Investigation on the Actual Robustness of GNSS-based Timing Distribution Under Meaconing and Spoofing Interferences

Investigation on the actual robustness of GNSS-based timing distribution under meaconing and spoofing interferences

Alex Minetto[1], Brendan D. Polidori[1], Marco Pini[2], Fabio Dovis[1]
[1]*Department of Electronics and Telecommunications (DET), Politecnico di Torino (Turin, Italy)*
[2]*Space and Navigation Technologies Area, LINKS Foundation (Turin, Italy)*

BIOGRAPHY

Alex Minetto received the B.Sc. and M.Sc. degrees in Telecommunications Engineering from Politecnico di Torino, Turin, Italy and his Ph.D. degree in Electrical, Electronics and Communications Engineering, in 2020. He joined the Department of Electronics and Telecommunications of Politecnico di Torino in 2019 as research and teaching assistant and in 2022 as assistant professor. In 2015, he was an intern at European Organization for the Exploitation of Metereological Satellites (EUMETSAT), Darmstadt, Germany. His current research interests cover signal processing and advanced Bayesian estimation applied to Global Navigation Satellite System (GNSS) in space and critical infrastructure.

Brendan D. Polidori received the B.Sc. and M.Sc. degree respectively in Electronic and Telecommunications engineering from Politecnico di Torino, Turin, Italy, in 2019 and 2021. He joined the Department of Electronics and Telecommunications of Politecnico di Torino in 2022 as a research assistant. His research interests include methods of RF interference mitigation, detection and localisation, along with SDRs and digital signal processing.

Marco Pini received the M.Sc. and Ph.D. degrees in telecommunications engineering from Politecnico di Torino, Turin, Italy, in 2003 and 2006, respectively. He heads the Navigation Technologies research area with Istituto Superiore Mario Boella, Torino, Italy. Because of the experience gained on GNSS receivers and performance, he has been responsible for several R&D activities and projects. His research interests include the field of baseband signal processing of new GNSS signals, multi-frequency RF front-end design, and software radio receivers.

Fabio Dovis received his M.Sc. degree in 1996 and his Ph.D. degree in 2000, both from Politecnico di Torino, Turin, Italy. He joined the Department of Electronics and Telecommunications of Politecnico di Torino as an assistant professor in 2004 and since 2014 he is associate professor in the same department where he coordinates the Navigation Signal Analysis and Simulation (NavSAS) research group. He has a relevant experience in European projects in satellite navigation as well as cooperation with industries and research institutions. He serves as a member of the IEEE Aerospace and Electronics Systems Society Navigation Systems Panel. His research interests cover the design of GPS and Galileo receivers and advanced signal processing for interference and multipath detection and mitigation, as well as ionospheric monitoring.

ABSTRACT

Long-term stability and accurate time synchronization are at the core of timing network facilities in several critical infrastructures, such as in telecommunication networks. In these applications, timing signals disciplined by Global Navigation Satellite Systems (GNSS) receivers, i.e., One Pulse-per-Second (1-PPS), complement Primary Reference Time Clocks (PRTCs) by compensating for long-term drifts of their embedded atomic clocks. However, GNSS receivers may expose timing distribution networks to Radio Frequency (RF) vulnerabilities being the cause of possible degraded or disrupted synchronization among the nodes. This paper presents a test methodology assessing the resilience of new GNSS timing receivers to different classes of intentional RF interferences. The analysis of the results compares the effects of practicable spoofing and meaconing attacks on the 1-PPS generated by three Commercial off-the-shelf (COTS) GNSS timing receivers, currently employed in timing applications. On one hand, the results emphasised the robustness of State-of-the-Art (SoA) mitigation technologies compared to previous generations' devices. On the other hand, the vulnerability of SoA receivers to meaconing attacks highlights the limits of such mitigation solutions that may turn to severe effects on telecommunication networks' performance.

I. INTRODUCTION

Defense against spoofing and meaconing attacks have attracted the GNSS community since the early phases of such Positioning, Navigation and Timing (PNT) technology. A remarkable effort has been spent on identifying misleading behaviours affecting positioning and velocity solutions, and several algorithms and countermeasures have been developed to ensure protection from

Table 1: Absolute and relative synchronization requirements in 5G NR networks (Osseiran et al., 2016; Venmani et al., 2018; 3GPP, 2020). MIMO transmit diversity is highlighted as reference tolerance for 1-PPS misalignment in the current study.

Technology	Time-error Tolerance	Timing reference
Rack Unit - GrandMaster Clock (RU-GMC)	$\pm 1.5\ \mu$s	*Absolute*
Intra-band Non-Contiguous Carrier Aggregation (CA)	± 130 ns	*Relative*
Inter-Band CA	± 130 ns	*Relative*
Coordinated Multi-Point (CoMP)	± 130 ns	*Relative*
Intra-Band Continuous CA	± 65 ns	*Relative*
MIMO Transmit Diversity	± 32 ns	*Relative*

these events (Schmidt et al., 2016). Besides spoofed or disrupted positioning capabilities, malicious attacks can stealthily induce misleading time shifts (Dovis, 2015), thus representing a serious threat in those applications relying on accurate time information (Lu et al., 2021). Among these, precise and reliable time synchronization is a requirement for many critical infrastructures (Whitty and Walport, 2018; Skey, 2017; CISA, 2019). Specifically, modern telecommunication networks are lowering accuracy bounds to guarantee phase synchronization between different base stations, thus enabling an assortment of groundbreaking high-performance solutions. A set of carrier-phase-related technologies and their synchronization requirements are summarised in Table 1. This study mainly refers to *relative* time synchronization between nodes that leverage the generation of timing signals simultaneously clocking at different locations. As a reference, we consider that *relative* synchronization error among network nodes must be within ± 32 ns for the attainment of Multiple-Input Multiple Output (MIMO) in 5G New Radio (NR) infrastructures. Technical justifications for such synchronization requirements are out of the scope of this work and are left to specialized literature on the topic (Access, 2014; Farkas et al., 2019; Li et al., 2017; Osseiran et al., 2016; Infinera, 2022; Venmani et al., 2018). In a modern network infrastructure, sub-microsecond synchronization requires a multiplicity of reliable clocks such as Rubidium (Rb) and Cesium (Cs) atomic oscillators. However, these technologies are too expensive to be deployed throughout multiple nodes (Commissariat, 2021) in vast network infrastructures. To overcome deployment costs, some atomic clocks deployed in timing networks are being replaced or complemented by less-expensive GNSS receivers that provide a stable timing signal, namely the 1-PPS (Pini et al., 2021; Keten, 2021). The 1-PPS is a Transistor-Transistor Logic (TTL) electrical signal with a width of less than one second and a sharply rising or abruptly falling edge that accurately repeats once per second. High-quality, reliable 1-PPS generation turns any GNSS receiver into a timing source capable of mitigating the long-term drift of 10 MHz reference signals provided by Primary Reference Time Clock (PRTC) (Bauch and Whibberley, 2017; Niu et al., 2015). Therefore, a growing interest is paid towards complementing expensive atomic clocks with advanced solutions such as enhanced GNSS-equipped PRTC (ePRTC) by also embedding secure timing protocols to guarantee high-accuracy time synchronization, e.g., White Rabbit Precise Time Protocol (WR-PTP) (Girela-López et al., 2020; Lipiński et al., 2011). However, the presence of GNSS receivers' antennas exposes the network to the growing risk of RF attacks (Papadimitratos and Jovanovic, 2008; Falletti et al., 2019), thus introducing a significant security flaw in the timing infrastructure. This research sought to determine the effects of intentional, feasible RF interference on GNSS SoA timing receivers, intending to assess the reliability of their generated 1-PPS. While jamming signals are easily detected by modern interference mitigation algorithms, meaconing and spoofing attacks can still act by stealthily forcing a 1-PPS shift in victim receivers. These two modern-day threats were investigated in this work by also considering *preemptive interfering actions* (e.g., receiver reset, multi-band jamming) against the GNSS receivers under test.

The rest of this Section recalls the fundamentals on GNSS-based time synchronization by means of 1-PPS generation and clarifies how RF attacks may impact such an output timing signal. Section III presents the selected tests and their experimental procedures along with schematics of the testbed setup. Section IV presents the effect observed on the 1-PPS provided by each Device Under Test (DUT) during the experimental campaigns. Contextually, it summarizes the different attacks and the associated vulnerability of the DUTs. Eventually, Section V tracks the current robustness of SoA receivers while proposing future advances for next-gen, resilient timing receivers.

II. BACKGROUND

1. GNSS-based Time Synchronization

Jointly to being a well-known positioning and navigation facility, GNSS constellations constitute accurate time and frequency transfer systems that can be employed to guarantee ns-level accuracy in both *relative* and *absolute* synchronization between satellites and receivers timescales (Defraigne, 2017). The structures of GNSS signals are indeed functional to the generation of local timing signals by GNSS receivers, i.e., the 1-PPSs, that can be assumed synchronous on a global scale. GNSS-disciplined 1-PPSs, emitted at different nodes, can be used as input signals for disciplining integrated clocks (i.e., ePRTC) that independently run at different locations (Chowdhury, 2021). This paradigm allows to exploit GNSS time and frequency transfer to synchronize

a sparse network of nodes with a sub-microsecond accuracy, even among COTS receivers.

a) Principles of GNSS Timing and Synchronization

Global Positioning System (GPS), Galileo, GLONASS and Beidou transmit Pseudo Noise (PN) ranging codes, often referred to as Pseudo-Random Noise (PRN), that support both ranging and time synchronization of the receivers. Independently from the different signal plans adopted by each constellation, GNSS satellites keeps the carrier, PN codes, subcarriers and data edges aligned for each of their navigation signals. The signal transmitted by a generic i-th satellite belonging to an unspecified GNSS constellations reaches the receiver's antenna and can be modelled as

$$s_{RF,f_c}(t) = \sqrt{P_{R,i}} D_i(t-\tau_i) C_i(t-\tau_i) S(t-\tau_i) \cos\left(2\pi \left(f_c + f_{d,i}(t)\right) t + \triangle\Phi_i\right) + n(t) \tag{1}$$

where $P_{R,i}$ is the received signal power, $D_i(t)$ is the navigation data bit stream, $C_i(t)$ is the pseudo-random code sequence, $S_i(t)$ is the subcarrier, f_c is the carrier frequency shifted by the observed Doppler shift $f_{d,i}$, τ_i is the propagation delay and $\triangle\Phi_i$ is the phase offset. Finally, $n(t)$ is the thermal noise contribution. Secondary (i.e., Galileo) or overlay (i.e., GPS) codes are omitted for the sake of brevity.

The code tracking of a single navigation signal would be enough to emit regular 1-PPS signals. Furthermore, high-accuracy disciplination of the 1-PPS can be further achieved by means of carrier phase tracking. However, unknown propagation time and local clock biases at the receiver will lead to misaligned 1-PPSs for each received signal and a further overall bias w.r.t. the actual GNSS reference time. Therefore, the generation process of the 1-PPS makes use of the i) PN code with its phase offset, ii) the message preamble, and iii) the navigation data to output a clock signal that provides *absolute* synchronization to the constellation timescale. The code phase offset observed at the receiver depends on the following terms that influence pseudorange estimation

- Satellite Clock bias, δt_s: is compensated through a first or second order polynomial of the clock bias correction parameters carried by the navigation message, i.e., clock offset, clock drift and clock drift rate
- Receiver Clock bias, δt_u: common to all the received signals, is estimated through the Position, Velocity and Time (PVT) algorithm
- Atmospheric delays, δt_a: can be compensated through the ionospheric parameters included in the navigation message and troposphere models at the receiver
- Propagation time, τ_i: is reflected into a number of integer code replicas of duration δt_p, and a fractional part, δt_c, that is estimated by code correlation and finely tracked by receiver's Delay Lock Loop (DLL)

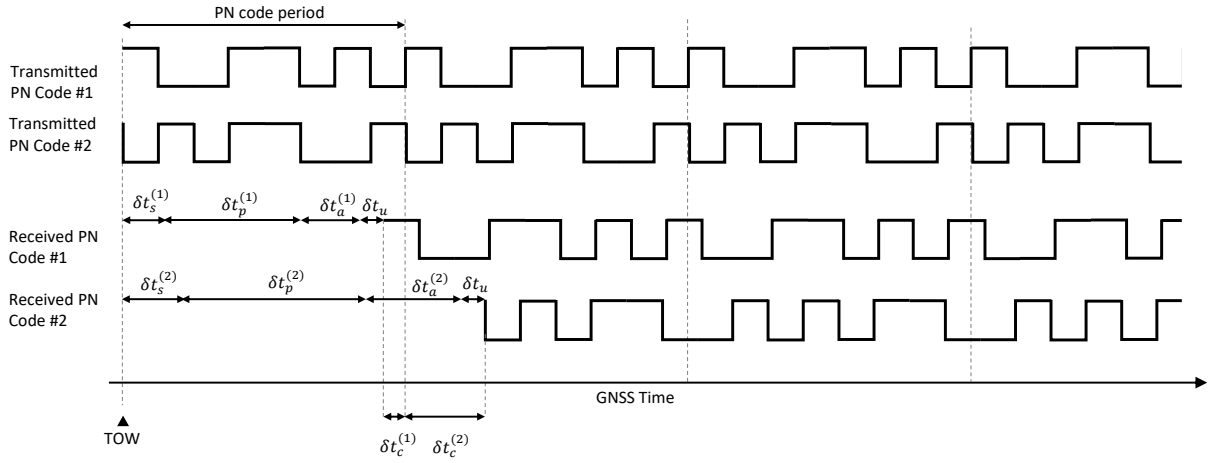


Figure 1: Pictorial diagram of the misalignment between two received PN codes at the same GNSS receiver. 1-PPS alignment to the corresponding GNSS constellation requires the estimation of the code offset w.r.t. the transmitting time (TOW) (Pini et al., 2012). Code phase delay, δt_c, is recovered by receiver tracking loop for the 1-PPS.

Figure 1 shows the different delay contributions to the signal propagation and code phase offset for a pair of simplified spreading codes. The diagram takes as a reference the 1-PPS of the constellation that provides the reference timescale, depicted as dashed vertical lines. To achieve time synchronization to a given GNSS constellation a receiver must account for all the listed delays.

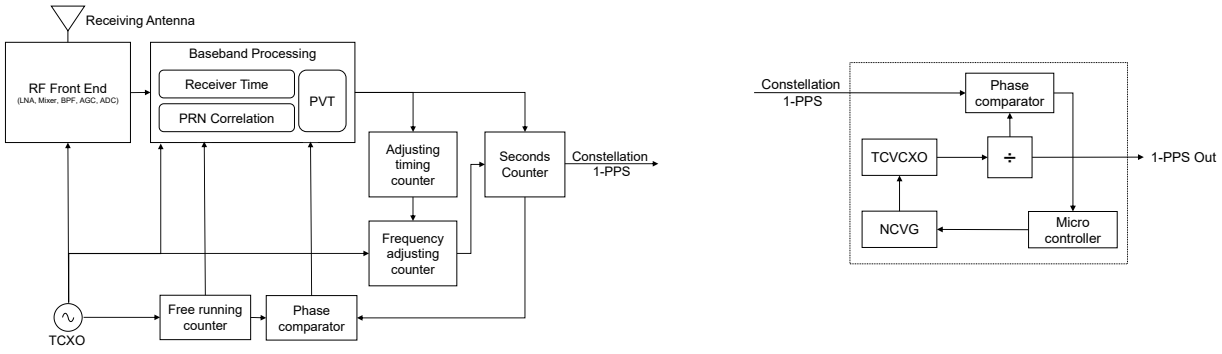


Figure 2: High-level block diagram of a 1-PPS generation architecture in a GNSS receiver (a) and of an external DO (b). Specialized GNSS timing receivers typically integrate the two architectures by transferring the constellation PPS to the DO. The DO makes use of a Numerically Controlled Voltage Generator (NCVG), along side a Temperature Compensated Voltage Controlled Crystal Oscillator (TCVCXO).

The receiver can eventually steer the local oscillator or an external GNSS-Disciplined Oscillator (DO) to output the physical 1-PPS signal whose wavefronts are aligned to the GNSS reference timescale with a given uncertainty. Any action that can alter the aforementioned delays may affect the disciplination of the output 1-PPS.

b) 1-PPS hardware generation

A sample, high level architecture for the generation of the 1-PPS is shown in Figure 2a, as patented in (Kazunori, 2015). A combination of counters and phase detectors inside the receiver allows to take advantage of both the short term stability of the local clock and the long term stability of the constellation 1-PPS. A local 1-PPS, generated from the Temperature Compensated Crystal oscillator (TCXO), is used in combination with the 1-PPS extracted from the incoming signals, that we refer to as "constellation" 1-PPS. The mechanism of re-positioning the initial code sample for each correlation interval is critical. It provides a structure to align the boundary of a millisecond, data bit, and second in the incoming digital signal (Chun, 2002). It is of paramount importance in obtaining the data bit synchronization and frame synchronization for data demodulation, while also being the fulcrum of the "constellation" 1-PPS generation (Chun, 2002). The "constellation" 1-PPS from the signals is matched with a timing corresponding to the beginning of a code pattern in the PRN code, which repeats every millisecond (Doberstein, 2012). Doppler rate on PRN chips induces an irregular duty-cycling of the PRN code, thus it must be compensated to grant high-accuracy alignment (Foucras et al., 2014). Once each channel of the receiver is aligned with the code phase that it is tracking, the receiver clock bias can be estimated through the PVT, thus determining the aforementioned "constellation" 1-PPS.

If taking in consideration timing receivers with their higher costs, it is reasonable to assume that they could be equipped with an additional DO to further increase stability of the generated 1-PPS. We can see an example of how an additional DO could be used in the system in Figure 2b. We can find an application of this type in (Osterdock et al., 1995) and (Gregor, 2014), in both the DO is a 10 MHz clock, that can also be used as an output.

By assuming a continuous adjustment of the 1-PPS wavefronts and a conventional rising edge in the origin of the time axis, i.e., $t = 0$, we model each pulse as a delayed rectangular pulse

$$\Pi_{\text{PPS}}(t) = \Pi\left(t - \frac{T_{\text{PPS}}}{2}\right) = \begin{cases} 0 & t \leq 0 \\ A & 0 \leq t \leq T_{\text{PPS}} \\ 0 & T_{\text{PPS}} \leq t \leq T_{\text{DT}} \end{cases} \tag{2}$$

where T_{PPS} is the pulse duration and it can be typically customised in high-end receivers, T_{DT} is the duty cycle duration, and A is the amplitude of the electrical pulse, in volts. T_{DT} is equal to 1 s by definition of 1-PPS. An ideal periodical square wave with a duty cycle of 1 s is hence the expected output of a receiver 1-PPS interface, as shown in Figure 3. In real implementations, approximated waveforms may be used to guarantee physical feasibility of $\Pi_{\text{PPS}}(t)$. 1-PPS signal shaping is achieved by means of steep roll-off factor, while the duty cycle is continuously adjusted by the steering of the oscillator. The $PPS(t)$ signal shown

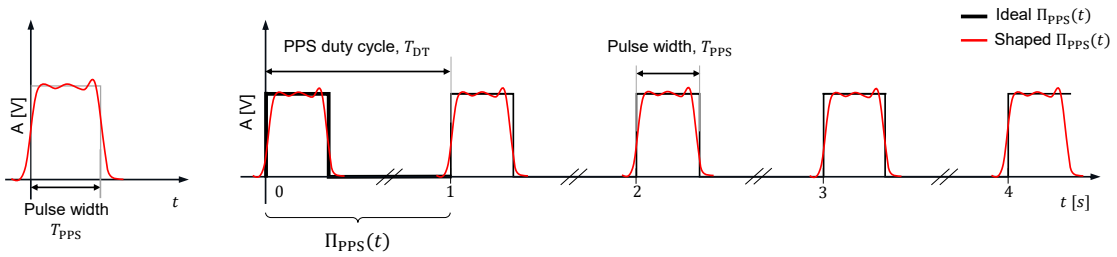


Figure 3: Pictorial view of 1-PPS showing its characteristics, i.e. duty cycle, amplitude and pulse width (not to scale). Black and red lines represent ideal and realistic pulse shaping.

in Figure 3 can be modelled as a train of (2)

$$\mathrm{PPS}(t) = n(t) + A \sum_{k=-\infty}^{\infty} \Pi_{\mathrm{PPS}}(t - kT_{\mathrm{DT}} + a(t)) \tag{3}$$

where $n(t)$ models the amplitude thermal noise of the output interface, being typically negligible w.r.t. the nominal output voltage of the pulse. The term $a(t)$ is a random variable that models the noisy correction term introduced by the 1-PPS generation chain to keep the alignment of each new pulse to the constellation 1-PPS. The probability density of $a(t)$ may follow different distributions according to the adopted hardware/software architecture for the 1-PPS generation. However, a non-zero mean value at a given time instant causes a time-shift of the pulse and is assumed to reflect the effects of malicious timing attacks. The index k assumes integer values to describe the periodicity of the signal with duty cycle T_{DT}.

2. Theoretical modelling of interference signals and effects on the 1-PPS

To better understand how each method of interference affects the receiver, the fundamentals of the adopted interfering signals are hereafter recalled (Dovis, 2015).

Frequency Modulated Jamming signal

Jamming, in the form of a chirped signal, adds additional power to the GNSS signal spectrum, thus interfering with nominal acquisition and tracking operations of the receiver. An example of a cosine, linearly frequency modulated chirp is defined as

$$w(t) = A_j \cos(2\pi f(t)t + \phi) \tag{4}$$

where A_j is the amplitude of the sinusoidal term $f(t) = \frac{k}{2}t + f_0$ and where, in turn, k is the frequency rate defined as $(f_1 - f_0)/T$, and T is the time that it takes to sweep from the initial frequency f_0 to f_1, i.e., sweep time. The term ϕ identifies the initial phase offset. Different modulation laws are exploited by current, documented jamming signals. However, Linearly Frequency-Modulated (LFM) chirps, still represent one among the most popular jamming signals. When under jamming, the receiver obtains a signal as

$$y_{RF,f_c}(t) = \bar{s}_{RF,f_c}(t) + \sqrt{2P_j}w'(t) + n(t) \tag{5}$$

where $\bar{s}_{RF,f_c}(t)$ is a noiseless GNSS legitimate signal derived from (1), P_j is the received jamming power and $w'(t)$ is a continuous, cyclic jamming signal with a given periodicity. Jamming signals may introduce additional noise in the disciplined 1-PPS due to a reduction of the Carrier-to-noise ratio, thus to an increment of the tracking jitter. Given that similar phenomena can be automatically detected by modern anti-jamming algorithms, these signals cannot be used to stealthily alter time keeping at the receiver. Furthermore, their effect on the 1-PPS is not under control. Therefore, in this study chirped jamming signal will be used as a preemptive action to weaken receivers' tracking loops or disrupt other available bands while spoofing is operated.

Meaconing

Meaconing signals consist of an amplified and delayed version of the legitimate signals. In the case of malicious attacks it is typically performed by retransmitting the received GNSS signals to the victim receiver from a remote location. The receiver then obtains the sum of the legitimate and delayed signals as

$$y_{RF,f_c}(t) = \bar{s}_{RF,f_c}(t) + \sqrt{2P_m}\bar{s}_{RF,f_c}(t - \tau_m) + n(t) \tag{6}$$

where P_m is the received meaconing power, that ideally is greater than that of the legitimate signals in order to fool the receiver. When the receiver acquires and tracks meaconed GNSS signals, the code-phase delays of the incoming PN codes are equally altered w.r.t. to the legitimate signals. This effect injects a common bias to all the pseudorange measurements that is extracted

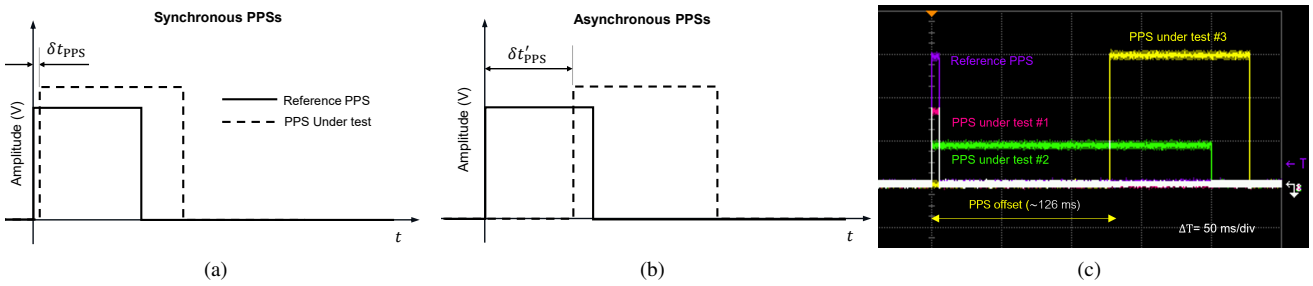


Figure 4: Pictorial view of the behaviour of a GNSS-disciplined 1-PPS in nominal conditions (a), under a malicious "timing attack" (b) and real example of oscilloscope measurement showing 3 synchronous 1-PPS and a further misaligned one (c). Reference PPS is used to verify relative synchronization among the DUTs.

through the PVT estimation along with the local clock bias, δt_u. When the meaconer is receiving the legitimate signal at the same location of the victim, no effects on the position and velocity estimates can be observed, while time is instead shifted.

Non-coherent spoofing

A single spoofing signal that imitates a legitimate GNSS one can be an arbitrarily-delayed version of (1) or a independently-generated one. The difference may lie in a set of altered data transmitted through the navigation message. Spoofing signal is identified hereafter through the apex by means of

$$s\prime_{RF,f_c}(t) = \sqrt{P_{R,l}} D'(t-\tau')C(t-\tau')S(t-\tau')\cos(2\pi f_c t + \Delta\theta') + n(t) \tag{7}$$

where D' and τ' identify altered navigation bits and propagation delay, respectively. The receiver then obtains the sum of the legitimate and spoofing signals as

$$y_{RF,f_c} = \bar{s}_{RF,f_c}(t) + s'_{RF,f_c}(t) + n(t) \tag{8}$$

The definition can be extended to an arbitrary set of GNSS signals with the aim of partially or fully replacing concurrent legitimate constellation. If the spoofing delay, τ', is larger than the ephemeris validity, coherency checks operated by the receiver may allow for detection.

a) Interference effects on 1-PPS generation

As discussed in Section II.1 b) the 1-PPS is generated through a combination of elements. Among these, the Constellation 1-PPS is considered. By degrading the quality of the received GNSS signals or by transmitting fake signals towards a victim receiver, the attacker may induce non-negligible variance in the estimated clock bias or introduce a further bias that is interpreted as a local time shift. If the receiver finds an incorrect solution for the PVT, meaning also for the clock bias, the system adjusts the 1-PPS incorrectly, introducing an error into the system. If the receiver position is known a-priori by the attacker, insidious repercussions will only affect the time estimation, thus being possibly undetectable.
Figure 4a shows a nominal condition in which a 1-PPS under test is roughly aligned to the reference 1-PPS. Figure 4b shows a larger 1-PPS offset that may be induced by estimation errors or by malicious attacks. Figure 4c, eventually shows a real screenshot of an oscilloscope measuring 4 PPSs at the same time and showing both the conditions depicted in Figures 4a and 4b in a real, experimental scenario. In the case of coherent spoofing, the receiver would calculate a correct position but it could be induced into computing an increasingly incorrect time, which in critical infrastructures such as power grids or telecommunication networks would wreak havoc.

Therefore, the proposed testing methodology aimed at causing a shift of the 1-PPS at the victim receivers without altering their position and velocity estimates. Without specific algorithms to detect the erroneous behaviour of the estimated clock bias or clock drift, such attacks led to a local time shift and an asynchronous 1-PPS w.r.t. the chosen time scale. In Figure 4c we can see these repercussions. From a timing network standpoint, these attacks can trigger a de-synchronization of the node.

III. METHODOLOGY

1. Experimental Setup

Within this study, three COTS, multi-constellation, timing GNSS receivers were considered as Devices Under Test (DUTs) for the analysis. We can see the characteristics for each in Table 2. Further commercial details about the receivers are omitted on purpose. A fourth GNSS receiver, referred to as RX0 or *reference receiver* (same device as RX3), was used to generate

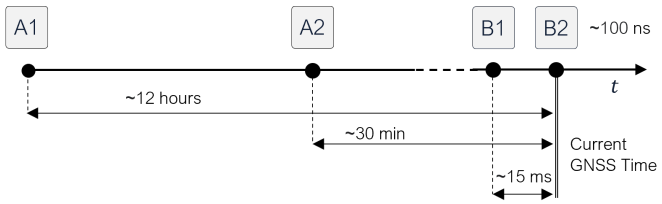


Figure 5: Reference timeline for the classification of the attacks according to the proposed criteria.

a reference 1-PPS signal under nominal conditions (i.e., without interfering signals). The different 1-PPSs generated by the receivers are in line with (3), but each with its own pulse width and amplitude. All the receivers were fed by a multi-band GNSS antenna, and illegitimate signals were injected through a RF, two-way power combiner whose output was split to feed RX1, RX2, and RX3 simultaneously. Output 1-PPSs were monitored in real-time through a multi-channel oscilloscope to continuously verify the alignment of 1-PPSs wavefronts.

Table 2: Receivers used in the study and globally referred to as DUTs in the text.

	Firmware	Channels	Bands Covered		Timing accuracy	Timing Jitter
RX1	2018	72	single band	L1	≤ 20 ns	± 11 ns
RX2	2019	184	multi-band	L1/L2/E5b	≤ 5 ns	± 4 ns
RX3	2021	448	multi band	L1/E1, L2, L5/E5a-E5b	≤ 2 ns	± 4 ns

2. Time coherence as a feasibility metrics of malicious attacks

Performing effective meaconing and spoofing attacks against GNSS receivers generally requires niche expertise. However, the affordable costs of mass-market electronics (e.g., digital front-end) and the availability of commercial and open-source software makes the risk tangible. In this paper, we propose a further level of classification for spoofing and meaconing attacks by blurring the line between the traditional definitions. By assuming a known receiver location, we rely on two main aspects: i) the required technology and associated cost to pursue the attack (i.e., hardware and software) (Psiaki and Humphreys, 2016); ii) the time coherence of the illegitimate signals w.r.t. the current GNSS time at the victim location. While the first aspect is mainly related to the cost of the malicious operation, the latter is related to the attacker's expertise and to the deployment of the action itself. Figure 5 shows a timeline on top of which the following classes of attack are reported

A. *Non-coherent spoofing* through record and playback of live signals using Ettus Research (ER) Universal Serial Radio Peripheral (USRP) N210. Different ageing of the recorded signals were considered, as shown in Figure 5. For the A1 test older recorded signals were used and for the A2 test more recent recordings.

B. *Digital* (B1) or *analog meaconing* (B2) obtained by retransmitting delayed live signals and performed through USRP N210 in transceiver mode (B1), and by means of a delayed and amplified line (B2), respectively.

3. Preemptive malicious actions to maximize susceptibility

For each attack listed above and indicated in Figure 5, we identified two preemptive actions to further stress the DUTs and assess they ability to mitigate or annihilate the interference.

- *Jamming interference*: a multi-band chirped jamming signal, as described in (4), was preemptively transmitted until 1-PPS generation was interrupted. The spoofing and meaconing attacks were initiated while the jamming was still active. During the meaconing and spoofing attacks that involve only transmitting replica signals on L1/E1, the jammer is kept active on all other frequencies (L2/E5b). Equations (6) and (7) show how the single frequency meaconing and spoofing signals are obtained by the receiver.
- *Receiver reset* (software cold restart): a software reset is applied which forces a memory flush and drives the receivers to a cold start acquisition of GNSS signals. The action can be performed remotely by assuming a concurrent network vulnerability, e.g., violation of authenticated access to the receiver configuration, in the timing infrastructure.

The two preemptive actions require in one case no experience, and in the other high skills to afford cyberattacks to the receiver configuration (Berbecaru and Lioy, 2022). The distinction of complexity of the two makes the probability of occurrence a variable to be considered in possible threatened scenarios.

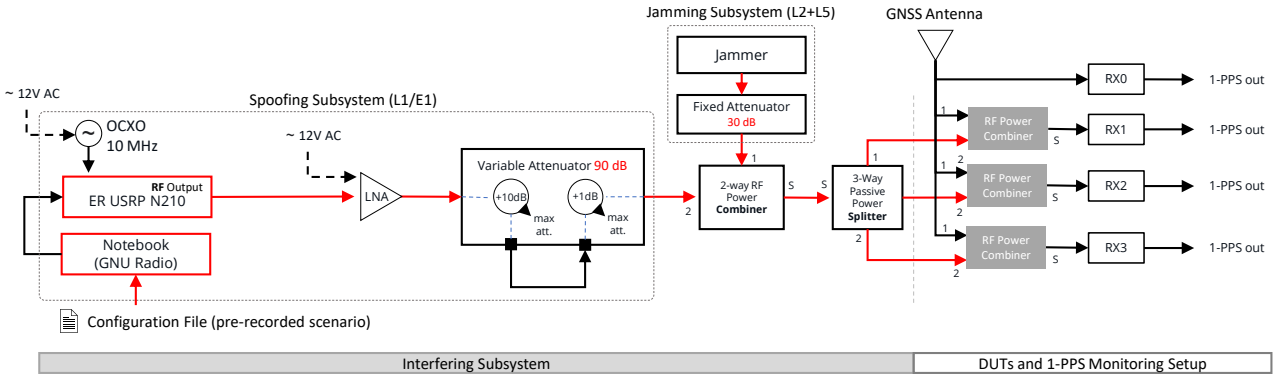


Figure 6: Scheme of the testbench for non coherent spoofing tests (A1, A2). The jamming subsystem located at the top of the scheme is activated as preemptive action.

4. Test procedures

Specific test procedures were designed to intentionally alter the time keeping of the receiver and to force a time-shift on the 1-PPS generation. The tests leveraged incremental power steps to identify a point of non return for the 1-PPS bias, as depicted in the example of Figure 4c. 1-PPS calibration was ensured before running the tests. Attacks were declared effective once the time shift, δt_{PPS}, induced to the 1-PPS w.r.t. to the reference one stably overcame tolerance requirements established for phase synchronization in MIMO applications for 5G networks, as provided in Table 1.

a) Non-coherent spoofing

Often referred to as *simplistic* spoofing (Dovis, 2015), it can be achieved with COTS RF front-ends, Software Defined Radio (SDR) equipment, and open source signal generators. Therefore, it represents an affordable methodology to execute timing attacks. In our test, pre-recorded scenarios were replayed with the aim of shifting absolute time at the victim devices. In Figure 6, we can see the setup used for the non coherent spoofing attacks against the DUTs. From left to right we first find the combination of notebook and USRP N210, that are used to record a legitimate GNSS signal stream from an antenna and replay it at a later date/time. The signal gain is directly controlled through the GNU Radio interface on the notebook, that allows for fine adjustments of the input and output power. Implementation details are omitted to avoid spreading sensitive information on feasible attacks. The spoofing attacks were designed to incorporate a preemptive jamming strike on all frequencies before the spoofing signal was introduced. This was expected to force the receiver into acquisition mode and possibly induce a higher rate of disruptive attacks. During the attack, jamming is utilised to block all frequencies on which spoofing is not occurring. The interfering signals are then combined with the legitimate GNSS signals and are fed to the DUTs.

b) Analog Meaconing and Digital meaconing

Analog meaconing emulates the re-transmission of a signal from a pre-defined location with the ability to control the transmitting power. Similarly to spoofing, it aims at forcing the receiver to track delayed signals, thus shifting its 1-PPS accordingly. We can see the scheme for analog meaconing in Figure 7. The legitimate GNSS signal is first amplified using a Low Noise Amplifier (LNA) and then propagated through a RF cable, that delays the signal. As seen in (6), with analog meaconing all frequencies and all signals are received, delayed and re-transmitted, thus being a multi-frequency attack with a low cost. The delay is estimated approximately as $\tau_M = \frac{l}{\frac{2}{3}c}$, where c is the speed of light and l is the cable length in meters. Using this formula the expected 1-PPS offset should be $\delta t_{\text{PPS}} \simeq 5\,\text{ns}$ for each meter of cable used. Connectors, adaptors and combiners introduce additional delay and attenuation to the signal. Once the signal exits the RF cable, it is passed through a stepped attenuator that is used to control the power, with attenuation granularity of 1 dB. The delayed and attenuated output is then fed to the DUTs.

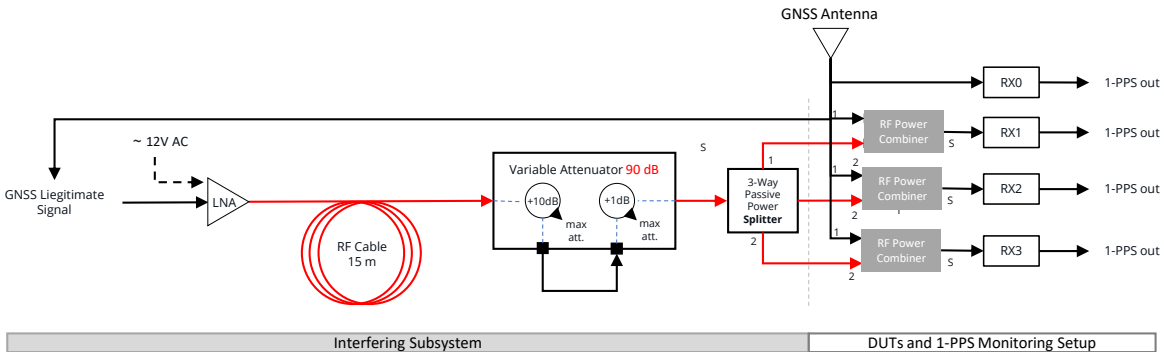


Figure 7: Scheme of the testbench for the analog meaconing (B1) using a coaxial cable to delay the legitimate signal and use it as interfering signal.

Digital meaconing implies an Analog to Digital Conversion (ADC) and a subsequent Digital to Analog Conversion (DAC) operated by a specific SDR device. It is performed utilising the combination of GNU Radio and the USRP N210. We called this method Meaconing in the Loop (MITL), given the internal wiring design of the USRP. We can see the scheme for MITL in Figure 8. Using GNU Radio, the USRP can be configured to receive a signal and "immediately" re-transmit it. The time offset introduced by the USRP was approximately 12.5 ms, later discussed and seen in Section IV. In order to optimise the ADC/DAC of samples from the USRP, an external reference clock signal was provided by a 10 MHz Oven Controlled Crystal Oscillator (OCXO).

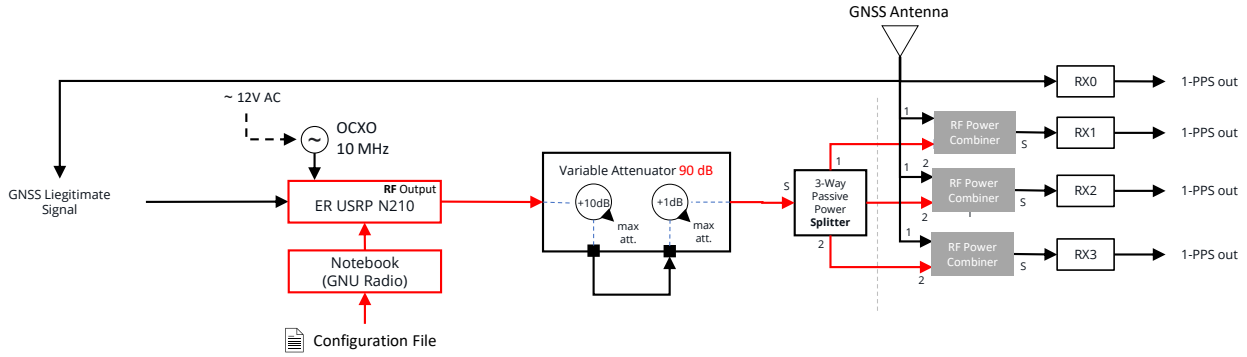


Figure 8: Scheme of the testbench for MITL (B1) using ER USRP N210 to delay the legitimate signal.

IV. RESULTS AND DISCUSSION

Preliminary test campaigns highlighted a remarkable resilience of all the DUTs within the proposed test schemes. However, a number of effective attacks have been carried out that exhibit how such schemes can introduce time shifts in the 1-PPS, thus causing a de-synchronization of the timing node.

1. A1 results (spoofing with long replay delay)

This attack shows the difference between modern SoA receivers w.r.t. older generation ones in terms of interference detection and mitigation. Using only spoofing with a long delay (i.e., no jamming or reset preemptive actions), only RX1 is fooled into following the old signals. As an example, Figure 9 shows that RX3 was not vulnerable to the spoofing attack (A1) even after both the preemptive jamming strike, during which the 1-PPS generation was interrupted, and the continued jamming on L2/E5b. Once the jamming is removed, RX3 is able to re-establish a correct 1-PPS generation (synchronous to the reference constellation 1-PPS). When attacked with a combination of jamming and spoofing, both RX1 and RX2 were affected by a non negligible time shift and they steadily disciplined a biased 1-PPS. This shows how older generation receivers are susceptible to a combined jamming plus spoofing attack. It is worth recalling that many of these receivers are in use in critical infrastructures,

thus representing a potential vulnerability of the timing facility (Falletti et al., 2019). Furthermore, RX3 interpreted the spoofing signal as generic interference and not as spoofing threat. This classification is significant, since the receiver is also able to detect coherent spoofing. One method to evaluate if incoming signals belong to a spoofer is to analyse the power levels of each different channel. Simplistic spoofing can be mitigated by using a real time clock inside the receiver. During the preemptive jamming the receiver is forced into acquisition, and once it is removed the receiver restarts the acquisition and tracking procedures. It then checks the time extracted from the navigation message of the spoofed signal and whether it matches, within a given margin, with the real time clock in the receiver. If a threshold is exceeded then the signals are rejected and classified as spoofing. If the receiver is forced to reset while the spoofing is active, then there is no chance of it being able to recognise which signals are authentic and which are not, since the legitimate signal power is lengths below the spoofing signal power. This leads to all receivers generating an incorrect 1-PPS.

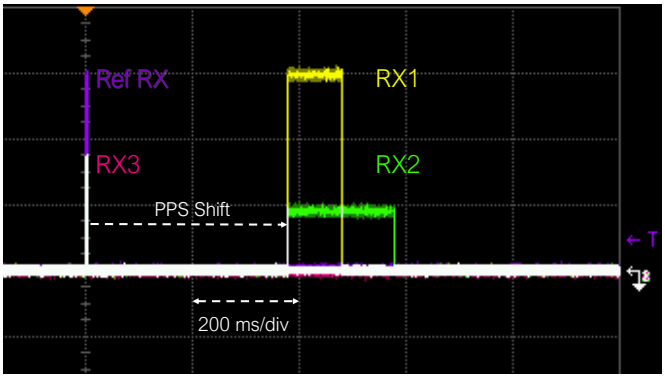


Figure 9: Realization of the effects of A1 effective timing attack supported by preemptive jamming on all frequencies and continued jamming on L2/E5b against the DUTs . A time shift of about 400 ms is shown for RX1 and RX2.

2. A2 results (spoofing with short replay delay)

This attack uses signals captured about 30 minutes prior. In Figure 10 we can see the effect of only the spoofer (USRP) being used. RX1 is fooled into tracking the spoofing signals, the parameter that determined the success of the attack was the spoofing signal power, likewise as for the previous test. Once it overpowered the legitimate signals, RX1 was forced into acquisition, as if attacked by jamming, and then locked on to the incoming spoofing signals. This overwhelming power, forces the receiver to lose lock on the legitimate GNSS signals and follow the incoming spoofing ones, even if these are non-coherent with the legitimate signals. When both preemptive jamming and continued jamming on L2/E5b are used, then also RX2 is vulnerable to this short delay spoofing attack, as previously seen in the long delay attack A1. During this attack, similarly to what happened in A1, RX3 was able to identify and mitigate the spoofing signals, while RX1 and RX2 suffered a shift in their 1-PPS. An attack with a short replay time poses a serious risk to a fixed node, as an attacker could prepare it in a short time period and possibly from a remote location. There was some difficulty in replicating an effective spoofing attack for RX2 on which the resulting success of a spoofing attack is highly dependent on the power ratio between legitimate and spoofed signals. As shown later in Table 3 we also tested this attack adding a receiver reset when introducing the spoofing signals to the system. A reset guaranteed an effective outcome on all receivers, since none are able to distinguish which signals are legitimate and which are not.

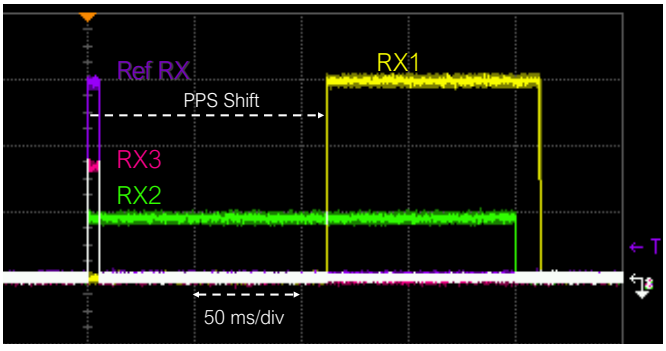


Figure 10: Realization of the effects of short delay spoofing without jamming or reset (A2) on RX1. RX2 and RX3 instead are not affected.

3. B1 results (meaconing in the loop)

MITL using the USRP N210 without additional jamming or reset had severe effect on RX1 and RX2, while RX3 was able to continue normal 1-PPS generation, ignoring the delayed signals. This can be attributed to the fact that the signals are delayed in the ms order of magnitude. This large delay exceeds any reasonable signal propagation multipath. We can see in Figure 11 how the different 1-PPSs are shifted w.r.t the reference 1-PPS during a simple meaconing attack. Both RX1 and RX2 present a shift of 12.5 ms, that can be attributed to the internal delays created by the USRP. As in the spoofing attacks, the signal power was the main contributing parameter to effective attacks against the receivers. The receivers are able to track the legitimate signals until the meaconing power exceeds them, which acts similar to jamming and forces the receivers into acquisition. When the receivers lose the legitimate signals their 1-PPS is also affected, RX1's 1-PPS starts to drift indicating a holdover mode, while RX2's 1-PPS is terminated after signal loss. When a preemptive jamming strike is used, combined with a continued jamming on L2/E5b, the RX3's 1-PPS is effectively shifted, preceded by a short anomaly. The meaconing signals are introduced to the system as jamming on L1/E1 is removed, while that on L2/E5b remains, this prevents the receivers from generating a correct 1-PPS using the L2/E5b signals. In Figure 12a we can see how RX3's 1-PPS initially jumps backwards, to then jump to the "correct" meaconing 1-PPS position in Figure 12b. RX3 disciplined a shifted 1-PPS for only a few minutes ($\leq$ 10) while presenting errors such as no PVT and spoofing flags. RX1 and RX2 instead continued generating a shifted 1-PPS until the meaconing signals were removed from the system. In order to achieve an effective meaconing attack using the USRP on RX3, the power of the meaconing signals needs to greatly exceed that of the legitimate signals and slowly be lowered to the point of being accepted by the receiver, this combined with continued jamming on L2/E5b. This tuning process in a real world attack would be difficult to achieve, since a direct connection to the receiver is necessary to observe its behaviour. None the less, if an attacker is able to access the user interface, such an attack can be perpetrated.

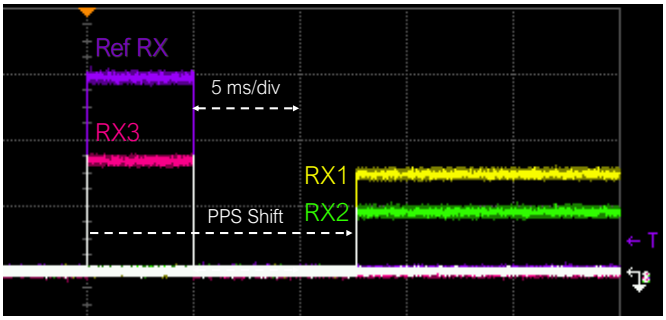
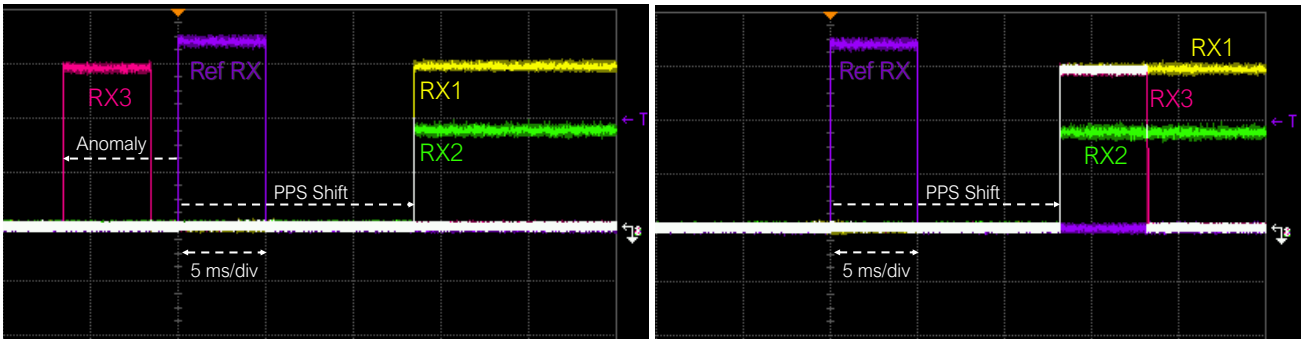


Figure 11: Effects of MITL (B1), on RX1 and RX2 with 1-PPS positive shift $\delta_{\text{PPS}} > 12\,\text{ms}$. RX3 keeps accurate synchronization to the reference timescale with a negligible synchronization uncertainty.



(a) (b)

Figure 12: Realization of the initial (a) and subsequent (b) effects of a MITL (B1) attack with preemptive jamming on all frequencies and a continued jamming on L2/E5b along with the meaconing signals. All the DUTs experience a positive 1-PPS shift with $\delta_{\text{PPS}} > 12\,\text{ms}$. An anomaly for RX3 occurred when jamming is slowly removed as meaconing is introduced while its power is modulated (a).

4. B2 results (Analog Meaconing)

This attack proved to be the most insidious, shifting the 1-PPS by more than 100 ns and never being detected. In Figure 13 we can see how the receiver clock bias is affected by analog meaconing. There are two sudden jumps that occur when the

interfering signals are introduced and removed. When introduced to the receiver, being delayed signals, the receiver's clock needs to "slow down" in order to compensate. We can also explain the positive spike since the receiver's clock bias would indicate a large positive difference w.r.t the time contained in the delayed signals. This explains the first negative correction in receiver clock bias. When the interfering signals are removed the receiver locks on to the legitimate signals and therefore needs to "accelerate" its internal clock to match them. This can be seen as the positive adjustment after the negative spike. Therefore we can explain the negative spike since the receiver clock bias would be behind the legitimate system time extracted from the navigation message. We can see the effect of the attack on the 1-PPS generation of the receivers in Figure 14. A non negligible shift of more than 100 ns is introduced in all DUTs. In (Marnach et al., 2013) a method for detecting this type of meaconing attacks is proposed, based on the monitoring of the receiver clock bias, and as we can see from Figure 13 there is certainly an opportunity to detect this type of interference. RX3 interpreted the introduction of the delayed signals as an increased multipath in the signal. During the attack the multipath mitigation values for each signal were between $+5$ m and -10 m, and after the attack is over, there is a notable remaining shift between $+3$ m and $+10$ m. Comparing this scenario with the MITL (B1), we can see how the difference in delay affects the success rate of the attack. The higher the delay the lower the probability of an effective attack. This does not exclude that, in combination with jamming, the attacks are not effective, simply that the receivers can detect the meaconing signals given the larger delay.

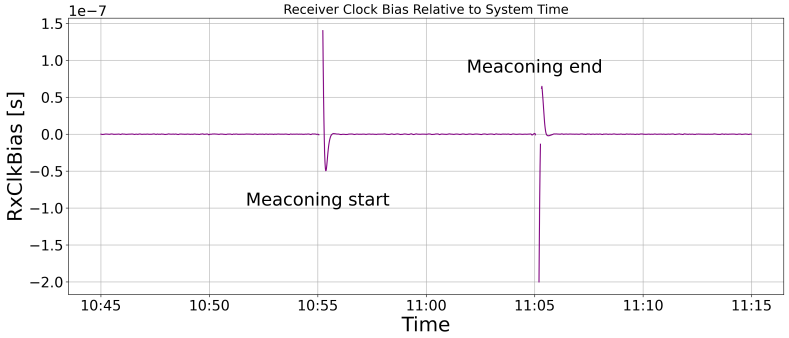
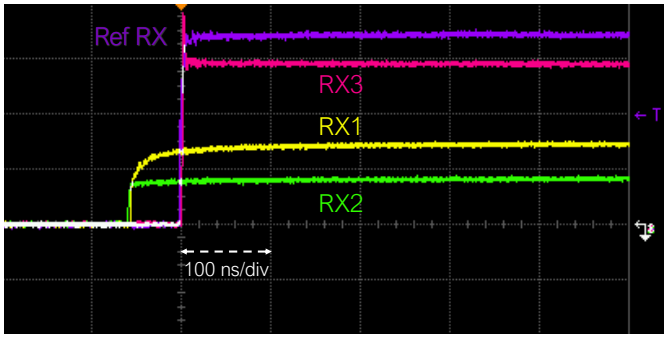
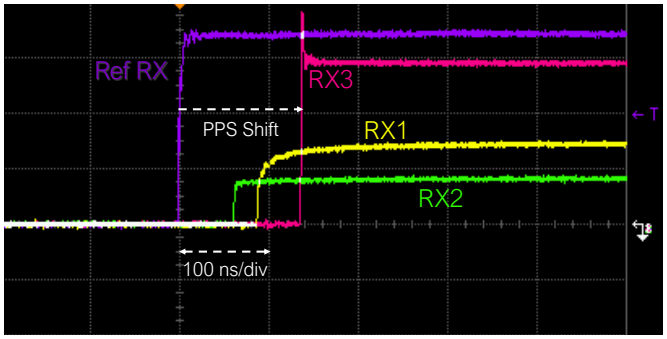


Figure 13: Effects of analog meaconing (B2) on RX3's clock bias, that presents discontinuities in correspondence with the introduction of the meaconing signals and their interruption.



(a) Normal operation 1-PPS alignment.



(b) Effects of an effective B2 attack that results in 1-PPS misalignment of 100 ns.

Figure 14: Normal operation with mis-calibration of RX1 and RX2 (a) and realization of the effects of an effective meaconing attack causing a 1-PPS shift $\delta_{\text{PPS}} > 100$ ns on all the DUTs (B1).

Table 3, summarises vulnerabilities of the DUTs to the proposed attack schemes. Attack complexity defines the level of expertise required to perform the attack on a scale ranging from 1 to 3. As a general comment, we observe how preemptive actions can increase the risk of each attack inducing a 1-PPS shift in all the receivers under test. Non-coherent spoofing represents the less harmful attack for SoA receivers (i.e., RX2, RX3) as it requires a receiver reset to be effective. However, old-gen receivers may be severely impacted by such an attack. MITL induces de-synchronization of RX2 and RX3 only when preemptive actions were taken to accomplish the test. Thanks to its multi-constellation, multi-frequency nature, analog meaconing can defeat nominal 1-PPS generation in all the receivers at the lowest complexity. The test campaign showed how analog meaconing can be easily put in place by tampering with the infrastructure, and represent a non-negligible risk to the synchronization of the network nodes.

Table 3 also allows assessing that the risk of effective attacks increases with the time-coherence of the attack itself. However, achieving accurate time-coherence is directly proportional to the complexity of the attacks except for the analog meaconing.

Table 3: Summary table showing test features and occurrence of time shift on the 1-PPS under attack for each receiver under test. Triangles in coloured cell state the vulnerability of the receivers. Transmitting power levels for the interfering signals are omitted on purpose.

Attack ID	Attack Description	Spoofing RF Stream Age	Interfering Signals				Preemptive Jamming	Reset	Receivers Affected by PPS time shift under effective attack			Attack Complexity
			GPS	GAL	BEI	GLO	*Until PPS Failure*		RX1	RX2	RX3	
	Replay After Long Time	~12 Hours	L1	E1	B1C	-	-	-	△	-	-	1
A1	Replay After Long Time + Jamming		L1	E1	B1C	-	•	-	△	△	-	2
	Replay After Long Time + Receiver Reset		L1	E1	B1C	-	-	•	△	△	△	3
	Replay After Short Time	~30 Minutes	L1	E1	B1C	-	-	-	△	-	-	1
A2	Replay After Short Time + Jamming		L1	E1	B1C	-	•	-	△	△	-	2
	Replay After Short Time + Receiver Reset		L1	E1	B1C	-	-	•	△	△	△	3
	MITL	~15 ms	L1	E1	B1C	-	-	-	△	-	-	1
B1	MITL + Jamming		L1	E1	B1C	-	•	-	△	△	△	2
	MITL + Receiver Reset		L1	E1	B1C	-	-	•	△	△	△	3
	Analog Meaconing	~100 ns	All	All	All	All	-	-	△	△	△	1
B2	Analog Meaconing + Jamming		All	All	All	All	•	-	△	△	△	2
	Analog Meaconing + Receiver Reset		All	All	All	All	-	•	△	△	△	3

V. CONCLUSIONS

Accurate time synchronization is of prominent relevance in critical infrastructures such as telecommunication networks. GNSS can support time synchronization by complementing expensive and non-scalable solutions embedding atomic clocks. However, modern GNSS timing receivers might still be vulnerable to meaconing and spoofing attacks, thus introducing vulnerabilities in the timing infrastructure. Simplistic spoofing signals are typically well-handled by the receivers under test unless a high-power illegitimate transmission is performed that causes a loss of tracking of the legitimate GNSS signals. Meaconing tests instead highlighted non-negligible susceptibility in the receivers in this study. Throughout the tests, only the most advanced receiver proved to be an excellent, robust time-keeping source, able to satisfy stringent synchronization requirements under attack. It also performed with excellent interference mitigation capabilities, but ultimately was defeated by analog meaconing. Within this study, analog meaconing (B2) proved to be the most insidious threat to introduce a time shift in the 1-PPS generation disregarding the class of receiver under attack. This is because even SoA receivers tolerate the delayed signals as caused by the multipath effect. In this work we have showed that an alarm could be sounded by monitoring the receiver clock bias, which would indicate an analog meaconing attack (B2), as also shown in Marnach et al. (2013). The adoption of signal authentication techniques, such as Galileo Open Service Navigation Message Authentication (OSNMA) and GPS Chimera, is going to play a fundamental role in defeating malicious RF attacks. However, as this study demonstrates, modern receivers already put forward effective

countermeasures against spoofing and meaconing that only yield under specific conditions and preemptive actions. Intermediate or advanced spoofing attacks using coherent spoofing signals may still impair SoA receivers similarly to the investigated analog meaconing. However, they are expected to be counteracted by authentication strategies. Therefore, a further effort needs to be paid to mitigate meaconing attacks that might be stealthily used to disrupt synchronization in GNSS-based timing networks. Future works will extend the analysis of the GNSS-disciplined 1-PPS stability across a whole timing infrastructure in the domain of the telecommunication networks.

ACKNOWLEDGEMENT

This work was developed within the ROOT project (www.gnss-root.eu) funded by the European Agency for the Space Programme (EUSPA) under the European Union's Horizon 2020 – G.A. n. 101004261. The content of the present article reflects solely the authors' view and by no means represents the official view of the EUSPA. In any reproduction of this article there should not be any suggestion that EUSPA or this article endorse any specific organisation or products.

REFERENCES

3GPP, E. T. S. I. (2020). Base Station (BS) radio transmission and reception. Technical report, European Telecommunications Standards Institute - 3GPP.

Access, E. U. T. R. (2014). Requirements for support of radio resource management. *Release*, 10:V10.

Bauch, A. and Whibberley, P. (2017). Reliable time from GNSS signals. *Inside GNSS*, 44:38–44.

Berbecaru, D. G. and Lioy, A. (2022). Attack strategies and countermeasures in transport-based time synchronization solutions. In Camacho, D., Rosaci, D., Sarné, G. M. L., and Versaci, M., editors, *Intelligent Distributed Computing XIV*, pages 203–213, Cham. Springer International Publishing.

Chowdhury, D. D. (2021). *GNSS Time*, pages 51–64. Springer International Publishing, Cham.

Chun, Y. (2002). Method and device for rapidly extracting time and frequency parameters from high dynamic direct sequence spread spectrum radio signals under interference. `https://patents.google.com/patent/US6407699B1`.

CISA (2019). Time – the invisible utility. `https://us-cert.cisa.gov/sites/default/files/documents/Corporate_Leadership_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf`.

Commissariat, T. (2021). Atomic clock is smallest on the market. `https://physicsworld.com/a/atomic-clock-is-smallest-on-the-market/`.

Defraigne, P. (2017). GNSS time and frequency transfer. In *Springer handbook of global navigation satellite Systems*, pages 1187–1206. Springer.

Doberstein, D. (2012). *Fundamentals of GPS Receivers*. Springer New York, New York, NY.

Dovis, F. (2015). *GNSS interference threats and countermeasures*. Artech House.

Falletti, E., Margaria, D., Marucco, G., Motella, B., Nicola, M., and Pini, M. (2019). Synchronization of critical infrastructures dependent upon GNSS: Current vulnerabilities and protection provided by new signals. *IEEE Systems Journal*, 13(3):2118–2129.

Farkas, J., Varga, B., Miklós, G., and Sachs, J. (2019). 5G-TSN integration meets networking requirements for industrial automation. *Ericsson: Stockholm, Sweden*, pages 0014–0171.

Foucras, M., Julien, O., Macabiau, C., and Ekambi, B. (2014). Detailed analysis of the impact of the code Doppler on the acquisition performance of new GNSS signals. In *Proceedings of the 2014 International Technical Meeting of The Institute of Navigation*, pages 513–524.

Girela-López, F., López-Jiménez, J., Jiménez-López, M., Rodríguez, R., Ros, E., and Díaz, J. (2020). IEEE 1588 high accuracy default profile: Applications and challenges. *IEEE Access*, 8:45211–45220.

Gregor, S. J. (2014). Method and apparatus to improve performance of GPSDOs and other oscillators. `https://patents.google.com/patent/US20140125418`.

Infinera (2022). *Synchronization Distribution in 5G Transport Networks*. Infinera.

Kazunori, M. (2015). System and device for generating reference signal and timing signal supply device. `https://patents.google.com/patent/US9001865`.

Keten, U. (2021). GPS/GNSS independent time transfer over telco IP core networks using DTM overlay. In *2021 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, pages 1–4.

Li, H., Han, L., Duan, R., and Garner, G. M. (2017). Analysis of the synchronization requirements of 5G and corresponding solutions. *IEEE Communications Standards Magazine*, 1(1):52–58.

Lipiński, M., Włostowski, T., Serrano, J., and Alvarez, P. (2011). White rabbit: a PTP application for robust sub-nanosecond synchronization. In *2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, pages 25–30.

Lu, Q., Feng, X., and Zhou, C. (2021). A detection and weakening method for GNSS time-synchronization attacks. *IEEE Sensors Journal*, 21(17):19069–19077.

Marnach, D., Mauw, S., Martins, M., and Harpes, C. (2013). Detecting meaconing attacks by analysing the clock bias of GNSS receivers. *Artificial Satellites*, 48(2).

Niu, X., Yan, K., Zhang, T., Zhang, Q., Zhang, H., and Liu, J. (2015). Quality evaluation of the pulse per second (PPS) signals from commercial GNSS receivers. *GPS solutions*, 19(1):141–150.

Osseiran, A., Monserrat, J. F., and Marsch, P. (2016). *5G mobile and wireless communications technology*. Cambridge University Press.

Osterdock, T. N., Westcott, D. C., and Hua, Q. D. (1995). GPS synchronized frequency/time source. US Patent 5,440,313.

Papadimitratos, P. and Jovanovic, A. (2008). Protection and fundamental vulnerability of GNSS. In *2008 IEEE International Workshop on Satellite and Space Communications*, page 167–171, Toulouse. IEEE.

Pini, M., Falco, G., and Presti, L. L. (2012). Estimation of satellite-user ranges through GNSS code phase measurements. *Global Navigation Satellite Systems: Signal, Theory and Applications*, pages 107–126.

Pini, M., Minetto, A., Vesco, A., Berbecaru, D., Murillo, L. M. C., Nemry, P., De Francesca, I., Rat, B., and Callewaert, K. (2021). Satellite-derived time for enhanced telecom networks synchronization: the ROOT project. In *2021 IEEE 8th International Workshop on Metrology for AeroSpace (MetroAeroSpace)*, pages 288–293.

Psiaki, M. L. and Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, 104(6):1258–1270.

Schmidt, D., Radke, K., Camtepe, S., Foo, E., and Ren, M. (2016). A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Comput. Surv.*, 48(4).

Skey, K. M. (2017). Responsible use of GPS for critical infrastructure.

Venmani, D. P., Lagadec, Y., Lemoult, O., and Deletre, F. (2018). Phase and time synchronization for 5g c-ran: Requirements, design challenges and recent advances in standardization. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, 5(15).

Whitty, C. and Walport, M. (2018). Satellite-derived time and position: A study of critical dependencies. *Government Office for Science: London, UK*.