applied sciences

MDPI

Article

Results and Achievements of the ALLIANCE Project: New Network Solutions for 5G and Beyond

Davide Careglio [1,*,†], Salvatore Spadaro [2,†], Albert Cabellos [1,†], Jose Antonio Lazaro [2,†], Pere Barlet-Ros [1,†], Joan Manel Gené [2,†], Jordi Perelló [1,†], Fernando Agraz Bujan [2,†], José Suárez-Varela [1,†], Albert Pàges [2,†], Jordi Paillissé [1,†], Paul Almasan [1,†], Jordi Domingo-Pascual [1,†] and Josep Solé-Pareta [1,†]

[1] Department Computer Architecture, Universitat Politecnica de Catalunya, 08034 Barcelona, Spain; albert.cabellos@upc.edu (A.C.); pere.barlet@upc.edu (P.B.-R.); jordi.perello@upc.edu (J.P.); jose.suarez-varela@upc.edu (J.S.-V.); jordi.paillisse@upc.edu (J.P.); felician.paul.almasan@upc.edu (P.A.); jordi.domingo@upc.edu (J.D.-P.); josep.sole@upc.edu (J.S.-P.)

[2] Department Signal Theory and Communications, Universitat Politecnica de Catalunya, 08034 Barcelona, Spain; salvatore.spadaro@upc.edu (S.S.); jose.antonio.lazaro@upc.edu (J.A.L.); joan.gene@upc.edu (J.M.G.); fernando.agraz@upc.edu (F.A.B.); albert.pages-cruz@upc.edu (A.P.)

* Correspondence: davide.careglio@upc.edu; Tel.: +34-93-401-6985

† These authors contributed equally to this work.

Abstract: Leaving the current 4th generation of mobile communications behind, 5G will represent a disruptive paradigm shift integrating 5G Radio Access Networks (RANs), ultra-high-capacity access/metro/core optical networks, and intra-datacentre (DC) network and computational resources into a single converged 5G network infrastructure. The present paper overviews the main achievements obtained in the ALLIANCE project. This project ambitiously aims at architecting a converged 5G-enabled network infrastructure satisfying those needs to effectively realise the envisioned upcoming Digital Society. In particular, we present two networking solutions for 5G and beyond 5G (B5G), such as Software Defined Networking/Network Function Virtualisation (SDN/NFV) on top of an ultra-high-capacity spatially and spectrally flexible all-optical network infrastructure, and the clean-slate Recursive Inter-Network Architecture (RINA) over packet networks, including access, metro, core and DC segments. The common umbrella of all these solutions is the Knowledge-Defined Networking (KDN)-based orchestration layer which, by implementing Artificial Intelligence (AI) techniques, enables an optimal end-to-end service provisioning. Finally, the cross-layer manager of the ALLIANCE architecture includes two novel elements, namely the monitoring element providing network and user data in real time to the KDN, and the blockchain-based trust element in charge of exchanging reliable and confident information with external domains.

Keywords: SDN/NFV; RINA; KDN; monitoring; blockchain

Citation: Careglio, D.; Spadaro, S.; Cabellos, A.; Lazaro, J.A.; Barlet-Ros, P.; Gené, J.M.; Perelló, J.; Agraz Bujan, F.; Suárez-Varela, J.; Pàges, A.; et al. Results and Achievements of the ALLIANCE Project: New Network Solutions for 5G and Beyond. *Appl. Sci.* **2021**, *11*, 9130. https://doi.org/10.3390/app11199130

Academic Editor: Carla Raffaelli

Received: 16 August 2021
Accepted: 27 September 2021
Published: 30 September 2021

1. Introduction

In recent years, the 5G paradigm has been gaining momentum with many global research and development (R&D) initiatives launched in major economies worldwide. Referring in particular to Europe, 5G has been recognised as the key enabler for the digitisation of the European economy [1]. Although the current and future 5G applications are countless, many of them share one thing in common. To provide a good user experience is no longer enough to provide high bandwidth alone but there is a strong requirement to increase other eight technical parameters [2], ranging from area traffic capacity (an increase of 100× per squared-km) to network energy efficiency (100× more efficient). As the commercial rollout of 5G continues in many countries around the world, now is the ideal moment to identify attractive subjects and research lines for the next decade, which will set the groundwork for B5G system.

Network infrastructure in this 5G/B5G era needs to go well beyond the evolution of today's transport networks and must be properly designed to support end-to-end sophisti-

cated vertical applications as envisaged by the 5G Infrastructure Public–Private Partnership (5G PPP) initiative [3]. In particular, 5G/B5G promises to focus on three outstanding features not seriously considered in the previous generations, namely large-scale machine type communication, ultra-reliable low-latency service and enhanced mobile broadband. In summary, 5G/B5G must deliver not only a better performing network, but also one that can become an infrastructure capable of supporting ubiquitous services, while at the same time meeting the performance and commercial requirements of multiple stakeholders.

The research community is therefore pursuing new models to alleviate the scalability issue of the current client-server architecture while meeting the strict requirements imposed by 5G/B5G. For instance, solutions such as edge computing, fog computing, cloudlets, server mesh, etc., are currently gaining momentum to this end, with SDN/NFV providing the framework to effectively control and manage the distribution of functions across network levels. Nonetheless, these developments considerably increase the complexity in networking as well as in networked applications, fueling therefore the need for improved network automation. AI approaches—in particular those based on Machine Learning (ML) techniques—are today considered the key drivers to keep network operations simpler, smarter, safer, and speedier.

In this direction, in 2018 we started a 45-month Spanish project called Architecting a knowledge-defined 5G/B5G-enabled network infrastructure toward the upcoming digital society (ALLIANCE) where several researchers with different backgrounds and skills (e.g., physical layer experts, ML experts, protocol designers, data science specialists, etc.) have collaborated with the aim of investigating novel network solutions for 5G/B5G. Now that the ALLIANCE project is approaching its end, in this paper we present an overview of our research activities. Section 2 is hence focused on presenting the ALLIANCE network architecture and its principal building components as well as summarising the main results and achievements compared with the state of the art. Each one of these components has been selected and included in the ALLIANCE architecture for specific reasons explained below.

One of the ambitious goals of the ALLIANCE proposal has been the design and development of the KDN framework, implementing AI/ML techniques. Section 3 is hence dedicated to describing this KDN framework, present our practical ML-based solution for the routing problem and demonstrate its ability of supporting optimal end-to-end service provisioning. In Section 4, we introduce the novel network-monitoring element designed in ALLIANCE based on a combination of Deep Packet Inspection (DPI) and ML. This element is in charge of providing accurate and relevant information from the networks and the users to the KDN to make proper dynamic decisions based on the current and future status of the network. In our KDN framework, decisions are taken according to the data coming from users and networks and, with the current proliferation of untrusted and malicious sources, it is of great importance having an efficient distributed system able to provide the necessary confidence to these data. For this very reason, we have proposed (Section 5) a new solution to distribute, control and authenticate routing information between different administrative domains using blockchains as an alternative to conventional Resource Public Key Infrastructure (RPKI).

Finally, under the umbrella of KDN, we have investigated the appropriateness of two networking solutions for 5G/B5G: one focused on the well-established SDN/NFV technology and the other adopting an outside the box technology called RINA. The research activities in the SDN/NFV domain is presented in Section 6. For this domain, we have considered an overall architecture (i.e., both the control and the optical layers) where an IA-based orchestrator is in charge of controlling and managing an ultra-high-capacity spatially and spectrally flexible all-optical network infrastructure. On the contrary, we have only considered the packet layer for the RINA domain as this solution is still in development and limited technologies is currently supported. In Section 7 we describe our experiments and findings about its capability of offering digital services with isolated network slices and guaranteed Quality of Service (QoS). In addition to describing the main

conclusions of the ALLIANCE project, in Section 8 we highlight the key lessons learned with a vision towards the future 6G.

2. Network Architecture and Project's Main Achievements

2.1. ALLIANCE Network Architecture

Figure 1 shows an overview of the general ALLIANCE network architecture. It consists of different main blocks. On the top side, there is the **KDN-based orchestration layer** which is empowered with ML techniques (e.g., deep-learning tools) to increase the efficiency of the management of the overall resources. On the right-hand side, the cross-layer manager considered in ALLIANCE consists of two elements: the **monitoring element** in charge of collecting users, networks and Information Technology (IT) resources data and the **trust element** in charge of assuring confidence and reliability to external information. On the bottom side, the network infrastructure can consist of any levels including access, metro, core and DC network segments. We have considered two different network solutions to control this network infrastructure and provide end-to-end services. An **SDN/NFV**-enabled control layer has been developed to deliver network slices customised to the requirements of the vertical services and applications. This solution focuses on an ultra-low-latency, ultra-high-capacity optical infrastructure where both the packet and the optical layers are considered. Studies have been carried out to improve both the physical layer with investigations on novel modulation formats and the control layer to be able to take autonomous and automatic decisions to keep the best possible network performance. As an alternative solution for legacy protocols, we have also investigated the **RINA** network architecture. RINA is a clean-slate recursive multi-layer architecture based on a single type of layer and two programmable protocols. For this solution, we only focused on the multi-layer packet network for access and metro segments.

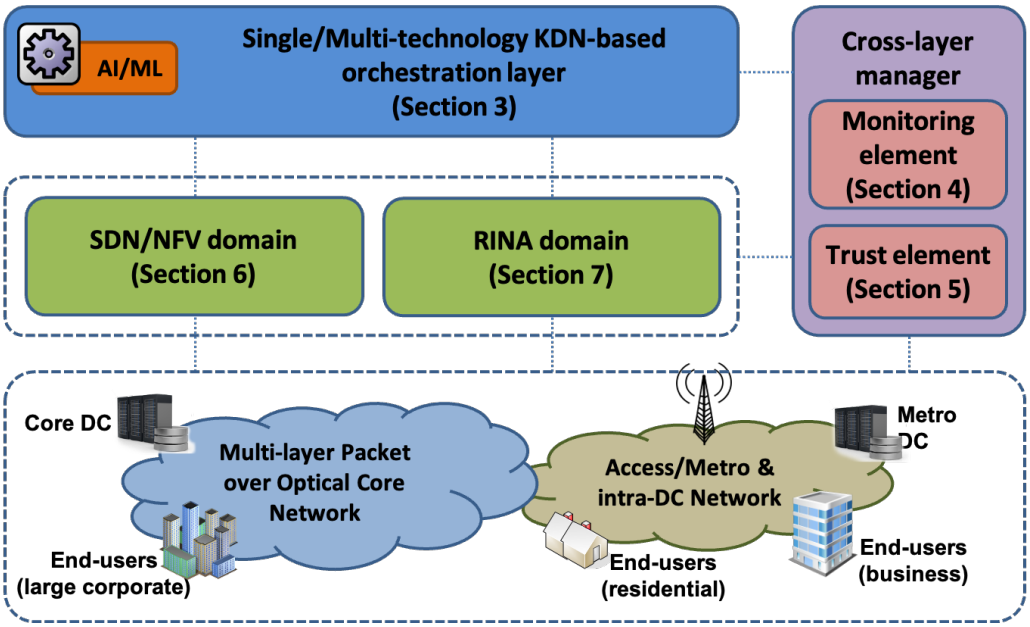


Figure 1. The ALLIANCE network architecture.

We would like to point out that the final intention of this project was not to fully integrate all previous introduced blocks in one single platform. On the contrary, our idea was to investigate several network solutions addressing different problems and converge and combine some of them when practical and convenient. Therefore, the experiment setups and the main results presented throughout this paper are mostly related to a single or a couple of components of the ALLIANCE reference architecture. For example, the monitoring element fed the KDN framework with processed data containing a rich and timely view of the network states. If the data come from external entities, the trust

element can guarantee integrity and reliability before entering the monitoring element and, in turn, the KDN. The approaches developed in this project to take optimal, automatic and autonomous decisions regarding the network resources, consider the ML algorithms investigated in the KDN framework.

2.2. Achievements

We summarise the main results and achievements of the project below. More details are then further provided in the following sections dedicated to each of the main components of the ALLIANCE network architecture.

2.2.1. The KDN Framework

We have proposed and evaluated a novel method that combines Deep Reinforcement Learning (DRL) and Graph Neural Networks (GNN) to optimise the routing configuration in a KDN-based network scenario. The evaluation shows that the proposed DRL + GNN optimisation architecture outperforms state-of-the-art DRL agents (based on fully connected neural networks) when it is applied over different networks unseen during the training phase. This reveals an unprecedented ability of the proposed DRL + GNN agent to generalise over networks, which is a fundamental feature to achieve practical ML-based solutions for networking. We also extend the evaluation of our DRL + GNN agent to 136 real-world topologies of Internet Topology Zoo, again showing good generalisation capabilities over networks and achieving an important improvement over the application of a classic load-balancing routing policy (21.39% better performance on average).

2.2.2. Monitoring Element

We have carried out the design of functional and efficient solutions to collect, process, and maintain a rich and timely view of the network state in KDN-based environments. We started from the optic of the SDN paradigm, which offers data-plane devices with enhanced computing and storage capabilities, and a flexible Southbound Application Programming Interface (API)—OpenFlow, in our case– to retrieve statistics from the data-plane (e.g., traffic measurements). As a result, a novel OpenFlow-based flow-level traffic measurement system with good scalability properties has been proposed. Moreover, we have presented a system that combines DPI and ML to efficiently classify the applications generating traffic in the network. The resulting system has been carefully designed to achieve a good tradeoff between accuracy (both in traffic measurements and application classification), and the cost to deploy and execute it in networks.

2.2.3. Trust Element

We have investigated how to transfer routing information between different administrative domains, such as different operators. Taking into account that they do not necessarily trust each other, we have analysed the advantages and disadvantages of blockchains as an alternative to classical RPKI to distribute, control and authenticate this information. We have built and evaluated two prototypes, one that acts as a distributed mapping system, and another to perform access control.

2.2.4. The SDN/NFV Domain

SDN/NFV is one of the technology domains investigated in ALLIANCE. For this domain, we have proposed an overall solution where an SDN/NFV orchestrator controls an ultra-high-capacity spatially and spectrally flexible all-optical network infrastructure. In particular, three main achievements can be highlighted:

1. The Non-Orthogonal Multiple Access (NOMA) modulation with multiband Carrierless Amplitude and Phase (NOMA-CAP) modulation format has been experimentally validated for the Passive Optical Network (PON) infrastructure using Radio-over-Fibre (RoF) technology and for split-enabled optical interconnects.

2. To enabling an efficient Spatial Division Multiplexing (SDM), MultiCore Fibre (MCF)-based optical infrastructure have been deeply analysed with special emphasis on the optimal crosstalk level that optimises the aggregated capacity of MCFs.
3. Finally, we have designed and experimentally validated an AI-empowered control/management and orchestration framework allowing the automatic and autonomous deliver of network slices customised to the requirements of the vertical services and applications.

2.2.5. The RINA Domain

We have successfully deployed RINA (the other technology domain) in an emulated network scenario consisting of a service provider network on top of an infrastructure provider network. The overall scenario included 10 nodes spanning from end-users to DC servers. We accomplished the following two tests:

1. The evaluation of the RINA QoS support by injecting synthetic traffic flows reproducing diverse network applications and load conditions and measuring the perceived QoS metrics. This test proved the ability of RINA to effectively deliver packets with the required QoS between distributed applications in a multi-layer packet network.
2. The demonstration of a real High Definition (HD) video streaming in highly congested network scenarios, with perfect users' Quality of Experience (QoE).

2.3. Review of Similar Projects

Recent advancements in AI have led to a new era of ML techniques. In particular, ML applied to networks is today an established focus on the research community and generates high expectations. Several projects started in the past few years promoting the deployment of AI/ML in the network with the focus on minimising manual intervention, maximising the network use and QoS/QoE, reducing the energy footprint, facilitating the data processing, signal processing, and the integration between different network segments, etc. Among all initiatives, we consider that the following three projects present most similarities with ALLIANCE.

DAEMON (Network intelligence for aDAptive and sElf-Learning MObile Networks, https://h2020daemon.eu, accessed on 20 September 2021) is a European-funded project started in 2021. Its main argument is that AI is not the best solution for every network task but only for those hard problems requiring inferring complex relationships from massive data. Therefore, its goal is to provide a solid set of guidelines for the use of ML and design tailored AI models that respond only to the specific needs of given network functions.

AI@EDGE (A Secure and Reusable Artificial Intelligence Platform for Edge Computing in Beyond 5G Networks, https://aiatedge.eu, accessed on 20 September 2021) is another example of European project started in 2021 focused on AI/ML for 5G/B5G. This project aims at building a platform and tools enabling the concept of reusable, secure, and trustworthy AI for network automation in large-scale edge and cloud compute infrastructures. In addition, it targets a solution for a converged connect-compute platform for creating and managing resilient, elastic, and secure end-to-end slices capable of supporting a diverse range of AI-enabled network applications.

5GZORRO (Zero-tOuch secuRity and tRust for ubiquitous cOmputing and connectivity in 5G networks, https://www.5gzorro.eu, accessed on 20 September 2021) is a project started in 2019, few months after ALLIANCE. The main goal of 5GZORRO is to transform network orchestration and management into a cognitive process through which the network can self-adapt and self-react to changing conditions with minimal manual intervention. In addition, blockchain is proposed for implementing distributed security and trust across the various parties involved in the 5G service chain.

All projects leverage on cutting-edge technologies such as SDN/NFV, edge/fog computing, enhanced mobile broadband networks, etc. Being European projects, they are clearly larger than ALLIANCE, their goals include many more aspects and objectives, and in the end each one wants to deliver and demonstrate a complete global solution. On the

contrary, in ALLIANCE we have focused on proposing solutions that point to significant advances in different fields, which are mostly not addressed in the other projects. For example, we have pioneered the first application of GNN (in combination with DRL) to computer networks, allowing us to predict accurate performance metrics per flow for known networks and produce accurate estimates for unknown networks. We have demonstrated the potentiality of RINA as a viable solution for B5G, with its inherent ability to support security, programmability, virtualisation and mobility by design. The focus of most of the similar projects is on the mobile network; in ALLIANCE we have investigated new modulation formats and new design tools for both the access and the transport segments of a high-capacity and ultra-low-latency optical infrastructure. These are just three examples to differentiate ALLIANCE from similar projects; other novel achievements are reported throughout the document.

3. The KDN Framework

3.1. Background on KDN

In the last decade, the networking community has witnessed the so-called "softwarisation" process. As a result, networks are shifting towards increasingly programmable control planes. At the same time, a series of breakthroughs during the last decade in the ML field have marked the start of a new era of AI [4].

In this context, KDN [5] emerges with the goal of facilitating the deployment of AI/ML techniques for network orchestration. To this end, KDN restates the concept of a knowledge plane for networks, earlier proposed in [6]. As initially proposed, the knowledge plane was a construct combining AI tools and cognitive systems to control and operate the network efficiently (e.g., via network orchestration). In this construct, the use of AI-based solutions was expected to achieve better-than-human network operation timescales and optimise the resource use in complex network environments beyond existing solutions (e.g., heuristics, analytical models).

However, despite the much interest raised by the knowledge plane among the networking community, no prototype of this construct was built for real network deployments, mainly due to important technical limitations. According to the authors of KDN, one of the main limitations to deploy AI/ML techniques in legacy networks is that they are intrinsically distributed. Network devices have only a partial view of the network state, and their actions have an impact only on a small portion of the network—typically on their neighborhood. One example of this is routing in legacy networks, where forwarding devices are limited to select the next hop based on their local state.

In this vein, KDN highlights the rise of two key technologies that may act as a catalyst to construct a functional and efficient AI-enabled knowledge plane: (i) the SDN paradigm, and (ii) modern network analytics techniques. First, in SDN the control plane permits the gathering of knowledge about the network state in a logically centralised entity. This may bring many advantages for modern ML-based network orchestration solutions, which can leverage the global state information to make decisions over the network as a whole. Second, data-plane devices in SDN offer improved computing and storage capabilities with respect to traditional networking equipment [7,8]. This paves the way to develop a new breed of monitoring techniques—also known as telemetry [9]—that enable the maintenance of measurements in data-plane devices and collect timely information about the network state in a centralised platform. At this point, network analytics becomes an essential pillar to collect, structure, process, and maintain efficiently the network state information, which in real-world networks typically turns into Big Data.

As a result, KDN proposes to leverage recent advances in the AI field—and specifically in ML [10,11]—to construct a knowledge-based layer for efficient network orchestration in SDN-based networks. The resulting AI-empowered knowledge plane can be beneficial to efficiently implement emerging networking trends based on complex high-level operational goals, such as Intent-Driven Networking [12], or Beyond-Shannon Semantic

communications [13]. Since it was conceived, KDN has served as a reference for a large body of literature aiming to deploy AI/ML techniques for network automation [14–16].

3.2. Research Activity

Recent advances in ML have attracted a lot of interest from the networking community, which has recently started to investigate how to build cost-efficient ML-based solutions to address network-related problems, such as routing optimisation, performance prediction, or traffic classification [10,11]. Additionally, DL models in combination with optimisation strategies, such as reinforcement learning algorithms, have opened the possibility to efficiently solve complex decision-making and automated control problems [17–19].

In the ALLIANCE project, we have investigated how to effectively apply modern DRL methods to optimise the routing configuration in networks. In this context, previous DRL-based attempts for routing optimisation have failed to achieve good results, often under-performing traditional heuristics. In contrast to previous DRL-based solutions, in ALLIANCE we first proposed to use a more elaborate network representation that facilitates DRL agents to learn efficient routing strategies in optical networks [20], while also demonstrated the possibility to apply this network representation to other optimisation problems, such as QoS-aware routing optimisation in IP networks [21].

Second, we have proposed the use of GNNs [22] as effective tools for network modelling and optimisation (e.g., network orchestration). GNN is a recently proposed family of neural networks specifically intended to learn and generalise over graph-structured information. These models are focused on learning the relationships between different inter-connected elements in graphs, by exploiting the structure of the graph itself. As a result, they show good generalisation properties when applied to different graphs not seen during the training phase—i.e., they show strong relational inductive bias over graphs [23]. We refer the reader to [22–24] for more generic background on GNN. Earlier attempts to apply Deep Learning for network optimisation propose the use of well-known neural network models (e.g., fully connected, convolutional, recurrent neural networks, auto-encoders), which have been popularised for their outstanding applications in other fields (e.g., computer vision, natural language processing). However, these types of neural networks are not suitable for understanding and extracting deep knowledge from graph-structured data and, as a result, they show poor generalisation capabilities when applied to different network scenarios than those seen during the training phase (e.g., other topologies, routing configurations, traffic) [25]. In this context, we argue that many fundamental components in network optimisation problems involve data that is fundamentally represented as graphs (e.g., topology, routing, inter-flow dependencies) [26]. This makes GNN an especially well-suited neural network family for learning and reasoning about this network-related information. In the networking context, GNNs can be especially beneficial for global optimisation tasks, which often involve global graph-structured network state information and complex high-level optimisation goals (e.g., minimise end-to-end latency, maximise bandwidth). In general, these networking problems typically involve different network elements (e.g., routers, links, users, traffic flows) with associated state information and complex relationships between them that must be modelled and exploited to effectively pursue the global optimisation goal.

In the ALLIANCE project, we have proposed RouteNet [27], a custom GNN-based architecture for network performance evaluation. This GNN model has as input: a network topology, a routing configuration, and a src-dst traffic matrix; and it produces as output accurate predictions of flow-level QoS metrics (e.g., delay, jitter, loss). A main advantage of this GNN model with respect to other traditional network modelling solutions (e.g., queuing theory, packet-level simulators) is that it can produce very accurate performance estimates at limited cost. This can be particularly interesting for online optimisation tasks, where the GNN model can be combined with an optimisation algorithm (e.g., reinforcement learning, heuristics) to evaluate the performance of different candidate configurations, and eventually find a configuration that meets the target optimisation

goals [26]. In this context, we have applied RouteNet for automatic routing optimisation in several QoS-aware optimisation use cases (e.g., minimise end-to-end delay, jitter). Our experimental results show that unlike previous ML-based proposals, this GNN model can operate successfully in network scenarios with different topologies, routing configurations, and traffic never seen during the training phase [28]. Likewise, we have recently pioneered the first network optimisation architecture that combines DRL and GNN for routing optimisation [25], and have applied it to a classic routing optimisation problem in optical networks, as well as to traffic engineering in IP networks [29]. The following subsection features some remarkable results obtained in [25], which leverages our novel DRL + GNN agent to optimise the routing configuration in a KDN/SDN-based optical network scenario, as the one previously introduced in Figure 1.

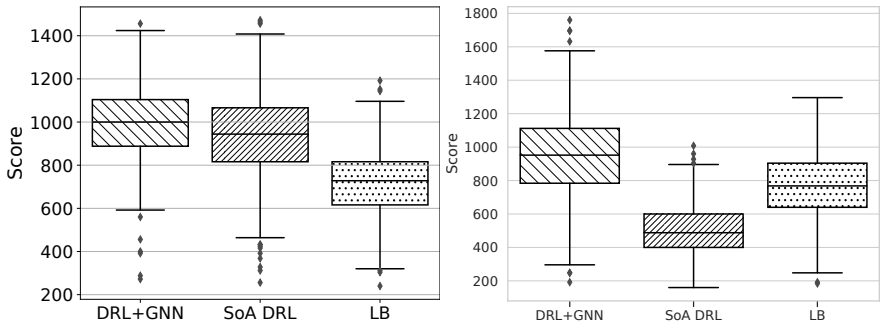
3.3. Evaluation of a DRL + GNN Agent for Routing Optimisation in Optical Networks

A main limitation of existing DRL-based solutions for networks is that they are not able to generalise properly across different network scenarios (e.g., different topologies, configurations) than those seen during the training phase. This limits their applicability to commercial products, so that DRL agents can be trained in controlled testbeds and then be deployed in any real-world network, regardless of its topology. The reason behind this limitation is that existing DRL solutions for networking use standard neural networks (e.g., fully connected, convolutional) that are not suited to learn data from computer networks, whose information is intrinsically structured as graphs [26].

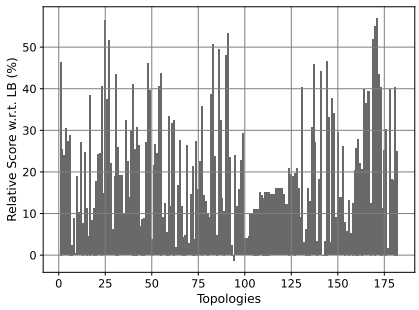
In virtue of the generalisation capabilities of GNNs to model network-related information (structured as graphs), we argue that the integration of such models into DRL agents may enable the building of more efficient solutions for network optimisation. In particular, the use of GNN could help the DRL agent generalise better to different scenarios from those observed during the training phase, which is an essential learning aspect to achieve functional solutions for networking. In this vein, the GNN model can help the agent acquire deeper knowledge about networks, by learning how the state of different network elements (e.g., forwarding devices, flows) relate to a particular target optimisation goal (e.g., maximise congestion). As a result, in the ALLIANCE project we have proposed a novel architecture that integrates a GNN model into a DRL algorithm [25]. We show that the resulting DRL + GNN agent can learn the complex relationships between the different elements of the network, reason about these relationships, and optimise the routing configuration over an Optical Transport Network scenario. In particular, we consider a KDN/SDN-based scenario, where a centralised controller receives information of new traffic demands to be routed *{source, destination, estimated bandwidth}*, and our DRL + GNN agent—running in the controller— selects the best src-dst path for each demand, with the ultimate goal of maximising the amount of traffic volume served by the network, which is a classic Traffic Engineering goal.

The proposed DRL + GNN agent implements Deep Q-Network (DQN) [19] as a reinforcement learning algorithm, and a custom GNN model (coded in TensorFlow) that incorporates state information from links (use) and their relations according to the network topology and the traffic demands routed through the network. In our experiments, we generate different network optimisation episodes, which are defined by: a network topology, and a sequence of src-dst traffic demands randomly generated that the DRL agent must incrementally allocate on particular sequences of lightpaths (i.e., end-to-end paths). We train the DRL agent for 1000 episodes, where each episode ends when the agent allocates a demand to a path (i.e., sequence of lightpaths) that does not have enough available capacity. The immediate reward is the traffic volume of the current traffic demand if it was successfully allocated by the agent, and zero otherwise. Thus, the agent is intended to maximise in the long-term the amount of traffic volume successfully routed. Please note that since the generation of traffic demands is random, the agent cannot exploit any meaningful information to predict the traffic demands that will come in the future, which makes this problem more challenging.

Figure 2a,b show a comparison of the proposed DRL + GNN agent [25] against a state-of-the-art DRL solution using fully connected neural networks (SoA DRL) [30], also presented as an earlier work within the ALLIANCE project. In Figure 2a, we can observe that when both DRL-based solutions are trained and evaluated in the same network topology (NSFNet; 14 nodes), they achieve a similar score (i.e., amount of src-dst traffic volume successfully routed through the network). In particular, the bloxplots show the performance achieved across 1000 evaluations with different src-dst traffic demand sets randomly generated. As a reference, we also show the performance achieved by a traditional Load-Balancing policy (LB). Thus, we can also observe that LB achieves ≈30% less performance than our DRL + GNN agent if we compare the median values obtained across all evaluations. Likewise, Figure 2b shows the results when the DRL agents are trained in a network (NSFNet; 14 nodes) and then tested in another network unseen during the training phase (Geant2; 24 nodes). In this case, we can observe that the state-of-the-art DRL agent (using a fully connected NN) considerably degrades its performance, falling behind a traditional LB policy. This is due to its lack of generalisation capability over different networks. In contrast, the proposed DRL + GNN agent achieves a good performance level in this new network unseen during training, which reveals the capability of this solution to flexibly adapt to new network scenarios, by exploiting the information of networks structured as graphs. To further evaluate the DRL + GNN agent in other networks, we apply it over a set with 136 real-world topologies from the well-known Internet Topology Zoo repository [31]. The plot of Figure 2c shows the improvement (%) over a LB routing policy across all these networks (x-axis), which were not seen by the DRL agent during the training phase. Overall, we can observe an average improvement of 21.39% in performance compared to the traditional LB baseline, again reflecting the outstanding capability of the DRL + GNN agent to generalise to other networks. We refer the reader to [25] for a more extensive evaluation of this work.



(**a**) (**b**)



(**c**)

Figure 2. Evaluation of our DRL + GNN agent for routing optimisation in optical transport networks: (**a**) Training/Evaluation in the same topology (NSFNet); (**b**) Training/Evaluation in different topologies (trained in NSFNet; evaluated in Geant2); (**c**) Evaluation of our DRL + GNN agent over 136 topologies from Internet Topology Zoo unseen during the training phase.

4. Monitoring Element

4.1. Introduction

Presently, network monitoring encompasses a combination of efficient network measurement techniques and Big Data processing methods that, in SDN, are intended to provide a rich view of the network state to the centralised control plane. This eventually enables the automation and improvement of network control and management tasks, such as adapting the network configuration (as the use case previously presented in Section 3.3), predicting traffic and application trends, or preventing potential problems (e.g., performance degradation, security breaches).

The huge scale and diversity of presently' networks makes it difficult to measure and maintain accurate and timely statistics of the network state. In this context, the SDN paradigm offers the advantage of a data-plane populated by devices with enhanced computing and storage capabilities, as well as a centralised control plane that permits the collection of all the state information maintained in data-plane devices. For instance, OpenFlow [7] offers support to maintain flow-level traffic measurements in forwarding devices (e.g., traffic volume, flow duration) and provides an API to report this information to SDN controllers.

However, despite SDN solves some classic problems of network measurement in distributed environments, it brings new challenges to address. The decoupling of the control and data planes adds new implications that need to be identified and considered for the design of efficient network analytics solutions. For example, this separation introduces a latency in the communication between the control and data planes (i.e., between SDN controllers and forwarding devices). Thus, this latency is not only affected by the delay of the connection itself, but also by other factors such as the current workload of the devices and their availability. Likewise, the fact that SDN controllers are centralised entities that typically manage many forwarding devices, makes them prone to become bottlenecks. This adds the need to avoid possible scalability issues by carefully selecting the tasks that are processed in controllers and those that may be devolved to data-plane devices.

In addition, the use of modern ML and Big Data processing techniques enables the provision of a deep insight about all the information collected from the network. In this vein, one application that may be particularly beneficial for network operation is to classify the traffic by applications. This can be done using supervised ML methods, such as decision trees, Support Vector Machines, or Deep Neural Networks, which can be trained with labeled data to then classify the applications from a limited set of network measurements. For instance, some works leverage basic flow-level traffic measurements (e.g., traffic volume) to discover —with ML—the applications in the network [32,33].

4.2. Research Activity

In the ALLIANCE project, we have investigated the design of efficient traffic measurement tools in the context of KDN. Network monitoring becomes a more and more complex task considering that the state information collected from the data-plane involves an ever-increasing massive amount of data (i.e., Big Data) in real network deployments. We have analyzed the main aspects to consider when measuring and classifying traffic in KDN/SDN environments (e.g., scalability, accuracy, cost). As a result, we propose a practical solution that generates flow-level traffic measurement reports in SDN environments, similar to those of NetFlow/IPFIX [34] in traditional networks. The proposed system uses only functions supported by OpenFlow, which is among the most popular standards in SDN, and allows the efficient maintenance of traffic statistics on network devices with basic characteristics (e.g., switches, routers), to finally send them to the control plane in an asynchronous way. In [35] we propose a monitoring platform that integrates the previous measurement system with a novel traffic classification module, also proposed as part of the ALLIANCE project, combining DPI and ML (decision trees), to efficiently identify the applications that generate traffic in the network.

Likewise, in [36] we have investigated the use of ML-based techniques (Support Vector Machines, Decision Trees) for detecting cryptocurrency mining activity in the network, using only basic information from the measurement reports offered by Network/IPFIX, which is a widely deployed standard in real-world networks presently. This can be especially useful to detect potential cryptojacking attacks, which are becoming more and more common presently. In particular, this type of attack consists of compromising machines within a network to exploit their resources for cryptocurrency mining, which is often a high power-consuming process.

4.3. Implementation and Evaluation of the Proposed Monitoring Platform

The monitoring platform proposed in [35] keeps updated traffic measurements in a distributed manner in the switches, while devices send asynchronously summaries of these measurements to the control plane. Moreover, we have proposed a novel classification system on top of the previous measurement system to identify the applications that generate traffic in the network. Presently, it is more and more common to find very diverse applications specifically under web-based services and encrypted traffic (e.g., VoIP, cloud storage, video streaming), which may have very different networking requirements (e.g., low delay, high bandwidth). This makes it particularly interesting to identify the applications generating traffic under this type of traffic (e.g., HTTP, HTTPS, SSL/TLS). In this context, the proposed classification system combines ML and DPI techniques, with special attention to the identification of applications that generate web and encrypted traffic [37]. In particular, this system first uses a decision tree-based classifier (c5.0 decision tree [38]) to discover the application-level protocol of traffic flows (e.g., HTTP, HTTPS, SSH, SMTP, DNS), and then applies more specific DPI techniques on web and encrypted flows to identify the application names within this type of traffic (e.g., Netflix, YouTube, Dropbox). Please note that these latter DPI techniques—that leverage functionalities from the open-source nDPI [39] and Bro IDS [40] tools—are applied only over the first few packets of web and encrypted flows. In particular, they use information at the beginning of HTTP sessions (e.g., from the HTTP GET header) and the initial handshakes of SSL/TLS connections (Server Name Indication field in certificates), thus incurring in limited processing overhead for the proposed monitoring platform.

We have implemented a prototype of this network-monitoring platform in the OpenDaylight controller [41]—which is well known in the SDN domain—and evaluated this prototype in a test environment with Open vSwitch [42]. Our evaluation results, using real traffic from three different networks, show that the proposed system achieves good accuracy levels for both measuring and classifying traffic; while maintaining a reasonable execution cost. As an example, Table 1 shows the accuracy achieved by the proposed classification system over several well-known web-based applications. These results were obtained through experiments with real-world traffic from a 10 Gbps access link of a large Spanish university network [37]. Applications are identified by their domain names, extracted either from HTTP headers or SSL/TLS certificates at the beginning of connections (packets transmitted during the first 40 ms of web and encrypted flows). We refer the reader to [35,37] for a detailed analysis on the tradeoff between accuracy and cost in the proposed monitoring platform. Finally, our prototype was integrated with a commercial network visibility platform to showcase its usefulness in a practical demonstration using real-world traffic [43].

Table 1. Per-application accuracy achieved by the proposed classification system (processing only packets transmitted in the first 40 ms of web and encrypted flows). Summary of experimental results from [37]

Domain Name	Application	Accuracy (%)
drive.google.com	Google Drive	95.4 %
mail.google.com	Gmail	94.7 %
netflix.com	Netflix	97.3 %
web.whatsapp.com	WhatsApp web	89.2 %
youtube.com	YouTube	87.8 %

5. Trust Element

5.1. Introduction

In some situations, network operators need to exchange different kinds of information among them. For example, in the context of 5G networks, operators may want to exchange the locations of 5G subscribers in their respective networks, to locate roaming user devices [44,45]. Another example is some SDN deployments that leverage overlay networks that must maintain a database of overlay addresses to underlay addresses (usually called Mapping System [46,47]). In addition, this information can be more complex, such as access control policies or QoS information.

However, exchanging this information between networks in different administrative domains requires trusting external networks (Figure 3). In other words, network A has to accept information from the external network B that can potentially influence routing behavior in network A. Hence, this situation is sometimes judged inappropriate by some operators [48].

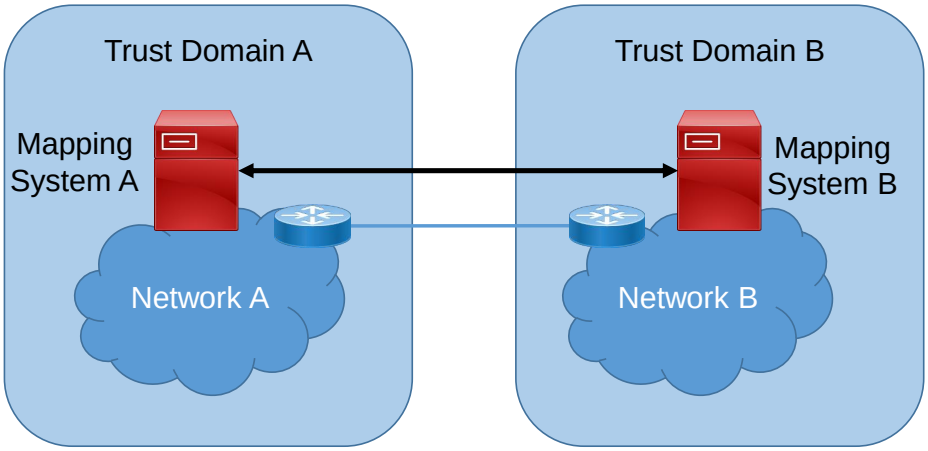


Figure 3. Exchange of routing information between two networks in different administrative domains. The Mapping System is a server that stores overlay-to-underlay mappings, and other network metadata.

The current solutions to transfer this information are usually complex to operate, e.g., in the area of Mapping Systems LISP-TREE [49] is similar to the DNS in configuration complexity. In addition, if we want to add security properties to such systems, such as confidentially or authentication, we must leverage centralised systems, i.e., Certification Authorities (CAs) to manage digital certificates. Although CAs are extremely convenient for single administrative domains, their centralisation is not convenient for a scenario with multiple administrative domains, because a single party can change the status of the database. There exist some distributed alternatives to centralised CAs, but they require complex configuration or do not scale well, such as cross-certification or bridge CA certificates [50,51].

On the other hand, blockchains have a decentralised trust architecture. Each participant of the blockchain has full control of its database entry, and it cannot be modified by

the other participants. Taking this into account, we have proposed leveraging the inherent decentralisation of blockchains to exchange information between different trust domains in a decentralised way (Figure 4). Thanks to the properties of blockchains, we can provide a shared database among a set of cooperating network operators that do not necessarily trust each other. At the same time, the data from each operator is protected from modification by the other operators.

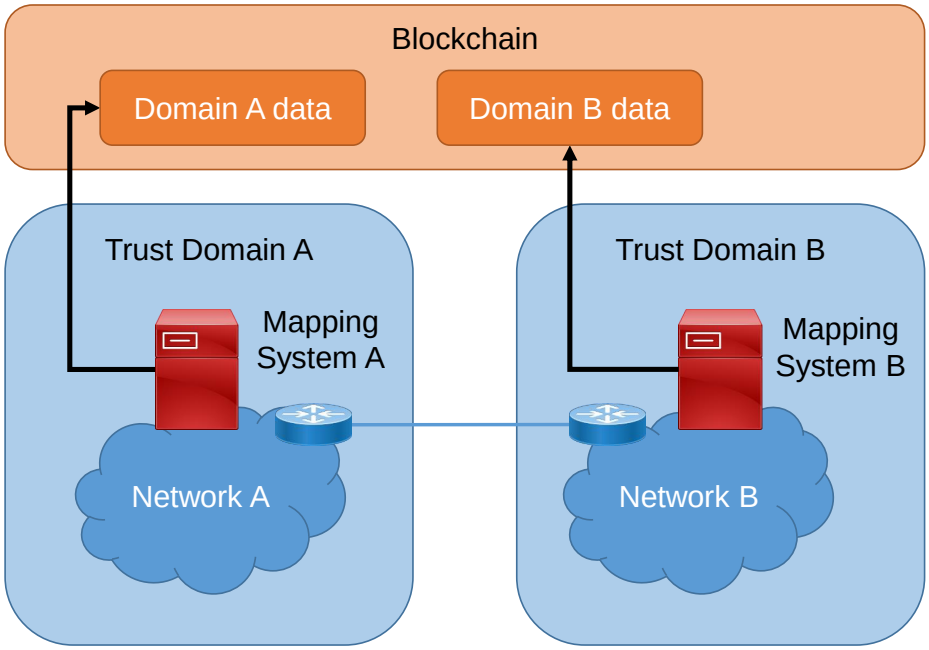


Figure 4. A blockchain can serve as a shared database between networks from different trust domains to share network metadata.

5.2. Research Activity

In the context of the ALLIANCE project, we have investigated how to leverage the properties of blockchains to share information between different trust domains, and the advantages and disadvantages of such system. We focused on two scenarios: first, recording the allocations and delegations of public IP addresses, as well as bindings of IP prefixes to Autonomous System Numbers (ASN) in a blockchain. Second, storing access control policies for networks belonging to different enterprises.

Regarding the allocation of IP addresses, we have proposed storing IP prefixes in a blockchain similarly to cryptographic coins in financial blockchains, such as in Bitcoin [52]. This way, participants can exchange, transfer and split blocks of IP addresses as in a financial blockchain. As we mentioned, this approach does not rely on centralised CAs, and decentralises trust: users do not depend on the actions of the CAs, since each IP prefix is tied to the public–private keypair of the operator. In addition, we can add metadata to each transaction. Since these metadata are included with the blockchain transaction, they are cryptographically verifiable. Two metadata are especially interesting: Autonomous System Numbers (ASN) and IP addresses. In the first case, since we are binding an IP prefix to an ASN, we can use these data to validate BGP messages in the context of interdomain routing security. In other words, we can verify if an IP prefix should be originated by the legitimate ASN, or has been modified along the path. This approach is an alternative to the RPKI [53], the current system to perform such validation, which is based on centralised CAs [54,55]. In the second case, we are binding an IP prefix to an IP address. This can be interpreted as a mapping of an overlay address to an underlay address, such as the ones used in mapping systems for SDN-based overlay networks. As we mentioned earlier, this mapping system can be used to share the location of 5G subscribers across networks from different operators.

With respect to access control policies, we focus on a scenario of different enterprises that want to allow access to some of their resources among them. The different enterprises leverage a blockchain to write their access control policies, and the routers query the blockchain to allow or deny connections. Since data in the blockchain is controlled by the associated private key owner, each enterprise can revoke any of their access policies at any moment. Moreover, we argue that a system based on a blockchain scales better than PKI-based alternatives such as cross-certification. A detailed evaluation of the scalability of this proposal can be found in [56].

5.3. Open-Source Prototypes

We built and evaluated two prototypes for the aforementioned use cases, and open-sourced their code. Table 2 summarises the prototypes we built, as well as some parameters of the experiments. The first prototype is a distributed mapping system for overlay networks [57]. It performs the basic functions of any blockchain: create and send transactions, run the consensus algorithm, create new blocks, etc. More specifically, it is engineered to support IP prefixes in its transactions: it allows recording, transferring, and splitting an IP prefix, as well as adding metadata to it. In addition, it enforces the basic rules for these transactions, such as verifying that new transactions reference an existing IP prefix, or that the issuer of a new transaction actually owns the IP prefix. This prototype (*Public v1* in Table 2) leverages Proof of Stake (PoS) as a consensus algorithm, but relies on a centralised random beacon to select the block signers. We have carried out an experiment to allocate 150k IP prefixes among 9 nodes that yielded a throughput of 6 transactions per second. We built a second version of this prototype to select the block signer in a distributed way. To this end, we have based the consensus algorithm in the DFINITY blockchain [58]. This second prototype is configured with a block time of 40 s, block size of 2 MB, and can reach a throughput of 10 transactions per second. A detailed evaluation can be found in [55].

Table 2. Summary of the different blockchain prototypes and experiment results. *tps* stands for transactions per second.

Prototype	Consensus Algorithm	Chain size	Number of prefixes	Throughput	Nodes
Public v1	PoS—centralised random beacon	1 GB	150k	6 tps	9
Public v2	PoS—decentralised random number generation	2.5 GB	350k	10 tps	2
Private	Hyperledger endorse-all and SOLO ordering	40 MB	5k	∼625 tps	8

Finally, *Private* is a blockchain prototype built on top of the Hyperledger Fabric blockchain platform [59]. We have chosen this platform because it is designed for enterprise use cases, and it allows controlling the participants in the blockchain. This property aligns well with this use case, since the enterprises want to share data among them, but it is not necessary that the access control data are public. We have defined several objects in the Hyperledger blockchain, such as users, departments, or resources, and configured it with a global constraint so that only the enterprise that owns the object can modify it. In addition, we have included a command line to make it easier to manage these objects. We have used Hyperledger's consensus algorithm that is based on Byzantine Fault Tolerant algorithms. Since Hyperledger is a permissioned blockchain, it can provide significantly higher transaction throughput than the public prototypes. The code of this prototype is also available on GitHub [60].

6. The SDN/NFV Domain

The need to deploy different services, each with their quality requirements on the same physical/logical infrastructure has fueled the introduction of concepts such as "Network slicing". It basically involves splitting the physical and logical resources of the network to

isolate the resources used to support a specific service, while guaranteeing the provision of said services. In this sense, the progress of novel technologies such as SDN and NFV has opened the possibility of providing such services. Indeed, the underlying physical network of an infrastructure operator/owner can now be abstracted, combining the resulting elements into complete and self-contained virtual infrastructures (slices).

In this section, we discuss the investigations carried out in ALLIANCE related to SDN/NFV-controlled optical networks. In this domain, we have considered both the packet and the optical layers, meaning that we have proposed an overall solution where an SDN/NFV orchestrator controls an ultra-low-latency and ultra-high-capacity spatially and spectrally flexible all-optical network infrastructure. In particular, our research activities to improve the optical layer are first introduced in Sections 6.1 and 6.2, with special emphasis on advanced modulation formats for both access and transport networks. Therefore, we present the proposed control layer based on an SDN/NFV orchestrator enhanced with our KDN vision and fed with the data collected by the monitoring element in Section 6.3. The overall solution enables the automatic and autonomous deliver of network slices customised to the requirements of the vertical services and applications while optimising the use of both the IT and the optical layer resources.

6.1. Transmission Layer

Today, the push towards 5G services and applications that require, among others, low latency and high capacity, poses new technological challenges. For example, the increased use of streaming, edge and cloud applications popular at portable devices requires architectural changes to satisfy the 5G/B5G mobile network specifications. Especially in Cloud RAN (C-RAN) optical fibre-based mobile fronthaul, provides the required flexibility, low latency and high capacity [61]. This context, Open Base Station Standard Initiative (OBSAI) and Common Public Radio Interface (CPRI) are common transmission techniques in 4G fronthaul networks, though inadequate for massive 5G/B5G services. Later, Ethernet-based CPRI (e-CPRI), digitalizing the RF signal is commonly used in 5G fronthaul network rollouts, due to its flexibility, efficiency and low quantisation resolution required [62–64].

Despite all these benefits, e-CPRI requires important Digital Signal Processing (DSP) resources in the Remote Radio Head (RRH) that increases the system power consumption. RoF technique has recently proposed as provides the required bandwidth while simplifies the interface of the RRHs [65–68]. NOMA-CAP modulation has recently been investigated as a promising B5G modulation format candidate to increase the capacity and flexibility of future mobile networks. In the framework of the ALLIANCE project, we have experimentally demonstrated the convergence of a NOMA-CAP wireless waveform with a single-carrier wired signal in a PON scenario using RoF technology [69]. Figure 5 shows the reference scenario for this work where the Pulse Amplitude Modulation 4-level (PAM4) has been used for legacy systems and NOMA-CAP for the future B5G fronthaul. Two NOMA levels (strong and weak) have been considered per each CAP band [69]. We have also first experimentally demonstrated NOMA-CAP as a modulation format for split-enabled optical interconnects with a capacity of up to 630 Gb/s using 7-core MCF and requiring an electrical bandwidth of 25 GHz. More details about this experiment and results can be found in [70]. In addition, we have provided an optical power budget enhancement in 50–90 Gbps IM-DD PONs with NOMA-CAP using Semiconductor Optical Amplifier (SOA)-based amplification [71]. Finally, this technique has also been used to provide a flexible resource provisioning for polarisation independent coherent PONs thanks to NOMA and multiCAP modulation, increasing at the same time the data-rate, up to 20 Gbps, and providing flexible reach among and existing PON, 20 km to 40 km, and a new extended nested PON, extra 20 km to 70 km, and users, from initial 32–64 to more than 380 users [72].

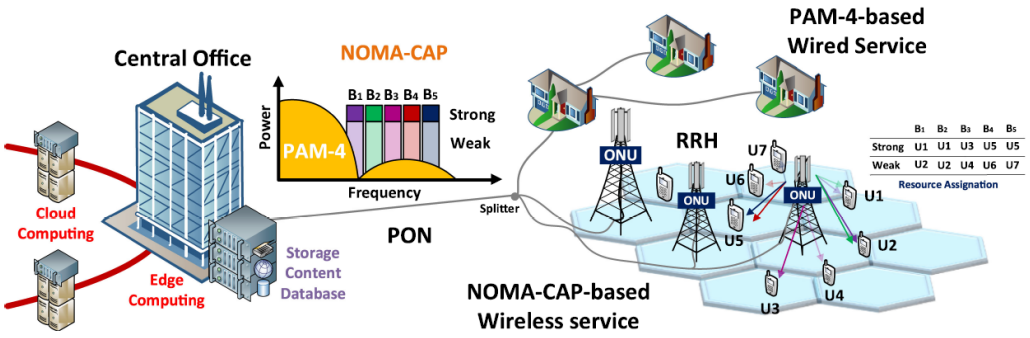


Figure 5. Conceptual diagram of a converged B5G fronthaul and PON architecture.

6.2. Multicore Fibres and Constellation Shaping

One of the challenges of B5G systems is how to provide such a huge bandwidth increase in the transport networks. The easiest solution would be installing more fibres. However, this is an obsolete technology and would have the biggest economic impact in the long run. Another alternative would be increasing the capacity of the installed fibre plant. This requires a more efficient spectrum usage (spectral efficiency) and/or expanding the available optical bandwidth (multiband communications). This is the preferred solution for the operators in the midterm. A more disruptive technology would be replacing the old fibre plant by a new optical fibre technology. Several candidates are being evaluated such as hollow-core fibres, multimode fibres or MCF. MCF is much more mature than the other alternatives and is much less demanding in terms of digital signal processing than the multimode counterpart.

In the framework of ALLIANCE project, it has been found that there exists an optimum multicore crosstalk level of about -55 dB/km which optimises the aggregate capacity of MCF [73] (see Table 3). This level sets the maximum number of cores that can be deployed in a given cladding diameter. This finding simplifies dramatically the design of MCFs to be used in future applications.

Table 3. Summary of experimental results from [73]. (Diameter: cladding diameter. Reach: transmission distance. SE: maximum aggregate spectral efficiency. XT: optimum aggregate multicore crosstalk. Cores: optimum number of cores.)

Diameter	Reach	SE	XT	Cores
125 microns	100 km	75 b/s/Hz	−63 dB/km	4
	1000 km	50 b/s/Hz	−63 dB/km	4
	10,000 km	25 b/s/Hz	−63 dB/km	4
200 microns	100 km	220 b/s/Hz	−55 dB/km	13
	1000 km	130 b/s/Hz	−55 dB/km	14
	10,000 km	50 b/s/Hz	−58 dB/km	14
260 microns	100 km	400 b/s/Hz	−50 dB/km	24
	1000 km	230 b/s/Hz	−52 dB/km	26
	10,000 km	85 b/s/Hz	−58 dB/km	27

On the other hand, we have experimentally demonstrated that a single transponder can operate at any distance, from DCs to transoceanic communications, using tunable probabilistic constellation shaping (PCS) [74] (see Figure 6). This proves the potential for PCS to adapt to any rate/reach requirement using the same hardware platform.

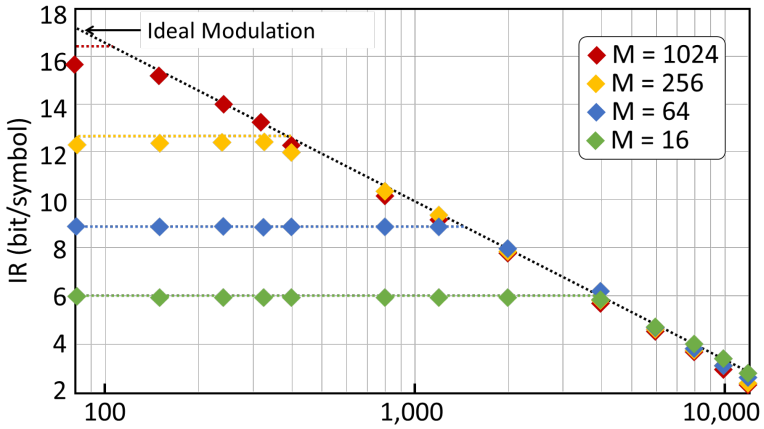


Figure 6. Experimental data from [74] for probabilistically shaped M-QAM signals. Symbols correspond to measured points. Dashed lines correspond to a linear interpolation

6.3. Control/Management/Orchestration Architecture

In ALLIANCE, a complete SDN/NFV-based control/management/orchestration architecture has been designed to deliver network slices customised to the requirements of the vertical services and applications [75–77]. The major challenge in this regard is that the provisioning of network slices may affect multiple SDN-controlled segments/technologies (optical access networks, metro, core and DCs). Moreover, special attention must be dedicated to the quality maintenance of the slices during their runtime. Since slices are employed to support several services on top, it becomes essential to monitor selected Key Performance Indicators (KPIs) of the slices to identify situations in which the current quality of services could be compromised. This way, the maintenance of slice QoS as well as the quality experienced by the user (i.e., QoE) can be achieved.

The proposed architecture has been inspired by the approach known as the MAPE cycle (Monitoring, Analysis, Planning and Execution): the four steps of this approach allow the automatic and autonomous management of the optical networks and the DCs resources. The first step (monitoring) is based on the collection of the different metrics that can be collected through sensors. The second step (analysis) consists of the analysis of the data collected to determine the need for actions to maintain the quality of the supported slices/services. Taking into account the enormous volume of data collected, the application of ML techniques can detect in advance possible failures in the infrastructure. The third step (planning) is required in the case of detecting the need for reconfiguration of the network to continue providing the service with the same quality. In particular, it refers to defining the actions to be enforced, thus determining the fourth step (execution) that represents the implementation of the defined reconfigurations.

In the context of the application of the MAPE approach for the maintenance of quality of the deployed network slices, end-to-end QoS-based monitoring tools have been designed and implemented. The designed architecture also enables reception of a direct QoE input that can provide valuable information on the service state as perceived by the user/vertical. In particular, a Mean Opinion Score (MOS) value is constantly collected. In our approach, both types of parameters (Qos and QoE) are constantly monitored, and upon a negative user feedback, a new architectural component, i.e., the QoE optimiser, has been introduced, being in charge of maintaining awareness of the user QoE to guarantee the correct service operation.

We have experimentally assessed the overall architecture using a three-segment network scenario, based on the interconnection between (cloud and/or edge) DCs through wide-area networks [75]. In particular, each network segment is connected to its OpenDayLight (ODL)-based SDN controller, while each DC is managed by a single OpenStack entity. Each DC hosts a single virtual machine and network connectivity is delivered across the three network segments. The QoS metric for the deployed slice is the packet

loss ratio (PLR) experimented by the data flows across the Virtual Network Functions (VNFs). Hence, we have implemented a policy stating that as a result of a PLR greater than a pre-defined threshold, the configured slice network bandwidth must be increased to suitable levels. In particular, we have validated that once the PLR reaches the threshold, the policy is activated increasing the bandwidth of the provisioned network resources and successfully dropping PLR to a negligible value. In summary, we have proved that the proposed architecture can maintain the desired QoS levels over the time under dynamic conditions that may affect the quality of the delivered services.

7. The RINA Domain

7.1. Basic Concepts

Current 5G approaches still model the network as a flat collection of physical devices forwarding data between interfaces, hiding the underlying complexity via overlays. This suffers of scalability issue on the one side and still maintain the complexity of managing the network infrastructure on the other side. A completely different focus has been taken in RINA.

RINA is a back-to-basics approach learning from the experience with TCP/IP, which reminded us that from the earliest days, networking was viewed as Inter-Process Communication (IPC) [78]. Thus, RINA starts from the premise that networking is IPC and only IPC. In particular, networking provides the means by which application processes on separate systems communicate, generalising the model of local IPC. In contrast to the fixed, five-layer model of the Internet, where each layer provides a different function, RINA is based on a single type of layer, implementing only two protocols called Error and Flow Control Protocol (EFCP), and Common Distributed Application Protocol (CDAP), which is repeated as many times as required by the network designer. The layer is called a Distributed IPC Facility (DIF), which is a distributed application that provides IPC services over a given scope to the distributed applications above (which can be other DIFs or regular applications). These IPC services are defined by the DIF Application Programming Interface (API), which provides operations to: (i) allocate flows to other applications by specifying an application name and a set of characteristics for the flow (such as delay, loss, capacity), (ii) read/write data from/to the flows, and (iii) deallocate flows and free the resources associated with them.

A key characteristic of RINA is its design based on the separation of all functions in mechanisms and policies, which dramatically simplifies networking. Although all DIFs implement the same two protocols (EFCP and CDAP), the specific operation of each DIF can be customised to its particular scope via programmable policies. In this way, the routing or packet forwarding policies configured in a backbone DIF can differ from those in a DC DIF, as their topological characteristics and dynamicity of the supported traffic can differ significantly.

To succeed in our endeavor, in ALLIANCE we used several open-source implementations and tools made available by previous research projects and by the RINA research community such as the IRATI RINA Stack (an open-source implementation of RINA for OS/Linux systems) and iporinad (a daemon program which is able to tunnel IP traffic over a RINA network) [79,80].

7.2. Research Activity

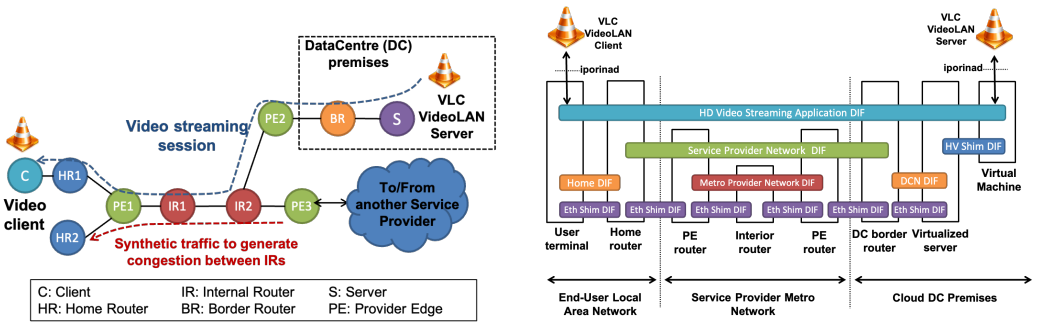
We started collaborating in RINA development back in 2014. Recently, we extended the concept of Degradation of Quality (ΔQ) [81] proposed for IP networks and designed the new Quantitative Timeliness Agreement Multiplexor (QTA-Mux) scheduling policy [82] for RINA. In contrast to simpler QoS differentiation solutions, where QoS services are provided in a priority order, QTA-Mux provides a way for an application and a network to negotiate performance in terms of bandwidth, urgency and cherish. The QoS class (called QoS Cubes in RINA) differentiation is enforced by a Cherish/Urgency (C/U) matrix which enables an inter-flow resource contention based on both losses and delay and by

a Policer/Shaper module which addresses the intra-flow contention. Since a common API is enforced between the DIFs, specific QoS Cubes can be requested by an IPC to the underlayer DIF during the flow allocation.

In ALLIANCE, our goal was to evaluate in a prototype the RINA QoS support by means of this QTA-Mux scheduler. Therefore, we set up a RINA network infrastructure shown in Figure 7a, consisting of 10 nodes in total, spanning from the end-user terminal to the server where applications run in a DC. This scenario is composed by 2 Internal Routers (IRs) interconnecting 3 Provider Edge (PE) routers, one of them providing connectivity to two Home Routers (HRs), another one to the DC where the VLC VideoLAN server runs, and a last one providing connectivity to another Service Provider.

Figure 7b depicts the configuration of DIFs. An Ethernet Shim DIF has been configured over the Ethernet links interconnecting the physical nodes, allowing the use of RINA over this legacy communication technology. On top of these Shim DIFs, a Metro Provider Network (MPN) DIF interconnecting PE routers has been configured, as well as a Service Provider Network (SPN) DIF extending the communication between HRs and the DC BR, a DC Network (DCN) DIF inside the DC, a Home DIF inside the end-user home, and an upper-level Video Streaming Application DIF supporting the delivery of the video streaming sessions to end-users across the VLC VideoLAN Server, the DC BR and the HRs. As VLC VideoLAN is an application that runs over IP, iporinad is required on the video streaming session endpoints, to create IP point to point tunnels over the RINA network.

Two sets of experiments were conducted. The goal of the first experiment was to evaluate the ability of RINA to guarantee QoS-specific requirements between the layers and compare it with a case where it cannot be provided as in TCP/IP. The second experiment focused on demonstrating a successful transmission of a HD video streaming in highly congested network with perfect users' QoE. More detailed explanation of these experiments and the results obtained are reported in [83].



(**a**) (**b**)

Figure 7. The RINA experiment network: (**a**) The 10-node infrastructure; (**b**) The configuration of the DIFs

7.3. QoS Support Evaluation

In this experiment, we compared two cases: in the first one, we have RINA with QoS support in all layers (called **full RINA**); in the second one, the application-specific QoS requests cannot cross layers, meaning the MPN layer is not able to allocate SPN flows with given QoS differentiation (called **TCP/IP-like**).

In full RINA, QTA-Mux is thus available at both SPN and MPN DIFs. Four QoS Cubes (A1, A2, B1, B2) have been considered in the MPN DIF, according to the 2×2 Cherish/Urgency (C/U) matrix depicted in Figure 8 (right). Please note here that the C/U matrix describes the operation of the C/U multiplexer within the QTA-Mux policy, able to enforce a bi-dimensional relative QoS Cube differentiation based on delay and loss requirements. For instance, flows over the MPN DIF assigned to QoS Cube A1 will be prioritised with respect to losses (i.e., they will be more cherished) and delay (i.e., they will be served with higher urgency) requirements. In contrast, flows assigned to QoS Cube B1,

for example, will still be prioritised with respect to losses, but un-prioritised with respect to delay (i.e., they will experience, and thus should tolerate, higher delays).

Moving up to the SPN DIF, one additional QoS Cube has been considered to better differentiate among heterogeneous application flows (i.e., with finer granularity). Specifically, the five QoS Cubes offered here are: Gold, Silver, Bronze, Sensitive Best Effort (BE) and BE, as described in the 3×2 C/U matrix depicted in Figure 8 (left). It is important to remark here that flows assigned to QoS Cubes in the SPN DIF will have to be transmitted over A1, A2, B1 and B2 flows across the MPN DIF. Therefore, an adequate mapping of SPN DIF to MPN DIF QoS Cubes becomes crucial to provide the expected QoS to end-user applications. In the ERASER scenario, both Gold and Silver flows in the SPN DIF are mapped to A1 flows in the MPN DIF, Sensitive BE flows to A2 ones, Bronze flows to B1 ones and, finally, BE flows to B2 flows in the MPN DIF.

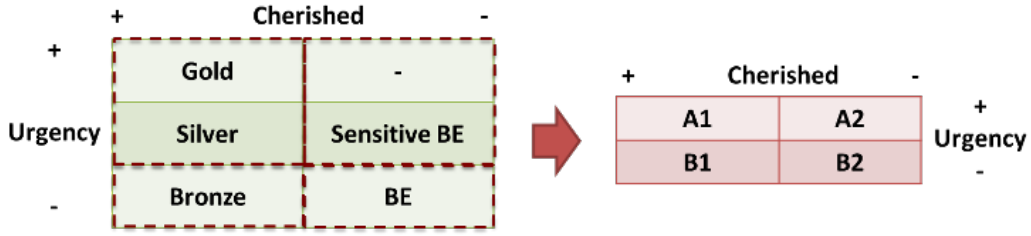


Figure 8. QoS Cubes defined in the SPN (**left**) and MPN (**right**) DIFs for full RINA scenario.

For the TCP/IP-like case, QoS class differentiation is available at the SPN layer only. Therefore, five different QoS classes are still offered to the application layer but only one class is available at the MPN layer, i.e., all five QoS classes are mapped to a single class in the MPN layer, which performs a First-In First-Out (FIFO) default scheduling policy.

To compare these two scenarios, we injected synthetic application traffic with 5 different specific flow characteristics specified in Table 4. In particular, we injected 5 flows of each type between PE3 and HR2, thus allocating 25 bidirectional flows in total over the SPN DIF. Finally, we set the total amount of these traffic to occupy an average of 70%, 80% or 90% of the capacity of the IR1-IR2 link.

Table 4. Synthetic application traffic flow characteristics and QoS class assignment.

Application Type	Traffic Distribution	Details	Requirements	QoS Class
HD video call	CBR	CBR bitrate: 1.5 Mbps	No delay No losses	Gold
Online gaming	ON-OFF	ON-OFF periods: 4 s–2 s CBR bitrate during ON: 4 Mbps	Avg. delay No losses	Silver
VoIP	ON-OFF	ON-OFF periods: 3 s–3 s CBR bitrate during ON: 64 kbps	No delay Tolerant to losses	Sensitive BE
File sharing	ON-OFF	ON-OFF periods: 2 s–1 s CBR bitrate during ON: 5 Mbps	Tolerant to delay Avg. losses	Bronze
Interactive traffic	Poisson	Avg. bitrate: 2 Mbps	No requirements	BE

Table 5 presents all latency (minimum, maximum, average) and packet loss measurements collected in both cases. Due to the lack of space, only measurements under 90% offered load are shown. First and foremost, full RINA seems to properly enforce

QoS differentiation based on delay. Indeed, outcomes perceived by most urgent synthetic traffic flows (HD Video Call, Online Gaming and VoIP) become quite constant, which does not happen for the least urgent ones (File Sharing and Interactive traffic flows). As for the experienced packet losses, full RINA allows for an effective differentiation, reaching a maximum value of 1.42% for Interactive traffic. Packet losses are significantly lower, around 0.00064%, for file-sharing traffic, with the same Urgency but a higher Cherish level.

In contrast, configuring the TCP/IP-like case neither succeeds in providing QoS differentiation in terms of end-to-end latency nor in terms of packet losses. In fact, although the applications may be able to request a given QoS differentiation at the edge of the network (i.e., SPN), it cannot be guaranteed at the core (i.e., MPN). The final result is that all types of applications experience similar loss and latency levels under every offered load scenario.

Table 5. Latency and packet loss at 90% offered load.

Scenario	Traffic Type	Min. Latency (ms)	Max. Latency (ms)	Avg. Latency (ms)	Avg. Packet Loss
full RINA	HD video call	0.190095	1.0508	0.51765	0
	Online gaming	0.195035	1.0397	0.51995	0
	VoIP	0.184455	1.0033	0.51845	0
	File sharing	0.18789	217.07	15.419	0.000643
	Interactive	9.196455	198.04	14.492	1.418555
TCP/IP-like	HD video call	0.16851	245.21	18.3975	0.073067
	Online gaming	0.17064	239.18	18.5635	0.102037
	VoIP	0.155495	245.145	18.112	0.084521
	File sharing	0.144350	240.945	18.232	0.101328
	Interactive	0.15236	245.89	20.9095	0.094567

7.4. HD Video Streaming Demonstration

For this demo, we have injected the same synthetic application flows in the network between PE3 and HR2, measured the carried average traffic between IR1 and IR2, and limited the capacity of this link reproducing a 90% load scenario.

In this congested network scenario, we have established a HD video streaming session over UDP from server node S to the client node C, transmitting a 1080p HD video file using VLC VideoLAN v3.0.1. Setting up an IP tunnel interface using iporinad, we have been able to transmit the IP traffic of the video streaming session over the HD Video Streaming Application DIF.

In full RINA scenario, we have been able watch it with perfect QoE, highlighting the adequacy of the RINA QoS support. In the TCP/IP-like case, QoE of the received client has been significantly worse, observing that it starts and stops constantly (video stuttering), also skipping a substantial number of frames each time it starts playing again. Both effects seem caused by the high congestion existing in the bottleneck link between IR1 and IR2 nodes in the 10 node RINA scenario. In fact, the video streaming session increases previous congestion even more, as this traffic around 10 Mbps was not considered when limiting link capacity to reproduce the 90% offered load scenario.

8. Final Discussion and Conclusions

In this paper, we have reviewed the main achievements obtained in the ALLIANCE project, a 45-month Spanish-funded national project started in 2018 and currently approaching its end. We have presented the novel architecture composed by 5 key blocks: the monitoring element, the trust element, the SDN/NFV cross-layer domain, the RINA domain, and the KDN orchestration layer. This project has focused on providing several

solutions to different networking problems in this 5G/B5G era. Results obtained in each of these blocks show superior performance with respect to the state of the art and motivate us to continue with these solutions in our future activities.

For instance, we have investigated new modulation formats and new design tools for both the access and the transport segments of a high-capacity and ultra-low-latency optical infrastructure. We have proposed an enhanced fixed mobile convergence using a NOMA-CAP wireless waveform with a single-carrier wired signal in a PON scenario. Although in its infancy, RINA has showed the potentiality to be a viable solution for B5G. Security, programmability, virtualisation and mobility are inherent part of the architecture by design, largely simplifying the control and management tasks between different network segments and operators. Indeed, we have showed in this work how it is possible in RINA to control and guarantee the application-specific QoS requirements between different providers.

Although recent advances in AI have led to a new era of ML techniques and the application of ML to networking is today a consolidated focus on the research community, it has not fulfilled its high expectations yet. In fact, existing state-of-the-art proposals seem unable to meet and outperform traditional approaches. In ALLIANCE, we have presented our KDN framework, which provides a suitable and practical environment for large-scale communications, as the network can learn from data by itself and provides efficient and automatic answers to most of the possible events, in a simpler, smarter, safer, and speedier way. For example, we have pioneered the first application of GNN to computer networks enabling the prediction of precise per-flow performance metrics for known networks and producing accurate estimates for unseen networks, outperforming state-of-the-art schemes in terms of accuracy and cost. Another example is the MAPE approach, which can autonomously maintain the desired QoS levels of the deployed services over the time, even under adverse dynamic conditions. These noteworthy contributions pave the way for an intelligent network knowledge plane which, making use of accurate and trusted data, can provision end-to-end services, with QoS guarantees, across one (or several) underlying Network Service Providers (NSPs).

Our future works will continue in this direction aiming at investigating new ways to accelerate GNN inference via software and hardware techniques. The new intelligent network knowledge plane based on accelerated GNNs will orchestrate and deliver service-aware end-to-end network services across different NSPs with the capability to self-evolve upon changes in the underlying programmable domains. In turn, NSPs also incorporate AI within their domains, allowing automation of specific network functions (such as self-orchestration) and the provisioning of intra-NSP services and resources as desired.

Regarding the SDN/NFV domain, we will investigate distributed AI functions at network nodes and MEC elements to enforce self-optimisation and self-configuration capabilities, as well as the new concept of AI-supported generic transceiver to adapt and control the working conditions towards an optimal performance under diverse application scenarios. Regarding the RINA domain, in future works we will focus on further improving its capability of providing QoS guarantees by modelling the characteristics of the DIF layers and feed GNNs with this information to obtain accurate performance metric predictions.

Author Contributions: Section 1, D.C.; Section 2, all; Section 3, A.C., J.S.-V., P.A.; Section 4, P.B.-R., J.S.-V., J.S.-P.; Section 5, S.S., J.A.L., J.M.G., F.A.B., A.P.; Section 6, D.C., J.P. (Jordi Perelló); Section 7, A.C., J.P. (Jordi Paillissé), J.D.-P.; Section 8, all. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been partially funded by the Spanish Ministry of Economy and Competitiveness under contract FEDER TEC2017-90034-C2 (ALLIANCE project) and by the Generalitat de Catalunya under contract 2017SGR-1037 and 2017SGR-605.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The access to the different data and/or datasets publicly available from the ALLIANCE project to the research community is indicated in each of the previous sections dedicated to the results.

Acknowledgments: We would like to thank Albert Lopéz for his invaluable support and all of our students for their contributions to the ALLIANCE project.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
ALLIANCE	Architecting a knowledge-defined 5G-enabled network infrastructure toward the upcoming digital society
ASN	Autonomous System Number
B5G	Beyond 5G
BGP	Border Gateway Protocol
C-RAN	Cloud RAN
CA	Certification Authority
CPRI	Common Public Radio Interface
DL	Deep Learning
DPI	Deep Packet Inspection
DRL	Deep Reinforcement Learning
DSP	digital signal processing
e-CPRI	Ethernet-based CPRI
GNN	Graph Neural Network
HD	High Definition
KDN	Knowledge-Defined Networking
MCF	Multicore Fibre
MEC	Multi-access Edge Computing
ML	Machine Learning
MPN	Metro Provider Network
NFV	Network Function Virtualisation
NOMA	Non-orthogonal multiple access
NOMA-CAP	NOMA with multiband Carrierless Amplitude and Phase
OBSAI	Open Base Station Standard Initiative
PCS	Probabilistic Constellation Shaping
RPKI	Resource Public Key Infrastructure
PON	Passive Optical Network
PoS	Proof of Stake
PPP	Public–Private Partnership
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Networks
RINA	Recursive Inter-Network Architecture
RoF	Radio-over-Fibre
RPKI	Resource Public Key Infrastructure
RRH	Remote Radio Head
SDN	Software Defined Networking
SPN	Service Provider Network

References

1. European Commission. Shaping Europe's Digital Future. 2021. Available online: https://digital-strategy.ec.europa.eu/en/policies/5g (accessed on 30 July 2021).
2. Sampson, N.; Erfanian, J.; Hu, N. NGMN 5G Whitepaper. 2020. Available online: https://ngmn.org/wp-content/uploads/NGMN-5G-White-Paper-2.pdf (accessed on 30 July 2021).

3. Redana, S.; Bulakci, Ö.; Mannweiler, C.; Gallo, L.; Kousaridas, A.; Navrátil, D.; Tzanakaki, A.; Gutiérrez, J.; Karl, H.; Hasselmeyer, P.; et al. 5G PPP 5G Architecture—White Paper. 2020. Available online: http://doi.org/10.5281/zenodo.3265031 (accessed on 30 July 2021).
4. LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. *Nature* **2015**, *521*, 436–444. [CrossRef]
5. Mestres, A.; Rodriguez-Natal, A.; Carner, J.; Barlet-Ros, P.; Alarcón, E.; Solé, M.; Muntés-Mulero, V.; Meyer, D.; Barkai, S.; Hibbett, M.J.; et al. Knowledge-defined networking. *ACM SIGCOMM Comput. Commun. Rev.* **2017**, *47*, 2–10. [CrossRef]
6. Clark, D.D.; Partridge, C.; Ramming, J.C.; Wroclawski, J.T. A knowledge plane for the Internet. In Proceedings of the ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Stockholm, Sweden, 28 August–1 September 2000.
7. McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Peterson, L.; Rexford, J.; Shenker, S.; Turner, J. OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Comput. Commun. Rev.* **2008**, *38*, 69–74. [CrossRef]
8. Bosshart, P.; Daly, D.; Gibb, G.; Izzard, M.; McKeown, N.; Rexford, J.; Schlesinger, C.; Talayco, D.; Vahdat, A.; Varghese, G.; et al. P4: Programming protocol-independent packet processors. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 87–95. [CrossRef]
9. Kim, C.; Sivaraman, A.; Katta, N.; Bas, A.; Antonin, D.; Advait, W.; Lawrence, J. In-band network telemetry via programmable dataplanes. In Proceedings of the ACM SIGCOMM Posters and Demos, London, UK, 17–21 August 2015.
10. Fadlullah, Z.M.; Tang, F.; Mao, B.; Kato, N.; Akashi, O.; Inoue, T.; Mizutani, K. State-of-the-art deep learning: Evolving machine intelligence toward tomorrows intelligent network traffic control systems. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2432–2455. [CrossRef]
11. Wang, M.; Cui, Y.; Wang, X.; Xiao, S.; Jiang, J. Machine learning for networking: Workflow, advances and opportunities. *IEEE Netw.* **2017**, *32*, 92–99. [CrossRef]
12. Pang, L.; Yang, C.; Chen, D.; Song, Y.; Guizani, M. A survey on intent-driven networks. *IEEE Access* **2020**, *8*, 22862–22873. [CrossRef]
13. Strinati, E.C.; Barbarossa, S. 6G networks: Beyond Shannon towards semantic and goal-oriented communications. *Comput. Netw.* **2021**, *190*, 107930. [CrossRef]
14. Hyun, J.; Tu, N.V.; Hong, J.W.K. Towards knowledge-defined networking using in-band network telemetry. In Proceedings of the 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS 2018), Taipei, Taiwan, 23–27 April 2018.
15. Fang, H.; Lu, W.; Li, Q.; Kong, J.; Liang, L.; Kong, B.; Zhu, Z. Predictive analytics based knowledge-defined orchestration in a hybrid optical/electrical datacenter network testbed. *IEEE/OSA J. Light. Technol.* **2019**, *37*, 4921–4934. [CrossRef]
16. Li, Q.; Fang, H.; Li, D.; Peng, J.; Kong, J.; Lu, W.; Zhu, Z. Scalable knowledge-defined orchestration for hybrid optical-electrical datacenter networks. *IEEE/OSA J. Opt. Commun. Netw.* **2019**, *12*, A113–A122. [CrossRef]
17. Mnih, V.; Kavukcuoglu, K.; Silver, D.; Rusu, A.A.; Veness, J.; Bellemare, M.G.; Graves, A.; Riedmiller, M.; Fidjeland, A.K.; Ostrovski, G.; et al. Human-level control through deep reinforcement learning. *Nature* **2015**, *518*, 529–533. [CrossRef] [PubMed]
18. Silver, D.; Hubert, T.; Schrittwieser, J.; Antonoglou, I.; Lai, M.; Guez, A.; Lanctot, M.; Sifre, L.; Kumaran, D.; Graepel, T.; et al. Mastering chess and shogi by self-play with a general reinforcement learning algorithm. *arXiv* **2017**, arXiv:1712.01815.
19. Mnih, V.; Kavukcuoglu, K.; Silver, D.; Graves, A.; Antonoglou, I.; Wierstra, D.; Riedmiller, M. Playing Atari with Deep Reinforcement Learning. *arXiv* **2013**, arXiv:1312.5602.
20. Suárez-Varela, J.; Mestres, A.; Yu, J.; Kuang, L.; Barlet-Ros, P.; Cabellos-Aparicio, A. Routing based on Deep Reinforcement Learning in Optical Transport Networks. In Proceedings of the 2019 Optical Fiber Communication Conference (OFC2019), San Diego, CA, USA, 3–7 March 2019.
21. Suárez-Varela, J.; Mestres, A.; Yu, J.; Kuang, L.; Feng, H.; Barlet-Ros, P.; Cabellos-Aparicio, A. Feature engineering for Deep Reinforcement Learning based routing. In Proceedings of the 53rd IEEE International Conference on Communications (ICC 2019), Shanghai, China, 20–24 May 2019.
22. Scarselli, F.; Gori, M.; Tsoi, A.C.; Hagenbuchner, M.; Monfardini, G. The graph neural network model. *IEEE Trans. Neural Netw.* **2009**, *20*, 61–80. [CrossRef] [PubMed]
23. Battaglia, P.W.; Hamrick, J.B.; Bapst, V.; Sanchez-Gonzalez, A.; Zambaldi, V.; Malinowski, M.; Tacchetti, A.; Raposo, D.; Santoro, A.; Faulkner, R.; et al. Relational inductive biases, deep learning, and graph networks. *arXiv* **2018**, arXiv:1806.01261.
24. Wu, Z.; Pan, S.; Chen, F.; Long, G.; Zhang, C.; Yu, P.S. A Comprehensive Survey on Graph Neural Networks. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *32*, 4–24. [CrossRef] [PubMed]
25. Almasan, P.; Suárez-Varela, J.; Badia-Sampera, A.; Rusek, K.; Barlet-Ros, P.; Cabellos-Aparicio, A. Deep reinforcement learning meets graph neural networks: Exploring a routing optimization use case. *arXiv* **2019**, arXiv:1910.07421.
26. Rusek, K.; Suàrez-Varela, J.; Mestres, A.; Barlet-Ros, P.; Cabellos-Aparicio, A. Unveiling the potential of Graph Neural Networks for network modeling and optimization in SDN. In Proceedings of the ACM 2019 Symposium on SDN Research (SOSR2019), San Jose, CA, USA, 3–4 April 2019; pp. 140–151.
27. Rusek, K.; Suàrez-Varela, J.; Almasan, P.; Barlet-Ros, P.; Cabellos-Aparicio, A. RouteNet: Leveraging Graph Neural Networks for network modeling and optimization in SDN. *IEEE J. Sel. Areas Commun. (JSAC)* **2020**, *38*, 2260–2270. [CrossRef]
28. Suárez-Varela, J.; Carol-Bosch, S.; Rusek, K.; Almasan, P.; Arias, M.; Barlet-Ros, P.; Cabellos-Aparicio, A. Challenging the generalization capabilities of Graph Neural Networks for network modeling. In Proceedings of the 2019 ACM SIGCOMM Posters and Demos, Beijing, China, 21 August 2019.

29. Almasan, P.; Suárez-Varela, J.; Wu, B.; Xiao, S.; Barlet-Ros, P.; Cabellos-Aparicio, A. Towards Real-Time Routing Optimization with Deep Reinforcement Learning: Open Challenges. *arXiv* **2021**, arXiv:2106.09754.
30. Suárez-Varela, J.; Mestres, A.; Yu, J.; Kuang, L.; Feng, H.; Cabellos-Aparicio, A.; Barlet-Ros, P. Routing in Optical Transport Networks with Deep Reinforcement Learning. *IEEE/OSA J. Opt. Commun. Netw.* **2019**, *11*, 547–558. [CrossRef]
31. Knight, S.; Nguyen, H.X.; Falkner, N.; Bowden, R.; Roughan, M. The internet topology zoo. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 1765–1775. [CrossRef]
32. Carela-Español, V.; Barlet-Ros, P.; Cabellos-Aparicio, A.; Solé-Pareta, J. Analysis of the impact of sampling on NetFlow traffic classification. *Comput. Netw.* **2011**, *55*, 1083–1099. [CrossRef]
33. Aceto, G.; Ciuonzo, D.; Montieri, A.; Pescapè, A. Mobile encrypted traffic classification using deep learning. In Proceedings of the 2018 Network Traffic Measurement and Analysis Conference (TMA2018), Vienna, Austria, 26–29 June 2018.
34. Claise, B. NetFlow Services Export Version 9 Status (RFC 3954), Internet Engineering Task Force, 2004. Available online: https://tools.ietf.org/html/rfc3954 (accessed on 15 September 2021).
35. Suárez-Varela, J.; Barlet-Ros, P. Flow monitoring in Software-Defined Networks: Finding the accuracy/performance tradeoffs. *Comput. Netw.* **2018**, *135*, 289–301. [CrossRef]
36. Zayuelas, J.; Suárez-Varela, J.; Barlet-Ros, P. Detecting cryptocurrency miners with NetFlow/IPFIX network measurements. In Proceedings of the 2019 IEEE International Symposium on Measurements and Networking (M&N2019), Catania, Italy, 8–10 July 2019.
37. Suárez-Varela, J.; Barlet-Ros, P. Towards accurate classification of HTTPS traffic in Software-Defined Networks. In Proceedings of the 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC2018), Houston, TX, USA, 14–17 May 2018.
38. Data Mining Tools See5 and C5.0. Available online: https://www.rulequest.com/see5-info.html (accessed on 30 July 2021).
39. nDPI: Open and Extensible LGPLv3 Deep Packet Inspection Library. Available online: https://www.ntop.org/products/deep-packet-inspection/ndpi/ (accessed on 15 September 2021).
40. Paxson, V. Bro: A system for detecting network intruders in real-time. *Comput. Netw.* **1999**, *31*, 2435–2463. [CrossRef]
41. OpenDaylight. Available online: https://www.opendaylight.org (accessed on 30 July 2021).
42. Open vSwitch. Available online: https://www.openvswitch.org (accessed on 30 July 2021).
43. Suárez-Varela, J.; Barlet-Ros, P. SBAR: SDN flow-Based monitoring and Application Recognition. In Proceedings of the 2018 ACM Symposium on SDN Research (SOSR2018), Los Angeles, CA, USA, 28–29 March 2018.
44. Fafolahan, E.M.O.; Pierre, C. A Seamless Mobility Management Protocol in 5G Locator Identificator Split Dense Small Cells. *IEEE Trans. Mob. Comput.* **2020**, *19*, 1745–1759. [CrossRef]
45. Wu, Q.; Wu, C.M.; Luo, W. Distributed mobility management with ID/locator split network-based for future 5G networks. *Telecommun. Syst.* **2019** *71*, 459–474. [CrossRef]
46. Hoefling, M.; Menth, M.; Hartmann, C. A Survey of Mapping Systems for Locator/Identifier Split Internet Routing. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1842–1858. [CrossRef]
47. Mathy, L.; Iannone, L. LISP-DHT: Towards a DHT to map identifiers onto locators. In Proceedings of the 2008 ACM International Conference on Emerging Networking EXperiments and Technologies (CoNext 2008), New York, NY, USA, 10–12 December 2008.
48. Cooper, D.; Heilman, E.; Brogle, K.; Reyzin, L.; Goldberg, S. On the risk of misbehaving rpki authorities. In Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks (HotNets-XII), New York, NY, USA, 21–22 November 2013.
49. Jakab, L.; Cabellos-Aparicio, A.; Coras, F.; Saucez, D.; Bonaventure, O. LISP-TREE: A DNS Hierarchy to Support the LISP Mapping System. *IEEE J. Sel. Areas Commun. (JSAC)* **2010**, *28*, 1332–1343. [CrossRef]
50. Jøsang, A. Pki Trust Models. In *Theory and Practice of Cryptography Solutions for Secure Information Systems*; IGI Global: Hershey, PA, USA, 2013; pp. 279–301. Available online: https://www.igi-global.com/chapter/content/76520 (accessed on 12 August 2021).
51. Slagell, A.; Bonilla, R.; Yurcik, W. A survey of pki components and scalability issues. In Proceedings of the 2006 IEEE International Performance Computing and Communications Conference (IPCCC 2006), Phoenix, AZ, USA, 10–12 April 2006.
52. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Tech. Rep.* **2008**. Available online: https://nakamotoinstitute.org/bitcoin/ (accessed on 12 August 2021).
53. Lepinski, M.; Kent, S. An Infrastructure to Support Secure Internet Routing (RFC 6480), Internet Engineering Task Force, 2012. Available online: https://tools.ietf.org/html/rfc6480 (accessed on 15 September 2021)
54. Paillisse, J.; Ferriol, M.; Garcia, E.; Latif, H.; Piris, C.; Lopez, A.; Kuerbis, B.; Rodriguez-Natal, A.; Ermagan, V.; Maino, F.; et al. IPchain: Securing IP Prefix Allocation and Delegation with Blockchain. In Proceedings of the 2018 IEEE International Conference on Blockchain (Blockchain 2018), Halifax, NS, Canada, 30 July–3 August 2018.
55. Paillisse, J.; Manrique, J.; Bonet, G.; Rodriguez-Natal, A.; Maino, F.; Cabellos, A. Decentralized Trust in the Inter-Domain Routing Infrastructure. *IEEE Access* **2019**, *7*, 166896–166905. [CrossRef]
56. Paillisse, J.; Subira, J.; Lopez, A.; Rodriguez-Natal, A.; Ermagan, V.; Maino, F.; Cabellos, A. Distributed Access Control with Blockchain. In Proceedings of the 53rd IEEE International Conference on Communications (ICC 2019), Shanghai, China, 20–24 May 2019.
57. Open Overlay Router Project. Ipchain: A Blockchain-Based Mapping System. 2019. Available online: https://github.com/OpenOverlayRouter/blockchain-mapping-system (accessed on 12 August 2021).
58. Hanke, T.; Movahedi, M.; Williams, D. Dfinity Technology Overview Series, Consensus System. *arXiv* **2018**, arXiv:1805.04548.

59. Linux Foundation Projects. Hyperledger Fabric. 2018. Available online: https://www.hyperledger.org/projects/fabric (accessed on 12 August 2021).
60. Subira, J. Blockchain for Distributed Group Based Policies. 2018. Available online: https://github.com/JordiSubira/DGBP (accessed on 12 August 2021).
61. Sun, A.G.; Xiong, K.; Boateng, G.O.; Ayepah-Mensah, D.; Liu, G.; Jiang, W. Autonomous resource provisioning and resource customization for mixed traffics in virtualized radio access network. *IEEE Syst. J.* **2019**, *13*, 2454–2465. [CrossRef]
62. Iovanna, F.P.; Cavaliere, S.; Stracca, L.; Giorgi, F. Ubaldi. 5G Xhauland service convergence: Transmission, switching and automation enabling technologies. *IEEE/OSA J. Light. Technol.* **2020**, *38*, 2799–2806. [CrossRef]
63. Dominique, F. Requirements of 5G radio networks on optical X-haultransport. In Proceedings of the 2019 Optical Fiber Communication Conference (OFC2019), San Diego, CA, USA, 3–7 March 2019.
64. CPRI. Common Public Radio Interface: eCPRI Interface Specification. *eCPRI Specification v2.0*. 2019. Available online: http://www.cpri.info/downloads/eCPRI_v_2.0_2019_05_10c.pdf (accessed on 15 September 2021).
65. Kim, H. RoF-based optical fronthaul technology for 5G and Beyond. In Proceedings of the 2018 Optical Fiber Communication Conference (OFC2018), San Diego, CA, USA, 11–15 March 2018.
66. Kim, B.G.; Kim, H.; Chung, Y.C. Impact of multipath interference in the performance of RoF-based mobile fronthaul network implemented by using DML. *IEEE/OSA J. Light. Technol.* **2017**, *35*, 145–151. [CrossRef]
67. Kim, B.G.; Bae, S.H.; Kim, H.; Chung, Y.C. Feasibility of RoF-based optical fronthaul network for next-generation mobile communications. In Proceedings of the Opto-Electronic Communication Conference and Photonic Global Conference (OECC/PGC2017), Singapore, 31 July–4 August 2017.
68. Sarmiento, S.; Altabas, J.A.; Spadaro, S.; Lazaro, J.A. Experimental assessment of 10Gbps 5G multicarrier waveforms for high-layer split U-DWDM-PON-based fronthaul. *IEEE J. Light. Technol.* **2019**, *37*, 2344–2351. [CrossRef]
69. Sarmiento, S.; Mendinueta, J.M.D.; Altabás, J.A.; Spadaro, S.; Shinada, S.; Furukawa, H.; Olmos, J.J.V.; Lázaro, J.A.; Wada N. High Capacity Converged Passive Optical Network and RoF-Based 5G+ Fronthaul Using 4-PAM and NOMA-CAP Signals. *IEEE/OSA J. Light. Technol.* **2021**, *39*, 372–380. [CrossRef]
70. Mendinueta, J.M.D.; Sarmiento, S.; Altabás, J.A.; Spadaro, S.; Shinada, S.; Olmos, J.J.V.; Lázaro, J.A.; Furukawa, H. NOMA-CAP Modulation Format for Next Generation Converged Fronthaul-Optical Access and Data Center Interconnect Networks. In Proceedings of the 22nd International Conference on Transparent Optical Networks (ICTON2020), Bari, Italy, 19–23 July 2020.
71. Sarmiento, S.; Mendinueta, J.M.D.; Altabás, J.A.; Spadaro, S.; Shinada, S.; Furukawa, H.; Olmos, J.J.V.; Lázaro, J.A.; Wada, N. Optical Power Budget Enhancement in 50–90 Gb/s IM-DD PONs With NOMA-CAP and SOA-Based Amplification. *IEEE Photonics Technol. Lett.* **2020**, *32*, 608–611. [CrossRef]
72. Izquierdo, D.; Altabás, J.A.; Barrio, M.; Clemente, J.; Millan, P.; Sarmiento, S.; Lázaro, J.A.; Rommel, S.; Puerta, R.; Vegas-Olmos, J.J.; et al. Flexible resource provisioning of polarization independent coherent PONs based on non-orthogonal multiple access and multiCAP modulation. *IEEE/OSA J. Opt. Commun. Netw.* **2021**, *13*, 140–146. [CrossRef]
73. Gené, J.M.; Winzer, P.; Chen, H.; Ryf, R.; Hayashi, T.; Sasaki, T. Towards Broadly Optimum Multi-Core Fiber Designs. In Proceedings of the 45th European Conference on Optical Communication (ECOC2019), Dublin, Ireland, 22–26 September 2019.
74. Gené, J.M.; Chen, X.; Cho, J.; Chandrasekhar, S.; Winzer, P. Experimental Demonstration of Widely Tunable Rate/Reach Adaptation from 80 km to 12,000 km using Probabilistic Constellation Shaping. In Proceedings of the 2020 Optical Fiber Communications Conference (OFC2020), San Diego, CA, USA, 8–12 March 2020.
75. Spadaro, S.; Pages, A.; Biosca, J.; Agraz, F. Enabling Service Provisioning and Quality Maintenance in Sliceable Optical Networks. In Proceedings of the SPIE Photonic West 2021, San Francisco, CA, USA, 23–28 January 2021.
76. Spadaro, S.; Agraz, F.; Pages, A.; Montero, R. Autonomic 5G and beyond network management. In Proceedings of the 22nd International Conference on Transparent Optical Networks (ICTON2020), Bari, Italy, 19–23 July 2020.
77. Montero, R.; Agraz, F.; Pages, A.; Spadaro, S. Real-time Maintenance of Latency-sensitive 5G Services through Network Slicing. *Photonic Netw. Commun.* **2020**, *40*, 221–232. [CrossRef]
78. Day, J. *Patterns in Network Architecture: A Return to Fundamentals*; Prentice Hall: Hoboken, NJ, USA, 2008.
79. Pouzin Society. Available online: http://pouzinsociety.org (accessed on 30 July 2021).
80. 5G & IoT—RINA. Available online: https://i2cat.net/research-topics/recursive-internetwork-architecture/ (accessed on 30 July 2021).
81. Davies, N. Delivering predictable quality in saturated networks. *Tech. Rep.* **2003**. Available online: http://www.pnsol.com/public/TP-PNS-2003-09.pdf (accessed on 30 July 2021).
82. León, S.; Perelló, J.; Careglio, D.; Grasa, E.; Tarzán, M.; Davies, N.; Thomson, P. Assuring QoS guarantees for heterogeneous services in RINA networks with ΔQ. In Proceedings of the 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom2016), Luxembourg, 12–15 December 2016.
83. Perelló, J.; López, A.; Careglio, D. Experimenting with Real Application-specific QoS Guarantees in a Large-scale RINA Demonstrator. In Proceedings of the RINA 2019 Workshop, Co-Located with the 2019 Innovation in Clouds, Internet And Networks Conference (ICIN 2019), Paris, France, 18 February 2019.