Mohammad Mahmoodian, Paper Reading #4

5 Softwarization and 5G Service Management and Orchestration

In this chapter we look at the advances in the design of the 5G management and orchestration plane to support the concept of slicing.

Network slicing refers to the existence of multiple, possibly isolated, service and network architectures to support different usage scenarios, in particular services hosted by different verticals. Network slicing has evolved as a fundamental feature of the emerging 5G systems enabling dynamic multi-service support, multi-tenancy and the integration means for vertical market players.

To be able to uniformly manage the multiple slices that an operator is expected to host, programming interfaces to the virtualization infrastructures need to be exposed. The infrastructure needs to be capable of hosting multiple tenants and to be able to distinguish between the various types of flexibility and control required in the virtualized cloud resources. This chapter covers these advances in Section 5.1 under advances in supporting technologies.

5.1 Enabling Technologies

Programmable virtualized infrastructure is considered a main supporting technology to realize slicing.

5.1.1 Multi-Tenancy Support

Multi-tenancy support is at the heart of the slicing-based business model for providing services. Without multi-tenancy, multiple simultaneously existing services cannot be provided by the 5G operator and rendering the concept of slicing moot.

While multi-tenancy support in the cloud environment already exists, for 5G the following three aspects of the multi-tenancy with respect to the Network Slicing design paradigm are considered:

- Infrastructure Sharing.
- Spectrum Sharing.
- RAN Sharing.
- Network Sharing: the underlying SDN technology has been extended by defining and integrating SDN-based controller paradigms in the form of SDM-O, SDM-C and SDM-X functional components.

5.1.1.1 Multi-tenancy in the RAN

The RAN sharing problem is related to the design and implementation of policies that are able to effectively schedule Resource Blocks effectively between different MVNOs with respect to specific differentiation objectives and with isolation guarantees.

5.1.2 Cloud and Virtualization Technologies

In the path toward network softwarization, the decomposition and modularity concepts will become increasingly relevant and the granularity of the decomposition will be finer. Software routers are an example: elementary packet processing functions can be composed to build a complex node function (e.g. a router/NAT/firewall). Hardware accelerators on NICs can execute packet processing functions designed in software. The architectural model for 5G should be flexible enough to support and take advantage from this heterogeneity.

The concept of VNF should be generalized to cover different type of functions (not only networking functions, but any kind of processing) and to cover a wide range of granularity in the definition of a VNF.

The concept of Reusable Functional Block (RFB) as a generalization of VNFs, and the concept of RFB Execution Environment (REE) to cover the heterogeneous infrastructure that can support the service execution.

5.1.3 Network Programmability

Programmability is a key supporting technology for the realization of dynamism in the 5G service and slice architecture.

In this section we look at the objectives of introducing programmability in a particular technology domain: the Radio Access Network (RAN) to create programmable abstracted network models for use at the higher layers in the orchestration framework.

A coherent representation of the network state and infrastructure resources is crucial for effective RAN coordination and control of programmable infrastructures and services.

At the low layers, the status information is abstracted and fed to the higher control layers to generate network views.

5.2 Services and Service Design

The ability to support multiple services simultaneously and dynamically is expected to be the driving force behind 5G success.

5.2.1 Service description

For the description of both individual network functions as well as entire services, a couple of de facto standards are emerging. The de facto standards start from the ETSI model and make some straightforward extensions.

The following subsections present a brief survey of the current service description standards performed within the 5GPPP.

5.2.1.1 ETSI NFV

ETSI NFV is actively working on the definition of Network Service Templates that could allow the instantiation of services, understanding them as a composition of several linked VNFs, including some information regarding the (virtual) links connecting them in the forwarding graph.

5.2.1.2 OASIS TOSCA

TOSCA, as defined by OASIS, serves as language and metamodel to describe services, its components, relationships and management procedures.

5.2.1.3 IETF Service Function Chaining

The Service Function Chaining (SFC) working group [5-8] in IETF defines a service architecture around three main components to be deployed in an SFC-enabled domain, used to compose the service end-to-end:

- Service functions (SFs)
- Service function forwarders (SFFs)
- Service classification functions (SCFs)

5.2.1.4 OGF NSI

The Network Service Information (NSI) [5-8] proposal of OGF allows for requesting Connectivity services including service-specific information as follows

- Ingress and egress Service Termination Points (STPs)
- Explicit Routing Object (ERO)
- Capacity of the Connection
- Framing information

5.2.2 On-demand composition

As a mechanism to achieve the mapping of the conventional and new telco services to the new Cloud-enabled infrastructures, Service Function Chaining (SFC) techniques have been applied.

Software Defined Networking (SDN) mechanisms for SFC [5-23] are the most prominent candidates to enforce traffic steering through a logical network graph and to achieve certain service functionality among the virtualized components.

To fully implement and support SFC, the conventional protocols plus some SDN adaptations can be used, or novel dedicated mechanisms can be adopted for a full compliance with the standards.

5.2.3 Verification of deployed services

The 5G network management architecture will allow operators and third parties to quickly instantiate services composed of network functions.

To ensure that we can provide high levels of reliability we need to have tools to assess the correctness of configurations using model checking.

Network data plane verification tools based on formal software verification techniques are an alternative and very promising approach. Such tools work by using a snapshot of the network data plane, including router FIBs, tunnelling configurations and VNF processing specifications and simulate what happens when a generic packet (with wildcard fields) is injected at one of the network ports.

Symnet, our symbolic execution tool, takes a network described in SEFL, together with links between boxes and a port where a symbolic packet should be injected.

The job of Symnet is to simulate how all the possible concrete packets will be treated by the given network: which path they will take, how their fields will be changed, when and whether they will be dropped, and so forth.

5.2.4 Machine learning in Service Planning

Machine learning services are proposed to be used to provide more efficient network management. The work presented on SLA management and monitoring as presented in Section 5.3 focuses on FCAPS (fault, configuration, accounting, performance and security).

The work done in 5GPPP phase 1 offers an integrated set of services that can be selected by operators based on the individual needs of an operator.

The services are offered in three layers, Data services are used to import and process the data required by the machine learning modules.

Machine learning services provide the core predictive functionality and the planning services orchestrate the predictive services for action recommendation and policy implementation.

The services are divided in five categories.

- Data Services
- Quality Assurance Services
- Network Demand Prediction Services
- Location-based Services
- Planning Services

5.3 Management and Orchestration

5.3.1 Embedding of Virtual Functions

Embedding or placing virtual network architecture that form a service is one of the most important aspects of 5G.

The heuristic mapping algorithm searches for (possibly a number of) embedding of service chains, considering a greedy step as the united mapping of a network function and an adjacent service graph link.

If the greedy search fails, a bounded backtracking procedure is responsible for exploring a subset of the state space by trying locally less preferred steps.

5.3.2 Service Assurance and Monitoring

The 5G deployment envisions that a number of inter-operating virtualisation environments are used, some of which provide integrated telemetry (monitoring) solutions such as Celiometer in OpenStack.

A specific case in 5G is the telemetry platform that can be used to support diverse virtualised environments and bare metal.

5.3.3 Life-Cycle Management

5G will be built upon softwarisation and virtualization technologies, particularly SDN and NFV. The 5GPPP effort has designed and prototyped a complete management of SDN and NFV Apps, thereby paving the way for truly dynamic, on-demand, flexible and automated/autonomic SDN/NFV service deployment through an orchestrator. This Apps Management subsystem has the following advantageous features. Firstly, it provides a fully automated lifecycle management of NFV and SDN applications, Secondly, it provides common Apps lifecycle mechanisms and procedures for various kinds of Apps including VNFs, SDN Apps, SDN controller Apps, and Physical Network Functions (PNFs) for backward compatibility.

5.3.3.1 Automated deployment of physical and virtual infrastructures

The 5GPPP effort has achieved integrated management of physical and virtual infrastructures, which enables automated deployment of 5G infrastructures and services running on top of them, including virtualization services, cloud computing, Multi-access Edge Computing (MEC), SDN/NFV services and valueadded services such as Service Function Chaining (SFC).

Management of the physical layer has been achieved by using the latest version of the MaaS software package provided by Ubuntu.

5.3.4 Multi-Domain and Multi-Operator Operation

The key component of 5G is going to be the inclusion of verticals into the telecommunication evolution.

To achieve multi-operator interaction work has been done in defining the interfaces and components between the operators' multi-domain orchestrators (MdOs).

While the business level relationships such as pricing are not yet clarified the catalogue management system implements the service repository.

The components of the architecture for inter-operator orchestration can be classified into three main groups, according to the core functionalities of the MdO.

- Components that gather resource and service related information: are responsible for capabilities and resource acquisition.
- Components that relate to the orchestration procedure: are responsible for service request deployment (e.g., orchestration)
- Assurance components for the deployed service: are in charge of service assurance and SLA management

The main challenge of multi-domain operations comes from the fact that each operator exposes a very limited/abstracted view of the topology to other operators.

5.3.4.1 Secure Multi Domain Interfaces

The security of such a multi-operator instantiation entails multiple actors who are using different MdO interfaces, and a trust model needs to be defined for each of them.

The following actors inside MdO security trust model have been considered:

- Customers (tenants) interact with Multi Domain Orchestrator (MdO) through interface I1 (B2C interaction), that provides a set of services to operate with VNFs and NSs. These customers are 'private' to the MdO they're interacting with.
- MdOs collaborate one with another (B2B interaction) using I2 services. These services are exclusive for the MdO to MdO communication, and can't directly be used by other actors.
- The SW modules and components of an implementation of MdO are another relevant actor for the security, and need to be protected inside an MdO specific trusted zone of the provider space.