Titre: Title:	CABBA: Compatible Authenticated Bandwidth-efficient Broadcast protocol for ADS-B
Auteurs: Authors:	Mikaela Stéphanie Ngamboe Mvogo, Xiao Niu, Benoit Joly, Steven P. Biegler, Paul Berthier, Rémi Benito, Greg Rice, Jose Manuel Fernandez, & Gabriela Nicolescu
Date:	2025
Type:	Article de revue / Article
Référence: Citation:	Ngamboe Mvogo, M. S., Niu, X., Joly, B., Biegler, S. P., Berthier, P., Benito, R., Rice, G., Fernandez, J. M., & Nicolescu, G. (2025). CABBA: Compatible Authenticated Bandwidth-efficient Broadcast protocol for ADS-B. International Journal of Critical Infrastructure Protection, 48, 100728 (17 pages). https://doi.org/10.1016/j.ijcip.2024.100728

Titre de la revue: Journal Title:	International Journal of Critical Infrastructure Protection (vol. 48)
Maison d'édition: Publisher:	Elsevier
URL officiel: Official URL:	https://doi.org/10.1016/j.ijcip.2024.100728
Mention légale: Legal notice:	©2024 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by- nc-nd/4.0/).

international journal of critical infrastructure protection 48 (2025) 100728

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

CABBA: Compatible Authenticated Bandwidth-efficient Broadcast protocol for ADS-B

Mikaëla Ngamboé [a,*], Xiao Niu [a], Benoit Joly [b], Steven P. Biegler [b], Paul Berthier [d], Rémi Benito [c], Greg Rice [b], José M. Fernandez [a], Gabriela Nicolescu [a]

[a] Department of Computer and Software Engineering, Polytechnique Montréal Technological University, Montréal, Québec, Canada
[b] Collins Aerospace, Cedar Rapids, IA, United States
[c] Bombardier, Montréal, Québec, Canada
[d] Rhea Group, Montréal, Québec, Canada

ARTICLE INFO

Keywords:
ADS-B
Security
Authentication
Backward compatibility
Bandwidth efficiency
TESLA
PKI

ABSTRACT

The Automatic Dependent Surveillance-Broadcast (ADS-B) is a surveillance technology mandated in many airspaces. It improves safety, increases efficiency and reduces air traffic congestion by broadcasting aircraft navigation data. Yet, ADS-B is vulnerable to spoofing attacks as it lacks mechanisms to ensure the integrity and authenticity of the data being supplied. None of the existing cryptographic solutions fully meet the backward compatibility and bandwidth preservation requirements of the standard. Hence, we propose the Compatible Authenticated Bandwidth-efficient Broadcast protocol for ADS-B (CABBA), an improved approach that integrates TESLA, phase-overlay modulation techniques and certificate-based PKI. As a result, entity authentication, data origin authentication, and data integrity are the security services that CABBA offers. To assess compliance with the standard, we designed an SDR-based implementation of CABBA and performed backward compatibility tests on commercial and general aviation (GA) ADS-B in receivers. Besides, we calculated the 1090ES band's activity factor and analyzed the channel occupancy rate according to ITU-R SM.2256-1 recommendation. Also, we performed a bit error rate analysis of CABBA messages. The results suggest that CABBA is backward compatible, does not incur significant communication overhead, and has an error rate that is acceptable for Eb/No values above 14 dB.

1. Introduction

Automatic Dependent Surveillance-Broadcast (ADS-B) is an aircraft surveillance technology [1] that allows aircraft to broadcast information about their identification, position, speed, and other data acquired from onboard sensors [2–4]. It supports many airborne and ground safety applications [5]. For example, Air Traffic Control (ATC) can use ADS-B information as an alternate means of surveillance, complementary to radar, to improve efficiency of controlled airspace [6,7]. Furthermore, ADS-B provides an alternate source of information to allow airborne aircraft to maintain traffic separation.

ADS-B was originally designed in the early 2000s to replace radars as part of the United States Federal Aviation Administration (FAA) NextGen initiative [8]. It has since been adopted worldwide. Indeed, there are three certified ADS-B data links: the Universal Access Transceiver (UAT), which operates only in the United States at the 978 MHz frequency and uses 420-bit messages (272 bits for the payload); the 1090 MHz Extended Squitter (1090ES), an internationally adopted link with 112-bit messages (56 bits for the payload); and the VHF Digital Link (VDL) MODE 4, which operates in the 108-136 975 MHz range with a message structure similar to that of the 1090ES, is most adopted in Northern Europe but is also rarely used due to the requirement for equipment upgrades [9].

Unfortunately, the ADS-B was conceived without any communication security mechanisms [10,11], which represents a significant threat to aviation safety. Indeed, by using low-cost equipment such as a Software Defined Radio (SDR), attackers could easily transmit false ADS-B messages [10–12] to create a confused and false picture of traffic for controllers and pilots. This can potentially lead to flight delays, separation conflicts between aircraft or unnecessary maneuvers by pilots. In addition, spoofed ADS-B messages received and processed

* Corresponding author.
E-mail addresses: mikaela-stephanie-2.ngamboe-mvogo@polymtl.ca (M. Ngamboé), xiao.niu@polymtl.ca (X. Niu), Benoit.Joly@collins.com (B. Joly), Steven.Biegler@collins.com (S.P. Biegler), p.berthier@rheagroup.com (P. Berthier), Remi.Benito@aero.bombardier.com (R. Benito), greg.rice@collins.com (G. Rice), jose.fernandez@polymtl.ca (J.M. Fernandez), Gabriela.nicolescu@polymtl.ca (G. Nicolescu).

https://doi.org/10.1016/j.ijcip.2024.100728
Received 6 June 2024; Received in revised form 20 November 2024; Accepted 26 November 2024
Available online 7 December 2024

by Traffic Collision and Avoidance Systems (TCAS) in the cockpit could affect the decision-making ability of air crews [13]. Therefore, the use of ADS-B in ATC and traffic avoidance can represent a security risk.

Based on the foregoing, it is necessary to secure ADS-B. In particular, to prevent spoofing attacks, there must be a method to ensure *identity authentication* of the senders and *message authentication* of transmitted ADS-B messages. This is achieved through the simultaneous fulfillment of these three security goals:

1. *Data integrity*, is the assurance that data has not been altered in an unauthorized manner.
2. *Entity authentication*, also known as *Identity Authentication*, is the assurance of the identity of a given entity interacting with a system.
3. *Data origin authentication*, also known as *Message Authentication*, is the assurance that a given entity was the original source of received data.

Furthermore, any solution to secure ADS-B must adhere to the operational requirements delineated in the Minimum Operational Performance Standard (MOPS) for the 1090 MHz frequency [3], which serves as the primary channel for ADS-B communications. Specifically, the solution must be backward compatible with current receivers, ensuring their ability to accurately receive, interpret, and display position information for nearby traffic. Additionally, the solution is mandated to minimize the utilization of the congested 1090ES, which is extensively utilized by Secondary Surveillance Radar (SSR) and Extended Squitter (Mode S) transmitters, such as radar, multi-lateration, and airborne TCAS [6,7].

Several cryptographic solutions have been proposed to secure ADS-B. None of them appear to meet all the security goals and operational requirements listed above. Therefore, we consider that the question of how to secure ADS-B while meeting security and operational constraints is still open.

To that effect, in this paper, we introduce a solution called Compatible Authenticated Bandwidth-efficient Broadcast protocol for ADS-B (CABBA). CABBA integrates the Time Efficient Stream Loss-tolerant Authentication (TESLA) mechanism [14,15] with phase overlay modulation techniques and a Public Key Infrastructure (PKI). By leveraging TESLA and PKI, CABBA fulfills all the security objectives specified earlier to prevent ADS-B spoofing attacks. This includes data integrity, data origin authentication, and identity authentication. Furthermore, by integrating the phase overlay modulation in CABBA's physical layer, we aim to align our solution with the operational requirements outlined by the MOPS.

Given the consequences of a potential attack exploiting the ADS-B vulnerability, one would hope that ADS-B be replaced as quickly as possible by a secure alternative. Unfortunately, such a one-to-one replacement will be lengthy and difficult in the context of aviation. First, it will likely take several years for an accepted standard to be drawn, discussed, approved, and then made mandatory by civil aviation authorities—at least 5 to 10 years. Second, considering the long lifetime of aircraft and their avionics, it is very likely that CABBA-capable and ADS-B legacy avionics would have to co-exist and use the same communication channels during the long transition period from initial deployment to full worldwide adoption. While it is paramount that CABBA-capable receivers be able to authenticate messages from CABBA-capable transmitters, it is equally important in terms of aviation safety that in the transition period both CABBA-capable and legacy ADS-B receivers be able to receive and interpret ADS-B messages from legacy ADS-B transmitters.

In light of these operational requirements, the two most important questions regarding any secure ADS-B solution, in particular CABBA, that needs to be answered are:

1. Could CABBA be gradually deployed while ensuring that legacy ADS-B equipment continues to operate?
2. What would be the viability of deploying CABBA in terms of communication channel saturation?

To evaluate the backward compatibility of CABBA, we have constructed an SDR-based implementation. We have used this implementation to test backward compatibility with two different suites of commercial-off-the-shelf (COTS) ADS-B In solutions: One is used in General Aviation (GA), and the other is used in business jets and airline transport aircraft. We also used this lab implementation of CABBA to test and analyze its bit error rate (BER). A channel occupancy rate (COR) analysis was also undertaken to quantify the channel occupancy overhead of CABBA in a likely real-world scenario. Besides, a safety impact assessment of unauthenticated messages was conducted to evaluate the effect of CABBA on the situational awareness of pilots and air traffic controllers.

Considering the above discussion, the contributions of this work can be summarized as follows:

1. We introduce CABBA, a secure variant of ADS-B technology that is bandwidth-efficient, backward compatible, and offers an adequate level of security by providing simultaneously two security services: aircraft identity authentication and ADS-B message authentication.
2. We use the D8PSK phase overlaid modulation technique, as defined in the MOPS, to support the transmission of additional security information required by CABBA while preserving bandwidth usage. To the best of our knowledge, this is the first proposal to use the phase overlay technique as specified in the MOPS.
3. We performed tests on a commercial aviation avionics suite and with a general aviation ADS-B in receiver to check whether our solution would be backward compatible with legacy equipment.
4. We carried out a channel occupancy analysis to verify the operational viability of our solution, in terms of channel occupancy.
5. We conducted a safety impact of unauthenticated messages to assess their effects on the situational awareness of pilots and controllers.
6. We provide a detailed specification of the CABBA protocol, including the structure of the different packet types (in-phase and quadrature), the authentication mechanism and the decision logic used to discriminate between genuine and false packets. This specification is sufficiently detailed to allow anyone to implement the CABBA solution, and serve as the basis for subsequent standardization and adoption by the aviation industry.

The remainder of the paper is structured as follows. Section 2 reviews prior works on cryptographic approaches for securing ADS-B. Section 3 outlines the operational details of the TESLA protocol. Section 4 describes how phase overlay modulation techniques can be applied to ADS-B to increase data throughput while keeping the channel activity rate constant. Section 5 introduces CABBA, a cryptographic approach for securing ADS-B that integrates the TESLA authentication protocol with phase overlay modulation techniques. Section 6 details the experimental procedures used to assess CABBA backward compatibility and Section 7 the methodology for evaluating bit error, channel occupancy, and uncertainty delays. We conclude in Section 8 with a summary of our findings, describing their consequences in terms of possible real-world deployment of CABBA and highlight necessary future work in this direction.

2. Overview of cryptographic solutions for ADS-B

In this section, we review previous works and characterize the security goals and operational performance requirements they did not meet. We group these works into three categories, they use symmetric, asymmetric, and hybrid cryptography (see Table 1).

Table 1
An overview of cryptographic techniques for enhancing ADS-B security. The approaches are categorized into three groups based on their use of symmetric, asymmetric, or hybrid cryptography.

	Cryptographic primitive	Security goals			Operational performances	
		Origin Auth	Integrity	Entity Auth	Backward compatibility	Bandwidth preservation
Symmetric	Encryption [16–20]	✗	✗	✗	✗	✓
	MAC [21,22]	✗	✗	✗	✓	✗
Asymmetric	Digital signature using certificate-based PKI [10,23,24]	✓	✓	✓	✓	✗
	Digital signature using Identity-based PKI [25–30]	✗	✗	✗	✓	✗
	Digital signature using certificateless PKI [31–34]	✓	✓	✗	✓	✗
Hybrid	Encryption using TESLA with Certificate-based PKI [35]	✓	✓	✓	✗	✗
	MAC or Digital signature using TESLA with certificate-based PKI [36,37]	✓	✓	✓	✓	✗
	MAC using TESLA with certificate-based PKI and phase overlay techniques (this paper)	✓	✓	✓	✓	✓

2.1. Symmetric cryptography-based protocols

The studies that use symmetric cryptography to secure the ADS-B rely on cryptographic primitives such as encryption or message authentication code.

Format-preserving encryption, or FPE, involves encrypting data in a manner such that the resulting *ciphertext* preserves the format of the original *plaintext* [38]. Some studies employ this approach because it aligns with the technological requirements of the ADS-B standard in preserving the bandwidth of the 1090ES channel [16–20]. However, encryption schemes fall short of meeting the backward compatibility criteria of the ADS-B standard, primarily because navigation data are not transmitted in *plaintext*. To overcome that limitation, it has been suggested to use instead message authentication codes or MAC [21,22]. For the MAC approach to be effective, there must be symmetric trust assurance between the communicating parties. However, it is challenging to achieve in open communications such as that of the ADS-B because it is often impossible to manage and master the parties involved in the broadcast. In such a scenario, knowing that when employing symmetric cryptography every receiver must know the symmetric key, a malicious actor can impersonate a sender and forge messages to other receivers.

To ensure authenticated broadcast, ADS-B requires an asymmetric process enabling every receiver to ascertain the genuineness of received messages, devoid of the ability to produce genuine messages from received ones [39]. Asymmetric cryptography, particularly digital signature, is the standard technique to achieve this [40].

2.2. Asymmetric cryptography-based protocols

In *asymmetric or public-key cryptography*, a pair of keys (public and private) is used for encryption and digital signatures. The *private key* is kept secret, while the *public key* is shared for secure communication. To guarantee authenticity, the public key must be confirmed by a certification authority (CA) through a public key certificate that links the key to an entity [41]. The system responsible for issuing, maintaining, and revoking certificates is known as a PKI [42–44]. For ADS-B, the literature proposes three types of PKI to manage aircraft certificates: certificate-based, identity-based, and certificateless.

Among the certificate-based PKI solutions proposed to secure ADS-B is an authentication scheme that relies on Elliptic Curve Digital Signature Algorithm (ECDSA) signatures and X.509 certificates [23]. Although this solution might fulfill the demands of the ADS-B protocol regarding security, it fails to meet the standard's technological performance criteria. In addition, the authors leave open the issue of certificate distribution and do not address that of certificate revocation. To address the weaknesses of [23], a lightweight PKI solution is recommended in [10], where the ADS-B message is signed, and its signature is partitioned across N messages. It is suggested that keys distribution occurs during the routine maintenance of the aircraft. Furthermore, still to address the limitations of [23], a dual path PKI solution that aims to handle the certificate revocation problem by using session certificates is proposed in [24]. According to this scheme, an aircraft should have certificates from both their home country's National Aviation Authority (NAA) and the local ATC center where they are currently located. Thus, the dual certification is evidence that the aircraft has been granted permission to fly, as well as validated as a safe and current entity within the local center from which it is flying. We argue that the adoption of the PKI proposed in [24] will raise the operational expenses of the ADS-B system and render its use cumbersome, especially for international flights. In general terms, using certificate-based PKI for ADS-B security has two limitations. First, it significantly increases communication costs, conflicting with the bandwidth preservation criteria of the ADS-B standard, proof of which is that none of the above-mentioned solutions [10,23,24] meet this need. Second, establishing and operating a PKI for these solutions is impractical in the current state of global coordination among ICAO and NAAs.

Identity (ID)-based PKI attempts to eliminate the key distribution problem of certificate-based PKI. In ID-based PKI, public keys are derived from easily identifiable user attributes, such as email addresses, eliminating the need for traditional certificates and the complex infrastructure that supports them [45]. This is achieved through a central entity called a private key generator (PKG), tasked with computing each user's private key based on their corresponding public key [45,46]. Several studies have used the ID-based authentication approach to secure ADS-B communications. For instance, a scheme that signs ADS-B messages in two stages, online and offline, has been developed to increase the efficiency of the signature generation process [25]. Furthermore, a broadcast authentication technique incorporating batch verification of digital signatures[1] has been proposed to reduce the time and computational expense involved in the signature verification process for ADS-B messages [26]. Subsequently, a broadcast authentication protocol that relies on ID-based signature and enables message

[1] Batch verification allows to simultaneously verify multiple digital signatures, whether they were produced by one signer or several.

recovery has been designed [27]. Aware that working with a single PKG in large-scale endeavors is not viable [47], the authors of the contribution [28] took inspiration from the hierarchical ID-based cryptosystems[2] presented in [47,48] and implemented an authentication framework that relies on hierarchical ID-based signature (HIBS) and performs signature batch verification. However, the need for intricate hash-to-point operations during signature and verification processes renders the scheme [28] non-lightweight, reducing its deployability. To overcome this limitation, a three-level hierarchical ID-based signature scheme (TLHIBS) that relies solely on general hash functions has been introduced in [29]. Despite this effort, the issue of computational overhead persisted. In response, an alternative scheme that avoids employing any intricate bilinear pairing operations over elliptic curves has been implemented in [30]. This approach slightly reduces the computational overhead when compared to the previous works [25–29]. Besides, all these solutions have two additional drawbacks. First, they increase communication overhead, violating ADS-B bandwidth requirements for the 1090ES channel, which makes them unimplementable. Second, they are vulnerable to key escrow, a privacy issue in ID-based cryptosystems, allowing an untrustworthy PKG to decrypt messages and forge signatures by accessing users' secret keys [33]. This vulnerability raises substantial concerns about the overall security of these proposed solutions.

Certificateless PKI eliminates the key escrow problem by splitting the private key generation process between the PKG and the user. The PKG generates a portion of the private key, while the user creates a random value for the remaining portion, which is kept confidential. This approach has been used to implement ADS-B messages authentication schemes that rely on certificateless short signatures [31,32]. These schemes were subsequently enhanced by integrating privacy-preserving and aggregate signature methods to ensure sender anonymity and reduce the computational cost of signature verification [33,34]. The concept of certificateless short signature is new, and while it appears promising, it is not yet mature enough to be adopted. Indeed, a significant challenge in certificateless cryptography lies in the establishment of security schemes that can ensure a satisfactory level of protection against attackers attempting to manipulate users into employing counterfeit public keys. This difficulty arises from the absence of digital certificates to unequivocally verify the authenticity of a public key [49].

2.3. Hybrid cryptography-based protocols

So far, we have seen that there are two approaches to secure ADS-B while adhering to the standard's backward compatibility criteria. Through MACs using symmetric cryptography or through digital signatures using asymmetric cryptography, notably that based on certificate-based PKI. The digital signature approach is secure, however, the generated signatures are too long, which causes problems if we consider the requirement of preserving the 1090ES's bandwidth. On the other hand, the MAC approach allows generating short signatures, nevertheless, it is not secure since symmetric trust cannot be ensured between communicating parties. As a result, some authors have proposed using hybrid cryptography, particularly the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol [15]. Details of how TESLA operates can be found in Section 3.

Security in the Air using TESLA or SAT, is an authentication protocol that adapts TESLA to the requirements of ADS-B [36]. It replaces TESLA's synchronization protocol with onboard GPS clock time and employs certificate-based PKI for aircraft and message authentication. SAT, tested on `gr-air-modes`, shows potential backward compatibility with existing ADS-B receivers. However, it has two limitations. Firstly, it increases bandwidth usage by requiring three types of packets for message authentication. For simplicity of explanation, we refer to them as Type A, B and C packets. Standard 112-bit ADS-B packets are replaced with Type A packets that include a 16-bit MAC code and 8-bit sequence number, increasing to 136 bits (a 14% increase). Type B packets, containing TESLA authentication keys, are 184 bits long, and Type C packets containing aircraft certificates are 1520 bits long. Let Δ_B be the time between transmission of Type B packets (originally set to 5 s), and Δ_C be the time between transmission of certificate packets (originally set to 30 s). Assuming a mean transmission rate $\bar{f}_A$ of 6.2 ADS-B messages per second per aircraft, the use of SAT results in an additional transmission overhead per aircraft per minute given by:

$$O_{\min} = (\bar{f}_A \cdot 60 \cdot 24) + \left(\frac{60}{\Delta_B} \cdot 184\right) + \left(\frac{60}{\Delta_C} \cdot 1520\right) = 14752. \quad (1)$$

This results in a total overhead of 245.8 bps over the normal bit rate of 694.4 bps for standard ADS-B message transmission, a total 35% increase in bandwidth usage. The second limitation is related to security. To limit bandwidth usage, the authors of SAT limited the size of the MAC to 16 bits. Truncating the MAC like this is a standard described and accepted by FIPS standard 198-1 [50] and described in FIPS Standard Publication 800-107 [51]. In this case, the residual attack risk is two-fold:

1. The attacker is lucky and guesses the right MAC for a spoofed message he desires to send. This will happen with probability 2^{-16}.
2. The attacker floods the channel with spoofed messages with all MAC possibilities, i.e. he sends $65536 = 2^{16}$ messages hoping that the ADS-B receivers ignore the ones with a wrong MAC and process and accept the one with the correct.

In an ideal scenario where bandwidth is not constrained, we believe a larger MAC size would provide better security, ideally with a minimum of 32 bits, forcing the attacker to be extremely lucky or have to send an astronomical number of messages (over 4 billion messages) for his attack to be successful.

Securing Open Skies or SOS, is a solution that integrates TESLA with a mechanism for collectively verifying all messages transmitted by an aircraft within a specified timeframe [37]. Unlike the SAT method, which authenticates messages individually using MAC, SOS opts for batch authentication through digital signatures. This strategy is designed to effectively tackle the bandwidth consumption limitations of SAT and the broader challenge of bandwidth constraints in the 1090ES band. However, although transmitting one digest per message pool takes less bandwidth, the SOS technique can be troublesome in some instances. In the case of message injection, for example, the receivers must get the set of genuine messages. The authors propose a community server-based majority voting filtering stage. To identify the correct message sequence, servers try various message combinations as well as hash operations and comparisons. We argue that if an attacker injects false messages at a high rate, it will result in computation and a time-consuming task. Furthermore, should any of the ground receivers fail to receive a single packet, all packets delivered during that interval cannot be validated, posing a serious safety issue.

The solution presented in [35], combines Format-preserving, Feistel-based encryption, and TESLA to ensure the confidentiality and integrity of ADS-B messages. However, due to the lengthy security parameters required in their authentication technique, their solution necessitates the transmission of five ADS-B messages for every navigation data sent by an aircraft. This results in significant bandwidth consumption, thereby failing to meet the bandwidth preservation requirement outlined in the standard. Additionally, their proposed encryption of the ICAO code contradicts backward compatibility criteria. Consequently, this solution fails to comply with any of the operational requirements specified in the MOPS for ADS-B.

[2] In a hierarchical ID-based cryptosystem, multiple PKGs create a tree-like structure [47,48]. The primary PKG generates private keys for its subordinates, who, in turn, produce private keys for PKGs beneath them [47,48]. PKGs at the edges generate private keys for users [47,48].

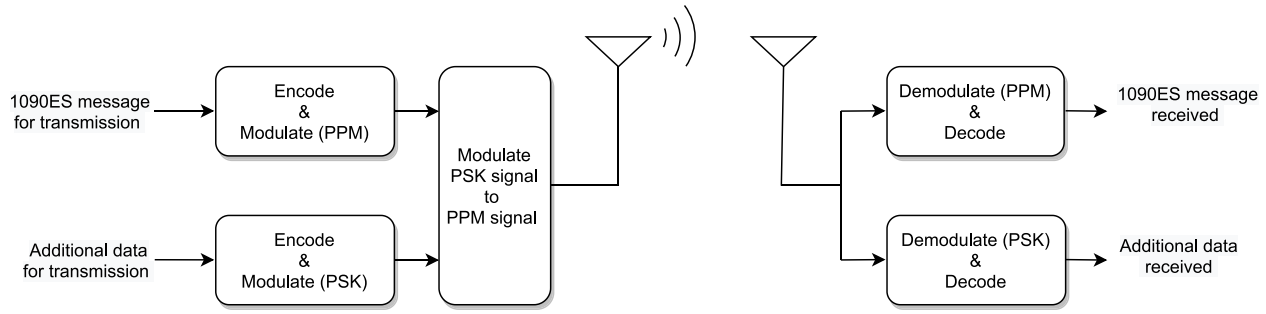


Fig. 1. Block diagram for the use of phase overlay method to add more data to a 1090ES message, as explained in the patents [52,53]. To perform an SDR-based implementation using an I-Q modulator at the input of the transmitting antenna and an I-Q demodulator at the output of the receiving antenna is the most practical way to proceed. In this way, the 1090ES message is conveyed in the in-phase (I) component of the carrier and the additional data in its quadrature (Q) component.

3. Background

In this section, we give a detailed explanation of how TESLA [15] protocol operates.

3.1. Timed Efficient Stream Loss-tolerant Authentication (TESLA)

The TESLA protocol combines asymmetric and symmetric cryptography to capitalize on their respective advantages. The core concept underlying TESLA is that the sender, Alice, adds to every packet a MAC computed with a secret authentication key K' known only by her. The receiver, Bob, buffers the packet when it arrives because he lacks the key to authenticate it. Only when Alice sends it to him, a while later, will he be able to verify the authenticity of the packet. To function properly, TESLA requires time synchronization of senders and receivers and, a trustworthy method for producing keys at the sender and authenticating them at the receiver.

The authentication keys are generated by the sender, Alice, before the broadcast begins. First, she divides the broadcast period into N time intervals. Second, she constructs a one-way keychain of length N, the last key generated K_0, serves as a pledge spanning the whole chain and may be used to verify any of the keys in the chain using the formula $K_0 = F^i(K_i)$. Third, she applies a one-way function F' to the keys of the keychain. This process generates the TESLA *authentication keys* $K'_i = F'(K_i)$, which are used to calculate the MAC of the messages to be broadcast.

Before starting to broadcast, Alice communicates the key disclosure delay d and the pledge to the keychain K_0 to Bob, the receiver, via a secure channel. Then, to broadcast a message m_j at time interval i, Alice must first compute the MAC = MAC(K'_i, m_j), then build the TESLA packet P_j which is then broadcast.

$$P_j = m_j \parallel \text{MAC}(K'_i, m_j) \parallel K_{i-d} \tag{2}$$

When Bob receives P_j, he stores the triplet $(i,\ m_j,\ \text{MAC}(K'_i, m_j))$ in a buffer while waiting for the TESLA interval key that will allow him to deduce the authentication key K'_i and validate the MAC of the message m_j. Furthermore, Bob checks the authenticity of the origin of the interval key K_{i-d} by determining whether there exists a small integer v (i.e. of size commensurate with the number of intervals in a typical flight) such that $K_0 = F^v(K_{i-d})$. In such an event, Bob computes the authentication key $K'_{i-d} = F'(K_{i-d})$ and then validates the integrity of the messages broadcast within the time interval $i - d$ by computing their MAC and comparing them with the stored ones.

4. Phase overlaid modulation techniques

In this section, we focus on phase overlay modulation techniques and describe how they can be applied at the physical layer of ADS-B to increase data throughput while keeping the channel activity rate constant.

Systems that are currently envisioned by avionics system designers will most likely require more data transmission than the 6.2 messages per second restriction allowed by the ADS-B standard [3,52]. Furthermore, increasing data throughput is a *sine qua non* condition for securing the protocol. Both industry and academia are aware of this need and have begun to look for methods to increase data throughput while meeting the standard's requirements of preserving the 1090ES band [3, 52,54–56]. There are three versions of ADS-B, with the most recent (Version 3) released in the 2020 MOPS [3]. This version of the MOPS incorporates the notion of phase overlay capacity, which involves using alternate modulation techniques to increase data throughput without increasing channel activity rate. Although phase overlay is not required in this version of the MOPS, it is included so that stakeholders can begin designing, manufacturing and testing equipments and systems with the capability [57].

The MOPS proposes the use of the phase overlay functionality to encode additional bits of information into a conventional 1090ES message beyond the original 112 bits. The phase overlay method proposed is that described in a patent [52]. As depicted in Fig. 1, this can be done by performing a pulse position modulation (PPM) on the 1090ES message to be transmitted, then performing a phase shift keying (PSK) modulation on the additional data to be transmitted. To complete the process, the PSK signal resulting from the previous step has to be modulated to the PPM signal resulting from the first step.

PSK is a modulation technique in which data is transmitted by altering the phase of the carrier wave. It was chosen as the overlay modulation method because it can be individually demodulated (Fig. 1) and is non-destructive to the original message sent by amplitude modulation [52,53]. In principle, changing the phase of the carrier signal should not affect the older hardware's ability to decode the original 1090ES message [52,53]. However, although there is agreement on the usage of PSK modulation as the overlay modulation technique, stakeholders are still divided on which combination to adopt. The study [56] suggest using the binary phase shift keying (BPSK) method, which allows doubling the throughout, sending a total of 224 (112*2) bits. However, this amount of bits is insufficient when we consider that the smallest digests produced by SHA-2 (SHA-224) and SHA-3 (SHAKE 128) are 224 bits and 128 bits, respectively [58,59]. Furthermore, the smallest ECDSA signature is 256 bits [40]. It is precisely in order to allow signing of ADS-B messages that researchers [54,55] have advocated using the Differential 16-Phase-Shift Keying (D16PSK) as it allows quintupling the throughput. However, as is widely known, increasing the modulation order increases BER. This tradeoff in transmission reliability is probably one of the reasons why the RTCA [3] advocates using D8PSK modulation, in combination with error correction codes such as Reed–Solomon or Low-Density Parity-Check. As a result, only 204 of the 336 extra bits provided by D8PSK can be used to convey extra information. Thus, while phase overlay techniques increase data capacity, there are still certain constraints when it comes to securing ADS-B communications. Traditional digital signatures using certificate-based PKI continue to be a concern regarding the communication cost,

Table 2
A Comparison of CABBA's packet structure with that of earlier TESLA-based solutions. In CABBA, Type B packets are replaced with Type B1 Packets at the beginning of each interval (each $T_B = T_{B1}$ seconds) and by Type B2 packets every T_{B2} seconds. Type C packets are shorter than in SAT and sent with period T_C.

Type				Content	Period	Size (bits)			
TESLA	SAT	SOS	CABBA			TESLA	SAT	SOS	CABBA
A				Message, MAC	–	–	–	–	–
	A			ADS-B message, MAC, sequence no.	–	–	136	–	–
		A1		ADS-B message	–	–	–	112	–
		A2		MAC	T_{A2}	–	–	128	–
			A	ADS-B message, MAC, sequence no.	–	–	–	–	112
B				Interval key	T_B	128	–	–	–
	B			Interval key	T_B	–	184	–	–
		B		Interval key	T_B	–	–	128	–
			B1	Interval key	T_{B1}	–	–	–	128
			B2	Interval key and signature	T_{B2}	–	–	–	210
	C			Interval key and signature; Aircraft public key and signature	T_C	–	1520	–	–
			C	Aircraft public key and signature	T_C	–	–	–	242

and this despite the increase in data capacity. In contrast, short signatures employing hybrid cryptography appear to be a more attractive option.

5. CABBA: Compatible Authenticated Bandwidth-efficient Broadcast protocol for ADS-B

The CABBA solution is presented in this section. CABBA seamlessly integrates phase-overlay modulation into the ADS-B physical layer and TESLA authentication into its application layer, while using a certificate-based public key infrastructure. CABBA is based on a new approach in which the fundamental TESLA concept of MAC-based message authentication and key disclosure delay remains intact, while introducing a significant transformation in the way information is transmitted and the type of information transmitted to enhance security. In the following lines, we delve into how CABBA distinguishes itself from previously proposed TESLA-based solutions, i.e. (1) the integration of phase overlay modulation and (2) enhanced packet structure.

Integration of phase overlay modulation. First, we enhance the physical layer of ADS-B by incorporating the phase overlay modulation technique proposed in the patent [52] recently promoted by the RTCA in the most recent version of the ADS-B MOPS [3]. As detailed in Fig. 1, part of the information is conveyed in the in-phase component of the carrier, and the remaining information is in its quadrature component. For this purpose, we consider the two phase overlay modulation techniques mentioned earlier:

1. the D8PSK method advocated by RTCA [3], and
2. the D16PSK method proposed by academia [54,55].

To determine which of these techniques is most appropriate for CABBA, we first implemented and conducted backward compatibility tests with both of them. Most importantly, we set to identify which of these modulation techniques provides an optimum trade-off between higher data throughput and acceptable quality of signal, i.e. a lower BER, by conducting a simulation study. This is described in Section 6. Nonetheless, since D8PSK is the proposed standard and for the sake of simplicity of explanation, in the rest of this section we describe only the implementation with D8PSK. This configuration allows for an additional 336 (3*112) bits to be sent together with the ADS-B 112-bit original message.

Enhanced packet structure. The second distinction between CABBA and previous works relates to the content and structure of the packets to be transmitted, as highlighted in Table 2.

In TESLA, the security information in Type A packets (the MAC) and the interval key subsequently received via Type B packets allows the receiver to verify *data integrity* of the message. *Data origin authentication* is achieved by cross-referencing the information in Type B packets with additional data shared from sender to receiver via a secure communication channel. Both protocols, TESLA [15] and SOS [60], assume pre-existing trust between communicating parties, presupposing that the receiver possesses the sender's certificate beforehand.

In real-life operation, however, an aircraft cannot anticipate precisely which other planes it will encounter along its flight path. Consequently, the authors of SAT [36] propose a practical solution: distributing certificates through type C packets—an approach we endorse. Nonetheless, there are at least three aviation scenarios in which Bob (the receiver) may not require the certificate, as he may already possess the sender's public key and have duly authenticated its legitimacy. These scenarios are:

1. Bob, as an ADS-B ground station, receives messages from aircraft either directly (via Line-of-Sight RF signal) or indirectly (via satellite). To authenticate these messages, Bob's ground station can access a PKI containing public keys of worldwide aircraft, indexed by their ICAO ID. This setup enables instant entity authentication without relying on aircraft to transmit certificates.
2. Alice, another ADS-B ground station, transmits information to airborne aircraft like Bob through LOS signal. Here, it is reasonable for the aircraft's receiver to hold a small, infrequently updated database of public-key certificates provided by the NAA (e.g., FAA) for authentication.
3. Air-to-air ADS-B transmissions pose challenges as it is impractical to preload worldwide aircraft public keys into each aircraft's receiver, let alone update them frequently due to aircraft turnover. However, future adoption of integrated digital communications like ATN could enable real-time access to remote PKIs, allowing aircraft to cache recently encountered aircraft's public keys for authentication.

To accommodate for such situations where the transmission of certificates might not be needed or not be needed as often, we propose the packet structure that follows :

Type A. Contain the ADS-B message its MAC and sequence number under the interval

Type B1. Contain the interval key K_i

Type B2. Contain K_i and the digital signature of K_i.

Type C. Contain the aircraft public key K_{pub} and its signature by the CA

Unlike SAT [36], Type C packets in CABBA do not contain interval key information or interval key signatures, and are therefore shorter. Signed interval keys are transmitted in a new type of packet, Type B2, which contains only an interval key and its signature. This has the advantage that signed keys can be sent with a lower frequency than certificates, resulting in a better use of bandwidth. In addition, this CABBA packet structure has the advantage of reducing bandwidth usage by eliminating the redundant transmissions of the interval keys, as it was the case in SAT [36].

5.1. CABBA on the sender side

CABBA requires airplanes to have a private–public key pair (K_{pr}, K_{pub}) and a certificate issued by a well-known and trusted certification authority. Before the flight begins, Alice, the sender, divides its duration into equal intervals of d seconds, and generates an authentication key for each interval. The process for generating these keys is the same as that used in TESLA and SAT. During the flight, the ADS-B messages and their MAC, the authentication keys of the intervals, and the certificate of Alice's aircraft are sent as described below.

5.1.1. Sending a message and its MAC

To send an ADS-B message m at time interval i, Alice first produces the security data σ for message m. This includes:

1. The message MAC, formed by the λ leftmost bits of the message $\text{HMAC}(m, K'_i)$
2. The message sequence number s for m within that interval i

In other words $\sigma = \text{MAC} \parallel s$. As before, this information will continue to be encoded into the in-phase component of the RF signal. We denote by $P_{A-I} = m$ the message information sent in-phase. The security information σ will be sent using the quadrature component of the RF signal and is thus denoted $P_{A-Q} = \sigma$.

With the same packet length (112 bits) and containing the same information encoded in the same manner as standard ADS-B packets, P_{A-I} packets are intended to be fully intelligible by legacy ADS-B receivers. A logical packet P_{A-Q}, on the other hand, will in principle only be intelligible with CABBA-compliant receivers. With the choice of D8PSK, the highest quantity of bits that can be encoded in the quadrature component is 336 bits. Nonetheless, not all of these bits are available to encode the security information σ. The RTCA recommends using 12 bits to encode a reference phase and 120 parity bits to support the $\texttt{RS(54,34)}$ error-correcting code, which must be applied to the σ security data. This means a maximum size of 204 bits for σ, which with the 8-bit sequence number s results in a maximum size of 196 bits for the MAC, i.e. $\lambda \leq 196$.

Alice uses the logical packet P_{A-I} to perform PPM on a pulse train to generate the signal $S_{A-I}(t)$ as follows:

$$\begin{aligned} S_{A-I}(t) &= \sum_{k=0}^{111} g(t - t_k) \quad ; \\ t_k &= kT_S + m_t(1 - P_{A-I}(k)) \end{aligned} \tag{3}$$

where $T_S = 1\,\mu\text{s}$ is the symbol period for 1090ES transmissions, $m_t = T_S/2$ is the PPM time-modulation index and $P_{A-I}(k)$ is the value of the kth bit which will be transmitted at time $k * T_S$. Alice simultaneously uses logical packet P_{A-Q} to perform D8PSK modulation on a sine wave to generate the signal $S_{A-Q}(t)$ as follows:

$$\begin{aligned} S_{A-Q}(t) &= \sum_{k=0}^{111} \sin(\omega_c t - \theta_k) \quad ; \\ \theta_k &= \frac{2\pi}{8}\,\text{symbol}_{P_{A-Q}}(k) \end{aligned} \tag{4}$$

where ω_c represents the carrier signal frequency, θ_k is the phase associated to the 8PSK symbol $\text{symbol}_{P_{A-Q}}(k) \in [0, 7]$, which is computed from the three bits from P_{A-Q} to be transmitted at time $k * T_S$.

$$\begin{aligned} \text{symbol}_{P_{A-Q}}(k) =& 2^2 P_{A-Q}(3k) + 2^1 P_{A-Q}(3k+1) + \\ & 2^0 P_{A-Q}(3k+2) \end{aligned} \tag{5}$$

These two signals $S_{A-I}(\text{t})$ and $S_{A-Q}(\text{t})$ are then used by Alice to I-Q modulate (Eq. (6)) the 1090ES carrier and so, produce the radio signal S_A to be broadcast.

$$S_A(t) = S_{A-I}(t)\cos(\omega_c t) + S_{A-Q}(t)\sin(\omega_c t) \tag{6}$$

5.1.2. Sending authentication keys and their signatures

In order to allow the receiver to authenticate the Type A messages sent in interval i, the sender must later disclose the corresponding interval keys and their signatures. This is done by sending Type B1 and B2 packets in subsequent intervals.

Type B1 packets contain the TESLA interval K_i (128 bits) from which the authentication key $K'_i = F'(K_i)$ of the interval i is calculated. The corresponding packet P_{B1} will be transmitted during the next time interval $i + 1$. These packets are sent at the beginning of each interval, i.e. every $T_{B1} = T_{int}$ seconds.

The signature of the authentication keys is added in Type B2 packets. B2 packets replace B1 packets at the beginning of the interval, every fixed number k of intervals. Their transmission period T_{B2} is thus a multiple of T_{B1}, with $T_{B2} = kT_{B1}$. A typical packet P_{B2} of this type will contain:

$$P_{B2} = K_i \parallel \text{sig}_{K_{pr}}(K_i) \tag{7}$$

where the $\text{sig}_{K_{pr}}$ represents the chosen signature-generating function with private key K_{pr}.

For Type B1 packets, the logical information P_{B1} is split between packets P_{B1-I} and P_{B1-Q} that will be transmitted through the in-phase and quadrature components of the RF signal. The in-phase packet P_{B1-I} contains the 50 leftmost bits of the K_I and the quadrature packet P_{B1-Q} contains the remaining 78 bits, as indicated in Fig. 3(a).

For Type B2 packets, the information is similarly split into packets P_{B2-I} and P_{B2-Q}. The in-phase component P_{B2-I} contains the entire interval key K_i and the leftmost 14 bits of the signature, while the quadrature component P_{B2-Q} contains the remaining 498 bits of the 512-bit signature.

The signal components S_{B1-I}, S_{B1_Q}, S_{B2-I} and S_{B2-Q} are then generated similarly as for Type A packets (Eqs. (3), (4) and (6)).

5.1.3. Sending the certificate of the transmitting aircraft

Alice will broadcast the certificate of aircraft every T_C seconds. The Type C packet P_C contains the public key of the aircraft K_{pub} and the signature of this key $\text{sig}_{K_{prCA}}(K_{pub})$. With a security strength of 128 bits, an ECDSA public key size of 256 bits is required, resulting in a signature size of 512 bits [42]. The first 181 bits of the public key K_{pub} are encoded in the in-phase packet P_{C-I} and the remaining 75 bits at the beginning of the quadrature packet P_{C-Q}. The 512 bits of the signature sig are also encoded into P_{C-Q}.

After encoding P_{C-I} and P_{C-Q}, the sender generates the signals S_{C-I}, S_{C-Q}, and finally the signal S_C which she broadcast. The procedure for producing these signals is the same as for producing signals for Type A and B packets.

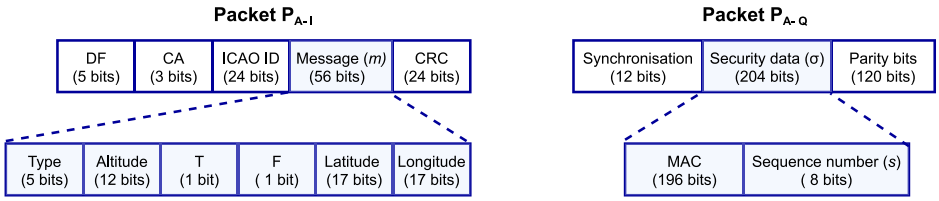
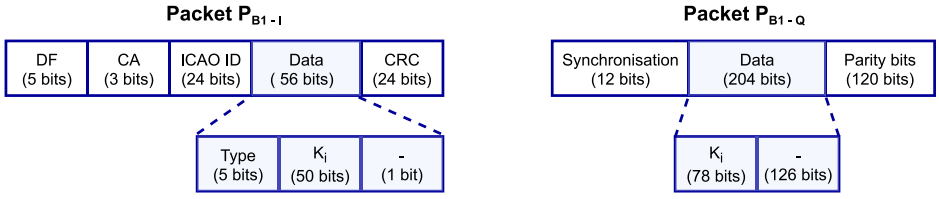
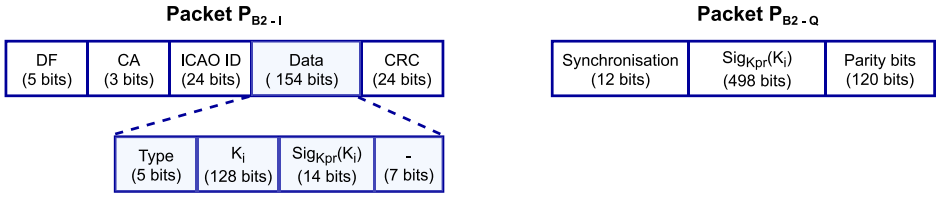


Fig. 2. Structure of the Type A packets in CABBA. The ADS-B message m encoded in the in-phase component P_{A-I} (in this example an airborne position report) and the security data σ in the quadrature component P_{A-Q}. These two logical packets are then used to generate the in-phase and quadrature signal components S_{A-I} and S_{A-Q} of the RF signal to be transmitted S_A.



(a) Structure of Type B1 packets, 112 bits for P_{B1-I} and 336 bits P_{B2-Q}



(b) Structure of Type B2 packets, 210 bits for P_{B2-I} and 630 bits P_{B2-Q}

Fig. 3. Structure of Type B1 and B2 packets, conveying only the authentication key or the authentication key and its signature, respectively.

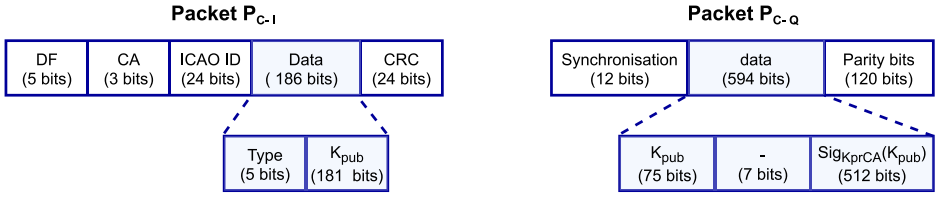


Fig. 4. Structure of Type C packets. They contain the public key K_{pub} of the aircraft and the signature of said key $\text{sig}_{K_{prCA}}(K_{pub})$. These packets are then used to generate the transmitted signal S_C.

5.2. CABBA on the receiver side

5.2.1. Reception and demodulation of signals

The process of receiving and demodulating messages by Bob (the receiver) is the same for all packet types. The received signal S is first demodulated with quadrature local oscillators to obtain the in-phase component S_I and the quadrature component S_Q. Bob then performs PPM demodulation onto S_I and D8PSK demodulation onto S_Q, to generate logical packets P_I and P_Q, respectively. Depending on the format of these packets, Bob determines the original packet type (A, B1, B2 or C) and processes them accordingly. The processing of the CABBA messages contained within these logical packets is detailed below and depicted in the state diagram in Fig. 5.

5.2.2. Processing the ADS-b message and its security data

As described above, the ADS-B message information and its security data is contained in Type A packet P_{A-I} and P_{A-Q}, respectively. Bob thus extracts the message m' from P_{A-I} and the security data σ (its sequence number s and the MAC) from P_{A-Q}. Lastly, he stores the triplet (m', s, MAC) in a buffer until he can verify the integrity of the message.

5.2.3. Verification of security properties

CABBA is an asynchronous protocol and there is no guarantee that messages corresponding to a particular aircraft will be received in any particular order. The state diagram in Fig. 5 describes the various states in which the receiver of CABBA could be depending on what security information, i.e. what CABBA packet types, have been received so far. Note that such a state diagram is used for all messages received with the same ICAO ID, i.e. purportedly corresponding to the same aircraft.

The state machine is initialized at state S_0 when the first packet for a given ICAO ID is received. If it is a Type A packet, it will be stored and the machine stays in the same state. Reception of type B1 packet containing an interval key will generate a transition to State S_1. Reception of a Type B2 packet, a *signed* interval key, will make the state machine transition to State S_2. Finally, the (unlikely but possible) reception of a certificate in a Type C packet before a Type B1 or B2 packet will transition to State S_3. In all of these states (S_1, S_2 and S_3), subsequent reception of ADS-B messages in Type A packets and further interval keys in Type B packets causes no transitions.

At this point, the receiver is unable to perform either entity authentication or data origin authentication of any messages received because some security information is missing (has not been received), i.e. either a validate certificate in the case of State S_2, a signed interval key in the

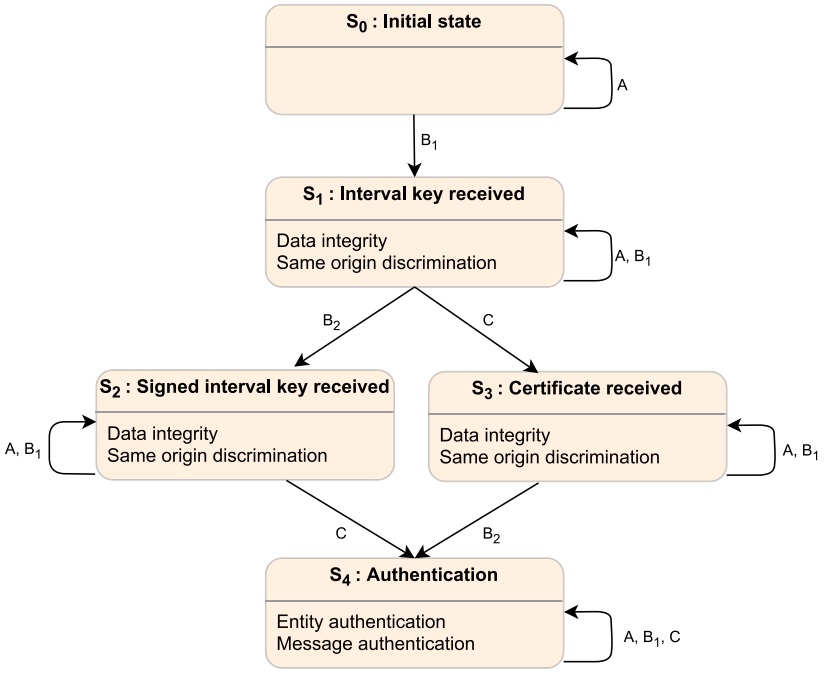


Fig. 5. State diagram illustrating the authentication process for ADS-B messages on the receiver side.

case of State S_3, or both in State S_1. Nonetheless, the receiver is able to perform data integrity verification of the ADS-B messages received in previous intervals.

Data integrity. In order to validate the message integrity of a message m' received during interval i, Bob must have already received Type B1 packets P_{B1-I} and P_{B1_Q} at the beginning of the next interval $i+1$. From these packets, he will be able to reconstruct the interval key K_i by concatenating the first 50 bits contained in P_{B1-I} and the remaining 78 bits contained in P_{B1-Q} (as shown in Fig. 2). The next step is to calculate the authentication key $K_i' = F'(K_i)$. Then, Bob calculates the "correct" HMAC of the received message m' with this authentication key K_i' as follows $\text{HMAC}' = \text{HMAC}(m', K_i')$. Finally, Bob compares the λ leftmost bits of HMAC$'$ with the received MAC. If they coincide, Bob will accept the message m', otherwise, he will ignore it.

Note that this verification only meets the goal of *data integrity* of the message m', i.e. that the message has not been modified after its MAC was computed by its originator, whomever the originator might be (friend or foe, real aircraft or hacker).

Same-origin discrimination. While in States S_1, S_2 and S_3 the receiver is unable to perform data origin authentication, there is an important security property that can be asserted at this point: *same-origin discrimination*, i.e. the ability to determine which message was sent by which sender, without necessarily having authenticated them.

To better understand this property, consider the following spoofing scenario. The attacker is aware that Alice's aircraft with ICAO ID X_A is currently broadcasting ADS-B messages that Bob is receiving. The intent of the spoofer is to send counterfeit ADS-B messages bearing the same ICAO ID X_A. Aware that the aircraft ADS-B transmitter and the receiver have implemented CABBA, the spoofer can generate his own interval key sequence and use it to authenticate his fake messages. More precisely, let $K^* = K_0^*, \ldots, K_N^*$ be the interval sequence generated by the aircraft and let $K^\dagger = K_0^\dagger, \ldots, K_N^\dagger$ be the sequence generated by the spoofer. The spoofer then generates his own messages, including hashes computed with his own key sequence.

If both spoofer and Alice's aircraft are in Bob's reception range, Bob would then receive these two message streams corresponding to the same ICAO ID X_A, potentially contradictory. Thus, while Bob may not be able to determine which messages came from the spoofer and which came from Alice's aircraft, he will still be able to correctly associate a new message m' with either stream. He does this by identifying the TESLA keychain to which the interval key used to compute the MAC of m' belongs, as described in Formula (8).

Consider two messages m_1 and m_2 received by Bob at intervals i_1 and i_2, $i_2 > i_1$, respectively, and whose integrity was verified by Bob in the subsequent intervals $i_1 + 1$ and $i_2 + 1$ with interval keys K_{i_1} and K_{i_2}, respectively. Then if:

$$K_{i_1} = F^{(i_2 - i_1)}(K_{i_2}) \tag{8}$$

then Bob knows that m_1 and m_2 were sent by the same sender. In other words, in the above scenario Bob will be able to detect that there are two different senders A^* and $A^\dagger$ sending messages with the same ICAO code, and further know which message corresponds to which sender. He will not, however, know which one corresponds to the real aircraft A.

Authentication. When Bob has received all required security information, i.e. a signed interval key and a certificate, he can then perform both identity authentication of the sender and message authentication (i.e. data origin authentication) of previously received messages. This will be possible when the state machine transitions to State S_4.

Identity Authentication Upon receiving Type C packet P_{C-I} and P_{C-Q}, the public key K_{pub} is extracted by concatenating the 181 bits in P_{C-I} and the first 75 bits in P_{C-Q}. The key signature $\text{sig}_{K_{prCA}}(K_{pub})$ is extracted from the remaining 512 bits of P_{C-Q}, as shown in Fig. 4. Since Bob knows the public key K_{pubCA} of the Certificate Authority, he is able to verify the validity of the signature of the aircraft key the corresponding signature verification procedure `Verify`, that returns a boolean of `true` if the signature is valid. In other words, let v_1 be the result of this first signature verification:

$$v_1 = \texttt{Verify}(K_{pubCA}, \text{sig}_{K_{prCA}}(K_{pub}), K_{pub}) \tag{9}$$

Message authentication Finally, having received a Type B2 packet P_{B2-I} and P_{B2-Q}, Bob proceeds to extract the key K_i from P_{B2-I}. To obtain the signature $\text{sig}_{K_{pr}}(K_i)$, he concatenates the 14 bits from P_{B2-I} with the 498 bits from P_{B2-Q}. Using this information, Bob verifies

the authenticity of the interval key K_i. Let v_2 be the result of this verification procedure, as defined by the equation:

$$v_2 = \texttt{Verify}(K_{pub}, \text{sig}_{K_{pr}}(K_i), K_i) \tag{10}$$

If v_2 evaluates `true`, it means that the key K_i is authentic, i.e. that it has been generated by Alice. Furthermore, this outcome also implies that all ADS-B messages for which the MAC has been computed using K_i can also be deemed authentic.

6. Backward compatibility experiments

We conducted backward-compatibility tests to verify that the phase overlay capability, as implemented in CABBA, does not affect the ability of existing hardware to decode the original ADS-B messages that are transmitted in the in-phase component of the 1090ES carrier.

To do so, we built an SDR-based implementation of CABBA and tested its backward compatibility with two distinct COTS ADS-B solutions:

1. The Appareo Stratus II ADS-B receiver, a non-certified portable device used in general aviation (GA) aircraft. The Stratus II was connected via Wi-Fi to an IPad running the ForeFlight application displaying ADS-B traffic information.
2. The Collins TSS-4100, a certified avionics device integrating TCAS, transponder and ADS-B traffic surveillance capabilities, used in business jets and airline transport aircraft. This equipment was connected to a Collins AFD-6520 Adaptative Flight Display to render the traffic information.

The experimental setup we employed involved the following steps:

1. Generate ADS-B messages and corresponding CABBA packets using custom-made scripts.
2. Generate and transmit the corresponding RF signals using the HackRF One SDR.
3. Receive these RF signals with the corresponding COTS receiver.
4. Check that the transmitted ADS-B information is received and correctly interpreted. We consider the test successful if the transmitted traffic information is displayed with the correct information (call sign, position, etc.).

In our experimental setup, the ADS-B messages and the corresponding packets were generated using custom-made scripts. These scripts are based on the *ADSB_Encoder.py* [61] scripts. This original script only generates ADS-B messages of the position report type, when given the ICAO, latitude, longitude, and altitude of an aircraft as inputs. However, the logic of ADS-B receivers is such that in order for them to consider a given aircraft's traffic information, they must receive all required ADS-B message types, i.e. identity, speed, status, and operating status, at the frequency prescribed by the protocol. Thus, to conduct these tests, we built scripts that generate the remaining types of ADS-B messages[3].

The scripts we constructed further added the functionality required to generate CABBA messages (keys and certificates) and the corresponding packets. This includes among others functions to compute the MAC of ADS-B packets, to apply DPSK modulation to data to be transmitted in quadrature, to I-Q modulate the in-phase data in PPM with the quadrature data in DPSK.

For these backward-compatibility experiments, we only constructed and transmitted type A messages, which carry the ADS-B message and its security data. We did not transmit the other types of CABBA messages (B1, B2 and C), as these would be ignored by legacy receivers since they do not contain ADS-B data.

[3] For this purpose the book *The 1090 Megahertz Riddle* [62] was an invaluable resource.

Our tests reveal that CABBA is backward-compatible with the two ADS-in receivers under test. Fig. 6 shows the display of the ForeFlight application on the IPAD connected to the Stratus II receiver. The information displayed corresponds exactly with the information sent from the Hacker RF One SDR. The same is true for the information displayed on the AFD-6520 connected to the TSS-4100 transponder, as shown in Fig. 7. The results suggest that using CABBA with legacy equipment will not compromise safety during the transitional period, where some aircraft would not yet have CABBA-capable ADS-B receivers. This finding supports the assumptions behind the MOPS used in CABBA and provides encouraging evidence for our implementation of it. However, further analysis and testing with a wider range of equipment in laboratory settings is needed, including packet reception analysis and, interoperability and stability tests. Once these tests are satisfactory, in-flight tests should follow, ideally in environments with high ADS-B channel usage and with sources of interference, such as multi-path transmissions due to terrain (mountains, water surface) or man-made obstacles (buildings, antennae, etc.). While we do not think that the use of the MOPS would affect backward compatibility in such real-world conditions, we do believe that it is important to study how transmission and bit error rate for the quadrature signal would be affected by such sources of interference and in high-channel usage.

7. Operational viability of CABBA

While CABBA as proposed could provide a high level of security in terms of message authentication, there are some open questions regarding the viability of employing it in real-world situations due to operational and technological constraints.

First, we must determine which modulation scheme is most appropriate, D8PSK or D16PSK. Second, we must evaluate the bandwidth overhead of CABBA. Even with the use of PSK modulation, CABBA still requires more transmission time than plain ADS-B. It thus remains to be seen whether the resulting bandwidth overhead challenges its use in the already congested 1090 MHz frequency. In this section, we describe our preliminary analysis of these questions using simulations to evaluate BER and real-world ADS-B data to conduct COR analysis.

7.1. Comparative BER analysis of CABBA with D8PSK vs. D16PSK

The aim of this BER analysis, is to determine which of the two phase overlay modulation schemes, D8PSK or D16PSK, provides the best balance between higher data throughput and acceptable signal quality, i.e. ADS-B service quality.

We used Simulink [63] to model the communication link of the CABBA protocol. Then, we used the MATLAB program `bertool` to perform Monte-Carlo simulations to determine the BER across an Additive White Gaussian Noise (AWGN) channel.

A lower BER indicates a better performance; for ADS-B, the standard establishes a maximum BER of $10^{-}6$ [3]. The BER curves of the two implementations of CABBA that we wanted to compare, as well as the BER curves of the D8PSK, D16PSK, and D32PSK modulations, are depicted in Fig. 8. By observing these curves, we notice that:

1. When implemented with D8PSK, CABBA fulfills the requirements of the standard for normalized signal-to-noise values (Eb/No) greater than or equal to 15 dB. For these values, the BER is equal to zero, indicating that the transmission is error-free.
2. When implemented using D16PSK, CABBA fails to meet the requirement of the standard.

Based on these results, we find that the D8PSK technique is the best method for implementing phase overlay functionality in avionics systems operating in the 1090ES band. In the ADS-B context, the D16PSK technique has a significant impact on data quality and reliability. Given the high error rates provided by D16PSK, the increase in throughput may not be worth it.

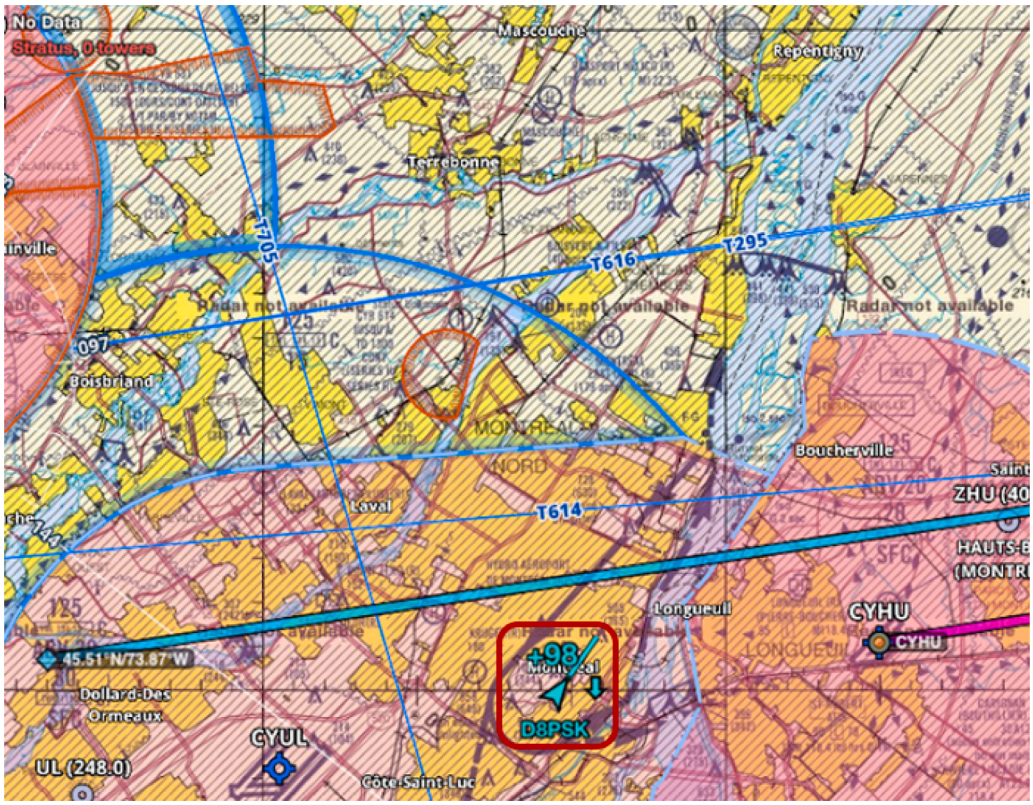


Fig. 6. Screen capture of the ForeFlight Maps display with traffic option activated, showing the correct information for the "synthetic" aircraft with call sign "D8PSK", obtained from an IPad connected to the Stratus II receiver.

Fig. 7. Here is a picture of the display AFD-6520 Adaptive Flight Display showing the correct information for the "synthetic" aircraft with call sign "D16PSK".

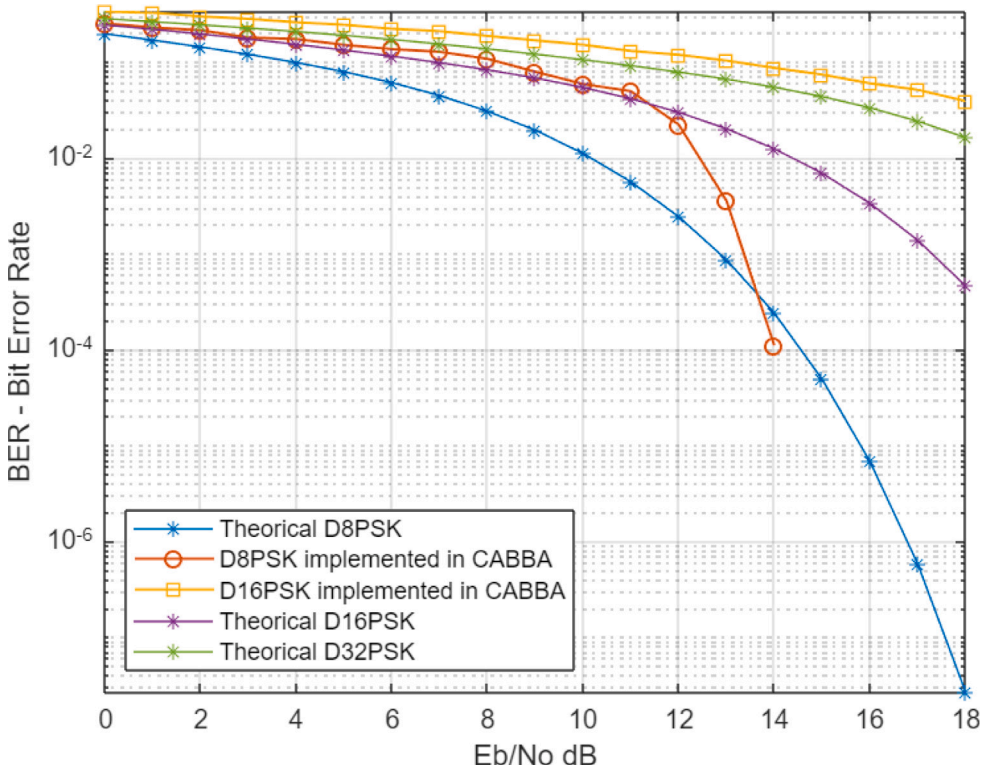


Fig. 8. BER analysis shows that CABBA meets the standard's requirements for normalized signal-to-noise values (Eb/No) greater than or equal to 15 dB when implemented with D8PSK. Indeed, the standard requires a BER $< 10^{-6}$ and from Eb/No = 15 the BER is equal to 0.

7.2. Channel occupancy rate (COR) analysis

We conducted a COR analysis to determine to what extent the transmission of non-standard ADS-B information, which are essential for CABBA support, decreases the available bandwidth.

The ITU report ITU-R SM.2256-1 [64] provides a detailed discussion on different approaches for measuring and evaluating spectrum occupancy, i.e. a methodology to conduct COR analyses. We used it as a guide to conduct our analysis. Indeed, the activity factor (γ) reflects how active the communication channel is. It is defined as follows [65]:

$$\gamma = \frac{\sum_{i=1}^{n} \Delta t_i}{\Delta t} \tag{11}$$

where Δt_i represents the channel occupation time for the ith active transmission and Δt represents the total duration of the period being considered.

We created a baseline of normal 1090ES channel occupancy levels using real ADS-B data retrieved from the OpenSky Network database [66]. Since 2013, the OpenSky Network has been gathering continuous air traffic surveillance data as a non-profit community-based receiver network [67]. All unfiltered raw data is kept by OpenSky and made available to academic and institutional researchers.

To collect data for our research, we chose a receiver near Paris Orly airport (IATA code ORY, ICAO code LFPO). We chose this receiver because of the high density of aircraft traffic that can come within its reception range, including:

1. Aircraft transiting through the Northern France airspace, i.e. Paris Area Control Center (ACC), one of the busiest aerial corridors in the World. The ADS-B station could receive signals from aircraft at cruise altitude (30–35,000 ft) up to 200 nautical miles (360 km).
2. Aircraft transiting through the Paris Terminal Maneuvering Area (TMA) that are landing or departing from Paris Charles de Gaulle, Orly or Le Bourget, some of the busiest airports in Europe.
3. Aircraft on the ground at the Orly airport taxiing with transponders on.

Table 3
Transmission period parameters for each of the four scenarios for which we computed the COR values.

	Scenario 1	Scenario 2	Scenario 3	Scenario 4
T_{B1}	5 s	5 s	5 s	5 s
T_{B2}	5 s	10 s	10 s	15 s
T_C	5 s	15 s	20 s	30 s

We obtained a data capture of all traffic for this station for a 24-hour period on 3 August 2023. Obviously, aircraft traffic varies during the day, and hence so does 1090ES transmissions. We sampled the traffic within each 1-hour period and observed the transmission rate within 30 second-long periods within that hour. Taking six such samples for every hour, we observe quite a bit of variation in the number of transmissions within each hour; the corresponding confidence intervals are included in our results below (see Fig. 9).

In CABBA, we transmit four different types of packets, i.e. packet types A, B1, B2 and C. All packets of the same type have the same length and occupy the channel for the same duration. Let Δt_A, Δt_{B1}, Δt_{B2} and Δt_C be the transmission times for each of these packet types. These values are proportional to the bit length of these packets (Table 2) *plus* the fixed 8-bit preamble. Given the 1090ES channel bit rate of 1 megabit/s, this results in 120 ms, 120 ms, 218 ms and 250 ms, respectively.

For each sampled time interval, let n_A, n_{B1}, n_{B2} and n_C be the number of packets of each that would be transmitted with CABBA. The resulting COR value is given by

$$\gamma = \frac{n_A\,\Delta t_A + n_{B1}\,\Delta t_{B1} + n_{B2}\,\Delta t_{B2} + n_C\,\Delta t_C}{\Delta t} \tag{12}$$

For our analysis, we conservatively consider that all aircraft in the dataset are CABBA-capable and are sending all CABBA packet types as

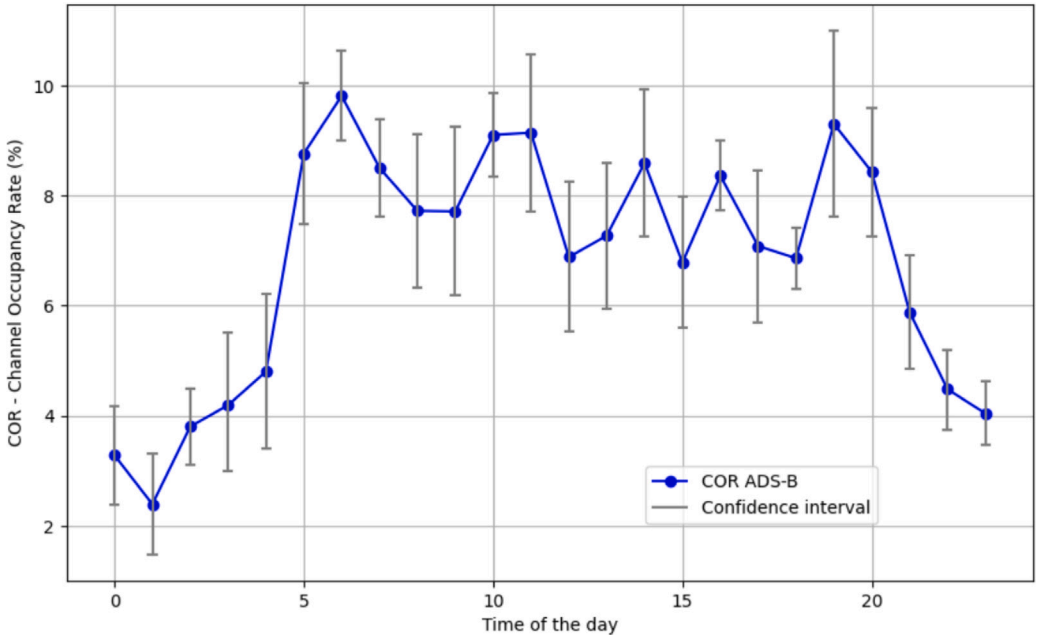


Fig. 9. Mean COR for ADS-B transmissions with confidence intervals, computed with a sampling of six 30-second periods for every hour of the day, on 3 August 2023.

described in the protocol description in Section 5. Of course, our dataset only includes standard ADS-B packets and does not provide us with packet counts for non-standard CABBA packet type, except for Type A packets for which the count number n_A is the same as the number of ADS-B packets. For the other packet types, we estimate the number of transmissions to be equal to the number of different aircraft seen in the previous T seconds [68], where T is the transmission period of that type of packet. For example, let us consider Type B1 packets, i.e. packets containing unsigned interval keys. Each aircraft will send such a packet every T_{B1} seconds, i.e. with a T_{B1}-second period. At a given time t, let x be the number of different aircraft (with different ICAO ID) we have seen in our data set in the previous T_{B1} seconds. During that time period, some aircraft will have arrived in range and some others will have departed. If we assume that within the sampling interval (30 s) both the arrival and departure rate of aircraft are relatively small and similar to each other, we then can safely approximate the number of Type B1 packets that will be sent during that period to be x, i.e. $n_{B1} \approx x$. The same can be said for the counts n_{B2} of Type B2 and n_C of Type C packets which we approximate to be the number of different ICAO ID received in the previous T_{B2} and T_C seconds, respectively.

With these approximations, we are then able to compute the COR value γ from Eq. (12). We consider four different parameter settings, described in Table 3. In all scenarios, we keep the same 5-second Tesla interval duration set in SAT. In the first scenario, Type C packets are sent at every Tesla interval along with Type B2 packets; Type B1 packets are thus never sent. This is the "safest" scenario in which CABBA-compatible receivers must wait at most 5 s until being able to authenticate messages, in the sense that the uncertainty period for CABBA receivers where originators cannot be authenticated is minimized. The fourth scenario is the most bandwidth efficient, with Type B2 packets being sent every other Tesla interval and Type C packet every six intervals.

The first finding of this study is that COR values for standard ADS-B vary between 2.4% and 9.8%, for the quietest and busiest hours, 01h00 and 06h00 UTC, i.e. 03h00 and 08h00 Paris local time, respectively. Second, with respect to CABBA we observe that the maximum overhead corresponds, obviously, to Scenario 1, with the lowest interarrival times for Type B1, B2 and C packets. In Scenario 1, the average overhead in terms of packets transmitted is 3.76% per 30-second period, with an observed maximum of 5.76% during that day. In comparison, for the most bandwidth-efficient Scenario 4, the average overhead is 1.56% and maximized at 2.38%. With respect to channel occupancy levels observed on that day, this results in a maximum COR increase of 0.43% of total bandwidth capacity for the most bandwidth-consuming Scenario 4. These results are represented graphically in Fig. 10.

In summary, whatever the parameter setting scenario we choose, the impact of implementing CABBA in terms of bandwidth is negligible. The overhead in terms of packets sent is capped at less than 6%. This is in sharp contrast with the original SAT proposal, which has an estimated overhead of 35%.

At the observed channel occupation levels, i.e. COR values between 2% and 10%, the COR increase for CABBA even its most bandwidth-consuming setting is less than 1%. Even in more congested airspaces with hypothetical COR values of up to 40%, implementing CABBA would increase COR to less than 43%, a very acceptable compromise.

7.3. Safety impact of unauthenticated messages

The key idea in TESLA that enables authenticated broadcast is the *delayed* key disclosure. However, this feature introduces a safety trade-off: messages cannot be immediately authenticated, resulting in an *uncertainty delay* Δ_u between message arrival and authentication.

As discussed in Section 5.2, to authenticate a message the following information must be in possession of the receiver: (1) the interval key for that message, (2) a signed interval key from this or a previous interval, and (3) the sender's certificate. This information may have already been received in Type B1, B2 or C packets. While the delay of arrival of such information is bounded by their respective interarrival periods, their order of arrival at the receiver is non-deterministic and thus the actual value of Δ_u is also non-deterministic.

Further analysis of what these uncertainty delays are and what is their impact on aviation safety depends on in what application and context the ADS-B information is being used. We analyze various scenarios in TCAS and ATC applications below.

7.3.1. Impact of packet loss on uncertainty delay

In addition, we have to consider packet loss from noise, interference, or collisions due to congestion, which could introduce a further delay due to having to wait an additional 1 or 2 subsequent periods. The following equation describes the expected value of Δ_u as a function

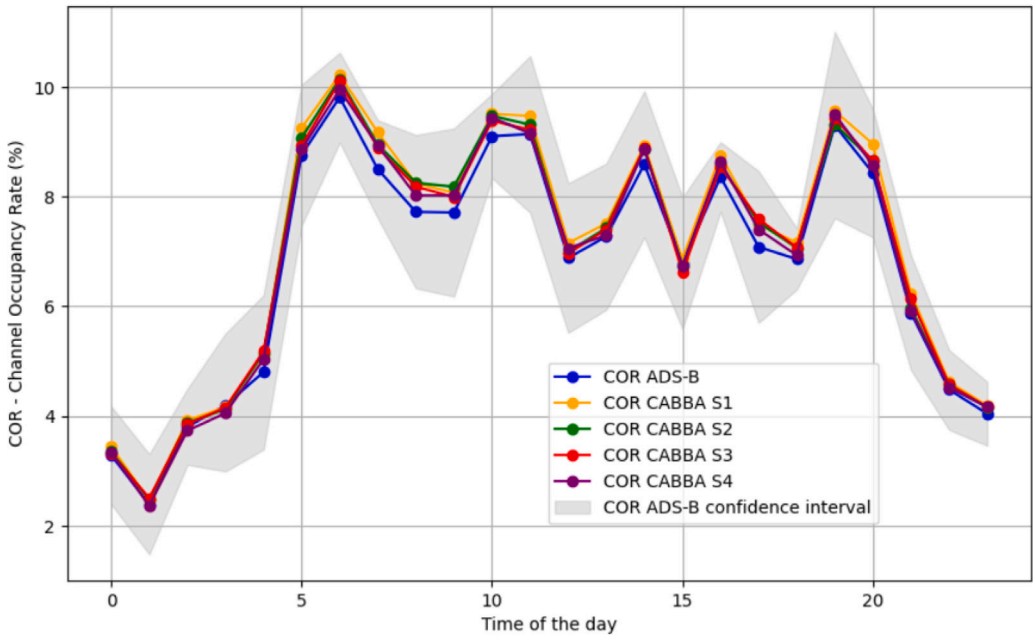


Fig. 10. Estimated mean COR values per hour for every hour of 3 August 2023, for ADS-B and for CABBA in each of the three possible parameter settings described in Table 3.

of the probability of packet loss p and the interarrival period T of the required information, where the first term corresponds to the packet being successfully received in the first interval, the second term in the second interval, etc.

$$\overline{\Delta_u} = (1-p-p^2)\frac{T}{2} + p\left(T+\frac{T}{2}\right) + p^2\left(2T+\frac{T}{2}\right) = \frac{T}{2}(1+2p+4p^2) \quad (13)$$

Previous works [67,69] have explored the packet loss ratio for ADS-B. They apply a conservative definition, where packet loss occurs if *any* receiver within the aircraft's range is missing the corresponding reception record. In the rest of this section, we approximate the probability of packet loss at a particular receptor, by interpolating from the empirical cumulative distribution function between packet loss and distance in [69].

7.3.2. Uncertainty delays in TCAS

TCAS technology is essential in two environments: (1) non-radar environments, like oceanic regions, where ATC may be unable to provide separation services, and (2) dense traffic areas, such as busy airport terminals, where separation conflicts are likely to occur. The TCAS standards and supporting equipment ensure pilots have sufficient situational awareness of nearby aircraft within predefined *protection volumes*. These volumes are defined to address potential separation conflicts within specific *time* periods: 20–48 s for traffic advisories (TA) and 15–35 s for resolution advisories (RA) [70]. These intervals provide pilots with adequate time to enhance their situational awareness of incoming traffic (TA) and to execute evasive maneuvers (RA). It is thus very important that uncertainty delays do not significantly reduce the reaction time for pilots.

For aircraft in flight, the line-of-sight range corresponds to the distance to the horizon. For typical altitudes that are small in comparison with the radius of the Earth, this can be approximated as follows:

$$\text{LOS range (in NM)} = 1.06 * \sqrt{\text{altitude (in feet)}} \quad (14)$$

In remote and oceanic areas, TCAS establishes a maximum lateral closure rate of 1200 knots (1200 nautical miles (NM) per hour = 2222 km/h) [70], resulting in protected volumes with radii of 16 NM for TA and 11,6 NM for RA (distances corresponding to this closure velocity and the specified time periods for TA and RA). At a cruise altitude of 35 000 ft, the line-of-sight (LOS) range between aircraft is approximately 396,6 NM, providing 19,8 min of transmission time before the aircraft enters the protected volume. In terminal areas, arriving aircraft typically operate between 10 000 and 3000 ft, resulting in a worst-case minimum LOS range of 116,1 NM (both at 3000 ft). With a speed limit of 250 knots and a maximum closure rate of 500 knots, these aircraft will enter LOS range at least 13,9 min before entering each other's protected volumes. In both cases, this is significantly larger than the proposed T_{B2} and T_C periods, which guarantees reception of the required Type B1 and C packets, with high probability, even accounting for the packet loss rates at those distances. Thus, the only significant delay to be considered is the one due to the delayed transmission of the interval keys (T_{B1}), as shown in Table 4.

At distances commensurate with the radii of protected volumes, the probability of packet loss for Type B1 packets is modest and the resulting expected value of Δ_u is less than 3,0 s, for both TA and RA. In other words, the use of CABBA reduces reaction time by at most 3 s, which we deem acceptable compared with the above-mentioned overall reaction times for TA and RA protected volumes.

7.3.3. Uncertainty delays in ATC

In ATC, air traffic controllers utilize interconnected air traffic management (ATM) systems that can communicate with airborne aircraft via digital channels (e.g. ACARS, CPDLC). It is reasonable to expect that these systems will have access to a PKI with aircraft certificates or receive them along with flight plan information. The same can be said of signed keys for the initial interval of a flight, that could be transmitted by the aircraft at the gate. In this case, the primary factor affecting uncertainty delays would be the interarrival time of interval keys, i.e. the parameter T_{B1}.

If the certificate or signed key is unavailable, then the ATM system may have to rely on their transmission by CABBA through Type B1 and C2 packets, with the corresponding authentication uncertainty delay. The impact of this uncertainty will depend on the type and size of airspace being controlled.

Airport control zones (aka "Tower"). A sector centered on an airport, with a typical radius of 5 NM and a maximum altitude of 3000 ft.

Table 4
Packet loss probability and uncertainty times for TCAS. We give the *radius* for the corresponding protected volume, the derived probability p of packet loss at that distance (as per [69]), the resulting expected authentication delay due to interval key transmission $\Delta_u(T_{B1})$, and compare it with the total reaction time as per the TCAS standard [70]. In addition, we compare the time in the LOS range with the expected uncertainty delay for transmission of Type C packets $\Delta_u(T_c)$. Here, we use the parameters for the "worst-case" Scenario 4 of Table 3, i.e. $T_{B1} = 5$ s and $T_{B2} = T_C = 30$ s.

TCAS	Radius	p (%)	$\Delta_u(T_{B1})$ (s)	Time (s)	LOS (min)	$\Delta_u(T_C)$ (s)
TA	6,6–16 NM (12,2–29,6 Km)	8,9	3,0	20–48	13,9–19,8	18,1
RA	5–11,6 NM (9,3–21,5 Km)	6,4	2,9	15–35	13,9–19,8	17,2

Table 5
Packet loss probability and uncertainty times for ATC. We give the *radius* for the corresponding control area, the derived probability p of packet loss, the expected authentication delay for interval key reception $\Delta_u(T_{B1})$, and compare it with the typical radar update rate. We also compare the time in the LOS range with the expected uncertainty delay for Type C packet reception $\Delta_u(T_c)$. We use the same parameters as before, i.e. $T_{B1} = 5$ s and $T_{B2} = T_C = 30$ s.

ATC	Radius	p (%)	$\Delta_u(T_{B1})$ (s)	Update (s)	LOS (min)	$\Delta_u(T_C)$ (s)
Tower	5 NM (9,3 Km)	2,8	3,0	10	13,9	16,3
Terminal	5–40 NM (9,3–74,1 Km)	22,2	4,1	10	28,4	25,0
ACC	100–150 NM (185,2–277,8 Km)	83,3	14,0	10	18,6	82,1

Terminal areas. A inverted-cone shaped sector above the control zone, with up to 40 NM in radius and up to 12 500 ft.

Area Control Center. A large sector, covered by surveillance from a single surveillance installation (radar or ADS-B receiver), typically with a 100–150 NM radius, to ensure that all aircraft in the area are well within minimum LOS range (approx. 140 NM for typical cruise altitudes 18–60 000 ft in class A controlled airspace).

For tower and terminal areas, the LOS range is 58 and 118,5 NM, respectively. With a maximum speed of 250 knots, this results in minimum time in LOS for approaching aircraft of 13,9 and 28,4 min, respectively. For ACC, the LOS range is 140 NM for aircraft in Class A airspace, which at an unrestricted max cruise speed of 450 knots, results in a minimum time in LOS range of 18,6 min. As was the case with TCAS, in all of these cases, these LOS range transition times are widely sufficient for the ADS-B receiver to receive Type B2 and C packets with high probability, even considering the packet loss probabilities for those distances, as shown in Table 5.

As for the uncertainty delay created by the reception of the interval keys, in the case of tower and terminal areas, these are 3,0 and 4,1 s respectively, which compares very favorably with the refresh rate of typical Secondary Surveillance Radar (SSR) installations used for ATC (6 antenna rotations per minute, resulting a 10 s refresh period). The worst case here is that of the ACC, where the delay can be up to 14 s, which remains comparable to the delay found in traditional radar-based infrastructures.

8. Conclusion

In this paper, we have explored the Compatible Authenticated Bandwidth-efficient Broadcast protocol for ADS-B (CABBA), a proposal designed to secure the Automatic Dependent Surveillance - Broadcast (ADS-B) protocol used in aviation. CABBA integrates the TESLA authentication protocol into the application layer of ADS-B. It also incorporates the phase overlay modulation techniques outlined in the Minimum Operational Performance Standard (MOPS) [3] into the physical layer of ADS-B. With these enhancements, CABBA strengthens ADS-B security and ensures the safety of the protocol by complying with the rigorous operational standards set by MOPS.

From an *operational and technical* point of view, CABBA shows promise. On one hand, preliminary tests indicate that the use of phase-overlay modulation techniques (D8PSK) proposed in the MOPS does not affect the capacity of legacy receivers to correctly interpret ADS-B messages. This would enable CABBA-compliant ADS-B hardware to co-exist with legacy ADS-B equipment without compromising safety. On the other hand, simulations using real ADS-B traffic data from high-traffic environments suggest a tolerable channel occupancy rate overhead when deploying CABBA. The results indicate that the bandwidth overhead when using CABBA is very reasonable and should not impede its deployment, even in congested airspace. Moreover, given the hardware and software architecture of most modern avionics systems, transforming legacy ADS-B equipment to support CABBA could probably be done with a firmware and software upgrade (e.g. in avionics using FPGA for signal processing). In such situations, the cost of upgrades and time to availability and certification would be less than a full avionics replacement.

From an *organizational* point of view, however, a robust international public-key infrastructure (PKI) must be established and operated. While there are ICAO ID databases in operations, they do not currently support certificate-based PKI sharing of aircraft public keys. Implementing such a PKI would require global agreement on trustworthy organizations to manage, share, and store aircraft public keys and their certificates. Although this poses a significant challenge, we believe it is doable in the relatively short term. A similar infrastructure exists for the sharing and storage of public keys for electronic Machine Readable Travel Documents (eMRTDs), including biometric passports [71]. It is currently supported by the ICAO Public Key Directory (PKD) with 90 participating countries [72]. We believe this framework could be expanded to include aircraft certificates for authenticating CABBA messages.

In conclusion, for all of these reasons supported by our experimental work and analysis, we believe that CABBA offers the best choice for a quicker deployment of a secure ADS-B solution that meets operational and technological requirements, while simultaneously achieving security and aviation safety objectives.

CRediT authorship contribution statement

Mikaëla Ngamboé: Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Xiao Niu:** Software. **Benoit Joly:** Writing – review & editing, Validation, Supervision, Investigation. **Steven P. Biegler:** Validation, Resources, Investigation. **Paul Berthier:** Methodology. **Rémi Benito:** Writing – review & editing, Validation, Project administration. **Greg Rice:** Writing – review & editing, Validation, Supervision, Resources, Methodology, Investigation. **José M. Fernandez:** Writing – review & editing, Validation, Supervision, Methodology, Investigation, Formal analysis, Conceptualization. **Gabriela Nicolescu:** Writing – review & editing, Validation, Supervision, Resources, Project administration, Funding acquisition, Formal analysis.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author(s) used DeepL, Quillbot, ChatGPT, Grammarly and Turnitin in order to: (1) translate from French and Spanish to English (DeepL), (2) rephrase some sentences from previous work to write the SOTA (Quillbot and ChatGPT), (3) enhance the quality and clarity of specific sentences (ChatGPT), (4) check grammar and spelling mistakes (Grammarly), check for plagiarism (Turnitin). After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Mikaëla Ngamboé reports financial support, equipment and writing assistance were provided by Collins Aerospace. Mikaëla Ngamboé reports financial support and writing assistance were provided by Bombardier. Mikaëla Ngamboé reports financial support was provided by International Air Transport Association. Gabriela Nicolescu reports financial support was provided by Carrillon Information Security. Gabriela Nicolescu reports financial support was provided by Rhea Group. Gabriela Nicolescu reports financial support was provided by Natural Sciences and Engineering Research Council of Canada. Gabriela Nicolescu reports financial support was provided by Centre de Recherche et Inovation en aérospatial du Quebec. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors would like to thank the partners of the CyberSA project: Queen's University, Bombardier, Collins Aerospace, Rhea Group, Carillon Information Security, the International Air Transport Association (IATA), the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Consortium for Research and Innovation in Aerospace in Québec (CRIAQ). Their support has been pivotal in bringing this research to fruition. We sincerely appreciate their collaborative efforts to advance research in the field of avionics systems cybersecurity.

Data availability

The data that has been used is confidential.

References

[1] X. Yang, J. Sun, R.T. Rajan, Aircraft trajectory prediction using ADS-B data, in: Pre-Proceedings of the 2022 Symposium on Information Theory and Signal Processing in the Benelux, 2022, p. 113.

[2] RTCA, Minimum Operational Performance Automatic Dependent Surveillance-Broadcast (ADS-B) and Traffic Information Services-Broadcast (TIS-B), Technical Report DO-260B, Radio Technical Commission for Aeronautics, Washington, DC, 2011.

[3] RTCA, Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B), Technical Report DO-260C, Radio Technical Commission for Aeronautics, Washington, DC, 2020.

[4] ICAO, Doc 4444, Procedures for Air Navigation Services — Air Traffic Management, Technical Report Doc 4444 PANS-ATM, International Civil Aviation Organization, Montréal, QC, 2016.

[5] S. Thompson, D. Spencer, J. Andrews, An Assessment of the Communications, Navigation, Surveillance (CNS) Capabilities Needed to Support the Future Air Traffic Management System, Technical Report, Massachusetts Institute of Technology, Lincoln Laboratory, Cambridge, MA, 2001.

[6] EUROCAE, Technical Specification for the ADS-B Ground Station, Technical Report ED-129, European Organisation for Civil Aviation Equipment, Paris, FR, 2010.

[7] EUROCAE, Technical Specification for a 1090 MHZ Etended Squitter ADS-B Ground Station, Technical Report ED-129, European Organisation for Civil Aviation Equipment, Paris, FR, 2015.

[8] Next Generation Air Transportation System (NextGen), Federal Aviation Administration (FAA), 2022, [Online]. Available: https://www.faa.gov/nextgen.

[9] ICAO, Surveillance of Remotely Piloted Aircraft Systems (RPAS) and Cybersecurity, Tech. Rep. A39-WP/296, Technical Commission Russian Federation, 2016, [Online]. Available: https://www.icao.int/Meetings/a39/Documents/WP/wp_296_en.pdf.

[10] A. Costin, A. Francillon, Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices, Black Hat USA 1 (2012) 1–12.

[11] M.R. Manesh, N. Kaabouch, Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system, Int. J. Crit. Infrastruct. Prot. 19 (2017) 16–31.

[12] M. Strohmeier, M. Schäfer, V. Lenders, I. Martinovic, Realities and challenges of nextgen air traffic management: the case of ADS-B, IEEE Commun. Mag. 52 (5) (2014) 111–118.

[13] L. Ryon, G. Rice, A safety-focused security risk assessment of commercial aircraft avionics, in: 2018 IEEE/AIAA 37th Digital Avionics Systems Conference, DASC, IEEE, 2018, pp. 1–8.

[14] A. Perrig, R. Canetti, J.D. Tygar, D. Song, The TESLA broadcast authentication protocol, Rsa Cryptobytes 5 (2) (2002) 2–13.

[15] A. Perrig, J. Tygar, TESLA broadcast authentication, in: Secure Broadcast Communication, Springer, 2003, pp. 29–53.

[16] C. Finke, J. Butts, R. Mills, ADS-B encryption: confidentiality in the friendly skies, in: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, ACM, 2013, pp. 1–4.

[17] C. Finke, J. Butts, R. Mills, M. Grimaila, Enhancing the security of aircraft surveillance in the next generation air traffic control system, Int. J. Crit. Infrastruct. Prot. 6 (1) (2013) 3–11.

[18] R.S. Huang, H.M. Yang, H.G. Wu, Enabling confidentiality for ADS-B broadcast messages based on format-preserving encryption, in: Applied Mechanics and Materials, vol. 543, Trans Tech Publ, 2014, pp. 2032–2035.

[19] R. Agbeyibor, J. Butts, M. Grimaila, R. Mills, Evaluation of format-preserving encryption algorithms for critical infrastructure protection, in: International Conference on Critical Infrastructure Protection, Springer, 2014, pp. 245–261.

[20] J. Habibi Markani, A. Amrhar, J.-M. Gagné, R. Landry Jr., Security establishment in ADS-B by format-preserving encryption and blockchain schemes, Appl. Sci. 13 (5) (2023) [Online]. Available: https://www.mdpi.com/2076-3417/13/5/3105.

[21] K. Samuelson, E. Valovage, D. Hall, Enhanced ADS-B research, in: 2006 IEEE Aerospace Conference, IEEE, 2006, pp. 7–pp.

[22] T. Kacem, D. Wijesekera, P. Costa, Integrity and authenticity of ADS-B broadcasts, in: 2015 IEEE Aerospace Conference, IEEE, 2015, pp. 1–8.

[23] Z. Feng, W. Pan, Y. Wang, A data authentication solution of ADS-b system based on x. 509 certificate, in: 27th International Congress of the Aeronautical Sciences, ICAS, 2010, pp. 1–6.

[24] A.K. Buchholz, DPP: Dual Path PKI for Secure Aircraft Data Communication (Ph.D. thesis), Virginia Polytechnic Institute and State University, 2013.

[25] J. Baek, Y.-J. Byon, E. Hableel, 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, IEEE, 2013, pp. 358–363.

[26] H. Yang, H. Kim, H. Li, E. Yoon, X. Wang, X. Ding, An efficient broadcast authentication scheme with batch verification for ADS-B messages, KSII Trans. Internet Inf. Syst. (TIIS) (TIIS) 7 (10) (2013) 2544–2560.

[27] H. Yang, R. Huang, X. Wang, J. Deng, R. Chen, EBAA: An efficient broadcast authentication scheme for ADS-B communication based on IBS-MR, Chin. J. Aeronaut. 27 (3) (2014) 688–696.
[28] A. Yang, X. Tan, J. Baek, D.S. Wong, A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification, IEEE Trans. Serv. Comput. 10 (2) (2015) 165–175.
[29] D. He, N. Kumar, K.-K.R. Choo, W. Wu, Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system, IEEE Trans. Inf. Forensics Secur. 12 (2) (2016) 454–464.
[30] G. Thumbur, N. Gayathri, P.V. Reddy, M.Z.U. Rahman, et al., Efficient pairing-free identity-based ADS-b authentication scheme with batch verification, IEEE Trans. Aerosp. Electron. Syst. 55 (5) (2019) 2473–2486.
[31] A. Braeken, Holistic air protection scheme of ADS-B communication, IEEE Access 7 (2019) 65251–65262.
[32] Z. Wu, A. Guo, M. Yue, L. Liu, An ADS-B message authentication method based on certificateless short signature, IEEE Trans. Aerosp. Electron. Syst. 56 (3) (2019) 1742–1753.
[33] A. Asari, M.R. Alagheband, M. Bayat, M.R. Asaar, A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems, Comput. Netw. 185 (2021) 107599.
[34] J. Subramani, A. Maria, R.B. Neelakandan, A.S. Rajasekaran, Efficient anonymous authentication scheme for automatic dependent surveillance-broadcast system with batch verification, IET Commun. 15 (9) (2021) 1187–1197.
[35] H. Yang, M. Yao, Z. Xu, B. Liu, LHCSAS: a lightweight and highly-compatible solution for ADS-B security, in: GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, 2017, pp. 1–7.
[36] P. Berthier, J.M. Fernandez, J.-M. Robert, SAT: Security in the air using tesla, in: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference, DASC, IEEE, 2017, pp. 1–10.
[37] S. Sciancalepore, R. Di Pietro, SOS-securing open skies, in: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, 2018, pp. 15–32.
[38] NIST, Recommendation for Block Cipher Modes of Operation: *Methods for Format-Preserving Encryption*, Technical Report NIST Special Publication (SP) 800-38G Rev. 1, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2019.
[39] Y. Challal, H. Bettahar, A. Bouabdallah, A taxonomy of multicast data origin authentication: Issues and solutions, IEEE Commun. Surv. Tutor. 6 (3) (2004) 34–57.
[40] NIST, Digital Signature Standard (DSS), Standard FIPS PUB 186-4, U.S. Department of Commerce, Gaithersburg, MD, 2013, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.
[41] NIST, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, Technical Report NIST Special Publication (SP) 800-175B Rev. 1, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2020.
[42] NIST, Digital Signature Standard (DSS), Standard FIPS PUB 186-5, (FIPS PUB 186-5) U.S. Department of Commerce, Gaithersburg, MD, 2023, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.
[43] H.C. Van Tilborg, S. Jajodia (Eds.), Encyclopedia of Cryptography and Security, second ed., Springer New York, New York, NY, 2011, http://dx.doi.org/10.1007/978-1-4419-5906-5.
[44] NIST, Recommendation for Key Management: *Part 2 – Best Practices for Key Management Organizations*, Standard NIST SP 800-57 PT . 2 R EV . 1, U.S. Department of Commerce, Gaithersburg, MD, 2019, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf.
[45] A. Shamir, Identity-based cryptosystems and signature schemes, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1984, pp. 47–53.
[46] X. Hu, T. Wang, H. Xu, Cryptanalysis and improvement of a HIBE and HIBS without random oracles, in: 2010 International Conference on Machine Vision and Human-Machine Interface, IEEE, 2010, pp. 389–392.
[47] S.S. Chow, L.C. Hui, S.M. Yiu, K. Chow, Secure hierarchical identity based signature and its application, in: International Conference on Information and Communications Security, Springer, 2004, pp. 480–494.
[48] C. Gentry, A. Silverberg, Hierarchical ID-based cryptography, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2002, pp. 548–566.
[49] A.W. Dent, Certificateless cryptography, in: H.C.A. van Tilborg, S. Jajodia (Eds.), Encyclopedia of Cryptography and Security, Springer US, Boston, MA, 2011, pp. 192–193, http://dx.doi.org/10.1007/978-1-4419-5906-5_314.
[50] NIST, The Keyed-Hash Message Authentication Code (HMAC), MD, Standard FIPS PUB 198-1, U.S. Department of Commerce, Gaithersburg, MD, 2008, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf.
[51] NIST, Recommendation for Applications Using Approved Hash Algorithms, Standard NIST SP 800-107 Rev. 1, U.S. Department of Commerce, Gaithersburg, MD, 2012, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf.
[52] S. Gregory T., Systems and Methods for Enhanced ATC Overlay Modulation, (no. EP 2661039 B1) 2016, [Online]. Available: https://patents.google.com/patent/EP2661039B1.
[53] S. Gregory T., Systems and Methods for Providing an Advanced Atc Data Link, (no. US 20100079329 A1) 2010, [Online]. Available: https://patents.google.com/patent/US20100079329.
[54] O. Yeste-Ojeda, R. Landry, ADS-B authentication compliant with mode-s extended squitter using PSK modulation, in: 2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC). Proceedings, 2015, pp. 1773–8.
[55] A.-Q. Nguyen, A. Amrhar, J. Zambrano, G. Brown, J. Landry, O. Yeste, Application of phase modulation enabling secure automatic dependent surveillance-broadcast, J. Air Transp. 26 (4) (2018) 157–170.
[56] M. Leonardi, M. Maisano, Backward compatible physical layer protocol evolution for ADS-B message authentication, IEEE Aerosp. Electron. Syst. Mag. 35 (5) (2020) 16–26.
[57] A. Doug, Future ADS-B Applications, Technical Report Technical On-Line Workshop for the NAM/CAR Regions (ADS-B/OUT/W), ICAO, 2021, [Online]. Available: https://www.icao.int/NACC/Documents/Meetings/2021/ADSB/P05-FutureADS-B-ENG.pdf.
[58] NIST, Secure Hash Standard (SHS), Standard FIPS PUB 180-4, U.S. Department of Commerce, Gaithersburg, MD, 2015, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.
[59] NIST, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Standard FIPS PUB 202, U.S. Department of Commerce, Gaithersburg, MD, 2015, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf.
[60] S. Sciancalepore, R. Di Pietro, SOS: Standard-compliant and packet loss tolerant security framework for ADS-B communications, IEEE Trans. Dependable Secure Comput. 18 (4) (2019) 1681–1698.
[61] L. Yusupov, ADSB_Encoder.py, 2017, [Online]. Available: https://github.com/lyusupov/ADSB-Out.
[62] J. Sun, The 1090 Megahertz Riddle: A Guide to Decoding Mode S and ADS-B Signals, second ed., TU Delft OPEN Publishing, 2021.
[63] C. Moler, MATLAB version 9.11.0.1873467 (R2021b) Update 3, 2021, [Online]. Available: https://www.mathworks.com/products/matlab.html.
[64] ITU-R, Spectrum Occupancy Measurements and Evaluation, Technical Report Report SM.2256-1(06/2016), ITU, 2016, [Online]. Available: https://www.itu.int/pub/R-REP-SM.2256-1-2016.
[65] J. Sun, J.M. Hoekstra, Analyzing aircraft surveillance signal quality at the 1090 megahertz radio frequency, in: Proceedings of the 9th International Conference for Research in Air Transportation, 2020.
[66] OpenSky, OpenSky raw data, 2018, [Online]. Available: https://opensky-network.org/datasets/raw/protected.
[67] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, M. Wilhelm, Bringing up OpenSky: A large-scale ADS-B sensor network for research, in: Proceedings of the 13th International Symposium on Information Processing in Sensor Networks, IPSN, 2014, pp. 83–94.
[68] T. Kistan, A. Gardi, R. Sabatini, S. Ramasamy, E. Batuwangala, An evolutionary outlook of air traffic flow management techniques, Prog. Aerosp. Sci. 88 (2017) 15–42.
[69] S. Sciancalepore, S. Alhazbi, R. Di Pietro, Reliability of ADS-b communications: Novel insights based on an experimental assessment, in: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, 2019, pp. 2414–2421.
[70] FAA, Introduction to TCAS II Version 7.1, U.S Department of Transportation Federal Aviation Administration, 2011, [Online]. Available: https://www.faa.gov/documentLibrary/media/Advisory_Circular/TCAS%20II%20V7.1%20Intro%20booklet.pdf.
[71] ICAO PKD, ICAO Public Key Directory ICAO PKD White Paper – System Specification for participants, White Paper, ICAO, Montréal, QC, 2020, [Online]. Available: https://www.icao.int/Security/FAL/PKD/Documents/PKDTechnicalDocuments/ICAO%20PKD%20White%20Paper_2020-07.pdf.
[72] ICAO Security and Facilitation, ICAO PKD participants, 2022, [Online]. Available: https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx.