

Advanced NFV Features Applied to Multimedia Real-Time Communications Use Case

Ana Pol*, Anton Roman*, Panagiotis Trakadas†, Panagiotis Karkazis†, Evgenia Kapassa‡, Marios Touloupou‡, Dimosthenis Kyriazis‡,
Juan L. de la Cruz§, Pol Alemany§, Ricard Vilalta§, Raul Munoz§
*Quobis, O Porrino, Spain, Email: [ana.pol,anton.roman]@quobis.com
†Synelixis Solutions S.A. 157, Perissou, str., 14343, Athens, Greece, Email: [ptrak,pkarkazis]@synelixis.com
‡Department of Digital Systems, University of Piraeus, Piraeus, Greece, Email: [ekapassa, mtouloup,dimos]@unipi.gr
§CTTC, Castelldefels, Spain, Email:[jdelacruz,palemany,rvilalta,rmunoz]@cttc.es

Abstract— Real-time communications are services with very demanding requirements in terms of reliability and Quality of Service (QoS) that is not easy to be reached. 5G technologies provide tools and techniques that promise to overcome the current shortcomings and thus give the opportunity to service providers to offer better services to the end users. This paper aims at describing how an existing real-time communications service can leverage the innovative features offered by the SONATA Service Platform (SP), such as network slicing, automated monitoring management and Service Level Agreement (SLA) enforcement, to meet the challenging requirements of the service. In this paper, we especially focus on the specific mechanisms implemented to support different QoS profiles at network level and automatic scale in/out of the service depending on the system load.

Keywords— Real-time communications, 5G technologies, QoS Enforcement, SLAs, Monitoring, Slicing

I. INTRODUCTION

While the 5G concept is still rather unclear in certain dimensions [1], the evolved 5G network will be, for sure, characterized by agile, resilient and converged network realization, based on one hand on the disruptive core and radio access technologies and on the other hand on the network softwarization context brought by Network Function Virtualization (NFV) and Software Defined Networking (SDN) technologies. In the network softwarization frontier, a handful of commercial as well as open source Management and Orchestration (MANO) platforms have emerged (e.g. OSM [2], ONAP [3], Cloudify [4], SONATA [5], OPNFV [6]), considered as suites of functionalities for the management and orchestration of virtual resources related to the instantiation of Network Services (NS) consisting of Virtual Network Functions (VNFs) and their real-time provisioning.

These MANO platforms are expected to add value to operators by reducing costs and deployment time and simplifying the management of the VNF and NS throughout their lifecycle. By capitalizing on the implemented techniques of the 5G innovative concepts, these platforms are able to accommodate different types of services and deal with the complexity of the NS-specific requirements. SONATA platform is an open source MANO framework whose functionalities are currently extended under the scope of the 5GTANGO H2020 project [7], offering unique advantages and innovative features demanded by real use cases. In particular, those features include a) an automated network monitoring framework, b) novel policy and SLA management and c) implementation of network slicing. This paper describes and evaluates the implementation of a real-time

application service on top of the SONATA (powered by 5GTANGO) service platform.

The remaining of the paper is organized as follows. Section II presents the state of the art of this work, while Section III introduces the overall SONATA (powered by 5GTANGO) Service Platform. Section IV describe in detail then enhanced proposed features, specially focusing on the recently new-added features such as QoS and multi-WIM support. This section describes also the principles of SONATA (powered by 5GTANGO) Monitoring Manager as well as the insights of the realization of the SNMP solution that has been utilized in this pilot. Additionally, this section presents the role of the SLA Manager and how it enables the definition and enforcement of SLAs, as well as the Slice Manager which helps to meet the QoS requirements of the network service. Section V presents the corresponding real-time communications use case, while Section VI states the evaluation of the proposed architecture. Finally, in Section VII, we close up with ideas for future experiments and current study capabilities.

II. STATE OF THE ART

Active and advanced work has been conducted on multimedia real-time communications use cases implied in 5G-enabled network softwarization technologies. In this direction, there are several approaches and architectures enabling effective communication between IP Multimedia Subsystems (IMS) and Web Real-Time Communication (WebRTC) users. The authors in [8], introduced a novel architecture supporting WebRTC users for smart community services, and proposed an optimization model to design and allocate resources for such systems while ensuring the desired QoS level. Furthermore, worth mentioned is the work conducted in [9], where the authors presented an open-source platform enabling developers to create and deploy RTC applications with advanced media processing capabilities. For this, they introduced the concept of Media Pipeline which is in fact chains of interconnected media processing elements. Their approach was also based on ETSI NFV recommendations. Henceforth, another interesting work was introduced in [10]. In this paper, a set of three software architectures were introduced for efficient virtualization of IMS in different operator environments responding to the high-level requirements of the ETSI NFV use case for virtualizing operator core network functions. In addition, based on their experiments, they have successfully managed to simplify the deployment and runtime orchestration of such a virtual service on top of a cloud infrastructure. Not only that, but also in [11], an analysis of next generation network architectures enabling real time multimedia communications was conducted.

The novelty and contribution of this paper lies in the fact that: a) the described functionalities are already implemented and given to the research and industrial community as open source code, and b) the evaluation is based on a real service provided by Quobis offering a first-class opportunity to validate the benefits of the implemented 5G network softwarization characteristics.

III. SONATA SERVICE PLATFORM OVERVIEW

Before proceeding with the description of the service and the results of our work, we will briefly describe the main components of the SONATA (powered by 5GTANGO) platform. In brief, its open source software is comprised by three main components: the Software Development Kit (SDK) [12], the Verification and Validation (V&V) Framework [13] and the Service Platform (SP) [14]. The entry point of the SONATA platform is the SDK, which is a CLI based toolkit that allows NS packages creation, on-boarding, towards the V&V component that is responsible for the verification and benchmarking of NS's and their constituent VNFs. Afterwards, the SP takes the control of the NFV Management and Orchestration (MANO) features. Figure 1 depicts the overall SONATA (powered by 5GTANGO) service platform architecture, indicating the interactions between the SP and the rest of the components. The main focus of this paper will be in the description of the internal components of the SP, giving emphasis to advanced features that provide support to a real-time communication NS, running on top of a virtualized infrastructure.

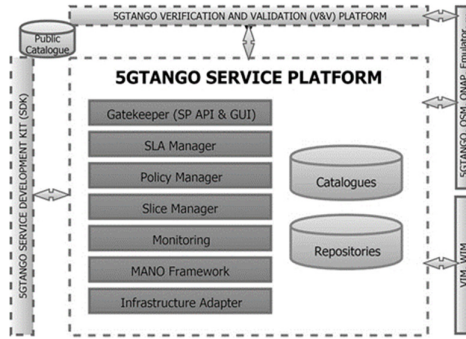


Fig. 1: SONATA (powered by 5GTANGO) architecture.

In accordance with ETSI NFV [15], the SP follows a Catalogue-driven approach, meaning that the deployment of VNFs and NS's follow the descriptors, as well as other information stored in the Catalogue (on-boarding process). As the name implies, the descriptors describe the resources to be used, the configurations to be done, and the monitoring metrics that will be automatically collected via SNMP, based on which, SLAs will be evaluated. The Gatekeeper is the entry point of the SP, controlling who attempts to access the inner components of the SP and checks the privileges to do so. The Gatekeeper exposes API endpoints for QoS management, as well as validates and forwards requests to the rest of the components (e.g. SLA Manager, Slice Manager etc). The Gatekeeper also serves an important and active role in implementing the MANO Framework communication interfaces. When there is a service instantiation request, the Gatekeeper forwards to the MANO Framework all the necessary data (i.e. NS descriptor, SLA descriptor, Slice Descriptor) for the required resource allocation at the Virtual Infrastructure Management (VIM) and WAN Infrastructure Management (WIM) levels. The SLA Manager is a newly introduced component which considers real operator scenarios, where the service providers need to ensure a certain QoS by establishing SLAs with their customers, as will be

described in sub-section F of section IV. Additionally, the SP follows a policy-driven approach through the Policy Manager, meaning that the full operations can be controlled by a set of policies that determine the behavior of the NSs. Policies materialize the zero-touch service management (ZSM) concept, enabling the automation of the decision-making process. Another new component is the Slice Manager, which is described in more detail in sub-section G of section IV, allowing the creation of multiple slices on top of a single infrastructure. For that, it uses NFV artifacts as building blocks (i.e. NSs), interconnecting them in order to build end-to-end slices, capable to cope with the 3GPP requirements. Moreover, in order to monitor not only the infrastructure resources, but the performance of a service either on VNF or NS level, the SP includes a Monitoring Manager, with new features, enabling the proper management of the use case specific requirements, as will be described in sub-section C of section V. At a lower level, the SP takes advantage of the MANO Framework, implementing the functions of Network Service Orchestration (NSO), Resource Orchestration (RO) and VNF Management. Mapping to the ETSI NFV Architecture, this roughly corresponds to the NFV Orchestrator (NFVO) and VNF Manager (VNFM) components. In terms of infrastructure, the SP is ready to support multiple NFV Infrastructures (NFVIs) and VIMs, using an Infrastructure Adaptor (IA) component to abstract the particularities of each infrastructure. Currently, two technologies are supported, Openstack and Kubernetes, but others can be added by extending the platform with new plugins.

IV. PROPOSED FEATURES

This section describes the proposed features that was introduced into the SONATA (powered by 5GTANGO) SP architecture, that allow the enhanced management and orchestration of a real-time communication service. The next subsections are going to describe advanced features like a) End-Point Support, b) Multi-WIM and QoS Support, c) the WIM TAPI extension, d) the SSM and FSM implementation, as well as enhanced components such as a) Monitoring Manager, b) SLA Manager and c) Slice Manager.

A. End-point support

According to ETSI NFV MANO, an NS is composed by a set of interconnected VNFs, which can be spread among multiple VIMs/PoPs. Usually, the NS borders are confined to the datacenter, and the connection points to the outside coincide with the connection points to the first and last VNFs, respectively. The confinement of a NS to the datacenter makes difficult to assure the end-to-end QoS as the WAN segment between the client and the service is not controlled by the service provider. In order to enable a full end-to-end control, this model needs to be extended to allow the Virtual Links (VL) to map with the access network until the client, enabling the QoS provisioning in that segment. The SP supports the deployment of NS's where the endpoints are not confined to a datacenter but are extended towards any datacenter-external network endpoint. To create this WAN leg, the SP invokes a WIM that enforces the creation of a tunnel with certain QoS parameters. In the use case that is going to be described in this paper, it looks as depicted in the Figure 2.

B. Multi-WIM and QoS support

The SP can be simultaneously attached to multiple WIMs which can be of different types. The IA component provides a common and abstracted northbound interface (NBI) view of

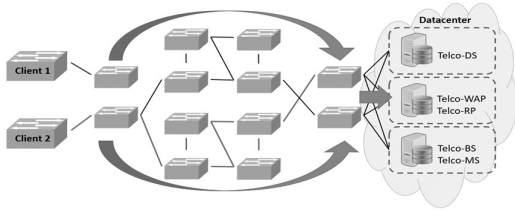


Fig. 2: WAN paths created to meet QoS requirements

the infrastructure, no matter the underlying technology that is actually in use. Currently, the SP supports two WIM plug-ins: Transport API (TAPI), defined by the Open Networking Foundation (ONF) and VTN (Virtual Tenant Networking), an OpenDayLight (ODL) application. Moreover, the SP has been enhanced to support QoS mechanisms. In order to implement QoS in an end-to-end manner, the SP is able to enforce QoS both within datacenter Point of Presence (PoP) as well as in WAN segments. Within PoPs, it is the VIM responsibility to enforce QoS among virtual networks and workload, while in WAN segments it is the duty of the WIM to apply such QoS. The support of QoS enforcement within the datacenter is implemented thanks to the QoS configuration options exposed the Openstack VIMs. Openstack supports two QoS mechanisms: bandwidth limit and minimum bandwidth. The former drops packets above a certain limit, while the latter ensures that a certain amount of traffic is guaranteed (the most useful one). The enforcement of both is done at the connection point (CP) level, although it can also be applied at the VL level (applied to all connection points of the VL). The minimum bandwidth is only supported using the Single-Root Input/Output Virtualization (SR-IOV) technology. It is worth mentioning that the SP supports QoS enforcement on TAPI based WIMs. The actual enforcement of certain QoS on such networks can be done by using either SDN or traditional mechanisms associated to operators' Network Management Systems (NMS). In particular, TAPI can be used to guarantee a certain level of bandwidth in a given predefined path among a transport network.

C. WIM Tapi extension

In order to setup networking connectivity between VNFs and WAN terminations as shown in Figure 2, each link has to be created in the physical infrastructure. In the use case that is going to be described later on this paper, two different PoP sites were used, that are connected through a fabric of SDN-controlled virtual switches combined with several optical switches, using a hierarchal SDN control plane. To enable connectivity, a WIM plugin has been developed using the TAPI specification [16]. When a NS deployment is initialized by the user, IA communicates to each WIM which endpoints are to be connected and this information is mapped using WIM database to Service Interface Points (SIP) that describes each connector in TAPI. Finally, it creates - abstracting lower level controllers - MPLS unidirectional flows through the previously mentioned fabric. Depending on the requested QoS, WIM can establish different routes through packet or optical domains, based on bandwidth or latency requested. Having a granularity of two unidirectional flows per WAN termination- VNF connection it is possible to perform load-balancing or priority routing, for providing the desired service.

D. SSM and FSM implementation

In order to support the new features, it was necessary to develop a Service Specific Manager (SSM) plugin for the

initial setup of the NS and a Function Specific Manager (FSM) plugin for the VNFs. The VNFs need an FSM to modify the configuration of their internal services. Each VNF counts with one or more services running in the inside that need the URL information of other VNF to enable the internal communication between VNFs within the NS deployed. Nevertheless, the information relative to other VNFs (e.g. IPs, hostnames and ports) is not accessible at FSM level. The solution to this problem was to implement an SSM which operates at service level to extend the information received by each FSM. Therefore, each FSM will receive all the information it requires for the configuration of the NS through the SSM.

E. Monitoring Manager

The SONATA Monitoring Manager [17] that has been extended in 5GTANGO project is responsible for collecting and processing data from several sources, providing the ability to activate metrics and thresholds to capture generic or service-specific behavior. Moreover, the Monitoring Manager provides interfaces in order to define rules based on metrics gathered from one or more VNFs deployed in one or more NFVIs and creates notifications in real time. Monitoring data and alerts are also accessible through a RESTful API. Although several possibilities to send monitoring data to the Monitoring Manager were available, during the 2nd ETSI NFV Plug-Tests, it became obvious that the Monitoring Manager should be also able to provide a way to collect monitoring data without the need for installing probes within the VNF. This would provide the advantages that there is no need for "injecting" software in the VNFs. Addressing the abovementioned requirement from the industry, in the latest release, Monitoring Manager provides the ability to collect data from VNFs using SNMP protocol. This functionality increases the flexibility of the Monitoring Manager taking into account that many VNF developers use SNMP, as a standard and widely accepted approach, to provide metrics that are related with the performance of their services. Currently, implementation supports public access via SNMPv2 and also secured access via SNMPv3. In order to enable the SNMP functionality, the developer must provide the necessary information (metrics, SNMP OIDs, time interval, etc.) inside the VNF descriptor.

F. SLA Manager

With many real-time communication companies already striving for a high level of service, the need for rock solid SLAs becomes a challenge. Therefore, one of the requirements in the described use case pilot is, among others, the usage of the SLA management feature within the 5GTANGO SP. Effective SLAs not only go a long way in retaining customers, but also, they can create clear and defined communication boundaries. The benefits of supporting SLAs exist for both real-time communication service providers and customers, as they guarantee that NSs and their correlating VNFs can be effectively controlled. The capabilities of these technologies can be optimized by properly instantiating Network Slices with the corresponding SLA. The overall SLA management workflow, of three phases: a) definition and advertising of the capabilities of network operators in SLA Template forms, b) creating the Agreements upon a slice instantiation and c) SLA violation records management [18]

- 1) *SLA Template Creation*: The first phase of the SLA management is the SLA Template Creation, where four (4) parameters are mandatory for the successful generation. The most important thing is the selection of

the real-time communication service in the presented use case, which will be correlated with a new SLA template. At the same time, a SLA name is required (i.e. Gold, Silver) with a valid expiration date. Additionally, at least one SLO should be included in the template, as described in the system requirements of the service.

- 2) *Agreement Creation*: As long as the communication service is successfully instantiated within a Network Slice, the Agreement is automatically created, during the second phase. Specifically, once the deployment of the service is completed, the corresponding SLA template is promoted to an actual agreement that is being enforced (i.e. instance of the SLA template). Once the agreement is established the guaranteed requirements of the service (i.e. packet loss, throughput, RTT, URR) start being monitored and checked for breaches of contract.
- 3) *SLA Violations*: In the last phase, the SLA violations management takes place upon the real-time communication service deployment. The SLA Manager is able to identify any violations occurred and to take the necessary actions. Specifically, upon receipt of the measured metrics through the Monitoring Framework and in case of a violation is not prevented in time, an alert is sent towards the SLA Manager. Upon receipt, the latter calculates the overall value of that specific metric and makes the decision whether the SLA for the corresponding service into the slice instance is violated or not.

The established SLAs can create a formalized communication process that both the service provider and the customers agree upon, so both parties can be as efficient and successful as possible. The customer gets guaranteed service quality and the service provider works within precisely defined responsibilities and tasks. Working according to SLA guarantees, providers have predictable resource spending, uninterrupted end-user experience and boost of their brand loyalty.

G. Slice Manager

One of the requirements in the use case pilot is the use of the Network Slice management feature within the SP [19]. The main goal of using slices in this pilot is to provide flexibility when deploying different QoS over the same physical network. The idea is to create two equal network slices as presented in Figure 3. Both network slices will have exactly the same services but each one with a different QoS. By doing this, the owner of the physical resources will be able to create multiple network slices and manage them by fulfilling each one individually with QoS requirements. To define these QoS requirements at a slice level, it is used the 5QI parameter (defined by the 3GPP) which references to a set of 5G QoS characteristics [20]. To fulfil the QoS at a slice level, the idea is to use each individual SLA associated to each network service within the network slice. This means that all individual SLAs must work together to reach the expected Slice QoS. As previously described, there will be two Slice QoS (Gold and Silver), meaning two different Network Slice Templates Descriptors (NSTD). In each NSTD there is the list of network services. Both have the same service but each one mapped with a different SLA fulfilling the selected 5QI.

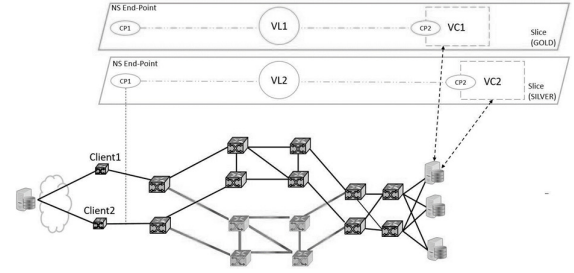


Fig. 3: Network Slice use case architecture

V. REAL-TIME COMMUNICATIONS USE CASE

A. Service definition

The real-time communications service offered by Quobis and described in this paper is based on WebRTC [21]. The main feature of the system is the establishment of audio and video sessions between several participants, but it also supports other collaboration services such as group-chat, screen-sharing and whiteboard. The state of the different elements of the service is stored in a No-SQL database and the internal communication between processes is handled by a messaging broker. The media is received using WebRTC from web clients running in WebRTC-capable browsers. The fact of being an existing system gives special value to this use case since it shows how a legacy service can be migrated to an NFV SP by separating its functionalities in Virtual Network Functions (VNFs). In order to deploy the service on SONATA SP, the functionality of the original service is divided into functional entities which are encapsulated in VNFs and then connected to configure the complete network service (NS). The system is divided in the following VNFs for both functional and architectural reasons.

- *Reverse Proxy (VNF-RP)*: This VNF provides standard reverse proxy functionality. It receives all the HTTPS and WebSocket Secure (WSS) traffic coming from the internet and deliver it to the right service. The corresponding VNF is expected to be needed by almost any Web-based service.
- *WebRTC Application Controller (VNF-WAC)*: The WebRTC Application Controller (WAC) provides the back-end functionality of the service. This VNF handles authentication, user provisioning, log collection and other minor features required to build mobile and web applications.
- *Media Service (VNF-MS)*: The MS runs a SFU (Selective Forwarding Unit) which relays the DTLS-SRTP [22] media flows from each participants in the video conference. This VNF is the most QoS-sensitive and also the most demanding one in terms of server resources, and especially bandwidth.
- *Dispatcher (VNF-Dispatcher)*: The Dispatcher acts as a registry service (using cloud terminology) for the MS instances. When a new MS is instantiated, it contacts the Dispatcher so that the service knows the number of instances which are available at any moment.
- *Backend Service (BS)*: Both the WAC and the Dispatcher VNFs need to persist data in a database and then exchange messages using the message broker. This VNF implements both the aforementioned services.

B. Use Case Scenarios

In this paper, four different scenarios have been defined, covering different complexity cases the system should be able to cover once the service is deployed in the platform:

- *Best-effort video-conference*: The network service provides best-effort real-time communication capabilities to the users in order to enable video-conferences, IM and additional real-time collaboration tools.
- *Premium video-conference (Gold and Silver QoS)*: The network service is sensitive to some of the QoS measures such as bandwidth, packet loss and jitter. We should take under consideration that there are two kinds of users with different QoS requirements using our application.
- *Edge video-conference*: The video-conference service is improved considering the delay sensitive VNFs such as the media server (VNF-MS). This improvement is achieved by moving the VNF-MS to the edge of the network in order to reduce the latency and the potential high jitter.
- *Video-conference scaling out/in*: The NS should be able to scale in and out the number of VNF-MS and VNF-WAC instances in order to adapt the capacity of the service regarding the number of the registered users but also the simultaneous calls to the service.

C. QoS requirements

In order to meet the specific QoS demands of this pilot it was necessary to cover some specific requirement. Most of them are related to the QoS-sensitive nature of the service (real-time multimedia communication) but there are also requirements related to its capacity and reliability. The different use case scenarios defined above introduced the need of different QoS guarantees. For the pilot purposes, the expected QoS of each use case was classified in two levels: “Gold” and “Silver”. These QoS levels would match with different classes of SLAs that an operator could compromise with their subscribers under contractual conditions. For each SLA level, a set of specific Service Level Objectives (SLOs) are considered. Each SLO is defined by the maximum values and thresholds allowed for a set of network and service-specific parameters: packet loss, throughput, jitter and number of users registered per second. The main requirement regarding the service is to be able to provide QoS and use stats to the NFV platform in near real-time. In this specific pilot this was achieved by using a set of SNMP variables updated by different VNFs as described in section IV-B. Table I gathers the SLOs for two levels (i.e. Gold and Silver) of QoS defined for the pilot. The threshold values are chosen for the pilot convenience, but it may not reflect the real values which would be adopted for a production environment.

TABLE I. DEFINED SLA LEVELS

QoS Level	Packet Loss	Jitter	Throughput	Registration Rate
Gold	< 1%	10 ms	120 Mbps	15 Rps
Silver	< 2%	20 ms	90 Mbps	10 Rps

VI. EVALUATION RESULTS

In order to evaluate the performance of the proposed real-time communication NS in terms of efficiency and ease of use, the proposed architecture was included in the innovative 5GTANGO Service Platform. The evaluation of the

developments described in this work was carried out by deploying the services in the Centre Tecnològic de Telecomunicacions de Catalunya (CTTC) lab Network. The NS was deployed using Gold flavor. It should be mentioned that load test of 100 video-conferences was launched in order to check if the networking QoS levels were met. In Figure 4 is presented the jitter level of the outgoing audio channel measured in milliseconds at the user endpoint. The value has a peak of 4ms which is below the limit for the defined Gold QoS level. Moreover, in Figure 5 and 6 respectively, are depicted the cumulative values of packet-loss for sent and received video flows of a video-conference during the load test. The plots indicate a 300 second range with a target packet rate of 60 packets per second so the packets-loss rates are 0.02% and 0.04% for sent and received respectively. Both values meet the Gold QoS level.

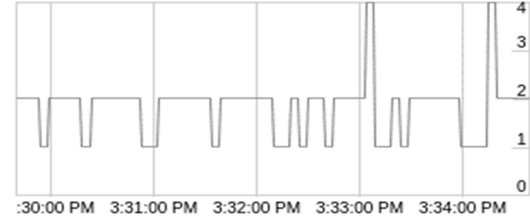


Fig. 4: Jitter experienced in audio channel for a Gold service

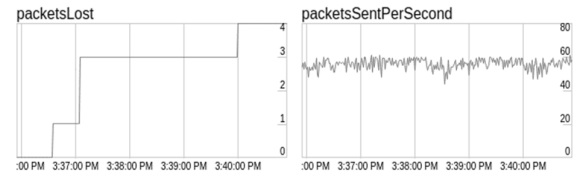


Fig 5. Cumulative value of sent packet lost and rate of packets sent per second.

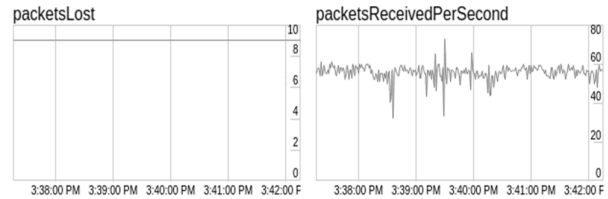


Fig 6. Cumulative value of received packet lost and rate of received packets per second.

Based on the captured results, concerning the QoS results of the running communication service, we resulted that through the presented architecture, the NS is feasible to meet the guaranteed SLA levels, cooperating smoothly with the monitoring and slicing mechanism of the SP.

CONCLUSIONS

Concluding, in this paper, we have introduced a novel architecture of a real-time communication network service, integrated in a real 5G Platform - the NFV enabled SONATA (powered by 5GTANGO) service platform. The presented work gathers all the new features which were necessary to be introduced. The innovative combination of Network Slices and SLAs enable the application of different QoS not only within the datacenter but also in network segments controlled by the service operator using the WIM TAPI extension. The new features of the SP it is feasible to deploy successfully

demanding network services, where reliable QoS is a strong requirement. Additionally, the proposed architecture was evaluated, and the results of our experiments indicate several insights in regards of the service's behavior. Specifically, based on the monitored performance of the service, we have concluded that the signed SLAs can be met, proving that the promised quality of service by the service provider is feasible.

Finally, it should be mentioned that apart from real-time human communication, there are many existing and future services which can take advantage of these features such as automotive applications, videogaming, e-health and industrial control. Thus, our future work includes the evaluation of the architecture with additional heterogeneous services and applications.

ACKNOWLEDGMENT

This work has been partially supported by the 5GTANGO project, funded by the European Commission under Grant number H2020ICT-2016-2 761493 through the Horizon 2020 and 5G-PPP programs (<http://5gtango.eu>).

REFERENCES

- [1] R. Nelson, "Ecosystem gears up as world awaits 5G rollout." *EE-Evaluation Engineering*, vol. 57, no. 6, pp. 6-10, 2018.
- [2] "Open Source Mano – OSM", Available at: <https://osm.etsi.org/>
- [3] "Open Network Automation Platform – ONAP", Available at: <https://www.onap.org>
- [4] "Cloudify - Cutting Edge Orchestration", Available at: <https://cloudify.co/>
- [5] "SONATA NFV: Agile Service Development and Orchestration in 5G Virtualized Networks", Available at: <http://sonata-nfv.eu/>
- [6] "Open Platform for NFV - OPNFV", Available at: <https://www.opnfv.org/>
- [7] D. T. Nguyen, Nguyen, K. K., Khazri, M. Cheriet, "Real-time optimized nfv architecture for internetworking web rtc and ims", 17th International Telecommunications Network Strategy and Planning Symposium (Networks), pp. 81-88, 2016.
- [8] B. García, M. Gallego, L. López, G.A. Carella, A. Cheambe, "NUBOMEDIA: An Elastic PaaS Enabling the Convergence of Real-Time and Big Data Multimedia", *IEEE International Conference on Smart Cloud (SmartCloud)*, pp. 45-56, 2016.
- [9] G. Carella, et al., "Cloudified IP multimedia subsystem (IMS) for network function virtualization (NFV)-based architectures", *Symposium on Computers and Communications (ISCC)*, pp. 1-6, 2014.
- [10] "5G Development and Validation Platform for Global Industry-Specific Network Services and Apps", Available at: <https://www.5gtango.eu/>
- [11] M. Scarlato, C. Perra, "Next generation architecture for real time multimedia applications", *AEIT International Annual Conference*, pp. 1-6, 2017.
- [12] M. Peuster, H. Karl, "Understand Your Chains and Keep Your Deadlines: Introducing Time-constrained Profiling for NFV", 4th International Conference on Network and Service Management, pp. 240-246, 2018
- [13] P. Twamley et al., "5GTANGO: An Approach for Testing NFV Deployments", *European Conference on Networks and Communications*, pp. 1-218, 2018.
- [14] C. Parada et al., "5GTANGO: A Beyond-Mano Service Platform", *European Conference on Networks and Communications*, pp. 26-30, 2018.
- [15] "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification", *ETSI Group Specification*, 2019.
- [16] V. Lopez et al., "Transport API: A Solution for SDN in Carriers Networks", 42nd European Conference on Optical Communication, pp. 1-3, 2016.
- [17] P. Trakadas et al., "Scalable Monitoring for Multiple Virtualized Infrastructures for 5G Services", *Proceedings of the Seventeenth International Conference on Networks, (ICN)*, 2018.
- [18] "System Architecture for the 5G System (3GPP TS 23.501 version 15.2.0 Release 15)", Available at: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.02.00_60/ts_123501v150200p.pdf
- [19] E. Kapassa, M. Touloupou, P. Stavrianos, G. Xylouris, D. Kyriazis "Managing and Optimizing Quality of Service in 5G Environments Across the Complete SLA Lifecycle", *Advances in Science, Technology and Engineering Systems Journal*, vol. 4, no. 1, pp. 329342, 2019.
- [20] "WebRTC 1.0: Real-time Communication Between Browsers", Available at: <http://www.w3.org/TR/2012/WD-webrtc-20120821>
- [21] R. Vilalta, P. Alemany, et al., "Zero-Touch Network Slicing Through Multi-Domain Transport Networks", 20th International Conference on Transparent Optical Networks, 2018.
- [22] D. McGrew, E. Rescorla, "RFC 5764: Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", *RFC Editor*, 2010.