Deployment of 5G Network Applications over Multidomain and Dynamic Platforms

Ana Hermosilla*, Jorge Gallego-Madrid*, Pedro Martinez-Julia†, Ved Kafle†,
Kostis Trantzas‡, Christos Tranoris‡, Rafael Direito§, Diogo Gomes§, Jordi Ortiz¶,
Spyros Denazis‡ and Antonio Skarmeta*
*Odin Solutions, Spain.
Email: {ahermosilla, jgallego, skarmeta}@odins.es
†National Institute of Information and Communications, Japan.
Email: {pedro, kafle}@nict.go.jp
‡University of Patras, Greece.
Email: {ktrantzas, tranoris, sdena}@ece.upatras.gr
§ Instituto de Telecomunicações, Portugal.
Email: {rdireito, dgomes}@av.it.pt
¶ University Center of Defense at the Spanish Air Force Academy, Spain.
Email: jordi.ortiz@cud.upct.es

***Abstract*—5G mobile communications are bringing a plethora of applications that are challenging existing network infrastructures. These services demand a dynamic, flexible and adaptive infrastructure capable of fulfilling the rigorous requirements they need to operate correctly. Another key point is the need of real-time reactions in the architecture configurations to effectively satisfy changes in the user's behavior. To address these issues, *Network Function Virtualization* (NFV) and *Software-Defined Networking* (SDN) paradigms arise as enablers of the network infrastructures of the future. These technologies will permit the design and development of a new set of network applications that will be dynamically managed and orchestrated over multiple domains in an effortless way. In this work, we present an architecture that interconnects two facilities located in Spain and Japan, which permits the deployment of distributed applications. Besides, we detail how the control and data planes are managed to enable the operation of the system.**

Keywords: NetApps, NFV, SDN, 5G, multidomain, testbeds, SMEs, dynamic deployment, interconnection, automatization.

I. INTRODUCTION

5G mobile communication services are supposed to bring a significant change in the way network infrastructures are designed and used. From some years now, monolithic servers are being extensively used thanks to the disruptive technologies of *Network Function Virtualization* (NFV) and *Software-Defined Networking* (SDN). The networking paradigm has completely changed and evolved with dynamic, programmable, and adaptive resources. This paradigm led to the development of 5G infrastructures and architectures designs, which are characterized by being dynamic and adaptive in almost real-time, to allow the deployment of applications and services compliant with the stringent requirements demanded by new applications.

The softwarization of network and computing resources is also changing the way in which the applications and services are envisioned and developed. The flexibility of these infrastructure designs and management allows the creation of more powerful and complex services, mainly exploiting the geographically distributed components to reduce latencies or offload computational task from end-devices. This strategy is known as *Mobile Edge Computing* (MEC) and it is one of the driving forces of 5G architectures[1]. One of the main problems that arose with the adoption of these new paradigms is the knowledge needed to tailor existing services to 5G. From the developer's perspective, besides the application design and development, an understanding of the architecture details is also required to leverage the potential of these solutions. In order to solve this problem, the European Commission pushed with ICT-41-2020 call an effort to ease the adoption of 5G technologies and infrastructures. One of the representative research projects is H2020 5GASP[2] , which aims to offer an automatized and dynamic platform over existing 5G infrastructures to facilitate the deployment of end user applications. In this way, application owners need to be concerned about their applications, obviating the underlying and complex process of deploying them.

Regarding the applications to be deployed over these 5G infrastructures, the term *Network Application* (NetApp) is

---

This work has been supported by Fundación Séneca—Agencia de Ciencia y Tecnología de la Región de Murcia—under the FPI Grant 21429/FPI/20, and co-funded by Odin Solutions S.L., Región de Murcia (Spain); by the Spanish Ministry of Science and Innovation under the DIN2019-010827 Industrial PhD Grant, and co-funded by Odin Solutions S.L.; and by the European Commission under the 5GASP (Grant No. 101016448) project.

introduced, representing an application that will be deployed over them, offering certain functionalities with added value to the society. The network is provided with the characteristics, requirements, or behavioral profile of an application and ensures they will be provided by the network. One of the main challenges while providing and ensuring *end-to-end* (E2E) service provisioning is the multi operator environment alongside the coordination and agreement of the involved entities.

Therefore, in this paper, we propose an architecture that enables the effortless deployment of network applications in multi-domain and dynamic 5G platform facilities. Besides, it includes some enhancements, such as mechanisms to centralize the involved facilities, improvements over existing tools, interconnection of the facilities' private networks, and automated tests and *Quality of Service* (QoS) granted over the infrastructure. In this line, Section II will expose the background required to understand the proposed solution; Section III will show the tools, technologies, processes, and novelties exposed; Section IV will explain the integration between two facilities, located in two different countries (Spain and Japan) and how the improvements proposed in section III enhance the integration between them; and finally, section V will show the conclusion and future work related with this paper.

II. BACKGROUND

In recent years, next-generation networks have been the focus of researchers' efforts, being the central hub around which a large amount of important digital work has been performed [3][4]. They offer new capabilities that were impossible in the past, mainly due to the nature of previous networks and how they were deployed. However, the cost of deploying and maintaining a 5G infrastructure (in economic, knowledge, and time terms) is not trivial, which means that SMEs are not able to compete on the same terms as large technology companies, since the formers cannot afford to spend the required resources on the task. In this way, offering access and development capabilities to SMEs over already deployed infrastructures (called testbeds) avoids the necessity of self-managed and owned infrastructure reducing CaPex and Opex.

Furthermore, SDN and NFV, which enable the programming of the network and the deployment of network resources on-demand respectively, in addition to network slicing, are considered the key enablers of the development of 5G technologies. Network slicing is defined by 3GPP as a paradigm where logical networks/partitions are created, with appropriate isolation, resources and optimized topology to serve a purpose or service category[5]. That means a network slice can be instantiated across multiple parts of the network and may consist of a set of dedicated or shared resources. If dedicated or properly arranged virtual resources are used, the slice is considered as completely isolated from other network slices.

To define a network slice, two terms are defined by GSMA[6]. One term is GST (*Generic network Slice Template*), which defines the attributes that characterize a type of network slice, and the other term is NEST (*NEtwork Slice Type*), that defines a recommended minimum set of attributes and their suitable values. This set of attributes with their values complies with a given set of requirements, derived from a use case defined by a network slice customer. Hence, NEST is used as an input for the preparation of a network slice.

Regarding NetApps, they can be seen as cloud-based applications highly tied to the network vs heavily relying on the characteristics offered by 5G to provide with the service envisioned. In that line, NetApps require high isolation not only in terms of access control and management but also in terms of ensured capabilities. For that, MEC and slicing technologies are envisioned as key to assure the minimal requirements. But NetApps are not simple applications that rely on proper QoS values to provide the service but rather complex and composite enhancements that need to be also certified from a service provisioning point of view, therefore, a mechanism to certify that the network can cope with the requirements and ensure they are met is needed alongside a mechanism to ensure that the service offered by the NetApp is within the specified parameters.

There are several projects that aim to solve all those problems, such as H2020 5GASP[2], which offer an automatized and standard model over existing 5G virtualized infrastructures. In this way, the deployment of end user applications is considerably simplified, since developers only need to be concerned about their applications, therefore obviating the underlying and complex process of deploying them. For this purpose, 5GASP leverages the mainstream idea of the general use of regular testbeds but taking it a step further, offering them throughout a portal (called NetApp portal) where developers can onboard and deploy their NetApps on the infrastructure prefered/needed. The NetApp portal is based on Openslice[7], an OpenSource OSS for delivering *Network Slice as a Service* (NSaaS), which offering not only the testbeds but also all their particular capabilities, even Network Slicing, in a unified and flexible way.

Apart from that, there are also other efforts to improve this kind of infrastructure with a different perspective, such as NICT's *OpenSource Distributed Mano* (OSDM), an enhanced version of the well-known ETSI's OSM[8], which aims to improve OSM's performance by adding support for Quality of Service and Quality of Experience (QoS/QoE) metrics for future network services. It also includes a decentralized publish-subscribe system that provides high performance for multi-destination messaging (used mainly in telemetry) among OSM modules and other virtualized infrastructure management systems, such as OpenStack, SDN switches, and OSS/BSS interfaces.

III. MULTIDOMAIN AND DYNAMIC TESTBEDS

Nowadays services are worldwide and distributed, which means NetApp developers may need an equivalent environment to certify that their developments are valid, compatible and, if necessary, deployable in different testbeds. Thus, offering multi-domain testbeds is a crucial approach for the development of universally usable NetApps. Therefore, this work interconnects two testbeds, one in Spain and the other in Japan, and flexibly operates them through Openslice. With this scenario, it is possible to illustrate how facilities geographically separated can be orchestrated and managed in conjunction to enable the onboarding and deployment of multi-domain NetApps. Besides, the platform integrates an improvement in the NFVO aimed to increment the performance in terms of response times particularly relevant in scenarios geographically separated such as the one described (10000 km and more than 200ms RTT).

A. Dynamic infrastructure

One of the main characteristics of 5G infrastructures is that they need to be dynamically reprogrammable, changeable and scalable. NFV and SDN are indispensable component technologies as they allow to reconfigure the network on-demand. Therefore, our testbed platforms use OSM as *NFV Orchestrator* (NFVO) and Openflow switches to redirect flows when and where required. The Spain site is currently equipped with multiple Openflow-powered switches that interconnect the nodes of two Openstacks acting as *Virtual Infrastructure Managers* (VIMs). As aforementioned, OSM is used to orchestrate the deployed VNFs, and multiple versions are available.

Furthermore, another novelty added to 5G infrastructure is the NICT's OSDM testbed platform, as it improves the performance of regular OSM deployments by introducing a decentralized control bus, instead of the centralized Kafka that OSM usually employs. This change enhances the performance of the messaging among OSM control and management components as well as the managed entities of the infrastructure. Moreover, it also will enable the resource allocation and dynamically adjustment of the OSDM modules located in different parts of the network. It compresses and processes telemetry data at the source points as much as possible to improve the control response times (latency) and reduce bandwidth consumption.

B. Onboarding

The onboarding process is a crucial step in the deployment of NetApps. This term represents the process by which the descriptors that define a NetApp are uploaded (or "onboarded") to the available platform and instantiated to deploy. The onboarding process is the first step to deploying a NetApp on the distributed 5G service platform. As NetApps are expected to be complex, and probably very different from each other, the onboarding process requires standardization of the descriptors used. For this purpose, some templates are commonly used to define the requirements and components of a NetApp. These templates include regular NFV descriptors (VNFDs/NSDs), some tests to perform before uploading and instantiating the NetApp, and the NEST descriptor that defines the network slices. They, together, constitute the 5GASP proposed "triplets", that is, the conjunction of NFV descriptors, Tests, and NEST.

1) Triplets:

The idea for the Triplets is to create a "meta-package" that includes the Network Slice requirements (NEST information), the NSDs that conform to the NetApp (with their respective VNFDs), and the tests the user wants to perform over them to validate the NetApp responsiveness and operation. Figure 1 shows the concept of a triplet.

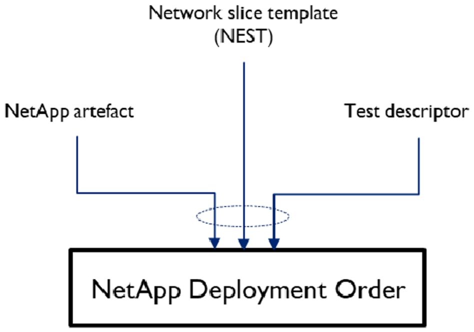

Fig. 1. Triplet

- **VNFD/NSD packages:** Regular VNFD/NSD packages used by define the resources and connections of our application.
- **GST/NEST:** NEST file, with the network requirements of the application.
- **Test Descriptor:** File that describes the test plan to be performed over the NetApp once deployed.

2) Test Descriptors:

Two different types of Test Descriptors can be defined: regular test descriptors and Test VNFs. Test descriptors are those that are envisioned to be executed in already scheduled or preexisting resources such as the VMs integrating the VNF itself. On the other hand Test VNF are separate VNFs whose solely purpose is to execute tests to other VNFs implying resource reservation for the testing and therefore not affecting the behaviour of the VNF under inspection. The ability to onboard these tests simultaneously to NEST and NFV descriptors is one of the novelties that Openslice offers.

C. Openslice

Openslice is an opensource OSS as aforementioned which is still in prototype phase. Its firm alignment with TM Forum's (TMF) TMF909 API Component Suite[9]enables the exposure and management of network services, while supporting an extensive set of Operational Domains at the same time. The aforementioned suite, being widely followed by the industry, not only facilitates the interworking of the several Operational Domains with other OSS/BSS platforms and domains of 3rd party service providers but also accommodates the reusability of APIs' functionality, though the offered standardized Open API families. This lack of need to introduce a set of proprietary solutions also provides for the simplification of the APIs required, further reducing the initial and maintenance costs. With that being said, Openslice enables SMEs to materialize on-demand private network scenarios, simultaneously maintaining the ability to interoperate with the public operators' large-scale networks through standardized interfaces.

Regarding the exposure of northbound interfaces, Openslice supports a wide range of TMF's OpenApis family, including Service Catalog, Ordering, Inventory, and Resource Management among others. Employing these APIs and models, which are extensively embraced by the telco industry, offers a familiar environment for 5G vertical customers and developers to interact. Specifically, developers can onboard NFV artifacts which are eventually utilized to design respective services. The offered services are modelled under the TMF's Service Specification entity, simultaneously encapsulating network requirements, expressed in GSMA's NEST properties, as Service Specification's characteristics. Eventually, a 5G vertical customer can browse the available offered services and place a corresponding order, modeled through TMF's Service Order entity. Once the order is placed, the service fulfillment process is instantiated by a Service Order Manager engaging the corresponding Service Orchestrator(s). Here, the requested service specification is decomposed up to the required network-level operations, and eventually, the execution of the aforementioned operations onto an administrative domain is performed.

Additionally, Openslice incorporates an ETSI SOL005[10] compliant component which transforms the selected network-level operations into their corresponding network service life cycle actions for the MANO administrative domain. These actions are handed over to the respective NFVO by employing the ETSI-defined Os-Ma-Nfvo interface[11]. The same interface is also utilized to extract network service details during the provisioning and runtime phase ultimately exposing them via TMF's Service Inventory to all intended actors.

Last, horizontal (east-west) interoperability with other OSS is supported via TMF APIs as well. From the vertical's perceptive, this is achieved by the provision of Service Specifications from additional domains to browse upon, in the form of Service Catalogs. Respectively, from the orchestration's perceptive, Openslice can communicate with other Service Orchestrators and issue or receive Service Orders from them.

D. NetOr

Network Orchestrator (NetOr) is an OSS/BSS system under development that manages 5G infrastructures and services. This tool allows the deployment of *Vertical Service Instances* (VSIs) and several additional resources via its *Northbound API* (NBI), which implements the TS 28.541[12], SOL005[10], and SOL006[13] standards. Besides this, its *Southbound API* (SBI) is also highly standardized through the implementation of the TS 28.530[14], TS 28.531[15], TS 28.541[12], TS 28.801[16], SOL005[10], and SOL006[13] standards. The existence of standardized APIs heavily contributes to the immense interoperability of this tool, which can easily be used to manage and orchestrate 5G services in different infrastructures.

Being able to deploy 5G services and perform runtime operations over these, NetOr is capable of instantiating E2E services across several domains without prior negotiations. This is made possible by instantiating a *Network Slice Instance* (NSI), composed of several distinct *Network Slice Subnet Instances* (NSSIs), one for each domain. Each NSSI comprises a Wireguard peer that enables *Virtual Private Network* (VPN) tunnels between the different domains. Wireguard was the tool chosen to achieve these interdomain scenarios because of its minimalism, performance, and straightforward instantiation. To deploy interdomain services, NetOr must exist as an independent tool deployed outside of the domains that will be tied. Although, NetOr must be able to communicate with the *Network Function Virtualization Orchestrators* (NFVOs) of each domain. Through these NFVOs, NetOr is in charge of deploying and configuring the required NSSIs. The peers' configuration will also be orchestrated by NetOr, which will perform all the necessary runtime operations to create the different VPN tunnels.

When the VPN tunnels are established and entirely configured, they will transparently enable the communication between components deployed in different domains, thus fully enabling the deployment of NetApps in inter-domain scenarios.

IV. INTEGRATION OF NICT'S OSDM AND UMU'S OSM

In this section, the integration of both NICT (Japan) and University of Murcia (UMU, Spain) sites is explained. It also discusses how the integrated platform results in a solution capable of offering NetApps in a unified way using Openslice, plus enabling interconnection between their private networks by leveraging NetOr. This solution is the central and fundamental capability this work presents, as it provides end users with complex and heterogenous testbed platforms that can be managed in an uniform way. It enables those separated platforms to act as only one in interconnection terms. Namely, the NetApps deployed in one site can communicate with the functionalities already deployed in other sites transparently, thanks to NetOr, and could even enable deploy a fully distributed NetApp whose components are distributed across different sites.

A. Interconnection of Control Plane using Openslice

As previously explained, one of the aims of this work is to offer different infrastructures across a unique entity, even though they are part of different domains. In this way, SMEs or any other final user will be able to use them transparently, selecting the more appropriate location for their NetApps among all available ones depending on their necessities. To achieve that, both sites' Control Planes are connected via Openslice, as it acts as the OSS/BSS of their NFVO. In this way, Openslice is the entity in charge of managing and requesting the NFV instantiations, whereas OSM / OSDM are the entities that request their respective VIMs to deploy them. Furthermore, Openslice also guarantees the required QoS (both network and instances) and the proper functioning of the deployed instances thanks to the use of NEST and the test included on the triplets, respectively.

To access Openslice, it is reached by a public IP address through which it is exposed to customers; also, it communicates with OSDM using a VPN, as it's not needed nor recommended to expose publicly the NFVO. As Openslice is deployed on the Spain Site, it is not needed to use any mechanism to reach its OSM, but if Openslice is deployed elsewhere, another VPN tunnel would be needed. In fact, OpenSlice is candidate to be deployed in commercial cloud services.

Once Openslice starts a deployment process, it communicates with the NFVO involved and requests the deployment. From this point on, the process follows the same pattern as regular NFV deployments: NFVO asks its VIM to deploy the instances defined on the selected descriptors, and once they are deployed, the NFVO indicates if everything has been properly performed. This process is shown in figure 2.

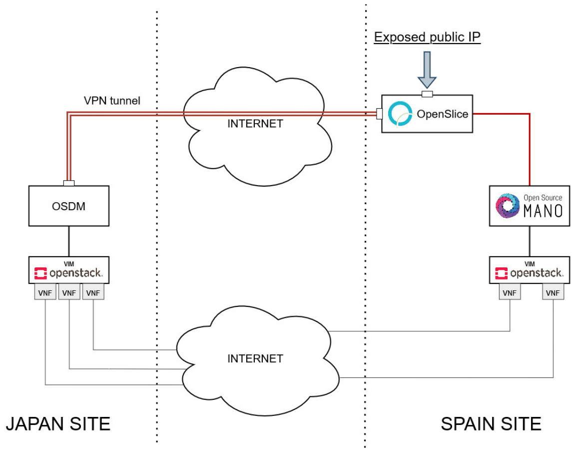

Fig. 2. Interconnection between the NFVOs of Japan and Spain sites using Openslice

One of the main advantages of this approach is not only offering the option of choosing the most appropriate location for the NetApp, but also the ability to even split the NetApp into pieces, deploying each of them in a different site, exploiting the advantages of the MEC paradigm. For example, some parts near a Data Center and other ones in a completely different place located thousands of km away, but in a transparent way and with no concern about the subjacent characteristics nor having to manually deploy the NetApp in two different locations. In this way, developers do not need to be aware of and consider the interconnection between each component, also simplifying the process since everything is presented to them as a single domain abstraction.

B. Interconnection of dataplane using NetOr

As mentioned in section III-D, one of the main problems with dynamical deployments in multi-domain testbed platforms is the interconnection between internal networks, as they are fully isolated and therefore disconnected. NetOr solves this issue as it can offer a flexible way to interconnect two different private networks. This simplifies multi-domain deployments, as it allows that two (or more) machines located in different places can communicate in a transparent way using only their private network, therefore acting as if they were actually connected to the same network segment. To achieve this, NetOr automatically deploys two (or more) wireguard peers, establishes a tunnel between them, and configures them to forward the received traffic to the other peer. Thus, the instances deployed on the private network located in the UMU Spain site can communicate with the ones deployed in NICT Japan site across the deployed wireguard tunnel, in a completely transparent way.

In this way, different parts of the NetApp can be located in different locations, and yet they run in exactly the same way as if they were directly connected. This, therefore, also simplifies both the deployment and development process, as there's no need to plan every site's network and how they will connect.

Regarding the location of NetOr over the infrastructure, it is not relevant nor critical since, as with Openslice, it does not matter where it's deployed if it can communicate with both NFVOs. Similarly to OpenSlice this component could be easily deployed on commercial cloud services, to exemplify that this deployment's NetOr is located on ITAv's site

The detailed process to deploy the tunnels is as follows: firstly, NetOr orchestrates the deployment of the wireguard peers in those networks that need to be interconnected, using for that purpose the NFVOs involved (that is, the ones in charge of the involved infrastructures). This process is automatic and consists of the deployment and configuration of the peers, which establish a wireguard tunnel (or a mesh, if required, although in this example we only work with two sites and therefore is a tunnel). Once this is performed, and the internal networks are interconnected, the NetApps are deployed on-demand over those networks, using the wireguard tunnels to communicate between them if they're located in different private networks. In figure 3 this deployment is shown.

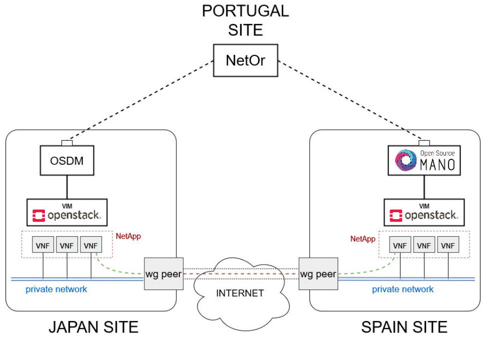

Fig. 3. Interconnection of both private network dataplanes using NetOr's wg peers

V. Conclusion

Next-generation networks, lead by 5G heavily relying on NFV, have overcome the historical networks limitations regarding flexibility and the need to acquire and deploy expensive equipment to keep up the pace of technology. SMEs and network service developers adapting to the expectations generated by newer technologies need also to adapt to environments where multiple administrative and geographically distributed domains may be involved. In that line, this work introduces the work done towards the realization and evaluation of an architecture that aims at simplifying the development and more importantly validation of network applications (NetApps) affecting multiple sites.

Even though the adoption of OpenSlice together with NetOr provides with a centralized point to manage the two testbeds involved is a great step forward for the developers and SMEs, there is still place for improvement. Site dataplane connectivity via NetOr might be dynamically deployed in a zero-touch approach simplifying the onboarding process and reducing the OpEx. Also in line with zero-touch and the proposal from ETSI ZSM, each administrative domain can enhance their intelligence on the orchestration, in particular, NICT is planning to employ ARCA[17] while UMU would rely on the Security Orchestrator[18] to adopt policy based security network orchestration. Indeed, ARCA and Security Orchestrator would address different aspects of intelligent orchestration and could therefore be used all together.

This paper, the proposed architecture and the deployment described alongside with the NetApp concept are envisioned as key features for the deployment of end-to-end network services on top of 5G.

REFERENCES

[1] "Test measurement and kpis validation working group, "basic testing guide, a starter kit for basic 5g kpis verification," 5GPPP, Tech. Rep., 2021. [Online]. Available: https://doi.org/10.5281/zenodo.5704519

[2] "H2020 5gasp," 2021. [Online]. Available: https://www.5gasp.eu/

[3] J. Gallego-Madrid, R. Sanchez-Iborra, P. M. Ruiz, and A. F. Skarmeta, "Machine learning-based zero-touch network and service management: a survey," *Digital Communications and Networks*, vol. 8, no. 2, pp. 105–123, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864821000614

[4] "Architecture working group, view on 5g architecture," 5GPPP, Tech. Rep., 2021, accessed: 2022-04-28. [Online]. Available: https://doi.org/10.5281/zenodo.5155657

[5] 3GPP, "Ts 128.530," accessed: 2022-04-28. [Online]. Available: \url{https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/16.02.00_60\/ts_128530v160200p.pdf}

[6] "Gsma generic network slice template, version 5.0," accessed: 2022-04-28. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.116-v5.0-7.pdf

[7] C. Tranoris, "Openslice: An opensource OSS for delivering network slice as a service," *CoRR*, vol. abs/2102.03290, 2021. [Online]. Available: https://arxiv.org/abs/2102.03290

[8] "Etsi open source mano." [Online]. Available: https://osm.etsi.org

[9] "Tmf 909a – network as a service (naas) api component suite profile," TMForum, Tech. Rep., 2019.

[10] "Gs nfv-sol 005 - v2.6.1 - network functions virtualization (nfv) release 2; protocols and data models; restful protocols specification for the os-ma-nfvo reference point," ETSI, Tech. Rep., 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/005/02.06.01_60/gs_nfv-sol005v020601p.pdf

[11] "Gs nfv-ifa 031 - network functions virtualisation (nfv) release 3; management and orchestration; requirements and interfaces specification for management of nfv-mano," ETSI, Tech. Rep., 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/031/03.03.01_60/gs_NFV-IFA031v030301p.pdf

[12] "Management and orchestration; 5g network resource model (nrm); stage 2 and stage 3 (3gpp ts 28.541 version 15.0.1 release 15)," 3GPP, Tech. Rep., 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_TS/128500_128599/128541/15.00.01_60/ts_128541v150001p.pdf

[13] "Gs nfv-sol 006 - v3.3.1 - network functions virtualisation (nfv) release 3; protocols and data models; nfv descriptors based on yang specification," ETSI, Tech. Rep., 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/006/03.03.01_60/gs_NFV-SOL006v030301p.pdf

[14] "Management and orchestration; concepts, use cases and requirements (3gpp ts 28.530 version 15.0.0 release 15)," 3GPP, Tech. Rep., 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/15.00.00_60/ts_128530v150000p.pdf

[15] "Management and orchestration; provisioning (3gpp ts 28.531 version 15.0.0 release 15)," 3GPP, Tech. Rep., 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/128500_128599/128531/15.00.00_60/ts_128531v150000p.pdf

[16] "Tr 28.801-v15.1.0-study on management and orchestration of network slicing for next generation networks." [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3091

[17] P. Martinez-Julia and S. Homma, "Intelligent Reasoning on External Events for Network Management," Internet Engineering Task Force, Internet-Draft draft-pedro-nmrg-intelligent-reasoning-01, Mar. 2020, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-pedro-nmrg-intelligent-reasoning-01

[18] A. Molina Zarca, M. Bagaa, J. Bernal Bernabe, T. Taleb, and A. F. Skarmeta, "Semantic-aware security orchestration in sdn/nfv-enabled iot systems," *Sensors*, vol. 20, no. 13, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/13/3622