Concept of Group Key Distribution Procedures for the L-Band Digital Aeronautical Communications System (LDACS)

Thomas Ewert
Technical University Munich (TUM)
Munich, Germany
{thomas.ewert}@in.tum.de

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

Abstract—**Since the beginning of the century, an increasing amount of air traffic has pushed current aeronautical communication systems to their limits. Therefore, a modernization process is ongoing aiming to digitalize previously analog systems and prepare them for future requirements. Among these efforts is the L-Band Digital Aeronautical Communication System (LDACS). Being the worldwide first integrated Communication, Navigation and Surveillance (CNS) system, it will replace legacy analog voice communications in the future. Any newly developed system must provide strong cyber security, especially when deployed within critical infrastructures. While previous work has been focused on implementing Mutual Authentication and Key Establishment protocols in LDACS, applying security mechanisms in a group wise fashion has not been evaluated yet. As LDACS control messages apply to all members of an LDACS cell, Group Key Management (GKM) methods are a vital step in introducing control channel security to LDACS. The objective of this paper is to evaluate GKM procedures to support secure group communication within LDACS control channels.**

Index Terms—**LDACS, Cybersecurity, Group Key Management, Control Channel Protection, Communication Performance**

I. Introduction

In 2010, 19% of all delays were caused by air traffic control capacity problems. The European Commission estimated the ensuing cost for airlines between 1.3 to 1.9 billion euro per year [9], [36]. One contributing factor is the increased saturation of the Very High Frequency (VHF) band, which serves as the main communication channel for Air Traffic Management (ATM). Even with the development of air travel fluctuating with the global economic situation, long-term trends have indicated that the passenger demand will further increase [17].

In 2007, the International Civil Aviation Organization (ICAO) has therefore recommended rationalizing the aeronautical communication infrastructure in order to handle future traffic needs and to implement additional functions [18]. Projects such as Next Generation National Airspace System (NextGen) in the USA or Single European SKY ATM Research (SESAR) in the EU assist since then in the transition to digital systems by defining, developing or delivering improved technologies and procedures [34]. In Europe, one step of this transition is the development and implementation of the L-band Digital Aeronautical Communication System (LDACS) as continental air-to-ground communication standard.

Any newly developed systems must cope with new cybersecurity threats. With the introduction of Software Defined Radios (SDRs), adversaries can carry out unauthorized interference with wireless communication more easily. Therefore, security measures have to be implemented in order to ensure availability, reliability, integrity and confidentiality of transmitted data.

LDACS is based on a wireless cell structure, with one Ground Station (GS) connected to multiple Aircraft Station (AS), thus forming a communication group [21]. In case the sender wants to reach all group members, it is often more efficient to transmit one broadcast message instead of delivering multiple replicas of the same message to each intended recipient. As at least the integrity of messages should be guaranteed, a common key has to be shared among the participants in order to support algorithms such as message authentication codes. The process of maintaining this shared secret key is called Group Key Management (GKM).

The objective of this work is to evaluate the applicability of group key procedures for the protection of LDACS control channels. We establish a criteria catalogue to select a well-suited GKM protocol for LDACS among a list of presented approaches, as well as discuss good approaches for implementation of GKM within LDACS.

II. Background

A. The L-band Digital Aeronautical Communication System (LDACS)

LDACS is a future aeronautical communication system aiming to replace current aeronautical continental communications technologies which are limited in capacity and available security measures. It is based on technologies from mobile communication standards such as 4G and has been adapted for safety critical infrastructure requirements [22].

It provides a cellular structure with point-to-multipoint connections for Air-To-Ground (A2G) communication. The ground segment contains several GSs, each controlling an airspace of up to 200 Nautical Miles (NM) with a maximum capacity of 512 AS [11]. Aircraft with their respective radio communication unit (AS[1]) flying through this area are connected to the same GS via a full duplex radio link. [21]

The LDACS architecture comprises a Physical (PHY), Medium Access Control (MAC), LDACS Management Entity (LME), Data Link Service (DLS), Voice Interface (VI) as well as a Sub-Network Protocol (SNP) layer.

The physical layer is responsible for the transmission of data over the radio channel. Depending on the sending direction, it is being distinguished between Forward Link (FL) for ground-to-air and Reverse Link (RL) for air-to-ground transmission. Both links are separated by Frequency Division Duplex (FDD) [9], the FL transmits on a 1110 - 1156 MHz frequency range while the RL is located at 964 - 1010 MHz [11], [21].

In order to enable a GS to provide bi-directional links to multiple AS within its cell, different AS are separated on the RL in time (via Time Division Multiple Access (TDMA)) as well as in frequency (via Orthogonal Frequency Division Multiple Access (OFDMA)). While the GS is transmitting a continuous stream of data, every AS has to request its respective resources on the RL. This can happen on-demand, but also permanently reoccurring resources can be requested. Each AS has therefore a defined sending time-slot making all RL transmission scheduled and deterministic. The only exception are Random Access (RA) messages transmitted by the AS during the cell-entry procedure [9].

Communication with the PHY layer is achieved via the MAC sub-layer, which forms the lower half of the Data Link Layer (DLL). It consists of the MAC entity, which is providing means for physical access to higher layers as shown in Figure 1. As these components have no information about the physical layer or the methods of transmission, they are only communicating with another utilizing logical channels [9]. The MAC unit is mapping those logical channels between the peer DLL entities onto resources of the physical layer [11].

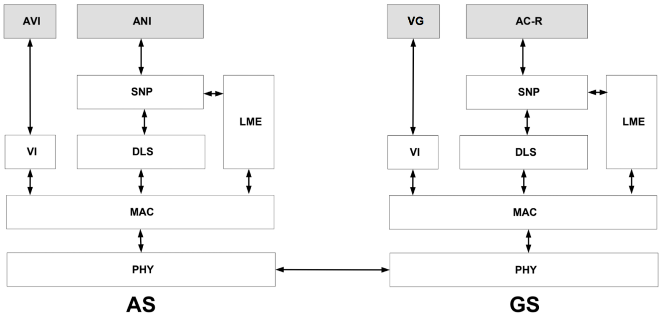


Fig. 1: LDACS protocol stack [9]. The Airborne Voice Interface (AVI), Airborne Network Interface (ANI) as well as Voice Gateway (VG) and Access-Router (AC-R) are external, higher level services LDACS can be connected to.

Parallel to the VI and DLS, the LME is located on the stack. The GS LME is responsible for link maintenance and managing the cell-entry (join) and cell-exit (leave) of AS. Therefore, it is also of special interest for this paper, as any GKM protocols would be implemented in it. Additionally, the GS LME manages the resource allocation on the forward and reverse link as well.

The logical channels used for communication among the peer DLL entities of the AS and GS can be divided into control and user data plane channels. While the latter one consists of the Data Channel (DCH) only, the control plane comprises four different channels. The Random Access Channel (RACH) and Dedicated Control Channel (DCCH) are located on the Reverse Link, while the Forward Link entails the Broadcast Control Channel (BCCH) and Common Control Channel (CCCH).

Information required for registration is being transmitted by the GS in the BCCH to all new aircraft. The counterpart to this channel is the RACH in the RL, which enables up to two aircraft within the same frame segment to transmit an unscheduled cell-entry request. Having successfully entered the LDACS cell, further control messages of the LME are transferred utilizing the CCCH or DCCH respectively [11]. While assignment of transmission slots on the ground-to-air link can be processed locally within the GS, each AS LME has to request the required resources at its GS counterpart. Hereby, the DCCH is being used for the requests, while the resource allocation messages are being transmitted by the GS via the CCCH. [9]

When payload data is being transferred, it is exchanged between the local MAC sub-layer and the Physical Layer (PHY) in form of a FL or RL Physical Layer Service Data Unit (PHY-SDU). Before being sent over the air, the data is going through a process of coding and modulation, creating a stream of modulated symbols. Mapping those symbols to FL or RL is carried out in blocks, which are called Physical Layer Protocol Data Unit (PHY-PDU).

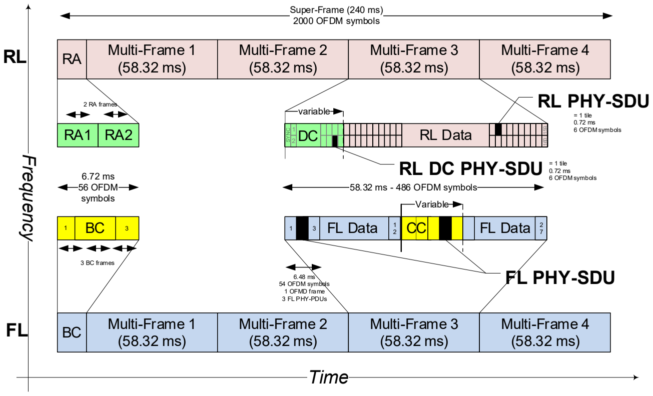


Fig. 2: Frame structure of LDACS [11]

Therefore, one PHY-PDU contains the data of one

[1] Within the scope of this paper, the terms *aircraft* and *Aircraft Station (AS)* are used interchangeably

PHY-SDU, and has a variable size which depends on the Orthogonal Frequency-Division Multiplexing (OFDM) frame type and the used coding and modulation [11]. With improving channel quality the coding and modulation of the individual PHY-SDU packets can be adjusted to provide a higher data rate. Please note, LDACS always encodes control data with the most robust coding and modulation [21].

Data transfer heavily depends on LDACS' frame structure depicted in Figure 2. FL and RL are based on the transmission of hierarchically structured Super Frames (SFs), each 240 ms long. Every SF starts with a general access slot of 6.72 ms in length, followed by four consecutive Multi Frame (MF) spanning 58.32 ms each [24]. The individual structure of the general access and MFs differ between the forward and reverse link. However, any MF consist of a data and control channel slot, which are in turn constructed of individual PHY-PDUs. In the FL, the Common Control (CC) slot is controlled by the GS, can span up to eight PHY-PDUs, each containing 728 b and therefore providing a maximum size of 5,824 b. PHY-PDUs in the RL are assigned per AS, have a size of 83 b, and each Dedicated Control (DC) PHY-PDU is controlled by the AS, the GS assigned it to.

B. Group Key Management (GKM)

In general, the process of maintaining and distributing the required keys for re-keying and encryption to several clients can be summarized under the term Group Key Management (GKM) [6].

All participants in the communication group are sharing a common encryption key, known as *Group Key (GK)*, *Traffic Encryption Key (TEK)* or *Group TEK (GTEK)*, which is used for the underlying algorithm. Depending on the protocol, a key to encrypt the GK for transmission, the *Key Encryption Key (KEK)* or *Group KEK (GKEK)* is required.

The difficulty of sending data securely within a communication group has consequently been shifted to the challenge of establishing and distributing such group keys among authorized participants of the communication in a secure manner [19]. Nevertheless, most protocols are based on pairwise exchanged keys between the group controller and each member.

III. Method

The individual LDACS control channels have different characteristics and therefore show varying possibilities to apply GKM protocols.

The BCCH as well as the RACH are both intended for handling aircraft which are not part of the GS managed cell yet. Consequently, no shared secrets have been exchanged between the GS and the aircraft at this point, making group key procedures impractical.

CCCH and DCCH are vital to the LDACS operation as they do not only provide the means necessary for resource allocation on the data channel but also transmit keep-alive, link management and configuration messages. Tampering with data transmitted on these control channels would render the system unusable, as e.g., no resource allocation would be possible anymore. Depending on the message type, they are either directed to a single AS or broadcast as they contain information important to all members of the group (e.g. CC slot descriptor). Therefore, the applicability of group key procedures to protect the CCCH and DCCH is investigated further. A threat assessment serves as a foundation to determine the required measures needed to secure the channels appropriately.

A. Risk Analysis of Control Channels

In order to evaluate the individual security requirements of the control channels, the basic security goals of the CIA triad (Confidentiality, Integrity, Availability) are being used as a reference to identify critical areas [33]. Furthermore, additional features such as *authenticity*, *non-repudiation*, *accountability* and *reliability* are considered as well.

The definitions contained in RFC 4949 [35] aim to support the creation of material within the Internet standards process. Therefore they are used to outline the scope of the individual terms used in this paper as well. Table I resembles an overview of the single elements as well as an assessment of the necessity to be considered for LDACS' CC/DC channels.

During the analysis, the key security characteristics needed for a stable LDACS operation have been identified as availability/reliability, authenticity and integrity. If e.g., the latter one is absent, an attacker could affect the resource allocation process by injecting false messages or altering existing ones. By advising all aircraft to transmit in the same time-slot and thereby interfering with another, the entire system could become inaccessible.

While availability and reliability are considered important control channel security characteristics, physical attacks such as jamming can hardly be prevented by protocol design. However, by implementing cryptographic means such as access credentials or signatures, resources can be kept available to legitimate users by preventing processing of malicious messages. Therefore, measures for integrity and authenticity protection indirectly also contribute to an available and reliable control channel.

Confidentiality of transmitted control messages has not been identified as a required security measure, which is based on the nature of the transmitted information.

B. Securing LDACS CCCH/DCCH Control Channels

The required security characteristics can be achieved by various methods and on different levels within LDACS. However, as performance parameters such as latency and available bandwidth should be affected as little as possible, certain restrictions apply.

Digital Signatures:

A very common cryptographic method to verify the origin and integrity of a message are digital signatures. In order to achieve a security comparable to symmetric cryptography algorithms, public key algorithms require longer operands and therefore are up to 2-3 times slower than symmetric algorithms. [27]

TABLE I: Overview of different security goals, the associated threats and applicability to LDACS

Security Value	Definition [35]	Threats	required
Availability	*The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever a user requests it.*	When the e.g., CCCH Channel is not available, the GS is unable to assign resources anymore and the system's functionality is lost. An attack scenario could be jamming the channel.	yes
Authenticity	*The property of being genuine and able to be verified and be trusted.*	If the origin of messages cannot be validated, unauthorized messages can be injected into the system or an authorized user can be impersonated. An attacker could e.g., send false allocation messages to schedule all aircraft onto the same time-slot, creating a blockage of the individual signals and impairing system performance and usability.	yes
Integrity	*The property that information has not been modified or destroyed in an unauthorized manner.*	Unauthorized message alteration (e.g., by delay, modification or re-ordering) can create the same disruption of service as missing authenticity.	yes
Confidentiality	*The property that data is not disclosed to system entities unless they have been authorized to know the data.*	With no confidentiality protection in place, unauthorized user can gain information via e.g. eavesdropping. However, analyzing the content of control messages have shown little confidential information included in such. Confidentiality protection is therefore not considered necessary.	no
Non-Repudiation	*A security service that provides protection against false denial of involvement in an association (especially a communication association that transfers data).*	It is assumed, that AS within the cell have authenticated to the ground infrastructure prior, hence are considered as trustworthy and only send messages they are authorized to. Impersonation of e.g., the ground station, by an AS is therefore not seen as probable.	no
Accountability	*The property of a system or system resource that ensures that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions.*	Similar to *Non-Repudiation* it can be assumed that users authorized to participate in the LDACS cell are trustworthy.	no
Reliability	*The ability of a system to perform a required function under stated conditions for a specified period of time.*	As the system is not functional without its control channels, their reliability is important as well.	yes

Furthermore, the resulting signature sizes are not negligible as well. While achieving a 128 b security level, e.g. RSA-3072 requires a 3072 b long key and computes a 3072 b long signature. Algorithms based on elliptic curves, e.g. ECDSA, work with 256 b long keys and are able to reduce the signature size down to 520 b. Further advances in the quantum attack resistant algorithms, such as GeMMS 128, allow for signatures with only 258 b in length, however require public keys with 352.19 KB in size which are several magnitudes larger than conventional public keys [5].

As this information needs to be distributed to the AS and GS as well, the large signature and/or public key sizes make an application for LDACS' small control channels impracticable.

Message Authentication Codes (MACs):

While Message Authentication Codes also provide authenticity and integrity of data, they are based on symmetric cryptography and therefore require the recipient and sender to share a secret key before any transmission can be protected [27]. In digital aeronautical communications security, MACs are used for instance in the ACARS Message Security (AMS) system [2], [3]. Due to the short message sizes and low throughput of the initial Aircraft Communications Addressing and Reporting System (ACARS) (2.4 kbps) [1], with updates of ACARS via VHF Digital Link Mode 2 (VDLm2) (31.5 kbps) in the 90's [31], the length of used MACs in AMS is truncated to 32 b [3]. The probability of an attacker guessing the correct MAC being $\frac{1}{2^{32}}$ combined with the short validity of the key of maximum one flight, the usage of such shortened MACs has been evaluated as being sufficient [3].

Similar considerations are applicable within LDACS. As all CC/DC transmissions are deterministic, bruteforcing MACs is limited to the specific time slots in which CCCH/DCCH are sent, reducing the probabilities of a successful attack.

Therefore, due to higher efficiency by smaller message overheads, fewer required memory and faster execution, the use of MACs over digital signatures is desirable.

Security Overhead:

In the following, the bits created by MACs in relation to the secured message will be summarized under the term *security overhead*. With a constant sized MAC, the relation between the two values is inversely proportional.

Therefore, the overhead depends on the level MACs are utilized on, which in turn is affected by characteristics of LDACS. When recalling the exact layout of the LDACS frame structure from Figure 2, it can be seen that the CCCH is shifted in time by approximately half a MF duration in respect to the

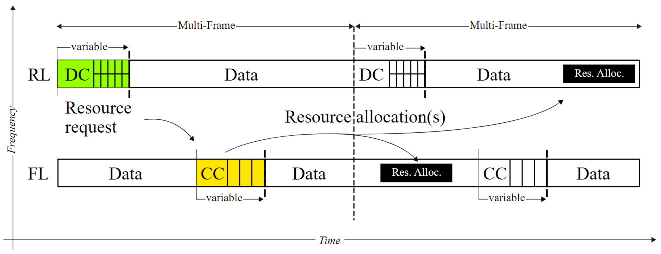


Fig. 3: Shift between control channels in the FL and RL.

DCCH. This enables an alternating use of both channels, i.e. messages sent in the DCCH can be answered in the CCCH following approximately 30 ms later and vise versa as shown in Figure 3. Latency is reduced by one MF per round trip, while the minimal timely distance of 15.12 ms between the end of a full CC slot and the next DC slot has to be observed and serves as the maximum time any verification process might take. Preserving this alternating control slot use can be achieved by selecting an optimal level for MAC deployment. The smallest entity, security can be applied to, are the control messages themselves. Processing can start with the reception of the message and therefore not influence the system's latency significantly. With control message sizes varying between 16 to 96 b [11], even small MACs create a high security overhead and reduce the available bandwidth significantly. While this approach would allow a use of pairwise keys between GS and AS for individual messages, broadcasts still require a common shared secret in order to avoid multiple transmissions. Reducing the security overhead can be achieved by applying MACs to larger data packets. As the control channels consists of blocks, each PHY-PDU can be protected, benefiting the CCCH with its comparably large 728 b long unit the most. Similar to protecting individual messages, latency would not be impaired noticeably. Due to multiple AS transmitting during one DC slot, the PHY-PDU with its 83 b is the largest entity which can be protected in the RL. However, as the GS is the only intended recipient of such messages, pairwise exchanged keys can be used for MAC calculation, provided the GS is capable of having all required keys in store or load them in the respective timely manner. As the GS is the only entity transmitting in the FL, MACs could also be applied to an entire CCCH slot. While reducing the security overhead, retransmission of the entire slot is necessary if any of the PHY-PDUs has not been received correctly. Further reduction can be achieved by protecting an entire FL MF, which requires its complete reception prior to its verification. The subsequent calculations then take place while the next DCCH slot is already ongoing, limiting the alternating control channel use. As the data channel within a MF might contain individually protected data, applying a common security is impractical as well.

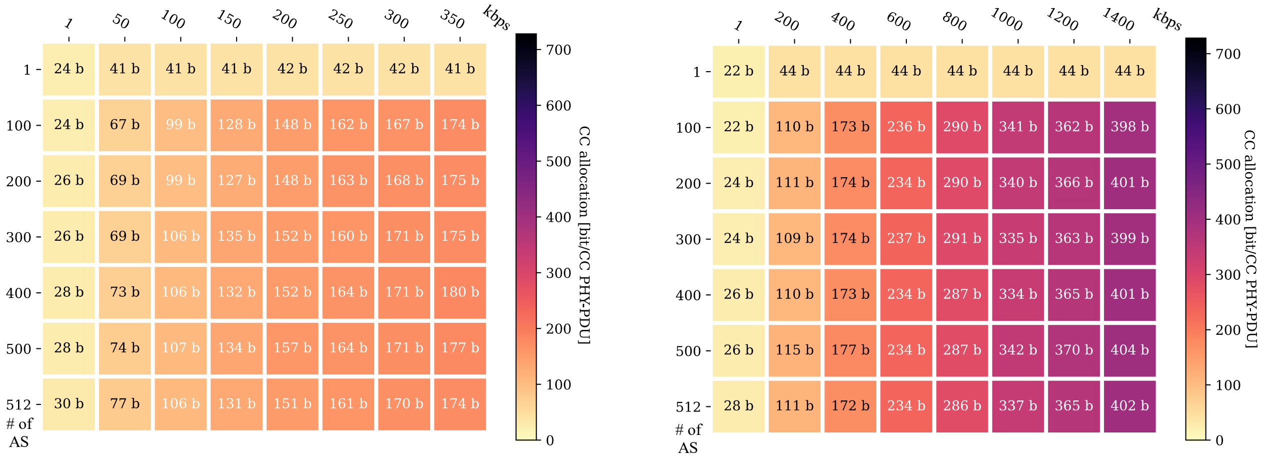
In conclusion: to allow any AS to read and verify information within the CCCH, applying MACs for cryptographic integrity and authenticity checks on individual PHY-PDUs is the most suited solution. Due to the underlying symmetric cryptography, the required shared secret within a LDACS cell calls for a GKM, responsible for establishing and maintaining such keys. However, most GKM protocols require all members to have a pairwise shared secret with the group controller. Within LDACS it is foreseen, that an individual aircraft will share a secret with the GS, established in a previous Mutual Authentication and Key Exchange (MAKE) protocol executed during the cell entry process. A Key Derivation Function (KDF) will be used to derive a key used for protecting individual communications between the AS and GS. As information sent by one AS in its assigned time slot is only addressed to the GS, the derived, shared key can be used for securing the DCCH as well. While the theoretical considerations support the choice of MACs for security, it has to be evaluated if the bandwidth constraint environment holds enough additional capacity for the security data.

Concept for Securing the CC/DC Channel:

To find out CCCH, as well as DCCH allocations, different data throughput $\in \{1, 50, 100, 150, 200, 250, 300\}$ kbps were simulated for different amount of AS $\in \{1, 100, 200, 300, 400, 500, 512\}$ in an LDACS cell with the Framework for Aeronautical Communications and Traffic Simulations 2 (FACTS2) [12].

LDACS Coding and Modulation Scheme (CMS) is set to one, representing the most robust CMS scheme of LDACS. With that the highest throughput, LDACS can handle is 315 kbps in the FL and 280 kbps in the RL [11], [25]. The chosen throughput covers that range. To test for higher datarates, an additional run with CMS=8 was performed with a data throughput range of $\{1, 200, 400, 600, 800, 1000, 1200, 1400\}$ kbps. At CMS=8, LDACS can handle 1428 kbps in the FL and 1390 kbps in the RL. For all test scenarios, realistic data traffic patterns [10] were used, with 74% small packets with 125 B and 26% large packets with 1400 B in the FL and 80% small packets with 125 B and 20% large packets with 1400 B in the RL.

Figure 4 shows the allocation of CC data per CC PHY-PDU in the 99-percentile (i.e., $P_{99\%}$) at two different LDACS CMS (i.e., 1 and 8). Over all simulation results, only two occurrences with over 640 b per CC PHY-PDU are observed. 640 b marks the boundary for which 128 b MACs per CC PHY-PDU would not be possible anymore. Observing the DC allocations revealed, that with increasing amount of AS, small DC allocations in the range of 12-32 b increase, while with growing data rates, more, larger DC allocations in the range of 64-82 b are observed. Comparing both simulated CMS reveals, at 1 AS, 200 kbps, CMS=1, the mean is at 64.40 b, the $P_{99\%}$ at 78 b, while at the same number of AS and data rate but CMS=8, the mean was at 62.50 b and $P_{99\%}$ at 78 b. Increasing the amount of aircraft to 100, taking the same data rate and comparing the two CMS reveals 16.23 b mean and 42 b $P_{99\%}$ at CMS=1 and 14.97 b mean and 42 b $P_{99\%}$ at CMS=8. These examples demonstrate the aforementioned observation of many small DC allocations at a high number of AS and many large DC allocations at a low numbers of AS, independent of the chosen CMS. With these numbers, the path



(a) $P_{99\%}$ CC PHY-PDU allocation @CMS=1

(b) $P_{99\%}$ CC PHY-PDU allocation @CMS=8

Fig. 4: $P_{99\%}$ CC allocations per CC PHY-PDU (c.f. total size of 728 b)

forward for LDACS control channel security becomes clear:

- **CCCH security** - Figure 4 shows the CCCH to have enough capacity left to add a 32/64/96 b truncated or even full 128b MAC for each CC PHY-PDU. To calculate and verify that MAC, the TEK will be used, as every aircraft in the cell need to be able to verify the integrity and authenticity of the CC. Another option is replacing the current Cyclic Redundancy Check (CRC) attached to each CC message with a combined CRC plus MAC approach [7], calculated over an entire CC PHY-PDU data block. As there are approximately 20 CC messages in one CC PHY-PDU data block (i.e., with 35 b average CC message size: 728 $b/35\ b = 20.8$) [11], this approach saves $20.8 \times 8\ b = 166.4\ b$, enabling the space to use one 128 b combined CRC and MAC per CC PHY-PDU data block.
- **DCCH security** - The explanations above reveal the DCCH to not have enough capacity left to add a MAC of any size (i.e., 16/32/64/96/128 b). Therefore the only way to ensure data protection is to use the individual, shared keys between AS and GS, negotiated during the initial MAKE protocol of LDACS [23], [26], and to encrypt the DC payload with an algorithm negotiated in the MAKE procedure. As the DC size is 83 b, a stream cipher, like *ChaCha20* is required for that [29].

To summarize: GKM are only considered for the protection of the CCCH.

C. Evaluation Criteria of Group Key Management procedures

Overall the following criteria have been identified to evaluate a GKM procedure for suitability for LDACS.

- Network overhead: All messages needed for the operation of the GKM protocol are summarized in this section as they influence the required bandwidth. However, the length of an encrypted re-keying message greatly depends on the used algorithm and the number of plain text bits. Therefore, a minimum implementation is assumed, with the message length equal to the size of the plain text.
- Computational overhead: This category describes the required calculations needed for e.g., re-keying message encryption. $\mathcal{O}$-Notation is used to qualify the complexity of the operation, as actual execution speed and delay vary with the underlying hardware. A distinction between different types of mathematical operations is made.
- Storage overhead: Each key used in the GKM procedure has to be stored with the respective entity. This category analyzes the total storage costs, while distinguishing between a Group Member (GM) and the Group Controller (GC).

D. Selection of Group Key Management procedures

Throughout this paper only *Centralized Group Key Management* procedures are regarded to reflect the LDACS use case. In this approach one entity is responsible for controlling the whole group and distributing the TEK to the members [19]. The complexity and trust is put into a single system, which can be handled by either a GC or Key Server (KS) [38]. Commonly used protocols such as Kerberos are based on centralized systems as well. With increasing group sizes or geographical distribution, central management with its associated operations might become difficult, though. [8] In the next section we will compare and evaluate the suitability of Group Key Management Procedure (GKMP) [13], [14], Logical Key Hierachy (LKH) [30], One-way Function Tree (OFT) [41], Centralized Flate Table Key Management (CFKM) [39], Chinese Remaindering Group Key (CRGK) [42], CRT-GKM [38] and Central Authorized Key Extension (CAKE) [15] for LDACS.

IV. Results

A. Theoretical Evaluation of Network, Computational and Storage Overheads of selected GKM

The previously described metrics are summarized for each named protocol or cryptographic scheme in Table II. Rather

TABLE II: Comparison of different GKM procedures under the proposed evaluation criteria

Protocol	Network Overhead (in bit)	Computational Overhead	Storage Overhead
GKMP [13]	Join: Broadcast: $2 \times k$ Unicast: $2 \times k + k$ Leave: $(n-1) \times 2k$	GC: Join: $\mathcal{O}_K(1)$ Leave: $\mathcal{O}_K(n)$ Group Member: Join/Leave: $\mathcal{O}_K(1)$	GC: n KEK + GTEK + GKEK Group Member: 1 KEK + GTEK + GKEK
LKH [40]	Join: Broadcast: $2log_2(n) \times k$ Unicast: $1 \times k$ Leave: $(2log_2(n) - 1) \times k$ [28]	GC: Join: $\mathcal{O}_K(log_2(n))$ Leave: $\mathcal{O}_K(log_2(n))$ Group Member: Join: $\mathcal{O}_K(log_2(n))$ Leave: $\mathcal{O}_K(log_2(n))$	GC: $(2n-1)$ keys Group Member: $log_2(n) + 1$ keys [6]
OFT	Join: Broadcast: $log_2(n) \times k$ Unicast: $log_2(n) \times k + k$ Leave: $log_2(n) \times k$ [20]	GC: Join: $\mathcal{O}_K(log_2(n))$ Leave: $\mathcal{O}_K(log_2(n))$ Group Member: [37] Join: $\mathcal{O}_K(log_2(n))$ Leave: $\mathcal{O}_K(log_2(n))$	GC: $(2n-1)$ keys Group Member: $log_2(n) + 1$ keys [6]
CRGK [38], [42]	Join: Multicast: $\|CRT(n)\|$ Unicast: prime-length in Leave: $\|CRT(n)\|$	GC: Join/Leave: $\mathcal{O}_C(n)$ Group Member: Join/Leave: $\mathcal{O}_{XM}(1)$	GC: $2n$ + 1 keys Group Member: $user_{prime}$ + TEK
CRT-GKM [38]	Join: Multicast: $\|CRT(n)\|$ Unicast: prime-length in Leave: $\|CRT(n)\|$	GC: Join/Leave: $\mathcal{O}_{add/sub}(1)$ Group Member: Join/Leave: $\mathcal{O}_M(1)$	GC: $4n + 3$ keys Group Member: $user_{prime}$ + TEK
CAKE	Join: Broadcast: $2 \times k$ Unicast: $2 \times k + k + p$ bit Leave: $\|CRT(log_3(n^2))\| + k + (log_3(n) - 1) \times \|CRT(3)\|$	GC: Join: $\mathcal{O}_K(1)$ Leave: $\mathcal{O}_L(log_3(n^2)) + \mathcal{O}_K(1)$ Group Member: Join: $\mathcal{O}_K(1)$ Leave: $\mathcal{O}_L(log_3(n^2)) + \mathcal{O}_K(1)$	GC: $n + (1 + 3^k)$ Group Member: $(2 + k) + 1$

than focusing on the individual message numbers in the network overhead, the total amount of bits required to be transmitted for each group operation is evaluated. In order to compare different computational overheads, required complexities to compute a XOR ($\mathcal{O}_X$), to encrypt/decrypt keys ($\mathcal{O}_K$), to create/solve a CRT system ($\mathcal{O}_C$) as well as for modulo operations ($\mathcal{O}_M$) or any combination of such are used.

B. LDACS Centered Evaluation of GKM Procedures

When applying GKM procedures within LDACS, not all mentioned criteria are valued equally within the evaluation process. As LDACS will be deployed primarily in commercial aircraft with engine driven electrical generators [32] and custom made hardware, it can be assumed that the operating environment of LDACS is neither power nor computational restricted. Required storage capacities can be provided easily within the hardware design as well, but limitations due to e.g. the use of a Trusted Platform Module (TPM) might apply.

With bandwidth being very restricted within the LDACS system, it is a critical category for the evaluation. As additional latency imposed by the GKM protocol on the communication is also influenced by the amount of bits needed to be transferred, the network overhead is the main focus for further comparison of the proposed protocols. Computational as well as storage overhead play a subordinate role.

While Table II gives a mathematical explanation of the required bits to be transmitted, the comparison can be visualized more easily by using a sample computation among the different algorithms. As the network overhead is depending on the number of users n in each of the described protocols, the largest number of bits can be seen when looking at a full LDACS cell. Therefore, Table III represents the individual bits assuming the maximum amount of users, 512, as well as an underlying key size of 128 b for each different application (individual user key, KEKs and TEKs).

V. Evaluation and Discussion

All analyzed GKM protocols rely on the transmission of broadcast messages. Without creating additional traffic by utilizing acknowledgement messages, finding a way to reliably send broadcasts is a key requirement for any GKM implementation.

TABLE III: Sample calculation of network overhead in bit for different GKM protocols

Protocol	Join Operation (Cell Entry)	Leave Operation (Cell Exit)
GKMP	Broadcast: $2 \times 128\ b = 256\ b$ Unicast: $2 \times 128\ b + 128\ b = 384\ b$	$(n-1) \times (2 \times 128b) = 511 \times 256\ b = 130,816\ b$
LKH	Broadcast: $2log_2(512) \times 128\ b = 2,304\ b$ Unicast: $128\ b$	$(2log_2(512) - 1) \times 128b = 2,176\ b$
OFT	Broadcast: $log_2(512) \times 128\ b = 1,152\ b$ Unicast: $log_2(512) \times 128\ b + 128\ b = 1,280\ b$	$log_2(512) \times 128\ b = 1,152\ b$
CFKM	Broadcast: $2 \times 24 \times 128\ b = 6,144\ b$ Unicast: $24 \times 128\ b + 128\ b = 3,200\ b$	$2 \times 24 \times 128\ b = 6,144\ b$
CRGK	Broadcast: $CRT(512) \approx 69,120$ b[2] Unicast: 136 b	$CRT(511) \approx 68,985$ b
CRT-GKM	Broadcast: $CRT(512) \approx 69,120$ b Unicast: 136 b	$CRT(511) \approx 68,985$ b
CAKE	Broadcast: $2 \times 128\ b = 256\ b$ Unicast: $2 \times 128\ b + 128\ b + 136\ b = 408$ b	$CRT(log_3(n^2))$ + k + $(log_3(n) - 1) \times \lvert CRT(3) \rvert$ = $3,936$ + 128 + $4,960$ b = $9,024$ b

Tables II and III from the previous sections have listed the corresponding message bits for a user join and leave operation. As each AS has to enter the cell and cannot remain indefinitely within, the total amount of network overhead per AS can be seen as the sum of bits required to be sent for both operations.

Figure 5 visualizes the different amount of bits needed for each protocol's join and leave operation. Hereby, a logarithmic scale has been used in order to accommodate protocols such as OFT and CRGK reasonably within the same graphic.

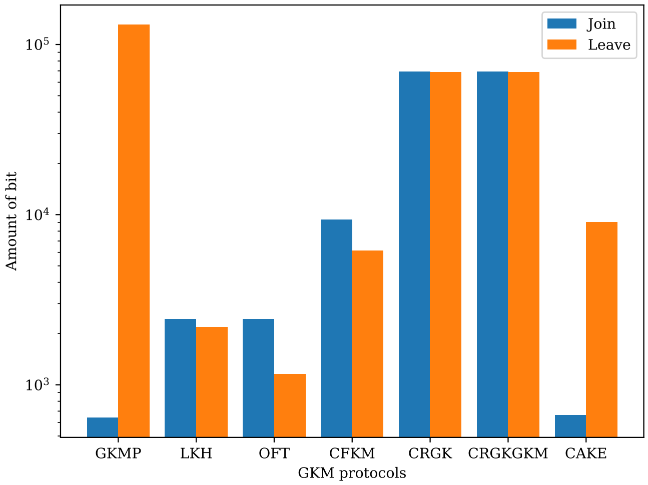


Fig. 5: Visualization of Table III by using a logarithmic scale on the y-axis to display the bit amount. OFT can be identified as the protocol with the least bits required, especially within the leave process.

Even though Chinese Remainder Theorem (CRT) based protocols generally require only one message to be transmitted, the underlying cryptographic calculations lead to a greatly increased message size as explained in Table III. Therefore, the implementation of this algorithm is not practical for the LDACS use case.

While CAKE utilizes a 3-ary LKH in order to reduce the required network overhead for group leave operations, the CRT algorithm is applied as well. Similar to CRGK, the message size can still be considered too large for the LDACS control channel use case, considering especially the CRT based tree operation in the leave process.

The simple GKMP uses smaller individual messages sizes, each being the length of the used keys, however requires the transmission in a one-to-one fashion for group leave operations.

Due to the number of bits of the identifier used in LDACS, the CFKM protocol is showing results greater than CAKE and can be excluded for further considerations as well.

Compared to previous protocols, the proposed tree key hierarchy approaches manage to reduce the number of keys needed to be updated notably. While additional bits needed for e.g., message header information, have not been considered in Table II or Table III, they can be kept to a minimum when all group members have knowledge of the general tree structure.

With a full LDACS cell containing 512 users, a full binary tree structure would only require 9 KEKs to be updated. While LKH encrypts every new KEK with each of its sibling's keys, OFT further reduces the transferred bits by establishing a functional dependency among the KEKs. This reduction in message size however requires, that each joining user is receiving the blended keys for its ancestor sibling set in a unicast fashion. Thus, the benefit from OFT becomes more visible in case of a member leaving the group. As both operations happen within the group equally, OFT can save $log_2(n) \times key\text{-}length$ bit per AS compared to LKH.

The goal for the chosen GKM protocol is to keep the network overhead as minimal as possible. As shown in Table II and III, OFT meets these requirements among the described protocols best.

VI. Conclusion

This work has analyzed the characteristics and security requirements of the control channels of LDACS for the application of GKM procedures, proposed an area of application, a suitable algorithm and a point for implementation.

[2] The solution of the CRT congruence system is unique modulo the product of the individual primes [4]. When using a prime length of 136 b, as suggested in [16], and assuming an average value being half of the maximum, it corresponds to a length of 135 b. With 512 AS within a cell, $(2^{135})^{512} = 2^{135 \times 512} = 2^{69120}$ corresponds to a length of 69,120 b as the maximum value of the unique solution of the system. This formula is the basis for all $CRT(x)$ calculations within CRGK and CRT-GKM.

We have provided a comprehensive overview of the LDACS system and gave an introduction to GKM.

An assessment of the control channel security requirements resulted in integrity and authenticity being the main security characteristics for the CCCH/DCCH. While those properties can be achieved in different ways, a short MAC has been suggested due to a prevailing restricted bandwidth within the channels. We identified the CCCH as suitable to be protected via short MACs and a group key derived from the GKM procedure, as every aircraft needs to be able to read and verify all CC message sent by the ground-station. This approach is not viable for the DCCH, due to limited space and all aircraft contributing individually to the DCCH. However, information transmitted within the DCCH are intended for the GS only and can therefore use pairwise exchanged keys for protection which are not managed by the GKM protocol.

The symmetrical key establishment for the protection of the CCCH can be achieved via GKM protocols, from which the OFT is considered the most suitable due the minimum amount of bits needed for its operation among all other listed protocols.

Future work will comprise the incorporation of the proposed GKM protocol into the existing LDACS security architecture. This also includes the integration of a reliable broadcast, required by most GKM protocols.

Appendix

A2G	Air-To-Ground
ACARS	Aircraft Communications Addressing and Reporting System
AC-R	Access-Router
AMS	ACARS Message Security
ANI	Airborne Network Interface
AS	Aircraft Station
ATM	Air Traffic Management
AVI	Airborne Voice Interface
BCCH	Broadcast Control Channel
CAKE	Central Authorized Key Extension
CC	Common Control
CCCH	Common Control Channel
CFKM	Centralized Flate Table Key Management
CMS	Coding and Modulation Scheme
CRGK	Chinese Remaindering Group Key
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem
DC	Dedicated Control
DCCH	Dedicated Control Channel
DCH	Data Channel
DLL	Data Link Layer
DLS	Data Link Service
FACTS2	Framework for Aeronautical Communications and Traffic Simulations 2
FDD	Frequency Division Duplex
FL	Forward Link
GC	Group Controller
GK	Group Key
GKEK	Group KEK
GKM	Group Key Management
GKMP	Group Key Management Procedure
GM	Group Member
GS	Ground Station
GTEK	Group TEK
ICAO	International Civil Aviation Organization
KDF	Key Derivation Function
KEK	Key Encryption Key
KS	Key Server
LDACS	L-band Digital Aeronautical Communication System
LKH	Logical Key Hierachy
LME	LDACS Management Entity
MAC	Medium Access Control
MAKE	Mutual Authentication and Key Exchange
MF	Multi Frame
NM	Nautical Miles
OFDM	Orthogonal Frequency-Division Multiplexing
OFT	One-way Function Tree
PHY	Physical Layer
PHY-PDU	Physical Layer Protocol Data Unit
PHY-SDU	Physical Layer Service Data Unit
RACH	Random Access Channel
RL	Reverse Link
SDR	Software Defined Radio
SF	Super Frame
SNP	Sub-Network Protocol
TEK	Traffic Encryption Key
TPM	Trusted Platform Module
VDLm2	VHF Digital Link Mode 2
VHF	Very High Frequency
VI	Voice Interface
VG	Voice Gateway

References

[1] ARINC, "Aircraft Communications Addressing and Reporting System," Aeronautical Radio, Incorporated (ARINC), Tech. Rep., February 1998, [Online]. Available: https://web.archive.org/web/20120510105708/https://www.arinc.com/cf/store/catalog_detail.cfm?item_id=561 [Accessed: January 23, 2021].

[2] ——, "DATALINK SECURITY PART 2 – KEY MANAGEMENT," Aeronautical Radio, Incorporated (ARINC), Tech. Rep., March 2003, [Online]. Available: https://standards.globalspec.com/std/1039315/ARINC823P1 [Accessed: February 23, 2021].

[3] ——, "DATALINK SECURITY PART 1 – ACARS MESSAGE SECURITY," Aeronautical Radio, Incorporated (ARINC), Tech. Rep., 12 2007, [Online]. Available: https://standards.globalspec.com/std/1039315/ARINC823P1.

[4] G. Baumslag, B. Fine, M. Kreuzer, and G. Rosenberger, *A Course in Mathematical Cryptography*. Walter de Gruyter GmbH & Co KG, 2015.

[5] A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem, "GeMSS: A great multivariate short signature," *Submission to NIST*, 2017. [Online]. Available: https://www-polsys.lip6.fr/Links/NIST/GeMSS.html

[6] Y. Challal and H. Seba, "Group key management protocols: A novel taxonomy," *International journal of information technology*, vol. 2, no. 1, pp. 105–118, 2005.

[7] E. Dubrova, M. Näslund, G. Selander, and F. Lindqvist, "Message authentication based on cryptographically secure CRC without polynomial irreducibility test," *Cryptography and Communications*, vol. 10, no. 2, pp. 383–399, 2018.

[8] N. Felde, T. Guggemos, T. Heider, and D. Kranzlmüller, "Secure group key distribution in constrained environments with IKEv2," in *2017 IEEE Conference on Dependable and Secure Computing*, 2017, pp. 384–391.

[9] T. Gräupl and M. Ehammer, "The LDACS1 Link Layer Design," in *Future Aeronautical Communications*, S. Plass, Ed. Rijeka: IntechOpen, 2011, ch. 14.

[10] T. Gräupl and M. Mayr, "Method to emulate the l-band digital aeronautical communication system for sesar evaluation and verification," in *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, 2015, pp. 2D1–1–2D1–11.

[11] 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].

[12] 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*, 2019, pp. 63–66.

[13] H. Harney and C. Muckenhirn, "Group Key Management Protocol (GKMP) Architecture," RFC 2094 (Experimental), RFC Editor, Fremont, CA, USA, RFC 2094, Jul. 1997. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2094.txt

[14] ——, "Group Key Management Protocol (GKMP) Specification," RFC 2093 (Experimental), RFC Editor, Fremont, CA, USA, RFC 2093, Jul. 1997. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2093.txt

[15] P. Hillmann, M. Knüpfer, and G. Dreo Rodosek, "CAKE: Hybrides Gruppen-Schlüssel-Management Verfahren," in *10. DFN-Forum Kommunikationstechnologien*, P. Müller, B. Neumair, H. Raiser, and G. Dreo Rodosek, Eds. Bonn: Gesellschaft für Informatik e.V., 2017, pp. 31–40.

[16] P. Hillmann, M. Knüpfer, T. Guggemos, and K. Streit, "Cake: An efficient group key management for dynamic groups," *arXiv preprint arXiv:2002.10722*, 2020.

[17] IATA, "IATA Forecasts Passenger Demand to Double Over 20 Years," 10 2016, [Online.] Available: https://www.iata.org/en/pressroom/pr/2016-10-18-02/[Accessed: September 22, 2020].

[18] ICAO, "Aeronautical Communications Panel (ACP) - First Meeting," International Civil Aviation Organization (ICAO), Tech. Rep., May 2007, [Online.] Available: https://www.icao.int/safety/acp/prl/acp-1-english/acp.1.wp.006.2.complete.en.pdf [Accessed May 10, 2021].

[19] N. Karuturi, R. Gopalakrishnan, R. Srinivasan, and C. Rangan, "Foundations of Group Key Management - Framework, Security Model and a Generic Construction," *IACR Cryptology ePrint Archive*, vol. 2008, p. 295, 01 2008.

[20] V. Kumar, R. Kumar, and S. Pandey, "A computationally efficient centralized group key distribution protocol for secure multicast communications based upon RSA public key cryptosystem," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 9, pp. 1081–1094, 2020.

[21] N. Mäurer, T. Graeupl, and C. Schmitt, "L-Band Digital Aeronautical Communications System (LDACS)," 02 2021, work in Progress, draft-ietf-raw-ldacs-07, [Online.] Available: https://datatracker.ietf.org/doc/draft-ietf-raw-ldacs/ [Accessed May 10, 2021].

[22] N. Mäurer, T. Gräupl, and C. Schmitt, "Evaluation of the LDACS Cybersecurity Implementation," in *38th Digital Avionics Systems Conference (DASC)*. San Diego, CA, USA: IEEE, September 2019, pp. 1–10.

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

[24] Mäurer, N., Gräupl, T. and Schmitt, C., "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS," in *39th Digital Avionics Systems Conference (DASC)*. Online: IEEE, October 2020, pp. 1–10.

[25] ——, "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS," in *39th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, Oct. 2020, pp. 1–10.

[26] Mäurer, Nils and Gräupl, Thomas and Schmitt, Corinna, "Cybersecurity for the L-band Digital Aeronautical Communications System (LDACS)," in *Aviation Cybersecurity: Foundations, Principles, and Applications*, H. Song, K. Hopkinson, T. d. Cola, T. Alexandrovich, and L. D., Eds. London, UK: IET, June 2021, pp. 1–38.

[27] C. Paar and J. Pelzl, *Understanding cryptography: A textbook for students and practitioners*. Springer Science & Business Media, 2009.

[28] A. R. Pais and S. Joshi, "A new probabilistic rekeying method for secure multicast groups," *International Journal of Information Security*, vol. 9, no. 4, pp. 275–286, 2010.

[29] G. Procter, "A Security Analysis of the Composition of ChaCha20 and Poly1305," *IACR Cryptol. ePrint Arch.*, vol. 2014, p. 613, 2014.

[30] D. Rafaeli, S.and Hutchison, "A Survey of Key Management for Secure Group Communication," *ACM Comput. Surv.*, vol. 35, no. 3, p. 309–329, Sep. 2003.

[31] RTCA, "DO-281C, Minimum Operational Performance Standards (MOPS) for Aircraft VDL Mode 2 Physical Link and Network Layer," Radio Technical Commission for Aeronautics (RTCA), Tech. Rep., September 2018, [Online]. Available: https://www.rtca.org/products/do-281c-electronic/ [Accessed: January 05, 2021].

[32] B. Sarlioglu and C. T. Morris, "More Electric Aircraft: Review, Challenges, and Opportunities for Commercial Transport Aircraft," *IEEE Transactions on Transportation Electrification*, vol. 1, no. 1, pp. 54–64, 2015.

[33] A. S. Sendi and M. Cheriet, "Cloud Computing: A Risk Assessment Model," in *2014 IEEE International Conference on Cloud Engineering*, 2014, pp. 147–152.

[34] SESAR JU, "SESAR Vision," 2021, [Online.] Available: https://www.sesarju.eu/vision [Accessed May 10, 2021].

[35] R. Shirey, "Internet Security Glossary, Version 2," RFC 4949 (Informational), RFC Editor, Fremont, CA, USA, RFC 4949, Aug. 2007. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4949.txt

[36] B. Vaaben and J. Larsen, "Mitigation of airspace congestion impact on airline networks," *Journal of Air Transport Management*, vol. 47, pp. 54–65, 2015.

[37] B. P. Varthini and S. Valli, "An Enhanced One Way Function Tree Rekey Protocol Based on Chinese Remainder Theorem," in *Computer and Information Sciences - ISCIS 2005*, P. Yolum, T. Güngör, F. Gürgen, and C. Özturan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 33–43.

[38] P. Vijayakumar, S. Bose, and A. Kannan, "Chinese remainder theorem based centralised group key management for secure multicast communication," *IET information Security*, vol. 8, no. 3, pp. 179–187, 2014.

[39] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The VersaKey framework: versatile group key management," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 9, pp. 1614–1631, 1999.

[40] D. Wallner, E. Harder, and R. Agee, "Key Management for Multicast: Issues and Architectures," RFC 2627 (Informational), RFC Editor, Fremont, CA, USA, RFC 2627, Jun. 1999. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2627.txt

[41] X. Xu, L. Wang, A. Youssef, and B. Zhu, "Preventing Collusion Attacks on the One-Way Function Tree (OFT) Scheme," in *Applied Cryptography and Network Security*, J. Katz and M. Yung, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 177–193.

[42] X. Zheng, C.-T. Huang, and M. Matthews, "Chinese Remainder Theorem Based Group Key Management," in *Proceedings of the 45th Annual Southeast Regional Conference*, ser. ACM-SE 45. New York, NY, USA: Association for Computing Machinery, 2007, p. 266–271.