Secure Point-to-Point Long-Distance Multi-Hop Connections in a Dense Airplane Mesh-Network using LDACS

Leonardus J.A. Jansen, Nils Mäurer, Thomas Gräupl
Institute of Communication and Navigation
German Aerospace Center (DLR)
Wessling, Germany
{leonardus.jansen, nils.maeurer, thomas.graeupl}@dlr.de

***Abstract*—The capacity of current aeronautical datalinks is reaching its limits and becomes a hindrance for growth of worldwide civil aviation. To modernize Air Traffic Management (ATM) and digitize aeronautical communications, successors for current technologies are being researched and deployed. The envisioned successor for the VHF Datalink mode 2 (VDLm2) for European air traffic is the L-band Digital Aeronautical Communications System (LDACS). Similar to VDLm2, LDACS is a terrestrial, cellular Air-Ground (A/G) communications system. Contrary to VDLm2, LDACS shall also provide an Air-Air (A/A) communication mode in the future, called LDACS A/A, which operates in a radius of 200 Nautical Miles (NM) for aircraft above altitude of 3000m. Long-distance multi-hop A/A communications could be used to extend the range of LDACS ground stations into oceanic and remote areas, increasing the utility of the terrestrial infrastructure. While LDACS A/G offers sound cybersecurity measures, the development of such for an LDACS A/A extension is currently in its infancy and needs to be investigated thoroughly. One particular design constraint for cybersecurity for aeronautical multi-hop A/A networks is the topology of the underlying mesh network. The objectives of this paper are to investigate (1) the number of concurrent aircraft that are within communication range to each other and (2) the number of hops necessary to cover given distances and (3) to propose possible cybersecurity approaches for LDACS A/A in particular. With actual flight traces data from the OpenSky database for European air traffic, we identify high fluctuations of results based on the time of day and region. The following results were obtained: (1) concurrent aircraft are ranging from 0 to 258, (2) on an exemplary route from Istanbul to Dublin, ranging roughly 3000km, 9 hops were necessary on average with stable routes lasting 1m 21s on average and (3) up to 19% of the total stable connection time is used for establishing a secure Peer-to-Peer (P2P) tunnel via mutual authentication between all hops.**

***Index Terms*—Aeronautical Communications, Air-to-Air, LDACS, Mesh-Network, FANET, Cybersecurity**

I. Introduction

In recent years LDACS, the modern digital alternative to analog VHF aviation communication protocols, has been developed. The LDACS A/G protocol is currently being standardized by ICAO [1] and IETF [2]. Aircraft will use LDACS A/G to securely connect to a Ground Station (GS) and use that connection for the exchange of data related to the safety and regularity of flight. Safety critical data in Air Traffic Management (ATM) consists of Aeronautical Traffic Control (ATC), Aeronautical Traffic Service (ATS) and Aeronautical Operational Control (AOC) data, with LDACS offering enough capacity for future applications such as 4D trajectories. However, this limits the use of LDACS to regions where GSs can be deployed. To have a secure digital connection over Oceanic, Polar, Remote (OPR) areas, LDACS A/A has to be used.

LDACS A/A, however, is in its infancy and only technical proposals have been made [3] [4] [5]. Research has been done on the feasibility of a general ad-hoc mesh network [6] and routing strategies for maximizing the throughput of all nodes within the network such as Geographic Load Share Routing (GLSR) [7]. The focus of this paper is on enabling the airborne internet for ATM by developing secure LDACS A/A.

In LDACS A/G, security is fully implemented. Among its features is a MAKE protocol with a three-way handshake and the use of a full Public Key Infrastructure (PKI) is defined. There is, however, to the best of our knowledge, no research on the security of LDACS A/A yet.

In this paper, we investigate the feasibility of using the state-of-the-art security mechanisms of LDACS A/G in LDACS A/A. To assess whether current security practices in LDACS, such as a three-way handshake are feasible within a plane mesh network to set up a multi-hop tunnel, we investigate the theoretical lower bound of the needed resources. For this, we analyze real air traffic from ADS-B data and analyze the properties of multi-hop routes over long distances with aircraft as hops. The used metrics include the average number of hops per distance and the stability of these routes over time. By analyzing this data, we provide information on the feasibility of establishing such connections given the time constraints, based on real flight patterns.

This paper is structured as follows. In this Section I we introduced the paper. In Section II we give background information the topic and present related work. We describe our methodology in Section III and present the results in Section IV. Section V holds our discussion and we conclude this paper in Section VI.

II. Background

Here we introduce related work on aircraft-aircraft mesh-network research, background on LDACS A/A and LDACS A/G and A/A security considerations, as well as the OpenSky database, and close with a section about multi-hop security.

A. Related Work

In 2008, Medina et al. [6] have shown the feasibility of an ad-hoc network above the North Atlantic corridor by assuming the existence of a communication data link. Their work focuses on routing on the networking level and shows that greedy packet forwarding (i.e., greedy routing) is near-optimal in the needed number of hops, despite being a very simple algorithm. In [8] Medina et al. propose a GLSR algorithm to mitigate congestion in a multihop wireless network.

In 2012 Medina et al. [9] showed that in general a multihop internet connection in an airborne mesh network can have a lower propagation delay than a connection via a geostationary satellite link (250 ms). However, their research does not take into account the establishment of a connection between two nodes, nor overhead from security mechanisms.

The work of Medina et al. [6]–[8] focuses on routing and load sharing. The described protocols and methods work on the networking layer and are therefore link independent. No concrete link was being considered. Now, LDACS has been established as the future communications link for digital aeronautical communications. Therefore, we can now discuss the suitability of the airborne internet as proposed by Medina et al. on top of a real aeronautical datalink. Please note that, in contrast to the work by Medina et al. which envisions enabling an A/A connection for passenger entertainment data, our work is aimed at transmitting safety of flight (i.e., ATM) data via the A/A link.

At FL350, the theoretical maximum range for air-to-air communication is 450 NM [8], however, this can only be achieved with highly directional antennas. A solution to this is beamforming, which has been investigated for the use with LDACS by Gürbüz et al. [10].

Hoffmann et al. [11] propose a protocol architecture for internet connectivity for flight guests. They conclude that routing on the network level is the most efficient way. Barrit et al. [12] propose temporospatial software defined routing. Numani et al. [13] compare topology-based and position-based routing algorithms. They conclude that the position-based algorithm is very susceptible to overloading in terms of throughput and needs lots of administration, as nodes (aircraft) are always moving. The topology-based algorithm outperforms the position-based one in terms of throughput and stability but loses on connection establishment time. Amponis et al. [14] propose a "universal and standardized hardware testbed" [14] to make simulating different routing protocols easier and automatically adjust for "physical-layer related information regarding power consumption" [14]. Hassan et al. [15] propose to install dedicated stationary ships in the ocean to connect to the internet cables lying there. This way, they can act as a router to connect aircraft to the internet. Xue et al. [16] propose to use Dynamic Source Routing, in which "each packet caries [the] complete routing information from source node to destination node" [16]. In their simulations of four different routing algorithms, DSR has the lowest overhead and the second-lowest end-to-end delay. Gurumekala et al. [17] propose a combination of deep learning and fuzzy logic to solve the routing problem in aeronautical ad-hoc mesh networks.

B. LDACS A/G Security

In the domain of LDACS A/G security, many topics were already covered. In [18], the first cybersecurity concept for LDACS A/G was introduced and detailed further several times in following works. However, even the first concept proved very effective in mitigating threats as shown in [19]. In [20] different Mutual Authentication and Key Establishment (MAKE) procedures were compared, including Post Quantum Cryptography (PQC) based options for LDACS and also a completely new MAKE concept, based on Physical Unclonable Functions (PUFs), was investigated for LDACS [21]. The security properties of the LDACS MAKE protocol were in [22]. In [23], cipher-suites, as well as LDACS certificate content was further detailed, concluding in an updated version of a secure cell-attachment for LDACS. As of the development stage of LDACS A/G security as of 2021, a dedicated LDACS PKI is foreseen, with pre-deployed certificates at each end-entity, such as Aircraft Station (AS) and GS. LDACS signatures use Elliptic Curve Digital Signature Algorithm (ECDSA) with Secure Hash-Algorithm (SHA) and elliptic curve point compression for pre-quantum signatures resulting in ECDSA-SHA-256, P-256/brainpoolP256r [24]–[26] curves and 257-bit sized signatures for pre-quantum Security Level (SL) 1 and ECDSA-SHA-384, P-384/brainpoolP384r [24]–[26] and 385-bit sized signatures for pre-quantum SL 2. For post-quantum cases, LDACS relies on FALCON [27]. This results in FALCON-512 and 5,328-bit sized signatures for post-quantum SL 1, and FALCON-1024 and 10,240-bit sized signatures post-quantum SL 2 [23], [27].

LDACS A/G foresees three options for broadcast protection: (a) a group-key based MAC [28] attached to a message, with every recipient having access to that group key being able to verify that the message was sent by someone also in possession of that key, (b) Timed Efficient Stream Loss-tolerant Authentication (TESLA), where the key required to verify attached MACs to a message, is released after a certain time interval, making the sender the only communication member in possession of that key at the previous time interval and essentially achieving asymmetric cryptographic properties with a symmetric scheme and (c) certificate based signatures attached to messages, achieving message origin-authenticity, which can be verified by all aircraft in possession of the sender aircraft certificate.

For point-to-point protection LDACS A/G uses a PKI, certificates, Online Certificate Status Protocol (OCSP), a MAKE protocol and established keys for user- and control-data protection, detailed in [23]. Especially the MAKE protocol is interesting for the LDACS A/A use-case, as it takes time for participants to authenticate to one another and establish keys. Depending on the number of necessary hops in an A/A route, and the time that connection remains stable, different MAKE approaches must be regarded. For the purpose of this work, we use results from [23] and assume that the LDACS A/A MAKE causes similar added latency as for LDACS A/G. As such, a MAKE attempt latency is regarded as 811ms throughout this work (c.f., [20], [23]).

Some of the security concept aspects, such as authentication and key establishment, along with protecting user-data were demonstrated in flights trials and published by Bellido et al. in 2021 [29]. During the same flight trials, the viability of transmitting Ground Based Augmentation System (GBAS) data via LDACS, and securing that transmission with the Timed Efficient Stream Loss-tolerant Authentication (TESLA) broadcast authentication scheme was demonstrated [30]. In follow-up studies, the initial security data overhead was reduced by a factor of 4.5 and the minimal latency by a factor of 22 [31], [32].

These works help pave the way for the standardization of LDACS A/G security and are currently being considered at International Civil Aviation Organization (ICAO) [1] and Internet Engineering Task Force (IETF) [2].

At the time of this writing, there is no publication on LDACS A/A security considerations, which makes this work the first. In the following, the LDACS A/A is introduced.

C. LDACS A/A

The initial idea for an LDACS A/A mode was proposed by the German Aerospace Center (DLR) in 2018 by Bellido [3] being responsible for the initial draft of its design. Use cases mentioned in [3] spread from enhanced situational aware of the aircraft by broadcasting and monitoring Automatic Dependent Surveillance-Broadcast (ADS-B) reports, but also other surveillance concepts such as Automatic Dependent Surveillance-Contract (ADS-C) are viable options. Lastly, LDACS A/A can be used as an extension for beyond Radio Line-Of-Sight (RLOS) communications or used in regions, where terrestrial infrastructure is not available, such as in the OPR domains. The next step after the definition of desired capabilities of LDACS A/A was to design viable Medium-Access Control (MAC) schemes, which were presented in [4] in 2019. Since then, frequency planning took place and was presented in 2021 by Bellido et al. [5].

While development progresses, the demand for security in the LDACS A/A mode, aligning with security ideas for LDACS A/G becomes apparent and hence, this work is designed as a first step in that direction.

D. Ad-hoc Multihop Security

In their 2014 survey, Di Pietro et al. [33] investigated the security risks and requirements for different kind of ad-hoc networks. The different kinds they compare are Wireless Sensor Network (WSN), Unattended WSN (UWSN), Wireless Mesh Network (WMN), Delay Tolerant Network (DTN) and Vehicular Ad-hoc Network (VANET). Di Pietro et al. notice that, although they are all wireless ad-hoc networks, “different network technologies present distinctive features, due to specific requirements and challenges imposed by their application setting” [33]. Our case has the most similarity with VANETs, as in both cases, the nodes (vehicles or aircraft) are moving and therefore the structure of the network changes over time.

Di Pietro et al. notice that the biggest security risks for VANETs are malicious nodes that inject false traffic information, for example to selfishly clear up the way up front or unnecessarily block the road. To protect against this, message authenticity, integrity, and liability are needed, such that messages can be verified and malicious actors can be identified and eventually taken down. Many cryptographic schemes to solve different aspects of the problem are been mentioned, but no algorithm is concluded to be the solution.

Another problem in VANETs, according to Di Pietro et al., is data privacy: speed, trajectories and locations tell a lot about someone’s personal life. Privacy in VANETs means that messages can be sent anonymously such that no datamining can be performed on individuals. This is identified as challenging, as “liability and anonymity are conflicting in nature” [33].

Although the aircraft ad-hoc network has similarities to VANETs, there are distinguishing factors, such as the range of the communication links, the number of expected participants in the network, and the velocity of the nodes (vehicles and aircraft). Therefore, the term Flying Ad-hoc Network (FANET) is used to describe a network consisting of aircraft.

Since no security concept for LDACS A/A exists yet, the following two capabilities seem of particular interest: (1) securing broadcast communications, since LDACS A/A will distribute information to all neighboring aircraft and (2) secure link establishment, ranging from authentication, key establishment to data-protection capabilities, which is important if data shall be transmitted in a point-to-point manner via aircraft over a remote domain to its destination (e.g., ATM related data from London to New York).

III. Methodology

Here, the methodology of this work is introduced. The declared goals are (1) to evaluate the feasibility of security measures to protect broadcast exchanges among neighboring aircraft and (2) to evaluate the feasibility via real air traffic patterns to establish a secure communications channel in a multi-hop ad-hoc network based on aircraft as hops. Similar to LDACS A/G, LDACS A/A is limited in bandwidth to best-case scenarios of 230 - 1400kbps, hence adding significant security additions to a multitude of concurrent connections (i.e., aircraft broadcasting to all aircraft in the vicinity) or to establish a short-lived connection among multiple hops could prove challenging.

To answer these questions the following steps were performed.

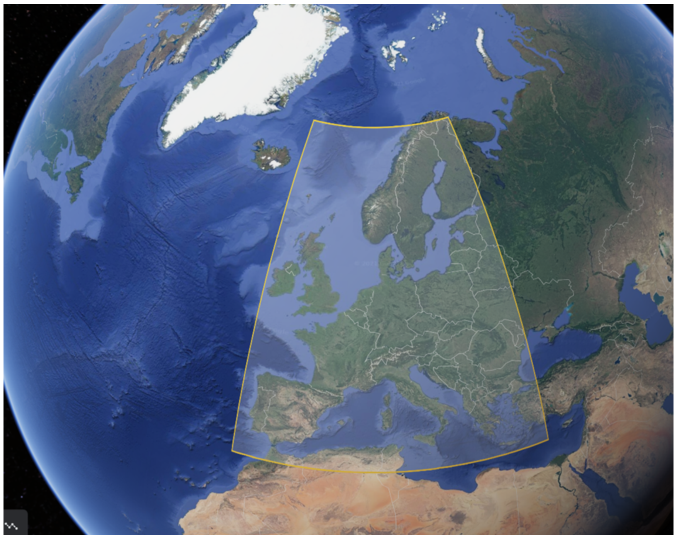


Fig. 1: Selected geographical region for flight traces: latitudes 34 degrees North and 70 degrees North, longitudes 11 degrees West and 30 degrees East.

A. OpenSky Network Data

As mentioned in Section II, the OpenSky [34] database, provides ADS-B and Mode S generated flight data as open source to the research community. Similar to works conducted by Ewert et al. [35], EUROCONTROL released information on recorded Instrument Flight Rules (IFR) flights per year in aggregated form [36] which were consulted to identify interesting days in European air traffic and provide different traffic forecast scenarios for the upcoming years [37]. With 2019 being the busiest year of air traffic so far [38], the 25th of June 2019 has been chosen as one of the busiest days in civil aviation history, according to EUROCONTROL [36].

Data within the OpenSky Network are available in different formats such as aggregated per flight, flight state or unprocessed raw data and timestamp updates with up to second-precision are provided, the data suits our requirements perfectly. Due to flexibility in the database queries, preprocessed position reports have been utilized. As LDACS will be initially deployed within Europe [39], the analyzed data has been restricted within the latitudes 34 degrees North and 70 degrees North as well as the longitudes 11 degrees West and 30 degrees East as shown in Figure 1.

As the available position reports in the OpenSky Network database were not assigned to a particular flight, a preprocessor with the following rules helped retrieve the individual flight paths:

- A flight starts, when the first record for an aircraft's ICAO 24 bit address is detected and no previous active flight is known
- A flight ends, when the aircraft reports *on ground*. Alternatively, if no position report within 15 minutes has been received, the flight is ended as the *on ground* message might not have been received due to e.g., shadowing of the signal near ground.
- As the operation area of LDACS is the En-Route (ENR), only flights reaching an altitude over 10,000 ft are considered.

Having applied the pre-processor, 28,944 complete flight traces were available for this day. The difference to the official EUROCONTROL data, listing 35,270 flights, can be explained geographically, as our evaluation area differs. Areas such as Turkey (3,341 flights), Ukraine (582 flights), Marocco (555 flights), Israel (533 flights), or Cyprus (243 flights) are not (fully) included in our traces, while being part of the official EUROCONTROL data. The remaining difference of 1,072 flights results from incomplete traces or filtering conditions of our preprocessor.

Finally, these 28,944 complete flight traces provide the database for the next computation steps.

B. Aircraft-Aircraft Computations

First, the extracted flight traces needed to be filtered to match the technical descriptions of the LDACS A/A mode: (1) operations within an altitude between 3,000m and 18,000m and (2) within a maximum range of 200 Nautical Mile (NM) of neighboring aircraft. The next steps were performed with the help of Framework for Aeronautical Communications and Traffic Simulations 2 (FACTS2) [40].

First, since the complexity of computing routes meant an exponential complexity in the worst case, reducing the update rate of flight traces helped alleviate computation effort. As such, route updates were streamlined to one minute updates. Next, the target operation area of LDACS A/A was taken into account and the data further updated.

With the dataset prepared like that, distances among aircraft were calculated with the help of the Haversine equation, depicted in Equation 1.

$$d = 2 \cdot r \cdot arcsin(\sqrt{sin^2(\frac{\phi_2 - \phi_1}{2}) + cos(\phi_1) \cdot cos(\phi_2) \cdot sin^2(\frac{\lambda_2 - \lambda_1}{2})}) \quad (1)$$

r is set as radius of the earth with 6,371km, ϕ_1, ϕ_2 as latitude and longitude of point 1, λ_1, λ_2 as latitude and longitude of point 2 and d as the distance between point 1 and point 2 along a great circle of the sphere (i.e., the earth).

a) Number of nearby aircraft computation: With the Haversine equation 1 and minute accurate updates for all 28,944 flights over Europe on 06/25/2019, we computed the number of all neighboring aircraft at a certain point in time on that day in the pre-defined 200 NM radius. Hence, at the end of our calculations, every flight trace update of every aircraft had a list of all neighboring aircraft at that time with the associated relative distance to the aircraft for which neighbors where calculated.

b) Number of aircraft hops for given route: Since, we are mainly interested in the minimum number of aircraft hops for a stable LDACS A/A route between two ground points on the European continent, we implemented a greedy routing algorithm. Since the LDACS A/A scenario assumes the necessity to transmit data between ground points via the

LDACS A/A route, we began by filtering out aircraft in the vicinity of the starting point, within a 140NM radius. We chose this distance as the radio horizon for two differently elevated points can be calculated via Equation 2

$$d = \sqrt{2 \cdot \frac{4}{3} \cdot r \cdot h_1 + {h_1}^2} + \sqrt{2 \cdot \frac{4}{3} \cdot r \cdot h_2 + {h_2}^2} \quad (2)$$

r is set as radius of the earth with 6,371km, h_1 is the antenna height above ground for antenna 1 and h_2 is the antenna height above ground for antenna 2. Assuming that one antenna is at least at 3000m altitude and the other is based on ground the distance is roughly 140NM.

For the aircraft within the 140NM radius across the starting point, the optimal aircraft, i.e., the one with the closest distance to the target is chosen, and then subsequently all following aircraft are calculated from that point, with the respective next hop chosen based on the criteria of being the closest one to the target, in 200NM vicinity to the current hop and in a time range of +/-2 minutes from the investigated point in time. The time range is necessary, as the OpenSky data misses position updates for several points in time, and thus setting a -/+2 minute frame around the investigated point helps alleviate this problem. If no such next hop exists, then the next best hop, i.e., with the second shortest distance to the target is taken as the next hop, and so forth. If a route does not have a start aircraft or never reaches the vicinity, i.e., a 140NM radius around the target, we declare the routing as failed. If an aircraft as hop is visited twice, a circular route has been found and we skip that route and proceed with the next flight in the initial flight list around the starting area.

With the area, that we investigate clarified in Figure 1, we chose start and target points that present major airport and are close the edge of our predefined region. As such the airports of Helsinki at 60.3196 latitude, 24.9682 longitude, Istanbul at 41.2838 latitude, 28.7174 longitude, Athens at 37.9353 latitude, 23.9457 longitude and Dublin at 53.4289 latitude, -6.2642 longitude were of special interest to measure North-South and East-West routes.

Additionally other major airports were investigated for shorter distances: Amsterdam, Bucharest, Copenhagen, Frankfurt, Lisbon, London, Madrid, Oslo, Paris, Rome, Stockholm, Vienna, Warsaw, Zurich.

Please note, routes are established in our evaluations at the same time, so when at a certain point in time a route between Istanbul and Lisbon can be established, it is established at that precise time, for example at 13:32h.

IV. Results

Via the presented methodology in Section III, the following results were obtained.

A. *Number of Concurrent Connections*

As the total number of aircraft operating in 3,000m - 18,000m altitude vastly differs during the day, the same is true for the number of neighboring aircraft. Figure 2a shows the total number of aircraft above 3000m altitude and the mean, 95- and 99-Percentile values for the number of nearby aircraft for all aircraft over the investigated region, set in Section III. Since the number of nearby aircraft is also highly dependent on the geographic location of the investigated plane, only averaged values can be found in Figure 2a. Still we can see the peak of number of aircraft above 3000m is reached at 725 aircraft at 10:03h UTC, along with the mean value for neighboring aircraft at 26 and the 95-percentile value at 67. On the other hand, at remote locations or early or late periods in the day, no neighboring aircraft were detected as a minimum value.

Figure 2b shows flight EZY82CP near London at 13:32h UTC, as here the total maximum of concurrent possible connections with 258 neighboring aircraft were detected.

Essentially these result helps us answering (1) "to evaluate feasibility of security measures to protect broadcast exchanges among neighboring aircraft" from Section III.

B. *Number of Hops for Multi-Hop Connection*

With the greedy routing algorithm described in Section III-B, different routes were tested for various airport as start- and endpoints of communications.

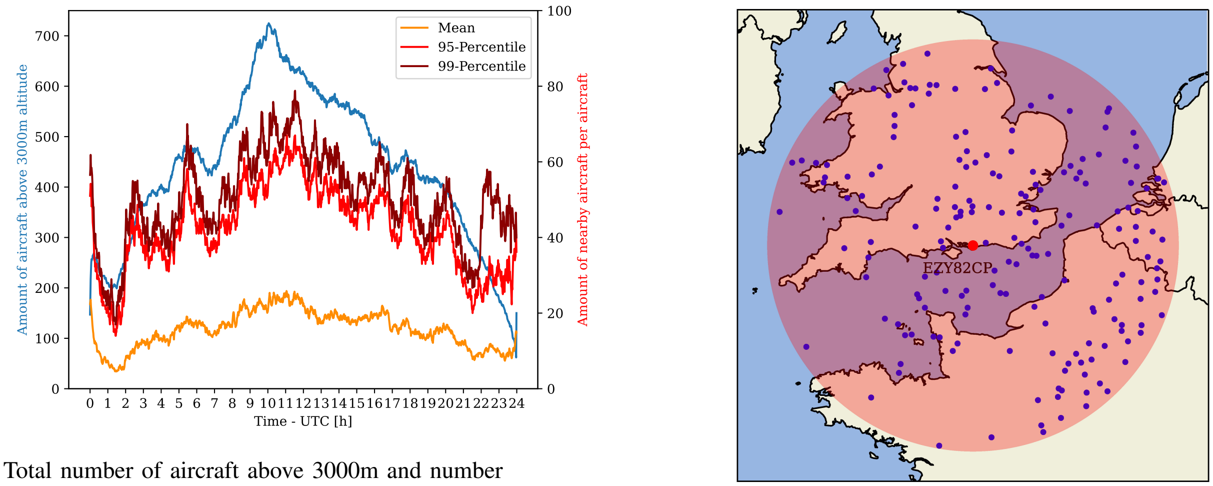
On the West-East axis, values for a route Istanbul-Dublin can be found in Figure 3a. On average 9.38, and in the 95-percentile 11 hops are necessary for the connection to be established, with a minimum value of 8 and maximum value of 13 hops. On the other hand, these specific connections are not long lived, with their minimum stable route duration of 1 minute, a mean value of 1.35, a 95-percentile value of 3 and a maximum of 23 minutes. On the other hand any route between Istanbul to Dublin was possible in 94.375% of all cases.

On the South-North axis, values for a route Athens-Helsinki can be found in Figure 3b. Here a minimum of 7, a mean value of 9.58, a 95-percentile case of 12 and a maximum value of 13 hops are necessary to successfully transmit data. Stable connection duration have a minimum value of 1, a mean value of 1.17, a 95-percentile value of 2 and a maximum of 10 minutes. Overall, a route can be established successfully in 49.44% of all cases.

To get a better view on how the actual routes look like, Figure 4a and 4b show the actual routes for min, mean and maximum hop numbers from the statistical results depicted in Figure 3a and 3b.

Since we investigated more airports than the previously depicted four (c.f., Figure 3), we also obtained interesting results for stable route duration and successful connection establishment rates: With a stable duration time of 22.15 minutes on average, the connection Istanbul to Bucharest via 1 to 5 hops, was the most stable one in our evaluations. Lastly, the most reliable route establishment observed in our experiments took place between Amsterdam-London with 99.2% connection establishment success rate.

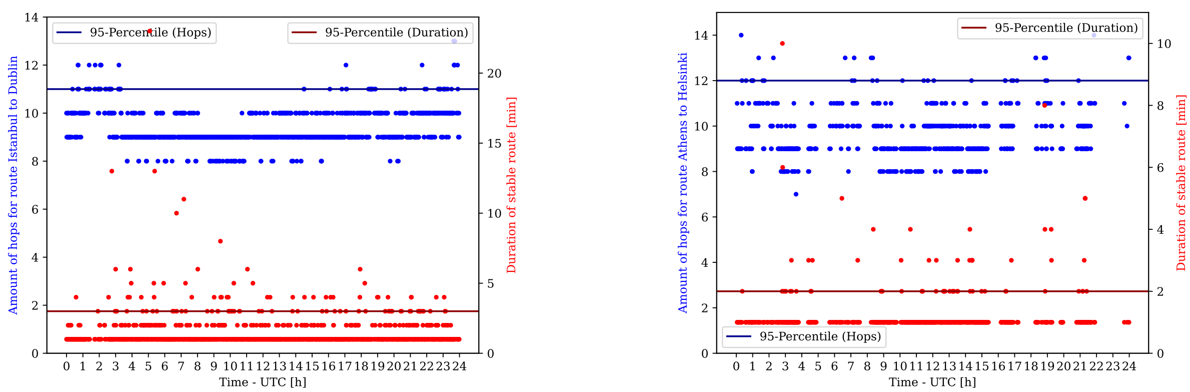
Essentially these result helps us answering (2) "to evaluate the feasibility via real air traffic patterns to establish a secure communications channel among multi-hop ad-hoc network



(a) Total number of aircraft above 3000m and number of concurrent connections for aircraft to nearby aircraft on average, in the 95- and 99-Percentile case. Minimum connection number is 0 and maximum is 258.

(b) Flight EZY82CP near London at 13:32h UTC with 258 neighboring aircraft in a 200NM radius.

Fig. 2: Results for the number of neighboring aircraft at a certain point in time.



(a) Number of hops between Istanbul and Dublin, along with stable connection duration in minutes, hence the time until one hop move out of reach of each other.

(b) Number of hops between Athens and Helsinki, along with stable connection duration in minutes, hence the time until one hop move out of reach of each other.

Fig. 3: Results for the number of hops for a route between two geographical points.

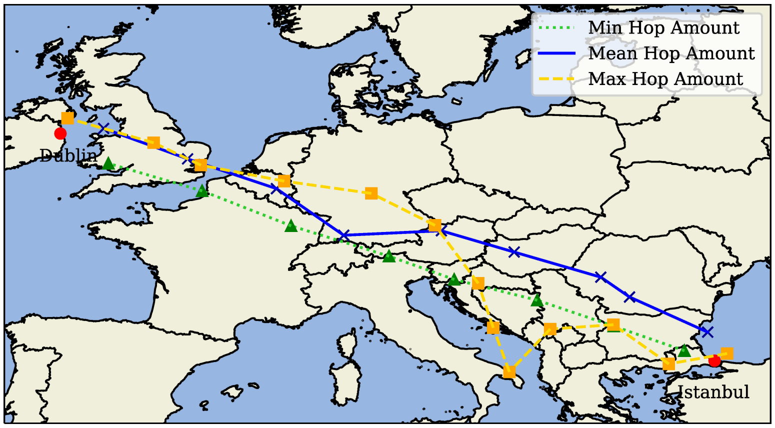
based on aircraft as hops" from Section III. These results provide the baseline to answer (1) and (2) in the next Section.

C. *Feasibility of Security Concepts*

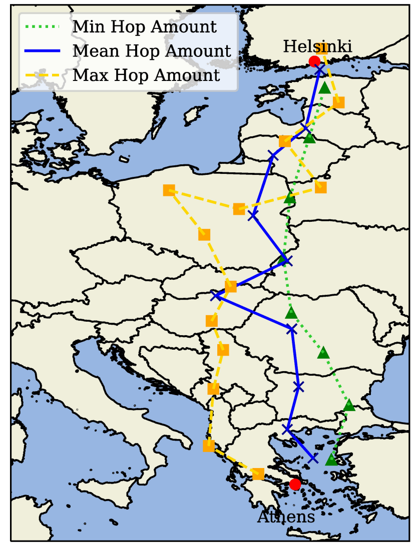
Here we discuss the feasibility of the envisioned security concepts for the L-band Digital Aeronautical Communications System (LDACS) A/A link based on the measured values in Section IV-B. First we discuss the feasibility of broadcast signatures, then multi-hop Peer-to-Peer (P2P) tunnels.

a) Broadcast Signatures: We see that over the course of the examined day on 2019-06-25, there is a mean peak value of 26, a 95-Percentile peak value of 67, and a maximum peak value of 258 for concurrently visible aircraft above FL 100 in the range of the one investigated aircraft. It is not feasible, nor necessary, to establish a direct tunnel to every aircraft to send out secured broadcast messages. For aeronautical services, based on broadcast messages, such as ADS-B, Traffic Collision Avoidance System (TCAS), GBAS or voice communications with party-line effect, we argue the confidentiality of a message does not need to be protected. However, the integrity and authenticity, do. Therefore, *we propose to use certificates to create signatures for protected broadcast messages*. As explained in Section II-A, LDACS certificates are pre-deployed at the AS and the certificates themselves are relatively small (in the order of a few 100 Bytes for pre-quantum and several 100 Bytes for post-quantum [23]). Our focus here, however, is the signature size as given in Section II-B.

As an example application, we assume ADS-B with one message transmission per second. We have seen that on a busy day, an aircraft is in range of up to 258 other aircraft. For the



(a) Routes from Istanbul to Dublin.
8 hops for minimum route at 20:16h,
9 hops for mean route at 23:20h,
13 hops for maximum route at 23:39h.



(b) Routes from Athens to Helsinki.
8 hops for minimum route at 02:58h,
10 hops for mean route at 03:16h,
13 hops for maximum route at 01:20h.

Fig. 4: Routes for min, mean and maximum hop number between two points in Europe.

use case of ADS-B, this means that this aircraft will receive up to 258 ADS-B messages per second. In Table I we show the sizes of the signatures, as they are used in LDACS A/G. Given the peak number of visible hops at the same time, we calculate the expected accumulated size of all signatures that an aircraft receives per second, i.e., with one message per second and a maximum of 258 aircraft. For the link throughput, LDACS A/G offers a worst-case 230 kbps and best-case 1400 kbps. For LDACS A/A, we assume the same rates [4].

From this, we can see that with a slow connection 28.2% and 42.2% of the channel capacity would have to be used for LDACS signatures on pre-quantum SLs 1 and 2 respectively. As the post-quantum signatures are a lot bigger, they require a lot more channel capacity. We see that for post-quantum SL 2, 184.2% channel capacity would be needed best-case and 1,121.7% channel capacity worst-case for transmitting certificates only. In our worst case, with one-second message updates for 258 aircraft, it is therefore not feasible to have a signature on every message on post-quantum SLs. Only on pre-quantum SLs with a best-case connection case, there is an acceptable proportion of the channel capacity required for adding a signature to every message.

b) P2P Tunnels: To establish a multi-hop tunnel over a long distance, a connection from and to every individual hop hop needs to be set up. As pointed out in Section IV-B, we have investigated two example routes: Istanbul to Dublin (i.e., East-West) and Athens to Helsinki (i.e., South-North). As seen in Figure 4a, a minimum of 8 hops, a mean of 9 and a maximum of 13 hops are necessary for a Istanbul to Dublin route. Figure 4b depicts routes for Athens to Helsinki with 8, 10 and 13 hops as minimum, mean and maximum values.

As LDACS A/A does not yet exist, there are no real-life measurements for LDACS A/A yet regarding latency and we, therefore, for now, assume it to have the same latency for connection establishment as LDACS A/G, which is 811 ms (c.f., Section II-B). To this, 60 ms have to be added, because this is the length of a frame in LDACS and therefore this time is guaranteed to pass until the secure connection establishment to the next hop can be started [39]. This totals in a latency of at least 871 ms for every hop.

On a busy day in the early morning the best case on the Istanbul to Dublin route was observed. The connection is stable for up to 23 minutes and requires 10 hops, resulting in a connection establishment time of 10×871 ms $= 8.71$ seconds, which only takes approximately 0.57% of the time that a connection is theoretically possible to establish that connection. The average case, with a stable connection time of 1.35 minutes and 9 hops, takes 9×871 ms $= 7.839$ seconds, hence requires approximately 9.7% of the total possible communication time. In the worst case, a connection is only stable for one minute and takes 13 hops to establish. Connection establishment time is 13×871 ms $= 11.323$ seconds, hence requires 18.9% of the total possible communication time.

We see that the route Athens-Helsinki is less stable. Over the whole day, not even half of the time (49.44%) could a route be established. The best case was observed with a stable connection time for at most 10 minutes, with 10 hops. With a connection establishment time of 10×871 ms $= 8.71$ seconds, therefore, it takes about 1.5% of the total theoretically available connection time in the best case. The

	Pre-Q SL 1	Pre-Q SL 2	Post-Q SL 1	Post-Q SL 2
Signature size in bit	257	385	5,328	10,240
Expected incoming in kbps	66.31	99.33	1,374.62	2,641.92
channel capacity needed in % (worst case, 230 kbps)	28.8	43.1	597.6	1,148.7
channel capacity needed in % (best case, 1400 kbps)	4.7	7.1	98.2	188.7

TABLE I: Expected number of signature related kbps for pre-quantum and post-quantum LDACS SLs [23] in the worst case with a maximum of 258 connections and one message per aircraft per second.

average value with 1.17 minutes stable connection duration and 10 hops costs 12.4% of total communication time. The worst case is similar to the Istanbul to Dublin route with 1 minute connection duration and 13 hops resulting in a connection establishment cost of 18.9%.

V. Discussion

In our results, the 811 ms LDACS A/G secure connection establishment time is asssumed [20]. However, this is a four-way handshake MAKE protocol and connection establishment could be sped up by using a three-way handshake. We, therefore, expect that the connection establishment time can be brought down by roughly 25% removing one MAKE message from the secure connection establishment protocol.

Medina et al. focus their work on the area of the North Atlantic Corridor (NAC), where there are two bursts of flights every day: one eastward and one westward [7]. As a result, connections established in that area tend to be very stable over time, because the aircraft are likely to fly in the same direction. In our work, however, we use flight data from the European continental area where aircraft fly all-over in a vast variety of directions, instead of a relative two. Therefore, it is to be expected that the connections in our work do not hold as long as those over the NAC.

The used signature schemes from LDACS A/G can not simply be copied into an LDACS A/A specification. We see in Table I clearly, that for Post-Quantum SLs of up to 11 times the channel capacity would be needed just for sending the signatures, message content not yet included. Even for the Pre-Quantum SLs, up to 42.2% of the channel capacity would be needed for the signatures alone (again assuming a maximum of 258 concurrent connections and a message update rate of 1 Hz). It is clear that for message integrity to be ensured in LDACS A/A, other cryptographic schemes will have to be proposed or designed that take into account the available channel capacity.

VI. Conclusion

We have used real flight data from the OpenSky database to analyze the number of aircraft within range of each other in a 200 NM radius. Based on this information and the signature sizes used in LDACS A/G, we showed that only with a best case connection and with the pre-quantum signature schemes, it is feasible to sign every broadcast message. If the channel does not provide the optimal capacity or Post-Quantum signatures are used, in a crowded area it is not feasible anymore to transmit and receive a signature on every message assuming a one second update rate for each message from each aircraft.

By calculating the number of hops needed for a long distance multi-hop P2P tunnel and using actual connection establishment times from LDACS A/G measurements, we were able to estimate the duration of a connection establishment for the whole tunnel. We found that in the best case for an example case between Istanbul and Dublin, a connection of 10 hops was stable for 23 minutes. It only requires 0.57% of the theoretically available connection time to establish that connection. In the worst case, a route consisting of 13 hops only holds for 1 minute, resulting in a required 18.9% time cost for connection establishment.

In this work, we assumed that a P2P connection has to be completely re-established, as soon as one hop fails. In future work we will assess the possibility to speed up the connection re-establishing process by reusing partly intact connection.

In case of both investigated route examples (Istanbul to Dublin and Athens to Helsinki), we see that most connections only hold up for 1 minute, which is the time resolution of our data. Therefore, to do more precise claims on the connection time, a future work can assess the data with a higher time resolution.

Acronyms

ADS-B Automatic Dependent Surveillance-Broadcast
ADS-C Automatic Dependent Surveillance-Contract
AOC Aeronautical Operational Control
AS Aircraft Station
ATC Aeronautical Traffic Control
ATM Air Traffic Management
ATS Aeronautical Traffic Service
DTN Delay Tolerant Network
ECDSA Elliptic Curve Digital Signature Algorithm
ENR En-Route
FACTS2 Framework for Aeronautical Communications and Traffic Simulations 2
FANET Flying Ad-hoc Network
GBAS Ground Based Augmentation System
GLSR Geographic Load Share Routing
GS Ground Station
ICAO International Civil Aviation Organization
IETF Internet Engineering Task Force
IFR Instrument Flight Rules
LDACS L-band Digital Aeronautical Communications System

MAKE	Mutual Authentication and Key Establishment
NAC	North Atlantic Corridor
NM	Nautical Mile
OCSP	Online Certificate Status Protocol
OPR	Oceanic, Polar, Remote
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptography
RLOS	Radio Line-Of-Sight
SHA	Secure Hash-Algorithm
SL	Security Level
TCAS	Traffic Collision Avoidance System
TESLA	Timed Efficient Stream Loss-tolerant Authentication
UWSN	Unattended WSN
VANET	Vehicular Ad-hoc Network
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network

References

[1] ICAO, "CHAPTER 13 - L-Band Digital Aeronautical Communications System (LDACS)," International Civil Aviation Organization (ICAO), INTERNATIONAL STANDARDS AND RECOMMENDED PRACTICES - ANNEX 10 - AERONAUTICAL TELECOMMUNICATIONS VOLUME III – COMMUNICATION SYSTEMS, Mar. 2022, work in Progress. [Online]. Available: https://portal.icao.int/CP-DCIWG/ACPWGF/SARPSDevelopment/DevelopmentofFInalSARPS/LDACS_DraftFinalSARPs20220331(002).docx

[2] N. Mäurer, T. Gräupl, and C. Schmitt, "L-band Digital Aeronautical Communications System (LDACS)," Internet Engineering Task Force, Internet-Draft draft-ietf-raw-ldacs-10, Mar. 2022, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-raw-ldacs-10

[3] M. A. Bellido-Manganell, "Design Approach of a Future Air-to-Air Data Link," in *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, 2018, pp. 1–9.

[4] M. A. Bellido-Manganell and M. Schnell, "Towards Modern Air-to-Air Communications: the LDACS A2A Mode," in *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*, 2019, pp. 1–10.

[5] ——, "Feasibility of the Frequency Planning for LDACS Air-to-Air Communications in the L-Band," in *2021 Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2021, pp. 1–14.

[6] D. Medina, F. Hoffmann, S. Ayaz, and C.-H. Rokitansky, "Feasibility of an Aeronautical Mobile Ad Hoc Network Over the North Atlantic Corridor," in *2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2008, pp. 109–116.

[7] D. Medina, F. Hoffmann, F. Rossetto, and C.-H. Rokitansky, "North Atlantic Inflight Internet Connectivity via Airborne Mesh Networking," in *2011 IEEE Vehicular Technology Conference (VTC Fall)*, 2011, pp. 1–5.

[8] ——, "Routing in the Airborne Internet," in *2010 Integrated Communications, Navigation, and Surveillance Conference Proceedings*, 2010, pp. A7–1–A7–10.

[9] ——, "A Geographic Routing Strategy for North Atlantic In-Flight Internet Access Via Airborne Mesh Networking," *IEEE/ACM Transactions on Networking*, vol. 20, no. 4, pp. 1231–1244, 2012.

[10] A. Gürbüz, D. M. Mielke, and M. A. Bellido-Manganell, "On the Application of Beamforming in LDACS," *ICNS 2022*, 2022.

[11] F. Hoffmann, D. Medina, and A. Wolisz, "Protocol architecture analysis for Internet connectivity in aeronautical ad hoc networks," in *29th Digital Avionics Systems Conference*, 2010, pp. 3.C.4–1–3.C.4–12.

[12] B. Barritt, T. Kichkaylo, K. Mandke, A. Zalcman, and V. Lin, "Operating a UAV mesh amp; internet backhaul network using temporospatial SDN," in *2017 IEEE Aerospace Conference*, 2017, pp. 1–7.

[13] A. Numani, S. J. Nawaz, and M. A. Javed, "Architecture and Routing Protocols for Airborne Internet Access," in *2018 IEEE International Conference on Consumer Electronics - Asia (ICCE-Asia)*, 2018, pp. 206–212.

[14] G. Amponis, T. Lagkas, P. Sarigiannidis, V. Vitsas, and P. Fouliras, "Inter-UAV Routing Scheme Testbeds," *Drones*, vol. 5, no. 1, 2021. [Online]. Available: https://www.mdpi.com/2504-446X/5/1/2

[15] N. Hassan and N. M. Khan, "Cost-effective reliable transmission service for Internet of Flying Things," *International Journal of Distributed Sensor Networks*, vol. 17, no. 6, p. 15501477211017820, 2021.

[16] X. Xue, J. Cao, G. Meng, P. Zheng, and L. Gao, "Evaluation of Routing Protocol for Aircraft Ad Hoc Networks Communication," in *2021 Cross Strait Radio Science and Wireless Technology Conference (CSRSWTC)*, 2021, pp. 301–303.

[17] T. Gurumekala and S. Indira Gandhi, "Toward in-flight Wi-Fi: a neuro-fuzzy based routing approach for Civil Aeronautical Ad hoc Network," *Soft Computing*, no. 1433-7479, pp. s00 500–021–06 677–2, 2022.

[18] N. Mäurer and A. Bilzhause, "A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)," in *37th Digital Avionics Systems Conference (DASC)*, 09 2018, pp. 1–10.

[19] N. Mäurer and C. Schmitt, "Towards Successful Realization Of The LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- And Risk Analysis," in *19th Integrated Communications, Navigation and Surveillance Conference*. IEEE, 2019, pp. 1–13.

[20] N. Mäurer, T. Gräupl, and C. Schmitt, "Comparing Different Diffie-Hellman Key Exchange Flavors For LDACS," in *39th Digital Avionics Systems Conference*. IEEE, 2020, pp. 1–10.

[21] N. Mäurer, T. Gräupl, C. Schmitt, and G. Dreo Rodosek, "PMAKE: Physical Unclonable Function-Based Mutual Authentication Key Exchange Scheme For Digital Aeronautical Communications," in *IFIP/IEEE International Symposium on Integrated Network Management*. IEEE, 2021, pp. 1–9.

[22] N. Mäurer, C. Gentsch, T. Gräupl, and C. Schmitt, "Formal Security Verification Of The Station-to-Station Based Cell-Attachment Procedure Of LDACS," in *18th International Conference on Security and Cryptography*. SCITEPRESS Digital Library, 2021, pp. 1–8.

[23] N. Mäurer, T. Gräupl, C. Gentsch, T. Guggemos, M. Tiepelt, C. Schmitt, and G. Dreo Rodosek, "A Secure Cell-Attachment Procedure for LDACS," in *1st Workshop on Secure and Reliable Communication and Navigation in the Aerospace Domain (SRCNAS) on 6th European Symposium on Security and Privacy (Euro S&P)*, 07 2021.

[24] E. Barker, "Digital Signature Standard (DSS)," https://doi.org/10.6028/NIST.FIPS.186-4, accessed 04/06/2022, National Institute of Standards and Technology (NIST), FIPS.186-4, 2013.

[25] NIST, "Secure Hash Standard (SHS)," https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf, accessed 04/06/2022, National Institute of Standards and Technology (NIST), FIPS 180-4, 08 2015.

[26] J. Merkle and M. Lochter, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation," RFC 5639, 03 2010. [Online]. Available: https://www.rfc-editor.org/info/rfc5639

[27] D. Soni, K. Basu, M. Nabeel, N. Aaraj, M. Manzano, and R. Karri, "FALCON," in *Hardware Architectures for Post-Quantum Digital Signature Schemes, pages=31-41*. Springer, 2021.

[28] T. Ewert, N. Mäurer, and T. Gräupl, "Group Key Distribution Procedures for the L-Band Digital Aeronautical Communications System (LDACS)," in *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*, 2021, pp. 1–10.

[29] M. A. Bellido-Manganell, T. Gräupl, O. Heirich, N. Mäurer, A. Filip-Dhaubhadel, D. M. Mielke, L. M. Schalk, D. Becker, N. Schneckenburger, and M. Schnell, "LDACS Flight Trials: Demonstration and Performance Analysis of the Future Aeronautical Communications System," *IEEE Transactions on Aerospace and Electronic Systems*, pp. 1–19, 09 2021.

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

[31] T. Gräupl and N. Mäurer, "Performance-Optimizing Secure GBAS over LDACS," in *21th Integrated Communications, Navigation and Surveillance Conference*. IEEE, 04 2021, pp. 1–6.

[32] N. Mäurer, M. Caamano, D. Gerbeth, and T. Gräupl, "A Secure Broadcast Service for LDACS with an Application to Secure GBAS," in *40th Digital Avionics Systems Conference (DASC)*, 10 2021, pp. 1–10.

[33] R. Di Pietro, S. Guarino, N. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks – A survey," *Computer Communications*, vol. 51, pp. 1–20, 2014.
[34] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm, "Bringing up OpenSky: A Large-scale ADS-B Sensor Network for Research," in *Proceedings of the 13th IEEE/ACM International Symposium on Information Processing in Sensor Networks (IPSN)*, April 2014, pp. 83–94.
[35] T. Ewert, N. Mäurer, and T. Gräupl, "Improving Usable LDACS Data Rate via Certificate Validity Optimization," in *22th Integrated Communications, Navigation and Surveillance Conference*. IEEE, 2022, pp. 1–10.
[36] EUROCONTROL, "Daily Traffic Variation - States," https://www.eurocontrol.int/Economics/DailyTrafficVariation-States.html, accessed 17/04/2022, EUROCONTROL, Brussels, Belgium, Tech. Rep., 04 2022.
[37] ——, "Seven-Year Forecast," https://www.eurocontrol.int/sites/default/files/content/documents/official-documents/forecasts/seven-year-flights-service-units-forecast-2015-2021-Feb2015.pdf, accessed 01/29/2022, EUROCONTROL, Brussels, Belgium, Tech. Rep., 02 2015.
[38] ICAO, "Presentation of 2019 Air Transport Statistical Results," https://www.icao.int/annual-report-2019/Documents/ARC_2019_AirTransportStatistics.pdf, accessed 08/30/2021, International Civil Aviation Organization (ICAO), Tech. Rep., 12 2020.
[39] T. Gräupl, C. Rihacek, and B. Haindl, "LDACS A/G Specification," 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 07/16/2021, German Aerospace Center (DLR), SESAR2020 PJ14-02-01 D3.3.030, 2020.
[40] T. Gräupl, N. Mäurer, and C. Schmitt, "FACTS2: Framework for Aeronautical Communications and Traffic Simulations 2," in *Proceedings of the 16th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks*, ser. PE-WASUN '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 63–66.

2022 Digital Avionics Systems Conference (DASC)
September 18-22, 2022