ADS-B Authentication Compliant with Mode-S Extended Squitter Using PSK Modulation

Omar A. Yeste-Ojeda, *Member, IEEE*, René Jr. Landry, *Member, IEEE*
LASSENA Labs
École de Technologie Supérieure
Montreal, Canada

Abstract—**This work proposes to use Differential 16 Phase-Shift Keying (D16PSK) modulation for embedding a digital signature within Mode-S Extended Squitter (ES) Automatic Dependent Surveillance-Broadcast (ADS-B) messages. The purpose is to provide a security mechanism in order to protect systems against the injection of malicious Hazardously Misleading Information (HMI). The use of digital signatures for ADS-B has been previously analyzed in the literature. Our contribution and focus are devoted to the physical layer used to transmit such a signature. The proposed method generates ADS-B messages compliant with current standards, thus can be interpreted by current equipment. However, only a modified receiver shall be able to extract the embedded signature and authenticate the message. This work describes possible architectures for the ADS-B transmitting and receiving devices. An analysis of the expected maximum range and bit error rate for various PSK modulations is provided. In addition, the use of timestamps to protect against message replays is proposed and studied in the final part of the paper. In summary, this paper proposes a backward compatible way to secure the ADS-B system for the Mode-S ES data link, providing regulatory authorities with the means in case they opt for the use of digital signatures. The proposal is inspired from the idea behind the wireless security encryption method of Nagravision used in the Satellite TV broadcasting.**

Keywords—ADS-B, digital signature, spoofing, authentication

I. Introduction

The Automatic Dependent Surveillance-Broadcast (ADS-B) system is the key element of global next generation air traffic management initiatives, such as NextGen [1] or SESAR [2]. ADS-B has been devised to satisfy the challenging requirements from the increased traffic density expected for the following decades. Through ADS-B, a participant (aircraft, ground vehicle or obstacle) broadcasts its own position (computed by other means, such as a Global Navigation Satellite System, GNSS, receiver) to other participants through a data link. This data link is based on 1090 MHz transponder Mode-S Extended Squitter (ES) messages internationally or, currently only approved in the US, the Universal Access Transceiver (UAT).

Recently, some voices within the aeronautical communities have raised their concerns about whether the current security level of the ADS-B system would be enough [3], [4]. Because the ADS-B system depends on GNSS, it can be attacked either directly via Mode-S RF signal hacking or indirectly through GNSS. Our purpose herein is to focus on those threats that are specific to ADS-B, and more precisely, on those affecting the transponder Mode-S ES data link. Namely, the potential intentional threats to ADS-B that have been identified so far, to the authors' knowledge, are [5], [6]:

1) Eavesdropping, which is inherent to ADS-B since messages are intentionally not encrypted so that a large number of users can receive the broadcast messages without increasing the system's complexity. Nonetheless, some previous works have proposed the use of cryptography to deal with potential threats arising from eavesdropping [8].
2) Jamming or denial of service, through a transmitter operating at the 1090 MHz channel.
3) Radiation of Hazardously Misleading Information (HMI), which can manifest in the following forms:
    a. Spoofing (or impersonation) of ADS-B messages since messages are not authenticated. Currently, the only way to verify ADS-B messages is through additional systems, such as multilateration, which nonetheless do not represent a definite solution.
    b. Message manipulation, by corrupting the message at the receiver's end.
    c. Message injection or replay, since any attacker can generate apparently legitimate messages or simply record and playback at a different time legitimate messages.

This work proposes a backward compatible mechanism to sign ADS-B messages, therefore enabling a seamless transition from the current system to a secure one. The signature allows the ADS-B receiver to authenticate the message, i.e., to determine whether the identity claimed in the message truly originated it. Since any message alteration will produce an authentication failure, signing ADS-B messages shields the system against radiation of HMI in the form of spoofing, message manipulation, or message injection. Moreover, although no timestamp is transmitted within the message, it can be attached at the end so that a paired message plus timestamp is signed. Only the message and the signature are transmitted, and the receiver adds the timestamp in order to authenticate the message. Obviously, this approach requires certain time

978-1-4673-6596-3/15 $31.00 © 2015 IEEE
DOI 10.1109/ITSC.2015.288

synchronism between the ADS-B transmitting and the receiving devices, which is already available through the GNSS measurement unit.

In order to secure ADS-B data link, several approaches have been proposed in the literature: multilateration, hashing, symmetric and asymmetric encryption. The main advantage of multilateration is that it does not require any modification on current ADS-B transmitting devices. But it needs at least four receiving devices to verify the ADS-B information using the physical parameters of the signal (power, time of arrival, or Doppler frequency shift) [6], [7]. Moreover, it requires very precise synchronization between the receiving participants, which highly complicates the use of multilateration by airborne participants. Furthermore, it cannot prevent HMI injection through, e.g., a drone, and it will limit the range of usage. Symmetric [8], [9] and asymmetric [7], [10] encryption introduce extra complexity in the system, and makes ADS-B messages illegible for current equipment. In addition, encryption introduces the additional risk of messages not being received because of a failure in the management or a misuse of keys.

For these reasons, this work is based on the use of digital signatures (hashing) for securing ADS-B from HMI. Several previous works have proposed the use of digital signatures for ADS-B [11]-[14]. However, these works focus on the UAT data link and the security framework. They propose to include the signature as part of the ADS-B message, either by increasing the message length, changing the signal modulation or by substituting part of the message. This cannot be extrapolated to Mode-S ES messages without compromising on performance due to capacity limitations.

On the contrary, this work focuses on how to transmit the signature within a Mode-S ES message format and proposes a method which is fully compatible with current standards. Similar objective was pursued in [11] for ADS-B over UAT. This means that current ADS-B equipment will see our signed messages as valid, and will be able to retrieve the same information as from a not signed message. In addition, compatible ADS-B receivers will be able to extract the signature and authenticate the message as well.

This backward compatibility is attained by transmitting the digital signature using Phase-Shift Keying (PSK) modulation, since current Mode-S ES messages use Pulse Position Modulation (PPM).

II. System description and security improvement

Using the Mode-S ES format, ADS-B messages use Pulse Position Modulation (PPM) at 1 Mbps and are 112 bits long [15]. ADS-B messages are preceded by an 8-µs Mode-S preamble, which can be seen as the sequence of symbols: "11N00NNN", where "N" symbol stands for "no pulse". After it, the first 5 bits indicates the Mode-S downlink format, which for ADS-B is 17, "10001", or 18 "10010", depending on whether the ADS-B subsystem is a transponder-based one or not, respectively. The following 3 bits are equipment dependent, and the next 24 bits are used to identify the transmitter [16]. Then, 52 bits containing the ADS-B payload follow, and the message ends with 24 bits of parity.

In [17], Wesson analyzes the problem of securing ADS-B messages. It proposes the use of digital signatures over symmetric and asymmetric encryption. A signature length of 448 bits is required to achieve a security level equivalent to a 112-bit symmetric key (cryptographically secure until 2030). This signature is four times longer than the ADS-B message.

The proposal of this paper is based on the security framework proposed in [17], however it uses a complete different approach for the physical layer. Instead of using additional Mode-S ES messages to transmit the signature, which compromises on the maximum number of users on the data link, our proposal consists of embedding the 448-bit signature into a standard ADS-B message using Differential 16 Phase-Shift Keying (D16PSK) modulation. Thus, every pulse contains 4 bits of the digital signature, for a total of $112 \times 4 = 448$ bits. We propose the use of differential encoding in order to avoid the need of a carrier tracking loop in the receiver, which will exhibit difficulties in locking the preamble, as well as keeping track during the message due to the pulsed nature of ADS-B messages.

A. ADS-B Transmitting Subsystem

1) Digital Signature Insertion

For illustrative purposes, Fig. 1 represents an initial scheme of the block diagram of the digital signature insertion process proposed for Mode-S ES ADS-B. As it will be explained, that scheme does not meet the requirements stated in [15], [16] and needs some modifications. The upper branch generates a standard baseband ADS-B message (at 2 MSPS) based on a PPM modulator. The phase modulation used for the signature is generated in the lower branch. In order to account for the Mode-S preamble, the signature is zero-padded with 32 zeroes that will serve at the receiver as a phase reference. The zero-padded signature is then fed into a D16PSK Gray coder at 4 MSPS, so the symbol rate at the output matches that of the ADS-B message at 1 MSPS. Finally, the signature is interpolated by repeating samples ("nearest-neighbor" interpolation) in order to match the sampling rate of the PPM modulator's output (2 MSPS). Both outputs represent the phase and the amplitude of the secure ADS-B message, which are converted into a complex sequence. Since the signature is a complex sequence, the secure ADS-B message is complex as well. Therefore, an IQ modulator is required to perform the subsequent frequency up-conversion (not shown in Fig. 1).

2) RF Spectrum Mask

Since Mode-S messages must respect the spectrum mask defined in [15], it is important to study the effect of the digital signature in the spectrum of ADS-B messages. First of all, the bandwidth of the transmitter must be large enough to allow a pulse rise time lower than 0.1 µs [15]. However, phase transitions cannot be so fast in order to respect the spectrum

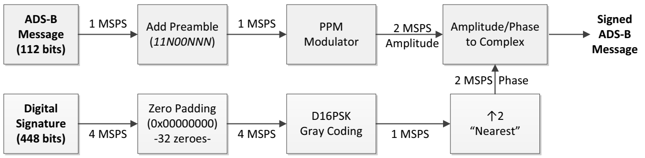

Fig. 1. Baseband generation of the secure ADS-B message. (Initial Scheme)

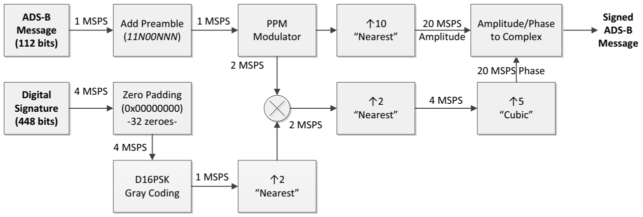

Fig. 2. Proposed baseband generation of the secure ADS-B message.

mask. Hence, the signature must be filtered prior to modulate the ADS-B message.

Fig. 2 shows the proposed modifications in order to achieve different transition times for the phase and the amplitude of the secure ADS-B message. Once the phase and the amplitude have been generated according to initial scheme proposed in Fig. 1, the amplitude is then interpolated ("nearest" method) up to 20 MSPS. This guarantees that the pulse rise time is less than one sample period, i.e., 0.05 µs. As regards the phase, it is first multiplied with the PPM signal, so that the phase returns to zero in the periods of absence of pulse. Then, it is interpolated up to 4 MSPS in order to achieve phase transitions of 0.25 µs. It has been observed through simulation that faster phase transitions produce messages whose spectrum does not respect the mask. Finally, in order to match the phase and the amplitude sampling rate, the phase sequence is smoothly interpolated through cubic interpolation up to 20 MSPS prior to the generation of the secure ADS-B message.

Fig. 3 shows the normalized spectrum (in dBc) of both the standard (unsigned) and signed ADS-B messages, along with the spectrum mask specified in [15]. These RF spectrums have been computed using the method described in Fig. 2, i.e. pulse rise/decay times of 0.05 µs, and phase transitions of 0.25 µs long. As it can be seen, the secure ADS-B message respects the spectrum mask. In addition, the peak at the carrier frequency has disappeared by effect of the phase modulation.

3) Pulse Amplitude Ripple

Instead of generating phase and amplitude independently, other option to respect the spectrum mask is to generate the signed message with abrupt phase transitions and use a filter afterwards in order to make the spectrum fit into the mask. The problem with using a filter and D16PSK modulation is that the amplitude falls down in the case of a symbol transition. . The effect that this may have on the receiver is unknown at this time, and could probably depends on the receiver implementation. However, it has been observed in simulations that the minimum bandwidth required in order to keep the amplitude above 90% for a merged pulse is 8 MHz.

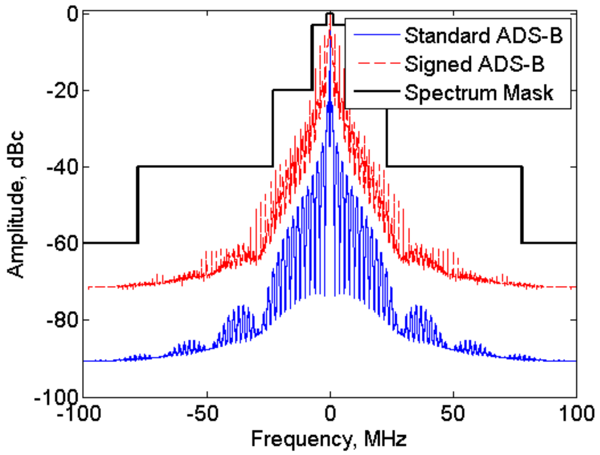

Fig. 3. Spectrum of the standard and signed ADS-B messages compared to the spectrum mask.

B. ADS-B Receiving Subsystem

For the ADS-B receiving device, it is proposed the architecture shown in Fig. 4. The outputs of the receiver are both the ADS-B message information and the digital signature. The digital signature is utilized to authenticate the message, which is not included in the figure.

1) ADS-B Message Extraction

This first part of the receiver consists of a standard ADS-B receiver. The incoming complex baseband equivalent signal is passed through an AM demodulator in order to extract the amplitude of the signal. This signal is compared with a threshold in order to detect the preamble, which can be carried out through a usual detector at the output of a correlator matched to the sequence "11N00NNN". Once the preamble is detected, the symbol synchronism can be determined. Note that Mode-S ES requires every pulse to start at multiple of 0.5 µs from the leading edge of the first transmitted pulse. The tolerance in this requirement for all transmitted pulses is ±0.05 µs [15]. Therefore, the starting point of the preamble defines the symbol synchronism with enough accuracy. When the symbol synchronism has been recovered, it is quite simple to implement a PPM demodulator using the amplitude of the signal as input. The binary sequence corresponding to the ADS-B message is obtained at its output.

2) Digital Signature Extraction

The extraction of the digital signature is a process a bit more complex. It is based on a differential D16PSK demodulator. This D16PSK process extracts the symbol by comparing the phase between two pulses corresponding to consecutive bits of the PPM message. Therefore, it requires the symbol synchronism as well as the sequence of the transmitted bits in order to determine on which half of the bit duration

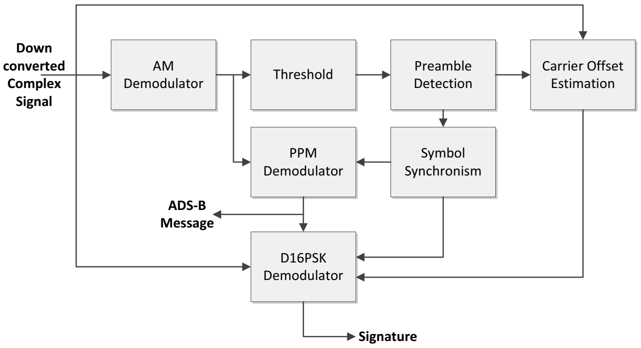

Fig. 4. Architecture proposed for the secure ADS-B receiver.

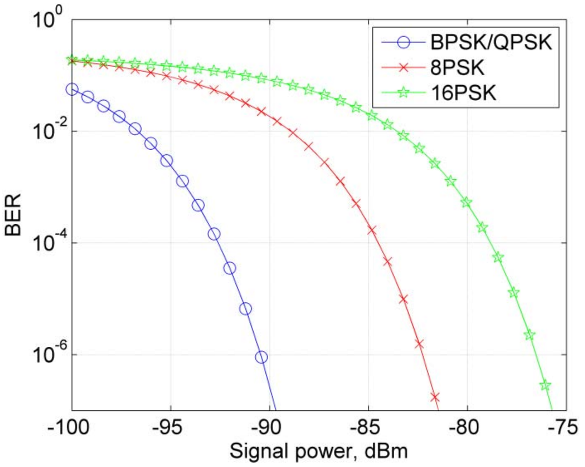

Fig. 5. BER as a function of the signal power at the receiver.

these two pulses are located.

Moreover, the D16PSK demodulator must account for the possible existence of a carrier offset. The standard allows an error up to ±1 MHz in the carrier frequency of the transmitter [15]. It means that the phase difference between pulses induced by the carrier offset becomes ambiguous after 1 µs. During the preamble, two pairs of pulses spaced by 1 µs are transmitted. In addition, the phase of all these pulses is the same, since no signature is transmitted during the preamble. As a result, the phase difference induced by a carrier offset can be determined from the phase received during the preamble. The value computed is used as input by the D16PSK demodulator so that the carrier offset can be compensated. This block also decodes the received symbols yielding the binary sequence of 448 bits corresponding to the digital signature.

III. Analysis and Discussion

A. BER and Maximum Range Analysis

The purpose of this section is to determine the most suitable PSK modulation for transmitting the digital signature. The error detection code of Mode-S ES has been designed so that the probability of a bit error being undetected is less than 10^{-7} as specified by [15]. This value will be used as targeted BER at the reception of the digital signature.

Let's assume a receiver noise figure of $F = 10$ dB, which is a pessimistic value. Considering a noise spectral density of $N_0 = -174$ dBm/Hz, Fig. 5 plots the theoretical BER achieved by different PSK modulations using Gray coding. These curves follow the expression:

$$BER = \frac{1}{2}\operatorname{erfc}\left(\sqrt{\frac{P_S T}{N_0 F}}\right) \tag{1}$$

For BPSK and QPSK modulation, where P_s is the signal power at the receiver, and $T = 0.5$ µs is the pulse duration. For higher order PSK modulation, the approximation for high SNR has been used:

$$BER = \frac{1}{k}\operatorname{erfc}\left(\sqrt{\frac{P_S T}{N_0 F}}\sin\left(\frac{\pi}{2^k}\right)\right) \tag{2}$$

where k is the number of bits per symbol.

As expected, the higher the order, the higher the BER. These are well known curves, so no further discussion is needed. It is now useful to convert the sensitivity values at $BER = 10^{-7}$ into maximum range for a received signal power above the sensitivity level, which is shown in Table I.

The values in the table are neither too optimistic nor too pessimistic, and they should be used just as approximate values. On the one hand, only free-space path loss is considered (optimistic), and a joint TX/RX antenna gain of 8 dB (neutral) has been used in the computations. On the other hand, in addition to the pessimistic noise figure, the transmitted power values shown correspond to the minimum power requirements in [16] (pessimistic), which depend on the ADS-B equipment capabilities. It is probable that most of the equipment will exceed these values in practice.

The intended maximum range according to the desired capabilities [18] also depends on the equipment capabilities. Table I gathers in the last rows the intended range for the most stringent ones, Class A3 and A3+, whose receiver sensitivities are -81.0 dBm and -83.5 dBm, respectively [16]. Note that 16PSK modulation cannot meet the maximum range requirements for Class A3+ in all cases (boldface in Table I). However, Class A3+ ADS-B receivers are expected to be high-end, and the desired maximum range would be reached by decreasing the receiver's noise figure by 2.5 dB, from 10 dB to 7.5 dB which is technically easily achievable. Therefore, the proposal to use 16PSK modulation with the digital signature is fully valid.

B. Protection Against Message-Replay Attack

By introducing the proposed digital signature, the secured ADS-B system can be protected against HMI introduced through 1) spoofing, as long as the private key remains secret; 2) message manipulation, since the signature authenticates both the message and its origin; and 3) message injection, as illegitimate users lack their own recognized private key. However, there is still a HMI threat that cannot be neutralized: message replay.

Our proposal against message replay consists of time stamping and setting a temporal validity for every message. Currently, ADS-B transmitting equipment can be synchronized

TABLE I. Maximum Range Analysis

Modulation	Sensitivity	Maximum Range		
		70W	***125W***	***200W***
BPSK/QPSK	−88.7 dBm	213NM	285NM	361NM
8PSK	−82.8 dBm	108NM	145NM	183NM
16PSK	**−76.8 dBm**	**54NM**	**73NM**	**92NM**
Class A3	−81.0 dBm	34NM	64NM	90NM
Class A3+	−83.5 dBm	35NM	**85NM**	**120NM**

or not to UTC (Coordinated Universal Time) by means of the time mark pulse provided by the onboard GNSS receiver. This capability is indicated within the "TIME" subfield (1-bit) in ADS-B position messages. However, there is no message field allocated for timestamp information, and even for UTC synchronized ADS-B systems, the receiver infers the time of applicability of the message from the time at which it is received.

The "CPR Format" subfield, which indicates if the ADS-B message is "even" or "odd", can be used to some extent to discriminate replayed messages. However, this becomes ineffective against messages replayed with a delay greater than 200 ms, as the receiver will expect again a message with the same CPR Format. Long delays are indeed the ones yielding the most dangerous HMI. Thus, it is proposed to generate a signature from the pair message-timestamp, where the timestamp is the time of applicability of the information transmitted within the ADS-B message. This time of applicability is an exact 0.2 s sub-epoch for UTC synchronized equipment, or the estimated UTC time of transmission for non-synchronized ones. This timestamp (time of applicability) must be computed in both ADS-B transmitting and receiving equipment [16]. Because there are no bits available to transmit the timestamp, this will not be transmitted. On the contrary, the transmitting equipment signs the pair message-timestamp, but only the message is transmitted along with the signature. On the receiver's end, the signature is validated against the same pair message-timestamp.

In order to avoid an authentication failure due to a mismatch between the time of applicability computed at the transmitter and the receiver, it is important to study the range of this difference. We will focus on the case of UTC non-synchronized ADS-B transmitting equipment, as it leads to the greatest variability. Fig. 6 defines the different delays involved from the time at which a measurement is made (T_m) until the time at which the message is time stamped at the ADS-B receiver's end.

δ_{GNSS} is the latency of the GNSS receiver in reporting the transmitted information, which is in the range [0, 0.5] s [18]. δ_{DB} is the delay in the data bus from the ADS-B information source to the ADS-B transmitting device, typically negligible [16], but bounded to 0.2 s for delay computations [18]. δ_{Out} is the latency of the ADS-B transmitting device, i.e. the delay in transmitting the message once the information is available at its input. The transmitting device is required to compensate its own latency with an error ε_{Out} bounded to ±0.1 s. When setting the timestamp, the ADS-B transmitting device knows the time of measurement T_m (as reported), estimates its own delay ($\delta_{Out} + \varepsilon_{Out}$), but it cannot compensate for the unknown values of δ_{GNSS} or δ_{DB}. As a result, the timestamp on the transmitter's side is

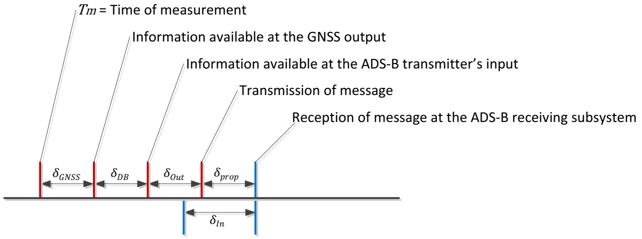
Tm = Time of measurement
Information available at the GNSS output
Information available at the ADS-B transmitter's input
Transmission of message
Reception of message at the ADS-B receiving subsystem
δ_{GNSS}
δ_{DB}
δ_{Out}
δ_{prop}
δ_{In}

Fig. 6. Different delays involved in the time stamping processes.

$$\mathrm{TS}_{Out} = T_m + \delta_{Out} + \varepsilon_{Out} \tag{3}$$

On the receiver's side, the timestamp becomes:

$$\mathrm{TS}_{In} = T_m + \delta_{GNSS} + \delta_{DB} + \delta_{Out} + \delta_{prop} - \delta_{In} \tag{4}$$

where δ_{prop} is the propagation delay across the RF medium, which results into 1.2 ms for a maximum distance between the transmitter and the receiver of 200NM. Therefore, δ_{prop} can be ignored. δ_{In} is the delay between the time reference and the ADS-B receiving device. Using the same considerations as for the transmitter ($\delta_{GNSS} + \delta_{DB}$), this delay will be within the range [0, 0.7] s.

The difference between the timestamps generated by the transmitting and receiving devices becomes:

$$\Delta_{TS} = \mathrm{TS}_{In} - \mathrm{TS}_{Out} \tag{5}$$

$$\Delta_{TS} = \varepsilon_{clock} + \delta_{GNSS} + \delta_{DB} - \varepsilon_{Out} + \delta_{prop} - \delta_{In} \tag{6}$$

where ε_{clock} stands for the clock (UTC reference) error between transmitter and receiver. This error can be ignored as the typical accuracy achieved by a GNSS-based timing reference is within the range ±1 μs [18].

For the ranges provided above, it can be seen that the uncertainty in the timestamp is $\Delta_{TS} \in [-0.8, 0.8]$ s. Thus, the proposed solution is to use a time resolution of 2 s for the timestamps. Then, at the receiver, the signature is validated against all the possible timestamps within the limits: $\mathrm{TS}_{In} \pm$ 0.8 s. The proposed method guarantees that a message-replay attack will only be authenticated at the receiver for few seconds (up to 2.8 s) after the legitimate message is sent. Therefore, the hazard caused through this kind of attack is very limited.

IV. Conclusion

Amongst the wide variety of solutions to prevent HMI injection in ADS-B system, multilateration and the use of digital signatures are the most promising ones. Multilateration has the advantage of being independent from the transmitting device, but also the disadvantage of requiring highly precise time synchronization between at least four receiving participants. On the contrary, digital signatures can be verified by a single participant, but there is an increased complexity emanating from the management of keys.

This work describes a solution, at the physical layer, for the use of digital signatures on the Mode-S ES data link, which could also be applied for UAT version. The solution is based on embedding the signature into the ADS-B message by using D16PSK modulation. It allows the use of signatures up to 448-bits long, which are supposed to be safe until 2030. Moreover, and what is more important, the resulting ADS-B messages are compliant with current standards, in terms of pulse shape and spectrum mask. As a result, current ADS-B receiving devices shall be able to decode messages from the new secure ADS-B system thus enabling a seamless transition. But only new secure devices will be able to authenticate the origin of the message.

This paper has described one possible architecture for both the secure ADS-B transmitting and receiving devices. For the transmitting device, special care must be taken to generate short pulse rise times and smoother phase transitions, in order to respect the spectrum mask. On the receiver side, it is important to take into account the carrier frequency offset, which can be compensated during the message preamble.

16PSK modulation has been selected because it achieves the desired performance within the desired range of coverage. However, other lower order PSK modulations can be used as well, with increased robustness and coverage range. The cost is that the whole signature cannot be authenticated from a single ADS-B message, as it would not fit in one message, but several messages would be required in order to receive the entire signature.

Finally, as regards the use of timestamps during the signing process, it has been shown that an appropriate resolution for the timestamp is 2 s. This value is obtained by rounding up the maximum difference between the estimated transmission and reception times. The use of timestamps protects the ADS-B system against messages replayed more than 2.8 s after the legitimate massage was sent. Further analysis is required to determine if this vulnerable time interval is short enough, depending on the air-traffic dynamics and the fact that the ADS-B system is designed for an uncertainty in the time of applicability of the information up to 1.6 s.

REFERENCES

[1] Next Generation Air Transportation System (NextGen), Federal Aviation Administration, [online] 2015, http://www.faa.gov/nextgen/, (Accessed: April 10, 2015)

[2] SESAR, Parterning for smarter avitation, Single European Sky ATM Research Joint Undertaking (SESAR JU), [online] 2015, http://www.sesarju.eu/, (Accessed: April 10, 2015)

[3] ICAO Asia and Pacific Office, "Report of The ADS-B Seminar and Thirteenth Meeting of Automatic Dependent Surveillance – Broadcast (ADS-B) Study and Implementation Task Force (ADS-B SITF/13)," *Agenda Item 7*. Hong Kong, China, Apr-2014.

[4] Federal Aviation Administration, "ADS-B Benefits Are Limited Due to a Lack of Advanced Capabilities and Delays in User Equipage," *Report Number: AV-2014-105*. 11-Sep-2014.

[5] A. Costin and A. Francillon, "Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," in *BLACKHAT 2012*, 2012.

[6] K. Sampigethaya, R. Poovendran, and L. Bushnell, "Assessment and mitigation of cyber exploits in future aircraft surveillance," in *IEEE Aerospace Conference Proceedings*, 2010, pp. 1–10.

[7] K. Sampigethaya, R. Poovendran, and L. Bushnell, "A Framework for Securing Future eEnabled Airplane Navigation and Surveillance," in *AIAA Infotech@Aerospace Conference*, 2009.

[8] S.-H. Lee, Y.-K. Kim, J.-W. Han, and D.-G. Lee, "Protection Method for Data Communication between ADS-B Sensor and Next-Generation Air Traffic Control Systems," *Information*, vol. 5, no. 4, pp. 622–633, Dec. 2014.

[9] S. Amin, T. Clark, R. Offutt, and K. Serenko, "Design of a cyber security framework for ADS-B based surveillance systems," in *2014 IEEE Systems and Information Engineering Design Symposium, SIEDS 2014*, 2014, pp. 304–309.

[10] S. H. Lee, J. W. Han, and D. G. Lee, "The ADS-B protection method for next-generation air traffic management system," in *Ubiquitous Computing Application and Wireless Sensor*, vol. 331, J. J. Park, Y. Pan, H.-C. Chao, and G. Yi, Eds. Dordrecht: Springer Netherlands, 2015, pp. 105–113.

[11] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ADS-B Research," in *2006 IEEE Aerospace Conference*, pp. 1–7.

[12] J. Baek, Y.-J. Byon, E. Hableel, and M. Al-Qutayri, "An Authentication Framework for Automatic Dependent Surveillance-Broadcast Based on Online/Offline Identity-Based Signature," in *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 2013, pp. 358–363.

[13] R. Chen, C. Si, H. Yang, and X. Zhang, "ADS-B Data Authentication Based on AH Protocol," in *2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing*, 2013, pp. 21–24.

[14] W.-J. Pan, Z.-L. Feng, and Y. Wang, "ADS-B Data Authentication Based on ECC and X . 509 Certificate," *J. Elecdtronic Sci. Technol.*, vol. 10, no. 1, pp. 51–55, 2012.

[15] RTCA Special Committee 209, "Minimum Operational Performance Standards for Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/Mode S) Airborne Equipment," *RTCA/DO-181E*. 2011.

[16] RTCA Special Committee 186, "Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B)," *RTCA/DO-260B*. 2009.

[17] K. D. Wesson, "Secure Navigation and Timing Without Local Storage of Secret Keys," The University of Texas at Austin, 2014.

[18] RTCA Special Committee 186, "Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B)," *RTCA/DO-242A*. 2002.