SBAS Data Authentication: A Concept of Operations

Andrew Neish, Todd Walter, J. David Powell

Stanford University

Abstract

Previous work in data authentication for SBAS has focused on the authentication schemes and the key management architecture. As these designs mature, concepts of receiver operations need to be defined before any impacts to the SBAS service can be evaluated. In this work, several authentication schemes are put forward along with a concept of operations (CONOPS) that defines how receivers act on authenticated and unauthenticated information. The CONOPS developed here allow SBAS services providers to incorporate data security while producing minimal impacts to performance for users.

Introduction

Mitigation against spoofing attacks has been a major research focus for the last several years. There have been many different methods proposed in recent years, ranging from physical hardware changes used to detect direction of the arrival of signals [1] to cryptographic markers placed within the chipping code that are later used to verify that the ranging signal was generated on board the satellites [2]. While much of the research has been focused on protecting the information coming from the Global Navigation Satellite Systems (GNSS) satellites, there are other signals that safety of life systems rely upon. This paper focuses on securing the data sent by Satellite Based Augmentation Systems (SBAS).

SBAS satellites deliver wide area corrections data to GNSS users along with integrity information concerning the GNSS satellites. This data is currently delivered in an open format that is unencrypted and unauthenticated. Malicious attackers wishing to put an SBAS user in harm's way could transmit false SBAS data and have the victim user create a position solution outside the safety limits bounded by their own protection level calculations. This attack is carried out by spoofing only one signal, the SBAS signal, and so represents a serious vulnerability for SBAS users. While not all SBAS services include a ranging component as a part of the geostationary satellite (GEO) broadcast, all SBAS services require the use of data streaming from the GEOs. Because of this, spoof mitigation for SBAS satellites has been focused on protecting the data content streaming from the GEOs.

Authenticating the data streaming from SBAS satellites has the ability to protect SBAS users from most malicious SBAS targeted attacks. Due to the limited bandwidth available in the SBAS broadcast, most schemes used for internet protocol (IP) authentication are not suitable. There have been a number of papers over the years looking into various adaptions of cryptographic schemes that can be used to authenticate GNSS signals [3]–[7]. This research has guided the authentication scheme search to three main candidates: The Timed Efficient Stream Loss-Tolerant Algorithm (TESLA) [8], Elliptic Curve Digital Signature Algorithm (ECDSA) [9], and Elliptic Curve Schnorr (EC-Schnorr) [10]. There are other schemes that are being reviewed, namely post-quantum cryptographic schemes, that will likely be included in future work. In addition to research into schemes, there has also been work done to implement a key management structure that would allow these SBAS users to update important cryptographic key information using messages broadcast by the SBAS satellites themselves [11].

The research field is getting closer to the point where actual operational decisions can be made concerning whether these authentication methods should be implemented. One missing feature so far has been a full impact analysis on how these authentication services will impact SBAS users. In order to carry out an evaluation of the impact to users, a concept of operations (CONOPS) must first be defined. This work uses the term CONOPS as a catch-all term for receiver operations related to authentication procedures. Listed here are just a couple examples of the CONOPS questions that must be answered:

1) What should a receiver do with information that hasn't been authenticated yet?
2) What should a receiver do with information that can't be authenticated, due to a corrupted signature?
3) How should a receiver react in the event that an authentication has failed, i.e. the data received does not match the signature that was received?

All these questions and more must be addressed before a nominal impact to users can be assessed. This paper aims to provide several suggested answers to these questions and give justification for the CONOPS presented here. The paper is split into the following sections: Following this introduction, a short section dedicated to the description of the schemes employed is given. Then, the Key Performance Indicators (KPI) used to measure the impact of these schemes along with a discussion on CONOPS is given that builds the framework around how a receiver should handle the authentication service. Following this discussion is a brief introduction to the receiver simulation methodology employed and then an impact analysis is carried out. Finally, the paper is concluded, highlighting the findings of this work and suggesting the work that will be necessary in the future.

Authentication Scheme Overview

This section gives a brief overview of the schemes that are currently being considered for SBAS data authentication. Two are variants of TESLA are introduced here along with an ECDSA design. The ECDSA variant includes a parallel message stream in the Quadrature channel (Q-channel) of L5. A more detailed description of the implementation of ECDSA is given in [11]. Figure 1 shows an example message sequence where s[] in the Q-channel represents a signature of the corresponding messages in the I-channel and OTAR stands for Over-The-Air-Rekeying bits that deliver key management information through the SBAS data stream. Figure 2 depicts the contents of the signature message for the Q-channel. The data field for an L5 message is 216 bits. With a 448-bit signature, ECDSA obtains a security level of 112-bits and in this case is strung across two 250-bit message fields to create one Q-channel message. The remaining 52 bits are used for key management.

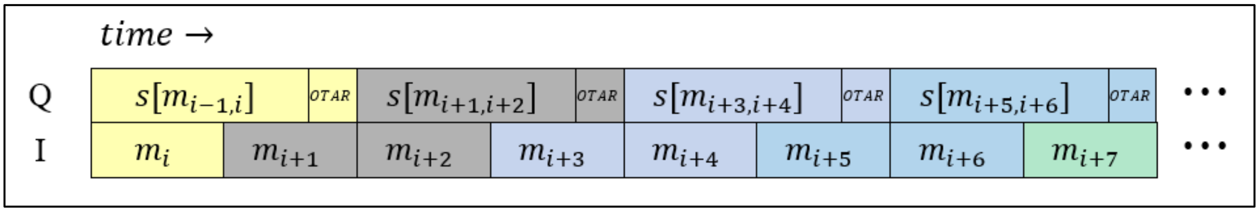


Figure 1: Q-Channel ECDSA Implementation

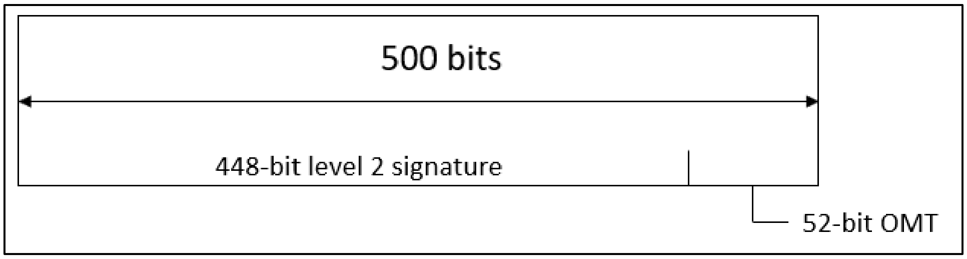


Figure 2: ECDSA Authentication Message Contents

The I-channel implementation requires that the signature message be contained within one message. In other words, the signature must be less than 216 bits and still retain a high enough security level. In this case TESLA is found to be a viable candidate as the combination of the message authentication code (MAC) and the TESLA key can fit within these bounds. An example implementation of TESLA can be seen in Figure 3.

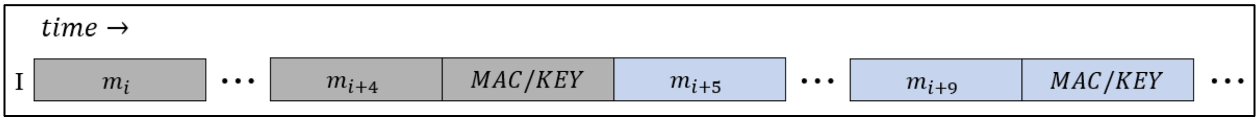


Figure 3: I-channel TESLA implementation

There are several papers that give full descriptions of the TESLA scheme [8], [11], but in summary, there are two main distinctions between TESLA and other authentication schemes that must be understood in practice. The first is that TESLA is inherently a symmetric scheme that obtains asymmetry through the delay release of keys. As an example, in Figure 3, the MAC that signs the data $[m_i \rightarrow m_{i+4}]$ is signed with the key that is released after m_{i+9}. The security of this scheme depends on this delayed release of keys, and so loose time synchronization is required from the receiver. The second important aspect that must be understood is that the keys must be authenticated before they can be used. TESLA does this through the establishment of a keychain. These keys are all linked through a one-way function that allows users to derive previous keys without giving any insight into future keys. The root key of the entire keychain is then signed by a truly asymmetric scheme, such as ECDSA, and so if a user is able to verify that the key that they've received is a part of the authenticated keychain, then the key can be used to verify the previously received MAC.

An example message structure of an I-channel authentication message is shown in Figure 4. The typical implementation of TESLA creates a single MAC for a set of previous messages. The bandwidth of the I-channel is impacted as it is, however, and so an inclusion of an authentication message limits the frequency at which these messages can be sent. In this design, a nominal Time Between Authentication (TBA) is designed to be 6 seconds. This implies that in order to properly carry out the TESLA signature protocol for a set of messages, all messages must have been received correctly. The converse of this means that if a single message is not demodulated correctly, then all messages that were a part of that authentication group can no longer be authenticated.

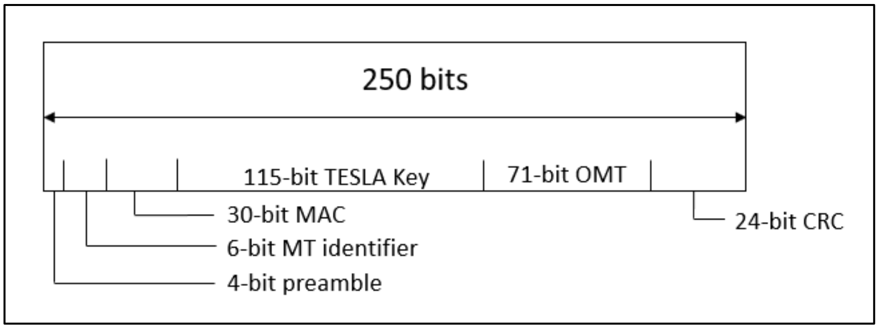


Figure 4: TESLA - BigMAC Authentication Message Contents

In order to mitigate this, a new design is put forward. Instead of signing all previous messages with a single MAC, individual MACs are instead delivered, and all signed using the same key. An example authentication message for this implementation is given in Figure 5. From here on, the original implementation shown in Figure 4 is referred to as TESLA-BigMAC and the authentication message depicted in Figure 5 is referred to as TESLA-LittleMACs. The 30-bit MAC for the TESLA-BigMAC case was designed to limit the probability of any successful guess of the MAC to less than 10^{-9} [11]. In the case of TESLA-LittleMACs, this probability is reduced to less than $\sim 10^{-3}$ for each 10-bit MAC, but as described later in the CONOPS section of this paper, the security of the scheme is retained through the approach to a failure to authenticate scenario. The clear advantage of the TESLA-LittleMACs design is that it mitigates the effects of a single missed message on a batch of messages intending to be authenticated.

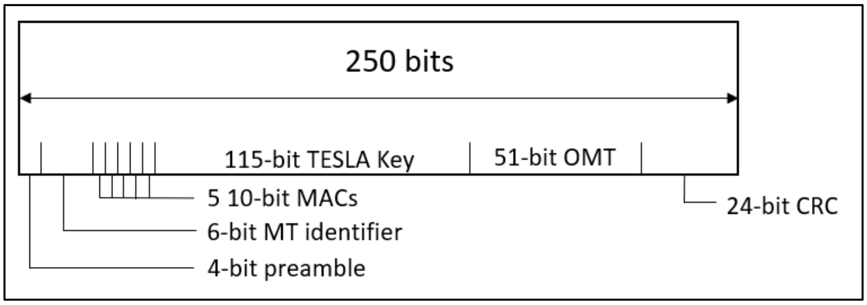


Figure 5: TESLA - LittleMACs Authentication Message Contents

Key Performance Indicators and Definitions

There are three possible outputs from an authentication attempt. The first, defined as “Authentication Passed”, occurs when all messages have been received correctly by the receiver (all CRCs pass), and the signature algorithm output on these messages is true. The second output is defined as “Authentication Failed”. In this case, all messages have been demodulated correctly, and the signature algorithm output is false. This indicates that either an error has occurred at the service provider level or that the receiver is receiving unauthorized broadcasts of SBAS data. The final output that can occur from a signature algorithm is defined as “Authentication Unavailable”. In this case, at least one of the messages to be authenticated or the authentication message itself has been demodulated incorrectly (bad CRC), which renders the receiver unable to authenticate other information surrounding the missed messages. The CONOPS plays an important role in how a receiver deals with authentication outputs, as will be seen in later sections.

During the development of authentication implementations for SBAS, several key performance indicators (KPIs) have been established that quantify the impact to users. There are many that are associated with the implementation of any scheme, but this paper highlights a few that are used to quantify the impact of the schemes set forth here.

The first two KPIs are already defined in the context of non-authenticated SBAS operations. The first is Availability, which denotes the probability that the SBAS service will be available to the user at a given time. The second is Continuity, which is defined as the probability that the service will remain available during a phase of operation (given to be 15 seconds here), given that the service was initially available at the beginning of said phase.

Three more KPIs are defined that are more specific to the products of authentication. The Authentication Error Rate (AER) is defined as the rate at which authentications fail or are unavailable. The Time Between Authentications (TBA) is defined as the duration of time between authentications. Nominally this is a constant value, but in practice it may vary when authentication messages cannot be processed by the receiver due to incorrect demodulation of the incoming data or alert scenarios that may upset the normal cadence of SBAS messages. The final KPI that we will examine pertaining to authentication is the Authentication Latency (AL) and in this particular case, the median AL. In aggregate, this simply looks at the median time that it takes to authenticate messages once they have been received. These KPIs, along with the defined receiver outputs, now allow us to dive into the CONOPS design.

Concept of Operations (CONOPS)

A CONOPS sets forth how a receiver reacts in all possible scenarios. The goal of implementing an authentication service to SBAS is to minimize any impact to users while delivering a secure service. The CONOPS is where compromise between these often-competing goals is found. This section is organized as a series of operational considerations posed as questions which are then addressed in the paragraphs that follow.

How does a receiver treat unauthenticated data? Does a receiver use data that has not yet been authenticated?

SBAS users rely on the service to provide vital information must be protected from potential hampering. If a receiver uses data before it has been authenticated, it may be exposing itself to misleading information before it can verify the data’s authenticity. For these reasons, receivers do not use most information that is received before that information has been authenticated. All messages received from the SBAS GEOs have a period of validity. In the most stringent operations, receivers cannot miss two of the same message types in succession. For the most critical information, such as the (Dual Frequency Range Errors) DFREs delivered in the MT35 and MT32 messages, the time of validity is 12 seconds. The Q-channel scheme introduced here has a nominal TBA of 2 seconds, while the I-channel schemes have a nominal TBA 6 seconds. With this in mind, receivers can wait to apply the messages received from the SBAS satellites until that information has been authenticated.

One caveat to this is that SBAS systems must meet time to alert (TTA) requirements. These alerts are delivered to users through an increase in (DFRE Indicators) DFREIs associated with faulted measurements. In order to meet the TTA requirements, it is proposed that users immediately incorporate increases to DFRE information when that information is available, but not incorporate decreases to DFREs until that information has been authenticated. Data that cannot be authenticated due to “Authentication Unavailable” events are never incorporated in the integrity estimation except for the aforementioned increases to DFREIs.

How does a receiver react to an “Authentication Failed” scenario?

In the event that an authentication has failed, either as a failure in the data authentication or key management delivery, the receiver makes two different decisions depending on the authentication scheme employed. In the case of Q-channel ECDSA and I-channel TESLA-BigMAC, the receiver reverts using data from another GEO as long as that data remains authenticated and only returns to the original GEO once it has been established that the service is authenticated once again. In the case of I-channel TESLA-LittleMACs, all data used from the GEO is cleared, the receiver reverts to using data from another GEO if it is available and authenticated, and only returns to the original GEO once the authentication service is available once again.

This is a key feature of the TESLA-LittleMACs implementation that allows for smaller, distributed MACs. If any, of the five MACs delivered in a single authentication message outputs as a failure, all data from that GEO is purged from the receiver. If an attacker were to attempt to forge messages in this case, they have a higher chance of successfully replacing a single message than in the TESLA-BigMAC case, but if the attacker wished to spoof multiple successive messages, the probability of detection of such an attack increases dramatically. In this way, TESLA-LittleMACs can mitigate the impact to other messages when CRCs don’t pass for a single message while still delivering a secure authentication service. In all cases, if another GEO cannot be authenticated, then the service is no longer available, and the user must resort to other means of navigation until an authenticated service is available once again.

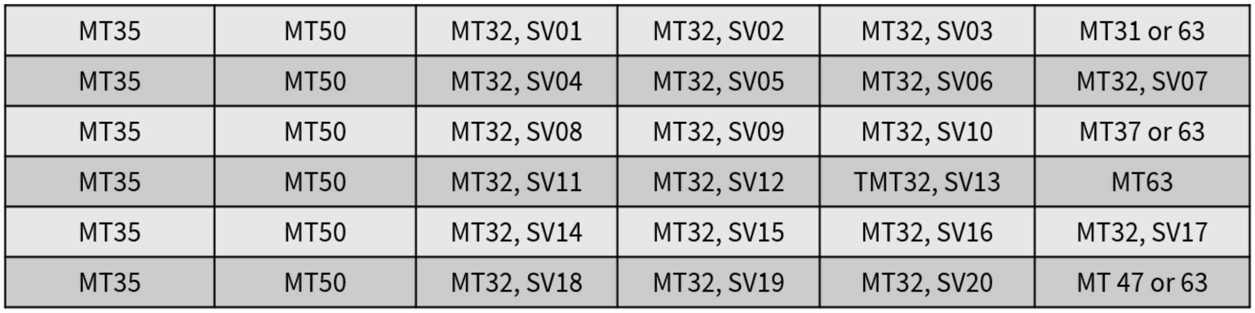
What is the impact to the service if a message times out and is no longer available?

Different messages within the L5 broadcast stream have different impacts to user performance. In the case of MT35, which carries the crucial DFRE information, if that message is not available, then the service is no longer available. In the case an MT32 which sends corrections specific to each satellite, if the message is not available, then the satellite corrected by that message is not available. Whether this leads to a loss of service or only a degradation depends on the geometry of the satellites and flight operation currently being executed by the aircraft.

Analysis – Simulator and Scenario Setup

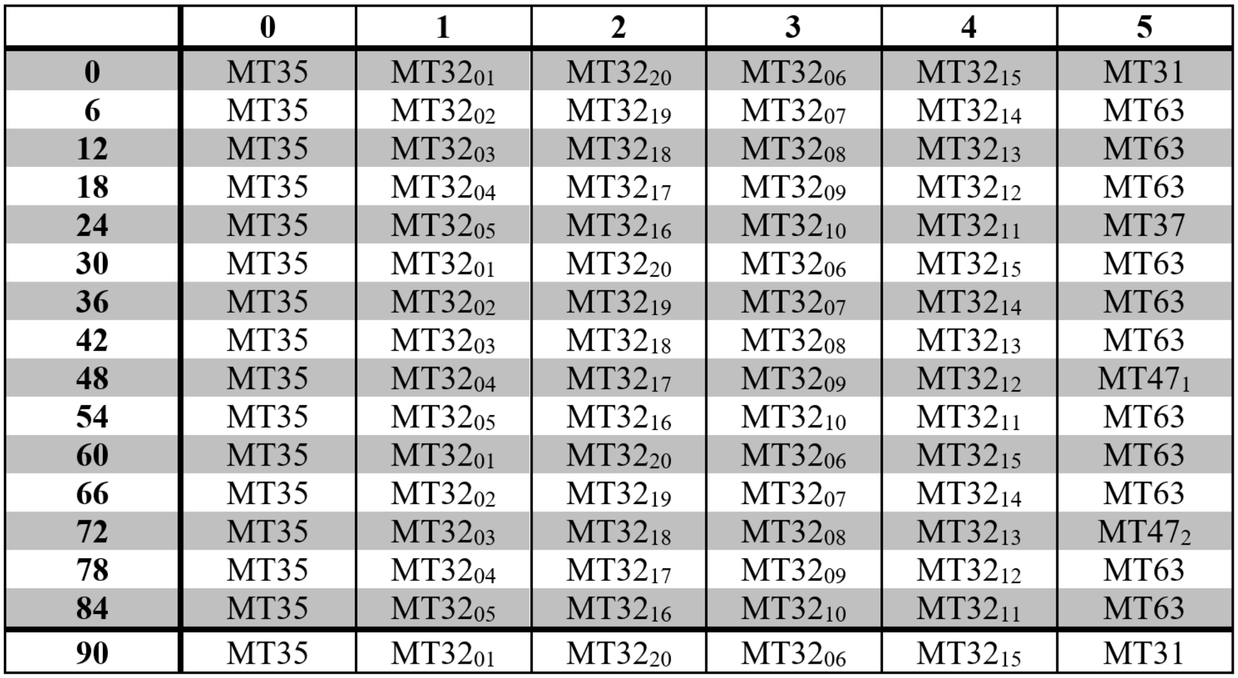
Once a CONOPs and authentication scheme has been defined, the KPIs can be estimated and the impact to the users can be measured. For this paper only nominal, non-spoofed and alert free, scenarios are considered.

Two different message streams were generated to deliver SBAS messages on the L5 frequency. The first, shown in Figure 6, depicts a message set for the I-channel authentication cases. Figure 7 shows the message structure for the Q-channel implementation. It should be noted that both charts read the same way; time increases from left to right and from top to bottom. These are all rigid and repeating message structures as well. For the I-channel implementation, the message “MT50” is defined as the authentication message type that carries the information shown in Figure 4 and Figure 5.



MT35	MT50	MT32, SV01	MT32, SV02	MT32, SV03	MT31 or 63
MT35	MT50	MT32, SV04	MT32, SV05	MT32, SV06	MT32, SV07
MT35	MT50	MT32, SV08	MT32, SV09	MT32, SV10	MT37 or 63
MT35	MT50	MT32, SV11	MT32, SV12	TMT32, SV13	MT63
MT35	MT50	MT32, SV14	MT32, SV15	MT32, SV16	MT32, SV17
MT35	MT50	MT32, SV18	MT32, SV19	MT32, SV20	MT 47 or 63

Figure 6: I-channel message stream with I-channel authentication



	0	1	2	3	4	5
0	MT35	MT32$_{01}$	MT32$_{20}$	MT32$_{06}$	MT32$_{15}$	MT31
6	MT35	MT32$_{02}$	MT32$_{19}$	MT32$_{07}$	MT32$_{14}$	MT63
12	MT35	MT32$_{03}$	MT32$_{18}$	MT32$_{08}$	MT32$_{13}$	MT63
18	MT35	MT32$_{04}$	MT32$_{17}$	MT32$_{09}$	MT32$_{12}$	MT63
24	MT35	MT32$_{05}$	MT32$_{16}$	MT32$_{10}$	MT32$_{11}$	MT37
30	MT35	MT32$_{01}$	MT32$_{20}$	MT32$_{06}$	MT32$_{15}$	MT63
36	MT35	MT32$_{02}$	MT32$_{19}$	MT32$_{07}$	MT32$_{14}$	MT63
42	MT35	MT32$_{03}$	MT32$_{18}$	MT32$_{08}$	MT32$_{13}$	MT63
48	MT35	MT32$_{04}$	MT32$_{17}$	MT32$_{09}$	MT32$_{12}$	MT47$_{1}$
54	MT35	MT32$_{05}$	MT32$_{16}$	MT32$_{10}$	MT32$_{11}$	MT63
60	MT35	MT32$_{01}$	MT32$_{20}$	MT32$_{06}$	MT32$_{15}$	MT63
66	MT35	MT32$_{02}$	MT32$_{19}$	MT32$_{07}$	MT32$_{14}$	MT63
72	MT35	MT32$_{03}$	MT32$_{18}$	MT32$_{08}$	MT32$_{13}$	MT47$_{2}$
78	MT35	MT32$_{04}$	MT32$_{17}$	MT32$_{09}$	MT32$_{12}$	MT63
84	MT35	MT32$_{05}$	MT32$_{16}$	MT32$_{10}$	MT32$_{11}$	MT63
90	MT35	MT32$_{01}$	MT32$_{20}$	MT32$_{06}$	MT32$_{15}$	MT31

Figure 7: I-channel message stream with Q-channel authentication

A receiver architecture was emulated in MATLAB that incorporated the CONOPS discussed in the section above and these receivers were simulated in aggregate in order analyze these operations. Figure 8 gives a pictorial description of the basic simulation architecture. First, inputs are given that define the number of receivers to be tested and for how long each is tested for. The word error rate (WER) that is incorporated in the simulation is also defined in this initial configuration stage. Then a series of messages is generated and delivered to the receivers through an emulated environment that at times causes messages to be demodulated incorrectly, leading to "Authentication Unavailable" events. Finally, all receivers keep track of the validity of the received messages and at the end of the simulation statistics are gathered to produce the KPIs.

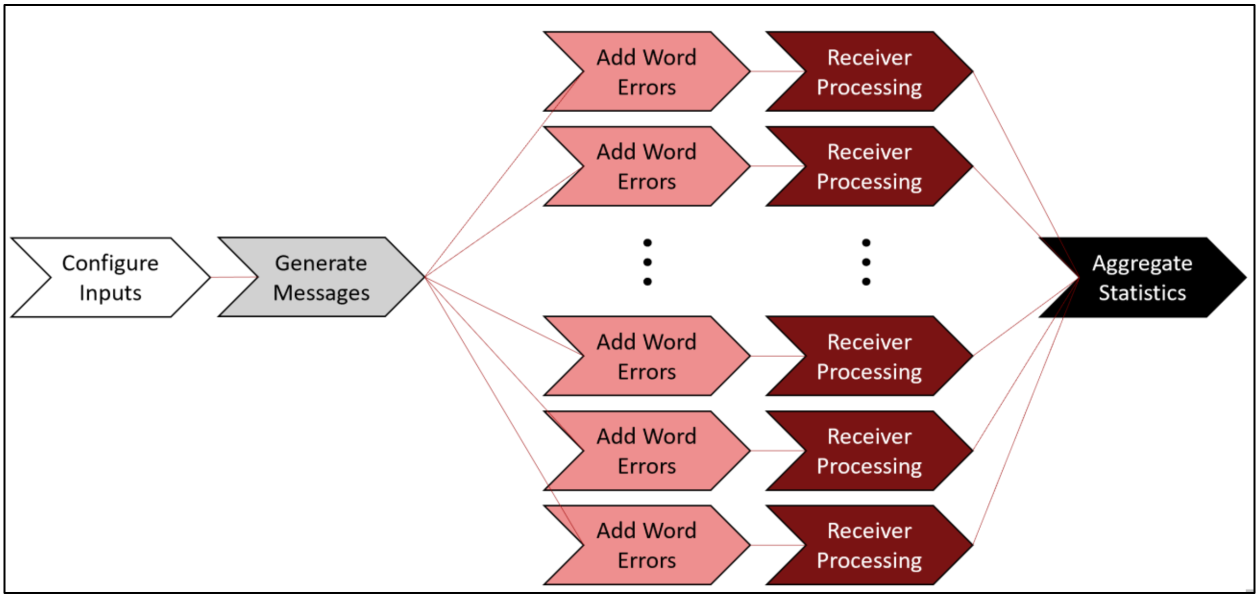


Figure 8: Simulator Architecture

One assumption made for these simulations was that the loss of an MT32 for a specific satellite would lead to a loss of service 10% of the time. For most users it is common to have 10 satellites in view and in this case, we assume one of those 10 to be crucial to the availability of the service due to geometry.

Two WER models were used in producing the results. The first was a uniform random distribution of word errors in the messages. This is equivalent to sporadic losses of data where each message loss is independent of the reception of all other messages. In practice, it has been shown that this loss may not be completely independent, and that in some cases these errors are correlated in time [12]. These messages may be dropped due to interference events that last for several seconds or occlusions to the SBAS GEO which may be from a wing or other structural member of the airplane. This correlated WER is modeled as a Markov chain and is depicted in Figure 9. Here π represents a transition probability from one state to another. From [12], these values are $\pi_{RR} = 0.999$ and $\pi_{LL} = 0.9078$. These values have shown to be rather pessimistic and maybe revised in future evaluations.

Two different assumptions of the WER are considered for the Q-channel. These assumptions are that the word errors present on the I-channel and Q-channel are either correlated or uncorrelated. For the correlated case, it is assumed that if an error is present in a given I or Q-channel message, then it is also present in the other. In the uncorrelated case, errors on the I and Q-channel are treated as independent.

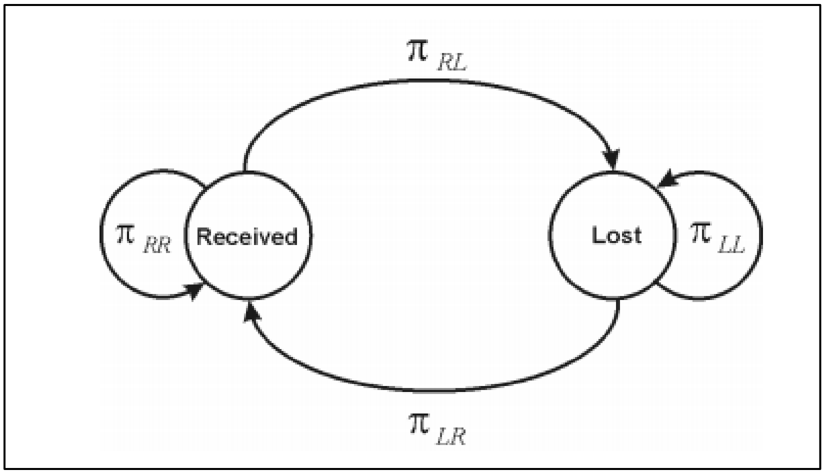


Figure 9: Markov chain model for burst errors

Results

The simulation was configured to emulate 10000 receivers for 1 hour of SBAS messages, summing to a total of 36 million received messages for each authentication configuration. For the uniform WER distribution, an error rate of 10^{-3} was simulated, reflecting the requirement that todays SBAS users must be able to operate through word error rates of this magnitude. Table 1 shows the resulting KPIs for these candidate schemes along with a benchmark "No Authentication" case reflecting the level of performance available today.

Table 1: Simulation results for uniform WER of 10e-3

Authentication Method	Availability	Continuity Risk	AER	Nominal TBA (s)	MedianAL (s)
No Authentication	0.999 9984	3.111e-6	N/A	N/A	N/A
TESLA – BigMAC	0.999 9110	3.344e-5	0.0060	6	9
TESLA – LittleMACs	0.999 9952	3.111e-6	0.0030	6	9
ECDSA (correlated)	0.999 9821	9.722e-6	0.0030	2	1
ECDSA (uncorrelated)	0.999 9571	2.333e-5	0.0040	2	1

Several important insights can be gleaned from these results. The first is in the comparison between the availability and continuity of the no authentication case versus the cases with authentication. All show a degradation in performance, which is to be expected, but the case of TESLA-LittleMACs, which was explicitly designed to mitigate the impact of "Authentication Unavailable" scenarios, offers a service with minimal degradation in performance. Even though the authentication error rate (AER) is shown to be on the order of 3/1000, the service is robust to losing certain messages sporadically. Table 2 shows the results of the Markov chain WER model with significantly deprecated results in all cases. In this case, the WER model appears to be overly pessimistic and so these model inputs will be explored in further detail in the future.

Table 2: Simulation results for Markov chain WER model

Authentication Method	Availability	Continuity Risk	AER	Nominal TBA (s)	MedianAL (s)
No Authentication	0.992 9675	6.073e-3	N/A	N/A	N/A
TESLA – BigMAC	0.986 8317	6.514e-3	0.0239	6	9
TESLA – LittleMACs	0.989 7897	6.108e-3	0.0239	6	9
ECDSA (correlated)	0.992 3089	6.613e-3	0.0127	2	1
ECDSA (uncorrelated)	0.988 9997	9.685e-3	0.0231	2	1

Finally, a sensitivity analysis was run looking at different values of uniform WER distributions ranging from 10^{-4} to 10^{-1}. The results for the availability and continuity are shown in Figure 10 and Figure 11, respectively. At higher word error rates, the performance of all variants drops off. Availability remains quite high for some variants with WER < 10^{-2}. There is a clear trend in the continuity risk and how it is related to the WER. For low WER, the data becomes less reliable since the simulations did not appear to collect enough data to produce precise statistics, but the trends are clear from the higher word error rates. As promisingly shown in Table 1 and again seen here in Figure 11, the continuity risk of the TESLA-LittleMACs scheme tracks closely to that of the legacy service.

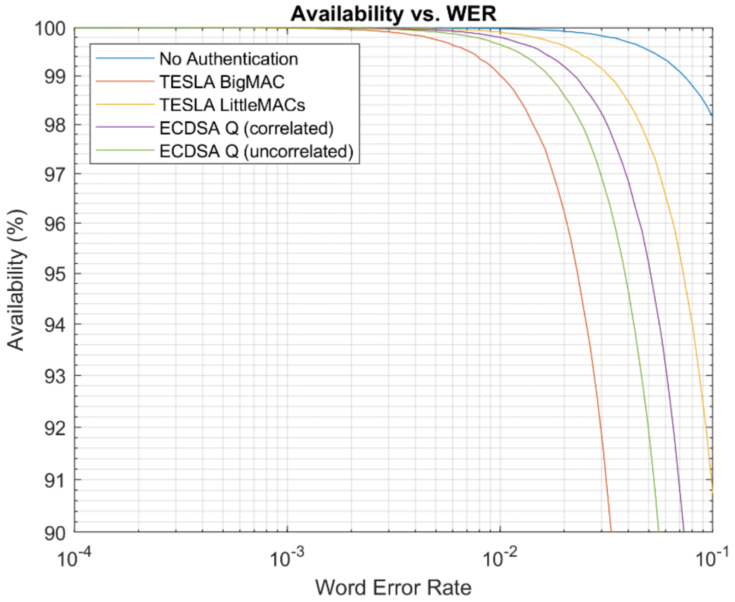


Figure 10: Availability vs. WER for a uniform distribution

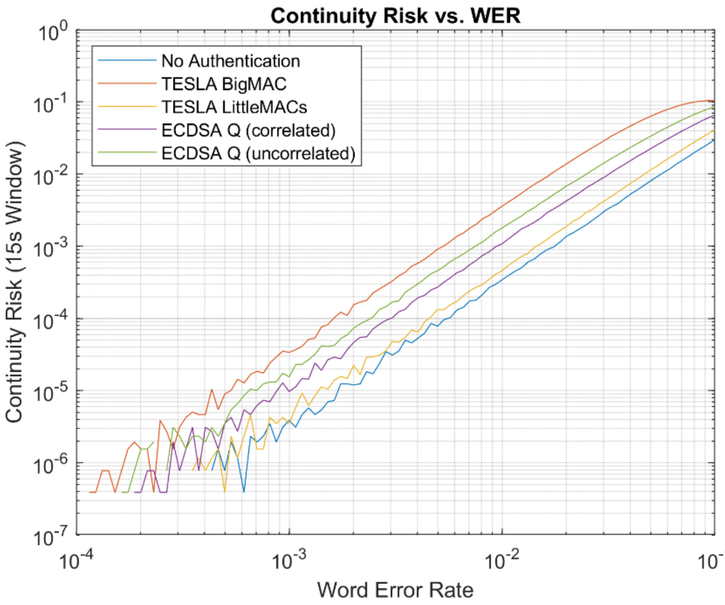


Figure 11: Continuity Risk vs. WER for a uniform distribution

Conclusions and Future Work

These results show that the impact of SBAS data authentication may be minimal with a proper design of the concept of operations. The concept of operations developed here does not allow for receivers to use any unauthenticated information that could be hazardous or misleading. An important result to note is that a variant of the TESLA scheme has shown promise in delivering a service that meets current performance requirements. The receiver emulators that have been built here also serve as an instrumental tool in the development of these authentication CONOPS and can be modified and improved upon as more testing scenarios are developed.

The final design of an authentication scheme is now closer, but there is still work that must be done. The problem of loose time synchronization in the case of TESLA necessitates the incorporation of requirements on time keeping for receivers. A state machine that defines the states of an SBAS receiver and how this loose time synchronization is achieved will be presented in the future. This may incorporate the inclusion of different instances of the TESLA keychain which will lead to changes in the authentication message type structure. In addition to this, alert and off-nominal scenarios will be incorporated in future authentication CONOPS evaluations to verify that the service TTA requirements are met.

ECDSA, up until now, has been chosen as the Q-channel authentication scheme because it is standardized by NIST. EC-Schnorr is another asymmetric scheme that offers a smaller signature length for the same security level. It is not currently standardized, but it is a provably secure scheme that may be considered for the Q-channel going forward.

Finally, there is still bandwidth that is available in all L5 rigid message schedules presented here. These are currently represented as MT63 and can be replaced with methods to authenticate data from the core GNSS constellations. Moreover, the signatures of these data can use the same keys as those used to sign the SBAS information.

References

[1] F. Rothmaier, Y. Chen, and S. Lo, "Per-satellite Confidence Estimation for Direction of Arival Based Spoof Detection," in *ION GNSS+ 2019*, 2019.

[2] J. M. Anderson *et al.*, "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," *Proc. 30th Int. Tech. Meet. Satell. Div. Inst. Navig. (ION GNSS+ 2017)*, pp. 2388–2416, 2018.

[3] S. Lo and P. K. Enge, "Authenticating aviation augmentation system broadcasts," in *IEEE/ION Position, Location, and Navigation Symposium*, 2010, pp. 708–717.

[4] J. T. Curran, M. Paonni, and J. Bishop, "Securing the Open-Service: A Candidate Navigation Message Authentication Scheme for Galileo E1 OS," in *European Navigation Conference, (ENC-GNSS)*, 2014.

[5] P. Walker *et al.*, "Galileo Open Service Authentication: A Complete Service Design and Provision Analysis," in *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015)*, 2015, pp. 3383–3396.

[6] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION*, vol. 59, no. 3, pp. 177–193, 2012.

[7] I. F. Hernández, V. Rijmen, G. S. Granados, J. Simón, I. Rodríguez, and J. D. Calle, "Design drivers, solutions and robustness assessment of navigation message authentication for the galileo open service," in *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation, (ION GNSS 2014)*, 2014, pp. 2810–2827.

[8] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, 2000, pp. 56–73.

[9] NIST, "FIPS PUB 186-4: Digital Signature Standard (DSS)," 2013.

[10] G. Neven, N. P. Smart, and B. Warinschi, "Hash function requirements for Schnorr signatures," *J. Math. Cryptol.*, vol. 3, no. 1, pp. 69–87, 2009.

[11] A. Neish, T. Walter, and J. D. Powell, "Design and Analysis of a Public Key Infrastructure for SBAS Data Authentication," *Navigation*, 2019.

[12] R. Fuller, T. Walter, and P. Enge, "Burst Mode Message Loss Effects On WAAS Availability," in *ION GPS*, 2000, no. September, pp. 19–22.