Efficient Control-Channel Security for the Aeronautical Communications System LDACS

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

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

***Abstract*—Since Air Traffic Management (ATM) is still conducted largely via analogue voice communications, the digitization of data transmission is crucial to automate and secure ATM in civil aviation. For that purpose, several new digital data links are developed. The continental, terrestrial long-range candidate is the L-band Digital Aeronautical Communications System (LDACS), which is a cellular, ground-based digital communications system for flight guidance and communications related to the safety and regularity of flight. The security of LDACS has been the focus of recent works, however, the problem to secure data on its small control-channels remains unsolved. The objective of this work is to propose slim and efficient security measures to protect data on the LDACS control-channels and evaluate their security and performance impact. First, via a 3-pass instancing of the ISO/IEC 11770-3:2021 "Key agreement mechanism 7" protocol, keys to secure LDACS control-channels are established between air and ground radios. Second, via these point-to-point keys and point-to-multipoint group keys, the control-channels are secured. Thereby the limitations set by the limited bandwidth are respected and cryptographic overhead optimized. Finally, the security of our proposal is validated using a symbolic model with the Tamarin proof system. Also, via computer simulations, the LDACS performance impact of the control-channel security solutions is evaluated.**

***Index Terms*—LDACS, Cybersecurity, Aeronautical Communications, Applied Cryptography, Critical Infrastructure, Wireless Security, Performance Evaluation**

I. Introduction

Current Air Traffic Management (ATM) suffers from three major issues: (1) analogue voice communications result in increased workload in the flight deck and on ground, allow for misunderstandings and are spectrum inefficient, (2) spectrum is scarce, especially in the Very High Frequency Band (VHF) band leading to the current digital terrestrial system - the VHF Datalink Mode 2 (VDLm2) - already reaching its capacity limits and (3) most combinations of aeronautical datalinks, network layer and applications lack any cybersecurity measures, resulting in a large attack surface [1]–[3].

In Europe, these shortcomings are largely addressed by a transition of the current Communications, Navigation and Surveillance (CNS) infrastructure from analogue to digital technologies. One cornerstone hereby is the introduction of spectrum efficient, secure, broadband datalinks, raising the current available bandwidth from few kbps to Mbps and adding security to the link layer. Additionally, end-to-end connectivity is transitioning from the "plain old" ACARS to the Aeronautical Telecommunications Network (ATN)/IP-Protocol Suite (IPS), where IPv6 is used to route traffic from air traffic controller to the aircraft [3].

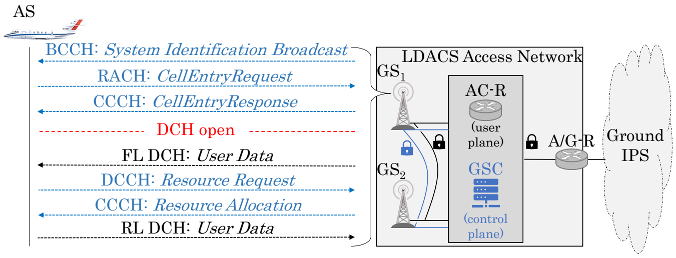

Fig. 1: LDACS A/G and access network segment. The focus here is on the LDACS A/G section and its control-channels. Solid lines show wired, dotted lines wireless communications. Black lines show user-plane data, blue control-plane data.

The datalink candidate for long-range terrestrial Air-Ground (A/G) communications and focus of this work is the L-band Digital Aeronautical Communications System (LDACS). It is a cellular broadband communications system for flight guidance, digital voice and data communications related to safety and regularity of flight and currently on technical readiness level TRL 6 [4]. Additionally, the LDACS signal can also be used for navigational purposes [5]. The system is currently under standardization at the International Civil Aviation Organization (ICAO) and standardized by the Internet Engineering task Force (IETF), and has been successfully flight trialled multiple times [6]–[8]. An overview of involved entities (Aircraft Station (AS), Ground Station (GS), Ground Station Controller (GSC), Access-Router (AC-R), Air/Ground-Router (A/G-R)) and channels (Broadcast Control Channel (BCCH), Random Access Channel (RACH), Common Control Channel (CCCH), Dedicated Control Channel (DCCH), Forward Link (FL)-, Reverse Link (RL)-Data Channel (DCH)) is depicted in Figure 1.

Regulatory documents such as ARINC 858 [9] or ICAO Doc 9896 [10] state clear cybersecurity goals for ATN/IPS enabling datalinks: "[Provide] a secure channel between the airborne radio systems and the peer radio access endpoints on the ground [...] to ensure authentication and integrity of air-ground message exchanges" [9]. While previous works [11], [12] have already addressed the challenge of LDACS user-data security, control-channel security remains an unsolved problem.

Our contributions are three-fold: First, a range of (cryptographic) countermeasures to address the lack of authentication is proposed: For the *CellEntry* phase of an aircraft, a symmetric signature is embedded into the BCCH, CCCH and DCCH, allowing for an AS/GS to verify the respective sender. An optimized 3-pass Mutual Authentication and Key Establishment (MAKE) between AS and GS is proposed, which establishes keys for user- and control-channel protection. In comparison to previous works, the protocol requires one message less and thus the security-overhead in the cell-attachment procedure is reduced [11], [12]. Second, the correctness of the changes to the MAKE protocol are validated using a symbolic proof system in the Tamarin framework. Third, the proposed countermeasures are evaluated with respect the their performance impact on the overall system.

II. Background

LDACS operates on ground-based cells managed by GSs, each of which can serve up to 512 ASs. An LDACS cell is always under full control of a GS, meaning that resources, AS data transmission, timing and so on are fully managed by the GS. LDACS radios are addressed by two different types of identities: global long-term addresses, the Unique Address (UA), and local temporary addresses, the Sub-net Access Code (SAC). There are two directions for communication between GS and the AS: the FL $GS \rightarrow AS$ and the RL $AS \rightarrow GS$. LDACS employs a dynamic Coding and Modulation Scheme (CMS), depending on channel quality, and offers 230.5 to 1428.3 kbps in the FL and 235.3 to 1390.4 kbps in the RL for user data per operated cell. LDACS entities are initially addressed via a global Unique Address (UA) and, once registered within a cell, via a local, temporary Sub-net Access Code (SAC) (cf. Figure 1).

LDACS uses a fixed frame structure defining the intervals in which messages for each communication channel can be embedded into the radio signal. This frame-structure is synchronized between all communication participants. Overall, that frame-structure consists of a Super Frame (SF) of 240 ms duration, which in turn is split in four Multi Frame, each lasting 58.32 ms.

The FL frame-structure begins with the BCCH (split into 3 slots, cf. Table I), in which the GS announces the existence of a specific LDACS cell once at the beginning of each Super Frame in form of the System Identification Broadcast (SIB). The second control channel in the FL is the CCCH, occurring in every Multi Frame, where resources are assigned (e.g., time slots for AS data transmission in the RL). The last part of the FL is the user-DCH, occurring in every Multi Frame, where GS can directly transmit data [4].

The RL frame structure consists of one RACH (split into 2 slots, cf. Table I) at the beginning of each Super Frame, where AS request access to an LDACS cell, the DCCH, occurring in every Multi Frame, and the user RL-DCH, also occurring in every Multi Frame. AS have to request resources in the DCCH, which are granted by the GS in the CCCH, before the AS can transmit user data in the RL-DCH (cf. Figure 1). The resulting LDACS frame structure and size and recurrence of each channel is summarized in Table I.

TABLE I: Technical Details of LDACS Channels [4]

Purpose	Channel	Recurrence	Size	Occupied
Control Data	RACH 1/2	every 240 ms	54 bit	54 bit
	DCCH	every 60 ms	83 bit	16 - 81 bit
	BCCH 1/3	every 240 ms	528 bit	88 - 416 bit
	BCCH 2	every 240 ms	1000 bit	56 - 688 bit
	CCCH	every 60 ms	1-8 × 728 bit	56 - 5128 bit
User Data	FL DCH	every 60 ms	CMS dependent: 13,832 - 85,696 bit	0 bit
	RL DCH	every 60 ms	CMS dependent: 14,336 - 83,424 bit	0 bit

III. LDACS Control-Channel Security

The novel contributions in this section by the authors is the extension of the LDACS cell-entry, a new MAKE protocol and the actual control-channel protection mechanism.

A. Control-Channel Security Requirements

Throughout this work, we assume the Dolev-Yao attacker model [13]. In this model, attacks on control-channel data are possible due the lack of *authentication* and *replay-protection*:
BCCH: An attacker spoofs an LDACS ground station signal which reduces the terrestrial navigation capabilities.
CCCH: The modification of resources allocations results in resource starvation of an aircraft, effectively removing the capability to communicate with the ground stations.
DCCH: Modifying acknowledgment messages leads to the continuous transmission of the same user data message until timeout, reducing LDACS user data capacity.

As such, *authentication*, *integrity* and *replay-protection* are mandatory security properties for LDAC control-channel messages. Confidentiality protection is not required as the content of the control-channel message does not reveal any secret information [12], [14], [15]. The key material for protecting the control-channels must further fulfil the *good key*, *key integrity*, *consistency* and (for point-to-point keys) *perfect forward secrecy* security properties [12], [14].

As shown in Table I, another security solutions requirement is, it must fit in the small and well-filled LDACS control-channels. In [15], group-key schemes to secure FL control-channels were already investigated to reduce security traffic.

B. Enhanced Authentication and Key Establishment

The LDACS cell-attachment is a 2-step procedure with AS and GS first establishing a basic connection via the cell-entry protocol, before the LDACS DCH becomes available, allowing for the exchange of larger packets for the MAKE protocol. Table II shows the used notation of this section.

As described in [11], [12], LDACS entities are registered within a dedicated LDACS PKI by their UA and receive end-entity certificates $Cert_{AS/GS}$ before the radios are rolled-out.

TABLE II: Notation of Cryptographic Primitives

Notation	Operation	Meaning
m	$m \leftarrow m_1 \| m_2$	Message and message concatenation $\|$
k	$k \leftarrow \text{KDF}(z, N, UA)$	Symmetric key and key derivation function with shared secret z, nonce N, identity UA
$Cert_A$	-	Entity A certificate with its public key pk_A and signature σ of authorized PKI entity
$OCSP_{Cert}$	-	Validity proof for $Cert$
c	$c \leftarrow \text{ENCRYPT}(k, m)$ $m \leftarrow \text{DECRYPT}(k^{-1}, c)$	Encryption of m with key k Decryption of c with key k
t	$t \leftarrow \text{MAC}(k, m)$ $\{0, 1\} \leftarrow \text{VERIFY}(k, m, t)$	MAC tag computation t with key k Verification of MAC tag t with key k
σ_A	$\sigma_A \leftarrow \text{SIG}(\text{sk}_A, m)$ $\{0, 1\} \leftarrow \text{VERIFY}(\text{pk}_A, m, \sigma_A)$	Signature generation with private key sk_A Signature verification with public key pk_A
P, x, z	$(P, x) \leftarrow \text{KEYGEN}(1^n)$ $z \leftarrow \text{GENSECRET}(P_A, x_B)$	Ephemeral key pair (P, x) generation A, B shared secret z generation
N	$N \leftarrow \text{RAND}(1^n)$	Nonce generation

The GSs establish a secure ground connection to certificate distribution and validation services of the LDACS PKI. The GS also generates secret group keys with sufficient entropy, k_{BC}, k_{CC}, prior to any cell-attachment. Lastly, the GS announces all available ciphers in `cipher-suite`. With these prerequisites, the LDACS cell-attachment is shown in Figure 2 and described here:

Step 1: The GS broadcasts the *SIB*, revealing its identities (UA_{GS}, SAC_{GS}) and relevant BCCH messages m_{BC}, including the current SF number SF_i. To protect the messages, the GS concatenates all m_{BC} with the current SF_i and computes a MAC tag $t_{BC} \leftarrow \text{MAC}(k_{BC}, m_{BC} \| SF_i)$.

Step 2: The AS looks up whether it has stored the current $Cert_{GS}$ locally, denotes that result in `scgs` and replies with its own address UA_{AS} and `scgs`.

Step 3: The GS receives and stores these message, assigns a new temporary address to the AS, SAC_{AS}, and sends CCCH messages m_{CC}, including all available cipher-suites `cipher-suite`. To protect the messages, the GS concatenates all m_{CC} with the current Multi Frame (MF) number MF_j and computes a MAC tag $t_{CC} \leftarrow \text{MAC}(k_{CC}, m_{CC} \| MF_j)$. After that, the DCH is open.

Step 4: The GS generates an ephemeral key pair (P_{GS}, x_{GS}) and a nonce N_{GS} and sends these.

Step 5: The AS selects algorithms from `cipher-suite` which it stores in `algo`. Then it generates an ephemeral key pair (P_{AS}, x_{AS}) and a nonce N_{AS}, computes the shared secret $z \leftarrow \text{GENSECRET}(P_{GS}, x_{AS})$ and derives shared session keys: $k_{AS,GS}, k_{DC}, k_M, k_{KEK} \leftarrow \text{KDF}(z, N_{AS}, N_{GS}, UA_{AS}, UA_{GS})$. It prepares $m_{AS} \leftarrow \text{P}_{\text{AS}} \| \text{P}_{\text{GS}} \| \text{UA}_{\text{GS}} \| \text{SAC}_{\text{GS}} \| \texttt{scgs} \| \texttt{algo} \| N_{\text{AS}}$ and computes $t_{\text{AS}} \leftarrow \text{MAC}(k_M, m_{AS})$ and $\sigma_{\text{AS}} \leftarrow \text{SIG}(\text{sk}_{AS}, m_{AS})$.

Step 6: The GS fetches the current $OCSP_{Cert_{AS/GS}}$ based on the respective $UA_{AS/GS}$ from the ground based LDACS PKI validation server. It then verifies the $Cert_{AS}$ validity. By rebuilding m_{AS} and fetching pk_{AS} from $Cert_{AS}$, it verifies σ_{AS}: $\{0, 1\} \leftarrow \text{VERIFY}(\text{pk}_{AS}, m_{AS}, \sigma_{AS})$. It then computes the shared secret $z \leftarrow \text{GENSECRET}(P_{AS}, x_{GS})$ and derives shared session keys as the AS in step 5. Next, the validity of t_{AS} is checked: $\{0, 1\} \leftarrow \text{VERIFY}(k_M, m_{AS}, t_{AS})$. Then, all group-keys are concatenated $m_{k_{set}} \leftarrow k_{BC} \| k_{CC}$ and encrypted with authentication using k_{KEK}: $c_{k_{set}} \leftarrow \text{ENCRYPT}(k_{KEK}, m_{k_{set}})$. GS prepares $m_{GS} \leftarrow \text{P}_{\text{GS}} \| \text{P}_{\text{AS}} \| \text{UA}_{\text{AS}} \| \text{SAC}_{\text{AS}} \| \texttt{cipher-suite} \| N_{\text{GS}} \| c_{k_{set}}$ and computes $t_{\text{GS}} \leftarrow \text{MAC}(k_M, m_{GS})$ and $\sigma_{\text{GS}} \leftarrow \text{SIG}(\text{sk}_{GS}, m_{GS})$. Depending on `scgs`the GS adds $Cert_{GS}$ to the next message or not.

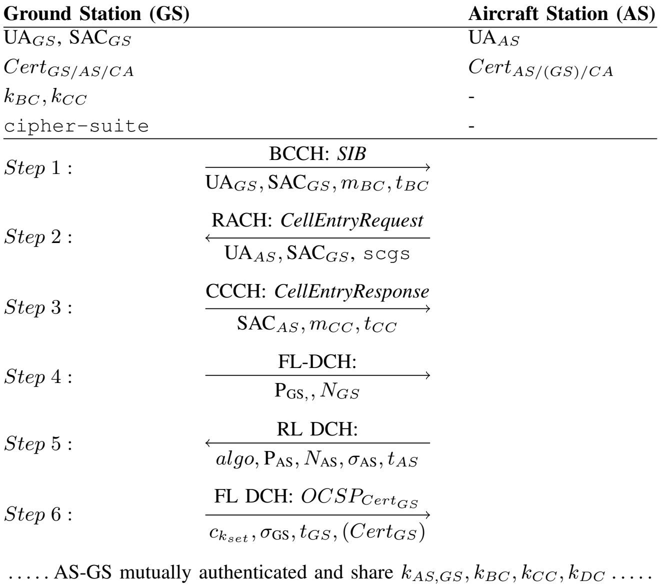
Ground Station (GS)
Aircraft Station (AS)
UA_{GS}, SAC_{GS}
UA_{AS}
$Cert_{GS/AS/CA}$
$Cert_{AS/(GS)/CA}$
k_{BC}, k_{CC}
-
cipher-suite
-
$Step\ 1:$
BCCH: *SIB*
$\text{UA}_{GS}, \text{SAC}_{GS}, m_{BC}, t_{BC}$
$Step\ 2:$
RACH: *CellEntryRequest*
$\text{UA}_{AS}, \text{SAC}_{GS}$, scgs
$Step\ 3:$
CCCH: *CellEntryResponse*
$\text{SAC}_{AS}, m_{CC}, t_{CC}$
$Step\ 4:$
FL-DCH:
$\text{P}_{\text{GS},}, N_{GS}$
$Step\ 5:$
RL DCH:
$algo, \text{P}_{\text{AS}}, N_{\text{AS}}, \sigma_{\text{AS}}, t_{AS}$
$Step\ 6:$
FL DCH: $OCSP_{Cert_{GS}}$
$c_{k_{set}}, \sigma_{\text{GS}}, t_{GS}, (Cert_{GS})$
..... AS-GS mutually authenticated and share $k_{AS,GS}, k_{BC}, k_{CC}, k_{DC}$ .....

Fig. 2: LDACS Cell-Attachment Procedure

Step 7: The AS verifies the validity of the current $Cert_{GS}$ with $OCSP_{Cert_{GS}}$. By rebuilding m_{GS} and fetching pk_{GS} from $Cert_{GS}$, it verifies σ_{GS}: $\{0, 1\} \leftarrow \text{VERIFY}(\text{pk}_{GS}, m_{GS}, \sigma_{GS})$. Using k_M, it verifies $\{0, 1\} \leftarrow \text{VERIFY}(k_M, m_{GS}, t_{GS})$. It decrypts $m_{k_{set}} \leftarrow \text{DECRYPT}(k_{KEK}, c_{k_{set}})$ and can finally verify t_{BC} and t_{CC} as it now has access to the keys k_{BC}, k_{CC}, messages and SF or MF number SF_i, MF_j: $\{0, 1\} \leftarrow \text{VERIFY}(k_{BC}, m_{BC} \| SF_i, t_{BC})$, $\{0, 1\} \leftarrow \text{VERIFY}(k_{CC}, m_{CC} \| MF_j, t_{CC})$.

C. Control-Channel Protection Scheme

As described in Section III-B, BCCH and CCCH protection is handled via GS generated group-keys k_{BC}, k_{CC} since many different AS in an LDACS cell need to access messages in both channels, which makes using individual point-to-point keys and MAC tags per message expensive. DCCH protection is handled via the point-to-point key k_{DC}. The RACH does not receive any additional protection as the only message here is the *CellEntry* message, which already completely fills the RACH slot with its 54 bit [4]. BCCH, CCCH, and DCCH security is implemented by adding a MAC tag message, cryptographically securing the channel contents. The entire protection scheme is shown in Figure 3.

a) BCCH Protection: BCCH messages are concatenated as $m_{BC} \leftarrow m_{BC_1} \| m_{BC_2} \| ... \| m_{BC_n}$. One of the m_{BC_k} must always include the current SF number SF_i. SF_i acts as replay-protection mechanism and sequence number here. Then, the GS computes the BCCH MAC tag as follows: $t_{BC} \leftarrow \text{MAC}(k_{BC}, m_{BC} \| SF_i)$. As long as that specific LDACS cell remains active, m_{BC} and t_{BC} are transmitted

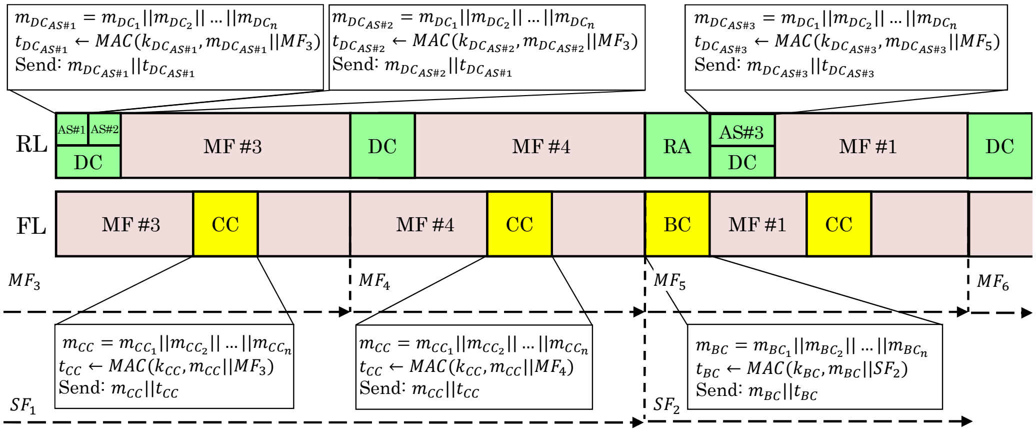
$m_{DC_{AS\#1}} = m_{DC_1}||m_{DC_2}|| \ldots ||m_{DC_n}$
$t_{DC_{AS\#1}} \leftarrow MAC(k_{DC_{AS\#1}}, m_{DC_{AS\#1}}||MF_3)$
Send: $m_{DC_{AS\#1}}||t_{DC_{AS\#1}}$
$m_{DC_{AS\#2}} = m_{DC_1}||m_{DC_2}|| \ldots ||m_{DC_n}$
$t_{DC_{AS\#2}} \leftarrow MAC(k_{DC_{AS\#2}}, m_{DC_{AS\#2}}||MF_3)$
Send: $m_{DC_{AS\#2}}||t_{DC_{AS\#1}}$
$m_{DC_{AS\#3}} = m_{DC_1}||m_{DC_2}|| \ldots ||m_{DC_n}$
$t_{DC_{AS\#3}} \leftarrow MAC(k_{DC_{AS\#3}}, m_{DC_{AS\#3}}||MF_5)$
Send: $m_{DC_{AS\#3}}||t_{DC_{AS\#3}}$
RL
AS#1
AS#2
DC
MF #3
DC
MF #4
RA
AS#3
DC
MF #1
DC
FL
MF #3
CC
MF #4
CC
BC
MF #1
CC
MF_3
MF_4
MF_5
MF_6
$m_{CC} = m_{CC_1}||m_{CC_2}|| \ldots ||m_{CC_n}$
$t_{CC} \leftarrow MAC(k_{CC}, m_{CC}||MF_3)$
Send: $m_{CC}||t_{CC}$
$m_{CC} = m_{CC_1}||m_{CC_2}|| \ldots ||m_{CC_n}$
$t_{CC} \leftarrow MAC(k_{CC}, m_{CC}||MF_4)$
Send: $m_{CC}||t_{CC}$
$m_{BC} = m_{BC_1}||m_{BC_2}|| \ldots ||m_{BC_n}$
$t_{BC} \leftarrow MAC(k_{BC}, m_{BC}||SF_2)$
Send: $m_{BC}||t_{BC}$
SF_1
SF_2

Fig. 3: LDACS A/G Control-Channel Protection

in the BCCH. When an AS has successfully completed the cell-attachment, it gets access to k_{BC} and can then proceed to verify the BCCH content's integrity and authenticity.

b) CCCH Protection: CCCH messages are concatenated as $m_{CC} \leftarrow m_{CC_1}||m_{CC_2}||...||m_{CC_n}$. Since four MF occur in one SF, the current MF_j is computable by $MF_j = SF_i \times 4 + 1$, whenever SF_i is announced. If no SF_i is announced in that MF, MF_j is incremented by one. MF_j acts as replay-protection mechanism and sequence number here. Then, the GS computes the CCCH MAC tag as follows: $t_{CC} \leftarrow \text{MAC}(k_{CC}, m_{CC}||MF_j)$. As long as that specific LDACS cell remains active, m_{CC} and t_{CC} are transmitted in the CCCH. When an AS has successfully completed the cell-attachment, it gets access to k_{CC} and can then proceed to verify the CCCH content's integrity and authenticity.

c) DCCH Protection: DCCH messages are concatenated as $m_{DC} \leftarrow m_{DC_1}||m_{DC_2}||...||m_{DC_n}$. Every AS shares its individual point-to-point key k_{DC} (denoted as $k_{DC_{AS\#1}}, k_{DC_{AS\#2}}$ etc. in Figure 3) with the GS. Up to 32 different DCCH slots can be allocated to 32 different AS per MF. As such, using MF_j again as replay-protection and sequence number is secure, despite having multiple DCCH slots occur per MF: combinations of the same sequence number and key never occur. Then, the AS computes the DCCH MAC tag as follows: $t_{DC} \leftarrow \text{MAC}(k_{DC}, m_{DC}||MF_j)$. As long as that specific LDACS cell remains active, m_{DC} and t_{DC} are transmitted in each DCCH slot. When an AS has successfully completed the cell-attachment, GS and AS have derived the shared k_{DC} key and can then proceed to verify the AS's DCCH slots content's integrity and authenticity.

IV. Evaluation and Results

First, security properties of the LDACS cell-attachment, especially for control-channel protection keys k_{BC}, k_{CC}, k_{DC}, are proven using the symbolic model-checking tool Tamarin [16]. Second, using the Framework for Aeronautical Communications and Traffic Simulations 2 (FACTS2), the LDACS protocol is fully implemented including the introduced control-channel protection scheme [17]. Then, LDACS performance is compared in terms of latency and user-data throughput with the scheme enabled, compared to the baseline with no control-channel protection.

A. Security Evaluation

a) Control Channel MAC Tag Length Evaluation: LDACS foresees AES-CMAC for the computation of MAC tags [12]. NIST SP 800-38B gives recommendations for the use of CMACs [18]: First, with the MAC tag length t_{len} providing protection against guessing attacks, an attacker can guess a correct MAC tag with a probability of $\frac{1}{2^{t_{len}}}$. Second, this attack type can further be mitigated by limiting the number of unsuccessful verification attempts for each key. Third, t_{len} should be at least 64 to provide sufficient protection against guessing attacks. Fourth, Equation (1) quantifies the risk with t_{len} being the MAC tag length, $MaxInvalids$ being the limit on the number of times that the MAC tags verification can fail before the key is retired, and $Risk$ the highest acceptable probability for an inauthentic message to pass the verification process [18].

$$t_{len} \geq log_2(MaxInvalids/Risk) \qquad (1)$$

If we set $MaxInvalids$ to the maximum amount of BCCH/CCCH/DCCH messages that can occur in a given times span. We assume a maximum AS length of stay of 3 hours per LDACS cell, which coincides with the k_{DC} validity period, and k_{BC}, k_{CC} updates every 24 h. This results in a maximum of $\approx 2^{19}$ BC, $\approx 2^{21}$ CC and $\approx 2^{18}$ DC MAC tag verification fails.

LDACS is designed for safety critical message exchanges. This means that the probability of a message with a guessed MAC being recognized as valid, i.e. $Risk$, must be below 10^{-9} or 2^{-30} [4].

With these two values for all control-channels, Equation (1) gives a minimum MAC tag value of 49 bit for BC, 51 bit for CC and 48 bit for DC messages. Based on these results and the third recommendation of [18], we recommend a MAC tag lenght of 64 bit for all control-channel MACs.

b) Tamarin Proof: Modelling the pre- and post-quantum key establishment variations, as well as the choice to send the $Cert_{GS}$ certificate in the last MAKE message (see Step 6 in

Figure 2) resulted in four models: one for a Diffie-Hellman based key exchange and one for a key transport scheme, resembling current post-quantum candidates for key establishment[1], times the GS certificate being stored at AS or not. The authentication property is modeled in Lowe's hierarchy of authentication specification as "injective agreement" [14], the consistency and perfect forward secrecy properties as defined in [14].

Proving the pre and post-quantum variations were done in the automatic mode and in both cases, all ten lemmas could be verified. All four Tamarin proofs are published on GitHub[2] and results can be seen in Table III. The lemmas *exists session*, *mutual authentication*, *session uniqueness*, *secrecy*, *perfect forward secrecy* and *key consistency* were proven with the Tamarin prover version 1.6.1.

TABLE III: Tamarin LDACS cell-attachment verification results. Pre- and post-quantum variations as "Pre" and "Post".

Lemma	Scope [-traces]	Result	#Steps	
			Pre	Post
Session Exists	Exists	✔	32	32
Mutual Authentication	All	✔	72	84
Session Uniqueness	All	✔	38	38
Secrecy	All	✔	146	122
PFS Secrecy	All	✔	146	122
Key Consistency	All	✔	1138	1066

B. *Performance Evaluation*

FACTS2 is a computer simulation framework based on service-oriented software architecture enabling an accurate simulation of LDACS, as verified with real radio hardware during flight trials [7], [19].

a) Cell-Attachment Performance: LDACS uses elliptic curve Diffie-Hellman and ECDSA signatures based on NIST P-256/P-384 curves on pre-quantum and Kyber-512/768 and Falcon-512/1024 on post-quantum security levels. This results in the cryptographic sizes summarized in Table IV. Results for one AS performing the cell-attachment protocol 100 times in an otherwise empty cell based on the design goal Bit Error Rate (BER) of LDACS, 10^{-6} [4], are given in Table V.

TABLE IV: Sizes of security additions in bit [b] and Byte [B].

Security Level	P_{GS}	P_{AS}	$\sigma_{\text{GS/AS}}$	Cert_{GS}	$OCSP$	$c_{k_{set}}$	$t_{\text{GS/AS}}$
1 (pre-q)	257b	257b	512b	348B	174B	776b	128b
2 (pre-q)	385b	385b	768b	396B	206B	1288b	256b
1 (post-q)	800B	768B	666B	1814B	776B	776b	128b
2 (post-q)	1184B	1088B	1280B	3324B	1390B	1288b	256b

Compared to values given in [12], latency improves by about 30% from 811 ms to 571 ms for pre-quantum levels.

b) Control-Channel Security Performance Impact: [20] analyzed the typical aeronautical data traffic pattern consisting of 76% 270 Byte high, 24% 1400 low priority Byte packets on the FL and 80% 121 Byte high, 20% 1400 low priority Byte packets on RL. Using this traffic pattern an experiment is designed which tests LDACS at full capacity: 1000 kbps FL/RL data modeled as exponential distribution and randomly assigned to 512 AS, at BER=10^{-6} with 100 seconds simulation time in LDACS acknowledged transmission mode. We compare the load on all channels, as well as the user-data throughput with and without control-channel security enabled.

TABLE V: 95th percentile latency [ms] and security data overhead [b] for the LDACS cell-attachment procedure.

Security Level	AS has Cert		AS needs Cert	
	[ms]	[b]	[ms]	[b]
1 (pre-q)	571	5473	571	8257
2 (pre-q)	571	7137	571	10,305
1 (post-q)	577	53,099	582	57,281
2 (post-q)	582	60,065	688	87,743

The first result of this experiment is that almost no user-data throughout is measured with control-channel security enabled. This is due to the 83 bit small DCCH. Here, 32-bit ACK messages signal the GS the successful reception of a user-data message. With a 64 bit DC MAC tag, these do not fit here anymore. As such, the experiment is repeated, but this time increasing the DC MAC tag size bit by bit. Results are depicted in Figure 4.

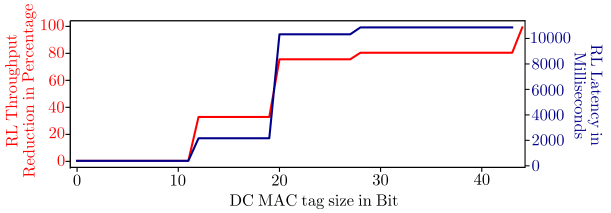

Fig. 4: DCCH MAC tag performance impact

Until 11-bit, the performance does not change but at a 12-bit DC MAC tag, LDACS performance already drops by 30%. Given that an ACK message must be sent per priority and the DCCH has a 8-bit CRC, this results a full 83-bit DCCH [4]. For the purpose of this evaluation the DC MAC tag is set to 11 bit and the experiment is run again. Results are shown in Table VI.

TABLE VI: LDACS control-channel security performance impact measured in average throughput

Type	Channel				
	BCCH	CCCH	DCCH	FL DCH	RL DCH
[kbps] w/o sec.	4.80	45.39	18.23	997.65	961.91
[kbps] w sec.	5.77	46.71	24.15	997.54	958.75
[%] sec. overhead	20.21	2.90	32.47	00.10	3.29

Table VI shows that while the security measures have a relatively large impact on the control-channel fullness (up to 32% increase in the DC case), the actual user-data throughput rate does not decrease by much. On FL only 0.10% and on RL 3.29% are measured. These results show the effeciveness of the design of LDACS control-channel security.

[1] https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022, accessed February 25, 2023

[2] https://github.com/zag0fop/LDACS_cell-attachment, accessed February 28, 2023

V. Conclusions

This study proposes authentication measures for LDACS control-channels and an improved cell-attachment protocol for establishing cryptographic keys. In the FL control-channels, two group keys are used to reduce security load by computing one MAC tag over all messages to different recipients. The LDACS inherent frame numbers are used for replay protection. On the RL control channel, a point-to-point key is established during cell-attachment and used to compute one MAC tag over the content of the entire DCCH slot.

The study evaluated the appropriate MAC tag length for LDACS control-channels and found that a 64-bit tag is suitable, but this is impossible for the DCCH. Here, the overall LDACS performance in acknowledged transmission mode already drastically decreases at a 12 bit MAC tag. This remains an open problem. The study also proved via Tamarin the necessary security properties of the introduced cell-attachment, and performance evaluations showed a 30% latency improvement. Furthermore, control-channel security measures had minimal impact on user-data throughput rates, decreasing performance by only 0.1-3%. In conclusion, this work addresses a key issue in the LDACS cybersecurity architecture, making an important contribution to LDACS security.

Acronyms

AS	Aircraft Station
BCCH	Broadcast Control Channel
CCCH	Common Control Channel
DCCH	Dedicated Control Channel
DCH	Data Channel
FL	Forward Link
GS	Ground Station
GSC	Ground Station Controller
LDACS	L-band Digital Aeronautical Communications System
MAKE	Mutual Authentication and Key Establishment
MF	Multi Frame
RACH	Random Access Channel
RL	Reverse Link
SAC	Sub-net Access Code
SF	Super Frame
UA	Unique Address

References

[1] M. S. B. Mahmoud, A. Pirovano, and N. Larrieu, "Aeronautical Communication Transition From Analog to Digital Data: A Network Security Survey," *Computer Science Review*, vol. 11-12, pp. 1–29, 2014.

[2] SESAR JU, "VDL Mode 2 Capacity and Performance Analysis," https://www.sesarju.eu/sites/default/files/documents/news/SJU_VDL_Mode_2_Capacity_and_Performance_Analysis.pdf (accessed January 20, 2023), European Union (EU), SESAR SJU Study v.1., 2015.

[3] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and G.-C. S., "Security in Digital Aeronautical Communications - A Comprehensive Gap Analysis," *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100549, 2022.

[4] 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 January 20, 2023), German Aerospace Center (DLR), Tech. Rep. SESAR2020 PJ14-02-01 D3.3.030, 2020.

[5] O. Osechas, S. Narayanan, O. C. Crespillo, G. Zampieri, G. Battista, R. Kumar, N. Schneckenburger, E. Lay, B. Belabbas, and M. Meurer, "Feasibility Demonstration of Terrestrial RNP with LDACS," in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, Florida, USA, 2019, pp. 3254–3265.

[6] N. Mäurer, T. Gräupl, and C. Schmitt, "L-Band Digital Aeronautical Communications System (LDACS)," RFC 9372, Mar. 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc9372

[7] 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*, vol. 58, no. 1, pp. 615–634, 2021.

[8] T. Gräupl *et al.*, "LDACS Flight Trials: Demonstration of ATS-B2, ATN-IPS, and Seamless Mobility," in *2023 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, Herndon, VA, USA, 2023.

[9] ARINC, "Internet Protocol Suite (IPS) for Aeronautical Safety Services Part 1 Airborne IPS System Technical Requirements," https://standards.globalspec.com/std/14391274/858p1 (accessed January 20, 2023), Aeronautical Radio, Incorporated (ARINC), Tech. Rep. ARINC SPECIFICATION 858P1, 2021.

[10] ICAO, "Doc 9776 - Manual on VHF Digital Link (VDL) Mode 2," http://www.icscc.org.cn/upload/file/20190102/Doc.9776-ENManualonVHFDigitalLink(VDL)Mode2.pdf (accessed January 20, 2023), International Civil Aviation Organization (ICAO), ICAO Doc 9776, 2015.

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

[12] N. Mäurer, T. Gräupl, C. Schmitt, G. Dreo-Rodosek, and H. Reiser, "Advancing the Security of LDACS," *IEEE Transactions on Network and Service Management*, pp. 1–15, 2022.

[13] D. Dolev and A. Yao, "On the Security of Public Key Protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[14] C. Boyd, A. Mathuria, and D. Stebila, *Protocols for Authentication and Key Establishment*. Berlin, Heidelberg, Germany: Springer, 2020.

[15] 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)*, San Antonio, TX, USA, 2021, pp. 1–10.

[16] S. Meier, B. Schmidt, C. Cremers, and D. Basin, "The TAMARIN Prover For The Symbolic Analysis Of Security Protocols," in *25th International Conference on Computer Aided Verification (CAV)*, Saint Petersburg, Russia, 2013, pp. 696–701.

[17] 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*, Miami Beach, FL, USA, 2019, pp. 63–66.

[18] NIST, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf (accessed January 20, 2023), National Institute of Standards and Technology (NIST), Tech. Rep. NIST SP800-38B, 2016.

[19] 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.

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