Performance-optimizing Secure GBAS over LDACS

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

***Abstract*—VHF Data Broadcast (VDB) currently used by GBAS has been identified as a potential source of cyber-security concerns. The use of an alternative datalink providing the bandwidth for more capable security protocols has therefore been proposed and demonstrated on the basis of the L-band Digital Aeronautical Communication System (LDACS). However, the first demonstration of secure GBAS over LDACS suffered from some performance degradation. This paper provides an improved method for secure GBAS over LDACS on the basis of a rigid performance analysis. Optimized parameters are derived and evaluated. The results point the way for further performance enhancements for even more challenging GBAS scenarios.**

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

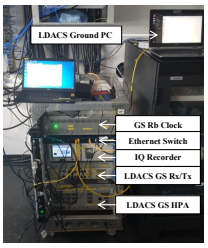
I. Introduction

The Ground Based Augmentation System (GBAS) is used to improve the accuracy of Global Navigation Satellite Systems (GNSSs) to allow GNSS-based instrument landings of aircraft. It is based on reference stations with known positions at airports, which generate correction data and integrity parameters from GNSS measurements. Correction and integrity data are transmitted to approaching aircraft. Based on this data, aircraft can calculate their position with precision and confidence in the integrity of the solution. GBAS enables modern aircraft to perform safe and secure GNSS-based landings while offering advantages over the Instrument Landing System (ILS) commonly used today [7].

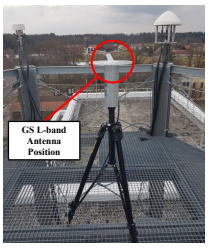
GBAS requires a datalink to transmit GNSS correction data to the on-board avionics of the aircraft. As of now, this datalink is specific to GBAS: The VHF Data Broadcast (VDB). [12]

The VDB datalink has been identified as potentially limiting the evolution of GBAS: Lee et al. have critized that VDB can only transmit corrections for the L1 frequency of GPS satellites, which may be problematic in terms of availability in equatorial zones [11]. Feuerle et al. and Stanisak et al. have noted that VDB does not provide sufficient throughput for correction and integrity data for multiple constellations and frequencies [8], [16]. Finally, Felux et al. and Garcia et al. have called attention to the issue that VDB does not provide cyber-security measures on par with modern wireless systems [6], [9]. This lead Felux et al. to propose the use of an alternative datalink for GBAS [9]: The L-band Digital Aeronautical Communication System (LDACS), which is a general purpose broadband datalink for aeronautical communication related to safety and regularity of flight [15].

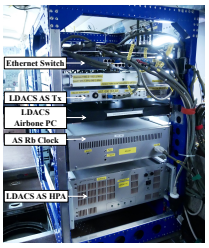
(a) DLR's research aircraft Falcon 20-E5 (D-CMET).



(b) Ground station



(c) LDACS antenna



(d) A/C installation

Fig. 1: Airborne and ground GBAS/LDACS equipment

GBAS over LDACS was demonstrated by Mäurer et al. in the MICONAV project[1] [12]. The results demonstrated the general feasibility of GBAS over LDACS. It showed that the GAST-C[2] and GAST-D[3] requirements can be satisfied. In addition to these performance goals, the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol was used to authenticate GBAS broadcast data demonstrating *secure* GBAS. However, the result obtained during MICONAV also revealed the need for a more optimized approach of integrating GBAS, TESLA security, and LDACS protocols.

This work proposes an improved method for transmitting TESLA secured GBAS correction data over LDACS resulting in overall better performance. The results in this paper were obtained by analysing the performance of an improved implementation of the MICONAV demonstration, while using the actual LDACS latency measurements recorded during the flight trials.

[1]Migration towards Integrated COM/NAV Avionics (MICONAV) was a research project co-funded by the LuFo program of the Federal Republic of Germany.

[2]Supporting category I precision approach capability.

[3]Supporting category II/III precision approach capability.

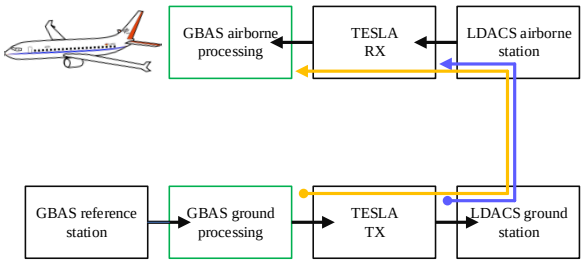


Fig. 2: Experimental setup of Mäurer's demonstration of GBAS over LDACS. The blue and orange arrows indicate the reference points at which the LDACS (blue) and secure GBAS latency (orange) was measured. The applicability of the GAST latency requirements is indicated in green.

II. Mäurer's Demonstration of GBAS over LDACS

GBAS over LDACS was first demonstrated in the MICONAV project as reported by Mäurer et al. [12] and Bellido et al. [3]. The main purpose of the GBAS over LDACS experiment was to demonstrate the ability of LDACS to provide a secure, broadband datalink for GBAS. For this purpose a co-located LDACS ground station and GBAS reference station, as well as a software-based GBAS receiver were deployed for flight trials in the vicinity of Munich, Germany. GBAS ground processing in the ground station (Fig. 1b and 1c) generated correction and integrity data from the received GNSS signals. This data was forwarded to the LDACS ground-station software. It was then cryptographically authenticated with the TESLA protocol. The secured GBAS message was then transmitted to the aircraft via LDACS (Fig. 1a and 1d). The setup of the experiment is outlined in Fig. 2.

A. Background on TESLA

The use of TESLA for secure GBAS was motivated by its comparative computational efficiency and and low overhead. The naïve way to authenticate broadcast packets, would be to append digital signatures to each packet. However, this would require the use of public key cryptography. The sender would have to use its private key to digitally sign each packet and the recipient would have to to know and use the sender's public key to verify the signatures. This leads to two drawbacks:

First, the calculations for generating and verifying a digital signature are several orders of magnitude more computationally expensive than performing a symmetric operation, such as generation a Message Authentication Code (MAC). Secondly, the size of digital signatures is currently in the order of 512b or 64B, which generates significant overhead. If a MAC were used, the security overhead could be reduced. Using TESLA for secure GBAS has therefor the potential to reduce the computational effort and decrease the amount of security data overhead.

The general idea behind TESLA is to split time into even intervals T_{int}. These time intervals are used to generate a one way-key chain by assigning a key k_i to each interval. The interval's key is then used to compute a Message Authentication Code (MAC) for each packet transmitted during this interval. A formal illustration of this protocol is displayed in Fig. 3.

The MAC of each packet needs to be verified after reception. The necessary key k_i, so far only known to the transmitter, is sent to all receivers in an interval where it is no longer used by the transmitter. This interval is called the key disclosure delay d, measured in T_{int} intervals. A recipient of a TESLA-secured packet will therefore (1) receive a packet, (2) buffer it and, when it received the key after d intervals, (3) verify its authenticity. Only after step 3 is a TESLA-secured packet considered securely received.

The TESLA protocol has several requirements to work: Sender and receivers have to be loosely time synchronized; they have to have previously agreed upon key derivation, MAC tag generation, and verification algorithms; and every new participant has to receive the TESLA parameters in an authentic manner. [13]

Analysis of Mäurer's results [12] indicated that the configuration of the TESLA protocol has a profound impact on the overall performance of secure GBAS over LDACS. The main TESLA parameters, that are relevant in the context of this paper are: the interval time T_{int}, the key disclosure delay d, and the key k_i for generating a MAC of a message m to be sent in interval i.

B. Performance Impact of TESLA

Mäurer et al. [12] presented two measurement results for the communication latency of secure GBAS over LDACS. The results are displayed in Fig. 4a and Fig. 4b. The results represent latency measurements from two flight experiments called *experiment 01* and *experiment 06*[4] with different TESLA configurations. The benchmark for the results are the GAST-C and GAST-D GBAS Approach Service Type (GAST) requirements, which translate (among others) into communication latency requirements shown in the figures (yellow line for GAST-C, green line for GAST-D requirement).

In both results the measured communication latency of secure GBAS correction data transmitted over LDACS is displayed. The *communication latency* measurement indicates the cumulative latency introduced by the LDACS datalink (blue line) for transmitting all fragments of the GBAS message, without taking the TESLA protocol into account. The *authentication latency* measurement also takes the time until the packet could be verified through TESLA into account (orange line). In the context of *secure* GBAS, the GAST requirements have to be applied to the latter result. Visually comparing the results of *experiment 01* and *experiment 06* indicates that fulfilling the GAST requirements depends on the TESLA configuration (the orange line should be below the green line) since LDACS

[4]For consistency we use the numbering introduced in Table 1 of [12]. Only experiment 01 and 06 are relevant in the context of this paper. Experiment 02 and 03 used similar parameters as experiment 01. Experiment 04 and 05 did not use TESLA.

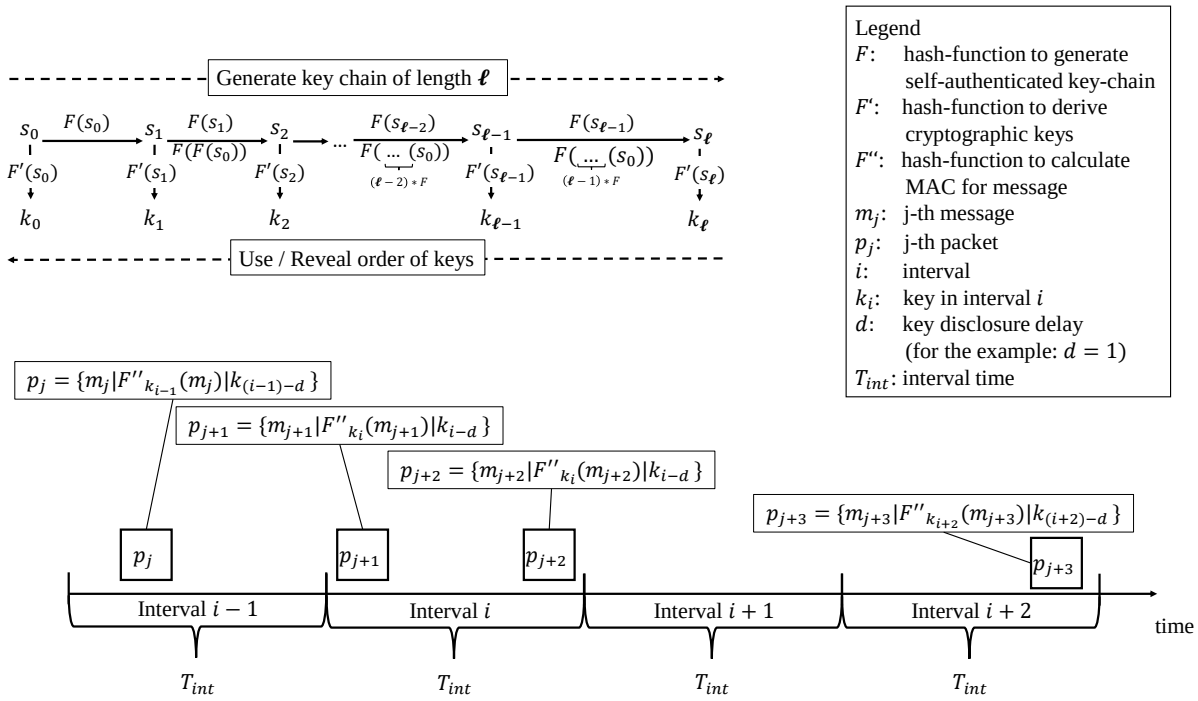


Fig. 3: Overview of the TESLA key-chain generation, key use order and construction and content of TESLA-secured data packets [12]

performance is always sufficient (blue line indicating the cumulative LDACS latency of fragmented GBAS messages).

C. Theoretical Optimum Performance

What is the minimum latency that can be achieved with TESLA-secured GBAS over LDACS? Ideally all fragments of a GBAS message would be authenticated by the first fragment of the next message. In this case the minimum latency that could be achieved would be the update interval of GBAS plus the time required for the transmission of one additional fragment providing piggy-backed key disclosure.

In *experiment 01* the measured 95%-percentile of the LDACS latency for a GBAS message fragment was $111.99ms$. In *experiment 06* the measured 95%-percentile of the LDACS latency was slightly larger at $147.37ms$. Thus, the achievable minimum latency should be approximately the update rate, in which GBAS packets are sent, plus the measured 95%-percentile of the LDACS latency. The update rate for GBAS packets was 1Hz in *experiment 01* and 2Hz in *experiment 06*, resulting in $1s + 0.11199s = 1.11199s$ for *experiment 01* and $0.5s + 0.14737s = 0.64737s$ *experiment 06* in the 95%-percentile, respectively.

A quick inspection of the results in Fig. 4 shows that this goal has mostly been achieved in *experiment 01*, but not in *experiment 06* although GBAS correction data is sent twice as often. Why is that so?

D. Performance Analysis

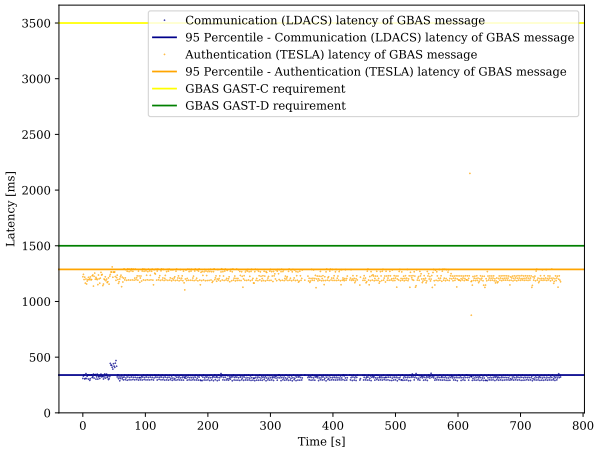
Mäurer used two different TESLA configuration sets for the MICONAV demonstration of secure GBAS over LDACS. The LDACS configuration was not changed between the experiments: QPSK modulation, coding rate $1/2$, resulting in an approximate ground-to-air data rate of 300 kbit/s [3] of which less than 50 kbit/s were used for secure GBAS.

Experiment 01 used an interval time $T_{int} = 1s$ and a key disclosure delay of $d = 1$. In this experiment GBAS correction data was transmitted in five fragments once every second. All five fragments needed to be received.

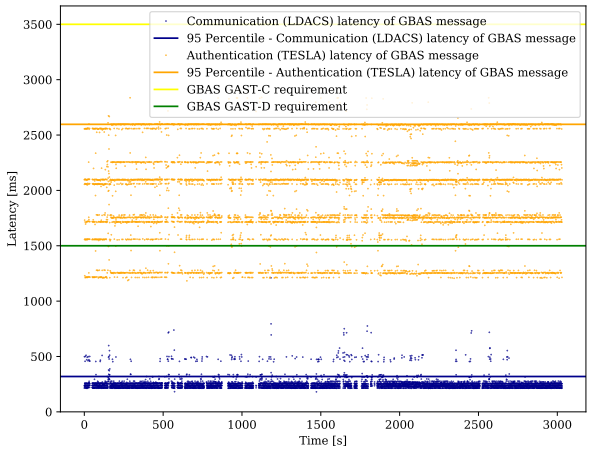
Experiment 06 used a more conservative TESLA configuration. $T_{int} = 1s$ remained unchanged, however, the key disclosure delay was set to $d = 2$. The GBAS correction data format was changed to require only two (slightly larger) fragments, both of which needed to be received. The GBAS update interval was reduced to send correction data twice per second.

The analysis of Mäurer's results revealed the following issues with these configuration sets:

1) T_{int} was too long: A problem with these parameter choices was, that a time interval of $T_{int} = 1s$ already approaches the GBAS GAST-D data update interval requirement of 1.5 s [14]. Since the key disclosure delay d is measured in multiples of T_{int}, the introduced authentication delay makes it hard to meet these requirements. Especially if $d > 1$. Indeed, it can be seen in Fig. 5 that it is the authentication delay (orange line) that determines if the GAST-D requirement (green line) is met, since the contribution of the LDACS radio latency (blue) remains mostly unchanged. Clearly, T_{int} should be shorter, although the concrete value is not obvious, yet.

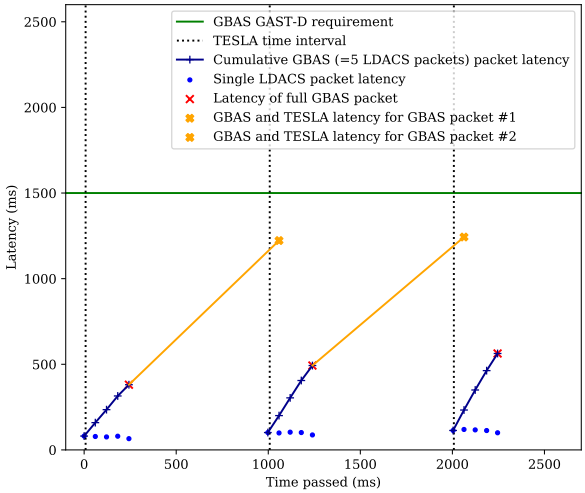


(a) Experiment 01 ($T_{int} = 1s$, $d = 1$)
GBAS correction data is transmitted at 1 Hz
GAST-D requirement fulfilled

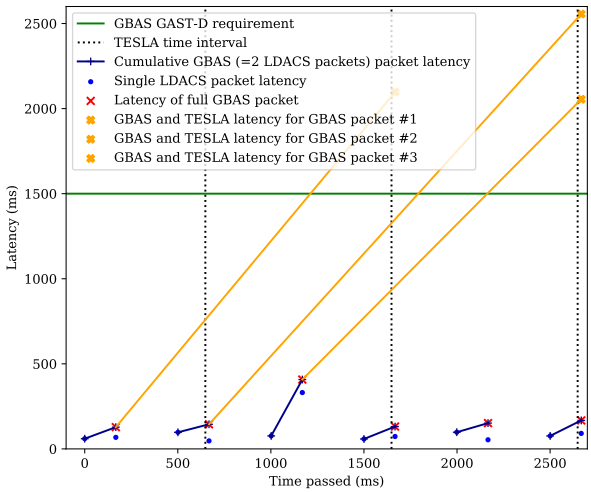


(b) Experiment 06 ($T_{int} = 1s$, $d = 2$)
GBAS correction data is transmitted at 2 Hz
GAST-D requirement *not* fulfilled

Fig. 4: Measured latency of secured GBAS messages in Mäurer's demonstration [12].



(a) Experiment 01: GBAS correction data is transmitted in *five* packets *once* per second. When all five fragments have been received (the cumulative LDACS latency is shown by the blue line), TESLA authentication is performed over the time of $d = 1$ interval of length $T_{int} = 1s$ (orange line) . Only after successful TESLA authentication the data is considered received.

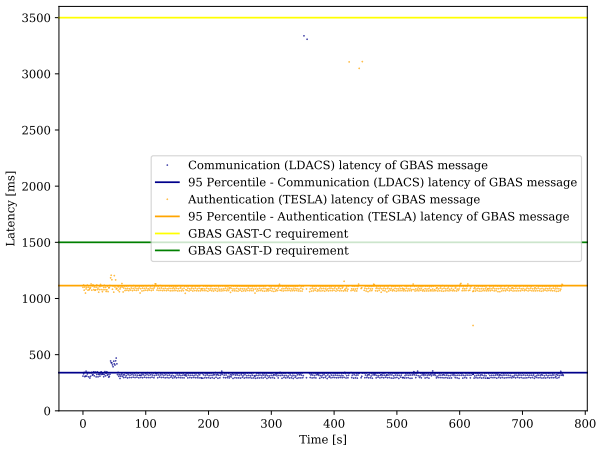


(b) Experiment 06: GBAS correction data is transmitted in *two* packets *twice* per second. When both fragments have been received (the cumulative LDACS latency is shown by the blue line), TESLA authentication is performed over the time of $d = 2$ intervals of length $T_{int} = 1s$ (orange line) . Only after successful TESLA authentication the data is considered received.

Fig. 5: Analysis of the measured latency of the first secured GBAS messages in Mäurer's demonstration [12].

2) d was too large: In *experiment 06* the key disclosure delay d was set to $d = 2$. In combination with $T_{int} = 1s$ this lead to an authentication delay of at least $T_{int} = 1s$ and up to $d \cdot T_{int} = 2s$. Clearly, this allowed only few packets to satisfy the GAST-D requirement of $1.5s$. This is discernible in Fig. 4b. Setting d to a value greater than 1, can prevent race conditions between key usage and key disclosure if clocks are not perfectly synchronized. Since GBAS can obviously use GNSS as a common time source, this does not apply. Clearly, d should be set to $d = 1$.

3) GBAS and TESLA time framing were not aligned: Both GBAS and TESLA use time intervals to structure their protocols. These two structures were not aligned in both experiments, which led to performance degradation. This is best illustrated looking at the example of Fig. 5a: The first fragment (blue dot) of the first GBAS message carries the key for TESLA interval 0. Fragment 2 (shortly after the vertical dotted line indicating the start of TESLA interval 1) carries the key for interval 1, allowing the verification of the authenticity of the first fragment. Fragments 2, 3, 4 and 5, the remaining parts of the first GBAS message, are signed with the key of interval 1, and can therefore only be verified with the key of interval 2. That is, the message cannot be accepted until the start of the next interval, although all fragments of the



(a) Experiment 01 (optimized configuration: $T_{int} = 750ms$, $d = 1$)
GBAS correction data is transmitted at 1 Hz
GAST-D requirement fulfilled.

(b) Experiment 06 (optimized configuration: $T_{int} = 300ms$, $d = 1$)
GBAS correction data is transmitted at 2 Hz
GAST-D requirement fulfilled

Fig. 6: Latency of secured GBAS messages using the optimized configuration sets.

first GBAS message have been received after 380ms. At time 997ms the first fragment of the second GBAS message is sent, which is still in TESLA interval 1. Only after the start of the second TESLA interval, when fragment 2 of the second GBAS message is sent, the key for the fragments of the first GBAS message becomes available. This fragment is received at time 1222ms. This is also the cumulative latency of the first GBAS message accrued at this time. In *experiment 06* the misalignment is even worse, since the key of the previous message is only disclosed in the last fragment of the following message as shown in Fig. 5b. Clearly, the time intervals of GBAS and TESLA could have been better aligned to avoid changing the TESLA interval during the transmission of the GBAS message. Ideally, the TESLA interval should change between GBAS messages.

4) Cryptography overhead can be reduced: In addition to optimizing the TESLA timing parameters, the cryptography algorithm used to generate the MACs could also be improved. Mäurer [12] used the *blake2b* algorithm from *python3*'s *hashlib* library [1]. The *blake2b* algorithm uses a 64B key, a 16B salt value, and produces a 64B MAC digest. This results in 144B overhead. This overhead can be reduced using more suitable algorithms, such as *blake2s*, which uses a 32B key, a 8B salt value, and produces 32B MAC digests. An alternative way to reduce the overhead is to combine *HMAC* [10] with hashes from suitable hash-families, e.g. *SHA-3* [4] or *SHAKE* [2]. Assuming a minimum key size of 16B, the German Bundesamt für Sicherheit in der Informationstechnik (BSI) recommends a minimum message MAC tag size of 12B [5]. Thus, taking this into account, it is reasonable to use 16B key + 12B tag, or 16B key + 16B tag, resulting in 28B or 32B minimum overhead, respectively, for each key and MAC tag applied to a message.

III. Improved Method for GBAS over LDACS

In the previous section four recommendations have been derived for the improvement of the secure GBAS protocol:

- T_{int} should be short: $T_{int} \ll 1.5s$
- d should be set to $d = 1$
- TESLA intervals should change between GBAS messages
- Cryptographic functions requiring smaller keys and resulting in smaller MAC tags should be used

The first and the third recommendations are related to each other, since they allow to derive an optimal TESLA interval time T_{int}: The optimal value for T_{int} is shorter than the largest time gap between the last fragment of the previous message and the first fragment of the next message. This ensures, that the first fragment of the next packet will always disclose the key for all fragments of the previous GBAS message. Making T_{int} even smaller results in no further improvement, since only completely reassembled GBAS messages can be used.

This approach resulted in the following configuration sets:

Experiment 01: In this experiment the maximum duration of the gap between two GBAS messages was measured to be $756ms$. Thus, the TESLA interval length was set to the slightly smaller value of $T_{int} = 750ms$, and the key disclosure delay to $d = 1$ intervals.

Experiment 06: Following the same approach, the TESLA interval length was set to $T_{int} = 300ms$, and the key disclosure delay to $d = 1$ intervals.

The improved TESLA configuration sets were evaluated using the GBAS messages recorded during Mäurer's demonstration. The recorded GBAS messages were processed by the improved TESLA protocol. Instead of sending the messages over an actual LDACS link, the latency measured in the flight trials was used. This approach could be used, because the introduced improvements of the TESLA protocol did not change the size or sending pattern of the GBAS fragments i.e.

the LDACS packets. The improved cryptography algorithms were not used, to avoid changing messages sizes.

IV. Results

The result of the application of the improved method to *experiment 01* is presented in Fig. 6a. The mean TESLA latency is $1105.44ms$ and the 95%-percentile latency $1113.97ms$. For comparison, the non-optimized mean latency was $1219.52ms$, and $1287.96ms$ in the 95%-percentile. The 95%-percentile was, thus, improved by 15.62% and is now even closer to the estimated optimum latency of $1111.99ms$.

The result of the application of the improved method to *experiment 06* is presented in Fig. 6b. For $d = 1$ and $T_{int} = 300ms$, experiment 06's mean latency is $617.94ms$ and the 95%-percentile latency $632.98ms$. The original latency measured in [12], was $1932.67ms$ in the mean, and $2596.76ms$ in the 95%-percentile. The optimized latency is therefore improved by 410.24% in the 95%-percentile and close to the estimated optimum latency of $647.37ms$.

V. Discussion

The evaluation of the proposed improved method for secure GBAS indicates, that all issues identified in the analysis of Mäurer's secure GBAS demonstration could be resolved. Indeed, the results show, that it is possible to configure TESLA in such a way, that near optimal performance can be achieved.

Although not evaluated, the potential reduction in security overhead of the improved method is also easily estimated: The originally used hash function *blake2b* required 64B key and 16B salt input values and produced a 64B message digest. This 144B security overhead can be reduced using *HMAC* [10] with hashes on the basis of *SHA-3* [4] or *SHAKE* [2] to a 16B key and a 16B message digest. For a typical 1000B GBAS packet this would reduce the security overhead from 14,4% to 3,2%, which is a welcome improvement.

The results also provide an outlook on the possibilities of securing GBAS with the TESLA protocol. Considering the estimated theoretical optimal performance of GBAS over TESLA, and that 1 Hz data updates are only the current GBAS use case, the results for *experiment 01* indicate only what can be achieved today. However, if GBAS correction data for additional GNSS frequencies and constellations is added, as desired by the GBAS community, this would increase the number of packets and thus reduce latency even further. This has already been demonstrated in *experiment 06*. In summary, more demanding TESLA secured GBAS via LDACS scenarios can be supported with even better performance.

VI. Conclusion

GBAS over LDACS was first demonstrated by Mäurer in the MICONAV project. The analysis of the results indicated several possible points of refinement. In particular, the configuration of the TESLA authentication protocol has been identified as a major source for performance degradation. The objective of this paper was thus to propose an improved method for securing GBAS correction data with TESLA. Two optimal configuration sets were derived from the analysis of the original measurements. The enhanced TESLA configuration was then evaluated on the basis of the original measurements.

The results of the evaluation indicate, that the improved configuration parameters provide near-optimal performance. TESLA induced latency could by reduced by a factor of four in one case. In addition, the analysis, leading to the enhanced parameters, points also the way for further improvements for more challenging GBAS scenarios.

Appendix

GAST	GBAS Approach Service Type
GBAS	Ground Based Augmentation System
GNSS	Global Navigation Satellite System
LDACS	L-band Digital Aeronautical Communication System
MAC	Message Authentication Code
MICONAV	Migration towards Integrated COM/NAV Avionics
TESLA	Timed Efficient Stream Loss-tolerant Authentication

References

[1] J.-P. Aumasson, S. Neves, Z. Wilcox-O'Hearn, and C. Winnerlein, "Blake2: simpler, smaller, fast as md5," in *International Conference on Applied Cryptography and Network Security*. Springer, 2013, pp. 119–135.

[2] P. Barsocchi, G. Oligeri, and C. Soriente, "Shake: Single hash key establishment for resource constrained devices," *Ad hoc networks*, vol. 11, no. 1, pp. 288–297, 2013.

[3] 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," *submitted to IEEE Transactions on Aerospace and Electronic Systems*, 2021.

[4] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Keccak," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2013, pp. 313–314.

[5] BSI, "Cryptographic Mechanisms: Recommendations and Key Lengths," Federal Office for Information Security Germany, Tech. Rep. BSI TR-02102-1, March 2020.

[6] M. Felux, T. Gräupl, N. Mäurer, and M. Stanisak, "Transmitting GBAS messages via LDACS," in *37th Digital Avionics Systems Conference (DASC)*. New York, NY, USA: IEEE, September 2018, pp. 1–7.

[7] M. Felux, T. Dautermann, and H. Becker, "GBAS landing system–precision approach guidance after ILS," *Aircraft Engineering and Aerospace Technology*, 2013.

[8] T. Feuerle, M. Stanisak, S. Saito, T. Yoshihara, and A. Lipp, "GBAS interoperability and multi-constellation/multi-frequency trials," in *ENRI International Workshop on ATM/CNS*. Singapore, Singapore: Springer Singapore, June 2019, pp. 162–174.

[9] J. García, "Broadband connected aircraft security," in *2015 Integrated Communication, Navigation and Surveillance Conference (ICNS)*. IEEE, 2015, pp. 1–23.

[10] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104 (Informational), RFC Editor, Fremont, CA, USA, Feb. 1997, updated by RFC 6151. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2104.txt

[11] J. Lee and M. Kim, "Optimized GNSS station selection to support long-term monitoring of ionospheric anomalies for aircraft landing systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 1, pp. 236–246, 2017.

[12] 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 CommunicationSystem (LDACS)," *IEEE Aerospace and Electronic Systems Magazine*, pp. 1–19, 2021.

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

[14] RTCA, "DO-253D, Change 1, Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment," Radio Technical Commission for Aeronautics (RTCA), Tech. Rep., 06 2019, [Online]. Available: https://www.rtca.org/products/do-253d-electronic/.

[15] M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger, "LDACS: future aeronautical communications for air-traffic management," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 104–110, 2014.

[16] M. Stanisak, A. Lipp, and T. Feuerle, "Possible VDB formatting for multi-constellation/multi-frequency GBAS services," in *Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS'15)*, 2015, pp. 1507–1518.