MODULAR ARCHITECTURE PROVIDING CONVERGENT AND UBIQUITOUS INTELLIGENT CONNECTIVITY FOR NETWORKS BEYOND 2030

Luis M. Contreras[1], Javier Serrano[2], Lefteris Mamatas[3], Giacomo Bernini[4], Paolo Monti[5], Mario Antunes[6], Udayanto Atmojo[7], Eli Tocker[8], Iñaki Val[9], Andrea Sgambelluri[10], Jérôme Härri[11], Antonio Lioy[12], Pedro Martinez-Julia[13], José González[14], Jorge Sánchez-Garrido[15], Hitoshi Asaeda[13]

[1]Telefónica CTIO, Ronda de la Comunicación s/n, 28050 Madrid, Spain [2]Signals, Systems and Radiocommunications (SSR) Dept., Universidad Politécnica de Madrid, Avda. Complutense, 30, 28040 Madrid, Spain [3] Department of Applied Informatics, University of Macedonia, 156 Egnatia Street, GR-546 36 Thessaloniki, Greece [4]Nextworks s.r.l., via Livornese, 1027 , 56122 Pisa, Italy, [5]Chalmers University of Technology, 41296 Gothenburg, Sweden [6]Instituto de Telecomunicações, Campus Universitario de Santiago, Universidade de Aveiro, 3810 193 Gloria e Vera Cruz, Portugal [7]Department of Electrical Engineering and Automation, Aalto University, Ootakari 1, 02150 Espoo, Findland [8]ECI Telecom (Ribbon Communications), 30 HaSivim St., 4959388 Petah Tikva, Israel [9]Ikerlan Technology Research Centre, Basque Research and Technology Alliance (BRTA), P.º J.M. Arizmendiarrieta 2, Arrasate/Mondragon, Spain [10]Scuola Superiore Sant'Anna, Via G. Moruzzi, 1 56100 Pisa, Italy [11]EURECOM, Route des Chappes 450, Campus SophiaTech, 06410 Biot, France [12]Politecnico di Torino, Dip. Automatica e Informatica, c. Duca degli Abruzzi, 24, 10129 Torino, Italy [13]Network Architecture Laboratory, National Institute of Information and Communications Technology (NICT), 4-2-1, Nukui-Kitamachi, Koganei, 184-8795 Tokyo, Japan [14]AUSTRALO Interinnov Marketing Lab SL, Pompeu Fabra 1. 08860 Castelldefels, Spain [15]Orolia Spain S.L.U, Edf. CETIC, Calle Periodista Rafael Gómez Montero, 2, 18014 Granada, Spain

NOTE: Corresponding author: Luis M. Contreras, luismiguel.contrerasmurillo@telefonica.com

---

Abstract – *The transition of the networks to support forthcoming beyond 5G (B5G) and 6G services introduces a number of important architectural challenges that force an evolution of existing operational frameworks. Current networks have introduced technical paradigms such as network virtualization, programmability and slicing, being a trend known as network softwarization. Forthcoming B5G and 6G services imposing stringent requirements will motivate a new radical change, augmenting those paradigms with the idea of smartness, pursuing an overall optimization on the usage of network and compute resources in a zero-trust environment. This paper presents a modular architecture under the concept of Convergent and UBiquitous Intelligent Connectivity (CUBIC), conceived to facilitate the aforementioned transition. CUBIC intends to investigate and innovate on the usage, combination and development of novel technologies to accompany the migration of existing networks towards Convergent and Ubiquitous Intelligent Connectivity (CUBIC) solutions, leveraging Artificial Intelligence (AI) mechanisms and Machine Learning (ML) tools in a totally secure environment.*

Keywords – A*rchitecture, beyond 5G, 6G, smartness*

1. INTRODUCTION

Beyond 5G (B5G) and 6G services are expected to introduce very stringent requirements to existing networks which can be only overcome by combining and exploiting together a variety of technologies and techniques currently being under initial development or experimentally researched. The key concept for future advanced networks is the one of *Smartness* as introduced in [2], which means that the network should be able to continuously take into consideration the specific context of the end users as well as the status of the network itself. The network should be understood in a broad sense, spanning from the connectivity context, and the availability of computing facilities for the deployment of service functions or applications, to the virtualization mechanisms for dynamic instantiation. All of these provision aspects impact on provisioning and operation of end-to-end services according to specific Service Level Objectives (SLOs). Last, but not least, it should operate in a multi-stakeholder zero-trust environment. This vision calls for a new architectural framework being able to smoothly integrate these capabilities.

The starting point for such evolution is defined by the present capabilities of existing networks, being rolled out nowadays targeting the needs of 5G in scope. 5G has been transformational across multiple technologies, processes and network segments, implying an overall network evolution surrounding the development of a new radio generation, as it is considered happening with 6G.

In the pace of adoption of advanced 5G and beyond technologies there will be a stepwise transition across the different releases of 5G as defined by 3GPP. Release 17, to be fully completed by mid-2022, will include advancements for the industrial Internet, integrated access and backhaul, network slicing, enhanced battery health, and satellite integration. Release 18 will then enable 5G advanced, expected to be commercially available by 2024, and including new 5G use cases such as 5G satellite network access, sub-5 MHz carriers for smart grids and railways, enhanced coverage, and a 50% higher energy efficiency due to small packet optimization. After that, releases 19 and 20 would produce improvements to 5G advanced, with a basic 6G expected for Release 21, around 2027/28, with 2030 appearing as the potential date for a full-fledged 6G solution.

Thus, the networks supporting 6G will build on top of existing capabilities which need to be properly extended and complemented, while ensuring preservation of current investments as well as facilitating a smooth incorporation of B5G and 6G advancements from now till 2030.

As a main contribution, this paper presents a novel modular architecture conceived with the concept of Convergent and UBiquitous Intelligent Connectivity (CUBIC) in mind, pursuing such an idea as smartness and gradually integrating, in a scalable and flexible way, the advances that the industry is producing in different fronts such as data plane evolution. In this sense, the key advances of the architecture we propose derive from its focus on resolving the challenges present in the network landscape, such as management automation [39] [40], taking decisions based on intelligence collection and processing [41], multi-vendor, multi-tenant, and multi-domain operations, and the overall coverage of the different levels of QoS and QoE already exposed by 5G and projected to B5G/6G environments.

2. RELATED WORK

Existing networks are embracing the network softwarization trend, fostered by the development of technologies facilitating network programmability, virtualization, and ultimately, slicing. A short and mid-term analysis of available enabling technologies is available in [7].

It is expected that novel developments and research will build on top of such state-of-the-art situations. Several academic and industrial proposals, analysis

and views are appearing with the aim of providing insights on the implications of 6G.

Samdanis and Taleb [3] provides an overview of the different technological evolution serving as a base of B5G and 6G networks, such as new radio paradigms, the paradigm of micro-services as a pattern for deploying functions, the need for data analytics for automation, as well as deterministic and reliable data planes. Akyildiz et al. [5] provide further insights on the evolution of wireless solutions, including the introduction of AI capabilities on them. Yazar et al. work in [6] presents 6G key enablers from the perspective of flexible management and operation of the networks, in order to accomplish the agreed SLOs and maximize the usage of involved resources.

Ziegler et al. [4] proposes evolutionary paths for a 6G network architecture, relying on a number of constituent building blocks, namely platform (e.g. with distributed compute and communication resources), functional (e.g. facilitating dynamic re-configurability), specialized (e.g. enabling deep slicing), and orchestration (e.g. implementing cognitive closed loops and automation).

Equipment manufacturers have also provided their own views on the evolution to 6G. Vendors like Samsung [8], Ericsson [9] and Nokia [4][10] have explored the use cases and related requirements to do prospects on technology evolution. Similarly, network operators, mainly in Asia [11][12][13], have analyzed the implications of the new 6G services from an operational point of view.

There are also specific regional views on the evolution to 6G across the world, in Europe [14], Asia [15][16] and Americas [17], complemented with others at the international level [18].

From all of this background, it can be concluded that the new architectures for 2030 supporting advanced B5G and 6G services need to incorporate basic features such as support of communications with strict guarantees, automated control assisted by intelligent mechanisms, possibility of controlling infrastructures and resources (both compute and network) from multiple stakeholders, all of that in a zero-trust ecosystem. These main principles form then the baseline for the CUBIC approach.

3. CUBIC CONCEPT

The architecture proposed in this article intends to accompany the migration of existing networks towards Convergent and UBiquitous Intelligent Connectivity (CUBIC)-like solutions.

The smart networks approach, as defined in [1], assumes a *"combination of Smart Connectivity, Data Analytics (AI and ML), high performance distributed computing and Cybersecurity"*. The principles of CUBIC are based on the capabilities associated to each of these four dimensions, as follows:

- *Smart Connectivity*, by leveraging the particular and specific characteristics of a variety of transport network solutions pursuing the optimal selection of technology according to the different types of B5G/6G services to be delivered, as well as combining mechanisms considered up to now as orthogonal, such as "soft and hard" slicing, i.e., expressing the slice resource isolation level required.
- *Data Analytics*, extracting the appropriate monitoring and telemetry information from the underlying supportive infrastructure as well as from the running services on top of it, arranging the best decision at every moment, and considering different time scales and points of decision in a cooperative approach. This allows us to predict and react to service degradations and failures in a prompt manner to future events, e.g. due to situations like rapid changes on the demand (flash crowd events), network congestion, etc.
- *Distributed computing*, assuming the availability of several coexisting centralized and edge computing environments, used intelligently to enforce B5G/6G service Key Performance Indicators (KPIs), by dynamically instantiating both customer-oriented and provider-oriented network functions and applications. As part of that distributed computing substrate, the resources from third parties such as Over-The-Top (OTT) providers are also considered going in the direction of multi-cloud networks.
- *Cybersecurity*, tackling the security and privacy concerns of future communications systems, where the existence of zero-trust cooperative environments will become even more crucial due to the expected interaction of multiple stakeholders in the provision of any end-to-end service.

To accomplish the challenges imposed by these four dimensions above, and in syntony with the B5G/6G evolution as described in, for example [14], the CUBIC architecture is designed with a number of key areas in mind.

The first one is related to the interplay of novel data plane solutions in a convergent manner. This is intended to be achieved by defining an architecture able to integrate multiple deterministic data plane technologies such as optical networking, Time Sensitive Networking (TSN) or Flexible Ethernet (FlexE), complemented with packet switching to allow statistical multiplexing gains for traffic of the same kind using resources of that deterministic solutions. There is then a combination of high capacity transport technologies with deterministic and predictable ones in terms of latency behavior. All of this will constitute an adaptive data plane.

The second aspect is the support of smart and flexible control plane mechanisms making such connectivity infrastructure flexibly programmable by combining and integrating Software-Defined Networking (SDN) solutions adapted to these different technologies, including programmable data planes. That is, an integrated control of the overall transport infrastructure to adapt it to the specificities of the demanded service. There are initial frameworks that can be extended in the direction here shown, as in [19], by adding low-level deep programmable capabilities like the ones enabled by P4 as part of the overall control plane solution.

Third, the usage of multiple virtualization approaches, like unikernels, serverless technologies or containers managed by Kubernetes, fitted to the specific needs of the service and/or the constraints of the compute execution environment, e.g. the location to instantiate functions and applications. From the services' point of view, the trend towards cloud-native architectures is now clear [20], enabling fast, flexible and lightweight virtualization. On the other hand, from the infrastructure point of view, a variety of computing infrastructures will become available [21], offering a diversity of environments and managed in a non-homogeneous way. Different virtualization options can be suitable to distinct operational circumstances [22], as for example the availability of resources in a given moment.

Fourth key area is an overarching end-to-end orchestration system maintaining an overall view of the integrated system capabilities and coordinating the lifecycle of end-to-end B5G/6G services, taking care to compose them by integrating the various domain specific capabilities as exposed by the edge and the transport network segments.

All of this, as the fifth key area, assisted by advanced and computational efficient AI/ML algorithms, providing the necessary insights for intelligent
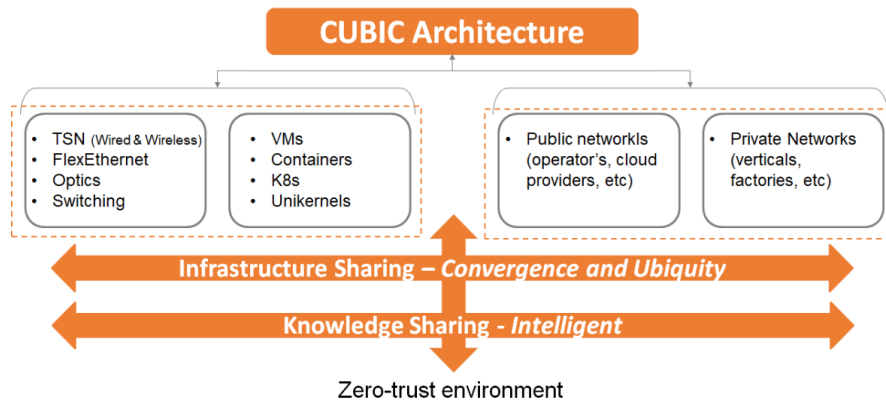
Fig. 1 – High-level CUBIC approach

decisions, implementing a robust, secure-by-design ecosystem, as the final sixth focus area.

It is important to consider that the ownership of the infrastructure supporting B5G/6G services will be shared among different actors, leading to a variety of multi-provider scenarios, with different but complementary types of capabilities and resources on each of the involved administrative domains. The multi-domain aspects, being fundamental for B5G/6G, have to be considered in the architecture from the perspective of a public operator (federation of providers), using infrastructure from third parties (such as the aforementioned OTTs or even from infrastructure providers playing the role of neutral hosts) for complementing its commercial offering, and also from the perspective of private-public interconnection where vertical industries can bring and integrate their own infrastructures as part of the CUBIC end-to-end ecosystem.

Fig. 1 summarizes the scope and ambition of CUBIC.

4. CUBIC ARCHITECTURE

CUBIC is intended to derive and classify service specific requirements that need to be supported by the end-to-end orchestration system, as well as the elastic and adaptive control and data planes. These imply, e.g. the automated provisioning of B5G/6G services across distinct infrastructures from multiple providers, the existence of an end-to-end management and control of the slices required for the instantiation of those services on a large scale, as well as the smart and secure run-time operation of those services leveraging AI/ML techniques.

The end-to-end orchestrator, as an integral part of the CUBIC architecture, will be in charge of coordinating resources, services and capabilities

from different administrative domains, including private networks, in a harmonized manner according to the service intents expressed by the customers of CUBIC. Those service intents will be translated in terms of advanced slices, flexibly combining soft plus hard approaches, maximizing the usage of compute and network resources from the adaptive data plane. Once deployed, a combination of reactive and proactive AI/ML will be applied to assist the operation and guarantee corresponding SLAs. Finally, security is applied to the system to protect the service execution and infrastructure integrity.

4.1 Architecture framework

In the evolution towards B5G/6G it is expected that a number of providers (i.e., application, service, infrastructure providers) need to commercially and technically cooperate for enabling end-to-end service delivery. This is clear when thinking of the need to increase the footprint of edge computing capabilities towards the access, with the rise of private networks, or simply with the trend of hyper-scalers targeting cloud-based services and infrastructures.

CUBIC is conceived as a modular architecture that can be adapted to different scenarios and adopted by different kind of actors. Such an architecture can largely simplify interaction and integration while pursuing such cooperation.

4.1.1 CUBIC domain

CUBIC considers as basic building block a single administrative domain with different infrastructure capabilities in terms of computing and networks controlled by a domain controller, as presented in Fig. 2. This same administrative domain can provide
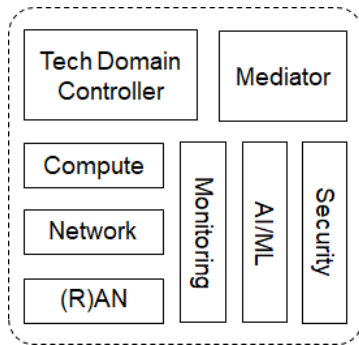
Fig. 2 – CUBIC domain

monitoring information of the infrastructure behind the domain and can also incorporate AI/ML and security capabilities to internally operate the infrastructure or be exposed towards external systems. On top of that, a number of open, standard and augmentable APIs (via the mediator) are available for facilitating easy integration with other domains, with well-defined abstraction models, common control and monitoring capabilities.

The basic components of a CUBIC domain allow for local control loop management through a visualization / analysis / control cycle. The monitoring component permits extract relevant monitoring and telemetry information (visualization stage) that can be further processed by the AI/ML component (analysis stage) for identifying the necessary actions on resources and services (control stage). This local loop can be further integrated on a global loop through proper APIs facilitating a similar visualization / analysis / control cycle but on a larger scale.

4.1.2 End-to-end CUBIC architecture

One service provider or operator can integrate multiple of these single administrative CUBIC domains via an integration fabric, each of them representing specific per-technology domains (e.g. specialized domains dedicated to satisfy certain performance requirements) or third party infrastructures, complementing the service provider footprint on a given geographical area (e.g. as offered by external infrastructure providers). As described before, an end-to-end orchestrator will be in charge of coordinating all the resources and services within an administrative domain, as depicted in Fig. 3.

For the interworking of multiple administrative domains and to satisfy B5G/6G services with stringent performance requirements, CUBIC considers an overarching orchestration layer able to manage all these diverse domains in an integrated and consistent manner. The latter are able to interact through the referred integration fabric, accessed by normalized CUBIC APIs. Similarly, the orchestration layer can be accessible to the customers by a module supporting powerful intent-based service exposure and delivery mechanisms for translating customer B5G/6G service requests to advanced slices in the underlying compute and network substrate.

This modular architecture can even be replicated for the federation of providers and for the interconnection of private to public networks, leveraging, one more time, the integration fabric. With the aim of implementing a truly agile and flexible end-to-end system, ready to cope with the high dynamicity of B5G/6G services (in both time and space), CUBIC primarily aligns with the ETSI ZSM approach where APIs are defined in the context of such an integration fabric that regulates the interactions among the end-to-end orchestration layer and the domain controllers for various service management aspects (i.e., including resource control and provisioning, service monitoring, data analytics, etc.), and offering the possibility to delegate some of these aspects to the domain controllers. Finally, the interconnection of private networks, such as the ones represented by vertical industries, is also intended to be realized through the same set of CUBIC APIs and the integration fabric enabling the multi-domain case. Fig. 3 shows the modular approach of CUBIC integrating multiple domains and interacting with different public and private stakeholders.

Thus, the key element helping to provide a vertebrate to all the interactions among components is the integration fabric. This integration fabric provides the necessary abstractions that could later on allow interaction with the different data plane and virtualization technologies, for both networking and computing environments. In order to do so, it facilitates the expression of B5G/6G service requirements to produce proper allocation and placement algorithms by the orchestration engine. It also supports monitoring and allows the sharing of knowledge for the AI/ML algorithms. Moreover, it incorporates the necessary security features to enable a trusted interaction among parties. The APIs supporting such integration fabric enable the integration of providers, facilitating sustainability and economic viability through the reduction of integration times and providing openness to the market.

4.2 Technical approach

The very stringent requirements of B5G/6G services (e.g. extremely low latency, large bandwidth or high resiliency), pave the way for tremendous innovation and novel solutions targeting 2030 networks. It needs fresh thinking about finding a compromise between reliability, dedicated bandwidth and minimum latency. Communication paths should be selected with ultra-high capacity and very low latency in mind, with a trade-off between reliability and latency tailored to the application requirements. Thus, end-to-end communication requires smart and agile end-to-end orchestration logics to integrate the various domain technologies and segments and follow the dynamicity and heterogeneity of B5G/6G services. The following sections present the technical ambition of CUBIC.

4.2.1 Integration of low latency and high bandwidth data plane technologies

The smooth integration of distinct data plane solutions is an enabler for B5G/6G services.

The emerging need for deterministic real-time communications has pushed recent developments in the framework of low latency networks, but today's most industrial networks rely on vendor-locked solutions, having therefore important flexibility problems.

A number of technologies can be considered at the time of providing determinism. The IEEE Time Sensitive Networking set of standards [23] represent an enhancement to Ethernet that aims to ensure a minimum reserved bandwidth, bounded end-to-end latency, and deterministic time transfer for critical control traffic, thus bridging the gap between regular Ethernet and real-time applications. This enhancement allows the coexistence of both deterministic traffic and ordinary (best-effort) Internet-like traffic on the same physical network. Developments on wireless solutions are intending similar behavior, pursuing a wireless TSN approach, as in [24]. The final objective is to seamlessly integrate both wired and wireless TSN as a common TSN asset, allowing the extension of the TSN flows up to the wireless end devices. The approach is to dynamically control and monitor both wired and wireless elements through a common TSN controller (based on IEEE 802.1Qcc).

Another deterministic technology in consideration is Flexible Ethernet (FlexE). FlexE logically divides the network interface capacity into physically isolated Ethernet channels of varying rates (through aggregation of such channels) emulating a Time Division Multiplexing (TDM) behavior with a standardized granularity of 5 Gbps. This permits adaptation to multiple rates (leveraging schemas such as traffic grooming, interface and slots bonding etc).
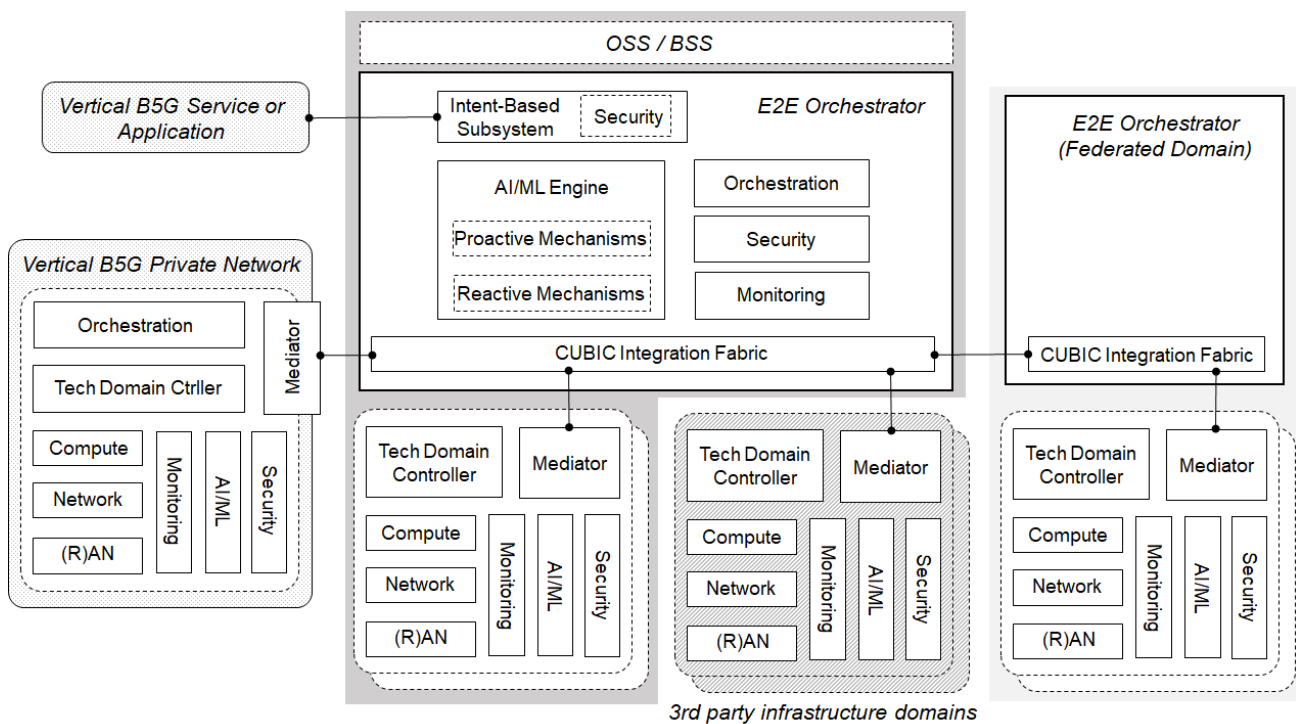

Fig. 3 – Overview of the CUBIC architecture

Complementary to that, adaptive and elastic optical networks can utilize wavelengths and optical spectral resources efficiently. The adaptive and elastic optical networks (with Flexgrid capability) will utilize all spectral resources in the network by using all available multiple degrees of freedom (e.g. leveraging the modulation method, baud rate, FEC, etc), while allocating the minimum necessary bandwidth to client requirements, keeping QoS targets.

4.2.2 Adaptive programmatic network

The gradual introduction of programmability in existing networks provides a baseline framework for network control, as described in [19][25]. Such architectures leverage programmatic interfaces offered by network elements, and on the usage of YANG-based data models for network and device configuration [26]. This provides a first level of programmability but is constrained to the capabilities predefined by the specific data models.

Deeper programmability can be performed by programming the device packet processors' data plane. The most prominent solution nowadays is the P4 (Programming Protocol-independent Packet Processors) language [27]. P4 follows the SDN paradigm and it is conceived as an abstract programming language of networking chips that applies custom/specific forwarding schemes.

P4 allows for the development of new protocols, advanced forwarding and congestion control strategies, ad-hoc monitoring and telemetry functions without the need for costly/dedicated proprietary devices or time-consuming hardware firmware upgrades. By means of parsers, metadata, conditional controls, tables, and a set of actions, it provides the main building blocks of a network node, implementing packet-forwarding policies and algorithms, producing portable implementations over different hardware targets (e.g. NICs, FPGAs, software switches, bare metal switches and hardware ASICs).

Considering multilayer networks scenarios, the enforcement of SDN-based Traffic Engineering (TE) techniques is possible by steering the traffic according to policies. The policies are configured using specific flow entries, based on static or stateless match conditions. However, when traffic conditions change, the controller has to react re-computing and reconfiguring new policies by relying on complex monitoring and telemetry techniques, producing severe scalability issues on it.

CUBIC envisages the adoption of the P4 language to enable a multilayer/multi-technology (i.e., packet over optical, or packet over FlexE) aggregation with an advanced and programmable SDN forwarding plane, with nodes that need dynamic and specific treatment of vertical traffic, guaranteeing QoS and TE requirements. The SDN controller, a part of using YANG models for conventional equipment, will be responsible for table entries' population, service deployment and pipelining enforcement, programming multiple functions at the same device, including TE/QoS features (e.g. latency-aware forwarding and dynamic offloading) and security applications (e.g. mitigation, traffic telemetry and anomalies reports). By resorting to artificial intelligence and machine learning techniques (as commented later), real-time and fine-grade statistics can be processed, enabling feedback-based automatic SDN intervention procedures.

The overarching SDN control, following the same strategy as in [19], can also integrate with IEEE 802.1Qcc for the TSN part and with the optical controller for the optical part.

4.2.3 Intelligent utilization of compute environments

The cloud-native approach allows rapid creation and updating of services, while being agile, scalable and interoperable with other applications. The microservices paradigm [28] realizes large-scale services based on modular, autonomous, single-purpose software entities communicating with each other. Microservices are characterized by resilience, agility, scalability and flexibility. Consequently, network functions, microservices, as well as the involvement of resource-constrained edge cloud technologies, call for efficiently orchestrated solutions that are very flexible and lightweight. Such Lightweight and Fluid Virtualization (LFV) approaches include the containers [29][30], the unikernels [31][32] and those following the serverless paradigm [33].

Containers are standardized units of software that contain the implemented application and all its dependencies pre-installed. They provide a high degree of portability, have smaller sizes compared to VMs, improve the allocation of computing resources and can launch really fast. They also enable the DevOps paradigm, supporting the Continuous Integration / Continuous Delivery (CI/CD) of services. However, they operate in a shared kernel space, so they face security and isolation issues.

Unikernels are single-purpose appliances that are specialized at compile-time into standalone kernels, acting as individual software components and being sealed against modification when deployed in a cloud platform. Unikernels, compared to containers, are tiny in size and demand less resources, i.e., they can (i) boot rapidly, in milliseconds; and (ii) are isolated and have a smaller attack surface. However, the unikernel approach has issues with multi-threading execution, a lack of orchestration capabilities and appropriate environments to operate them in edge clouds.

Finally, the serverless paradigm orchestrates and executes units of code on-demand over scalable virtualized server environments. This approach brings the advantages of reducing the administration and server management cost and the development time, and introducing new billing models (e.g. pay-per-execution).

CUBIC targets a uniform orchestration of services, LFV resources and data plane aspects, for achieving maximum improvements in performance and resource allocation efficiency. The purpose is the support of different heterogeneous LFV approaches with appropriate virtual resource abstractions and APIs, e.g. unikernels for edge clouds and containers for core clouds. In addition to that, the solution is conceived to provide fluid elasticity capabilities in edge cloud deployments. For that, CUBIC handles the orchestration complexity of the fluid virtual resources leveraging AI/ML mechanisms (as described later) utilizing monitoring information from services, networks and virtual resources, as well as associated predictions for the traffic requirements.

CUBIC architecture and intelligent features, such as the appropriate abstractions and APIs over heterogeneous lightweight virtualization technologies, provide the missing aspects of unikernel-based deployments, i.e., orchestration capabilities and appropriate features to operate in edge clouds. The lack of multi-threading execution is handled by the adoption of the microservice-based architectural paradigm, where single-purposed service nodes communicate between each other with tuned resource consumption and can be scaled according to the service needs, the resource consumption level and the number of users requesting the particular service. Nevertheless, a network of application service graph can constitute by different virtualization technologies, depending on their diverse performance and resource demands (e.g. the need for rapid deployment can be addressed by unikernels and robust service performance by containers). A relevant extensive performance evaluation along with particular architectural requirements, which we considered in the design of CUBIC, can be found in [22].

4.2.4 Smart orchestration of multiplicity of service requirements

With the objective of supporting B5G/6G services, the telecommunications industry needs to consider comprehensive orchestration solutions to ease the deployment of heterogeneous services on tailored allocated resources (in the form of advanced network slices) across several technology domains. In this respect, the ability of addressing a multiplicity of requirements in terms of time sensitivity and ultra-low latency will be of paramount importance.

Nowadays, network slicing allows joint orchestration of resources (i.e., network, computing, storage) and virtualized or physical network functions.

Current approaches are based on monolithic control and orchestration solutions, mostly dedicated to the management of NFV-like pipelined network services, where the lack of agility in the service lifecycle and operation is still a clear limitation, especially when it comes to fulfilling time sensitive networking and ultra-low latency service constraints posed by B5G/6G services. Moreover, the capability of such orchestration approaches to fulfill heterogeneous service constraints and requirements is still to be proved, as often requires per-service customizations and human-driven adjustments of the operation / configuration to support end-to-end deployments.

In addition, the adoption of AI and ML technologies for cognitive-based optimizations, including their interaction across the different technological domains (e.g. network-related, edge computing-related, cloud computing-related) and their tight integration with the service and slice lifecycle management is at its early stages. The traditional monolithic end-to-end control and service orchestration architectures need to evolve to respond to spatially and temporally changing device densities, traffic patterns, and spectrum and infrastructure availability [34], as changing of service conditions will be at higher speeds in B5G/6G services requiring less overbooking at the

edge and more agile service components and functions deployments to quickly adapt to changing contexts. This goes in the direction of the zero-touch service management proposed and under definition in ETSI ZSM [35], that targets a novel, horizontal and vertical end-to-end operable framework for agile management and automation of emerging and future networks and services. ZSM envisages the clear identification and separation of management domains to provide the means to isolate management duties (possibly referring to very heterogeneous technologies), considering boundaries of different nature (i.e., technological, administrative, geographical, management scope etc.). An end-to-end service management domain is a special management domain responsible for the cross-domain management and coordination, which integrates all of the single domain management services, functions and endpoints through a cross-domain integration fabric, which facilitates the provision of services and the access to them.

CUBIC design delivers such an end-to-end service control and orchestration framework. First, by providing seamless orchestration of heterogeneous network sections and compute domains, with automatic translations of service intents (objectives) to network slices (QoS profiles) and related network services and network functions with appropriate placement matching the time sensitive requirements of vertical services. This is enabled by the integration of several network and compute domains by means of smart federation logics driven and coordinated by the end-to-end service orchestration. Additionally, CUBIC will adopt the intent-based approach not only to express networking but also for security, so that services and applications will express their end-to-end connectivity and security requirements in a high-level way and then the CUBIC orchestrator will take care to implement them in the best possible way.

Moreover, advanced vertical services and slices optimization can be supported through the integration of AI and ML-based adaptive operations into service run-time mechanisms.

The CUBIC end-to-end service control and orchestration framework also supports and reconciles different virtualization technologies across the network sections, enabling the deployment of network functions and vertical application functions as a combination of regular NFV functions at the core with cloud-native and serverless function at the edge, exploiting micro-clouds for private networks and service meshes.

CUBIC also proposes the integration of advances schemes and architectures for management automation, such as Autonomic Resource Control Architecture (ARCA) [39] [40]. It enables the tenants of the CUBIC networks and its solutions to ensure their services meet the target operational constraints, such as a high degree of stability, reliability, or even availability. These qualities are essential for the development of B5G/6G services.

Thus, CUBIC facilitates the migration from pipelined network service paradigm (NFV-like) to more agile microservice and service-based architectural approaches based on ML and AI decisions. This leverages the CUBIC integration fabric providing continuity of communication, with intra-domain and cross-domain communication fabrics following the approach defined by ETSI ZSM. The integration fabric enables federation and cooperation through local autonomous domain controllers to manage service lifetime and dynamics locally.

These functions are supported by the integration of the latest solutions to monitor and collect data, which are aligned with ETSI ENI (Experiential Network Intelligence) [41], which provides high-quality data collection, as well as the required processes to extract information and knowledge, which enables CUBIC to deliver accurate management decisions.

4.2.5 Smart connectivity platforms

Smartness will be a necessary capability for handling the complexity and variety of requirements and service situations expected for 2030. Thus, the deployment and integration of mechanisms and algorithms that could assist on the automated planning and operation of the network are essential.

The control and orchestration layer needs more intelligence and functionality to meet the ever-growing requirements in the support of B5G/6G services.

At the control plane level, models can be used to forecast traffic characteristics and resource usage parameters, providing the mechanisms for an accurate resource consumption prediction, while additionally enabling native security mechanisms through anomaly detection. The determination of future traffic demands is useful to implement a smart distributed scheduler capable of maximizing the resources available dynamically and provide a smart QoS (e.g. by means of automatic QoS reservation).

At the data plane level, a separate set of models can be used to dynamically classify, group, and forecast traffic characteristics, also determining the best forwarding strategy while dealing with abnormal information flows. The traffic can be classified into profiles, defined by real-time analysis of traffic samples, in a way that for each profile there will be a prediction for the expected data plane forwarding strategy. With this information, the devices at the edge are able to optimize routing, QoS, and other capabilities to better fit to the characteristics of the current traffic.

Traffic flow classification is an extremely hard classification problem [36]. First, the nature of the underlying model is complex. Second, the traffic may be encrypted limiting the number of features that can be effectively used. Finally, and related to the previous point, security and privacy issues.

In order to make the network control and orchestration layer become a smart connectivity platform, there is a need to add much more intelligence to it. Adhering to B5G/6G, in the sense of accommodating new applications that require lots of "ultra" (i.e., latency, reliability, capacity) and full dynamicity on all levels, achieving latency demands and reliability targets depends on using intelligent network-based decisions that leverage AI/ML techniques.

CUBIC objective is to leverage the potential of AutoML, transfer and federated learning as the cornerstones for the development of cognitive-based optimizations.

Automated Machine Learning (AutoML) is a paradigm shift in the usage of AI/ML models, instead of relying on a domain expert or a data scientist to carefully design a model, it relies on advanced search algorithms that combine multiple ML methods into a single model capable of providing a reasonable performance. The training model trades model performance for execution time, meaning that instead of finding the model with minimal error, it trains a model with minimal error within the time limit given for the training phase. This provides the means to control the time spent on the training phase of the models.

Transfer Learning (TL) is a machine learning method where a model developed for a task is reused as the starting point for another task. This allows the usage of pre-trained models as the starting point for complex tasks, easing the costs of training a model for such scenarios.

Federated Learning (FL) is a learning method that decentralizes the traditional learning process. In traditional ML, the data is aggregated into a single computer and the model is trained using the resources of that single computer. In FL the learning process is distributed through several edge devices.

The first paradigm helps to develop models with minimal input from domain experts and allows the fine control of the execution time. The last two paradigms are focused on data, model and train sharing through several nodes

Adding an additional intelligent layer to the orchestration while using AI/ML-based applications which optimize current decision making and identifies/predicts new verticals of constraints as input to the Path Computation Element (PCE) engine, allows us to reach the optimal and risk-less path which can accommodate application needs at a specific moment.

With the B5G/6G orchestration capabilities, PCE-like engines will address adaptive and dynamic traffic network engineering. The constraints are dynamically assigned and the PCE will work according to the policy constraints. More intelligence will be added to the orchestration layer from a network engineering perspective, end to end, (radio to core) by looking at the overall network rather than handling a specific node (specific node attention derived from a network-based decision). Dynamic switching can be performed over Flex Ethernet/optical links (e.g. as in the case where the FlexE is dynamically controlled and the optical layer is impairment aware and adaptive). The KPI's collection will be done by metering engines in the transport domain to support intelligent-based decisions and assurance. Finally, AI/ML engines will support routing decisions looking into network constraints (e.g. network status, operational aspects such as planned maintainability or business considerations such as changing cost of infrastructure).

4.2.6 Zero-trust softwarized ecosystem

Security in an ecosystem transitioning to 2030 networks is a multi-faceted problem as it involves virtualization, softwarization, heterogeneity of users, devices, and applications, as well as different administrative domains.

One frequently adopted paradigm is Security-as-a-Service (SECaaS). It provides end-to-end security by using virtual Network Security Functions (vNSFs) deployed on demand across distributed network

infrastructures. These are software-based security functions (e.g. virtual firewall, virtual IDS) that could be linked to each other through a set of virtual links to form a Service Function Chain (SFC), which represents a complete end-to-end security service. A complex challenge in this scenario is how to dynamically configure those services, starting from specific high-level requirements (i.e., end-user security policies). This challenge has been often addressed by using policy-based management, in particular mechanisms of policy refinement, analysis, and reconciliation. The ICT infrastructure itself needs protection. This is normally achieved by classical perimeter defense mechanisms (i.e., network firewalls, secure web gateways, VPNs). In addition, mechanisms to attest physical and virtual nodes are usually in place (i.e., remote attestation such as OpenCIT) protecting against malicious code injection or software manipulation.

Another recent security approach is the zero-trust security paradigm. This has not been completely integrated yet in the softwarized ecosystems, because it requires deep changes in the infrastructure design and management. Nevertheless, it could be crucial in B5G/6G technologies, where security requirements are even tougher and more sophisticated. Zero-trust security rejects the notion of a network perimeter. Once a user obtains access to resources in a traditional perimeter-based security architecture, he or she can move laterally and try to access and exploit any system or application within the network. The zero-trust paradigm does not allow these actions and follows a different approach based on the concept "trust nothing, verify everything". The access is granted on a "per-connection basis": the trust of who is trying to access a resource is evaluated before granting any kind of permission. Moreover, authentication to a specific resource does not automatically mean having access to the others.

Micro-segmentation is one key element to implement this paradigm. In modern infrastructures, services are deployed leveraging lightweight virtualization technologies (e.g. Docker, Containered, etc). Their elementary units are containers or pods. Micro-segmentation is an approach where at the container level most of the security access policies are enforced, so that the access to resources is fine-grained. Different technologies within the orchestration platform allow also the encryption of communication on a container basis (e.g. Istio [38]).

Another pivotal concept of zero-trust is continuous monitoring. Indeed, a monitoring system could be used to collect logs and metrics regarding the current status of the infrastructure. This data could be used also for other security mechanisms in place on the infrastructure (i.e., periodic remote attestation of the nodes).

From a cybersecurity perspective, new challenges and opportunities arise. These are related to the advent of quantum computers, the paradigm-shift from SaaS to Sensing-as-a-Service with the beginning of the IoT era, the new European Data Protection Regulation (GDPR), the introduction of Intent-Based-Networking (IBN), the requirement for interoperability among different administrative domains, and the introduction of cross-domain blockchain.

Quantum Cryptography (QC) is a challenge for security because it promises to break many widely adopted cryptographic algorithms, therefore new quantum-resistant cryptographic solutions must be developed and adopted. At the same time, QC is an opportunity because it enables new fast and efficient optimization algorithms (e.g. those based on quantum annealing) that could be used for the optimal allocation of network resources.

The large-scale adoption of IoT poses challenges because these components could be easily manipulated by attackers with logical or physical access. Hence, suitable security techniques must be adopted to ensure the trustworthiness of IoT-supplied data. For example, this can be based on ML to detect anomalies, or trusted-computing to verify the integrity of the nodes.

GDPR imposes strong protection of customer data, hence the need for security techniques that do not violate customer privacy. For example, avoid deep packet inspection in favor of user-independent data analytics (e.g. based L3/L4 features, excluded the network addresses that are considered personal information).

The integration of multiple administrative and security domains creates problems, for trust and secrecy (each domain would like to disclose the minimum amount of information about its internals to enable interoperability and interconnectivity) as well as for access control (e.g. user authentication for services or application authentication for a multi-domain blockchain). The usage of an intent-based approach for both networking and security can help to mitigate these problems, by expressing

high-level requirements and letting the various domains implement them with their own approach.

For end-to-end security, CUBIC proposes to extend the SECaaS paradigm to integrate the user intents in the deployment and configuration of vNSFs. In particular, user intents could lead to the automatic configuration of the security functionalities exploiting AI/ML mechanisms as well as reconciliation processes among different domains.

CUBIC adopts the zero-trust security model, exploiting AI/ML techniques to improve the detection of malicious actors and actions, even inside encrypted traffic. To enhance the robustness of the infrastructure, trusted computing will be used for "zero-trust continuous monitoring" to verify periodically the integrity of the nodes. The integrity reports could be stored in a distributed ledger to avoid manipulation from attackers and provide undeniable evidence.

5. CONCLUSIONS

Current networks are facing an important transformation with the purpose of supporting 5G services, embracing the generic idea of network sofwarization which implies the operational introduction of network virtualization, programmability and slicing. Forthcoming B5G and 6G services will introduce new and more stringent requirements that will motivate a new radical change, building on top of the technologies and capabilities available nowadays.

The key idea in such a transition is the one of smartness, pursuing an overall optimization on the usage of network and compute resources (from multiple stakeholders), with tailored connectivity to the specific needs of the customers, and leveraging AI/ML techniques for efficient control and management of the available assets, all in a secure environment.

This paper has presented CUBIC, a novel modular and scalable architecture which aims to facilitate such a transition in the time frame of 2030. In its inception CUBIC incorporates six main design directions: (i) the smooth integration of different low latency and high bandwidth data plane technologies; (ii) control capabilities to allow an adaptive end-to-end programmatic network; (iii) the intelligent utilization of different kinds of compute environments, even those of different ownership; (iv) smart orchestration of multiplicity of assets to satisfy very different service requirements; (v) smart connectivity platforms assisted by AI/ML techniques for analysis and prediction; and (vi) secured operation in a zero-trust softwarized ecosystem.

Such design approaches justify the advances of the architecture to the state of the art. In particular, AI/ML mechanisms provide the required management automation functions [39][40], the incorporation of ZSM facilitates the provision of end-to-end services that meet tenant QoS end QoE requirements, the exploitation of ENI [41] leverages available knowledge to resolve intelligence collection and processing, and the integration fabric (core component) provides the qualities to enable multi-vendor, multi-tenant, and multi-domain operations.

As future lines of work, several aspects require more analysis, definition and validation. This is the case of the combined local/global orchestration and the feasibility of the integration fabric (including the definition of APIs supporting its operation). This is expected to happen as part of joint innovation projects targeting the goal of 2030 and beyond networks.

REFERENCES

[1] Networld2020, "Smart Networks in the context of NGI", 2018.

[2] ITU-T FG Net2030, "Representative use cases and key network requirements Network 2030", Jan. 2020.

[3] K. Samdanis and T. Taleb, "The Road beyond 5G: A Vision and Insight of the Key Technologies," in IEEE Network, vol. 34, no. 2, pp. 135-141, March/April 2020, doi: 10.1109/MNET.001.1900228.

[4] V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen and K. Hätönen, "6G Architecture to Connect the Worlds," in IEEE Access, vol. 8, pp. 173508-173520, 2020, doi: 10.1109/ACCESS.2020.3025032.

[5] I. F. Akyildiz, A. Kak and S. Nie, "6G and Beyond: The Future of Wireless Communications Systems," in IEEE Access, vol. 8, pp. 133995-134030, 2020, doi: 10.1109/ACCESS.2020.3010896.

[6] A. Yazar, S.D. Tusha, H. Arslan, "6G vision: An ultra-flexible perspective", ITU Journal on Future and Evolving Technologies, Volume 1, Issue 1, Pages 121-140, December 2020.

[7] J. Ordonez-Lucena, P. Ameigeiras, L.M. Contreras, J. Folgueira, D.R. López, "On the Rollout of Network Slicing in Carrier Networks: a Technology Radar", *Sensors* 23: 8094, 2021.

[8] Samsung, "6G – The next hyper-connected experience for all", 2020.

[9] Ericsson, "6G – connecting acyber-physical world", February 2022.

[10] Nokia Bell-Labs, "Communications in the 6G era", 2020.

[11] NTT DOCOMO, "5G evolution and 6G", January 2020.

[12] KDDI, "Beyond 5G/6G", October 2021.

[13] G. Liu, Y. Huang, N. Li, J. Dong, J. Jin, Q. Wang, N. Li, "Vision, Requirements and Network Architecture of 6G Mobile Network beyond 2030", China Communications, pp. 92-104, September 2020.

[14] 5G Infrastructure Association, "European vision for the 6G network ecosystem", June 2021. Available at: https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf

[15] Beyond 5G Promotion Consortium, "Beyond 5G White Paper 〜Message to the 2030s〜", March 2022.

[16] NICT, "Beyond 5G/6G", August 2021.

[17] 5G Americas, "Mobile communications towards 2030", 2021.

[18] 6G Flagship University of Oulu, "White paper on 6G networking", June 2020.

[19] Telecom Infra Project, "Open Transport SDN Architecture", 2020. Available at: https://cdn.brandfolder.io/D8DI15S7/at/jh6nnbb6bjvn7w7t5jbgm5n/OpenTransportArchitecture-Whitepaper_TIP_Final.pdf

[20] 5G-PPP, "Cloud Native and 5G Verticals' services", February 2020. Available at: https://5g-ppp.eu/wp-content/uploads/2020/02/5G-PPP-SN-WG-5G-and-Cloud-Native.pdf

[21] 5G-PPP, "Edge Computing for 5G Networks", January 2021. Available at: https://bscw.5g-ppp.eu/pub/bscw.cgi/d397473/EdgeComputingFor5GNetworks.pdf

[22] P. Valsamas, L. Mamatas, L.M. Contreras, "A Comparative Evaluation of Edge Cloud Virtualization Technologies", *IEEE Transactions on Network and Service* Management, vol. 19, no. 2, pp. 1351-1365, June 2022.

[23] http://www.ieee802.org/1/pages/tsn.html

[24] O. Seijo, X. Iturbe and I. Val, "Tackling the Challenges of the Integration of Wired and Wireless TSN with a Technology Proof-of-Concept," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3131865.

[25] L. M. Contreras, Ó. González, V. López, J. P. Fernández-Palacios and J. Folgueira, "iFUSION: Standards-based SDN Architecture for Carrier Transport Network," 2019 IEEE Conference on Standards for Communications and Networking (CSCN), 2019, pp. 1-7, doi: 10.1109/CSCN.2019.8931386.

[26] B. Claise, J. Clarke, J. Lindblad, *Network Programmability with YANG: The Structure of Network Automation with YANG, NETCONF, RESTCONF, and GNMI*, Addison Wesley, 2019.

[27] p4.org

[28] D. Bhamare, et al., "Exploring Micro-Services for Enhancing Internet QoS", Transactions on Emerging Telecommunications Technologies, 2018

[29] "Docker", The Docker Containerization Platform, 2016 [Online]. Available: https://www.docker.com/

[30] https://linuxcontainers.org

[31] A. Madhavapeddy and D. J. Scott, "Unikernels: Rise of the virtual library operating system," Queue, vol. 11, no. 11, 2013

[32] http://cnp.neclab.eu/clickos/

[33] S. Shillaker, et al., "Faasm: Lightweight Isolation for Efficient Stateful Serverless Computing." arXiv preprint arXiv:2002.09344, 2020

[34] K. Letaief, et al., "The Roadmap to 6G: AI Empowered Wireless Networks", IEEE Communications Magazine. 57, 2019

[35] https://www.etsi.org/technologies/zero-touch-network-service-management

[36] F. Pacheco, et al. "Towards the deployment of machine learning solutions in network traffic classification: a systematic survey." IEEE Communications Surveys & Tutorials 21.2, 2018

[37] https://github.com/opencit/opencit

[38] https://istio.io/

[39] P. Martinez-Julia, V. P. Kafle and H. Harai, "Exploiting External Events for Resource Adaptation in Virtual Computer and Network Systems," in IEEE Transactions on Network and Service Management, vol. 15, no. 2, pp. 555-566, June 2018, doi: 10.1109/TNSM.2018.2794530.

[40] P. Martinez-Julia, V. P. Kafie and H. Asaeda, "Explained Intelligent Management Decisions in Virtual Networks and Network Slices," 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2020, pp. 221-227, doi: 10.1109/ICIN48450.2020.9059462.

[41] Experiential Networked Intelligence (ENI) https://www.etsi.org/technologies/experiential-networked-intelligence?highlight=YToxOntpOjA7czo2OiJzZWFyY2giO30%3D

AUTHORS

Luis M. Contreras holds an M.Sc. in telecommunications from the Universidad Politécnica de Madrid (1997), an M. Sc. in telematics jointly from the Universidad Carlos III de Madrid and the Universitat Politèctina de Catalunya (2010), and a Ph.D. *cum laude* in telematics from the Universidad Carlos III de Madrid (2021). In 1997 he joined Alcatel Spain taking several positions (R&D, standardization, product development and customer engineering) in both wireless and fixed network fields. In 2006 he joined the network planning department of Orange in Spain taking responsibilities for the IP backbone planning. Between 2002 and 2010 he was also adjunct lecturer at the Telematics department of the Universidad Carlos III. Since August 2011 he is part of Telefónica I+D / Telefónica Global CTO, working on scalable networks and their interaction with cloud and distributed services, and participating in several projects (lately 5G-Transformer, NECOS, 5G-EVE, 5GROWTH, or 5G-DIVE). He is an active contributor to different SDOs, such as IETF (author of 6 RFCs), O-RAN, ETSI, etc.

Javier Serrano graduated in sound and image engineering by Universidad Politécnica de Madrid (UPM) and did a research master's in signal, image, speech and telecommunications at Institut Polytechnique (INP) de Grenoble (France). He is working now at Grupo de Aplicación de Telecomunicaciones Visuales (GATV) of UPM on testing and validation of new UHD and immersive content delivery models in next-generation mobile networks. He is a Ph.D. candidate at UPM focusing on the intelligent optimization of virtualized services over new generation networks.

Lefteris Mamatas is an assistant professor in the Department of Applied Informatics, University of Macedonia, Greece. Before that, he was a researcher at University College London, Space Internetworking Center/ Democritus University of Thrace, and DoCoMo Eurolabs in Munich. His research interests lie in the

areas of software-defined networks, cloud computing and network function virtualization. He participated in many international research projects, such as NECOS (H2020), UNIC FED4FIRE+ Open Call (OC) 4, CORAL WiSHFUL OC2 project, MEC MONROE OC2 project, Dolfin (FP7) and UniverSELF (FP7). He has published more than 50 papers in international journals and conferences. He served as a general or TPC chair for the WWIC 2016 and 2012 conference, the INFOCOM SWFAN 2016 and 2017 workshops, and the E-DTN 2009 conference. He was a guest editor for the Elsevier Ad Hoc Networks Journal.

Giacomo Bernini received the Italian Laurea degree in telecommunication engineering from the University of Pisa, Italy, in 2006. Currently he is R&D Technical Coordinator at Nextworks, and his research interests include 6G, 5G network slicing and orchestration, and zero-touch network and service management. He participated in design, development and demonstration activities in several FP6, FP7 and H2020 projects, as well as industrial projects on WSON GMPLS, Multilayer PCE, and NFV technologies among others. He is currently a technical manager in the H2020 5GZORRO project, and contributing to the EDIDP DISCRETION, and H2020 LOCUS, INGENIOUS, HEXA-X projects. He is also very active in standardization, serving as a leader in various ETSI STFs in the area of NFV API conformance testing and OpenAPIs for NFV.

Paolo Monti is a professor and the head of the Optical Networks Unit at Chalmers University of Technology. He works on the design and operation of optical communication infrastructures focusing on energy efficiency, resiliency, programmability, automation, and techno-economics. He published more than 150 papers in international journals and conferences. Dr. Monti is serving on the editorial boards of the IEEE Communications Letters, the IEEE Networking Letters journals, and the IEEE Open Journal of the Communications Society. He also participates in the TPCs of the major IEEE and OSA conferences, including OFC, IEEE Globecom, and IEEE ICC. He has been the general chair of ONDM 2021, the ONS Symposium chair at the IEEE Globecom 2017, and the TPC chair of IEEE HPSR 2017, IEEE

OnlineGreenComm 2016, and ONDM 2014. Dr. Monti is a senior member of IEEE.

Mário Antunes received his computer and telematics engineering M.Sc. degree in 2011, with first-class honors, from the Electronics, Telecommunication and Informatics Department, University of Aveiro, Portugal. And concluded his doctoral program in computer science from MAPi in 2018, achieving the position of finalist in three international competitions: ERCIM Cor Baayen Young Researcher Award 2019, Altice International Innovation Award 2019 and "Melhor Tese de Doutoramento em STI - 2019". His main research areas focus on knowledge extraction and context storage in the Internet of Things (IoT) scenarios using machine learning techniques and big data repositories. His work includes developing efficient ways to deal with unstructured information, detection patterns and model time-series. These techniques are being implemented and evaluated in advanced machine-to-machine projects, such as APOLLO, SCOT and SGH. He is currently working as a researcher for the 5G-Contact project at IT-Aveiro.

Udayanto Dwi Atmojo received his PhD degree in electrical and electronic engineering from The University of Auckland, New Zealand in 2017, with a research topic on a software programming framework for IoT and distributed intelligent systems, demonstrated on robotic and industrial automation use case. He received the merit-based 'The University of Auckland Faculty of Engineering Doctoral Scholarship' for his PhD study. He is a recipient of the prestigious IEEE IES Student and Young Professionals Paper Assistance Award in 2016 to attend the IEEE 14th International Conference on Industrial Informatics in Poitiers, France. Right after the completion of his PhD, he started his postdoctoral research position at the School of Electrical Engineering at Aalto University until now. He also holds a formal role of "data agent", in the Research Data Management (RDM) support service at Aalto University who promotes good practice of open science and assists researchers on how to properly manage and handle their research data at Aalto University. His research area includes industrial informatics, factory automation, Industrial IoT, and embedded systems.

Eli Tocker is a program manager at ECI, in charge of all technical and project aspects of activities relating to IIA (Israel Innovation Authority) – Israeli Consortia and worldwide cooperation programs. Eli brings with him vast experience as a VP R&D (ECI, Foxcom and Gasngo), in system engineering and in project management. Eli holds a BSc in electrical engineering from the Technion and an MBA from Tel Aviv University.

Iñaki Val received B.Sc. and M.Sc. degrees from the Department of Electronics Engineering at the University of Mondragon (Spain) in 1998 and 2001, respectively, and a Ph.D. degree from the Department of Signals, Systems and Radiocommunication at Polytechnic University of Madrid (Spain) in 2011. Since 2001, he has been with the Communications Systems Group of IKERLAN, Mondragón (Spain), and in the past he has been with Fraunhofer IIS of Erlangen (Germany) as an invited researcher (2005–2006). Currently, he is the team leader of the Communication Systems group. His research activities include the design and implementation of digital wireless communications systems for industrial communications, and digital signal processing.

Andrea Sgambelluri is an assistant professor at the Scuola Superiore Sant'Anna of Pisa, Italy, since 2019. He published more than 110 papers (source Google Scholar, Mar 2022) in international journals and conference proceedings. In March 2015 he won the grand prize at 2015 OFC Corning Outstanding Student Paper Competition with the paper "First Demonstration of SDN-based Segment Routing in Multi-layer Networks". His main research interests are in the field of control plane techniques for both packet and optical networks, including Software-Defined Networking (SDN) protocol extensions, network reliability, industrial Ethernet, switching, segment routing application, YANG/NETCONF solutions for the dynamic management, telemetry, P4, (re)programming and monitoring of optical devices.

Jérôme Härri received an M.Sc. degree and a Dr. ès sc. (PhD) degree in telecommunication from the Swiss Institute of Technology (EPFL), Lausanne. He is currently a professor at the Communication Systems Department, where he leads the Connected Automated Transport System (CATS) team. Previously, he led the Traffic Telematics Junior Research Group at the Institute of Telematics of the Karlsruhe Institute of Technology (KIT), Germany. His research is related to Internet of Things (IoT) and connected transportation, including wireless vehicular communication and networking, transportation modeling, positioning and localization, or control system optimization. Jérôme has authored and coauthored over 100 international journal and conference papers and is involved in various national and European research projects related to connected and automated mobility.

Antonio Lioy, Ph.D, is a full professor of computer engineering at POLITO and leads the TORSEC research group, which has been working in the field of computer and network security since 1994. His research interests are on trusted computing, PKI, electronic identity, network and application security, big data analytics, and policy-based and ontology-based design of the protection for large information systems. Prof. Lioy served as a member of the ENISA PSG (Permanent Stakeholder Group), is regularly an evaluator and reviewer for the EC, and has published more than 100 scientific papers, mostly related to the cybersecurity area.

Pedro Martinez-Julia is a full-time researcher at the National Institute of Information and Communications Technology, Japan. He received a B.S. in computer science from the Open University of Catalonia, an M.S. in advanced information technology and telematics and a Ph.D. in computer science from the University of Murcia, Spain. He has been involved in EU-funded research projects since 2009, leading several tasks/activities, and participating in IETF/IRTF for

the standardization of new network technologies. He has published over twenty papers in refereed conferences and journals. His main expertise is in network architecture, control and management, with particular interest in overlay networks and distributed systems and services. He is a member of ACM and IEEE.

Jose Gonzalez is the CEO at AUSTRALO. He graduated with honors as a telecommunications engineer from the Technical University of Madrid, where he worked as a project manager and launched two business ideas; in 2020 he founded AUSTRALO with the ambition to bridge the divide between technology, research and the market.

Jorge Sánchez Garrido received his B.Sc. in telecommunications engineering in 2013 and his master's degree in data science and computer architecture in 2016, both from the University of Granada (Spain). He previously worked as a consultant at Deloitte Spain in Madrid (2014-2015), and then started a Ph.D. programme in time-sensitive networking at the University of Granada (2015-2021) with interests in White Rabbit timing, deterministic networks, smart grid, and FPGA-based systems design. He has been an active researcher in several transfer projects into the industry and currently holds an R&D engineering position with Orolia Spain.

Hitoshi Asaeda is a director of Network Architecture Laboratory, National Institute of Information and Communications Technology (NICT). He received a Ph.D. degree from Keio University. He was previously with IBM Japan, Ltd., a research engineer specialist at Inria, and a project associate professor at Keio University. He was a chair of IEICE Technical Committee on ICN from 2017 to 2019. He was a general co-chair of IEEE/ACM IWQoS 2021 and ACM ICN 2022. His research interests include information-centric networking, high-quality streaming, and distributed computing networks. He has been actively working in the IETF standards body. He received the IEICE Communications Society Outstanding Contributions Award in 2019. He is a senior member of IEEE and IEICE, and a member of ACM.