© istockphoto.com/franckreporter

From Data Schemes to Supersonic Codes GNSS Authentication for Modernized Signals

The problem of GNSS signal authentication is expected to draw ever more attention in an operational environment that poses a growing risk – and consequences – for "spoofing" attacks. A team of researchers present an overview of the requirements and methods for verifying the authenticity of the signals and introduce a novel scheme for authentication of open GNSS signals using supersonic codes.

OSCAR POZZOBON, GIOVANNI GAMBA, MATTEO CANALE, SAMUELE FANTINATO
QASCOM S.R.L.

A decade has passed since the first GNSS system-level authentication protocols were proposed, and yet the current ongoing discussion is still, *"Do we really need GNSS signal authentication?"* Indeed, the current argument is whether we need authentication at the system level (the satellite broadcast service) or whether user-based authentication (anti-spoofing) is sufficient for a number of application requirements.

Risk analysis for every application should produce security requirements that would allow us to discriminate determine the actual need of either user-based or system-based techniques. For instance, if the likelihood of a spoofing attack on your favorite car navigator is quite low and the resulting effect would be negligible, car navigators probably will not require use of encrypted signals with security module for authentication. Some simple checks on the receiver time bias and carrier-to-noise power density (C/N_0) will do the job to fulfill these requirements.

On the other hand, unfortunately, we expect a growing number of threats and cyber-attacks in the future: the Internet has three billion users today, and the annual impact of attacks on the global economy has risen to $445 billion. With GNSS having more than two billion devices in operation today and seven billion predicted for 2020, a number of GNSS safety and financial critical applications will demand more and more security and trust.

This article will take up the problem of GNSS signal authentication, beginning with the definition and classification of requirements and presenting a categorization of applicable schemes. We will provide an extensive summary on state-of-the-art, data-level authentication schemes, based on well-established broadcast authentication protocols that can be exploited for providing efficient navigation data authentication. In particular, we introduce a novel scheme for open signal authentication using *supersonic codes.*

Foundations of Signal Authenticity

GNSS authentication is a complex multi-domain problem. A receiver estimates its own position and time by calculating ranges and time bias from satellites, with satellite positions and system time obtained from the same source. This leads to the conclusion that GNSS authentication is achieved by:

- the level of trust in the range estimation
- the level of trust in satellite position and system time information
- the level of trust in the component equipment that calculates position, time, and velocity from the foregoing factors.

Various branches of science and engineering help us address these three problems, particularly, signal estimation theory, information source authentication and non-repudiation, and physical and software security.

As physical and software security pertains to receiver design requirements, we will focus on range estimation and data authentication and trust for the system-level aspects. One complexity in GNSS signal authentication design is that the use of data-level authentication does not necessarily fulfill the trust requirement for range estimation, and trust in range estimation does not satisfy the trust requirement for the authenticity of satellite data.

Another crucial point to discuss in requirements analysis is the need for source authentication or *non-repudiation*, the ability to ensure that a party to a communication cannot deny its authenticity. For example, in cryptography source authentication can be achieved with a *message authentication code* (MAC). "Alice" sends information with an attached MAC to "Bob," and Bob can verify the source authentication. However, MAC does not achieve satisfy the need for non-repudiation, as an impartial third party cannot verify the origin of the message because both Alice and Bob own the secret key to generate the MAC.

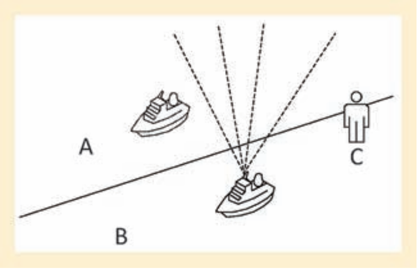


FIGURE 1 Hypothetical GNSS application scenario where non-repudiation may be required: a ship sailing in country B's territorial waters wants to prove, via an impartial third party C, that its position claim is authentic.

In GNSS non-repudiation could be a requirement worth considering. For example, as illustrated in **Figure 1**, a ship might be navigating in water from Country B, and Country A might challenge its position as being within Country A's territorial boundary. The ship's crew might reply that the ship position only appears to be in Country A because of a spoofed signal, but it actually did not cross the borderline. Country C would be the impartial third party that has the capability to verify if Country B used authentic signals.

We can summarize the requirements for GNSS authentication in terms of the following factors:

- navigation data integrity, source authentication, non-repudiation and/or position/velocity/time (PVT) authentication
- performance, such as time to authentication (TTA) and accuracy of authentic position
- probability of failure
- robustness
- interoperability.

Time to authentication refers to the time required by the system to detect an anomaly and respond to it. In signal authentication, TTA is an important requirement, as the receiver time and dynamics will be compromised from the beginning of a spoofing attack until its detection. Therefore, these effects need to be minimized quickly and appropriately, based on application requirements.

Probability of failure refers to the trust that one can give to the authentication scheme. This includes the probabilities of missed detection and false alarm, and is fundamental for the determination of the integrity risk in safety-critical applications. For example, if we want to use an authenticated signal in a safety-of-life (SoL) application with an integrity risk requirement of 3.5 x 10^{-7} over 150 seconds, these requirement constraints are expected to represent the lower bound for the probability of failure of the authentication protocol.

Robustness refers to the capability to mitigate a number of known attacks. For example, some application may require protection from replay attacks, while others may not.

Finally, *interoperability* refers to the capability of the authentication scheme to be used by a number of different applications in various environmental contexts, and to be transparent to legacy equipment. For example, providing support to L1 frequency without compromising other navigation service performance represents an important interoperability requirement.

Authentication Domains

To date, GNSS authentication protocols have been proposed in three domains: data level, signal level, and hybrid level (data + signal).

Data-level authentication schemes refer to the implementation of cryptographic protocols in the navigation data. In simple words, such approaches can be seen as "digitally signing" the navigation data in order to authenticate the source of the data generator and ensure the integrity of the received message.

In a 2005 paper by C. Wullems *et alia* (listed in the Additional Resources section near the end of this article), we introduced the concept of data-only authentication, calling the technique "navigation message authentication" (NMA). NMA has the advantage of having a low system impact, as it requires only upgrades of the GNSS satellites' navigation data generation subsystem along with a low-cost implementation on the receiver side. NMA can be implemented through various schemes that we will discuss later in this article.

Disadvantages of NMA include TTA performance, which is limited to the specific implementation (e.g., digital signatures, block hashing, hash chaining, etc.), as well as the required bandwidth to implement NMA. The probability of failure for an NMA scheme depends on the number of bits included in the authentication function and on the size of the authentication payload. For instance, if 30 seconds of data are authenticated, a single bit error not detected by the channel-coding scheme would result in a false alarm. On the other hand, a missed detection in nominal conditions (not under attack) is unlikely with a well-designed NMA scheme.

Unfortunately, NMA is exposed to replay attacks if the spreading codes are public and available to everyone for the estimation and replay of the symbols. This forces the receiver to integrate a trusted clock in order to increase robustness.

Signal-level schemes tackle the vulnerability to replay attacks by exploiting the properties of spread spectrum signals, which in GNSS are below the thermal noise. For an attacker, with standard equipment and without knowledge of the secret code, it is therefore very difficult to demodulate the signal. Only the knowledge of the secret code, in fact, allows the signal despreading to perform ranging and data demodulation.

This article will discuss the state of the art in data-level authentication, and a new approach for signal-based authentication capable of carrying high data rate needed to achieve an efficient hybrid authentication scheme (data+signal authentication).

GNSS Data-Level Authentication

In the field of broadcast authentication, GNSS data authentication seeks to provide a set of security properties, including data integrity, data authentication, and possibly non-repudiation. In particular, GNSS data authentication aims at providing *source authentication,* that is, at ensuring that a legitimate GNSS satellite actually generated the navigation data received by generic user equipment.

The simplest broadcast data authentication schemes are based on standard applications of authentication solutions, such as message authentication codes (MACs) and digital signatures (DSs), including variations such as hash-based MACs and cipher-based MACs. In general, MACs provide data integrity and data authentication together with bandwidth and computational efficiency but cannot ensure non-repudiation. Moreover, they require secure use and storage of symmetric keys (e.g., via smartcards) in order to prevent a malicious user from compromising the security of the entire authentication service by disclosing the secret keys.

Digital signatures, on the other hand, address all the required security properties (integrity, authentication, and non-repudiation). Unfortunately, they result in high computational and per-packet communication overheads.

More elaborate broadcast data authentication schemes leverage the aforementioned standard authentication solutions and trade-off the following features: computation and communication overhead, buffer space requirements, authentication delay, verification probability, and loss tolerance as opposed to reliable delivery. In the following, three main families of broadcast authentication schemes are considered: block hashing, hash chaining, and MAC-based source authentication schemes. **Figure 2** depicts the taxonomy of the broadcast authentication schemes considered.

Block hashing schemes follow the paradigm of spreading the cost of the signature operation among a number of blocks by using the properties of hash functions. The main idea is that, for each set of blocks, a single signature is transmitted together with the hashes of each block. This allows the receiver to verify the authenticity of all blocks, by checking the consistency of each hash with the digital signature.

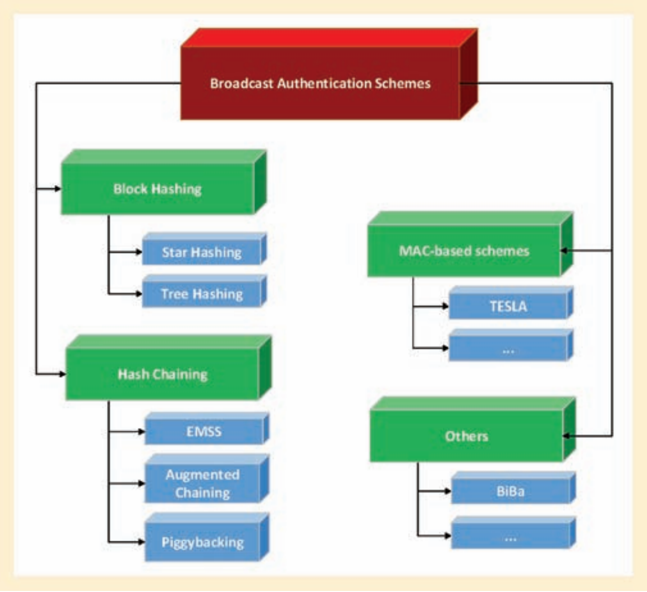


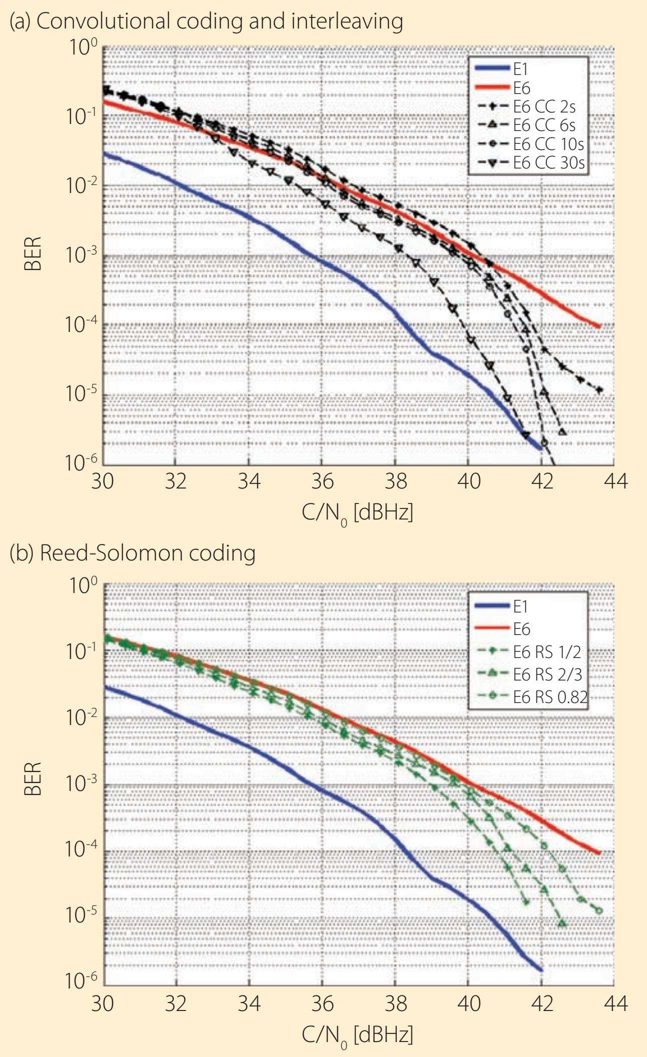
FIGURE 2 Taxonomy of broadcast data authentication schemes.

Block hashing can use either a star or a tree-based approach, depending on the hierarchy of the authenticated blocks. This type of hashing leverages the reduced size of hashes as compared with digital signatures in order to minimize both the bandwidth and the computational requirements. In the context of GNSS authentication, blocks could be identified either with corresponding portions of data (e.g., the same pages) sent by different satellites, or with different navigation message chunks in each satellite (e.g., different pages in a sub-frame).

Hash chaining is a further technique for authenticating streaming data, based on a hash chain commitment via digital signature. The hash chaining can be either "forward" (signature follows data packets, thus resulting in a delayed authentication) or "backward" (signature is transmitted first, thus allowing immediate authentication).

Hash chaining schemes require the sender to know the entire data stream in advance (and is therefore applicable to GNSS ground segment design). In its standard application, however, hash chaining does not tolerate packet loss. Because of this, its application in GNSS authentication is limited, as the bit error rate rapidly degrades with lower satellite visibility at the receiver.

Variations of standard hash chaining have been proposed to address this issue, based on multiple hash chains and resulting in a higher per-packet communication and computational overhead. *Efficient multi-chained stream signature* (EMSS) is an example of such an authentication protocol, supporting loss-resilient and probabilistic authentication verification. EMSS is based on hash chains of degree k, meaning that each packet's hash is sent in k different packets, with random chaining sequences leading to a higher probability of verification. *Augmented chaining* is another strategy that, based on the transmission of redundant hashes, provides resiliency



(a) Convolutional coding and interleaving

(b) Reed-Solomon coding

FIGURE 3 Comparison of the bit error rate as a function of carrier-to-noise density ratio (C/N$_0$) between the Galileo Open Service (E1) and the Commercial Service (E6).

against errors burst. Finally, the *piggybacking* scheme deals with the case where data carried by different packet has more or less importance from the point of view of the application level.

Various levels of priorities could be assigned to data packets, so that the higher the priority of a packet, the more redundant will be the hash chaining of packets belonging to that class. This approach allows tailoring the robustness of packets against bursty losses as a function of their priority. In the context of GNSS such a technique could be used for maximizing the robustness of the authentication scheme for some selected data (e.g., time of week (TOW), ephemerides, and so on) as compared with less critical types (e.g., the almanacs).

MAC-based source authentication schemes are hybrid solutions that jointly use MACs and digital signatures in order to provide broadcast authentication. More precisely, these schemes are based on four main ingredients: one-way hash chains, (loose) time synchronization, MACs, and digital signatures for the source verification of hash chain commitments.

A remarkable example of MAC-based source authentication is the timed efficient stream loss-tolerant authentication (TESLA) protocol and its extensions, including instant authentication, management of concurrent instances, and increased robustness to denial-of-service attacks. It is worth mentioning that the authors of TESLA also presented another protocol, BiBa (bins and balls signature), that falls in none of the previous three families of authentication schemes. BiBa is based on one-way hash functions without a trapdoor: to sign a message, the signer uses the message to seed a random process, which throws a set of balls into bins. The balls represent SElf-Authenticating Values or SEALs, random numbers generated in a way that the receivers can instantly authenticate them with the public key. The bins correspond to the range of the hash function. When enough balls fall into the same bin, the combination of those balls constitutes a signature.

As a conclusion to this overview, we should note that the robustness of any data-level authentication protocol to transmission errors could also be increased — that is, the probability of authentication failure could be decreased — by using forward error correction (FEC) schemes.

In this context, as described in the paper by M. Canale *et alia* (Additional Resources), we have tested two different solutions for enhancing the data-level authentication with FEC on the Galileo Commercial Service. The first solution employs a common and effective code concatenation: the inner convolutional code (already available in Galileo) is coupled with an outer Reed-Solomon (RS) block code. These two codes respectively combine good performance in the presence of random and bursty errors. The second solution is based on the nested use of convolutional encoding and interleaving, achieving a double time diversity of the data broadcasting, while keeping the same end-to-end delay of a block interleaver.

Figure 3 shows the performance of the proposed schemes with various parameters in terms of bit error rate (BER) and carrier-to-noise density ratio (C/N$_0$) when a second layer of FEC is applied. The top panel (a) shows convolutional code and interleaving (CC) for various lengths of the input data stream, e.g., two seconds for a single E1 page. The bottom panel (b) illustrates the performance of Reed-Solomon codes with rates 1/2, 2/3, and 0.82 Note that the length of the input data stream has little effect on the E6 BER.

Even though these schemes are proposed in order to compensate the gap between the Galileo Open Service and the Galileo Commercial Service in terms of bit error rate, their use could be extended to an arbitrary data-level authentication scenario. (Due to the E6 SIS design, however, the BER on the CS navigation messages is considerably higher than the one measured on the E1 Open Service for the same signal-to-noise ratio.)

GNSS Signal-Level Authentication

A known technique to provide signal authentication as well as access control is the full encryption of the spreading code. This approach, however, lacks the interoperability property and requires time knowledge (time fix) for the acquisition of the signal.

The first signal-level authentication proposal that allowed interoperability was presented in a 2003 paper by L. Scott (Additional Resources) with a scheme called *spread spectrum security codes* (SSSCs), which also proposed a data-supporting infrastructure. A similar approach was proposed in 2004 by M. G. Kuhn. Later, in the paper by O. Pozzobon *et alia* (2010) we proposed a concept based on the dissemination of encrypted chips with a scheme called *signal authentication sequences* (SAS). A drawback of all these signal-based authentication schemes is a weakness in TTA. They also require an aiding channel or a dedicated bandwidth as chips are transmitted in the navigation data.

One interesting approach that Qascom has investigated is the transmission of secret codes multiplexed with open codes, to achieve what is also known as "signal watermarking." This led us to the concept of supersonic GNSS authentication codes[18], a solution that provides hybrid authentication achieving both data-only, signal-only, or combined data- and signal-level authentication. The scenic term "supersonic" derives from the fact that authentication could be achieved faster than the symbol speed.

We designed the protocol in order to fulfil the previously mentioned requirements for signal authentication. Particularly, we considered these main drivers:

- Low probability of failure in nominal conditions. The protocol can define the code length in order to satisfy the desired probability of failure requirements.
- Legacy hardware support via combination with an open signal (multiplexing). The main idea is to transmit the supersonic codes multiplexed with open codes (such as GPS C/A or Galileo OS) to allow interoperability with open services and support mass-market applications.
- Based on symmetric cryptographic schemes. This is required for signal-level authentication.
- Based on block ciphers. The supersonic codes are block ciphered and in code phase with open codes, and the same code is repeated for a predefined security period. This allows direct authentication without time dependency, as opposed to stream-cipher-based solutions.
- High data rate capability to support the transmission of data authentication schemes such as block hashing digital signatures or hash chains as discussed before.

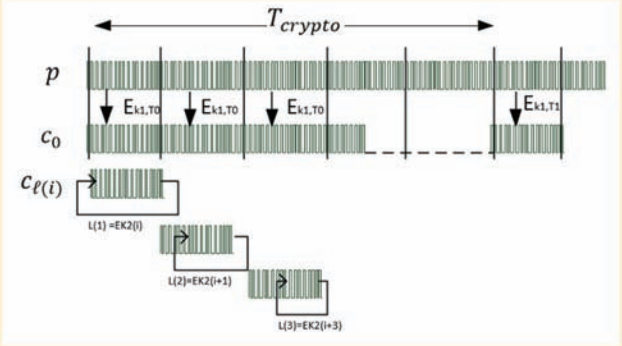


FIGURE 4 High-level concept of supersonic codes generation.

- Comprises two stages, for achieving different security levels based on robustness requirements and/or receiver constraints.

High-Level Protocol Description

As an introduction to the proposed authentication scheme, the following section provides a high-level description of supersonic code generation.

The proposed protocol assumes that the supersonic codes are multiplexed with an open code, and that they are synchronized to it. This scheme is based on the block-cipher encryption of the open code, resulting in an encrypted code valid for a predetermined crypto-period T_{crypto} (**Figure 4**). When a crypto-period expires, a new initialization vector (IV) is provided as input to the block cipher and a new encrypted spreading code is generated. In the following discussion, we refer to the encrypted code as "fundamental code."

This strategy allows a receiver that knows the IVs (for example, through previous transmission via navigation data) to select the IV to be used with a loose system time synchronization of the receiver and without a time fix. For example, a receiver clock with poor performance (e.g., 10^{-5} seconds in a one-second drift) could guess a five-minute window after one year. So, a receiver lacking a time fix can still acquire the supersonic code based on a rough estimate of time.

The fundamental code is then modulated with a code-shift-keying (CSK) modulation, where the CSK shifts are generated by time-dependent unpredictable symbols. This ensures that the scheme is not vulnerable to an attack based on coherent integration and forces an adversary to continuously read the CSK shifting in order to perform a signal-based replay attack, by making the attack very complex and unlikely.

As a further benefit, GNSS signal design is looking to CSK as a new opportunity to increase the bit rate of GNSS signal data components and extend the possibility of adding new services. Indeed, with the introduction of new dataless (pilot) signal components that enables receivers to achieve precise synchronization on the pilot channel alone removes the need to adopt BPSK modulation for the data.

Supersonic Codes: An Analytical Description

We will now describe the process of generation of the supersonic codes with an analytical approach. First, we will detail the signal generation process, then describe the estimation at the receiver, and follow up with an explanation of the procedure for verifying signal authentication.

Signal Generation. Let p and c_0 be the open and a fundamental code, respectively, and L_p and L_c the corresponding number of chips. In addition, let T_p and T_c be their respective chip period, so that the fundamental code duration T_s is defined as $T_s = T_c \bullet L_c$, corresponding to a symbol-rate of $R_s = 1/T_s$.

In order to allow synchronization, the number of chips of the fundamental code c_0 shall be chosen such that:

$$L_P = N \cdot L_c, \tag{1}$$

where N is integer and $T_p = T_c$. Note that this also ensures that the signal carrying the secure code has the same chipping rate as the open code.

The first step of the supersonic authentication scheme consists of the generation of a fundamental crypto-code c_0 that is used as a baseline for a subsequent CSK modulation. This secret code c_0 is valid for a crypto-period $T_{crypto} >> T_s$, and is then renewed; the time slots associated with each crypto-period are denoted by *j*, so that the fundamental code for the *j*-th slot is denoted by $c_0(j)$.

More precisely, the fundamental code is generated for each crypto-period as follows:

$$c_0(j) = E_{k_1}\big(p, IV_1(j)\big), \qquad (2)$$

with E_{k_1} being a block cipher (e.g., AES-CBC) indexed with a secret key k_1, and $IV_1(j)$ representing the initialization vector. Note that (2) takes into account neither the truncation nor the padding that may be required for meeting the synchronization condition (1). Such parameters depend both on the specific block cipher used for the encryption and on L_p. For the sake of readability, in the following discussion, the dependency of the fundamental code on *j* is omitted in the notation.

From a security perspective, the fundamental code described in (2) ensures that c_0 is not known to an adversary who does not have access to the secret key k_1. In principle, this should ensure that the attacker is not able to despread the signal. However, as mentioned earlier, the scheme is vulnerable to a coherent integration attack, and this vulnerability is the main driver for the design of the second step.

The second step of the supersonic authentication scheme, in fact, addresses this security issue by leveraging the CSK modulation, that is, by circularly shifting the fundamental code c_0 for every time slot of duration T_s (in the following, each of these time slots is indexed with *i*).

The CSK shift is chosen by means of a cryptographic data authentication function in the symbols modulation. This ensures its unpredictability for the adversary and prevents coherent integration. The alphabet of possible CSK shifts is denoted by δ and is a sampled sub-set of $\{0,1 \ldots, L_c - 1\}$ with cardinality *M*; each shift can therefore be uniquely identified by $B = \log_2(M)$ bits.

For each time slot *i* of duration T_s, the CSK shift $\ell(i)$ is generated by taking as input symbols of the data to be transmitted via the CSK shifts (e.g., the navigation data authentication payload) and the time reference *i* (e.g., the TOW). These data are then encrypted and authenticated with a standard authenticated encryption scheme (e.g., AES-GCM). Special attention must be paid to the design of the overall authentication scheme — and in particular to the cryptographic shift generator — in order to prevent side-channel attacks on the scheme. Both unpredictability and authenticated integrity are in fact mandatory for the security of the proposed scheme.

A particular note: CSK shifts should be generated with a bit rate at least equal to $B \bullet R_s$ bps in order to follow the signal generation dynamics. Therefore, the *B*-bit shift (in chips) generation can be summarized in the following equation:

$$\ell(i) = AE_{k_2}\big(i, IV_2(i), d(i)\big), \qquad (3)$$

where AE_{k_2} is an authenticated encryption scheme indexed with a secret key k_2, $IV_2(i)$ is a initialization vector, and *d(i)* is the input data bit to be modulated over the *i*-th CSK symbol.

Given this offset, the shifted code $c_{\ell(i)}$ is obtained by circularly shifting c_0 by $\ell(i)$ chips. Then, the CSK-modulated waveform corresponding to $c_{\ell(i)}$ can be written as

$$s_{\ell(i)}(t) = \sum_{\hbar=1}^{L_c} c_{\ell(i)}[\hbar] \cdot \mathrm{rect}_{T_c}(t - \hbar T_c) \qquad (4)$$

where $c_{\ell(i)}[\hbar]$ {−1,1} is the value of *k*-th chip of $c_{\ell(i)}$, and rect_{T_c} is the standard rectangular function.

Then, the overall signal that is generated can be written as

$$s(t) = \sum_{i=-\infty}^{+\infty} s_{\ell(i)}(t - i \cdot T_s). \qquad (5)$$

Shift Estimation at the Receiver. Assuming an ideal propagation channel, the received signal, after rescaling and given a perfect code and carrier wipe-off, can be written as

$$r(t) = s(t) + n(t), \qquad (6)$$

where *n(t)* is AWGN with unitary variance and zero mean.

The impact of noise on the performance of the authentication scheme has effects to the probability of failure (mainly false alarms). Let $r^*(k)$ be the sampled version of *r(t)*, that is,

$$r^*(k) = r(kT_{ADC}), \qquad (7)$$

where T_{ADC} is the sampling period of the analog-to-digital converter. By considering the *i*-th time slot (in which the time reference can be derived from the code offset of the open code), equation (7) becomes

$$r_i^*(k) = s_{\ell(i)}(k) + \eta_i(k), \qquad (8)$$

where $kT_{ADC} \in \{iT_s,(i + 1)T_s\}$, and $s_{\ell(i)}(k)$ and $\eta_i(k)$ are the sampled version of equation (4) and the sampled contribution of noise on the *k*-th sample, respectively.

The signal $r_i^*(k)$ is then correlated with the sampled local replica $c_0(k)$ of the fundamental code, thus getting

$$w_i(k) = IFFT\big[FFT\big(c_0(k)\big) \cdot FFT\big(r_i^*(k) + \nu_i(k)\big)\big], \qquad (9)$$

where $\nu_i(k)$ is the correlated noise.

Finally, the estimated CSK shift at the receiver for the *i*-th time slot can be derived as

$$\hat{\ell}(i) = \arg\max_{\ell\in\delta}\big(w_i(k)\big). \qquad (10)$$

Figure 5 illustrates this process schematically.

Authentication Verification. Based on the signal-generation procedure, which is structured in two fundamental steps (generation of the fundamental code c_0 and of the unpredictable, time-dependent shifts $\ell(i)$), authentication verification foresees two subsequent stages, as depicted in **Figure 6**.

The first stage verifies the presence of the CSK-modulated code, whereas the second checks the consistency of the authen-

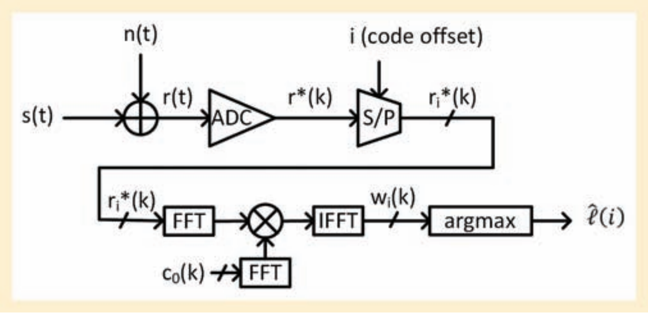


FIGURE 5 Signal chain describing the estimation of the CSK shift at the receiver.

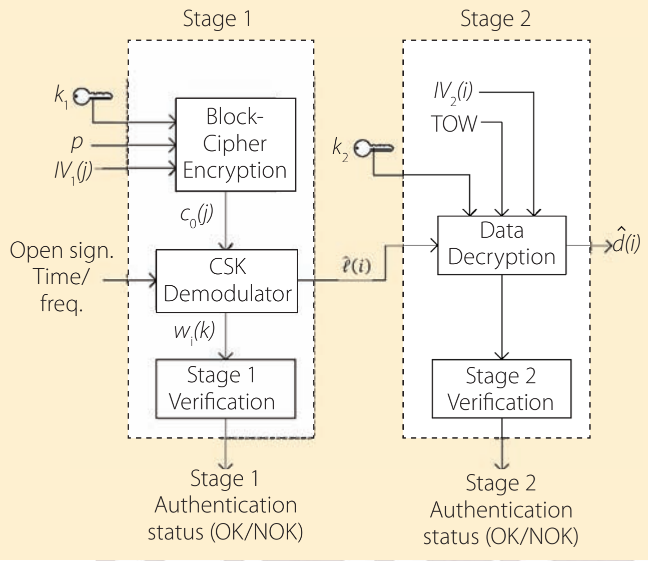


FIGURE 6 Authentication verification stages for the supersonic authentication scheme

ticated data and its alignment against time. Both stages require the receiver to know the secret keys k_1 and k_2, for the generation of the local replica of the fundamental code and the CSK-shifts consistency check, respectively. Further, stage 2 requires time-synchronization in order to uniquely identify the codes time slots (as shown in Figure 6).

More formally, we can write the two steps with which to verify signal authentication as follows:

- **Stage 1**

The stage 1 the signal detection is successful if the correlation on the supersonic signal, phase, and frequency aligned with the open signal exceeds a predefined threshold w_{th}, that is:

$$\max|\mathrm{w_i(k)}| \geq \mathrm{w_{th}}$$

In particular, assuming a classical non-coherent binary decision testing, the threshold w_{th} shall be chosen as a function of the required probability of false alarm. The output of the Stage 1 authentication verification can therefore be written as

$$V_1 = \begin{cases} 1, & \text{if } \max|\mathrm{w_i(k)}| \geq \mathrm{w_{th}} \\ 0, & \text{if } \max|\mathrm{w_i(k)}| < \mathrm{w_{th}} \end{cases}$$

where “1” indicates an authentic signal, and “0” a non-authentic one.

- **Stage 2**

The stage 2 authentication verification is considered valid if the estimated symbols from the CSK shift $\hat{\ell}(i)$ at the output of the CSK demodulator are successfully authenticated and decrypted (thus returning the originally transmitted data payload), and if the decoded time reference is consistent with the expected TOW derived from the open signal.

Cryptographic key renewal. As a final comment to this section, we should stress that the cryptographic keys k_1 and k_2 used for the two-stage authentication verification shall be renewed with a frequency which depends on the chosen cryptographic schemes and on the respective parameters. In general, k_1 shall be valid for a period T_{k_1} and k_2 for a period T_{k_2}, with $T_{k_1} \neq T_{k_2}$.

Preliminary Parameters Design and Performance Analysis

We performed a preliminary performance tradeoff analysis in order to derive a realistic signal design. To tackle this problem, the system designer should consider users’ GNSS authentication requirements. However, as anticipated, this aspect of GNSS operations lacks sufficient investigation.

Because intentional interference such as spoofing or meaconing could be disastrous in safety-critical applications, some believe that an integrity-equivalent time to alarm and prompt alerts of authentication/cryptographic integrity failure might be required for upcoming GNSS authentication services. Here, we will propose a simplified approach.

Our analysis considers three main drivers for selecting signal parameters: the feasibility of maintaining a low, target authentication failure rate (in the absence of attacks); the capability of achieving very fast authentication through Stage 1 as described in the previous section, and the potential integration of the scheme into an existing GNSS signal (e.g., Galileo E1) via multiplexing.

On the basis of these conditions, we can express the problem as one of bi-dimensional optimization. This consists of selecting the minimum values of T_s and C/N_0 that allow the fulfillment of the target probability of missed detection P_{md} regarding the authenticity (or inauthenticity) of the CSK demodulator output. Note that a short code duration T_s allows fast Stage 1 authentication and low C/N_0 raises the possibility of multiplexing an additional signal component in Galileo E1, minimizing the losses to the other signal components and the effect on open signal processing in legacy receivers.

In our analysis, the probability of false alarm is kept constant to the value of 2 * 10^{-7} over 10 seconds. Assuming a CSK non-coherent demodulation process, the estimated symbols are modeled with a central chi-square probability density function with two degrees of freedom (in-phase and quadrature components). **Figure 7** shows the results of the dimensional optimization. For example, considering the Galileo E1B signal, the practical code lengths (T_s) for fulfilling equation (1) are four milliseconds and eight milliseconds.

In addition to the signal parameters, we have analyzed the achievable CSK symbol rate and its error rate as functions of C/N_0. As previously described, $\hat{\ell}(i)$ is generated via a crypto-

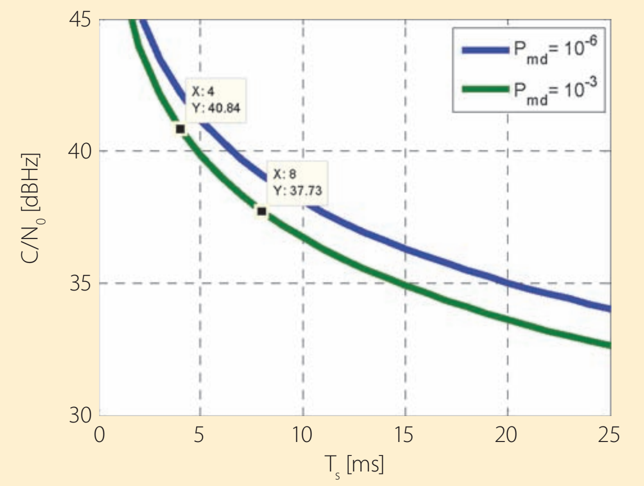


FIGURE 7 Optimal (T_s, C/N$_0$) curve

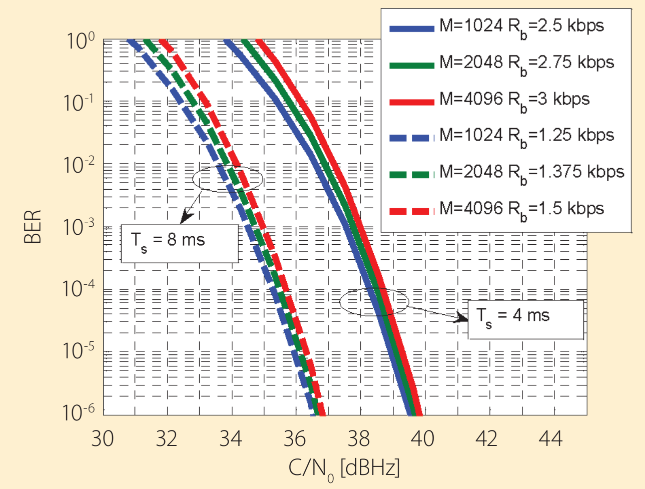


FIGURE 8 CSK symbol rate and symbol error rate with for code duration T_s = 4 ms and T_s = 8 ms

graphic function that depends on a data stream *d(i)* representing a data service to be broadcasted through the supersonic code signal component.

In **Figure 8** the CSK symbol rate for T$_s$ = 4 milliseconds and T$_s$ = 8 milliseconds is shown as a function of *C/N$_0$*. Note that, with the proposed signal configuration, CSK modulation can achieve a symbol rate between 1.5 kbps and 3 kbps, which is higher than any other GNSS signal data rate.

The symbol error rate is approximated, using a union bound, with the following equation [20, 21]as discussed in the papers by H. Sun *et alia* and A. Garcia-Peña *et alia* (Additional Resources):

The following discussion presents a hypothetical scenario on how to multiplex the supersonic code signal with the other signals already transmitted by Galileo in the E1 band.

Galileo E1 employs an *interplex* scheme to multiplex the E1-A, E1-B, and E1-C components within a composite constant-envelope signal. The task of adding a fourth component is not trivial in terms of efficiency, especially considering the particular nature of the composite binary offset carrier (CBOC) signal. However, under the assumption that the supersonic code signal can be transmitted with a sharing loss three decibels lower than the open service, at least two multiplexing schemes could be adopted: the interplex itself, which would allow the integration of the additional component minimizing the multiplexing losses, and the *intervoting* method. The latter approach is considered the most interesting as it outperforms the others in terms of backward compatibility.

Robustness Against Known Attacks

To conclude our theoretical and signal analysis, we performed a preliminary assessment of the robustness of the supersonic authentication scheme in the presence of three types of known GNSS attacks: meaconing of the open and supersonic signal, spoofing of the open signal only, and replay of open and supersonic signal with CSK chips estimation.

In the meaconing case, the supersonic authentication scheme has the same limitations as the other authentication approaches, both at the data and signal levels: the attack cannot be mitigated unless the receiver embeds a trusted clock with high accuracy.

In the second case, however, when the receiver is tracking a spoofed open signal, the channels with the embedded supersonic codes can detect the attack at Stage 1 and block signals from entering into the correlator. One limitation of the Stage 1 authentication verification is that sophisticated spoofers (aligned in power and frequency) can be detected only if at least two peaks appear in the autocorrelation function (ACF). These peaks are detectable if the error τ imposed due to the spoofer is misaligned by a substantial number of chips.

The detector searches for peaks in the absolute value of the ACF, i.e., applying a non-coherent detection. The first peak can be associated with the presence of a signal, while the presence of a secondary peak is an index indication of possible misalignment caused by a spoofing attack. The code cross-correlation terms have also been considered as they have a significant influence, especially for high *C/N$_0$*.

A closed form analytical derivation of the detection threshold is not trivial; so, we derived it by simulation, imposing a low probability of false alarm, $P_{fa} = 10^{-8}$. After deriving the detection threshold, the probability of detecting a secondary peak is estimated. **Figure 9** reports the results of a simulation obtained using a T$_s$ of four milliseconds for various *C/N$_0$* levels. Clearly, only *C/N$_0$* levels above 45 dBHz allow the detection of a secondary peak, when the displacement caused by the spoofer is roughly of 2,000 chips. Using higher *C/N$_0$* allows the detection scheme to shorten this delay, but Stage 1 alone has limitations for synchronized attacks if low P_{fa} is required.

However, as previously discussed, the detection protocol also includes a second stage that improves the robustness of authentication and enables verification of the authenticity of the open signal. Given the chip period T_c, in fact, the spoofing is detected as soon as it induces

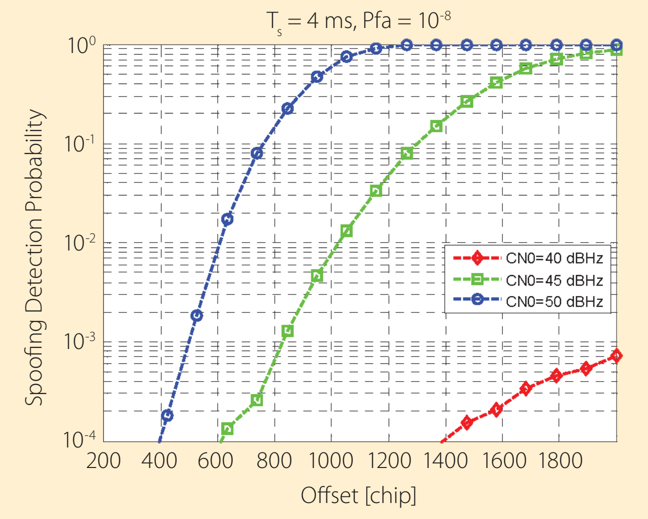


FIGURE 9 Probability of Stage 1 spoofing detection on various spoofer code-phase and with low probability of false alarm P_{fa}.

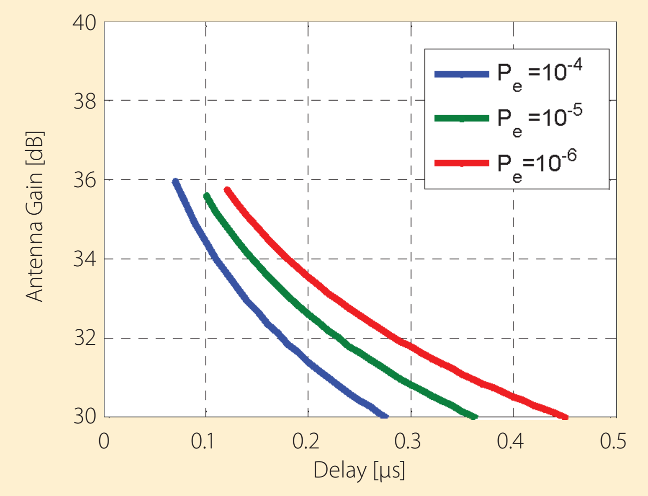


FIGURE 10 Antenna gain and delay introduced in a replay attack for a fixed chip error rate

a wrong code phase offset (i.e., pseudorange offset) higher than $T_c M/2L_c$. This condition produces an incorrect estimation of the CSK shift, triggering the detector of the Stage 2.

The third type of attack that we analyzed is the *replay attack* of both the open and the supersonic signals. In this case, the attacker attempts to estimate the unknown code and to replay it with the smallest delay. This process introduces errors in the chip estimation and a time drift that can be detected by the receiver as explained in the article by T. Humphreys listed in Additional Resources.

Figure 10 shows, for different target chip estimation error rate (10^{-6}, 10^{-5} and 10^{-4}), the antenna gain that the attacker needs and the delay that it introduces in replaying the signal. For example, an attack performed with a three-meter dish antenna that can achieve 30 decibels of gain would introduce at least 0.3μs of delay, which could be detected by a receiver with a high-quality clock.

Conclusions

This article has reviewed the problem of GNSS signal authentication, beginning with the definition and classification of requirements and leading to the categorization of applicable schemes. It provided an extensive summary on state-of-the-art, data-level authentication schemes, based on well-established broadcast authentication protocols that can be exploited for providing efficient navigation data authentication.

In particular, we presented a novel scheme for open signal authentication using supersonic codes. This scheme achieves a very fast time-to-authentication and provides additional bandwidth for GNSS services (such as navigation data authentication) at a high data rate. Being at an early stage of design, and given their innovative approach, supersonic codes present interesting opportunities for future development for this purpose. Enhancements to Stage 1 authentication, which is still limited in fine code-phase tuning attacks, should be investigated.

A more detailed cryptographic design (key distribution and renewal) and a thorough security analysis (including side-channel attacks) in the data channel would consolidate the solution presented here in order to allow its implementation in real-world applications. Finally, further performance assessments with various channel propagation models, as well as the analysis of the impact of noise and interference on the failure probability, could further strengthen (and possibly demonstrate) their applicability to multiple realistic scenarios.

Acknowledgments

The authors wish to thank Dr. José Angel Ávila Rodriguez, Dr. Massimo Crisci, and Dr. Rigas T. Ioannides from the European Space Agency for the fruitful discussions on signal design, Ignacio Fernández Hernández from the European Commission for the important considerations on data schemes, and Prof. Vincent Rijmen from KU Leuven University for his insightful support on cryptographic features.

Additional Resources

[1] Bellare, M., and R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," *Advances in Cryptology, CRYPTO '96* (Vol. 1109), Springer-Verlag, 1996

[2] Canale, M., and S. Fantinato, and O. Pozzobon, Qascom S.r.l, "Performance Comparison of Different Data Authentication Solutions for the Galileo CS", in *NAVITEC 2014 Conference Proceedings*, Noordwijk, Netherlands

[3] Dworkin, M. J., *Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, Special Publication 800-38B*, National Institute of Standards and Technology, 2005

[4] Fernández-Hernández, I., "GNSS Authentication: Design Parameters and Service Concepts," *Proceedings of European Navigation Conference GNSS 2014*

[5] Garcia-Peña, A., "Analysis of Different CSK Configurations in a Urban Environment When Using Non-coherent Demodulation," *Proceedings of Navitec 2014*

[6] Garcia-Pena, A., and D. Salos, O. Julien, L. Ries, and T. Grelier, "Analysis of the Use of CSK for Future GNSS Signals, 26th International Technical Meeting of the Institute of Navigation Satellite Division, (ION GNSS+ 2013), Nashville, Tennessee USA

[7] Gennaro, R., and P. Rohatgi (1997), "How to Sign Digital Streams," *Advances in Cryptology, CRYPTO'97,* 1997

[8] Gennaro, R., and P. Rohatgi (2001), "How to Sign Digital Streams," *Information and Computation,* 165(1):100–116, February 2001

[9] Golle, P., and N. Modadugu, "Authenticating Streamed Data in the Presence of Random Packet Loss," NDSS'01: The Network and Distributed System Security Symposium, 2001

[10] Humphreys, T., "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronics Systems,* vol. 49, no. 2, pp. 1073–1090, April 2013

[11] Kuhn, M. G., "An Asymmetric Security Mechanism for Navigation Signals", in 6th Information Hiding Workshop. LNCS 3200, Springer-Verlag, pp. 239-252, 2004

[12] Merkle, R. C. "Advances in Cryptology – CRYPTO '87," *Lecture Notes in Computer Science 293,* p. 369, 1988

[13] Miner, S., and J. Staddon, "Graph-Based Authentication of Digital Streams," *IEEE Symposium on Security and Privacy, 2001*

[14] Paonni, M., and M. Bavaro, M. Anghileri, and B. Eissfeller, "On the Design of a GNSS Acquisition Aiding Signal, *Proceedings of ION GNSS+ 2013,*" Nashville, Tennessee USA

[15] Park, J-M., and E. KP. Chong, and H. Siegel, "Efficient Multicast Packet Authentication Using Signature Amortization," *Proceedings of the 2002 IEEE Symposium on Security and Privacy*

[16] Perrig, A., and R. Canetti, J. D. Tygar, and D. Song "The TESLA broadcast authentication protocol," *CryptoBytes*" Volume 5, No. 2 (Summer/Fall 2002), RSA Laboratories, EMC Corporation, Hopkinton Massachusetts USA

[17] Perrig, A., and R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast." Network and Distributed System Security Symposium, NDSS. Vol. 1. 2001.

[18] Perrig, A., "The BiBa One-Time Signature and Broadcast Authentication Protocol," *Proceedings of the 8th ACM conference on Computer and Communications Security*, 2001

[19] Pozzobon, O. (2010), and L. Canzian, M. Danieletto, and A. D. Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, Netherlands, 2010

[20] Pozzobon, O. (2014), and G. Gamba, M. Canale, and S. Fantinato, Qascom S.r.l., "Supersonic GNSS Authentication Codes, *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014),* Tampa, Florida USA

[21] Scott, L., "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems," *Proceeding of ION GPS/GNSS 2003,* Institute of Navigation, Portland, Oregon, 2003, pp. 1542–1552

[22] Sun, and G. Bi, Y. Guan, and Y. Shi, "Performance analysis of M-ary CSK Based Transform Domain Communication System," *Proceedings of the 2nd International Conference on Circuits, Systems, Control, Signals (CSCS 2011)*

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

Authors

Oscar Pozzobon is the founder and technical director of Qascom. He received a degree in information technology engineering from the University of Padova, Italy, and a master degree from the University of Queensland, Australia, in telecommunication engineering. He has coordinated various projects addressing interference and signal authentication with the European Space Agency (ESA), the European GNSS Agency (GSA), and the European Commission. Currently, Pozzobon is involved in the design of the ESA advanced multi-constellation simulator and in the design of the Galileo Commercial Service (CS) demonstrator authentication schemes. He has worked for Thales Alenia Space on Galileo in-orbit validation and full operational capability (FOC) validation and verification. He has been involved in the area of GNSS authentication since 2001 and has been one of pioneers of the concepts of trusted GNSS receivers, mavigation message authentication (NMA), signal authentication sequences (SAS), remote processing authentication (RPA) and supersonic GNSS authentication codes. His main interests are GNSS and cryptography, where he has published more than 30 publications and holds 3 patents.

Giovanni Gamba received his Ph.D. degree in information engineering from the University of Padova, Italy. He worked for the Italian National Research Council (IEIIT-CNR) on interference detection and mitigation for industrial applications operating in the 2.4-GHz band. Since 2010, he has been an R&D engineer at Qascom, and is involved in theoretical design and development of interference detection and mitigation algorithms for different GNSS projects and products.

Matteo Canale is a cryptography and cyber-security engineer at Qascom. He obtained an M.Sc. degree in communications engineering and a Ph.D. in information engineering from the University of Padova. His main interests include network security, cryptography, and GNSS security. He is currently working on the definition, specification, and implementation of authentication services for the Commercial Service Demonstrator in the framework of the AALECS project.

Samuele Fantinato is a radionavigation system engineer at Qascom, Italy. He received a master's degree in telecommunication engineering from the University of Padova and is currently involved in ESA and European Commission projects related to development of GNSS test beds for interference and spoofing mitigation and for implementation of authentication schemes in the Galileo Commercial Service. Fantinato previously worked for Thales Alenia Space in the navigation technologies and products department with a focus on signal processing and performance assessment of Galileo and EGNOS ground reference station receivers. In 2008 he was a Young Graduate Trainee at the European Space Agency.

Prof.-Dr. Günter Hein serves as the editor of the Working Papers column. Until the end of 2014, he was the head of the EGNOS and GNSS Evolution Program Department of the European Space Agency. He continues to support all scientific aspects of the ESA Navigation Directorate as well as now serving as a member the ESA Overall High Level Science Advisory Board Previously, he was a full professor and director of the Institute of Geodesy and Navigation at the Universität der Bundeswehr München. In 2002, he received the Johannes Kepler Award from the U.S. Institute of Navigation (ION) for "sustained and significant contributions" to satellite navigation. He is one of the inventors of the CBOC signal.