Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals

Article *in* Navigation - Journal of The Institute of Navigation · September 2017

CITATIONS
22

READS
1,201

8 authors, including:

J. T. Gillis
The Aerospace Corp.
14 PUBLICATIONS **243** CITATIONS
SEE PROFILE

Joseph Rushanan
MITRE
43 PUBLICATIONS **655** CITATIONS
SEE PROFILE

Logan Scott
University of Colorado Boulder
16 PUBLICATIONS **389** CITATIONS
SEE PROFILE

Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals

Jon M. Anderson (Canyon Consulting), Capt Katherine L. Carroll (AFRL/RVEP), Nathan P. DeVilbiss (ATA-Aerospace), James T. Gillis (Aerospace), Joanna C. Hinks (AFRL/RVEP), Brady W. O'Hanlon (The MITRE Corporation), Joseph J. Rushanan (MITRE), Logan Scott (LSC), Renee A. Yazdi (MITRE)

ABSTRACT

In this paper, Chips Message Robust Authentication, or Chimera, is proposed to jointly authenticate both the navigation data and the spreading code of a GPS civilian signal. Authentication schemes protect the user community, especially critical infrastructure users, against spoofing attacks by providing evidence that the received signal is from a reliable source. Chimera employs the concept of time-binding, in which the spreading code is punctured by markers that are cryptographically generated using a key derived from the digitally signed navigation message. The navigation message and the spreading code cannot be independently generated. Bit commitment ensures that a spoofer cannot generate the correct marker sequence until after it has been broadcast. Two variations are discussed: a "slow" channel for standalone users and a "fast" channel for more rapid authentication when out-of-band information is available. Appropriate performance metrics and architectures for Chimera are proposed, and the choice of specific parameters is explained in the context of expected performance. These design principles are illustrated with a specific implementation of Chimera for the GPS L1C signal.

I. INTRODUCTION

Spoofing is defined to be the deliberate introduction of counterfeit satellite navigation signals to supplant authentic satnav signals, e.g., to induce a user receiver to generate an anomalous position, navigation, timing (PNT) solution. Spoofing attacks against GPS civilian signals have been described and discussed in literature [1], as have been the potential end effects and consequences of such attacks [2]. The openness of GPS civilian signals means that anyone with the right skills and equipment can generate synthetic versions of these GPS signals, possibly for spoofing purposes. In fact, researchers have demonstrated successful spoofing attempts [3], [4]. The potential for spoofing motivates the need to authenticate the legitimate signals.

Numerous papers have been published describing methods to counteract potential spoofing attempts [5], [6], [7], [8], [9], [10], [11], [12]. Much of the literature has concentrated on devising ways to enable a receiver to infer the legitimacy of a signal by observing aspects of its physical manifestation (e.g. received signal power or directionality) or by observing anomalous receiver outputs. Other efforts tie the signal to its origin using cryptographic methods, including Navigation Message Authentication (NMA), Timed Efficient Stream Loss-tolerant Authentication (TESLA) and out-of-band digital signatures [13], [14], [15], [16], [17], [18]. Each of the proposed solutions offers protection against certain attack vectors accompanied by costs and limitations. For example, see Table 1 in [19]. None of the methods cited above

explicitly bind the navigation message with the spreading codes to achieve a comprehensively authenticated signal, although a method to address this shortcoming is addressed in [18].

In this paper, we propose Chips Message Robust Authentication, or Chimera, to achieve this binding between a satnav signal message and spreading code. The Chimera approach is a practical implementation of the Spread Spectrum Security Code first proposed in [13] and further refined in [20]. This paper explores the scope of system impacts and limitations that implementing a Chimera-enabled signal might entail (for example, it will not protect a user from repeater attacks).

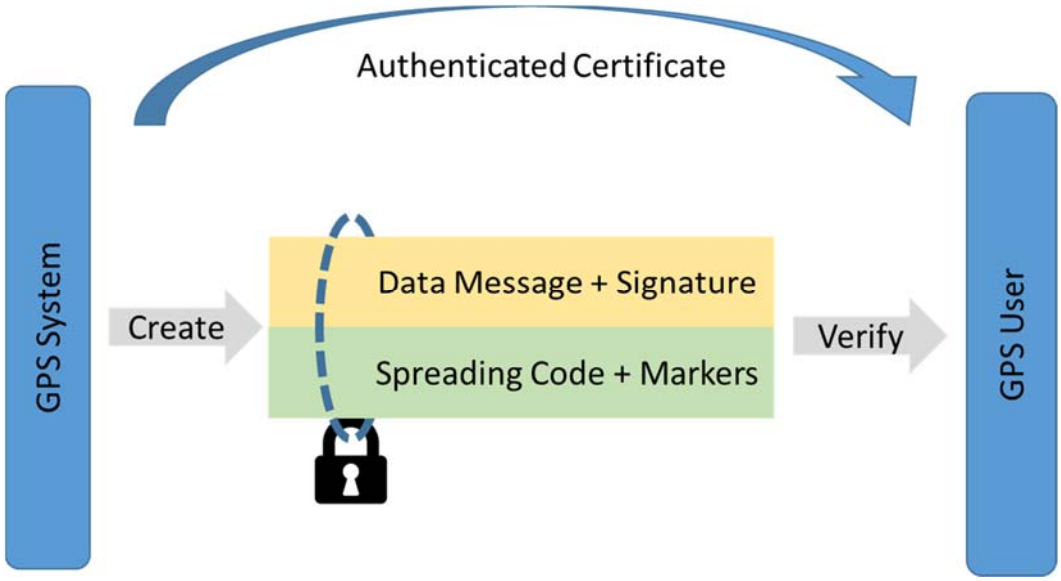

Figure 1: Binding the data message and spreading code.

We first discuss the Chimera theory of operation, explain the time-binding concept, propose metrics to assess Chimera performance and impact, and present an overview of the Chimera signal design. We then discuss potential architectures for implementing Chimera, including the "slow" and "fast" channel options and the overall impact on a GPS system architecture needed to bring the concept into being. We then describe how specific parameters for Chimera are chosen, and propose a specific implementation of Chimera for the GPS L1C signal. We conclude with observations about the role of Chimera as one component in user defense against spoofing, and with a brief discussion of the additional work that remains to fully mature this concept.

II. PROPOSED AUTHENTICATION APPROACH

In this section, we discuss the concepts behind the Chimera signal authentication approach.

A. Cryptography for GPS Signals

Cryptographic methods divide naturally into three types: symmetric key algorithms (used for encryption), hashing (including the notion of bit commitment), and asymmetric or public key algorithms (including digital signatures). Symmetric key algorithms are the traditional encryption algorithms, where both parties share a key in order to generate ciphertext that can be recovered only by a key holder. Examples include the Advanced Encryption Standard (AES).

Hash functions implement a one-way function that can reduce a set of bits to a usually-smaller hash value. Examples include the Secure Hash Algorithm, e.g., SHA-512. Finally, asymmetric algorithms employ key pairs and have the property that only the holder of a private key can perform one algorithm, e.g., digitally signing, while anyone with the public key can execute the complementary algorithm, such as signature verification. Good general tutorial references in cryptography are the web tutorial by Guttman [21] and the text by Mel and Baker [22]. More technical descriptions of the algorithms are in the text by Schneier [23] and the handbook by Menezes, et al [24].

Cryptographic functions can be applied in both the physical components (spreading code, carrier, etc) in the GPS signal and in the data components. Cryptographic methods in the physical components are used to bind time, because the signal features, such as spreading code chips, are changing fast enough that authenticating the chips amounts to authenticating time to a fine scale. In general, we use the term "marker" to denote these signal features that are used to bind time. Historically, these methods have relied on shared (symmetric) key cryptography.

Data protection methods include digital signatures and TESLA, and to date have concentrated on NMA (e.g., [18]) and variations on this approach. These methods do not authenticate time of transmission, because the data bit values change at too slow a rate; data-only authentication methods are still susceptible to more sophisticated attacks.

Chimera combines data authentication with methods in the spreading code components to authenticate time. Chimera is a general technique of an idea first suggested by Scott [13]. It extends the NMA concept by using the digital signature to generate cryptographic markers interspersed in the spreading code. Once in possession of an authenticated public key for the GPS enterprise, a user can authenticate both the navigation message data and the spreading code as originating from the same, legitimate source – and do so for each Chimera-enabled signal being tracked.

B. Authentication Metrics

Chimera is proposed as a long-term solution. It leverages the expectations of improved flexibility of a future GPS space segment and additional processing power and efficiency available to receivers to afford a new layer of protection against an increasingly sophisticated adversary. It is a system-level security implementation, requiring an enterprise-level commitment to protection for GPS users. This section describes some proposed metrics for Chimera authentication, which are summarized in Table 1 at the end of the section.

System Openness: To maintain GPS signals as an open signal and distribute the cryptographic material to innumerable and anonymous users (including potential spoofers), the authentication scheme is based on public key cryptography. This allows for wide and open distribution of keys to users without shared secrets and the corresponding security measures necessary to protect them.

To bind the navigation data with the spreading code, the cryptographic markers embedded in the spreading code are derived from the digital signature in the navigation data through a process that involves both cryptographic hashing and symmetric cryptography, as described in the

Chimera design section (following). To maintain the open nature of the authentication protocol, a "bit-commitment" approach is used, in which the ciphertext (e.g., the sequence of markers) is first exposed, and the cryptographic key (e.g., the digital signature) is revealed some time later. The length of time between the exposure of the ciphertext and the cryptographic key reveal must be sufficient to render useless any attempt by the spoofer to use the key to generate alternate but plausible ciphertext. In a GPS context, where the navigational value of the signal is so short-lived, a few seconds of latency between the exposure of the ciphertext and the cryptographic key revelation is sufficient.

Initial Bit-Commitment Latency: While necessary to the security of the system, the bit-commitment latency also creates a period of uncertainty between the times that a receiver channel has begun to track a signal in space (SIS) and the time that the SIS authenticity can be initially verified (or refuted). This represents another measure of effectiveness (MOE), referred to in this paper as the time to first authenticated channel (TTFAC). This metric is different from, but related to, the time to first authenticated fix (TTFAF) metric proposed in [25]. TTFAF refers to the time needed to calculate a position fix based on at least four authenticatable satellites. TTFAC refers to the time from the acquisition to the authentication of a single signal.

Recurring Bit-Commitment Latency: Recurring re-authentication is necessary to guard against a spoofer capturing a signal that is already being tracked. The time between authentications (TBA) metric, also suggested in [25], indicates the elapsed time (for an ideal system) between two successive authentications for a given signal.

Security: The cryptographic system employed must be strong enough to prevent a malevolent actor from predicting or forging viable ciphertext and posing as a valid signal. Thus, a key MOE is the cryptographic strength of the authentication system, expressed in bits.

Acquisition Performance Impact: The authenticated system navigation performance must be no worse for users than the legacy system, whether or not they use the authentication capability. Impact to signal acquisition is an MOE defined as the increase to the space vehicle transmit power needed to compensate for the correlation loss resulting from the authentication scheme making portions of the spreading code unpredictable to the user, as discussed in the Analysis section on marker duty factors.

Authentication Failures: Broadly speaking, two forms of authentication error are possible: missed detections (the authentication check returns a negative even though the digital signatures and markers were correct) and false alarms (the authentication check returns a positive even though the digital signature and markers were incorrect). The Authentication Error Rate (AER) is tentatively established to address both types of error; more rigorous treatment is deferred for later work. Note that Chimera authentication is a two-step process; data authentication (e.g., the digital signature verification) and code phase authentication (e.g., marker correlation) must both be successful to yield full signal authentication. A complete treatment of the AER must account for the relationship between these steps, but is beyond the scope of this paper.

Table 1: Summary of Chimera Design Considerations and Features

Chimera Design Considerations	Feature or Metric
System Openness	Public Key Cryptography Bit-Commitment of Shared Secret Keys
Initial Bit-Commitment Latency	Time to First Authenticated Channel (s)
Recurring Bit-Commitment Latency	Time Between Authentications (s)
Security	Bit Strength (bits)
Acquisition Performance Impact	Correlation Power Loss (dB)
Authentication Failures	Authentication Error Rate

C. Chimera Design

The Chimera authentication protocol implements interdependent security features that are expressed in both the navigation data and in the spreading code:

- Navigation message data are protected by digitally signing most or all of the data within a set of navigation message frames. Subsequent sets of navigation messages are each uniquely signed.
- Authentication markers (hereafter "markers") replace a fraction of the spreading code chips and may be used to authenticate the spreading code.

The markers are the core of the Chimera concept. The satellite transmits these markers as spread spectrum symbols that are "buried" in the primary spreading sequence. This can be done in several ways. As a baseline approach, we use puncturing, whereby marker symbols replace the primary spreading symbols (e.g. L1C or L5 codes) at a specified duty factor. Since Chimera authentication is used when the user is already tracking the signal, Doppler and code phase are precisely known. While receiving the satellite signal, the user does not know where these punctures occur or what their values are. Thus the user must store raw analog-to-digital converter (ADC) samples in memory and correlate with the marker samples after the key is received. Once the marker key is known, the marker symbols can be generated as a reference sequence, and the locations of the markers in time are also known. Correlation of the marker reference sequence against a sufficient sample size in memory yields a positive detection.

One important issue faced is the distribution of the key mentioned above. We considered that many users will want, or need, an authentication system that is fully contained within the signal in order to provide the service to standalone or isolated receiver sets. Conveying the key though the navigation message is a logical means to achieve this capability, but the slow data rates and the existing subscriptions to the navigation data bandwidth will limit the rate at which such keys may be distributed. We also believe that, in the future, receivers are increasingly likely to be networked to external data sources via links with much higher data rates, and will have the capability to receive new keys at a comparatively rapid rate. These approaches are labeled the "slow channel" and the "fast channel", respectively. We show that we are able to accommodate both approaches simultaneously in our design.

The Chimera generic signal design is based on the use of a public/private certificate set to generate cryptographic protections in both the navigation data and the spreading code. This

design requires the receiver equipment to have occasional contact, say once a year, through non-GPS channels to receive the public certificates.

The Chimera slow channel protocol calls for the transmitter to use the private certificate to digitally sign some portion of the navigation message data, in the manner of Navigation Message Authentication [14] [15]. The transmitting platform then passes the digital signature through a secure hashing algorithm to create a hash that is then used as the marker key, or K_{marker}. The marker key is then used in a cryptographic engine operating on plaintext frames to generate two separate sequences of ciphertext used for the markers. The bits from the first cyphertext sequence are used for the marker symbol values; the bits from the second cyphertext sequence are used for marker placement values, which guide the placement of markers within the spread spectrum sequence. Upon receipt of the entire digital signature, a participating user will be able to authenticate the contents of the navigation message and derive the markers and their placements to create a marker reference signal; non-participating users may ignore the digital signatures and use the data message content as always.

For the "fast channel", the marker keys would be generated, signed and distributed through alternate (non-SIS) channels (hereafter "out-of-band") to users. This approach eliminates the need for users to demodulate the navigation message data, and opens the possibility of changing the marker keys more rapidly. Navigation data may also be signed and transmitted out-of-band to users (users also retain the option to demodulate the navigation data from the SIS).

Here we must introduce a construction called a Chimera epoch. The Chimera epoch represents the entire symbol stream that carries the complete transmission (or receipt) of a related set of a digital signature and the derived markers. For the slow channel, the Chimera epoch is more conveniently defined in terms of a set of data frames which convey the digital signature, the signed data, and the derived markers. For the Chimera fast channel, the Chimera epoch is a selected period of time over which a marker key is fixed; the fast channel epoch is independent of the slow channel epoch and notionally, is around 2 seconds. The duration of the Chimera epoch is equal to the TBA metric defined in the previous section and is dependent on the specific signal structure to which the protocol is being applied.

The Chimera authentication process remains secure until the marker key (or the basis for generating it) is revealed. To fulfill the principle of bit commitment, the release of the marker key (or the basis for deriving it) must be deferred until the end of the Chimera epoch:

- In the case of the Chimera slow channel, the principle of bit commitment demands that the digital signature, or the final portion of it, always be included as the last of the navigation data frames in the Chimera slow channel epoch.
- In the case of the Chimera fast channel, the marker keys are released after the expiration of the associated Chimera fast channel epoch.

In either case, bit commitment requires the user to save the unprocessed ADC samples they receive for some period sufficient to reliably detect markers.

Upon receipt of either the complete digital signature or the signed marker key, the user first verifies the digital signature using the public certificate. The slow channel user then uses the secure hash to derive the marker key. Each user then replicates the steps described above to derive the marker values and their placements. The marker reference sequence (non-zero only at marker insertions), is then correlated against the previously collected ADC samples at prompt code phase to establish whether they are present and at the correct code phase. If the digital signatures were verified and the correlation indicates a positive detection, the Chimera-enabled SIS is authenticated.

The authentication process for a single Chimera epoch for the transmitter and the receiver are shown in **Figure 2** and

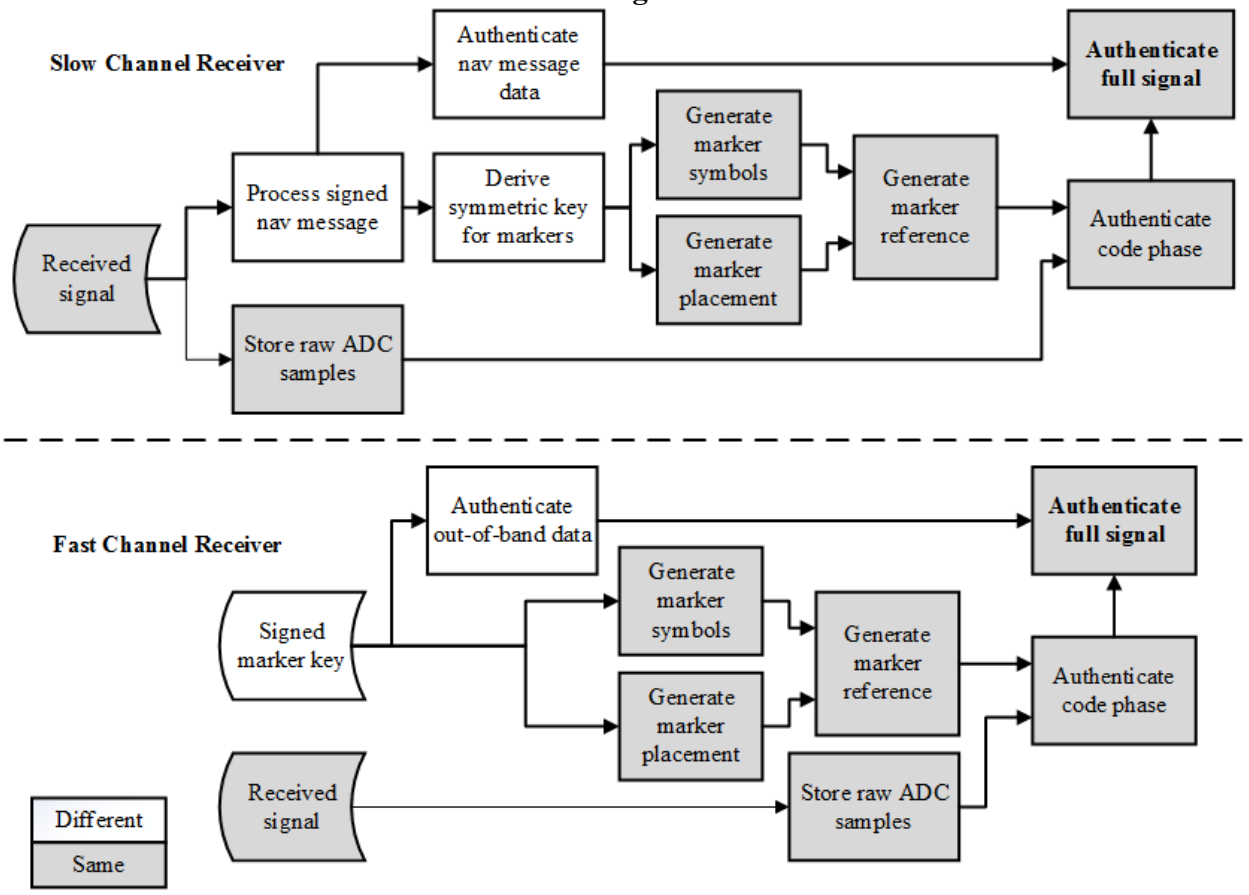

Figure 3, respectively.

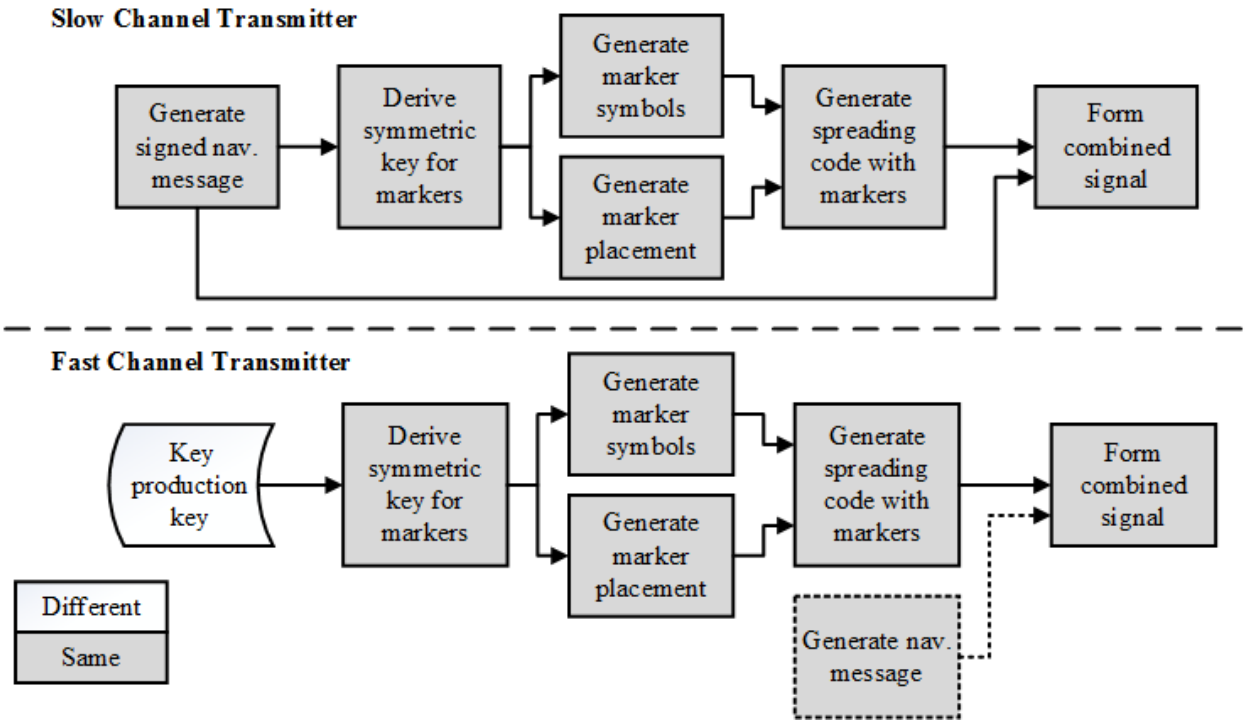

Figure 2: Transmitter operations for a single Chimera epoch for slow and fast channels.

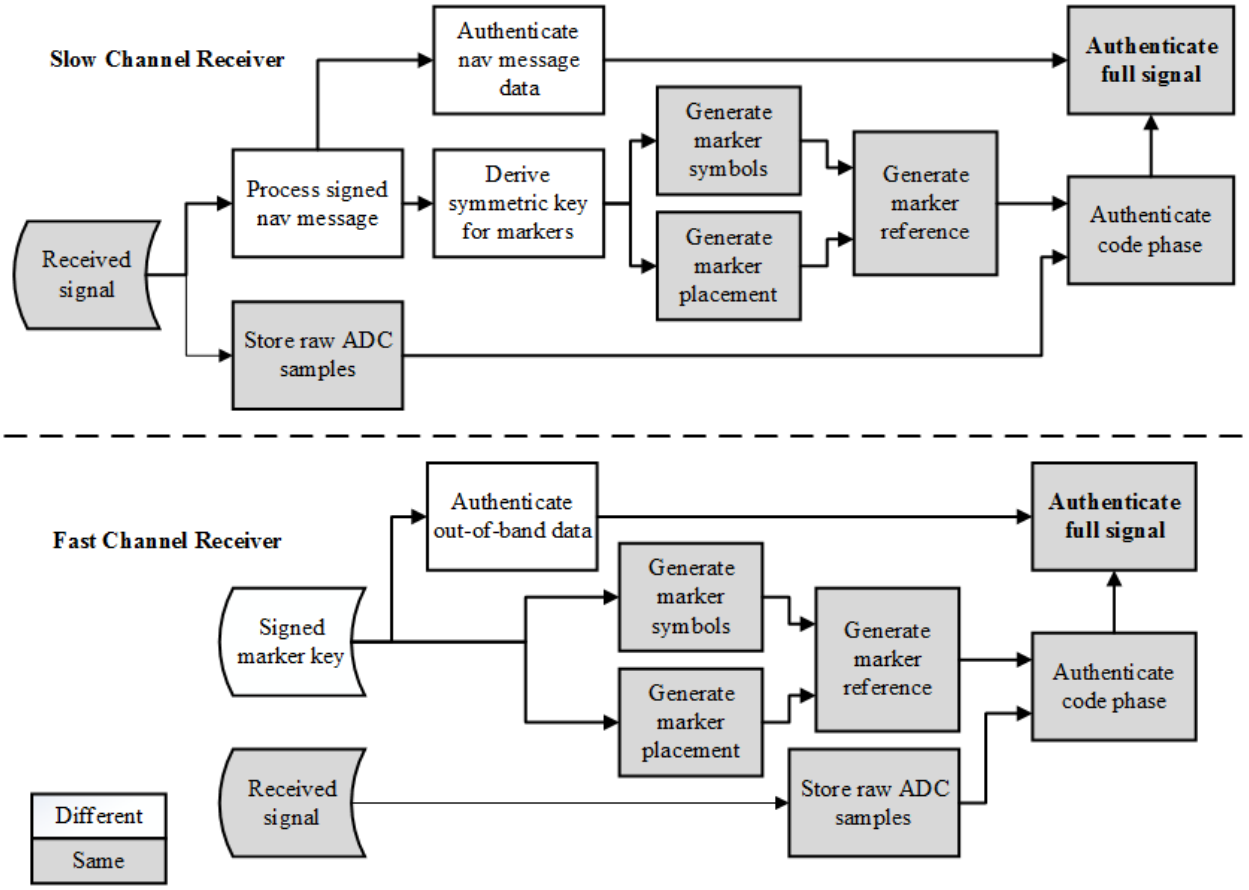

Figure 3: Receiver operations for a single Chimera epoch for slow and fast channels.

III. APPLICATION AND ANALYSIS

We illustrate the application and analysis of the Chimera protocol through a notional implementation on the GPS L1C signal. This implementation incorporates both the Chimera slow channel and fast channel concurrently.

A. GPS L1C Signal Description

The GPS L1C signal is described in [26]. This modernized civilian signal is to be broadcast on the L1 frequency beginning with the launch of GPS III space vehicles. The L1C signal comprises:

- A pilot signal, denoted $L1C_P$, to which is assigned 75% of the L1C signal power. The $L1C_P$ carries no navigation data, but is constructed by the modulo-2 addition of the spreading code with an overlay code of rate 100 bps and length 18 seconds. The $L1C_P$ is modulated onto the L1 carrier using time multiplexed binary offset carrier, with 29 out of 33 $L1C_P$ spreading code chips modulated using BOC(1, 1) and the remainder modulated with BOC(6, 1).

- A data signal, denoted $L1C_D$, uses the remaining 25% of the L1C signal power. The $L1C_D$ navigation data is applied at 100 symbols/s and formatted into messages 1800 symbols long. The message data is modulo-2 added to the $L1C_D$ spreading code, and then modulated onto the L1 carrier using BOC(1,1) modulation.

The spreading codes for pilot and data signal components are constructed similarly but are distinct codes. Each code has a chipping rate of 1.023 MHz, with a sequence length of 10230 chips. This results in chip sequences that repeat 100 times each second.

The L1C navigation message format is referred to as CNAV-2. It is organized into frames of 883 bits, and further divided into three subframes of 9 bits, 600 bits, and 274 bits for subframes 1, 2, and 3, respectively. Once the data message is prepared, it is encoded and interleaved to create the 1800-symbol frame of navigation data.

A detail relevant to Chimera is that subframe 3 is used to convey "pages" of ancillary navigation data. Six pages are currently defined in the L1C specification, but the message design is flexible enough to accommodate additional page definitions. Furthermore, the actual order for transmitting subframe 3 pages is flexible. The application of Chimera to the L1C signal will leverage the definition of a new page to carry digital signatures.

B. Marker Duty Factor

For the initial baseline design, puncturing was chosen as originally proposed by Scott [13]. Puncturing is the process of replacing some of the chips in a primary spreading sequence with alternate chips at a specified duty factor (**Figure 4Error! Reference source not found.**). The user who is tracking the primary sequence will experience a small correlation loss, which can be compensated for with increased average transmitter power. Since Chimera relies on bit commitment, and the sequence of markers is only known well after the signal is useful for tracking, both participating and non-participating users experience the same correlation loss.

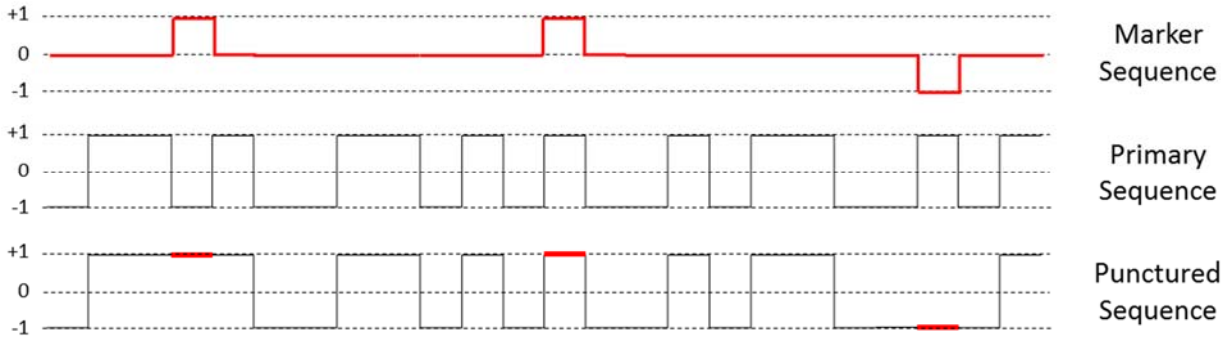

Figure 4: Puncturing

One of the first issues was to establish the duty factor of the markers. The driving factors for determining the appropriate duty factor are detection performance, correlation loss (related to additional required transmitter power), and receiver memory storage.

As shown in **Figure 5Error! Reference source not found.**, the basic Chimera process includes storage of RF samples in memory, along with time and Doppler information obtained in real-time while tracking the GPS signal. A core assumption in the baseline Chimera design is that authentication is only used when the receiver is tracking the signal and (for the slow channel) demodulating the data. When the receiver authenticates the signal using the stored RF samples at some time ΔT after the samples have been stored, the frequency and timing information obtained during tracking is used to match the cryptographically generated reference markers to the stored RF data and to compensate for Doppler effects. Coherent integration may be used, since phase information is known.

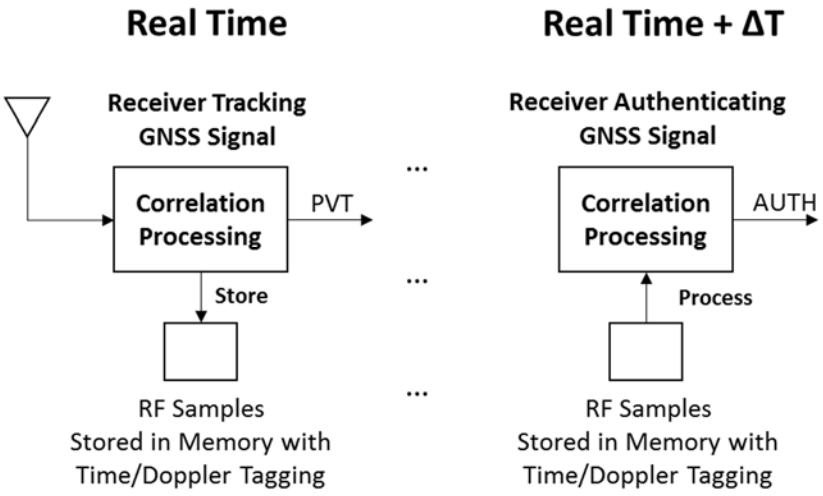

Figure 5: High Level Receiver Processing

Detection performance was evaluated in an additive white Gaussian noise (AWGN) channel using the generalized Marcum Q-function [27] for fixed false alarm rates. Assuming perfect phase lock, the signal-to-noise ratio (SNR) at the correlator output is given by:

$$\rho = 2T\left(\frac{C}{N_0}\right)_{eff} \quad (1)$$

where T is the integration time in seconds and $(C/N_0)_{eff}$ is the effective carrier-to-noise density ratio in s^{-1}. Chimera authentication is also usable without coherent tracking but may require shorter coherent integration followed by noncoherent summation. The integration time is a product of the observation time (segment time stored in memory) and the duty factor (DF):

$$T = DF \cdot T_{obs} \quad (2)$$

Since the Chimera slow channel relies on reliable demodulation of the navigation data message, the minimum expected C/N_0 is based on the data demodulation threshold. Modern GPS signals utilize error correction coding, yielding demodulation thresholds below 20 dB-Hz for L1C and 22 dB-Hz for L5 [28]. For evaluation purposes, 25 dB-Hz was used for evaluating detection as a function of duty factor. Nominal conditions for GPS are likely to be 10-20 dB higher for "clear sky" channel conditions.

Figure 6 shows probability of detection (P_d) as a function of duty factor and observation time for two different probabilities of false alarm (P_{fa}) with C/N_0 fixed at 25 dB-Hz and assuming phaselock. The left-hand figure shows P_d for $P_{fa}=10^{-3}$ and the right-hand figure shows P_d for a $P_{fa}=10^{-6}$. The selection of false alarm rate is dependent upon the verification strategy used by the receiver.

The key limiting factor for duty factor is the correlation loss caused by puncturing. Average correlation loss [13], [20] is:

$$L_{corr}(dB) = 10 \cdot \log_{10}[(1 - DF)^2] = 20 \cdot \log_{10}[1 - DF] \quad (3)$$

Figure 7 shows the correlation loss as a function of duty factor. The correlation loss is about 0.9 dB for 10% DF and 0.4 dB for 5% DF.

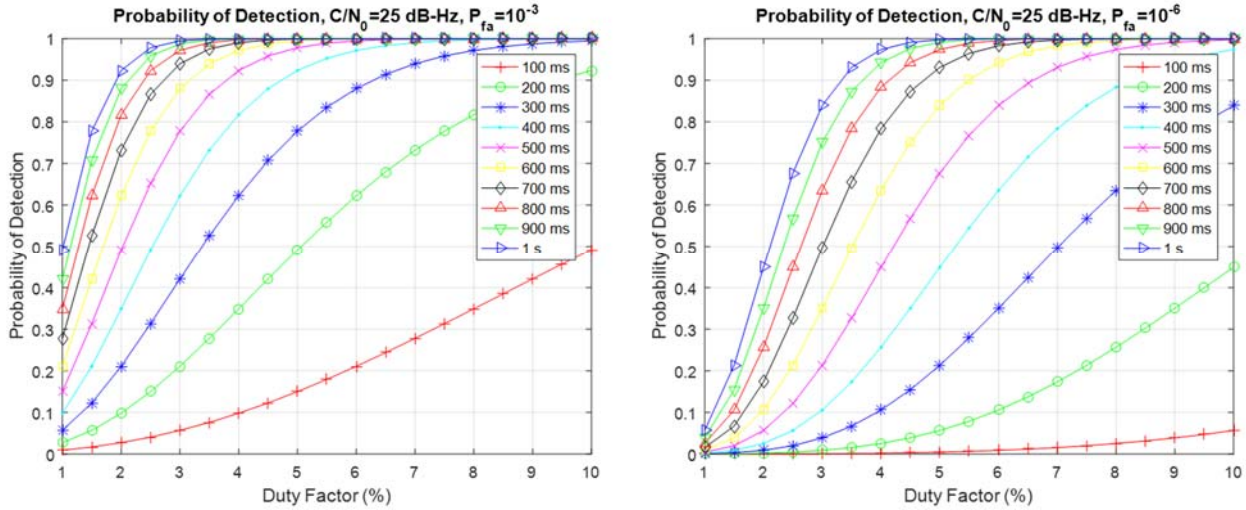

Figure 6: Probability of Detection vs. Duty Factor for C/No of 25 dB-Hz

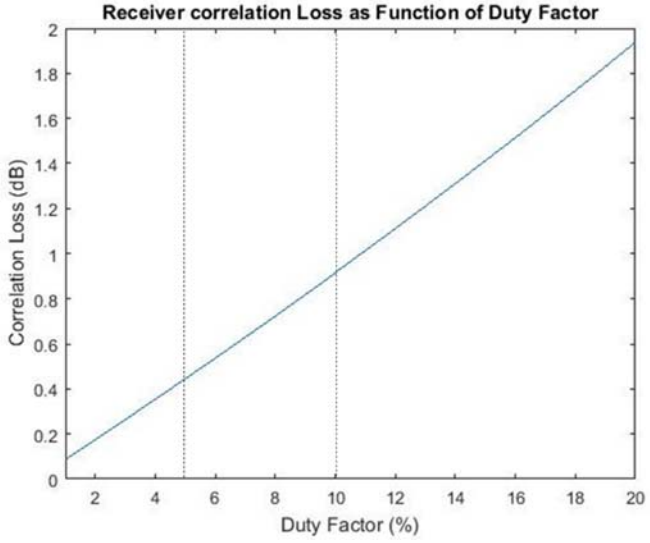

Figure 7: Receiver Correlation Loss vs. Duty Factor

Because marker placements are *a priori* unpredictable and multiple satellite signals are present simultaneously, marker collection is performed by recording raw ADC samples over the required collection interval and with the required bandwidth. For L1C, the nominal collection bandwidth is ~5 MHz and for L5, the collection bandwidth needs to be around 20 MHz. **Table *2*** shows total memory storage requirements as a function of collection time assuming 2-bit (or 1.5 bit) ADC conversion and a low IF frontend. Staggering Chimera epochs between satellites can increase memory requirements but even in that event RF sample storage should not be a significant factor for receiver implementation.

Table 2: Chimera Memory Storage Requirements

Signal:	L1C	L5
Sample Size (bits):	2	2
Sample Rate (MHz):	10	40
Corresponding bytes/sec:	2500000	10000000
Collection Interval (sec)	**Storage Requirement (Mbytes)**	
0.10	0.25	1.00
0.20	0.50	2.00
0.50	1.25	5.00
1.00	2.50	10.00
2.00	5.00	20.00
5.00	12.50	50.00

A duty factor of 5% for each the fast and slow channels was selected for further analysis and a baseline design. This yields a total marker insertion duty factor of 10% and a correlation loss of 0.9 dB, while supporting reasonable memory storage and detection performance. Detection performance as a function of C/N_0 for 5% duty factor is shown in **Figure 8**. The left-hand figure shows P_d for $P_{fa}=10^{-3}$ and the right-hand figure shows P_d for a $P_{fa}=10^{-6}$.

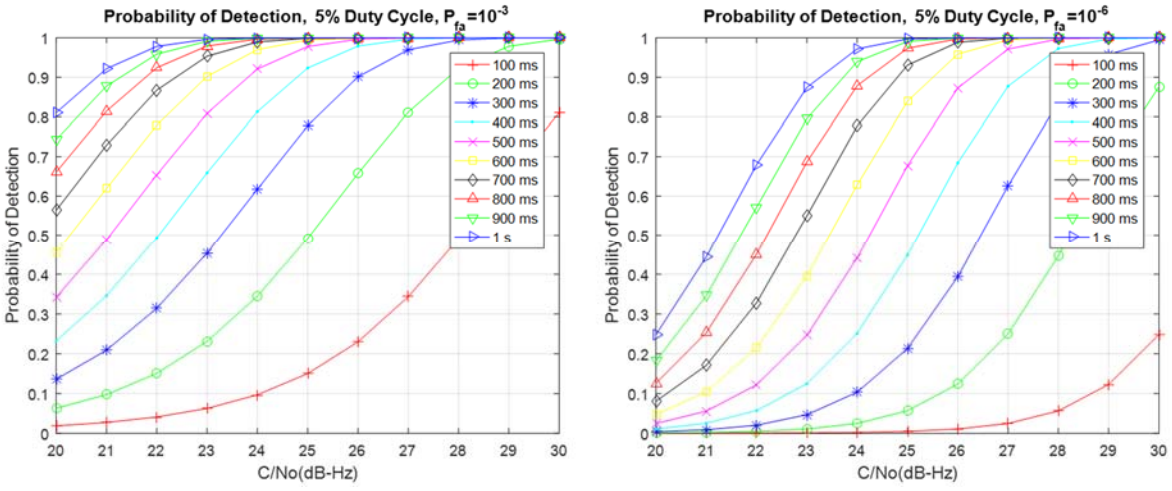

Figure 8: Probability of Detection vs. Duty Factor vs. C/N_0 for 5% Duty Factor (PLL)

The user will have a variety of options for implementing a suitable authentication strategy. Two examples will illustrate this.

Example 1: The user desires reliable authentication (≥ 95% per signal) in low C/N_0 conditions, near the data demodulation threshold of 25 dB-Hz. False alarm probability is set to 10^{-6} and a single observation is made during the Chimera epoch. From the right-hand part of **Figure 8**, the required observation time is 800 ms to achieve 95% detection probability at 25 dB-Hz.

Example 2: The user desires to minimize memory storage requirements and expects to only need authentication for C/N_0 of 30 dB-Hz or greater. Two observations will be made, separated in time sufficiently so they can be considered independent. A successful authentication will be declared when both observations result in a positive detection. To achieve 95% probability with two independent observations, the detection probability needs to be greater than 0.97 (the square root of 0.95). Using **Figure 9**, where a false alarm probability of 10^{-3} has been chosen, the required observation time for detection probability ≥ 0.97 at 30 dB-Hz is about 150 ms. For two observations, the total storage time required is 300 ms.

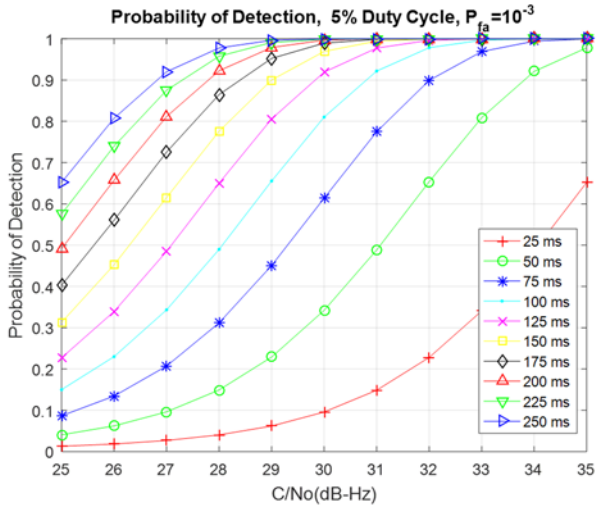

Figure 9: Probability of Detection vs. Duty Factor for 5% Duty Factor

In practice, the receiver developer will likely experimentally tune the authentication implementation to accommodate more realistic channel conditions, operational needs, initial time uncertainty, and verification strategies.

C. Distributing Markers for Fast and Slow Channels

To take advantage of the higher signal power available, the markers for the L1C signal are allocated to the L1C pilot signal. Marker insertion locations are cryptographically determined at the chip level so as to confound denial of service, power modulation, and other attacks on markers. In our current baseline, BOC(6,1) modulated chips are placed off limit and fast channel and slow channel insertions are non-conflicting. The process uses cryptographically driven selection tables to select specific insertion sites and to control duty factors.

The interspersion of BOC(6, 1) modulation throughout the pilot signal spreading code sets constraints on the placement of markers, but also provides a convenient basis for organizing the distribution of markers in the spreading code. The SIS specification implies the division of the 10230 chip spreading code sequence into 310 segments of 33 chips each, and specifies that chips 0, 4, 6, and 29 in each of these segments are to be modulated as BOC(6,1).

Referring to **Figure *10***, we colloquially referred to the 33-chip segments as "marker frames". Allocating alternating marker frames between the slow and fast channels results in 155 marker frames for each. Ignoring the Look-Up Table Schedule for the moment, for each marker frame, 8 bits of ciphertext selects one of 256 specific insertion patterns to be used for that marker frame using a fixed lookup table by using the ciphertext as an address.

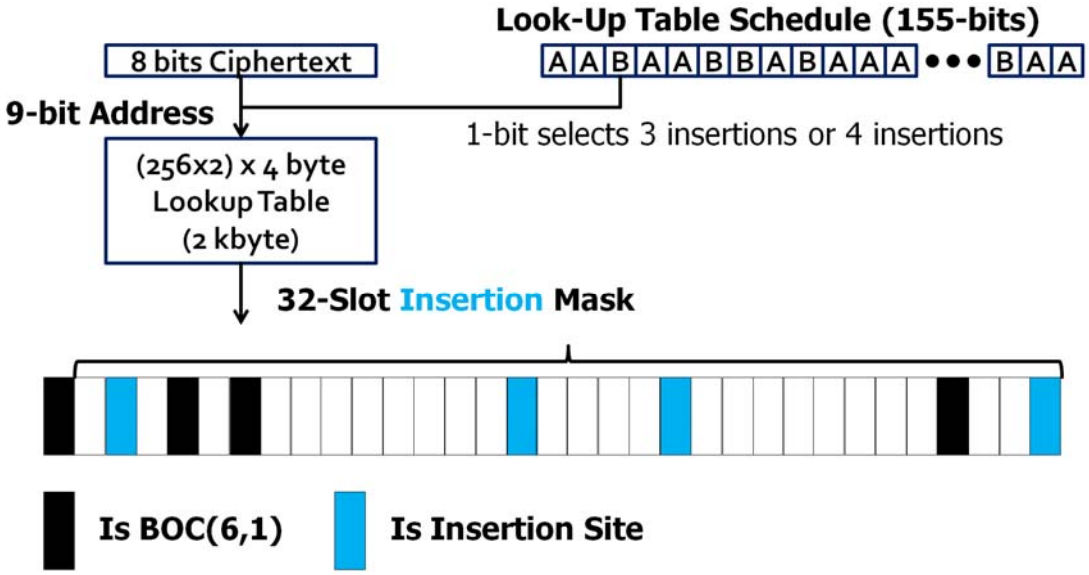

Figure 10: Simplified Marker Insertion Table Process for Fast Channel (or Slow Channel)

The L1C$_P$ spreading code sequence of 10230 chips repeats over each overlay bit. Applying an overall 10% puncture over this sequence implies the need for 1023 marker symbols over both channels, or 511.5 marker symbols per channel. If we were to use 3 marker insertions per marker frame, then the overall duty factor would be 3/33=9.1%. Using 4 markers per marker frame yields 4/33=12.1% duty factor. To obtain finer control, a separate 155 bit Look-Up Table Schedule selects whether 3 insertion sites or 4 insertion sites will be generated. This is done by appending the 1-bit value to the ciphertext so as to generate a 9 bit address. With this scheme, relatively fine control over duty factor can be obtained. Using a slightly more complex approach, constraints on fast and slow channel marker frame duty factors and placements can be also be removed.

Our concept is to concatenate the 128-bit outputs of a 256-bit Advanced Encryption Standard (AES-256) cryptographic engine into two long random sequences, one as a source for marker values and the other as a source for marker placements. From these sequences, marker values

and marker placements are drawn as needed. The AES-256 outputs are obtained by encrypting deterministically defined 128-bit plaintext frames using a 256-bit marker key.

The marker key will be supplied differently for each of the slow channel and fast channel. The slow channel user will derive the marker key from the digital signature (see the next subsection). For the fast channel, the user receives a signed copy of the marker key from an out-of-band source. After verifying the signature, the fast channel marker key is used directly.

D. Digital Signature and Chimera Slow Channel Definition on L1C

In keeping with the desire to preserve margin for other future uses, we arbitrarily chose to limit the imposition of additional subframe 3 pages dedicated to Chimera to no more than 20% of the total subframe 3 traffic.

The most convenient means of conveying the digital signature is to define new pages for subframe 3 dedicated to the task. Subframe 3 comprises 250 bits of information and a 24-bit CRC. In practice, 14 bits of the 250 must be reserved for an 8-bit PRN field and a 6-bit page identification number, leaving 236 bits in which to define a digital signature format. We consider a 236-bit digital signature to be too small; hence, we must accept that at least two subframe 3 pages will be needed to convey the digital signature, with a maximum length of 472 bits. This approach has the additional benefit that attacks such as the forward estimation attack outlined in [29] are not effective since the message covered by low density parity check (LDPC) forward error correction comprises mainly signature bits that are *a priori* unpredictable.

We chose the Elliptic Curve Digital Signature Algorithm (ECDSA) P-224 for its balance between bit-strength (112 bits) and data burden. The ECDSA P-224 results in a 448-bit digital signature; dividing this signature in two would require room for 224 bits in each of two CNAV-2 digital signature pages, with 12 bits of margin. At least one of those bits, and perhaps more, should be allocated to identify which part of the digital signature the present page carries, thus allowing the signature to be reconstructed in the correct order.

If two message frames must be dedicated to carrying the complete digital signature, and given the self-imposed constraint on impact to navigation message traffic, then an entire digital signature would be conveyed at most once every 10 messages, or every 180 seconds. This is the basis for the Chimera epoch for the slow channel on the L1C signal being 180 seconds.

To best preserve the security of the Chimera signal, we stipulate that one of the two digital signature frames always be placed in the last message of the epoch. The other digital signature page may be placed in any of the preceding nine frames.

We tentatively propose that the data to be signed will be drawn from every subframe 1, every subframe 2, and the remaining eight subframes 3 (those not carrying the digital signatures) within the current Chimera epoch. The actual specification of which data to sign should await more detailed trade studies.

Given the dependence of marker generation and placement, as well as the overall authentication scheme, on the correct demodulation of the digital signature, an initial analysis of the error probability is warranted.

Authentication error probability, which is called Authentication Error Rate (AER) in the literature, is predicated in part on the probability of an uncorrected bit error. For L1C, there are three different types of encoded messages to consider, each having a different probability of bit error calculation methodology. **Figure 11** shows the three message types in the frame. Each message type resides in a subframe.

Subframes 2 and 3 are encoded with a LDPC. The probability of error of LDPC codes is not easily evaluated with a closed form solution. Published data from [30] was used to approximate message error for L1C subframes 2 and 3.

The probability of error of subframe 1 can be calculated as in [31] using the following approximation based on the error-function Q (not to be confused with the Marcum's Q function):

$$P_{err} < \sum_j A(d_j)\, Q\left(\sqrt{2 d_j E_b / N_0}\right) \qquad (4)$$

where A and d are a multi-dimensional constant of the form (and zero elsewhere),

$$A(20) = 51, \quad A(24) = 204, \quad A(28) = 204, \quad A(32) = 51, \quad A(52) = 1$$

Message error for L1C subframe 1, L2C, and L5 was approximated using the following equation:

$$P_m \approx 1 - (1 - P_{err})^N \qquad (5)$$

where, N is the number of bits in the message. If the message error probabilities are considered largely independent, but not mutually exclusive, then two message error probabilities can be combined to calculate total AER for NMA for two messages, by using the equation:

$$AER = P_{m1} + P_{m2} - P_{m1} P_{m2} \qquad (6)$$

This equation can be expanded to multiple messages, as needed, depending on how the messages are being used and combined for different trades.

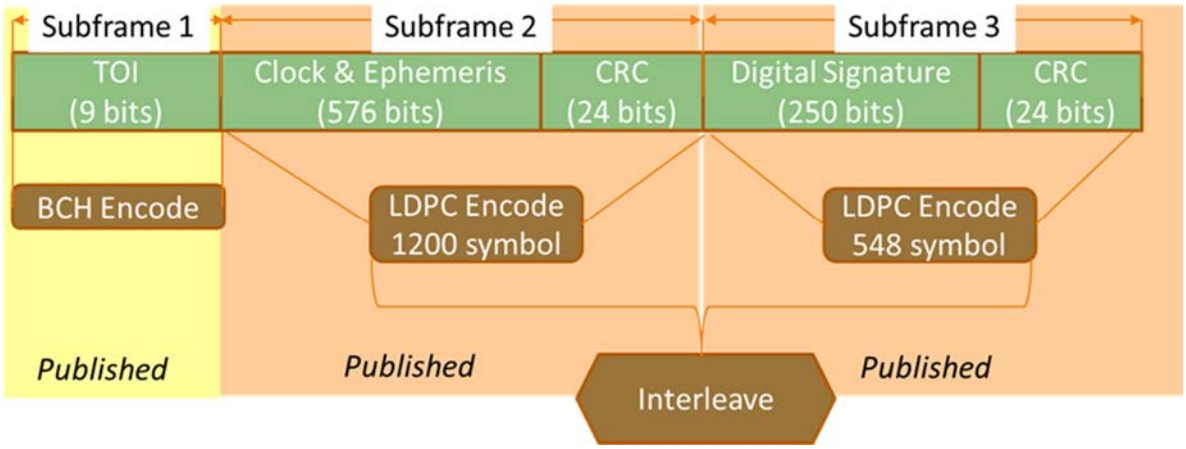

Figure 11: L1C Message Structure

Figure 12 shows the impact of number of messages signed on AER for L1C as a function of data channel $L1C_D$ C/N_0, given perfect carrier tracking. In general, digital signature verification error is not very sensitive to how many messages are signed, but it is sensitive to which messages are signed. A verification error is declared if there is an error anywhere in the messages being signed or in the digital signature. So, in the case of L1C, where there are three different message error probabilities, the verification error will be driven by the message with the highest error probability, not the number of messages signed. The messages that are the most important to sign and critical are designed to arrive with a low error probability. They are also the most impacted by verification error. Subframe 1 is designed to have low error probability for C/N_0 of greater than 10.5 dB-Hz, with perfect carrier tracking. As was previously discussed, digital signatures are placed in subframe 3, since that is the only subframe that has the ability to add message types, but subframe 3 messages are designed for $L1C_D$ C/N_0 that are greater than 18 dB-Hz. In other words, in degrading channel conditions, verification errors caused by unrecoverable bit errors in subframe 3 are likely to occur well above the threshold at which the integrity of data in subframe 1 is significantly threatened. Strategies for handling this potential situation, along with many others, are best evaluated and selected by the receiver designer.

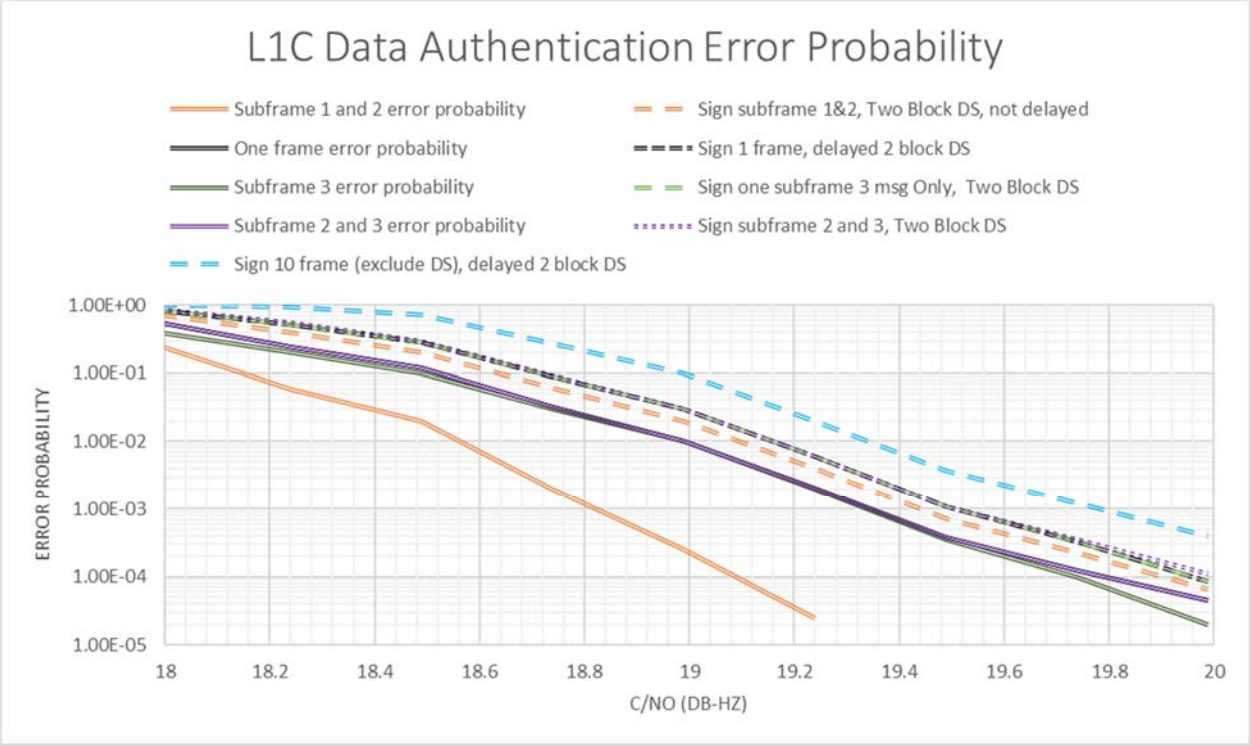

Figure 12: L1C Digital Signature Authentication Error Probability

Because of the periodicity of the slow channel digital signature, there is a risk that a nefarious operator might attempt a denial of authentication attack. One way to do that would be to attack only the second part of the digital signature of the slow channel implementation. Subconstellation staggering, where Chimera epochs are staggered between satellites, provides a measure of defense against such an attack and in any event, such attacks are easy to detect. The receiver should put in place some mechanisms to detect and respond appropriately.

E. Chimera Fast Channel Definition on L1C

For the Chimera fast channel on L1C (as on any signal), the Chimera epoch may be set to any arbitrary length that can be supported by the out-of-band delivery of the marker keys. We believe a 2 second fast channel Epoch is achievable and relevant to safety-of-life applications.

IV. ARCHITECTURE

Chimera is a system-level protocol, and its implementation will have impacts on all three segments of a GPS system (Control, Space and User Segments). The logical architectural highlights for the slow and fast channel versions of Chimera are shown in **Figure 13** and **Figure 14**, below, while **Table 3** compares and contrasts their functional roles.

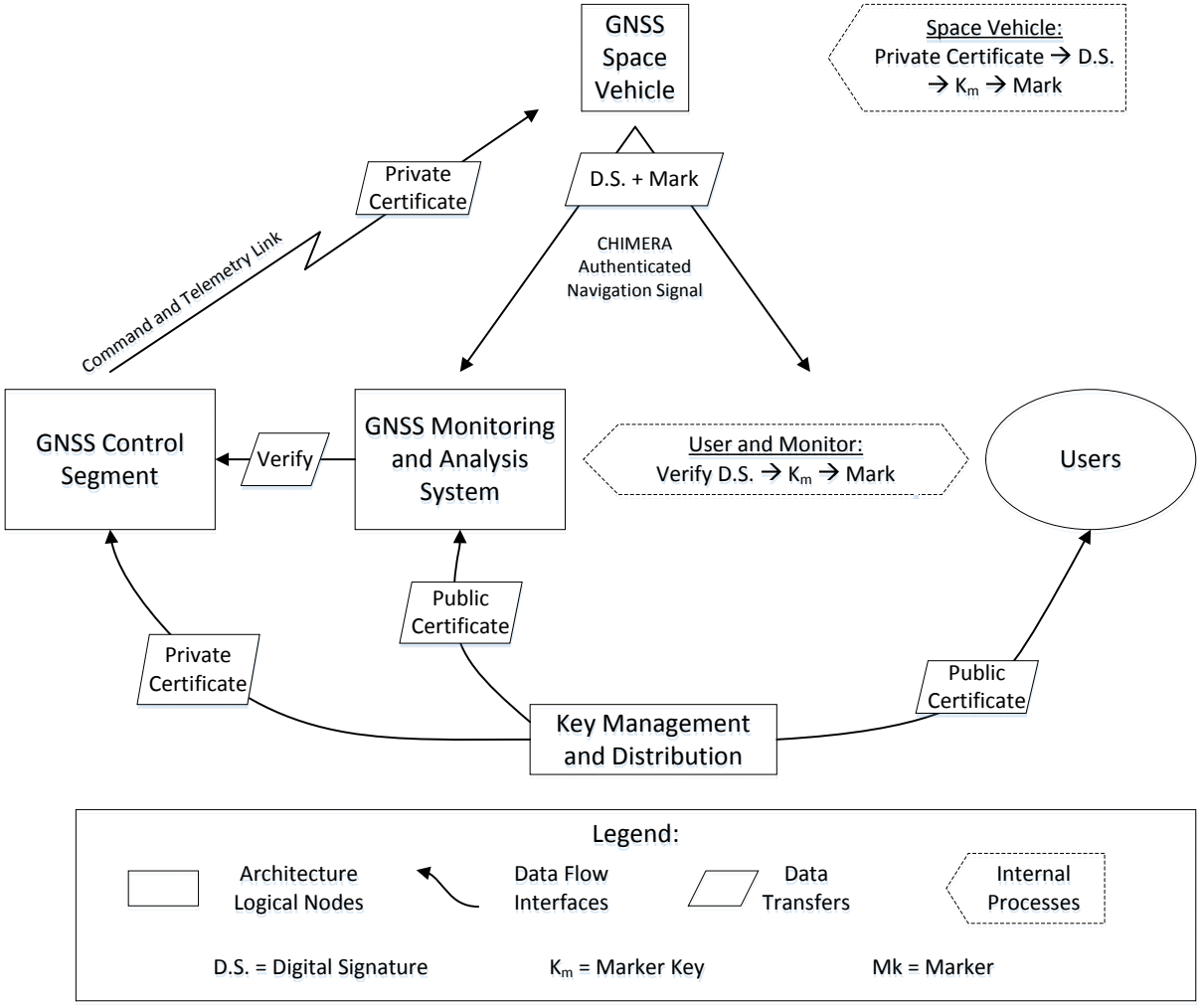

Figure 13: Chimera slow channel logical architecture.

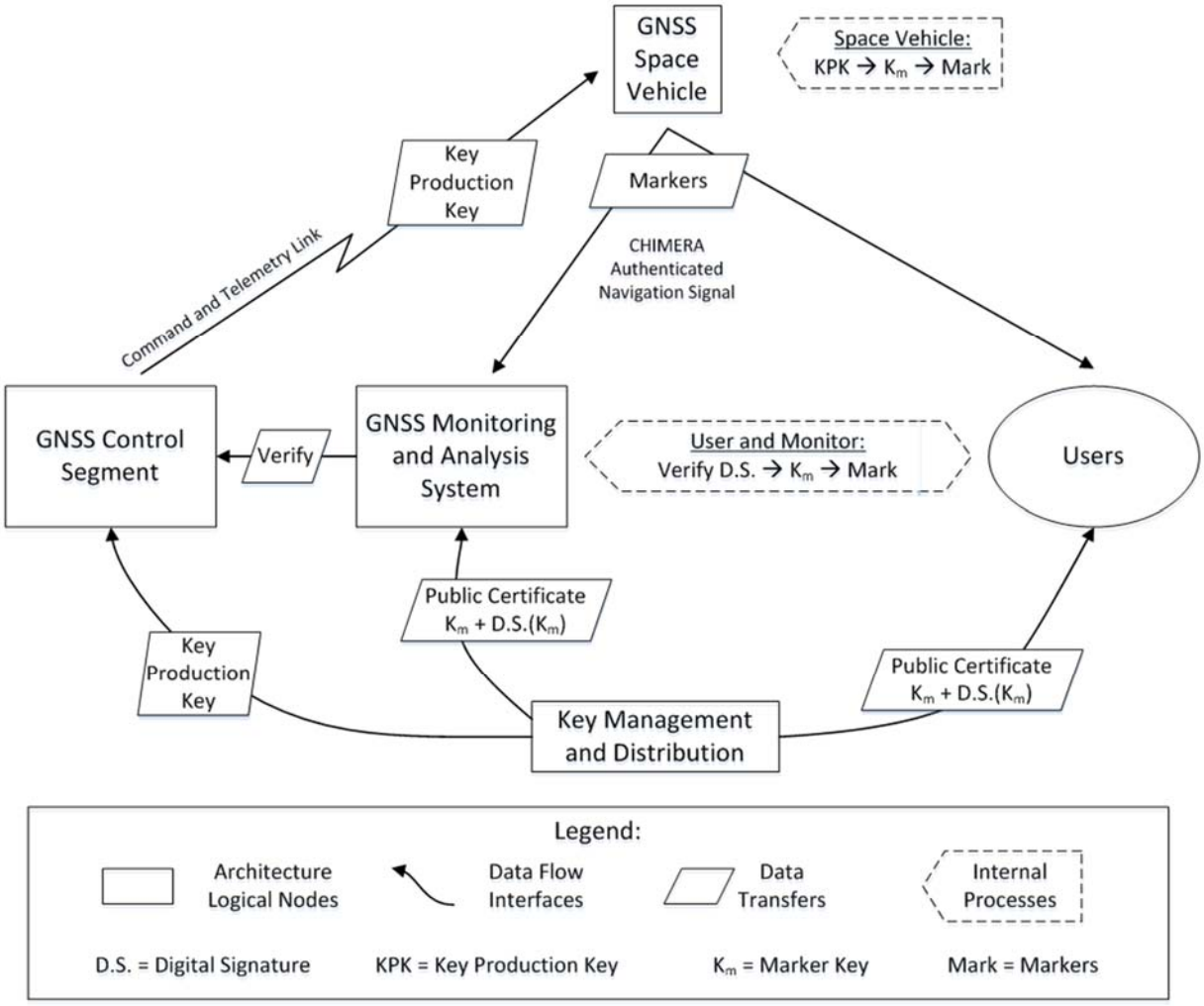

Figure 14: Chimera fast channel logical architecture.

Table 3: Functional description of the Chimera logical architecture nodes.

Logical architecture node	Slow channel function	Fast channel function

Key Management and Distribution	• Creates the private and public certificates on a periodic basis • Distributes private certificate to the control segment for upload to the space segment • Makes public certificate available to users and the monitoring system • Generates replacement certificates for contingencies	• Creates the key production key (KPK) and the private and public certificates on a periodic basis • Distributes the KPK to the control segment for upload to the space segment • Distributes signed marker keys to users and the monitoring system • Makes public certificate available to users • Generates replacement certificates for contingencies
Control Segment	• Uploads the private certificate to the space vehicle • Executes anomaly contingency plans as needed	• Uploads the KPK to the space vehicle • Executes anomaly contingency plans as needed
Space Vehicle	• Generates the slow channel Chimera authenticated navigation channel in accordance with the process described in Analysis section	• Generates the fast Channel Chimera authenticated navigation channel in accordance with the process described in Analysis section
Users	• Collects and verifies the slow channel Chimera authentication markers as described in Analysis section	• Collects and verifies the fast channel Chimera authentication markers as described in Analysis section
GPS Monitoring and Analysis System	• Collects and verifies the slow channel Chimera authentication markers as described in Analysis section • Verifies authentication signal compliance • Provides status and warning to GPS Control Segment	• Collects and verifies the fast channel Chimera authentication markers as described in Analysis section • Verifies authentication signal compliance • Provides status and warning to GPS Control Segment

There is no escaping the increased complexity and functional burden on the whole of the GPS enterprise, should it choose to implement Chimera. We assess the impacts in the following subsections.

A. Key Management and Distribution

The means to generate the cryptographic materials – the private and public certificates and, in the case of the Chimera fast channel, the KPK– must be identified, and the means of production must be afforded physical, procedural, and cyber protections. While the details differ from current GPS Control Segment responsibilities, public certificate distribution is commonplace in the commercial sector.

A trusted distributor must be responsible for distributing the public certificates (slow and fast channels) and signed marker keys (fast channel) to users. It may or may not be part of the GPS enterprise.

Security considerations may shape the alignment of functions between key management infrastructure and trusted distributors to make security requirements more congruent, particularly in the case where both slow and fast channel services are offered simultaneously. In any case, plans and procedures must be devised to protect the integrity of the key management and distribution, but these are beyond the scope of this paper.

B. Users

Whichever version of Chimera is implemented, Chimera users will need a capable receiver and some means to ingest a public certificate and/or signed marker keys to enable the authentication. In the case of the fast channel and its rapid dissemination of the signed marker keys, the receiver will almost certainly require continuous network access.

Implementing Chimera can be expected to result in increased size, weight and power (SWaP) relative to a standard receiver, all else being equal. A significant question is how the additional SWaP compares to the SWaP imposed by other anti-spoof methodologies, and the relative security value gained for the cost.

One key feature of Chimera is that the loss of a Chimera-enabled receiver poses no threat to the security of the remaining users. The receiver will have only public certificates, marker keys, and publicly available algorithms.

The impact to PRN code correlation must also be considered. The presence of the markers within the spreading code will result in, on average, approximately half of the punctured chip values being inverted, and these differences are by design unknown to the users. This is addressed in detail in the Analysis section on marker duty factors. We propose that the space segment power output be increased slightly to counteract this correlation loss, as discussed below.

The ultimate impact on the receiver equipment will very much depend on the value-added decisions made by the receiver manufacturers. Chimera provides a per-channel authentication that defends against some threats. Achieving an overall defense posture must rest with receiver manufacturers, who must address such issues as:

- How to interpret and handle potential missed authentications or other potential failures
- Whether and how to incorporate complementary anti-spoofing features to provide a depth-of-defense against various threats
- How to handle the satellite constellation evolution, while Chimera-capable SVs are being deployed, and not all navigation signal channels are capable of being authenticated

These receiver-level design decisions are beyond the scope of this paper.

C. GPS Space Vehicle (SV)

Anticipating both the desire to reduce the demands on the Control Segment and the potential for certain on-board management of the navigation message data, our proposed architecture allocates to the SV responsibility for generating digital signatures, marker keys, and punctured spreading code sequences. The SV must have the data processing and storage capabilities to enable the generation of the Chimera signal.

Alternately, it is possible to allocate much of the generative function to the Control Segment, adjusting both the CONOPS and the detail design to accommodate. The space vehicle in this case must be capable of handling the additional uplink time and the data storage necessary to enable this approach. The space vehicle will also require increased power generation and waste heat rejection capacity to compensate for the correlation loss incurred by modifying existing signals.

Finally, to compensate for the correlation loss caused by the spreading code markers, the SV transmitter could allocate additional RF power to the Chimera-enabled signal (See the Analysis section on marker duty factors).

D. GPS Control Segment

The enterprise business model chosen for implementing Chimera will affect the allocation of functions between the GPS Control Segment and the GPS Monitoring and Analysis System. In this paper, we limit the scope of the GPS Control Segment to be those functions directly related to the command, control, and maintenance of the SV, while the GPS Monitoring and Analysis System is allocated those functions related to monitoring and assessing Chimera signal health.

The Control Segment must interface with the key management infrastructure. It must accept the private certificates for uplink to the SV, and it must be enabled to perform maintenance, troubleshooting, and recovery of the SV subsystems needed to implement Chimera. These requirements place additional burdens on the Control Segment systems, of course, but also must be factored into the overall security, procedure development, and training implemented.

E. GPS Monitoring and Analysis System

As with standard GPS navigation signal monitoring, the Chimera-enabled system must include a monitoring capability to ensure adequate surveillance of Chimera availability and performance.

While Chimera is not intended to be the sole means of defense for any receiver, it will likely afford protection against a distinct subset of spoofing attacks. The Chimera signal must therefore be reliable and trustworthy, with the signal quality guaranteed to support a specified level of performance.

The potential for a spoofing attempt may be enhanced in times of systemic failures of the Chimera signal. If some systemic failure results in one or more transmitters broadcasting non-compliant Chimera markers or message content, the failure should be assumed to be visible to the malevolent actors as well, who may be prepared to exploit the opening. In such a situation, timely detection and alerting of users is critical.

The actual implementation of a monitoring and analysis system might be done by upgrading existing monitoring sites or by deploying a dedicated Chimera monitoring network. In either case, if the navigation signal monitors use the Chimera signal to generate tracking measurements, the quality of those observations and the validity of the solutions to which they contribute should be verified.

V. FUTURE WORK

The concept of Chimera appears feasible at this analytical level. So far, however, neither the potential failure modes nor the full implications of implementation on the control infrastructure, the transmitting platform, or the receiver have been investigated. Follow-on efforts to this paper will include a laboratory instantiation of Chimera, with an intent to generate empirical data regarding performance metrics and estimates of the system impacts. One specific target of study should be the marker placement algorithm, and whether alternate approaches might be more efficient to apply.

Indeed, to enable a thorough and meaningful evaluation as described, relevant and incisive metrics must be defined. Performance metrics are a bit easier, and we've been able to draw from work such as [25]. The major challenge is to distinguish between metrics that apply to the specific Chimera process as applied to a single signal, the metrics that apply to the authentication and tracking of multiple Chimera-enabled signals at the receiver level, and the Chimera contribution to overall system security, particularly when the threat does not have a clear mathematical description.

If the Chimera conceptual design survives scrutiny, it would be prudent to perform "red team" evaluations against the signal, both in laboratory and in field conditions.

There are also variations to the baseline design to consider as well. One variation for authenticating the navigation data is to implement the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) process, such as described in [17] and [18]. In summary, TESLA involves creating a chain of Message Authentication Codes (MAC) through the repeated application of a one-way hash function, then revealing the chain of MACs to the users in the reverse order of their creation, until finally the root key is revealed. The implementation likely entails spacing the issue of digital signatures several Chimera epochs apart, and including the MAC chains in the intervening Chimera epochs. Incorporating TESLA in the Chimera protocol for a single transmitter is straightforward and requires only minor adjustment to the marker key derivation process, but it appears to offer very little advantage relative to the perceived loss of security robustness (based on cryptographic bit-strength). More intriguing is the potential to use TESLA in a cross-satellite authentication capacity, as described in [32]. In this scheme, the hash chain and the anchoring digital signatures are distributed throughout the GPS constellation, and the contents of all navigation data messages are interdependently authenticated. An initial examination of this scheme suggests advantages for TTFA at the receiver level. Again, we defer to future work a more detailed analysis of the benefits, costs and risks of this approach.

The use of the navigation messages to convey digital signature data to standalone users via the Chimera slow channel is a driver for the length of the Chimera epochs for each signal. The

available data bandwidth limits the TTFAF/TTFAC that can be achieved. Meanwhile, the addition of the Chimera digital signatures to the message train reduces the opportunity to apply those traffic margins to other purposes. Therefore, another line of inquiry is the potential to use alternate modulations to convey digital signature data. Concepts that would apply modifications to the signal amplitude, the subcarrier, or the chip shape are under consideration, and some preliminary analysis is in progress.

The Chimera framework proposed in this paper is intended as a tool in the defense against spoofing; it provides an indication of the authenticity of each received signal. Chimera does not prescribe a specific way in which this tool should be used. There are still many open questions revolving around how a receiver should respond when a signal fails to authenticate. These include:

- What action(s) should a receiver take in the event of: A single-signal authentication failure? One or more authentication failures for a signal that was previously authenticated? More than one signal failing to authenticate? All signals failing to authenticate?
- Should a receiver respond differently depending on where the authentication failure occurred (data authentication versus code phase authentication)?
- Is there a C/N0 below which authentication should not be attempted because false alarms become too probable?
- Should receivers implement techniques analogous to RAIM for situations with mixed authenticated/unauthenticated signals?
- Are there reasons why one might wish to use both slow and fast Chimera simultaneously?
- What actions should receivers take to detect and mitigate a "Denial of Authentication" attack?

It is expected that receiver manufacturers will answer these questions differently depending on target users and use cases.

Implementing Chimera will have implications for the Control Segment as well. Lines of investigation address the operations concepts for maintaining the SVs; methods for monitoring the Chimera signal; reaction to and recovery from SV anomalies; architecting the interfaces to and interactions with the key management and distribution functions; and security against asymmetric attack, especially cyberattack, including recovery from a breach.

VI. CONCLUSION

We propose that a system-level authentication approach such as that described above would provide a useful means for authenticating a satnav signal, doing so in a way that effectively binds the navigation message data with the spreading code to achieve increased security against more sophisticated spoofing attacks.

We emphasize that this technique addresses a user's ability to authenticate a signal that has been acquired and is being tracked. It does not "mitigate" spoofing. That is, Chimera cannot prevent a spoofer from capturing a tracking loop. Instead, it offers a means for a user to learn that a

spoofing attempt is underway, and to treat the receiver's navigation and timing outputs with wariness.

Even if the Chimera design is implemented on multiple signals, there remains for the receiver design a large trade space for how to handle the multiple signals needed to form a navigation solution; how to leverage a partial constellation during the deployment period; how to distinguish between and characterize random, occasional errors and a systemic failure to authenticate one or more signals; and how to incorporate complementary security features to buttress Chimera's "blind spots."

Finally, we stress that Chimera is not a panacea solution to spoofing but it is a powerful tool in creating a defense in depth and, it renders well known "signal generator" attacks such as those demonstrated by Humphreys [19] and others ineffective. The availability of an authenticatable signal can also play a role in defending against suborned receiver software and cyberspoofing by providing a mechanism for detecting false position reports [20]. The receiver design and deployment advice offered in [33] will remain as relevant in the future as it is now. In the end, truly effective satnav security must be a deliberate, system-level approach in any context.

We also mention that while this paper explicitly addresses satnav implementations for Chimera, it could be applied in similar systems, such as pseudolites and cellular ranging signal components.

References

[1] C. Gunther, "A Survey of Spoofing and Counter-Measures," *NAVIGATION: Journal of the Institute of Navigation,* vol. 61, no. 3, pp. 159-177, 2014.

[2] John A. Volpe National Transportation Center, "Vulnerability Assessment of the Transport Infrastructure Relying on the Global Positioning System," Office of the Assistant Secretary for Transportation Policy, US Department of Transportation, 2001.

[3] A. J. Kerns, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," *Journal of Field Robotics,* vol. 31, no. 4, pp. 617-636, 2014.

[4] D. A. Divis, "GPS Spoofing Experiment Knocks Ship Off Course," *Inside GNSS,* 31 July 2013.

[5] D. M. Akos, "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)," *NAVIGATION: Journal of The Institute of Navigation,* vol. 59, no. 4, pp. 281-290, 2012.

[6] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen and L. Gerard, "Pre-Despreading Authenticity Verification for GPS L1 C/A Signals," *NAVIGATION: Journal of The Institute of Navigation,* vol. 61, no. 1, pp. 1-11, 2014.

[7] V. Dehghanian, J. Nielsen and G. Lachapelle, "GNSS Spoofing Detection Based on Receiver C/No Estimates," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, 2012.

[8] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon and G. Lachapelle, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, 2012.

[9] J. Nielsen, A. Broumandan and G. Lachapelle, "GNSS Spoofing Detection for Single Antenna Handheld Receivers," *NAVIGATION: Journal of The Institute of Navigation,* vol. 58, no. 4, pp. 335-344, 2011.

[10] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio and L. Lo Presti, "Signal Quality Monitoring Applied to Spoofing Detection," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, Portland, OR, 2011.

[11] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard and T. E. Humphreys, "Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals," *NAVIGATION: Journal of The Institute of Navigation,* vol. 60, no. 4, pp. 267-278, 2013.

[12] J. Nielsen, V. Dehghanian and N. Dawar, "GNSS Spoofing Detection Based on Particle Filtering," in *Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, 2013.

[13] L. Scott, "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems," in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, Portland, OR, 2003.

[14] G. W. Hein, F. Kneissl, J.-A. Avila-Rodriguez and S. Wallner, "Authenticating GNSS: Proofs Against Spoofs, Part 1," *Inside GNSS,* pp. 58-63, July/August 2007.

[15] G. W. Hein, F. Kneissl, J.-A. Avila-Rodriguez and S. Wallner, "Authenticating GNSS: Proofs Against Spoofs, Part 2," *Inside GNSS,* pp. 71-78, September/October 2007.

[16] O. Pozzobon, "Keeping the Spoofs Out: Signal Authentication Services for Future GNSS," *Inside GNSS,* pp. 48-55, May/June 2011.

[17] C. Wullems, O. Pozzobon and K. Kubik, "Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems," in *Proceedings of the European Navigation Conference GNSS, 2005*, Munich, Germany, 2005.

[18] K. Wesson, M. Rothlisberger and T. Humphreys, "Practical Cryptographic Civil GPS Signal Authentication," *NAVIGATION: Journal of The Institute of Navigation,* vol. 59, no. 3, pp. 177-193, 2012.

[19] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE,* vol. 104, no. 6, pp. 1258-1270, 2016.

[20] L. Scott, "Proving Location Using GPS Location Signatures: Why it is Needed and A Way to Do It," in *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, 2013.

[21] P. Gutmann. [Online]. Available: https://www.cs.auckland.ac.nz/~pgut001/tutorial/. [Accessed 24 March 2017].

[22] H. X. Mel and D. Baker, Cryptography Decrypted, Addison-Wesley, 2001.

[23] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley and Sons, 2007.

[24] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[25] I. Fernandez-Hernandez, "GNSS Authentication: Design Parameters and Service Concepts," in *Proceedings of the European Navigation Conference 2014*, Rotterdam, Netherlands, 2014.

[26] Global Positioning Systems Directorate, *Navstar GPS Space Segment/User Segment L1C Interface, Revision D,* Vols. IS-GPS-800D, 2013.

[27] D. A. Shnidman, "The calculation of the probability of detection and the generalized Marcum Q-function," *IEEE Transactions on Information Theory,* vol. 35, no. 2, pp. 389-400, 1989.

[28] J. T. Curran, M. Navarro, M. Anghileri, P. Closas and S. Pfletschinger, "Coding Aspects of Secure GNSS Receivers," *Proceedings of the IEEE,* vol. 104, no. 6, pp. 1271-1287, 2016.

[29] J. T. Curran and C. O'Driscoll, "Message Authentication, Channel Coding & Anti-Spoofing," in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, Portland, OR, 2016.

[30] J. W. Betz, Engineering Satellite-Based Navigation and Timing, Hoboken, NJ: John Wiley and Sons, 2016.

[31] J. W. Betz, M. A. Blanco, C. R. Cahn, P. A. Dafesh, C. J. Hegarty, K. W. Hudnut, V. Kasemsri, R. Keegan, K. Kovach, L. S. Lenahan, H. H. Ma, J. J. Rushanan, D. Sklar, T. A. Stansell, C. C. Wang and S. K. Yi, "Description of the L1C Signal," in *Proceedings of the*

19th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2006), 2006.

[32] I. Fernandez-Hernandez, V. Rijmen, G. S. Granados, J. Simon, I. Rodriguez 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)*, Tampa, FL, 2014.

[33] US Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team, "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure," 6 January 2017. [Online]. Available: https://ics-cert.us-cert.gov/Improving-Operation-and-Development-Global-Positioning-System-GPS-Equipment-Used-Critical. [Accessed 28 March 2017].