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

Document Identifier:	D2.2
Document Title:	**Network monitoring in virtualized mobile networks**
Source Activity:	WP 2
Main Editor:	Edgardo Montes de Oca
Authors:	EXFO, MI, TUC
Status / Version:	Draft / Under BSCW version control
Date Last changes:	14.03.2016
File Name:	D2.2_Network_monitoring_in_virtualized_mobile_networks.docx

Abstract:

This document presents challenges and solution alternatives for monitoring of virtualized networks. Traditional probe based solutions, virtual analyzer solutions and hybrid solutions are presented.

Keywords:

SDMN, monitoring, NFV, VNF

Document History:	
15.12.2015	Document created. Updated after first review round Reviewed, all changes integrated

Table of Contents

Authors

Partner	Name	Phone / Fax / e-mail
EXFO	Jorma Ikäheimo	
	Phone:	+358 40 3010215
	e-mail:	jorma.ikaheimo@exfo.com
Montimage	Edgardo Montes de Oca.	
	Phone: +331 53 803577	
	e-mail: edgardo.montesdeoca@montimage.com	
TUC	Marcus Eckert	
	Phone: +49 371 531 39581	
	e-mail: marcus.eckert@etit.tu-chemnitz.de	

Executive Summary

One of the biggest transformations in Wireless Networks industry is Network Functions Virtualization (NFV) and the Software Defined Networks (SDN). NFV is ETSI standardized architecture that separates network functionality from the hardware. NFV means that network functions (such as MME and HSS) will be running as a service in commercial off-the-shelf HW (COTS-HW, e.g., standard or high performance commercial servers).

WP2's scope is to analyse what impacts NFV has on the management and monitoring of mobile networks and what innovation possibilities they open up in these areas.

This document investigates challenges introduced by the virtualized network resources in Software Defined Mobile Network (SDMN) that need to be tackled by an efficient network monitoring solution and presents solution alternatives for implementing network monitoring solutions. Traditional probe based solutions, virtual analyzer solutions and hybrid solutions alternatives are presented for monitoring SDMN.

List of terms, acronyms and abbreviations

API	Application Programming Interface
COTS	Commercial off-the-shelf
CTRL	Controller
DFI	Deep Flow Inspection
DPI	Deep Packet Inspection
EMS	Entity Management System
EPC	Evolved packet core
FPGA	Field Programmable Gate Array
GUI	Graphical User Interface
ISAAR	Internet Service quality Assessment and Automatic Reaction
KPI	Key Performance Indicator
MMT	Montimage Monitoring Tool
MOS	Mean Opinion Score
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
OTT	Over The Top
PCC	Policy and Charging Control
PDF	Probability Distribution Functions
POC	Proof of Concept
PPS	Packets Per Second
QMON	QoE Monitoring
QoE	Quality of Experience
QoS	Quality of Service
QRULE	QoE Policy and Rules
QEN	QoE Enforcement
RTP	Real Time Protocol
SDM	Software Defined Monitoring
SDMN	Software Defined Mobile Network
SDN	Software Defined Network
SLA	Service Level Agreement
vAnalyzer	Virtual analyzer
VM	Virtual Machine
VMI	VM Introspection
VNE	Virtualized Network Element
VNF	Virtual Network Function
VN	Virtual Network Slice
VS	Virtual Switch
vProbe	Virtual probe
XDR	Extended call/session record

List of Figures

1. Introduction

SDN brings new challenges to network trouble-shooting and monitoring. In order to understand problems in a network, the interfaces between the network elements need to be monitored with network monitoring tools. Due to the nature of virtual systems, virtual functions can be dynamically scaled-up, moved between cloud hardware units, etc. Also, it might be possible that there is no physical interface for monitoring a network interface. This dynamicity tends to make network monitoring more difficult, if not impossible, reducing the visibility of system behaviour required by network operators.

WP2's scope is to analyse what impacts NFV has on the management and monitoring of mobile networks and what innovation possibilities they open up in these areas. This document investigates challenges introduced by the virtualized network resources in SDMN that need to be tackled by an efficient network monitoring solution and presents alternative means of implementing network monitoring solutions.

Currently NFV technology is in a Proof-of-Concept (PoC) stage, but already data centres are being deployed that address NFV ETSI standards. Mobile Network multi-vendor PoCs have been finalized and the first implementations of operational EPC/IMS elements in NFV environments have started to appear in 2015. Thus investigating monitoring challenges and proposing adequate solutions in such environments is of high importance.

The rest of the document is organized as follows. "Chapter 2: Monitoring with traditional network monitoring probes". This chapter introduces how traditional network probes can be used for monitoring of SDMN. "Chapter 3: Cloudification (NFV) of the network monitoring" will describe a virtualized monitoring system that can be integrated as part of the virtualized SDMN. Chapter 4 will draw the conclusions made by the participating partners: EXFO, MI and TUC.

2. Monitoring with traditional network monitoring probes

This chapter introduces the existing challenges in monitoring SDMN with traditional network probes and how the traditional network probes can be used for monitoring SDMN. Two existing solutions proposed by the partners are presented: ISSAR and MMT.

2.1 ISAAR solution

2.1.1 ISAAR architecture

The logical architecture of the ISAAR framework is shown in Figure 1. The framework architecture is 3GPP independent but closely interworks with the 3GPP PCC (Policy and Charging Control). If available, it can also make use of flow steering in SDN networks using OpenFlow. This independent structure generally allows for its application in non-3GPP mobile networks as well as in fixed line networks. ISAAR provides modular service specific quality assessment functionality for selected classes of services combined with a QoE rule and enforcement function. The assessment as well as the enforcement is done for service flows on packet and frame level. It incorporates PCC mechanisms as well as packet and frame prioritisation in the IP, Ethernet, and the MPLS layer. MPLS as well as OpenFlow can also be used to perform flow based traffic engineering to direct flows in different paths. Its modular structure in the architecture elements allows for later augmentation towards new service classes as well as a broader range of enforcement means as they are defined and implemented. Service Flow Class Index and Enforcement Database register the available detection, monitoring and enforcement capabilities to be used and referenced in all remaining components of the architecture.

ISAAR is divided into three functional parts which are the QoE Monitoring (QMON) unit, the QoE Rules (QRULE) unit and the QoE Enforcement (QEN) unit. These three major parts are explained in detail in the following sections.

The interworking with 3GPP is mainly realized by means of the Sd interface [3GPP SD] (for traffic detection support), the Rx interface (for PCRF triggering as application function and thus triggering the setup of dedicated bearers) and the Gx / Gxx interface [3GPP GX] (for reusing the standardized Policy and Charging Enforcement Function (PCEF) functionality as well as the service flow to bearer mapping in the BBERF).

Since ISAAR is targeting also default bearer service flow differentiation, it makes use of DiffServ Code Point (DSCP) markings, Ethernet priority markings, MPLS Traffic Class (TC) markings as well as OpenFlow priority changes if available. This is being enforced within the QEN by Gateway and Base Station (eNodeB) initiated packet header priority marking on either forwarding direction inside as well as outside of the potentially deployed GTP tunnel mechanism. This in turn allows all forwarding entities along the packet flow path through the access, aggregation and backbone network sections to treat the differentiated packets separately in terms of queuing, scheduling and dropping.

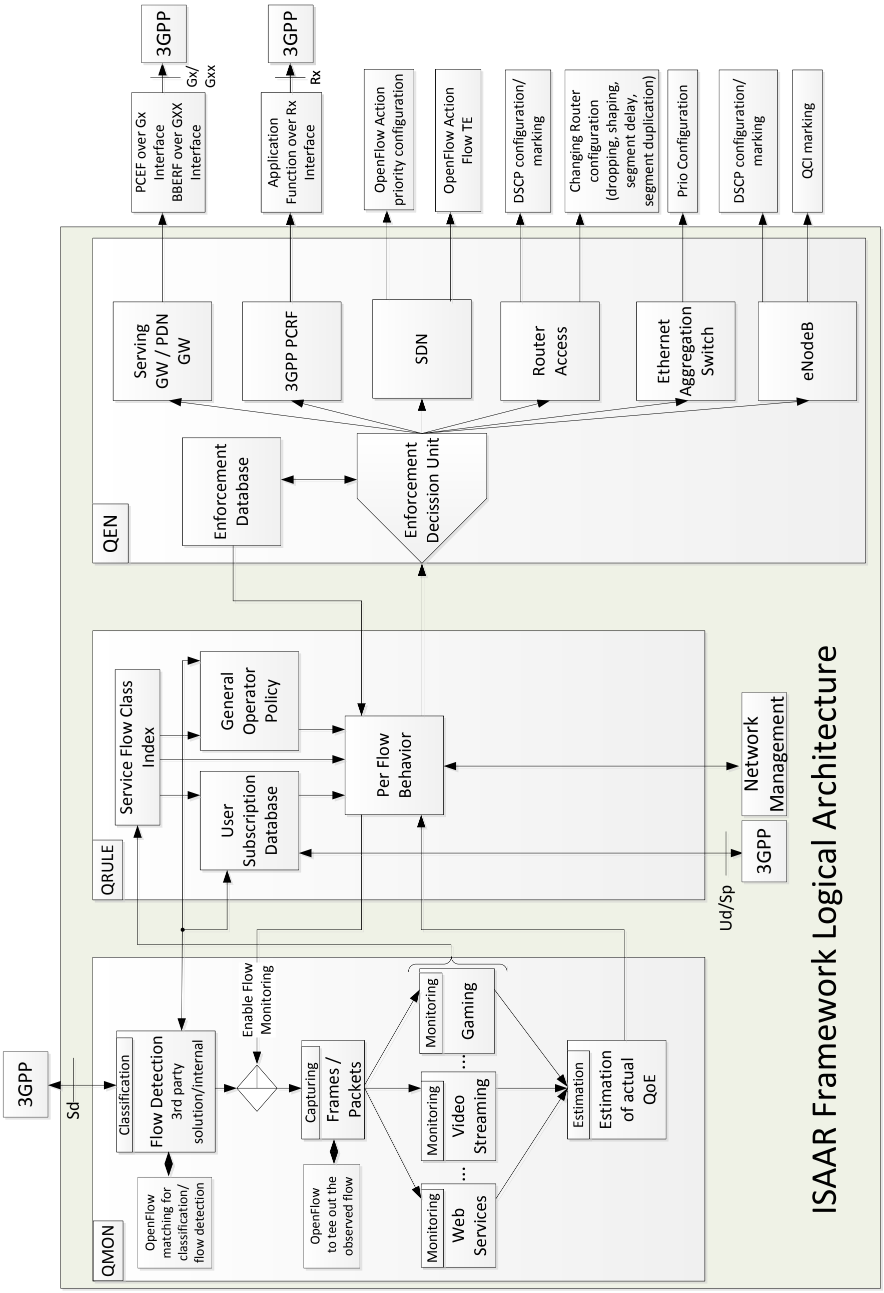

ISAAR Framework Logical Architecture
QEN
Enforcement Database
Enforcement Decission Unit
Serving GW / PDN GW
3GPP PCRF
SDN
Router Access
Ethernet Aggregation Switch
eNodeB
PCEF over Gx Interface BBERF over GXX Interface
Application Function over Rx Interface
OpenFlow Action priority configuration
OpenFlow Action Flow TE
DSCP configuration/ marking
Changing Router configuration (dropping, shaping, segment delay, segment duplication)
Prio Configuration
DSCP configuration/ marking
QCI marking
Gx/ Gxx
Rx
3GPP
3GPP
QRULE
Service Flow Class Index
General Operator Policy
User Subscription Database
Per Flow Behavior
Network Management
3GPP
Ud/Sp
QMON
3GPP
Sd
Classification
Flow Detection 3rd party solution/internal
OpenFlow matching for classification/ flow detection
Enable Flow Monitoring
Capturing
Frames / Packets
OpenFlow to tee out the observed flow
Monitoring
Gaming
Monitoring
Video Streaming
Monitoring
Web Services
...
...
Estimation
Estimation of actual QoE

Figure 1: SDN enabled ISAAR framework

The modular structure of the three ISAAR units (QMON, QRULE and QEN) allow for a centralized as well as a decentralized deployment and placement of the functional elements. The QMON function is described in the following but QRULE and QEN will be described in SIGMONA WP3.

2.1.1.1 QoE Monitoring (QMON)

Today's mobile networks carry a mix of different services. Each traffic type has its own network transport requirements in order to live up to the user expectation. To observe the achieved transport quality and its resulting user service experience, network operators need to monitor the QoE of the respective services. Since the quality of service experienced by the user is not directly measurable within the network, a new method is required, which can calculate a QoE Key Performance Indicator (KPI) value out of measurable QoS parameters. The most challenging and at the same time most rewarding service QoE estimation method is the one for video streaming services. Therefore, QMON will focus on video quality monitoring and estimation, not limiting the more general capabilities of ISAAR for all sorts of service KPI tracking. YouTube is the predominant video streaming service in mobile networks and ISAAR is consequently delivering a YouTube based QoE solution first. Within this YouTube monitoring ISAAR is able to detect and evaluate the QoE of MP4, Flash Video (FLV) as well as WebM video in Standard Definition (SD) and High Definition (HD) format. There are some client based video quality estimation approaches around (e.g. the YoMo application [YoMo]), but we consider such end device bound solutions as being cumbersome and prone to manipulation. Therefore, ISAAR will not incorporate client-side solutions but concentrates on simple, transparent and network-based functionality only.

Some other monitoring solutions follow a similar way of estimation, like the Passive YouTube QoE Monitoring for ISPs approach [YoMoISP. However, they are not supporting such a wide range of video encodings as well as container formats.

Another approach is the Network Monitoring in EPC [MevD51] system, but this does not focus on flow level service quality.

2.1.1.1.1 Flow Classification

The ISAAR framework is meant to work with and without support of an external Deep Packet Inspection (DPI) device. Therefore it is possible to use a centralized DPI solution like the devices provided by Sandvine [Sandv]. For unencrypted and more easily detectable traffic flows the cheaper and more minimalist DPI algorithm which is built in the ISAAR framework can be used. In the first version the build in classification is limited to TCP traffic, focussing on YouTube video stream detection within the operator's network. Extended with SDN support there is a third possibility: given the proper configuration, the matching function from OpenFlow could be used to identify the supported service flows within the traffic mix.

In the centralized architecture the flow detection and classification is most suitably done by a commercial DPI solution. In this case the QoE monitoring units have to be informed that a data stream was found and the classification unit has also to tell them the data stream specific “five tuple”. Contained in the five tuple are the source and destination IP address as well as the source and destination port and the used transport protocol. The QoE measurement starts as soon as the flow identification information (five tuple) is available.

Due to the new SDN features provided by OpenFlow it is not only possible to identify specific data flows within the Internet. OpenFlow is also capable of teeing out a stream which matches a specific pattern. Thereby, the QoE estimation could be distributed to different monitoring units e.g. depending on the specific Internet application. OpenFlow disposes the right flows to the right monitoring unit.

2.1.1.1.2 Flow Monitoring

In the ISAAR framework the flow monitoring is application specific, i.e. for each service that should be monitored, a specific measurement algorithm has to be provided. Our current implementation comprises the YouTube Video QoE estimation. It works transparently and independently from the user's end device. Therefore, no tools have to be installed and no access on the end device has to be granted. The QoE estimation method relies on video stalling events and their re-buffering timings as a quality metric for the video QoE instead of fine grained pixel and block structure errors. To determine the number and duration of re-buffering events it is necessary to comprehend the fill level of the play out buffer at the client, but without access to the end device QMON has to estimate the fill level out of the accessible TCP information within the operator network. Note that focusing on YouTube video incurs TCP encoded HTTP streaming transport. The detailed description of the method can be found in [NetMM and [ANetMM. Three variants of the method exist - an exact method, an estimation-based method and a combination of the two.

2.1.1.1.3 Location aware monitoring

Due to the fact that it is probably not possible to measure all streams within an operator network, a subset of flows has to be chosen either randomly or in a policy based fashion. For example, the samples could be drawn based on the tracking area the flow goes to. If it is possible to map the eNodeB cell IDs to a tracking area, the samples can be drawn in a regionally distributed fashion. With that, it could be decided whether a detected flow is monitored or not due to the respective destination region. Over the time, this sample selection procedure can shift the policy focus to regions with poor QoE estimation results in order to narrow down the affected regions and network elements.

2.1.2 Challenges and solutions

2.1.2.1 Capturing and identification of measurable data

For observing video streams ISAAR has to be able to detect the regarded flows within the traffic mix. In the traditional ISAAR a simplified DPI was used, which was able to sort out TCP based YouTube video traffic by an analysis of http requests. Therefore, each packet had to be examined until a data flow containing a video stream was found. As soon as a video is detected the stream is followed by using a five tupel consisting of source and destination IP-address, source and destination port as well as the used transport protocol.

2.1.2.2 Deciphering

In case the analyzed traffic is ciphered, for instance NAS in S1-MME interface, deciphering keys should be provided for being able to decipher the traffic.

2.1.2.3 QoE evaluation based on QoS parameters

QoE is not directly measurable because of the subjective experience of each individual. To derive the QoE out of measurable QoS parameters perceptive user tests have been driven out. Due to the fact that common Key Performance Indicators KPIs like pixel or block structure errors and artefacts are not applicable for progressive download video services and considering the user tests three criteria are vital for the QoE calculation for progressive download video. The first one is the number of occurred stalling events, the second one is the duration of the corresponding stall and the third one is the time since the last stall finished.

To represent the QoE a five point Mean Opinion Score (MOS) is used as a common scale for user experience. Following the approach in [Ouellette] the scale reaches from 4.5 as the best mark to 1 at the worst. The three parameters are merged into a so called "Negative Impact" (NI). For each video a basic MOS of 4.5 is assumed and is decreased by the calculated NI at each point in time.

2.2 MMT solution

2.2.1 MMT architecture

MMT (Montimage Monitoring Tool) is a monitoring solution that combines data capture, filtering and storage, events extraction and statistics collection, and, traffic analysis and reporting providing, network, application, flow and user level visibility. Through its real-time and historical views, MMT facilitates network performance monitoring and operation troubleshooting. With its advanced rules engine, MMT can correlate network and application events in order to detect performance, operational, and security incidents. An easy-to use customizable graphical user interface makes MMT suitable for different user needs.

MMT is composed of three complementary, yet independent, modules:

- **MMT-Extraction** is the core packet processing module, it is a C library that analyses network traffic using Deep Packet and Flow Inspection (DPI/DFI) techniques in order to extract hundreds of network and application based events, measure network and per-application QoS/QoE parameters and KPIs. MMT-Extraction is powered with a plugin architecture for the addition of new protocols and attributes, and a public API for integration in third party probes. Notably, plugins have been developed to extract meta-data from RTP and OTT video flows.
- **MMT-Correlation** or analysis modules are advanced rule engines that analyse and correlate network and application events to detect performance, operational and security incidents. They are powered with self-learning capabilities to derive the baseline network and application parameters for dynamic threshold based analysis. A Quality Monitoring engine has been developed that allows deriving the Quality Index of video flows from the KPIs extracted by the RTP and OTT plugins. This Quality Index corresponds to the impact on the user’s Quality of Experience due to the network performance.
- **MMT-Operator** collects and aggregates extracted data, generates network and application statistics, and presents them via a graphical user interface. MMT-Operator is customizable; the user can define new statistics to be collected and configure new views or customize the large list of predefined ones. With its generic connector, MMT-Operator can be integrated with third party traffic probes.

Figure 2 shows the modular architecture of MMT that can be easily extended with the following:

- Plugins to classify and extract data and meta-data of new protocols or any observable structured information (e.g., application traces, system logs, messages).
- Analysis modules implementing algorithms that analyze the extracted data to allow assessing the network using event correlation and machine learning techniques.
- User defined reports and views that present the information and notifications in a way that corresponds more closely to the user’s needs.

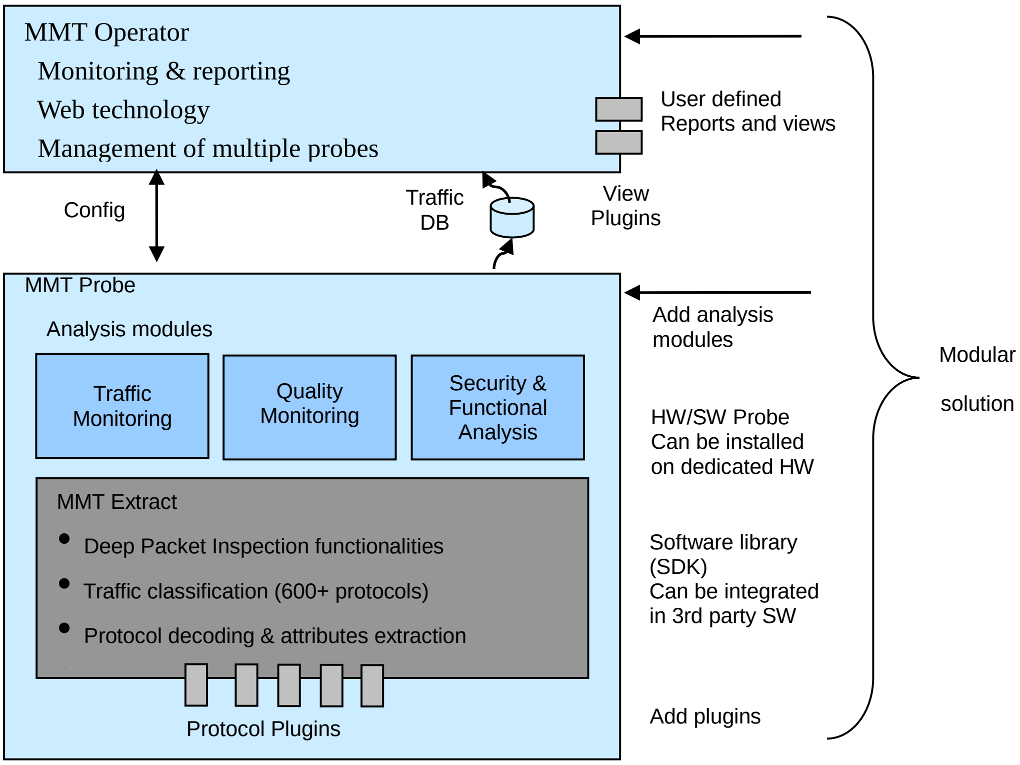

MMT Operator
Monitoring & reporting
Web technology
Management of multiple probes
User defined Reports and views
Config
Traffic DB
View Plugins
MMT Probe
Analysis modules
Traffic Monitoring
Quality Monitoring
Security & Functional Analysis
MMT Extract
Deep Packet Inspection functionalities
Traffic classification (600+ protocols)
Protocol decoding & attributes extraction
Protocol Plugins
Add analysis modules
HW/SW Probe Can be installed on dedicated HW
Software library (SDK) Can be integrated in 3rd party SW
Add plugins
Modular solution

Figure 2: MMT's modular architecture

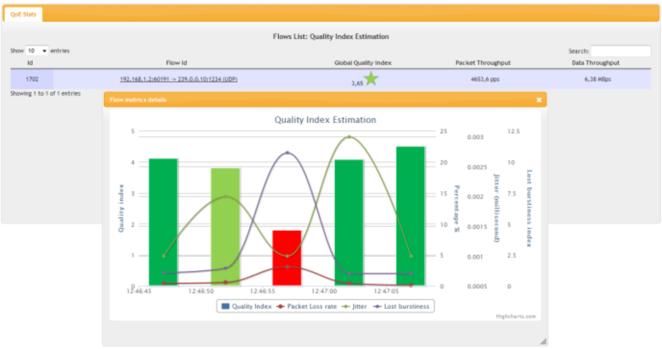
2.2.1.1 **MMT Features**

- Granular traffic analysis capabilities through the ability to extract a wide range of network and application based traffic parameters and events (RTT, jitter, loss, HTTP response time, VoIP MOS, Video QoE, etc.)
- Application classification making possible the detection of applications using non standard port numbers like P2P applications.
- Powerful rule engines and analysis modules: that allow the application of machine learning algorithms and the detection of the occurrence of complex sequence of events that conventional monitoring does not detect. This can be used for example to detect anomaly or attacks, or advanced performance incidents.
- Configurable reports: MMT traffic reports and charts are extensively configurable. The user can edit pre-configured reports and create new ones. Different chart types and graphs can be used including (pie, bars, XY-charts, Stacked area charts, sequence charts, tables, hierarchical tables, etc.).
- Per application reports: MMT is capable of decoding and analysing the message exchange of more than 600 widely used application protocols (HTTP, POP, SMTP, etc.). This gives a possibility to create application based reports. This can be useful for example to monitor the response time of an HTTP server, the variation over time of the quality of VoIP calls, or to draw the message exchange sequence with a business application.
- Multi-platform solution: MMT is available on Windows and Linux based distributions. It can be installed as software on commodity hardware or optimized for integration in dedicated probes.

2.2.1.2 QoS/QoE Analysis

- QoS/QoE modular solution: can be provided as a standalone tool or as a set of libraries to be integrated in a third party solution.
- Different protocols and streaming technologies: MMT supports different video protocols (e.g. IPTV, RTP, and OTT) and deals with different streaming technologies (adaptive bitrate switching, scalable video coding, etc).
- KPI extraction: Computation and extraction of relevant network QoS parameters at the session level (e.g. jitter, packet loss rate, burstiness rate etc.). These parameters may impact video Quality of Experience (QoE).

- <u>OTT services:</u> MMT allows the computation of application level impairment (like freeze time, frequency of freezes, number of bitrate switching, etc.) due to different network conditions. These impairments may also impact the video QoE.
- <u>QoE estimation:</u> the estimation of the quality of experience of video streaming services based on network and application level parameters is an experimental module that relies on a fuzzy logic expert system.
- <u>QoS/QoE reports:</u> Default reports and chart are specified for video services QoS/QoE analysis. These reports are configurable. Figure 3 represents an online real-time report provided by the Quality Module using fuzzy logic techniques to estimate the Quality Index of RTP video flows from the extracted QoS parameters.



QoE Stats

Flows List: Quality Index Estimation

Show 10 entries　　Search:

Id	Flow Id	Global Quality Index	Packet Throughput	Data Throughput
1702	192.168.1.2:60191 -> 239.0.0.10:1234 (UDP)	3,65 ★	4653,6 pps	6,38 MBps

Showing 1 to 1 of 1 entries

Flow metrics details

Figure 3: Quality Index report

The video quality estimation technique follows a methodology that consists of conducting subjective tests with end user participants in order to build a learning set for correlating objective network QoS metrics with the subjective QoE provided by the participants. This correlation was then used to build the membership functions and inference rules of our fuzzy expert system for video QoE estimation.

From the subjective test, a learning set is built that consists of the mapping between the participants' scores and the QoS metrics for each of the considered video clips. A probabilistic approach is used to correlate QoS metrics to the participants' scores. Therefore, for every QoS metric, five different Probability Distribution Functions (PDF) are built (one function per QoE score) that provide the variation of the participants' ratio (%) with the QoS metric for a specific QoE score. This probabilistic information is changed into a fuzzy set by dividing the PDF by its peak value (normalized PDF) [Anoop]. The fuzzy set, which has the same form as that of the original PDF, is converted into an equivalent triangular or trapezoidal fuzzy set by using a curve fitting method [Matlab]. The triangular or trapezoidal fuzzy set represents the membership functions for the different QoS metrics. More information can be found in [Pokhrel].

2.2.2 MMT Challenges and solutions

Legacy solutions to assess QoS and QoE can also be used in SDMN. These types of networks bring better flexibility for managing the network performance and assuring expected QoS and QoE defined by Service Level Agreements.

One of the main advantages of SDN is that it simplifies network management, and facilitates the upgrade of functionality and debugging. SDN enabled centralized control and coordination makes it possible to deliver the state and policy changes more efficiently, and deploy corrective measures more rapidly. Network Functions Virtualization (NFV) also brings advantages since it improves scalability of applications such as QoS monitoring and by introducing virtualized abstraction, the complexity of hardware devices is hidden from the control plane and SDN applications. Furthermore, managed network can be divided into virtual networks that share the same infrastructure but are governed by different SLA policies. SDN and NFV makes possible the sharing, aggregation and management of available resources, enables dynamical reconfiguration and changes of policy, and provides granular control of network and services through the abstraction of the underlying hardware.

2.2.2.1 Capturing data from SDMN

Existing QoS/QoE solutions, like the work presented in the previous subsections, need to be adapted and correctly controlled since they were meant mostly for physical and not virtual systems and boundaries and do not allow fine-grained analysis adapted to the needs of SDMN network management. The lack of visibility and controls on internal virtual networks created and the heterogeneity of devices used make many performance assessment applications ineffective. On one hand, the impact of virtualisation on these technologies needs to be assessed. For instance, QoS monitoring applications need to be able to monitor virtual connections. On the other hand, these technologies need to cope with ever-changing contexts and trade-offs between the monitoring costs and the benefits involved. Here, virtualisation, as well as SDN, facilitate changes making it necessary for monitoring applications to keep up with this dynamicity.

To be able to perform end-to-end QoS a monitoring architecture needs to be defined and deployed that will measure and analyze the network flows at different observation points that could include the devices of the end-users, as well as the virtual and physical machines. Setting up several observation points is necessary to better diagnose the problems detected. With SDN it is possible to create network monitoring applications that collect information and make decisions based on a network-wide holistic view. This enables centralised event correlation on the network controller, and allows new ways of mitigating network faults.

SDN and NFV introduce virtualized networks and functions that need to be monitored. This can be done by probes deployed in virtual machines, but another technique that can be used is virtual machine introspection (VMI). Using this technique, the monitoring function is co-located on the same machine as the host it is monitoring and leverages a virtual machine monitor to isolate it from the monitored host. In this way the activity of the host is analyzed by directly observing hardware state and inferring software state based on a priori knowledge of its structure.

VMI allows the monitoring function to maintain high levels of: visibility, evasion resistance (even if the host is compromised), and attack resistance (isolation), and even enables the manipulation of the state of virtual machines. Unfortunately, VMI based monitoring software depends on the operating system, application type and versions. Furthermore, VMI require privileged access, meaning that cloud providers need to authorize its use. Nevertheless VMI can be a cloud service provided by cloud providers.

2.2.2.2 Scaling

Cloud infrastructure introduces elasticity and scalability that can benefit the monitoring tasks, but also help improve the monitored cloud services, the resource utilization, the performance load and the capacity planning. The goal is to guarantee the end-users an acceptable performance with a minimum of resources defined by Service Level Agreements (SLAs) negotiated between customer and provider. As done for video flows, imprecise data can be modeled with fuzzy logic, or other machine learning techniques, to be used in a behavior, load and performance prediction model. In this way the scaling mechanism offered by the cloud can be optimized.

3. Cloudification (NFV) of the network monitoring

Network virtualization introduces many benefits that can be used by the network monitoring functions and solutions. According to the market study carried out by SDNCentral [NV report] these are mainly, in order of importance: Flexibility, OPEX savings, Agility, Scalability and CAPEX savings; as shown in Figure 4.

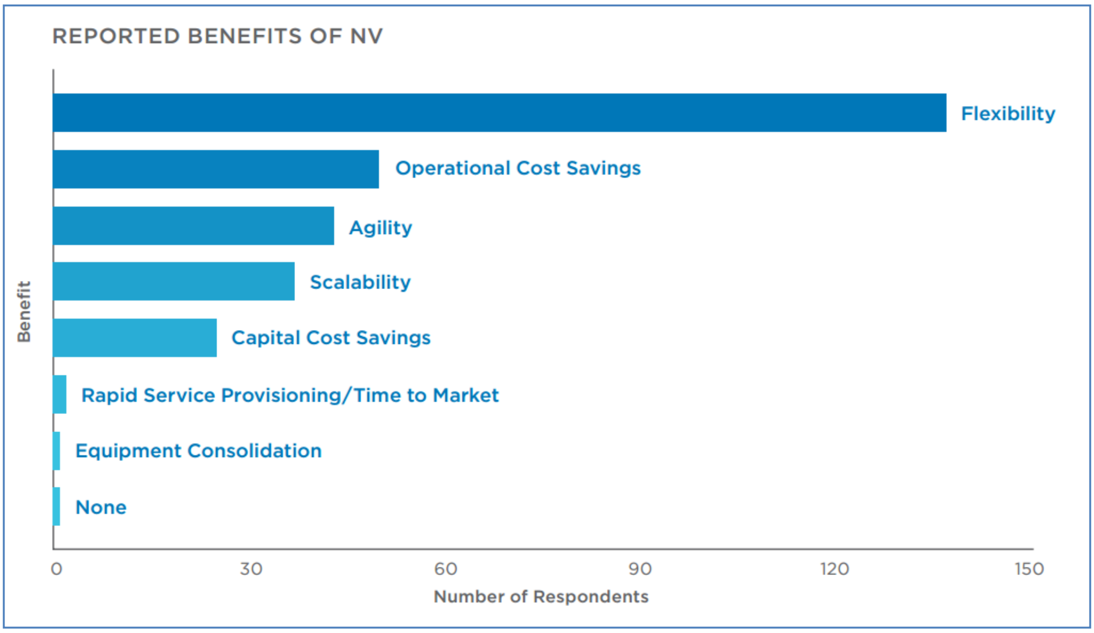


Figure 4: Benefits of network virtualization

In the advent of widespread adoption of SDN and SDMN, the way the network is monitored will change. Dedicated monitoring systems will eventually be replaced by software-based systems integrated as part of SDMN, because of the benefits virtualization technologies offer. The next subsections introduce three different solutions for virtualized monitoring system that can be integrated as a part of virtualized SDMN.

The introduction of what can be called software defined monitoring introduces several advantages:

- Abstraction: SDN approach abstracts the control from the physical constructs of the network, for instance, the stateful firewalls and wire sniffers, and replaced by a set of flexible controls in the form of policy envelopes blanketing the virtualized (or physical) assets. With this level of abstraction, it is possible to establish common security or performance models that can easily be replicated across the network without recourse to the actual capabilities of the underlying physical hardware.
- Automation: Using SDN, each redeployed asset automatically inherits the predefined security or performance policy. In this way it is easy to mitigate or eliminate inadvertent operator errors and ensure that no asset is deployed without being automatically attached to the required policies and control, unlike traditional solutions that heavily depends on manual detection, action, and administration to deal with anomalies.
- Scalability and flexibility: With SDM, over-dependence on physical hardware is eliminated. This means that monitoring can be implemented in a case by case basis depending on what is considered appropriate for each network scenario and business needs. In other words, given that the monitoring functions are implemented on software, they are more flexible and can easily be scaled up across a cluster or a data center.
- Control orchestration: SDM integrates multiple network controls into a single coordinated engine for intelligent analysis and actions such as monitoring and remediation. Hence unlimited amount of input can be channeled into a policy-driven orchestration framework. This will ultimately improve the accuracy of the collected data and the effectiveness of the corresponding actions. Such orchestration is crucial to ensure compliance with designed policies since all major compliance standards dictate a variety of controls as parts of the specifications.
- Portability: Cloud-based SDM data centers allow assets to retain their settings even when they change location.
- Economically viable: With virtualization, SDM security functions are dynamically deployed on already existing network infrastructure with minimum CAPEX costs. This also makes for a more flexible management

schemes such as dynamic configuration, and countermeasures leading to reduced OPEX costs. With traditional monitoring appliances, these features are difficult to implement and would come at much higher costs.

- Easy deployment: SDM, as a new model of flow monitoring, supports the easy deployment of advanced monitoring and performance/security applications on the networks. SDM enables the high speed and high quality flow measurement of network traffic at the application layer.

3.1 Power Hawk Pro Solution

3.1.1 Challenges

In a physical network environment the switches connecting network elements provide tools like port mirroring for capturing traffic between the network elements. In virtualized environment the switches and other network elements can be virtualized making traffic capturing a bit harder. Virtual OS vendors have solved this problem by providing tools for capturing and filtering captured traffic [VMW] between ingress and egress points of VM and providing the captured traffic to virtual monitoring machines and to legacy monitoring systems connected to monitoring ports.

However it would be good to have monitoring system as VNF in SDMN , for instance in order to be able to reduce the cost of the monitoring system, to be able to scale monitoring systems according load of the SDMN.

3.1.2 Architecture

Virtual analyzer is based to EXFO's Power Hawk Pro probe software. It integrates to virtual switch to capture packets for analysis. Virtual analyzer performs control plane call and session analysis and provides results out-of-band for various functions to perform network monitoring or troubleshooting tasks.

Figure 5 describes architecture of virtual analyzer in reference to NFV architecture of ETSI [NFV]. vAnalyzer is the component performing the actual call and session analysis and writing results to XDR and KPI databases (or to flow/DPI database in case of user plane analysis) and writing analyzed packets (raw data) to capture file storage. Analyzer GUI is the application used to view analysis results It reads the results from respective result databases, visualizes the results and provides drill down between KPIs, calls and session and packets. vAnalysis manager is the component monitoring the load of the vAnalyzers and controlling up/downscaling of vAnalyzer instances.

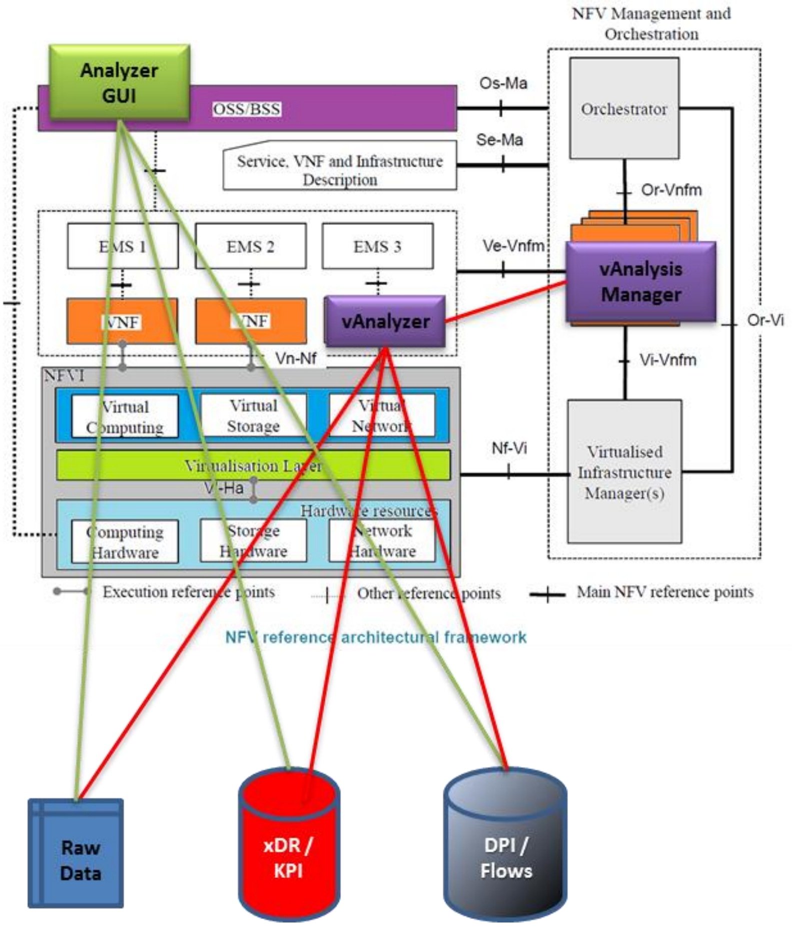


Figure 5 vAnalyzer target architecture

Figure 6 describes minimum architecture used in proof of concept to validate functionality and performance of the virtual analyzer concept. In the proof of concept only the actual analyzer component is virtualized and integrated with the VNFI, management of vAnalyzer instances is taken care manually and external Analyzer GUI is used to view the results.

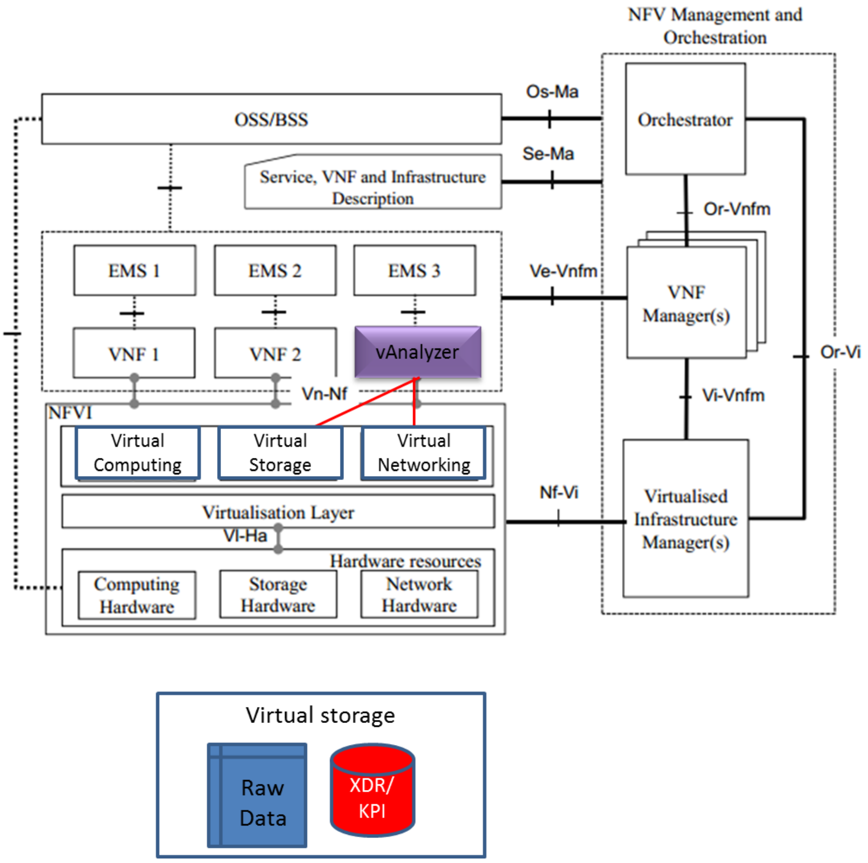


Figure 6: Virtual analyzer architecture, proof of concept

Figure 7 presents the architecture of EXFO vAnalyzer in NFV system. SAM VNF function captures packets from vSwitch, performs control plane analysis and writes results to call and session DB (XDR DB) and XDR flat files. The DB is separated to another VNF (not presented in the figure) in order to keep DB unaffected of SAM VNF scaling. vAnalyzer EMS is controlling instances of SAM VNF according load in monitored SDMN. Analysis results are provided through DB interface and in CSV (Comma separated value) files to OSS/BSS utilizing the results in network monitoring and trouble shooting.

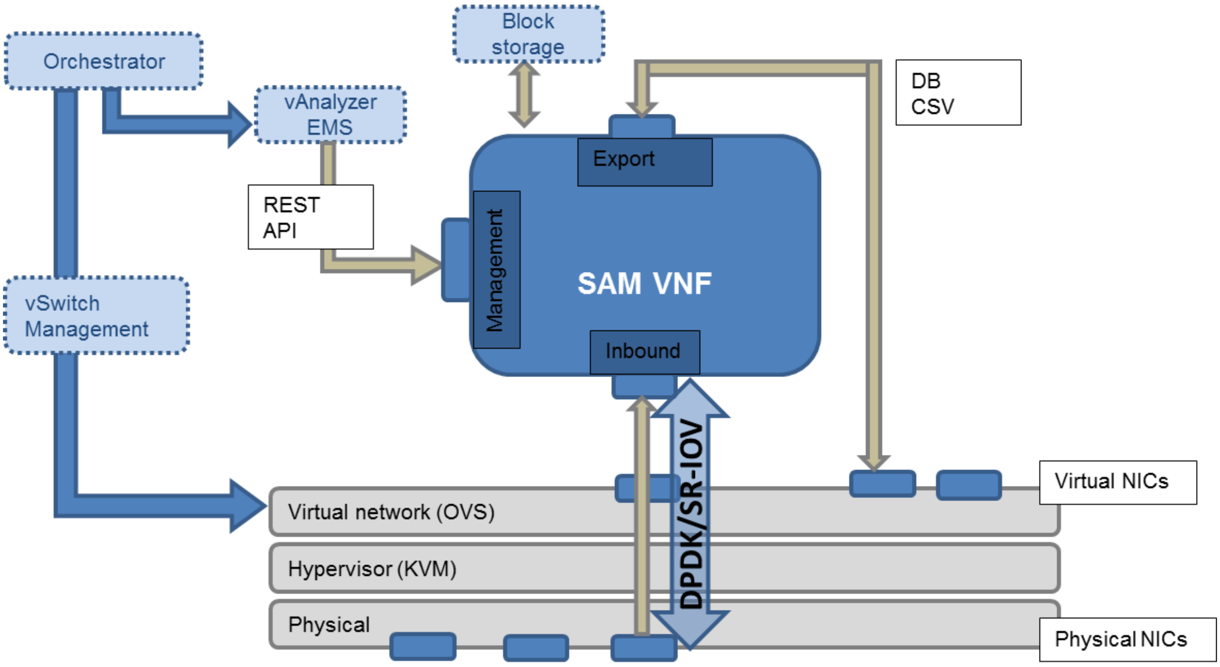


Figure 7: Architecture of vAnalyzer

3.1.3 Challenges and solutions

3.1.3.1 Capturing data

Packet capture performance is critical considering the whole NFVI performance, SR-IOV (single-root I/O Virtualization) is required for performance optimization. The SR-IOV standard allows network cards shared among multiple virtual machines while optimizing packet delivery to the VMs. With the SR-IOV required performance can be achieved [Dong].

In order to monitor virtualized telecommunication network, it should be possible to monitor inter VNF communication, however such monitoring may not be possible. Current OpenStack specifications [Openstack] provide blueprints for the solution, but it's not yet implemented.

3.1.3.2 Performance

According EXFO's experiences gained from LTE monitoring, LTE control plane traffic of 2M subscribers is approximately 300Mbps/300Kpps when S1-MME, S6a and S11 interfaces are monitored.

3.1.3.2.1 Capture to memory performance

According [Intel] when using Intel DPDK poll mode drivers capture to memory is not a problem. DPDK optimized packet capture is capable of millions of PPS.

3.1.3.2.2 Analysis performance and resources

EXFO's current analyser SW is able to perform 300Mbps analysis with 6 cores@3GHz, maximum amount of memory required is 64GB.

3.1.3.2.3 Capture to disk performance and capacity

Capture to disk is used to store raw packets for drilldown to be used in troubleshooting. Capture to disk performance is depended of the virtual storage, LTE control plane traffic of 2M subscribers is approximately 300Mbps, the virtual storage must be selected to fulfil throughput and capacity requirement. Normally a few days of storage capacity is required. *Table 1:Packet capture storage capacity* provides examples of storage capacity requirements.

Table 1:Packet capture storage capacity

throughput Mbps	storage days	total required storage TB
300	1	3,1
300	3	9,3
300	7	21,6

3.1.3.3 Scaling

Scaling of vAnalyzer instances in controlled by vAnalysis EMS, it collects statistics from analyzer and starts/stops instances of vAnalyzer according to estimated load. Analyzer EMS should collect long term and busy hour statistics to be able to launch analyzer instances at correct time. The result storage must be separate from vAnalyzer instances so that results can be used when actual analyzer is not running.

3.1.3.4 Deciphering

In case the analyzed traffic is ciphered, for instance NAS in S1-MME interface, deciphering keys should be provided for being able to decipher the traffic. EXFO’s current analyzers can capture required decipher keys from S6a interface.

3.1.3.5 Licensing

Software licensing is an issue not yet solved, it can be solved by using external license manager, but preferable a way would be not to require license management but take care of the issue with contract agreements.

3.1.3.6 Load balancing

Load balancing is performed by vAnalyzer EMS by sharing incoming data to multiple SAM VNF instances. For example, transport layer IP addresses can used for load balancing. Load balancing is done by setting suitable filters to network card during set-up of network port for VNF.

3.1.3.7 Filtering

Filtering is used to filter in analyzed traffic and filter out for example user plane traffic. Filtering is controlled by vAnalyzer EMS by setting suitable filters to network card during set-up of network port for VNF.

3.2 SDN/NFV-ISAAR Solution

In order to achieve acceptable service quality, the broad spectrum of Internet services requires differentiated handling and forwarding of the respective traffic flows within increasingly “Internet Protocol (IP)” based mobile networks. The “3rd Generation Partnership Project (3GPP)” standard based procedures allow for such service differentiation by means of dedicated “GPRS Tunnelling Protocol (GTP)” tunnels, which need to be specifically setup and potentially updated as the mixture of client initiated service consumption changes. The ISAAR (Internet Service quality Assessment and Automatic Reaction) framework augments existing quality of service functions in mobile networks by flow based network centric quality of experience monitoring and enforcement functions. The ISAAR framework is meant to be an all in one solution for service quality monitoring and QoE enforcement within an operator network.

In the following the SDN/NFV ISAAR Framework is described, but the monitoring is only one functional block of this framework.

3.2.1 Solution architecture

ISAAR consist of three functional blocks the quality monitoring (QMON), the quality rules entity (QRULE) and the quality enforcement (QEN). The task of QMON is flow detection and assessment as well as monitoring and estimation of the Quality of Experience of the respected Internet services. QRULEs tasks are creation of policy rules for each observed flow and the flow manipulation for the respective flows is handled by QEN. The architecture and the function of the former version of ISAAR without SDN and NFV support are described in detail in the paper “ISAAR (Internet Service Quality Assessment and Automatic Reaction) a QoE Monitoring and Enforcement Framework for Internet Services in Mobile Networks” [ISAAR].

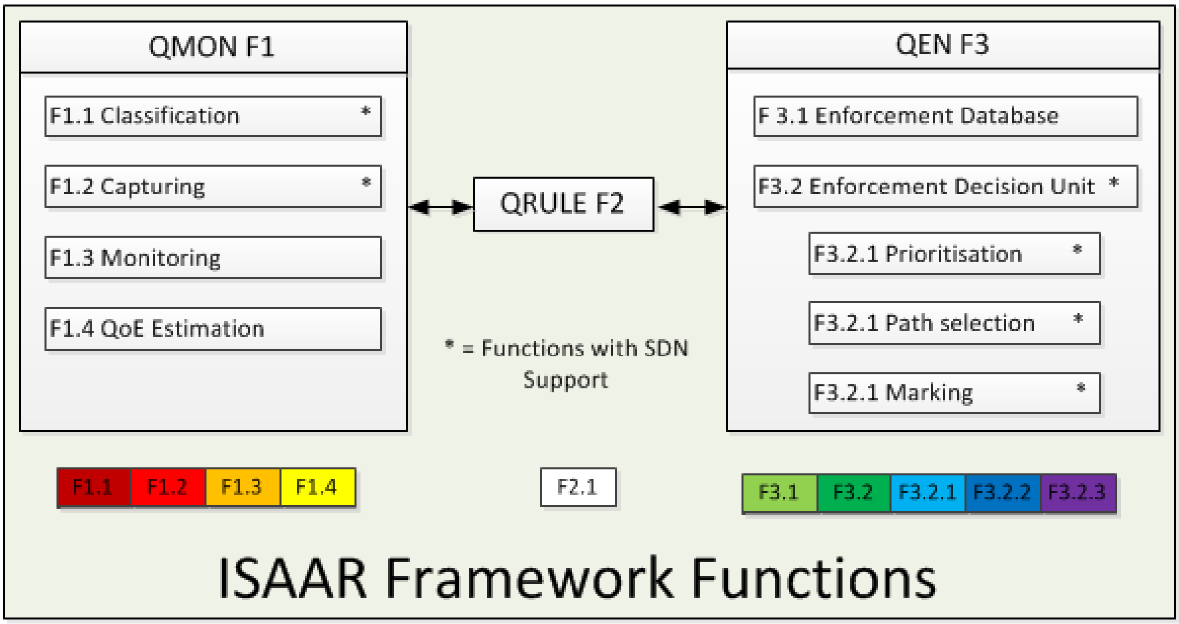


Figure 8 ISAAR functional blocks with function split

Each of the frameworks functional blocks can be split in single functions as shown in Figure 8.

Until now the deployment of ISAAR was either a distributed or a centralized approach. In the centralized version the only view monitoring and manipulation probes were deployed e.g. at the Gi/SGi interfaces of a mobile network. In the distributed approach many probes shall be deployed and spread all over the network, e.g. at Base Stations, NodeBs or eNodeBs. Both approaches have one thing in common on each observation/manipulation point a middle box has to be installed for monitoring and enforcement and each of the boxes has to be able to carry all the functions mentioned in Figure 8.

One approach to overcome this limit is the utilization of Software Defined Networking (SDN) and Network Function Virtualization (NFV). The first step is the creation of an SDN only ISAAR which is shown in Figure 9.

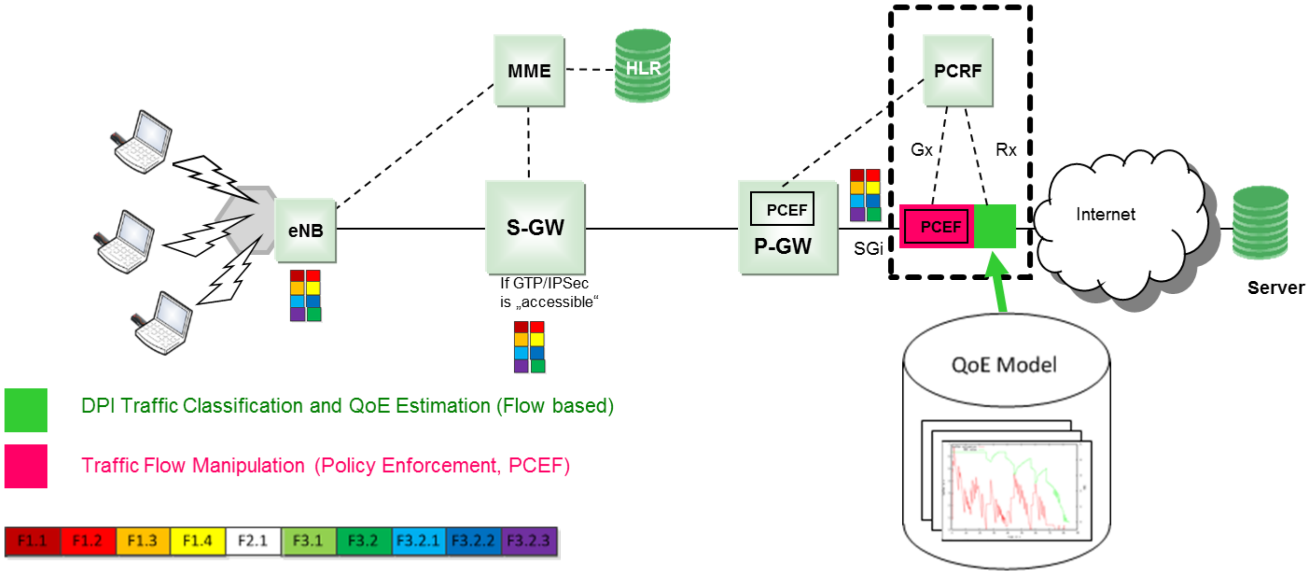


Figure 9 SDN enhanced ISAAR

Two out of three functional blocks of ISAAR, the Quality Monitoring (QMON) and the Quality Enforcement (QEN) can benefit of using the functionalities of SDN. The quality monitoring of Internet services starts with identification of the respected flows within the traffic mix. Normally a lot of processing is needed for this detection, due to the Deep Package Inspection (DPI). To simplify that mechanism the SDN matching rules can be used. Therefore, the SDN controller has to be configured in a way which allows identifying measurable traffic by using the matching rules and teeing it out for to one of the measuring points of ISAAR. The next advantage which can be derived is the real time tee out of regarded traffic. In most SDN implementations there are all mechanism which are needed to copy the measured traffic to an own port or switch a path to a measuring probe, enabling the usage of viewer more centralized probes.

On the other side SDN functionalities can be used for changing the per hop behaviour (PHB) for each traffic flow. If the quality is changing, ISAAR can signal the change in the PHB to the controller. But only the change, increasing or decreasing the priority of the flow, will be signalled the SDN controller decides on its own how the change in priority is done. This means that the SDN controller becomes the QEN of ISAAR. Hence, it could be possible to monitor a certain stream, calculate the QoE of the service and react on the estimated value. If the service has a high MOS then ISAAR can signal the SDN controller to reduce the priority of the respected flow. If there are no other enforcement mechanisms within this network, the QEN functional block of the framework will be completely replaced by SDN.

However, the middle boxes still need to do every function in the place where they are deployed. Here the NFV is taken into account. Some of the function in the ISAAR framework can be virtualized and placed in a datacentre. For example the whole QRULE functional block can be realized in software and put anywhere in the network. Only the quality information of the observed flows has to be signalled to the rules entity and the designed behaviour has to be sent to the QEN functions. The quality monitoring, the QoE estimation, the enforcement database and the enforcement decision unit can be virtualized and placed in a datacentre, too. But, there are still functions which have to stay within the user data path. Out of these thoughts two versions of the SDN/NFV ISAAR were designed, the light version and the full version.

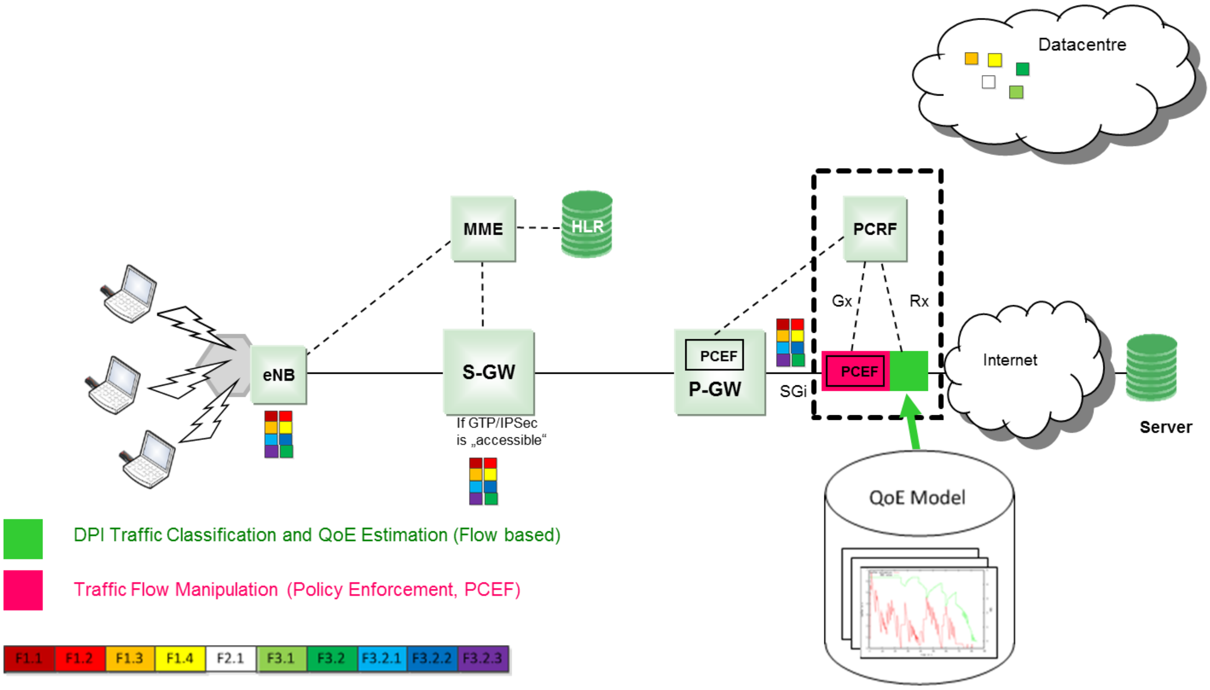


Figure 10 SDN/NFV enhanced ISAAR light version

Within the light version which is shown in Figure 10 the possible functions were virtualized and processed within a datacentre but they are still implemented in the middle boxes. In this case the QoE estimation can be done in the middle box but if the processing capacity is not sufficient the respected data streams can be teed out to a datacentre where the virtualized QoE estimation is running and can be processed there.

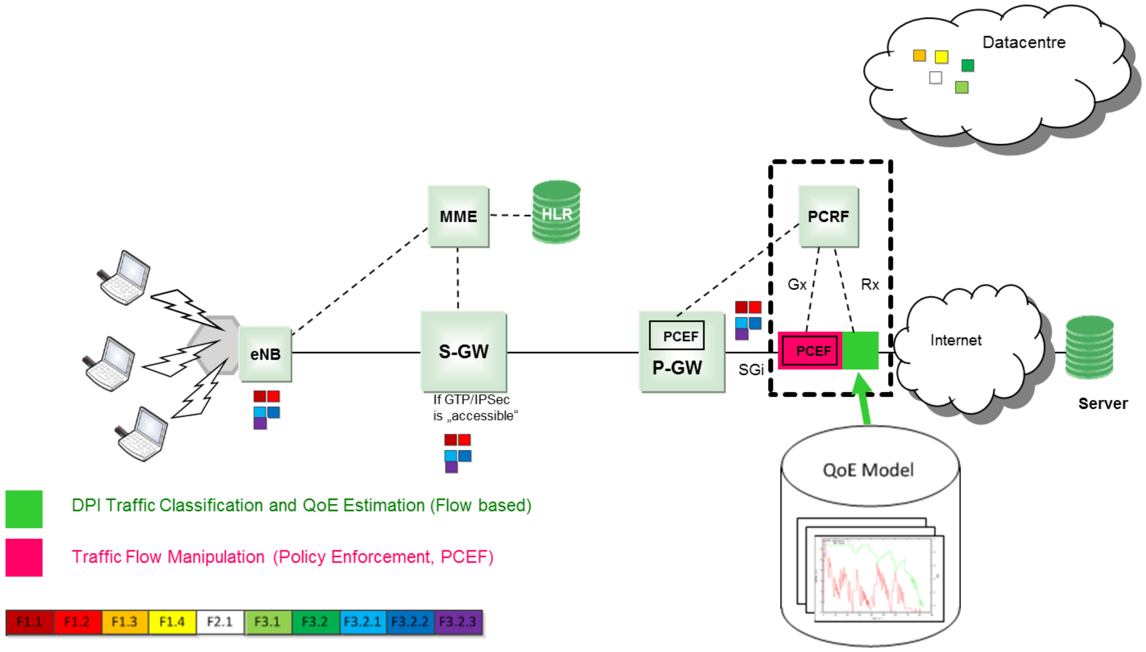


Figure 11 SDN/NFV enhanced ISAAR full version

In the full version the virtualized functions are only processed in the cloud, meaning the middle boxes are not able to perform these tasks. The benefit of leaving out the virtualized functions from the middle boxes is the saved processing capacity which possibly leads to leaving out the middle boxes themselves and implement the remaining functions like the classification, the capturing and some enforcement functionalities in the common network equipment like eNodeB, routers or switches or using the already implemented function within these network elements.

Both SDN/NFV ISAAR versions are still utilizing the SDN mechanisms for flow detection, teeing out the respective traffic transport the necessary information to the datacentres where the VNFs are running and implement the QoE enforcement to the remaining traffic according to the rules functions.

3.2.2 Challenges and solutions

3.2.2.1 Capturing data

The main challenge in the traffic capturing is the distributed fashion of SDN/NFV ISAAR. Therefore, the captured data have to be correlated and mapped to the single stream to which they belong.

3.2.2.2 Deciphering

In case the analyzed traffic is ciphered, for instance NAS in S1-MME interface, deciphering keys should be provided for being able to decipher the traffic.

3.2.2.3 Scaling

Distributing the monitoring tasks and the use of virtualized resources facilitates the scaling of the monitoring function.

3.3 MMT Solution

3.3.1 MMT Architecture

Figure 12 represents how MMT is deployed in an SDN environment. As depicted, MMT probes capture performance and security meta-data either: 1) from a virtual machine to perform introspection (VMI) or monitoring of mirrored virtual traffic; 2) an application running in a virtual machine to perform monitoring of deployed NFV's; or, 3) a performance/security appliance to perform monitoring of mirrored physical links.

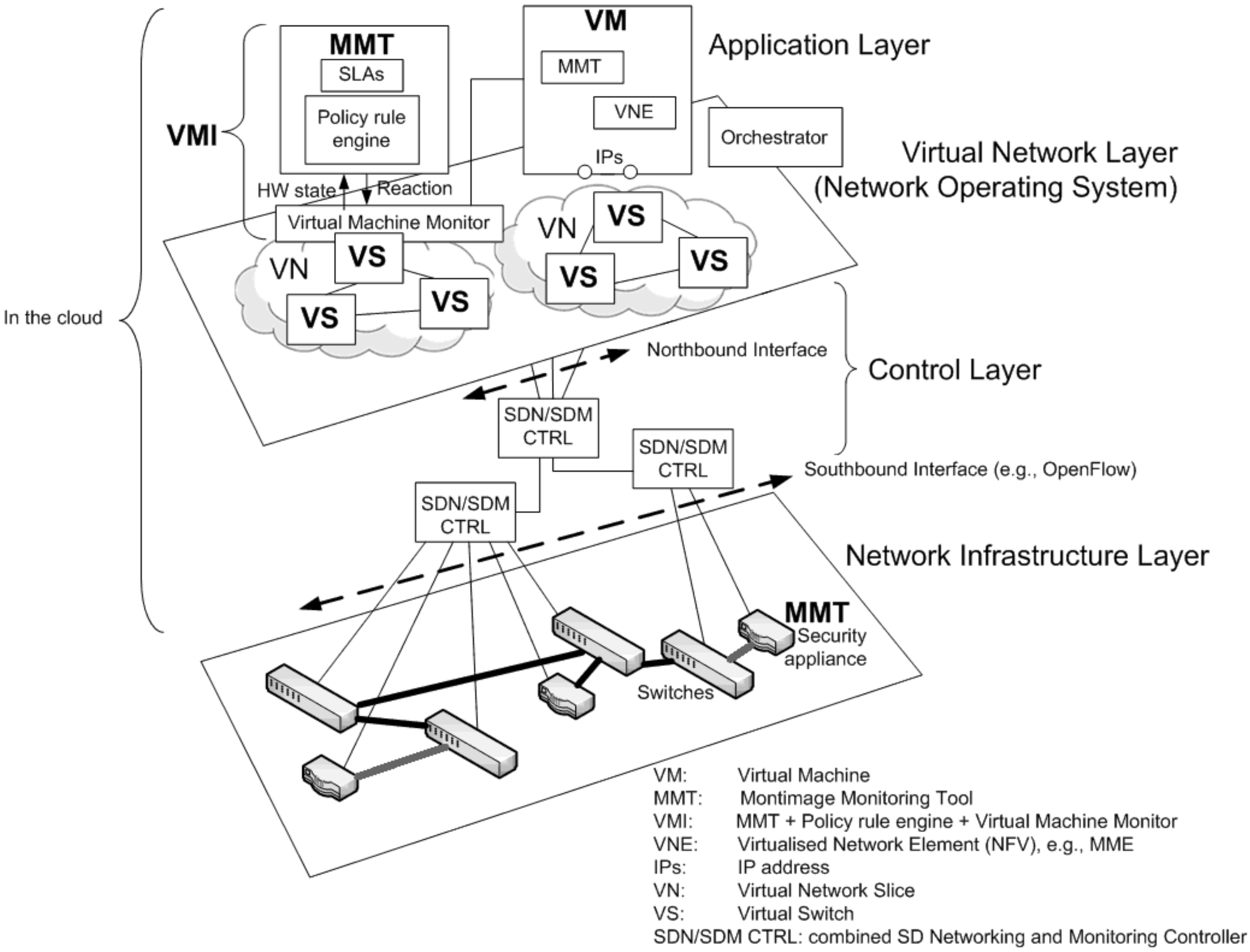

MMT
SLAs
Policy rule engine
VM
MMT
VNE
IPs
Application Layer
Orchestrator
VMI
HW state
Reaction
Virtual Machine Monitor
VN
VS
VS
VS
VN
VS
VS
VS
Virtual Network Layer
(Network Operating System)
In the cloud
Northbound Interface
Control Layer
SDN/SDM CTRL
SDN/SDM CTRL
SDN/SDM CTRL
Southbound Interface (e.g., OpenFlow)
Network Infrastructure Layer
MMT
Security appliance
Switches
VM: Virtual Machine
MMT: Montimage Monitoring Tool
VMI: MMT + Policy rule engine + Virtual Machine Monitor
VNE: Virtualised Network Element (NFV), e.g., MME
IPs: IP address
VN: Virtual Network Slice
VS: Virtual Switch
SDN/SDM CTRL: combined SD Networking and Monitoring Controller

Figure 12: MMT Network Monitoring Virtaulisation

Besides capturing meta-data, a centralized MMT application (MMT_Operator) needs to be deployed that will correlate events captured by the distributed probes and generate the specified reports, alarms and trigger any required remediation.

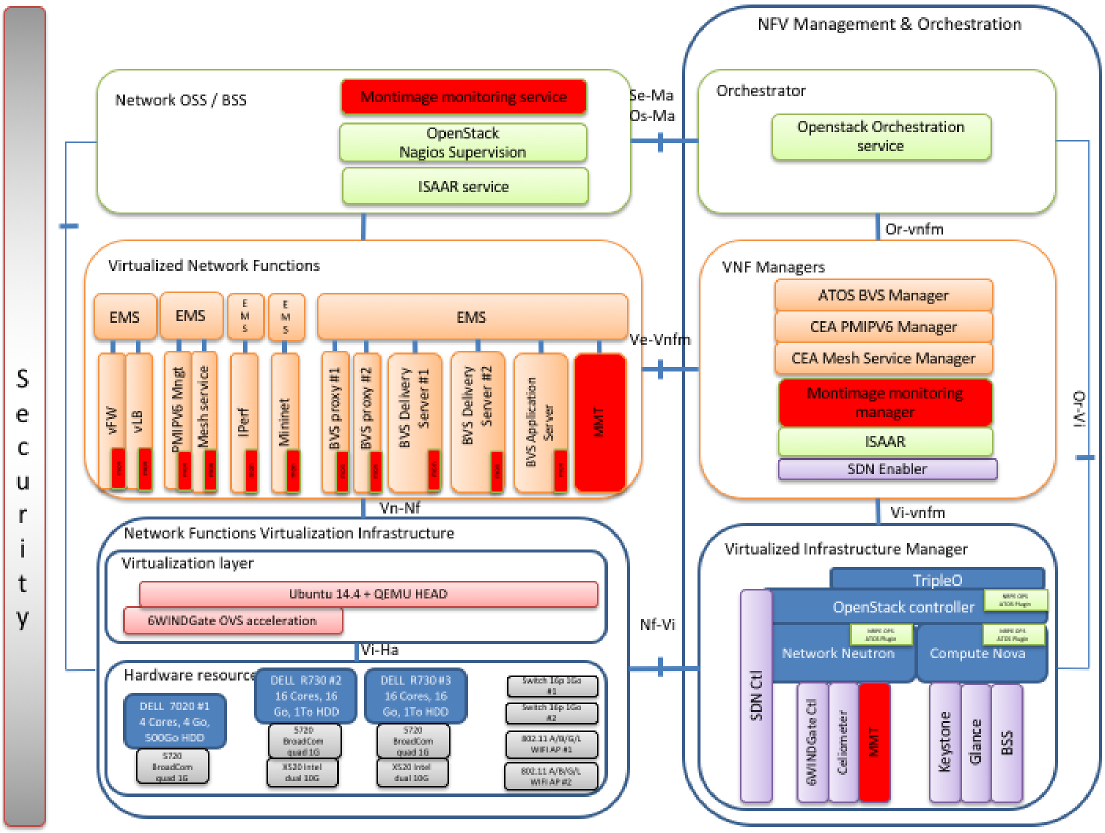


Figure 13: High level NFV management framework.

Figure 3 shows how SDM monitoring probes map to the NFV architecture proposed by European Telecommunications Standards Institute (ETSI) [NFV]. As an example, in this figure these modules are integrated into the OpenStack cloud computing software platform [Tokyo] and handle the deployment and management of the probes in the virtualized environment.

The key components of SDM Framework that are being developed and tested are:

- Monitoring Probes (embedded MMT): Probes are needed for obtaining performance, security or behavior related information. They can be passive (performing only analysis without disturbing the traffic) or active (in which case they will carry out prevention, mitigation or corrective actions). They can be deployed in the virtualized control plane (e.g., virtualized monitoring probes, MMT) or the physical data plane (i.e., hardware appliances), as a standalone network function or collocated with other network functions to address different needs. They can also complement the basic monitoring functions (e.g., OpenStacks Celiometer [Ceilometer]) of the virtualized infrastructure manager.
- Montimage Monitoring Manager: This component is part of the NFV Management and Orchestration for specifically deploying and dynamically configuring the probes in the virtual machines.
- Montimage Monitoring Service: This component is part of the OSS/BSS Business and Operations Support System that will perform the standard management of monitoring functions such as network inventory, service provisioning, network configuration and fault management. This component is a centralized application that acts as a decision point, correlates data from the distributed monitoring probes and provides a dashboard for their management (MMT-Operator).
- SDM Controller (stand alone MMT virtualised network function): This component is an extension of SDN controller or is separate but interacts with it. SDN controllers allow extracting some information from the routers using, for instance, the OpenFlow interface; but, OpenFlow is primarily designed for routing applications and deals with flows rather than individual packets. It is used for notifying events (e.g. changes in link state, the arrival of new flow, etc.), flow statistics and packet-in messages containing part of certain packets related to error conditions, mismatches or explicit requests [Foundation]. Making all packets available to the controller using packet-in messages would be inefficient. The SDN controller needs to be extended or complemented by

an SDM controller to enable better packet sampling, packet/flow metadata extraction and packet/flow redirection. Thus in order to address the requirements of security and traffic analysis applications, it will allow the controlling of monitoring functions (e.g., management of network monitoring appliances, traffic mirroring, traffic load balancing and aggregation) and accept requests from network functions and applications. These controllers can be distributed following either a peer-to-peer or hierarchical model. They interact with the management monitoring functions and act as distributed analysis or decision points for enforcing the defined service and security policies (SLAs). The SDM controller can be virtualised (stad alone MMT Network Function) and managed by the Montimage Monitoring Manager (NFV Manager). This is one option. Other options are also being studied to integrate ONF's OpenFlow-enabled SDN and ETSI's NFV architectures.

- SDM Control Interface (not shown in the Figure): This interface can be seen as an extension of the SDN control interface that allows better packet and flow analysis, controlling the use of monitoring resources, and recuperating traffic and metadata for analysis.

3.3.2 MMT Challenges and solutions

3.3.2.1 Capturing data

Data and meta-data can be captured by deploying MMT probes in the virtualised and physical planes.

3.3.2.2 Performance

3.3.2.2.1 Capture to memory performance

For analysis of large bandwidth traffic, caching is necessary (on disk or on RAM memory). Overall the system can be optimised to be able to handle this traffic since it is never continuous. For instance, traffic could be at its maximum only during part of the day and could be much lower at night time, making it possible to processed cached data without losing any information.

3.3.2.2.2 Analysis performance and resources

Standard multi-core routers (e.g., 32 cores) allow processing up to 10Gbps. Analysis involving complicated algorithms and many rules requires more complex HW architectures that incorporate filtering and load-balancing techniques. Software controlled FPGAs and load balancing techniques are being studied to optimize these tasks.

3.3.2.3 Scaling

Distributing the monitoring tasks and the use of virtualized resources facilitates the scaling of the monitoring function.

3.3.2.4 Deciphering

Part of the monitoring can be done using the unencrypted part of the headers and statistics that do not require deciphering. For deeper analysis, monitoring of encrypted traffic needs to be done at the end-points.

3.3.2.5 Licensing

Mixed open source /commercial licensing. The use of the software for non-commercial use is possible. Integrated SW/HW solutions for commercial or non-commercial use require licences.

3.3.2.6 Correlation of the results

MMT_Operator will allow the correlation of the results obtained from the deployed probes to produce reports that consolidate the data obtained from the distributed probes.

3.3.2.7 Load balancing

For the physical links, load balancing will be possible through the SDM/SDN-CTRL interfaces. Similarly, for the virtual links the Virtual Switches will allow separating and aggregating traffic to improve the effectiveness of the distributed monitoring function. In this way, the different probes can analyse parts of the traffic that has been split respecting the sessions (referred to as stick sessions).

3.3.2.8 Filtering

Several types of filtering can be used to improve the efficiency of the monitoring function: discarding unnecessary packets, recuperating only packet segments, etc. For instance many control packets are not useful for analysing performance or security, and completely analysing large payloads is not always required and can be truncated.

4. Conclusions

SDN and NFV make possible the sharing, aggregation and management of available resources, enables dynamical reconfiguration and changes of policy, and provides granular control of network and services through the abstraction of the underlying hardware.

The lack of visibility and controls on NFV internal virtual networks and the heterogeneity of devices make many performance assessment applications ineffective. On one hand, the impact of virtualization on these technologies needs to be assessed. For instance, network monitoring applications need to be able to monitor virtual connections. On the other hand, these technologies need to cope with ever-changing contexts and trade-offs between the monitoring costs and the benefits involved. Here, virtualization, as well as SDN, facilitate changes making it necessary for monitoring applications to keep up with this dynamicity.

With SDN it is possible to create network monitoring applications that collect information and make decisions based on a network-wide holistic view. This enables centralized event correlation on the network controller, and allows new ways of mitigating network performance and security incidents.

The idea of transferring network monitoring operations to software working in conjunction with configurable hardware (that can be referred to as SDM) will help address the limitations of the current monitoring systems that rarely have the ability to support the inevitably high monitoring demands of 5G mobile networks both in terms of traffic flow and highly dynamic network environments. The adoption of SDN/NFV offer a series of promising features that can well address the limitations of current monitoring solutions. However they also inherit some of the vulnerabilities of traditional software based solutions and cloud systems. Although SDM eliminates heavy dependence on physical resources, it also introduces new elements into the network such as the intelligent controller.

The limitations of current monitoring techniques have been identified and these include lack of interoperability, vendor specific network monitoring infrastructures, distributed and uncoordinated monitoring systems, high dependence on physical resources, rigid monitoring policies, distributed infrastructures, and un-automated mitigation actions. Various features of SDM set to address each of these limitations have been also identified. For instance, the logically centralized control feature of SDM simplifies network management and maintenance, eliminates the need for distributed infrastructures and vendor specific mechanisms, enables more coordination in monitoring and dynamically adjusts mechanisms to meet existing network demands. The programmability feature automates mitigation actions, reduces dependence on physical resources, and makes adaptation easy. Overall, the use of software to replace physical resources reduces the overall cost of monitoring.

On the side of its challenges, SDM is prone to scalability and performance problems given that it needs to fit multiple monitoring and network scenarios and still maintain specific service quality, hence the need for dynamicity. SDM also needs to be compatible with current monitoring systems so as to interoperate effectively. Other challenges include the need to adapt Deep Packet Inspection (DPI) to SDM, control the accuracy of the measurements, and adapt current monitoring techniques to handle virtualized contexts. It is therefore required that SDM addresses these limitations so as to be an effective monitoring solution for future telecommunication networks.

5. References

[3GPP GX] 3GPP TS 29.210: “Charging Rule Provisioning over Gx Interface”.

[3GPP SD] 3GPP TS 29.212. “Policy and Charging Control (PCC); Reference points”.

[ANetMM] Knoll T.M., Eckert M.: An advanced network based method for Video QoE estimation based on throughput measurement; EuroView 2012; http://www.euroview2012.org/fileadmin/content/euroview2012/abstracts/05_04_abstract_eckert.pdf

[Anoop] M. Anoop, K. B. Rao, and S. Gopalakrishnan, “Conversion of probabilistic information into fuzzy sets for engineering decision analysis,” Computers &amp; Structures, vol. 84, pp. 141–155, 2006.

[Ceilometer] Wiki, “OpenStack Telemetry (Ceilometer) .” OpenStack, Date accessed, Nov. 2, 2015.

[Dong] Y. Dong, X. Yan, X. Li, J. Li, K. Tian, H. Guan High Performance Network Virtualization with SR-IOV

[Intel] “Intel® Open Network Platform Server Reference Architecture (Version 1.1)” [Online]. Available https://01.org/sites/default/files/page/intel_onp_server_release_1.1_solutions_guide_v1.1.pdf

[ISAAR] Knoll T. M., Eckert M.: ISAAR (Internet Service Quality Assessment and Automatic Reaction) a QoE Monitoring and Enforcement Framework for Internet Services in Mobile Networks; 4th International Conference, MONAMI 2012;

[Foundation] O. N. Foundation, “Openflow switch specification, version 0.9. 0 (wire protocol 0x98),” Jul, vol. 20, pp. 1–36, 2009.

[Matlab] MATLAB, “Fuzzy logic toolbox.” [Online].

Available: http://www.mathworks.fr/products/fuzzy-logic

[MevD51] Wehbi B., Sankala J.: Mevico D5.1 „Network Monitoring in EPC”, Mevico Project (2009-2012)

[NetMM] Rugel S., Knoll T. M., Eckert M., Bauschert T.: A Network-based Method for Measurement of Internet Video Streaming Quality; European Teletraffic Seminar Poznan University of Technology, Poland 2011; http://ets2011.et.put.poznan.pl/index.php?id=home

[NFV] ETSI GS NFV 002 (V1.1.1) (10-2013): "Network Functions Virtualisation (NFV); Architectural Framework".

[NV report] Network virtualization report, 2014 Edition [Online]. Available: https://www.sdxcentral.com

[Openstack] Blueprint “neutron-services-insertion-chaining-steering” [Online]. Available: http://stackalytics.com/report/blueprint/neutron/neutron-services-insertion-chaining-steering

[Ouellette] Ouellette, S., Marchand, L., Pierre, S.: A Potential Evolution of the Policy and Charging Control/QoS Architecture for the 3GPP IETF-Based Evolved Packet Core. In: IEEE Communications Magazine May 2011 pp. 231-239. IEEE Communications Society, New York (2011)

[Pokhrel] J. Pokhrel, B. Wehbi, A. Morais, A. Cavalli, and E. Allilaire, “Estimation of QoE of video traffic using a fuzzy expert system,” in10th annual IEEE Consumer Communications & Network-ing Conference (CCNC’13), Las Vegas, Nevada,2013.

[Sandv] Sandvine Incorporated ULC: Solutions Overview. (2012);

[Tokyo] O. S. Tokyo, “Open Source Software for Creating Private and Public Clouds .” OpenStack, 2015.

[VMW] VMWare knowledgebase article. Monitoring network traffic from within a virtual machine on a VMware vSphere ESX/ESXi server [Online]. Available: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1038847

[YoMo] Wamser F., Pries R., Staehle D., Staehle B., Hirth M.: YoMo: A YouTube Application Comfort Monitoring Tool; March 2010

[YoMoISP] Schatz R., Hossfeld T., Casas P.: Passive YouTube QoE Monitoring for ISPs. 2nd International Workshop on Future Internet and Next Generation Networks (Palermo, Italy): June 2012