Project Number:	**CELTIC / CP2012-2-5**
Project Title:	SDN Concept in Generalised Mobile Network Architectures– SIGMONA
Document Type:	I (Internal)

Document Identifier:	D 1.2
Document Title:	**2nd Consolidated view of SIGMONA Software Defined Mobile Network Architecture**
Source Activity:	WP 1 - Software Defined Mobile Network Architecture
Main Editor:	Tero Lotjonen, Costa Requena Jose, Olivier Jard
Authors:	All partners contributed, see the list of main authors below
Status / Version:	Draft / 1.0
Date Last changes:	14.01.2016
File Name:	SoftwareDefinedMobileNetwork_Architecture-D1.2.doc

Abstract:	SIGMONA project SDMN architecture mapping to the ETSI ISG NFV architectural framework. Main SDMN Basic assumptions redefinitions.

Keywords:	Architecture, SDMN, SDN, NFV

Document History:	
08.04.2015	Document created with D1.1-1
24.12.2015	Partner contributions
14.01.2016	Added partners reviews

Table of Contents

Authors

Partner	Name	Phone / Fax / e-mail
AALTO	Jose Costa-Requena	
		Phone: +358 5 0577 0142
		E-mail: jose.costa@aalto.fi
Nokia Networks Finland		
	Tero Lötjönen	
		Phone: +358 40 5747842
		E-mail: tero.lotjonen@nokia.com
	Pekka Korja	
		Phone:
		E-mail: pekka.korja@nokia.com
	Jukka Salo	
		Phone:
		E-mail: jukka.salo@nokia.com
Nokia Networks Hungary	Zoltan Vincze	
		Phone: +36 20 977 7797
		E-mail: zoltan.vincze@nokia.com
Technical University of Budapest – Mobile Innovation Centre		
	László Bokor	
		Phone: +36 1 4633420
		E-mail: bokorl@hit.bme.hu
	Zoltán Faigl	
		Phone : +36 1 4633420
		E-mail: zfaigl@mik.bme.hu
Bull SAS		
	Gérard Jacquet	
		Phone :
		E-mail : gerardjacquet@atos.net
	Olivier Jard	
		Phone:
		E-mail: olivier.jard@atos.net
	Patrick Crambert	
		Phone:
		E-mail: patrick.crambert@atos.net

Coriant	Juha-Petteri Nieminen	
	Phone:	+358 40 41312215
	E-mail :	juha-petteri.nieminen@coriant.com

TT Argela		
	Aydın Ulaş	
	Phone :	+90 212 707 1259
	E-mail :	aydin.ulas@argela.com.tr
	Serdar Tan	
	Phone :	
	E-mail :	

AVEA	Engin Zeydan	
	Phone:	+90 216 987 6386
	E-mail:	engin.zeydan@avea.com.tr

Technical University of Chemnitz	Thomas Bauschert	
	Phone:	
	E-mail:	thomas.bauschert@etit.tu-chemnitz.de

Montimage	Edgardo Montes de Oca	
	Phone :	+33 1 77 19 68 99
	E-mail :	edgardo.montesdeoca@montimage.com

CWC	Suneth Namal	
	Phone:	+358 41 7282646
	E-mail:	gkarunar@ee.oulu.fi

EXFO	Kari Hyväri	
	Phone:	+358 40 3010317
	E-mail:	kari.hyvari@exfo.com

CEA		
	Mohamed LABRAOUI	
	Phone :	
	e-mail :	mohamed.labraoui@cea.fr
	Michael BOC	
	Phone :	
	e-mail :	Michael.boc@cea.fr

VTT			
	Kari Seppänen		
		Phone:	
		E-mail:	kari.seppanen@vtt.fi
	Pirkko Kuusela		
		Phone:	
		E-mail:	pirkko.kuusela@vtt.fi

Executive Summary

In the context of frequent transformation and evolution, Mobile Telecommunication carriers are aiming to turn to the deployment of Telecom services through carrier grade SDN/NFV infrastructure. Historically, telecom applications were provided in a silo fashion, in the form of costly proprietary appliances that are hardly scalable.

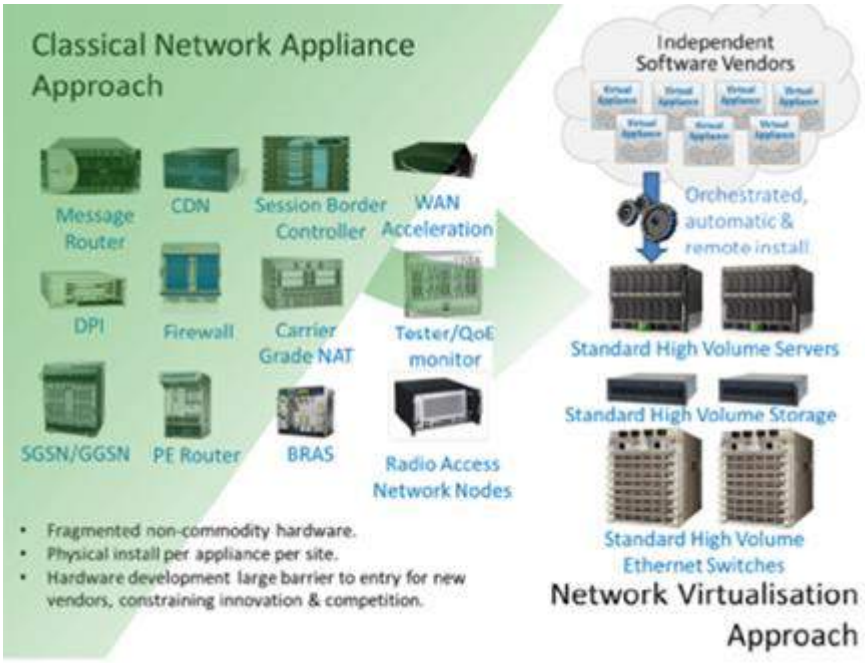

Figure 1: Vision for Network Function Virtualisation

SDN/NFV is an attempt to provide better control and automation of resource management (e.g., network, computing and storage) by dynamically allocating the resources to meet the needs of consumers and corporate customers. The shift from classical network appliance approaches to network virtualisation approaches in shown in Figure 1. Instead of just *Best Effort* services, SDN/NFV can be used to provide Carrier Grade Services (CG). CG means that there is a clear definition of the traffic, its properties and the path of the traffic. The goal is to provide elastic and agile tailoring of the resource allocations to the demand. Due to the control plane and data plane split, SDN provides better hardware independence for the operators. In addition, NFV and the use of standard datacentre hardware provides economies of scale in computing and storage resources.

SDN's centralised controller system provides the possibility to differentiate the service by controlling what service is available to whom and where. Centralisation makes it easy to implement many functions that are uneconomical or infeasible in a distributed setting. Examples include: residual capacity routing for network provisioning; better network based end system security through the enforcement of consistent policies irrespective of location/roaming; sharing evidence of malicious activity and aggregation of this evidence; and, introduction of reputation based methods.

From the business side, the SDN/NFV architecture lowers the initial network investment, energy consumption and network management costs for the MNOs. At the same time, SDN/NFV encourages openness and competition, as well as promotes new investments into the mobile connectivity and content industry. In addition, SDN/NFV changes the competitive advantage of the different operator types (e.g., challenger, incumbent, global hub, virtual infrastructure, cloud/non-cloud) with each other and with the infrastructure vendors. SDN/NFV also opens the possibility for each service provider to decide what exactly needs to be invested in infrastructure, software or customer service; as well as, determine what is needed to increase the speed at which the new services are implemented and delivered.

This document completes the D1.1 SIGMONA consolidated view of Software Defined Mobile Networks (SDMN) architecture [1]. It focuses on mapping the defined SIGMONA architecture model to the ETSI ISG NFV architectural framework. The goal is to ensure future proof-of-concept solutions that take into consideration the standardisation guidelines. In addition, D1.1 defined various requirements for future networks that have led to the definition of a set of basic assumptions and uncertainties.

A selection of requirements and basic assumptions have been refined to identify a set of strategies, proof-of-concept solutions, use cases and associated metrics.

List of terms, acronyms and abbreviations

Active communication	In 3GPP, (PS) active communication is defined by the existence of one or more Activated PDP contexts that generate IP traffic to/ from servers or/and end users. For Evolved Packet System (EPS) term EPS bearer context [2] is used. Active communication is required to perform an Activity in the Use Case.
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Controller	Logical realization of the SDN control plane where a centralised SW element manages/controls the SDN data plane.
End-to-End (E2E) Architecture	An architecture encompassing all NFs and resources owned by an operator
Hypervisor	Also called virtual machine manager (VMM), is one of many hardware virtualisation techniques allowing multiple operating systems, termed guests (VMs), to run concurrently on a host computer. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems.
Independent Software Vendor (ISV)	An ISV makes and sells software products that run on one or more computer hardware or operating system platforms.
LTE network elements	The network components required in LTE control plane such as MME, P/S-GW, PCRF, AAA, etc.
Multi-tenancy	Enables sharing of resources and costs across a large pool of users thus allowing for: Centralisation of infrastructure in locations with lower costs (such as real estate, electricity, etc.), Peak-load capacity increases (users need not engineer for highest possible load-levels), Utilization and efficiency improvements for systems that are often only 10–20% utilised.
Network Function (NF)	A functional building block within an operator´s network infrastructure, which has well-defined external interfaces and a well-defined functional behaviour. Note that the totality of all network functions constitutes the entire network and services infrastructure of an operator/service provider. In practical terms, a Network Function is today often a network node or physical appliance.
NF forwarding graph	A graph specified by a Network Service Provider of bi-directional logical links connecting NF nodes.
NF set	A collection of NFs with unspecified connectivity between them
Network virtualisation	The process of combining hardware and software network resources and network functionality into a single, software-based administrative entity, a virtual network. Network virtualisation involves platform virtualisation, often combined with resource virtualisation.
Network Function Virtualisation Infrastructure (NFVI)	The Network Function Virtualisation Infrastructure (NFVI) contains all the hardware and software components that constitute the environment in which VNFs of the MNO are deployed, managed and executed. The NFVI includes resources for computation, networking and storage.
Resource management	Resources can be physical resources, logical elements, processes in the cloud, etc. Both user plane and control plane resources.
Resource pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacentre). Examples of resources include storage, processing, memory, and network bandwidth.

Software Defined Networking (SDN)	A term used for networks in which the control plane is decoupled from the data plane and made the control plane remotely accessible and remotely modifiable via third-party software clients. SDN requires some method for the control plane to communicate with the switch data path. One such mechanism is OpenFlow protocol.
Virtualisation	Hardware virtualisation or platform virtualisation refers to the creation of a virtual machine (VM) that acts like a real computer with an operating system, but is separated from the underlying hardware resources. Technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.
Virtual Machine (VM)	A program and configuration of part of a host computer server. Note that the Virtual Machine inherits the properties of its host computer server e.g. location, network interfaces. A completely isolated guest operating system installation within a normal host operating system. Modern virtual machines are implemented with either software emulation or hardware virtualisation or (in most cases) both together.
Virtualised Network Function (VNF)	An implementation of an executable software program that constitutes the whole or a part of an NF that can be deployed on a virtualisation infrastructure.
VNF Forwarding Graph (VNF-FG)	A NF forwarding graph (of logical links connecting NF nodes) where at least one node is a VNF through which network traffic is directed for the purpose of creation a set of network functions. (ETSI NFV term for Service chaining)
VNF set	A NF (Network Function) set where all the NFs are VNFs.
Virtualisation levels	Different levels of virtualisation; 1) transport network, 2) full LTE network including transport and network elements

AAA	Authentication, Authorization and Accounting
AF	Application Function
AKA	Authentication and Key Agreement
ALTO	Application-Layer Traffic Optimization
AMNS	Automated Mobile Network Slicing
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
API	Application Programming Interface
APN	Access Point Name
CAPEX	Capital Expenditure
CDN	Content Delivery Network
CDR	Charging Data Record
CES	Customer Edge Switching
CG	Carrier Grade
CGF	Charging Gateway Function
COTS	Commercial off-the-shelf
CQI	Channel Quality Indicator
C-RAN	Cloud Radio Access Network
DB	Database
DMM	Dynamic Mobility Management
DoS	Denial-Of-Service
DPI	Deep Packet Inspection
ECM	EPS Connection Management
EMM	EPS Mobility Management
EMS	Element Management System
eNB	Evolved Node B (eNodeB)
EPC	Evolved Packet Core

ePDG	Evolved Packet Data Gateway
ESM	EPS Session Management
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FCA	Flow Control Agent
GRX	GPRS Roaming eXchange
GTP	GPRS Tunnelling Protocol
HIP	Host Identity Protocol
HO	HandOver
HSS	Home Subscriber Server
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IFOM	IP Flow Mobility and Seamless WLAN Offloading
ISAAR	Internet Service quality Assessment and Automatic Reaction
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IPX	IP eXchange
IPS	Intrusion Prevention System
JSON	JavaScript Object Notation
LMA	Local Mobility Anchor
LTE	Long Term Evolution
MAC	Medium Access Control
MAG	Mobile Access Gateway
MDM	Mobile Device Management
MIH	Media Independent Handover (IEEE 802.21)
MIP	Mobile IP
MM	Mobility Management
MME	Mobility Management Entity
MNO	Mobile Network Operator
MPLS	Multiprotocol Label Switching
NF	Network Function
OCS	Online Charging System
OF	Open Flow
OFCF	Offline Charging Function
OPEX	Operating Expenses
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-GW	Packet Data Network (PDN) Gateway
PHB	Per Hop Behaviour
PLMN	Public Land Mobile Network
PMIP	Proxy Mobile IP
QoE	Quality of Experience
QoS	Quality of Service
RAT	Radio Access Technology
REST	REpresentational State Transfer
SCTP	Stream Control Transmission Protocol
SDM	Software Defined Monitoring
SDMN	Software Defined Mobile Network
SDN	Software Defined Networking

SIEM	Security Information and Event Management
S-GW	Serving Gateway
SON	Self-Organizing Network
SPAP	Security Policy Administration Point
SSL	Secure Socket Layer
TDF	Traffic Detection Function
TLS	Transport Layer Security
TNO	Transport Network Operator
TRILL	Transparent Interconnection of Lots of Links
UE	User Equipment
UFA	Ultra Flat Architecture
VIM	Virtual Infrastructure Manager
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMNO	Virtual Mobile Network Operator
VoLTE	Voice over LTE
VPN	Virtual Private Network
WLAN	Wireless Local Area Networks

1. Introduction

Concepts such as Network Function Virtualisation (NFV), Software Defined Network (SDN) and open protocols such as OpenFlow (OF) become the key enablers for the next generation of mobile networks.

Ultimately, the value of such approaches resides in the fact that it extends the dynamic scalability and malleability of virtualisation to the underlying network domain.

However, this is possible only if the strong constraints of telecom applications are addressed. These are:

- Support very high network loads and / or the ability to handle large bandwidth variations without degrading the quality of service. The concept of "capacity on demand" should be extended to the network elements.
- Guarantee real-time performance. Using appliances on generic x 86 infrastructures but also the introduction of centralised management concepts. SDN must not jeopardize the performance requirement of telecom networks.
- Assure carrier grade availability. The redundancy principles and tolerance requirements must be preserved or improved with these new ecosystems.
- Provide coexistence with legacy networks.

The integration of SDN/NFV in mobile networks requires maintaining basic functionalities such as policy control and charging. Scalability, security and resiliency are key factors to be taken into account if SDMN is to become the next infrastructure for 5G mobile networks. Finally, SDMN should bring some benefits to both mobile operators as well as the end user.

The SIGMONA architecture considers multiple options for the placement of the SDN controller. We introduce a vision for integrating SDN in the mobile network, where mobile specific functionalities are implemented as SDN applications.

2. Scope of the document

This document presents the SIGMONA partners' research in the areas of Network Function Virtualisation and Software Defined Networking applicable to mobile core and transport networks.

It proposes a consolidated partner SDMN architecture mapping to the ETSI ISG NFV referential framework.

The requirements and basic assumptions identified during the project have been refined to propose a set of proof-of-concept solutions, use cases and associated metrics. This has led to the definition of Key Performance Indicators that allow quantifying the benefits that are expected to be obtained over current architectures.

3. Main SDMN Basic assumptions definition

3.1 Migration: Compatibility with the legacy systems vs. Clean-slate deployment

The integration of SDN and network function virtualisation into LTE should minimize the changes in network elements, thus providing a seamless migration based on operator needs. This allows incremental updates of network elements in certain parts of the network while keeping legacy elements in other parts of the network. Multivendor compatibility is considered an underlying challenge in SIGMONA. When specifying the new SDN/virtualisation/cloud technology-based systems for mobile telecommunications the clean-slate approach (i.e., full deployment at once) is not an option to be followed. In SIGMONA, legacy support has been determined as a major requirement; but, the migration should also enable the adoption of new technologies that are currently being defined, such as Device-to-Device (D2D) communications.

3.1.1 SIGMONA Approach

Before migrating to these new technologies, Service Providers need to identify their main objectives.

CAPEX/OPEX saving and fast deployment of services may be key drivers, but it is also important to identify where to use SDN technologies. The main target areas that have been identified are:

1. IP Routing Configuration and Service Automation
    - Service Provisioning of existing infrastructure,
    - vPE,
2. Data center network
    - Data Center Service Elasticity,
    - Service Chaining: Multi-Layer / Data Center Service Chaining,
    - DPI / Policy based Service Chaining,
    - Virtual CDN deployment with traffic optimization,
    - Video optimization,
3. WAN Transport Network
    - Traffic Engineering,
    - Network / Service Restoration,
    - Converged Transport Controller across packet and optical,
4. WAN to Data Center connectivity
    - Dynamic end to end bandwidth regulation,
5. SDN based Network Programmability & Application Awareness
    - HTTPs / HTTP 2.0 traffic steering,
    - Intelligent Traffic Management & Delivery,
    - Dynamic vCDN deployment,
6. Gateway end to end deployments

- vHGW,
- vCPE,
- Virtual Enterprise,

The complexity of the solution depends on the migration strategy. Figure 2 below illustrates the basic target architecture where the network logic is decoupled from physical location. 3GPP already separated the user and data planes for specific mobile functionality, but SDN and NFV go further and separate networking functionality into control and data planes.

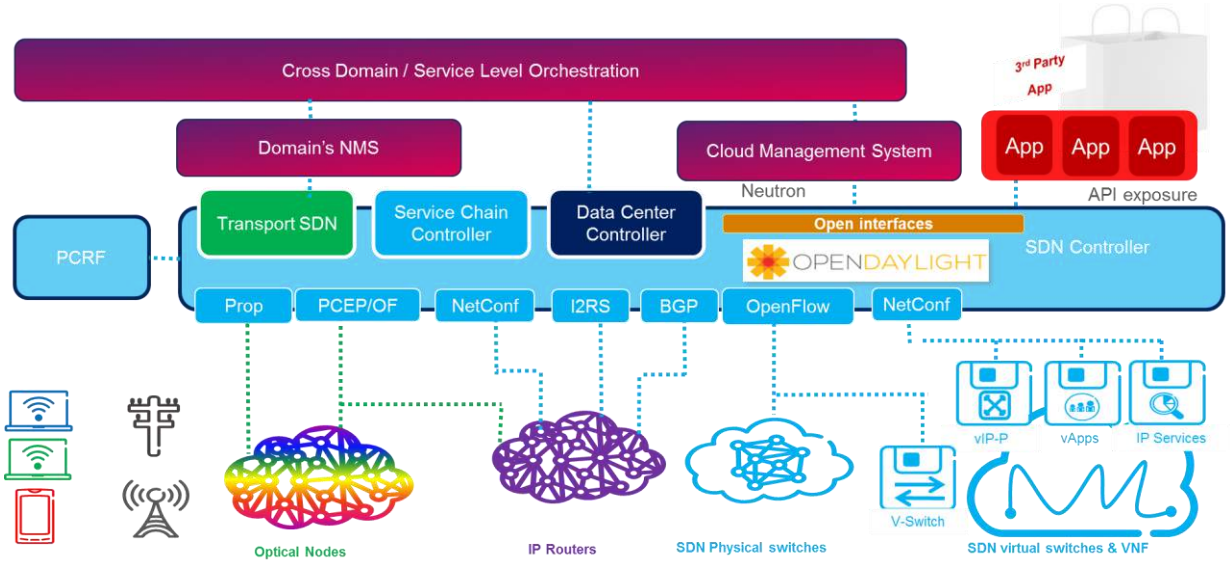

Figure 2: Target Architecture

3.1.1.1 SIGMONA Migration Strategy

Open Network Foundation Migration Body specifies a few migration methodologies [3]. The best approach identified by the SIGMONA partners is presented here.

Introduction of new technologies always remain a great challenges at the time of deployment in real settings as they can raise the need to redefine the organisation and the competencies required. The **mixed-approach** can minimize the risks by allowing progressive deployment. It consists of deploying an OpenFlow Switch between Gateways and services as shown in the Figure 3 below.

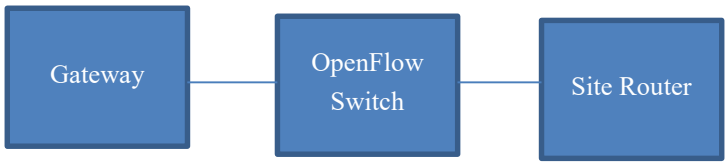

Figure 3: Mixed Approach

The benefits of this approach are that legacy networks could remain unchanged. On the other hand, a disadvantage is that new switching equipments need to be deployed.

Note that the use of hybrid equipments can be an option. Hybrid means that legacy and OpenFlow switching functions are supported by the same equipment. The disadvantage of this method is that existing network nodes need to be replaced or upgraded with a potential impact on existing traffic and services.

Datacentres

Datacentres can greatly benefit from Software Defined Networking and Network Function Virtualisation.

Multiple tenants must typically share the same physical resources. Virtualisation of computing resources has become almost a necessity, with robust features such as Virtual Machine migration facilitating a variety of capabilities, including resource balancing, maintenance, and disaster recovery. Soft Switches within the computing resources themselves are a dominant component of the architecture. Scalability of the datacentre implies the scalability of the overlay network as well. Software Defined Networking devices help address these requirements.

Datacentres, especially small to mid-scale enterprise centres, have already benefited from virtualisation and SDN concepts. These datacentres go well with **green-field migration** where end-to-end OpenFlow architectures are used. However, existing datacentre deployments are subject to mixed-network implementations that need to follow a phased approach before reaching the target architecture.

Transport Networks

IP/MPLS networks use routing protocols (e.g., OSPF, BGP) to control packets forwarding. When introducing SDN into an IP/MPLS network, it is unrealistic to expect moving all nodes to SDN planes.

This means that nodes that are not under SDN control continue to expect routing protocol exchanges with nodes that are under SDN control. The Hybrid mode is the case where a node supports SDN control interfaces and legacy routing protocols. This mode is only required in those nodes that are connected to non-SDN controlled legacy elements.

Deploying segment routing concepts is important here. Controlling labels across subsets of regions will make deployment of service controlled network concepts easier to realize.

3.2 Resilience: Fault tolerant SDN/NFV based mobile networks

SDN based networks should be fault tolerant and fall back to standard behaviour. This means that it is necessary that the last best known flow tables/actions or the preconfigured flow tables/actions are to be used as default in case of a failure. The SDN networks should not be prone to misconfiguration and should avoid single points of failure that could be introduced by centralised controllers. The SDN based mobile networks should fulfil similar levels of reliability as are obtained by current mobile networks: 99,999% availability. The flexibility of the SDN concept might facilitate finding a good trade-off between complexity and reliability. The controller can move redundant modules of the network to reinforce reliability in parts as needed, thus providing sufficient reliability with reasonable complexity.

3.2.1 SIGMONA approach

Resilience is a very wide topic as it covers trustworthiness and challenge tolerance (i.e., tolerance to different types of problems such as faults, traffic peaks, etc.). Trustworthiness consists of dependability, security and performability. It refers to measurable quantities of a network that are seen from the outside (e.g., availability). Challenge tolerance consists of survivability, disruption tolerance and traffic tolerance. It involves issues related to internal system design with impact from the outside.

For SIGMONA the scope of resiliency needs to be narrowed significantly and security related issues are not addressed under resilience. Because SDN/NFV is a major change in technology and logic of communication networks, the focus of resilience is related to assuring good internal system design. SDN/NFV can provide means to improve resilience of networks but it may also introduce unforeseen side effects and problems. Given the early stage of solutions in SIGMONA, the first approach should be to capture internal system design resilience problems and then focus on measurable and performance aspects of resilience.

The topics of challenge tolerance are:

Survivability: There are many failures present in the network. Note that with many failures the perfect network state information may not be a realistic assumption. Monitoring of the network may be only partial and information on components may be incorrect. Monitoring typically relies on the same network that is being monitored. Thus failures could degrade the network and the monitoring at the same time. Furthermore, network partitioning may prohibit obtaining the necessary information.

Fault tolerance: There are few and random failures present in the network. The situation is more challenging when there are few failures with abnormal conditions (such as increased legitimate traffic or delays). Note that in some cases it is not failures, but the traffic, that causes the network to collapse. This may happen particularly when there is a common external cause for network failures and an increase in traffic.

Disruption tolerance: This topic covers the examination of the level of disruption tolerance due to the networking environment (e.g., delays or mobility) and due to the physical environment (e.g., loss of energy or loss of connectivity due to heavy rain).

Traffic tolerance: This topic covers the examination of the level of tolerance to legitimate traffic with focus on performance and QoS issues.

Robustness against misconfiguration: SDN provides efficient means for network configuration, but also for unintended misconfigurations. How is the SDN network protected from misconfigurations? Virtualisation and dynamic reconfiguration can also be a source of errors. SDN may help by easing software configurations, but on the other hand the number of configuration may increase and lead to misconfiguration events. With SDN a misconfiguration can quickly affect a large portion of a network.

3.2.2 SIGMONA Resiliency Strategy

The SIGMONA partners have analysed the different use cases that lead to system unreliability. These use cases are summarised in the Appendix 7.1 and 7.2. In the following is presented the proposed strategy to address these use cases to increase the system's reliability.

3.2.2.1 VIM Controller Resiliency

Controller clustering, High Availability and load balancing of each service can be done using the following functions or elements:

- HAProxy: VIP Management for services and load balancing.
  Loss of services on a controller will not affect the service except for the live request on the failing node.

- Pacemaker: Cluster resources management.
  It is the central high availability component of the controller nodes. Pacemaker is in charge of starting, stopping and checking the cluster resources. The clustering management node is based on a quorum algorithm where each node owns a vote. The cluster will keep alive if there is at least a minimum quorum of two votes, and the faulting node will be stopped.

- Other Clustered functions: Rabbitmq cluster, Mongodb cluster and MySQL cluster (Galera).

The Table 1 below lists the mode of operation of each of the services to ensure high availability.

Components	Subcomponents	Functionality	HA Mode	HA functionalities
Horizon	*	IHM	Active/Active	HAProxy/Pacemaker
Keystone	*	Identity Management(token)	Active/Active	HAProxy/Pacemaker
Nova	*	VNF Management	Active/Active	HAProxy/Pacemaker
Neutron	* (connectivity L3 Excepted)	Network Management	Active/Active	HAProxy/Pacemaker
	Connectivity L3	Routing L3 et NAT 1 pour 1	Active/Passive	HAProxy/Pacemaker
Cinder	cinder-api	Api Cinder	Active/Active	HAProxy/Pacemaker
	cinder-scheduler	Cinder Scheduler	Active/Active	HAProxy/Pacemaker
	cinder-volume	Volumes management	Active/Passive	HAProxy/Pacemaker
Glance	*	Images Management	Active/Active	HAProxy/Pacemaker
Ceilometer	* (agent-central excepted)	Performances Management	Active/Active	HAProxy/Pacemaker
	ceilometer-agent-central	polling stats resource's	Active/Passive	HAProxy/Pacemaker
Heat	* (engine excepted)	Stack Management	Active/Active	HAProxy/Pacemaker
	heat-engine	Heat Orchestration	Active/Passive	HAProxy/Pacemaker
rabbitMQ	*	inter-components message management	Active/Active	Interne/Pacemaker/HAProxy
MySQL	*	OpenStack database	Master/Master	Galera/HAProxy/Pacemaker
MongoDB	*	Ceilometer database	Primary/Secondary	Replication internal REPLICATION/Pacemaker

Table 1 : High Availability Controller services

3.2.2.2 VIM Compute node resiliency

As shown in the Figure 4 below, five levels of failures can occur depending on the causes of the component failures (Table 2).

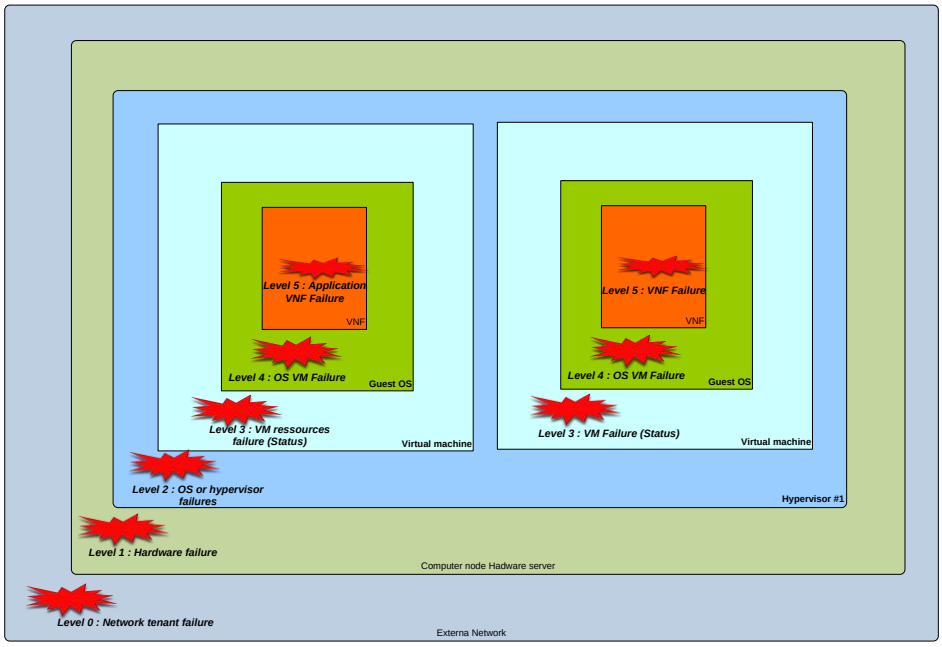

Figure 4 : Hypervisor level failure.

In each case, a dedicated action is triggered to resume the VNF to nominal state.

levels	Cause	Watchdog detection	Resilience actions
0	Hypervisor network failure: Server is unreachable or one of these interfaces is down.	Check snmp hypervisor OS status Check network reachability	Cold evacuation of hosted VM
1	Hardware Server hypervisor is down and unreachable (power off, memory or CPU failures…).		

2	Operating system hypervisor is down		
3	Hypervisor resource or services failures	Check hypervisor services Check hypervisor resources (vcpu/vmem/vdisk...)	Restart services or evacuate hosted VM
4	VM unreachable (VM network unreachable, SNMP status fails…)	SNMP status request to OS VM through the tenant networks	Restart VM or cold evacuation of hosted VM
5	VNF failure	Not Applicable	Managed By VNF.

Table 2 : Failures Description

An external watchdog dedicated to the hypervisor node monitors each hypervisor to detect failure events and react to recover to nominal state.

To check the hypervisor node's health the following actions are done:

- Check the server SNMP status to detect levels 0, 1 and 2 failures,
- Check the hypervisor service or process to detect level 3 failures,
- Check the hypervisor's global state from the controller,
- Check the VM states to detect level 4 failures.

Recovery principles are shown in the figures that follow.

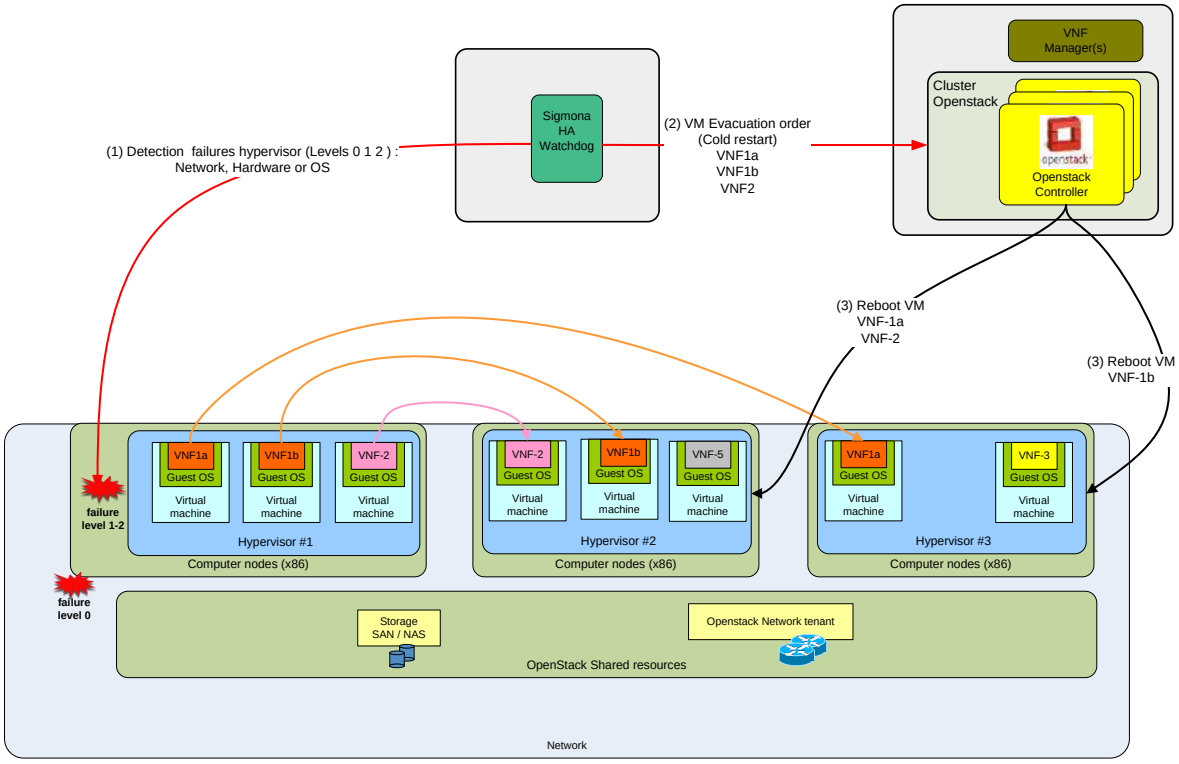

Figure 5 : Hypervisor level failures and VM evacuation (level 0, 1, 2)

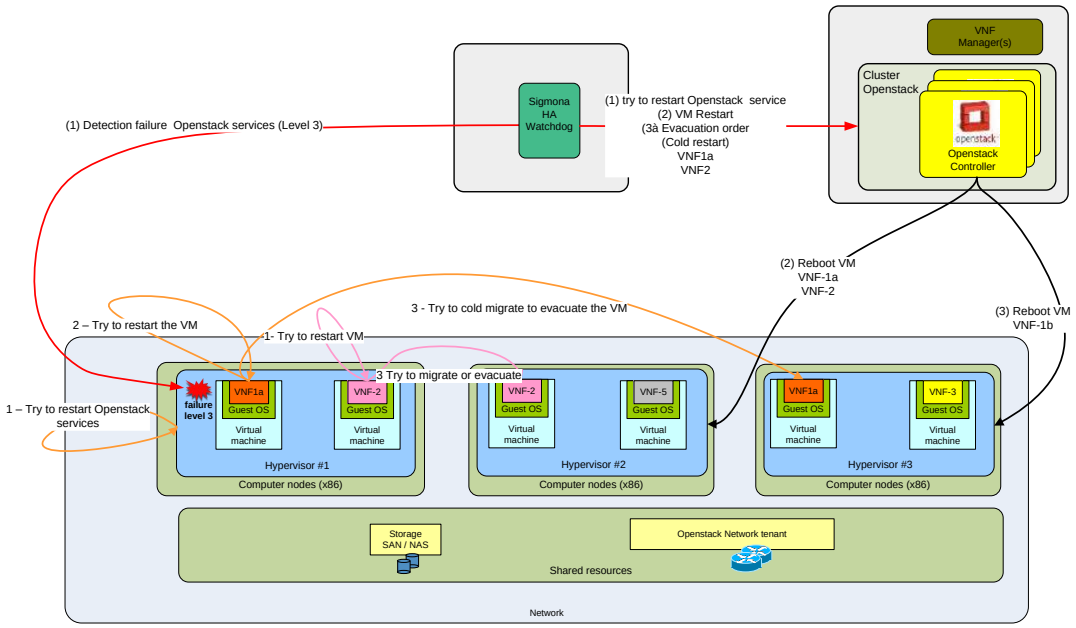

Figure 6 : Hypervisor service failures and VM evacuation (level 3)

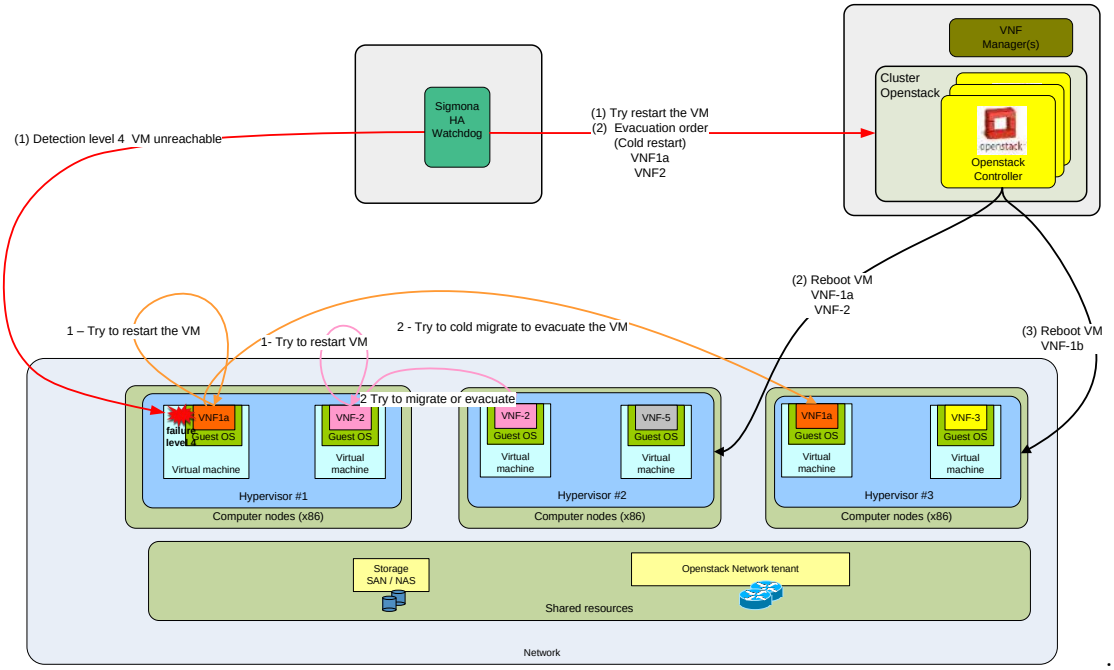

Figure 7VM failure and recovery (level 4)

VM evacuation from a hypervisor is done in either live or in cold modes. The type of evacuation will be done according to the VM initial state and the type of storage used.

A live evacuation will be only done for VM using an external storage shared between hypervisors. Otherwise, if storage is located on the local hypervisor's disk, the VM will be always be restarted in cold mode (i.e., shutdown and reboot).

When a hypervisor failure is detected, the watchdog searches all the hosted VM on the faulty device to be restarted. The hypervisor is then disabled.

The cold evacuation is done with the following actions:

- Stop and kill the VM,
- Reboot it (Cold evacuation).

3.3 QoS provision in virtualised mobile core networks in SDN-based forwarding paths

The usage of policy control is optional in operator networks, therefore it depends on the operators' decision whether it will be applied in the future. Until this time the RAN part of the network represented the bottleneck, hence QoS rules had to be applied in RAN. Assuming that the transport network guaranty sufficient bandwidth, over-provisioning is the common applicable method.

3.3.1 SIGMONA approach

Our assumption in the SIGMONA project is that dynamic, service data flow-based policy control will be more and more needed by mobile network operators due to the increasing diversity of services and the related policy rules. Hence, in general, the QoS provisioning mechanisms specified by 3GPP, such as EPS bearers or PDP contexts and policy control by PCRF should be kept also in case of virtualisation of mobile core and transport network.

The service-chaining concept requires network function forwarding paths both through virtual and traditional transport network segments. Operators need to be able to control logical and physical interconnections, configure traffic class conditioning and forwarding behaviours (capacity, priority, packet loss, delay, shaping, dropping etc.), and to map traffic flows to appropriate forwarding behaviours.

3.3.2 SIGMONA QoS provisioning strategy

SIGMONA partners have identified a set of QoS metrics (Table 3) for monitoring in order to improve the QoS provisioning in the system. The QoS monitoring system will communicate these metrics to the system manager or orchestrator in order to reduce those metrics.

#	Use Cases Description	Proposed metrics
1	QoS in SIP Messaging with SDN	Packet Loss, Latency
2	Optimal routing	Power consumption, Link utilization

Table 3 Proposed Use Cases and Metrics

3.4 Managing the security functions of physical and virtual elements and interfaces

Security in virtual and SDMN will be managed using centralised controllers. This necessitates that the controller must be secured and security of virtual and physical network elements and interfaces need to be managed and assured. Virtual and Software Defined Network techniques make it easier to modify and configure network functions using centralised controllers, making it not necessary to intervene directly on different network elements. This makes a controller a critical element in the network that needs to be secured, guaranteeing high availability at all times.

The security management is referring to the way of controlling/managing the security function in the physical or virtual network interfaces (e.g.,. doing packet inspection) and what is the relationship with the virtualised elements (e.g., SDN controllers, virtual FW running in the cloud). The virtual security components need to be able to identify to which virtual network the packets belong to in order to apply the required security policy.

It is assumed that besides securing the controller, the virtual network elements and interfaces are secured, and both MNOs and Virtual MNOs can define and manage their security policies.

3.4.1 SIGMONA approach

The SIGMONA partners have studied the delays incurred due to security systems. The main motivation is to maintain a minimal level of delay when deploying security functions. Moreover, the security-delay cost trade-off should be within the defined constraints so that it does not deteriorate network performance. Delay in maintaining security of a network is unavoidable but can be delimited. Security systems (or functions) for communication networks are broadly categorised into the following by ITU-T:

- Access Control,
- Authentication,

- Non-Repudiation,
- Data Confidentiality,
- Communication Security,
- Data Integrity,
- Availability,
- Privacy.

Delay due to security systems depends on the type of security it provides. The above security mechanisms could be categorised according to the delay in the following:

- Authentication, Access control, Availability,
- Communication Security, Data integrity, Privacy, Data Confidentiality and Non-Repudiation,
- Security monitoring (include security systems for IDS/IPS/DoS attacks or any of the above).

For security, monitoring the delay could be caused by:

- Delay in reading/capturing the necessary information,
- Delay in assessing/analysing the information,
- Delay in implementing corrective measures (e.g., performing counter-measures).

3.4.2 SIGMONA security delays strategy

The SIGMONA partners have analysed the different security threats and the security delays (detailed in the Appendix 7.4) incurred when applying current solutions to address these threats. Following this analysis a set of metrics and solutions have been proposed as shown in the following Table 4.

Security System	**Reasons for Delay**	**Metrics or KPI**	**Implementation in h/w, s/w and SDN Plane i.e. App. Plane/ Ctrl. Plane/ Infra. Plane**
Security management and monitoring: Two monitoring techniques can be used: **passive** (non-obtrusive monitoring) and **active** (monitoring probes act as FW). Passive will not disrupt the network traffic but does not allow to react to block unwanted traffic in near real-time. The use of one or the other depends on the security use case and its requirements.	**Active** monitoring: processing of traffic incurs delays and will vary according to what type of analysis is required (packet headers, DPI, DFI) and how many rules need to be verified. Blocking traffic (filtering) will not introduce extra delays besides the packet processing since the monitoring probe will act as a FW. Reaction to security breaches will be delayed if **passive** monitoring is used (e.g., FW needs to be reconfigured).	For a given security use case: 1) measure the latency introduced with respect to the number of rules that need to be analysed; 2) measure the total delay (i.e., data extraction, analysis, reaction) in the implementation of the counter-measures when passive and active monitoring is used.	Depending on the security use case, the implementation involves SW or HW, virtual or host, application, data or control planes.
Security management and monitoring:	Security monitoring delay. Delay in implementing the output of the assessed information	Measure the duration from the identification of a security threat to the implementation of a suitable counter measure. Measure the duration from the activation of the countermeasure until the deployment to the network.	Implementation in control plane and propagation to data plane.

Authentication system: A system that minimizes delay in authenticating the possible large number of applications. Moreover, the techniques provide access control to applications within short duration. The system focuses on categorizing various applications beforehand, according to their requirements from the underlying network such as reading topology, switch statistics, or writing flow rules etc.	Authentication and Access Control	Number of authentication requests, and time duration of an authentication procedure e.g. in Ms.	The system works between the SDN application and control planes.
Security between control plane and data plane: We propose a novel IPsec based SDMN backhaul traffic architecture to overcome the limitations in legacy IPsec mechanisms. It is a "bump-in-the-wire" security architecture based on HIP. Our architecture proposes four main changes to SDMN architecture. First, distributed SecGWs (Security Gateways) are utilised to secure the controller from the outside network. Second, new Security Entity (SecE) is added as a control entity to control SecGWs. Third, a Local Security Agent (LSA) is installed in each DP switch to handle security related functions in the switch. Fourth, IPsec BEET (Bounded-End-to-End Tunnel) mode tunnels are used to secure the control and data channels communication.	HIP-based IPSec secure tunnel establishment between LSA and SecGW, extra layer of encryption	Latency(ms) during normal operations, in the duration of attacks on the control channel, and percentage of tunnel establishment duration	Data Channel, Control Channel.

Table 4. Partners input

3.5 Network monitoring adapted to network virtualisation

Network monitoring facilitates verification and validation of SLAs, managing performance (QoS) and user experience (QoE), troubleshooting, and assessment of optimizations and use of resources. On one hand, network virtualisation sets new requirements for mobile network monitoring. On the other hand, it provides the means for implementing advanced network monitoring solutions. NFV/SDN enables the integration of cloud infrastructure that can provide high degrees of freedom regarding the placement of measurement points and the flexible control of traffic flows. An advanced and effective QoS monitoring solution should comprise both a distributed (SDN / NFV-based) QoS measurement system and a centralised evaluation system.

3.5.1 SIGMONA approach

The SIGMONA partners have listed the different areas for monitoring to provide proper end-to-end system functionality adapted to the needs and constraints imposed by the SDMN architecture.

3.5.2 SIGMONA monitoring strategy

The proposed strategy consists in defining the different scenarios where the system requires proper monitoring. A synthesis presented in the next Table 5. The table also includes the metrics that need to be measured for assuring the effectiveness of the monitoring functions and communicated to the system manager or orchestrator for maintaining proper system functioning.

Use Cases Description	Proposed metrics
Improvement of scalability, performance, costs, managing QoS/QoE, in the case of network monitoring adapted to network virtualisation.	Measure scalability, in terms of cost and performance, of monitoring video transmission for analysing QoS/QoE. Compare monitoring in virtual and physical scenarios. Quantitative analysis: Measure resources needed to monitor video transmissions in different bandwidths settings (e.g., 100M, 1G, 10G). Measure any loss of precision due to loss of information. Scalability graph : Functionality : different levels of analysis and methods used; Cost : estimated cost of CPU/Memory/HW needed and deployment/operation efforts; Performance: resources needed with respect to functionality and timeliness of detections.
Troubleshooting and detecting performance problems	Compare monitoring in virtual and physical scenarios in the detection and localization of network performance problems. Qualitative analysis: Determine the flexibility and effectiveness to detect and locate problems.
Correlate data from different sources (physical and virtual)	Determine the advantages (if any) in correlating metadata captured from the physical and virtual equipment and functions. Qualitative analysis: Determine advantages in using metadata from different sources.
Maintainability: (“The ability of an entity to facilitate its diagnosis and repair."): Take a monitoring, diagnosis and recovery aspect of survivability, disruption tolerance or traffic tolerance use case. Monitoring of the control and data planes enables the maintainability, diagnosis and repair of the SDMN. Automation of the diagnosis (QoS/QoE or security) and repair or mitigation introduces SON characteristics, improving reliability. However, need to assure/prove that the monitoring and reaction is reliable.	Measure of the time to restoration from the last experienced failure (corrective maintenance only). Evaluate the effort to diagnose, maintain and repair the system manually versus automatically.

Table 5 Proposed Use Cases and Metrics

3.6 Service provisioning and optimization orchestrator entities

In SDN networks, control applications have full view of network configuration.This, together with status information provided by network monitoring and data collection systems, enables mobile network orchestrator applications to optimize service (e.g., latency) and/or resource usage more easily than in the case of traditional networks that need to rely on signalling. The orchestrator, via the control applications, can manage multiple network elements, potentially provided bydifferent vendors. This allows introducing new services by programming or modifying the orchestrator; whereas in traditional networks, all equipment needs to be upgraded to support the new service type. It is assumed that SDMN will not be implemented in a clean-slate approach, and that legacy and SDN network management solutions will coexist for some time. In order to exploit the potentials of SDN it is required that legacy and SDN management solutions cooperate (e.g., by introducing an abstraction and automation layer for legacy network parts).

3.6.1 SIGMONA approach

The basic assumptions presented in the section above, suggest that SDN can effectively help improve the efficiency of the considered network (i.e., the infrastructure part) thanks to the centralisation of the infrastructure state view and the improved automation of actions (Software Defined).

Considering the centralisation of the infrastructure state view, federation of heterogeneous devices through a common SDN southbound API certainly helps to achieve such an objective. In case interoperability with legacy systems is required, deployments may rely on the enhancement of the SDN controller with legacy network monitoring/management systems (e.g., some controller implementations supports OpenFlow as well as NetCONF, SNMP, etc.). However, there is no clear analysis on the potential improvement on the amount of overhead (i.e., signalling) generated.

If we now consider the efficiency improvement promise, some southbound protocols such as OpenFlow enable a very close monitoring/management of traffic and routing performance. Other protocols enable monitoring/management of hardware performance and configuration changes. Used together, the southbound protocols might allow on-the-fly resource usage improvement by using, among other, less saturated links, reducing CPU usage on some routers, redirecting traffic to less congested or closer gateways.

With this information in mind, it is required to highlight such potential improvements through use case scenarios and metrics discussed in the next section.

3.6.1.1 SIGMONA Service provisioning strategy

The SIGMONA partners have identified, in following Table 6, the scenarios and required metrics to ensure optimised service provisioning.

Use case scenario	Proposed metrics
Flexible deployment of Wireless Mesh Network: update of routes and full gateway rerouting	- Traffic average bandwidth - Traffic latency - Route convergence time - Improvement on data path signalling - Required signal path load
Self-organizing network concept for mobile backhaul: QoS and QoE improvement in Mobile Backhaul	- Traffic latency - Level of hardware resource usage (CPU, bandwidth allocation) - Required signal path load
Routing improvement in the core network: traffic rerouting to avoid congested routes	- Route path lengths - Traffic bandwidth (UDP and TCP) - Required signal path load
Improvement on the control of the S/P-GW data path: gateway relocation and gateway selection	- Average path lengths - Traffic bandwidth (UDP and TCP) - Average traffic overhead (GTP overhead)

Table 6 Proposed Use Cases and Metrics

3.7 Cost reduction impact of LTE network virtualisation

Virtualisation of the LTE network is assumed to provide cost savings from standardised network elements and higher capacity utilization. For instance, SDN provides for easier network management due to the separation of data and control planes. However, virtualised network elements may increase the need for more computing power, more complex network management and create more complex value networks. The net benefit of SDN in LTE networks should be examined further in SIGMONA.

3.7.1 SIGMONA approach

When analysing the cost reduction that can be obtained by using virtualisation and SDN, the SIGMONA partners have identified the main parameters for cost modelling as defined in the following diagram.

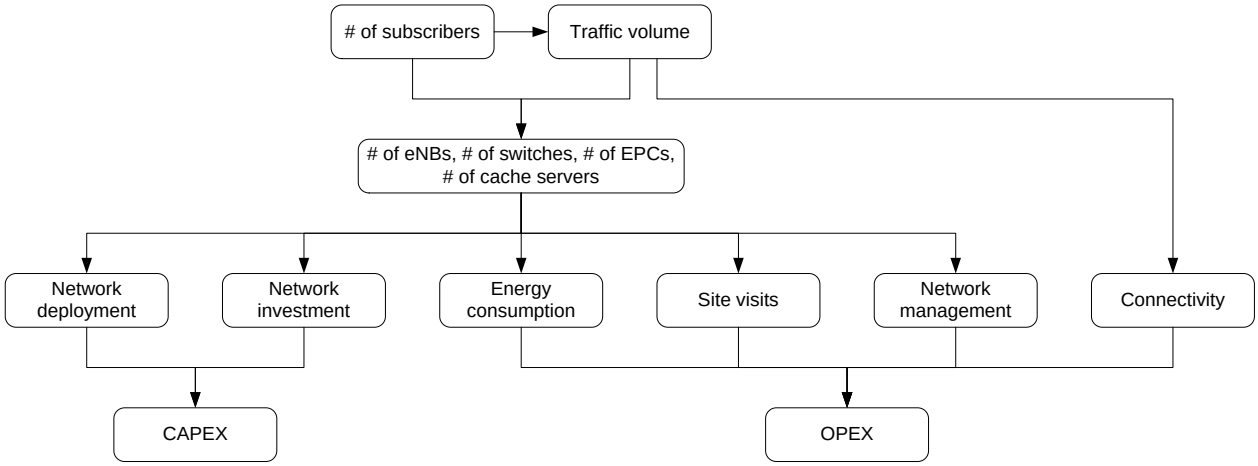

Figure 8: Cost reduction parameters

3.7.1.1 SIGMONA Cost Reduction Strategy

For each of the parameters depicted in the Figure 8, the SIGMONA partners have defined the factors that should be measured and minimised through the NFV functionality in order to reduce the overall cost of the system. These factors and their consequences are:

Complexity:

If a SDN switch is more complex in design and implementation than current switches, SDN is less cost effective. This has to be measured at the network level, not just in individual devices.

Standardisation:

If a SDN network has more standardised HW and interfaces, it should be more cost effective.

Automation

Automation level of the network affects the OPEX. The more automated, the more cost effective it will be.

Deployment time

Deployment time (that is manual installation and configuration of new devices) in SDN compared to current network. The shorter the time, the more cost effective it will be.

Physical resources

Additional capacity needed which cannot be provided with current system/transport. Virtualisation could lower the need of physical components and use virtualised resources instead.

4. Architecture model

This chapter focuses on the latest research carried out by the partners with regards to SDMN architecture mapping to the ETSI architectural framework.

4.1 ETSI ISG NFV

The ETSI Industry Specification Group Network Function Virtualisation is an industry consortium with over 200 member companies, including over 30 network operator companies [4]. NFV is defining the end-to-end architecture that focuses on making the deployment and management of virtualised network functions different to the current physical network appliance or network function. The functional model identifies the main functional groups, which are required in order to realize NFV. The Figure below shows high-level functions and their interfaces. For a detailed description of each function, see ETSI E2E Architectural Framework document [5].

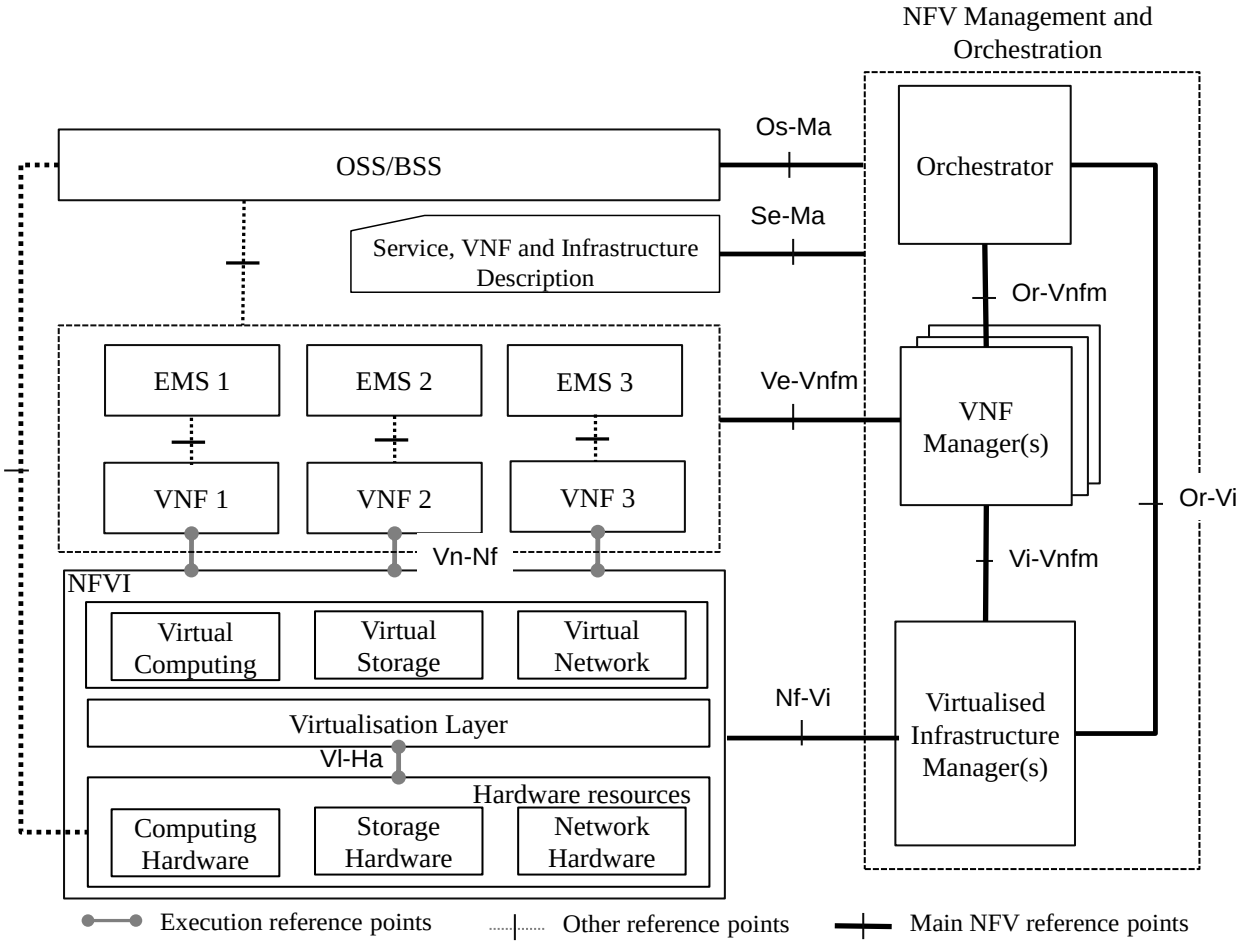

Figure 9: NFV E2E Architecture Overview

NFV is about creating virtual network functions, managing, and orchestrating them on a virtualised infrastructure. NFV approach could be defined as “Evolution of network elements”. The ETSI ISG NFV documents reached stable status in June 2014, and they were moved to change control. ETSI’s Network Functions Virtualisation (NFV) Industry Specification Group (ISG) has successfully completed Phase 1 of its work with the publication of 11 ETSI Group Specifications in January 2015. [6]:

- Infrastructure overview,
- Hypervisor domain,
- Compute domain,
- Infrastructure Network domain,
- Infrastructure Interfaces and abstractions,

- Software Architecture: VNF Architecture,
- Management and Orchestration,
- Performance and portability best practice,
- Security problem statement.

The planning for NFV Phase 2 is now complete and work has commenced with agreement on the objectives and scope to:

- Grow an interoperable NFV Ecosystem,
- Specify reference points and requirements defined in Phase 1,
- Further, grow industry engagement to ensure that NFV requirements are satisfied,
- Clarify how NFV intersects with SDN and related standards, industry, and open source initiatives.

NFV is highly complementary to SDN. These topics are mutually beneficial but are not dependent on each other. Network functions can be virtualised and deployed without an SDN being required and vice-versa.

The OpenStack community has a mission to produce an open standard cloud-computing platform for both public and private cloud providers regardless of the size [7]. OpenStack is a suite of software tools that is seen as one of the means to provide the orchestration layer for NFV infrastructure, aimed at building and managing cloud networks. Nevertheless, the challenge is that OpenStack alone might not be enough for a carrier-grade NFV orchestration as telecom applications span over multiple virtual machines, especially when it comes to a carrier-grade NFV deployment.

In a recent publication by the ETSI EVE group, five potential SDN controller locations in the reference model are proposed and analysed [8].

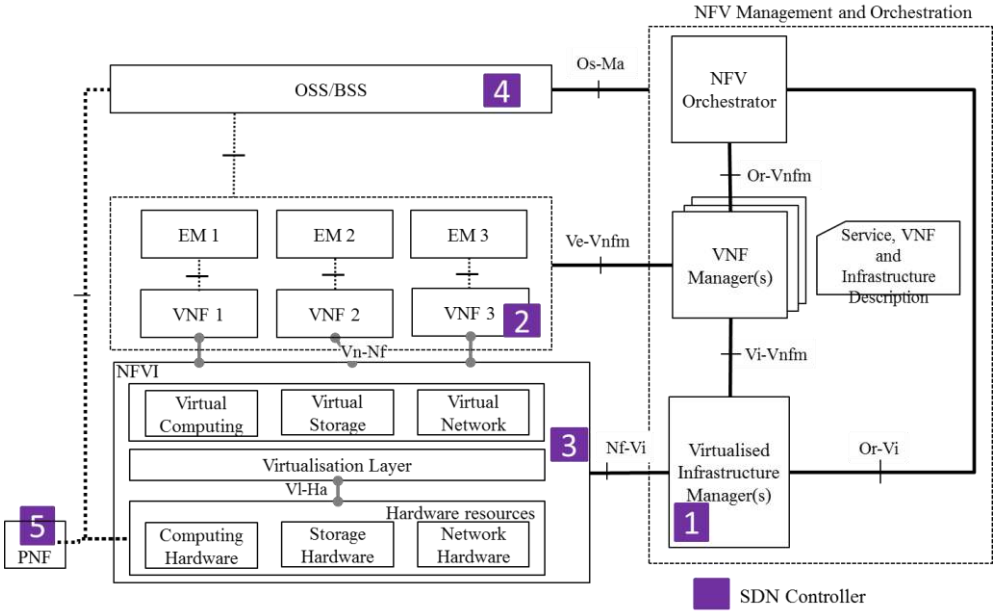

Figure 10 Possible SDN Controller Locations in the NFV Architectural Framework

One case will be further studied in the present document: Case 3 where the SDN controller is located in the NFVI.

4.2 SIGMONA architecture models

Current SIGMONA architecture overview is shown in the figure below where the mobile specific network , as defined by 3GPP, become logical components in the cloud. This architecture keeps the 3GPP interfaces and network elements as they are. However, the signalling elements are virtualised and move to the cloud. Moreover, this architecture benefits

from SDN and NFV in the networking and transport where control and data plane are also decoupled. This allows moving the control components of the networking to the cloud together with the signalling network elements defined by 3GPP.

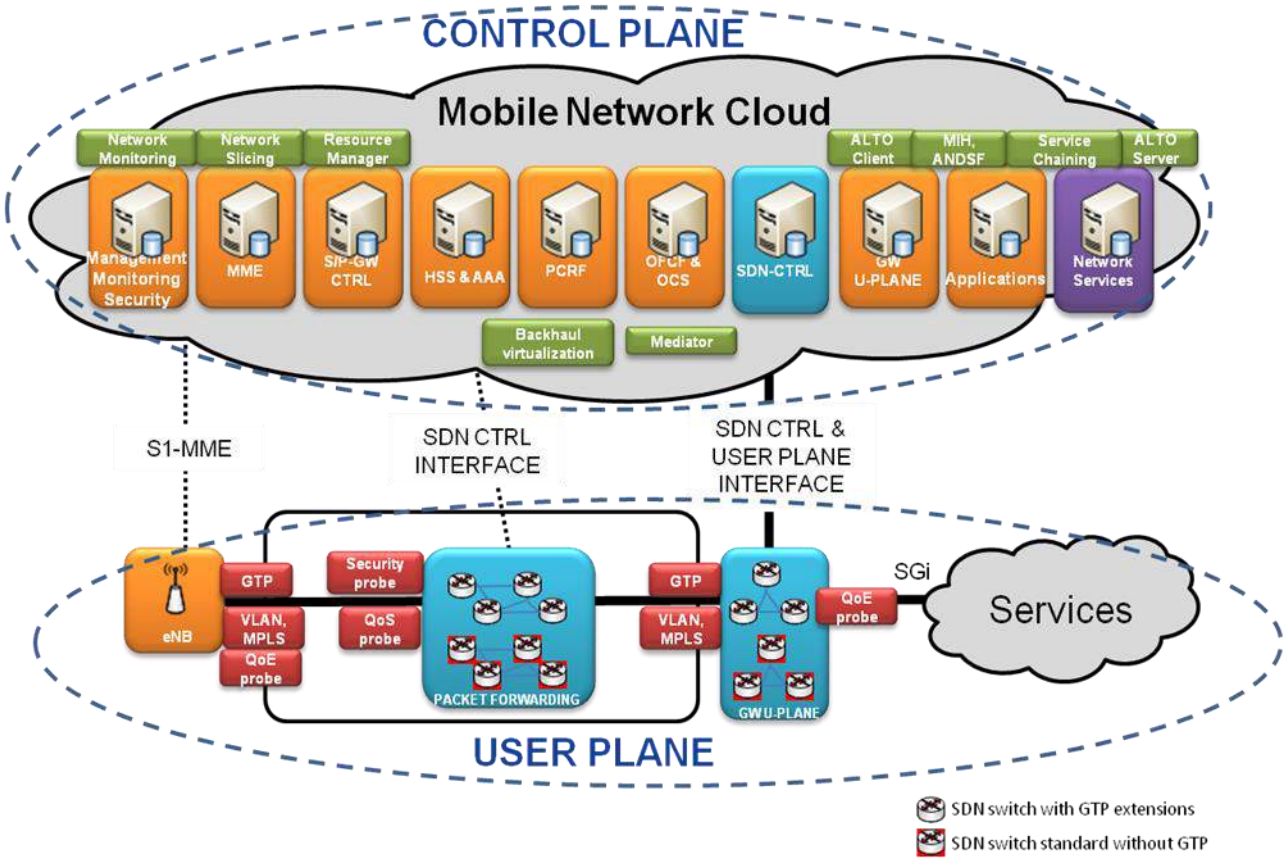

Figure 11. SIGMONA project Software Defined Mobile Network reference architecture.

Further details can be found in the SoftwareDefinedMobileNetwork_Architecture-D1.1 document [1].

4.3 Partners Mapping to the ETSI NFV architectural framework.

4.3.1 QoS, mobility and SW accelerated architecture Mapping

This mapping is based on the shared testbed environment. This platform is composed of

- Hardware resources
  - Servers x86 based,
  - Switch and Wi-Fi AP,
  - SDN switches are emulated via *mininet*.
- OpenStack Virtualisation solution with 6WIND OVS acceleration
- SDN capabilities provided by CEA SDN Controller
- Tenant VNF
  - BVS Application,
  - PMIPV6 service,

- Mesh service,

The monitoring function is ensured by Montimage's MMT product.

Some VNF have their own VNFm to provide communication between NFV Management and orchestration blocks and Network Functions Virtualisation Infrastructure blocks.

4.3.1.1 SDN controller flow requirements and positioning

Three communication channels have been identified:

- The northbound interface to provide communication to VNFm ,orchestration services and Hypervisor network components,
- The East/west interface to provide communication between SDN controllers,
- The Southbound interface (OpenFlow) to communicate to SDN switches.

Among the potential positions of the SDN controller in the ETSI NFV reference model, the most adequate choice regarding our requirements is to place the controller in the NFVI.

The choice is driven by the low delays required by our SDN applications (PMIPv6, Mesh services and Video Services), so that the SDN controller must be as close as possible to the user plane (network elements).

Having the controller working directly in the NFVI entity enables to ensure the availability of necessary hardware resources to manage the various services. That is guaranteed due to the fact that, positioned directly in the NFVI entity, the SDN controller will benefit of resource availability and virtualisation scalability offered as well as security features.

In addition of resource availability and the proximity with the mobile network elements, this position will allow to communicate easily with the whole ETSI architecture elements using the existing communication channels without any modification.

The main motivation is to maintain a minimal level of delay while deploying our services. Moreover, if we suppose another placement of the controller, multiple issues should be addressed: which communication channels will be used to ensure the reachability of the controller from the VNF.

In such a model, it is assumed that reactive application routing configuration cannot be generalised if low delay is required. Proactive routing configuration is preferred.

The mapping to the ETSI Architectural Framework is shown in Figure 12 below.

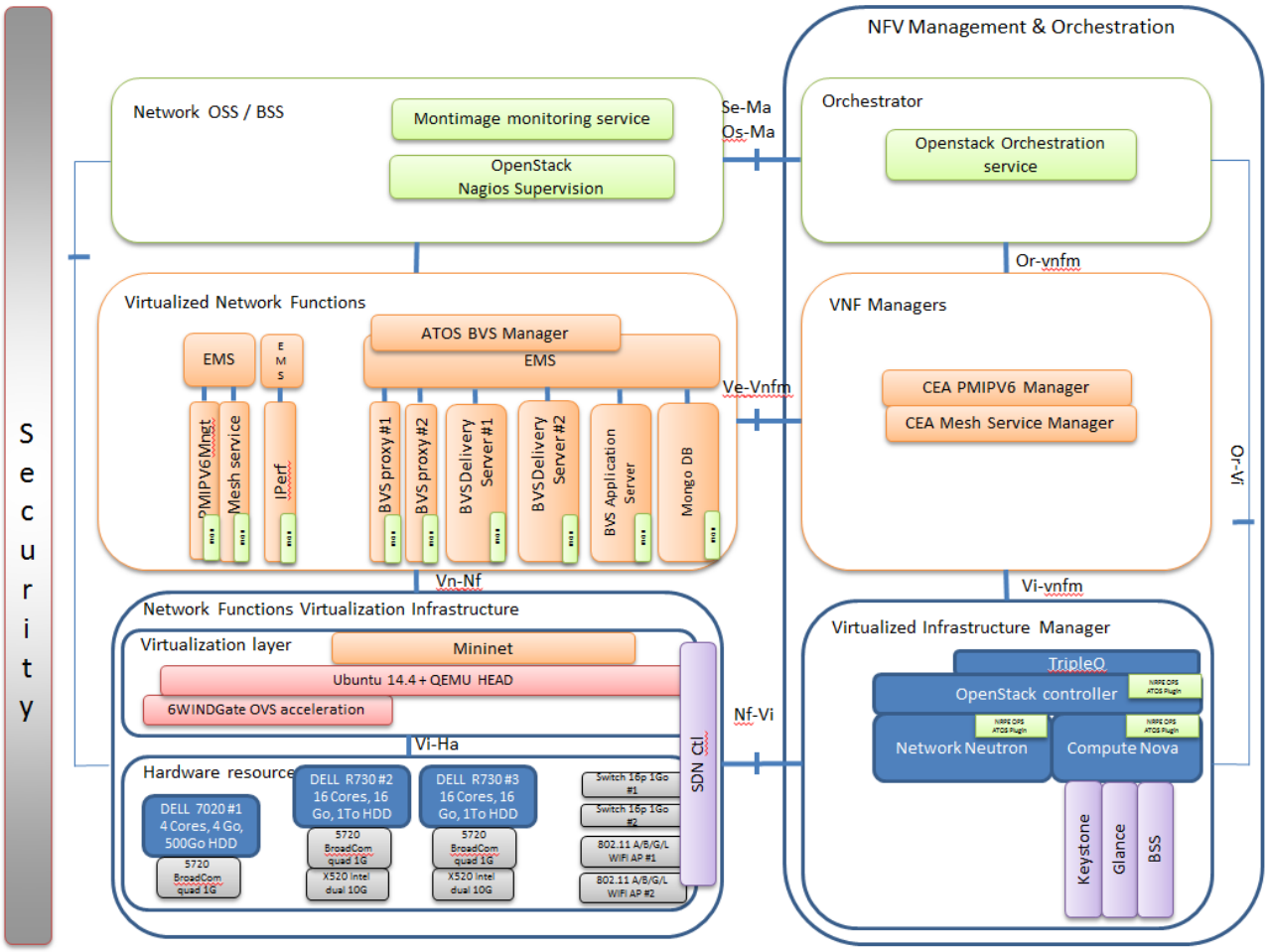

Figure 12. SIGMONA French project Software Defined Mobile Network mapping.

4.3.1.2 Components Description:

4.3.1.2.1 PMIPv6

This VNF investigates the concrete evolution of the standardised Proxy Mobile IPv6 (PMIPv6) mobility management protocol for SDN-NFV architectures. Our objective is to design the PMIPv6 evolution that takes full advantage of the SDN-NFV concept. This use case requires an SDN southbound protocol able to provide low-level link technology information such as Received Signal Strength Indicator, wireless channel frequency, information about neighbouring wireless access-points.

4.3.1.2.2 Data Offloading SDN-controlled IP wireless mesh

Through this NFV, we address the opportunity of offloading the Radio Access Network by the use of IP Wireless Mesh Network (e.g. Wi-Fi). Here we consider SDN control of IP communications in the edge networks, meaning that smartphones are SDN capable. It is commonly assumed that such a target would be handled by end-terminals themselves as a completely distributed system without mobile network supervision. This research topic investigates whether the mobile network operator can keep control of these communications to redirect traffic to a different access network (e.g., fixed).

4.3.1.2.3 Virtual Accelerator

6WIND Virtual Accelerator ensure that performance level of Mobile Network applications in terms of networking, storage and other features (cryptography for instance) can be offered and guaranteed in a portable way.

On the networking side, 6WIND Virtual Accelerator can be controlled as a SDN component capable of Layer 2, Layer 3 and Layer 4 functions:

- Simple switching, MPLS, L2TP...
- Ipv4 and Ipv6 Routing
- IPSec aggregation
- In the future TCP offloads and protections (the technology is present but not yet exposed)

Most of the components reside in the NFV Infrastructure, in hypervisor domain of Compute Nodes and on Network Nodes. Thanks to industry's efforts in ETSI and OPNFV, there will be additional open source components available for VNF.

4.3.1.2.4 VNF managers

A VNF Manager is responsible for VNF lifecycles management (e.g. instantiation, update, query, scaling and termination).

4.3.1.2.5 BVS application

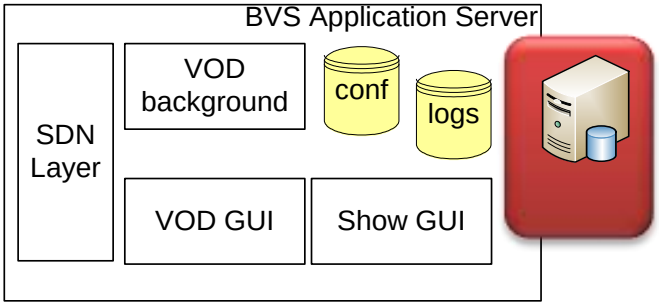

Figure 13 – Application server

The modules are:

- A Web "VOD GUI" application that interacts with the end user, it provides access to the catalogue of VOD, manages the purchase dialog and initiates the final reading.
- An application "VOD background" that runs in the background (no UI)
  - responsible for non-interactive parts of the system,
  - Some information collected by this module will be used in the "Services GUI" (for example, deciding not to use saturated content server),
- " SDN Enabler" Rest interface to interact with SDN controller,
- A series of compounds of configuration elements (PHP flat files)
  - Catalogue of available VOD,
  - Authorised users to buy / read VOD, including the SLA,
  - The characteristics of delivery,
- A "Show GUI" Web application graphically animated that allows for the demo to monitor real-time interactions between the various components ,
- Application and technical logs storage.

4.3.1.2.6 BVS Delivery

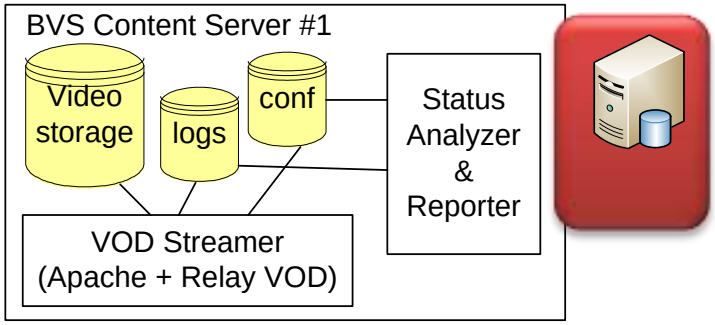

Figure 14 – Delivery server

The module of delivery servers are:

- A repository containing the VOD catalogue,
- The configuration items,
- A Streamer composed with :
    - Apache based server,
    - "Service Relays" application module placed between the content server and the end user,
- A module "Analyzer & Reporter Status" that will be responsible to analyse the available evidence on the server (VOD relay logs, Apache logs and network throughput ...) to make them available to the module “Show" app.

4.3.1.2.7 BVS Proxy

This component is a streaming proxy to optimize Video customer delivery

4.3.1.2.8 Monitoring service and probes

A security and management monitoring tool developed by Montimage includes a security and QoS performance probe (i.e., sensor or monitoring agent) that captures the metadata needed by the different network functions to assure network reliability. This probe is deployed in the virtual machines hosting the different network functions. It serves to monitor the ongoing activity to detect security and performance events and incidents that can either trigger an automated local reaction or report to the centralised monitoring service part of the OSS/BSS management system. In turn, the centralised monitoring service allows analyzing the events and incidents, correlating the information received, present this information to the human operators, and act as a decision point to remediate any deficiencies in an automated or semi-automated way.

The management of the probes will be carried out by the centralised service. This system brings the possibility of deploying and enforcing policies and rules related to the network functions and services (and not just of the virtual machines as provided by the VIM), and gives operators improved visibility and control of their networks.

4.3.1.3 Interfaces description

4.3.1.3.1 Vn-Nf

Northbound interfaces to VNF are located on the Vn-Nf reference point and will be compliant to ETSI NFV Extensible Para virtualised abstract interfaces (EPD):

- EPD-net : virtual Network Interface Card
- EPD-crypto: accelerated crypto operations
- EPD-IPSec: full IPSec offload
- EPD-RDMA: portable RDMA for high performance applications

As defined in ETSI NFV, it is not expected to have southbound interfaces to have common interface to hardware, as this would jeopardize creativity of vendors.

In addition, additional interfaces for acceleration management will be offered on the Nf-Vi reference point as they become standardised.

VNF are connected to the controller through a TCP/IP connection and use the northbound API to query information’s about active network devices. The northbound API relies on the command packets format (JSON). When the target of the command is a specific infrastructure device, the controller validates the service credentials and transfers the command packet to the right device.

The interface, in addition to the classical information is needed for optimal routing, flows monitoring, resources management and so on, and must capture the following specific information’s:

- Bandwidth remaining percent for each of the LTE network elements, within the context of congestion monitoring,
- Information allowing to distinguish between UEs, WiFi AP, LTE forwarding devices. Indeed, this information is useful in order to achieve the following tasks:
    - Dedicated processing in function of the network element type,
    - Detect a potential mesh networks based on the UEs,
    - Redirect traffic to WiFi APs for the case of offloading.

- Detailed information's of the WiFi interfaces present in the mesh network, allowing to estimate the performance of the mesh network,
- The Channel Quality Indicator (CQI) delivered by the eNB. As the name implies, it is an indicator carrying the information on how good/bad the communication channel quality is. It will allow deducing the performance of the eNB,
- LTE Buffer Status Report (BSR), allowing to anticipate the traffic load on in the cellular network,
- Statistics covering specific information about the interfaces status. For instance, the operation mode (station, access-point, ad-hoc, etc.), the capabilities (mesh mode capable, etc.), the BSSID, the neighbouring MAC addresses, Tx/Rx count, if the interface is managed by OpenFlow, etc.,
- The capacity to gain multi-hops information about the network performance, e.g., the current round trip time (RTT) with a specific target device,
- The capacity of configuring how devices behave according to their direct neighbours. For instance defining how local network services should forge ICMP and/or ND control packets,
- The capacity to control the configuration of other local applications and libraries such as Open vSwitch (OpenFlow application),
- Some specific events occurring at the device level may require immediate attention of the controller and services, e.g., a wired Ethernet cable unplugged or a new WiFi USB dongle plugged. Devices send "event" packets to the controller detailing the reason of the event.

4.3.1.3.2 Ve-Vnfm

In addition, of the current recommended usages i.e. resource allocation requests by the VNF Manager, virtualised hardware resource configuration and information state (e.g. events) exchange, some more specific features are required:

- Allow SDN VNF to be as close as possible from the SDN controller, and this to ensure a certain level of reactivity between the VNFs-controller,
- Ensure to have at any moment another copy of the ongoing SDN VNF ready to take place in the failure case (redundancy),
- Secure and ensure the access to the databases used by the SDN VNF.

4.3.2 Optimal Routing Application Mapping

4.3.2.1 Components description:

The optimal routing application uses both the network topology (virtual switches or bare-metal) and the power consumption of the nodes on the network for routing decisions. At the final stage, the application checks the resiliency admissibility by considering vertex connectivity and adds the least power consuming port/switch (es) to the routing decision for robustness. Two scenarios can be considered:

- All switches are bare-metal (physical OF switches),
- There are nodes in the network that can act as vSwitches.

4.3.2.1.1 Optimal Routing VNF

For both of the cases above, the Optimal Routing application works as a VNF. For the bare-metal case, the Optimal Routing application communicates with the ***OF Controller*** through OF APIs for routing, switch and port enabling/disabling, statistics and configuration purposes. All these interfaces should be (usually are) defined in the Controller which sits on top of the virtualisation layer. Usually, OpenFlow is used for routing decisions, statistical data collection (sFlow, etc. is also possible) and OFConfig (or OVSDB, etc.) is used for switch configuration. The information coming from the network is relayed to the Optimal Routing application and the application decides the routing rules and configuration changes in the network.

4.3.2.1.2 Optimal Routing Manager

In the case where there are virtual switches in the network, disabling/enabling a port/switch might also mean to create a new VM on a server or disabling the VM. In this case, this decision from the Optimal Routing VNF should reach the VIM and this communication is carried out through the Optimal Routing Manager that is one of the VNF managers. The Optimal Routing Manager then coordinates these requests with the vRouter Manager in the VIM (working with OpenStack or equivalent).

4.3.2.1.3 vRouter Manager

When a request for instantiating/deinstantiating a VM is requested from the Optimal Routing Manager according to the directions of the Optimal Routing VNF, this module creates and makes ready (or deletes) the VM for carrying out the defined vSwitch duty on the node specified.

In both scenarios, since the OF controller sits on top of the Virtualisation layer, it is used for statistics collection, executing routing decisions and port/switch disabling and it does not need to know about the structure of the switch, it only needs to execute the decisions from the Optimal Routing VNF.

4.3.2.2 Interfaces description:

4.3.2.2.1 Vn-Nf

This Interface ensure the communication between Optimal Routing VNF and NFVI based on REST API. Via Vn-Nf interface, Optimal Routing VNF is able to change routing roles and configuration for the traffic flows by communication with OF Controller that runs on the top of virtualised layer of NFVI. Vn-Nf interface conveys parameters to share topology of the network with Switch-specific attributes (MAC and IP), Link-specific attributes (Source MAC, Source Port, Destination Port and Capacity) and Host-specific attributes (Switch port, Switch MAC, IP and MAC) from controller to VNF. Optimal Routing VNF makes routing decisions by receiving Source/Destination IP and path rate attributes from controller and provides path information attribute such as Source/Destination Port and Source/Destination MAC.

4.3.2.2.2 Ve-Vnfm

This interface enables communication between Optimal Routing VNFs and Optimal Routing Manager on REST API. Via Ve-Vnfm interface, Optimal Routing Manager is able to deploy instantiate, halt and configure virtual instances and control interconnection attributes such as IP connectivity for the Optimal Routing VNF coordinating with vRouter Manager.

4.3.2.2.3 Nf-Vi

This reference point enables communication between vRouter Manager and NFVI based on REST API. Via Nf-Vi interface, vRouter Manager is able to manage the virtualised resources of the NFVI platform allocated for Optimal Routing VNF. Three different interface enable communications between vRouter-Compute Interface, vRouter-Network Interface and vRouter-Virtualisation Layer Interface. VRouter-Compute Interface conveys NFVI's resource and system utilization parameters such as CPU usage, Memory usage and availability of the infrastructure. VRouter-Network Interface supplies agility for vRouter to manage and monitor virtualised NFVI-PoP network resources such as sub-net, switch bridging, multi-tenant and provider network and port configurations. VRouter-Virtualisation layer interface enables vRouter to manage the virtualised resources of NFVI platform such as initiating, running, halting and scheduling.

4.3.3 Integrated RAN and Backhaul Control and Management mapping

An integrated Radio access Network (RAN) and Mobile Backhaul (MBH) control plane is instrumental for providing policy- and class-based QoE in SDMN. The general QoE-aware architecture for RANC- and MBHC-integrated SDMN in SIGMONA framework is shown in Figure below. Integration with MBH allows the feedback of RANC information to the MBHC. This integration has the following purposes with the perspective of QoE:

- MBHC control over RANC as a higher layer in the controller hierarchy: MBHC may poll RANC for retrieving RAN state and control RANC as the higher-in-command in the control plane,
- Synchronization of RAN and MBH resource allocation: An efficient control plane should provide an end-to-end control of network resources and entities. Accordingly, different network segments should be managed in an integrated and consistent manner,
- QoS control based on MBH state: This aspect is related to previous item and requires MBHC and RANC cooperation,
- Resilience and fault-tolerance: MBHC can switch to different RANC or execute load-balancing actions for evading RANC failure cases.

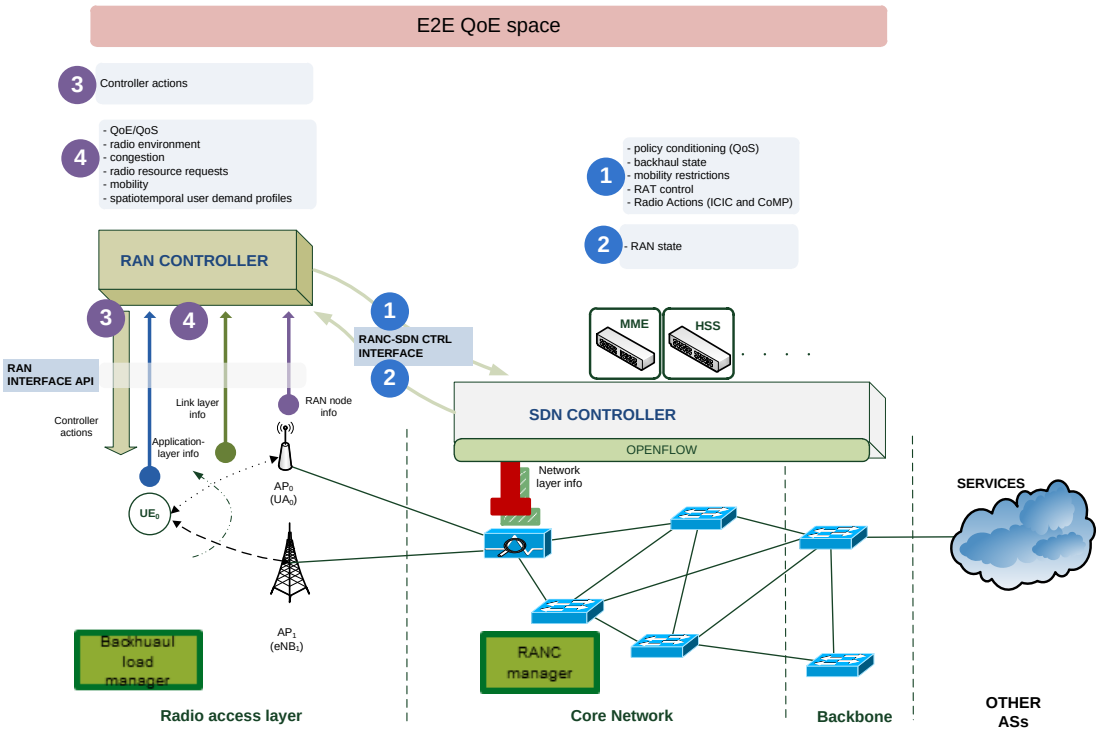

Figure 15 Integrated RAN and backhaul control stratum for QoE support.

The potential NFV mapping is based on RAN controller and backhaul controller dichotomy and consists of two main components, namely RAN Controller (RANC) Manager and Backhaul Load Manager (MBHC)

4.3.3.1 RANC Manager

RANC application can work as a VNF. The southbound interface RIA towards RAN elements collect system information such as congestion, link states, and service requests. The time scale of data gathering period is flexible and can be altered according to the dynamism of the RAN. The RIA layer provides the monitoring and control mechanisms for resource management and radio specific functions. The RIA protocol between RANC and the network elements (i.e. eNodeB, switch or router) is used to monitor the resources in the RAN network elements as well as radio optimization handling enforced from the controller. RANC also interfaces backhaul controller via the interconnection between RANC and MBHC through a Northbound API layer (RAN-SDN Controller Interface - RASCI). This interface allows the MBHC to improve its operation according to RAN state. Moreover, it provides the means to MBHC to control RANC in line with its position in the controller hierarchy.

4.3.3.2 Load-aware Backhaul Manager

There are two application-programming management interfaces that MBHC is exposing: Northbound API and Southbound API.

- Northbound APIs: For MBHC, the Northbound APIs for backhaul management are used to configure the backhaul network based on the demands of the applications in the top layer. Backhaul reconfiguration, mobility management and route establishment management are performed based on the information about the radio connection's characteristics obtained from RANC as well as the demands of the network applications and services running on top of MBHC,
- Southbound APIs: For MBHC, the Southbound APIs are used to configure the network elements. For the backhaul network, network elements are assumed to be configured using the OpenFlow protocol. Backhaul network configuration can be considered controlled using built-in OpenFlow capabilities of conventional SDN controllers.

4.3.4 Service Chaining Application mapping

4.3.4.1 Components description

Ericsson's approach will be to develop an SDN controller module with a mechanism taking jointly into account server loads for inline services and routes towards these servers. Thus, end-to-end routing application for service chaining can be implemented according to both server and route congestion/loads. Getting periodic updates and integrating with OSS/BSS in order to provide input for the mechanism is part of the research.

4.3.4.1.1 Service Chaining VNF

In order to implement end-to-end routing application for service chaining according to both server and route congestion/loads, statistics information (load/congestion) can be collected from data plan. In addition, current figures of networks can be gathered via a monitoring tool such as sFlow. Moreover, these information's are stored in DB (NoSQL DB). Both current figures and historical statistics of network can be used with routing application and service-chain use-case. These implementations (statistics/updates collection) can set into VNF part or OSS/BSS part in the above architecture. Service chaining applications is also responsible to update flow rules (routing rules) according to service-chain use case. For flow rule update implementation, the Service Chaining application works as a VNF.

Service Chaining application communicates with the OF Controller through Controller APIs. Controller communicates to the switches through Southbound APIs (OpenFlow).

4.3.4.1.2 Service Chaining Manager

Creating a new VM on a server or disabling the VM or scaling up/down a VM operation can be implemented according to service-chain use-case. For this purpose, Service-Chain VNF should reach the VIM by using the Service-Chain manager (Service-Chain in VNF Manager)

4.3.4.2 Interfaces description:

Vn-Nf: This interface between Service-Chain VNF and controller (NFVI) based on Java API and REST API.

4.3.5 Consolidated EPC Control plane mapping

The Consolidated Control Plane principle targets to optimize EPC architecture for the Telco/NFV cloud architecture. The different user's subscription context data maintained currently within the core network elements (e.g., MME, S-/P-GW) is largely independent from each other; this enables parallel processing of user's subscription context data. Cloud-based scaling methods can be utilised with this entity, which have the functional capability to manage all the functional needs of a single user's state management, rather than the separate network elements.

The EPC S/P-GW functionality is separated to control and user plane functionalities with the SDN principles. The architecture combines MME and S/P-GW-C functionality with GW User Plane context creation capability and integrates that with the split GW user plane and OpenStack environment.

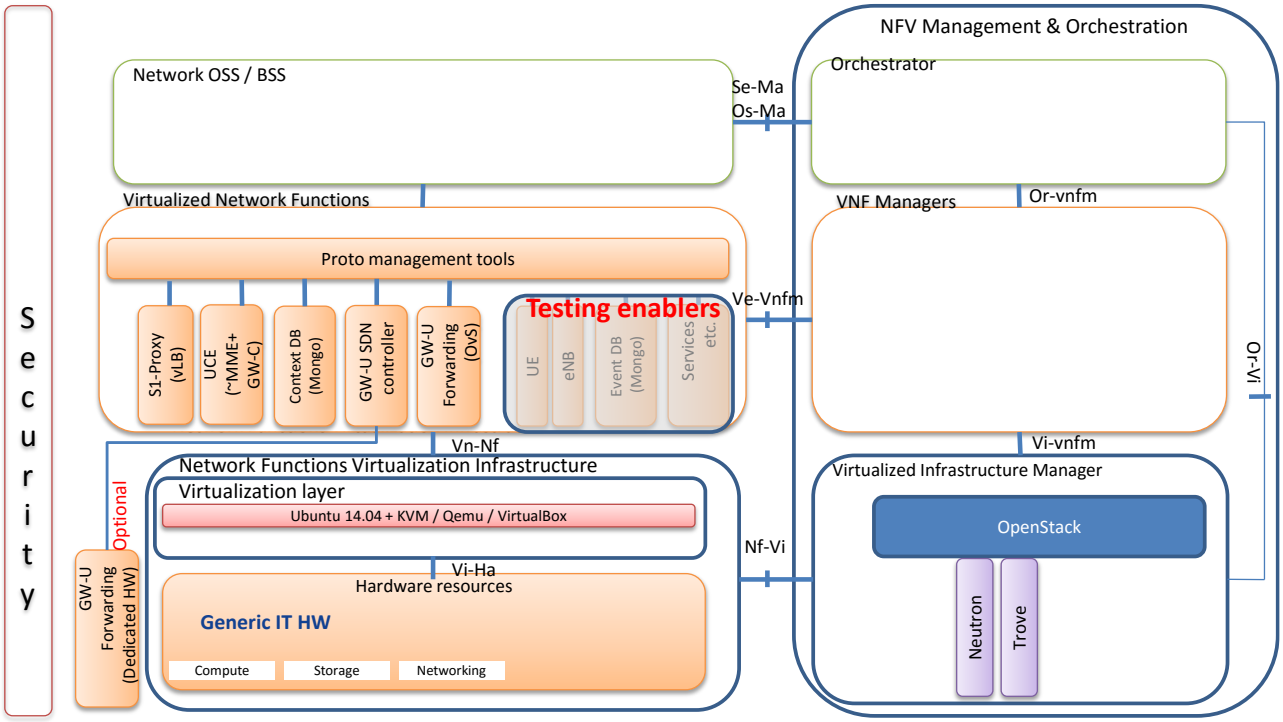

Figure 16. Consolidated EPC Control plane research mapping to NFV.

4.3.5.1 Components Description

The concept functionality is deployed as VNFs in the NFV model and utilizing the OpenStack VIM services. It is supposed that there are other (like orchestration and management) components available, but these have not been in the research focus.

The Consolidated Control Plane concept implemented as User Control Entity (UCE) handles the EPC transactions (Attach, mobility management, Detach...) of the set of UEs. The UCE may hold state information until a transaction is completed and update subscription session context database as needed but at least on transaction completion. Between the transactions, there is no UE state in the Consolidated Control Plane virtual machine and the next transaction might be handled by some other parallel Consolidated Control Plane VNF instance.

The same subscription context data is accessible by all the UE context related control plane functions. The shared subscriber context data is stored in database for the transaction handlers, and this database functionality may be provided as OpenStack DBaaS (Database as a Service, Trove project).

The S1-Proxy VNF provides the load balancing functionality for the S1-AP interface connected eNBs and scalable set of transaction handlers (UCEs).

The UCE PoC implementation reuses parts from the other research project and open source platform:

- OpenFlow Controlled S-/P-GW user plane, with a dedicated purpose build own SDN controller,
- Modified Open vSwitch (OvS) based forwarding plane implementation, enabling dynamically allocating the tunnel termination point to different locations. This functionality may be provided with the dedicated HW forwarding element,
- OpenStack Cloud Platform, providing cloud environment and some needed services (like Neutron for providing the overlay networking for the dynamic user plane).

The implementation concentrates on the essential functionality for this concept, and uses simplified functions, interfaces and protocols in other parts of the system (like eNB and UE are emulated). The implementation principles are kept according to standard definitions.

4.3.5.2 Interfaces Description

S1-AP and S1-U interfaces remain as 3GPP specified. S11 interface (between MME and S-GW) diminishes due to combined functionality. Even the S- and P-GW user plane functionality can be separated; there is no S5/S8 interface currently available in the system.

The subscription context database interface is based on the database specific interface model and JSON data format.

The control plane session flow control information is exchanged with the SDN controller via defined northbound API (JSON).

The SDN controller feeds the flow information to the proper GW forwarding elements (OvS) with the extended OpenFlow 1.3 protocol.

4.3.6 virtual EPC mapping

Aalto proposes the integration of SDN controller with EPC functionality to become virtualised EPC running as VNF components. In addition to virtualised EPC Aalto proposes new network element to optimize the mobile backhaul by removing the GTP use SDN for managing mobility, charging and traffic optimization.

Aalto proposes virtual EPC as NFV component integrated with SDN functionality. Aalto platform is composed of

- Hardware resources
  - Servers x86 based,
  - MPLS switch SDN support (Coriant)
  - SW based SDN switches (Openvswitch).
  - LTE eNB (Nokia)
  - Virtualised monitoring (EXFO)
- OpenStack Virtualisation
- SDN capabilities provided by Ryu controller

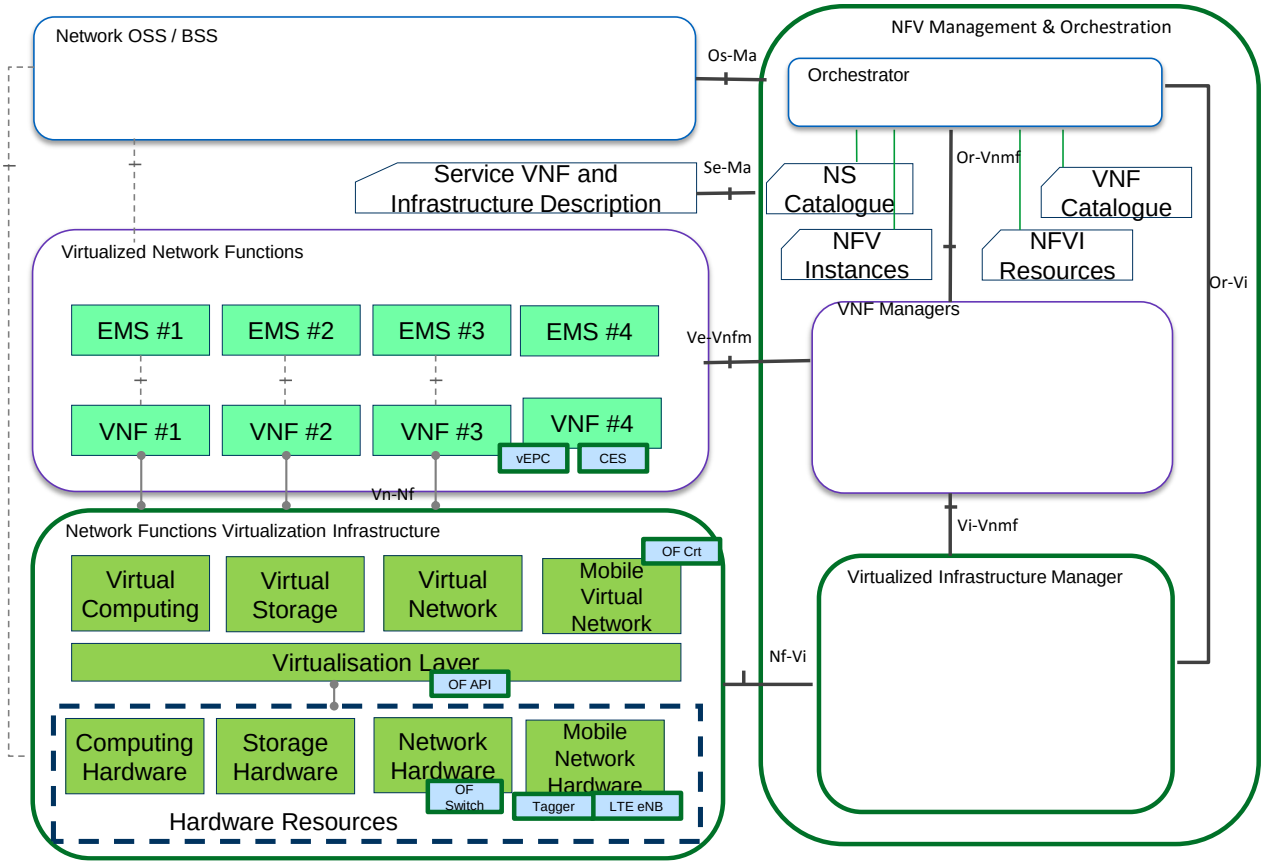

Figure 17 ETSI Mapping

4.3.6.1 Components Description

The virtual EPC (vEPC) includes the EPC functionality of MME and S-GW, HSS and PCRF (Not completed yet). The vEPC talks to the SDN controller through Vn-Nf interface using internal calls to manage the SDN switches part of the Network Hardware.

The tagger consists of network Hardware or SW component running in either the eNodeB or network switch to remove the GTP and instead use SDN for mobility and traffic management.

4.3.6.2 Interfaces Description

S1-AP interfaces remain as 3GPP specified to maintain the signaling between eNB and MME. The S1-AP interface becomes Vn-Nf interface to manage the mobile specific Hardware such as the eNodeBs.

The S11 interface (between MME and S-GW) disappears since MME includes the S-GW functionality.

The user information is stored into the database directly from the MME.

The SDN controller provides network virtualisation to the vEPC running as NFV component. The SDN controller will manage directly the network Hardware to provide the required routing and flow information to the SW switch (OvS) with OpenFlow 1.3 protocol.

4.3.7 Virtualised backhaul mapping

VTT proposes SDN controlled virtualised backhaul system that can support SDN incompatible backhaul networks such as wireless mesh networks (WMN). This system features automatic small cell deployment and backhaul resource provisioning. Furthermore, multi-tenancy at backhaul transport level is supported via network virtualisation. Integration of WMN and SDN control is achieved using network abstraction that hides WMN specific aspects from SDN controller layer.

The platform is composed of:

- Hardware resources,
  - x86 servers
  - Ethernet switches
  - Wireless mesh nodes
- OpenFlow controllers (Ryu),
- Network virtualisation (OVX),
- Small cell authentication (RADIUS server),
- Mediator and front-end switching function (in-house software and Indigo switch),
- WMN control software.

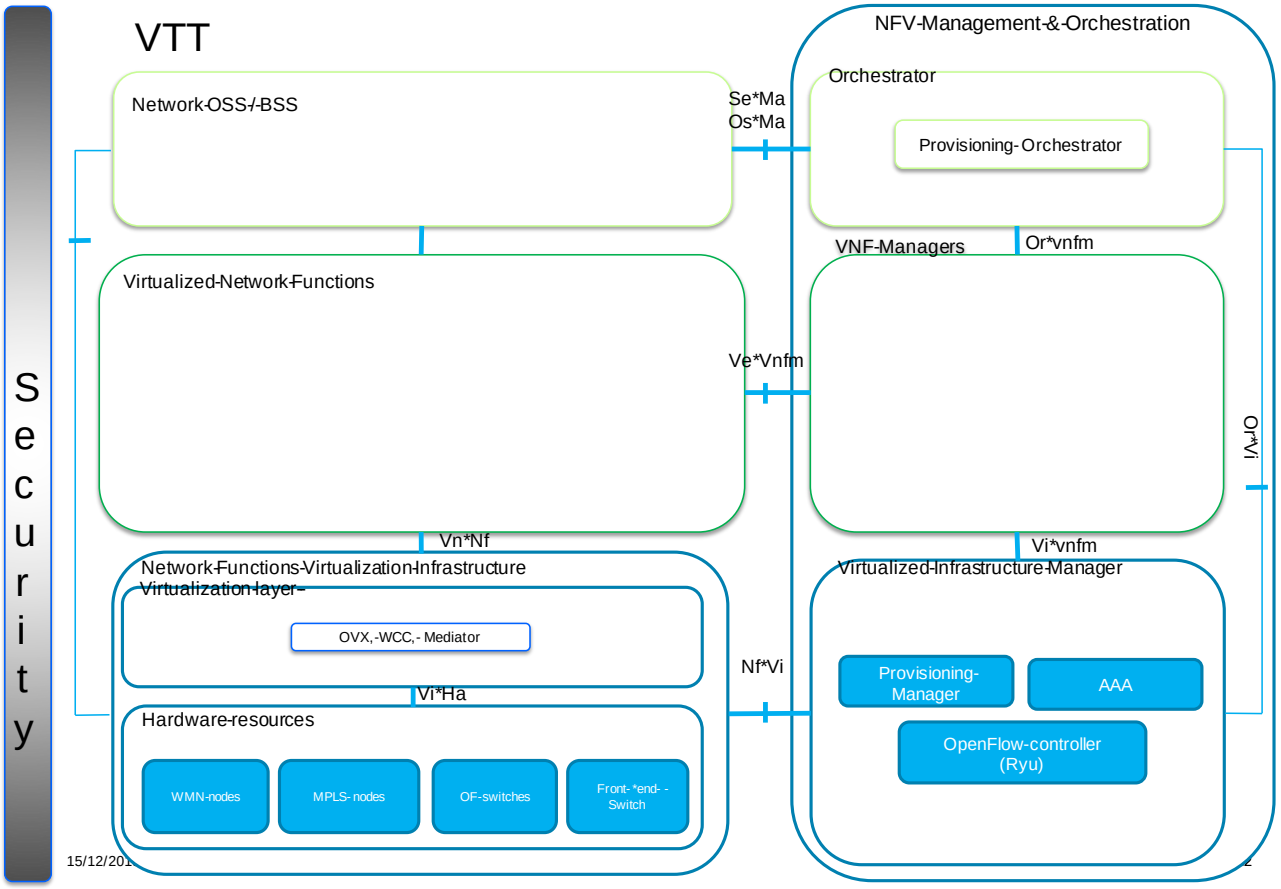

Figure 18 ETSI Mapping

4.3.7.1 Components Description

Virtualised backhaul components are 1) Network Virtualisation that is controlled by Provisioning Manager, 2) Provisioning Manager that together with authentication module takes care of automatic small cell deployment and backhaul resource allocation and 3) Mediator function that hides WMN behind network abstraction and translates OF commands to WMN control messages.

4.3.7.2 Interfaces Description

Virtualised backhaul offers normal OF control and data path interfaces towards mobile network operator and it is in that sense transparent transport service. Small cell authentication is based on EAPOL protocol and it assumes that each small cell is equipped with EAPOL supplicant.

4.3.8 Virtualised Backhaul Router Components

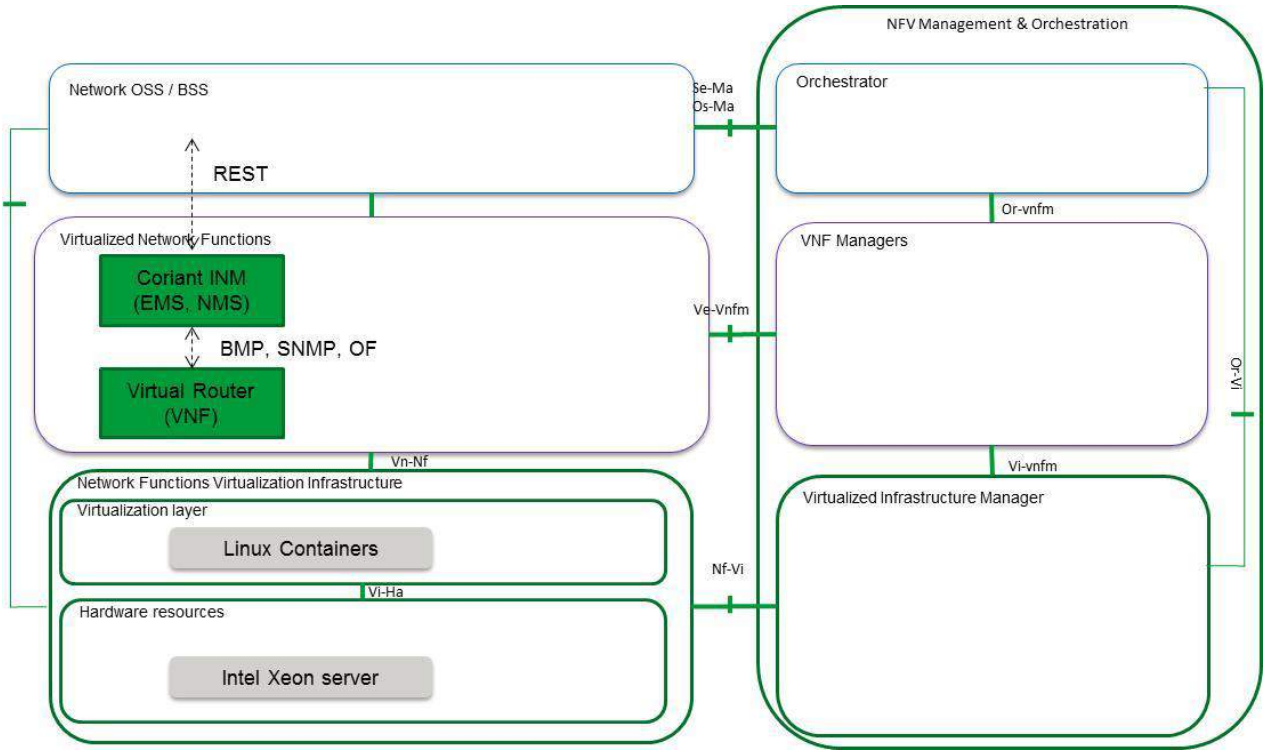

Figure 19 Virtual Router Application Components

The virtual router application runs mobile backhaul IP/MPLS router as a VNF in a virtualised Intel x86 environment. In the Sigmona testbed virtualisation is done by using Linux Containers (LXC) technology.

4.3.8.1 Components Description

Virtualised router provides similar forwarding functions (IP VPNs, VPLSes, PWs,) as well as protocol support (BGP, OSPF, LDP, etc) to harware appliance based routers. Virtualised router can be used e.g. at gateway sites that implement all functions by using virtualised hardware.

4.3.8.2 Interfaces Description

Virtual router provides BMP (Coriant proprietary management protocol), SNMP and Openflow interfaces towards Coriant INM that acts EMS as well as NMS. Coriant INM provides REST interface towards OSS/BSS systems as well as SDN orchestrators.

4.3.9 SDN and SON for Self-aware Mobile Backhaul System

The SON for mobile backhaul concept shows how advanced analytics and software defined networking (SDN) work together to create programmable, self-aware networks that assure an optimal service experience end-to-end. The self-aware network extends SDN beyond automated service provisioning to automatically reconfigure network resources based on analysis of the factors that impact customer experience and service level agreements. By reversing the conventional paradigm - in which services must conform to the network - SON adapts the mobile backhaul network to the demands of mobile services. This results in a better perceived Quality of Experience because high service quality is maintained every time a user runs an application. Figure 20 shows how the components of the concept can be mapped to the NFV architecture.

4.3.9.1 Components description

The SON MBH Agents are running on or attached to mobile network nodes (eNB, SAE-GW) and have the task to monitor user and control plane traffic as well as network quality indicators. The filtered and pre-processed measurements are

forwarded to the SON MBH Manager that is connected to all Agents and has a central view of the network. The Manager continuously evaluates the network status, conducts anomaly detection and performs optimization. Based on the outcome of those processes it dynamically reconfigures network resources to improve service quality. Mobile network node resources are reconfigured via the Agents while backhaul resources are reconfigured via the SDN controller. The MBH optimization process running in the OSS/BSS provides important business value information to the SON MBH Manager during determining the necessary optimization tasks. E.g. it can help prioritizing reconfiguration steps for eNBs serving high value customers.

4.3.9.2 Interface description

The interface between the Manager and the SDN controller is a REST API that allows the creation/modification of transport services. The Agents communicate with the Manager via a JSON based interface. The interface between the SDN controller and the SDN routers can be any SDN protocol (e.g. OpenFlow).

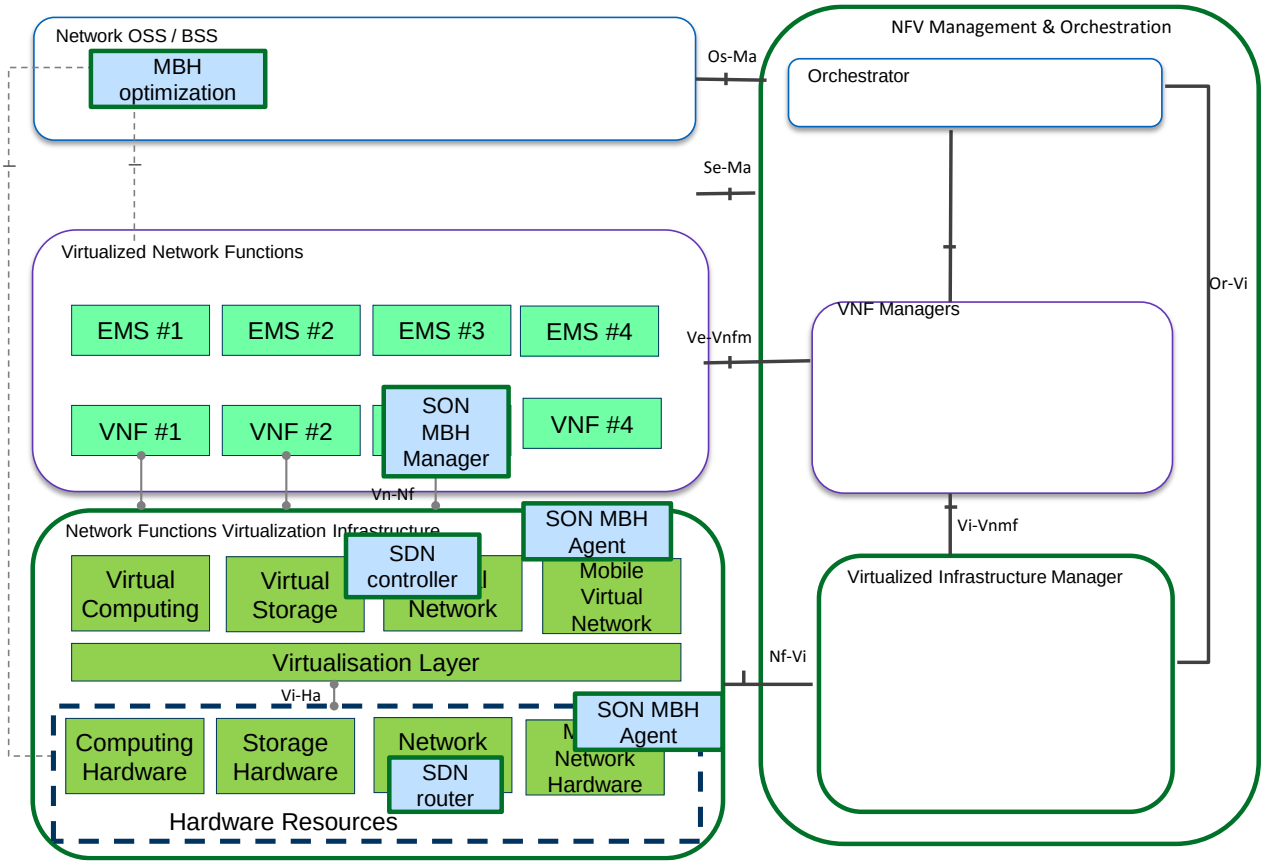

Figure 20: Self-aware mobile backhaul

4.3.10 Security Monitoring mapping

The Spanish partners propose the integration of SDN controller with SIEM functionality to become virtualised security systems running as VNF components.

The platform for security management and monitoring proposes virtualised security sensors running as NFV integrated with SDN functionality.

The platform is composed of:

- Hardware resources
  - Servers x86 based,

- Floodlight v1.1 as the SDN controller,
- Virtual box 5.0.8 Virtualisation,
- OVS 2.3.1Virtualisation layer,
- OpenFlow v1.3 protocol for control-plane flow management,
- SDN capabilities provided by Floodlight1.1 controller,

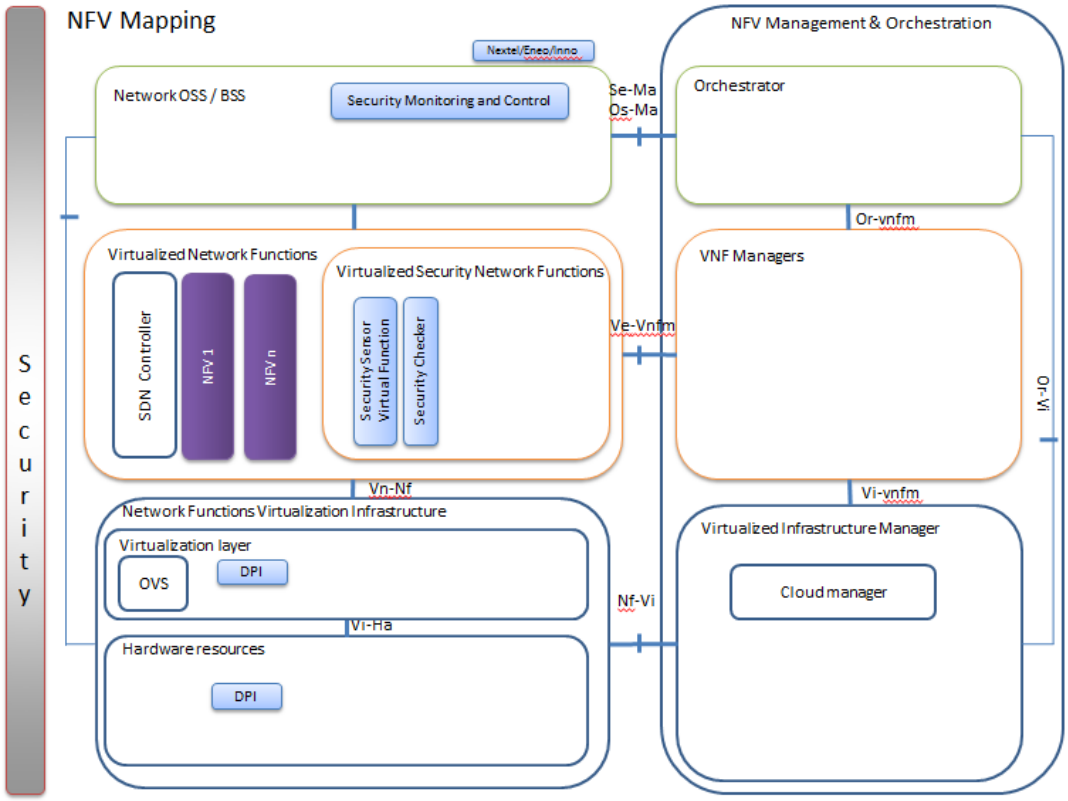

Figure 21 ETSI Mapping

4.3.10.1 Components Description

Virtualised security network functions will be 1) Security sensor virtual function and 2) Security checker. These components recollect information from virtualisation layer using DPI techniques and others and will consolidate this information together with network and security conditions. The information compiled in the Virtualised Security Network Functions will be consolidated in Security Monitoring and Control component, which will represent a more that useful information for security monitoring and awareness management.

4.3.10.2 Interfaces Description

Security Monitoring and Control interacts with NB API of the SDN controller, to deploy security countermeasures in accordance with security events and threats detected by the Virtual Security Network Functions deployed sensor and consolidated in the Security Monitoring and Control. Interface between virtualised security functions and network functions Vn-Nf, should provide virtual network monitoring mirrored port to the sensor. Interface between Network function virtualised and virtualised infrastructure manager should provide configuration about the forwarding ports in the OVS, required to be managed to provide required visibility.

4.4 Consolidated SIGMONA View

The following figure includes the mapping of multiple research contributions from different partners to the SDMN architecture.

This mapping results in multiple components that utilize SDN/NFV as basic technology to deploy the required functionality on areas such as EPC user plane control, transport, load balancing, security, monitoring, QoE, resource optimization, etc.

The goal of such proposition is to ensure future proof-of-concept solutions that take into consideration standardisation guidelines such as the ETSI ISG NFV architectural framework.

The following Figure 22 shows the different components proposed by the SIGMONA partners that are to be deployed in the SDMN architecture to fulfil the identified requirements and basic assumptions. This figure includes the elements and modules described in the previous sections that have been deemed necessary to provide the functionality to obtain a Carrier Grade SDMN solution. The functionality includes: resiliency assurance, QoS provision, security management and enforcement, monitoring, service provisioning and chaining, mobility, optimal routing, SON, integrated RAN and backhaul control.

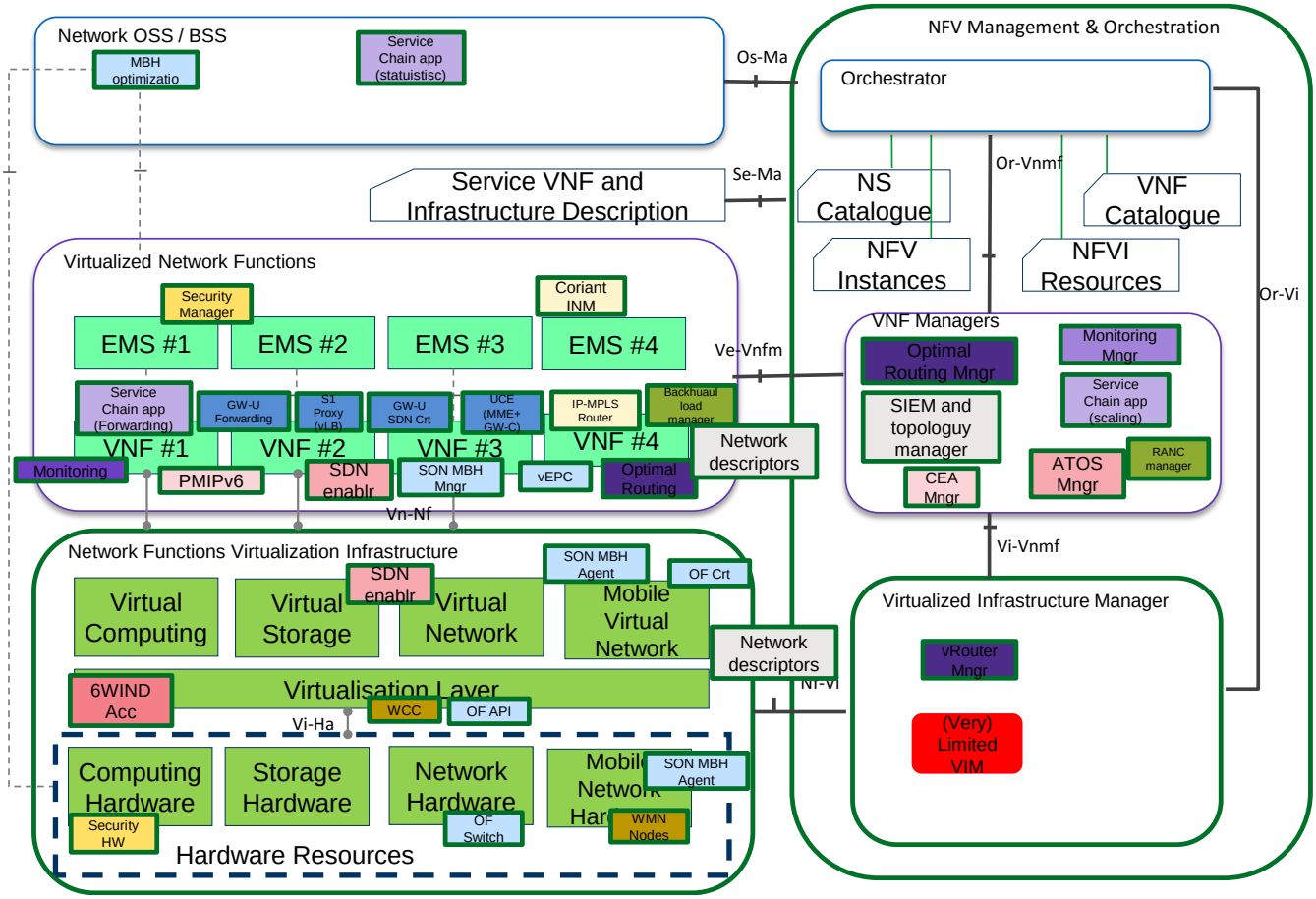

Figure 22. Software Defined Mobile Network consolidated mapping.

5. Conclusions

The proposed Software Defined Mobile Network (SDMN) architecture options help transform the current rigid and disparate mobile networks into scalable and dynamic ecosystems. SDN/NFV is considered the enabling technology for SDMN, making it the future paradigm for obtaining more flexible networks that can dynamically adapt to the needs of users, operators, content providers and service providers. Network horizontal scalability linked to cloud computing abilities promises a drastic change and simplification of the operators' networks. There is no doubt that new business models could emerge and motivate changes, but technical challenges are still heavy.

The proposed architecture, where the mobile network user plane is based on SDN/NFV technology, facilitates the migration by maintaining a part of the legacy network functions. The introduction of virtualisation and the separation of control and data forwarding enables a more efficient usage of network resources and improved security features running on the cloud. The NFV based SDMN architecture allows the core network to adapt to the service requirements dynamically. Different end user applications require different properties, like latency, capacity, optimum mobile tunnel termination location, etc. These various requirements can be served better with an evolved flexible architecture that better supports an evolution path with respect to legacy systems. The centralised control plane in the cloud enables optimal usage of resources and use of the emerging cloud platform native services.

In SIGMONA, work has been undertaken to identify the positive and negative aspects of introducing virtualisation, SDN and NFV to build future mobile network architectures. Key performance indicators and measures, synthesised in this document, have been identified as needed to assess the deployments in order to improve them and assure that the benefits that will be obtained will be worthwhile. Testbeds have allowed implementing the architecture mappings presented here and carry out experiments that validate the expected results.

Operators will profit from solutions integrating the proposed modifications by:

1) Allowing the virtualisation of at least part of the monitoring tasks;

2) Improving the operators' visibility to their network status from both security and performance perspectives;

3) Allowing them to deal with new vulnerabilities introduced by SDN/NFV;

4) Improving and managing the resiliency, QoS, mobility, routing, RAN, backhaul and other network functions;

5) Introducing more easily new paradigms such as service chaining, M2M, D2D, or even Named Data Networks… without negatively affecting the operation of the network;

and, 6) Reducing CAPEX and OPEX, thanks to SDN/NFV enabled flexibility, capacity control and automation.

SDN/NFV brings new methods to monitor and manage the network, which is translated into better controls for improved end user experience. However, optimization methods have to be applied for proper allocation and placement of cloud resources (e.g., for processing, storage and forwarding) to benefit from this flexibility to obtain cost savings. But flexibility (e.g., switching from one virtual machine to the other) is also a challenge and there is still much work to be done (in the deployments, the interoperability and the standardisations) to achieve the Carrier Grade availability and performance required by current and future networks and services.

6. References

[1] SIGMONA deliverable D1.1: “SoftwareDefinedMobileNetwork_Architecture-D1.1.pdf”, 2015

[2] 3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for E-UTRAN access, V13.0.0, 2014-09

[3] Migration Use Case and Method
https://www.opennetworking.org/images/stories/downloads/sdn-resources/use-cases/Migration-WG-Use-Cases.pdf

[4] General information about the ETSI ISG NFV: http://www.etsi.org/technologies-clusters/technologies/nfv

[5] ETSI ISG NFV Architectural Framework, ETSI GS NFV 002 (V1.2.1, 2014-12):
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf

[6] ETSI ISG NFV published documents: http://docbox.etsi.org/ISG/NFV/Open/Published/

[7] OpenStack Community Welcome Guide, Revision 11, released 24. Jun. 2014:
http://www.openstack.org/assets/welcome-guide/OpenStackWelcomeGuide.pdf

[8] https://docbox.etsi.org/ISG/NFV/Open/Drafts/EVE005_SDN_usage_in_NFV_Report/NFV-EVE005v020.zip

[9] ETSI Network Functions Virtualisation (NFV), Resiliency Requirements ETSI GS NFV-REL 001 V1.1.1 (2015-01)

[10] E. Haleplidis, Ed., K. Pentikousis, Ed., S. Denazis, J. Hadi Salim, D. Meyer, O. Koufopavlou, “SDN Layers and Architecture Terminology”, http://www.ietf.org/id/draft-irtf-sdnrg-layer-terminology-04.txt

7. APPENDIX

7.1 Reliability SDN Use Cases

Potential fault use cases are arranged according to the above topics. Each case has an ID, a short description, an estimate of occurrence frequency and comments. Not all cases are relevant to every partner solution, but the list should capture at least some relevant issues in each SIGMONA solution.

In the table below freq. stands for a frequency class (D = daily, W= weekly, M= monthly, Y+= up to few times per year, Y=once a year, Y10= once in 10 years). At this moment, only tentative values are provided. The event frequency depends on the size and use of the network. The reference has been a national production network.

fault case IDs	fault/challenge	freq.	comments
FC1:	If the network does not auto recover from a fault, what will the controller do?	(Y)	
FC2:	SDN controller goes down.	(Y+)	
FC3:	Network has partitioned and some partitions have lost connection to the controller.	(Y)	Can controller hierarchy solve this? How each isolated network partition is controlled? How does the system change from partitioned to fully connected operation?
FC4:	There is an overflow of messages to SDN controller.	(M)	In what situations this can happen and how the controller handles this?
FC5:	There is a single network element failure.	(D)	Demonstrate fast recovery and low overhead.
FC6:	There are multiple network element failures (either occurred one by one or started at the same time).	(D,W)	Indicate advantages of SDN assisted recovery of a larger failure case over traditional approaches. Measure the speed of recovery or the degree of automation (if applicable).
FC7:	Indicate the source and scenario of a disruption. Does SDN provide benefits over non-SDN solutions?	(Y)	Note: After energy outage, SDN may help in re-establishing the network, i.e., updates on QoS treatment to run network in limited capacity mode. Note also that network monitoring and knowledge on the network state may be affected by the disruption.
FC8:	There are problematic signaling delays in the network (specify what kind of delay is seen problematic). Show/explain that resilience is still effective and the SDN solution can cope with network disruptions.	(Y)	Note: this is also related to the monitoring basic assumption. What is the priority of SDN monitoring if there is a CPU shortage?
FC9:	There is unusual but legitimate traffic load in the network.	(Y)	Demonstrate/explain how the used SDN solution improves handling this situation.
FC10:	Traffic is directed to a wrong virtual network.	(Y)	What may have caused this? How is it detected?

fault case IDs	fault/challenge	freq.	comments
FC11:	MNO is configuring its own virtual network slice, which affects a) physical network, b) operations of other virtual networks. How this is a) prevented, b) detected and c) how network recovers from this?	(Y)	Note: this is also related to the security basic assumption.
FC12:	Isolation of virtual network slices: Indicate that one virtual network slice cannot overload network so that it will have effect on the capacities of other virtualisations.	(Y)	

Table 7 SDN Resiliency

7.2 NFV Reliability Use Cases

Network Function Virtualisation is in tight relation of virtualised infrastructure datacentre domain.
The table bellows presents the selected ETSI requirements [9] in the scoped of the SIGMONA Project.

Request ID	Global Requirements
Req.4.2.4	The NFV-MANO function shall provide the necessary mechanisms to recreate VNF automatically after a failure, such as a Virtual Machine (VM) failure.
Req.4.2.6	Failures in the NFVI shall be handled (i.e. detection and remediation) in the NFVI layer or the NFV-MANO (e.g. hardware failure, loss of connectivity, etc.).
Req.4.2.7	The NFVI shall provide the necessary functionality to enable high availability at the VNF level, such as failure notification and remediation.
Req.4.2.9	Storage and transfer of state information need to be provided by the NFVI, where the VNF defines the information to be stored and the NFVI provides the respective object store.
Req.4.2.10	The NFV-MANO functions need to support capacity limitations per instance as part of the deployment instructions of a VNF.
Req.4.2.12	On the NFVI level, there should be an automated fail-over in the case of for example compute, memory, storage or connectivity failures.
Req.4.2.13	There is an overall requirement that a NFV framework shall not contain a single point of failure with the potential to endanger service continuity.
Req.4.2.14	All resiliency mechanisms shall be designed for a multi-vendor environment, where for example different vendors may supply the NFVI, NFV-MANO, and VNFs.
Req.5.4.1	When an anomaly event, which causes hardware/software failure or resource shortage/outage, occurs, the corresponding VNF should be able to be migrated (relocated and restored) with preserving its configuration (e.g. IP address or MAC address) in order to provide service continuity.
Req.5.4.6	When a VNF needs to be migrated to another VM or hardware due to anomaly event, the NFV MANO should be able to access the VNFD to retrieve the deployment conditions and/or constraints of the VNF.
Req.5.4.9	Replication of a VNF and distribution of the load to those VNFs should be supported.
Req.5.4.10	VIM should be able to monitor the used and available resources of the hardware infrastructure and to balance the resource usage among VNFs as appropriate.

Table 8: ETSI requirements

Requirements are further studied in the context of a particular Open Source product: OpenStack Virtual Infrastructure Manager, enhanced with additional tools and functionalities.

7.3 Security delay threats and measurements

In SDMN, if a security system is implemented as an SDN application, then reading the information would include communication delays incurred when reading information from the infrastructure plane, and providing it to the appropriate application for performing counter-measures in the application plane or SDN orchestrator. This process is depicted in figure below. The reading delay might be shorter if the security system, such as network monitoring, is place closed to the infrastructure plane or is co-located with the data plane.

Delay in the phase of assessment or information analysis is security system or function specific. Some security applications might need to observe samples of flow over certain time duration, whereas, some other applications might need to read the switch statistics which might be a one-time or periodic information retrieval operation. Moreover, software based systems have different delays as compared to hardware based systems.

Delays in implementing the necessary security actions in SDMN might need interaction between application, control and infrastructure planes, if the security system is implemented as SDMN application. For example, changing flow rules to divert specific flows to security middle boxes, or dropping packets might incur communication delays between the control and data planes. If the security system is a standalone system, it might require authenticating itself with the SDN controller before issuing/changing flow rules in the data path. In this case, the delay can be even higher.

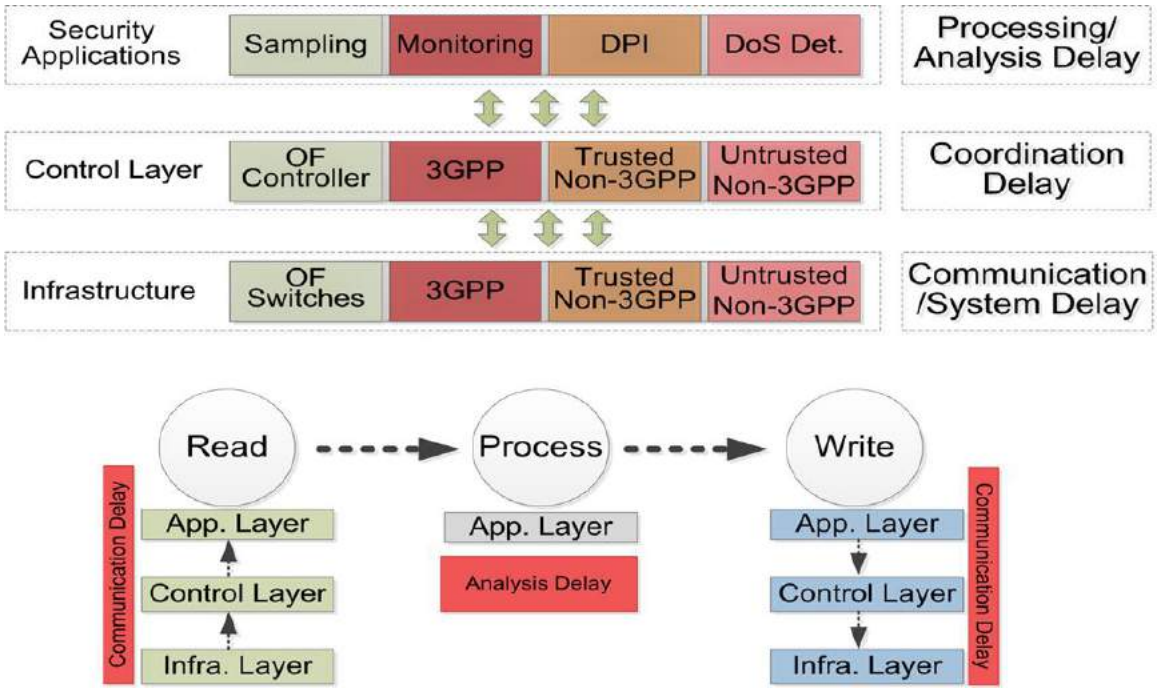

Figure 23Representation of Security systems delay in SDMNs

The main security threats are mentioned in **Error! Reference source not found.** that represents the security threats organised according to the SDN plane/layer and interface. Please mention your security system and the possible reason of delay that could be caused by your system. It is also possible that delays are caused by external factors such as link/channel conditions or load on the controller. However, try to find all the possible reasons and write in **Error! Reference source not found.Error! Reference source not found.** and then mention it for your system in **Error! Reference source not found.**. It will also be helpful if you mention the type of security systems in terms of being software or hardware and SDN layer of implementation or layers involved.

SDN Layer	***Type of Threat***	***Threat Reason/Description***
Application	Lack of authentication & authorization	Possible huge number of (third-party) apps.
	Fraudulent rules insertion	Malicious applications generated false flow rules.

	Access control & accountability	Lack of binding mechanisms for apps.
Control	DoS, DDoS attack, Controller hijacking or compromise	Visible nature of Ctrl-plane.
	Unauthorised controller access	No compelling mechanisms for enforcing access ctrl on apps.
	Scalability or availability	Centralised intelligence.
Data Plane	Fraudulent flow rules	Lack of intelligence.
	Flooding attacks	Limited capacity of flow tables.
	Controller masquerading	Data plane dependence on Ctrl- plane and its security.
Ctrl-Data Int.	TCP-Level attacks	TLS is susceptible to TCP-level attacks.
	Man-in-the middle attack	Optional use of TLS, & complexity in configuration of TLS
App-Ctrl Int.	Illegal controller access, policy manipulation & fraudulent rule insertion	Limited secure APIs, lack of binding mechanisms b/w Apps. & controller.

Table 9 Summary of Security Threats in SDN

Reason for delay	**Explanation**
Communication delay	Delay in cross layer communication in retrieving information from infrastructure up-to controller or to application layer.
Reading Delay	Delay in collecting information such as collecting samples, IP packets.
Observation Delay	Delay in observing network behavior for example, the system needs to collect switch statistics for a certain time.
Analysis Delay	Delay in analyzing information such as checking samples of packets for IDS/IPS/DoS attacks.
System Limitation	Delay due to system is inherent limitations e.g. the system can execute a certain amount of information at a time.
Authentication & Access Control	Time required authenticating or providing access control to network users or applications.
Control Plane Coordination	In federated environments, multiple controllers might need to coordinate.
Counter-measures	Delay between detection and application of counter-measures.
Packet processing delay	Traffic latency introduced in the case of active monitoring.

Table 10 Reasons for delay briefly described.

7.4 Security delay evaluation

In this section, the SIGMONA partners have evaluated the different delays based on the threats and solutions used to mitigate those threats.

7.4.1 Security between control plane and data plane experimental evaluation

IPsec tunneling and security gateways are widely used to secure backhaul communication channels in present mobile networks. Thus, we investigate the usability of these technologies to secure SDMN communication channels and highlight limitations in legacy IPsec mechanisms. Then, we propose a novel secure communication channel architecture by using HIP not only to overcome the identified limitations but also to provide the required level of security for SDMN communication channels.

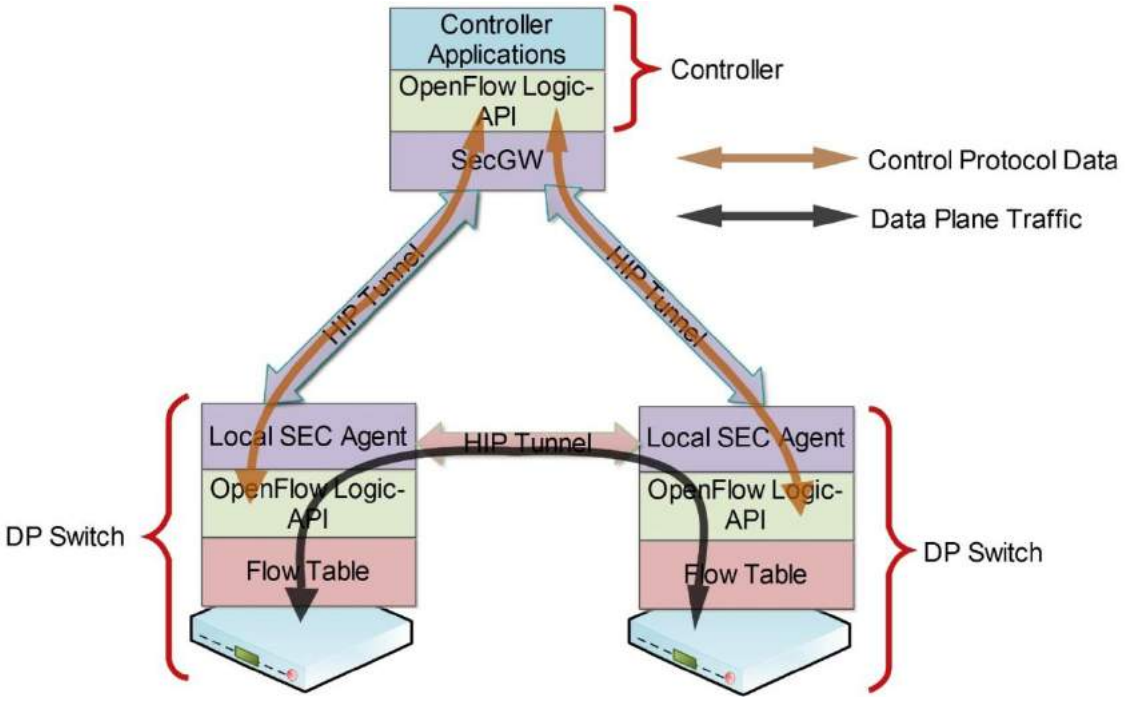

Figure 24 secure communication channel architecture

The delay measurements are given in the following tables The experiment results (**Error! Reference source not found.**) indicate that proposed secure channel has significantly increased the connection establishment delay. The extra HIP tunnel establishment between LSA and SecGW has added extra latency. On the other hand, proposed secure channel has increased flow table update delay only by 4% at steady state of operation (i.e. after the connection is established). The extra layer of encryption is the main reason for the deficient performance of proposed secure channel.

Performance Metric	**Existing SDMN Data Channel**	**Proposed Secure Data Channel**
TCP Throughput (Mbps)	93.5514	91.8054
UDP Throughput (Mbps)	95.2845	92.3828
Latency (ms)	36.6514	37.6452
Jitter (ms)	0.34522	0.4651

Table 11Data Channel Performance without Attack (Normal Operation)

Performance Metric	OpenFlow With TLS/SSL	Proposed Secure Control Channel
Connection Establishment Delay (ms)	58.3224	135.4165
Connection Establishment Delay under TCP SYN DoS Attack (ms)	—	135.9145
Flow Table Update Delay (ms)	30.85645	32.1573
Flow Table Update Delay under TCP Reset Attack (ms)	—	32.2472

Table 12. Control Channel Performance under TCP DoS attack

Furthermore, we have compared the performance of tunnel management mechanisms for the SDMN architecture. LTE defines static channel durations while deploying security systems but we have used the algorithm presented in [10] to estimate the next tunnel duration. We have changed the mean session duration to measure the performance.

We have simulated a backhaul network, stochastic Kronecker graphs, comprising 100 backhaul devices having the bandwidth of 100Mbps in OMNET++. The simulation model establishes IPSec tunnels between the backhaul devices with Poisson arrival process where the session duration is an exponential distribution. We change the mean session duration to measure the performance. The result of the number of tunnel establishment instances per session against the average session duration is presented in **Error! Reference source not found. Error! Reference source not found.** (left). The experiment is run for 1000 times and the average values are shown for five LTE cases where the tunnel duration is predefined at 20, 40, 60, 80, and 100 minutes. The experiment results show that the performance of SDMN is independent of session duration in which the tunnel duration is increased dynamically to adjust to the session duration. As a result, the numbers of tunnel establishment instances are reduced. We also measured the percentage idle time against the average session duration by running the experiment for 1000 times to present the average values. The experiment results shown in **Error! Reference source not found.** (right) reveal that the performance of SDMN is independent of session duration. The tunnel idle time is 30% under the utilised algorithm; however, the performance can be improved with better tunnel establishment algorithms. Since the LTE architecture is highly dependent on the session duration, i.e. converging to 50% in steady state, SDMN has better performance than LTE.

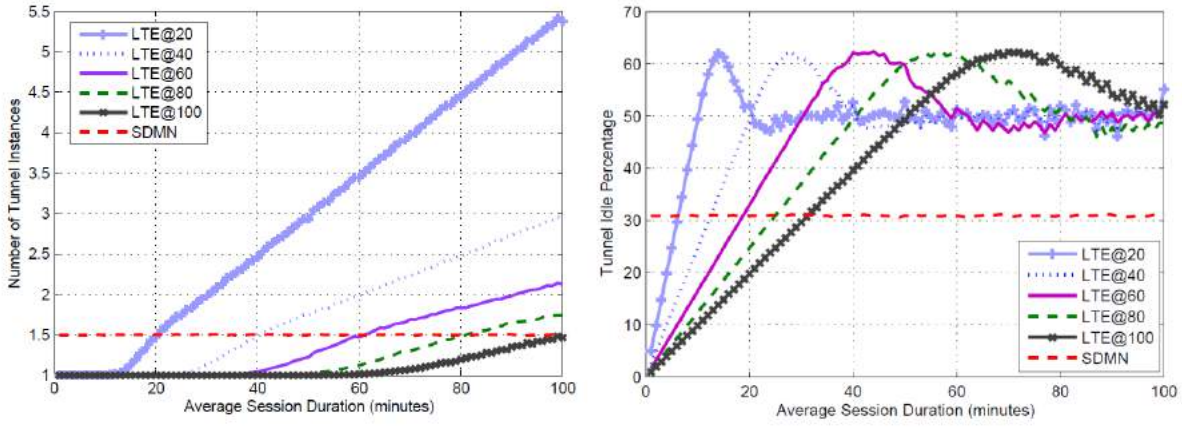

Figure 25 Tunnel establishment instances per session (left) & Percentage Tunnel Idle Time (right).