Self-Healing in Multi-Constrained Multi-Actor Virtualization Orchestration

J. Harmatos, D. Jocha, R. Szabó and B. Gerő
Ericsson Research
Email:janos.harmatos@ericsson.com

B. Németh, J. Czentye and B. Sonkoly
Budapest Univ. of Tech. and Economics
Email:{nemethb,czentye,sonkoly}@tmit.bme.hu

***Abstract*—Multi-constrained multi-provider orchestration is alone challenging, which we complemented with an automated multi-layered failure recovery mechanism. Our proof of concept prototype demonstrates information models (both bottom-up and top-down), orchestration and recovery workflows with delegation, trial and error based backtracking among the chain of federated providers in an Industry 4.0 use-case for critical machine type communication (C-MTC). With a remote factory scenario, we show fault recovery from single to multi provider involvement. We provide insights into the responsibility split for failure handling between service agnostic resource orchestration and service specific lifecycle management components.**

I. Introduction

The improved capabilities and features of 5G network make possible to introduce much wider range of services as existing today. Ultra-low latency provided by the new generation 5G radio as well as the flexible and programmable core network guarantee the handling of such services (e.g., Critical Machine Type Communication (C-MTC) use cases), which claim extreme requirements on the network (such as 1ms latency/ultra-high service reliability).

Furthermore, Network Function Virtualization (NFV) has also driven a paradigm changing in the existing networking ecosystem. NFV as a cornerstone of 5G network will lead to a new treatment of the services offered by 5G networks. The services typically built up by multiple (virtualized) components with corresponding relationship among them. Depending on the service requirements, the components can be deployed on different network domains, which can belong to even different providers in some cases. For example, in a factory automation use-case, where the capabilities of 5G networks could be extensively utilized, the ultra-low delay control of the factory devices requires a nearby control function deployment (e.g., on network edge datacenter), while higher level control entities can be placed on a remote site, covered even by a different providers. To sum up, efficient service deployment requires an orchestration system, which can handle the different service requirements in an integrated way, while on the other hand can deploy the service over multiple technology (network and compute) as well as administrative domains. In the mentioned ecosystem each provider's has its own *NFV Orchestrator* (NFVO), which manages the service deployments and the required domain capability-related and service request deployment-related information exchange with the NFVOs belonging to other providers. The topology among the NFVOs can be appropriate by forming an orchestration hierarchy through the involved providers.

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement n 671636 – 5GExchange)

The 5G network-based virtualized services and the multi-domain, multi-provider ecosystem put the reliability handling also into a new context. At one hand, during the service deployment phase the orchestration system should find a service deployment state spanning over the multi-domain/provider environment, where the service reliability requirements are endorsed. On the other hand, it should also be considered that in some cases, when a failure occurs, the domain- or provider-level fault handling is not enough to recover the service, e.g., due to lack of the necessary resources of the current provider. (For example, in the case of a datacenter failure, the impacted service component(s) cannot be re-deployed to another datacenter of the same provider with the fulfillment of the latency requirement). Consequently, to guarantee the appropriate service recovery, the impacted service components have to be migrated to other providers.

In our demonstration we show how a multi-domain, multi-provider orchestration system can handle multiple service requirements (such as latency and reliability) in an integrated way for service fulfillment and assurance. Our contributions are the extended information models for the multi-provider reference points and the distributed self-healing methods and workflows.

II. Demonstration

By demonstrating the service healing capabilities a Balancing Robot Control as an Industry use case is selected where both the latency and reliability requirements are critical. A LEGO Robot is used, which is controlled by a virtualized balancing control VNF entity (e.g., PID controller) running in a Docker container. The Robot has two WLAN interfaces, so duplicated connections can be established if multiple controller entities are available. Fig. 1 shows the demonstration setup. The data-centers of the different Operators are realized on a micro-cloud cluster as Docker-based cloud environment, while the networking infrastructure is implemented by Mikrotik SDN switches and there are two WiFi APs to which robots can connect to.

According to Fig. 1, an Enterprise User initiates a Balancing Control service request to Op. 3 by providing his assigned factory robot's attachment points and subscriber IDs (MAC addresses in our case). Balancing Control, however, is provided as a Reliable Balancing Control as a Service (RBCaaS) – a VNF as a Service (VNFaaS) instance – by a third party provider (3PP). The virtualization lifecycle management for the RBCaaS is provided by the VNF Manager (VNFM) in the Op. 3 domain. The resource orchestration request for the NFVO in Op. 3 is the combination of the Enterprise User's service parameters (attachment points, end-to-end latency, service function chains) and the 3PP's service definition (latency/bandwidth constrained resilient sub-service topology). Therefore, the resource orchestration request consists of – in the absence of further service components – two PIDs connected to the two interfaces of the robot with both latency limit between the robot and the PIDs, and path anti-affinity for the service components belonging to different physical interfaces of the robot. Assuming cloud infrastructure preferences (costs) in Op. 3 are Op. 3, the Factory, and finally Op. 1, i.e., Op. 1 is used only as a last resort. The initial resource assignment to the service request is shown in Fig. 1, where the Factory and home provider is used for cloud workloads, while connectivity is routed to ensure path anti-affinity, i.e., in our very case the shared use of the SDN networks must be avoided as they consist of a single switch only.

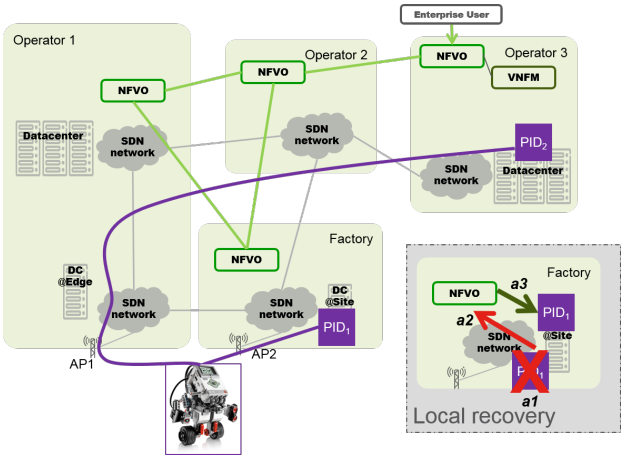

Fig. 1. Network topology & local recovery case

Service healing is demonstrated via an infrastructure monitoring agent notifying the local NFVO if any of the allocated workload terminates. In turn NFVO checks if the terminated VNF workload had a persistent flag on, indicating that the service component needs restoration unless decommissioned via an explicit orchestration request. Fig. 1/b shows the situation when the local NFVO can itself restore the workloads by re-issuing the genuine resource allocation request, see steps a1, a2, a3. Mind that even in this case the corresponding network forwarding behavior configuration must be decommissioned and re-created according to the new cloud workload allocations.

In the case where local recovery is not possible (see Fig. 2), the failure is propagated upstream backward of the situational orchestration hierarchy. B1, b2, ..., b5 in Fig. 2 show the sequence or orchestration actions to migrate PID2 from Op. 3 to Op. 1. In this case the NFVO at Op. 3 is also the top-level orchestrator. When the factory data-center goes down, however, the recovery can be successfully completed by the NFVO at Op. 2 via c1, c2, ..., c5 sequences; which deployment satisfies the original service and resiliency requirements. However, due to the cost preferences, it is highly non-trivial for the distributed orchestration to find the migration point and the route to it for PID1: for Op. 2 not seeing the internal topology of Op. 1 and the Factory, it must try and learn by multiple failures how to allocate and stitch the service from the Factory to Op. 1 satisfying full path anti-affinity.

For all the recovery steps, first a proper decommissioning of the corresponding network segments until the adjacent VNFs are done then a joint create for the network segment and cloud workload is issued.

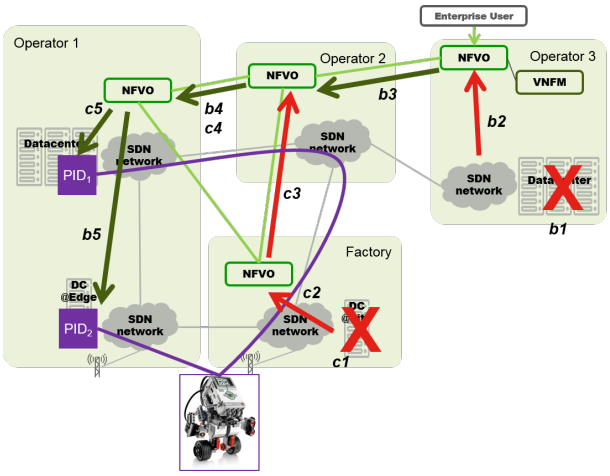

Fig. 2. Multi-provider self-healing workflows

III. Conclusions

While virtualization management frameworks (e.g., ETSI NFV) primarily focuses on the fulfillment phase, we provide insights that bottom-up information flows on topology of capabilities, resources and *service states* are equally important to assure running services' service level agreements. We show that resource level multi-layer service healing is possible, i.e., the error propagates upstream in the situational hierarchy of the providers until one can either restore the service or a service specific LCM may assist in the exploration of alternative service deployment options.

References

[1] ETSI *Network Functions Virtualisation (NFV); Management and Orchestration; Report on Architectural Options*, ETSI GS NFV-IFA 009 V1.1.1, 2016.

[2] R. Szabó, et al. *The Orchestration in 5G Exchange – A Multi-Provider NFV Framework for 5G Services*, IEEE Conference on Network Function Virtualization and Software Defined Networks, 2017