An autonomous GNSS anti-spoofing technique

An Autonomous GNSS Anti-Spoofing Technique

Gianluca Caparra

Department of Information Engineering
University of Padova
Padova, Italy
E-mail: caparrag@dei.unipd.it

Christian Wullems, Rigas T. Ioannides

ESTEC
European Space Agency
Noordwijk, The Netherlands
E-mail: {christian.wullems, rigas.ioannides}@esa.int

***Abstract*—In recent years, the problem of Position, Navigation and Timing (PNT) resiliency has received significant attention due to an increasing awareness on threats and the vulnerability of the current GNSS signals. Several proposed solutions make uses of cryptography to protect against spoofing. A limitation of cryptographic techniques is that they introduce a communication and processing computation overhead and may impact the performance in terms of availability and continuity for GNSS users.**

This paper introduces autonomous non cryptographic anti-spoofing mechanisms, that exploit semi-codeless receiver techniques to detect spoofing for signals with a component making use of spreading code encryption.

I. Introduction

In recent years, the resiliency of positioning, navigation and timing has received significant attention due to an increasing awareness of spoofing threats and the vulnerability of the current GNSS to this type of deliberate interference [1]. A significant body of research has focused on cryptographic techniques to defend against spoofing, both at data (symbol) [2]–[5] and signal layers (spreading code) [6]–[8]. Such techniques focus on providing the capability for authenticating the origin of the navigation message and providing assurance on the authenticity of ranging signals through methods such as spreading code encryption.

A limitation of cryptographic techniques is the significant overhead and impact the management of keys can have on the availability and continuity operations for GNSS users. Furthermore, compromise and rapid revocation can have devastating impacts on users, especially where users are dependent on the signal-in-space or an ancillary data channel for the dissemination of updated keying information.

This paper introduces an autonomous anti-spoofing technique, by using adapted semi-codeless receiver techniques to detect spoofing for signals with a component that uses spreading code encryption; however, the technique does not require keys to be installed on the receiver. The proposed technique is described in relation to the GPS L1 signal with C/A and GPS P(Y) signal components; although the technique is expected to be applicable to other signals as well.

The technique significantly limits the degrees of freedom of an attacker and provides the capability to detect the illegitimate signals from legitimate ones in a hostile environment.

The paper is structured as follows: Section II provides an introduction on GNSS authentication; III provides an overview of the Security Code Estimation and Replay (SCER) attack and presents results based on experimentation performed with real signals in both static and dynamic scenarios; and Section IV introduces semi-codeless techniques for anti-spoofing, high-level attack strategies, and describes the proposed autonomous anti-spoofing technique with a theoretical evaluation of performance. The paper concludes with a discussion on future work.

II. Background on GNSS authentication

The level of assurance of a Position, Velocity and Time (PVT) computed using GNSS signals is dependent on that of the GNSS receiver ranging and PVT computation functions and the capability of the receiver to differentiate between authentic and counterfeit signals. Mechanisms can be provided within the GNSS signal at both the signal and data levels to achieve this:

- *Signal level protection,* allows the receiver to determine whether the received signal originated from its claimed source or whether it is a forgery. Attacks at the signal level can affect the PVT by targeting the receiver's ranging function:
  - *Signal forgery:* generation of arbitrary navigation signals (*e.g.* signal spoofing using a signal generator, including reception of legitimate GNSS signals and replay of navigation message over simulated signals so that they appear legitimate to the receiver); and
  - *Signal relay:* recording and rebroadcast of RF signals (*e.g.* meaconing).
- *Data level protection,* allows the GNSS receiver to determine whether the received navigation message originated from its claimed source, and whether integrity of the message is assured (*i.e.* message has not been altered by unauthorised or unknown means). Such protections are referred to as data authentication and cryptographic integrity protection. Attacks at the data level can affect the PVT by targeting the receiver's PVT computation function, providing an incorrect navigation message.

For a more comprehensive analysis on the vulnerabilities of GNSS to intentional attacks, we refer the reader to [1].

Data level protection can be achieved with information security techniques usually referred to as Navigation Message Authentication (NMA) [2]–[5], which foresee the use of cryptographic mechanisms to authenticate the navigation message.

The problem of protection at the signal level belongs to the signal or channel estimation domain, and includes techniques such as Spreading Code Encryption (SCE) or watermarking (*e.g.* by Signal Authentication Sequence (SAS) [6], hidden markers [7], or Spread Spectrum Security Codes (SSSC) [8]). Strictly speaking, these are not authentication mechanisms, rather they increase the complexity and cost of accurately reproducing a legitimate signal to an intractable level, providing the receiver with the possibility to distinguish between authentic and illegitimate signals.

III. SCER

The goal of a SCER attack [9], [10] is to estimate a legitimate signal in order to generate a spoofed signal with minimal delay (if any). It is important to note that the estimation need not be perfect, only good enough so that the reproduced signal is indistinguishable from the authentic one, when corrupted by channel and noise at the receiver.

This type of attack represents a general threat that can be carried out irrespective of the particular cryptographic schemes employed in the signal (be it data layer schemes: *e.g.* NMA; or signal layer schemes: *e.g.* SCE, SSSC). The victim will receive both the authentic and spoofed signals below the noise floor; only after correlation, exploiting the processing gain, does the Signal-to-Noise Ratio (SNR) become sufficiently good to reliably process the signal.

In order to maximize the information obtained from the received signals, the detection statistic takes place before the correlation. Indeed, the correlation process increase the SNR thus reduce the noise contribution, but the effect of SCER is noticeable in the different noise distribution. Therefore, the correlation process itself help hiding the attack. If the SNR of the attacker is lower than the victim's, an increase in the noise variance of the received signal would be noticeable; otherwise, the receiver noise will hide the attacker.

The attacker's estimation will improve over time with the accumulated energy in the symbol (data level) or chip (signal level). Thus, after an initial transient, the attacker estimation becomes reliable and the difference between the legitimate and estimated signals tends to diminish, as we will see in the following.

In [9] three cases are considered for the estimator function: two time-invariant, the Maximum Likelihood (ML) and Maximum *A Posteriori* (MAP) estimators; and one time-varying, the Minimum Mean Square Error (MMSE) estimator. The MAP estimator is optimal for the purpose of minimising the estimate error probability $\mathrm{P}\left[\hat{w}_n(t) \neq w_n\right]$, where w_n represents the security code (T_w being its symbol period) that is unknown to the attacker. The remainder of this paper will focus on this approach:

$$\hat{w}_n(t) = \mu_{\mathrm{MAP}}[z] = \mathrm{sgn}(z) \tag{1}$$

The optimal detection strategy for SCER proposed in [9] and improved in [10], requires knowledge of the attack strategy used by the receiver; this is not obvious in the real world. There are a number of issues affecting the performance of the optimal SCER detection strategy in the real world.

Information of the received signal, which cannot be known unambiguously, is required. This information includes the noise variance of the signal. The receiver only has access to an estimation of the carrier to noise ratio, which to a certain extent can be influenced by the attacker without being detected. In order to obtain sufficient information from the noisy signal, the receiver shall accumulate energy for a long period. This becomes increasingly difficult in an environment where measurements of the signal can change rapidly (*e.g.* due to multipath or receiver dynamics, especially for low elevation satellites).

A simpler detection strategy is presented by [11], requiring less information of the received signal but achieving suboptimal performance. This proposal stores the first samples of each unpredictable symbol and evaluates the correlation with a local replica computed after the demodulation of NMA This proposal demonstrates the feasibility of detecting SCER attacks in an additive white Gaussian noise (AWGN) channel; however, performances in realistic real world conditions were not evaluated.

An extension of this detection strategy includes dividing the symbols in bins and computing the correlation for each bin in addition to the evaluation of the accumulated correlation on the first part of the unpredictable symbols. If the signal is authentic, every bin will have the same average correlation value, while if the signal is generated by a SCER attack a smaller correlation for the initial bins is expected.

A. Results on realistic signals

In order to assess the effectiveness of the SCER attach, an experiment was devised involving the use of real signals. Two scenarios were investigated:

1) *Static scenario:* in this case the signal was acquired through an omni-directional roof antenna equipped with a Low Noise Amplifier (LNA) with 30 dB gain and 1 dB Noise Figure (NF). The device used for sampling and replaying the signal was a HackRF One, an open source inexpensive Software Defined Radio (SDR) device [12]. The signal was sampled at 8 MHz with 8-bit I/Q quantisation.
2) *Dynamic scenario:* in this case the signal is the clean dynamic acquisition of the Texas Spoofing Test Battery (TEXBAT) dataset [13]. This signal was acquired with a sampling rate of 25 MHz and 16 bit I/Q quantisation, using a National Instruments PXIe-5663 Vector Signal Analyzer (VSA). The replay was performed using the HackRF One SDR.

Both the clean signal recorded from the antenna and the generated spoofed signals were replayed to a Septentrio PolaRx4 PRO with standard configuration.

For the sake of simplicity, when replaying the SCER signal, no authentic signal was present. The goal of the experiment was to verify weather the increase in the noise introduced by the attack was enough to prevent a professional receiver from decoding the navigation data and tracking the signal. The capture of the tracking loop was not implemented, since this would increase the complexity of the attack with respect to timing issues and power levels, but would not affect the attack strategy.

The employed estimator was the MAP (1). A zero delay attack was implemented, such that the attacker starts replaying the signal immediately after receiving the first sample of the authentic signal. Clearly, this initial estimation is rather poor and introduces a large amount of noise after the bit transition; however, this was used to evaluate the performance in the most challenging setting for the attacker. For the same reason, all 20 PRN repetitions of the C/A symbol were treated as independent in order to maximise the uncertainty for the attacker and the introduced noise. Due to the unreliable estimation of the first samples, a trivial extension of the attack is to start the attack using a few random samples, in order to generate a signal that arrives in phase at the correlation peak, producing a completely synchronised attack. In both experiments, the receiver was able to decode the navigation data and compute the PVT solution with the spoofed signal.

Two measures were defined to quantify the effectiveness of the attack:

- *Convergence time:* the time needed for the attacker estimation to stably reach the correct value, which can be written as:

$$C_t(n) = \max\{t \in [nT_w, (n+1)T_w], \text{ s.t. } \hat{w}_n(t) \neq w_n\} - nT_w \tag{2}$$

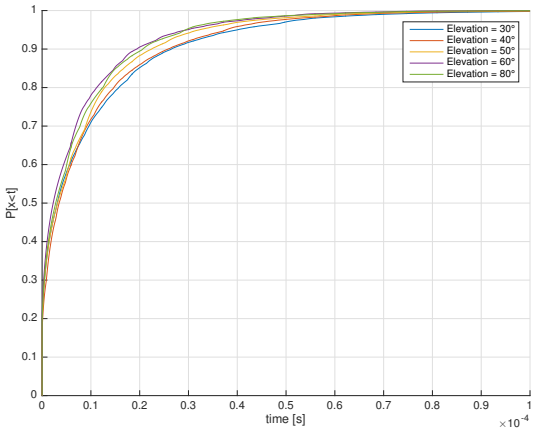
  In Fig. 1a the Cumulative Distribution Function (CDF) of C_t is reported for different elevation angles in the two scenarios considered.
- *Correlation reduction:* due to the initial uncertainty in the attack estimate, the victim receiver will observe a normalized reduction in the correlation peak:

$$\Delta C(n) = \frac{1}{T_w} \left| \int_{nT_w}^{(n+1)T_w} \hat{w}_n(t) - w_n \, dt \right| \tag{3}$$

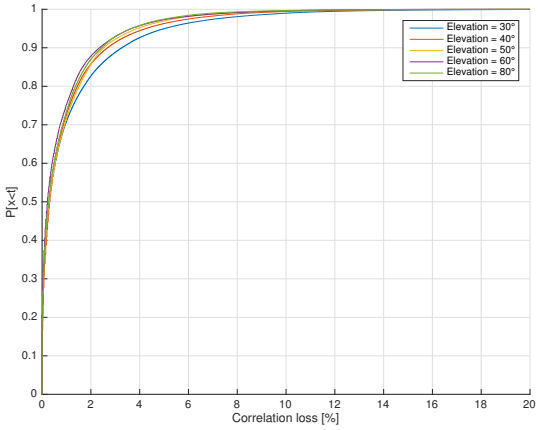
  In Fig. 1b the CDF of C_R is reported for different elevation angles in the two scenarios considered.

It can be seen from Fig. 1a that the time required to achieve the correct estimation with high probability (*e.g.* $> 95\%$) is in the order of 50 μs, which is only a small fraction of the symbol period for GPS C/A (20 ms) or Galileo E1B (4 ms). Therefore, the detection strategy should focus on this small fraction of each unpredictable symbol. Similar results were obtained in the dynamic scenario.

The long symbol periods of open service GNSS signals, yield a significant opportunity for the attacker. After reaching a reliable estimate $\hat{w}_n(t)$, the attacker can generate a signal that almost perfectly resembles the legitimate signal. The attacker is able to exploit the long integration time at the receiver side



(a)



(b)

Figure 1: CDF of (a) convergence time of SCER estimation and (b) the correlation reduction due to SCER attack in the static scenario, using MAP estimator.

to hide the initial uncertainty. Moreover, the noise level in the signal can be artificially increased in order to hide the initial uncertainty and make it comparable to the noise of the signal. Due to the long symbol period, the receiver will still track and demodulate the symbol correctly.

It is worth noting that with more recent signals such as the Galileo E1B or GPS L1C, which make use of channel coding to reduce the Bit Error Rate (BER), the attacker may even have his incorrect estimations corrected by the victim decoder itself and the FEC redundancy can be leveraged to mount a Forward Estimation Attack (FEA) attack [14].

An example of the result of the suboptimal detection strategy, computed in the dynamic scenario discussed above and with the corresponding zero-delay SCER generated signal with MAP estimator, is reported in Fig. 2. The bin width is 10 μs in Fig. 2a - Fig. 2b - Fig. 2c and 100 μs for Fig. 2d. Fig. 2a shows that for authentic signals all the bins have similar correlations. In Fig. 2b - Fig. 2d the spoofed signal was used and the tracked SV signal had a high C/N_0. Fig. 2c illustrates the case when

the tracked SV signal had a low C/N_0. As expected, the shorter the bin, the more evident the loss of correlation on the initial bins; however, the estimate also becomes noisier. For this reason a trade-off shall be found.

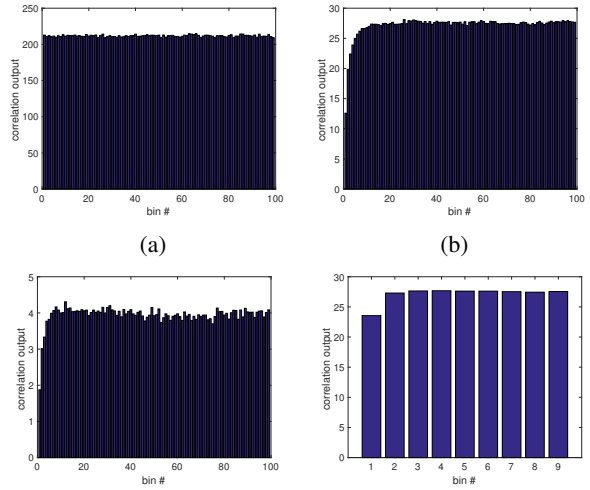


Figure 2: Suboptimal SCER detection output for the dynamic scenario. The bins length is 10 μs in (a) - (b) - (c) and 100 μs in (d). The signal reported are: authentic signals with high C/N_0 in (a); spoofed signal with high C/N_0 in (b) - (d); spoofed signal with low C/N_0 in (c).

If instead of a zero-delay attack the attacker is able to gain even a little time advantage by exploiting the receiver clock uncertainty, then the situation dramatically worsens for the receiver, which quickly loses the ability to detect the initial attacker uncertainty at all.

It is also clear from Fig. 2 that it is hard to define an optimal threshold to detect a spoofing attack for the receiver. Indeed, the correlation level heavily depends on the C/N_0 and thus on the noise variance of the received signal. As already discussed, the receiver cannot reliably determine his actual C/N_0 nor check if the estimated value corresponds to the expected one, predominantly due to effects linked to the environment. While it might be possible for a static receiver to do this in open sky conditions (*e.g.* where a model of the average C/N_0 based on the SV elevation could be used), it is not considered feasible for dynamic receivers. Furthermore, an attacker could easily influence the C/N_0 estimation by artificially introducing noise in the generated signal or intentionally flip (invert the phase) the generated signal for a fraction of the bin duration, to lower the measured correlation at the receiver side. In this way, the attacker could reduce the distance between the first bins and the rest of the symbol, relaxing the need for a perfect estimation since the beginning.

It is possible to formulate this attack as follows: the victim receiver makes use of the correlation based detection strategy, using N bins. Let C_n be the correlation value in the n-th bin and $\underline{C} = [C_1, \ldots, C_N]$. The detection strategy is to accept the signal as authentic if $\underline{C}$ lies within some predetermined set $\mathcal{C}_0$. The attacker, that is supposed to know N, aims at inducing a flat correlation observed by the receiver for each bin. In order to do this he can perform a training phase in which he obtains an estimation of the typical correlation shape by performing a dry run of the SCER attack and of the detection strategy. In this way he can achieve an estimation similar to the one in Fig. 2b. Now the attacker can balance the effect of the attack. Let us define N_s as the number of samples contained in each bin, A_s as the sample amplitude corresponding to the PRN processed, C_1 as the correlation value of the first bin and C_n as the correlation obtained in the n-th bin. The goal of the attacker is to reduce the average correlation obtained in the bin $n \geq 2$ to C_1. The number of samples that must be flipped, N_{flip_n}, can be computed as:

$$N_{flip_n} = \frac{C_n - C_1}{2C_1}$$

The generated signal presents a flat correlation over all the bins when transmitted; the knowledge of the receiver noise statistic is not needed, because this will be equally distributed over all the bins.

Table I details synthetic results and the corresponding parameters of the attack used to obtain the flat correlation shown in Fig. 3 in the previously described dynamic scenario. It is possible to see that artificially flipping only few μs of signal for each bin it is possible to obtain a flat correlation, aligned with the first bin. The small number of flipped chips makes detection very challenging, as the attack cannot be easily differentiated from effects linked to the environment (*e.g.* multipath).

C/N_0	T_{bin} [μs]	n_s	A_s	C_1	C_n	N_{flip_n}	T_{flip} [μs]	%
high	100	2500	27.6	58750	69000	185	7.4	7.4%
high	10	250	27.6	3145	6900	68	2.7	27%
low	100	2500	4	8750	10000	157	6.24	6.2%
low	10	250	4	58750	69000	68	2.7	27%

Table I: Summary of the parameters used to balance the effect of the SCER attack.

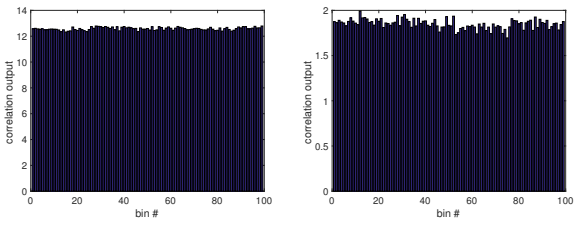


Figure 3: Suboptimal SCER detection output for the dynamic scenario with balance attack, corresponding to the signal of Fig. 2b and Fig. 2c.

The drawback of this attack strategy is the degradation of the C/N_0. In order to reduce this effect, the attacker can attempt to maximize the average correlation of the first bin

C_1, for example, using a time-varying strategy that reduces the power level of the first samples where he has the maximum uncertainty, and transmitting the last samples of the first bin at a higher power.

A method to limit the effectiveness of the attack is to increase the difficulty of estimating unpredictable symbols. This can be done by reducing the per symbol energy, either by reducing the transmission power or the symbol length.

Use of GNSS signals with much lower energy per symbol (higher chipping rate) can significantly increase the difficulty of an attack. For example the GPS P(Y) signal, with a chipping rate 10 times higher than the C/A code. The fact that the P(Y) spreading code is not public (i.e. modulo-2 sum of P-code and encrypting code), thus an attacker cannot exploit the processing gain, and the observed energy per symbol is significantly reduced. This, coupled with higher chipping rate, significantly increases the difficulty of the attack.

In the next section, a technique is presented that exploits the characteristics of the GPS P(Y) signal to restricting the degrees of freedom for the attacker.

IV. Semi-codeless techniques for anti-spoofing

The GPS Course Acquisition (C/A) code is the predominant signal used by civilian receivers today. Historically, this signal was used to facilitate the handover process from C/A to P(Y) code tracking, allowing the receiver to determine the correct P-code setup parameters and whether spreading code encryption was active. Today direct acquisition is possible for military users; however, the handover process is still used by some semi-codeless receivers in order to obtain multi-frequency measurements for high-precision applications. The P(Y) code is a modulo-2 sum of the P-code and W-code, an encrypting code which is not known to unauthorized users. The P code chipping rate is 10.23 Mchip/s and the W chipping rate is 20 times lower, 511.5 Kchip/s.

The GPS anti-spoofing mechanism not only limited the access to the higher-precision precision signal, but also to the L2 frequency where only the P(Y) signal was transmitted.

In order to have access to a second frequency, providing the possibility to correct for errors induced by the ionosphere, semi-codeless techniques allowed carrier phase measurements to be made on the L2 frequency without knowledge of the secret W code [15]. Simpler techniques (codeless), involved squaring of the received signal; however, the squaring operation also increases the noise (reducing signal to noise ratio). More sophisticated techniques exploited knowledge of the public P-code before squaring, maintaining uncertainty on the W-code. By wiping off the P-code, a 20 times reduction of the signal bandwidth was obtained. Thus by filtering the signal with a bandpass filter before the squaring operation, the noise could be reduced by 13 dB. These techniques are commonly referred to as P-code aided squaring.

Several additional techniques were proposed in the literature for combining the P(Y) signal transmitted in both the L1 and L2 frequency, allowing a further performance improvement. An interesting feature of these techniques is that instead of simply squaring the W code, they perform an estimation of the W-code, using a range of different estimator techniques.

Our work focuses on the first two techniques discussed as they only require the L1 signal component. We propose to exploit semi-codeless techniques for the purpose of anti-spoofing. Extension to multi-frequency receivers is trivial and may allow better performance to be achieved.

The following assumptions are made for the anti-spoofing technique presented in this paper:

- The receiver is static, in an open-sky environment tracking high-elevation satellites. It is assumed that the C/N_0 is relatively stable and that there are limited variation due to effects of the local environment such as multipath.
- The receiver may be under attack by a spoofer. The task of the receiver is to determine whether it is under attack and to provide the capability to distinguish between authentic and spoofed signals.
- It is assumed that the attacker is not able to block legitimate signals (*e.g.* unplugging the victim receiver antenna and connecting it directly to the spoofer). This means the technique may not be suitable for applications where the user himself is the attacker (*i.e.* self-spoofing).
- It is assumed the signal is unpredictable, such that an attacker is not able to generate a valid signal before the transmission of the authentic one from the satellite.

A high-level overview of attack strategies is described below:

- *Simple signal generation:* a non-sophisticated attacker may generate the C/A signal component only. The use of semi-codeless techniques allows the receiver to detect the lack of the P(Y) component or if the fixed power relations between the component is verified.
- *Complex signal generation:* a sophisticated attacker may generate both C/A and P(Y) components as per the Interface Control Document (ICD). Because the W code is not public, the victim is unable to directly check if the received signal is modulated by the correct W code. There are some techniques that attempt a cross-check between receivers [16] or to send the sampled RF signal to a secure server, which has access to the military code to perform the PVT computation. If generated signals can reach the receiver antenna synchronized with the authentic signals, the detection would be based on the difference of the W-code. In [16] the idea of extracting the W-code through a semi-codeless receiver and the comparison with an estimation coming from a ground infrastructure equipped with a high gain antenna is presented.
- *Meaconing:* the simplest way to spoof the signal with the authentic W code is to perform a meaconing attack. The attacker receives the signal, waits for a desired delay, and then retransmits the signal towards the victim receiver. The signals will not be aligned at the receiver antenna, thus at least two correlation peaks (both on C/A and P(Y)) would be found in the acquisition, but with the correct W-code. In the case of meaconing, ranges can only be delayed (not anticipated). Furthermore, this type of attack

would result in a spoofed signal that is noisier than the authentic one.

- *SCER:* a sophisticated attacker may try to reduce the noise on the spoofed signal by performing an estimation of the W-code. Even with this type of attack, a delay in the generation of the spoofing signal is introduced. Due to the very short bit duration (about $2\mu s$), the attacker is constrained in the amount of energy that can be accumulated in this duration without significant antenna gain (*e.g.* steerable dish antennas), see Fig. 1a. The difference with the SCER attack on the C/A is the symbol duration and therefore the amount of energy that can be accumulated. This permits a synchronized attack by generating random samples before sufficient energy has been accumulated and hiding this by adding noise once a reliable estimate has been obtained so that this type of attack cannot be easily differentiated from noise induced from the environment. Due to the limited energy that can be accumulated for a short P(Y) chip duration, techniques for hiding the attack strategy are very limited. The short bit duration therefore significantly reduces the effectiveness of a SCER attack, where significant additional gain would make an attack significantly more expensive and potentially visible (less covert).

Considering a signal with an unknown code and very short bit duration (e.g. P(Y) W-code bit), the degrees of freedom for the attacker to be able to generate an undetectable aligned spoofing signal with the correct code are very limited.

A. P(Y) acquisition with reduced search space

The first technique we propose consists in exploiting the semi-codeless tracking methods to obtain an estimate of the received W code, and to verify the consistency of the P(Y) code phase and carrier frequency with the C/A one. The concept is shown in Fig. 4. The digitized signal is acquired and tracked using the C/A component. The output of the tracking loop is used to wipeoff both ranging codes (C/A and P) and the result is filtered to reduce noise. Then, the carrier phase is removed using the PLL output. The only component left in the signal is the W code. Integrating at the W code rate and using an estimator (*e.g.* the MAP estimator discussed in the SCER section) allows to recover the secret W bits. Due to the independence of the cryptographical bits, no processing gain can be leveraged and thus there is no advantage in using longer integration time, thus each bit can be estimated independently. If the estimation is performed independently for each W chip, selecting the combination with the maximum energy detected among all the combinations used, this becomes a semi-coherent integration that provides advantage over a non-coherent integration [17]. Clearly, the reliability of the estimation depends on the C/N_0, the antenna gain, the estimator used and the noise figure of the receiver.

1) W Code Coherence: When a W bit sequence estimation is available, it is passed to a detector that compares the estimation coming from different tracking loops locked on different correlation peaks in order to verify if all the tracked

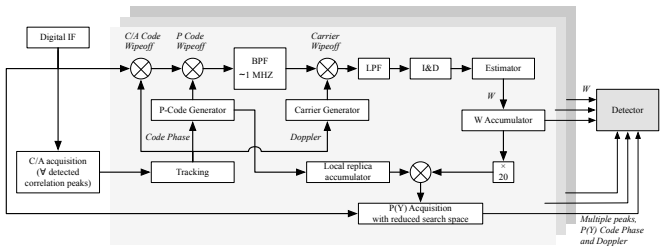


Figure 4: Proposed autonomous anti-spoofing scheme.

replicas are modulated by the same secret spreading code for that PRN. In order to compare between two estimations the cross-correlation is computed. We can distinguish three cases:

(a) both the signals are authentic, *e.g.* LOS and multipath of the authentic signal: in this case the cross-correlation should show a correlation peak.
(b) both the signal are spoofed, *e.g.* LOS and multipath of the spoofed signal: even in this case the cross-correlation should show a correlation peak, rendering the detection ineffective. For this reason we assume that at least one of the peak corresponds to an authentic signal.
(c) one signal is authentic and one signal is spoofed.

In order to discriminate between case (a) and (c), a characterization of the cross-correlation result is needed. Due to the independence of the W bits, a multibit statistic is just an extension of the single bit one. Let us denote by p the equivalent BER of the receiver, and by q the equivalent BER of the attacker. These include the channel effects, the antenna gain and the estimation strategy.

Let be x the random variable that represent the product of two W bit estimation. For the sake of simplicity we can assume a hard detection estimation that represent a pessimistic assumption for the performance. The probability mass density (pmd) of x when both the signals are legitimate $p_{x|ll}(a)$ and when a signal is legitimate and the other one is spoofed $p_{x|ls}(a)$ can be written as:

$$p_{x|ll}(a) = \begin{cases} p^2 + (1-p)^2 & a = 1 \\ 2p(1-p) & a = -1 \end{cases}$$

$$p_{x|ls}(a) = \begin{cases} p^2 q + q(p-1)^2 + 2p(p-1)(q-1) & a = 1 \\ (p-1)^2(1-q) + p^2(1-q) + 2pq(1-p) & a = -1 \end{cases}$$

The detection strategy for determining between the two cases is a hypothesis testing problem based on the cross-correlation of the two estimations:

$$y = \sum_{n=1}^{N} x_n$$

This sum is a random variable itself and it is possible to write it as the sum of two Gaussian variables:

$$N_+ = \sum_{n=1}^{N} \chi\{x_n = 1\} \sim \mathcal{N}\left(N p_{x|z}(1), N p_{x|z}(1) p_{x|z}(-1)\right)$$

$$N_- = \sum_{n=1}^{N} \chi\{x_n = -1\}$$
$$\sim \mathcal{N}\left(Np_{x|z}(-1), Np_{x|z}(-1)p_{x|z}(1)\right)$$
$$p_{y|z}(a) \simeq N_+ - N_- = N - 2N_-$$

where z can be ll or ls. The Kullback-Leibler (K-L) divergence between two Gaussian distributions $\mathcal{N}(\nu_a, \sigma_a^2)$ and $\mathcal{N}(\nu_b, \sigma_b^2)$ is given by

$$D(a,b) = \log\left(\frac{\sigma_a}{\sigma_b}\right) + \left(\frac{\sigma_a^2 + (\mu_a - \mu_b)^2}{2\sigma_b^2}\right) - \frac{1}{2}$$

When deriving $D(p_{y|ll}, p_{y|ls})$ and $D(p_{y|ls}, p_{y|ll})$, is seen that as $p \to 0.5$ both divergences are close to 0 irrespective of q. For $p \to 1$, the distinguishability depends on q: for q close to 0.5 it is very easy to detect the attack, while for q close to 1 it is more difficult.

It is possible to select the target p, q and compute the outer bound in the detection probability using the Likelihood Ratio Test (LRT), that is the strategy that yields the minimum p_{md} for any given constraint on p_{fa}, and *vice versa* [18, §3.3] [19] if both the statistics of the legitimate and spoofed signal are known (*i.e.* if the victim is aware of the particular strategy adopted by the spoofer). If the spoofer strategy is not known, a Generalized LRT (GLRT) strategy shall be used but will lead to worse results.

Based on the BER of both the attacker and the receiver, it is possible to find the minimum observation time to achieve the desired performance in terms of false alarm probability p_{fa} and of missed detection probability p_{md}. The bigger the attacker advantage over the victim receiver, the longer the necessary minimum observation time, which in turn leads to a longer Time Between Authentications (TBA).

An example is reported in Fig. 5, for (a) $p = 0.75$, $q = 0.9$ and (b) $p = 0.55$, $q = 0.9$. It is evident that when the attacker advantage is limited, the detection mechanism requires a short observation time; while when his advantage increases the receiver needs to accumulate more W chips, requiring a much longer time before being able to distinguish between the authentic and spoofed signals. An advantage of working with the W secret code is that due to its high rate of 511,5 Kbit/s, the 6 Mbit taken into account correspond to an observation period slightly shorter than 12 seconds.

In this section a detection statistic between two peaks was presented. The extension to a detection statistic that takes into account distorted (or multiple) auto-correlation peaks, possibly achieving better results by leveraging more signal features (*e.g.* correspondence to a multipath model), is left for future work.

2) P(Y) Acquisition: When a sufficiently long W sequence is estimated (in the order of tens of milliseconds), a second check can be performed. This check is a direct P(Y) acquisition. At this stage, the receiver has achieved a good time synchronization and knows which W sequence shall be used to build the local replica, thus there is no need to perform the acquisition over a big search space, and the computational complexity

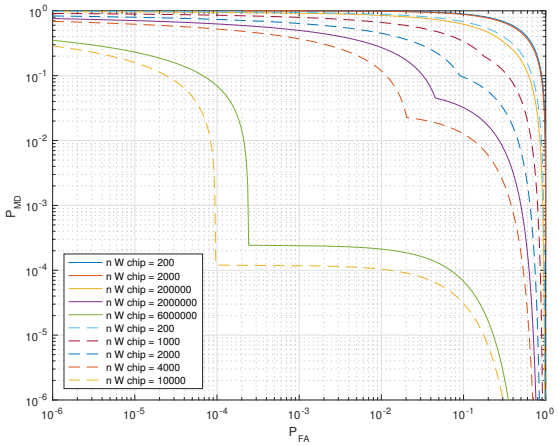


Figure 5: Outer bound of achievable performance for different p, q and observation time. $q = 0.9$, while $p = 0.55$ for solid lines and $p = 0.75$ for dashed lines.

can be reduced. On the other hand, a larger search space, improves the anti-spoofing performance. A tradeoff between the search space dimension and the search resolution shall be found. Moreover, the time required to perform this acquisition is not critical and can take up to some seconds, alleviating the computational requirement. Clearly, the performance depends on the BER on the W code estimation, and the worse the estimation performance, the longer the required integration time to achieve the desired detection capability.

The output of the acquisition stage are three measures: estimated carrier frequency, estimated code phase, and the number of correlation peaks. Two types of checks can be performed on these outputs. The first check is on the number of correlation peaks and on their relative position. If the signal is LOS, only one peak should be found. If LOS and multipath are present, secondary smaller delayed peaks can be found. The presence of two strong peaks very distant from each other, may indicate a meaconing attack. The estimated code phase and carrier frequency can be compared with the one obtained from the C/A acquisition in order to check the coherence of the measures. A mismatch may also indicate a spoofing attack. The value of the correlation peak can also be compared to that of the C/A in order to check the coherence with the fixed power relationship.

B. Estimation of residual energy

A second way to exploit semi-codeless tracking techniques is an iterative estimation and removal process.

The carrier-phase measurements are typically used in surveying applications due to the improved accuracy that they achieve with respect to code-phase measurements. Indeed, code-phase measurements are more affected by multipath and are in general much more noisier measurements. For these reasons, a second integrity check can be performed comparing carrier-phase measurements obtained from a different iteration of the processing.

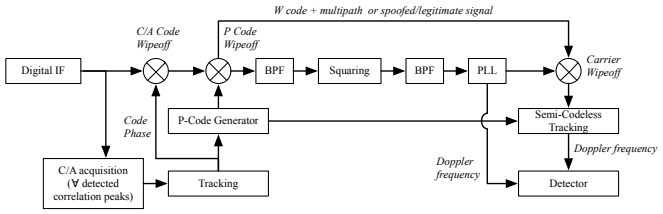


Figure 6: Proposed autonomous anti-spoofing scheme.

The scheme is shown in Fig. 6. The initial part of the processing is equivalent to the one proposed in Fig. 4. After the carrier wipeoff, besides the W code, other terms such as multipath or a spoofed signal are also present in the signal. Recognizing this, the processing is repeated on this residual energy. If the receiver is tracking a spoofed C/A signal, the residual energy will contain the non spoofed C/A and P(Y), which will be coherent between them. As an example, we can think of a P code aided squaring (also known as semi-codeless squaring) and to use long coherent integration time to obtain a low noise estimation of the Doppler frequency.

In the ideal case of LOS and of perfect tracking by the first tracking loop, no signal is present after the wipeoff, so the second tracking loop should not be able to acquire and track the signal. If the receiver is under spoofing attack, the second tracking loop should acquire and track a signal. The estimated Doppler frequency shall be different form the first one, as indeed the spoofed is trying to influence the PVT computation of the receiver by changing the ranging. If there is multipath, the second tracking loop should be able to acquire and track a signal.

This approach suffers from an important drawback: the estimation (even more in the case of squaring) introduces some interference into the remaining part of the signal. These terms will also include cross-correlation terms, and this may degrade the sensitivity of the scheme. This issue is even more evident if a codeless technique is applied, because the goal of the detection is to distinguish the Doppler frequency of all the legitimate SVs in view from possible unknown spoofing terms.

On the other hand, even if suffering from squaring losses, the receiver complexity is reduced with respect to relative to the semi-coherent estimation of the W code presented in the Section III. For these reasons the determination of an optimal detection strategy is postponed to future work.

V. Conclusion

The article, after introducing the predominant cryptographic anti-spoofing techniques such as NMA and SCE, has shown through some experimental results the feasibility of SCER attacks against GPS C/A using inexpensive hardware. This motivates the use of SCE techniques to protect against spoofing; however, in order to avoid the burden of key management, an adaptation of semi-codeless receiver techniques was presented, such that the method is independent of the cryptographic mechanism employed. A feasibility study on the usage of this approach was presented. Derivation of the optimal semi-codeless based anti-spoofing techniques and the verification with real-world scenarios is left for future work.

Acknowledgments

The authors gratefully acknowledge Dr. Nicola Laurenti for his comments and insight.

References

[1] R. T. Ioannides, T. Pany, and G. Gibbons, "Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques," *Proceedings of the IEEE*, vol. 104, pp. 1174–1194, jun 2016.

[2] C. Wullems, O. Pozzobon, and K. Kubik, "Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems," in *European Navigation Conference, (ENC-GNSS)*, pp. 1–10, 2005.

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

[4] P. Walker, V. Rijmen, I. Fernández-Hernández, G. Seco-Granados, J. Simón, J. D. Calle, and O. Pozzobon, "Galileo Open Service Authentication : A Complete Service Design and Provision Analysis," in *ION GNSS+ 2015*, (Tampa, Florida), 2015.

[5] G. Caparra, S. Sturaro, N. Laurenti, C. Wullems, and R. T. Ioannides, "A Novel Navigation Message Authentication Scheme for GNSS Open Service," in *ION GNSS+ 2016*, (Portland, Oregon), 2016.

[6] O. Pozzobon, L. Canzian, M. Danieletto, and A. Dalla Chiara, "Anti-spoofing and open GNSS signal authentication with signal authentication sequences," in *ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, NAVITEC*, pp. 1–6, IEEE, dec 2010.

[7] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," in *International Workshop on Information Hiding, IH* (J. Fridrich, ed.), vol. 3200 of *Lecture Notes in Computer Science*, (Berlin, Heidelberg), pp. 239–252, Springer Berlin Heidelberg, 2005.

[8] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," *Proceedings of the Institute of Navigation GPS/GNSS 2003 conference*, pp. 1543–1552, 2003.

[9] T. E. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, pp. 1073–1090, apr 2013.

[10] G. Caparra, N. Laurenti, R. T. Ioannides, and M. Crisci, "Improved Secure Code Estimation and Replay Attack and Detection on GNSS Signals," in *ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, NAVITEC*, 2014.

[11] I. Fernández-Hernández and G. Seco-Granados, "Galileo NMA Signal Unpredictability and Anti-Replay Protection," in *ICL-GNSS 2016*, 2016.

[12] Greatscottgadgets, "https://greatscottgadgets.com/hackrf/."

[13] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas Spoofing Test Battery : Toward a Standard for Evaluating GPS Signal Authentication Techniques," in *ION GNSS 2012*, (Nashville, Tennessee), pp. 3569 – 3583, 2012.

[14] J. T. Curran and C. O'Driscoll, "Message Authentication and Channel Coding," in *ION GNSS+ 2016*, (Portland, Oregon), 2016.

[15] K. T. Woo, "Optimum Semi-Codeless Carrier Phase Tracking of L2," in *Navigation*, vol. 47, pp. 82–99, 1999.

[16] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, pp. 2250–2267, oct 2013.

[17] R. T. Ioannides, L. E. Aguado, and G. Brodin, "Diverse Signals Combinations for High-Sensitivity GNSS," *Journal of Navigation*, vol. 60, p. 497, sep 2007.

[18] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume 2: Detection Theory*. New Jersey: Prentice-Hall Inc, 1993.

[19] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Transactions on Information Theory*, vol. 46, pp. 1350–1356, jul 2000.