On Experimenting 5G: Testbed Set-up for SDN Orchestration across Network Cloud and IoT domains

S. Fichera, M. Gharbaoui, P. Castoldi
Scuola Superiore Sant'Anna, Pisa, Italy
{s.fichera, m.gharbaoui, castoldi}
@santannapisa.it

B. Martini
CNIT, Pisa, Italy
barbara.martini@cnit.it

A. Manzalini
TIM, Torino, Italy
antonio.manzalini@telecomitalia.it

Abstract— **In this paper, we present an experimental set-up reproducing a convergent 5G service scenario spanning over SDN-based Edge network, Cloud and IoT domains. To address reliability and robustness requirements of future 5G networks, the set-up also includes an SDN orchestrator able to adaptively provision data delivery paths connecting service components running in those different domains. In particular, we demonstrate SDN orchestration capabilities in adapting data paths across IoT, Cloud and network domains based on the real-time load state of switches thereby recovering from congestions and assuring reliable data delivery services.**

Keywords—5G, Cloud/Fog Computing; Internet of Things; SDN; NFV; Orchestration; Service Chains, Edge Networks

I. Introduction

Over the last decades, legacy telecommunication infrastructures evolved into multi-layered heterogeneous platforms, with each layer managed by technology-specific OSSs/BSSs. Today, the business sustainability of such infrastructures calls for their evolution towards more flexible and programmable networks and service platforms capable of facing highly dynamic and changing service scenarios resulting from the application of the digital technology in all aspects of human society and business process, i.e., Digital Business Transformation [1]. Telco operators are realizing that the Softwarization of Telecommunications – and several other Industries – will be the natural next step of this Digital Transformation. Software Defined Networking (SDN) and Network Function Virtualization (NFV) are considered today two of the most promising enabling technologies to achieve the Softwarization of the telecommunication infrastructure [2]. Softwarization will allow decomposing the network and service functions into a set of software tasks to be executed according to a dynamically specified workflow, i.e., dynamic service chaining. Central Offices will become like Data Centers (DCs) offering virtualized network functions running on Virtual Machines (VMs) and elastically handling the traffic of the delivery, control and monitoring of data for specific network services (e.g., broadband access) [3].

There is an overall consensus that Next Generation Networks (i.e., 5G and beyond) will look like distributed clouds deployed in small/medium DCs, interconnected through ultra-low latency (radio and wired) connections, and capable of executing any software process or application while dynamically meeting Customers' needs. As a matter of fact, already today we are witnessing a growing diffusion of Internet of Things and Machine to Machine communications that are also creating a new generation of non-human Customers', such as Robots, Avatars and any sort of Artificial Intelligence applications. At the same time we are witnessing a sort of convergence of technology trajectories of Cloud, Edge and Fog Computing with SDN and NFV [4].

On the other hand, the envisioned scenarios imply higher and higher levels of management "complexity": in fact, rather than managing sets of homogeneous physical nodes and systems, it will be necessary allocating and orchestrating a huge number of software tasks, logically intertwined and dynamically moving. This "complexity" definitely outstrips human control and operational ability and can be tamed only by exploiting real-time Operating Platforms based on complex adaptive methods and systems, and supporting integrated management, control and orchestration functions across different domains of resources, i.e., Fog, Cloud/NFV and Edge Network infrastructure domains, also including Terminals. In particular, real-time Operating Platforms should provide capabilities of collecting, filtering and elaborating the infrastructure Big Data (e.g., logs, alarms, status, and data) aiming at "closing the loop" and making Big Data truly "actionable". Indeed, adaptive operations and dynamic provisioning of services need to be triggered according to the ever changing availability status of the infrastructure to assure proper user service experience despite the concurrent usage of underlying resources [5][28].

This work describes an experimental set-up reproducing a convergent 5G service scenario including both Cloud and IoT resource domains interconnected through an SDN network. SDN capabilities are also deployed within Cloud and IoT domains to exploit network programmability among virtualized functions and sensors, respectively. Moreover, the experimental set-up includes an SDN-based orchestrator able to dynamically adapt data delivery paths based on the current availability status (i.e., load) of network switches and links. Such path adaptation feature can be considered part of the orchestration capabilities of a real-time Operating Platform for 5G addressing reliability and robustness requirements of future 5G networks across IoT, Cloud and Edge Network domains. Finally, an experimental validation is presented aiming at demonstrating path adaptations triggered by congestion events at switches to assure proper level of data delivery services despite the concurrent usage of resources.

978-1-5090-6008-5/17/$31.00 ©2017 IEEE

II. Related Works

While complying with the Network Operating System (NOS) concept, i.e., platform-independent network abstraction and programmability, SDN plays a key role in harmonizing the control of network resources and data delivery services across different resource domains [6]. Indeed, SDN has been considered as a promising technological solution either in Fog (i.e., IoT), Cloud/NFV and Edge network domains. Within Cloud DCs, SDN has been mostly used to effectively implement traffic management and engineering solutions aiming at lower hardware costs and increase efficiency in the network service delivery in the cloud [7][8][9]. Recently, SDN control plane solutions have been also demonstrated for dynamic NFV deployments in the cloud [10]. In [11] a NOS for the IoT is presented based on SDN principles and leveraging the OpenFlow protocol (OF) while taking into account specific features of IoT components, e.g., wireless sensor and actuator networks. The usage of SDN at the Edge is gaining a great momentum as more network programmability and flexibility is needed closer to the Customers [4]. However, none of those works address SDN orchestration solutions involving both cloud, IoT and Edge network domains as this work does from an experimental point of view.

An integrated deployment of the IoT with SDN and Fog/Cloud computing has been recently demonstrated in [12] where the major focus has been however given to the coordinated deployment of VMs in the Cloud along with connectivity paths in the network, while the orchestration capability in terms of adaptability with respect to the availability status of underlying resources has not been addressed as this work does. The adaptability is an emerging and relevant aspect of orchestration in dynamic service chaining and 5G to adjust the provisioned services according to many ever-changing contextual data [5][13]. Indeed, in [14] the need of a monitoring framework is stated in dynamic service chaining to manage resource utilization and to enhance QoS provisioning to the users and applications through adaptive operations. In particular, traffic engineering operations are required that, based on collected network monitoring information, assess the performance of existing service chain paths and, in case, re-arrange the network settings to prevent QoS degradations [14]. A number of research works has been devoted to networking aspects of service chains, such as [15] [16] [17] providing SDN-based traffic steering solutions, and [18] [19] elaborating on NFV orchestration over SDN networks. However, none of them addresses the adaptability side of the orchestration process to prevent congestions or QoS degradations and to assure proper service level to applications as this work does. As far as our knowledge, SDN-based orchestration (i.e., adaptive) functions spanning IoT, Cloud and Edge network domains has not been neither investigated nor demonstrated yet.

III. 5G Operating Platform: Reference Scenario And Architecture

The increasingly availability of miniaturized systems with more powerful capabilities and the pervasive diffusion of ultra-broadband networks, portend a scenario with a floating "fog" of interconnected smart devices and terminals (i.e., sensors, robots, smart cars, autonomous machines) providing services for different application scenarios (e.g., smart cities, industrial automation). Terminals in the "fog" will be an integral part of the network, in many cases creating and using sub-networks by themselves. Moreover, the ever-growing availability of open source software, the cost reduction derived from software virtualization techniques and the increasing processing and storage capabilities of IT systems, are leading to the cloudification of many device capabilities and services to exploit flexibility and scalability features typical of cloud computing (i.e., Cloud Robotics, Edge/Fog Computing). On the other hand, SDN and NFV emerged as the breaking technologies for the telecommunication industry since they bring the use of standard hardware, cloud computing technologies and on-demand provisioning mechanisms into Telco deployments resulting in a convergent network-cloud ecosystem [20].

This generalized cloudification process, i.e., Softwarization, will make the major impact at the Edge of current telecommunication network infrastructure. As shown in Fig. 1, Edge networks, besides feeding wired/wireless access networks and aggregating traffics from users, will also include distributed micro-clouds of generalized Virtual Functions (VFs) running on standard hardware (i.e., servers) deployed in small datacenters and providing computational, storage and network capabilities (e.g., data analytics, middlebox services) according to the "as-a-service" paradigm in support of Fog and Edge Computing, Cloud Robotics, NFV clouds.

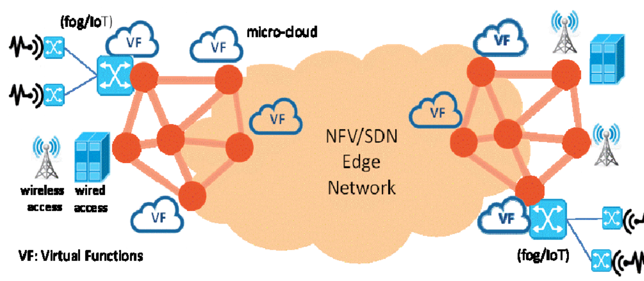

Fig. 1. Reference Scenario for 5G Operating Platform

As result of virtualization properties, e.g., self-contained service abstraction, heterogeneous resource capabilities offered by VFs can be uniformly exposed as *service components* with APIs and dynamically composed in the process of end-to-end service delivery. Indeed, an end-to-end service can be addressed as a composition of VFs, properly chaining application services (e.g., data analytics) as well as network services capabilities (e.g., virtual middlebox such as deep packet inspection) required to properly process the application data flow [13]. The composite set of VFs (i.e., service chains) are executed in a "slice" which is made of a set of logical resources (e.g., VMs or Containers) interconnected by a set of virtual links (e.g., Virtual Networks). This definitely requires that the abstraction process in terms of VFs will be coupled with the optimal selection, composition and provisioning (i.e., orchestration) of VFs [29]. Moreover, such orchestration mechanisms should not only rely on controllers for SDN (e.g., ONOS) and Cloud (e.g., OpenStack) but also other infrastructure controllers related to edge devices (e.g., IoT frameworks) and smart terminals (e.g., Robot Operating System). On the other hand, the use of SDN is emerging also outside the classic networking domain as demonstrated by recent developments for SDN-based IoT and Cloud [23] [22]. Thus, SDN can play a key role in harmonizing the control of network resources and data delivery services across Fog/IoT, Cloud/NFV and Edge network domains and in supporting orchestration functions to reliably deliver data flows in the Virtual Networks connecting VFs.

In such a scenario, we argue that the effective and reliable provisioning of 5G services should rely on a real-time 5G Operating Platform able to handle the heterogeneity and dynamicity of the 5G infrastructure as a flexible environment of virtual resources to orchestrate in a generalized way [5]. The real-time Operating Platform acts as an overarching orchestration framework operating over different infrastructure domains, i.e., IoT, Cloud/NFV and SDN Edge Network[1], where complex adaptive methods and systems, integrated management and control functions as well as generalized orchestration workflows are put in place as required by 5G scenarios [30]. The reference architecture and the main building block for the envisaged Operating Platform for 5G is depicted in Fig. 2. The real-time Operating Platform lies on top of resource infrastructure managers/controllers (i.e., IoT device manager, Cloud controller, SDN controller) thereby technology-specific capabilities of a different set of resources are offered to and handled by the Operating System (e.g., forwarding table set-up or traffic statistic collection at an SDN switch, VM set-up, IoT device monitoring).

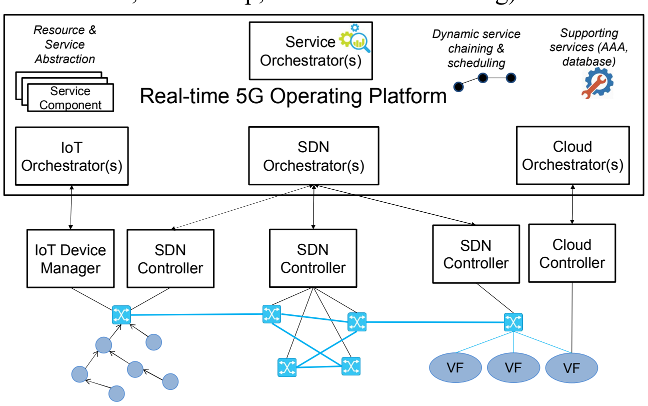

Fig. 2. Reference architecture and building blocks

While operating on top of abstracted *service components*, the Service Orchestrator(s) are in charge of the end-to-end service provisioning according to the application-specific logic (e.g., environmental temperature service) while addressing specified users' service requirements (e.g., reliable data repository, confidentiality). In the context of a specific user service request, Service Orchestrator(s) may cooperate to achieve more powerful service capabilities (e.g., temperature monitoring and video surveillance services along with high-available storage or image processing services). Service Orchestrator(s) rely on the IoT/SDN/Cloud orchestrators for the infrastructural service abstractions and for the invocation of services through intent-based interfaces [5].

[1] For sake of clearness of the picture and without lack of generality, smart terminals (i.e., robots) and mobile/5G access networks are not included neither as infrastructure capabilities nor as resource control frameworks.

Through the interworking between Service Orchestrator(s) and the IoT/SDN/Cloud Orchestrators, the real-time Operating Platform (i) provides an abstraction layer for network, compute, storage resources (e.g., switch/link capabilities, CPU, RAM, disk storage space) that will be logically partitioned (i.e.,. sliced) and exposed as service components (i.e., VFs, Virtual Networks); (ii) selects, allocates and composes VFs for executing end-to-end services as service chains deployed over "slices of resources"; (iii) provisions the ordered set of VFs in the selected "slices" by scheduling the execution of the software tasks in the VMs and deploying Virtual Networks through enforcement of data delivery configurations (i.e., dynamic service chaining); (iv) dynamically re-arranges (part of) provisioned VFs/Virtual Networks to adapt end-to-end service deployments to the current state of the infrastructure thus preventing service degradations that might occur as result of the concurrent usage of resources.

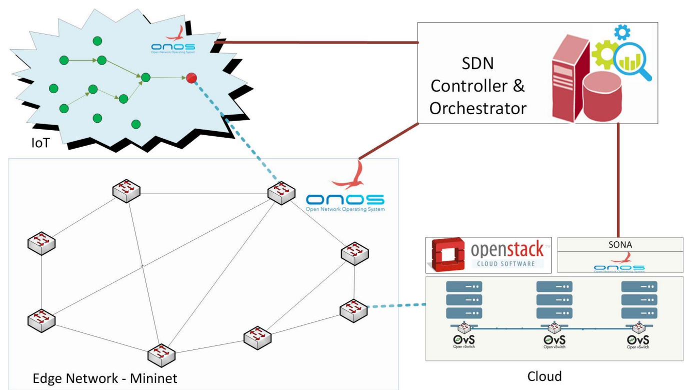

Fig. 3. Experimental setup: building blocks

As part of the real-time Operating Platform capabilities, in this paper we focus on the orchestration at the network infrastructure level across IoT, Cloud and Edge network domains while exploiting programmability features offered by SDN, i.e., SDN orchestration. In particular, we focus on the provision of network paths across domains while adapting them based on the switch/link states (i.e., load information) to preserve proper data delivery service performance (e.g., throughput).

IV. SDN Network Cloud and IoT: Experimental Set-up

This section describes the different components developed for and used in the realization of the convergent SDN infrastructure across IoT, Cloud and Edge Network domains. The SDN Edge Network serves as an interconnecting/transit domain between the SDN-WISE network and the Cloud resource domain. The set-up of building blocks is shown in Fig. 3 and detailed in the following sub-sections.

A. SDN-based IoT domain Set-up

We implemented the set-up of the SDN-based IoT environment by leveraging an open-source NOS for IoT [23]. The NOS has been obtained by extending ONOS with SDN-WISE platform [24] to support SDN in wireless sensor networks. The extended ONOS controller is able to decide and enforce the forwarding paths according to the network topology and based on service-related information, thereby optimally selecting the IoT gateways (if there are more than one) to send packets. Since service-related information can be handled by the controller as well, the gateways can be relieved from being aware of the service hosts the data are to be transferred to [24]. Fig. 4 shows the deployment of the IoT domain. Additional explanatory labels have been added for sake of clearness. In our experimental set-up we have an SDN-WISE network composed of 6 nodes representing wireless sensors (i.e., *sdnwise* nodes). One of them is also the gateway node (i.e., *sdnwise:01:00:01*) that connects the SDN-WISE network to the SDN Edge Network gateway (through entry node *of:1*).

B. SDN-based Cloud domain Set-up

The SDN-based Cloud domain has been set-up using OpenStack [21] combined with Simplified Overlay Network Architecture (SONA) [22], a set of ONOS application that provides an optimized and flexible multi-tenant network virtualization service for Cloud environments while relying on SDN capabilities. In OpenStack, virtual networking capabilities (i.e., multi-tenant VM connectivity) commonly involve the coordinated management of (i) virtual L2 and L3 networks/subnets connecting VMs across multiple compute nodes; (ii) a DHCP server for IP address distribution; (iii) virtual routers providing global connectivity and also involving NAT functionality; (iv) a security group as a set of rules to filter traffic flows. Virtual bridges/switches are used to connect VM's virtual interface to the physical interfaces of compute nodes and to connect VMs and subnets each other and with the external network through virtual routers. Such virtual networking capabilities are commonly provided by the Neutron component while relying on basic L2 and L3 networking features without flexible traffic management features (e.g., per-flow monitoring, filtering)

To benefit from improved traffic programmability features we opted for ONOS-SONA framework that relies on Open vSwitch (OvS) solution as an OF-based, software-based switching/bridging facility, specifically designed for virtualized environments. This allows to benefit not only of Linux kernel-level performance, but also of improved traffic manageability and programmability as result of SDN-based network control plane facility [21]. In fact, according to the ONOS-SONA framework, an ONOS controller is in charge of programmable network control plane functions (e.g., topology discovery, routing, enforcement of forwarding rules, traffic monitoring) along with effective interactions with external components, such as Neutron to manage network services in more effective way. As result, in our set-up we can benefit of VXLAN based L2 tunneling thereby overcoming the 4k limitation of the VLAN based solution used in Neutron. Moreover, the communication between VMs located in different compute nodes is direct, in each compute node just one virtual bridge is created and L2, L3 and DHCP functions are handled in the network controller, without relying on a distributed set of agents. In Fig. 5 the ONOS snapshot of the Cloud domain attached to the Edge Network is shown. Additional explanatory labels have been added for sake of clearness. The virtual topology we set-up in the Cloud domain is shown in the right side and includes 5 VMs and 2 OvS switches (i.e., *of:a1* and *of:a2*) connected to a virtual router (i.e., *of:a3*) acting as a gateway node toward the Edge Network domain. The VMs are located in two different VXLANs (i.e., 192.168.1.x and 192.168.2.x) and are supposed to host either kinds of VFs. The IoT domain is connected through the gateway node (i.e., *sdnwise:01:00:01*) to the Edge network entry node (i.e., *of:1*).

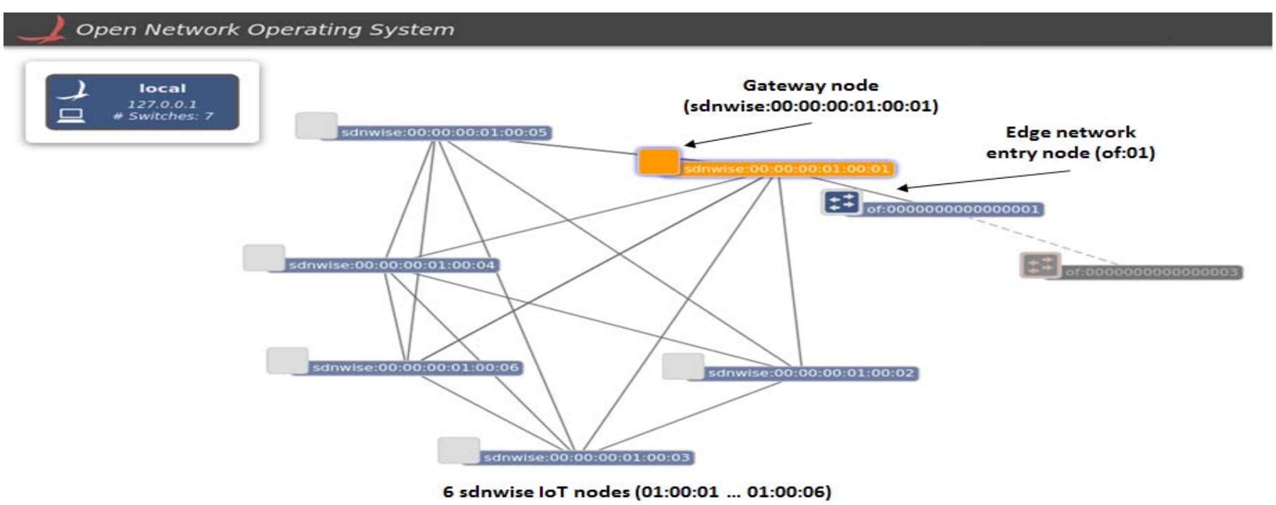

Fig. 4. ONOS snapshot of IoT set-up

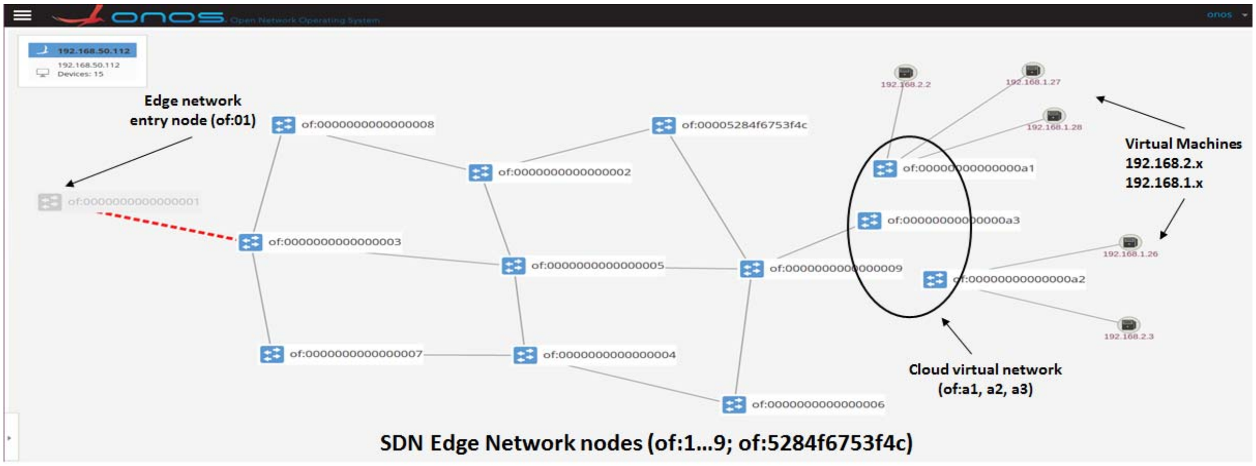

Fig. 5. ONOS snapshot of Cloud and Edge Network set-up

A. SDN Edge Network domain Set-up

The SDN Edge Network domain has been set-up using the Mininet environment (Fig. 5). The topology is composed of 9 OF switches (i.e., *of:2..9* and *of:5284f6753f4c*). Two of these switches behave as connecting points with the IoT domain and the Cloud domain (i.e., *of:1* and *of:9*, respectively). The ONOS controller deployed within the Cloud domain is also in charge of the SDN Edge network.

B. SDN Orchestrator

As one of the orchestration components of the real-time 5G Operating Platform, an SDN orchestrator is deployed to dynamically adapt data delivery paths connecting VFs deployed across IoT, Cloud and Edge network domains. The SDN orchestrator has been implemented as an application running on top of ONOS controllers of the underlying resource domains. The SDN orchestrator provides network service orchestration capabilities that allow for the programmable and adaptive provision of data delivery paths, possibly through a sequence of VFs, internally represented as end-points IP addresses. The specific tasks performed by VFs are irrelevant for the operation of the SDN orchestrator since only connectivity aspects are addressed. The SDN orchestrator exposes a RESTful interface which enables upper-layer orchestrators (e.g., NFV orchestrators, context-aware Service Delivery Platforms) to directly ask the set-up and the tear-down of delivery paths connecting specified end-points (also traversing a set of VF end-points, if specified) by using intent-based semantics, i.e., prescriptive rather descriptive directives, without the need to specify technology-specific low-level details. The provisioning details are then handled and coordinated by the SDN orchestrator which maps them into specific ONOS-compliant queries for the controllers. In turn, the underlying controllers handle the low-level directives (i.e., OF messages) to switches. Moreover, the SDN orchestrator offers adaptation capabilities for the established paths (i.e., path redirection) to recover from congestion events (e.g., service outages or degradation events) that are possible when a concurrent resource usage takes place. To this purpose, the SDN orchestrator collects traffic statistics from the switches and elaborates them to evaluate their current load. This redirection feature regulates the use of network resources while preventing that service degradations are perceived by users. Further details on the SDN orchestrator can be found in [26].

V. Experimental Validation

The goal of the experimental validation is to demonstrate the capability of the SDN orchestrator to promptly react to significant changes in the availability status (i.e., congestions) of the network switches/links by adapting paths in order to prevent performance (e.g., data throughput) degradations due to the concurrent usage of network resources across domains. If a throughput degradation occurs at a specified switch, this is detected by the SDN orchestrator based on background collected statistics (i.e., the measured throughput is higher than a given threshold). Consequently, the SDN orchestrator redirects the paths (or part of thereof) traversing the congested switch throughout other less used switches. This redirection of paths demonstrates the adaptation capabilities of the SDN orchestrator in the re-arranging the paths based on the switch availability status (i.e., load) thereby providing reliable data delivery in dynamic service chaining. It worth pointing out that this validation aims at demonstrating the proper operation of the redirection feature in an experimental testbed composed of different resource domains according to 5G scenarios. As for the effect of such operation in terms of switch utilization, a preliminary evaluation is shown in [26] using an emulated SDN domain, where we

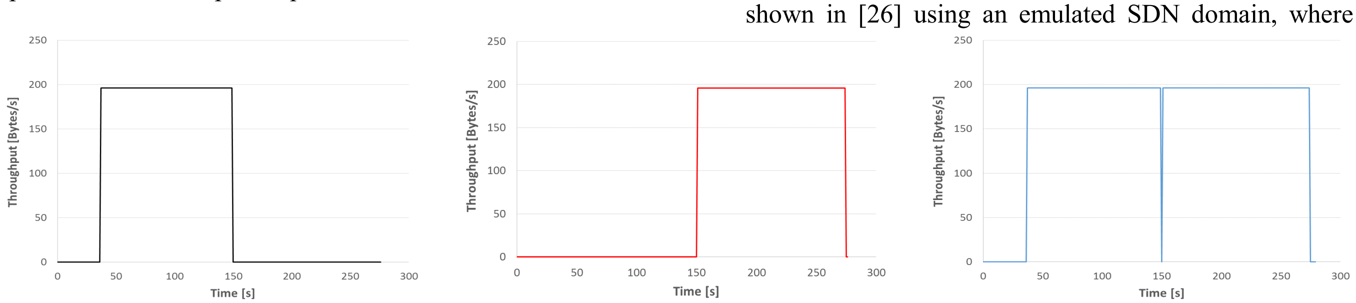

Fig. 6. Throughput measured at switch *of:4* (a), switch *of:2* (b) and switch *of:a1*(c)

demonstrated the effectiveness of the redirection in terms of load-balanced network resources usage and limited overhead.

To demonstrate path adaptation capabilities, we firstly set-up a number of delivery paths that traverse the three domains. The paths start from an end-point in the IoT domain (the IoT gateway node sdnwise:00:00:00:01:00:01), run through a given number of switches in Edge and Cloud Network domains and then end at one of the end-points (i.e., VMs) in the Cloud domain (e.g., 192.168.1.26, 192.168.1.27, 192.168.1.28, 192.168.2.2, 192.168.2.3). The end-points are chosen randomly among those available. Indeed, without lack of generality, it is assumed that the VMs run the same type of VFs and that they can be indifferently selected from the point of view of the application (e.g., NFV orchestrator).

Once the paths are established (i.e., flow entries are installed in the switches), we start sending data traffic. During the time of the experiment, the SDN orchestrator periodically collects, aggregates and elaborates monitoring data (i.e., throughput) on peer-switch basis for all the switches in the three domains. Fig. 6 plots the measured throughput using the Wireshark tool [27] at relevant ports of the switches *of:4*, *of:2* and *of:a1*. Results show that when we start sending the traffic, the throughput increases in the switches *of:4* and *of:a1*. As we cause a congestion at switch *of:4* (at 150s), the redirection of paths involving that switch is triggered by the SDN orchestrator. As result, the throughput is nullified in the switch *of:4* while it starts increasing in the switch *of:2*. Finally, the throughput at the *of:a1* remains stable. However, at the redirection time, we notice a small degradation: this corresponds to the interval of time in which the orchestrator deletes all the flows traversing the switch *of:4* and starts redirecting them through the switch *of:2*. Results also show that the redirection operation takes a very short time (in the range of tens of milliseconds) with a loss of packets that can be estimated in the order of bytes that is the penalty to pay to avoid more persistent service degradations due to packet drops at congested switches. Actions to mitigate this penalty are planned as future works.

VI. Conclusion

In this work, we have presented an experimental set-up of a convergent 5G service scenario involving IoT, Cloud and Edge network, all featured by SDN capabilities. The set-up included an SDN orchestrator able to recover from congestion events at network switches through the redirection of paths traversing congested switches/links that are detected relying on continuous monitoring of throughput data. Such adaptability feature has been demonstrated using the presented experimental set-up as one of the relevant capability of a real-time Operating Platform able to provide service assurance in the envisioned 5G scenarios.

Acknowledgement

The authors thank Dr. Anna Lina Ruscelli and Dr. Gabriele Cecchetti for their contribution to the setup of the testbed. This work was supported by the LASH-5G project approved within the 1st Call of the Fed4Fire+ project.

References

[1] Whitepaper "Digital Business Transformation – A conceptual Framework" available at www.imd/dbt/whitepapers/framework

[2] Y. Li and M. Chen, "Software-Defined Network Function Virtualization: A Survey," in *IEEE Access*, vol. 3, no. , 2015.

[3] Peterson et al., "Central office re-architected as a data center," in IEEE Communications Magazine, October 2016.

[4] A. Manzalini et al, "An edge operating system enabling anything-as -a-service," in IEEE Communications Magazine, March 2016

[5] A. Manzalini, et al, "A unifying Operating Platform for 5G end-2-end and multi-layer orchestration", NetSoft 2017, Bologna, Italy

[6] P.Berde, et al., "ONOS: towards an open, distributed SDN OS", In Proc. of HotSDN '14. ACM, New York, NY, USA

[7] https://cloudplatform.googleblog.com/2014/04/enter-andromeda-zone-google-cloud-platforms-latest-networking-stack.html

[8] https://code.facebook.com/posts/416590345118089/accelerating-network-innovation-with-the-open-networking-foundation/

[9] W. Cerroni, et al.,"Cross-layer resource orchestration for cloud service delivery: A seamless SDN approach," Computer Networks, 2015.

[10] F. Callegati, et al, "SDN for dynamic NFV deployment," in IEEE Communications Magazine, October 2016.

[11] G. Anadiotis et al "Towards a Software-Defined Network Operating System for the IoT",IEEE World Forum on Internet of Things, 2015.

[12] R. Munoz et al.,"The CTTC 5G End-to-End Experimental Platform: Integrating Heterogeneous Wireless/Optical Networks, Distributed Cloud, and IoT Devices," IEEE Vehicular Technology Mag., 2016.

[13] F. Paganelli, et al., "Context-aware service composition and delivery in NGSONs over SDN," IEEE Comm. Mag. Aug. 2014.

[14] A. M. Medhat; et al. "Service Function Chaining in Next Generation Networks: State of the Art and Research Challenges," in IEEE Comm. Mag. , October 2016.

[15] Ying Zhang et al., "StEERING: A software-defined networking for inline service chaining," 2013 21st IEEE ICNP, Goettingen, 2013.

[16] Z. Qazi et al., "Practical and Incremental Convergence between SDN and Middleboxes", Open Network Summit, Santa Clara, CA, 2013.

[17] B. Martini, et al. "SDN controller for context-aware data delivery in dynamic service chaining,", Proc. of NetSoft, London, April 2015.

[18] K. Giotis, et al., "Policy-based orchestration of NFV services in Software-Defined Networks," Proc. of NetSoft, London, 2015

[19] F. Callegati, et al., "Dynamic chaining of Virtual Network Functions in cloud-based edge networks," Proc. of NetSoft, London, 2015

[20] J. Soares et al., "Toward a telco cloud environment for service functions," in IEEE *Communications Magazine*, Feb. 2015.

[21] www.openstack.org

[22] https://wiki.onosproject.org/display/ONOS/SONA+Architecture

[23] http://sdn-wise.dieei.unict.it/

[24] L. Galluccio et al, "SDN-WISE: Design, protoyping and experimentation of a stateful SDN solution for wireless sensor networks", INFOCOM , May 2015.

[25] F. Callegati, et al,"Performance of Network Virtualization in cloud computing infrastructures: The OpenStack case," IEEE CloudNet, 2014.

[26] A. A. Mohamed et al, "SDN controller for network-aware adaptive orchestration in dynamic service chaining," NetSoft, Seoul, 2016.

[27] https://www.wireshark.org/

[28] F. Paganelli, et al., "Context-aware service composition and delivery in NGSONs over SDN," IEEE Communications Magazine, 2014.

[29] B. Martini, et al, "Latency-aware composition of virtual functions in 5G," Proc. of NetSoft, London, 2015.

[30] B. Martini, M. Gharbaoui, P. Castoldi, "Cross-functional resource orchestration in optical telco clouds," ICTON 2015.