP is the open-source program GNU Radio, meanwhile, the FPGA was developed using Xilinx System Generator. The SDR platform is a PicoZepto of Nutaq, equipped with a 12-bit ADC/DAC in LMS6002D. As part of AVIO-505 project, this system is also integrated in the PicoSDR platform, with the role of an application in Multi-Mode Software Defined Radio Architecture (MM-SDAR) [13]. Table III points out some critical parameters of the SDR platform used to develop the SASD-B Out and In, and will be used in the HIL simulation in the next section.

Depending on the utilization of the in-phase bits, these blocks in GPP can be modified adaptively. For example, in case of the fully digital signature, no Auxiliary Source is required. However, Encryption/Decryption Algorithm needs to be integrated. The encrypt and decrypt algorithm and function is developed based on the work of Müller with his gr-openssl Out-Of-Tree module [14]. Also, the SADS-B with digital signature needs a mechanism downstream to filter the invalid message regarding the signature.

At the transmission, after receiving the Amplitude and Phase data from GPP, the FPGA will calculate the corresponding outputs. At the reception, in order to maximize the performance of the current hardware, a particular architecture is developed to support a data rate of 40 Msps. In addition, as shown in Table III, low-IF is used to avoid some of the problems related to Zero-IF architecture of the SDR platform, such as DC Offset and IQ imbalance.

TABLE III
SELECTED SDR PLATFORMS AND IMPORTANT PARAMETERS

SDR Platform	PicoZepto	PicoSDR
RF Architecture	- Original: Zero-IF - Current: Low –IF (RX) with a shift of 5 MHz - Frequency Range: 300 – 1500 MHz - One TX/RX	- Original: Zero-IF - Current: Low-IF (RX) with a shift of 5 MHz - Frequency Range: 300 – 3800 MHz - Multiple TX/RX
ADC/DAC	- Integrated in Radio420X - 12 bits resolution - Max sampling rate: 40 MHz	
RX Gain	- Total gain control: 79 dB - Resolution: 1 dB	
TX Gain	- Total gain control: 70 dB - Max Output Power: 20 dBm	

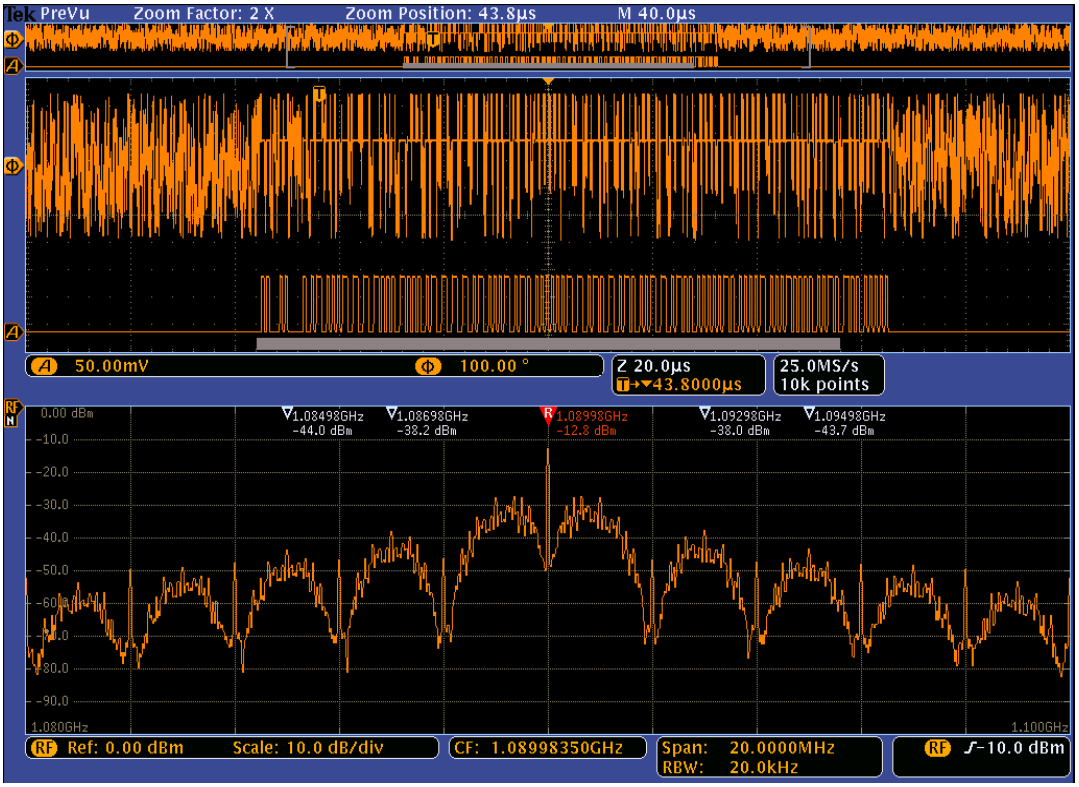

Fig. 9 ADS-B phase, amplitude, and spectrum.

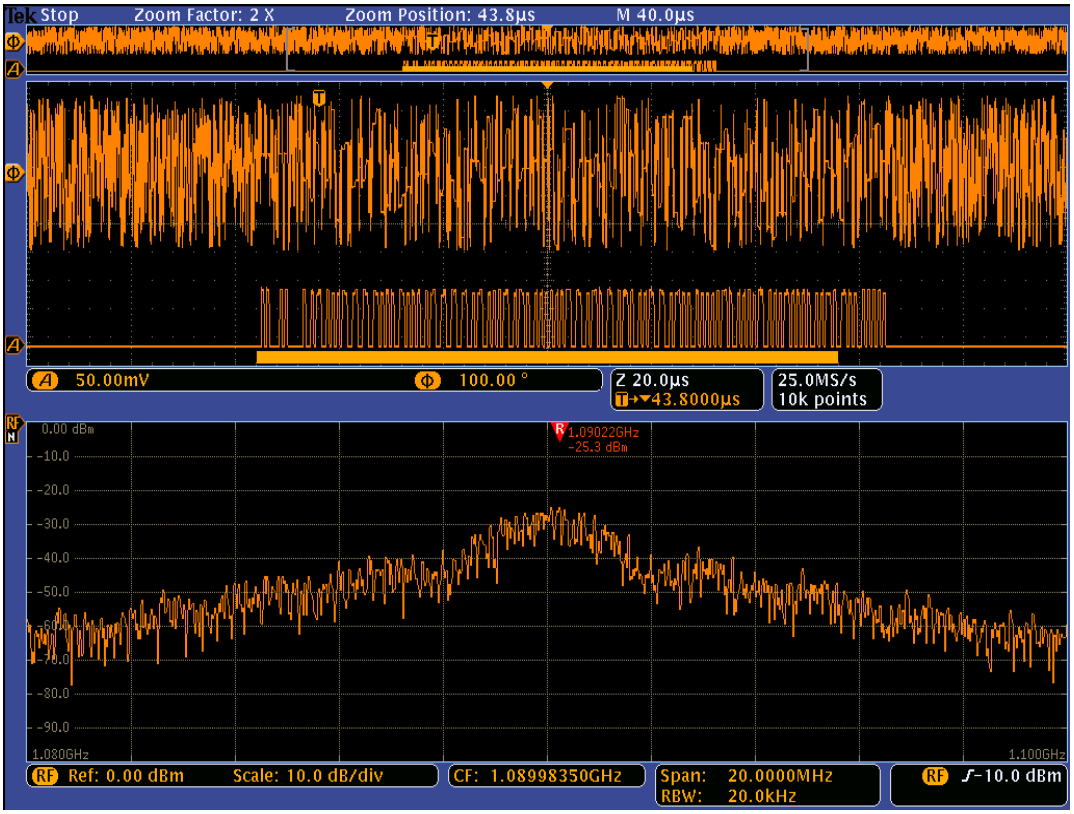

Fig. 10 SADS-B phase, amplitude, and spectrum

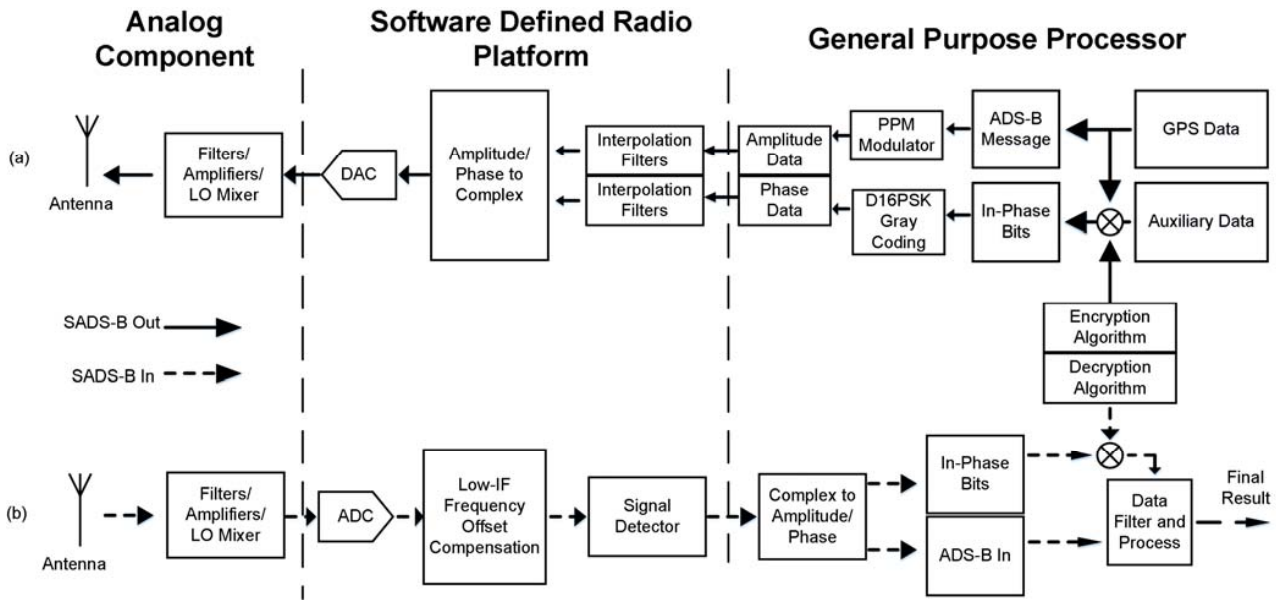

Fig. 11 SADS-B Out (a) and In (b) Architecture overview

C. Measurements and Validations

The measurement and validation of the SADS-B were done in a controlled environment in the laboratory using certificated equipment (Aeroflex IFR-6000), using the same procedure as the current-in-use ADS-B. Fig. 12 shows the result in the IFR-6000 for a SADS-B Out test, underlines the compatibility of the SADS-B Out signal with the current standard of ADS-B 1090 ES. Table IV summarises the results of the laboratory tests of the SADS-B Out, along with the corresponding standards. As it can be seen, these proposed avionics met all of the requirements.

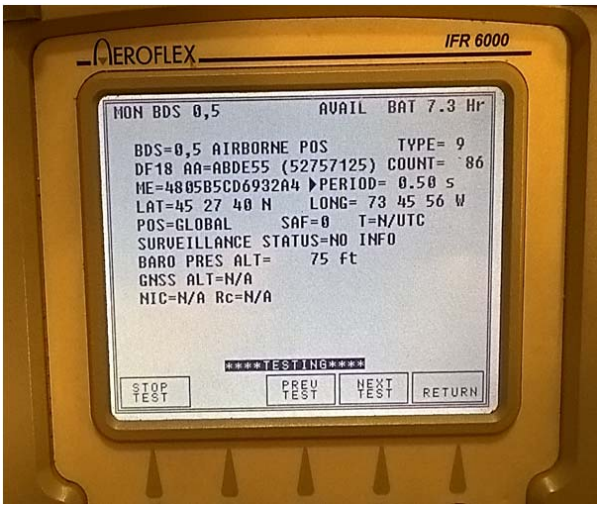

Fig. 12 SADS-B Out verified with IFR-6000

In order to evaluate SADS-B In, IFR-6000 was used as an ADS-B Out transmitter. An ADS-B In and a SADS-B In (both with Zepto as the SDR platform) were connected directly to the output of the IFR-6000. The number of decoded messages in one minute of each system with different output levels of the IFR-6000 was recorded. The RX gain of both system is set at the optimum level to have the best SNR. As it can be seen from Fig. 13, thanks to the modifications with low-IF and high data rate, SASB-D has better results compared to the standard ADS-B In, confirming the compatibility of ADS-B Out and SADS-B In.

From the results described above, Table V outlines the compatibility between SADS-B and ADS-B, for both In and Out modes. In order to demonstrate the functionality of SADS-B, HIL simulation was used. The scenarios and the setup of settings of these simulations tests can be separated into two cases, corresponding to the full-bit digital signature and full payload bits as aforementioned.

TABLE IV
PERFORMANCE OF SADS-B OUT VERIFIED BY IFR-6000

	Standards [8], [11]	SADS_B Out
Format for Type 9	Verified by IFR-6000	
Format for Type 4	Verified by IFR-6000	
Format for Type 19	Verified by IFR-6000	
Period for Type 9	0.5 s	0.5 s
Period for Type 4	5 s	5 s
Period for Type 19	0.5 s	0.5 s

TABLE V
COMPATIBILITY OF ADS-B AND SADS-B

Transmitter	Receiver	Data	Signature	Number of Useful (Decoded)Bit
ADS-B Out	ADS-B In	Yes	No	112 (112)
	SADS-B In	Yes	No	112 (112)
SADS-B Out	ADS-B In	Yes	No	560 (112)
	SADS-B In	**Yes**	**Yes**	**560 (560)**

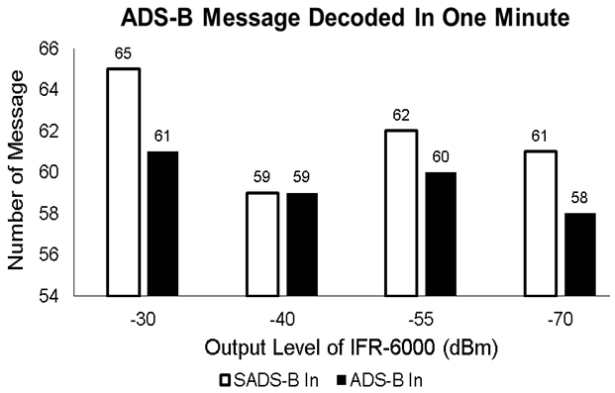

Fig. 13 Performance comparison of SADS-B In and ADS-B In

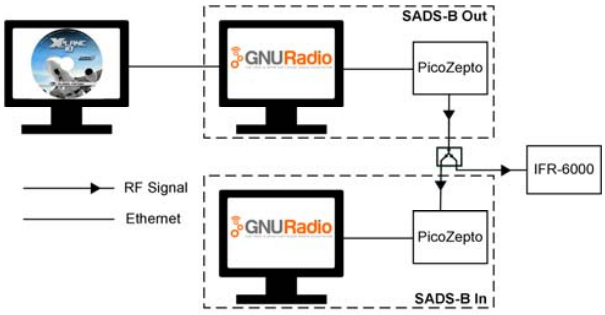

Fig. 14 Hardware-in-the-loop simulation setting

IV. Hardware-in-the-Loop Simulation

A. Scenario 1: 386-bit Digital Signature – High Secure Mode

Fig. 14 presents the connection of the systems for this HIL simulation. In short, GPS data, including position, speed, and UTC is generated by a scenario in X-Plane 10. These data will be passed to the GPP of the SADS-B Out, which will create the output standard message. Also, together with the UTC, this message will be used to create the digital signature by the AES algorithm via a 32-byte key. The output of the SADS-B Out is wired with the input of SADS-B In, as well as the IFR-6000 to monitor the message at all time. In the GPP of SADS-B In, the system will decode not only the data in PAM but also the bits in PSK using the same key as the SADS-B Out. After retrieving the [ADS-B message + UTC] field correctly, the receiver will filter out any invalid message, both data, and timeout, and then will keep only the authenticated data. In this test, the output rate of SADS-B is set at 2 Hz. Meanwhile, the update date rate of signature is around 1 Hz. After 90 seconds, the number of received message in the SADS-B In, as well as data related to the signature is analyzed. Fig. 15 illustrates the results in one of the tests with this scenario. As it can be seen, the SADS-B In received and decoded correctly the message SADS-B Out (the white diamond), regarding the trajectory (line). Along with these ADS-B data, the signature carrying the encrypted data is also decrypted and decoded, as described by the black circle. A statistical result analysis of this scenario for six tests is also presented in Table VI. From the results in the figure and the table, the following conclusions can be made:

- The SADS-B Out works well and is compatible with an ADS-B In, even though this receiver cannot detect the changes of the embedded signature (as monitored during the tests with IFR-6000).
- The SADS-B In receives and decodes the information in both PAM and PSK, even though the latter is a little less robust than the first, due to the nature of PSK modulation.
- The receiver received and decoded more than 81% of the signatures correctly from the transmitter, corresponding to a BER of 1.7×10^{-5}.
- Without synchronizing the Encryption and Decryption, the Decryption in SADS-B In was still able to output the correct data embedded in the signature. The rate at which the output data is correctly decrypted is therefore promising to and set to increase as long as a mechanism to synchronize the encryption is defined and established.

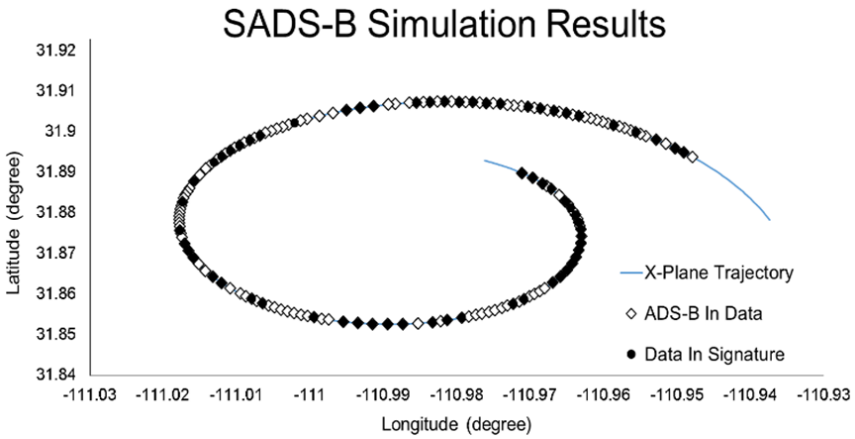

Fig. 15 SADS-B with digital signature HIL results

TABLE VI
SADS-B RESULT SUMMARY WITH DIGITAL SIGNATURE SIMULATION

Parameters	Receiver
Number of received messages	192
Average SNR Level of SADS-B In	~25 - ~30 dB
Received messages vs Output messages	96%
Number of received signatures	180
Correct signatures vs Received messages	81.33%
Received signatures vs Created signatures	92.42%
Decrypted data vs Correct signatures	78.8 %

B. Scenario 2: No Signature – Compressed SADS-B Mode

This scenario uses the same configuration of the one above. However, as mentioned by its name, the bits of PSK modulation are filled up with the ADS-B message from other airplanes. In this test, the PAM bits carry the position information of an airplane using the address ABDE55, transmitting at a rate of 2 Hz, as specified in the official documents [8]. In the PSK bits, the paired messages are filled with ID messages of two airplanes (D5A1C9 and A92492) and an airborne velocities message from the third airplane (9D4455). With unpaired messages, the phase-modulated bits also integrate the velocities message from the same airplane, however, the address data will be from two other airplanes (8E1810 and BF2235). After 120 seconds, the number of received messages, as well as the integrated data in the signature will be analyzed using the same methods as above. Fig. 16 shows the simulated trajectory, where the black crosses are the position decoded from SADS-B In. Meanwhile, Fig. 17 summarizes the results of these simulations, as an average of 10 simulation runs. From the figures, it can be seen that the integration of the PSK-modulated bits with compressed ADS-B data does not affect the performance of the main messages. SADS-B In received and extracted the position data in the PAM modulation correctly. More importantly, SADS-B In can also extract correctly the data from the ADS-B messages compressed in the PSK. In fact, with a high SNR value as in this test (~25 dB), the performance of the PSK bits is even more robust than PAM, as the SADS-B In received more data of other airplanes than the main airplane ABDE55. The statistic shows that with this application, SADS-B In gets 98.53 % correct signature regarding the created signature of ADS-B Out. A SADS-B system with the compressed ADS-B mode, therefore, offers the possibility of saving up to four times the transmitting power, without degrading the original ADS-B transmission. This value is worth to be mentioned, in particular for any applications that have power efficiency as the essential requirement.

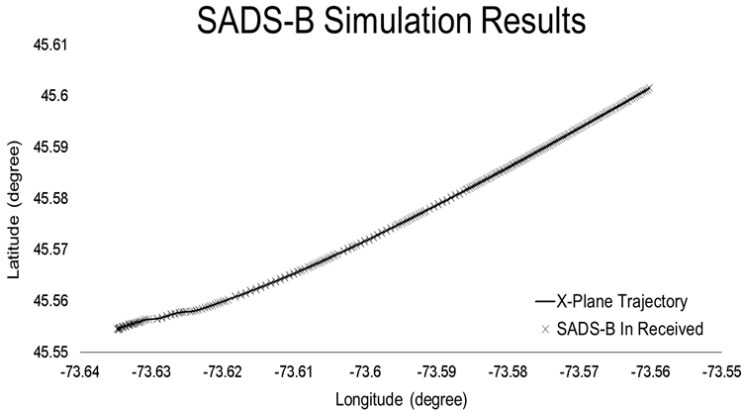

Fig. 16 ADS-B decoded data via SADS-B PAM bits

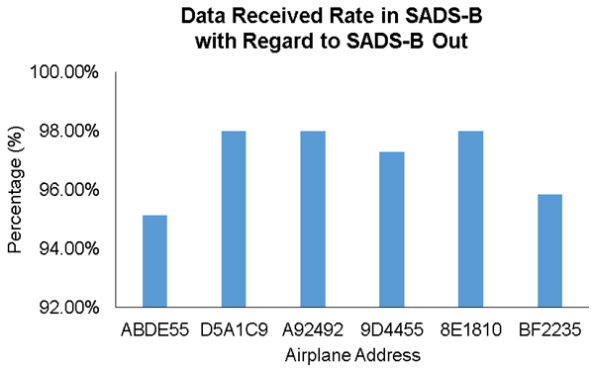

Fig. 17 Received data summarized for compressed ADS-B mode

V. FURTHER DISCUSSION AND CONCLUSION

In this paper, the authors have presented the implementation, testing and analysis of SASD-B to increase the security and capacity of the current ADS-B 1090 ES. As it can be seen from the HIL simulation results, the utilization of PSK-bits is feasible and promising, which can be easily integrated into the current-in-use infrastructure without the needs for expanding the bandwidth or modifying the spectrum. Furthermore, because SADS-B is compatible with ADS-B Out and ADS-B In, both system can co-exist and co-operate together, according to the different interests of the users.

In case of using the extra bits as a digital signature, SADS-B can achieve a higher security level compared to ADS-B. With authentication, the receivers such as Air Traffic Control and ground stations can have the necessary mechanism to

avoid HMI attacks using only the data in the messages. This approach is for sure a more robust answer, regarding the current costly multilateration solution. Furthermore, by replacing the zero-padding with data, this signature can also provide a privacy and secure channel to transmit specific data from air to ground. On another hand, the extra payloads offered by the PSK bits can also increase the data rate of the ADS-B, which can finally reduce the cost and hardware requirements for the future NextGen infrastructure. As demonstrated in the second scenarios, SADS-B can compress ADS-B data from multiple sources into one message, which is practical for satellite applications because of the economy in power, processing resources, etc. In addition, as it can be seen from Fig. 18, SADS-B can also become a promising solution for the future unmanned/manned interaction airspace. In order to have a safe and secure shared airspace for manned and unmanned vehicles, one of the solution, as mentioned in [15], [16], would be the integration of ADS-B into specific UAVs. The implementation of SADS-B in place of standard ADS-B will, therefore, not only reduce the requirements and cost of each unit but also protect the UAV airspace from any HMI attacks via ADS-B avionics.

Even though the above measurements and results are enough to show the functionalities and capabilities of SADS-B, they are not enough to make the conclusion about the live performance of this modified ADS-B. Real-world tests, particularly flight tests, will be the next essential steps for evaluating the proposed system.

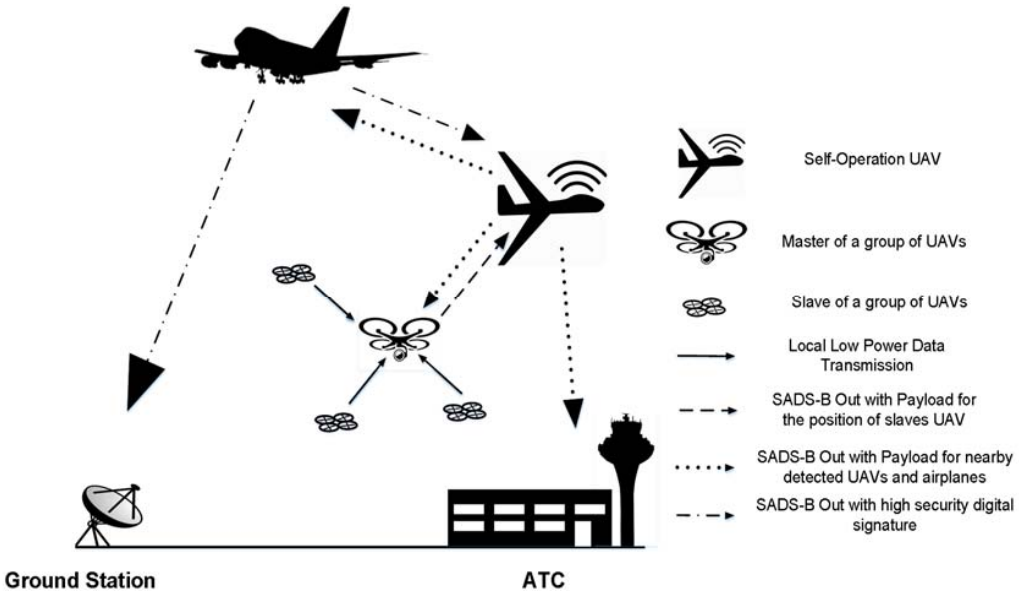

Fig. 18 Suggestion for global security and integration of SADS-B in all kind of flying planes

ACKNOWLEDGMENT

The works presented in this paper is a part of AVIO-505 project at LASSENA, ÉTS. It is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC), the Consortium for Research and Innovation in Aerospace in Quebec (CRIAQ) as well as three main strategic partners, namely Bombardier Aerospace, MDA, and Marinvent Corporation.

REFERENCES

[1] F. A. A. Federal Aviation Administration. NextGen (Online). Available: https://www.faa.gov/nextgen/

[2] Brad "RenderMan" Haines. Hackers+Airplanes: No Good Can Come Of This (Online). Available: https://www.defcon.org/html/links/dc-archives/dc-20-archive.html#Renderman

[3] D. L. McCallie, "Exploring Potential ADS-B Vulnerabilities in the FAA's Nextgen Air Transportation System," Air Force Institute of Technology2011.

[4] E. Valovage, "Enhanced ads-b research," in *25th Digital Avionics Systems Conference, 2006 IEEE/AIAA*, 2006, pp. 1-7: IEEE.

[5] J. Baek, E. Hableel, Y.-J. Byon, D. S. Wong, K. Jang, and H. Yeo, "How to Protect ADS-B: Confidentiality Framework and Efficient Realization Based on Staged Identity-Based Encryption," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 690-700, 2017.

[6] K. Lynch, "FAA Exploring Possible Privacy Protections for ADS-B," in *AINonline*, ed. Regulations and Government, 2015.

[7] O. Yeste-Ojeda and R. Landry, "ADS-B Authentication Compliant with Mode-S Extended Squitter Using PSK Modulation," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, 2015, pp. 1773-1778.

[8] RTCA Special Committee 186, "DO-260B Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance - Broadcast (ADS-B) and Traffic Information Services - Broadcast (TIS-B)," ed. Washington, DC: RTCA, Inc, December 2009.

[9] F. A. A. Federal Aviation Administration, "Automatic Dependent Surveillance - Broadcast (ADS-B) Out Performance Requirements To Support Air Traffic Control (ATC) Service; Final Rule," vol. 14 CFR Part 91, ed. Department of Transportation, 2009.

[10] 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 USA*, pp. 1-12, 2012.

[11] RTCA Special Committee 186, "DO-282B Minimum Operational Performance Standards (MOPS) for Universal Access Transceiver (UAT) Automatic Dependent Surveillance - Broadcast (ADS-B)," ed. Washington, DC: RTCA, Inc, December 2009.

[12] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the*

ACM, vol. 21, no. 2, pp. 120-126, 1978.
[13] A. Amrhar, A. A. Kisomi, E. Zhang, J. Zambrano, C. Thibeault, and R. Landry, "Multi-Mode reconfigurable Software Defined Radio architecture for avionic radios," in *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2017*, 2017, pp. 2D1-1-2D1-10: IEEE.
[14] S. Müller. gr-openssl Out-Of-Tree Package (Online). Available: https://github.com/sbmueller/gr-openssl
[15] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, "Realities and challenges of nextgen air traffic management: the case of ADS-B," *IEEE Communications Magazine,* vol. 52, no. 5, pp. 111-118, 2014.
[16] R. Carnie, R. Walker, and P. Corke, "Image processing algorithms for UAV" sense and avoid"," in *Robotics and Automation, 2006. ICRA 2006. Proceedings 2006 IEEE International Conference on*, 2006, pp. 2848-2853: IEEE.