Pouria Sayyad Khodashenas, Cristina Ruiz, Muhammad Shuaib Siddiqui, August Betzler, and Jordi Ferrer Riera

Fundació i2CAT, Internet i Innovació Digital a Catalunya
C/ Gran Capità 2-4, 08034
Barcelona, Catalunya

The role of Edge Computing in future 5G mobile networks: concept and challenges

Abstract

Future 5G technologies are expected to overcome the challenges of next generation networks aiming to tackle the novel and manifold business requirements associated to different vertical sectors. Extraordinarily high speeds and capacity, multi-tenancy, heterogeneous technologies convergence, on-demand service-oriented resource allocation or even coordinated, automated management of resources are only few examples of the complex demands 5G aims to undertake. The shift from centralised cloud computing-based services towards data processing at the edge is becoming one of the fundamental components envisaged to enable those future 5G technologies. Edge computing is focused on pushing processing to the network edge where all the actual interactions in the access networks take place and the critical low-latency processing occurs. Combination of Network Functions Virtualisation (NFV) and edge computing technologies and mechanisms provides a wide range of novel opportunities for added-value service provisioning covering different features required in future access networks, such as Quality of Service (QoS), security, multi-tenancy, and low-latency. This chapter provides an overview of edge computing technologies, from supporting heterogeneous infrastructure up to service provisioning methodologies related to the application-specific requirements. It describes the role of edge computing and NFV in future 5G mobile networks. It also provides an insight into how edge computing can potentially facilitate and expedite provisioning of security in 5G networks. The manuscript analyses the role of the networking resources in edge computing-based provisioning, where the demands of 5G mobile networks are to be met with wireless networking technologies, which in essence are different to wired technologies present in core data centres. Initial results obtained from the evaluations of wireless fog networking backhauls are presented and the challenges ahead of the actual implementation of those technologies are also analysed in the chapter.

1 Introduction

5G technologies are envisaged as a new networking paradigm in order to overcome the challenges and requirements associated to the future communication systems. In fact, 5G systems aim to support extraordinarily high speeds and capacity, multi-tenancy, fixed and wireless network convergence, self-X, unconventional resource virtualisation, on-demand service-oriented resource allocation and automated management and orchestration [1]. As a consequence, those 5G upcoming technologies will facilitate both the development and materialization of novel vertical sectors, such as Industry 4.0, Smart Grids, Smart Cities and e-Health. 5G deployment is envisaged therefore to accelerate industrial environments, facilitating them to enter the value chain and increase revenue generation. It is expected that, besides improving the citizen's digital experience, such a market revolution contributes billions to the EU economy each year and creates hundreds of thousands of new jobs, mostly for the small and medium-sized businesses (SMBs) [2].

The landscape of future communication is reshaped and redefined significantly by the ongoing digitalisation trends [3]. One of the main pillars of such revolution is the way that new network functions are introduced to the value chain. Traditionally, such a process demands deployment of specialized devices with 'hard-wired' functionalities. It implies that any adaptation to the ever increasing and heterogeneous market requirements demands a huge investment to change/deploy hardware. Thanks to the advent of cloud computing, Software Defined Networking (SDN) [4] and Network Function Virtualisation (NFV) [5], the idea of having general-purpose computing and storage assets at networks has been realised along with the virtualisation of networks and network functions, which enables the automation of network service provisioning and management [6].

This approach paves the way for various benefits both on network performance and network control and management aspects, including: (i) efficient management of hardware resources, (ii) rapid introduction of new network functions and services to the market, (iii) ease of upgrades and maintenance, (iv) exploitation of existing virtualisation and cloud management technologies for Virtual Network Function (VNF) deployments, (v) reduction in CAPEX and OPEX expenditures, (vi) enabling a more diverse ecosystem, and (vii) encouraging openness within the ecosystem, as defined by the European Telecommunication [7].

This chapter provides an overall and schematic review of the concept of virtualisation of networks and network functions, and then reviews their role to realise 5G challenging features, e.g. multi-tenancy and end-to-end security over Evolved Universal Terrestrial Radio Access (E-UTRA) [8], i.e. Radio Access Network (RAN) and backhauling network. In essence, in terms of multi-tenancy, the challenge remains on how the isolation among different tenants, utilising virtual networks on top of, possibly, the same physical infrastructure, can be ensured at all levels. For ensuring end-to-end security in 5G networks, a holistic approach is required, which takes into account not only the physical but also the virtual resources of the network. These challenges require a substantial change on the network devices, from being only network equipment to cloud-enabled devices enhanced with, e.g., novel processor architectures.

2 Multi tenancy over the Cloud-RAN

Traditionally, to provide coverage in one Point of Presence (PoP), actual installation of physical infrastructure, e.g. Small Cell (SC), is required. Despite the fact that mounting equipment in one place may not be possible (e.g. dense areas), such an ownership increases operators' CAPEX and significantly hampers business agility, particularly when considering the high degree of cell densification needed to deal with the 5G requirements. Moreover, the static nature of physical ownership makes it difficult (impossible in some cases) to handle scenarios with dynamic capacity requirements. For example, a flash crowd event at a venue (e.g., stadium, urban area, etc.) cannot be well-served without overprovisioning of the underlying physical infrastructure. It can be easily translated to more operators' expenses (CAPEX and OPEX), which, in turn, increases the service cost for the end users. To address this issue, the idea of multi-tenancy has been initiated in 3GPP [9] and it is expected to play a vital role in 5G networks [10]. In a multi-tenant scenario, a third party owns the underlying infrastructure and provides access to the actors of the telecom scene like network operators, service providers, Over-the-Top players, etc. Such a sharing increases service dynamicity and reduces the overall cost and energy consumption.

Furthermore, thanks to the advent of cloud computing, Software Defined Networking (SDN) and Network Function Virtualisation (NFV), stakeholders can enter the network value chain without deploying specialized 'hard-wired' devices. It relaxes the ever increasing cost of adaptation to heterogeneous market needs. This new concept calls for a substantial change on the architecture of current RAN nodes, from being only a wireless head to a cloud-enabled device equipped with, e.g., novel processor architectures, Graphics Processing Units (GPU), Digital Signal Processors (DSP), and/or Field-Programmable Gate Arrays (FPGA). In this line, new industry initiatives have already introduced the concept of Mobile-Edge Computing (MEC) [11] and the related key market drivers [12]. The resulting solution will allow several operators/service providers to engage in new sharing models of both access capacity and edge computing capabilities, i.e. the logical partitioning of the localized network infrastructure in one or more PoPs.

In this section, we review the implementation of Cloud-Enabled Small Cells (CESCs) as an example of future cloud-enabled 5G RAN node, able to support edge cloud computing in a multi-tenant, multi-service ecosystem. Then, some of its potential benefits and challenges are presented.

2.1 Enabling Technologies

In this subsection we introduce the basic concept of CESC and Light Data Centre (Light DC). The design originates from the SESAME project [13].

2.1.1 Cloud-Enabled Small Cell (CESC)

The concept of CESC, shown in Figure 1, is the key enabler in order to form a cloud-enabled network that supports both radio access and edge computational services at one PoP. It consists of the union of a SC, although it can be extended and applied to any other access network system, and a micro server in one single device. SC functionalities are foreseen to

be split into Physical Network Functions (PNFs) and SC Virtual Network Functions (VNFs) [14]. SC VNFs may represent different layers of the E-UTRAN protocol stack, while the rest of protocol entities will remain as PNF (e.g. below PDCP at data plane protocol stack). The use of SC VNFs provides the required support for splitting the SC resources in different virtual slices. Therefore, CESC is able support multi-tenancy in a cloud-RAN environment by instantiating a dedicated SC VNF per tenant, called also Virtual Network operator (VNO) from now, while keeping PNFs common for all.

SC VNFs, as well as service VNFS, are going to be hosted by the micro server, whose architecture and characteristics are optimized for the MEC environment. Instantiation of service VNFs (e.g. virtual firewall and virtual caching) over the CESC micro server aims to satisfy the identified requirements of 5G (e.g. low latency). CESC becomes the main serving node, it allows overall edge service provision avoiding data transfer to the core network.

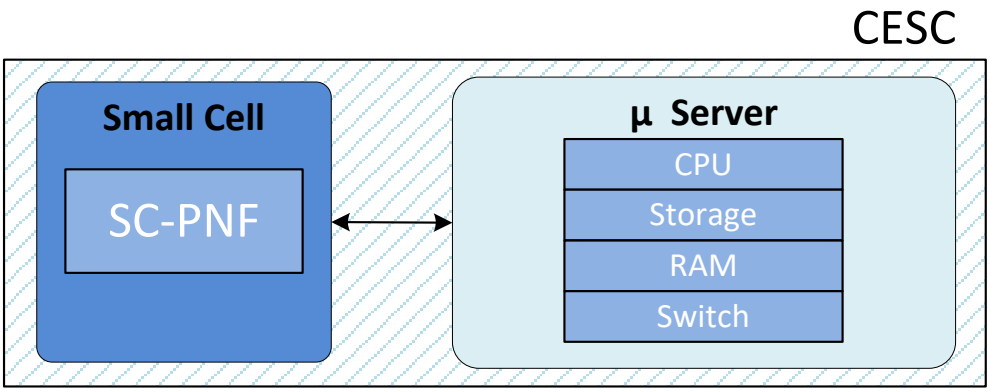

Figure 1 Cloud-Enabled Small Cell (CESC), consisting of the Small Cell radio head (SC – PNF) and the micro server.

2.1.2 Light Data Centre (Light DC)

As it may be inferred, resources on a single micro server (i.e. RAM, CPU, storage, HWA) might not be enough to support the mobile edge computing services of all tenants. CESC clustering enables the creation of a micro-scale virtualised execution infrastructure in the form of a distributed data centre, denominated Light DC, enhancing the virtualisation capabilities and processing power at the edge. The hardware architecture of the Light DC envisages that each micro server in a CESC will be able to communicate with all others via a dedicated network, guaranteeing the latency and bandwidth requirements needed for sharing resources. The resulting solution will allow virtual network operators/tenants not only to support connectivity but also to provide added value mobile edge services (e.g. caching, video transcoding, etc.) in a PoP.

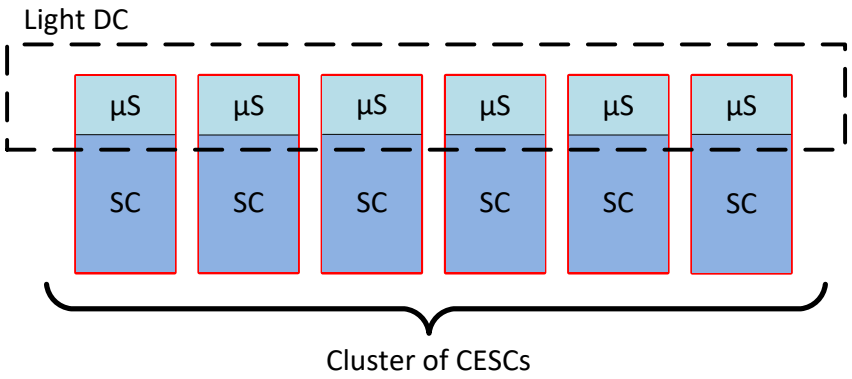

Figure 2 Light DC overview formed by all the micro-server in a CESC cluster.

Like any DC, Light DC is a pool of resources (computational, storage, network) interconnected using a communication network. Such a clustering can be achieved with different network topologies (e.g. star, tree, mesh, etc.) and technologies (e.g. Ethernet over copper or fibre, wireless radio, etc.). The network topology plays a pivotal role in the architecture, since it determines the scalability, robustness, performance (e.g. throughput and latency), efficiency and in simple words viability of a solution. Light DC might adopt and adapt any of well-known DC topologies such as three-tier, DCell, or even BCube. [15] However, considering metrics like performance, complexity and the number of network elements (i.e. NICs) required per micro server, the three-tier topology stands out as the most appropriate topology for the Light DC [16]. In small areas with no geographical barriers, such as a building or a hospital, the topology might be simplified to a flat tree or even a star topology, as shown in Figure 3. There are many (physical transport layer) technological options to form the selected network topology, such as Ethernet over copper or fibre, or even wireless radio. Section 5 will review these alternatives focusing on describing a wireless backhauling solution with more details.

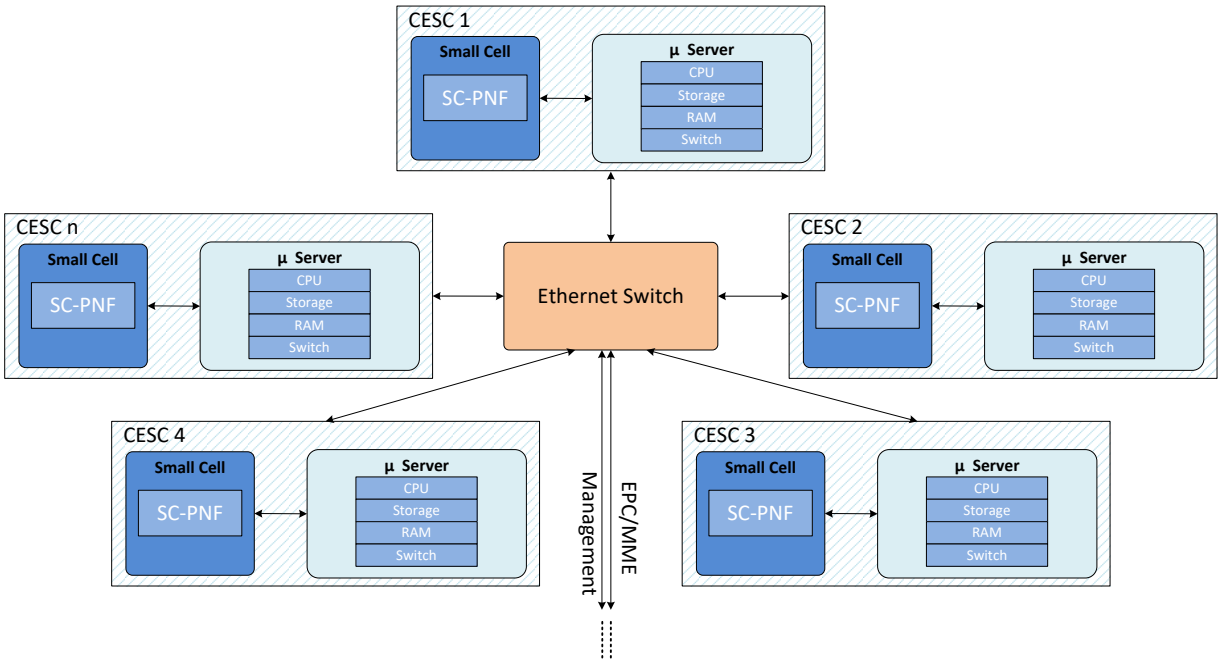

Figure 3 CESC cluster physical architecture

2.2 Multi-tenant multi-service management and orchestration

The Light DC concept offers a virtualisation platform to meet 5G requirements, however, management and orchestration of this uniform virtualised environment, able to support both radio connectivity and edge services, is a challenging task by itself. The most clearly highlighted specific challenges that a cloud-RAN environment entails are the dynamic composition of the Light DC resources based on the current status of CESC cluster(s), the coordination of specific type of resources (radio-related resources, service-related HW accelerators, etc.) and the isolation of dedicated network slices to each tenant.

Considering the aforementioned challenges, the SESAME project [17] proposes a solution to consolidate multi-tenancy and orchestration in SC cloud-enabled mobile communication infrastructure. The consolidation is built over the virtualization and NFV pillars. Figure 4 below better illustrates that consolidation as envisaged by SESAME through the high-level architecture. The diagram depicts the most relevant building blocks of the proposed system, as well as both their internal and external inter-connections.

On the right side of the Figure, the CESC Manager (CESCM) is the central service management and orchestration component in the architecture. This component, in essence, is responsible for the integration of all the traditional 3GPP network management elements, at the same time it adds the novel recommended functional blocks in order to materialise the NFV paradigm [18]. With respect multiplicities during deployment and operation time, the system has been designed to allow a single instance of a CESCM to control, monitor, and operate several cloud-enabled small cell clusters, whereby each cluster constitutes a Light DC, as described above. The clusters are independently controlled by a dedicated Virtual

Infrastructure Manager (VIM), whose responsibilities are bound within a single cluster. The CESCM holds a holistic view of the physical infrastructure, so to optimise its management.

There exists the possibility to chain distinct VNFs over the provided virtualised execution environment, i.e. a given Light DC, in order to meet the requirements of a given network service (NS) as requested by a tenant. It is worth to mention that, in this context, a NS is understood as a collection of VNFs that jointly supports data transmission between User Equipment (UE) and operators' Evolved Packet Core (EPC) network, with the possibility to involve one or several service VNFs in the data path. Therefore, each NS is deployed as a chain of PNF, SC VNFs and Service VNFs. Again, due to the distributed nature of the Light DC, the proposed VIM requires data packet extraction (from the traditional 3GPP data path) and a forwarding rule implementation to guarantee possible communication between SC VNFs and Service VNFs, which may reside in different CESCs. SDN principles are used to provide the system with the required scalability. In this way, the CESCM instructs the embedded SDN controller at VIM with the specific VNF forwarding rules, and the SDN controller in return applies them to support the desired connectivity within the Light DC.

We consider an Element Management System (EMS) deployed in the CESCM for each instantiated VNF. The EMS is responsible to perform fundamental management actions, such as fault monitoring, configuration, accounting, performance monitoring and security (FCAPS). Besides, the central management point for the whole network of the mobile operator is the Network Management System (NMS). Thus, the corresponding PNF EMS and SC EMS are respectively the elements accounted for carrying out respectively the management of the physical and virtualised network functions residing at the SC.

The VNF Manager (VNFM) carries out the basic lifecycle management of the deployed VNFs. It is included in the CESCM element. By leveraging on the monitoring mechanisms, the CESCM, in conjunction with the VNFM, is able to apply policies for NS-level rescaling and reconfiguration to achieve high resource utilization. It is worth to mention that monitoring mechanisms are dictated by the CESCM Service Level Agreements (SLA) monitoring unit that allows the monitoring of SLAs between different business role players. Two main role players interact in the proposed scenario, the Mobile Network Operator (MNO) is the owner of the radio access (Light DC) and management infrastructure, and offers sliced network services to different Mobile Virtual Network Operators (MVNO), which act as tenant mobile network operators.

Another essential component at the heart of CESCM is the NVF Orchestrator (NFVO). Besides management and orchestration of the above mentioned functionalities, NFVO composes service chains (constituted by two or more VNFs located either in one or several CESCs) and manages the deployment of VNFs over the Light DC. This includes not only the management of a typical Network Function Virtualisation Infrastructure (NFVI) (i.e. processing power, storage and networking), but also assignment of HW accelerators. Besides, to improve the energy efficiency of the proposed solution, NFVO may need to take care of switching on and off resources at CESC level.

The CESCM portal is a control panel web GUI that constitutes the main graphical frontend to access the cloud-RAN management platform. It includes two login procedures, a login for

the MVNO to retrieve monitoring information and be able to browse catalogues, request and delete NSs, and another login for the VNO administrator to register extra resources, add new NSs to the catalogues and configure CESCM elements.

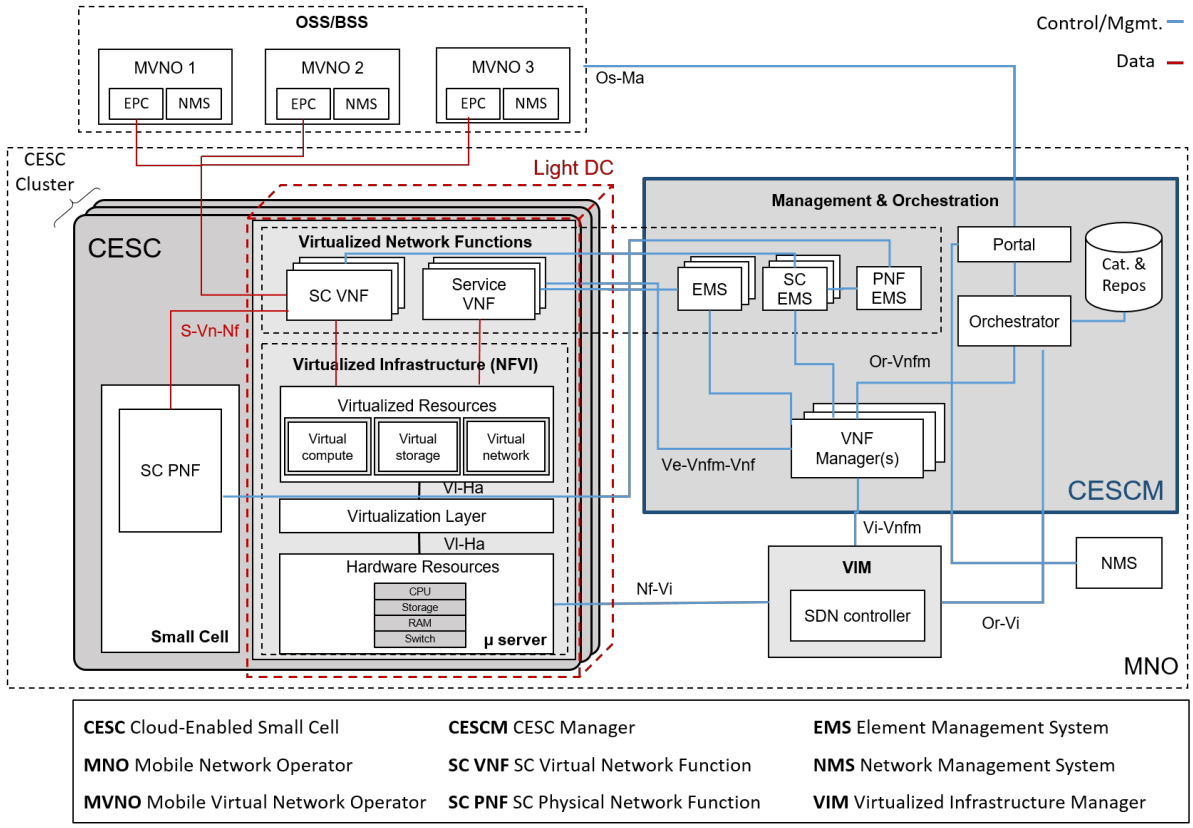

Figure 4 Possible cloud-RAN multitenant architecture based on ETSI MANO framework.

2.3 Benefits and challenges

As evaluated in [19] it is expected that in the framework of cloud-RAN networks the speed of service delivery significantly increases, since the edge cloud services are executed very near to the end user. It creates an excellent opportunity for stakeholders, e.g. operators and cloud based platforms, to serve customers (individuals and businesses) demand for intelligence and complex services in a practical and latency-free manner. Also, multi-tenancy achieved through the virtualisation of network resources, allows efficient use of deployed physical infrastructure at one PoP, via the on-demand network topology changes (e.g. add/drop of CESC to a cluster) and elastic per-tenant capacity allocation, aiming to guarantee the Quality of Experience (QoE) and reduce the total cost of operation. Having this in mind, compared to the current 4G systems, some of the cloud-RAN merits can be listed as follows [20]:

- Higher wireless area capacity and more diverse service capabilities: by deploying high-density multi-service multi-tenant SC networks higher traffic and capacity per geographical areas are supported.

- Reducing the average service creation time: the flexible design of the CESC platform and the associated management layers promotes a shared virtualised infrastructure,

i.e. a cloud environment, right at the network's edge which reduces the service deployment time scale.

- Creating a secure, reliable and dependable Internet with a "zero perceived" downtime for services provision: cloud-RAN solutions allow rapid integration of multiple virtual operators sharing the same infrastructure, thus allowing isolated and secure provision of vertical services for massive amount of connected devices. Also, automated network resource monitoring/optimization allows to provision them where they are needed the most, i.e. resource rebalancing/repurposing. It guarantees service reliability and minimizes service downtime.

Despite the potential technical benefits, there are many challenges to address. For example, viability of a solution strongly depends on the service provisioning model on the joint radio and cloud environment. The point is that, even though there is already a good understanding and experience available on the radio access and/or cloud computing service provisioning, there is no clear vision on a joint radio-cloud case which covers both worlds simultaneously. From the business perspective, three major role players are identified [21], as depicted in Figure 5: Function provider (FP), is the VNF developer which sells/develops VNFs; Service Provider (SP), is the one who composes NS –i.e. chain of VNFs, PNFs– with the available VNFs and offers them to the customer; customer is the one who purchases NSs. In multi-tenant cloud enabled RAN, there are two main possible ways to form a joint radio-cloud model with the above defined roles, as illustrated in Figure 5.

- **Mobile Edge Computing as a Service (MECaaS):** This model (depicted as option 1 in Figure 5) has been inspired mainly from the MNO-MVNO business relationship. Briefly, in this model, MVNO relies completely on the infrastructure and other services provided by the MNO. Bearing this in mind that, MVNO asks for high level KPIs on the service level agreement (SLA), e.g. on the radio connectivity at one area with support of a desired downlink/uplink capacity and on the cloud, e.g. support for a number of caching hits, transcoding delay less than a threshold, etc. Here, MVNO only has an overall vision of the system and MNO has to provide enough support, i.e. both in terms of hardware and number/composition VNF chains (i.e. NS), to meet the agreed KPIs. Performance reports are provided to MVNO on time intervals (even real time). In simple words, with this model, MVNO does not chain VNFs to form a mobile edge service (i.e. VNF1 connected to VNF2 connected to VNF3), and a high level KPI view is enough for it to request a service without going to details.

- **Radio Access Node as a Service (RANaaS):** In this model, shown as option 2 in the Figure 5, MVNO on SLA asks for connectivity in a certain coverage area with some radio KPIs as above and an aggregated cloud resources on the Light DC, e.g. a certain amount of GB of storage, of RAM, etc. This model corresponds with the famous Infrastructure as a Service (IaaS) paradigm, which is one of the three fundamental service models of cloud computing [22]. In an IaaS model, a third-party provider (MVO) hosts hardware (e.g. CESC), software (e.g. Hypervisor, VIM, CESCM, VNFs, etc.) and other required infrastructure components on behalf of its users (MVNO). IaaS providers also host users' applications (i.e. edge/cloud service) and handle tasks including system maintenance, backup and resiliency planning. With this model in

place, MVNO can compose VNF chains on demand, i.e. MVNO decides to have VNF1 connected to VNF2 connected to VNF3. As a consequence, any VNF instantiation (depending on the used hardware resources) consumes a portion of available MVNO's aggregated resources. Therefore, the deployment of VNF chains is conditioned to the amount of requested resources by the MVNO. Note that VNF (e.g. vCaching, vTranscoding) hardware resources are fixed and determined by the VNF developer (e.g. 2 GB of storage and 2 GB of RAM). Although, it is possible to have different flavours of one VNF in place, e.g. vCaching with extra/less storage capabilities, etc. In this case, MVNO has more choices among one family of VNF.

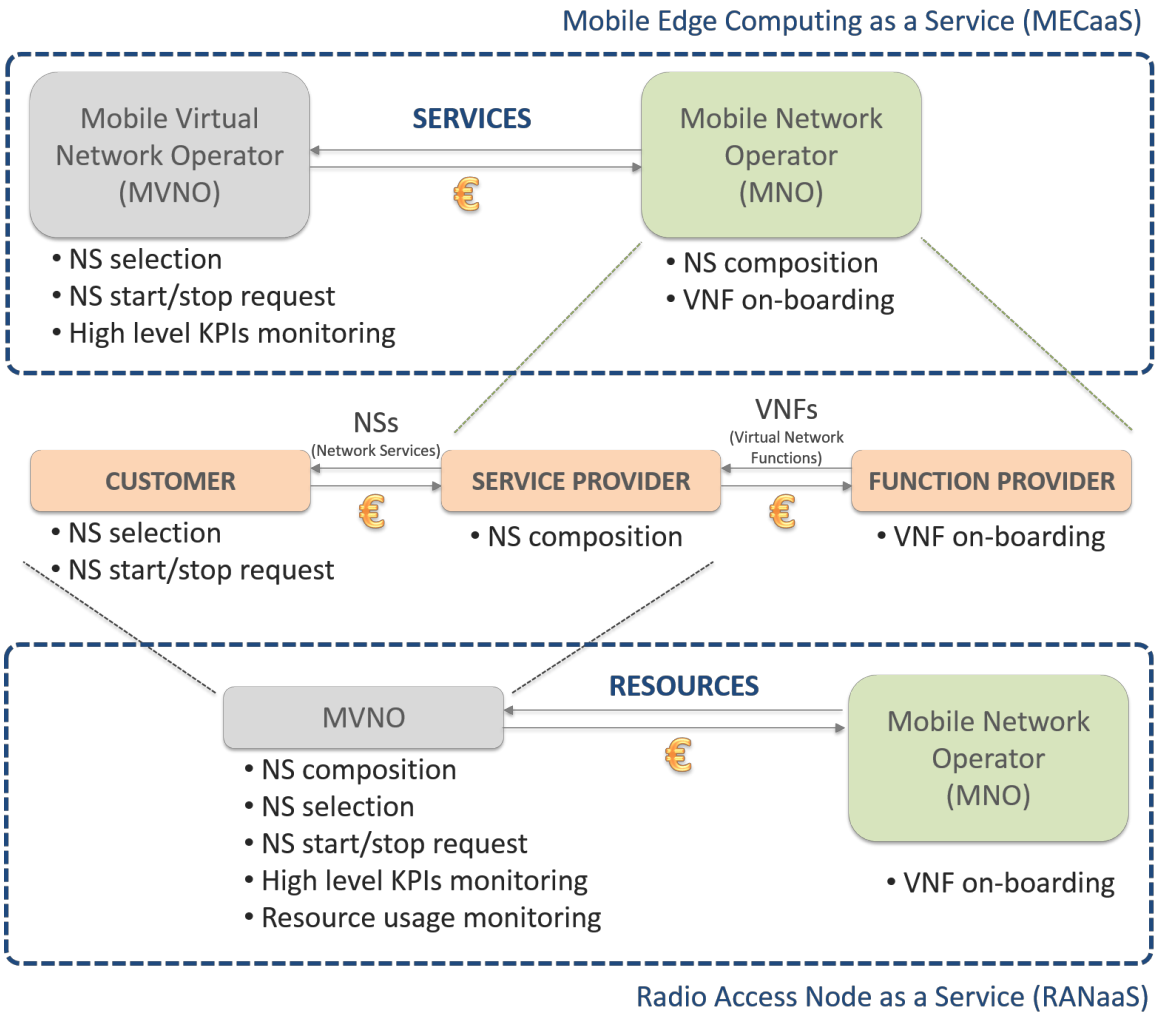

Figure 5 Cloud-RAN possible role players and service provisioning schemes.

The discussion above showed only a part of complexity of service provisioning in a joint cloud-radio environment. It is worth to note that, as mentioned above there are still many other open issues to address on a multi-tenant scenario, e.g. business related questions such as multi-tenant pricing procedure and technical questions such as VNF placement over the distributed light DC environment. These call for further discussions and efforts.

3 Security in 5G networks

5G enables innovative scenarios and applications making use of ultra-high speed, low-latency telecommunication networks for fixed and mobile users and machine-to-machine communications, as described by the 5G-PPP project CHARISMA (Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access) [22]. These scenarios, together with the introduction of the new paradigm for computing and network infrastructure which decouples the actual functionality from the underlying hardware and middleware functions (Cloud Computing and Software Defined Networks) further reinforces the need for automated management and control of the telecommunication infrastructure. In particular, since a cloud-based paradigm promotes that infrastructure is highly accessible and shared by multiple users (for instance, Virtual Network Operators), the concept of a highly secure network gains even more relevance. It is of outmost importance to be able to provide robust, flexible and proactive mechanisms to detect and prevent security issues, and to be able to perform that on real time and in an automated fashion.

3.1 Research Challenges

Today we can't foresee the new and ever changing threats that 5G networks will have to protect against, but we do have the basis to create autonomic network management solutions that shall cope with them, being fed with insights from governed real-time analytics systems on the one hand, and actuating on network resources in order to minimize or prevent the effects of the detected threats in real-time on the other hand.

The following research challenges are by no means an exhaustive list of security research challenges facing 5G networks however they represent few security aspects that must be considered in 5G networks.

- **Network service end-to-end security**
  This refers to all the different mechanisms that can be utilized to ensure confidentiality, integrity, availability and non-repudiation for a network service. These security mechanisms include authentication, authorization, user privacy/anonymity, anti-jamming, encryption, digital signatures, etc. which can be used, based on priorities and requirements, to mitigate service related vulnerabilities.

- **Tenant Isolation**
  Infrastructure sharing by multiple virtual network operators will require strict isolation at multiple levels in order to ensure absolute security. In particular, different aspects of control-plane, data-plane and resource isolation must be investigated and guaranteed to ensure zero correlation among different tenants operations. Tenant isolation is ultimately important in order to ensure a reliable and warranted service assurance, together with data and communication integrity and confidentiality.

- **Virtualised Security**
  Leveraging on the NFV environment, required network security functions could be deployed, orchestrated, and managed at different locations in the network as a VNF, also referred as Virtual Security Functions (VSFs). However, the security of VNF in itself as an element, e.g., VNF hardening, VNF verification/attestation, VNF code robustness, etc. has to be carefully considered [23].

- **Security Management**
  As mentioned earlier, the complexity of security mechanisms grow manifolds in the 5G networks not only due to virtualisation of resources but also due to security requirements at different levels or domains such as network slice, network service, and network resource (physical & virtual). Hence, a holistic security management system, guided by a set of defined security policies, is essential to ensure that security mechanisms functions are enforced as planned.

- **Trust Management**
  Another vital security challenge is the management of trust among the different modules of the NFV environment to ensure reliable and secure operation of the MANO framework.

3.2 A Potential Approach

As discussed in [24], the already high complexity of securing a network and its services has scaled up another notch with the introduction of SDN and NFV in 5G networks, i.e., due to softwarization and virtualisation of networks and network functions. In order to build a consistent and robust security ecosystem, network functions and network services in SDN/NFV environments require a comprehensive approach to end-to-end security for network resources, both physical and virtual, which ensures automated alignment of security policies to changes in network [25]. The dependence of security functions on monitoring information becomes even more crucial in SDN/NFV based 5G networks because greater level of security related monitoring is required as compared to the traditional non-SDN/NFV networks. This is mainly due to dynamic and automated provisioning, orchestration and management of networks, network functions and application services that SDN/NFV based network deployments allow. In 5G, the difficulty to examine the complete network, both virtual and physical, increases the complexity of security monitoring, in order to ensure consistent automated security monitoring management. Figure 6 shows the security management architecture proposed in the 5G CHARISMA project, mapped on an ETSI MANO framework inspired Control, Management and Orchestration (CMO) plane for a converged 5G access network.

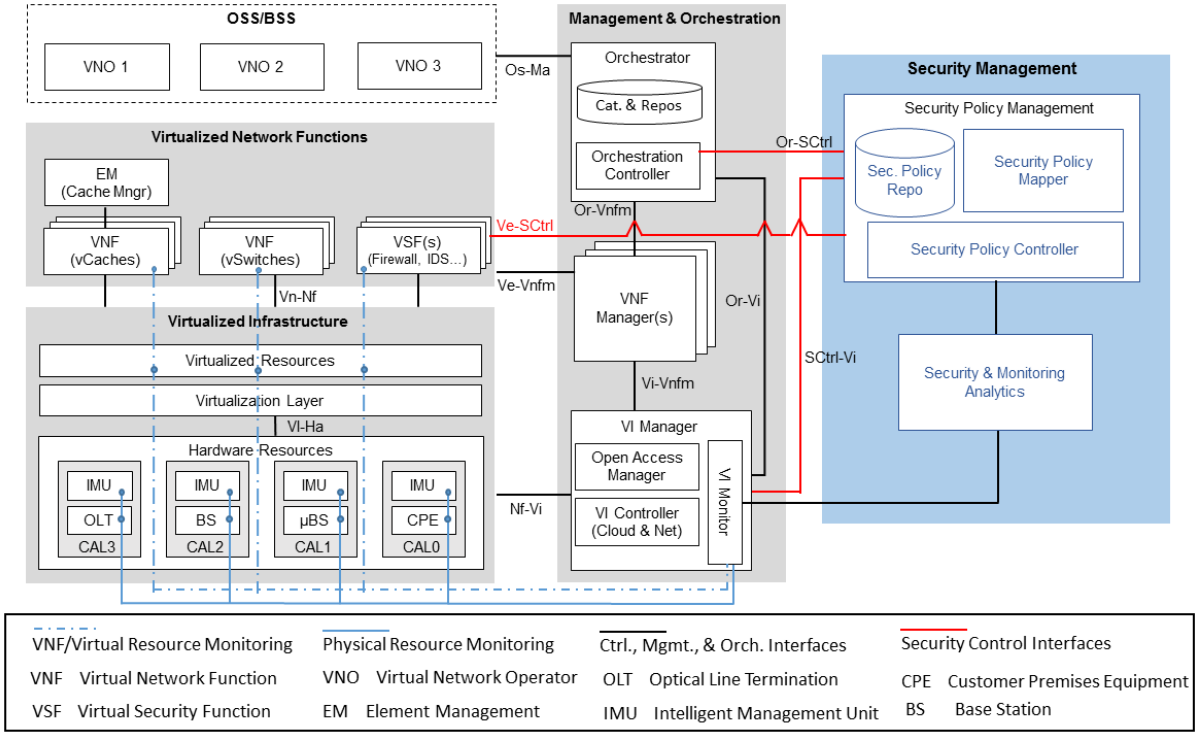

Figure 6 Possible Security Management architecture based on ETSI MANO framework.

The proposed security management architecture has two main sub-components, Security Policy Management (SPM) and Security & Monitoring Analytics (SMA). The SPM enables the management of end-to-end security policies at service level. It translates the defined security policy of a service into specific security requirements, e.g., a certain virtual security function (VSF), hardening configuration of the VM running a VNF, etc., and initiates their provisioning. The SMA receives monitoring information from all physical and virtual resources. As shown in Figure 6, monitoring data is gathered at service level (e.g., VNFs), virtual resource level (e.g., VMs) and physical resource level (e.g., server machine). Being provided with a holistic status of the entire network, the SMA can extract useable knowledge and recommendations, by running smart analytics/algorithms on the available information, for SPM consumption. Based on the monitoring knowledge/recommendations and defined policy of a service, the SPM can take further actions. It is worth mentioning that the above architecture also considers multi-tenancy; thus, the security policy management can also be observed on per tenant basis.

4 Wireless Backhauling in 5G

One of the main paradigms of 5G networks is to shift tasks originally performed in centralized clouds, such as caching or data processing (video acceleration, encoding, etc.), to the edge. There, a variety of services may run on different physical devices, occasionally requiring data to be moved between devices at the edge in order to provide the required services.

Thus, to deliver a high performance, the quick processing and forwarding of access data entering the edge network is required. Further, in cases where SFC is applied, trespassing

several services that may be running on different machines becomes necessary. This is only possible with a flexible and powerful backhauling infrastructure that connects the devices at the edge. A solution that promises to satisfy the requirements of 5G deployments are wireless mesh backhauls [26] [27].

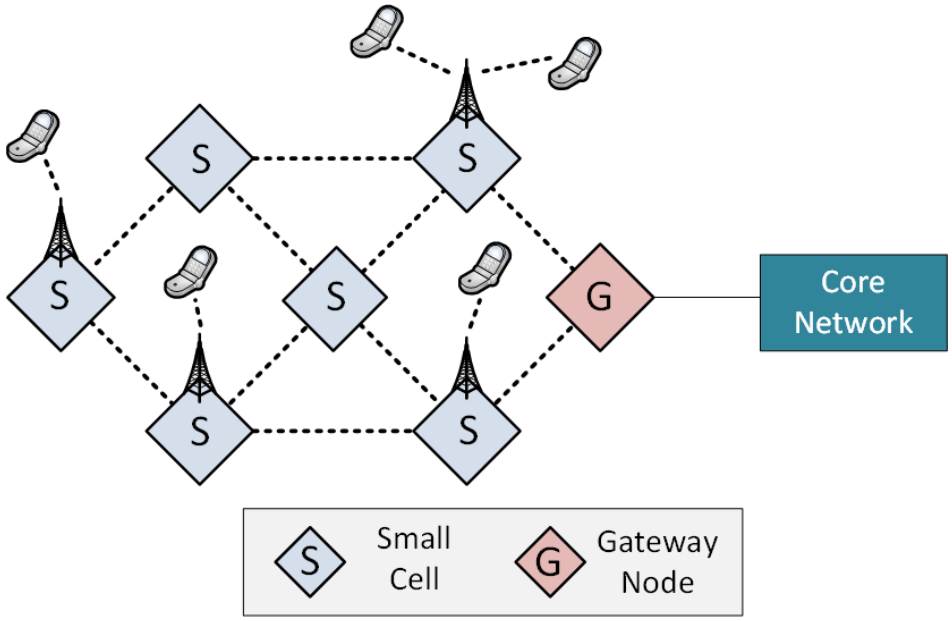

Figure 7 A Small Cell (S) deployment using wireless interfaces to form a mesh backhaul. The connection to the core network is established via a gateway node (G).

In this approach, the access nodes (small cells) are equipped with wireless radio interfaces that allow to establish links to other nodes within transmission range. Figure 7 shows an example of topology in a use case where several small cells equipped with additional wireless backhaul interfaces form a mesh network. Each node can act as relay for traffic exchanged between any two points of the network: whenever access traffic enters the backhaul, it can travel over multiple wireless links, either to reach one of the other nodes for further processing (at the edge), or to reach a gateway node. Gateway nodes dispose of additional network interfaces to establish a connection between the backhaul and the core network.

Wireless mesh networks may be composed of a heterogeneous mix of different wireless technologies that differ in terms of the used radio spectrum and communication standards or protocols. Well known standards like IEEE 802.11, operating at the 2.4 GHz and 5 GHz band, can coexist along with other radio technologies, for example 60 GHz band technologies [28]. Typical characteristics of aforementioned technologies, as well as the characteristics of wired technologies used for wireless backhauls are shown in Table 1.

Technology	1000BASE-T	1000BASE-SX	10GBASE-T	WiFi (sub 6 GHz)	WiFi (60 GHz)
Max. Data Rate	1 Gbit/s	1 Gbit/s	10 Gbit/s	< 300 Mbit/s	7 Gbit/s
Range	100 m	200 - 500 m	55 – 100 m	100 - 200 m	50 - 100 m
Medium	Copper	Fibre	Copper	Radio	Radio

Table 1 Typical characteristics of wired technologies used for backhauling in comparison with wireless backhauling technologies.

When comparing key features of wireless backhauls [29] with traditional, wired backhauls, certain advantages can be identified that can have a crucial impact on the performance of future 5G deployments:

- Wireless backhauls profit from a high dynamicity when it comes to the deployment of access nodes in the field. Contrarily to nodes that rely on a wired backhaul connection and require access to a physical infrastructure, nodes equipped with wireless interfaces are not bound to a particular physical location, as long as the connection over radio to at least one of the remaining nodes of the mesh network is guaranteed. Thus, using a wireless backhaul allows for a much more flexible deployment.

- The deployment of wireless backhauls is much less expensive when compared to the deployment of wired backhauls.

- The wireless backhaul architecture allows for a quick integration of new devices into the existing network infrastructure: newly deployed devices can join and leave the existing backhaul infrastructure at any moment. This can be of use whenever the network coverage needs to be increased.

- Since no wired infrastructure is required to interconnect the network nodes with each other and with the core network, the cost of deploying and extending the network is much lower when compared with traditional wired backhaul approaches.

Overall, as strong characteristics of wireless mesh backhauls the high flexibility and adaptability stand out, which can be useful in a large variety of use cases. The easy deployment and integration of new nodes into the already existing wireless backhaul infrastructure, facilitates the MNO to effectively increase the network coverage and capacity. This is particularly useful whenever during sporadically a large number of UEs needs to be supported in environments without static infrastructure, e.g., for flash events like music festivals in remote areas or other similarly crowded events. In other scenarios, the easiness of deploying and reshaping the network topology can be crucial. In situations where within a short period of time the deployed small cell infrastructure breaks down, it might be necessary to quickly re-establish network connectivity. A cause for the loss or malfunctioning of network operation can be natural catastrophes that destroy parts of the

deployed infrastructure. In such scenarios, a wireless backhaul provides the tools to quickly re-establish basic and emergency communications by reconfiguring the data plane of the backhaul to assure end-to-end user connectivity via alternative paths and by deploying new nodes at critical locations to regain access radio and backhaul connectivity in an area.

In spite of these clear advantages of wireless backhauls, several challenges arise for the design of such wireless architecture. For example, in contrast to wired solutions, noticeable fluctuations in the link qualities between the nodes of the network are possible. This can have a substantial impact on the stability of the backhaul and can also directly affect the achievable throughput.

Yet, it is possible to overcome possible issues since a careful planning of the spectrum to be used by the backhaul can avoid interference issues and in general there is path diversity between the nodes of the network.

Further, for an efficient operation of the backhaul during the network operation, forwarding policies are required to dynamically adapt the routes taken in the data plane of the backhaul. Simple policies can avoid problematic or poor performing links, whereas advanced policies can take into account elaborate interference models, cross-flows performance impacts, etc.

There exist centralized and decentralised approaches on how to determine the data plane routes. Centralized solutions can be SDN-based, where a network controller takes routing decisions by monitoring the network and installing forwarding rules in the nodes of the wireless backhaul. In decentralised approaches, routing decisions are taken from the nodes at the edge without a supervisor. In such cases, routing protocols such as OSLR are used.

Features like SFC of VNFs requires an SDN controller, which takes care of installing the forwarding rules in the network, enabling the necessary node-to-node and node-to-core communications.

In a wireless backhaul network, it is possible to extend these SDN controllers by additionally providing the controller with specific information about the status of the wireless backhaul, e.g., the availability and the quality of wireless links within the network, as well as the link utilization and ongoing transmissions. This information can be included in the metrics that are used for the calculation of optimal data paths. A wireless backhaul architecture for LTE traffic that implements such a type of logic has been designed and is currently verified [30]. The basics of intelligent, SDN-based wireless backhauls have also been evaluated in the context of fog computing networks, where even a backhaul formed of constrained devices has proven to deliver the required features for wireless backhauling [31]. These preliminary investigations show how a wireless, SDN-based backhaul is successfully deployed in a network of constrained devices. In spite of the constraints of the used hardware, SDN-based wireless backhauling solutions can be applied, which represents a corner stone towards using wireless backhauls in fog networking.

The analysed use case involves several constrained devices that use wireless transceivers to build a backhaul mesh network that reports channel load statistics to an SDN controller. The

controller uses the gathered information to apply load-balancing mechanisms in order to avoid the congestion of wireless links, which can be one of the main causes for performance losses in wireless networks.

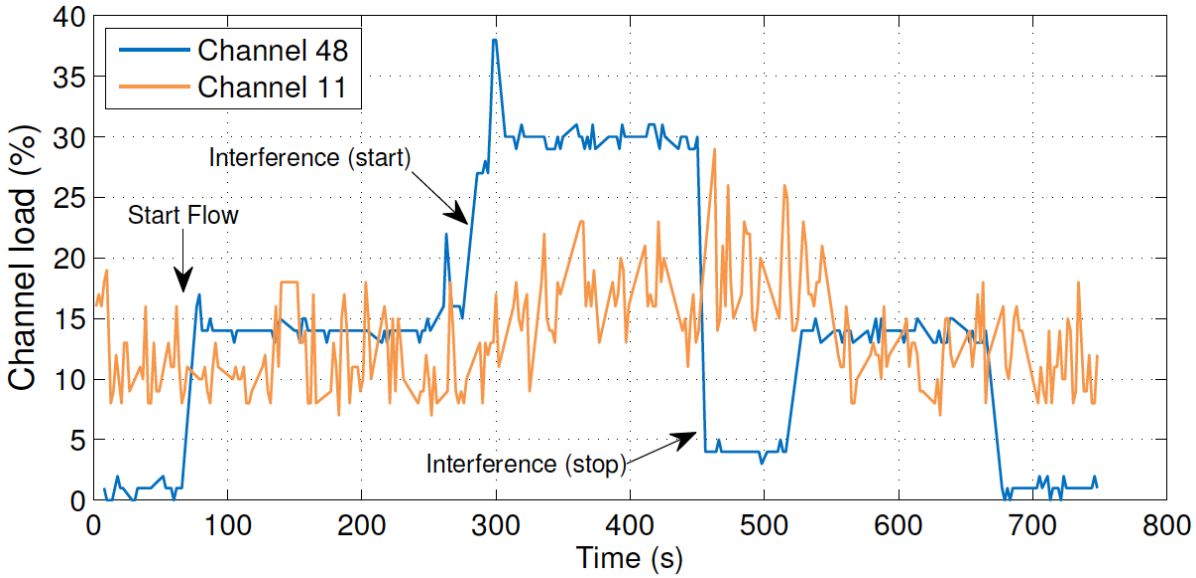

Figure 8 Channel load information gathered at a network node, showing how the decisions taken by the SDN-controller affect the cannel load of a wireless backhaul over the course of an experiment in a fog computing use case [31].

Figure 8 shows an excerpt from the results, where we can see the channel load statistics gathered by the SDN controller from a network device. The controller observes some background traffic on channel 11 and a soon as a traffic flow is generated by a device from the backhaul (t~70s), the data flow is allocated on the less busy channel 48. The reaction to strong external interference introduced at t ~ 290s on channel 48 then leads the controller to take the decision to rebalance the network load by reassigning the data flow to channel 11. As soon as the external interference stops, the data flow is reallocated to channel 48, again to balance the network load and avoid congestion. The load-balancing paradigm followed by the SDN controller in this example is just one out of many paradigms that can be used to determine how traffic is routed in wireless backhaul, be it for fog computing or other 5G use cases. The investigations performed in this works give a hint of the possibilities and capacities intelligent wireless backhauls might offer to us in future deployments.

Another important aspect of 5G networks is multi-tenancy, which imposes several requirements on the wireless backhaul. When accessing edge services, performing SFC, or accessing the core network, each mobile operator (tenant) may have different types of service subscriptions and SLAs with varying KPIs. Since the wireless backhaul has a direct and crucial impact on some of the KPIs (delay, data rate), it carries a high responsibility of delivering the QoS each tenant expects, making multi-tenancy one of the key design parameters for the wireless backhaul architecture.

One way to handle multi-tenancy in SDN-based solutions is the virtualisation of the backhaul network at several layers. At a higher abstraction layer, the backhaul nodes and the wireless links are virtualised and part of the virtualised infrastructure are assigned to each tenant

depending on its requirements on network coverage and edge services. On a lower layer of abstraction, the wireless radio resources, i.e., the data rate of wireless links, the wireless interfaces, etc., are virtualised and slices of the backhaul are assigned to each tenant [32].

The physical properties and limitations of the radio communications, per se are a challenge to overcome. They impose several restrictions when compared to wired solutions. In particular, the limited data rate capacities of wireless links compared to the bandwidths typical for wired connections and the fact that parallel transmissions on the same frequency may interfere each other. The issue of data rate limitations mainly affects communications in the sub 6 GHz band, for example the 2.4 GHz and 5 GHz bands used in IEEE 802.11, where data rates of up to 600 Mbit/s are possible. However, the use of the 60 GHz band gives access to data rates of up to 7 GBit/s, while covering ranges of up to 100 m between two nodes. The recent loosening of the limitations for the use of the 60 GHz spectrum have converted this technology in the most promising and attractive one for future 5G wireless backhaul deployments.

Further, the use of directional antennas in the sub 6 GHz band and a careful planning of the radio spectrum used for communications within the backhaul are two methods to reduce the degree of radio interference and assure a high network performance.

5 Conclusion

Needs and requirements for future 5G networks are very diverse and ambitious, hence they pose several important research challenges. In particular, one of the main stated paradigm, is the shift from centralized cloud-computing services towards an edge-computing service provisioning approach. This chapter highlights the most relevant subsequent challenges, including multi-tenancy, network security provisioning and wireless backhaul implementation. Furthermore, it gathers different ideas and proposals for innovative architectures as potential approaches to address some of the identified 5G requirements.

The presented concepts, along with their corresponding enabling technologies, constitute a promising set of topics under research that are paving the way to successfully accomplish the desired 5G networks requirements in a mobile edge-computing environment.

6 Acknowledgements

Content presented in this chapter covers work performed in the European H2020 SESAME (no. 671596), H2020 CHARISMA (no. 671704), H2020 5G-XHAUL (no. 671551) and FP7 FLEx (no. 612050) projects.

7 References

[1] European Commission, “5G Infrastructure Public Private Partnership (PPP): The next generation of communication networks will be made in EU,” *Digital agenda for Europe,* (Retrieved: May 23, 2016).

[2] European Commission, “Digital Agenda for Europe,” *Digital agenda for Europe,* (Retrieved: June 10, 2016).

[3] European Commission, "The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services.," *5G Vision,* (Retrieved: June 23, 2016).

[4] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE,* vol. 103, no. 1, pp. 14-76, 2015.

[5] European Telecommunications Standards Institute, “Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action,” *Network Functions Virtualisation – Introductory White Paper ,* 2012.

[6] H. Karl, S. Dräxler, M. Peuster, A. Galis, M. Bredel, A. Ramos, J. Martrat, M. S. Siddiqui, S. v. Rossem, W. Tavernier and G. Xilouris, “DevOps for network function virtualisation: an architectural approach,” *Transactions on Emerging Telecommunications Technologies,* vol. DOI: 10.1002/ett.3084, 2016.

[7] European Telecommunications Standards Institute, “Network Functions Virtualisation (NFV): Network Operator Perspectives on Industry Progress,” *Network Functions Virtualisation – White Paper,* 2013.

[8] P. Rost, A. Banchs and I. Berberana, “Mobile network architecture evolution toward 5G,” *IEEE Communications Magazine,* vol. 54, no. 5, pp. 84-91, 2016.

[9] 3GPP, “Network sharing; Architecture and functional description,” *TS 23.251 v12.0.0, Release 12,* December 2013.

[10] K. Samdanis, X. Costa-Perez and V. Sciancalepore, “From network sharing to multi-tenancy: The 5G network slice broker,” *IEEE Communications Magazine,* vol. 54, no. 7, pp. 32-39, 2016.

[11] European Telecommunications Standards Institute (ETSI), “Mobile-edge computing: Introductory technical white paper,” 2014.

[12] I. Son, D. Lee, J.-N Lee and Y. B. Chang, “Market Perception on Cloud Computing Initiatives in Organizations: An Extended Resource-based View,” *Information & Management,* vol. 51, no. 6, 2014.

[13] I. Giannoulakis, G. Xylouris, E. Kafetzakis, M. A. Kourtis, J. O. Fajardo, P. S. Khodashenas, A. Albanese, H. Mouratidis and V. Vassilakis, “"System architecture and aspects of SESAME: Small cEllS coordinAtion for Multi-tenancy and Edge services",” *IEEE ICC,* 2016.

[14] I. Giannoulakis, J. O.Fajardo, J. Garcia, P.S. Khodashenas, C. Ruiz, E. Kafetzakis, J. Pérez, A. Albanese, M. Paolino, L. Goratti, R. Riggio, “Enabling Technologies and Benefits of Multi-Tenant Multi-Service 5G Small Cells,” in *EuCNC*, Athens, Greece, June 2016.

[15] Y. Liu. J. K. Muppala, M. Veeraraghavan, D. Lin, M. Hamdi, Data Center Networks: Topologies, Architectures and Fault-Tolerance Characteristics, Springer, 2013.

[16] H2020 SESAME project, “Deliverable 4.1 "Light DC Architecture Design",” (Retrieved: March 10, 2016).

[17] H2020 SESAME project, “Deliverable 2.2 "Overall System Architecture and Interfaces",” (Retrieved: June 2, 2016).

[18] European Telecommunications Standards Institute (ETSI), “NFV Management and Orchestration - An Overview,” *GS NFV-MAN001 V1.1.1,* 2014.

[19] I. Giannoulakis, E. Kafetzakis, I. Trajkovska, P. S. Khodashenas, I. Chochliouros, C. Costa, I. Neokosmidis and P. Bliznakov, "The emergence of operator-neutral small cells as a strong case for cloud computing at the mobile edge," *Transactions on Emerging Telecommunications Technologies,* vol. DOI: 10.1002/ett.3077, 2016.

[20] H2020 SESAME project, “Deliverable 2.1 "System Use Cases and Requirements",” (Retrieved: May 10, 2015).

[21] P.S. Khodashenas, C. Ruiz, J. Ferrer Riera, J. G. Lloreda, J. O. Fajardo, B. Blanco, J. Pérez-Romero, O. Sallent, I. Neokosmidis, T. Rokkas, “Service Provisioning and Pricing Methods in a Multi-Tenant Cloud Enabled RAN,” in *IEEE CSCN*, Berlin, 2016.

[22] S. Sharma, “Evolution of as-a-Service Era in Cloud. A review on as-a-Service Framework (white paper):,” *Center for Survey Statistics and Methodology, Iowa State University.,* Ames, Iowa, USA, 2015.

[23] M. D. Firoozjaei, J. Jeong, H. Ko and H. Kim, “Security challenges with network functions virtualization,” *Elsevier Future Generation Computer Systems,* 2016, 10.1016/j.future.2016.07.002.

[24] P.S. Khodashenas, J. Aznar, A. Legarrea, C. Ruiz, M.S. Sidiiqui, E. Escalona, S. Figuerola, “5G Network Challenges and Realization Insights,” in *ICTON*, Trento (Italy), 2016.

[25] European Telecommunications Standards Institure (ETSI), “Security Management and Monitoring for NFV,” *NFV-Sec013, Release 2,* 2015.

[26] M. Coldrey, H. Koorapaty, J. Berg, Z. Ghebretensáe, J. Hansryd, A. Derneryd and S. Falahati, “Small-Cell Wireless Backhauling: A Non-Line-of-Sight Approach for Point-to-Point Microwave Links,” in *IEEE Vehicular Technology Conference*, Quebec, 2012.

[27] U. Siddique, H. Tabassum, E. Hossain and D. Kim, “Wireless backhauling of 5G small cells: challenges and solution approaches,” *IEEE Wireless Communications,* vol. 5, pp. 22-31, 2015.

[28] S. Hur, D. Love, J. Krogmeier, T. Thomas and A. Ghosh, “Millimeter Wave Beamforming for Wireless Backhaul and Access in Small Cell Networks,” *IEEE Transactions on Communications,* vol. 61, no. 10, pp. 4391-4403, 2013.

[29] G. Xiaohu, H. Cheng and M. Guizani, “5G wireless backhaul networks: challenges and research advances.,” *IEEE Network,* vol. 28, no. 6, pp. 6-11, 2014.

[30] FP7 FLEX project, “D5.1 Report on first Open Call activities (SODALITE),” (Retrieved: February 12, 2016).

[31] A. Betzler, F. Quer, D. Camps-Mur, I. Demirkol and E. Garcia-Villegas, “On the Benefits of Wireless SDN in Networks of Constrained Edge Devices,” in *27th European Conference on Networks and Communications*, Athens, 2016.

[32] H2020 SESAME project, “Deliverable 3.1 "CESC Prototype design specifications and initial studies on Self-X and virtualization aspects.",” (Retrieved: February 20, 2016).