A Secure Broadcast Service for LDACS with Application to Secure GBAS

Nils Mäurer, Maria Caamano, Daniel Gerbeth, Thomas Gräupl
Institute of Communication and Navigation
German Aerospace Center (DLR)
Wessling, Germany
{nils.maeurer, maria.caamanoalbuerne, daniel.gerbeth, thomas.graeupl}@dlr.de

Corinna Schmitt
Research Institute CODE
Universität der Bundeswehr München
Munich, Germany
corinna.schmitt@unibw.de

***Abstract*—The VHF Data Broadcast (VDB) data link, responsible for transmitting Ground Based Augmentation System (GBAS) corrections from the GBAS ground station to the aircraft, is one major bottleneck for the evolution and security of GBAS. It provides limited bandwidth, range, only line-of-sight capabilities and no cyber-security protections for the transmitted data. Hence the use of an alternative data link for GBAS, overcoming these constraints, is desirable. The L-band Digital Aeronautical Communications System (LDACS) has been demonstrated to overcome aforementioned issues. The first demonstration of secure GBAS over LDACS used the Timed Efficient Stream loss-Tolerant Authentication (TESLA) for broadcast authentication of GBAS data. In flight trials, the concept and support of TESLA secured GBAS via LDACS for GAST-D services, supporting category II/III precision approach capabilities, was demonstrated. In this work, different ways are investigated to further optimize latency and security data overhead for an optimized transmission of TESLA secure GBAS packets via LDACS. Initial evaluation show how promising the different options are. Further it is shown how the developed concept for secure GBAS can also be applied to generalized secure broadcast over LDACS.**

***Index Terms*—LDACS, GBAS, TESLA, cyber security, communication performance**

I. Introduction

The Ground Based Augmentation System (GBAS) is used to improve the accuracy and integrity of Global Navigation Satellite Systems (GNSSs) to allow GNSS-based precision approaches and automatic landings landings of aircraft. Several natural phenomena, such as ionospheric scintillations, ionospheric gradient or the troposphere's influence on GNSS signal transmission times, make exact positioning with decimeter accuracy in three dimensions difficult. GBAS reference stations on the ground with precisely known positions can generate correction data based on their received GNSS position and their known, exact position. These corrections, together with associated integrity parameters are broadcast to approaching aircraft. Based on this data, aircraft can calculate their position with up to decimeter precision and, even more important, with integrity bounds on the solution. GBAS enables modern aircraft to perform safe and secure GNSS-based landings while offering advantages over the Instrument Landing System (ILS) commonly used today [6].

GBAS requires a data link to transmit the GNSS corrections to the on-board avionics of the aircraft. As of now, this data link is specific to GBAS: The VHF Data Broadcast (VDB) [20]. The VDB data link has been identified as potentially limiting the evolution of GBAS in several ways [8], [9], [19], [31]. This lead Felux et al. to propose the use of an alternative data link for GBAS [7]: The L-band Digital Aeronautical Communication System (LDACS), which is a general purpose broadband data link for aeronautical communication related to safety and regularity of flight [27]. Flight trials demonstrated LDACS' capability to support GBAS Approach Service Type (GAST) type C and GAST type D with high accuracy, as well as the capability of LDACS to authenticate every GBAS message with the Timed Efficient Stream Loss-tolerant Authentication (TESLA) broadcast authentication protocol [20].

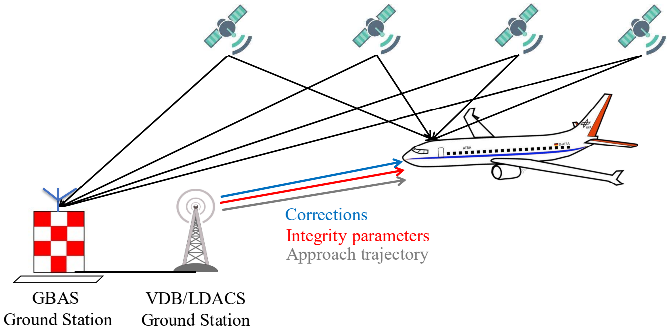


Fig. 1: Basic functionality of GBAS

In the aftermath of these flight trials, Gräupl et al. [11] showed that latency can be improved significantly by optimizing the TESLA parameters for GBAS. As stated in [11] further optimizations (e.g., by lowering the TESLA key disclosure delay d or the time interval T_{int}) are imaginable and LDACS is not limited to GBAS and might serve more broadcast services. Thus, the following two open questions are investigated in the current paper: (I) How to further optimize latency and security overhead for TESLA secured GBAS over LDACS. And (II) how to generalize these optimizations for usage in a multitude of broadcast applications. In order to answer these two questions the objectives of this work are two-folded: (O1) Optimization of latency times and data overhead sizes for TESLA secured GBAS via LDACS and (O2) Presentation of concepts for a broadcast authentication service integrated into LDACS, enabling low data overhead and low latency broadcast

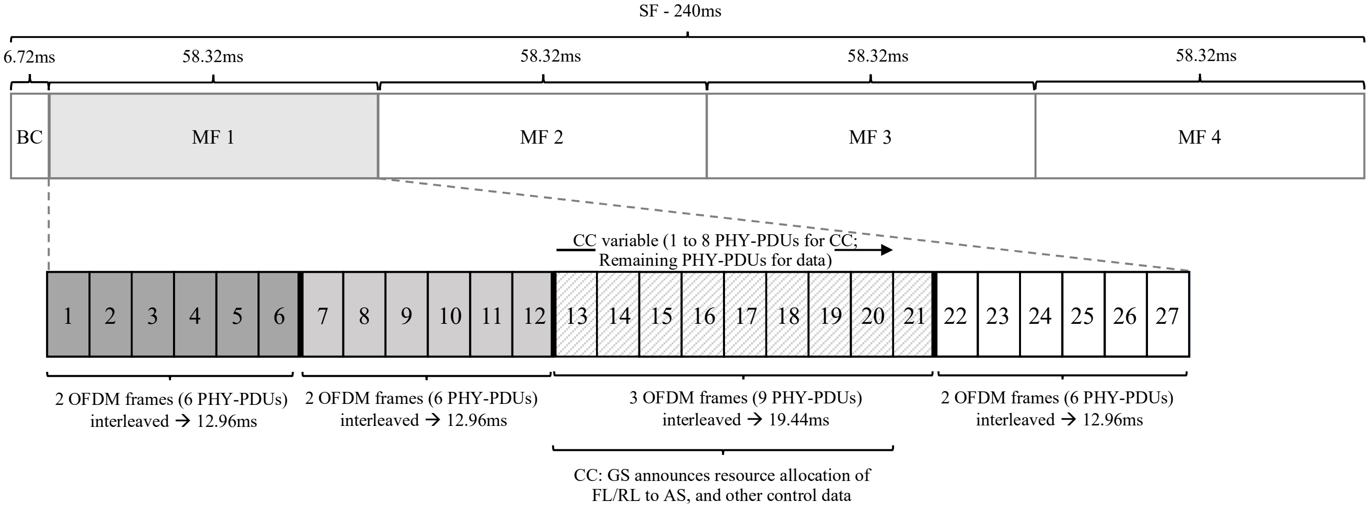

SF - 240ms
6.72ms
58.32ms
58.32ms
58.32ms
58.32ms
BC
MF 1
MF 2
MF 3
MF 4
CC variable (1 to 8 PHY-PDUs for CC;
Remaining PHY-PDUs for data)
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
2 OFDM frames (6 PHY-PDUs) interleaved → 12.96ms
2 OFDM frames (6 PHY-PDUs) interleaved → 12.96ms
3 OFDM frames (9 PHY-PDUs) interleaved → 19.44ms
2 OFDM frames (6 PHY-PDUs) interleaved → 12.96ms
CC: GS announces resource allocation of FL/RL to AS, and other control data

Fig. 2: LDACS FL frame structure and interleaving [13]

authentication solutions.

The paper is structured as followed: Section II includes all required information of LDACS, GBAS, and TESLA to understand why and how the presented solution was realized as described in Section III. The realized optimization solution is evaluated in Sections IV and V from different views. Section VI concludes the paper.

II. Background

In order to understand the realized optimization solution presented in Section III basic knowledge about the involved systems LDACS and GBAS is required. Further, TESLA is presented here, as it is used here to split time into equal intervals and apply a certain key to each interval increasing the security. All this is presented in the following.

A. Characteristics of LDACS

LDACS is a ground-based cellular digital aeronautical communications system for flight guidance and communications related to the safety and regularity of flight [28]. It has been developed in Europe, is currently under standardization in the International Civil Aviation Organization (ICAO) [16] and has been tested in experimental flight trials [20]. It is deployed as a cellular network, where every radio cell has a transmission site, called a Ground Station (GS), which can serve several hundred Aircraft Stations (ASs).

LDACS is a full-duplex communication system with two channels using Orthogonal Frequency-Division Multiplexing (OFDM). The communication channel from ground to aircraft is called Forward Link (FL), while the opposite channel is called Reverse Link (RL). As GBAS data is only transmitted from the ground to the aircraft, only the FL is considered here.

The LDACS specification [13] defines the FL frame structure of LDACS to be organized into recurring Super Frames (SFs) of 240 ms length. Each SF starts with a Broadcast (BC) slot of 6.72 ms length used for control data. It is followed by four Multi Frames (MFs) of 58.32 ms duration. Each MF is structured into 27 Physical Layer-Packet Data Units (PHY-PDUs) á 2.16 ms. Several PHY-PDUs are used for control data in each MF. The Common Control (CC) slot starts always in PHY-PDU 13 and its size can change dynamically according to the current amount of control data from one to eight PHY-PDUs. This is illustrated in Figure 2.

The PHY-PDUs of one MF are interleaved in a given pattern for increased interference robustness. All PHY-PDUs interleaved with each other must be received completely, before data can be successfully extracted. In each FL MF the PHY-PDUs 1 to 6, 7 to 12, 13 to 21, and 22 to 27 are interleaved with each other (cf. Figure 2 [13].

An AS only knows how to interpret data in the FL PHY-PDUs, when it has received the slot allocations in the CC slot. There, the allocations of data within the next MF are announced and only with those an AS knows which data from the GS is intended for it. The LDACS GS can constantly add data to the continuous FL data stream. However, the AS can only interpret received data as addressed to it after the entire reception of the CC slot. Also it has to wait for all interleaved PHY-PDUs to be successfully received, which happens in intervals of six (6×2.16 ms= 12.96 ms) or nine PHY-PDUs (9×2.16 ms= 19.44 ms) as indicated in Figure 2.

The LDACS specification defines different Coding and Modulation Scheme (CMS) schemes for user data, based on the current channel quality and resulting Bit Error Rate (BER). FL PHY-PDUs sizes range from 728, 960, 1080, 1456, 1936, 2176, 2928 to 3296 b, starting at 728 b with the Quadrature Phase-Shift Keying (QPSK) modulation and a convolutional coding rate of 1/2 and ending at 3296 with the 64-Quadrature Amplitude Modulation (64-QAM) modulation and a convolutional coding rate of 3/4 [13]. CC control data of LDACS remains at the lowest CMS scheme for maximum robustness. As mentioned above, 1 to 8 CC slots per LDACS MF are allocated, depending on the amount of AS in an LDACS cell or the current resource allocation scheduling demand by the AS. This allows for 728 to 5.824 b of CC data. Also, depending on the amount of CC slots allocated, the amount of data PHY-PDUs in the MF part three varies from 1 to 8 data PHY-PDUs.

B. Characteristics of GBAS

As explained in section I, GBAS ground stations use the VDB data link to broadcast differential corrections, integrity parameters, and approach path data to arriving aircraft (see Figure 1). Currently, only standards for single-frequency and single-constellation GBAS are available [15]. In this type of architecture, the transmission of Single Frequency and Single Constellation (SFSC) differential corrections for all satellites in view is ensured and the VDB capacity is typically not a problem. However, in addition to the transmission of all the required data, a sufficient VDB coverage must also be provided. This can be especially challenging in complex airports (e.g. Frankfurt), where the use of multiple VDB transmitters could be required in order to fulfil the VDB field strength requirements in the whole GBAS coverage area. In this case, the VDB transmitters operate in different time slots on the same channel. In such a setup, the main limiting factor is to find suitable locations for these additional VDB transmitters within the area of an airport, since GAST-D has other siting constrains associated which could make this task especially difficult. Also the data throughput is reduced inversely proportional to the number of VDB transmitters.

With the evolution of GBAS from a single-frequency single-constellation to a dual-frequency multi-constellation architecture the provision of the required data is a major concern. Different possibilities for future Dual Frequency and Multi-Constellation (DFMC) GBAS architectures are under discussion, each of which has a different impact in terms of required data link capacity. Within the framework of the European project SESAR2020 [29], a first architecture for DFMC called GAST-F has been proposed and a possible associated VDB structure was firstly introduced in [31]. Alternatively, a new concept for DFMC GBAS, which consist of transmitting the raw measurements and shifting most of the processing to the aircraft, has been recently proposed as part of the effort to standardize DFMC GBAS. This alternate concept has less reliance on legacy service processing, which could allow more flexible expansions of GBAS as, e.g., especially the use of a new data link as proposed in this paper.

For the analysis of potential latency improvements, the actual packet formats and packet sizes of current GBAS messages via VDB are essential to be understood. Radio Technical Commission for Aeronautics (RTCA) DO-253D [24] and DO-246D [25]- Minimum Operational Performance Standards (MOPS) for list packet formats do not yet apply to dual frequency, multi-constellation GBAS. For future GBAS operations Stanisak et al. [31] proposed a possible DFMC VDB message scheme, that is summarized in Table I. In this scheme a total of 859 B is required to provide all required information to the airborne users with appropriate update rates.

TABLE I: GBAS Message Type (MT), for number of satellites N and maximum size of message [31]

Packet Name	Packet Size [Byte]
MT2	51
MT50	29
MT42 (N=9)	133
MT1 (N=18)	215
MT4 (FAS)	51
MT11 (N=18)	140
MT50	29
MT1 (N=10)	127
MT11 (N=10)	84 B

From Table I it can be seen that the packet size heavily depends on the amount of observable satellites at any given time. Due to the slot structure of VDB, a message is limited to 222 B which allows single frequency corrections for a maximum of 18 satellites per VDB slot. Still, consecutive 0.5 s VDB frames can contain different satellites as long as the corrections fulfill the requirements in terms of applicability age. In [31] for example, corrections for a second frequency are provided for only 9 satellites per frame.

In the LDACS flight campaign, the use of up to 29 satellites for L1 100 s and 13 satellites for L5 100 s GBAS processing was demonstrated, [20] while providing all corrections at the full 2 Hz update rate. To transmit this amount of data, a dynamic number of 1000 B GBAS packets every half second was applied and, thus, fully utilizing the significantly higher data rate of LDACS. Instead of following the VDB format in Table I, a custom data stream was used as the focus of the demonstration was on the general feasibility of latencies. While the final structure of messages in future DFMC GBAS is still under investigation, e.g. in SESAR2020, payloads of maximum 888 B are likely to be expected in the future due to the implications of the VDB slot structure. Without loss of generality, for this work, further investigations were performed with packets of 859 B size.

C. Characteristics of TESLA

The basic idea of TESLA is to split time into equal intervals and apply a certain key from a cryptographically-linked key chain to each interval. The sender calculates a Message Authentication Code (MAC) for every message using the key of the current interval and applies that MAC, as well as a key from the key chain but from a prior interval, to each message. The key required to verify the current MAC is thus released later in time, making the sender of the message the only one in possession of the most recent key. Only with a certain delay, the recipient receives the required key and can verify the integrity of the attached MAC to a message. Hence, combining symmetric cryptographic measure, MACs and key chains, with a delay in the release of the key creates a signature-like scheme [23].

For TESLA to work properly, sender and receiver must be loosely time-synchronized and TESLA parameters such as interval duration T_{int} or key disclosure delay d must be distributed in an authentic manner. For the purpose of this work, especially the two aforementioned parameters T_{int} and d are important for latency optimizations. For optimizations of the security data overhead, different MAC generating functions, such as Cipher-based MAC (CMAC), Keyed-Hash Message Authentication Code (HMAC), KECCAK Message Authentication Code (KMAC) or *blake2b*/*blake2s*, as well as different key sizes are of interest.

III. Method for Optimizing Latency of TESLA secured GBAS via LDACS

Here, different options for latency and security data overhead optimizations are introduced.

A. Dimensions for Optimizations

Based on results in [11], [20], the following dimensions for optimization were identified:

- **Data Rate:** Overall LDACS provides up to 1428 kbps in the FL, while VDB provides a maximum of 31.5 kbps [25]. One dimension, in which optimize can be performed is the data rate required to transmit TESLA secured GBAS data via LDACS.
- **Timing in LDACS MF:** Another important detail is the analysis of the LDACS FL design and message prioritization method, allowing for a fixed and optimized transmission of TESLA secured GBAS data.
- **Choice of TESLA parameters T_{int}, d:** As identified in [11], [20], the main TESLA parameters to optimize are the time interval T_{int} and the key disclosure delay d.
- **Alignment of LDACS frames and TESLA intervals:** As TESLA requires a loose time synchronization between sender and receiver, the TESLA timing must be aligned with LDACS. In the best case, a key disclosure interval elapses between GBAS messages transmitted via LDACS.

As the data rate of LDACS is sufficient to try out different TESLA approaches, the focus lies on two things:

1) On the optimizing the choice of TESLA parameters T_{int}, d in the context of the LDACS MF and alignment and
2) On the way TESLA and GBAS is integrated into LDACS.

B. Optimizing Key Update Rates of TESLA

The work of Gräupl et al. [11] demonstrated the possibility of improving the latency of TESLA secured GBAS via LDACS relative to the Migration towards Integrated COM/NAV Avionics (MICONAV) flight trials by up to a factor of four. As a result it was concluded that the biggest problem in improving TESLA verification latencies, is the update rate in which GBAS data is sent. In [11], [20], the TESLA key required for verification was attached to each GBAS message, hence the overall TESLA secured GBAS via LDACS latency resulted in the GBAS update rate plus the LDACS transmission latency, assuming that the TESLA key, required for verification, is always sent in the next GBAS update. RTCA DO-253D [24] defines an update rate of 2Hz, hence the best possible cumulative LDACS and TESLA latency is 500 ms plus the LDACS latency [11]. This resulted in a 95-percentile latency of 632.98 ms [11]. However, the shortest key update rate would be transmitting a GBAS message and immediately sending the key update in the following message.

Hash-functions, key sizes and security data overhead:

During MICONAV, the *python3*'s *nacl* [2] crypto-libary with the *blake2b* hash function [26] for MAC key derivation and MAC generation was used. This resulted in a 144 B cryptographic overhead, consisting of 64 B key, 64 B MAC tag and 16 B salt value [20], producing a pre-image-security level of 481 b and a collision-security level of 224 b [14]. Given an overall [17] message size of 859 B, 144 B additional security seems excessive. Thus, other possibilities are investigated in the following:

- *blake2s* offers a pre-image-security level of 241 b and a collision-security level of 112 b [14] by introducing a 32 B key, 32 B MAC tag and a 8 B salt value, hence a 72 B security data overhead.
- Other possibilities are taken from standards from the standardization organ IETF (Internet Engineering Task force) proposing several MAC algorithms: HMAC [18], Cipher-based MAC (CMAC) [30], and KECCAK Message Authentication Code (KMAC) [17].

HMAC has to be used together with a hash-function, where the NIST (National Insitute of Standards and Technology) currently recommends Secure Hash Function (SHA)-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256 [22] or SHA3-224, SHA3-256, SHA3-384, and SHA3-512 [5] for that purpose. Assuming only hash-function from the SHA-2 and SHA-3 family, this results in using SHA-256 or SHA3-256 for 128 b collision resistance and 256 b pre-image resistance. Hence the overhead amounts to a 32 B key and a 32 B MAC tag [1].

CMAC is a MAC based on approved symmetric key block ciphers, such as the Advanced Encryption Standard (AES) [4]. For the purpose of this work, AES was assumed as the underlying block cipher with key-lengths of 128 b, 192 b and 256 b. Hence for a 128 b security level, the cryptographic overhead of AES-128-CMAC is 16 B key and a 16 B MAC tag.

Finally KMAC is a Pseudo Random Function (PRF) and keyed hash function based on KECCAK, which provides variable-length output [17]. It has two variants KMAC128 and KMAC256, which use cSHAKE128 and cSHAKE256 respectively. As the KMAC key length directly influences the security of the scheme, and an attacker can find a key K with $2^{len(K)}$ operations, given a small number of MAC, plaintext pairs, the key must not be shorter than 128 b. In terms of output, KMAC128 security is roughly equivalent to the AES-CMAC scheme, if a 128 b output length of KMAC128 is chosen [17]. With a 256 b input key and a 256 b output tag length, KMAC256 equals the security of HMAC-SHA-256 [17].

Summarizing this all up, means that if a 256 b security level (i.e., based on 256 b preimage resistance) is required, either *blake2s* with 72 B security overhead, *HMAC-SHA-256*/*HMAC-SHA3-256* with 64 B security overhead of *KMAC256* with 64 B security overhead are possible candidates. If a 128 b security level (i.e., based on 128 b pre-image resistance) is required, either *blake2s* with 16 B key and thus 40 B security overhead, AES-128-CMAC with 32 B security overhead, or KMAC with 16 B key and output and, thus, 32 B security overhead are an option.

Therefore, for the proposed optimization in this paper the lowest 32 B security overhead is proposed, hence either AES-128-CMAC or KMAC with 16 B key. With that, a TESLA secured GBAS message is 859 B +16 B +16 B = 891 B long.

Integration of secure GBAS into LDACS framing:

The general idea of reducing latency of TESLA secured GBAS is to send the TESLA key update as soon as possible after the actual GBAS data. For that purpose, 128 b dummy data is generated, a MAC on it calculated and that dummy data, the key update and the MAC sent after the TESLA secured GBAS message.

Following LDACS CMS scheme presented in Section II-A and data sizes per FL Data Channel (DCH) data PHY-PDU, and assuming best CMS, the 891 B TESLA secured GBAS message fits into three FL PHY-PDUs (i.e., $\lceil\frac{7128}{3296}\rceil = 3$). After that, in the next PHY-PDU the key update is transmitted with its 48 B or 384 b size.

With channel quality getting worse, at CMS=3, one interleaved MF part is not sufficient anymore for one TESLA secured GBAS plus the TESLA key update message (i.e., $\lceil\frac{7128}{1080}\rceil = 7 > 6$) and the message needs to be split up into two MF parts. In this case, the first seven PHY-PDUs carry the TESLA secured GBAS and the eighth PHY-PDU the TESLA key update message. Even at worst channel quality at CMS=1 (i.e., FL PHY-PDU block size of 728 b), still two interleaved blocks of six FL PHY-PDU each are sufficient, as $\lceil\frac{7128}{728}\rceil = 11 < 12$. Here 11 PHY-PDUs carry the TESLA secured GBAS and the twelfth PHY-PDUs the TESLA key update message. With that, the optimum latency for TESLA secured GBAS via LDACS is the length of one interleaved MF part, $\triangle L_{FL-MF-part}$, for CMS $\in \{4, 5, 6, 7, 8\}$, or two interleaved MF parts for CMS $\in \{1, 2, 3\}$, a delta for the transmission delay, $\triangle t$, and a delta for the processing delay on receiver end, $\triangle p$.

TESLA parameter choices:

Overall, this idea, sending TESLA secured GBAS data first and then immediately follow up with a key update, requires very exact scheduling on GS side. I.e. GBAS data and key updates must be prioritized high, i.e., via sending GBAS messages with a high LDACS Classes of Service (CoS), the TESLA parameter disclosure delay d must be one and the interval duration must be fairly short.

As the TESLA key schedule must align with the LDACS frame design, T_{int} was initially set to 6 ms. Now it had to be ensured that sending the TESLA secured GBAS part in the first PHY-PDUs and then the TESLA key update in the next PHY-PDU always has a TESLA key update in between those two messages. Further, this had to be checked for every CMS and with every starting position of the TESLA secured GBAS message within the SF of LDACS. If the TESLA secured GBAS message uses the key relevant at the beginning of sending the message for calculating the MAC, then that scheme works. For instance at $CMS = 8$ or $CMS = 7$, sending the GBAS message at the beginning of the first MF with $T_{int} = 6$ ms sets the key at k_1 for calculating the relevant MAC, while the key update in the later PHY-PDU contains the key k_2. For CMS $\in \{4, 5, 6\}$, the key in the key update message is k_3 and for CMS=3 or 2, the key in the key update message is k_4, and finally for CMS=1, the key in the key update message is k_5.

As the key update rate is very small with this scheme, AS and GS have to be synchronized well. As the proposed AES-128-CMAC calculations on a Field Programmable Gate Array (FPGA) have a throughput of 3.80 Gbps with a clock frequency of 302.84 MHz [3], the processing effort would be manageable, making this concept feasible.

C. Realistic Data Transmission Latencies, obtained in MICONAV Flight Trials

The previous analysis only looked at the theoretical possible latencies based on the LDACS frame structure. Here, actual latencies of LDACS FL data, observed in the MICONAV flight trials [20], are analysed. During MICONAV CMS=1 (i.e., FL PHY-PDU block size of 728 b) was used in the flight trials. With GBAS being a broadcast service, only the Unacknowledged (UNACK) data transmission of LDACS is analysed here.

Looking at the MICONAV actual flight data [20], out of 25867 successfully transmitted UNACK packets, 560 of them were transmitted with a latency below 30 ms, ranging from 23.02 ms to 24.53 ms, with a 95-percentile of 24.34 ms. Further, 3152 packets were successfully transmitted and received between 43.54 ms to 46.56 ms, with a 95-percentile of 44.49 ms. Finally, 22103 packets were successfully transmitted and received between 54.11 ms to 67.86 ms, with a 95-percentile of 61.21 ms. Everything is depicted in Fig. 2. In Section II-A the interleaving and FL resource allocation pattern was discussed and as Fig. 3 shows, the shortest latency to be 23.02 ms, which means, that for these shortest-latency-packets the third slot of a MF, the one which carries CC data and user plane data, was used. Hence, the AS receives the FL resource allocation, carried by the CC slot, and is then able to process the following GBAS packet right away.

IV. Results for LDACS DCH use for secure GBAS

In this section, different ways to minimize the latency for TESLA secured GBAS data are investigated. The basic idea is sending TESLA secured data first, immediately followed by a message carrying the required TESLA key of the next interval (Cf. Section III-B).

First, a theoretical optimal latency is presented, followed by a best case scenario, before demonstrating a realistic scenario, based on actual measurement data from the MICONAV flight campaign. Please note, all results assume deterministic scheduling on GS end, such that the TESLA key disclosure for the TESLA secured GBAS data happens within the same

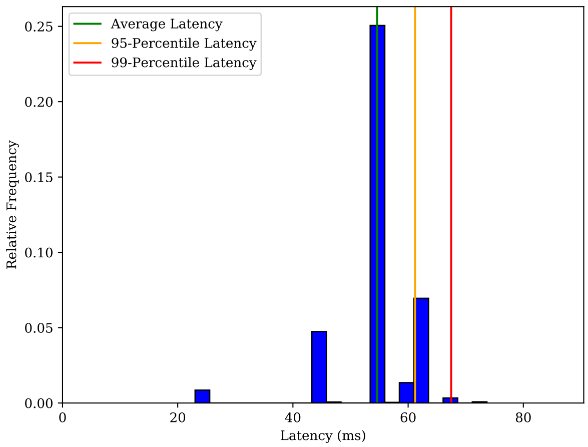


Fig. 3: Relative frequency distribution of LDACS latency in unacknowledged transmission mode obtained during the MICONAV flight trials.

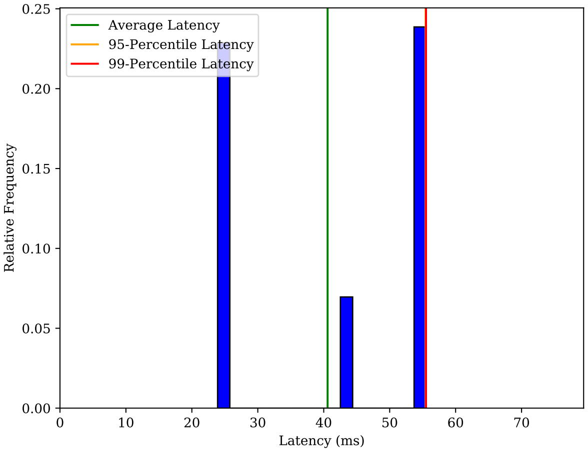


Fig. 4: Relative frequency distribution of LDACS latency in UNACK for 60B to 360B sized packets with high priority. Obtained during the MICONAV flight trials [21].

interleaved LDACS MF part, resulting in TESLA and LDACS latency being equally long. Please also note, that the verification time of the MAC is assumed as zero and a TESLA secured GBAS packet is considered received and verified, once it and the key, disclosed in the next TESLA interval, has reached the AS.

A. Calculation of Optimal Authentication Latency

In Section II-A, the interleaving pattern of LDACS in the FL is discussed. It can be concluded that the shortest interval in which TESLA secured GBAS data can be transmitted, received and verified, are the interleaved PHY-PDU parts, $\triangle L_{FL-MF-part}$, plus a delta for the transmission delay, $\triangle t$, and a delta for the processing delay on receiver end, $\triangle p$. In this subsection, for the sake of discussion, $\triangle p$ and $\triangle t$ are assumed to be 0.

TESLA parameters can be optimized with $d = 1$ and $T_{int} = 6$ ms. Hence, within one interleaved MF part, and LDACS $CMS = 8$, one TESLA secured GBAS message was transmitted in the first three PHY-PDUs, with the fourth PHY-PDU always landing in the next TESLA interval, disclosing the necessary key to verify the GBAS message in PHY-PDU one, two, and three. With all these assumptions, a theoretical optimum transmission and authentication latency for TESLA secured GBAS data via LDACS at $CMS = 8$ is ranging from 12.96 ms - 19.68 ms, depending on the amount of interleaved PHY-PDUs per MF part, with the mean latency being 15 ms and the 95-percentile being 19.50 ms.

B. Estimation of Optimal Authentication Latency in our Implementation

In Section III-C, measurements obtained during the MICONAV flight campaign were discussed. As it could be seen, for Unacknowledged (UNACK) LDACS, hence broadcast transmission, there are very short transmission and processing times possible with LDACS, ranging from 23.02 ms to 24.53 ms. For this best case scenario with possible processing and transmission times, latency for TESLA secured GBAS data via LDACS is ranging from 23.02 ms to 24.53 ms with the mean being 24 ms and the 95-percentile being 24.34 ms.

C. Estimation of Typical Authentication Latency in our Implementation

If a realistic latency for transmission and authentication times for TESLA secured GBAS via LDACS should be obtained, a statistical model of the latency measurements obtained during MICONAV and sort by priority and packet size is required to be build. As GBAS will be a high priority service, need to be found that resembling the size of actual TESLA secured GBAS packets, sized 891 B, plus the necessary TESLA key disclosure packet of 48 B size. Thus, packets of 939 B size are of interest.

In Section III-C, it was mentioned that the most robust CMS of LDACS being used during the MICONAV flight campaign. For the preservation of comparability, the GBAS packet size of 939 B need to be divided by a factor of $4.52\overline{74527}$ as $\frac{3296}{728} = 4.52\overline{74527}$. Keep in mind that the largest LDACS PHY-PDU size is 3296 b at $CMS = 8$ and the smallest is 728 b at $CMS = 1$. Hence for this demonstration of realistic transmission and authentication latencies, packets sized $\frac{939}{4.52\overline{74527}} \simeq 208$ B or 1660 b were of high interest. Unfortunately, no actual packet with that size has been transmitted during MICONAV. In order to receive a good approximation, packets with high LDACS CoS are considered (i.e., high LDACS priority, and range between 60 B to 360 B in size). 54 of 25867 packets were found, matching that selection. Their latency distribution is illustrated in Figure 4.

Hence, a realistic, optimized transmission and authentication latency for TESLA secured GBAS data via LDACS ranges from 23.90 ms to 55.56 ms, with the mean being at 40.59 ms and the 95-percentile at 55.45 ms.

D. Findings

Latency times of just the interleaved LDACS MF part of 12.96 ms to 19.68 ms are obviously not realistic, most of all, as $\triangle p$ and $\triangle t$ were deliberately set to 0, but times ranging from 23.02 ms to 55.56 ms, including transmission $\triangle t$ and packet processing time $\triangle p$, are. With that, optimized LDACS user-data channel based TESLA secured GBAS latency in the 95-percentile of 55.45 ms is possible. However, this strongly depends on several parameters, such as the traffic load in an LDACS cell, the prioritization of GBAS packets, the scheduling at GS, very accurate time synchronization between AS and GS and the overall implementation of interleaved MF packet processing and further data redirection to higher LDACS protocol levels. But this shows, that a further improvement from the 95-percentile of 632.98 ms in [11] by a factor of 11.4 to 55.45 ms is still possible, reducing the overall GBAS transmission and verification times drastically. However, this scheme comes with the drawback, that every time a TESLA secured GBAS packet is sent and immediate key disclosure requested, an additional 48 B, consisting of 16 B dummy data, 16 B key and 16 B MAC, have to be put in the DCH as broadcast message, increasing overall security data overhead. Also the TESLA parameters $d = 1$ and $T_{int} = 6$ ms to enable this low latency, especially the very small T_{int}, can become very expensive in computational overhead.

These drawbacks, originating mainly from the use of the LDACS DCH for TESLA key updates, point to an investigation of using LDACS control channels for that purpose.

V. Results for an LDACS Control Channel based Broadcast Authentication Service

In Figure 2, the frame structure of LDACS is depicted. The LDACS FL has two control channels, the Broadcast Control Channel (BCCH) at the beginning of each SF and the Common Control Channel (CCCH) during each MF. Both are investigated for suitability carrying a TESLA key update and thus enabling a control channel based data broadcast authentication service for LDACS.

A. Secure Broadcast in the Broadcast Control Channel

The BCCH of LDACS occurs every $240ms$ and consists of three slots. BC slot 1 and 3 have 528 b space and are $1.74ms$ long each, BC slot 2 1000 b and $3.24ms$ duration. The LDACS specification defines BC slots 1 and 3 to contain information about adjacent cells and BC slot 2 information about the current cell.

The only mandatory message each SF in BC slot 1,3 is the Adjacent Cell Broadcast (ACB) of 50-662 b size). Other optional messages in these slots are Scanning Table Broadcast (STB) sized between 38 b and 446 b), GS Position Broadcast sized 90-1178 b and GS Service Capability Broadcast sized 28-266 b. In BC slot 2 only the System Identification Broadcast (SIB) message with size 66 b is mandatory. Optionally the Voice Service Broadcast (VSB) sized 77-938 b can be transmitted here. The total size of BC slots is 2056 b and the sum of total mandatory message bits per SF is 728 b.

Offering enough space the TESLA key update is placed in BC slot 2, with the SIB being the message, on which the MAC is built upon. This way, the TESLA secured GBAS message can be sent in any DCH in any of the four MF per SF and then verified with the next broadcast beacon from the GS.

The TESLA parameters of this approach are $d = 1$ and $T_{int} = 240\ ms$, with the beginning of the TESLA interval synchronized again at the very beginning of the LDACS SF. The packet structure is SIB_0, $H_{K_i}(SIB_0)$, $K_{(i-1)}$.

Assuming a uniformly distributed probability of the GS sending a TESLA secured GBAS message in any DCH interleaved MF part, the latency can be calculated. From Section III-C, the possible transmission and processing time of 3.58 ms was taken. The minimum TESLA secured GBAS via LDACS latency for this broadcast authentication service in the BCCH is $12.96\ ms + 1.74\ ms + 3.58\ ms = 18.28\ ms$. This occurs, when the GBAS message is transmitted in the last MF part of the last MF in the SF. The maximum latency for this method is 12×12.96 ms $+4 \times 19.44$ ms $+1.74$ ms $+3.58$ ms $= 238.60$ ms, which happens if the GBAS message is transmitted in the very first interleaved MF part of the first MF. The mean latency of this method is 128.44 ms and 95-percentile latency 228.88 ms.

As for the data overhead, this method appends a TESLA key and a MAC of the SIB. Hence the overhead is 256 b per SF.

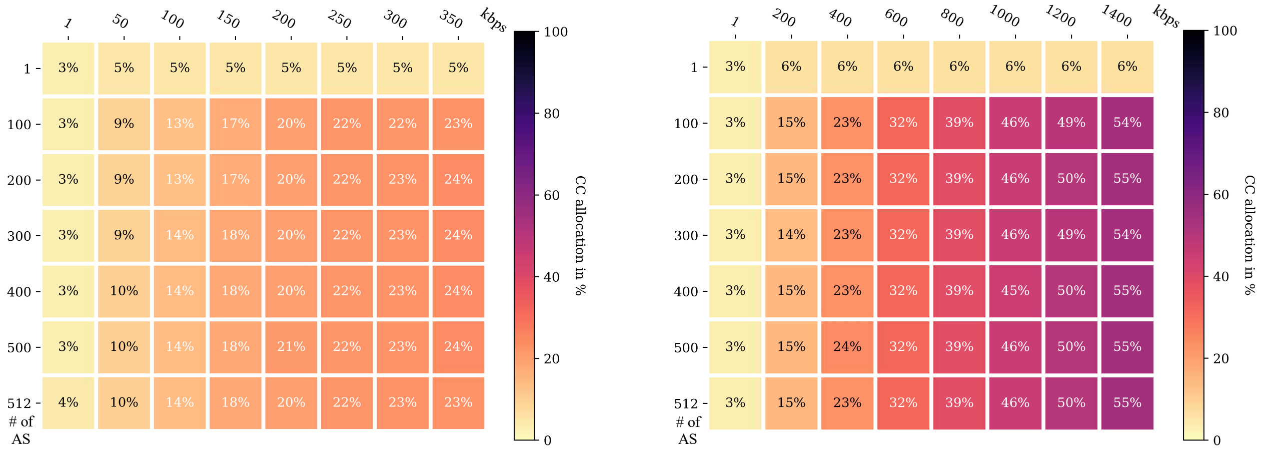
B. Secure Broadcast in the Common Control Channel

As depicted in Figure 2, the CCCH appears in every MF and can vary in length between 1 and 8 PHY-PDUs. First it needs to be investigated, whether there is enough space available in CC slots or if the effectiveness of LDACS would be reduced by placing TESLA data here.

The load on the CC heavily depends on (1) the number of aircraft in an LDACS cell, (2) the current data load in the cell depending on the chosen CMS and the (3) used traffic pattern. High loads on LDACS with $CMS = 1$ and $CMS = 8$ with the FACTS2 (Framework for Aeronautical Communications and Traffic Simulations 2) were simulated [12]:

The number of AS was modeled with #AS $\in$ {1, 50, 100, 150, 200, 250, 300, 350, 400, 450, 500, 512}, the throughput with $CMS = 1$ FL: 728 b per frame) $\in$ {1, 50, 100, 150, 200, 250, 300, 350}, with the maximum LDACS capacity being 315.5 kbps FL and 294.9 kbps RL at $CMS = 1$. For $CMS = 8$ FL: 3296 b per frame, RL: 528 b per tile) $\in \{1, 100, 200, 400, 600, 800, 1000, 1200, 1400, 1600\}$, 12 values were investigated as parameters, with the maximum LDACS capacity being 1428.3 kbps FL and 1390 kbps RL at $CMS = 8$. The used FL traffic pattern consists of 74% small 125 B packets and 26% large 1400 B packets. The RL traffic pattern was modeled with 80% small 125 B packets and 20% large 1400 B packets. It was investigated in [10] this traffic pattern to reflect realistic load for LDACS.

All scenarios were simulated for 1000 s, resulting in a total simulation time at $CMS = 1$ of 96.000 s and $CMS = 8$ of 120.000 s. The 99-percentile results are depicted in Figure 5a



# of AS	1	50	100	150	200	250	300	350
1	3%	5%	5%	5%	5%	5%	5%	5%
100	3%	9%	13%	17%	20%	22%	22%	23%
200	3%	9%	13%	17%	20%	22%	23%	24%
300	3%	9%	14%	18%	20%	22%	23%	24%
400	3%	10%	14%	18%	20%	22%	23%	24%
500	3%	10%	14%	18%	21%	22%	23%	24%
512	4%	10%	14%	18%	20%	22%	23%	23%

(a) CC allocation at LDACS CMS=1

# of AS	1	200	400	600	800	1000	1200	1400
1	3%	6%	6%	6%	6%	6%	6%	6%
100	3%	15%	23%	32%	39%	46%	49%	54%
200	3%	15%	23%	32%	39%	46%	50%	55%
300	3%	14%	23%	32%	39%	46%	49%	54%
400	3%	15%	23%	32%	39%	45%	50%	55%
500	3%	15%	24%	32%	39%	46%	50%	55%
512	3%	15%	23%	32%	39%	46%	50%	55%

(b) CC allocation at LDACS CMS=8

Fig. 5: CC allocation capacity utilization for the 99-percentile case in percentage, depending on number of AS and data load in kbps at lowest and highest LDACS CMS

for $CMS = 1$ and in Figure 5b for $CMS = 8$ and show the percentage of CC allocation over all eight possible CC PHY-PDUs.

With a maximum CC size of $8 \times 728\ b = 5.824\ b$, Figure 5a and 5b clearly show, that the CC is never at capacity limit in the 99-percentile. During all simulations, only in four cases total, more than 7 PHY-PDUs were required to transmit control data. This analysis clearly demonstrates the feasibility to add TESLA verification data within the LDACS CC slot, without reducing LDACS functionality.

The TESLA parameters of this approach are $d = 1$ and $T_{int} = 60$ ms, with the beginning of the TESLA interval synchronized 30 ms before or after the very beginning of the LDACS SF, so just before the beginning of the next CC part. The packet structure is CC_{data_0}, $H_{K_i}(CC_{data_0})$, $K_{(i-1)}$.

Now the latency and data overhead for this method can be calculated: From Section III-C, the possible transmission and processing time of 3.58 ms can be assumed. The minimum TESLA secured GBAS via LDACS latency for this broadcast authentication service in the CCCH is $12.96\ ms + 19.44\ ms + 3.58\ ms = 35.98\ ms$. This occurs, when the GBAS message is transmitted in the second MF part, just before the CC part. The maximum latency for this method is $3 \times 12.96\ ms + 19.44\ ms + 6.72\ ms + 3.58\ ms = 68.62\ ms$, which happens if the GBAS message is transmitted in the very last interleaved MF part of the last MF in a SF. With the possibility of the GS transmitting a GBAS message equally distributed over the LDACS SF, the mean latency of this method is 52.36 ms and the 95-percentile latency 67.16 ms.

As for the data overhead, this method appends a MAC of the CC data and a TESLA key, hence the overhead is 256 b per 60 ms.

VI. Discussions and Conclusions

During the course of this paper, the TESLA secured GBAS via LDACS latency and presented three possible ways of implementing them within LDACS was optimized. In Table II, the different approaches with their individual advantages and disadvantages are compared.

Table II reveals, that placing the TESLA relevant information within the DCH of LDACS, attached to a GBAS message, has the disadvantage, that only this specific message is protected. Or in other words: The latency and data overhead was optimized for that service, e.g., GBAS explicitly and other services within the DCH need to apply their own broadcast protection for timely updates of TESLA keys.

On the other hand, the control plane approaches, in column four and five in Table II, have the advantage, that the TESLA key update happens regularly, regardless of the underlying service that needs the key update. This allows any service that requires broadcast authentication to apply a MAC and a key to its message, and the key update happens either in the BC or CC slot. That way, more than just the GBAS service can benefit from the security of broadcast authentication. This clearly fulfils objective (O2) enabling low data overhead and low latency broadcast authentication solutions for LDACS.

Finally, a look on the different security data overheads, the different three methods presented in this paper generate, was done.

Figure 6 presents this, with BCCH approach requiring 1067 b/s, CCCH 4067 b/s and the DCH approach varying based on number of services and update rates. The ”x”s in Figure 6 show where the DCH approach matches the security overhead of BCCH and CCCH. For example, the DCH approach with one service matches the BCCH one at $240ms$ update rate and the CCCH based one at 60ms. This is expected, as T_{int} for TESLA anchored in BCCH and CCCH was chosen exactly at those values.

During this work, further optimizations of latency and security data overhead for TESLA secured GBAS via LDACS were investigated. Different ways for optimizations were presented, such as the concept of sending an immediate TESLA key

TABLE II: Comparison of TESLA integration approaches within LDACS

Source	Broadcast Authentication Strategy	Mean Latency	P_{95} Latency	Security Data Overhead for securing n services	TESLA parameters
[20]	TESLA message part attached to GBAS data in DCH	1219.52 ms	1287.96 ms	$n \times 144\ B$	$d = 1$, $T_{int} = 1s$
[11]	TESLA message part attached to GBAS data in DCH	617.94 ms	632.98 ms	$n \times 32\ B$	$d = 1$, $T_{int} = 300\ ms$
Section IV	TESLA message part attached to extra message in DCH	40.59 ms	55.45 ms	$n \times 48\ B$	$d = 1$, $T_{int} = 6\ ms$
Section V-A	TESLA message part attached to message in BCCH	128.44 ms	228.88 ms	$1 \times 32\ B$	$d = 1$, $T_{int} = 240\ ms$
Section V-B	TESLA message part attached to message in CCCH	52.36 ms	67.16 ms	$1 \times 32\ B$	$d = 1$, $T_{int} = 60\ ms$

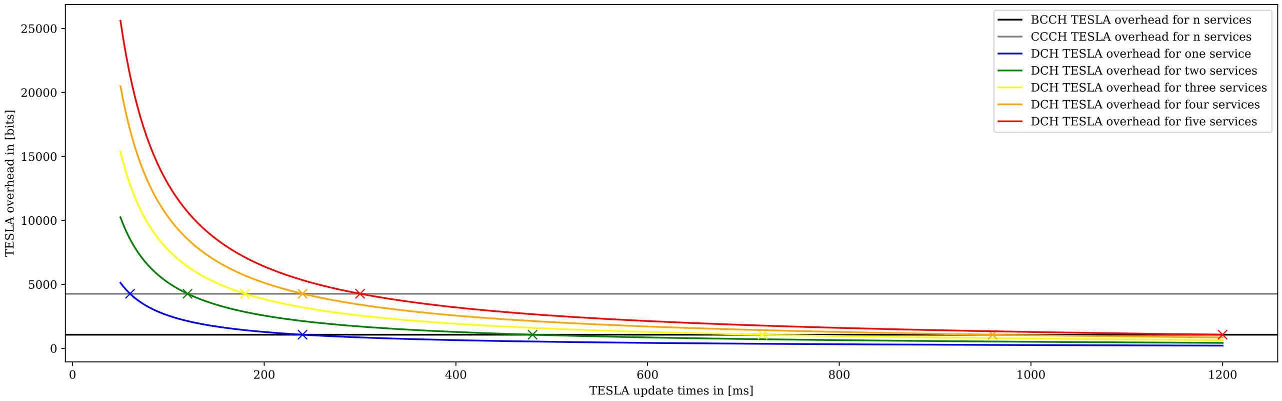


Fig. 6: TESLA induced security data overhead for the three approaches discussed above. Embedding TESLA into one of the two LDACS FL control channels (BCCH, DCCH) is beneficial for high update rates and high numbers of services. For a small number of services or low update rates it is more efficient (area below the BCCH or CCCH line in the graph) for each service to run it's own TESLA instance.

update after a GBAS message in the LDACS DCH and set TESLA parameters to $d = 1$ and a very short $T_{int} = 6\ ms$. With actual transmission times and latencies obtained during an LDACS flight campaign, an estimation for the processing δp and transmission delay δt was found at 3.58 ms. First optimizations for the DCH based scheme were shown with theoretical values at 19.50 ms, then best-case values of 24.34 ms and finally realistic values of $55.45\ ms$, all for the $P_{95\%}$ case. A possibility for TESLA key update within the BCCH and CCCH control channel of LDACS was reached. Both ways are feasible and this enables LDACS to protect an arbitrary amount of broadcast authentication requiring services via the timely key update in either BCCH or CCCH with security data overheads of 1067 b/s, respectively 4067 b/s. By doing so, latencies are optimized to 228.88 ms for the BCCH and 67.16 ms in the CCCH case, both for $P_{95\%}$. All three variations are a latency and data overhead improvement of the work done in [11] and clearly fulfil objective (O1), optimization of latency times and data overhead sizes for TESLA secured GBAS via LDACS.

To conclude, placing TESLA key updates either in the LDACS BCCH or CCCH channel is highly recommended and depends on the requirements of the target application: if update rates of 240ms are acceptable, as is the case with GBAS, then the BCCH approach is recommended. Otherwise it is recommend the CCCH approach for even shorter update rates.

This work shows LDACS's capability to secure an arbitrary amount of broadcast services with very little security overhead and demonstrates a further reduction of TESLA related latencies in LDACS. With a twenty-fold improvement in latency and a 4.5-fold improvement in security overhead, this marks an important step towards the integration of TESLA secured GBAS into LDACS.

Appendix

64-QAM	64-Quadrature Amplitude Modulation
AS	Aircraft Station
BC	Broadcast
BCCH	Broadcast Control Channel
BER	Bit Error Rate
CC	Common Control
CCCH	Common Control Channel
CMAC	Cipher-based MAC
CMS	Coding and Modulation Scheme
CoS	Classes of Service
DCH	Data Channel
DFMC	Dual Frequency and Multi-Constellation
FL	Forward Link
GAST	GBAS Approach Service Type
GBAS	Ground Based Augmentation System
GNSS	Global Navigation Satellite System
GS	Ground Station
HMAC	Keyed-Hash Message Authentication Code
ICAO	International Civil Aviation Organization
KMAC	KECCAK Message Authentication Code
LDACS	L-band Digital Aeronautical Communication System
MAC	Message Authentication Code

MF	Multi Frame
MICONAV	Migration towards Integrated COM/NAV Avionics
MOPS	Minimum Operational Performance Standards
MT	Message Type
OFDM	Orthogonal Frequency-Division Multiplexing
PHY-PDU	Physical Layer-Packet Data Unit
QPSK	Quadrature Phase-Shift Keying
RL	Reverse Link
RTCA	Radio Technical Commission for Aeronautics
SF	Super Frame
SFSC	Single Frequency and Single Constellation
TESLA	Timed Efficient Stream Loss-tolerant Authentication
UNACK	Unacknowledged
VDB	VHF Data Broadcast

References

[1] M. Bellare, "New Proofs for NMAC and HMAC: Security Without Collision-Resistance," in *Annual International Cryptology Conference*. Springer, 2006, pp. 602–619.

[2] D. Bernstein, "Cryptography In NaCl," *Networking and Cryptography library*, vol. 3, p. 385, 2009.

[3] I. Dhaou, T. Nguyen gia, P. Liljeberg, and H. Tenhunen, "Low-Latency Hardware Architecture For Cipher-Based Message Authentication Code," in *IEEE International Symposium on Circuits and Systems*, 2017, pp. 1–4.

[4] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," *National Institute of Standards and Technology (NIST)*, vol. 800, no. NIST.SP.800-38B, pp. 1–21, 2005.

[5] M. Dworkin, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," 2015.

[6] M. Felux, T. Dautermann, and H. Becker, "GBAS Landing System – Precision Approach Guidance After ILS," *Aircraft Engineering and Aerospace Technology*, pp. 1–7, 2013.

[7] M. Felux, T. Gräupl, N. Mäurer, and M. Stanisak, "Transmitting GBAS messages Via LDACS," in *37th Digital Avionics Systems Conference*. IEEE, 2018, pp. 1–7.

[8] T. Feuerle, M. Stanisak, S. Saito, T. Yoshihara, and A. Lipp, "GBAS Interoperability and Multi-Constellation/Multi-Frequency Trials," in *ENRI International Workshop on Air Traffic Management and Systems*. Springer, 2019, pp. 162–174.

[9] J. Garcia, "Broadband Connected Aircraft Security," in *Integrated Communication, Navigation and Surveillance Conference*. IEEE, 2015, pp. 1–23.

[10] T. Gräupl and N. Mäurer, "An Air Traffic Management Data Traffic Pattern for Aeronautical Communication System Evaluations," in *IEEE/AIAA 38th Digital Avionics Systems Conference*, 2019, pp. 1–6.

[11] T. Gräupl and N. Mäurer, "Performance-optimizing Secure GBAS over LDACS," in *21th Integrated Communications, Navigation and Surveillance Conference*. IEEE, April 2021, pp. 1–6.

[12] T. Gräupl, N. Mäurer, and C. Schmitt, "FACTS2: Framework for Aeronautical Communications and Traffic Simulations 2," in *16th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks*, 2019, pp. 63–66.

[13] T. Gräupl, C. Rihacek, and B. Haindl, "LDACS A/G Specification," German Aerospace Center (DLR), Oberpfaffenhofen, Germany, SESAR2020 PJ14-02-01 D3.3.030, December 2020, [Online]. https://www.ldacs.com/wp-content/uploads/2013/12/SESAR2020_PJ14-W2-60_D3_1_210_Initial_LDACS_AG_Specification_00_01_00-1_0_updated.pdf [Accessed: April 13, 2021].

[14] J. Guo, P. Karpman, I. Nikolic, L. Wang, and S. Wu, "Analysis of BLAKE2," in *Cryptographers' Track at the RSA Conference*. Springer, 2014, pp. 402–423.

[15] International Civil Aviation Organization (ICAO), "International Standards and Recommended Practices (SARPs). Annex 10 to the Convention of International Civil Aviation. Volume I -Radio Navigation Aids," International Civil Aviation Organization (ICAO), Tech. Rep., 2017.

[16] ——, "Finalization of LDACS Draft SARPs," International Civil Aviation Organization (ICAO), Tech. Rep., 2018.

[17] J. Kelsey, S.-J. Chang, and R. Perlner, "SHA-3 derived functions: cSHAKE, KMAC, TupleHash, and Parallel Hash," *National Institute of Standards and Technology (NIST)*, vol. 800, pp. 1–185, 2016.

[18] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," 1997.

[19] J. Lee and M. Kim, "Optimized GNSS Station Selection To Support Long-Term Monitoring Of Ionospheric Anomalies For Aircraft Landing Systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 1, pp. 236–246, 2017.

[20] N. Mäurer, T. Gräupl, M. Bellido-Manganell, D. Mielke, A. Filip-Dhaubhadel, O. Heirich, D. Gerbeth, M. Felux, L. Schalk, D. Becker, N. Schneckenburger, and M. Schnell, "Flight Trial Demonstration Of Secure GBAS Via The L-band Digital Aeronautical Communication-System (LDACS)," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 4, pp. 8–17, 2021.

[21] Mäurer, N. and Gräupl, T. and Bellido-Manganell, M.A. and Mielke, D.M. and Filip-Dhaubhadel, A. and Heirich, O. and Gerbeth, D. and Felux, M. and Schalk, L.M. and Becker, D. and Schneckenburger, N. and Schnell, M., "Flight Trial Demonstration of Secure GBAS via the L-band Digital Aeronautical Communications System (LDACS)," *IEEE Aerospace and Electronics Systems Magazine*, 2021.

[22] NIST, "Secure Hash Standard (SHS)," National Institute of Standards and Technology (NIST), Tech. Rep. NIST.FIPS.180-4, August 2015.

[23] A. Perrig and J. Tygar, "TESLA Broadcast Authentication," *Secure Broadcast Communication*, pp. 29–53, 2003.

[24] Radio Technical Commission for Aeronautics, "DO-253D, Change 1, Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment," Radio Technical Commission for Aeronautics (RTCA), DO-253D, 2019.

[25] RTCA, "GNSS-Based Precision Approach Local Area Augmentation System (LAAS) Signal-in-Space Interface Control Document (ICD) Change 1," Radio Technical Commission for Aeronautics (RTCA), DO-246E, 2017.

[26] M.-J. Saarinen and J.-P. Aumasson, "The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)," Internet Engineering Task Force, RFC 7693, 2015.

[27] M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger, "LDACS: Future Aeronautical Communications For Air-Traffic Management," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 104–110, 2014.

[28] Schnell, M. and Epple, U. and Shutin, D. and Schneckenburger, N., "LDACS: Future Aeronautical Communications For Air-Traffic Management," *IEEE Communication Magazine*, vol. 52, no. 5, pp. 104–110, 2014.

[29] SESAR JU, "SESAR2020 PJ14 Final Project Report," https://www.sesarju.eu/sites/default/files/documents/projects/FPR/SESAR2020_PJ14_D1.pdf, European Union, EUROCONTROL, Tech. Rep., December 2019, accessed May 8, 2021.

[30] J. Song, R. Poovendran, J. Lee, and T. Iwata, "The AES-CMAC Algorithm," Internet Engineering Task Force, RFC 4493, 2006.

[31] M. Stanisak, A. Lipp, and T. Feuerle, "Possible VDB Formatting For Multi-Constellation/Multi-Frequency GBAS Services," in *8th International Technical Meeting of the Satellite Division of the Institute of Navigation*, 2015, pp. 1507–1518.