Proc. of the IWAC2022
pp. XX–XX, Oct. 2022

A Secure Ground Handover Protocol for LDACS

Nils Mäurer[1)†], Thomas Gräupl[1)], Corinna Schmitt[2)], Christoph Rihacek[3)], and Bernhard Haindl[3)]

[1)] *Institute of Communications and Navigation, German Aerospace Center (DLR), Wessling, Germany*
[2)] *Research Institute CODE, Universität der Bundeswehr München, Munich, Germany*
[3)] *Frequentis AG, Vienna, Austria*
[†] *email: nils.maeurer.de*

The L-band Digital Aeronautical Communications System (LDACS), the worldwide first true integrated Communication, Navigation and Surveillance (CNS) system, is in the process of being standardized at the International Civil Aviation Organization (ICAO) and the Internet Engineering Task Force (IETF). The cellular system is considered a successor to the 30-years old Very High Frequency (VHF) Datalink mode 2 system (VDLm2) and intended for communications related to the safety and regularity of flight. With the initial rollout planned in the near future, the finalization of all its aspects, including security is of utmost importance. While previous works presented a cybersecurity architecture for LDACS, including a Public Key Infrastructure (PKI), certificates, a Mutual Authentication and Key Establishment (MAKE) procedure, as well as usage of established keys for protecting its user- and control-data plane, the protocol for secure LDACS handovers between cells has not been established. The objective of this work is to present a secure handover procedure for LDACS, fulfilling all security and performance requirements for data- and voice communications via LDACS.

Key Words : L-band Digital Aeronautical Communications System (LDACS), Cybersecurity, Handover, Protocol

1. Introduction

June 28, 2019 remains the busiest day in European air traffic with EUROCONTROl registering 37,228 flights over the European continent[4)] at the time of this writing. With the COVID-19 pandemic reducing European air traffic by 55% from its 2019 level, recovery from the pandemic progresses and is estimated to be completed by 2024.[5)] As such, air travel levels similar to 2019 are to be expected again. This becomes problematic, as the current terrestrial datalink, VHF Digital Link Mode 2 (VDLm2) has reached its capacity limit by 2015 on single frequency usage and will reach its limit by 2025 when extended to a four-frequency mode.[2)] As such, latest by 2024, the limitations imposed by VDLm2 become a hindrance to civil aviation growth once more.

The current Single European Sky ATM Research (SESAR) envisioned successor to VDLm2 for European Air Traffic Management (ATM) communications, 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.[6,7)] Since 2018 LDACS is under standardization in International Civil Aviation Organization (ICAO)[10)] and the Internet Engineering Task Force

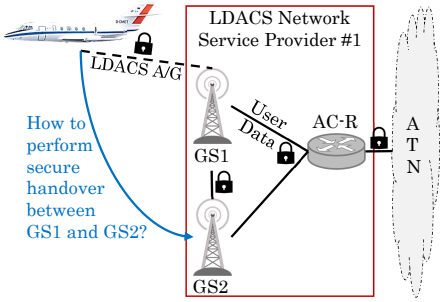

Fig. 1 Objective of this paper is depicted in blue.

(IETF),[9)] with Standards And Recommended Practises (SARPS) development expected to be completed in 2022. LDACS has successfully been validated in flight trials.[6,8)]

As LDACS is envisioned to deliver safety related ATS and AOC traffic via the ATN/IPS,[12)] link layer security imposed by regulatory documents ICAO Doc 9896[12)] or ARINC 858[11)] applies. The current LDACS security architecture foresees the usage of a dedicated LDACS Public Key Infrastructure (PKI), mutual authentication of ground and aircraft, key establishment, key derivation, protection of user and control channels, as well as multiple security levels to cope with future requirements on security.[13–15)] While LDACS A/G security has progressed far, a security concept for

ground connections is missing as of the time of this writing. Since LDACS transports data, a well as voice traffic, a fast, seamless handover between Ground Stations (GSs), e.g., due to dropping Signal-to-Noise Ratio (SNR), is of high importance to ensure the safe and timely delivery of voice data between air and ground. However, no concept for timely negotiating fresh key material and possibly re-authentication between new GS and Aircraft Station (AS) has been developed yet.

The objective of this paper is to develop a secure handover procedure between different GS and AS within the same LDACS network service provider domain as pointed out in Figure 1.

In Section 2. relevant technical and security details of LDACS are presented before looking at related works on secure handover procedures. Before the secure ground handover procedure can be developed, requirements and prerequisites must be defined, which happens in Section 3.. Additionally the evaluations methodology via the German Aerospace Center (DLR) air traffic simulator FACTS2 and the symbolic model checker Tamarin is presented. With prerequisites defined, the actual procedure is presented in Section 4.. In Section 5. evaluations on its security and performance are presented before concluding in Section 6..

2. Background on LDACS

LDACS is a ground-based digital bidirectional communications system for flight guidance and communications related to the safety and regularity of flight.[6,7] It covers current Air Traffic Services (ATS), Aeronautical Operational Control (AOC) data, digital voice and also foresees future applications, such as 4D trajectories. In the context of ICAO's Future Communications Infrastructure (FCI), LDACS is considered a link-layer network access technology for the Aeronautical Telecommunications Network (ATN)/IP-Protocol Suite (IPS). A single LDACS cell, operated by the LDACS GS, serves up to 512 AS and communications directions are denoted as Forward Link (FL) for ground-to-aircraft and Reverse Link (RL) for aircraft-to-ground. As it offers channel quality depending Coding and Modulation Scheme (CMS), a net user-data rate of 230 to 1428 kbps in the FL and 235 to 1390 kbps in the RL per LDACS cell is achievable, which is up to 90 times the net capacity compared to VDLm2.[1] Additionally, LDACS introduces message priorities into this domain and allows more important messages, such as ATS data, to be scheduled with a higher priority, reaching its destination faster than low prioritized messages. LDACS user-data, be it voice or otherwise, is transported via the Data Channel (DCH) while its control-data is split between four logical channels: (1) Broadcast Channel (BCCH) in the FL for GS broadcast cell information, (2) Common Control Channel (CCCH) in the FL for GS allowing to allocate resources to certain AS, enabling them to send user-data in the RL DCH, (3) Random Access Channel (RACH) for AS allowing to request cell entry, (4) Dedicated Control Channel (DCCH) in the RL enabling AS to request resources to send user-data. These channels appear at fixed locations in time, as defined by the LDACS frame structure [1, Chap. 8.5.3]. Over 240 ms there is the superframe, consisting of a 6.72 ms BCCH (in FL)/RACH (in RL) block followed by four multi-frames. These 58.32 ms long frames consist of blocks of DCH (in FL and RL) and CCCH (in FL)/DCCH (in RL). In the security context, ATS/AOC user-data in the FL/RL DCH, as well as RACH and DCCH control-data is considered as "point-to-point", while voice user-data in the FL/RL DCH[1], as well as BCCH and CCCH control-data is considered as "broadcast" transmission. As such, different protection mechanisms for point-to-point and broadcast transmissions are required.

LDACS security is based on a dedicated PKI, with pre- and post-quantum certificates rolled out and installed in AS and GS, along with certificate revocation checks to confirm the validity of used certificates during communications. When an AS comes into the vicinity of a GS, the *CellEntry* procedure takes place, allowing AS and GS to communicate via the DCH,[1] without allowing actual ATN/IPS traffic yet. First, a Mutual Authentication and Key Establishment (MAKE) protocol follows, resulting in AS and GS having mutually authenticated each other and established keys to secure its communications. Only then, ATN/IPS traffic is secured via exchanged keys and relayed between aircraft and ground.

2.1. Secure Handover Protocols

One of the most prominent mobility handover protocol is IKEv2 Mobility and Multihoming Protocol (MOBIKE),[18] which is based on the well known Internet Key Exchange version 2 (IKEv2).[19] While a new round of authentication and key establishment, based on elliptic curve cryptography, takes roughly 8,000 Bytes, MOBIKE handles the transition between IPs for the target host within roughly 500 Bytes. The general idea of MOBIKE is that once an IKEv2 has concluded successfully and a secret key (denoted in

[1] This is done mainly to maintain the party-line effect as elaborated by Gräupl et al. in.[17]

RFC 7296 as SK) has been established between initiator and responder, that SK is used to encrypt changing addresses and Security Associations (SAs), while basically retaining the same crytographic material, i.e., the same shared key SK. This avoids expensive key renegotiation and finishes the transition between IPs within (typically) four messages. However, for the LDACS case, freshly negotiated key material with minimum performance overhead is necessary, hence MOBIKE is not directly applicable to LDACS.

Another candidate is Mobile IPv6 Fast Handovers - RFC 5268.[20] It relies on IPSec[23] and IKEv2[19] to establish security associations. These are used to at least protect integrity and data origin authentication for the "handover initiate" and "handover acknoledgement" message in the proposed handover protocol. This protocol is also not directly applicable to LDACS, since again security associations are reused, instead of freshly negotiated.

Hence related standardized protocols do not fulfill requirements of LDACS and a new ground-handover protocol is necessary.

3. Design Goals and Prerequisites

The overall goal of the secure handover procedure is to enable a seamless handover between cells for the AS. The current LDACS specification foresees two handovers: one where interconnected adjacent GSs are coordinating the handover, and one where no coordination among GSs takes place (e.g., GSs are not interconnected).[1]

Since the second case works by terminating the old connection and establishing a new one with another GS, which results in breaking off the connection via a *CellExit* message with the old GS and the initiating a new connection with the new GS by running a new *Cell- Entry* and MAKE procedure resulting in establishing new keys with the new GS. Since a secure *Cell-Entry* and MAKE procedure have already been presented,[14] the focus of this work lies on on the first case, the handover type 2 as by the official LDACS specification.[1]

3.1. Assumptions

Several assumptions are required to design the intended security for MAKE[14] allowing a secure cell handover. Investigations in[14,25] led to the following four assumptions:

Assumption 1 *Data leaving the LDACS physical layer is error corrected as much as possible, with a residual Bit Error Rate (BER) of* 10^{-6} *at the working point of LDACS.*[1]

Assumption 2 (PKI)

- *AS and GSs are integrated in the LDACS PKI.*
- *A Certificate Distribution Center (CDS) is in place, which is responsible for the secure distribution of AS and GS certificates.*
- *An Online Certificate Status Protocol (OCSP) server is in place for certificate revocation purposes.*
- *GS and CDS are connected via an authenticated, encrypted channel.*
- *AS and GSs have stored locally an unrevoked, valid CA certificate* $Cert_{CA}$
- *AS and GSs have certificates for each* ($Cert_{AS}$, $Cert_{GS_1}$, $Cert_{GS_2}$) *and access to their respective private keys* ($PrivKey_{AS}$, $PrivKey_{GS_1}$, $PrivKey_{GS_2}$)

Assumption 3 *Certificate authorities of the LDACS PKI are trusted.*

Assumption 4 *All GS within one LDACS Network (NW) service provider domain are similarly configured, offering at least the security level (cf.*[14]*), that is initially established during the first MAKE. As such cipher-suites and choice of algorithms can be reused when switching between different GS of the same LDACS NW service provider.*

3.2. Prerequisites

As mentioned at the beginning of Section 3., several steps have to be performed before a handover can take place. These are briefly described in the following.

Entities (i.e., GSs) within the LDACS subnet hosted by the same LDACS NW service provider establish a secure (ground) channel among each other (as per [21, Chap. 2.8.2]). As this part is not the focus of this work, here are three suggestions on how to achieve this: (1) using Transport Layer Security (TLS) on transport[22] or (2) IPSec on network layer,[23] (3) inherent security features of the ATN/IPS.

When an AS comes into the vicinity of an LDACS cell (i.e., a GS), a successful *CellEntry* and MAKE procedure take place, resulting in AS having gained access to the LDACS cell. With that, the AS has registered successfully to an LDACS cell of one LDACS network service provider as shown in Figure 1. AS and GS now communicate via a secure channel using the following keys:

- $K_{AS,GS}$: AS, GS shared key used to (encrypt and) authenticate user-data packets between

AS and GS.

- K_{voice}: LDACS NW service provider wide group key, shared by all GSs to authenticate voice user-data traffic (as per[17]).
- K_{BC}: LDACS NW service provider wide group key, shared by all GSs to authenticate data in the BCCH and thus providing one layer of security to the LDACS Alternative Positioning Navigation and Timing (APNT) concept (as per[24]).
- $K_{CC_{GS}}$: LDACS GS cell wide group key protecting CCCH based traffic via Message Authentication Code (MAC) computed at GS and verified at AS (as per[15]).
- $K_{DC_{AS,GS}}$: AS, GS shared key used to authenticate control-data packets in the DCCH (as per[15]).

AS and GS communicate securely for a time, using the described keys and algorithms such as AES-CMAC or AES-CCM[14] and the AS measures the SNR to its current and other, nearby GS. During that process, that AS already obtains the addresses of nearby stations: UA_{GS_2} and SAC_{GS_2}. Once the SNR drops below a certain threshold (as per [1, Chap. 7]), a handover is triggered, which is exactly where the contribution of this work begins.

3.3. Requirements

The realized handover procedure in LDACS builds on security and performance requirements we need to ensure. Further it need to be kept in mind that in the context of ICAO's FCI, LDACS is considered a link-layer network access technology for the ATN/IPS. Our requirements are briefly mentioned here in order to understand our taken decisions in the final implementation.

3.3.1. Security Requirements

As shown in Figure 1, ATS/AOC data is provided by air traffic control via the ATN/IPS, and as such secured on transport layer by Datagram TLS.[16] However, ATN/IPS link-layer network access technologies also need to provide separate security measures for a defense in depth approach. More specifically, "*a secure channel between the airborne radio systems and the peer radio access endpoints on the ground is necessary to ensure authentication and integrity of air-ground message exchanges in support of an overall defense-in-depth security strategy*".[11]

As such, in[14] the *CellEntry* received new security functionalities and the MAKE procedure was updated from its initial draft in,[13] with LDACS user-data packets also receiving new fields for MACs and encryption options. As the here presented implementation builds on the existing MAKE procedure, it is clear that the defined security goals need to be ensured here as well. These are the following ones:

Security Goal 1 *Unilateral authentication of AS and GS following [21, Def. 14].*

Security Goal 2 *A shared session key should be established between GS and AS such that the key is fresh and known to at most GS and AS (following [21, Def. 15]). This includes key authentication, integrity and confirmation according to [21, Def. 17, 18] as well as strong mutual entity authentication of AS and GS following [21, Def. 13, 14].*

Security Goal 3 *The protocols should allow the parties to achieve (perfect/full) forward secrecy according to [21, Def. 21], integrity (according to [21, Def. 9]) and (optional) confidentiality (according to [21, Def. 4-7]) protection for LDACS user plane (DCH) and control plane (BC, CC, and DC channel) .*

For the secure handover procedure to fulfil these security requirements, some information from the secure channel establishment between AS and GS_1 (i.e., the "old" GS, the AS is connected to prior to a handover) is reused, while other information need to be re-negotiated between AS and GS_2 (i.e., the new GS to which the AS connects via handover):

- Since the UA is a permanent address, it is re-used again.
- By Assumption 4, different GS in the same subnet offer at least the same security level, hence cipher-suites `EPLDACS/CCLDACS` and the cipher-suite choice `algo` can be re-used.
- Finally, group keys, used by all GSs of the same service provider, can be re-used, such as K_{voice} and K_{BC}.
- Since AS and GS_1 , as well as GS_1 and GS_2 are mutually authenticated, trust between AS and GS_2 could implicitly be assumed. However, to fulfil Security Goals 1 and 2, a new mutual authentication between AS and GS_2 is performed. As such, new signatures (denoted σ_A) are exchanged.
- To fulfil Security Goals 2 and 3, new ephemeral (for pre-quantum; key encapsulation for post-quantum per[14]) values need to be exchanged and a new set of individual-connection-specific or cell-specific keys, de-

fined in Section 3.2. need to be established and derived between AS and GS_2.

To evaluate, that the proposed protocol fulfils these security properties, it is implemented and evaluated in the symbolic model checker Tamarin.[27)]

3.3.2. Performance Requirements

The first requirement is that the secure handover procedure should have less security data overhead than a complete, new *CellEntry* and MAKE procedure between AS and new GS_2. Table IX in[25)] lists these spanning 3,594, 4,682, 21,056, 38,544 bit without the additional exchange of a GS certificate and 6,378, 7,850, 35,568, 65,136 bit with GS certificate exchange.

The second requirement is that the secure handover procedure latency remains below the *CellEntry* and MAKE procedure latency of 811 ms.[25)] However, this is not enough, as voice data shall be transmitted seamlessly when an AS is switching cells. In[17)] the time from push-to-talk to successful reception of voice packet is listed as 118 ms in FL and 104 ms in RL, both in the 95%. As such, the handover procedure should not lead to more downtime (i.e., when switching between GS_1 and GS_2) than two multi-frames (i.e., 120 ms which is roughly two multi-frames as stated in Section 2.) of latency.

To evaluate the performance of the procedure depicted in Protocol 2, we implement it in the German Aerospace Center (DLR) air traffic simulator FACTS2[26)] and measure latency and security data overhead.

4. The Secure Handover Protocol

Here we present the secure handover protocol, which enables a seamless handover between cells for the AS. The notation for Protocol 2 is detailed in Table 1.

The protocol structure, along with computations of MAC or SIG, follow the work presented in.[14)] At the top of Figure 2, initially exchanged values from the prior *CellEnry* and MAKE procedure are listed.

AS: It triggers the "HO request" command, for which it either generates Diffie-Hellman Key Exchange (DHKE) (in the pre-) or Key Encapsulation Mechanism (KEM) (in the post-quantum case) values, a new nonce, a signature encapsulating all these values, Authenticated Encryption with Associated Data (AEAD) encrypts all of that, including its source and destination address (UA_{GS2}) with the AS-GS1 shared key $K_{AS,GS1}$, and sends it to the currently connected GS1.
GS1: *msg1* is decrypted, then AEAD encrypted with the GS1-GS2 shared key $K_{GS1,GS2}$ and forwarded to GS2.

Table 1 Notation for Protocol 2

Field	Description
UA_A	Permanent Unique Address of A
SAC_A	Temporary Sub-net Access Code of A
$Cert_A$	Certificate of A
$OCSP_{Cert_A}$	OCSP response to $Cert_A$
`scgs`	Field indicating whether AS stores GS certificate locally (=1) or not (=0)
$PrivKey_A$	Private Key of A
N_A	Nonce of A
P_A	Public part of DHKE/KEM of A
x_A	Private part of DHKE/KEM of A
`EPLDACS`	Cipher-Suite - MAKE and user-data protection options
`CCLDACS`	Cipher-Suite - control-data protection options
`algo`	Cipher-Suite choice from `EPLDACS`
m_A	MAC of A
σ_A	Signature of A
Keys	$K_{BC}, K_{CC}, K_{DC_{A,B}}, K_{voice}, K_{A,B}$ as in Sec. 3.2.

GS2: Here the message is decrypted and the AS signature verified. When the verification passes, also DHKE (in the pre-) or KEM (in the post-quantum case) values are generated, via a Key Derivation Function (KDF) with AS-GS2 shared secret, nonces and addresses, the new AS-GS2 keys are derived and the new CCCH protection key encrypted. A GS2 MAC (for key confirmation purposes at the AS), and a GS2 signature is computed, before, depending on the AS choice in `scgs`, the GS2 certificate along *OCSP* response is attached. Lastly, all that (denoted *msg2*) is encrypted again with the GS1-GS2 key.
GS1: *msg2* is once again de- and encrypted.
AS: *msg2* or the "HO command" is decrypted, similarly to the procedure at GS2, the new AS-GS2 shared keys are derived, GS2 MAC and signature verified and the new CCCH key decrypted. With GS2-AS authentication and key confirmation in place, the AS triggers the *CellExit* command.
GS1: It informs GS2 about the successful handover.
After this, AS and GS2 can start communicating securely.

5. Evaluation

Here, the protocol presented in Figure 2 is evaluated whether it fulfils necessary requirements stated in Section 3.3..

5.1. Security Evaluation

We implemented the secure LDACS handover procedure in Tamarin and differentiated between the cases that pre-quantum, i.e., DHKE, key establishment, post-quantum, i.e., KEM, key establishment is used, that the AS is in possession of the GS2 certificate (denoted "A" in Table 2)and that AS needs an au-

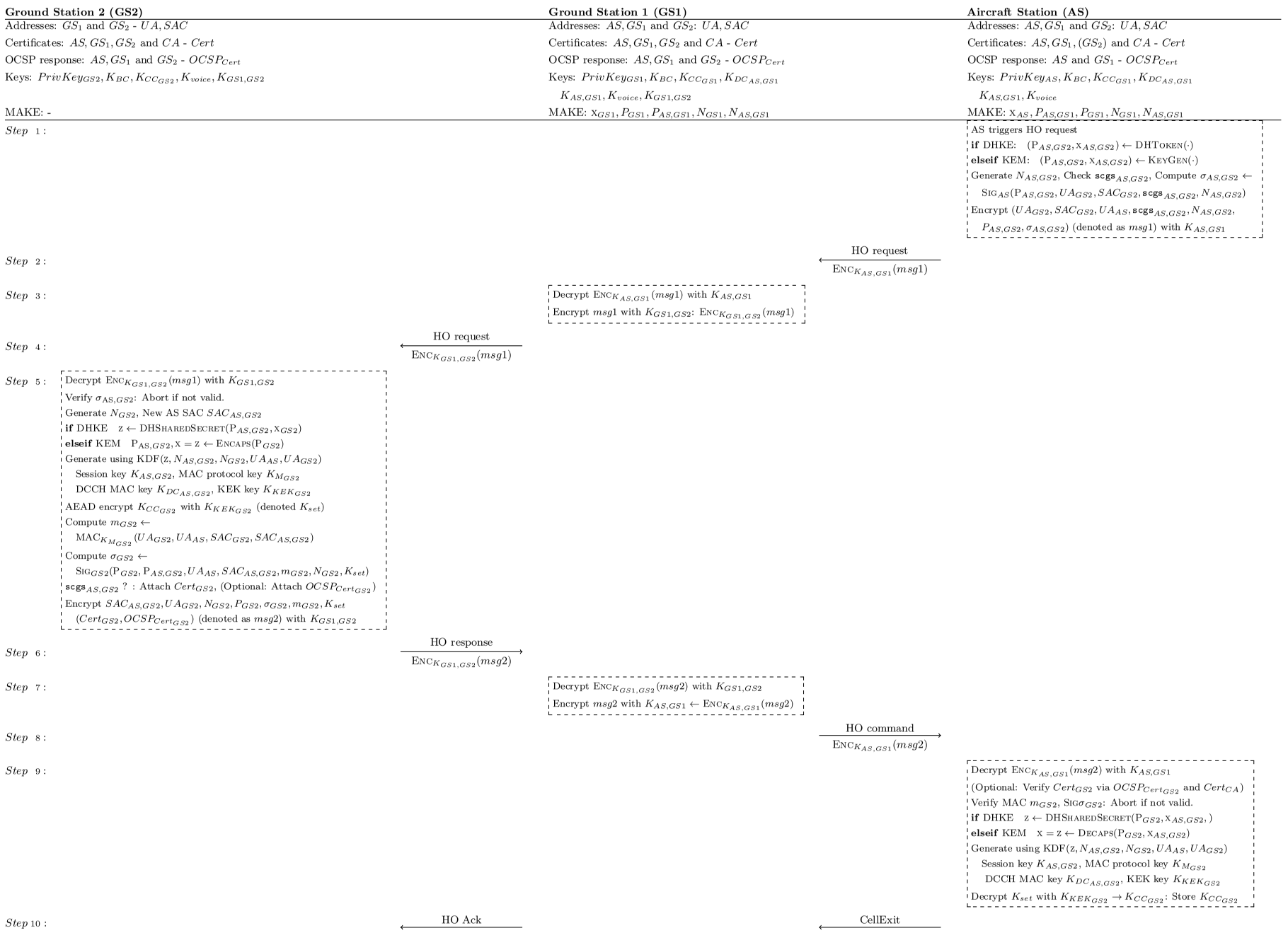

Fig. 2 LDACS Secure Ground Cell Handover protocol with Fresh Key Renegotiation

thentic copy of the GS2 certificate (denoted "B" in Table 2). This resulted in four different files, which can be found at `https://github.com/NilsMaeurer/LDACSSecureCellHandover`. We tested for a successful trace in one and multiple sessions, allowing the attacker to obtain values from previous sessions, as well as for "mutual-authentication", "session uniqueness", "key consistency" in both directions (from the perceptive of AS and GS2), and for "perfect forward secrecy" as set and defined in Section 3.3.. The lemmas were tested on a Ubuntu 20.04, WSL 2.0 machine with 64GB RAM and an Intel(R) Core(TM) i7-8850 6-Core processor.

Table 2 Tamarin results of LDACS secure handover

Lemma	Scope (traces)	Result	#Steps Pre- A	Pre- B	Post- A	Post- B
Session Exists	Exists	✔	27	28	26	27
2 Sessions Exist	Exists	✔	52	54	50	52
Mutual Authentication	All	✔	43	44	27	28
Perfect Forward Secrecy	All	✔	26	26	28	28
Session Keys Consistency	All	✔	152	155	86	89
Session Uniqueness	All	✔	28	30	28	30

As seen in the results in Table 2, all necessary security properties from Section 3.3.1. are fulfilled by the proposed LDACS secure ground handover procedure.

5.2. Performance Evaluation

Following the same primitive sizes as given in [25, Table VIII] and,[1)] the proposed LDACS secure ground handover procedure requires security data as indicated in Table 3.

Based on these sizes, we implemented the handover protocol in FACTS2 and evaluated the latency of the entire procedure (from "HO request" transmission from AS to *CellExit* reception at GS1) at BER= 10^{-6}, following Assumption 1, as well as (2) the total "down-time" of the connection (from *CellExit* transmission from AS to first GS2 data transmission to AS). Results are depicted in Table 3.

Comparing MAKE security data overhead sizes from Section 3.3.2.[25)] with values from Table 3, a big improvement is apparent for the "no GS certificate exchange" column, while values in the other remain comparable. In terms of latency, a huge improvement of up to a factor of 2.47 is observable. Lastly, the average down-time induced by switching cells remains at 26 ms, which is far below the required 120 ms.

Table 3. LDACS secure handover data overhead and latency

SL	Data Overhead `scgs=1`	Data Overhead `scgs=0`	Total Latency	"Down-time"
1 pre-q	2,115 bit	6,291 bit	328 ms	26 ms
2 pre-q	3,331 bit	8,147 bit	328 ms	26 ms
1 post-q	14,761 bit	35,481 bit	358 ms	26 ms
2 post-1	27,721 bit	65,433 bit	420 ms	26 ms

6. Conclusions

This work presents the first secure LDACS ground handover procedure, that fulfils both security and performance requirements posed by LDACS and according regulatory documents. We presented background information on LDACS and its current security architecture, stated design goals, assumptions, prerequisites and requirements and, based on these designed the secure LDACS ground handover procedure based on the MAKE procedure introduced in.[14,25)] We then implemented a symbolic proof of the protocol via Tamarin and could prove that all security requirements such as "mutual authentication", "perfect forward secrecy", "session uniqueness" and "key consistency" are fulfilled. With a performance evaluation in FACTS2, we could demonstrate a latency improvement of 2.5 compared to a break-before-make handover, which would result in the re-run of *CellEntry* and MAKE.

Future work consists of designing handover procedure between different LDACS subnets hosted by different LDACS network service providers.

Acronyms

AEAD	Authenticated Encryption with Associated Data
AOC	Aeronautical Operational Control
APNT	Alternative Positioning Navigation and Timing
AS	Aircraft Station
ATN	Aeronautical Telecommunications Network
ATM	Air Traffic Management
ATS	Air Traffic Services
BCCH	Broadcast Channel
BER	Bit Error Rate
CCCH	Common Control Channel
CDS	Certificate Distribution Center
CMS	Coding and Modulation Scheme

DCCH	Dedicated Control Channel
DCH	Data Channel
DHKE	Diffie-Hellman Key Exchange
FCI	Future Communications Infrastructure
FL	Forward Link
GS	Ground Station
ICAO	International Civil Aviation Organization
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange version 2
IPS	IP-Protocol Suite
KDF	Key Derivation Function
KEK	Key Encryption Key
KEM	Key Encapsulation Mechanism
LDACS	L-band Digital Aeronautical Communications System
MAC	Message Authentication Code
MAKE	Mutual Authentication and Key Establishment
MOBIKE	IKEv2 Mobility and Multihoming Protocol
NW	Network
PKI	Public Key Infrastructure
RACH	Random Access Channel
RL	Reverse Link
SNR	Signal-to-Noise Ratio
TLS	Transport Layer Security
VDLm2	VHF Digital Link Mode 2

References

1) T. Gräupl, C. Rihacek, B. Haindl, LDACS A/G Specification, SESAR2020 PJ14-02-01 D3.3.030, German Aerospace Center (DLR) (December 2020).

2) SESAR JU, VDL Mode 2 Capacity and Performance Analysis, European Union (EU), https://www.sesarju.eu/sites/default/files/documents/news/SJU_VDL_Mode_2_Capacity_and_Performance_Analysis.pdf, accessed 06/02/2022, (November 2015).

3) M. Slim, B. Mahmoud, A. Pirovano, N. Larrieu, Aeronautical Communication Transition From Analog to Digital Data: A Network Security Survey, Computer Science Review 11 (2014) 1–29. doi:10.1016/j.cosrev.2014.02.001.

4) EUROCONTROL, New traffic record set: 37,228 flights in one day, EUROCONTROL press release, https://www.eurocontrol.int/news/new-traffic-record-set-37228-flights-one-day, accessed 05/02/2022, (July 2019).

5) EUROCONTROL, Daily Traffic Variation - States, EUROCONTROL, https://www.eurocontrol.int/Economics/DailyTrafficVariation-States.html, 05/02/2022, (May 2022).

6) M. A. Bellido-Manganell, T. Gräupl, O. Heirich, N. Mäurer, A. Filip-Dhaubhadel, D. M. Mielke, L. M. Schalk, D. Becker, N. Schneckenburger, M. Schnell, LDACS Flight Trials: Demonstration and Performance Analysis of the Future Aeronautical Communications System, IEEE Transactions on Aerospace and Electronic Systems (2021), pp. 1–19. doi:10.1109/TAES.2021.3111722.

7) M. Schnell, U. Epple, D. Shutin, N. Schneckenburger, LDACS: Future Aeronautical Communications For Air-Traffic Management, IEEE Communications Magazine (2014), pp. 104–110, doi:10.1109/MCOM.2014.6815900

8) 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, M. Schnell, Flight Trial Demonstration of Secure GBAS via the L-band Digital Aeronautical Communications System (LDACS), IEEE Aerospace and Electronic Systems Magazine 36 (4), (April 2021), pp. 8–17. doi:10.1109/MAES.2021.3052318.

9) N. Mäurer, T. Gräupl, C. Schmitt, L-band Digital Aeronautical Communications System (LDACS), Internet-Draft draft-ietf-raw-ldacs-10, Internet Engineering Task Force, work in Progress (March 2022). https://datatracker.ietf.org/doc/html/draft-ietf-raw-ldacs-10.

10) ICAO, Finalization of LDACS Draft SARPs - Working Paper WP05 including Appendix, Tech. rep., International Civil Aviation Organization (ICAO) (October 2018).

11) Aeronautical Radio, Incorporated (ARINC), Internet Protocol Suite (IPS) for Aeronautical Safety Services Part 1 Airborne IPS System Technical Requirements, Arinc report 858p1, ARINC (June 2021).

12) ICAO, Doc 9896 — Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols, Tech. rep., International Civil Aviation Organization (ICAO), https://standards.globalspec.com/std/10026940/icao-9896, accessed 04/13/2022 (January 2015).

13) N. Mäurer, and A. Bilzhause, A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS), in: 37th Digital Avionics Systems Conference (DASC), IEEE, London, UK, 2018, pp. 1–10. doi:10.1109/DASC.2018.8569878.

14) N. Mäurer, T. Gräupl, C. Gentsch, T. Guggemos, M. Tiepelt, C. Schmitt, G. D. Rodosek, A Secure Cell-Attachment Procedure of LDACS, in: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 2021, pp. 113–122. doi:10.1109/EuroSPW54576.2021.00019.

15) T. Ewert, N. Mäurer, T. Gräupl, Group Key Distribution Procedures for the L-Band Digital Aeronautical Communications System (LDACS), in: 40th Digital Avionics Systems Conference (DASC), IEEE, San Antonio, USA, pp. 1–10. doi:10.1109/DASC52595.2021.9594319.

16) E. Rescorla, H. Tschofenig, N. Modadugu, The Datagram Transport Layer Security (DTLS) Protocol Version 1.3, RFC 9417 (April 2022), pp. 1–61. doi:10.17487/RFC9147. https://www.rfc-editor.org/info/rfc9147.

17) T. Gräupl, N. Mäurer, L. Jansen, T. Ewert, B. Haindl, C. Rihacek, LDACS Broadcast Digital Voice Concept and Expected Performance, in: 22nd Integrated Communications, Navigation and Surveillance Systems (ICNS) Conference, IEEE, Washington, USA, April 2022, pp. 1–10.

18) P. Eronen, IKEv2 Mobility and Multihoming Protocol (MOBIKE), RFC 4555 (June 2006), pp. 1–33. doi:10.17487/RFC4555. https://www.rfc-editor.org/info/rfc4555.

19) C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7296 (October 2014), pp. 1–142. doi:10.17487/RFC7296. https://www.rfc-editor.org/info/rfc7296.

20) R. Koodle, Mobile IPv6 Fast Handovers, RFC 5268 (June 2008), pp. 1–48. doi:10.17487/RFC5268. https://www.rfc-editor.org/info/rfc5268.

21) C. Boyd, A. Mathuria, D. Stebila, Protocols for Authentication and Key Establishment, Vol. 1, Springer, January 2018. doi:10.1007/978-3-662-58146-9.

22) E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446 (August 2018). doi:10.17487/RFC8446. https://www.rfc-editor.org/info/rfc8446.

23) S. Kent, K. Seo, Security Architecture for the Internet Protocol, RFC 4301 (December 2005). doi:10.17487/RFC4301. https://www.rfc-editor.org/info/rfc4301.

24) Osechas, Okuary, et al. 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). 2019.

25) N. Mäurer, T. Gräupl, C. Schmitt, G. Dreo-Rodosek, H. Reiser, Advancing the Security of LDACS, submitted to theIEEE Transactions on Network and Service Management, pp. 1–14, (June 2022).

26) T. Gräupl, N. Mäurer, 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, pp. 63–66, 2019.

27) S. Meier, B. Schmidt, C. Cremers, D. Basin, The TAMARIN Prover For The Symbolic Analysis Of Security Protocols, in: 25th International Conference on Computer Aided Verification (CAV), Springer, pp. 696–701, 2013.