Nanosecond-level Resilient GNSS-based Time Synchronization in Telecommunication Networks through WR-PTP HA

Alex Minetto [1], Benoit Rat [2], Marco Pini [2], Brendan Polidori [2], Ivan De Francesca [2], Luis M. Contreras [2], and Fabio Dovis [2]

[1]Department of Electronics and Telecommunications of Politecnico di Torino
[2]Affiliation not available

October 30, 2023

Abstract

In recent years, the push for accurate and reliable time synchronization has become increasingly important in crit?ical infrastructure, particularly in telecommunication networks. The enhanced performance of 5G New Radio and next-generation technologies rely on phase synchronization of Radio Access Network (RAN) nodes, which require sub-microsecond relative timing errors. Atomic clocks, integrated with Global Navigation Satellite Systems (GNSS) timing receivers, have been deployed in timing networks as Grand Master Clocks (GMCs). However, this solution does not scale well with the growing number of interme?diate nodes in current RANs. A more affordable and distributed solution is needed for scalability and time synchronization. GNSS timing receivers are a cost-effective solution providing stable reference clock signals, but a proliferation of GNSS antennas can expose the network to malicious radio-frequency attacks. This research proposes a solution for stable and resilient GNSS?based network synchronization, using the White Rabbit Precise Time Protocol and a timing source backup logic in case of timing-disruptive attacks. The solution was tested against popular jamming, meaconing, and spoofing attacks and was able to maintain 2 ns relative synchronization accuracy between its nodes under any of the tested attacks, without the support of an atomic clock.

Nanosecond-level Resilient GNSS-based Time Synchronization in Telecommunication Networks through WR-PTP HA

A. Minetto, *member, IEEE,*, B. Rat, M. Pini, B. D. Polidori, I. De Francesca, L.M. Contreras, and F. Dovis, *member, IEEE*

***Abstract*—In recent years, the push for accurate and reliable time synchronization has become increasingly important in critical infrastructure, particularly in telecommunication networks. The enhanced performance of 5G New Radio and next-generation technologies rely on phase synchronization of Radio Access Network (RAN) nodes, which require sub-microsecond relative timing errors. Atomic clocks, integrated with Global Navigation Satellite Systems (GNSS) timing receivers, have been deployed in timing networks as Grand Master Clocks (GMCs). However, this solution does not scale well with the growing number of intermediate nodes in current RANs. A more affordable and distributed solution is needed for scalability and time synchronization. GNSS timing receivers are a cost-effective solution providing stable reference clock signals, but a proliferation of GNSS antennas can expose the network to malicious radio-frequency attacks. This research proposes a solution for stable and resilient GNSS-based network synchronization, using the White Rabbit Precise Time Protocol and a timing source backup logic in case of timing-disruptive attacks. The solution was tested against popular jamming, meaconing, and spoofing attacks and was able to maintain 2 ns relative synchronization accuracy between its nodes under any of the tested attacks, without the support of an atomic clock.**

***Index Terms*—Telecommunications, Telecommunication Networks, Time dissemination, Network synchronisation, Telecommunication network reliability, Network Topology, Global Navigation Satellite Systems (GNSS), Precise Timing Protocol (PTP), 5G New Radio (NR)**

I. Introduction

In today's world, mobile traffic is scaling up and its patterns are rapidly changing [Al-Falahy and Alani, 2017] [Infinera, 2022], [Ericsson, 2022a]. This paradigm shift derives from the massive use of uplink-demanding applications such as cloud storage, personal broadcasting, virtual reality (VR), as well as from real-time applications, such as TV broadcasting and on-line gaming [Cai et al., 2022]. For these reasons telecommunications operators are adopting strategies that can satisfy both uplink and downlink spectrum usage with greater flexibility [Agiwal et al., 2016]. Higher data volume together with the steady progress of technology in telecommunications networks has brought the need for new technologies demanding for stringent synchronization requirements. According to [Qualcomm, 2022] and [Ericsson, 2022b], technologies such as 5G - New Radio (5G-NR) are projected to introduce $13+ trillion dollars of global economic output, $22.8 million new jobs created and $265 billion in global 5G Capital Expenditure (CAPEX) and R&D annually over the next 15 years. The extensive effort in research and development is in line with the impact that 5G-NR would have on the global economy. To illustrate why Global Navigation Satellite Systems (GNSS) time synchronization is put forward as a timing solution in telecommunication networks, we take a step back to clarify the need for accurate and stable synchronisation of current 5G-NR. 5G-NR is designed to support different use cases such as Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC) and massive Machine Type Communications (mMTC) [ITU, 2022]. It is intended to satisfy the performance requirements set by the International Telecommunication Union (ITU) for the International Mobile Telecommunications for the year 2020 (IMT-2020) [ITU, 2022], [Lin et al., 2019]. The IMT-2020 has defined some of the key capabilities of 5G-NR [Li et al., 2017a] by setting user experienced downlink and uplink data rates to $100\,$Mbit/s and $50\,$Mbit/s, respectively as well as a user plane latency of $4\,$ms for eMBB and $1\,$ms for URLLC. In conjunction with the previous capabilities, 5G-NR has been designed to operate in the spectrum ranging from sub-1 GHz to millimeter wave bands [Al-Falahy and Alani, 2017]. Two frequency ranges (FR) addressing the different use cases are defined in [Ghosh et al., 2019], i.e., FR1 ($450\,$MHz – $6\,$GHz) and FR2 ($24.25\,$GHz – $52.6\,$GHz). Both FR1 and FR2 bands are mostly based on Time Division Duplex (TDD) [Agiwal et al., 2016], [Ruffini et al., 2021], which is one of the factors contributing to the synchronization requirements addressed in this study. Indeed, TDD networks, both 4G LTE and 5G, require $1.5\,\mu$s maximum time error at the cell site to ensure compliant operation and effective resource sharing between uplink and downlink [Infinera, 2022]. The most stringent requirements come in the form of Time Alignment Error (TAE) between adjacent base stations, i.e., between different Radio Units (RUs). By looking forward towards high-throughput, in order to exploit Multiple-Input Multiple Output (MIMO) and transmitter diversity, *relative* synchronization between adjacent base stations is set to $\pm65\,$ns [Venmani et al., 2018a], [3GPP, 2020], that becomes a *relative* time error between base stations of $\pm32\,$ns. The time synchronization requirements identified in [Osseiran et al., 2016], [Venmani et al., 2018b], [3GPP, 2020], [Li et al., 2017b] are summarised for each specific technology in Table I. To meet these synchronization requirements, classi-

This paper was produced by the ROOT project consortium.
Manuscript received Month XX, 20XX; revised Month XX, 20XX.

TABLE I: Absolute and relative synchronization requirements in 5G-NR networks [Osseiran et al., 2016], [Venmani et al., 2018b], [3GPP, 2020]. The target upper bound for this study highlighted in grey.

Technology	Time-error Tolerance (TAE)	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*

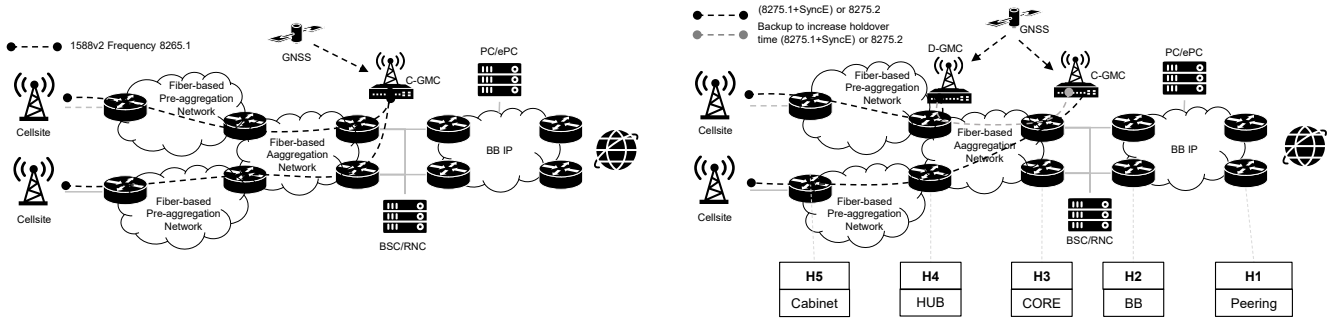
cal timing networks foresee a Centralised Grand Master Clock (C-GMC) node which generates a Coordinated Universal Time (UTC) traceable time reference by combining multiple time sources. The C-GMC obtains a 10 MHz clock signal from rubidium or cesium Atomic Clock (AC) and it steers such signal by means of a One Pulse-per-Second (1-PPS) signal generated by a GNSS timing receiver. In combination with a specifically chosen Precise Timing Protocol (PTP), the C-GMC distributes such information throughout the network nodes [Pini et al., 2021]. IEEE 1588:2008 PTP has been proposed by the telecommunications industry to distribute the time synchronization derived by GNSS receivers [Ruffini et al., 2021], and in particular IEEE-1588-2019 High Accuracy (HA) aims to bring sub-nanosecond accuracy [Pini et al., 2021]. Following the increasing amount of network nodes, such a timing reference must be moved as close as possible to the Radio Access Network (RAN) stations in order to preserve the synchronization budget typically spent across the network hops. This trend would require multiple atomic clocks and a distributed timing infrastructure based instead on Distributed Grandmaster Clock (D-GMC). As an affordable alternative, operators started deploying multiple GNSS receivers at every cell cite of the RAN, following the trend of Fixed Wireless Access (FWA) networks [Ericsson, 2022a]. This approach may expose the network to intentional and unintentional Radio Frequency Interferences (RFI) which may degrade synchronization and performance [ENISA, 2019]. Notwithstanding the advancements of GNSS receivers with their interference mitigation and synchronization performance, Radio Frequency (RF) attacks and interferences still pose a insidious threat to timing distribution. Such attacks could lead to inaccurate synchronization between the aforementioned network nodes up to disrupting network nominal operations along with critical infrastructures at a large extent. State-of-the-art, multi-frequency, multi-constellation GNSS timing receivers are proposed to guarantee reliable, ns-level accuracy in both *relative* and *absolute* synchronization between the GNSS constellations and the network timescale [Defraigne, 2017], [Thongtan et al., 2017]. Along with an enhanced timing accuracy, they indeed embed specific solutions to detect and mitigate common RFI such as jamming, meaconing and spoofing [Gioia and Borio, 2021]. To satisfy such stringent time and phase synchronization requirements as well as the resilience against RF attacks against the GNSS timing source, this work proposes a combination of state-of-the-art GNSS timing receivers embedded in dedicated timing units which support White Rabbit Precision Time Protocol (WR-PTP) for the distribution of ns-level timing information. This solution also contributes to trade-off the number of GNSS receivers deployed at the RAN nodes, thus reducing the entry points for possible attacks. The study focuses on demonstrating the stability and resilience of modern GNSS-based synchronization networks and on establishing the baseline architecture of D-GMC nodes for next-generation timing networks serving telecommunications networks, and critical infrastructures at a large extent. The outline of this manuscript is as follows. Section II details the architecture of a timing infrastructure in the context of telecommunication networks. It introduces the generation of the GNSS-disciplined timing signals, the potential threats to its integrity, and the operational principles of White Rabbit Precision Time Protocol High-Accuracy (WR-PTP HA). Section III describes the proposed network architecture and the testbed setup hosted at the Telefonica's Automation and Innovation Lab (Madrid, Spain). Section IV presents a set of sample results from the extensive stress tests and Section V draws the conclusions and final remarks.

II. Background

A. Timing in telecommunications networks

Throughout the years, to fulfil their service offering, telecom operators have deployed separate or overlapping networks specifically targeted for each service. This implies a multiplicity of redundant hardware that many times has to be upgraded in cascade as traffic increases. Given the need for clock densification and to avoid scalability issues, some operators are currently transforming their IP networks according to the FUSION concept of an all-IP network. This is the case, for instance, of Telefonica. This concept makes use of end-to-end Multiprotocol Label Switching (MPLS) technology and is structured in five hierarchical levels, where nodes with different functions in the previous architectures are consolidated into a single network element per level, thus improving scalability, security, flexibility and cost reduction. The FUSION hierarchy levels are described as:

- H5: the most distributed level where mobile Base Stations connect or a pre-aggregation level depending on the specifics of the country. Typically, it hosts Cell Site Routers (CSR) or small form-factor aggregation routers;
- H4: is the metro aggregation level where fixed subscriber access nodes (e.g., Gigabit Passive Optical Network (GPON) Optical Line Terminal (OLT)) are connected;
- H3: the regional level concentrator where typically different kinds of service platforms (e.g. Internet Protocol television (IPTV)) or control platforms (e.g. mobile Evolved Packet Core (EPC), AAA) are connected;



(a) (b)

Fig. 1: Paradigm shift in the synchronization of telecommunication networks based on GNSS-disciplined Grand Master Clock (GMC). Hierarchical levels are identified in (b) as referred throughout the present article.

- H2: national backbone level. The nodes at this level act as pure MPLS routers. These routers can be based on platforms optimized for plain packet switching, yielding a more cost-effective solution;
- H1: interconnection level to external networks.

Our research aims to understand the effect of RF attacks on different hierarchical nodes and the consequences on the network. Due to the location of C-GMCs and D-GMCs, the effect of RF attacks will be analysed over H5, H4 and H3 locations. As previously stated synchronization of the network is achieved with the combination of GNSS and WR-PTP.

B. GNSS timing sources and 1-PPS generation

Global Positioning System (GPS), Galileo, GLONASS and Beidou navigation signals carry specific Pseudo Noise (PN) ranging codes, usually referred to as Pseudo-Random Noise (PRN) codes, that enable satellites ranging and time synchronization at the receivers. Independently from the signal plans adopted by each constellation, GNSS transmitters keep the carrier, PN codes, subcarriers and data symbols edges aligned for each of their navigation signals. The signal transmitted by a generic GNSS satellite reaches the receiver's antenna and can be modelled through (1), where $P_{R,i}$ indicates the received signal power, D_i indicates the amplitude value of the data symbol, C_i indicates the amplitude value of the code symbol (i.e., chip), S_i indicates the amplitude value of the code subcarrier, and $f_{d,i}$ indicates the Doppler shift due to the relative velocity between the i-th satellites and the receiver. The code tracking of a single GNSS navigation signal is theoretically sufficient to discipline the generation of a rough clock signal. A higher precision can be achieved by means of carrier phase tracking [Kap, 2006]. However, code Doppler effect, unknown propagation time, and satellite's and receiver's oscillators biases make such a clock signal misaligned w.r.t. to any conventional time scale. To steer a dedicated local oscillator and discipline an actual 1-PPS timing signal aligned to a given GNSS constellation time-scale all of these biases must be compensated [Niu et al., 2015]. Therefore, the generation process of the 1-PPS strictly depends on the Positioning, Navigation and Timing solution [Minetto et al., 2022], thus making use of the PN code and its phase offset, the message preamble, and the navigation data. The code phase offset observed at the receiver depends on the following terms that all condition the estimated pseudorange measurements. The satellite clock bias, δt_s, is compensated through a first or second order polynomial model based on the clock bias correction parameters carried by the navigation message, i.e., clock offset, clock drift and clock drift rate [Kap, 2006]. The receiver clock bias, δt_u, is common to all the received signals, is estimated through the Position, Velocity and Time (PVT) algorithm as a further unknown of the multilateration problem. The atmospheric delays, δt_a, can be compensated through the ionospheric parameters included in the navigation message and troposphere models at the receiver. The signal propagation time, τ_i, is reflected into a number of integer code replicas of duration δt_p and its fractional part, δt_c, that is estimated by code correlation and finely tracked by receiver's Delay Lock Loop (DLL). 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 that is lower-bounded by the uncertainty of its clock bias estimation. Any action that can alter the aforementioned delays may affect the disciplination of the output 1-PPS. The system that generates the 1-PPS wavefronts is able to steer it almost continuously. If we consider a conventional rising edge in the origin of the time axis at $t = 0$, we can model each pulse as a delayed rectangular pulse:

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

where T_{PPS} is the pulse duration and it can be typically customised in high-end receivers, T_{DC} is the duty cycle

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

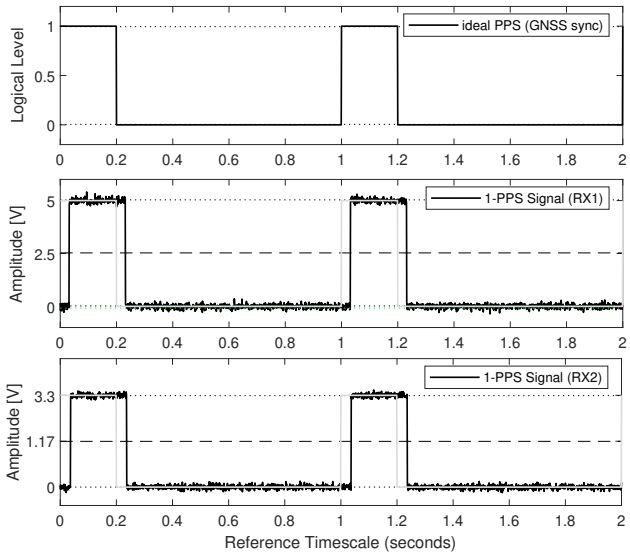


Fig. 2: Pictorial view of an ideal reference 1-PPS (top) and real (mid, bottom), noisy ones generated by a pair of GNSS receivers (i.e., RX1, RX2).

duration, and A is the amplitude of the electrical pulse, in Volts. T_{DC} is equal to 1 s by definition of 1-PPS. We expect an ideal square wave as output from the receiver, with a duty cycle of 1 s. In any implementation, the actual output is an approximation waveform that is used to guarantee the physical generation of (2). The 1-PPS signal can be shaped by using a steep roll-off factor. A PPS signal can be modelled as a train of (2):

$$\text{PPS}(t) = n(t) + A \sum_{k=-\infty}^{\infty} \Pi_{\text{PPS}}(t - kT_{DC} + a(t)) \quad (3)$$

as shown in the sample comparison of Figure 2, where two PPS show $k \in [0, 2]$ s, $T_{DC} = 1$ s, $T_{PPS} = 0.2$ s and amplitudes $A_{RX1} = 5$ V and $A_{RX2} = 3.3$ V,, respectively. An offset of 30 ms is present between the 1-PPS signals of the two receivers that, in real scenarios and with a proper scaling factor, can be attributed to the uncertainty of the clock biases estimates of the two receivers.

C. RFI degrading the 1-PPS

Reliable time, frequency and phase synchronization at GNSS receivers depends on the quality of the received signals, and can be severely impacted by RFI [Borio and Gioia, 2021]. Three main classes of interference were considered in this study, i.e., jamming, meaconing and spoofing. We recall their working principles and their expected effects when transmitted against a victim receiver [Dovis, 2015].

1) Frequency Modulated Jamming: The general aim behind this class of attack is to introduce additional noise in the GNSS signals bandwidth, since the incoming legitimate signals power is lower than the thermal noise floor, making it harder if not impossible for the receiver to be able to acquire and track them. One of the most common methods of jamming is carried out through the use of a cyclic chirp signal, that is by definition a signal with time-varying frequency within the legitimate signal bandwidth. In particular Linearly Frequency Modulated (LFM) chirps are the most common and they can be modelled as

$$w(t) = A_j \cos(2\pi f(t)t + \phi) \quad (4)$$

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 $(f_1 - f_0)/T$. T is the time that it takes to sweep from the initial frequency f_0 to f_1, i.e., the sweep time. The term ϕ identifies the initial phase offset. When a receiver is hit with a jamming attack the incoming signal can be written as

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

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. This class of attacks mainly affect the Carrier to Noise Ratio (C/N0), which impacts the receivers ability to acquire and track incoming signals. Regarding the timing, the attacker has no external control on the disciplined 1-PPS. Most Commercial off-the-shelf (COTS) receivers when jammed with a high enough power lose track of all GNSS signals and therefore are not able to produce an actual 1-PPS, while others go into holdover mode, which uses the internal clock and does not guarantee synchronization within the needed requirements. More specialized receivers that implement anti-jamming algorithms are able to mitigate such attacks but ultimately succumb to high power levels. Therefore in most complex attacks jamming is used as a preemptive strike to bring the receiver into an initial known state where it is not able to acquire or track any legitimate GNSS signals.

2) Meaconing: by definition it is the reception and re-broadcasting of signals. When targeting the time keeping capabilities of a GNSS receiver the objective is to shift the 1-PPS with respect to its correct time offset. By rebroadcasting a delayed and amplified version of the GNSS signals it is possible to fool the receiver into tracking the delayed signals instead of the legitimate ones. If receiver operations are not defeated, meaconing allows to operate a stealth malicious action that shifts the 1-PPS and causes a de-synchronization of the receiver w.r.t. the GNSS reference time-scale. When a meaconing attack takes place, the incoming signals at the receiver can be written as

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

where P_m is the received meaconing power, that ideally is greater than that of the legitimate signals in order to induce the receiver to track those GNSS signals showing a more favourable signal-to-noise ratio. When in nominal operations, the receiver is tracking the legitimate signals but when meaconing is introduced it may suddenly observe a discontinuity in signal power and delay, which separately could be attributed to normal operating conditions such as an improved visibility of satellites and multipath in a urban environment. While under meaconing, in the tracking loop the system observes the code-phase delays of the PRN codes all equally shifted w.r.t the

previous values. The PVT algorithm is now solving for the combined clock bias which derives in part from the receiver clock bias and in part from the meaconing injected bias. Meaconing can be extremely insidious on stationary receivers, since position and velocity estimates are not affected. The sudden change in both time and power of the incoming signals could be utilised as a warning system to prevent meaconing attacks, especially in static applications. However, this is typically not implemented in State-of-the-Art (SoA) timing receivers.

3) Simplistic Non-Coherent Spoofing: When working with static targets we define a non-coherent, simplistic spoofing attack as the injection of a signal which is either a recording of real GNSS signals or a realistic reproduction of them with the exception of time coherence. Spoofing attacks aim at fooling the receiver into believing that the incoming signals are legitimate ones, while actually they contain navigation information which is either out of date or incorrect. When non-coherent spoofing signals reach the receiver they can be modelled as

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

where D' and τ' identify altered navigation bits and propagation delay, respectively. The spoofing signals in combination with legitimate GNSS ones can instead be represented as

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

If the receiver processes the spoofing signals instead of the legitimate ones and extracts their navigation data this leads the PVT algorithm to calculate an incorrect position and time. Depending on the algorithms that are implemented in the receiver it can send an alarm if large changes in position or time are found. If the receiver switches from using legitimate GNSS signals to spoofed signals that are non-coherent a jump in the 1-PPS is to be expected. Solutions to countering simplistic, non-coherent spoofing can be as simple as using a Real Time Clock (RTC), that after initialisation is able to keep track of time within a certain error margin w.r.t system time. This margin can guarantee a threshold that blocks any non-coherent spoofing attacks that are above it. If working with static receivers large jumps or quickly changing clock parameters could be an indication of an attack.

D. White Rabbit PTP to distribute high-accuracy timing

The WR technology is an open-source synchronization project that was launched in 2009 [Lipiński et al., 2011], [Serrano et al., 2013], [Loschmidt et al., 2009], [Moreira et al., 2009]. It is developed through the collaboration of various international public scientific organisations, such as Conseil Européen pour la Recherche Nucléaire (CERN), the Society for Heavy Ion Research (GSI), and the University of Granada (UGR), as well as private companies like Seven Solutions, who first designed the WR-PTP switch hardware. This is achieved through the use of standard technologies such as Ethernet, PTP, and Layer 1 (ISO/OSI) synchronization, similar to Synchronous Ethernet (SyncE). The WR-PTP is known for its high-precision frequency distribution, with uncertainties within $50\,\text{ps}$. Its capability to enhance timing performance without requiring a complete overhaul of the fiber infrastructure has fostered its use in many scientific industrial facilities [Lipiński et al., 2018]. The standard WR-PTP link operates in a master-slave model, where time information is passed from the master to the slave node through regular fiber connectivity. Additionally, WR-PTP devices can also be configured as GMC to provide stable external time references. When configured as a GMC, the devices combine 1-PPS and $10\,\text{MHz}$ clock signals as a long-term-stable frequency reference and Network Time Protocol (NTP) for absolute Time of Day (ToD) information. WR-PTP technology originally supports $1\,\text{Gbit}$ Ethernet connections and does not degrade synchronization when mixing data packets with WR-PTP packets.

1) Working principles: The operational principles of WR-PTP can be explained in a few key mechanisms. Similarly to SyncE, Layer 1 synchronization uses a master clock to distribute time to slave devices. This process uses a technique called Clock Data Recovery (CDR) to extract the clock signal from the received data stream. This extracted clock is then used to regulate the local clock, creating a copy of the reference clock. WR-PTP performs time synchronization using an extended version of standard PTPv2 packets. These packets include special signalling messages for setting up the WR link, which also include additional information like calibration parameters in the event messages. This packet exchange process allows for the creation of hardware timestamps for both sending and receiving and uses this information to calculate the clock offset between the master and slave devices. To improve the accuracy of hardware timestamps up to ps-level, WR-PTP uses syntonization to perform phase measurements between the transmitted and received clocks of the master and slave devices. This information is used to enhance the timestamp data and increase the accuracy of clock offset calculations. A typical WR-PTP connection takes into account the asymmetry in propagation delay to eliminate uncompensated synchronization offsets, which makes the setup process easier by using pre-calibrated values to account for varying propagation speeds and fixed delays. The default pre-calibration settings allow for a maximum link distance of up to $10\,\text{km}$.

2) High-Accuracy standardisation: The IEEE 1588 Precision Time Protocol standard is set to include a new High Availability (HA) profile, based on the current WR-PTP technology and has been standardised in IEEE 1588-2019. The core principles of WR are retained in the standard implementation, but the protocol has been reworked to align with the other IEEE 1588 profiles, resulting in consistent nomenclature, state machines, and general mechanisms. This significantly improves interoperability and expands the scope of industrial applications that can be supported compared to the original WR implementation.

III. Methodology

A. Proposed hierarchical timing network

We assumed to distribute time synchronization through a dedicated timing network infrastructure composed of a dedicated timing node for each hierarchical level. To understand

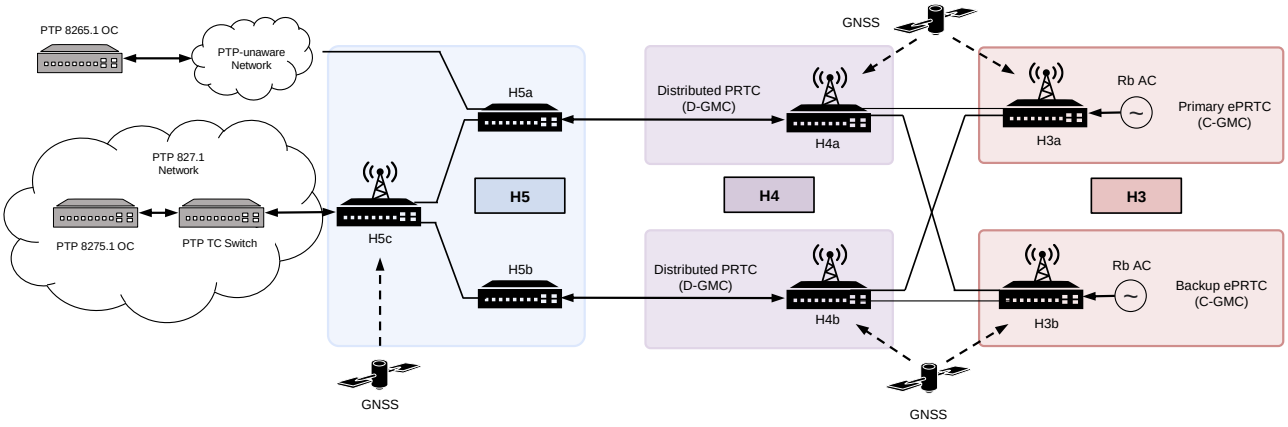


Fig. 3: Mapping of the ROOT timing network architecture to the reference topology of Figure 1b.

the methodology of the attacks on the different hierarchical levels we must first analyse how timing information is shared between the different levels. Figure 3 shows a diagram describing how synchronization is distributed throughout the network. The higher layer nodes and those which are equipped with a GNSS receiver utilise the GNSS timescale as their main timing source during nominal operation. In Figure 3, the nodes which are equipped with a GNSS receiver can be distinguished by the presence of the antenna, these would be H3a and H3b, H4a and H4b and H5c. The nodes that are not equipped with receivers, behave as followers, using WR-PTP to inherit accurate time and phase synchronization from a leader node.

B. Timing source backup logic FOCA vs BMCA

The Fail-Over Clock Algorithm (FOCA) has been designed as a decision making policy. In case of failure of the current timing source, it switches to the next ready timing source. The algorithm is based on the Best Master Clock Algorithm (BMCA) found in the PTP IEEE 1588-2019 standard, but unlike its predecessor it only switches in case of failure and not on what best clock source is present. Timing sources are also ranked by the user and the algorithm is set to follow the hierarchy. FOCA is deemed to provide a safer option than BMCA, when handling switching between multiple references. The FOCA i) provides a deterministic behaviour, ii) does not allow a new rogue node to become the active reference. Furthermore, iii) recovery to a normal state must be supervised by an operator. Eventually, FOCA iv) allows switching between cross WR-PTP profiles and multiple external timing sources, and v) is optimized for a tree network topology. In Figure 4 we can see how the timing sources are chosen. Starting in state t_1, the main WR0 source is seen as non reliable since it has reached a critical state (shaded box with dashed line). WR1 then becomes the main timing source (solid line box). When WR0 becomes available again the system does not switch back immediately since no error has been detected on WR1. At time t_3, when also WR1 fails, there are two ways for the algorithm to move forward: in t_{3-A} the first the algorithm re-evaluates all timing options and if the primary (WR0) is eligible is switches back to it, while in t_{3-B} the algorithm continues to fall down the hierarchy of timing sources, this time switching to the GNSS source. Clock failures can present themselves starting from many different causes some being when link is down or no packets are exchanged. Other error sources can be hard to identify. For additional details we invite the reader to refer to [Seven Solutions, 2022].

Fig. 4: FOCA decision making process for establishing the reference clock when time source faults occur.

C. Selection of GNSS Timing Receivers

In order to select the most suitable device for the proposed timing infrastructure, a set of GNSS timing receivers was tested against RF attacks in the early phase of the ROOT project [Pini et al., 2021]. Comparative analysis were performed to assess the robustness of state-of-the-art devices embedding dedicated anti-jamming and anti-spoofing capabilities [Minetto et al., 2022]. The selected multi-band, multi-constellation GNSS timing receiver demonstrated superior resilience against chirped jamming signals and simplistic spoofing attacks. However, within such an analysis, it has been understood that the selected timing receiver was vulnerable to spoofing if reboot is operated under attack and to Meaconing in the Loop (MITL) in any conditions (i.e., with and without jamming or reboot preemptive actions). Regarding jamming interferences, the effects were effectively mitigated up to the over-saturation of the front-end due to a high interfering power. The main technical features of the target GNSS timing receiver are included in [Minetto et al., 2022].

D. Experimental setup

The testbed shown in the block diagram of Figure 5 was deployed at the Telefonica Innovation and Automation Lab (Madrid, Spain). It was composed by four main items that were located in dedicated areas of the building:

A) Rooftop to basement wiring: RF equipment (i.e., antenna, Low Noise Amplifier (LNA)) and main GNSS signal provisioning wired line

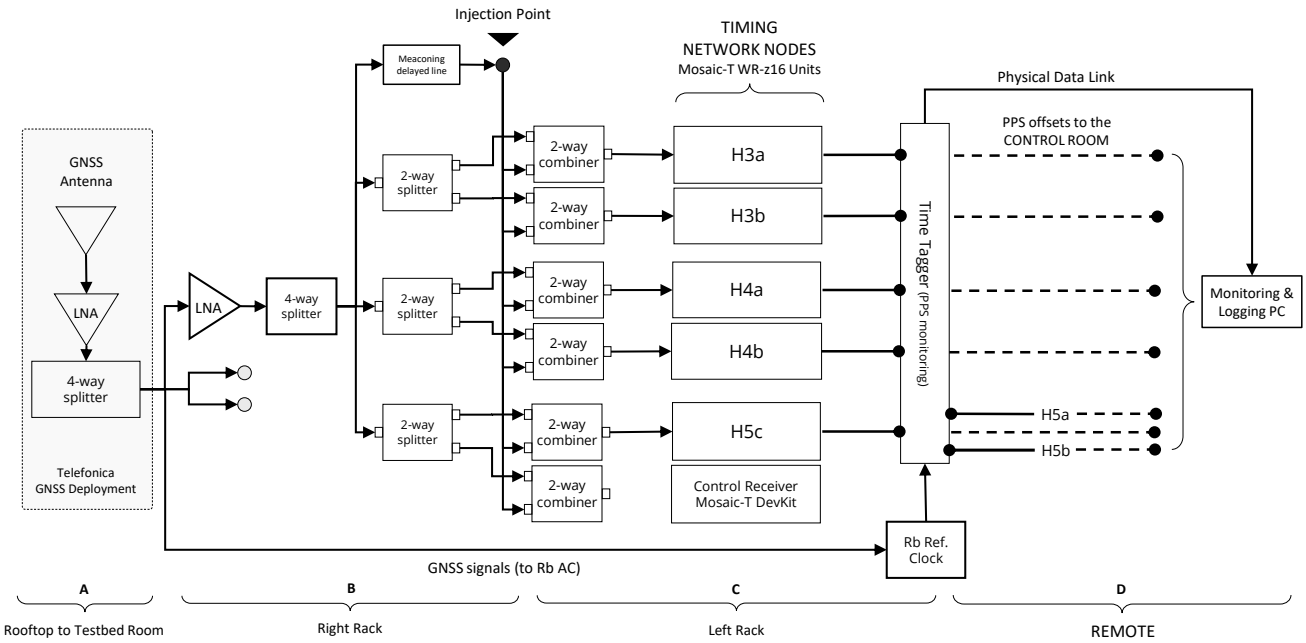


Fig. 5: Testbed for the analysis of the GNSS-based relative synchronization among timing nodes at various network hierarchical levels.

B) Testbed room (R-rack): GNSS signal conditioning subsystems, distribution, and interference generation units
C) Testbed room (L-rack): Timing network nodes, reference Rb AC, and 1-PPS time-tagger unit
D) Remote control room

The GNSS signals, received by a high-end choke ring antenna and pre-amplified at the building rooftop, had their power split to feed the timing network and the reference Rubidium (Rb) AC. A further amplification stage was ensured through a second LNA to compensate for the subsequent power splitting stages. Each hierarchical level was fed by a dedicated 2-way power splitter to supply all the network timing nodes. A 2-way power combiner was installed to merge legitimate and interfering signals provided through the *GNSS RF Attack Injection Point*. 1-PPS signals disciplined by each timing node were compared with a reference 1-PPS provided by a Rb AC at the time-tagger. A real-time monitoring of the 1-PPS signals was operated at the remote control room while test procedures were executed at the testbed room according to the test schedules.

E. Test Scenarios and Procedures

According to a plausible geographical deployment of the nodes belonging the different hierarchical layers, a set of meaningful scenarios was identified. The test scenarios listed in Table II are identified by a compact string which summarizes their description. The different attacks, designed according to the literature review of Section II, are mainly distinguishable by i) Class of RFI, ii) Single-node (SN) vs Multi-node (MN) targets, iii) Single-frequency (SF) vs. Multi-frequency (MF). When an attack was performed simultaneously on multiple nodes, the affected nodes were assumed reasonably co-located in a real network deployment, and possibly sharing the same GNSS antenna and wired line. The actual risk associated to the different attack scenarios have been analysed in [Minetto et al., 2022].

The test procedures designed for the execution of the attacks are summarised in the Tables III, IV, V. Test procedures were designed in the preliminary phases of the study and are detailed in [Minetto et al., 2022].

IV. Results

Sample results are selected from the ROOT test campaign and presented hereafter through the analysis of the 1-PPS trends, as they were recorded at the control room for each node of the timing network. The subset of experiments selected from Table II is representative of the major events that may occur under different threats. Furthermore, it has to be remarked that multiple realisations of the same test were pursued showing the same results. Each plot in Figure 6 shows the synchronization error between the 1-PPS at the output of the network timing node and the reference 1-PPS signal which was generated by the Rb clock deployed at the testbed. The labels on the y-axes indicate the corresponding network node (e.g., H3a in the upper subplot). The shaded background indicates the nodes under attack. Furthermore, for each subplot, a coloured strip on the top indicates the reference timing source used by the node. The lowest hierarchical level (i.e., H5) can have as reference timing sources any node belonging to higher hierarchical levels, thus showing strips of the same colour. For example, in Figure 6a, the H5a node is marked with a yellow strip for the whole duration of the experiment, like the H4a node. This means that node H5a was time-slaved (follower) to the node H4a (leader). On the contrary, the H5c node, even if belongs to the lowest hierarchical level, it is not inheriting timing from any superior node because it hosts

TABLE II: Batch of RFI vulnerability tests performed within the ROOT test campaign against the timing network. Results of the test on the highlighted scenarios are extensively discussed in Section IV.

Scenario	**RF attack description**	**Affected nodes**	**Affected GNSS bands**
a) SN-SF-WBJ	Single-node, single-band, WB jamming	H5c	L1/E1
b) MN-SF-WBJ	Multi-node, single-band, WB jamming	H3a, H4a	L1/E1
c) SN-MF-WBJ	Single-node, multi-band, WB jamming	H4a	L1/E1, L2, L5/E5
d) SN-MF-WBJ	Single-node, multi-band, WB jamming	H4b	L2, L5/E5
e) MN-MF-WBJ	Multi-node, multi-band, WB jamming	H3a, H4a, H5c	L1/E1, L2, L5/E5
f) SN-MF-AM	Single-node, analog meaconing	H3a	L1/E1, L2, L5/E5
g) SN-MF-AM	Single-node, analog meaconing	H4b	L1/E1, L2, L5/E5
h) SN-MF-AM	Single-node, analog meaconing	H5c	L1/E1, L2, L5/E5
i) MN-MF-AM	Multi-node, analog meaconing	H3a, H4a	L1/E1, L2, L5/E5
l) SN-SF-NS	Single-node, single-band, non-coherent spoofing	H4a	L1/E1

TABLE III: Reference jamming power for jamming scenarios (testbed fixed attenuation -50 dB)

Test phase	L1/E1 RFI power[1]	L2+L5/E5 RFI power[2]
R0	-73.80 dBm (noise floor)	-71.00 dBm (noise floor)
R1	-53.72 dBm	-56.40 dBm
R2	-32.20 dBm	-43.20 dBm
R3	-27.66 dBm	-33.85 dBm
R4	-26.80 dBm	-32.30 dBm
R5	End of Test (EoT $\rightarrow$ R0)	End of Test (EoT $\rightarrow$ R0)

[1]Reference signal bandwidth $B_{L1} = 40$ MHz.
[2]Reference signal bandwidth $B_{L2+L5} = 90$ MHz.

TABLE IV: Test phases for non-coherent meaconing scenarios

Test phase	RFI Action/Events
R0	Nominal GNSS signal conditions
R1	Meaconing signal switch-on (amplifier)
R2	Meaconing signal switch-off (amplifier)
R3	End of Test (EoT)

a GNSS receiver and in fact, it has a purple coloured strip, which does not appear in any of the nodes belonging to H4 and H5 levels. Before the test, the network was configured to have H5a slaved to H4a (yellow strip) and H5b slaved to H4b (green strip). All other nodes relied on their own GNSS-disciplined 1-PPS signal at the output of the GNSS receiver.

A. Single Node, Multi-band Wideband Jamming

The experiment was performed against the node H4b, according to the test phases of Table III. The time evolution of the 1-PPS signals are reported in Figure 6a. The test started with nominal GNSS signal conditions, then at approximately 11:16:49, the jammer was switched on (R1) and used to inject interfering signals with a power approximately equal to –53.72 dBm (L1/E1) and –56.40 dBm (L2+L5/E5). The jamming signal power was then increased (R2) up to -32.2 dBm (L1/E1) and -43.2 dBm (L2+L5/E5), then further increased (R3) up to -27.66 dBm (L1/E1) and –33.85 dBm (L2+L5/E5). Until the phase R4, no effect was evident on the network, i.e., the H4b node still considered its own clock reliable (green strip), due to the ability of the GNSS receiver to mitigate the jamming signals. When the jamming signal power was increased to -26.8 dBm (L1/E1) and -32.3 dBm (L2+L5/E5) (R4), it was observed that the 1-PPS was not available for few seconds at H4b, likely due to the unavailability of the GNSS-disciplined 1-PPS signal at the output of the GNSS timing receiver. Indeed, when the jamming power was too high to be handled by the interference mitigation algorithms, the receiver stops disciplining the 1-PPS. In such a case, the timing node detects its own GNSS-based timing source is no longer available/reliable and it switches to a different timing source, namely the H3b node. In fact, the coloured strip turns red for the last part of the experiment, even if the jamming was switched off. Interestingly, we can observe a cascading effect of the jamming attack. Node H5b was slaved to node H4b (i.e., green strip as for the H4b node), which was under attack. As soon as the GNSS timing receiver at H4b was no longer able to mitigate the interfering jamming signal, the 1-PPS signal was unavailable at node H5a for few seconds, as well. However, thanks to the autonomous switching mechanism, i.e. FOCA, implemented through the timing node logic, the H5b node locked onto a different timing source, considered reliable, in this case node H4a, with negligible effect on the overall synchronization network performance. Overall, the network synchronization is maintained with a maximum error of 2 ns in all the timing nodes.

TABLE V: Test phases for non-coherent spoofing scenarios and preemptive actions

Test phase	RFI Action/Events
R0	Nominal GNSS signal conditions
R1	Pre-emptive jamming on L1/E1 -26.8 dBm and on L2+L5/E5 -32.3 dBm
R2	Jamming off on L1/E1, spoofing signal on L1/E1 while jamming on L2+L5/E5
R3	Jamming and spoofing switch-off
R4	End of Test (EoT)

B. Multi-node, Multi-band Wideband Jamming

In this test, a wideband jamming covering three frequency bands, namely the L1/E1, L2 and L5/E5b, hits the GNSS receivers embedded in the timing node at nodes H3a, H4a and H5c. The time evolution of the 1-PPS signals are reported in Figure 6b. The test started with nominal GNSS signal conditions, then at approximately 9:45:24, the jammer was switched on and used to inject interfering signals with a power approximately equal to –53.72 dBm (L1/E1) and –56.40 dBm (L2+L5/E5) (R1). The jamming signal power was then increased up to –26.8 dBm (L1) and -32.3 dBm (L2+L5/E5)

(R4), following the phases reported in Table III. Until the end of phase R3, no effect was evident on H3a and H4a: both the nodes still considered their own GNSS based clocks reliable, likely due to the ability of the GNSS timing receiver to mitigate the jamming signal. When R4 started, the jamming signal power was at $-26.8\,\text{dBm}$ (L1/E1) and $-32.3\,\text{dBm}$ (L2+L5/E5): it was possible to observe that the 1-PPS was no longer available at H3a for the whole duration of the R4 phase, likely due to the unavailability of the GNSS-disciplined 1-PPS signal at the output of the GNSS timing receiver. At the end of the attack, the 1-PPS was again available, likely due to the ability of the GNSS timing receiver to recover the tracking of real GNSS signals and provide reliable timing signals. The 1-PPS was not available for few seconds at H4a, due to the unavailability of the GNSS disciplined 1-PPS signal at the output of the receiver. However, the timing node detected its own GNSS-based timing source was no longer reliable and it switched to a different timing source, i.e., the H3b node. In fact, the coloured strip turned red. It is possible to observe a cascading effect on the H5a node. Despite this node was not under attack, it was slaved to H4a, which was actually under attack. Thus, when the timing signal provided by H4a was no longer reliable, H5a took H4b as reference, preserving a reliable node synchronization, i.e., the difference between the 1-PPS signal of the node and the reference stays within 2 ns. The H5c node suffered from the jamming attack earlier than H3a and H4a. After the start of the R1 phase, i.e., the jamming signal power was approximately equal to $-53.72\,\text{dBm}$ (L1/E1) and $-56.40\,\text{dBm}$ (L2+L5/E5), it is possible to observe that the 1-PPS is not available at H5c for few seconds and the node switches to a reliable timing source, in this case H4a (purple strip turns yellow). A possible hypothesis of this higher sensitivity to jamming could be due to a worse signal-to-interference ratio caused by a greater attenuation of the GNSS signal at the input of the GNSS timing receiver embedded at the H5c node. We observe a cascading effect: when the H4a no longer provided a reliable timing source, the node took another reference to preserve its synchronization. In this case, H5c automatically switched to H4b (yellow strip turns green).

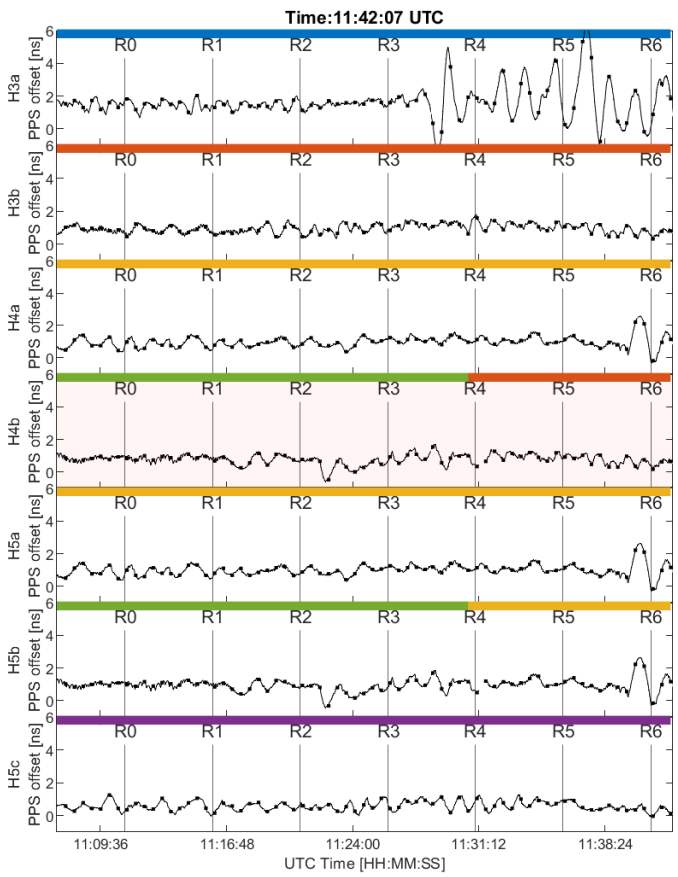
C. Single node meaconing

1) H4b: In this test, the GNSS timing receiver embedded in the network timing node H4b was attacked with a fixed delay meaconing. The real GNSS signal was received, delayed and amplified before being injected as an interference of the direct GNSS signal itself. The test phases are reported in Table IV while the its time evolution is depicted in Figure 6d. The test started with nominal GNSS signal conditions, then at approximately 13:56:33, meaconing signals were injected to interfere with the real GNSS signals at H4b. The GNSS timing receiver suffered this type of interference, without being able to mitigate the produced effect. For a few seconds the GNSS-disciplined 1-PPS signal was not available and thus, the logic of the timing node switched to a different timing source considered reliable, in this case the 1-PPS signal provided by the H3b (the green strip turns red). Since the attacked node (i.e.: H4b) was set as reference for H5b, the fact that the H4b timing signal was no longer considered reliable produces a cascading effect onto H5b, too. In fact, as soon as the meaconing induced a short unavailability of the 1-PPS at H4b, also H5b started using a different reference, in this case the 1-PPS from H4a (the green strip turns yellow). Overall, in this case the autonomous switching capability provided by the network timing node protected the network synchronization, with all nodes showing a maximum synchronization error within 2 ns for the whole test duration.

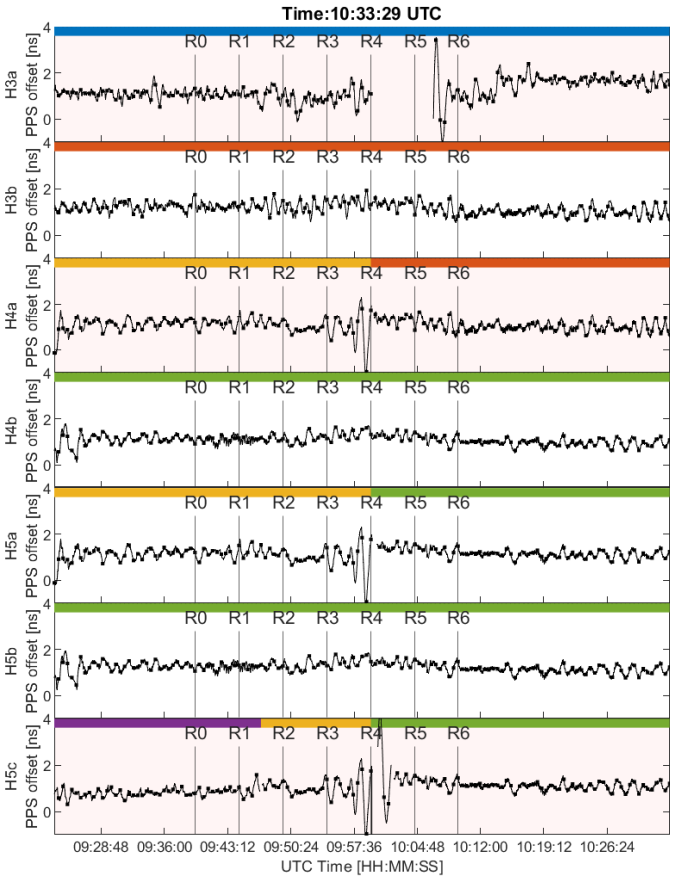
2) H3a: This test followed the same procedure as the test against H4b, but the attack was conducted against a node belonging to the highest hierarchical level of the network, i.e. H3a. The GNSS receiver embedded at the node H3a was attacked with a fixed-delay meaconing. The test started under nominal GNSS signal conditions, then at approximately 14:24:33, meaconing signals were injected to interfere with real GNSS signals at H3a. As per the test against H4b, the timing receiver was affected by the interference, without being able to mitigate the produced effect. For a few seconds the GNSS-disciplined 1-PPS signal became not available. Contrary to the previous case, the logic of the network timing node did not switch to a different timing source, being H3a at the highest hierarchical level of the network. It is also possible to note from the upper subplot of Figure 6d that the meaconing produced a timing error for the whole duration of the attack (R1 to R2). The error quickly overcame $10\,\text{ns}$ and it reached up to $150\,\text{ns}$ (out of plot limits for visualisation purposes). Eventually, it returns to near-zero values only at phase R2, when the meaconer was switched off. In this case, the meaconing attack produced i) short-lasting unavailability of the 1-PPS signal for few seconds at the beginning and the end of the attack; ii) a bias on the GNSS disciplined 1-PPS signal of approximately $150\,\text{ns}$, as evident in the upper subplot of Figure 6c. This result highlighted a residual vulnerability of the synchronization network to meaconing attack pursued to backup-free network timing nodes. The attacks was indeed not mitigated with the proposed solutions due to unavailability of a backup timing source in the testbed. However, all other timing nodes kept a maximum synchronization error within 2 ns w.r.t the reference.

D. Non-coherent, single-frequency, spoofing

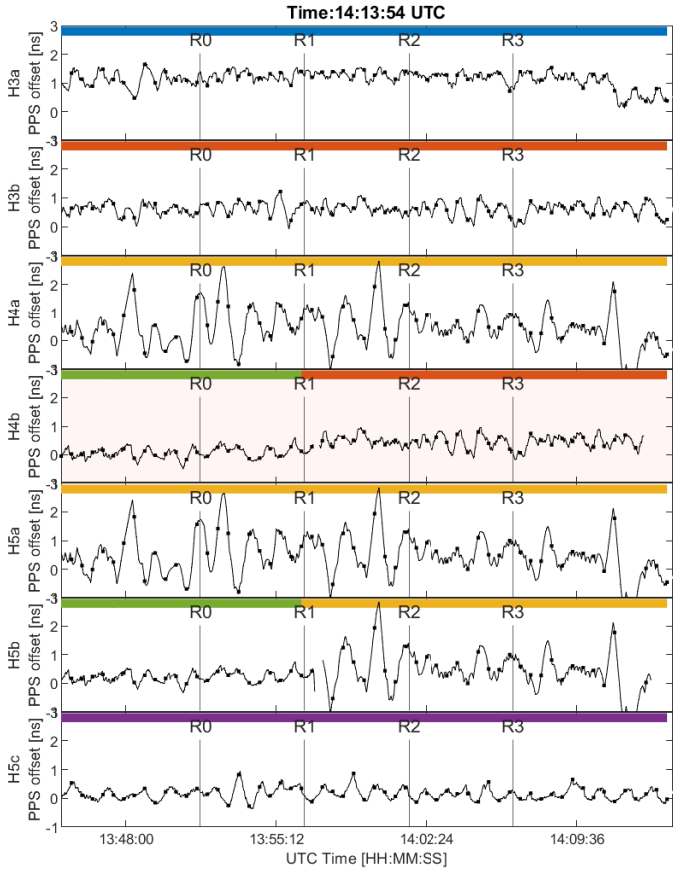
In this test, the GNSS timing receiver embedded in the network timing node at H4b was interfered with a non-coherent, simplistic spoofing attack on E1/L1, preceded by a short jamming attack to induce the GNSS receiver to lose the tracking of the real GNSS signals and force the processing of false, spoofed signals. The test was executed according to the test phases in Table V. The test started with nominal GNSS signal conditions, then at approximately 15:21:15, the jammer was switched on with the levels of signal power reported in Table V, similarly to the H4b_WB_J_L1L2L5 test. This pre-emptive jamming attack was conducted to force the GNSS timing receiver to unlock the tracking of real GNSS signals. However, in this case, the GNSS timing receiver was able to mitigate the interference due to its limited signal power, similarly to the R1-R3 phases of the H4b_WB_J_L1L2L5 test.



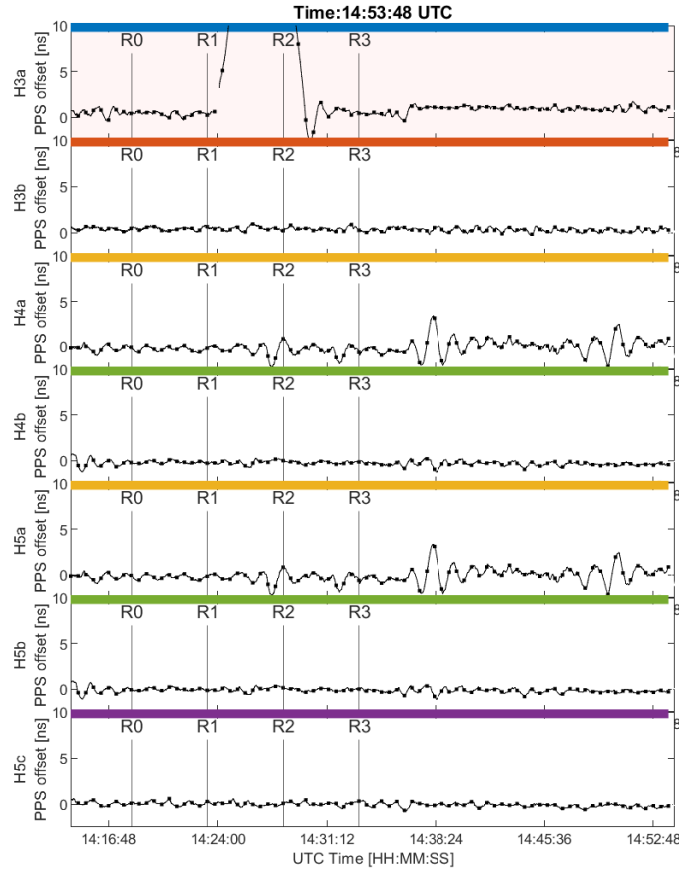
(a) SN-MF-WBJ: Single-node, multi-band, WB jamming



(b) MN-MF-WBJ: Multi-node, multi-band, WB jamming



(c) SN-MF-AM: Single-node, analog meaconing



(d) SN-MF-AM: Single-node, analog meaconing

Fig. 6: Sample results on PPS trends during RFI attacks against GNSS timing receivers embedded in the D-GMC.

The subsequent spoofing attack also failed: the receiver stayed in-lock with the legitimate GNSS signals and kept generating its 1-PPS signal, with a maximum error w.r.t the reference within 2 ns. With the GNSS timing receiver able to mitigate the attacks and protect the H4b node from interference, as expected, no other effects propagates throughout the network, which kept sufficient synchronization performance, with all nodes synchronized within 2 ns w.r.t. the Rb AC.

V. Conclusions

Since the introduction of 5G-NR, mobile broadband telecommunication networks have imposed stringent synchronisation requirements among RANs nodes. The scalability of atomic clock-based timing nodes within network timing infrastructures cannot easily sustain this trend, therefore high-accuracy timing transfer protocols are employed that may preserve the synchronization budget across the different network hierarchical levels. To cope with such needs, GNSS timing receivers in combination with the WR-PTP HA protocols have been proposed in this study to be integrated as D-GMCs at the different hierarchical layers of the network infrastructure. This solution is however affected by vulnerabilities, represented by GNSS antennas that expose the timing network to malicious RF attacks aiming at disrupting network operations. The extensive test campaign performed within the ROOT project assessed the capability of the WR-PTP HA timing network to maintain an inter-node synchronization within 2 ns among all the GNSS-disciplined nodes despite of any tested RF attack. The timing network has been demonstrated to be resilient to malicious actions by relying first on the embedded anti-jamming and anti-spoofing solutions of the state-of-the-art GNSS timing receivers, and, in case of effective RFI attacks, by leveraging on the proposed backup logic that switches among the different timing sources of the proposed network architecture.

Acknowledgements

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. A. Minetto acknowledges funding from the research contract no. 32-G-13427-5 DM 1062/2021 funded within the Programma Operativo Nazionale (PON) Ricerca e Innovazione of Italian Ministry of University and Research.

References

[Kap, 2006] (2006). *Understanding GPS: principles and applications*. Artech House mobile communications series. Artech House, Boston, 2nd ed edition.

[ITU, 2022] (2022). Minimum requirements related to technical performance for imt-2020 radio interface(s). page 11.

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

[Agiwal et al., 2016] Agiwal, M., Roy, A., and Saxena, N. (2016). Next generation 5G wireless networks: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, 18(3):1617–1655.

[Al-Falahy and Alani, 2017] Al-Falahy, N. and Alani, O. Y. (2017). Technologies for 5G networks: Challenges and opportunities. *IT Professional*, 19(1):12–20.

[Borio and Gioia, 2021] Borio, D. and Gioia, C. (2021). Interference mitigation: impact on GNSS timing. *GPS Solutions*, 25(2):37.

[Cai et al., 2022] Cai, Y., Llorca, J., Tulino, A. M., and Molisch, A. F. (2022). Compute- and data-intensive networks: The key to the metaverse. (arXiv:2204.02001). arXiv:2204.02001 [cs, eess].

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

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

[ENISA, 2019] ENISA (2019). *ENISA threat landscape for 5G networks: threat assessment for the fifth generation of mobile telecommunications networks (5G)*. Publications Office, LU.

[Ericsson, 2022a] Ericsson (2022a). Ericsson mobility report. https://www.ericsson.com/en/reports-and-papers/mobility-report.

[Ericsson, 2022b] Ericsson (2022b). This is 5G. https://www.ericsson.com/49f1c9/assets/local/5g/documents/07052021-ericsson-this-is-5g.pdf.

[Ghosh et al., 2019] Ghosh, A., Maeder, A., Baker, M., and Chandramouli, D. (2019). 5G evolution: A view on 5G cellular technology beyond 3GPP release 15. *IEEE access*, 7:127639–127651.

[Gioia and Borio, 2021] Gioia, C. and Borio, D. (2021). Multi-layer defences for robust GNSS timing retrieval. *Sensors*, 21(23):7787.

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

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

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

[Lin et al., 2019] Lin, X., Grovlen, A., Werner, K., Li, J., Baldemair, R., Cheng, J.-F. T., Parkvall, S., Larsson, D. C., Koorapaty, H., Frenne, M., and Falahati, S. (2019). 5G new radio: Unveiling the essentials of the next generation wireless access technology. *IEEE Communications Standards Magazine*, 3(3):30–37.

[Lipiński et al., 2018] Lipiński, M., van der Bij, E., Serrano, J., Włostowski, T., Daniluk, G., Wujek, A., Rizzi, M., and Lampridis, D. (2018). White Rabbit applications and enhancements. In *2018 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, pages 1–7.

[Lipiński et al., 2011] 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.

[Loschmidt et al., 2009] Loschmidt, P., Gaderer, G., Simanic, N., Hussain, A., and Moreira, P. (2009). White Rabbit - sensor/actuator protocol for the CERN LHC particle accelerator. In *SENSORS, 2009 IEEE*, pages 781–786.

[Minetto et al., 2022] Minetto, A., Polidori, B. D., Pini, M., and Dovis, F. (2022). Investigation on the actual robustness of GNSS-based timing distribution under meaconing and spoofing interferences. In *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, pages 3848–3862.

[Moreira et al., 2009] Moreira, P., Serrano, J., Wlostowski, T., Loschmidt, P., and Gaderer, G. (2009). White Rabbit: Sub-nanosecond timing distribution over ethernet. In *2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, pages 1–5. IEEE.

[Niu et al., 2015] 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 et al., 2016] Osseiran, A., Monserrat, J. F., and Marsch, P. (2016). *5G mobile and wireless communications technology*. Cambridge University Press.

[Pini et al., 2021] 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)*, page 288–293, Naples, Italy. IEEE.

[Qualcomm, 2022] Qualcomm (2022). Everything you need to know about 5G. https://www.qualcomm.com/5g/what-is-5g.

[Ruffini et al., 2021] Ruffini, S., Johansson, M., Pohlman, B., and Sandgren, M. (2021). 5G synchronization requirements and solutions. page 14.

[Serrano et al., 2013] Serrano, J., Cattin, M., Gousiou, E., van der Bij, E., Wlostowski, T., Daniluk, G., and Lipinski, M. (2013). The White Rabbit project.

[Seven Solutions, 2022] Seven Solutions (2022). *WR-Z16 The reliable precise time fan-out for White Rabbit distribution on 1G Ethernet-based networks.* Seven Solutions.

[Thongtan et al., 2017] Thongtan, T., Tirawanichakul, P., and Satirapod, C. (2017). Precise receiver clock offset estimations according to each global navigation satellite systems (GNSS) timescales. *Artificial satellites*, 52(4):99–108.

[Venmani et al., 2018a] Venmani, D. P., Lagadec, Y., Lemoult, O., and Deletre, F. (2018a). Phase and time synchronization for 5G C-RAN: Requirements, design challenges and recent advances in standardization. 5(15):7.

[Venmani et al., 2018b] Venmani, D. P., Lagadec, Y., Lemoult, O., and Deletre, F. (2018b). 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).

Alex Minetto (GS'17-M'20) 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 2021 as researcher and assistant professor. His current research interests cover navigation signal design and processing, advanced Bayesian estimation applied to Positioning, Navigation and Timing Technologies (PNT).

Benoit Rat obtained his MSc in communication systems in 2008 from the Swiss Federal Institute of Technology in Lausanne (EPFL) and joined Seven Solutions (acquired by Orolia in 2021) as Embedded Software Developer. In 2010, he started collaborating with CERN's Timing Group on the development of the White Rabbit Technology and since, he has continued bringing sub-nanosecond synchronization (PTP-HA v2019) to a wide range of devices in time-critical infrastructures. Currently, as Solution Architect, he is responsible of identifying market needs and trends (i.e. fintech, datacenters, telecom) and to design and deploy innovative solutions.

Marco Pini received the M.Sc. and Ph.D. degrees in telecommunications engineering from Politecnico di Torino, Turin, Italy, in 2003 and 2006, respectively. In light of the experience gained on GNSS receivers and performance, he has been responsible for several R&D activities and funded projects and acted as project coordinator of ROOT (Rolling Out OSNMA for the secure synchronization of Telecom networks), funded by the EC under the H2020 framework program. His research interests include the field of baseband signal processing of new GNSS signals, multi-frequency RF front-end design, and software radio receivers.

Brendan David 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.

Ivan De Francesca graduated in Electrical Engineering at Instituto Tecnológico de Buenos Aires (ITBA), in 2000. In 2011 he got a Postgraduate Diploma as Management Engineering Specialist from Universidad Tecnológica Nacional (UTN) in Buenos Aires. In 2000 he joined Alcatel-Techint as Project Engineer where he developed site engineering installation engineering design of SDH/SONET, DWDM & ADSL equipment. At present, he is a Transport Manager in Telefónica's GCTIO team, which he joined in 2011 from Movistar Argentina, where he started his career in Telefonica as Transmission Planning Engineer, in 2004. He currently addresses Optical and Microwave Technologies, Global Network Synchronization Strategy, Backhaul Planning and Network Evolution towards 5G deployments providing technical support to Group Operators, Global Procurement and Controlling areas.

Luis Contreras Murillo holds an M.Sc. in Telecommunications from the Universidad Politécnica de Madrid (1997), an M. Sc. in Telematics jointly from the Universidad Carlos III de Madrid and the Universitat Politècnica de Catalunya (2010), and a Ph.D. cum laude in Telematics from the Universidad Carlos III de Madrid (2021). In 1997 he joined Alcatel Spain taking several positions (research and development, standardization, product development and customer engineering) in both wireless and fixed network fields. In 2006 he joined the network planning department of Orange in Spain taking responsibilities for the IP backbone planning. Between 2002 and 2010 he was also adjunct lecturer at the Telematics department of the Universidad Carlos III. Since August 2011 he is part of Telefonica I+D, Telefonica CTIO, working on scalable networks and their interaction with cloud, distributed services, and participating in several research projects at National and European level. He is an active contributor to different SDOs, such as IETF (author of 6 RFCs), O-RAN, ETSI.

Fabio Dovis (GS'98-M'01) 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 2020 he is a full 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 GNSS signals and receivers, and advanced signal processing for interference and multipath detection and mitigation, as well as ionospheric monitoring.