Nanosecond-Level Resilient GNSS-Based Time Synchronization in Telecommunication Networks Through WR-PTP HA

Nanosecond-Level Resilient GNSS-Based Time Synchronization in Telecommunication Networks Through WR-PTP HA

Alex Minetto, *Member, IEEE*, Benoit Rat, Marco Pini, Brendan David Polidori, Ivan De Francesca, Luis Contreras Murillo, and Fabio Dovis, *Member, IEEE*

***Abstract*—In recent years, the push for accurate and reliable time synchronization has gained momentum in critical infrastructures, especially in telecommunication networks, driven by the demands of 5G new radio and next-generation technologies that rely on submicrosecond timing accuracy for radio access network (RAN) nodes. Traditionally, atomic clocks paired with global navigation satellite systems (GNSS) timing receivers have served as grand master clocks, supported by dedicated network timing protocols. However, this approach struggles to scale with the increasing numbers of RAN intermediate nodes. To address scalability and high-accuracy synchronization, a more cost-effective and capillary solution is needed. Standalone GNSS timing receivers leverage ubiquitous satellite signals to offer stable timing signals but can expose networks to radio-frequency attacks due to the consequent proliferation of GNSS antennas. Our research introduces a solution by combining the white rabbit precise time protocol with a backup timing source logic acting in case of timing disruptive attacks against GNSS for resilient GNSS-based network synchronization. It has been rigorously tested against common jamming, meaconing, and spoofing attacks, consistently maintaining 2 ns relative synchronization accuracy between nodes, all without the need for an atomic clock.**

***Index Terms*—5G new radio (NR), global navigation satellite systems (GNSS), network synchronization, precise timing protocol (PTP), telecommunication networks.**

Manuscript received 6 February 2023; revised 28 September 2023; accepted 6 December 2023. Date of publication 4 January 2024; date of current version 15 March 2024. This work was developed within the ROOT project (www.gnss-root.eu) funded by the European Agency for the Space Programme (EUSPA) in part by the European Unions Horizon 2020 under Grant 101004261. 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. *(Corresponding author: Alex Minetto.)*

Alex Minetto, Brendan David Polidori, and Fabio Dovis are with the Department of Electronics and Telecommunications, Politecnico di Torino, 10129 Turin, Italy (e-mail: alex.minetto@polito.it; brendan.polidori@polito.it; fabio.dovis@polito.it).

Benoit Rat was with the Orolia (Safran Navigation & Timing), 18014 Granada, Spain. He is now with Safran S.A., 18014 Granada, Spain (e-mail: benoit.rat@orolia.com).

Marco Pini was with the LINKS Foundation, 10138 Turin, Italy. He is now with Civitanavi Systems S.p.A., 63827 Pedaso (FM), Italy (e-mail: marco.pini@linksfoundation.com).

Ivan De Francesca and Luis Contreras Murillo are with the Telefonica Spain, 28013 Madrid, Spain (e-mail: ivan.defrancesca@telefonica.com; luis-miguel.contrerasmurillo@telefonica.com).

Digital Object Identifier 10.1109/JSYST.2023.3341243

I. Introduction

IN TODAY's world, mobile traffic is scaling up, and its patterns are rapidly changing [1], [2], [3]. 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, e.g., television broadcasting and online gaming [4]. For these reasons, telecommunications operators are adopting strategies that allow exploiting both uplink and downlink spectra with greater efficiency and flexibility [5]. The higher data throughput has stimulated high-efficiency technologies demanding for stringent synchronization requirements and reliability.

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 [6], [7]. 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 time synchronization based on Global Navigation Satellite Systems (GNSS) is put forward as a synchronization solution in telecommunication networks, we take a step back to clarify the need for accurate and stable synchronization 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) [8]. It is intended to satisfy the high-performance requirements set by the International Telecommunication Union (ITU) for international mobile telecommunications for the year 2020 (IMT-2020) [8], [9]. The IMT-2020 has defined some of the key capabilities of 5G-NR [10] by setting user experienced downlink and uplink data rates to 100 and 50 Mb/s, respectively, as well as a user plane latency of 4 ms for eMBB and 1 ms for URLLC. Furthermore, 5G-NR has been designed to operate in the spectrum ranging from sub-1 GHz to millimeter wave bands [1]. Two frequency ranges (FR) addressing the different use cases are defined in [11], 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) [5], [12], which is one of the factors contributing to the stringent synchronization requirements addressed in this study. Indeed, TDD networks, both 4G LTE and 5G, require 1.5 μs maximum time error at the cell site to ensure compliant

TABLE I
ABSOLUTE AND RELATIVE SYNCHRONIZATION REQUIREMENTS IN 5G-NR NETWORKS [14], [15], [16]

Technology	Time-error Tolerance (TAE)	Timing reference
Rack Unit – Grand Master 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*

The target upper bound for this study is highlighted in gray and matches the most stringent TAE.

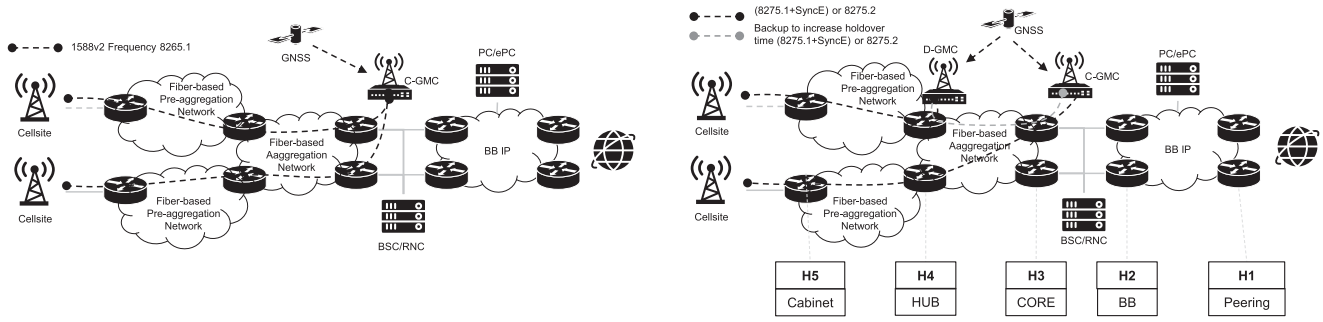

Fig. 1. Paradigm shift in the synchronization of telecommunication networks based on GNSS disciplined GMC. Centralized synchronization paradigm, based on C-GMC (a), is compared with a distributed approach featuring D-GMC and link backup for increased holdover time (b). FUSION hierarchical levels are indicated in (b), as referenced throughout the present article.

operation and effective resource sharing between uplink and downlink [2].

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 toward high-throughput, in order to exploit multiple-input multiple-output (MIMO) and transmitter diversity, *relative* synchronization budget between adjacent base stations is set to ± 65 ns [13], [14], that turns in a *relative* time error between base stations of ± 32 ns. The time synchronization requirements identified in [10], [14], [15], [16] are summarized for each specific technology in Table I.

As shown in the diagrams of Fig. 1, in order to meet these synchronization requirements, classical timing networks foresee a centralised grand master clock (C-GMC) node, which generates a coordinated universal time (UTC) traceable time reference by combining multiple timing sources. The C-GMC obtains a 10 MHz clock signal from rubidium (Rb) or cesium (Cs) 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, as show in Fig. 1(a). In combination with a specifically chosen precise timing protocol (PTP), the C-GMC distributes such an information throughout the network nodes [17]. IEEE 1588:2008 PTP has been proposed by the telecommunications industry to distribute the time synchronization derived by GNSS receivers [12]. Latest advances have been included in the PTP protocol through its high-accuracy profile, i.e., the IEEE-1588-2019 high accuracy (HA) that aims to bring subnanosecond accuracy by exploiting the white rabbit (WR) technology [17], [18].

However, following the increasing amount of network nodes, such a timing reference must be moved and replicated as close as possible to the radio access network (RAN) nodes 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 depicted in Fig. 1(b). 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 [3]. Although enhancing scalability, this approach may expose the network to intentional and unintentional radio frequency interferences (RFI), which may degrade synchronization and performance [19]. The limited awareness about this vulnerability is reflected by a lack of literature proposing suitable, state-of-the-art (SoA) solutions for counteracting such threats.

Indeed, 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 network nodes and may lead to disruption of nominal network operations along with distributed failures over critical infrastructures to a large extent.

SoA, multifrequency, multiconstellation GNSS timing receivers have been proposed to guarantee reliable, ns-level accuracy in both *relative* and *absolute* synchronization between the GNSS constellations and the network timescale [20], [21]. Along with an enhanced timing accuracy, they indeed embed specific solutions to detect and mitigate common RFI, such as jamming, meaconing, and spoofing [22]. However, RFI detection and mitigation at the timing receivers do not inherently ensure the network's insusceptibility to these events. The infrastructure is expected to autonomously discriminate reliable and

unreliable timing sources to maintain a trustworthy synchronization and sustain high-performance communication services.

To satisfy stringent time and phase synchronization requirements and ensure a high resilience against RF attacks against the GNSS timing source, this work proposes a combination of SoA GNSS timing receivers embedded in dedicated network timing units which support white rabbit precision time protocol (WR-PTP) for the distribution of ns-level timing information. Such SoA technologies are coupled with a novel algorithm for the autonomous discrimination of reliable timing sources which protect the network against potential GNSS vulnerabilities. This solution also contributes to tradeoff 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 to a large extent.

The rest of this article is organized as follows. Section II details the SoA in terms of timing infrastructures 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 WR-PTP 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. Finally, Section V concludes this article.

II. Background

A. Timing in Broadband 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 Telefónica. 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 follows.

1) H5: the most distributed level where mobile base stations connect or a preaggregation level depending on the specifics of the country. Typically, it hosts cell site routers (CSR) or small form-factor aggregation routers.
2) H4: is the metro aggregation level where fixed subscriber access nodes [e.g., gigabit passive optical network (GPON) optical line terminal (OLT)] are connected.
3) 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), authentication, authorization, and accounting) are connected.
4) H2: national backbone level. The nodes at this level act as pure Multiprotocol Label Switching (MPLS) routers. These routers can be based on platforms optimized for plain packet switching, yielding a more cost-effective solution.
5) H1: interconnection level to external networks.

By considering such a modern network architecture and stressing those levels embedding GNSS timing sources, our research aims to understand the effect of RF attacks on different hierarchical nodes and the cascading effects on the network. Due to the typical geo-location of C-GMCs and D-GMCs, the effect of RF attacks will be analyzed over H3, H4, and H5 levels. As previously stated, nodes synchronization is achieved with the combination of existing GNSS timing receivers and WR-PTP while robustness against the threats is pursued through a dedicated algorithm for the autonomous backup of the reference timing nodes in case of GNSS failures.

B. GNSS Timing Sources and 1-PPS Generation

Global Positioning System (GPS), Galileo, GLONASS, and Beidou navigation signals carry specific pseudonoise (PN) ranging codes, usually referred to as pseudorandom 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 radionavigation signal transmitted by a generic ith GNSS satellite reaches the receiver antenna and can be modelled as

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

where $P_{R,i}$ indicates the received signal power, D_i represents the amplitude value of the code subcarrier, C_i represents the amplitude value of the code symbol, i.e., the code chip, S_i represents the amplitude value of the code subcarrier, and f_c is the carrier frequency. The carrier frequency f_c is influenced by the term $f_{d,i}$, representing the Doppler shift due to the relative velocity between the ith satellite and the receiver. $\Delta\phi_i$ indicates a phase shift, and finally, $n(t)$ denotes the thermal noise term.

In principle, the code tracking of a single GNSS navigation signal is sufficient to discipline the generation of a rough clock signal. A higher precision can be achieved by means of carrier phase tracking [23]. However, code Doppler effect, unknown propagation time, and satellite's and receiver's oscillators biases make such a clock signal misaligned with respect to any conventional time scale.

To steer a dedicated local oscillator and discipline an actual one pulse-per-second (1-PPS) timing signal aligned to a given GNSS constellation time-scale, all of these biases must be compensated [24]. Therefore, the generation process of the 1-PPS strictly depends on the position, velocity, and time (PVT) solution [25], 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 [23]. The receiver clock bias, δt_u, is common to all the received signals and is estimated through the 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 time scale with a given uncertainty. Such an uncertainty is lower-bounded by the uncertainty of the receiver's clock bias estimation. The subsystem that generates the 1-PPS wavefronts is able to steer it almost continuously. Any action that can alter the aforementioned delays may immediately affect the disciplination of the output 1-PPS.

By assuming a conventional rising edge in the origin of the time axis at $t = 0$, we can model each pulse as a delayed rectangular pulse

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

where T_{PPS} is the pulse duration and it can be typically customised in high-end receivers, T_{DC} is the duty cycle 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 modeled as a train of (2)

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

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

C. RF Threats 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 [26]. 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 [27].

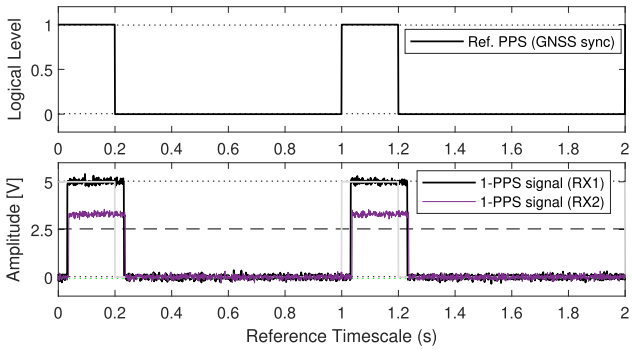

Fig. 2. Pictorial view of an ideal, reference 1-PPS (top) and real realizations (bottom), generated by independent GNSS receivers (i.e., RX1, RX2), and affected by thermal noise.

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 modeled 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 $(f_1 - f_0)/T$. 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

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

where $\bar{s}_{\text{RF},f_c}(t)$ 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 generate 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 antijamming algorithms are able to mitigate such attacks but ultimately succumb to high RFI 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 rebroadcasting of legitimate signals used as counterfait counterparts. 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 desynchronization 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

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

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 utilized as a warning system to prevent meaconing attacks, especially in static applications. However, this is typically not implemented in SoA timing receivers.

3) Simplistic, Noncoherent Spoofing: When working with static targets, we define a noncoherent, 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 w.r.t. the the current legitimate GNSS signals. 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 noncoherent spoofing signals reach the receiver they can be modeled as

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

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

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

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 PVT. Depending on the algorithms that are implemented in the receiver, it can send an alarm if large changes in the estimated states are detected. If the receiver switches from using legitimate GNSS signals to noncoherent, spoofed signals a jump in the 1-PPS is to be expected.

Solutions to countering simplistic, noncoherent spoofing can be as simple as using a real time clock (RTC), that after initialization is able to keep track of time within a certain error margin w.r.t. the system time. This margin can guarantee a threshold that blocks any noncoherent spoofing attacks inducing larger time offsets.

D. White Rabbit PTP to Distribute High-Accuracy Timing

The WR technology is an open-source synchronization project that was launched in 2009 [28], [29], [30], [31]. It is developed through the collaboration of various international public scientific organizations, i.e., 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. Sub-nanosecond time synchronization accuracy is achieved through the use of standard technologies, such as Ethernet, Precise Timing Protocol (PTP), and Layer 1 (ISO/OSI) synchronization, similar to Synchronous Ethernet (SyncE). The WR-PTP guarantees high-precision frequency distribution, with uncertainties within 50 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 [32], but its application to telecommunication networks is a current research frontier. The standard WR-PTP link operates in a master–slave model, where time information is passed from the parent to the child 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 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 Gb 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 parent clock to distribute time to child 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 parent and child 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 parent and child. 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 the propagation delay to eliminate uncompensated

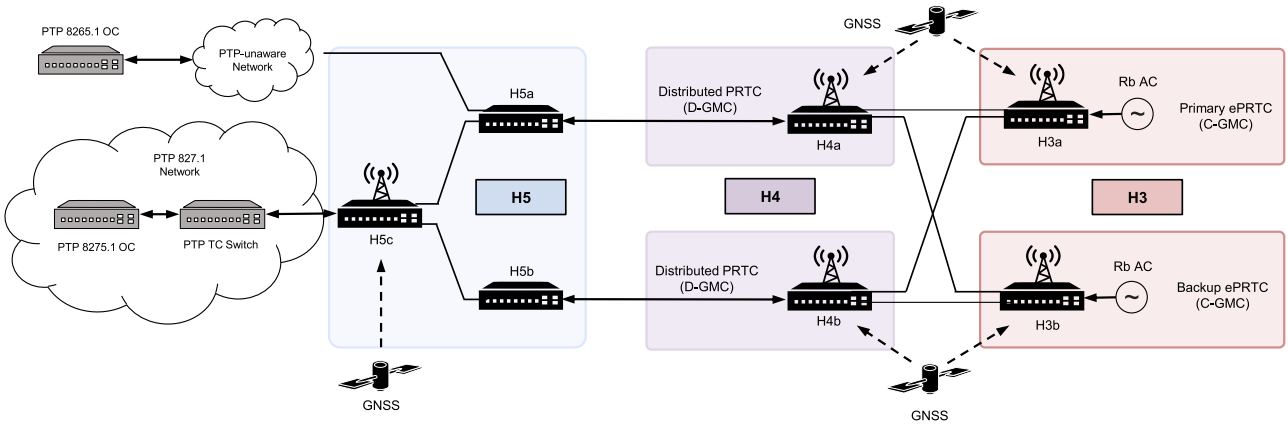

Fig. 3. Mapping of the ROOT timing network architecture to the reference topology of Fig. 1(b).

synchronization offsets, which makes the setup process easier by using precalibrated values to account for varying propagation speeds and fixed delays. The default precalibration settings allow for a maximum link distance of up to 10 km.

2) High-Accuracy Standardization: The IEEE 1588 Precision Time Protocol standard is set to include a new high-accuracy profile, based on the current WR-PTP technology and has been standardized 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 multiple, dedicated timing nodes for each hierarchical level.

To understand the methodology of the attacks against the different hierarchical levels we must first analyze how timing information is shared between the different levels. Fig. 3 shows a diagram describing how synchronization is distributed (right-to-left) throughout the proposed network architecture. The nodes at the upper layers, which are equipped with a GNSS receiver, utilise the GNSS timescale as their main timing source during nominal operation. Therefore, they are expected to be vulnerable to RF threats. In the diagram, the vulnerable 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. These hardware units are identical devices embedding WR-PTP HA capabilities and a GNSS timing receiver, while H5a and H5b do not host a GNSS timing receiver. Labels *a*, *b*, and *c* are generally used to distinguish timing nodes associated to the same hierarchical level. However, labels *a* and *b* are exploited for nodes at H3 level to discriminate main (*a*) and backup (*b*) timing node, respectively. The nodes that are not equipped with GNSS receivers, behave as followers, using WR-PTP to inherit accurate time and phase synchronization from a leader node.

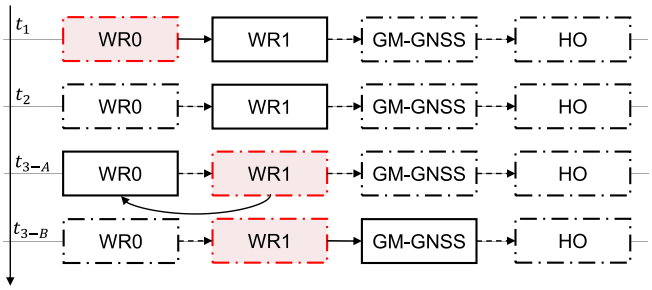

Fig. 4. FOCA decision making process for establishing the reference clock when time source faults occur. WR0 and WR1 labels Indicate WR-enabled units, GM-GNSS indicates GNSS-based timing nodes, while HO indicates holdover nodes in free-running.

B. Timing Source Backup Logic FOCA Versus 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 1) provides a deterministic behavior, 2) does not allow a new rogue node to become the active reference. Furthermore, 3) recovery to a normal state must be supervised by an operator. Eventually, FOCA 4) allows switching between cross WR-PTP profiles and multiple external timing sources, and 5) is optimized for a tree network topology. In Fig. 4, we can see how the timing sources are chosen. Starting in state t_1, the main WR0 source is seen as unreliable, 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 node, WR0, is eligible is switches back to it, while in t_{3-B} the algorithm continues to

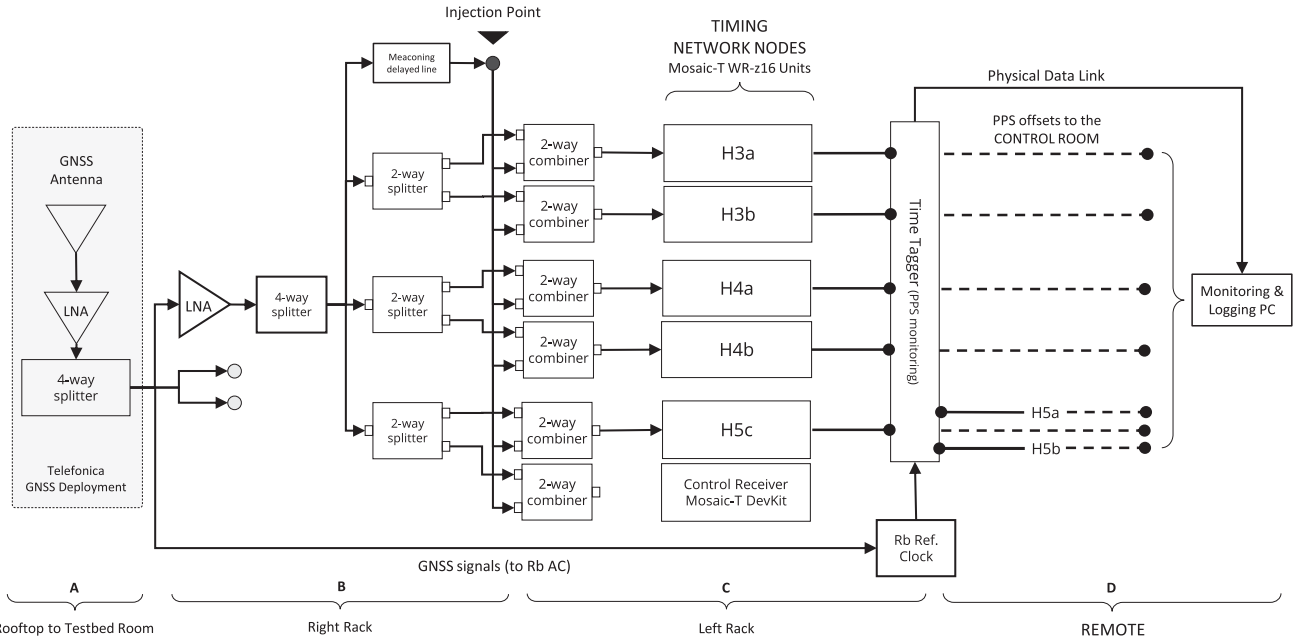

Fig. 5. Testbed for the analysis of GNSS-based relative synchronization among timing nodes at the various network hierarchical levels.

fall down the hierarchy of timing sources, this time switching to the GNSS source, i.e., GM-GNSS. Clock failures can occur due to many different causes among which link failure or drops in packets flow. Other error sources may be hard to identify. For additional details we invite the reader to refer to [33].

C. Selection of GNSS Timing Receivers

To select a suitable GNSS timing source for the proposed timing infrastructure, a set of SoA GNSS timing receivers was tested against RF attacks in the early phase of the ROOT project [17]. Comparative analysis were performed to assess the robustness of SoA devices embedding dedicated antijamming and antispoofing capabilities [25]. The selected multiband, multiconstellation GNSS timing receiver demonstrated a superior resilience against chirped jamming signals and simplistic spoofing attacks. However, the selected timing receiver was vulnerable to spoofing if rebooted 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 oversaturation of the front-end due to a high interfering power. The main technical features of the target GNSS timing receiver were discussed in [25].

D. Experimental Setup

The testbed shown in the block diagram of Fig. 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.
B) Testbed room (Right-rack): GNSS signal conditioning subsystems, distribution, and interference generation units.
C) Testbed room (Left-rack): Timing network nodes, reference Rb Atomic Clock (AC), and 1-PPS time-tagger unit.
D) Remote control room (REMOTE in Fig. 5).

The GNSS signals, received by a high-end choke ring antenna and preamplified 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 transferred through identical coaxial cables and 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 typical geographical deployment of network layers and nodes, a set of meaningful scenarios was identified in Table II. The different attacks, designed according to the literature review of Section II, are mainly distinguishable by: 1) class of RFI; 2) single-node (SN) versus multinode (MN) targets, and 3) single-frequency (SF) versus multifrequency (MF). When an attack was performed simultaneously on multiple nodes, the affected nodes were assumed reasonably colocated in a real network deployment, and reasonably sharing the same GNSS

TABLE II
BATCH OF RFI VULNERABILITY TESTS PERFORMED WITHIN THE ROOT TEST CAMPAIGN AGAINST THE TIMING NETWORK

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

Results of the test on the highlighted scenarios are extensively discussed in section IV.

TABLE III
REFERENCE JAMMING POWER FOR JAMMING SCENARIOS[1]

Test phase[1,2]	L1/E1 RFI power[1,3]	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 → R0)	End of Test (EoT → R0)

[1]Testbed fixed attenuation:−50 dB.
[2]Reference signal bandwidth $B_{L1} = 40$ MHz.
[3]Reference signal bandwidth $B_{L2+L5} = 90$ MHz.

TABLE IV
TEST PHASES FOR NONCOHERENT 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)

TABLE V
TEST PHASES FOR NONCOHERENT 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)

antenna and wired line. The actual risk associated to the different attack scenarios have been analyzed in [25].

The test procedures designed for the execution of the attacks are summarized in Tables III–V. Test procedures were designed in the preliminary phases of the study and are detailed in [25].

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 realizations of the same test were pursued showing the same results but they have been omitted from this article for the sake of synthesis.

Each plot in Fig. 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, and shown in Fig. 5. The labels on the *y*-axis indicate the corresponding network node, e.g., H3a in the upper subplot. The common *x*-axis depicts the timeline of each experiment. The change in the *x*-axis among the figures is due to the actual time-span at which experiments were performed during the test campaign. The dark-shaded background with the thicker curve indicates the nodes under attack. Furthermore, for each subplot, a colored 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 the upper hierarchical levels, thus showing strips of the same color. For example, in Fig. 6(a), 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 a GNSS receiver and in fact, it has a purple colored 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, Multiband 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 is reported in Fig. 6(a). The test started with nominal GNSS signal conditions, then at approximately 11:16:49 UTC, 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

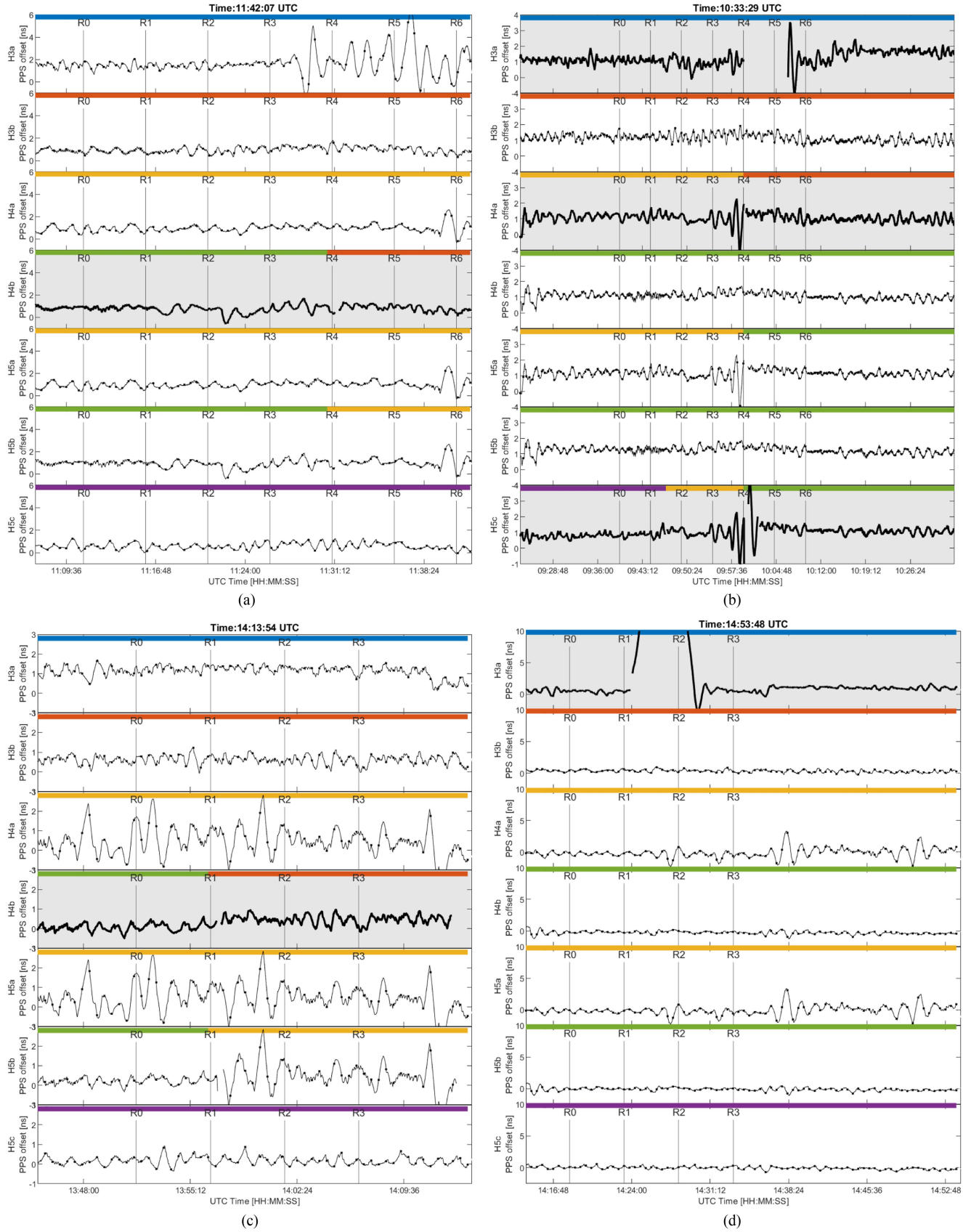

Fig. 6. Sample results on 1-PPS error trends during RFI attacks against GNSS timing receivers embedded in the D-GMC. Shaded subplots with thicker curves indicate nodes under attack. For details refer to Table II. (a) SN-MF-WBJ: Single-node, multiband, WB jamming. (b) MN-MF-WBJ: Multinode, multiband, WB jamming (c) SN-MF-AM: Single-node, analog meaconing (d) SN-MF-AM: Single-node, analog meaconing.

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 colored 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 H5b 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.

B. Multinode, Multiband 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 Fig. 6(b). The test started with nominal GNSS signal conditions, then at approximately 9:45:24 UTC, 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 dBm (L1/E1) and −32.3 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 colored 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 dBm (L1/E1) and −56.40 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 Fig. 6(d). The test started with nominal GNSS signal conditions, then at approximately 13:56:33 UTC, 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 node under attack, 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 UTC, 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 Fig. 6(d) that the meaconing produced a timing error for the whole duration of the attack (R1 to R2). The error quickly overcame 10 ns and it reached up to 150 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 1) short-lasting unavailability of the 1-PPS signal for few seconds at the beginning and the end of the attack and 2) a bias on the GNSS disciplined 1-PPS signal of approximately 150 ns, as evident in the upper subplot of Fig. 6(c). 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. Noncoherent, Single-Frequency, Spoofing

In this test, the GNSS timing receiver embedded in the network timing node at H4b was interfered with a noncoherent, 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. It started with nominal GNSS signal conditions, then at approximately 15:21:15 UTC, 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. The subsequent spoofing attack was not effective, as well: the receiver stayed in-lock with the legitimate GNSS signals and the node kept generating its 1-PPS signal, with a maximum error with respect to the reference within 2 ns. Given that a receiver reboot was not performed (as indicated for achieving effective attacks in reference [25]) since assumed unrealistic, and mainly due to the inconsistency of the received signals, the receiver kept tracking legitimate signals while disregarding illegitimate ones.

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. Conclusion

The rise of 5G-NR networks and related high-performance solutions demand submicrosecond synchronized RAN nodes, requiring, in turn, high-accuracy timing protocols to distribute atomic clock-based timing references. Combining GNSS receivers and WR-PTP HA protocols, proposed as D-GMCs, preserves the synchronization budget across the network layers. However, GNSS antennas expose vulnerabilities to malicious RF attacks, endangering network functionality. The solution proposed and tested through this study demonstrated WR-PTP HA's capability to maintain internode synchronization within 2 ns despite RF attacks. The network's resilience involves GNSS receivers' antijamming, antispoofing, and autonomous backup logic for source switching during RFI attacks, upholding tight nodes synchronization.

Acknowledgment

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 organization or products.

References

[1] N. Al-Falahy and O. Y. Alani, "Technologies for 5G networks: Challenges and opportunities," *IT Professional*, vol. 19, no. 1, pp. 12–20, Jan. 2017.
[2] Infinera, *Synchronization Distribution in 5G Transport Networks*. San Jose, CA, USA: Infinera, 2022.
[3] Ericsson, "Ericsson mobility report," Nov. 2022. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report
[4] Y. Cai, J. Llorca, A. M. Tulino, and A. F. Molisch, "Compute- and data-intensive networks: The key to the metaverse," in *Proc. 1st Int. Conf. 6G Netw.*, Paris, France, 2022, pp. 1–8, doi: 10.1109/6GNet54646.2022.9830429.
[5] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, Jul.–Sep. 2016.
[6] Qualcomm, "Everything you need to know about 5G," Aug. 2022. [Online]. Available: https://www.qualcomm.com/5g/what-is-5g
[7] Ericsson, "This is 5G," Aug. 2022. [Online]. Available: https://www.ericsson.com/49f1c9/assets/local/5g/documents/07052021-ericsson-this-is-5g.pdf
[8] Minimum requirements related to technical performance for IMT-2020 radio interface(s)," p. 11, 2022. [Online]. Available: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf
[9] X. Lin et al., "5G new radio: Unveiling the essentials of the next generation wireless access technology," *IEEE Commun. Standards Mag.*, vol. 3, no. 3, pp. 30–37, Sep. 2019.
[10] H. Li, L. Han, R. Duan, and G. M. Garner, "Analysis of the synchronization requirements of 5G and corresponding solutions," *IEEE Commun. Standards Mag.*, vol. 1, no. 1, pp. 52–58, Mar. 2017.
[11] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5G evolution: A view on 5G cellular technology beyond 3GPP release 15," *IEEE Access*, vol. 7, pp. 127639–127651, 2019.
[12] S. Ruffini, M. Johansson, B. Pohlman, and M. Sandgren, "5G synchronization requirements and solutions," p. 14, 2021. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-synchronization-requirements-and-solutions
[13] D. P. Venmani, Y. Lagadec, O. Lemoult, and F. Deletre, "Phase and time synchronization for 5G C-RAN: Requirements, design challenges and recent advances in standardization," *EAI Endorsed Trans. Ind. Net. Intell. Syst.*, vol. 5, no. 15, p. e3,Aug. 2018.
[14] E. T. S. I. 3GPP, "Base station (BS) radio transmission and reception," European Telecommunications Standards Institute - 3GPP, Tech. Rep., Jul. 2020.
[15] A. Osseiran, J. F. Monserrat, and P. Marsch, *5G Mobile and Wireless Communications Technology*. Cambridge, U.K.: Cambridge Univ. Press, 2016.
[16] D. P. Venmani, Y. Lagadec, O. Lemoult, and F. Deletre, "Phase and time synchronization for 5G C-RAN: Requirements, design challenges and recent advances in standardization," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 5, no. 15, pp. e3–e3, Aug. 2018.
[17] M. Pini et al., "Satellite-derived time for enhanced telecom networks synchronization: The ROOT project," in *Proc. IEEE 8th Int. Workshop Metrology AeroSpace*, Naples, Italy, 2021, pp. 288–293. [Online]. Available: https://ieeexplore.ieee.org/document/9511780/
[18] F. Girela-López, J. López-Jiménez, M. Jiménez-López, R. Rodríguez, E. Ros, and J. Díaz, "IEEE 1588 high accuracy default profile: Applications and challenges," *IEEE Access*, vol. 8, pp. 45211–45220, 2020.

[19] ENISA, "ENISA threat landscape for 5G networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G). LU: Publications Office, 2019. [Online]. Available: https://data.europa.eu/doi/10.2824/49299
[20] P. Defraigne, "GNSS time and frequency transfer," in *Springer Handbook of Global Navigation Satellite Systems*, Berlin, Germany: Springer, 2017, pp. 1187–1206.
[21] T. Thongtan, P. Tirawanichakul, and C. Satirapod, "Precise receiver clock offset estimations according to each global navigation satellite systems (GNSS) timescales," *Artif. Satellites*, vol. 52, no. 4, pp. 99–108, 2017.
[22] C. Gioia and D. Borio, "Multi-layer defences for robust GNSS timing retrieval," *Sensors*, vol. 21, no. 23,pp. 7787–7805 , Nov. 2021.
[23] *Understanding GPS: Principles and Applications*, 2nd ed.Boston, MA, USA: Artech House, 2006.
[24] X. Niu, K. Yan, T. Zhang, Q. Zhang, H. Zhang, and J. Liu, "Quality evaluation of the pulse per second (PPS) signals from commercial GNSS receivers," *GPS Solutions*, vol. 19, no. 1, pp. 141–150, 2015.
[25] A. Minetto, B. D. Polidori, M. Pini, and F. Dovis, "Investigation on the actual robustness of GNSS-based timing distribution under meaconing and spoofing interferences," in *Proc. 35th Int. Tech. Meeting Satell. Division Inst. Navigation*, 2022, pp. 3848–3862.
[26] D. Borio and C. Gioia, "Interference mitigation: Impact on GNSS timing," *GPS Solutions*, vol. 25, no. 2, 2021, Art. no. 37.
[27] F. Dovis, *GNSS Interference Threats and Countermeasures*. Norwood, MA, USA: Artech House, 2015.
[28] M. Lipiński, T. Włostowski, J. Serrano, and P. Alvarez, "White rabbit: A PTP application for robust sub-nanosecond synchronization," in *Proc. IEEE Int. Symp. Precis. Clock Synchronization Meas. Control Commun.*, 2011, pp. 25–30.
[29] J. Serrano et al., "The white rabbit project," 2013. [Online]. Available: https://cds.cern.ch/record/1743073
[30] P. Loschmidt, G. Gaderer, N. Simanic, A. Hussain, and P. Moreira, "White Rabbit - Sensor/actuator Protocol for the CERN LHC Particle Accelerator," in *Proc. Sensors*, 2009, pp. 781–786.
[31] P. Moreira, J. Serrano, T. Wlostowski, P. Loschmidt, and G. Gaderer, "White rabbit: Sub-nanosecond timing distribution over ethernet," in *Proc. Int. Symp. Precis. Clock Synchronization Meas. Control Commun.*, 2009, pp. 1–5.
[32] M. Lipiński et al., "White rabbit applications and enhancements," in *Proc. IEEE Int. Symp. Precis. Clock Synchronization Meas. Control Commun.*, 2018, pp. 1–7.
[33] Seven Solutions, *WR-Z16 the reliable precise time fan-out for white rabbit distribution on 1G ethernet-based networks*. Granada, Spain: Seven Solutions, 2022.

Alex Minetto (Member, IEEE) received the B.Sc. and M.Sc. degrees in telecommunications engineering, and the Ph.D. degree in electrical, electronics, and communications engineering from Politecnico di Torino, Turin, Italy, in 2013, 2015, and 2020, respectively.

He joined the Department of Electronics and Telecommunications of Politecnico di Torino, in 2021 as a Researcher and Assistant Professor. His current research interests cover navigation signal design and processing, advanced Bayesian estimation applied to positioning, navigation, and timing technologies.

Benoit Rat received the M.Sc. degree in communication systems from the Swiss Federal Institute of Technology, Lausanne, Switzerland, in 2008.

He joined Seven Solutions (acquired by Orolia in 2021) as an Embedded Software Developer. In 2010, he started collaborating with CERNs Timing Group to the White Rabbit Technology by enabling sub-nanosecond synchronization (PTP-HA v2019) to a wide range of devices in time-critical infrastructures. He is currently a Solution Architect and is responsible of identifying market needs and trends 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 led 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 in electronic and telecommunications engineering from Politecnico di Torino, Turin, Italy, in 2019 and 2021, respectively.

He joined the Department of Electronics and Telecommunications, Politecnico di Torino, in 2022 as a Research Assistant. His research interests include methods of radio frequency interference mitigation, detection and localization, along with software-defined radios and digital signal processing.

Ivan De Francesca received the graduat degree in electrical engineering from Instituto Tecnológico de Buenos Aires, CABA, Argentina, in 2000, and received the Postgraduate Diploma as management engineering specialist from Universidad Tecnológica Nacional, Buenos Aires, Argentina, in 2011.

At present, he is a Transport Manager in Telefónicas GCTIO team. He currently addresses optical and microwave technologies, global network synchronization strategy, Backhaul planning, and network evolution toward 5G deployments providing technical support to group operators, global procurement, and controlling areas.

Luis Contreras Murillo received the M.Sc. degree in telecommunications from the Universidad Politécnica de Madrid, Madrid, Spain, in 1997, the M.Sc. degree in telematics jointly from the Universidad Carlos III de Madrid, Madrid, Spain, and the Universitat Politèctica de Catalunya, Barcelona, Spain, in 2010, and the Ph.D. *(cum laude)* degree in telematics from the Universidad Carlos III de Madrid, Madrid, Spain, in 2021.

Since 2011, he is part of Telefonica I + D, Telefonica CTIO, working on scalable networks and their interaction with cloud, distributed services. He is an active contributor to different SDOs, such as IETF (author of 6 RFCs), O-RAN, and ETSI.

Fabio Dovis (Member, IEEE) received the M.Sc. and Ph.D. degrees in electronics engineering from Politecnico di Torino, Turin, Italy, in 1996 and 2000, respectively.

In 2004, he joined the Department of Electronics and Telecommunications of Politecnico di Torino as an Assistant Professor and since 2020, he has been a Full Professor in the same department, where he coordinates the Navigation Signal Analysis and Simulation (NavSAS) research group. 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.

Open Access funding provided by 'Politecnico di Torino' within the CRUI CARE Agreement