DETERMINISTIC6G

First report on time synchronization for E2E time awareness

D2.2

The DETERMINISTIC6G project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement no 1010965604.

First report on time synchronization for E2E time awareness

Grant agreement number:	101096504
Project title:	Deterministic E2E communication with 6G
Project acronym:	DETERMINISTIC6G
Project website:	Deterministic6g.eu
Programme:	EU JU SNS Phase 1
Deliverable type:	Report
Deliverable reference number:	D2.2
Contributing workpackages:	WP2
Dissemination level:	PUBLIC
Due date:	31-12-2023
Actual submission date:	21-12-2023
Responsible organization:	SAL
Editor(s):	Mahin Ahmed
Version number:	V1.0
Status:	Final
Short abstract:	This deliverable presents the first report on time synchronization mechanisms to achieve end-to-end time awareness. It presents the importance and challenges of time synchronization in future 5G-Adv/6G networks. It also discusses the time synchronization use cases targeted in the DETERMINISTIC6G project and other futuristic industrial uses cases. In terms of time synchronization mechanisms, it focuses on enhancing time synchronization by implementing redundancy to enable resilience in timing. It also discusses the enhancements to essential 3GPP network functions for efficient distribution of timing information and addresses the security of timing messages in the context of 5G-Adv/6G technology.
Keywords:	6G, TSN, DetNet, time synchronization, PTP, gPTP, Hot-standby

Contributor(s):	Edgardo Montes de Oca, Huu Nghia Nguyen (MI), Mahin Ahmed, Raheeb Muzaffar (SAL), Jose Costa-Requena (CMC) Marilet De Andrade Jardim (EAB), Drissa Houatra (OR),

Revision History

V 0.1	Initial draft
V 0.2	Internal review draft
V 0.3	PMT review draft
V 1.0	Final version

Disclaimer

This work has been performed in the framework of the Horizon Europe project DETERMINISTIC6G co-funded by the EU. This information reflects the consortium's view, but the consortium is not liable for any use that may be made of any of the information contained therein. This deliverable has been submitted to the EU commission, but it has not been reviewed and it has not been accepted by the EU commission yet.

Executive summary

This deliverable addresses the critical need for precise time synchronization within the context of 5G-Advance (5G-Adv) and sixth generation (6G) networks, which are expected to play a pivotal role in various industrial use cases (e.g., extended reality (XR), autonomous driving, robot assisted tele-surgery, exoskeletons, and adaptive manufacturing etc.). It highlights the importance of time synchronization as the physical and the digital worlds converge to a cyber physical continuum. It also discusses the challenges posed to time synchronization by the expanding scope and stringent quality-of-service requirements in such heterogeneous industrial environments, emphasizing the importance of resilience in time synchronization mechanisms. The report also explores a range of industrial use cases that benefit from precise temporal coordination.

It introduces initial steps aimed at fortifying the resilience of time synchronization, presents enhancements to the essential 3GPP network functions, and offers insights into time synchronization security within the 5G-Adv/6G landscape. In summary, this deliverable serves as a first step in developing resilient time synchronization solutions for future 5G-Adv/6G networks, paving the way for the establishment of next-generation dependable time synchronization standards and architectures. It aligns with the objectives of the Deterministic6G project, providing valuable input for dependable communication services and convergence, as well as a framework for further research and simulation scenarios in the field of time synchronization.

Contents

List of Figures

List of Tables

1 Introduction

The emergence of 5G-Advance (5G-Adv) and sixth generation (6G) networks represents a significant leap forward in the evolution of wireless technology. Envisioned as the successor to the current 5G standard, 6G aims to redefine the capabilities of communication networks to cater to the demands of an increasingly interconnected and data-driven world. As future networks evolve, they are expected to play a pivotal role in diverse application domains, including industrial automation, healthcare, and augmented reality [D6G-D1.1], among others requiring dependable communication. In other words, future communication networks should be able to quantitatively guarantee the agreed quality-of-service (QoS) performance. However, in the face of this rapid expansion in scope, applications, and scale, numerous critical challenges arise. These challenges encompass issues such as ensuring seamless integration and interoperability across diverse applications, managing the increased complexity of heterogenous network architectures, and addressing security concerns associated with the vast amounts of data transmitted in interconnected environments.

One of the critical challenges that future communication networks must address is the precise time synchronization across devices and network elements within heterogeneous industrial environments (mobile and static) and across heterogeneous communication technologies (wired and wireless). Time synchronization is fundamental to the proper functioning of various applications, particularly in industrial settings where coordination, automation, and data integrity are paramount. On one hand, precise time synchronization to achieve accurate temporal alignment of data and processes is essential for optimizing efficiency, minimizing errors, and ensuring seamless interoperability in these advanced industrial scenarios. On the other hand, it is equally imperative that time synchronization systems are resilient in the face of potential failures and fortified against security threats. Industrial environments are often prone to network disruptions, hardware malfunctions, and cyber-attacks, all of which can jeopardize the integrity of communication networks. Hence, a delicate balance must be struck between achieving time accuracy and implementing robust security measures to ensure reliable and secure operation of industrial processes.

1.1 DETERMINISTIC6G goal

Digital transformation of industries and society is resulting in the emergence of a larger family of time-critical services with needs for high availability and which present unique requirements distinct from traditional Internet applications like video streaming or web browsing. Time-critical services are already known in industrial automation; for example, an industrial control application that might require an end-to-end “over the loop” (i.e., from the sensor to the controller back to the actuator) latency of 2 ms and with a communication service requirement of 99.9999% [3GPP-TS22261]. But with the increasing digitalization similar requirements are appearing in a growing number of new application domains, such as extended reality, autonomous vehicles and adaptive manufacturing. The general long-term trend of digitalization leads towards a *Cyber-Physical Continuum* where the monitoring, control and maintenance functionality is moved from physical objects (like a robot, a machine or a tablet device) to a compute platform at some other location, where a digital representation – or digital twin – of the object is operated. Such Cyber Physical System (CPS) applications need a frequent and consistent information exchange between the digital and physical twins. Several technology developments in the ICT-sector drive this transition. The proliferation of (edge-) cloud compute paradigms provide new cost-efficient and scalable computing capabilities, that are often more efficient to maintain and evolve compared to embedded compute solutions integrated into the physical objects. It also enables the creation of digital twins as a tool for advanced monitoring, prediction and automation of system components and improved coordination of systems of systems. New techniques based on Machine Learning can be applied in application design, that can operate over large data sets and profit from scalable compute infrastructure. Offloading compute functionality can also reduce spatial footprint, weight, cost and energy consumption of physical objects, which is in particular important for mobile components, like vehicles, mobile robots, or wearable devices. This approach leads to an increasing need for communication between physical and digital objects, and this communication can span over multiple communication and computational domains. Communication in this cyber-physical world often includes closed-loop control interactions which can have stringent end-to-end KPI (e.g., minimum and maximum packet delay) requirements over the entire loop. In addition, many operations may have high criticality, such as business-critical tasks or even safety relevant operations. Therefore, it is required to provide *dependable time-critical communication* which provides communication service-assurance to achieve the agreed service requirements.

Time-critical communication has in the past been mainly prevalent in industrial automation scenarios with special compute hardware like Programmable Logic Controller (PLC), and is based on a wired communication system, such as EtherCat and Powerlink, which is limited to local and isolated network domains which is configured to the specific purpose of the local applications. With the standardization of Time-Sensitive Networking (TSN), and Deterministic Networking (DetNet), similar capabilities are being introduced into the Ethernet and IP networking technologies, which thereby provide a converged multi-service network allowing time critical applications in a managed network infrastructure allowing for consistent performance with zero packet loss and guaranteed low and bounded latency. The underlying principles are that the network elements (i.e. bridges or routers) and the PLCs can provide a consistent and known performance with negligible stochastic variation, which allows to manage the network configuration to the needs of time-critical applications with known traffic characteristics and requirements.

It turns out that several elements in the digitalization journey introduce characteristics that deviate from the assumptions that are considered as baseline in the planning of deterministic networks. There is often an assumption for compute and communication elements, and also applications, that any stochastic behavior can be minimized such that the time characteristics of the element can be clearly associated with tight minimum/maximum bounds. Cloud computing provides efficient scalable compute, but introduces uncertainty in execution times; wireless communications provides flexibility and simplicity, but with inherently stochastic components that lead to packet delay variations exceeding significantly those found in wired counterparts; and applications embrace novel technologies (e.g. ML-based or machine-vision-based control) where the traffic characteristics deviate from the strictly deterministic behavior of old-school control. In addition, there will be an increase in dynamic behavior where characteristics of applications, and network or compute elements may change over time in contrast to a static behavior that does not change during runtime. It turns out that these deviations of *stochastic characteristics* make traditional approaches to planning and configuration of end-to-end time-critical communication networks such as TSN or DetNet, fall short in their performance regarding service performance, scalability and efficiency. Instead, a revolutionary approach to the design, planning and operation of time-critical networks is needed that fully embraces the variability but also dynamic changes that come at the side of introducing wireless connectivity, cloud compute and application innovation. DETERMINISTIC6G has as objective to address these challenges, including the planning of resource allocation for diverse time-critical services end-to-end over multiple domains, providing efficient resource usage and a scalable solution [SPS+23].

DETERMINISTIC6G takes a novel approach towards converged future infrastructures for scalable cyber-physical systems deployment. With respect to networked infrastructures, DETERMINISTIC6G advocates (I) the acceptance and integration of stochastic elements (like wireless links and computational elements) with respect to their stochastic behavior captured through either short-term or longer-term envelopes. Monitoring and prediction of KPIs, for instance latency or reliability, can be leveraged to make individual elements plannable despite a remaining stochastic variance. Nevertheless, system enhancements to mitigate stochastic variances in communication and compute elements are also developed. (II) Next, DETERMINISTIC6G attempts the management of the entire end-to-end interaction loop (e.g. the control loop) with the underlying stochastic characteristics, especially embracing the integration of compute elements. (III) Finally, due to unavoidable stochastic degradations of individual elements, DETERMINISTIC6G advocates allowing for adaptation between applications running on top such converged and managed network infrastructures. The idea is to introduce flexibility in the application operation such that its requirements can be adjusted at runtime based on prevailing system conditions. This encompasses a larger set of application requirements that (a) can also accept stochastic end-to-end KPIs, and (b) that possibly can adapt end-to-end KPI requirements at run-time in harmonization with the networked infrastructure. DETERMINISTIC6G builds on a notion of time-awareness, by ensuring accurate and reliable time synchronicity while also ensuring security-by-design for such dependable time-critical communications. Generally, we extend a notion of deterministic communication (where all behavior of network and compute nodes and applications is pre-determined) towards dependable time-critical communication, where the focus is on ensuring that the communication (and compute) characteristics are managed in order to provide the KPIs and reliability levels that are required by the application. DETERMINISTIC6G facilitates architectures and algorithms for scalable and converged future network infrastructures that enable dependable time-critical communication end-to-end, across domains and including 6G.

1.2 Objective of the document

This deliverable presents a first report on establishing a resilient and secure time synchronization framework for future 5G-Adv/6G networks.

One of the central objectives of this deliverable is the exploration of mechanisms designed to introduce resilience into time synchronization, with a specific emphasis on redundancy as an enabler for resiliency. These mechanisms are poised to fortify the temporal accuracy and reliability of critical industrial processes in the face of potential disruptions. Additionally, this deliverable aims to present possible enhancements to the crucial 3GPP network functions required for seamless time synchronization within converged networks. These functions are essential for harmonizing time-critical operations across diverse network infrastructures. Moreover, the document delves into the imperative topic of time synchronization security, offering first insights on how to strengthen the integrity of time synchronization messages and mechanisms within the 5G-Adv/6G landscape. Furthermore, it sheds light on a spectrum of time synchronization use cases including not only the use cases addressed by the DETERMINISTIC6G project but also other future time synchronization use cases. Hence, demonstrating the multifaceted applications of precise temporal coordination n

In summary, this deliverable aims to serve as a starting point for the development and implementation of resilient time synchronization solutions within the scope of future 5G-Adv/6G networks, and it paves the way for the realization of next-generation dependable communication standards and architectures.

1.3 Relation to other work packages

Within the technical work packages of DETERMINISTIC6G project, D2.2 is part of WP2, which focuses on 6G-centric enablers for deterministic communication services. The relation of D2.2 to other work packages is shown in Figure 1-1. It takes input on the application requirements for time synchronization coming from WP1 [D6G-D1.1]. D2.2 takes input from the security mechanisms for deterministic communications presented in WP3 [D6G-D3.2]. The initial time synchronization scenarios presented in D2.2 will serve as input for the simulation scenarios in WP4, which focuses on a 6G deterministic communication validation framework.

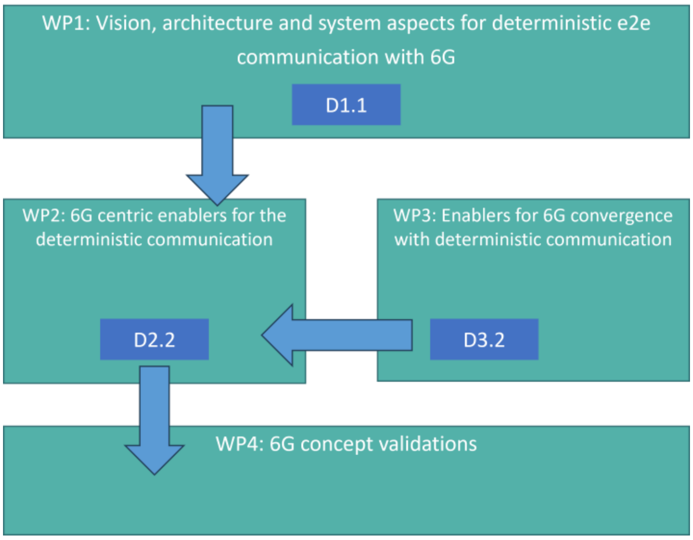

Figure 1-1 Relationship of D2.2 to other work packages and deliverables

1.4 Structure and scope of the document

After the introduction in Section 1, Section 2 presents the time synchronization for end-to-end time awareness where it focuses on the importance of time synchronization, the use cases where time synchronization is required and the challenges for time synchronization in future 5G-Adv/6G networks. In Section 3, the state-of-the-art for time synchronization is presented with a focus on time synchronization mechanisms in TSN networks, in 5G networks and 5G-TSN networks. Additionally, the time-error analysis as per 3GPP specifications is also presented in Section 3. This state-of-the-art sets the basics needed to grasp the discussions presented in Section 4 and 5. Section 4 presents the limitations in state-of-the-art time synchronization mechanisms. In Section 5, the time synchronization mechanisms are detailed. In particular redundancy in clock sources, enhancements to 3GPP network functions and secure distribution of timing information are presented. Finally, Section 6 concludes the deliverable with some discussions on the future work.

1.5 Terminology used in the deliverable

In this deliverable, we follow the inclusive terminology as decided by IEEE 1588 [IEEE P1588-D1.2] standardization bodies to describe the time synchronization architectures. Whereby the following should be kept in mind.

- Master is replaced with timeTransmitter (tT)
- Slave is replaced with timeReceiver (tR)
- grandmaster (GM) remains grandmaster
- best master clock algorithm (BMCA) is replaced with best timeTransmitter clock algorithm (BTCA)

2 Time synchronization for end-to-end time awareness

2.1 Overview

The rapid advancement in technologies like cloud and edge computing are revolutionizing the availability of computing and data storage, hence enabling digital twins and cyber-physical systems. These developments are expected to converge towards a cyber-physical continuum. The future communication networks are envisioned to integrate diverse and heterogeneous technologies, including modern cellular technologies, short-range wireless technologies, and wired communications. In particular, the 5G-Adv/6G networks providing intelligently networked infrastructures will serve as a critical link between the physical and digital worlds. This future landscape will be supported by massive multiple-input multiple-output (MIMO), terahertz communications, quantum communications, fog computing, edge computing, machine learning (ML), and artificial intelligence (AI) [GPM+20] [SAP+21] [SPS+23]. In this context, time synchronization is seen as an important enabler. As 5G-Adv/6G networks are still in the early stages of development, there are several open challenges that need to be addressed for time synchronization in these networks.

2.2 Importance of time synchronization

Many applications rely on reliable and timely delivery of information among the communicating devices. Time synchronization plays a crucial role in enabling dependable communications, where the timing of events and data transmissions is carefully orchestrated to meet stringent requirements, such as bounded latency, high reliability, and synchronized coordination among multiple devices or processes. It is envisioned in 5G-Adv/6G networks that as the digital and physical worlds come together, multiple technologies and devices must operate together in a coordinated manner to ensure optimal network performance and resource allocation [ZVF+20]. Time synchronization enables synchronized actions and coordinated operation among heterogeneous technologies, allowing seamless integration between different wired and wireless systems. This heterogenous landscape also relies on efficient spectrum utilization. Precise timing coordination between different technologies allows for synchronized transmission schedules and efficient frequency allocations. Hence, achieving optimized spectrum sharing and reduced interference.

Additionally, future industrial communication networks aim for different devices to seamlessly handover between different technologies without disruptions or loss of synchronization. A precise time synchronization is essential for enabling such smooth transitions and maintaining connectivity for users as they move across different technologies and coverage areas.

In the context of 5G-Adv/6G networks, time synchronization also plays a crucial role in enabling edge computing and network slicing capabilities. Synchronized timing information ensures precise coordination and synchronization between edge nodes, facilitating efficient data processing, real-time analytics, and seamless integration of network slices with varying performance requirements [HGL20].

Lastly, time synchronization enhances network resilience and security. Synchronized timing information enables efficient detection and mitigation of network anomalies, synchronization attacks, and time-based threats. It supports accurate event correlation, facilitating rapid incident response and ensuring the integrity and reliability of the network.

In summary, time synchronization is of paramount importance in E2E dependable communication network so that they can unlock their full potential for emerging use cases in the converged wired wireless network landscape. Additionally, a scalable and nanoscale precision time service for 5G-Adv/6G networks and industrial services can be seen as a key enabling service for building an edge-to-cloud industrial service continuum, which in turn contributes to the construction of an infrastructure supporting a cyber-physical continuum for industrial services.

2.3 Time synchronization use cases

In this section, we present different use cases which require time synchronization. Different industrial use cases put forward different requirements for time synchronization for their proper functioning and accurate realization.

2.3.1 DETERMINISTIC6G use cases

The use cases considered in the Deterministic6G project include extended reality, exoskeletons, adaptive manufacturing, and smart farming [D6G-D1.1]. It is important to note that where not all scenarios within these use cases require very high timing accuracy, these use cases in particular need resilience and security in the timing mechanisms which are targeting by this deliverable.

In extended reality (XR) applications like virtual reality (VR) and augmented reality (AR), along with bounded latency, precise synchronization is vital to ensure virtual objects align seamlessly with real environments, enhancing immersion. XR services and holographic applications utilize synchronized media layers, requiring time synchronization to align playout buffers [CAK23]. Time synchronization would be crucial in XR scenarios where information fusion takes place. For example, when you need to fuse the calculations done on the local device with those done on the edge/could, time synchronization errors should be minimal. Additionally, security measures prevent unauthorized access to sensitive training scenarios [SGZ+23]. Time synchronization between an XR device and the edge cloud processing can provoke security and safety issues. In particular, augmented reality is very sensitive to time synchronization attacks [D6G-D1.1].

Exoskeletons worn by industrial workers to enhance strength and safety demand accurate time synchronization [BSS+20] [SPS+23]. For preserving the safety of the user, time synchronization redundancy is desirable: despite the exoskeleton’s control system includes specific safety loops designed to detect any faults and/or unexpected behaviors, the presence of the secondary clock could increase the system robustness and prevent potential risks caused by the loss of time synchronization.

In adaptive manufacturing environments, where robots and machinery work are in close proximity, precise time synchronization is paramount. Deterministic timing ensures that collaborative robotic movements and interactions are precisely coordinated. Redundant time sources enhance reliability, ensuring that automated processes continue smoothly even in the event of time synchronization disruptions from one of the time sources.

Smart farming leverages technology to optimize agricultural operations. Accurate time synchronization is critical for coordinating tasks like automated irrigation, drone-based crop monitoring, and livestock management. Precision and accuracy are essential for timing irrigation cycles and pesticide application accurately, contributing to resource efficiency. Especially, for safety-critical applications, having redundancy as a source of resilience in time synchronization mechanisms and enhanced security would be greatly beneficial to achieve maximum resource efficiency.

2.3.2 Emerging time synchronization use cases

In this section, we present emerging time synchronization use cases in general where the e synchronization is required.

Autonomous vehicles and self-driving cars: The rise of autonomous and self-driving cars is propelling the digitization of embedded devices and vehicle functions, reshaping CAN architectures to resemble private 5G-Adv/6G networks. These changes are crucial for processing real-time data from diverse sensors like cameras, radar, and lidar, ensuring safe driving decisions. The resulting instructions, including honking and braking signals, necessitate reliable, real-time transmission through the CAN network for proper execution within the vehicle. In autonomous driving scenarios, TSN technologies and time synchronization play vital roles in CAN evolution, ensuring dependable and timely communications within the vehicle. This extends to inter-vehicle communication (V2V technologies) and communication with service provider-operated infrastructures (V2I technologies). Works like [BK21] and [WS20] exemplify the ongoing efforts in vehicular networks and V2X technologies, focusing on the critical element of time synchronization in these contexts.

Robot-assisted tele-surgery: Teleoperated surgery is an interesting use case to provide life-saving health care in extreme conditions (e.g., in space [HSB11]) and also helps remove any geographic or economic boundaries [BG03]. Time synchronization is crucial here to ensure precise coordination and communication between robotic components. It facilitates real-time communication, aligns imaging and data feedback accurately, integrates patient data effectively, enables instrument tracking, and enhances overall safety protocols.

Datacenters: The modern datacenter landscape varies from nano/micro to large-scale cloud datacenters, and the projected increase in data centers, driven by edge computing and 5G-Adv/6G applications, suggests that millions of servers will be interconnected in the future. Challenges include achieving synchronization accuracy (under 1 microsecond) and precision for distributed services across geographically dispersed datacenters. The Open Compute Project (Open Compute Project Time Appliance project (TAP)) [BLWB23, OCP-TAP] is an interesting example initiative to develop time synchronization solutions dedicated to time synchronization of datacenter servers operated by large scale cloud service providers and hyperscalers.

Hence, from the above analysis of application requirements for the different industrial use cases targeted within this project and other emerging time synchronization use cases, it becomes evident how the requirements intertwine to ensure proper functioning of these use cases. In each of these use cases, the requirements for accurate time synchronization play a pivotal role. They ensure that different technologies and systems work together harmoniously, providing the precision, reliability, and coordination necessary for optimal performance and outcomes in diverse industrial use cases.

2.4 Challenges for time synchronization in 5G-Adv/6G networks

As E2E deterministic networks, particularly in the context of 5G-Adv/6G networks, are still in the early stages of development, there are several open challenges that need to be addressed for time synchronization in these networks.

The E2E deterministic communications are envisioned to support ultra-low latency communication, which necessitates extremely precise and fast time synchronization mechanisms. Achieving sub-microsecond synchronization accuracy and minimizing synchronization overhead while considering the complexities of heterogeneous devices and communication technologies is a significant challenge. Coordinating time synchronization across these heterogeneous devices and technologies poses challenges due to variations in clock accuracy, and synchronization protocols. Developing synchronization techniques that can effectively handle this heterogeneity is crucial.

The emerging use cases will involve highly dynamic environments with mobile devices, autonomous vehicles, and robots. Synchronization mechanisms must accommodate frequent device mobility and changing network topologies while maintaining accurate and reliable time synchronization [CAK23]. Handling mobility-related challenges and ensuring synchronization continuity in dynamic environments are open research areas. High mobility-related challenges also include fast changing network conditions, such as interference, fading, and congested environments. These conditions can affect synchronization accuracy and reliability. Developing robust synchronization techniques that can adapt to changing network conditions, mitigate interference effects, and maintain synchronization performance is an important challenge.

The architecture of time synchronization systems heavily influences their performance and scalability. Developing new architectures that can accommodate the stringent timing requirements of E2E deterministic communication systems is a significant research challenge. In this context, time synchronization for these large-scale assets may be an important challenge. This could lead, in some cases, to bandwidth requirements much higher than those allowed by industrial 5G-Adv/6G networks. A solution to this would contribute to the exploitation of the full capabilities of massive industrial IoT installations.

With many different heterogeneous devices and technologies coming together to enable E2E deterministic communications, the need for secure time synchronization is even higher [GLA+20]. Protecting synchronization signals from attacks, ensuring authentication and integrity of synchronization messages, and preventing timing-based attacks are critical challenges. Hence, developing synchronization techniques that can withstand emerging threats is crucial.

The 5G-Adv/6G networks are expected to meet the sustainability and development goals of the United Nations. Adding the large scale of devices as mentioned above, achieving high energy efficiency is becomes an important aim of future communication systems. Hence, time synchronization mechanisms should be designed to minimize energy consumption while meeting the stringent timing requirements of various applications [GPM+20].

Finally, the development of common time synchronization protocols and standards to ensure high interoperability among diverse devices, networks and applications is a huge challenge. Standardization bodies need to address the challenges posed by different synchronization mechanisms, communications technologies and use cases to ensure a seamless integration and interoperability across the converged E2E deterministic network infrastructure.

Addressing these open challenges in time synchronization for E2E deterministic communications requires interdisciplinary collaboration and active involvement from the standardization bodies. Overcoming these challenges will contribute to the realization of diverse applications and services envisioned for the future industrial systems.

3 State-of-the-art

3.1 Basics of time synchronization

To understand the different synchronization protocols and techniques, we need to examine the architecture and functionality of a digital clock. Digital clocks consist of an oscillator and a counter, as shown in Figure 3-1. The oscillator generates a continuous signal with a defined frequency for determining the length of a second, while the counter keeps track of the number of seconds or clock cycles that have occurred [AAH97]. By knowing the cycle duration and the initial counter value, a clock can estimate the correct UTC time by adding the elapsed cycles.

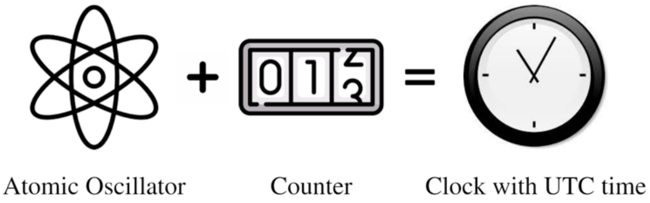

Figure 3-1 Architecture of a digital clock

However, real oscillators are affected by imperfections that reduce frequency accuracy and stability. Additionally, initializing the counters perfectly is also a challenge. Physical effects like oscillator aging, temperature gradients, vibrations, and counter quantization further impact the precision of the clock. Therefore, regular synchronization is necessary to maintain the required precision.

Clocks need to be aligned both in the frequency and time domains. There are different types of clock synchronization: frequency synchronization aligns oscillator frequencies, phase synchronization ensures trigger signals occur simultaneously, and time synchronization involves distributing a shared time reference. When clocks are frequency, phase, and time-synchronized, they display the same time.

Synchronization begins with a reliable and accurate time reference source. This can be a highly precise atomic clock or, a GNSS satellite system. The time reference source transmits its time, and all other devices will synchronize their clocks to this reference. There are different ways to accomplish this, such as broadcasting time signals over a network or sending periodic time updates to connected devices.

As mentioned in previous sections, achieving precise synchronization among distributed and heterogeneous devices is a significant challenge for the E2E deterministic communication networks. Equipping all devices with GNSS receivers is not feasible due to unreliable reception and cost concerns. Instead, packet-based synchronization protocols that utilize the existing network infrastructure can be used. The general procedure involves periodically broadcasting the reference time from a dedicated time source to all network devices. In order to align their clocks with the reference clock hosted by the source of time, the devices compensate for the time passed between the origin and reception of the reference time.

Different synchronization protocols and techniques are employed based on the specific application and the network infrastructure. Network time protocol (NTP) is one of the oldest general-purpose time synchronization protocols, providing accuracy in the millisecond range. Hence, NTP is not suitable for time-critical applications. Whereas the precision time protocol (PTP) (IEEE 1588) [IEEE1588-2019] is an Ethernet-based time synchronization protocol with sub-microsecond accuracy, given the ability to perform hardware stamping and residence time (details on the residence time are provided in later sections) compensation. In this project, we focus on the PTP protocol and its different profiles i.e., the gPTP (used for TSN networks) [IEEE 802.1AS-2020] and PTP-tele (used for transport network in 5G) [ITU-G8275.1, ITU-G8275.1]. In the upcoming sections, we provide details on how time synchronization with gPTP is achieved in TSN networks and with PTP-tele in 5G transport networks. These explanations help us in understanding how the time synchronization in a wired-wireless 5G-TSN network is achieved.

3.2 Time synchronization mechanisms for time sensitive networks

Synchronization in TSN networks is achieved through the IEEE 802.1AS standard [IEEE802.1AS-2020], which adopts the IEEE 1588v2 precision time protocol (PTP) and provides additional functionalities for addressing the requirements of cyber-physical systems. IEEE 802.1AS [IEEE802.1AS-2020] establishes generalized precision time protocol (gPTP) as the PTP profile. This section provides a comprehensive overview of IEEE 802.1AS gPTP and its relevant features in industrial communication, highlighting the differences from PTP.

gPTP is a packet-based protocol for distributing reference time information and selecting the reference time source in local area networks (LANs). It enables network-wide synchronization with sub-microsecond precision, requiring limited computing resources [GOT10]. A gPTP network is also known as a time-aware network. It includes multiple gPTP instances referred to as time-aware systems. A gPTP instance is a device running the IEEE 802.1AS protocol and operating within a single time aware system within exactly one domain. Unlike PTP networks, which allow non-PTP instances, a time-aware network exclusively consists of time-aware systems. gPTP defines two types of time-aware systems: gPTP end instances and gPTP relay instances. gPTP utilizes a dedicated mechanism to establish a tT-tR synchronization hierarchy across the time-aware network, with the GM at the top. The GM, which can be a gPTP end instance or gPTP relay instance with access to a time source like a dedicated GNSS receiver, provides the reference time information derived from its source to the other time-aware systems in the network. The synchronization hierarchy is crucial for synchronization of time-aware networks. gPTP supports both time and frequency synchronization. Frequency synchronization involves continuous measurement of clock rate ratios between neighboring clocks and the GM clock. The rate ratio describes the ratio between the clock frequency of a clock to its GM. Precise time synchronization is achieved by frequently distributing reference time information from the GM to all other systems in the network. As the timing information travels through the network, corrections are applied to account for network delays, consisting of propagation-, transmission-, processing-, and queueing-delays, according to [T07].

The gPTP simultaneously accomplishes time and frequency domain synchronization. On one hand, a clock adjusts its frequency offset to match the frequency of the GM clock. On the other hand, it fine-tunes its clock offset to align its reported absolute time as accurately as possible to the GM time. In order to achieve precise time and frequency domain synchronization, gPTP allows for estimation and measurement of several properties like neighbor rate ratio, propagation delay, rate ratio, and correction field [IEEE802.1AS-2020]. The neighbor rate ratio defines the ratio between the clock frequency of two adjacent clocks. The propagation delay accounts for the delay incurred by a message traversing the path between two clocks. The correction field is used to correct for the delay caused by the distribution of timing messages within the network. It is calculated and updated at any clock that propagates the timing information received from the GM [IEEE802.1AS-2020]. The neighbor rate ratio and propagation delay mechanisms are peer-to-peer properties, hence independent of the GM location. On the other hand, the rate ratio and correction field depend on the clock's location relative to its GM. The error in the estimation of these properties accumulates over multiple hops.

3.2.1 Grand timeTransmitter selection

The selection of grand tT is done either by external port configuration or by the Best TimeTransmitter Clock Algorithm (BTCA). The different port states of each time-aware system establish the time synchronization hierarchy in each gPTP domain. There are different PTP port states defined, namely the tT port, tR port, Passive port, and disabled port. The synchronization hierarchy is established as a spanning tree to avoid synchronization loops.

For the external port configuration, an external entity determines the synchronization spanning tree and sets the PTP port states. The external port configuration allows to choose a desired grand tT and corresponding desired time synchronization spanning tree.

For BTCA, the best tT selection information is exchanged between PTP Instances of time-aware systems via Announce messages. IEEE 802.1AS implements the BTCA as defined in the IEEE 1588-2019 standard. BTCA runs on each time-aware system independently, by comparing the clock datasets obtained in the Announce messages to determine whether the local or the external clock is more accurate. This decision, along with the source port information from the Announce message, helps the system determine its port states. The BTCA uses two distinct algorithms: one for comparing datasets and another for making state decisions. The dataset comparison algorithm establishes the best option among two compared datasets, while the state decision algorithm suggests port states based on various datasets. Moreover, BTCA ensures that all clocks within a subdomain have a clear hierarchy without the need for negotiations between them. This prevents potential conflicts and misconfigurations, such as the presence of multiple tT clocks or the absence of any timeTransmitter clocks, which could disrupt the synchronization process.

3.2.2 Support for redundancy

In order to ensure resilient synchronization, the standard introduces redundancy in GM devices and synchronization paths by supporting multiple gPTP domains, as shown in Figure 3-2. The redundant domain is used when the performance of the first domain degrades. Each gPTP domain represents a network segment that aligns its time to a shared time reference (GM) and can function at varying timescales. A time-aware system has the capability to be a part of multiple gPTP domains, thereby facilitating synchronization with different GMs. This allows for the time-aware system to process PTP messages from different domains. The time it uses to synchronize the application running on it is left up to the implementation. The process of GM selection and the establishment of synchronization hierarchies are performed for each individual gPTP domain.

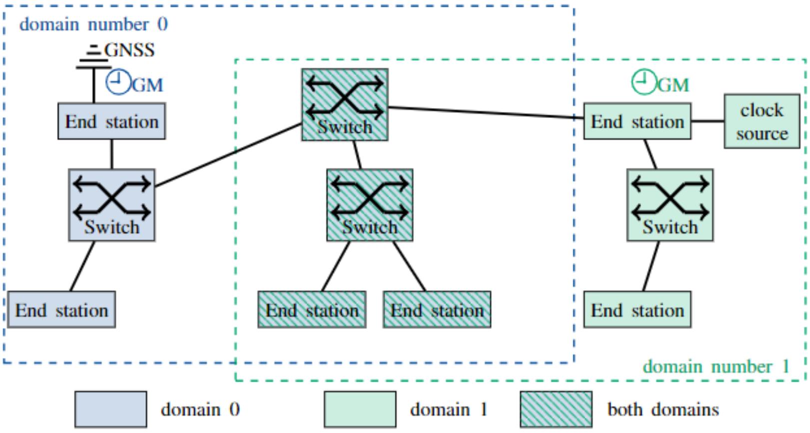

Figure 3-2: Time aware network with multiple gPTP domains

The process of selecting and configuring multiple GMs is currently the subject of discussions within the IEEE 802.1 standardization bodies. Initial efforts towards this aim are underway in the IEEE 802.1ASdm working group. A draft version of this amendment can be accessed on the IEEE 802.1 standards website.

The hot-standby amendment proposes a static configuration of two independent GMs by an external entity, such as a management client using the external port configuration option. Consequently, the BTCA is no longer employed to select a GM within a domain. The secondary hot-standby GM synchronizes itself with the primary GM before transmitting timing messages into its domain. This procedure ensures that the time provided by both GMs remains within a tolerance range, resulting in consistent time provision.

Once both GMs are configured, tRs continually receive timing information from both GMs. These tRs can then independently choose between the two timing sources for their applications, as the timing information remains consistent within a tolerable error range. The redundant GM continuously provides timing information to the network. Therefore, in the event of a primary GM failure, tRs can remain synchronized with the hot-standby GM, ensuring uninterrupted network time synchronization.

It's worth noting that the process of restoring a faulted GM is beyond the scope of this amendment. However, a split functionality has been defined to facilitate the resynchronization of the two GMs after the recovery of a faulted GM, supporting the synchronization of an out-of-sync GM with a synchronized GM.

3.3 Time synchronization mechanisms in 5G networks

Time synchronization is a critical aspect of 5G systems to ensure reliable and efficient communication between network elements and devices. In 5G networks, precise time synchronization is essential for several reasons including the coordination between cells on transmission and reception, interference avoidance between neighboring cells, handover procedure, and to meet the stringent ultra-reliable low latency communication requirements.

Most 5G deployments today use time division duplex (TDD) configuration of radio frames. The TDD configuration requires time and phase alignment between the base stations to prevent traffic losses.

However, TDD cells operating at the same or adjacent frequency require time domain isolation to prevent base-station-to-base-station and UE-to-UE radio frequency interference. Because in TDD configuration the uplink and downlink slots use the same frequency, the critical points for synchronization are when switching between the transmission and reception slots [EricssonWP].

The 5G system allows the use of various synchronization techniques to accurately distribute time between the network elements. The 5G baseband unit receives timing information from the global navigation satellite system (GNSS) as the source clock [SJP+21]. The fronthaul synchronization between the radio resource head (RRH) and the baseband unit is serviced via enhanced common public radio interface. The international telecommunication union - telecommunication sector (ITU-T) recommends a maximum timing error of +/- 1.5 µsec relative to the source clock for the neighbouring base stations to synchronize. Moreover, the frequency error at the base-station air interface must be +/- 50 ppb [3GPP-TS38133] in addition to +/- 500 µs time alignment requirement in NR-FDD. Synchronous Ethernet (SyncE) provides frequency synchronization in compliance with the ITU-T G.8262 and G.8262.1 specifications at the Ethernet physical layer to support packet transfer in the backhaul and mid-haul networks. The 5G RAN synchronization requirements are summarized in Table 1.

Table 1 Synchronization requirements of RAN technologies [EricssonWP]

Type	Requirement	Technology
Time synchronization	≤ 1 µs	Coordinated transmission or reception
	~1.5 µs	Time division duplex (NR-LTE-TDD) Carrier aggregation
	500 µ	NR-FDD
Frequency synchronization	50 ppb	LTE-FDD

The time distribution mechanism for 5G is specified in G.8275.1 [ITU-G8275.1] and G.8275.2 [ITU-G8275.2] ITU-T profiles. The ITU-T G.8275.1 and G.8275.2 recommends PTP telecom profile for phase/time synchronization with full timing support (FTS) and partial timing support (PTS), respectively from the network that can be used for synchronizing time in wireline mobile backhaul networks. The choice of FTS or PTS depends on the application synchronization needs. FTS is suitable for applications requiring high synchronization accuracy while avoiding GNSS receiver at every site whereas PTS or Assisted PTS (APTS) is suitable for small, indoor, last-mile deployments where the network has limited or no timing support through local GNSS receivers [ComcoresWP].

The ITU-T G.8275.1 profile is defined for the scenario where no support for the PTP protocol in intermediate nodes between the PTP tT and the PTP tR is available. It allows interoperability with existing synchronization networks such as synchronous Ethernet (syncE). SyncE is an Ethernet-based synchronization technology that enables frequency and phase synchronization for 5G networks over Ethernet connections.

The G.8275.1 profile provides the most accurate time synchronization solution to remain within the budget constraints of +/- 1.5 µs. The G.8275.1 suggests use of telecom boundary clocks (T-BC) clocks which receive timing information from the telecom grandmaster (T-GM) with primary reference time clock (PRTC) such as the GNSS. Each T-BC node acts as a PTP timeTransmitter for downstream nodes to deliver accurate time/phase synchronization to the end application. A simplified G.8275.1 architecture is presented in Figure 3-3.

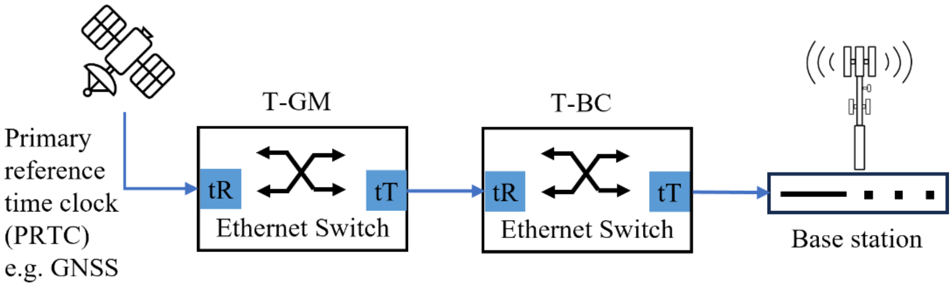

Figure 3-3 G.8275.1 Architecture

Conversely, G.8275.2 is designed to deliver accurate frequency synchronization, phase synchronization, and time of day (ToD) with only PTS where non-PTP nodes are also in the network path. Contrary to G.8275.1 where layer 2 multicast is used for time distribution, G.8275.2 allows PTP packets to be distributed using layer 3 (IPv4/IPv6) unicast transmission enabling PTP packets to be distributed over non-PTP networks and across layer 2 boundaries. Since not all network nodes have a physical layer frequency synchronization support, boundary clocks in G.8275.2 are referred to as partial-support telecom boundary clocks (T-BC-P). The G.8275.2 allows two PTP modes namely the hybrid and nonhybrid mode. In hybrid mode, PTP is used for phase synchronization and ToD distribution in the network with syncE support for frequency synchronization at T-BC-Ps whereby PTP is used without SyncE support in non-hybrid mode. A simplified G.8275.1 architecture is presented in Figure 3-4. An ATPS is also defined where PTP is used as a backup timing source to a local timing reference for up to 72 hours.

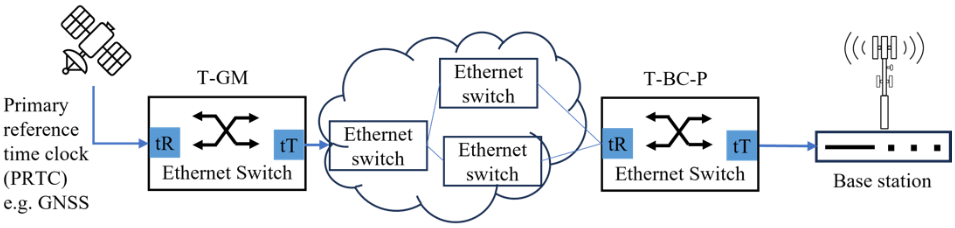

Figure 3-4 G.8275.2 Architecture

Time synchronization is also required in FDD networks when different radio coordination features are used. The ITU-T G.8265.1 [ITU-G8265.1] profile recommends functions that are necessary to ensure network element interoperability for frequency synchronization.

The open-RAN (O-RAN) alliance also addresses the synchronization aspects of fronthaul networks. O-RAN disaggregates 5G base station into three logical units namely the radio unit (RU), the distributed unit (DU), and the centralized unit (CU). The fronthaul is the connection between the DU and RUs which uses eCPRI for exchange of control and data packets whereas SyncE and PTP are used for timing synchronization. The fronthaul timing requirements are typically stringent since they support features such as carrier aggregation and distributed MIMO. The midhaul is the connection between the DUs and CU. The DUs must synchronize with each other within a maximum synchronization error of 3 µs, i.e, the maximum error between the source clock and the DU could be of 1.5 µs [MGG+23]. This, however, can be achieved using PTP over FTS, PTS, or APTS network. A feature proposed by the O-RAN architecture is the possibility of virtualizing the network components and the flexibility of deploying them on cloud platforms. Nevertheless, a precise time synchronization is required between the DUs and CU running on cloud environments, to provide a common time reference to each DU and the corresponding (remote) CU and ensure real-time execution of BBU functions across DU/CUs with strict time budget constraints.

Overall, time synchronization is a foundational element for the success of 5G systems, enabling efficient resource allocation, interference management, seamless mobility, and support for a wide range of applications with diverse requirements.

3.4 Time synchronization mechanisms in 5G-TSN networks

The time synchronization in a converged 5G-TSN system works independently for the TSN and 5G elements. TSN employs gPTP for achieving synchronization within its network elements. Within the 5G network, the time synchronization is divided into 5G Core (5GC) and 5G RAN synchronization. Within the 5G RAN, synchronization pertains to the alignment of the User Equipment (UE) and is managed by the Next Generation NodeB (gNB). This is achieved by utilizing an internal reference time indication, which makes use of either System Information Blocks (SIBs) or Radio Resource Control (RRC) messages [MAG+18] [FVM+19] [MAG+19] [GLR+20]. Moving on to the 5GC, the gNB takes on the responsibility of synchronizing the User Plane Function (UPF). This synchronization process is carried out through a PTP telecom profile (PTPtele) [ITUG8275.1] [GLR+20]. Timing information is conveyed to the UE via gNB using multicast or unicast messages [PRC20]. The gNB, as a tT, synchronizes UE and UPF, with a required accuracy of under 1 µs.

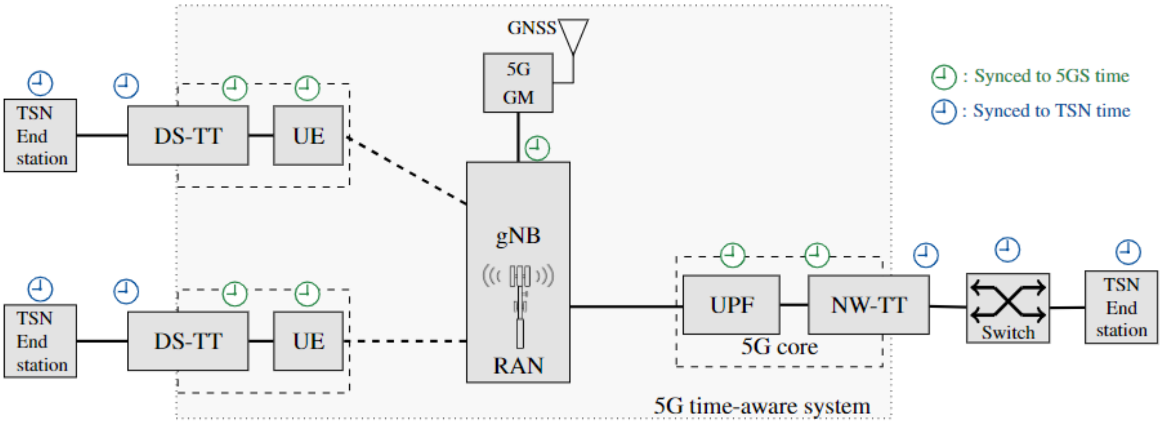

Figure 3-5 Time synchronization in 5G-TSN networks

For TSN synchronization with 5GS, boundary clock and transparent clock solutions are explored, [TS23.501]. Transparent clock solution has been standardized in 5G Release-16, while Release-17 supports the boundary clock solution as depicted in Figure 3-5. The dashed connection between RAN and UE represents the UU radio interface. In the boundary clock solution, the TSN GM clock directly connects to gNB via UPF, which distributes timing information to UEs. UEs synchronize connected TSN devices, ensuring uniform network-wide time. This method can also use the 5G internal clock as the time source for PTP GM, potentially eliminating the need for PTP message exchange, unlike the transparent clock solution. In the transparent clock solution, gPTP messages pass through Transparent

Clocks (TTs) for synchronization. As a gPTP message enters 5GS via UPF from the TSN domain, the ingress TT (e.g., NW-TT) generates an ingress timestamp (TSi) based on the 5G internal clock, then embeds it within the gPTP message. The gPTP message is transferred transparently through the 5G system till the egress TT (e.g., DS-TT). The egress TT receives the gPTP message (e.g., from the UE, in case of DS-TT) and generates an egress timestamp (TSe) based on 5GS internal clock provided by gNB. The time spent within 5GS (residence time) is calculated as TSe minus TSi and is added to the TSN synchronization packets' correction field (CF). The modified gPTP packet is then sent to the next connected TSN bridge or end station [AMS+21].

The gPTP payload can be a synchronization or follow-up message, adhering to IEEE 802.1AS QoS requirements. The timing error is affected by the accumulated hops between TSN GM clock and gNB. 5G-TSN integration supports multiple TSN working time domains, with gPTP messages carrying Ethernet destination MAC address and domain number to identify referred TSN time domain. TSN application function (TSN AF) or TSCTSF are responsible for configuration of PTP instances for DS-TT and NW-TT in 5G-TSN networks by sending port management information (PMIC) and user-plane node management information (UMIC) to DS-TT or NW-TT. Release-16 specifies downlink (DL) TSN time synchronization where TSN GM clock resides at NW-TT, while uplink (UL) TSN and UE-to-UE synchronization are developed in 3GPP Release-17 [TS23.700].

3.4.1 Downlink synchronization

A synchronization scenario known as Downlink (DL) synchronization is established by a network side GM. As illustrated in Figure 3-6, the GM resides within the TSN network on the network-side of the 5GS and connected to the UPF. This approach was standardized in the 3GPPP Rel. 16 and integrates seamlessly with the 5GS. It leverages the underlying synchronization of 5G virtual bridge components through the 5GS. gPTP messages traversing the 5GS are time stamped at ingress by NW-TT and at egress by DS-TT. The ingress and egress time stamps are based on the 5GS internal clock and are embedded in the gPTP message as a suffix. This facilitates the determination of the residence time that a given gPTP message spends within the 5G virtual bridge. The DS-TT modifies the TSN timing information based on the calculated residence time before forwarding the gPTP to the next time-aware system. Synchronization error for devices, which lie beyond the 5GS and are part of DL synchronization, is impacted by the 5GS residence time accuracy. This accuracy relies heavily on the 5GS internal clock-based synchronization of NW-TT and DS-TT.

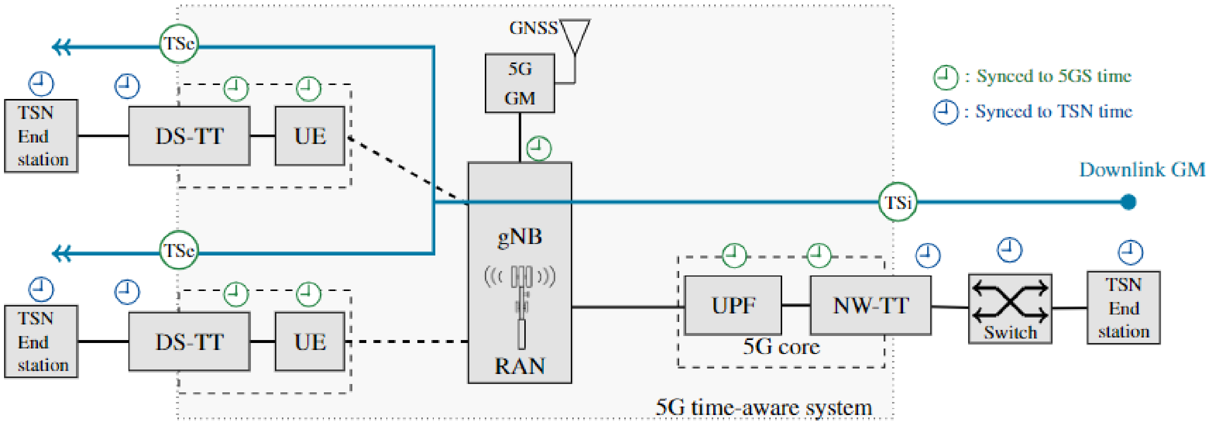

Figure 3-6 Time synchronization in 5G-TSN with downlink synchronization

3.4.2 Uplink synchronization

Different from DL synchronization, Uplink (UL) synchronization is established by a device side GM. As illustrated in the Figure 3-7, the GM resides within the TSN network on the device (UE) side of the 5GS. The synchronization of TSN end stations on the network side of 5GS follows a similar path as for DL synchronization in the reverse direction. However, the synchronization of other device side TSN end stations need to be carefully orchestrated. The gPTP messages originating at the GM traverse the 5GS and need to be reversed to DL direction at the UPF. Hence the gPTP messages to synchronize the other TSN end stations on the device side need to traverse the wireless link between UE and gNB twice. Similar to DL synchronization, the synchronization error is closely related to the accuracy of residence time estimation, which relies on the 5G internal clock.

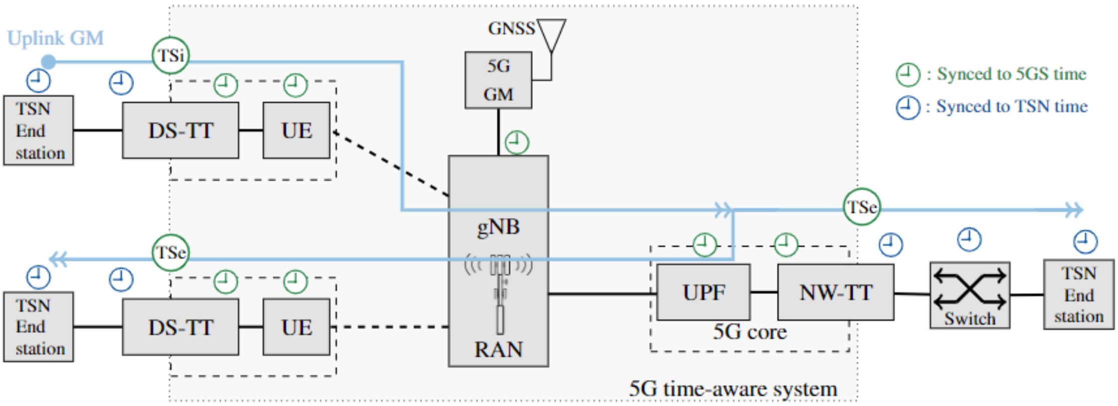

Figure 3-7 Time synchronization in 5G-TSN networks with Uplink synchronization

3.4.3 5G clock as GM

5GS utilizes the access stratum time distribution as specified in 3GPP Rel-17 TS38.331 to distribute the 5G GM time to external networks, i.e., the TSN end stations, as shown in Figure 3-8.

Accordingly, the 5G internal components including the UPF, NW-TT, DS-TT, and the UE are synchronized with the 5G internal clock. The 5G base station periodically broadcasts system information including the master information block (MIB) and system information block 9 (SIB9). The system information blocks are transmitted via the downlink shared channel and physical data shared channel. The timing information is contained in SIB9 and is accurate down to sub-µs level. For wide area scenarios where the UE and the RAN node may be far away, additional mechanisms compensate propagation delay on the radio interface. The DS-TT generates PTP messages (e.g., Sync, Follow-up and Announce messages) for the TSN devices on the device side of 5GS. In case DS-TT doesn’t support this, NW-TT can step-in and generate gPTP messages on behalf of the DS-TT. The NW-TT generates the PTP messages for the TSN devices on the network side of 5GS. TSN AF or TSCTSF are responsible to expose the 5G clock properties to the external network needed for GM selection using BTCA.

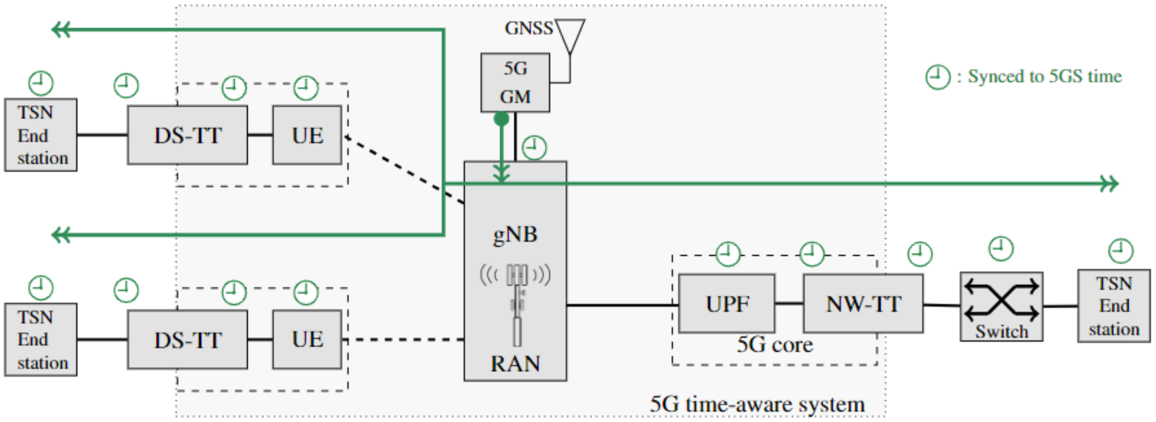

Figure 3-8 Time synchronization in 5G-TSN network with 5G clock as GM

3.4.4 Time error budget for 5G-TSN networks

As mentioned in Section 3.2 and Section 3.4, errors in the calculation of propagation delay and residence time can lead to inaccuracies in time synchronization. These inaccuracies are added by any node in the synchronization network. However, there is a maximum amount of time error that the synchronization may tolerate. For this reason, it was defined a time-error budget to be offered by the 5G system. For TSN service, it was defined a time-error budget of 900 ns. In this section, we present how this time-error budget is calculated and what are the components for this time-error budget in different scenarios.

The 5G time-error budget components are illustrated in Figure 3-9. Depending on the scenario, a maximum time-error budget was defined:

- Scenario 1: devices behind a target UE are synchronized to any time domain, from a GM behind the CN (GM clock is in the UPF side).
- Scenario 2: devices behind a target UE are synchronized to any time domain, from a GM behind the UE (GM clock is in the UE side, there is UE-to-UE time distribution).
- Scenario 3: devices behind a target UE are synchronized to the 5G GM time domain (5G is the GM clock).

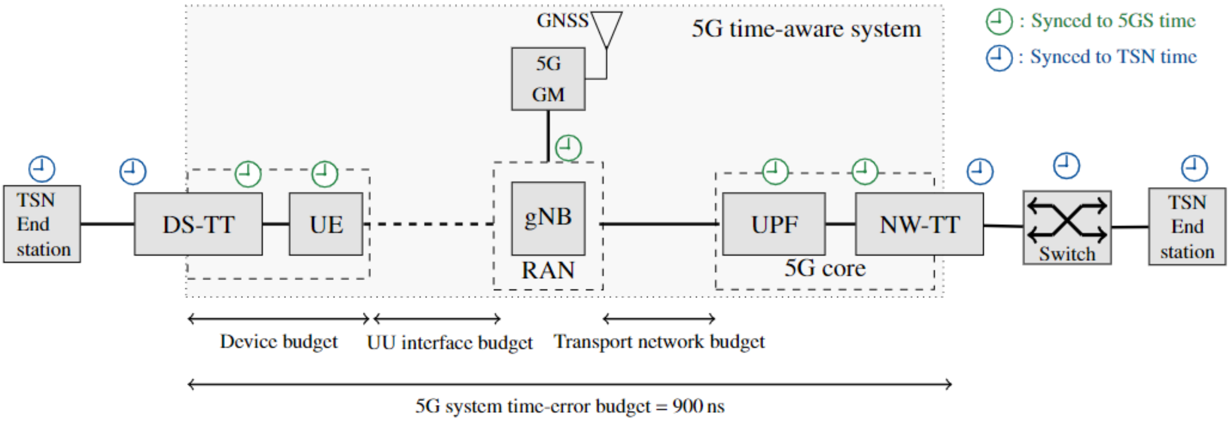

Figure 3-9 5G system time error budget and its components.

Per Uu interface time synchronization accuracy is important to determine the need for Propagation Delay Compensation method at gNB. The most stringent scenario is when UE-to-UE communications take place, see Figure 3-10. In this case the Uu budget = (900ns – 2xDevice -2xNetwork)/2, where Device corresponds to the inaccuracies added by the device (UE), and Network corresponds to the time error added by the 5G transport network.

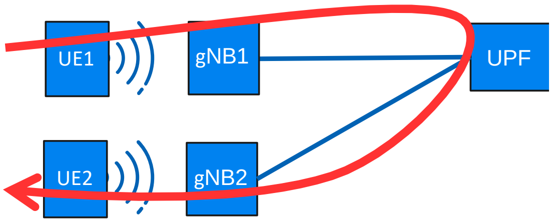

Figure 3-10 UE-to-UE communication

In general, TSCTSF may calculate the Uu interface time-error budget, based on the 5G time-error budget requested by application (AF). Then TSCTSF delivers this Uu interface time-error budget to the RAN node (gNB) for it to decide whether a propagation delay compensation method has to be applied.

3GPP has estimated the Uu time-error budget [R2-2100001] as follows:

The Uu interface budget for Scenario 1, 2 and 3 are respectively calculated as follows:

- Scenario 1: Uu budget = 900ns – Device – Network.
- Scenario 2: Uu budget = (900ns – 2xDevice – 2xNetwork)/2.
- Scenario 3: Uu budget = 1000ns – Device – Network.

The Device part time synchronization accuracy budget is assumed to be in the range ±50 to ±100ns, this applies to all three scenarios. Assuming the two Uu interfaces in Scenario 2 have the same time synchronization error budget

The Network part (gNB-UPF) time synchronization accuracy budget for Scenario 1, 2, and 3 are assumed to be the following:

- Scenario 1: ±120 to ±200ns (Network) (assuming 3-5 hops worst case scenario
- Scenario 2: ±240 to ±400ns (2xNetwork) (assuming 6-10hops worst case scenario)
- Scenario 3: ±100ns (Network)

The per Uu interface time synchronization accuracy for Scenario 1, 2 and 3 are as follows:

- Scenario 1: ±595ns to ±725ns
- Scenario 2: ±145ns to ±275ns
- Scenario 3: ±795ns to ±845ns

4 Limitations in the state-of-the-art time synchronization mechanisms

In the context of emerging 5G-Adv/6G use cases with stringent application requirements (as described in Section 2.3, and considering the state-of-the-art in current synchronization mechanisms (as detailed in Section 3), it becomes evident that certain critical challenges and open issues persist. In this subsection, we highlight key concerns and unanswered questions that are essential to address in order to ensure resilient and reliable time synchronization, particularly for the evolving landscape of industrial automation use cases.

4.1 Continuous time synchronization is vital

While both the 3GPP and IEEE 802.1 standardization bodies acknowledge the need for continuous time synchronization by introducing support for multiple GMs and multiple synchronization paths, limitations persist. For instance, the utilization of the Best Time and Clock Algorithm (BTCA) for selecting a new GM in the event of a failure introduces a downtime period until a suitable replacement is identified. Consequently, BTCA's response to device or link failures is characterized to be slow, which can be detrimental in time-critical applications.

4.2 Transient fault detection challenges

Furthermore, the IEEE 802.1AS based time synchronization, while robust in many respects, falls short in the realm of detecting transient faults within a GM. These transient faults, when not promptly identified, can lead to undesirable consequences, including what is colloquially referred to as a "ping-pong effect". This phenomenon unfolds as BTCA tirelessly seeks the best Time Transmitter in the network, often switching between multiple candidates without achieving stable synchronization.

4.3 Vulnerability to network delay

Excessive latency can lead to outdated time information being delivered to network devices, resulting in inaccurate time synchronization. PTP messages are delivered at a certain pace, and if those messages are delayed to a point that it exceeds their pace, then time synchronization in the network will miss out the updates of a number of PTP messages. For example, in gPTP profile, it is important to keep a maximum of 10 ms residence time in a time-aware system. To mitigate the impact of network latency on time synchronization it is necessary, for instance, to adopt network optimization techniques to reduce congestion and implement quality of service policies to prioritize time synchronization messages.

In the case of the 5G system internal processes, the delivery of time to the DS-TT and NW-TT is important to keep these entities synchronized with the 5G grandmaster clock. For NW-TT, the timing is delivered via a PTP-compatible 5G transport network. For the DS-TT, the timing is delivered to the UE (and then to DS-TT) via the air interface using SIB9 as described in 3.4.3. The propagation delay between base station and UE is not considered (as it would be considered in PTP), leading to an introduced timing error. To mitigate this effect, 3GPP has introduced propagation delay compensation methods in Release 17. The most important is that the 5G/6G-introduced timing errors are below the required time error budget for a certain application.

4.4 Security concerns

Time synchronization is necessary in many emerging applications (e.g., industry 5.0, robotics, virtual reality) but the dependence on precise timing introduces various vulnerabilities. These include:

- If GPS is used for accurate time synchronization: GPS signals are susceptible to jamming and spoofing attacks, leading to incorrect time synchronization.
- DDoS attacks on time synchronization servers can cause time synchronization failures or inaccuracies.
- Centralized time synchronization sources can lead to single points of failure, making them more vulnerable to attacks and failures.
- For performance reasons, time synchronization channels are not always secured (e.g., not encrypted, not well authenticated), facilitating the interception, modification or injection of messages.
- Inadequate monitoring and anomaly detection prevent timely detection of attacks on the synchronization.
- Vulnerabilities in the time synchronization protocols (e.g., NTP,PTP) can be exploited. If not well implemented, tested or in case of a lack of robust security measures, they could be susceptible to different attacks, such as man-in-the-middle, spoofing, replay, and DoS attacks.
- Other vulnerabilities can be due to hardware errors, backward compatibility, physical attacks, etc.

Even though 5G networks have introduced numerous improvements in terms of security, the above listed vulnerabilities remain, particularly concerning timing synchronization. Some of the existing shortcomings in the current security mechanisms for timing synchronization include: lack of end-to-end encryption, limited authentication, integrity and authenticity checks of the time sources, insufficient monitoring and anomaly detection, lack of redundancy, and limited standardized security mechanisms for timing synchronization across different vendors and network operators. Additionally, IEEE 802.1AS does not inherently address security concerns, and additional measures may be needed to protect against timing attacks.

These limitations underscore the need for innovative solutions and more sophisticated time synchronization mechanisms that can seamlessly adapt to the evolving demands of 5G-Adv/6G use cases while maintaining the resilience and dependability required for industrial automation and other time-critical applications. In the subsequent sections, we explore potential avenues for addressing these challenges.

5 Mechanisms to support end-to-end time awareness

5.1 Overview

Accurate time synchronization in future 5-Adv/6G networks demands several crucial mechanisms and technologies to ensure precision and reliability in timing information to enable dependable communications. In this first report, we present some mechanisms that in our opinion can enhance the resilience and reliability of timing information in the future 5G-Adv/6G networks.

To enhance reliability and resilience, redundancy in clock sources is crucial. In this context we propose to explore the use of a hot-standby clock source in 5G-Adv/6G networks. Some possible options for the placement of a redundant hot-standby clock source are presented. Efficient mechanisms for network-wide clock distribution are essential to minimize delays and jitter in timing messages. 3GPP compliant network functions to support distribution of timing messages with minimum jitter are also discussed. Finally, security measures are paramount to prevent malicious interference or tampering with timing information. These encompass cryptographic techniques, authentication, and access control mechanisms to safeguard timing messages from unauthorized access or tampering. We present some measures to enhance the security of timing information.

5.2 Redundancy in clock source

Redundancy in clock sources is crucial for resilient and continuous time synchronization because it enhances fault tolerance, reliability, and continuity in time synchronization. By deploying redundant grand tTs, the system can withstand hardware and software failures. This redundancy also enables scalability as the network expands and provides resilience to external factors like network outages or security breaches. Geographical distribution of redundant tTs further enhances resilience to regional disasters. In essence, redundancy ensures that time synchronization remains available, even in challenging conditions and high-demand environments.

5.2.1 Consideration for GM location

To qualify as a GM, a clock needs precise timing from sources like atomic clocks, GNSS, or oscillators, plus fine granularity. GNSS receivers, relying on satellite atomic clocks, provide unmatched accuracy in clock frequency [KO87]. However, not all devices can access GNSS due to cost and indoor limitations. Clock granularity depends on the oscillator's frequency, affecting time resolution. Synchronization quality also depends on communication links, with wireless connections being less accurate than wired ones. In large industrial networks, network topology and an end-station's proximity to the GM impact synchronization. Synchronization errors accumulate over hops, with more distant end-stations experiencing worse accuracy.

Studies on TSN and 5G-TSN networks show that synchronization precision degrades as information propagates from the GM [GSD+17]. In 5G-TSN, the GM's relative positioning matters, and integrating 5G introduces additional error [SDL+21] [S20]. Some propose using pre-selected ordered lists of GMs to avoid accumulation of error given consecutive exchange of messages in traditional BMTA [JLP14].

Next, we propose hot-standby architectures in the light of 3GPP and IEEE 802.1AS standards and the above-mentioned considerations for selecting a GM. In order to ensure resilient time synchronization, the 5G-TSN network is synchronized via a primary and a hot-standby secondary clock at the same time. Hence the following architectures present possible options for a primary clock and a hot-standby secondary clock.

5.2.2 Initial time synchronization with hot-standby GM

Since hot-standby solution for timing resiliency has not yet been considered for 5G-TSN networks either by 3GPP or IEEE standardization bodies, in this section we present possible time synchronization architectures in a 5G-TSN network. Additionally, we also provide details on how the system will behave in case either of the clocks fail.

Considering that in hot-standby enabled time synchronization architectures, we need to decide where to place the two GMs, several options are possible, as given below:

1. **Both primary and hot-standby GM on network-side TSN end-stations –** In this architecture, it's worth noting that both the primary and hot-standby GMs may lack access to a high-quality clock source. Moreover, given that the 5G-TSN network is specifically configured for use cases involving mobility or scenarios where Ethernet implementation is unfeasible, a disruption of the 5G virtual bridge would result in the end-stations on the device -side losing synchronized time from both GMs.
2. **Both primary and hot-standby GM on device-side TSN end-stations –** This architecture has similar drawbacks as the first architecture. Additionally, with both GMs on device-side TSN end-stations would mean a higher time error for device-side TSN end-stations given that UE-to-UE communication (as discussed in Section 3.4.4).
3. **Network-side TSN end station as primary GM and device-side TSN end station as hot-standby GM** – This architecture has a similar disadvantage in terms of clock source quality. However, in case there is a disruption of the 5G virtual bridge, each part of TSN network would still have access to synchronized time.
4. **5G GM as hot-standby GM and network/device-side TSN end station as primary GM** – This architecture is interesting but has some limitations. Considering the current recommendation in the IEEE 802.1ASdm working group, the hot-standby GM should synchronize to the primary GM before transmitting timing messages. Since 5G GM is also used to synchronize the other 5G elements like the gNB, UPF and other UEs for its proper functioning, this option would not be feasible. Hence keeping two clock sources, that are not themselves in sync would not provide the benefits we are aiming for with redundancy of clock sources.
5. **5G GM as primary GM and device-side TSN end-station as hot-standby GM –** This architecture has similar benefits of having the 5G GM as primary GM. Whereas, with the hot-standby GM on the device-side TSN end station could result in a higher time-error for other device-side TSN end stations (as discusses in Section 3.4.4).
6. **5G GM as primary GM and network-side TSN end station as hot-standby GM** – in this configuration, we benefit from the higher quality (access to GNSS time) 5G clock. On one hand, in case of failure of primary GM (i.e., loses access to GNSS time), the gNB can still support time synchronization using the own local clock. On the other hand, having the hot-standby GM on the network side helps keeps the time-error low for device-side TSN end-stations given the timing messages only travel once over the Uu interface.

Next, we delve into the intricacies of architecture 6, offering a comprehensive examination that includes insights into the events unfolding should either of the GMs fail to furnish essential timing information.

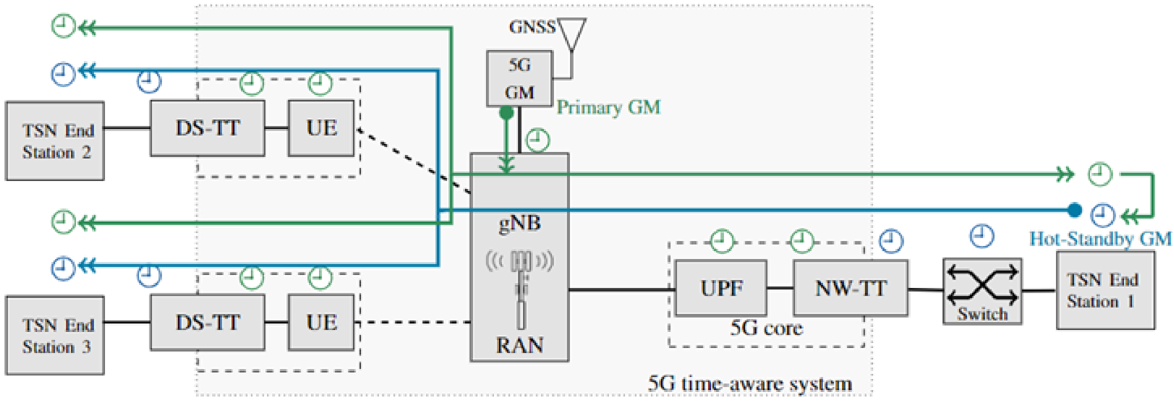

Figure 5-1 Time synchronization architecture with 5G GM as primary GM and network side TSN station as hot-standby GM

The 5GS GM is chosen as the primary grandmaster, given that most 5G grandmaster clocks have access to a GNSS receiver by design, and hence access to a higher quality of time. The synchronization domain for a primary 5G GM is shown in Figure 5-1 in green. The 5GS synchronizes the user plane nodes (i.e, the UE, gNB, and UPF) using the 5G GM and the user plane nodes do not synchronize to the external hot-standby GM in the TSN network. The 5GS GM will be identified by its domain number. In this domain, all the devices in the 5GS and the TSN network are synchronized to the same grandmaster clock. The 5GS will synchronize the user plane nodes and the TTs at the boundaries using the 3GPP compliant synchronization mechanisms. Whereas, the TSN end stations will be synchronized using IEEE 802.1AS gPTP messages.

The TSN end-station 1 on the network side of 5GS is chosen as the hot-standby GM, as shown in Figure 5-1. The GMs instances are configured statically using external port configuration option, support for which is provided by 3GPP since Rel-17 and by IEEE 802.1AS-2020. The two domains are identified by their domain IDs. The hot-standby GM does not start transmitting sync messages until it has fully synchronized in frequency and phase to the primary grandmaster, i.e., the 5G GM. In these scenarios, all devices within the 5GS and the TSN are synchronized to the same clock i.e., the 5GS clock. Each TSN end-station receives gPTP messages from both the primary and hot-standby GM. When the time aware system is in redundant state i.e., both primary and hot-standby GM are synched, then the end station chooses the primary clock time for its application clock target.

In case the secondary hot-standby GM fails, the end stations keep operating as normal as they are continuously synchronized to the primary GM. The system no longer has access to redundant timing, unless the hot-standby GM is restored by an external entity. Considering that the 5G-TSN network is specifically configured for use cases involving mobility or scenarios where Ethernet implementation is unfeasible, a disruption of the 5G virtual bridge would result in loss of connection between the network-side and device-side TSN end stations. In a rare case there is a disruption of the connection to the 5G virtual bridge, (i.e., the timing messages from the primary GM are no longer received) the TSN devices on the network side of 5GS have only access to the hot-standby GM time and have no longer redundant timing. On the other hand, the TSN devices on the device side of 5GS will lose synchronized time from both time domains, as the time synchronization messages from hot-standby

GM are no longer transmitted over 5G. Based on the accuracy of the local clocks, the devices will drift away from synchronized time and hence be no longer synchronized. Once the connection to the 5G virtual bridge is restored, the two GMs can resynchronize to provide redundant timing in the network. The question about how the two GMs are resynchronized is still open and left for implementation. The architectures presented above emphasize the importance of redundant paths.

5.3 Enhancements to the 3GPP compliant network functions to support dependable distribution of timing information

3GPP has defined the network functions in both the CN i.e., NW-TT and on the device side i.e., DS-TT to make 5G system time aware. These functions implement gPTP logical functions for the 5G network behaving as a transparent time-aware system. However, the functioning of gPTP to deliver accurate time synchronization relies on i) symmetric communications so the delay in both directions is the same and ii) low delay so the gPTP can deliver accurate time information to be compensated between the NW-TT and DS-TT.

5.3.1 3GPP time synchronization network function

The current 3GPP Rel 17 and Rel 18 have defined the basic architecture for distributing time synchronization though the 5G system. However, the variability of propagation delay in the air interface (Uu) impacts the time synchronization accuracy. This issue is more critical for UE-to-UE communications. Mechanisms for propagation delay compensation have been specified in RAN workgroups to solve this issue for 3GPP Rel 17 [3GPP-TS38300]. Of course, even higher accuracy can be achieved with more expensive devices that introduce less error, both at RAN and UE side.

The TSN-AF as defined in 3GPP Rel 16, interacts with the TSN Central Network Controller (CNC) for processing traffic requests and translates them into 5G system specific data flows. This entity also configures the ports with corresponding information about PTP instances, their port state, and other data sets specific for the gPTP profile which are defined by CNC. The time sensitive communication and time synchronization function (TSCTSF) has same functions as TSN AF, but for non-TSN type of time sensitive communication such as DetNet, and/or for supporting a generic time synchronization service (a profile of IEEE 1588-2019). In such case, there are also data sets used for configuration which are based on the time synchronization profile used. In the future, a 5G-Adv/6G system might be capable to predict failures and degradations of the time synchronization service. This could be based on synchronization measurements performed by the time synchronization platform in the system. If these measurements are available and provided via OAM to e.g., ML-based agents running at the network data analytics and automation function (NWDAF). As a result, 5G-Adv/6G system can use predictions to take early actions with respect to the time synchronization service. Monitoring and detection of time synchronization anomalies is however out of 3GPP scope as it depends on specifications by other standardization bodies such as ITU-T and IEEE.

5.3.2 Time synchronization optimization

The optimization of time synchronization requires enhancement of existing NF or design of additional logic for improving time synchronization. The current specifications define the end-to-end system between DS-TT in the UE and NW-TT in the UPF as virtual TSN switch. However, the traffic from the same UE when establishing additional PDU sessions might impact the PTP traffic between the DS-TT deployed in that same UE. Thus, network slicing technology could be considered to isolate the traffic from the UE and a dedicated network slice with URLLC type would be allocated for those devices.

According to IEEE 802.1AS Section B.2 Time-aware system requirements, the 5G residence time for the gPTP sync messages should be no more than 10 ms. Thus, specific QoS flow configuration for time synchronization is required such that the packet delay budget (PDB) is set below the 10-ms limit. Note that in a UE-to-UE communication, two concatenated communications sets (two PDU sessions: one uplink and one downlink) are required, meaning that the maximum per QoS flow is 5ms in each PDU session, for a total of 10 ms.

5.4 Secure distribution of timing information

5.4.1 Overview

Time is not only the primary performance metric but is also an attack vector. A missed deadline in critical applications due to an unexpected delay induced by an attacker can lead to severe consequences. Especially in E2E deterministic communication which consists of several different heterogeneous devices and technologies, the exposure of this attack vector to various security threats is increasing. In the worst case, due to its heterogeneous nature, an infrastructure component can even host an attacker, or be compromised by an attacker, making the comprehensive secure distribution of timing information in the network against a malware infiltration a very tedious task [WMs+21]. We present in this section a state of the art of the threats concerning the time synchronization processes as well as the countermeasures and attack mitigation techniques to develop strategies to strengthen these processes in networks against various attacker types.

Several security threats have been examined from academic literature and standardization work. They can be classified into 6 types according to different threats of attacks and targets of the well-known threat modelling framework, Microsoft's STRIDE: spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privilege.

The most common type of attack is the denial-of-services (DoS) threat possible on each data link [FBZ+21]. The second most common is information disclosure which happens when the information can be read by an unauthorized party. Elevation of privileges is all related to either gaining complete control of tTs or manipulating their data. Tampering and spoofing are related to packet data. Repudiation is from the external interactor which is usually omitted in the time sensitive networks.

Normally, a GM takes the role of a tT that distributes the reference time to the tR nodes, i.e., other down-stream nodes synchronizing to the common time. A compromised or impersonated grandmaster leads to the distribution of false synchronization messages, causing all down-stream clocks to be compromised. Compromise can be achieved via an elevation of privilege. For instance, an unauthorized element joins as a master clock, disrupting the election process and overriding the legitimate grandmaster. This might also be done by intervening in the distributed grandmaster election process when the nodes announce their priority to be selected as the master clock. The impersonation can be done by an attacker who is depicted as a legitimate master by generating and transmitting legitime protocol packets [WMs+21].

In the case of a usage of a single tT, sabotaging the tT, via DoS attacks, may result in a short desynchronization while a new tT is elected or when switching over to redundant one.

Targeting the master clock could be challenging because it is often one of the most protected assets in the network and would most likely require an insider attack. Tampering and forging time synchronization packets is another way to intervene in the time synchronization process.

[BCAMM+18] presented an attacker model in which the attacker can break into one or more tR to initiate the attack. By breaking into one device, the attacker has full control over this device, and gains access to the multicast and unicast keys used in the protocol communications. The attacker could spoof tR clocks through the injection of fake Sync messages, intercepting and dropping the GMC Sync messages, impersonating the GMC, injecting new Sync messages with a fake timestamp, and generating legitimate ICV for those messages using the PTP authentication key available at the compromised device.

The packet content manipulation attacks can be partially avoided using encryption and integrity protection of the packets to authenticate the content of message payloads in fixed networks. However, meta-information such as protocol specifications can still be neglected as confidential information. For instance, as PTPv2 is not backward compatible with PTPv1, mixing protocol version specifications can hinder a consistent time synchronization process in the overall network [DCJ+21] as summarized in Table 2. Furthermore, encrypting every packet will impact the latency.

Even though cryptography is a solution to protect against malicious packet modifications, it is not effective against delaying attacks that result in incorrect measurements of hop-to-hop latency, which is used to readjust timing information for eliminating propagation delays. A man-in-the-middle attack can even drop protocol packets which again either leads to clock synchronization errors of all clocks downstream or makes them go into free running mode [WMs+21]. The threats in time synchronization that can be considered are of three types: spoofing attack, tampering attack, and denial of service attack. These are detailed in Table 3.

[FBZ+21] proposed a novel anomaly detection system, which is based on the security mechanism per-stream filtering and policing (PSFP) defined in IEEE 802.1Q, to effectively solve the problem caused by DoS attacks and abnormal traffic behaviors. The list of security countermeasures that can be used in a TSN-type network, mainly includes firewalls, IDPS systems, cryptography, and access control as shown in Table 2.

Table 2 OSI models and security technologies [Lou et al.]

OSI layers	Security technologies		
	Isolation & Filtration	Detection & Defense	Authentication & encryption
Layers 5-7: HTTP, DoIP,		DPI	SecOC SSL/TLS/DTLS
Layer 4: TCP, UDP, PTP	Firewall (Port No.)	IDPS	
Layer 3: IP, ARP, PTP	Firewall (IP filter) VLAN (IP subnet)		SSL/TLS/DTLS
Layer 2: Ethernet, TSN	Firewall (Frame Length, Token Bucket, Meters, Input Gates, MAC, Tagged)	IDPS (PSFP)	MACsec

5.4.2 Timing distribution vulnerabilities and requirements

In this section, we summarize the discussion on [RFC-7384] about the security aspects of time distribution protocols in packet networks. This RFC focuses on the two most common protocols: the NTP and the PTP. It defines a set of security requirements for these time protocols.

The threat model classifies attackers based on two criteria:

- *Internal vs. external:* An internal attacker either has access to a trusted segment of the network or possesses the encryption or authentication keys. An external attacker, on the other hand, does not have the keys and has access only to encrypted or authenticated traffic.
- *On-path vs. off-path:* An on-path attack is in a position that allows to intercept, modify, or drop in-flight protocol packets, whereas an off-path attack can only inject protocol packets.

Table 3 presents a summary of the threat model and its impact on the time protocol synchronization network. The impact can be one of the following:

- DoS: the attack causes denial of service to the attacked node.
- Accuracy Degradation: the attack degrades the tR's accuracy but does not completely compromise their time and frequency.
- False Time: the attack causes false time or frequency values of timeReceivers.

Table 3 Time Protocols – Threats and Impacts Summary

Attack	**Attack Type**				**Impact**		
	Internal		**External**		**False Time**	**Accuracy Degradation.**	**DoS**
	On-Path	**Off-Path**	**On-Path**	**Off-Path**			
Manipulation *Attacker receives a packet, alter then replay it –> distribute false information*	+				+		
Spoofing *Impersonate the master (tT) → distribute false time* *Impersonate a clock (tR) to request the master (tT) → defeat delay computation*	+	+			+		
Replay attack *Replay a packet without modification → distribute false information*	+	+			+		
Rogue master (tT) attack *Manipulate the master (tT) election process to create a rogue master (iT) → distribute false time*	+	+			+		

Interception and removal *Drop packets → prevent destination node (tR) from receiving*	+		+			+	+
Packet delay manipulation *Add a maliciously computed delay in a packet → distribute false info*	+		+		+		
L2/L3 DoS attack *ARP or IP spoofing, MAC flooding, etc. → compromise the target's availability*	+	+	+	+			+
Crypt. performance attack *Send fake protocol packets → increase resource usage of the target's cryptographic engine*	+	+	+	+			+
Time protocol DoS attacks *Send an excessive number of time protocol packets → degrade the target's performance*	+	+					+
GM time source attack *Manipulate time source of the GM → distribute false time*	+	+	+	+	+		

Table 4 summarizes the different security requirements which are proposed by [RFC-7384] to be able to mitigate the attacks.

Table 4 Time Protocols - Security Requirements

Requirements	**Level**
Authentication & authorization of sender	MUST
Authentication & authorization of master	MUST
Recursive authentication & authorization	MUST
Authentication & authorization of timeReceivers	MAY
PTP: Authentication & authorization of P2P TCs by master	MAY
PTP: Authentication & authorization of Announce messages	MUST
PTP: Authentication & authorization of Management messages	MUST
PTP: Authentication & authorization of Signaling messages	MAY

Integrity protection	MUST
Spoofing prevention	MUST
Protection from DoS attacks against the time protocol	SHOULD
Replay protection	MUST
Key freshness	MUST
Security association	SHOULD
Unicast and multicast associations	SHOULD
Performance: no degradation in quality of time transfer	MUST
Performance: computation load	SHOULD
Performance: storage	SHOULD
Performance: bandwidth	SHOULD
Confidentiality protection	MAY
Protection against delay and interception attacks	MUST
Secure mode	MUST
Hybrid mode	SHOULD

6 Conclusion and future work

With the advent of 5G-Adv and 6G networks, the wireless technology landscape is poised for a profound transformation. These developments will redefine communication networks to meet the ever-increasing demands of a world that is increasingly interconnected and data-centric. The pivotal role these networks play in ensuring dependable communication across the physical and digital worlds. Additionally, with heterogeneous application domains, encompassing industrial automation, healthcare, augmented reality, and more, the need for dependable communication infrastructures is undeniable. However, the expansion of this scope, particularly within the context of cyber-physical continuum and future heterogeneous industrial networks, has put forward some challenges, most notably regarding the rigorous quality-of-service (QoS) requirements.

An important challenge is the precise and resilient synchronization of time across the physical and digital worlds along with a plethora of devices and network elements, spanning diverse industrial environments and communication technologies. This temporal synchronization is fundamental in realizing the seamless operation of a wide array of applications, particularly within industrial settings, where precision, automation, and data integrity hold paramount importance.

The significance of precise time synchronization is twofold. Firstly, it plays a pivotal role in the realization of industrial automation use cases, which encompass extended reality, distributed and adaptive manufacturing, e-health, exoskeletons, datacenters, autonomous and self-driving, and the coordination of autonomous systems. In these advanced industrial scenarios, end-to-end (E2E) dependable communications are indispensable, with accurate temporal alignment serving as the key player for optimizing efficiency, error reduction, and the seamless interoperation of these highly sophisticated systems. On the other hand, the resilience and security of time synchronization systems assume equal importance, given the tendency of industrial environments to network disruptions, hardware anomalies, and cybersecurity threats.

In this deliverable, we present a first report on resilient and secure time synchronization framework for the future 5G-Adv/6G networks. We first present some industrial use cases targeted by the DETERMINISTIC6G project along with some future time synchronization use cases, thereby illustrating the multifaceted applications of precise temporal coordination. Then we focus on mechanisms designed to introduce resilience, with a notable emphasis on redundancy as a means to support temporal accuracy and reliability within the domain of industrial processes. Furthermore, we have investigated the possible enhancements of essential 3GPP network functions required for the seamless synchronization of time within 5G-Adv/6G networks. Additionally, we have presented the first concepts on time synchronization security. With the first mechanisms presented in this deliverable, future work will encompass further development of discussed mechanisms to support end-to-end time awareness. In particular, the future work will focus on refining the architectures for redundancy in clock sources. In this context, we plan to address the open questions related to restoration and resynchronization of GMs. Additionally, we will focus on the analysis of the proposed architectures in terms of the time error analysis. With regards to enhancements for 3GPP compliant network functions, we will look at additional functions required to ensure the 5G system provides residence time under the PTP limits. Additionally, we will also evaluate the additional delays caused by in-band network telemetry on time synchronization packets. We will then simulate a packet replay attack scenarios to evaluate the detection ability of the security monitoring framework, and, if possible, evaluate the resilience of the time synchronization process.

References

[3GPP-TS23501]	3GPP, “TS 23.501: Technical specification group services and system aspects, system architecture for the 5G system (5GS),” Release-18, v18.0.0, 2022.
[3GPP-TS23700]	3GPP, “TS 23.700-20: Technical specification group services and system aspects; study on enhanced support of industrial internet of things (IIoT) in the 5G system (5GS),” Release-17, v1.0.2, 2020.
[3GPP-TS38133]	3GPP, “TS 38.133: Technical Specification Group Radio Access Network; NR Requirements for support of radio resource management”
[3GPP-TS38300]	3GPP, “TS38.300: NR; NR and NG-RAN Overall description; Stage-2”
[3GPP-TS22261]	3GPP TS 22.261, “Service requirements for the 5G system,” v19.4.0, 2016
[AAH97]	Allan, D. W., Ashby, N., & Hodge, C. C. The science of timekeeping (pp. 56-65). Palo Alto, CA, USA: Hewlett-Packard. 1997.
[AMS+21]	M. K. Atiq, R. Muzaffar, Ó. Seijo, I. Val, H.-P. Bernhard. “When IEEE 802.11 and 5G meet time-sensitive networking,” IEEE Open Journal of the Industrial Electronics Society, 3, 14-36, 2021.
[BCAMM+18]	B. Moussa, C. Robillard, A. Zugenmaier, M. Kassouf, M. Debbabi, and C. Assi, “Securing the Precision Time Protocol (PTP) Against Fake Timestamps,” IEEE Commun. Lett., vol. 23, no. 2, pp. 278–281, 2018.
[BG03]	Butner, S. E., and M. Ghodoussi. "Transforming a surgical robot for human telesurgery." IEEE Transactions on Robotics and Automation 19.5, 818-824, 2003.
[BK20]	Batiha, T, Krömer, P. Design and analysis of efficient neural intrusion detection for wireless sensor networks. Concurrency Computat Pract Exper., vol. 33, 2021
[BK21]	B. Brik and A. Ksentini, "Toward Optimal MEC Resource Dimensioning for a Vehicle Collision Avoidance System: A Deep Learning Approach," in IEEE Network, vol. 35, no. 3, pp. 74-80, May/June 2021, doi: 10.1109/MNET.011.2000577.
[BLWB23]	A. Byagowi, D. Levi, E. Wind and E. Blatt, “Open Source Time Synchronization Services for Data Center Operators”: https://developer.nvidia.com/blog/open-source-time-synchronization-services-for-data-center-operators/.
[BSS+20]	Bances, E., Schneider, U., Siegert, J., & Bauernhansl, T. Exoskeletons towards industrie 4.0: benefits and challenges of the IoT communication architecture. Procedia manufacturing, 42, 49-56, 2020.
[CAK23]	Chandramouli, D., Andres-Maldonado, P., & Kolding, T., Evolution of Timing Services from 5G-A towards 6G. IEEE Access. 2023.
[ComcoresWP]	Comcores ApS, "Delivering timing accuracy in 5G networks", Whitepaper
[D6G-D1.1]	D1.1 “DETERMINISTIC6G use cases and architecture principles”, DETERMINISTIC6G, June 2023.
[D6G-D3.2]	D3.2 ”Report on security measures”, DETERMINISTIC6G, Dec. 2023.
[DCJ+21]	D. Ergenc, C. Brulhart, J. Neumann, L. Kruger, and M. Fischer, “On the Security of IEEE 802.1 Time-Sensitive Networking,” 2021 IEEE Int. Conf. Commun. Work. ICC Work. 2021 - Proc., 2021.

[EricssonWP]	Ericsson, "Synchronization solutions in 5G transport network" Whitepaper", 2021.
[FBZ+21]	F. Luo, B. Wang, Z. Fang, Z. Yang, and Y. Jiang, "Security Analysis of the TSN Backbone Architecture and Anomaly Detection System Design Based on IEEE 802.1Qci", Secur. Commun. Networks, vol. 2021, 2021.
[FVM+19]	J. Farkas, B. Varga, G. Miklos, and J. Sachs, "5G-TSN Integration for Industrial Automation," Ericsson, 2019.
[GLA+20]	Gore, R. N., Lisova, E., Åkerberg, J., & Björkman, M., Clock synchronization in future industrial networks: Applications, challenges, and directions. In 2020 AEIT International Annual Conference (AEIT) (pp. 1-6). IEEE, 2020.
[GLR+20]	I. Godor, M. Luvisotto, S. Ruffini, K. Wang, D. Patel, J. Sachs, O. Dobrijevic, D. P. Venmani, O. L. Moult, J. Costa-Requena, A. Poutanen, C. Marshall, and J. Farkas, "A Look Inside 5G Standards to Support Time Synchronization for Smart Manufacturing," in IEEE Communications Standards Magazine, vol. 4, no. 3, pp. 14–21. 2020.
[GOT10]	Garner, G. M., Ouellette, M., & Teener, M. J.,"Using an IEEE 802.1 AS network as a distributed IEEE 1588 boundary, ordinary, or transparent clock." IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication. pp. 109-115. IEEE. 2010.
[GPM+20]	Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., & Zorzi, M., Toward 6G networks: Use cases and technologies. IEEE Communications Magazine, 58(3), 55-61, 2020.
[GSD+17]	M. Gutĭ errez, W. Steiner, R. Dobrin, and S. Punnekkat, "Synchronization quality of IEEE 802.1 AS in large-scale industrial automation networks," in IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), pp. 273–282, 2017.
[GH+20]	M. Gundall, C. Huber, P. Rost, R. Halfmann and H. D. Schotten, "Integration of 5G with TSN as Prerequisite for a Highly Flexible Future Industrial Automation: Time Synchronization based on IEEE 802.1AS," Annual Conference of the IEEE Industrial Electronics Society (IECON), pp. 3823-3830, 2020.
[HSB11]	Haidegger, Tamás, József Sándor, and Zoltán Benyó. "Surgery in space: the future of robotic telesurgery." Surgical endoscopy 25, 681-690, 2011.
[HGL20]	Huang, S., Guo, B., & Liu, Y., 5G-oriented optical underlay network slicing technology and challenges. IEEE Communications Magazine, 58(2), 13-19, 2020.
[IEEE802.1AS-2020]	IEEE Standard for Local and Metropolitan Area Networks--Timing and Synchronization for Time-Sensitive Applications. IEEE 802.1AS-2020, 2020.
[IEEE 1588-2019]	"IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," IEEE 1588-2019, 2019.
[IEEE p1588g-D1.2]	IEEE Draft Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems Amendment: Master-slave optional alternative terminology. Amendment to IEEE Std 1588-2019, 2022.
[ITU-G8265.1]	ITU-T G.8265.1, "Precision time protocol telecom profile for frequency synchronization"

[ITU-G8275.1]	ITU G.8275.1, “Precision Time Protocol Telecom Profile for Phase/Time Synchronization with Full Timing Support from the Network.”
[ITU-G8275.2]	ITU-T G.8275.2, “Precision time protocol telecom profile for phase/time synchronization with partial timing support from the network”.
[JLP14]	Y. Jeon, J. Lee, and S. Park, “An efficient method of reselecting grand master in IEEE 802.1 AS,” in The 20th Asia-Pacific Conference on Communication (APCC2014), IEEE, pp. 303–308, 2014.
[KO87]	H. Kopetz and W. Ochsenreiter, “Clock synchronization in distributed real-time systems,” IEEE Transactions on Computers, vol. 100, no. 8, pp. 933–940, 1987.
[MAG+19]	A. Mahmood, M. I. Ashraf, M. Gidlund, J. Torsner, and J. Sachs, “Time synchronization in 5G wireless edge: Requirements and solutions for critical-MTC,” in IEEE ComMag, vol. 57, no. 12, pp. 45–51, 2019.
[MAG+18]	A. Mahmood, M. I. Ashraf, M. Gidlund, and J. Torsner, “Over-theAir Time Synchronization for URLLC: Requirements, Challenges and Possible Enablers,” in 2018 15th International Symposium on Wireless Communication Systems (ISWCS), pp. 1–6. 2018.
[MBK+23]	Mahmood, N. H., Berardinelli, G., Khatib, E. J., Hashemi, R., De Lima, C., & Latva-aho, M., A Functional Architecture for 6G Special-Purpose Industrial IoT Networks. IEEE Transactions on Industrial informatics, 19(3), 2530-2540, 2023.
[MGG+23]	Municio, E., Garcia-Aviles, G., Garcia-Saavedra, A., & Costa-Pérez, X. , O-RAN: Analysis of Latency-Critical Interfaces and Overview of Time Sensitive Networking Solutions. IEEE Communications Standards Magazine, 7(3), 82-89, 2023.
[OCP-TAP]	https://www.opencompute.org/projects/time-appliances-project-tap
[PDR+21]	D. Patel, J. Diachina, S. Ruffini, M. De Andrade, J. Sachs, and D. P. Venmani, “Time error analysis of 5G time synchronization solutions for time aware industrial networks,” in IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS),pp. 1–6, 2021.
[PRC20]	T. K. Peter M. Rost, D. Chandramouli, “5G plug-and-produce,” Whitepaper, Nokia, 2020.
[Pres23]	https://iebmedia.com/technology/tsn/2023-time-sensitive-networking-technology-update/
[R2-2100001]	3GPP R2-2100001” Report of 3GPP TSG RAN2#112-e meeting”
[RFC-7384]	T. Mizrahi, "RFC 7384 - Security Requirements of Time Protocols in Packet Switched Networks", 2014.
[Rizk22]	https://developer.nvidia.com/blog/understanding-the-need-for-time-sensitive-networking-for-critical-applications, 2022.
[S20]	M Schüngel , Analysis of time synchronization for converged wired and wireless networks,” in 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), vol. 1, pp. 198–205, 2020.
[SAP+21]	Shahraki, A., Abbasi, M., Piran, M. J., & Taherkordi, A., A comprehensive survey on 6G networks: Applications, core services, enabling technologies, and future challenges, arXiv preprint arXiv:2101.12475., 2021.

[SDL+21]	M. Schüngel, S. Dietrich, L. Leurs, D. Ginthör, S.-P. Chen, and M. Kuhn, “Advanced grandmaster selection method for converged wired and wireless networks,” in 22nd IEEE International Conference on Industrial Technology (ICIT), vol. 1, pp. 1007–1014, 2021.
[SGZ+23]	Shen, X. S., Gao, J., Li, M., Zhou, C., Hu, S., He, M., & Zhuang, W. Toward immersive communications in 6G. Frontiers in Computer Science, 4, 1068478, 2023.
[SJP+21]	Stefano Ruffini, Mikael Johansson, Björn Pohlman, Magnus Sandgren, “5G synchronization requirements and solutions” Ericsson Technology Review, January 2021.
[SPS+23]	Sharma, G. P., Patel, D., Sachs, J., De Andrade, M., Farkas, J., Harmatos, J., ... & Gross, J., ”Towards Deterministic Communications in 6G Networks: State of the Art, Open Challenges and the Way Forward”. in IEEE Access, vol. 11, pp. 106898-106923, 2023.
[SS97]	U. Schmid and K. Schossmaier, “Interval-based clock synchronization,” Real-Time Systems, vol. 12, pp. 173–228, 1997.
[T07]	Tanenbaum, Andrew S. Distributed systems principles and paradigms. 2007.
[WS20]	D. Wang and T. Sun, "Leveraging 5G TSN in V2X Communication for Cloud Vehicle," 2020 IEEE International Conference on Edge Computing (EDGE), Beijing, China, pp. 106-110, 2020.
[WMs+21]	W. Alghamdi and M. Schukat, “Precision time protocol attack strategies and their resistance to existing security extensions,” Cybersecurity, vol. 4, no. 1, 2021.
[ZVF+20]	Ziegler, V., Viswanathan, H., Flinck, H., Hoffmann, M., Räisänen, V., & Hätönen, K., 6G architecture to connect the worlds. IEEE Access, 8, 173508-173520, 2020.
[Ga20]	I. Godor et al., "A Look Inside 5G Standards to Support Time Synchronization for Smart Manufacturing," in IEEE Communications Standards Magazine, vol. 4, no. 3, pp. 14-21, September 2020.
[ZSD+21]	H. Zhou, C. She, Y. Deng, M. Dohler and A. Nallanathan, "Machine Learning for Massive Industrial Internet of Things," in IEEE Wireless Communications, vol. 28, no. 4, pp. 81-87, August 2021.

List of abbreviations

Table 5 List of abbreviations

Acronym	Explanation
5G	Fifth generation
5GC	5G core
5GS	5G system
5G-Adv	5G advanced
6G	Sixth generation
AF	Application function
AI	Artificial intelligence
AR	Augmented reality
AVB	Audio video bridging
BTCA	Best timeTransmitter clock algorithm
CRR	Cumulative rate ratio
DetNet	Deterministic networking
DoS	Denial-of-service
DL	downlink
DS-TT	Device side TSN translator
E2E	End-to-end
gNB	Next generation NodeB
GM	Grandmaster
gPTP	Generic precision time protocol
GPS	Global positioning system
GNSS	Global navigation satellite system
IoT	Internet of things
LAN	Local area networks
ML	Machine learning
MIMO	multiple-input multiple-output
NTP	Network time protocol
NRR	Neighbor rate ratio
NW-TT	Network side TSN translator
PDU	Protocol data unit
PSFP	Per-stream filtering and policing
PTP	Precision time protocol
PTP-tele	PTP telecom
PMIC	Port management information
QoS	Quality of service
RAN	Radio access network
RRC	Radio resource control
SIBs	System information blocks

TSN	Time sensitive networking
TSCTSF	Time sensitive communications time sensitive function
TSe	Egress timestamp
TSi	Ingress timestamp
tR	timeReceiver
tT	timeTransmitter
UE	User equipment
UTC	Coordinated universal time
UMIC	User management information
UL	Uplink
UPF	User plane function
UU	Radio interface
VR	Virtual reality
XR	Extended reality