POLITECNICO DI TORINO
Repository ISTITUZIONALE

Satellite-derived Time for Enhanced Telecom Networks Synchronization: the ROOT Project

*Original*
Satellite-derived Time for Enhanced Telecom Networks Synchronization: the ROOT Project / Pini, Marco; Minetto, Alex; Vesco, Andrea; Berbecaru, DIANA GRATIELA; Miguel Contreras Murillo, Luis; Nemry, Pierre; De Francesca, Ivan; Rat, Benoit; Callewaert, Krel. - ELETTRONICO. - (2021), pp. 288-293. (Intervento presentato al convegno 2021 IEEE 8th International Workshop on Metrology for AeroSpace (MetroAeroSpace 2021) tenutosi a Naples (Italy) nel June 23 - 25, 2021) [10.1109/MetroAeroSpace51421.2021.9511780].

*Availability:*
This version is available at: 11583/2918537 since: 2021-09-20T11:24:11Z

*Publisher:*
Institute of Electrical and Electronics Engineers (IEEE)

*Published*
DOI:10.1109/MetroAeroSpace51421.2021.9511780

*Terms of use:*

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

*Publisher copyright*
IEEE postprint/Author's Accepted Manuscript

©2021 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collecting works, for resale or lists, or reuse of any copyrighted component of this work in other works.

(Article begins on next page)

12 October 2024

# Satellite-derived Time for Enhanced Telecom Networks Synchronization: the ROOT Project


Marco Pini
*Space and Navigation Technologies*
*Fondazione LINKS*
Torino, Italy
marco.pini@linksfoundation.com

Alex Minetto
*Dept. of Electronics and Telecommunications*
*Politecnico di Torino*
Torino, Italy
alex.minetto@polito.it

Andrea Vesco
*Cybersecurity Area*
*Fondazione LINKS*
Torino, Italy
andrea.vesco@linksfoundation.com

Diana Berbecaru
*Dept. of Automatic and Computer Science*
*Politecnico di Torino*
Torino, Italy
diana.berbecaru@polito.it

Luis Miguel Contreras Murillo
line 2: *dept. name of organization*
*Telefonica*
Madrid, Spain
luismiguel.contrerasmurillo@telefonica.com

Pierre Nemry
Septentrio
*Septentrio*
Leuven, Belgium
pierre.nemry@septentrio.com

Ivan De Francesca
*Telefonica*
Madrid, Spain
ivan.defrancesca@telefonica.com

Benoit Rat
*Seven Solutions*
Granada, Spain
benoit@sevensols.com

Krel Callewaert
*Valdani Vicari e Associati (VVA)*
Brussels, Belgium
k.callewaert@vva.it



***Abstract* — Satellite-derived timing information plays a determinant role in the provisioning of an absolute time reference to telecommunications networks, as well as in a growing set of other critical infrastructures. In light of the stringent requirements in terms of time, frequency, and phase synchronization foreseen in upcoming access network architectures (i.e., 5G), Global Navigation Satellite System (GNSS) receivers are expected to ensure enhanced accuracy and reliability not only in positioning but also in timing. High-end GNSS timing receivers combined with terrestrial cesium clocks and specific transport protocols can indeed satisfy such synchronization requirements by granting sub-nanosecond accuracy. As a drawback, the network infrastructure can be exposed to accidental interferences and intentional cyber-attacks. Within this framework, the ROOT project investigates the effectiveness and robustness of innovative countermeasures to GNSS and cybersecurity threats within a reference network architecture.**



***Keywords—GNSS, OSNMA, cybersecurity, 5G, Precision Timing Protocol, White Rabbit, jamming, spoofing, authentication***


## I. Introduction

A well-known study of critical dependencies upon Global Navigation Satellite Systems (GNSS) identifies telecommunications, emergency services, energy, finance, food, and transport as the sectors where GNSS plays a key role [1]. GNSS is used as a timing source for the synchronization of various types of networks and has been recently defined as *the backbone of the connected world* and the *invisible utility* [2][3] to highlight its pervasive presence in digital infrastructures. Some of these are classified as *critical infrastructures* [4] and, together with other service architectures, pose security-related requirements on top of timing accuracy requirements.

5G networks pose new challenges to the management of multiple timing sources across the network. To realize the benefits of new Time Division Duplex (TDD) spectral efficiency, and the full potential of 5G, highly accurate time synchronization is needed at different hierarchical levels of the network architecture. There is also a need for increased reliability of the timing sources. While nowadays Long-Term Evolution-Frequency Division Duplex (LTE-FDD) networks can continue operating for hours after losing the synchronization without significant degradation, in the future, loss of timing will have an immediate impact on Radio Access Network (RAN) performance, as already assessed by an early analysis performed by Ericsson researchers who surveyed several operators in North America [5].

The increased risk associated with the unavailability of GNSS signals includes the growth of intentional Radio Frequency (RF) attacks and cyber threats. Added to this is the fact that network operators rarely perceive the vulnerability of GNSS receivers to interference as a real problem. The awareness about GNSS spoofing, namely the transmission of false signals with the intent to fool receivers, seems limited to the specialists' sector, while in most cases users and stakeholders continue to consider GNSS a pure, non-critical, commodity. This is even more manifest in the case of other critical infrastructures, where the importance of GNSS is less apparent. Nonetheless, a stationary GNSS receiver used for timing and synchronization is an ideal target for malevolent attacks because the antenna is static and often sited in a visible location [6]. Not by chance, the U.S. Department of Homeland Security released a presentation about the *"responsible use of GPS in critical infrastructures*" [7] targeting receiver developers, product/system integrators, and end-users. The purpose is fostering best practices to increase the resilience of operations reliant upon the civil GPS service, by improving receivers and equipment installed in fixed infrastructures.

In addition to enhanced signal processing and the use of backup technologies, the proposition of authenticated GNSS signals is seen as a new way to increase the resilience of satellite-based time synchronization. In fact, besides GNSS jamming activities, either malicious or unintended, GNSS signals can be corrupted by spoofers [8]. Recognizing the crucial role of authentication features to verify that a signal in the receiver came from satellites, the European Galileo program is gradually implementing authentication services to its 1st and 2nd generation of satellite signals, in order to enable authentication functionalities for future civil receivers. Galileo will provide these functionalities through the Open Service Navigation Message Authentication (OSNMA) and the Commercial Authentication Service [9][10]. Potentially, such a capability allows the detection of a subset of spoofing attacks and threats and can protect the synchronization of networks dependent upon satellite-derived time provisioning [11].

## II. SYNCHRONIZATION IN UPCOMING TELECOM NETWORKS

Telecom networks are in constant evolution. The coexistence of mobile technologies, from still-operational 2G to emerging 5G, imposes the necessity of maintaining legacy synchronization strategies while deploying State-of-the-Art (SoA) ones. The deployment of LTE-Advanced, LTE-TDD , and 5G introduce stringent requirements among which phase synchronization becomes mandatory. TDD operation and advanced features, such as enhanced inter-cell interference cancellation, coordinated multipoint, interference rejection combining, or the adoption of massive Multiple Input Multiple Output (MIMO) arrays, are examples where this type of synchronization is essential. For example, different antennas and coordination schemes are being discussed within the industry, which requires phase alignment ranging from 65 ns to 130 ns for 5G front-haul applications.

To achieve such accuracy, a Centralized Grandmaster Clock (C-GMC) node generates a time reference by combining different time sources (i.e., multi-constellation, multi-frequency GNSS receivers, multiple co-located atomic clocks), whereas specific transport protocols are exploited to distribute the synch information across the network. Commonly, the C-GMC gets its time reference using conventional 1-Pulse Per Second (1-PPS) and 10 MHz clock signals from a GNSS receiver. The synch is then distributed via e.g. optical fiber to any other devices connected to the network with sub-nanosecond accuracy. To ensure the distribution of phase-synch quality signals throughout the entire network, proper signal regeneration is needed. Figure 1 shows a high-level network architecture, with phase synch distribution with enhanced holdover. If GNSS signals are degraded or blocked, because of intentional interference, local atomic clocks and robust network-distributed timing protocols can be seen as a temporary backup solution to preserve network operational capabilities. Increased robustness and resilience to any possible lack of a common time reference can be achieved through multiple reference clocks distributed across the network, namely Distributed GMC (D-GMC).

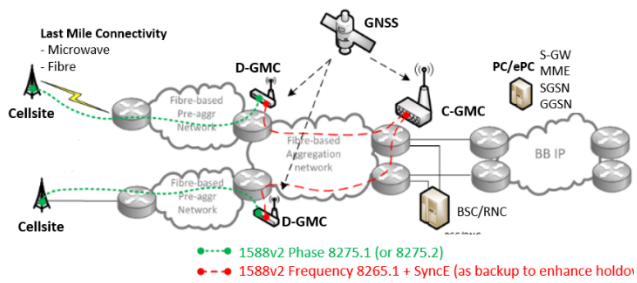


Figure 1: High-level diagram showing a possible implementation for phase synchronization distribution, with enhanced holdover

From the high-level diagram reported in Figure 1, one preliminary remark can be already derived. No matter if the deployment is completely based on GNSS receivers on every cell site, or only placed at C-GMC or D-GMC, all scenarios are pointing out a vulnerability of the network synch associated with the poor capability of many consumer-grade GNSS receivers to tackle jamming/spoofing attacks. On the other hand, it is also probable that current precision will no longer be sufficient for future 5G and beyond technologies or applications, which would consequently lead to clock densification in the network (i.e., large number of D-GMCs).

### A. GNSS timing receivers

Many current telecom applications typically require nodes synchronization with accuracy on the order of 100 ns. Such synchronization is achieved by setting up a GNSS antenna at a fixed, surveyed location, and determining time independently. Network equipment generally embeds specialized timing receivers, which produce a PPS clock signal synchronized with UTC. The precision of the PPS pulse corresponds to the precision at which the clock bias can be estimated by the Position Velocity and Time (PVT) algorithm. Today most of the GNSS-based time synchronization modules on the market are based on low-cost GPS-only, single-frequency modules, which provide PPS accuracy in the range of 20 to 100 ns. Under open sky conditions, those modules do provide a stable time reference but are very sensitive to degradations. Those degradations range from an increase of the PPS jitter, due to a reduced number of satellites in view, to a complete loss of the PPS synchronization, in the case of jamming of the single GPS L1 C/A signal. A low-cost module usually embeds a low-stability clock, so the PPS stability is broken as soon as the receiver stops computing a valid solution. Without any doubts, the majority of timing receivers are relatively easy to jam and spoof given the low signal level handled at the antenna [11].

The use of high-end GNSS receivers as sources for PPS synchronization signals first would allow for decreasing the noise/jitter on the PPS signal thanks to the use of multi-frequency multi-constellation positioning. A second relevant aspect is the quality of the embedded crystal oscillator in the module. Clocks used in high-end GNSS receivers have better short-term stability allowing the PPS signal to remain stable for several (tens of) seconds after a complete loss of positioning solution. In some cases of unintentional interference (e.g., some events detected in the proximity of highways), this allows the bridging of the time when the interference is active.

The delays induced by the antenna and the coaxial cable cause a non-negligible bias in the generation of the PPS signal. Such a bias is typically irrelevant in positioning applications but is detrimental for high-accuracy time synchronization. Typical antennas introduce delays of a few tens of nanoseconds. Cable delays depend on the cable type and length, with typical values around 5 ns/m. In nanosecond-level synchronization, a calibration process is essential and it is achieved by measuring and compensating those delays. Calibration has no impact on the precision of the PPS signal but removes the absolute bias with regards to an absolute time reference like UTC. By calibration, the PPS accuracy can be achieved in the order of a few nanoseconds.

### B. ePRTC in Telecommunication Networks

A traditional C-GMC integrating a calibrated GNSS reference is referred to as Primary Time Reference Clock (PTRC) and when combined with a cesium clock it is transformed into an Enhanced-PRTC (ePTRC). Defined by the ITU-T G8272.1 recommendation, the ePRTC aims to reduce the dependency on GNSS in case of outages by combining a primary time source to additional terrestrial atomic clocks deployed in the network. The system autonomously provides time, phase, and frequency references that are aligned and calibrated to the GNSS signal over a long

observation period, and then the time scale is maintained autonomously based on the stability of the atomic clock(s). To overcome costly upgrades, the evolution to phase-synch support is performed through the deployment of Distributed Grandmaster Clocks (D-GMC). Frequency synchronization with Synchronous Ethernet (SyncE) is still used as a backup for C-GMC in case of GNSS signal loss (red dashed lines in Figure 1). In such a way, phase synchronization accuracy in D-GMC can be maintained for a longer period.

### *C. Precise Timing Protocols for synchronization*

The Precision Time Protocol (PTP), also referred to as IEEE-1588 standard [12]-[15], aims to distribute time by measuring and compensating propagation time delays over the network. PTP defines an Ethernet-based distributed network of clocks organized in a master-slave hierarchy. A primary reference, namely the ePRTC, coordinates time across the entire PTP network. Redundant, secondary master clocks can take over when a failure is detected. PTP improves accuracy with respect to Network Time Protocol (NTP) by timestamping packets at the lowest levels of the hardware. PTP allows for synchronization in the range of 100µs being able to reach hundreds of nanoseconds through hardware assistance (SyncE) to comply with the requirements mentioned in Section II. Further enhancements to meet CERN tight requirements [16] has been achieved with the development of the White Rabbit PTP (WR-PTP) [17], an improved extension of PTP able to provide:

- absolute time synchronization and timestamping with sub-nanosecond accuracy;
- clock frequency distribution with a precision better than 50 ps;
- distribution through thousands of nodes and tens of kilometres, over standard optical fiber networks;
- not significantly dependent on network load, weather conditions or the number of hops.

Since WR-PTP has raised a great interest in the industry, it has been standardized into the new IEEE-1588-2019 High Accuracy (HA) profile to bring sub-nanosecond accuracy to a broader market, in particular addressing Telecom infrastructure.

Indeed, current network architectures might leverage WR-PTP/HA to achieve a synchronization across thousands of nodes with sub-nanosecond accuracy. In the ROOT framework, PTP and WR-PTP/HA are deployed in a realistic architecture by adopting redundant GNSS receivers which process OSNMA-authenticated Galileo signals, distributed over the network. Such receivers will act as multiple trustworthy time references, used to distribute synchronization through the network transparently. In addition to redundancy on the time references and sub-nanosecond time synchronization between nodes, WR-PTP/HA will be used to monitor the passive GNSS receivers.

## III. THE ROOT REFERENCE ARCHITECTURE

Over the years, to fulfill their service offering, Telecom operators have deployed separate or overlapping networks specifically targeted for each service (mobile traffic, fixed residential Internet traffic, fixed voice service, enterprise services...). This was partly motivated because of the time it has taken for Internet Protocol (IP) technology to become a universal protocol to carry any kind of service on top and based on the different Service Level Agreements (SLAs) required for each service.

A conventional architecture includes a Metro Ethernet aggregation network in parallel to a separate Mobile Backhaul, and then two different IP backbones, one for the residential services and another one for the corporate services. This implies a multiplicity of redundant hardware that many times has to be upgraded in cascade as traffic increases. This scenario leads to capital expenses and too complex architecture, resulting in an unsustainable network model to overcome the future challenges of providing new services and meeting explosive traffic growth.

To avoid scalability issues, Telefónica is currently transforming its IP networks according to the FUSION concept of an all-IP network. This concept makes use of end-to-end MultiProtocol Label Switching (MPLS) technology and is structured in five hierarchical levels, where nodes with similar functions in the previous architectures are consolidated into a single network element, thus improving scalability, security, flexibility, and cost reduction. Telefonica FUSION Hierarchy Levels (HLs) are the following:

- HL-5: the most distributed level where mobile Base Stations connect or a pre-aggregation level depending on the specifics of the country;
- HL-4: metro aggregation level where fixed subscriber access nodes (e.g. Gigabit Passive Optical Networks Optical Line Terminations) are connected;
- HL-3: regional level concentrator where typically different kinds of service platforms (e.g. IPTV) or control platforms (e.g. mobile Evolved Packet Core, Authentication, Authorization and Accounting) are connected;
- HL-2: 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;
- HL-1: interconnection level to external networks.

A mapping of the GNSS-based ePRTC time provisioning architecture is presented for the hierarchical levels of interest for the ROOT project in Figure 2.

## IV. INTENTIONAL CYBER-ATTACKS TO THE NETWORK SYNCHRONIZATION

Despite the remarkable advances in synchronization technologies, Radio-Frequency (RF) interferences can still disrupt time provisioning among the network nodes offered by GNSS, whereas the robustness of WR-PTP can be impaired by a few cyber-attacks acting at the network level.

### *A. RF interfering signals against GNSS Timing Source*

Several RF attacks can be performed to affect the time provisioning of GNSS receivers at the different HLs of the network architecture. Only a few of this can be considered likely to be directed against real network deployments [11]. A subset of possible harmful attacks can be considered according to both the cost at attacker side and the relevance to target network infrastructure: i) *Jamming,* consisting of specifically-designed RF transmission overlapping GNSS signals bandwidths using amplitude-modulated, continuous-

wave, or chirp signals; ii) *Meaconing* in different forms, leveraging on the retransmission of legitimate signals received at the attacker location; iii) *Intermediate Spoofing*, which foresees synchronously-generated counterfeit signals, trying to simultaneously attack each tracking channel of the target receiver.

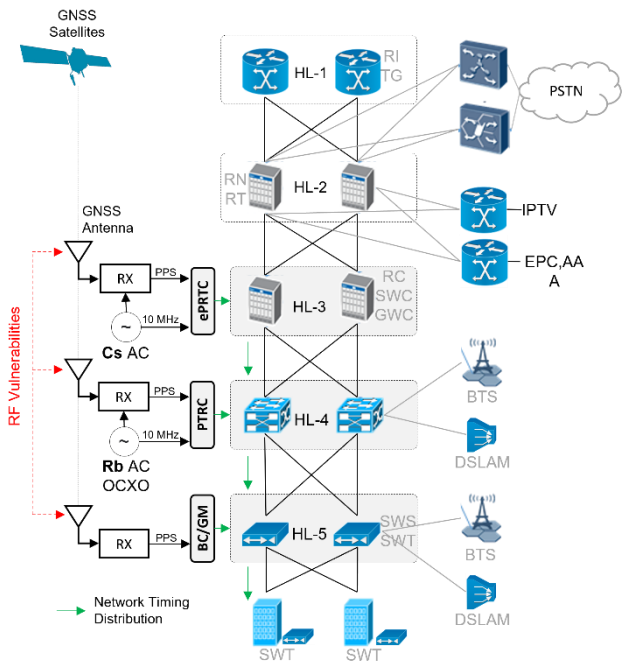


Figure 2: Telefonica's FUSION network architecture and mapping of GNSS-based accurate time provisioning. HLs 3 to 5 and the associated vulnerabilities are considered in the activities of the ROOT project.

Jamming attacks can prevent the reception of specific GNSS bandwidths, thus limiting the number of available signals and in turn the precision of the PPS generation. Wideband jamming attacks can totally disrupt signal reception, thus hindering the operational capability of the receiver and forcing free-run maintenance of the PPS generation.

More accurate, less evident but still harmful effects can be due to meaconing or spoofing attacks, specifically designed to alter the receiver clock bias estimation, thus the correction applied to PPS. Controlled nanosecond-level bias can be hence induced at PPS level by meaconing and spoofing attacks against specific network HLs. In absence of proper countermeasures, this could impact the overall synchronization w.r.t. the other subtended HLs of the network.

While live malicious RF transmissions could be practically unfeasible or unaffordable, low-cost Record and Replay approach increases the likelihood of such actions [18]**.** All the aforementioned attacks can indeed be performed through pre-recorded RF scenarios and reproduced through configurable Analog-to-Digital/Digital-to-Analog (ADC/DAC) converters.

Cryptographic solutions can be applied to the navigation message such as OSNMA or to the ranging code to counteract specific spoofing attacks while jamming threats have often to be handled at the receiver level through advanced consistency checks, adaptive notch filtering, and robust interference mitigation techniques. Anti-jamming alerts can notify jamming attacks and propagate warnings across the timing network.

### *B. Network Security Issues*

Network communication among PTP devices must ensure the availability, integrity, and reliability of the exchanged timing information since they represent a potential target for cyber-attacks [18]-[21]. These threats justify the adoption of secure communication channels that provide mutual authentication, the integrity of exchanged data, and confidentiality of the communication. Thus, protection from the man in the middle, replay, and filtering attacks would be ensured, provided that the digital certificates used in Transport Layer Security (TLS) configuration are properly issued and configured. Other techniques need to be employed instead to protect from the denial-of-service attacks, that might affect parts of the transport network.

The protection of the timing information in transit over the network approach is not enough and we also need to consider the attacks against the devices and network nodes themselves. For example, the (remote) configuration, management, and monitoring of the devices could be achieved by exploiting secure protocols, such as Secure Shell (SSH) [22] for remote access, specific protocols over TLS for network management, e.g. Network Configuration Protocol (NETCONF) via Hypertext Transfer Protocol Secure (HTTPS), or Simple Network Management Protocol (SNMPv3) [23] or Remote Authentication Dial-In User Service (RADIUS)[24] for authentication. Firewalls must be installed on selected devices and must be properly configured to block specific protocols/ports on the corresponding interfaces. Last but not the least, the protection from malware (software) attacks is of paramount importance. To detect possible intentional changes in the PTP logic, we will investigate and experiment with a solution to verify the integrity of the software running at each PTP device by exploiting trusted execution environments. In this sense, solutions based on local integrity check and remote integrity attestation of the devices involved in the network synchronisation distribution are considered relevant and promising [25]. Such solutions can detect cyber-attacks that are today considered viable. Moreover, to guarantee the continuity of the synchronization, a backup solution is foreseen according to the scheme in Figure 3, where one node receives a time signal from a remote node through a WR link. This can be used as a GNSS receiver backup in a remote location. The deployment shown in Figure 3 refers to GMC units capable to switch between different time references across the infrastructure, thus allowing the whole system to work with a common notion of time.

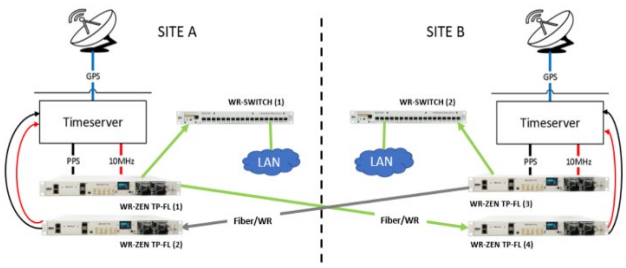


Figure 3: Network Architecture supporting GNSS/WR-PTP Synchronization

## V. THE ROOT PROJECT: OBJECTIVES AND METHODOLOGY

ROOT stands for "Rolling Out OSNMA for the secure synchronization of Telecom networks". It is funded by the European GNSS Agency in the framework of the H2020 Programme. ROOT evaluates new space-based technologies and protocols for the precise and reliable synchronization of telecom networks. These include novel GNSS receivers capable of processing the Galileo E1 OSNMA signal, namely the first civilian signal featuring authentication mechanisms. As described in the previous sections, the project pays particular attention to the resilience of GNSS-based network synchronization and accordingly to the timely detection of interfering signals to guarantee a reliable timing distribution even in case of attacks. In a nutshell, the ROOT project has six main objectives:

1. Propose advanced synchronization architectures for future telecommunications networks. This objective involves the study of the network topology presented in Section III able to satisfy the demanding phase synchronization between nodes. This objective asks for a thorough analysis of requirements from a network service point of view, the review of current standards, and the most updated scientific literature.
2. Assess the performance of a new type of GNSS receiver for timing, which features algorithms for jamming and spoofing monitoring, as discussed in Section IV. In addition to the increased level of robustness to interference, it is expected to provide more accurate timing signals, as it processes signals over different frequencies and from diverse constellations. The evaluation of performance will be based on lab tests and will consider the most likely types of intentional interference, discarding those considered too complex, costly, and therefore not plausible.
3. Experimentally evaluate secure "end-to-end solutions" able to mitigate specific cyber-attacks on the distribution of timing signals and data over the network, as presented in Section IV.B. Not only GNSS receivers are points of vulnerability, but also all devices and software dedicated to process and propagate timing data.
4. Quantify improvements and limits introduced by reliable synchronization mechanisms built upon the combination of new GNSS signals (i.e. OSNMA), technologies, and protocols. The central part of the project will address experimental tests in a laboratory dedicated to upcoming 5G [26].
5. Launch a successful market entry of the ROOT solution. This objective complements the previous ones and is important to ensure that the new technologies and protocols studied by ROOT can be effectively used and have a market.
6. Raise awareness of the benefits that the introduction of new Galileo signals in new timing applications can bring, so as to make network operators aware of the threats posed by intentional interference when the synchronization of networks is left to obsolete GPS receivers.

## VI. CONCLUSIONS

Existing operational networks are in a technological transition in order to enable 5G and next-generation networks, which are introducing a new set of stringent service requirements. This is happening by leveraging a number of new technological paradigms (such as programmability, virtualization, etc) that will transform the telecom networks, and will enable a more versatile manner of offering services. The synchronization schemes, fundamental to support the operation of the network, are also evolving. Important to say, it is becoming more and more critical to ensure adequate and robust mechanisms to avoid potential attacks and vulnerabilities in this respect. This paper describes the overall framework of accurate time synchronization and its vulnerabilities with regard to the ROOT project. It provides a reference network architecture that is representative of the next-generation deployments supporting 5G and future high-performance communications paradigms.

## ACKNOWLEDGMENT

Acknowledgment: This work was developed within the ROOT project (www.gnss-root.eu) funded by the European GNSS Agency under the European Union's Horizon 2020 – G.A. n. 101004261.

## REFERENCES

[1] Satellite-derived Time and Position: A Study of Critical Dependency, Blackett review, UK Government Office for Science, Jan. 2018. [Online]. Available: www.gov.uk/go-science

[2] Jones, S., "GPS pioneer warns on network's security," Financial Times, Feb. 13, 2014

[3] GPS World staff, "GNSS Vulnerable: What to do?", GPS World, Feb. 18, 2014. [Online]. Available at: http://gpsworld.com/gnss-vulnerable-what-to-do/

[4] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. 8 December 2008.

[5] Ericsson, "5G is all in the timing", [Online] Available at: https://www.ericsson.com/en/blog/2019/8/what-you-need-to-know-about-timing-and-sync-in-5G-transport-networks

[6] Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructures. White paper, U.S Homeland Security Department, 2016. [Online]. Available at: https://ics-cert.us-cert.gov/Improving-Operation-and-Development-Global-Positioning-System-GPS-Equipment-Used-Critical

[7] K. M. Skey, "Responsible Use of GPS for Critical Infrastructure," 6 Dec. 2017. [Online]. Available: https://www.gps.gov/multimedia/presentations/2017/12/CIPRNA/skey.pdf

[8] F. Dovis, GNSS Interference Threats and Countermeasures, Norwood, MA: Artech House, 2015.

[9] Galileo Commercial Service Implementation Decision: Commission Implementing Decision (EU) 2017/224 of 8 February 2017

[10] D. Margaria, B. Motella, M. Anghileri, J. J. Floch, I. Fernandez-Hernandez and M. Paonni, "Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives," IEEE Signal Processing Magazine, vol. 34, no. 5, pp. 27-37, Sept. 2017. doi: 10.1109/MSP.2017.2715898

[11] E. Falletti et al. "Synchronization of Critical Infrastructures Dependent upon GNSS: Current Vulnerabilities and Protection Provided by New Signals," (2019) IEEE Systems Journal, 13 (3), art. no. 8579173, pp. 2118-2129.

[12] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," in IEEE Std 1588-2002 , vol., no., pp.1-154, 31 Oct. 2002, doi: 10.1109/IEEESTD.2002.94144.

[13] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," in IEEE Std 1588-2002 , vol., no., pp.1-154, 31 Oct. 2002, doi: 10.1109/IEEESTD.2002.94144.

[14] "IEEE Standard for Local and Metropolitan Area Networks--Timing and Synchronization for Time-Sensitive Applications," in IEEE Std

802.1AS-2020 (Revision of IEEE Std 802.1AS-2011) , vol., no., pp.1-421, 19 June 2020, doi: 10.1109/IEEESTD.2020.9121845.

[15] "IEEE Draft Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications," in IEEE P802.1AS-Rev/D6.0 December 2017 , vol., no., pp.1-496, 9 Feb. 2018.

[16] M. Lipiński, T. Włostowski, J. Serrano and P. Alvarez, "White rabbit: a PTP application for robust sub-nanosecond synchronization," 2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Munich, 2011, pp. 25-30, doi: 10.1109/ISPCS.2011.6070148.

[17] 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," in IEEE Access, vol. 8, pp. 45211-45220, 2020, doi: 10.1109/ACCESS.2020.2978337.

[18] T. E. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," in IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 2, pp. 1073-1090, APRIL 2013, doi: 10.1109/TAES.2013.6494400

[19] K. O'Donoghue, "Emerging solutions for time protocol security," 2016 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), Stockholm, 2016, pp. 1-6, doi: 10.1109/ISPCS.2016.7579502.

[20] C. DeCusatis, R. M. Lynch, W. Kluge, J. Houston, P. A. Wojciak and S. Guendert, "Impact of Cyberattacks on Precision Time Protocol," in IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 5, pp. 2172-2181, May 2020, doi: 10.1109/TIM.2019.2918597.

[21] W. Alghamd and M. Schukat, "A Detection Model Against Precision Time Protocol Attacks," 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2020, pp. 1-3, doi: 10.1109/ICCAIS48893.2020.9096742.

[22] T. Ylonen, C. Lonvick, “The Secure Shell (SSH) Connection Protocol”, Jan. 2006, IETF RFC 4254.

[23] D. Levi, P. Meyer, B. Stewart, “Simple Network Management Protocol (SNMP) Application”, Dec. 2002, IETF RFC 3413.

[24] C. Rigney, S. Willens, A. Rubens, W. Simpson, “Remote Authentication Dial In User Service (RADIUS)”, June 2000, IETF RFC 2865.

[25] J. Christopher Bare, “Attestation and Trusted Computing,” CSEP 590: Practical Aspects of Modern Cryptography. March 2006.

[26] https://www.5tonic.org/https://www.5tonic.org/