

Orchestration and Control in Software-Defined 5G Networks: Research Challenges

Gianfranco Nencioni*, Rosario G. Garroppo[†], Andres J. Gonzalez[‡], Bjarne E. Helvik[§], and Gregorio Procissi[†]

* University of Stavanger, Stavanger, Norway – Email: gianfranco.nencioni@uis.no

[†] University of Pisa, Pisa, Italy – Email: {r.garroppo,g.procissi}@iet.unipi.it

[‡] Telenor ASA, Tromsø, Norway – Email: andres.gonzalez@telenor.com

[§] NTNU – Norwegian University of Science and Technology, Trondheim, Norway – Email: bjarne@ntnu.no

Abstract—The fifth generation (5G) of cellular networks promises to be a major step in the evolution of wireless technology. 5G is planned to be used in a very broad set of application scenarios. These scenarios have strict heterogeneous requirements that will be accomplished by enhancements on the radio access network and a collection of innovative wireless technologies. Software-defined technologies, such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV), will play a key role in integrating these different technologies. Network slicing emerges as a cost-efficient solution for the implementation of the diverse 5G requirements and verticals. The 5G radio access and core networks will be based on a SDN/NFV infrastructure, which will be able to orchestrate the resources and control the network in order to efficiently, flexibly, and scalably provide network services. In this paper, we present the up-to-date status of the software-defined 5G radio access and core networks and a broad range of future research challenges on the orchestration and control aspects.

I. INTRODUCTION

The fifth generation (5G) of cellular networks aims at revolutionizing the world of wireless communication. 5G will be characterized by ubiquitous connectivity, extremely low latency, and very high-speed data transfer. These characteristics will enable the use of 5G in a very broad set of application scenarios: from pervasive video to high user mobility; from broadband access everywhere to lifeline communications; from massive Internet of Things (mIoT) to broadcast-like services; from tactile Internet to ultrareliable communications [1]. For enabling this variety of applications, ambitious improvements with respect to 4G are needed: 10-100 times more connected devices; 1000 times higher mobile data volume per area; 10-100 times higher data rate; 1 ms latency; 99.999% availability; 10 times less energy consumption; 5 times less network management operation expenses. The motivation and explanation of such requirements are given for some specific use cases in [2].

A key aspect of 5G is the radical network transformation required for offering vertical services, with connectivity, storage and computing solutions tailored to the specific digital business case of different industries (e.g. health care, energy, multimedia, automotive, etc.). A vertical service relaxes the conceptual restriction of VNFs to networking functions, which is the main characteristic of a network service. In a vertical service, the virtual functions may perform arbitrary functionality in the application domain. A vertical service may also

include the end user devices or applications within them, which can be considered as physical or virtual functions. New business models will be developed using the integration of the requirements of multiple vertical industries. In some cases, stakeholders from vertical industries can take the role of service providers for end-users by exploiting the infrastructure and connectivity services of network providers. In others, they will instantiate a vertical service for improving the efficiency of their business infrastructure and for developing new production models. For example, in [3], the authors describe a vertical proof-of-concept aimed at providing more flexibility and higher efficiency to the “factory of the future” by integrating robots, machine intelligence and 5G. In [4], the authors describe how the 5G infrastructure implementing the vertical service concept can be used to offer Vehicle-to-Everything (V2X) safety applications. In this vertical service of the automotive domain, applications within a vehicle may be part of the service.

The transformation concerns two main aspects. An *evolutionary* aspect, where 5G will allow the same applications as today, but with much better performance. The work of 3GPP on New Radio (NR) and Next Generation Radio Access Network (NG-RAN) [5] aims at designing new radio interfaces for increasing the available data rate by taking into account the recent results on millimeter wave (mmWave) communications and massive Multiple Input and Multiple Output (MIMO).

A *revolutionary* aspect given by the 5G vertical concept is the key new business paradigm that implies the support of very heterogeneous services on the same infrastructure. Different services, such as vehicular networking and e-health, require from the mobile network very different Key Performance Indicators (KPIs) (e.g., low latency, high capacity or service continuity). Supporting all these requirements on the same infrastructure entails a disruptive re-engineering of the network architecture. This scenario requires a key feature to 5G: it should represent a holistic orchestration platform, where computing resources are distributed within the network including sites of the vertical industry stakeholders, within the base stations, in edge clouds at central offices, in regional and central clouds, and managed by different stakeholders. To this aim, the introduction and implementation of the network slicing concept is a key tool that can enable operators to deliver tailored and customized connectivity and services for different business verticals and use cases.

For achieving the challenging objectives of 5G, the research community is working in two complementary directions: (i) the NG-RAN in order to integrate heterogeneous radio network technologies, i.e. NR, massive MIMO, mmWave, and multi-tier architecture [6] [7]; (ii) Software-Defined Networking (SDN) and Network Function Virtualization (NFV), which are rising as key components that will enable the orchestration and control of the technological resources in the RAN, transport, and cloud network, in a flexible, scalable, efficient, and agile way [8].

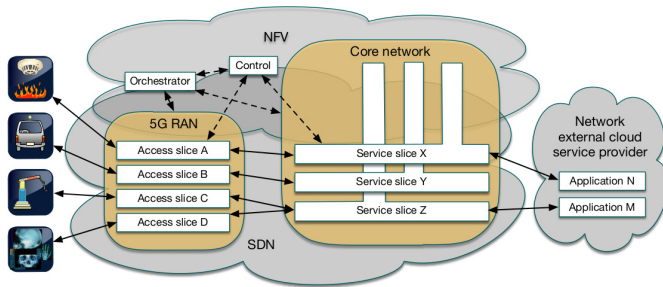


Fig. 1: Illustration of the software-defined 5G radio access and core networks.

This paper presents software-defined 5G radio access and core networks (see Figure 1) from a general point of view, including the last updates on the topic. Moreover, this paper extends the previous considerations [9] and outlines a broad range of the future research challenges in the orchestration and control in 5G system. Several research challenges are emerging in order to optimally manage the resources and provide advanced 5G services to the end users [10]. Current works are really specific, mainly addressing a particular task with a particular objective. On the contrary, this paper addresses orchestration and control in 5G from a holistic view by presenting its enabling technologies, tasks and objectives, and providing the details of the challenges related to each task.

This paper is organized as follows. In the next section the main features and concepts of SDN and NFV are presented. In Section III a more holistic view of 5G is presented, including RAN, core, softwarization, orchestration and management concepts. Successively, Section IV proposes a classification of the 5G implementation tasks and objectives, and for each class it describes the respective challenges of orchestrating and controlling 5G networks. Finally, Section V concludes the paper.

II. SOFTWARE-DEFINED NETWORKING

In the recent years, SDN and NFV emerged as innovative network paradigms that have attracted the interest of network operators and service providers. In this section, their main features and global architectures are presented in order to provide the background needed for the concepts presented in the paper.

A. Software-Defined Networking (SDN)

SDN is a networking paradigm that promises to improve the programmability and flexibility of networks. SDN assumes

programmable network devices in which the forwarding plane is decoupled from the control plane. In addition, the control plane is logically centralized in a software-based controller (“network brain”), while the data plane is composed of network devices (“network arms”) that forward packets.

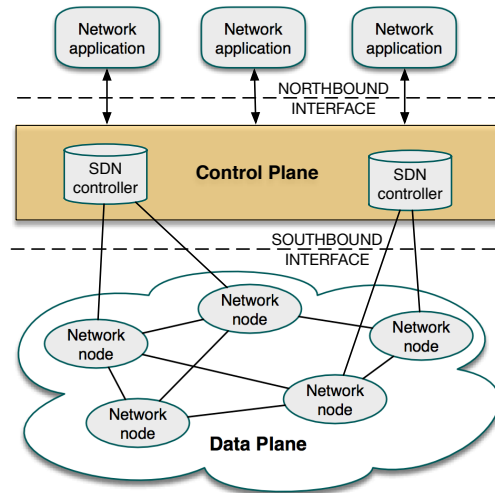


Fig. 2: SDN architecture.

Figure 2 depicts the SDN architecture. The control plane includes both northbound and southbound interfaces. The northbound interface provides a network abstraction to network applications. The southbound interface standardizes the information exchange between the control and data planes. SDN has been successfully introduced in data center environment by Internet content providers such as Facebook and Google.

As far as its deployment, the software-defined approach should allow *platform agnostic* implementations of the monitoring functions. However, after several years, the ultimate target of fully programmable devices still partially collides with the vendors need for closed platforms and portability is still mostly limited to software platforms. Nevertheless, significant steps forward have recently been made. As an example, the H2020 BEBA (*Behavioral Based Forwarding*) [11] project has successfully delivered monitoring and security applications to both OpenFlow controlled HW and SW platforms.

From a technological point of view, the maturity level attained by commodity hardware enables even standard PCs to handle the traffic volume of multi (10+) gigabit links. Indeed, the large number of cores available on affordable CPUs and the new generation of network interfaces that support multiple queues have determined a significant interest towards the proposal of software accelerated solutions for high-speed traffic retrieval. Indeed, software frameworks like PF_RING [12], Netmap [13], DPDK [14], PFQ [15], [16], currently allow very high speed data capture and processing on reasonably cheap commodity PCs. For example, in the aforementioned BEBA project, PFQ has been used to accelerate a repurposed version of the OpenFlow compliant software switch OFSoftSwitch [17] to perform packet processing up to full 10Gbps line speed [18].

B. Network Function Virtualization (NFV)

NFV is about transforming the way network operators design and operate networks and network services. NFV consists of applying IT virtualization technology to consolidate many specialized network equipment types onto industry of high volume servers, switches and storage units.

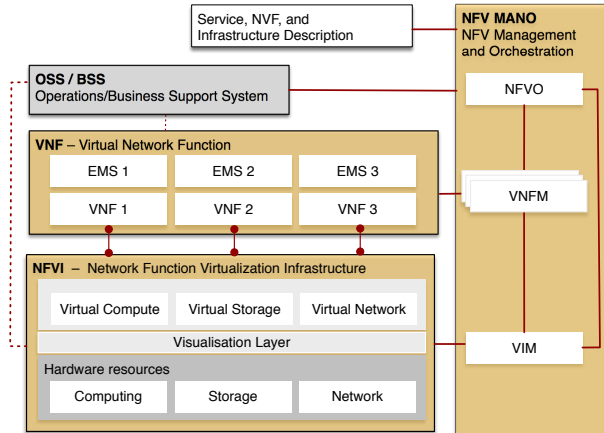


Fig. 3: NFV architecture.

The NFV architecture (see Figure 3) defines the following main architectural elements. The Network Functions Virtualization Infrastructure (NFVI) provides the virtual resources required to support the execution of the Virtual Network Functions (VNFs). The VNF is the software implementation of a network function that runs over the NFVI. It is the entity corresponding to a function of today's network nodes, which is now expected to be delivered as a software module running independently of the hardware. The NFV Management and Orchestration (MANO) covers the orchestration and lifecycle management of physical and/or software resources in order to provide network services. The NFV MANO is composed by three elements: Virtual Infrastructure Manager (VIM), VNF Manager (VNFM), and NFV Orchestrator (NFVO).

According to the ETSI NFV specifications, a network service can be defined as the subset of the end-to-end service formed by VNFs and the associated Virtual Links (VLs) instantiated on the NFVI (see Figure 4). This procedure is also known as Service Function Chaining (SFC) [19].

On providing the network service, the NFVO plays a key role by: (i) being the single point of access for all service requests; (ii) handling the lifecycle of network services and SFCs; (iii) and having the end-to-end view of the resources being allocated across network service and VNFs by VNFMs (which handle VNFs lifecycle).

Similarities and differences between SDN and NFV are summarized in Table I.

III. SOFTWARE-DEFINED 5G RADIO ACCESS AND CORE NETWORKS

If SDN and NFV are not dependent on each other, they are certainly mutually beneficial. For this reason, the full transformative value of 5G will require the adoption at large

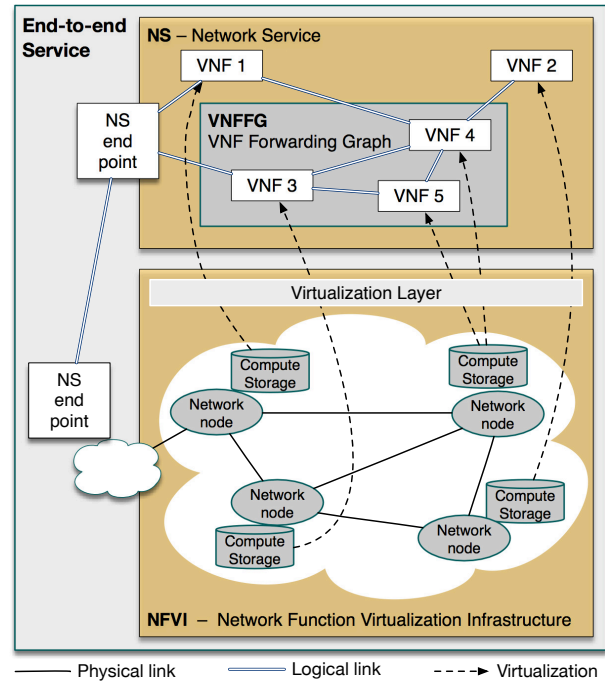


Fig. 4: Example of a Network Service (NS) as part of an end-to-end service with VNFs and a VNF Forwarding Graph (VNFFG) [20].

TABLE I: Summary of similarities and differences between SDN and NFV

Comparison between SDN and NFV	
<i>Differences</i>	<ul style="list-style-type: none"> The target of SDN is the control of the packets transmission in the network (Transmission Control) The target of NFV is the virtualization of the functionality needed to deliver a network service (Functionality Virtualization)
<i>Similarities</i>	<ul style="list-style-type: none"> SDN and NFV offer the advantage of having a better programmability and flexibility of the network, making their process more efficient and agile SDN and NFV are both software-oriented solutions, sharing the challenges of these kinds of softwareized solutions (see Section IV)
<i>Complement</i>	<ul style="list-style-type: none"> NFV and SDN can be implemented separately, but they can complement each other NFV can take advantage of SDN by concatenating network functions more efficiently (see Figure 4) SDN can take advantage of NFV by using it as one of the best use cases where transmission programmability is a big plus

scale of these two technologies to support a redesigned 5G system [21].

In the following, we first introduce the architecture of Software-Defined 5G Radio Access and Core Networks. Next, two essential aspects of the new architecture are discussed: the network slicing and the resource sharing. Finally, the current 5G testbeds are presented.

A. Architecture

As already mentioned, 5G systems must go much beyond the design of new high-speed radio interfaces. For instance, the new 5G RAN must have a high flexibility to allow operators managing a heterogeneous set of access technologies and to optimize the access according to the required service capabilities. 5G RAN is designed considering a large range of deployment scenarios, including a variety of static or moving nodes, with a much denser deployment of access points. Furthermore, 5G considers the software-defined radio access network and in particular refers to the cloud RAN (C-RAN) architectures to increase efficiency and bring down costs in future 5G RAN [22]. The C-RAN architectures offload baseband signal processing from individual Remote Radio Heads (RRHs) (i.e. the base stations in the “classical” notation) to a Baseband Unit (BBU). On one hand, this strategy allows to simplify network maintenance, to increase the efficiency of the processing resources utilization through statistical multiplexing at the BBU, to reduce costs at base station sites, to gain spectral efficiency from joint processing, such as coordinated multi-point (CoMP). On the other hand, C-RAN architectures need the deployment of a very demanding fronthaul (FH) network by transporting the raw in-phase/quadrature-phase (I/Q) samples from the RRHs to the BBUs for processing [23]. In general, current deployments use different transport networks and interfaces for FH (e.g., Common Public Radio Interface, CPRI) and backhaul (BH) traffic. However, the trend towards packet-based FH fosters a unified transport network to fulfil the requirements of all RAN splits (including regular BH traffic). Hence, recent research studies aim at designing an integrated FH and BH network architecture under the control of an SDN Transport Orchestrator [24] [25]. Furthermore, the envisaged deployment scenarios for 5G networks usually entails a variety of transport technologies that, ideally, should be managed homogeneously [26]. Hence, the general 5G RAN scenario requires an End-to-End orchestration of resources across multi-domain multi-technology transport networks (see Figure 5) for offering network slicing and vertical services. The figure depicts the system that is being studied in the 5G-TRANSFORMER project [27], which explores how network slicing can help verticals and mobile (virtual) network operators (MVNO), acting as customers, to deploy their service more quickly [28]. The system is composed of three major components: vertical slicer (VS), service orchestrator (SO) and mobile transport and computing platform (MPT). The VS coordinates and arbitrates the requests for vertical services, mapping their requirements at application level onto a set of VNF chained with each other and fine-grained instantiation parameters (e.g., deployment flavor) that are sent to the SO.

The SO provides end-to-end orchestration of services across multiple administrative domains by interacting with the local MTP and with the SOs of other administrative domains [29]. The MTP is responsible for orchestration of resources and the instantiation of VNFs over the infrastructure under its control, as well as managing the underlying physical mobile transport network, computing and storage infrastructure [4].

B. Network Slicing

Hosting different services with possibly conflicting requirements on the same infrastructure pushes for technical solutions that allow for both efficient resource sharing and multi-tenant infrastructure utilization. For this reason, one of the most promising solutions is network slicing [1], which gives to future 5G networks the scalability and flexibility features needed to support diverse services and scenarios. A network slice can generally be defined as an end-to-end logically isolated network that includes 5G devices in addition to access, transport, and core network functions.

In [30], three slice types are standardized: enhanced mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and mMTC. There can be several slices of each type and a UE should signal to which slice it should be connected when establishing a session. The network functions in a slice can be deployed differently depending on the requirements of the service. For examples, an eMBB core network function, such as a user plane function (UPF), can be deployed in a central cloud to increase scalability, whereas for a slice supporting URLLC the UPF can be deployed in an edge cloud to reduce latencies. For verticals with different needs, different network slices can be provided for each of the slice types.

The optimization of the physical network resources usage can be obtained by sharing the network functions between different slices. The abstraction of different physical infrastructures into a logical virtual network, in which VNFs are operated, allows the sharing of the physical network resources and functions between different slices. To achieve a high flexibility, which for instance allows running VNFs at various network locations, the ETSI proposes a logical reference architecture for the NFV MANO [20].

Each tenant should be able to perform both Management and Orchestration of the shared resources (e.g., transmission points, radio resources, transport and front-haul capacity, etc.) on a per-slice basis upon need. Meantime, the utilization of the physical shared resources should be maximized. Indeed, while resource pooling for storage and processing power may be less demanding due to theoretically large resource pools, the scarcity of radio resources in many cases requires an advanced resource management solution [31]. These goals can be achieved by splitting the Orchestration part in two submodules: the inter-slice and the intra-slice orchestration. The former module has a global view of the available resources, and optimally selects the resource quotas that are assigned to each slice (or tenant), exploiting the multiplexing gain. The latter module provides isolation between slices resources/functions. Thus, it performs resource orchestration on a per-slice basis, directly acting on the VNF and VIM modules.

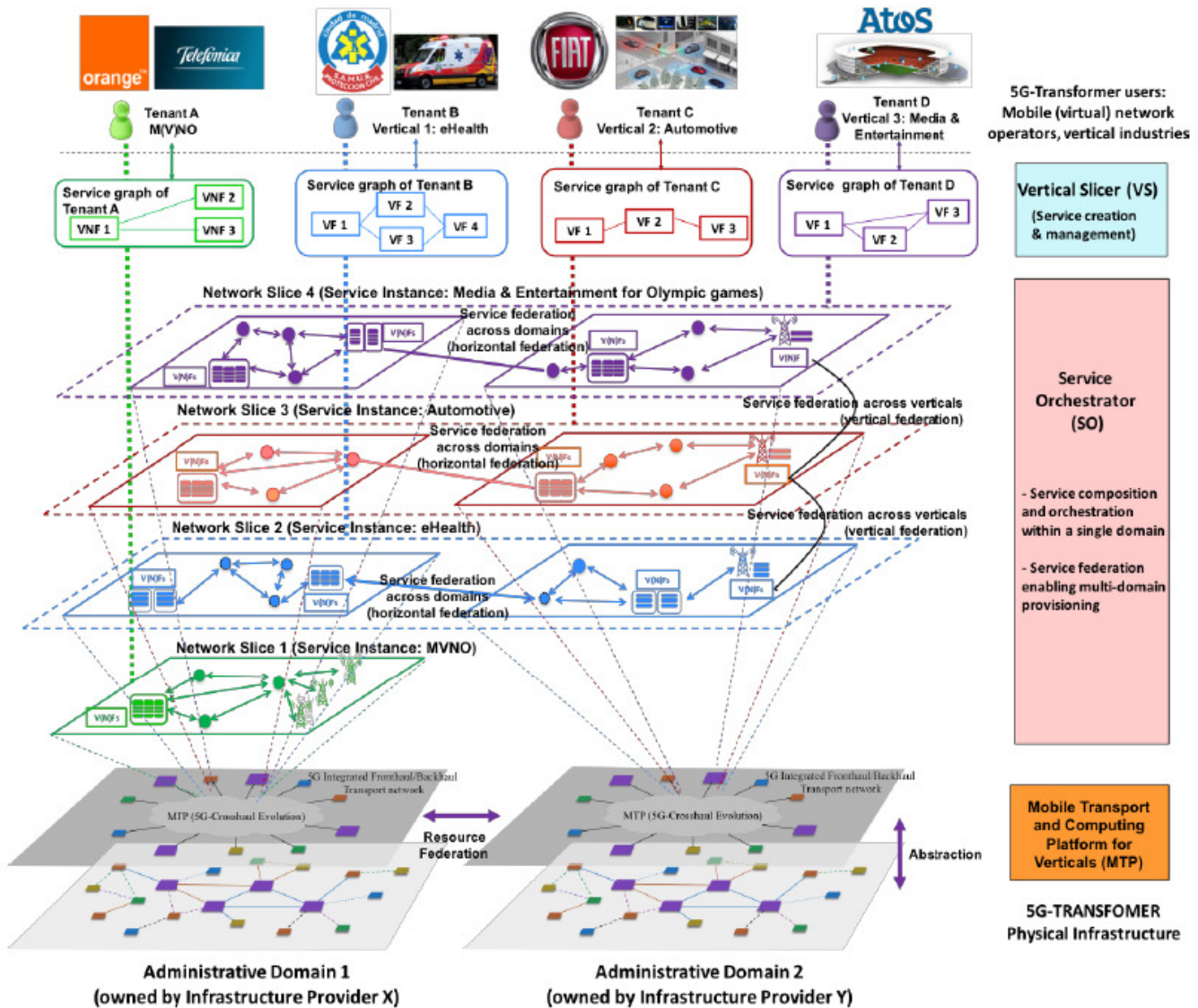


Fig. 5: 5G-TRANSFORMER initial draft architecture concept [27].

C. Resource Sharing

The support for multi-tenancy in 3GPP networks is related to early proposals on active RAN sharing, which enables network sharing based on contractual agreements. Recently, two active network sharing architectures are specified in 3GPP [32] to allow network operators to connect their own core network to a shared radio access network. These architectures are the Multi-Operator Core Network (MOCN), allowing each operator to share eNBs connected on a separate core network, and the Gateway Core Network (GWCN), where operators share additionally the Mobility Management Entity (MME). To enable Mobile Virtual Network Operators (MVNOs) to control the allocated resources, the document [33] describes concepts and high-level requirements for the Operations, Administration, Maintenance, and Provisioning (OAM&P) of network sharing.

These resource sharing architectures give the expected network utilization optimization and monetization only if traffic

and QoS control mechanisms and algorithms are added to the network infrastructure to leverage multiplexing gains of traffic among slices. SDN-based monitoring tools are necessary to acquire traffic information per slice in order to perform optimization in the resources allocated for each slice. In particular, the optimization of the physical network infrastructure usage requires new traffic control functions, such as (i) the prediction of “network slice” traffic based on measured traffic data and user mobility, (ii) the admission control for network slicing requests, (iii) the scheduling of network slicing requests in charge of meeting the agreed Service Level Agreements (SLAs), and (iv) the monitoring of traffic and KPIs for each slice.

D. Testbeds

To experimentally evaluate the performance and the functionality of the SDN/NFV 5G networks, a set of toolkits and testbeds are being available. These represent a critical

enabler of 5G evolution and allow acquiring experimental data for improving the standards and the deployment. To boost the visibility of these initiatives, the IEEE sets up an open catalogue to publicize them¹.

In the following, we describe some testbeds focused on the deployment of SDN/NFV/MEC/5G functionalities.

The 5G Berlin² is a comprehensive end-to-end testbed infrastructure relaying on multiple layers of infrastructure and software components. The testbed allows the direct integration of third party components and applications. 5G Berlin enables the setup of dedicated, specialised networks via “slicing” as required by general high-reliable networks, by automotive verticals, and by security/safety use cases. One of the two locations of 5G Berlin is 5G Playground³, which is an open testbed providing a comprehensive set of software toolkits enabling the setup and the development of 5G applications in an end-to-end testing environment. 5G Playground around the Fraunhofer FOKUS campus offers outdoor radio coverage using experimental licenses for 5G radio spectrum in the 700 MHz and 2600 MHz bands. The system combines 4G, 5G, WiFi, and LoRa WAN access technologies allowing the outdoor validation of experiments previously feasible in laboratories only.

The 5G Test Network (5gtn.fi) is one of the world’s wide 5G system with open access [34]. The 5G test system considers all aspects “from infrastructure to applications and services” and allows unique testing possibilities from prototype devices to complete solutions in a controlled environment. The testbed allows acquiring experience in testing and analysing data-intensive systems, such as 5G networks [35].

5G-EmPOWER⁴ is a Multi-access Edge Computing Operating System (MEC OS), which converges SDN and NFV into a single platform supporting lightweight virtualization and heterogeneous radio access technologies [36]. The platform allows the setup of small testbeds that can be used to implement and experimentally test algorithms and protocols, such as in [37].

Network Implementation Testbed using Open Source (NITOS⁵) is a remotely accessible and configurable testbed equipped with cutting-edge fully programmable networking equipment (LTE-A, LTE, WiMAX, WiFi, ZigBee, Software Defined Radio equipment, hardware OpenFlow switches, Cloud Computing infrastructure). The testbed is based on open-source software that allows the design and implementation of new algorithms, enabling new functionalities on the existing hardware. NITOS supports evaluation of protocols and applications under real world settings and is also designed to achieve reproducibility of experimentation.

The SoftFIRE⁶ is a federated testbed exploiting the NFV/SDN technologies for creating a secure, interoperable and programmable experimental infrastructure. The project comprises several independent testbeds that have been set up

in different EU countries. Giving the features of being a federated testbed and an orchestrated virtualization infrastructure, SoftFIRE paves the way towards the concurrent and conflict-free execution of radically different network scenarios, which can mimic network slicing. Providing the infrastructure for innovative experiments, SoftFIRE has identified and prototyped several levels of programmability that are useful for provisioning and managing 5G network slices. The project discovered and defined sets of problems to deal with during 5G network operation and offers managed solutions that are generic for NFV/SDN/5G environments. For example, in [38], the authors summarized their experimental activity aimed at designing, building, and testing a fully-functional virtualized mobile core network, pointing out lessons learned and recommendations for future improvements. In [39], the authors present the concept of a Scalable Service Function Chaining (SFC) Orchestrator capable of deploying SF Chains following the ETSI NFV architectural model, as well as orchestrating the runtime phase by rerouting the traffic to a different path in case of overload of certain SF instances.

The cooperation between Ericsson, Comau and TIM led to the realization of the proof-of-concept for the experimentation of an innovative vertical that combines robotics, machine intelligence and 5G to improve productivity in the Industrial 4.0 scenario [3]. The vertical is based on a slice supporting URLLC, where the UPF is deployed in an edge cloud to reduce latencies. The experimental system represents a key element of the factory of the future because it allows moving the control logic of robots from a control cabinet referred to as PLC (programmable logic controller) station to a cloud platform. This new approach allows easier implementation of new control features and adds high flexibility to the factory plant. By moving a relevant part of the control to the cloud enables the virtualization of those functionalities that can run as virtual machines on general purpose hardware. When new actuators are deployed, no new PLC hardware is needed. Furthermore, the flexibility is increased given that a different level of control functions (i.e. factory, cell, actuator level) can be deployed on the same platform.

IV. FUTURE RESEARCH CHALLENGES IN 5G ORCHESTRATION AND CONTROL

In the following, some of the research challenges in the 5G orchestration and control will be highlighted (see Figure 6 for a graphical summary).

The general *objectives* of 5G concern performance, dependability, energy efficiency, and economical cost reduction. The *tasks* to consider on the coordination capabilities of the orchestrator and of the controller are: to manage and orchestrate the different SDN and NFV technologies deployed; to implement a network slicing scheme that allows the efficient realization of the different expected 5G verticals; to allocate the wireless resources needed, and finally to monitor the different components of the 5G network.

There are technologies expected to deal with these functions. However, they are not yet proven to work on a scale as needed in the future 5G network. In addition, there will be

¹wiki.sdn.ieee.org

²5g-berlin.org

³5G-Playground.org

⁴5g-empower.io

⁵nitlab.inf.uth.gr/NITlab/nitos

⁶softfire.eu

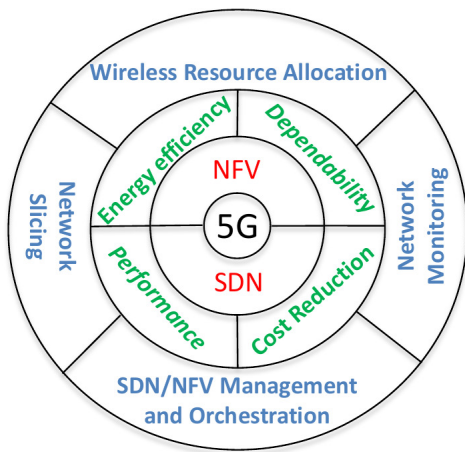


Fig. 6: Sketch of possible future research challenges – In red the softwarization technologies, in green the objectives, and in blue the tasks.

issues introduced by imperfect design, attacks and operational mistakes, tentatively in combinations, that may lead to misoperation or halt of network control and management functions. Multi-tenancy and multi-domain service management and orchestration in 5G require a tighter interaction and larger information exchange between simultaneously competing and co-operating market actors with respect to current networks. When it comes to a realization, these issues likely introduce additional constraints which will make the above outlined tasks even harder.

A. SDN/NFV Management and Orchestration

Together with the orchestration, the SDN/NFV management encompasses a wide range of tasks. SDN and NFV address different aspects of providing network-based services and may be operated independently. Their interworking with respect to Management and Orchestration (M&O) is still an open issue, where a number of options is proposed, see for instance [40], [41] for an overview. Hence, it is a prime research challenge how this best may be done, which is dependent on the networking context. From the authors' point of view, it is important to put emphasis on the provisioning of services in a multi-tenant and/or multi-domain context, such as the deployment of the virtual functions, the composition of the service function chaining and the related routing selection, etc..

The success of the network virtualization relies heavily on the M&O. The reduction of the operating costs (OPEX), by centralization and coordination, and the uniformity of the management interface as well as the automation, were the main motivations for adopting this technology. Furthermore, the increased flexibility and agility in service creation, the reduced time to market, and the ease of providing network services by simple applications are important motivations for the network virtualization. This technology is also an enabler for 5G, where network management is a core functionality in providing the network slicing, discussed in Section IV-B. However, realizing these ambitions is not straightforward and raises a number of

research challenges. Among the more important are dealing with the resulting complexity, the provision of sufficient dependability and security, and the ability to provide compound services based on co-operation of several market actors using a common physical infrastructure. These are briefly discussed below.

Complexity: Even though the management responsibility for the various parts of the network and service provisioning is well defined in the SDN and NFV architectures (see for instance Figure 3), the entire complexity of the M&O will increase significantly. This has many causes such as for instance: (i) the control and management activity is moved to separate platforms that must also be managed, see e.g. [42], [43] (ii) the system is in general multi-vendor, (iii) implementing the improved functionalities of the M&O causes additional complexity, etc. (iv.) efficient allocation, management and control of assigned resources in real-time, as presented for instance in [44]. Finally, continuous dynamic adaptation to changing workloads, new services, failures and repairs, and simultaneously provide service continuity amplify the challenges.

Most challenging is perhaps the dealing with the 5G slicing, where the different slices should provide services with highly differing requirements with respect to functionality, latency, reliability, security, latency and capacity. There is a number of fundamental questions on how to obtain efficient resource utilization, guaranteed QoS and proper isolation between slices. Some works proposed to use Artificial Intelligence and machine learning to deal with these issues, see for instance [45], [46]. However, these techniques are unproven and their ability to deal with unforeseen catastrophic events are questioned. This last aspect may be in opposition to the requirement of dependable and secure services, as discussed next.

Dependability and security: The SDN and NFV based 5G network will be a critical infrastructure in itself and will likely become a part of other critical infrastructure as energy (power) supply, payments, transport, etc.. The requirements for the dependability and the security of the services provided will be high, for some services. For instance, in the case of operation of autonomous vehicles, an outage or widespread malfunctioning of the network could provide catastrophic effects, [47]. Therefore, the network management should have functionality to meet these requirements.

A centralized management with knowledge of global state and control over the resources represents a good basis for dealing with most "everyday" failures of physical infrastructure elements, as well as crash failures of VNFs. The impact of such failures on the dependability is expected to become less than in the current system. However, little attention has been paid to failures of the M&O systems itself. These are likely to be unexpected and unforeseen 'black swan' type of failures, caused by the complexity of the system and its composition of software elements from a number of different vendors. Those non-conventional failures are hard to deal with, and may yield severe outages [42], [48]. Misoperation of M&O may have severe network-wide consequences. Significant effort must be put into designing an M&O system that is able to deal with failures of the platform where it is executed, including

its internal logical and configuration faults. Most important, it must not execute incorrect actions. Hence, it should be designed to have failure omission semantic [43].

In part, these challenges are due to the shift in paradigm from the current networks, whose basic design philosophy is to make it distributed with autonomous network elements giving an inherent robustness [49], to the logically centralized control and management of the emerging SDN-NFV.

The logical centralization does also yield an increased security risk. With respect to consequences, rather than “capturing” a single network device, an intruder has the potential to capture the entire network. Gathering all activities on the same platform increases the potential for illegal monitoring and the likeliness of intrusions. This is due to the increased complexity and the interaction between software from various vendors, which may incur into vulnerabilities that are hard to detect. There are efforts toward dealing with the threats to the security, see [50], [51].

Multi-actor issues: The Software-Defined 5G is expected to be multi-tenant, i.e., a number of autonomous network operators and service providers share the same physical infrastructure and computational platform. Furthermore, the service are expected to be provided by operators and providers in different domains, e.g., access domain, one or more core network domains and content provider domain. The network M&O has to deal with corresponding multi-tenant and multi-operator issues, as illustrated Figure 7. To be able to do that, there has to be an overall architecture in place that enables co-operation and coordination. In addition to the technical aspects, economic and legal issues must be dealt with in SLAs which get an increasingly important role, [52]. These issues have been addressed by a number of fora, projects and researches, see for instance [41], [53], [54], [55], [56]. However, no overarching outcome is seen, and this is still a major research challenge that must be resolved before the vision of 5G becomes a reality.

As discussed in [43], to deal with the issues raised in this subsection, more attention should be placed on the shift in risk profile, i.e., the use of virtualization may reduce the frequency and consequences of “everyday failures”. At the same time, this increases the probability and consequences of the unforeseen events that the system and operation and maintenance organizations are not prepared to deal with, the so called black swans [57]. Measures that should be considered is to design critical M&O functions so it may be guaranteed that they do not mis-operate, for instance by logical fault tolerance or giving them failure omission semantics, and to separate critical M&O from the infrastructure they manage to avoid mutual dependencies [43]. Other means that are important for the SDN/NFV M&O is the ability to manage the software unreliability, [58], [59], and to avoid dependent failures [48].

B. Network Slicing

Network slicing proposes the splitting of common physical infrastructure and virtual resources in isolated sub-groups (slices) able to provide independent specific network capabilities by fulfilling specific requirements that can be tailored

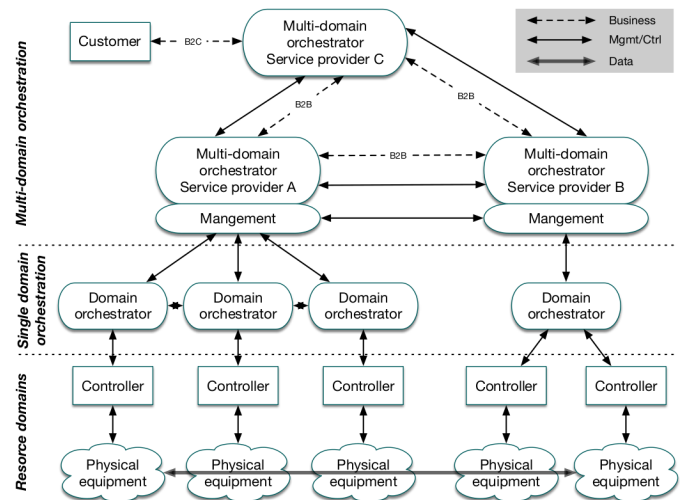


Fig. 7: Multidomain end-to-end M&O from [53].

according to the needs. Each network slice is an isolated logical network, tailored to different functional and performance requirements, running on a common virtual and physical infrastructure. For the sake of illustration, we mention some relevant slice types defined in [60]: (i) enhanced mobile broadband; (ii) massive machine-type communication; and (iii) ultra-reliable low-latency communication.

SDN and NFV are concepts that are fundamental for network slicing. Hence, the latter inherits most of the challenges presented previously. In terms of *complexity*, network slicing needs to have control on: resources at the access, transport and core network, edge and central cloud computing, and SDN Controller and NFV Orchestration functionalities. Therefore, the complexity of each of these components is inherited, with still many open issues. In addition, the main factor that makes network slicing very complex is the fact that it needs to articulate and integrate all those individual components, in order to offer the expected highly differentiated requirements of each slice. The perfect coordination required for that is a considerable extra challenge that must be addressed. *Dependability and security* is also a top priority here. In fact, some slices are expected to deliver Ultra-Reliable Communication (URC) with reliability requirements above 99.999%, as it was explicitly stated in the 5G vision [61]. As described for SDN and NFV, the dependability of network slicing should have two focuses. First, the dependability of the slices and services offered, where the network slice control and management play an important role. Second, the dependability of the network slice control and management components as such. A dependable network slicing scheme depends on the design of the adequate reaction mechanisms for recovery, based on accurate information of the failure events and the current state of the system. However, due to the size and complexity, having proper and reliable information demands a system with the smartness to efficiently detect and filter all the reported events, which is still an open issue. Finally, the *multi-actor issues* challenge is the essence of network slicing and hence, this is a challenge that is in its nature. In this section, we will

complement this issue by addressing the *isolation* challenge, which is closely related.

In addition to the challenges inherited from SDN and NFV, network slicing has some additional considerations that must be addressed.

Slice isolation: Isolation is the most important property of Network Slicing, but also the one that represents the main challenge for its realization. Slices should be independent and have an appropriate degree of isolation from each other, so that no slice can interfere with the traffic in another slices or in general all type of events should not propagate among them. First, it is important to notice that isolation is a set of several tools that can be selected and tuned in order to achieve the isolation desired on the different use cases. Isolation can be classified in 4 different areas [62]: traffic, bandwidth, processing, and storage isolation. Some of the methods available for achieving isolation are: language and sandbox based isolation for service instances and network slice instance, and for lower levels, approaches such as virtual machine and kernel based isolation, Physical Resource Block (PRB) scheduling, Channel Access Control, SDN-based isolation, hardware and physical isolation, etc [62]. In this context, the main challenge is the orchestration and control tasks that need to be implemented in order to harmonize the different isolation techniques in the different domains, in order to fulfil the requirements of each specific slice. This is even more complex due to the fact that there is not a holistic and final standardized network slice architecture, which keeps open the control and orchestration of unknown isolation techniques. Also, isolation techniques significantly rely considerably on SDN functionalities, but as it is explained in [62], some of these functions are not yet mature. Security and access control are also some of the isolation requirements that need to be enhanced, since for instance, devices from group 1 should have access to slice A and B, but never to slice C, which in practice demands diverse architectural and security considerations. Finally, the inclusion/exclusion of new slices is challenging in terms of isolation, since it has to guarantee that those kinds of procedures do not have any effect on the currently running slices. This demands an updated information of the network status and the proper estimation of all the implications of including/excluding components, in order to avoid undesirable side effects on operational services.

Standardized architecture: Another important challenge that needs to be addressed is the definition of a standardized network slicing architecture. The motivation, expectations and requirements of network nlicing are clear. However, the definition of a unified architecture with respective standards is still work in progress. The formalization of this concept was presented in [63], where a three-layer scheme is proposed (Service Instance, Network Slice Instance, and Resources). There are also efforts on standardization such as [64], [65] and [60], with important definitions such as: (i) the *Network Slice Management and Orchestration* block with a set of functions and subcomponents; (ii) the definition of sub-domains such as edge and central cloud solution, fronthaul, backhaul and core network; and (iii) initial definitions of the roles of SDN and NFV into the overall slicing scheme. Finally, some other works that contribute with valuables architectural

concepts can be found in [66], [67], [68], where details, such as the need of different control domains (global and specific), and the illustration of some specific slice orchestration workflows that include the SDN controller and the NFVO, are addressed. Despite all the different efforts made by industry, academia and standardization units, there is no concrete consensus on a final standardized network slicing architecture. However, the mentioned works are just a small subset of all the big efforts currently running and that will come in order to progress in this direction.

Performance: The performance offered by virtualized systems has been from the very beginning one of the main concerns for its implementation [69]. Therefore, in most of the ETSI-NFV proof of concepts [70], performance has been one of the first issues to test. Through the years, many of those tests have been successful, but each case must be tested separately, based on the specific technical characteristics and requirements. Performance issues need to be assessed at both the control plane [71] and at the data plane, where for instance, the need to meet the performance requirements has promoted the introduction of acceleration modules, such as DPDK (Data Plane Development Kit) [72], [73]. However, challenges such as increased complexity, the respective VNF validation and the live migration implementation when using DPDK still need to be investigated.

One of the concepts that may make very challenging the performance issue is the 3GPP proposal on recursive network slice [60], which is a concept that provides the ability of creating new slices from one that has been created and assigned. This in principle provides a higher flexibility and opens new business opportunities. However, as mentioned in [74] and [75], these types of nesting approaches have a negative impact which needs to be thoroughly assessed case by case.

Resource optimization: Under normal operations, it is expected that the potential combinations of network services and the respective resources assigned to them will be huge, and hence their distribution needs to be properly planned. The efficient use of the resources that a network operator has available is one of the main motivations for network slicing. Therefore, such planning must have optimization as one of its main strategies. The coming 5G networks are expected to have the capability to scale up and down at any time the deployed services, enable fast testing of new ideas, and in general be programmable and flexible to any new coming businesses and services. On the other hand, the amount of resources that need to be managed and assigned may be considerably large and diverse. In conclusion, for the implementation of network slicing is important to have clear policies and plans for the assignment of resources that: (i) enable cost efficient operations for the Network Providers; (ii) provide agile solutions that enable quick implementations; and iii) are capable to adapt to the varying conditions of the network slice environment.

Slices management hierarchy: The management and orchestration of slices can be classified in two big groups: inter-slice and intra-slice management. One of the challenges in this regard is the interaction and distribution of domains and responsibilities between them. On one hand, it can be

mentioned a *global management* of the entire network slice system, where despite the local managers, the central entity may have strong influence over all the components inside the existing slices. On the other hand, the *local-slice management* may have full autonomy and control of all the resources assigned inside a specific slice and its respective operation, so it never gets any type of interference from the global entity. Having a global management with decision over the entire system (including the resources already assigned to the slices) is a scheme that allows better control and a more flexible use of the resources. However, this goes against the principle of the slices independence. Under some circumstances (failures, emergencies, special events, etc), a bigger management capability of the global management is needed, being necessary a design that finds the right balance between these two options.

Table II presents the tradeoff of those two types of slice management hierarchies. However, today, it is not clear what should be the right level of influence of the global management on the local slices. This is a topic that needs to be analyzed and addressed, so future implementations may have clear procedures in this regard.

TABLE II: Trade-offs in the hierarchy of the M&O of slices

Full isolation in M&O of each slice	Pro-fused (global/local) M&O
<ul style="list-style-type: none"> • Dependability (avoiding error and failure propagation between slices) • Easier to guarantee QoS • Easier SLA handling (fewer parties and more control of resources) • Independence between and autonomy of tenants • Simpler and less failure prone M&O • Limited cross tenant orchestration 	<ul style="list-style-type: none"> • Better utilization of physical resources • Better utilization of available spectrum • Increased flexibility in dealing with unforeseen changes of traffic and configuration (failures) • More flexibility in adopting new slices/service types

C. Wireless Resource Allocation

A set of tasks that should be considered in the orchestration and control of Software-Defined 5G Radio Access Networks is the wireless resource allocation, which includes user association, power control, and channel selection.

User association in 5G is more complex than in current cellular network. In existing systems, a user is associated with a base station, mainly based on the received power from the surrounding base stations. Instead, 5G user association will exploit the multiple technologies that will compose the RAN: the user can be associated with a macro-cell, a small-cell, a relay, another user device (i.e. D2D communication), or even multiple combinations of them (i.e. CoMP).

User association in 5G has attracted strong interest in the past few years and a few surveys are already present in the literature [76] [77]. Current works are focusing on optimizing specific criteria, such as energy consumption, channel condition and bandwidth, interference, and load, and by using different approaches, such as stochastic geometry, combinatorial optimization, and game theory. In some of the current works,

the user association has been jointly addressed with other tasks. As in other wireless contexts, the use of interdisciplinary approaches will be important for the development of efficient and profitable algorithms [78][79][80].

Power control is one of these tasks. The power control consists of selecting the transmission power of the base station, which includes also powering it off. For this reason, it is often related to energy efficiency optimization [81]. A coordinated user association and power control is important because the variation of the transmission power of a base station affects the reachability and the data rate between a potential user and the base station [82]. An effective power control will need an accurate power model of all the transmission entities [83] in order to allow the development of performing algorithms [84].

Channel selection is another task which is important together with user association and power control for the interference management [85]. In 5G, the selection of the frequency channel is especially critical because of the high densification [86]. Moreover, one important 5G application will be IoT, where technologies, such as Cognitive Radio Network (CRN) and Software-Defined Radio (SDR), will enable advanced radio spectrum management [87].

Despite the effort of the research community, there are still several challenges that need to be addressed in the above tasks:

- The architecture considered in the current works does not usually include all the 5G radio access technologies. Moreover, future works should consider the SDN/NFV operation and management in both access and core networks. The impact of CRN and SDR on accomplishing the above tasks should be also further considered.
- Modelling a generic 5G channel is still an open issue due to the complexity of the 5G scenario, which includes innovative transmission technology, such as massive MIMO, NOMA, and mmWave. Furthermore, a related challenge is the development of learning algorithms for the dynamic management of the spectrum.
- Another aspect is related to the target of the allocation. In the current works the target has mainly been energy efficiency [88][89]. However, multiple targets need to be taken into account. They can be considered as a constraint, e.g. for avoiding that the reduction of active resources for energy efficiency purposes affects the dependability in case of failures or unexpected changes of traffic pattern.
- The targets of the wireless resource allocation depend on the type of application, and 5G network slicing will enable the provision of heterogeneous network services with different technical requirements. Since the 5G application will (partially) share the same resources of the radio access and mobile core network, the related allocation problem will be complex.
- Another aspect that needs to be further investigated is the different time scale of the approaches. The allocation methods can be applied at different intervals of time: real-time, daily fluctuation, long-term. The different approaches can be complementary and can focus on different scales (global/local).

Caching is a new opportunity in 5G wireless resource allocation, which researchers are working at [90] [91]. The idea is to offload traffic by caching contents in the edge (i.e. radio access) of the network, such as the different base stations, the relays, and potentially even in the end-user devices. Traffic offloading will enable to face the increase of traffic demand and achieve better Quality of Experience (QoE) [92].

In this scenario, the content placement [93] is a relevant task that researchers are working on. In particular, researchers are working on Mobile Edge Computing (MEC) [94] and on what, where, when, and how to log cache contents. In this context, coding [95] and machine learning [96] techniques can be applied. Example of typical scenarios are vehicular communications [97] and low latency applications [98].

At the best of our knowledge, a task that has not been yet investigated is the content delivery of the cached contents. Once decided what and where to cache, the retrieval of the content can be jointly realized through the wireless resource allocation in order to achieve content awareness [99].

The objectives of wireless resource allocation are broad and challenging, and having an inter-disciplinary (i.e. signal processing, networking, operation research) approach can be a valuable option.

D. Network Monitoring

The huge advance brought by the whole 5G ecosystem raises a number of technological challenges that strongly require an accurate knowledge of the status of the network, in terms of both operational conditions and traffic information. The motivations for network monitoring and measurements are manifold and span from the need to gather low level performance indicators to higher level information for user profiling and defence against cyber attacks.

Troubleshooting has been traditionally one of the key repellent for traffic monitoring. As of today, it is frequent practice for large scale operators to outsource the management of their communication infrastructures to the manufacturers that provided the network devices. However, the operators themselves are interested in either developing their own monitoring instruments or acquiring third party tools to check the status of their own networks as well as to verify the adherence with the operational conditions specified in the contracts with the manufacturers.

Performance metrics are also crucial in the 5G technological context that proposes extremely stringent constraints. Indeed network QoS parameters such as packet loss, available bandwidth, end-to-end latency must be constantly monitored to verify and promptly react against the performance degradation and to assess SLAs fulfilment. The latter reason is particularly relevant as multi-tenancy and network slicing will be common practices in the 5G operational scenario, and contract verification as well as slice planning will ultimately require real-time traffic information.

At higher level, traffic monitoring will definitely address the evaluation of the *user experience* and *profiling*. In particular, traffic classification plays a key role as the fine grained knowledge of the users behavior allow network operators huge opportunities for highly customized offers.

Finally, though perhaps most important, traffic monitoring becomes crucial to defend the whole communication infrastructure against cyberattacks, whose effects are even magnified in highly interconnected systems. The evidence of such issues is in everyday's news as, in 2017 only, cybercrime reportedly hit more than a billion people in the world and caused damages for around 500 billion dollars [100].

Nowadays, cyberthreats are continuously mutating into sophisticated, stealthy, targeted, and multi-faceted attacks to penetrate systems, study the critical components, impact their operations, and minimize the ability of the users to report the system's malfunction. As an example, this is the case of Advanced Persistent Threats (APTs), in which the attacker is tasked to perform an attack and will use any technique, over long periods of time, until the target is finally accomplished.

Scalability: The advent of 5G cellular network will further fuel the rapid increase of network traffic volume which will be soon measured in Zettabytes (1 billion terabytes) [101], with more than 20 billion connected devices forecasted by 2020 [102]. From this astonishing figures, scalability emerges as a primary issue, and clearly makes traditional monitoring approaches based on capture, storage and post-processing of data practically infeasible and obsolete. Indeed, the large volumes of traffic require the network nodes themselves to be the first monitoring players, by at least providing a first stage of coarse-grained processing over the live data, while delegating more sophisticated analysis to a second tier of specialized systems, such as middleboxes, Security Information and Event Managements (SIEMs), Deep Packet Inspection (DPI) modules, etc. This approach is perfectly in line with the SDN paradigm and the newly introduced flexibility may in fact readily enable the integration of monitoring capability into programmable nodes. As a result, network devices such as programmable switches or network interface cards, while being originally designed for performing network packets forwarding, can be *repurposed* to accommodate even complex monitoring tasks. In other words, network monitoring will not make an exception and will be treated as one of the network functions envisaged in the SDN/NFV model.

Programmable data plane: In the SDN model, network monitoring applications will have a portion of their logic offloaded to the programmable network devices. Processing in the infrastructure nodes will be instantiated through the SDN control plane (that still retains the full ownership of the process) by *delegating* tasks across the network nodes. In other terms, the underlying data plane will provide an Application Programmable Interface (API) to expose the set of supported monitoring (or, more generally, processing) *primitives* as well as a formal way of combining such instructions. In fact, this approach follows the one originally proposed by OpenFlow, which pragmatically adopts a simple Match-and-Action programmable abstraction, and more recently by P4 [103] that, instead, improves the programmability of packet processing pipelines through dedicated processing architectures or Reconfigurable Match-Action Tables as an extension of TCAMs (Ternary Content Addressable Memories). However, when the processing scope becomes more complex and (as in the network monitoring domain) possibly involves

stateful operations, the programming abstractions inherited by the switching domain show significant limitations and more sophisticated approaches, such as the one based on eXtended Finite State Machines (XFSM) [104], prove better potentials.

On the user side, the monitoring applications running on the end hosts will refine and complement the monitoring activities upon the data received from the inner nodes. At this stage, they may run algorithms and analytics in a centralized fashion on the received subset of pre-digested data, with beneficial effect in terms of accuracy and overall scalability.

Data analysis and protection: The types of applications and services that may benefit from the new programming paradigm is virtually unlimited. As an example, in the security domain, the model easily translates in distributed agents running locally on the nodes that continuously look for signals and threats. Once a signal is detected, the system dynamically “zooms” into the nodes that are interested by the suspected threat, collects the data and centrally runs more sophisticated analysis, such as anomaly detection, visualisation tools and threat analysis techniques and methods. The scope of applications can be further extended to include more traditional monitoring issues that require updated information about the network status, as in the recent P4-based *In-Band Network Telemetry (INT)* proposal [105] and in the ETSI driven *iOAM* [106] approach.

Typically, the centralized network element devoted to run fine-grained data analysis and visualization is the SIEM. In the heterogeneous 5G ecosystem, SIEMs are indeed expected to receive a large amount of data from different types of distributed sensors, including the less traditional outcomes of behavioral and sentiment analysis tasks. Therefore, they must address *data homogenization*, *aggregation* and *correlation*, as well as the adoption of suitable algorithms for big data analysis to provide the “visual awareness” of the infrastructure status.

SIEMs will also play a central role in Digital Forensics (DF) investigations and will be the technical basis for post-mortem analysis in forensic procedures by facilitating the DF process in determining significance, reconstructing data fragments of data and drawing conclusions based on the collected evidences. However, for the above process to be effective and deployable, a particular care must be dedicated to the *lawful implications* involved in monitoring of the infrastructure and collection of data in order not to infringe fundamental rights of potentially involved citizens, and to guarantee user’s privacy and data protection. As such, SIEMs will be called to implement proper techniques of *data protection and anonymization* as well as to conform to the international, European, national and local laws, rules and regulations.

E. Discussion

Ideally, the target of the research in the orchestration and control of software-defined 5G radio access and core networks is to find the optimization mechanism that dynamically allocates the resources associated with the tasks discussed in this section, and at the same time, ensure that the requirements of the services are met and that the operation is within the commercial constraint set by the market actors. In doing so, the researchers will initially focus on subsets of the objectives

and tasks, i.e. specific subset of the tasks-disc presented in Figure 6. Simultaneously, meeting the strictest requirements of all the applications is either infeasible (given the inherent trade-off between them) or, when feasible, techno-economically inefficient. Hence, there must be specific optimization objective for each application, and it must be assured that a global optimality is sought for the entire system, which is the main challenge for the orchestration and control. In general, a cross-layer and inter-disciplinary approach will be needed for obtaining solutions that are both practical and effective, and thus profitably applicable in the real world.

On the other hand, today it is clear that SDN, NFV and network slicing will be key concepts to achieve the 5G vision. Those technologies have been studied and tested during the last years, and have achieved a reasonable level of maturity. However, there are still many open issues that need to be addressed, such as the definition of an overall architecture of the holistic system, or the evaluation and testing that provide the confidence needed for an implementation phase.

Table III summarizes the above discussed challenges to motivate future works that lead to a successful 5G implementation.

TABLE III: Summary of main Future Research Challenges in 5G Orchestration and Control

5G Task	Challenges
<i>SDN/NFV M&O</i>	Complexity; Dependability and security; Multi-actor issues;
<i>Network Slicing</i>	Complexity; Dependability and security; Multi-actor issues; Slice isolation; Standardized architecture; Performance; Resource optimization; Slice management hierarchy;
<i>Wireless Resource Allocation</i>	User association; Power control; Channel selection; Caching; Impact of CRN and SDR; Dynamic management of the spectrum;
<i>Network Monitoring</i>	Measurements for troubleshooting; Performance metrics; User experience and profiling; Scalability; Programmable data plane;

V. CONCLUSIONS

This paper has presented the software-defined 5G radio access and core networks from a general up-to-date point of view by including both the enabling softwarization technologies, SDN and NFV, and the innovative wireless technologies, such as multi-RAT, multi-tier architecture, and CoMP and D2D communications.

The future research challenges in the orchestration and control has been highlighted. Different objectives, e.g., energy efficiency, dependability, performance, and cost reduction, have been considered, and different tasks, i.e., SDN/NFV management and orchestration, network slicing, wireless resource allocation, and network monitoring, has been investigated.

The paper shows how the orchestration and control of 5G systems are important to effectively coordinate and exploit the full potential of the 5G technology and identifies a number of fundamental issues that need to be resolved. Further efforts are needed to develop algorithms and methods that are able to manage the resources and provide advanced, dependable 5G services with appropriate QoS to the end users, and yield a cost efficient system.

In general, 5G networks are close to become a reality, thanks to the technological maturity and the numerous efforts that have been made during the last years. However, the challenges presented here show that additional efforts are still needed.

ACKNOWLEDGMENT

This work has been partially supported by the PRA 2018-2019 research project “CONCEPT – COMMUNICATION and NETWORKING for vehicular CybEr-Physical systems” funded by the University of Pisa.

REFERENCES

- [1] NGMN Alliance. (2015) 5G White paper. [Online]. Available: https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf
- [2] 5GPPP. (2016) 5G PPP use cases and performance evaluation models. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-use-cases-and-performance-evaluation-modeling_v1.0.pdf
- [3] P. Sabella, A. Thuelig, M. Carrozza, and M. Ippolito, “Industrial automation enabled by robots, machine intelligence and 5g,” *Ericsson Technology Review*, no. 2, pp. 2–12, February 2018.
- [4] P. Iovanna, T. Pepe, C. Guerrero, F. Moscatelli, A. Ksentini, C. F. Chiasserini, C. Casetti, J. Mangues-Bafalluy, L. Valcarengi, B. Martini, X. Li, and G. Zennaro, “5g mobile transport and computing platform for verticals,” in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, April 2018, pp. 266–271.
- [5] 3GPP, *Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description*, 3GPP TS 38.300 V15.1.0, Dec. 2017.
- [6] P. Marsch, I. D. Silva, O. Bulackci, M. Tesanovic, S. E. E. Ayoubi, T. Rosowski, A. Kaloxylas, and M. Boldi, “5g radio access network architecture: Design guidelines and key considerations,” *IEEE Communications Magazine*, vol. 54, no. 11, pp. 24–32, November 2016.
- [7] A. Maeder, A. Ali, A. Bedekar, A. F. Cattoni, D. Chandramouli, S. Chandrashekar, L. Du, M. Hesse, C. Sartori, and S. Turtinen, “A scalable and flexible radio access network architecture for fifth generation mobile networks,” *IEEE Communications Magazine*, vol. 54, no. 11, pp. 16–23, November 2016.
- [8] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, “NFV and SDN – key technology enablers for 5G networks,” *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2468–2478, Nov 2017.
- [9] G. Nencioni, R. G. Garroppo, A. J. Gonzalez, and B. E. Helvik, “Orchestration and Control in Software-Defined 5G Radio Access Networks,” in *9th Nordic Workshop on System & Network Optimization for Wireless (SNOW 2018)*, Feb 2018.
- [10] T. O. Olwal, K. Djouani, and A. M. Kurien, “A survey of resource management toward 5G radio access networks,” *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1656–1686, thirdquarter 2016.
- [11] Horizon 2020, “The BEBA (Behavioral Based Forwarding) project.” [Online]. Available: <http://www.beba-project.eu/>
- [12] F. Fusco and L. Deri, “High speed network traffic analysis with commodity multi-core systems,” in *Proc. of IMC '10*. ACM, 2010, pp. 218–224.
- [13] L. Rizzo, “Netmap: a novel framework for fast packet i/o,” in *Proc. of USENIX ATC'2012*. USENIX Association, 2012, pp. 1–12.
- [14] Linux Foundation, “DPDK – Data Plane Development Kit.” [Online]. Available: <http://dpdk.org>
- [15] N. Bonelli, S. Giordano, G. Procissi, and L. Abeni, “A purely functional approach to packet processing,” in *Proceedings of the Tenth ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, ser. ANCS '14. New York, NY, USA: ACM, 2014, pp. 219–230.
- [16] N. Bonelli, S. Giordano, and G. Procissi, “Network traffic processing with PFQ,” *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 6, pp. 1819–1833, June 2016.
- [17] E. L. Fernandes (Ed.), “OpenFlow 1.3 Software Switch (OF-SoftSwitch),” <https://github.com/CPqD/ofsoftswitch13>.
- [18] N. Bonelli, G. Procissi, D. Sanvito, and R. Bifulco, “The acceleration of ofsoftswitch,” in *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Nov 2017, pp. 1–6.
- [19] J. M. Halpern and C. Pignataro, “Service Function Chaining (SFC) Architecture,” RFC 7665, Oct. 2015. [Online]. Available: <https://rfc-editor.org/rfc/rfc7665.txt>
- [20] Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG), “ETSI GS NFV-MAN 001 V1.1.1: Network Functions Virtualisation (NFV); Management and Orchestration,” *Tech. Rep.*, Dec. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001099/001/01.01.0160/gsNFV-MAN001v010101p.pdf
- [21] 5GPPP – Software Networks WG. (2017) Vision on software networks and 5G. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_SoftNets_WG_whitepaper_v20.pdf
- [22] A. Checko, “Cloud RAN for mobile networks—a technology overview,” *IEEE Commun Surv Tutorials*, vol. 17, 2015. [Online]. Available: <https://doi.org/10.1109/COMST.2014.2355255>
- [23] J. Bartelt, N. Vucic, D. Camps-Mur, E. Garcia-Villegas, I. Demirkol, A. Fehske, M. Grieger, A. Tzanakaki, J. Gutiérrez, E. Grass, G. Lyberopoulos, and G. Fettweis, “5g transport network requirements for the next generation fronthaul interface,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, p. 89, May 2017.
- [24] EU H2020 5G Crosshaul, “The integrated fronthaul/backhaul project,” 2017. [Online]. Available: <http://http://5g-crosshaul.eu/>
- [25] J. Baranda, J. Nez-Martnez, I. Pascual, J. Mangues-Bafalluy, A. Mayoral, R. Casellas, R. Vilalta, R. Martnez, R. Muoz, J. X. Salvat, A. Garca Saavedra, X. Li, and J. Kocur, “Resource management in a hierarchically controlled multi-domain wireless/optical integrated fronthaul and backhaul network,” in *IEEE Conference on Network Function Virtualization and Software Defined Networks*, November 2017.
- [26] P. Chanclou, L. A. Neto, K. Grzybowski, Z. Tayq, F. Saliou, and N. Genay, “Mobile fronthaul architecture and technologies: A RAN equipment assessment [invited],” *IEEE/OSA Journal of Optical Communications and Networking*, vol. 10, no. 1, pp. A1–A7, Jan 2018.
- [27] H2020 5G-TRANSFORMER project: Report on vertical requirements and use cases. [Online]. Available: http://5g-transformer.eu/wp-content/uploads/2017/12/Report_on_vertical_requirements_and_use_cases.pdf
- [28] C. Casetti, C. F. Chiasserini, T. Dei, P. A. Frangoudis, A. Ksentini, G. Landi, X. Li, N. Molner, and J. Mangues, “Network slices for vertical industries,” in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, April 2018, pp. 254–259.
- [29] X. Li, J. Mangues-Bafalluy, I. Pascual, G. Landi, F. Moscatelli, K. Antevski, C. J. Bernardos, L. Valcarengi, B. Martini, C. F. Chiasserini, C. Casetti, D. Andrushko, N. A. Serrano, and A. Ksentini, “Service orchestration and federation for verticals,” in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, April 2018, pp. 260–265.
- [30] 3GPP, *Technical Specification Group Services and System Aspects; System Architecture for the 5G System*, 3GPP TS 23.501 V15.2.0, June 2018.
- [31] V. Sciancalepore, K. Samdanis, X. Costa, D. Bega, M. Gramaglia, and A. Banchs, “Mobile traffic forecasting for maximizing 5G network slicing resource utilization,” in *IEEE INFOCOM*, May 2017.
- [32] 3GPP, *Network Sharing; Architecture and Functional Description*, 3GPP TS 23.251 V14.1.0, Sept. 2017.
- [33] —, *Telecommunication management; Network Sharing; Concepts and requirements*, 3GPP TS 32.130 V14.1.0, Jan. 2018.
- [34] E. Piri, P. Ruuska, T. Kanstrn, J. Mkel, J. Korva, A. Hekkala, A. Pouttu, O. Liinamaa, M. Latva-aho, K. Vierimaa, and H. Valasma, “5gtn: A test network for 5g application development and testing,” in *2016 European Conference on Networks and Communications (EuCNC)*, June 2016, pp. 313–318.
- [35] T. Kanstrn, “Experiences in testing and analysing data intensive systems,” in *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, July 2017, pp. 589–590.
- [36] R. Riggio, M. K. Marina, J. Schulz-Zander, S. Kuklinski, and T. Rasheed, “Programming abstractions for software-defined wireless networks,” *IEEE Transactions on Network and Service Management*, vol. 12, no. 2, pp. 146–162, June 2015.
- [37] D. Harutyunyan, S. Herle, D. Maradin, G. Agapiu, and R. Riggio, “Traffic-aware user association in heterogeneous lte/wifi radio access networks,” in *2018 Proc. of IEEE NOMS*, April 2018.
- [38] D. Lake, G. Foster, S. Vural, Y. Rahulan, B. H. Oh, N. Wang, and R. Tafazolli, “Virtualising and orchestrating a 5g evolved packet core network,” in *2017 IEEE Conference on Network Softwarization (NetSoft)*, July 2017, pp. 1–5.
- [39] A. M. Medhat, G. A. Carella, M. Pauls, and T. Magedanz, “Orchestrating scalable service function chains in a nfv environment,” in *2017*

- IEEE Conference on Network Softwarization (NetSoft)*, July 2017, pp. 1–5.
- [40] M.-P. Odiñi, “SDN in NFV architectural framework,” *IEEE Softwarization*, May 2016. [Online]. Available: <https://sdn.ieee.org/newsletter/may-2016/sdn-in-nfv-architectural-framework>
- [41] C. J. Bernardos, A. Rahman, J. C. Zuniga, L. M. Contreras, P. Aranda, and P. Lynch, “Network virtualization research challenges,” IETF, Internet-Draft; Informational draft-irtf-nfvrg-gaps-network-virtualization-08, November 29 2017.
- [42] P. E. Heegaard, B. E. Helvik, and V. B. Mendiratta, “Achieving dependability in software-defined networking - a perspective,” in *7th International Workshop on Reliable Networks Design and Modeling [RNDM’15]*, Munich, Germany, October 5-7 2015, p. 7.
- [43] A. J. Gonzalez, G. Nencioni, A. Kamisinski, B. E. Helvik, and P. E. Heegaard, “Dependability of the NFV orchestrator: State of the art and research challenges,” *Accepted for publication in IEEE Communications Surveys & Tutorials*, 2018. [Online]. Available: DOI:10.1109/COMST.2018.2830648
- [44] S. Vassilaras, L. Gkatzikis, N. Liakopoulos, I. N. Stiakogiannakis, M. Qi, L. Shi, L. Liu, M. Debbah, and G. S. Paschos, “The algorithmic aspects of network slicing,” *IEEE Communications Magazine*, vol. 55, no. 8, pp. 112–119, 2017.
- [45] T. S. Buda, H. Assem, L. Xu, D. Raz, U. Margolin, E. Rosensweig, D. R. Lopez, M. I. Corici, M. Smirnov, R. Mullins, O. Uryupina, A. Mozo, B. Ordozgoiti, A. Martin, A. Alloush, P. O’Sullivan, and I. G. B. Yahia, “Can machine learning aid in delivering new use cases and scenarios in 5G?” in *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, April 2016, pp. 1279–1284.
- [46] K. Shimoto, “Research challenges for network function virtualization - re-architecting middlebox for high performance and efficient, elastic and resilient platform to create new services -,” *IEICE Transactions on Communications*, vol. E101.B, no. 1, pp. 96–122, 2018.
- [47] C. Esposito, A. Gouglidis, D. Hutchison, A. Gurtov, B. E. Helvik, P. E. Heegaard, G. Rizzo, and J. Rak, “On the disaster resiliency within the context of 5G networks: The RECODIS experience,” in *European Conference on Networks and Communications [EuCNC 2018]*, Ljubljana, Slovenia, June 18 - 21 2018.
- [48] G. Nencioni, B. E. Helvik, and P. E. Heegaard, “Including failure correlation in availability modelling of a software-defined backbone network,” *IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 1032 – 1045, Dec. 2017.
- [49] P. Baran, “On distributed communications networks,” *IEEE Transactions on Communications*, vol. 12, no. 1, pp. 1 – 9, march 1964.
- [50] S. Lal, T. Taleb, and A. Dutta, “NFV: security threats and best practices,” *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211–217, 2017.
- [51] S. Scott-Hayward, S. Natarajan, and S. Sezer, “A survey of security in software defined networks,” *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 623–654, Firstquarter 2016.
- [52] P. E. Heegaard, G. Biczok, and L. Toka, “Sharing is power: Incentives for information exchange in multi-operator service delivery,” in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–7.
- [53] R. Guerzoni, I. Vaishnavi, D. Perez Caparros, A. Galis, F. Tusa, P. Monti, A. Sganbelluri, G. Biczok, B. Sonkoly, L. Toka, A. Ramos, J. Melián, O. Dugeon, F. Cugini, B. Martini, P. Iovanna, G. Giuliani, R. Figueiredo, L. M. Contreras-Murillo, C. J. Bernardos, C. Santana, and R. Szabo, “Analysis of end-to-end multi-domain management and orchestration frameworks for software defined infrastructures: an architectural survey,” *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 4, 2017.
- [54] R. V. Rosa, M. A. S. Santos, and C. E. Rothenberg, “MD2-NFV: The case for multi-domain distributed network functions virtualization,” in *2015 International Conference and Workshops on Networked Systems (NetSys)*, March 2015, pp. 1–5.
- [55] R. Munoz, R. Vilalta, R. Casellas, R. Martinez, T. Szyrkowicz, A. Autenrieth, V. López, and D. López, “Integrated SDN/NFV management and orchestration architecture for dynamic deployment of virtual SDN control instances for virtual tenant networks,” *J. Opt. Commun. Netw.*, vol. 7, no. 11, pp. B62–B70, Nov 2015.
- [56] P. S. Khodashenas, B. Blanco, M. A. Kourtis, I. Taboada, G. Xilouris, I. Giannoulakis, E. Jimeno, I. Trajkovska, J. O. Fajardo, E. Kafetzakis, J. G. Lloreda, F. Liberal, A. Whitehead, M. Wilson, and H. Koumaras, “Service mapping and orchestration over multi-tenant cloud-enabled ran,” *IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 904–919, Dec 2017.
- [57] K. J. Hole, “Management of hidden risks,” *Computer*, vol. 46, no. 1, pp. 65–70, Jan 2013.
- [58] P. Vizarreta, P. E. Heegaard, B. E. Helvik, W. Kellerer, and C. M. Machuca, “Characterization of failure dynamics in SDN controllers,” in *9th International Workshop on Resilient Networks [RNDM 2017]*, 2017.
- [59] P. Vizarreta, K. Trivedi, B. Helvik, P. Heegaard, A. Blenk, W. Kellerer, and C. M. Machuca, “Assessing the maturity of SDN controllers with software reliability growth models,” *Accepted for publ. in IEEE Transactions on Network and Service Management*, 2018. [Online]. Available: doi:10.1109/TNSM.2018.2848105
- [60] IETF Network Working Group. (2017) Network Slicing Architecture. [Online]. Available: <https://tools.ietf.org/id/draft-geng-netslices-architecture-01.html>
- [61] 5GPPP. (2015) 5G Vision. [Online]. Available: <https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf>
- [62] Z. Kotulski, T. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J. P. Wary, “On end-to-end approach for slice isolation in 5G networks. fundamental challenges,” in *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Sept 2017, pp. 783–792.
- [63] NGMN P1 WS1 E2E Architecture Team. (2016) Description of Network Slicing Concept. [Online]. Available: https://www.ngmn.org/fileadmin/user_upload/160113_Network_Slicing_v1_0.pdf
- [64] 3GPP Standard Organization. (2017) Network Slicing. 3GPP Use Case. [Online]. Available: <https://tools.ietf.org/id/draft-defoy-netslices-3gpp-network-slicing-02.html>
- [65] 5GPPP Architecture Working Group. (2018) View on 5G Architecture. [Online]. Available: <https://5g-ppp.eu/wp-content/uploads/2018/01/5G-PPP-5G-Architecture-White-Paper-Jan-2018-v2.0.pdf>
- [66] T. Yoo, “Network Slicing Architecture for 5G network,” in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct 2016, pp. 1010–1014.
- [67] A. Mayoral, R. Vilalta, R. Casellas, R. Martinez, and R. Munoz, “Multi-tenant 5G network slicing architecture with dynamic deployment of virtualized tenant management and orchestration (MANO) instances,” in *ECOC 2016; 42nd European Conference on Optical Communication*, Sept 2016, pp. 1–3.
- [68] J. Ordóñez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Figueira, “Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges,” *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80–87, May 2017.
- [69] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, “Network function virtualization: Challenges and opportunities for innovations,” *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90–97, Feb 2015.
- [70] ETSI NFV. (2017) NFV Proofs of Concept. [Online]. Available: <http://www.etsi.org/technologies-clusters/technologies/nfv/nfv-poc>
- [71] A. J. Gonzalez, G. Nencioni, B. E. Helvik, and A. Kamisinski, “A fault-tolerant and consistent sdn controller,” in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.
- [72] G. Pongracz, L. Molnar, and Z. L. Kis, “Removing Roadblocks from SDN: OpenFlow Software Switch Performance on Intel DPDK,” *2013 Second European Workshop on Software Defined Networks. EWSN 2013*, Oct. 2013.
- [73] M. Kourtis, G. Xilouris, V. Riccobene, M. J. McGrath, G. Petralia, H. Koumaras, G. Gardikis, and F. Liberal, “Enhancing VNF performance by exploiting SR-IOV and DPDK packet processing acceleration,” in *IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2015, San Francisco, CA, USA, November 18-21, 2015*, 2015, pp. 74–78.
- [74] Christian Horn, RedHat. (2017) Inception: How usable are nested KVM guests? [Online]. Available: <https://www.redhat.com/en/blog/inception-how-usable-are-nested-kvm-guests>
- [75] J. Ren, Y. Qi, Y. Dai, Y. Xuan, and Y. Shi, “Nosv: A lightweight nested-virtualization vmm for hosting high performance computing on cloud,” *Journal of Systems and Software*, vol. 124, pp. 137 – 152, 2017. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0164121216302151>
- [76] D. Liu, L. Wang, Y. Chen, M. Elkaslan, K. K. Wong, R. Schober, and L. Hanzo, “User association in 5G networks: A survey and an outlook,” *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1018–1044, Secondquarter 2016.
- [77] H. Ramazanali, A. Mesodiakaki, A. Vinel, and C. Verikoukis, “Survey of user association in 5G hetnets,” in *2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*, Nov 2016, pp. 1–6.
- [78] B. Gendron, M. G. Scutellà, R. G. Garroppo, G. Nencioni, and L. Tavanti, “A branch-and-benders-cut method for nonlinear power

- design in green wireless local area networks,” *European Journal of Operational Research*, vol. 255, no. 1, pp. 151–162, 2016.
- [79] R. G. Garroppo, G. Nencioni, M. G. Scutellà, and L. Tavanti, “Robust optimisation of green wireless lans under rate uncertainty and user mobility,” *Electronic Notes in Discrete Mathematics*, vol. 52, pp. 221–228, 2016.
- [80] F. D’Andreaiovanni, R. G. Garroppo, and M. Maria G. Scutellà, “Green design of wireless local area networks by multiband robust optimization,” *Electronic Notes in Discrete Mathematics*, vol. 64, pp. 225–234, 2018.
- [81] A. Zappone, L. Sanguinetti, G. Bacci, E. Jorswieck, and M. Debbah, “Energy-efficient power control: A look at 5G wireless technologies,” *IEEE Transactions on Signal Processing*, vol. 64, no. 7, pp. 1668–1683, April 2016.
- [82] H. Zhang, S. Huang, C. Jiang, K. Long, V. C. M. Leung, and H. V. Poor, “Energy efficient user association and power allocation in millimeter-wave-based ultra dense networks with energy harvesting base stations,” *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 9, pp. 1936–1947, Sept 2017.
- [83] R. G. Garroppo, G. Nencioni, G. Procissi, and L. Tavanti, “The impact of the access point power model on the energy-efficient management of infrastructure wireless lans,” *Computer Networks*, vol. 94, pp. 99–111, 2016.
- [84] B. Gendron, R. G. Garroppo, G. Nencioni, M. G. Scutellà, and L. Tavanti, “Benders decomposition for a location-design problem in green wireless local area networks,” *Electronic Notes in Discrete Mathematics*, vol. 41, pp. 367–374, 2013.
- [85] Y. Lin, W. Bao, W. Yu, and B. Liang, “Optimizing user association and spectrum allocation in hetnets: A utility perspective,” *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1025–1039, June 2015.
- [86] I. P. Belikaidis, A. Georgakopoulos, P. Demestichas, B. Miscopein, M. Filo, S. Vahid, B. Okyere, and M. Fitch, “Multi-rat dynamic spectrum access for 5G heterogeneous networks: The SPEED-5G approach,” *IEEE Wireless Communications*, vol. 24, no. 5, pp. 14–22, October 2017.
- [87] G. Baruffa, M. Femminella, M. Pergolesi, and G. Reali, “A big data architecture for spectrum monitoring in cognitive radio applications,” *Annals of Telecommunications*, pp. 1–11, 2018.
- [88] H. Rocha, G. Delsart, A. Andersson, A. Bousselmi, A. Conte, A. Gati, A. M. Masucci, C. Grangeat, C. Cavdar, D. Marquet, E. Alexandri, G. Akpoli-Johnson, H. O. Scheck, J. Gascon, L. Nuaymi, L. Salahaldin, M. E. Tabach, M. M. A. Hossain, S. E. Elayoubi, S. Imadali, T. Chahed, V. Jonsson, W. Yoro, and X. Campderros, “Soogreen: Service-oriented optimization of green mobile networks,” in *2017 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, May 2017, pp. 1–8.
- [89] R. Garroppo, G. Nencioni, L. Tavanti, and M. Scutellà, “Does traffic consolidation always lead to network energy savings?” *IEEE Communications Letters*, vol. 17, no. 9, pp. 1852–1855, 2013.
- [90] E. Bastug, M. Bennis, and M. Debbah, “Living on the edge: The role of proactive caching in 5G wireless networks,” *IEEE Communications Magazine*, vol. 52, no. 8, pp. 82–89, Aug 2014.
- [91] T. X. Tran, A. Hajisami, and D. Pompili, “Cooperative hierarchical caching in 5G cloud radio access networks,” *IEEE Network*, vol. 31, no. 4, pp. 35–41, July 2017.
- [92] J. Du, E. Gelenbe, C. Jiang, H. Zhang, and Y. Ren, “Contract design for traffic offloading and resource allocation in heterogeneous ultra-dense networks,” *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2457–2467, Nov 2017.
- [93] S. H. Chae and W. Choi, “Caching placement in stochastic wireless caching helper networks: Channel selection diversity via caching,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6626–6637, Oct 2016.
- [94] C. M. Huang, M. S. Chiang, D. T. Dao, W. L. Su, S. Xu, and H. Zhou, “V2v data offloading for cellular network based on the software defined network (sdn) inside mobile edge computing (mec) architecture,” *IEEE Access*, vol. 6, pp. 17741–17755, 2018.
- [95] Y. Fadlallah, A. M. Tulino, D. Barone, G. Vettigli, J. Llorca, and J. M. Gorce, “Coding for caching in 5G networks,” *IEEE Communications Magazine*, vol. 55, no. 2, pp. 106–113, February 2017.
- [96] A. Sadeghi, F. Sheikholeslami, and G. B. Giannakis, “Optimal and scalable caching for 5G using reinforcement learning of space-time popularities,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 180–190, Feb 2018.
- [97] S. Zhang, N. Zhang, X. Fang, P. Yang, and X. S. Shen, “Self-sustaining caching stations: Toward cost-effective 5G-enabled vehicular networks,” *IEEE Communications Magazine*, vol. 55, no. 11, pp. 202–208, November 2017.
- [98] M. Chen, Y. Qian, Y. Hao, Y. Li, and J. Song, “Data-driven computing and caching in 5G networks: Architecture and delay analysis,” *IEEE Wireless Communications*, vol. 25, no. 1, pp. 70–75, February 2018.
- [99] R. G. Garroppo, G. Nencioni, L. Tavanti, and B. Gendron, “The greening potential of content delivery in residential community networks,” *Computer Networks*, vol. 73, pp. 256–267, 2014.
- [100] Associazione Italiana per la Sicurezza Informatica, “Rapporto Clusit 2018,” <https://clusit.it/rapporto-clusit/>.
- [101] Cisco Systems, “Cisco Visual Networking Index: Forecast and Methodology,” June 2017. [Online]. Available: <http://www.cisco.com>
- [102] Gartner, “Gartner Newsroom,” February 2017. [Online]. Available: <http://www.gartner.com/newsroom/id/3598917>
- [103] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, and D. Walker, “P4: Programming protocol-independent packet processors,” *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 87–95, Jul. 2014.
- [104] G. Bianchi, M. Bonola, A. Capone, and C. Cascone, “Openstate: Programming platform-independent stateful openflow applications inside the switch,” *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 2, pp. 44–51, Apr. 2014.
- [105] “In-band network telemetry,” <https://p4.org/p4/inband-network-telemetry/>.
- [106] “In situ oam,” <https://datatracker.ietf.org/wg/iaoam/>.