IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 10, 2021, accepted September 19, 2021, date of publication September 22, 2021,
date of current version September 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3114645

Enhancing a 5G Network Slicing Management Model to Improve the Support of Mobile Virtual Network Operators

ANDRÉS CÁRDENAS[1], (Member, IEEE), DAVID FERNÁNDEZ[1], CARLOS M. LENTISCO[1], RICARDO FLORES MOYANO[2], (Member, IEEE), AND LUIS BELLIDO[1]

[1]Departamento de Ingenieriìa de Sistemas Telemaìticos, ETSI Telecomunicación, Universidad Politécnica de Madrid, 28040 Madrid, Spain
[2]Departamento de Ingeniería en Ciencias de la Computación, Universidad San Francisco de Quito, Quito 170901, Ecuador

Corresponding author: Andrés Cárdenas (andres.cardenasc@alumnos.upm.es)

This work was supported in part by Spanish Ministry of Science and Innovation through the ECTICS Project PID2019–105257RB-C21, in part by Spanish Ministry of Science, Innovation, and Universities through the Go2Edge Project RED2018–102585-T, and in part by the Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), Ecuador, through a Scholarship Program under Contract CZ03–000415–2018. The work of Andrés Cárdenas was supported in part by the Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), Ecuador, through the "Convocatoria Abierta 2018" Scholarship Program under Contract CZ03–000415-2018, and in part by Huawei-UPM 5G Chair.

ABSTRACT Network slicing is a key element in 5G networks. It allows a mobile network operator (MNO) to offer multiple logical networks tailored to the requirements of different industry verticals over a shared infrastructure. From the point of view of an MNO, a mobile virtual network operator (MVNO) is a particular type of vertical network requiring not only the provision of logical networks with specific infrastructure resources but also customized management capabilities to allow the MVNO to offer network slice-based services to its clients over the infrastructure of multiple MNOs. However, the lack of flexibility to provide a customized and efficient network slice management system per tenant under the current proposals of the 3rd Generation Partnership Project (3GPP) and European Telecommunications Standards Institute (ETSI) limits the possibilities of MVNOs. This paper addresses this requirement by proposing a novel virtualized multidomain and multiclient orchestration system aligned with the functionalities of the network slicing management framework proposed by the 3GPP and ETSI. In particular, there are three contributions of this paper: (i) an extended service-based architecture is designed to provide an isolated management system to different MVNOs; (ii) a novel high-level slice instance template is defined to specify management and isolation requirements supporting network slicing as a service model; and (iii) finally, a teleoperated driving use case is described to showcase how our proposal provides an MVNO with an independent management system to orchestrate several network slices in cross-domain environments.

INDEX TERMS 5G, multiaccess edge computing, network slicing, network function virtualization, software-defined networks, virtualized network function orchestration.

I. INTRODUCTION

Mobile network operators (MNOs) are evolving their network infrastructure to profit from the advantages of network function virtualization (NFV) technologies. Specifically, NFV facilitates the agile deployment of innovative network services that cope with the requirements of different types of applications and the specific needs of industry verticals. These specialized industry verticals, often simply called *verticals*, are very diverse in their nature and the characteristics of the network services they demand from operators. To satisfy that demand, MNOs must be provided with the appropriate management and orchestration capabilities to properly use their physical and virtual resources to fulfill the network service requirements of all users in terms of security policies, isolation, reliability, bandwidth, and delay.

In this context, the 3rd Generation Partnership Project (3GPP) and the International Telecommunication

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

Union (ITU) have classified the services offered by 5G networks into three general groups: enhanced mobile broadband (eMBB), for services requiring high data rates (e.g., 3D video); massive machine type communications (mMTC), for environments with high device densities requiring low data rates; and ultrareliable low-latency communications (URLLC), for advanced latency-sensitive services, such as automotive use cases [1].

To offer and manage the network services that handle these use cases, MNOs incorporate the network slicing concept. A network slice is a logical network that provides specific network capabilities and network characteristics [2]. Each specific network slice is named a network slice instance (NSI). An NSI comprises different sets of network resources (physical or virtual) that may be distributed over several network segments. The set of resources of an NSI on each network segment is named a network slice subnet instance (NSSI) [3] and [4].

Creating a network slice involves the dynamic end-to-end management of resources in different technological domains such as access and transport networks and edge/cloud infrastructures. For that purpose, network slicing in 5G networks extensively uses software-based enabling technologies such as NFV, software-defined networks (SDNs), and edge/cloud computing [5].

In this light, the 3GPP has defined a network slicing management model that includes management functions to control NSIs and NSSIs [3]. Similarly, the European Telecommunications Standards Institute (ETSI) has proposed a network slice management framework based on NFV management and orchestration (MANO) systems [6]. Both system models must be combined to ensure an end-to-end (E2E) orchestration of the resources assigned to a network slice [7].

This approach allows MNOs to offer their network infrastructure to third parties, e.g., verticals, following the network slice as a service (NSaaS) paradigm [8]. NSaaS allows a vertical to define its network requirements as a service-level agreement (SLA) using a template that is later translated into the network resources needed to create a network slice that provides such service.

An interesting use case scenario of the NSaaS approach is mobile virtual network operators (MVNOs), which are mobile network operators whose infrastructure is composed of network slices obtained from MNOs. MVNOs use those resources to provide network services to their customers, playing the role of an MNO for them [9].

To accomplish their tasks, MVNOs must have the autonomy to define and manage the network service policies currently running on their allocated network slices [10]. Solution frameworks for providing and managing MVNOs must guarantee isolation among network slices and ensure a sufficient level of management capabilities for an MVNO to orchestrate its network slices.

However, the provision of logical networks with flexible and customized management systems is not yet fully considered by the 3GPP. For example, a vertical could only require a part of the functionalities provided by the MNO management system to orchestrate its slice, such as telemetry, automation services, controllers for service orchestration on computing domains, or controllers for transport and radio network services side. This lack of mechanisms to provide a customized management stack per tenant limits the flexibility needed to offer what MVNOs need.

Another critical aspect is the response time of the management procedures performed over the network slices, mainly when the management platforms are deployed far from the services and resources. For example, management systems are usually deployed in the network cores of MNOs. Therefore, actions performed on virtualized services such as scaling, migration decisions, reconfiguration, or topological changes could lead to high latencies, depending on the distance and capacities involved. This could be a problem for verticals that provide sensitive real-time services that require low latencies at the network and management level. Besides, the time involved in analyzing the service performance analytics during the runtime of network services also impacts the constraints defined in SLAs.

Therefore, the current network slice management model must be extended to consider the particular management needs of verticals such as MVNOs.

The present work proposes extending the network slicing system model defined by the 3GPP to provide MVNOs with network slicing management capabilities similar to those available for MNOs based on the NSaaS concept. A first approach to these extensions was introduced in [11]. This paper completes and extends the previous work with the following contributions:

- A new service-based architecture is proposed to provide independent network slice orchestration systems per vertical direction. This architecture is described using service-based components and an object-oriented information model. Besides, it addresses the challenges of decentralizing E2E network slice orchestration over multidomain and multitenant environments.
- An extension to the high-level slice instance template is defined to allow MVNOs to specify slice management capability requirements.
- An MVNO use case is described to validate the proposals and discuss the benefits of providing independent network slice management systems in cross-domain environments.

The remainder of the paper is structured as follows. Section II analyzes the related work and maps the contributions of the proposed approach to the state-of-the-art gaps. Section III expands some background concepts on which the proposal is based. Section IV describes the extensions of the proposed network slicing management model. Section IV also presents the implementation principles of the proposed system model, paying attention to the internal service components of management functions and the MVNO information model. Section V presents the use case regarding a teleoperated driving service in vehicular cloud networks, which is

used to validate and show the approach's benefits. Finally, Section VI summarizes the paper's conclusions and presents open challenges and future lines of work.

II. RELATED WORK

This section presents a detailed review of works related to the provision and management of network slicing and identifies the lack of mechanisms for providing management systems with a sufficient level of independence.

A. 5G NETWORK SLICING

As previously stated, 5G network slicing allows MNOs to create and manage different types of network slices with specific management and performance capabilities over a shared network infrastructure [12] and [13]. For example, network slices for time-sensitive applications require the deployment of 5G network functions close to the users that require ultralow latency and high availability [14]. Similarly, network slices for multimedia streaming require high bandwidth capabilities, mobility support, and the deployment of content delivery network (CDN) resources [15].

In this light, to offer NSaaS to clients, MNOs must include 5G network function catalogs and SDN/NFV management technologies in their platforms to provide scalable and secure cross-domain slice orchestration, as detailed in [16]. In this context, in [17] and [18], architectures for a 5G operating system based on functional hierarchical controller and orchestrator domains were proposed. These architectures define functional service and resource management blocks in which all performance, QoS, and SLA parameters are monitored and secured. However, they create a single point of failure problem in the management system.

B. END-TO-END SLICE MANAGEMENT

Providing E2E network slices that extend across multiple administrative domains with customized management requirements adds considerable complexity to 5G network infrastructures based on software [19]. E2E slice management requires coordinating network and cloud resources, network functions, and services in a multidomain scenario [20]. In this regard, an attractive ontology-based information model for network slice management, as well as a platform that orchestrates resources and services to meet the requirements of each network slice scenario, is proposed in [21]. In [22], a flexible and programmable architecture for 5G mobile networks was defined. This architecture, aligned with the 3GPP and ETSI standards, facilitates the provision of network slices with specific functionalities. However, the slice lifecycle management system remains centralized.

In [23], an IoT slice orchestrator that expands over edge and cloud computing domains is proposed. In the same way, in [24], a CDN slice orchestrator using the CDN as-a-service paradigm is defined. The work presents an architecture supporting video-on-demand streaming services. However, neither proposal is aligned with the 3GPP management framework. Furthermore, considering the diversity of use cases that a 5G platform must support, in [25], a component that allows verticals to define services on top of network services based on blueprints is defined. Finally, based on the context of network slices for multiple verticals, [26] extends the concept of the MANO framework and defines a new orchestration paradigm, MANOaaS, which provides each tenant with a MANO stack deployed as individual management components. This management approach reduces end-to-end slice control complexity at the orchestrator level, minimizing the need to add new features to orchestration systems. However, that proposal does not consider the slice management functions defined by the 3GPP.

Similarly, the work in [27] elaborates on how the proposals described in [26] address the challenges of provisioning network slice instances that support multiple use cases at the vertical level. Both works focus on providing network slices, but in [27], the authors integrate the 3GPP network slicing management system into the orchestration architecture. For that purpose, the concepts of use case-specific network slice instances and generic network slice instances (representing a bundle of subnetwork slices) are proposed to fulfill the performance requirements of each vertical use case. The main contribution comes from the flexibility added to the provision of network slice instances according to the vertical requirements. However, the method neither covers the system overload, performance, and isolation issues in a shared platform nor addresses the latency requirements at the management level. Besides, the method does not consider what strategy to follow when the centralized management system fails. The work presented in this paper addresses those questions by offering a slice instance template with novel management parameters to provide a customized management system per vertical.

C. SLICE-ENABLED MEC

Network slicing can benefit from using resources deployed at the edge of the network close to the users by exploiting the multiaccess edge computing (MEC) concept [28]. MEC brings the computing resources, previously centralized in large data centers, to the network's edge. MEC and NFV specifications have been developed separately. Nevertheless, since the management frameworks for MEC applications and virtual network functions (VNFs) share several similarities, the ETSI has begun to address combining both frameworks into a unified architecture. For example, [29] proposes deploying the management elements of the MEC framework as VNFs in an ETSI NFV-MANO system [30].

Although proposals by the 3GPP [31], ETSI [32], and others [33], [34] define how the MEC system can be integrated within the 5G architecture, the inclusion of NFV-based MEC systems as a functional part of 5G networks has yet to be fully addressed.

Moreover, in [35], a slice-enabled MEC management architecture deployed in 5G networks is proposed. Despite describing the different methods of communication between the MEC system and 5G network functions, the proposal

does not include an NFV-MANO framework where MEC and 5G network functions are orchestrated. In [36], an integration of MEC into the 5G network slicing context is defined. The proposed architecture uses the NFV-MANO platform to deploy MEC-enabled slice services and incorporates stand-alone and shared deployment scenarios of MEC components for each slice. However, the work does not consider orchestration in cross-domain environments. Similarly, other works [37]–[40] have defined MEC implementations that integrate EPC (evolved packet core) functions in NFV-MANO environments. Nonetheless, the management and orchestration procedures in the 3GPP network slicing context are not described.

D. CONTRIBUTIONS

The proposals reviewed thus far do not cover all the challenges for providing customized and independent NSaaS lifecycle management systems to verticals, mainly due to the difficulty of handling the heterogeneity among different technologies and standardization bodies. In this light, different unresolved issues have been identified at the network slice management level. Thus, there is a lack of standardized mechanisms and definitions to allow:

- R#1: agile provision of decentralized network slice orchestration systems for verticals with a high level of independence in NSaaS scenarios.
- R#2: agile provision of logical resources in multitenancy and cross-domain environments, integrating ETSI NFV-MANO, ETSI MEC, and 3GPP network slice management systems in a common framework.
- R#3: orchestration of fully decentralized management systems with a unified information model to ensure the orchestration of cross-domain network slices.

Our proposal addresses the gaps detailed above following a top-down approach through the following strategies:

- For R#1, an extension to the service-based network slice management architecture based on the network slice management model proposed by the 3GPP is defined in Section IV-A [3]. It abstracts the main management functions to provide an isolated orchestration system to each vertical. Furthermore, it adds a new service component to streamline the discovery and exposure of services between orchestration platforms.
- For R#2, an extended slice template including isolation levels for network slice management is defined in Section IV-B. The Generic Network Slice Template (GST) and the NEtwork Slice Type (NEST) template proposed by GSMA (Global System for Mobile Communications) in PRD NG.116 [41] allow fulfilling service level agreements to be satisfied by a network slice. The proposed template includes new fields that describe management capabilities at the service orchestration layer.
- For R#3, the service components and an object-oriented information model of the decentralized architecture are defined in Section IV-C and Section IV-E, respectively. Since the 3GPP and ETSI NFV-MANO information models focus on a single centralized management system, the proposed information model includes data information concepts related to the extensions described in this work.

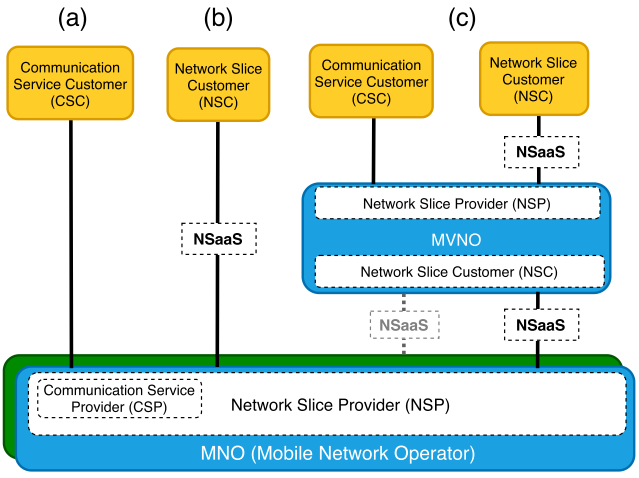

FIGURE 1. High-level model of roles and network slicing management.

III. BACKGROUND CONCEPTS

A. ROLES INVOLVED IN NETWORK SLICING

In the context of 5G network slice management and orchestration, it is crucial to clearly define the roles and responsibilities of the different stakeholders involved. Figure 1 illustrates the roles related to 5G network slicing management and provision, following the principles described in [42]. Considering common network slicing scenarios, the MNO simultaneously plays the role of a communication service provider (CSP) and network operator (NOP). The MNO provides communication service to its network slice customers (e.g., end-users, verticals, and enterprises), which may be unaware or aware of the network slice. In the former case, named *network slices as NOP internals* in [42], the network slice customers act as communication service customers (CSCs) and only consume the services provided by the CSC as end-users (Fig. 1a).

In the latter, named *network slice as a service* in [42], the network slice customers are aware of the instantiated network services. They can modify and update their network functions via the management exposure interface (Fig. 1b).

Furthermore, when using NSaaS, verticals that require full network slice management capabilities such as MVNOs can offer their network slices to their customers. In this case, they act as a network slice customer (NSC) down to the MNO, but they behave as network slice providers (NSPs) up to their customers (Fig. 1c). As previously described, customers can be aware or non-aware of the network slice.

Besides, MVNOs can enhance the network slice capabilities obtained from the MNO by adding their network functions or combining network slices from several MNOs.

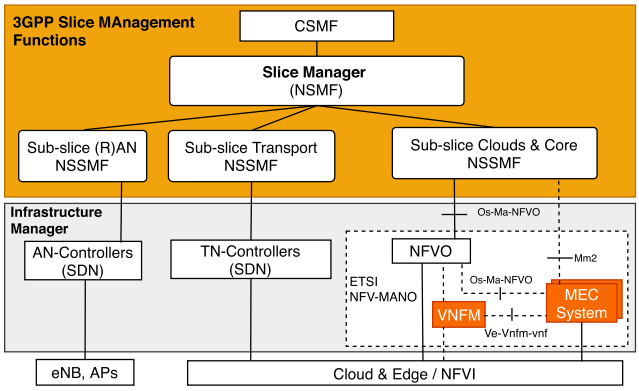

FIGURE 2. High-level E2E network slicing management architecture. mapping 3GPP management functions with ETSI NFV-framework.

B. 3GPP NETWORK SLICE MANAGEMENT MODEL

The 3GPP has defined a network slice management architecture composed of several functions for managing network slice instances and the corresponding subnets [3], as shown in Fig. 2.

The description of a network slice includes a set of attribute-value pairs that specify the service requirements defined as part of service-level agreements. The permitted attributes are described in the GST specified by GSMA [41]. These parameters are detailed in the NEST file, which is a filled GST with the values and attributes associated with the service-level agreement of a network slice, such as the slice coverage, the isolation level, or traffic characteristics.

The communication service management function (CSMF) is responsible for translating the service requirements in the NEST chosen by customers into the service profile: the set of logical network functions and resources interconnected following a specific topology needed to instantiate a network slice. the CSMF is the point of contact between customers and the 5G system management platforms provided by MNOs.

Once the service profile is created after processing the NEST file, the CSMF sends it to the network slice management function (NSMF) through a REST-API. The NSMF uses the service profile to create the NSIs, build its logical topology, and deploy essential network functions.

First, the NSMF divides the service profile file into the subnet descriptors that compose the network slice, sending each one to the corresponding network slice subnet management function (NSSMF), which manages the different network segments (access, transport, and cloud). Once the NSI is instantiated, the NSMF remains responsible for the management and operation of its lifecycle.

The information received by NSSMFs from the NSMF includes the description of the network functions required to create the NSSI to be instantiated and managed in each network segment. In access and transport networks, NSSMFs communicate with the controllers responsible for dynamic resource allocation and configuration, ensuring traffic isolation, applying QoS policies, and controlling the state of base stations and network elements. For example, the radio controller in charge of managing wireless access devices and the transport network controller focused on wide-area network elements will establish flow rules according to the resource availability and network slice requirements provided by the NSSMFs. Besides, the NSSMF that controls the cloud domains uses network service descriptors (NSDs) sent by the NSMF to deploy the network service composed of VNFs over the targeted NFV infrastructure (NFVI) domains. These descriptors will be onboarded to the corresponding NFV orchestrator (NFVO) to be later instantiated. The NSSMF should be able to differentiate between types of network functions (NFs), i.e., VNFs, physical network functions (PNFs), and MEC applications (MEC apps). The way MEC apps are deployed will depend on how NFV and MEC platforms are instantiated: through a specific interface if an NFV-based MEC system is used [29] or through a different NSSMF if a stand-alone MEC system is used.

Finally, in some cases, the radio, transport, cloud, and 5G core network (5GCN) controllers could act as NSSMFs and are part of the management system. In other cases, they could be external components, and the NSSMFs will play the role of clients that interact with those controllers (see Fig. 6).

IV. EXTENDED NETWORK SLICE MANAGEMENT ARCHITECTURE

In this section, the design principles of our proposal are detailed. Specifically, in Section IV-A, the extended architecture of the 3GPP network slice management model is described. In Section IV-B, an extended high-level slice template to be used by the MNO is defined. Section IV-C details the service components of each management function. Finally, in Sections IV-D and IV-E, the multidomain scenarios and orchestration information model are described.

A. PROPOSED SLICE MANAGEMENT MODEL

The network slice management model proposed in this paper extends the model defined by the 3GPP [3] described in the previous section. The key objective of the model is to instantiate slices as a service with a set of network, computing, and infrastructure resources where network services related to the network slice are deployed and operated with independent management functions. The network function requirements must be mapped to the infrastructure resources assigned to the network slice. This novel model is based on enabling extended customized management functionalities. Fig. 3 illustrates the extension proposed to the management model described by the 3GPP in [3]. An MNO (right side) provides independent network slice management functions to verticals (left side), requiring an NSaaS with isolated infrastructure and network service resources. Each management function (CSMF, NSMF, and NSSMF) manages the different layers that compose a network slice, such as the communication service, network slice, and network slice subnet. A simplified view of the model is described below.

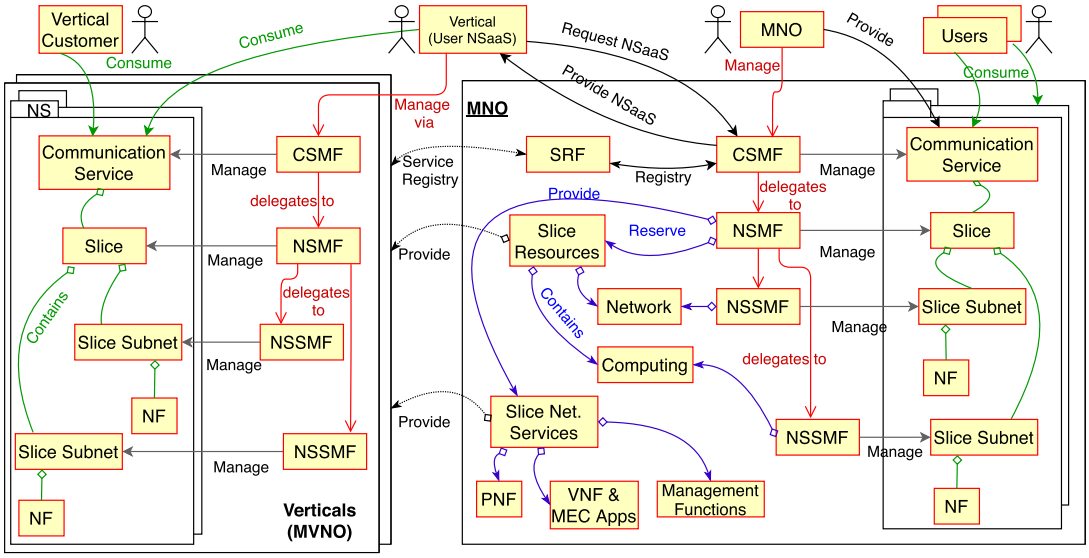

FIGURE 3. Provider-driven 5G network slice as a service management model.

The main idea of the model is to abstract and virtualize the 3GPP network slice management functions, henceforth called the slice management function (SMF) stack. The main goal of the model is to offer advanced management capabilities to MVNOs by providing each MVNO with its own SMF stack, hereinafter referred to as the MVNO SMF stack.

An MVNO SMF stack provides MVNO independence and flexibility to manage and orchestrate the network slice resources offered by the MNO through NSaaS. It also provides the autonomy to add new service packages and apply communication policies to their end-consumers. The central SMF stack manages the lifecycle (activation, configuration, scaling, migration, and decommissioning) of each MVNO SMF stack. Moreover, if the MVNO SMF stack experiences a failure, the MNO SMF stack keeps track of the lifecycle management over the services deployed by the MVNO. Depending on the isolation levels and management requirements defined by the vertical (described in Section IV-B), the central SMF stack will provide more or fewer control capabilities to the MVNO over network resources and orchestration systems.

Fig. 4 shows the proposed service-based model for the provision of an MVNO in the form of NSaaS. This management method is aligned with the information model defined by the 3GPP in TS 28.530 [42]. The figure includes a sequence of steps for creating, instantiating, and operating an MVNO slice.

First, the MVNO requests the creation of a network slice using the MNO NSaaS interface (step 1). For that purpose, it creates a NEST file with the service requirements, including the request for an MVNO SMF stack creation (step 2). The NEST is processed and translated into the resources needed to create the network slice (step 3). Besides, the MNO provider deploys the new MVNO SMF stack, typically as a standard NFV network service (NS) at the location specified by the MVNO according to its latency constraints and security factors (step 4). Next, the administrative operations of the central SMF stack on the MVNO SMF stack are performed employing the "associate" procedure via the Inter-SMF stack service-based bus communication interface (step 5).

The new MVNO SMF stack also enables external consumers to design and deploy their communication services by providing their catalogs and repositories of network services and network functions (step 6).

Finally, over-the-top service providers can leverage the MVNO SMF stack to deploy custom services without involving the central SMF stack. In this case, the over-the-top service providers can define specific performance parameters (e.g., latency, traffic data flow, number of users, and service performance) to their NSDs to ensure the policies of their services over the sliced infrastructure (step 7).

The following provides more details about the two main building blocks of the architecture:

1) MNO-PROVIDER

The MNO-Provider comprises the central SMF stack that defines access levels and rights access over the sliced network infrastructure and provides operational capabilities to the MVNO SMF stacks. Besides, it monitors and enables the MVNO SMF stack to perform lifecycle management actions within the boundaries established in the isolation and service agreements.

To allow any MVNO SMF stack to register, discover and consume additional services (e.g., automation models, VNF's testing and validation, and NFVIs) and resources (e.g., adding computing nodes, CPU, and RAM) from those initially provided by the central SMF stack, the SMF stack register function (SRF) is proposed as a new component of the SMF stack.

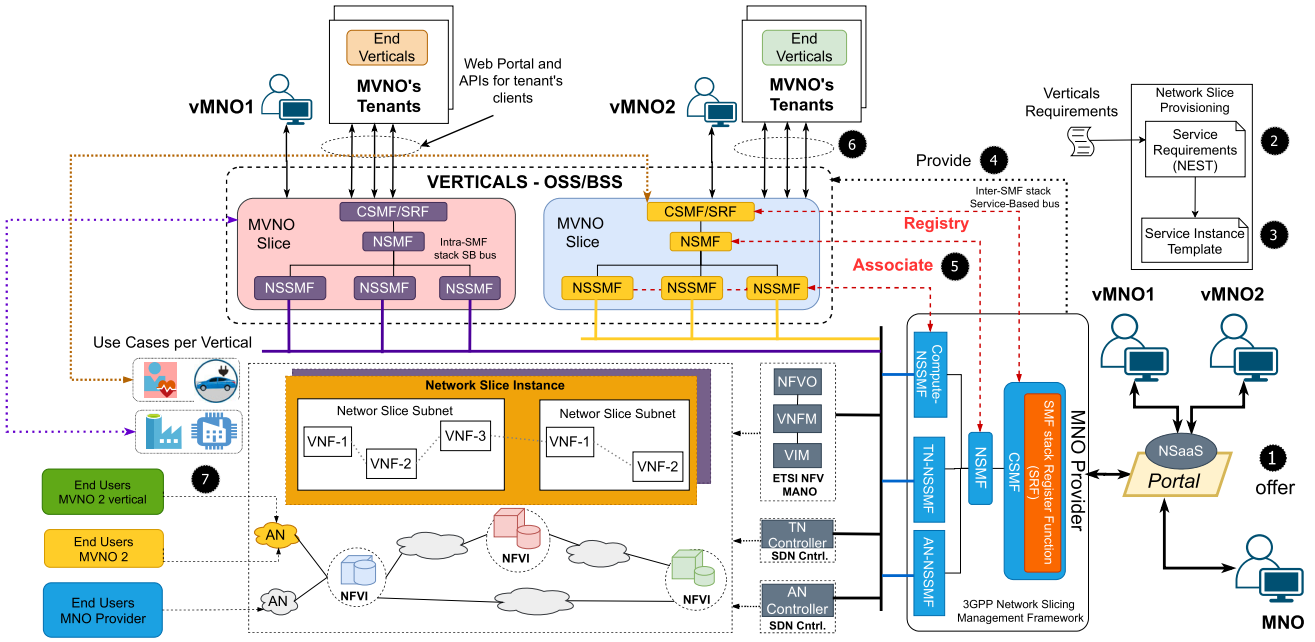

FIGURE 4. MVNO slice management system model. Extended 3GPP SMF stack to provide NSaaS to end customers.

In addition, the SRF can be used to register and discover SMF stacks and resources from other MNOs, for example, for reserving resources when a network slice requires cross-domain communication (see Section V-A).

Furthermore, the MNO-Provider could be employed as a new management function over the 3GPP management model or integrated as part of the CSMF. Once the MVNO SMF stack has been registered into the SRF, every management function from each SMF stack can communicate with each other to request particular functionalities, such as requesting network slice templates or network service descriptors.

TABLE 1. Differences between existing and extended 3GPP network slicing management model based on vertical service requirements.

Vertical Service Requirements	3GPP Management Model	Extended 3GPP Management Model
Multidomain Support	✓	✓
Multitenancy Support	✓	✓
Cross-Domain Management System Level Cooperation	✓ (based on roaming)	✓ (based on owned NsaaS)
Service Continuity Support	✓	✓
Decentralized Management System	x	✓
Management System per Vertical	x	✓
Low Latency Management System Support	x	✓
Customized Management System (Adapted to vertical performance needs)	x	✓
Multivendor flexibility	✓	✓
Service/Resource Management System Registry and Discovery	x	✓
Flexibility to select MANO systems (Independent or shared)	x	✓

2) MVNO-SLICE

Once an MVNO SMF stack is deployed and configured, it has full autonomy to orchestrate its own physical and virtual resources without the intervention of the central SMF stack. The MVNO SMF stack behaves as the central SMF stack, allowing the implementation of security rules, policies, and lifecycle operations over their network instances. Furthermore, the MVNO SMF stack can build its network services and offer them to external customers by onboarding and deploying slice templates. The central SMF stack supervises that new instantiated services do not incur SLA violations.

An MVNO SMF stack can also control and consume resources from other network providers through the communication between the SRFs of each SMF stack to add new technology domains to its slice resources. Finally, the communication between the NSMF and NSSMF entities within each SMF stack occurs through an intra-SMF stack service-based bus interface.

Table 1 summarizes the main functional differences between the existing 3GPP network slicing management model and the model proposed in this work. The comparison is conducted based on the vertical service requirements. It highlights the functional aspects that our system model supports when verticals require particular management systems adapted to the use cases they expect to instantiate over multidomain and cross-domain scenarios. The main characteristics described in Table 1 are explained in more detail in the following sections.

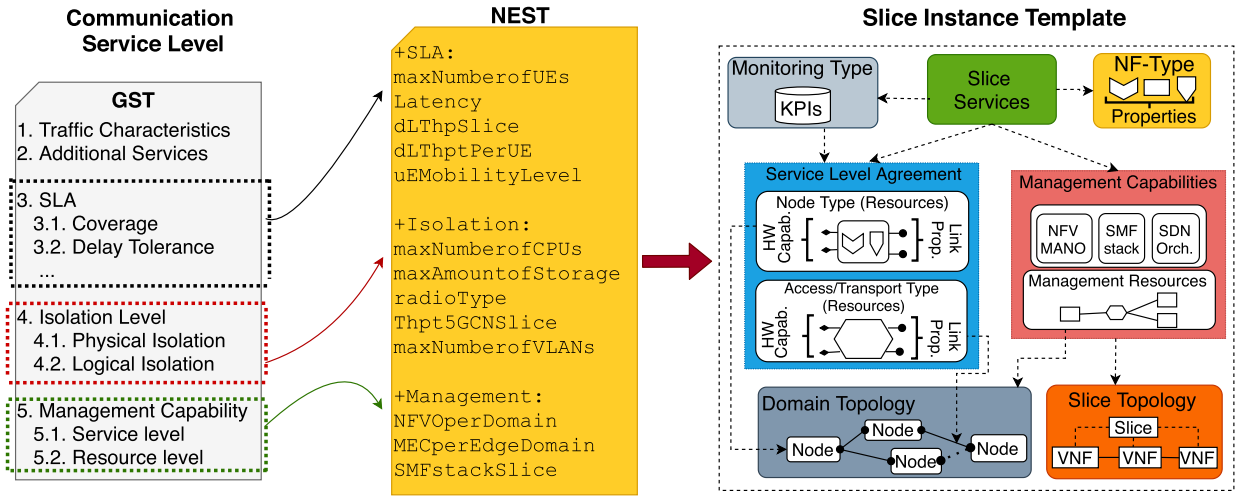

FIGURE 5. Example of the translation of vertical slice requirements to service descriptors.

B. MAPPING VERTICAL REQUIREMENTS TO NETWORK RESOURCES

As mentioned above, NEST files are the primary input used during the network slice preparation phase of NSaaS. They are translated into the corresponding blueprint called the service profile used to instantiate the network slice by selecting the appropriate logical resources and management attributes based on underlying infrastructure control needs [43]. Each service profile (e.g., smart home, e-health, and MVNO) imposes specific communication requirements (e.g., QoS and latency) through SLA attributes that need to be translated to hardware and virtual capabilities. All infrastructure resources, network functions (PNFs and VNFs), MEC apps, and management components must be registered in the operators' portfolios and repositories for their use during slice building.

Fig. 5 shows an example of translating verticals' service requirements, paying particular attention to isolation and management attributes (on the left) into service profile descriptors (on the right) from the top to bottom levels. Since the GST file already provides isolation level fields, they are extended by adding information fields related to the MVNO's management requirements. The isolation level attribute in the GST defines the physical and logical type of isolation. In the former case, network slices are separated by hardware (e.g., racks, servers, and location) and computational resources (e.g., storage and CPU). In the latter, network slices are isolated by virtual resources (e.g., virtual machines) and network functions (e.g., 5GCN).

At the management level, the new field allows verticals to select different types of management, as shown in Table 2. A specific SMF stack platform is instantiated only for the vertical if the *service level management* parameter is selected. In this case, the MVNO SMF stack will use MANO platforms shared with other tenants. Moreover, MVNO will control the network slice through the central SMF stack if a *resource-level management* parameter is selected. However, if both *service level management* and *resource level management* values are selected, independent MVNO SMF stack and MANO systems dedicated to the vertical (MVNO) are deployed (see Section IV-D). Finally, when the *no management* parameter is selected, the vertical will only have monitoring functionalities over the network slice.

The service profile derived from extended NEST translation is named the slice instance template (SIT). The SIT specifies the structure of the network slice instance in terms of domain types, types of network functions, domain topology, and management configurations (Fig. 5). Specifically, the SIT contains the following:

- NF-type. It maps several SLA parameters to define the network functions and MEC apps that compose a network slice. For example, computational (e.g., CPU, GPU, and TPU) and performance constraints (e.g., latency) impose whether the VNF is deployed as a virtual machine or as a container. The NF-type includes a field to specify if the NF is deployed as a VNF, PNF, or MEC app.
- Monitoring type. It includes fields that allow MVNO to specify isolated monitoring entities to collect data analytics to fulfill the key performance indicators (KPIs) from network services and NFVI domains.
- SLA. It represents the network slice performance and service parameter translation into hardware

TABLE 2. Management capabilities.

PARAMETERS	DESCRIPTION
Allowed Values	No Management Service Level Management Resource Level Management
Tags	Character attribute/Functional

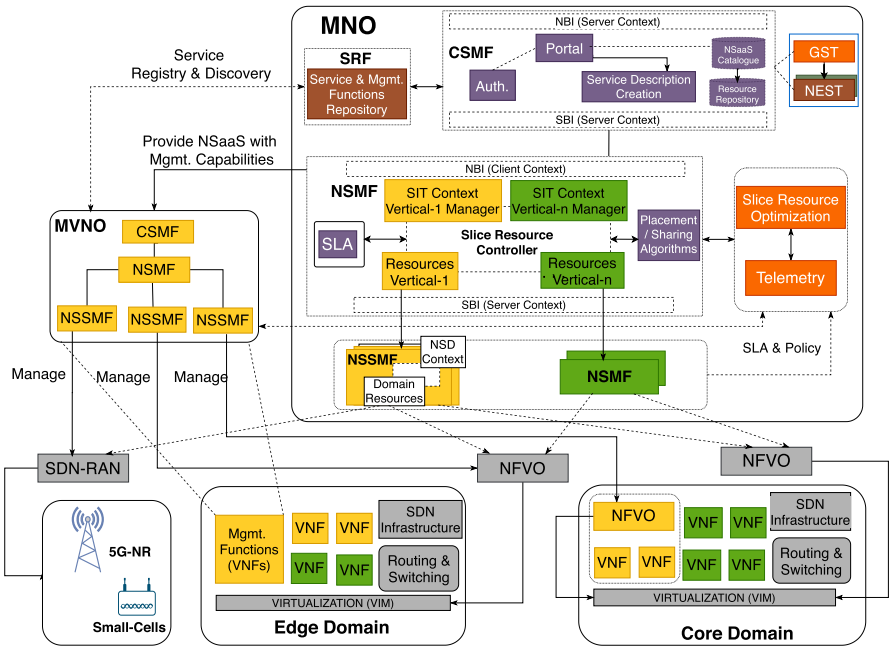

FIGURE 6. High-level MVNO slice service-based architecture.

characteristics based on physical (e.g., node) and link capability (e.g., port) information.

- Management Capabilities. They define the management systems required by a vertical to control the network slice mapped from the management parameters described in the GST as network service descriptors.
- Slice Topology. It maps the performance requirements of NSaaS into network services (e.g., 5GCN) comprised of chained network functions (e.g., vCPEs and MEC apps).
- Domain Topology. It maps the performance requirements in terms of availability and slice coverage that are represented as domain types (e.g., edge and cloud computing), access network types (e.g., WiFi and small cells), and transport network types (e.g., SDN and legacy-IP networks) [44]. Therefore, in this case, it is necessary to extend the information model of the VNF descriptors (VNFDs) and NSDs [45] by adding fields that define the NF-type (nf_typeID) and domain type (domainID) to select suitable network functions according to the domain type. For example, when the NF-type is an MEC app, the NSD must add the AppD_id field to link VNFs with MEC apps [46]. This approach allows instantiation of them on MEC systems in stand-alone or NFV-based mode.

At the network slice management level, the SIT is split into network service descriptors and SDN applications to instantiate the virtualized services over computational resources. By applying traffic flow rules over access, transport, and cloud networks, VNFs can be interconnected to provide E2E communication. At the infrastructure level, the service descriptors are translated into hardware characteristics to ensure the SLA and policy requirements per network slice.

C. SMF STACK SERVICE COMPONENTS

Fig. 6 shows a more detailed view of the SMF stack service components and their relationship with managed resources. Each management function (CSMF, NSMF, and NSSMFs) is composed of different service components that ensure the execution of the lifecycle management actions of the network slices. The core idea is to communicate the SMF stack functions through standardized APIs for the consumption and exposition of the relevant data of each slice. For example, the resource reservation procedure is performed via the client-server communication context. The idea is based on the network slicing vision proposed by the Open Networking Foundation (ONF) in the ONF TR-526 document, which was adopted by the ETSI in [6]. We adapt that vision to assign groups of resources to each vertical through the NSMF acting as a slice resource controller service. When an MVNO SMF stack is deployed, the MNO configures the management functions with the specific attributes to access only the assigned resource group. The management attributes refer to the endpoints and access URLs with authorization credentials for accessing the infrastructure managers in charge of controlling the network slice resources.

The communication between internal management functions is established through REST-API calls. For example, in a typical communication between a CSMF and an NSMF, the NSMF's northbound interface (NBI) takes the role of a client. In contrast, the CSMF's southbound interface (SBI) acts as a server, which gathers the isolated information requested by the vertical through the CSMF NBI.

Finally, as shown in Fig. 6, the CSMF acts as a front-end interface for the users to browse through the different

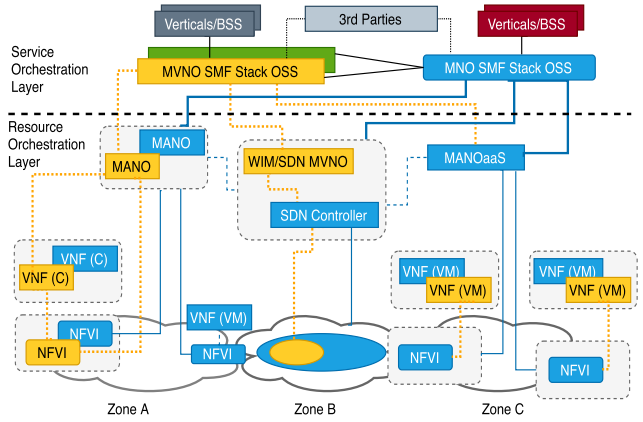

FIGURE 7. Example of MVNO slice information model.

network slice catalogs and blueprint repositories. It also implements translation, activation, and validation services. In turn, the NSMF implements planning, scheduling, optimization, and resource reservation procedures per slice to ensure multitenancy and multidomain paradigms. Furthermore, the NSMF is in charge of mapping the group of resources reserved with the specific NSSMFs to control and orchestrate the network services chained over multiple administrative domains. More precisely, it performs fault, configuration, accounting, performance, and security (FCAPS) operations and lifecycle management actions. Finally, the NSSMF integrates the resource broker service to interact with resource orchestration systems such as NFVOs, virtual infrastructure managers (VIMs), and SDNs to gather resource group information from the different technological domains by executing activation and configuration actions.

Note that the SMF stack, either MVNO or MNO, delegates VNF deployment to NFVOs. Nevertheless, the isolation requirement at the management and orchestration level will be provided in different ways depending on whether the MVNO uses an independent or a shared NFVO, always based on the service level requirements from the use cases (see Section IV-D).

Furthermore, the SMF stack and NFVO-MANO have different roles in controlling network services deployed over the network slice. NFVO handles the VNF lifecycle management that composes each NSSI deployed over NFVI domains. Conversely, the SMF stack has a high-level management view and performs different management procedures on the network services and network slice resources distributed over several domains. For example, the SMF stack can add more computing resources to the slice or trigger scaling methods for VNFs. The former procedure could be executed by interacting with VIMs through a specific NSSMF while the latter approach requires the SMF stack to send scaling actions to the NFVO through another NSSMF. The type of NSSMFs provided to any MVNO depends on the management and orchestration requirements described in the SIT file.

D. MULTIDOMAIN SCENARIOS

The proposed architecture provides an MVNO slice that crosses multiple domains with different controllers, SDN orchestrators, NFV-MANO, and NFVI providers. In this context, an MVNO can control the underlying network infrastructure through common orchestration platforms for all tenants (e.g., MANOaaS and MECaaS) or through deploying independent orchestration platforms. In the former case, the MVNO deploys services that do not require high-level security policies and low latency constraints within the system management and orchestration procedures. Therefore, the tenant's instantiation requests are queued based on instantiation priorities. Otherwise, the MVNO uses the latter case to fulfill those specific requirements. Therefore, this approach allows accomplishing the requirements of the services for both use cases.

In this light, there are two types of isolations at different levels, such as the network level (e.g., VNFs and PNFs), infrastructure management level (e.g., VIM), orchestration level (e.g., NFVOs and SDNs) and service level (e.g., SMF Stack), by having independent or shared resources and services. The options to be used should be chosen according to the management capabilities requested by the MVNO. The MVNO SMF stack has the flexibility to support both alternatives simultaneously.

As shown in Fig. 7, the E2E slice orchestration framework is divided into two layers following a bottom-up approach:

1) RESOURCE ORCHESTRATION LAYER

The resource orchestration layer comprises network infrastructure domains (e.g., NFVIs), network functions (e.g., VNFs and PNFs), MANO systems, and SDN controllers that control the traffic flow in the cloud, access, and transport networks. In this layer, the proposed architecture enables different types of isolation.

For example, as shown in Fig. 7, in zone A, the MVNO has a split NFVI domain controlled by an independent VIM-on-demand agent provided to the MVNO [47]. This NFVI is orchestrated through the NFV-MANO platform deployed exclusively for the MVNO. In this case, the MVNO has high-level management capabilities over the assigned resources. In zone B, the MVNO controls the dedicated infrastructure of transport networks with advanced isolation mechanisms by using an SDN controller that acts as a wide-area infrastructure manager (WIM) [48]. The management level in this zone depends on the WIM capabilities to allow multiple tenants to run on top.

Finally, the MVNO orchestrates the NFVI domains using a shared MANO platform (MANOaaS) for all the tenants in zone C. In this case, the management capabilities of the MVNO depend on the functionalities provided by the MANO system. For example, the differentiation between tenants in a shared NFVO is performed by creating independent profiles with particular VIMs assigned to the tenant's slice. Thus,

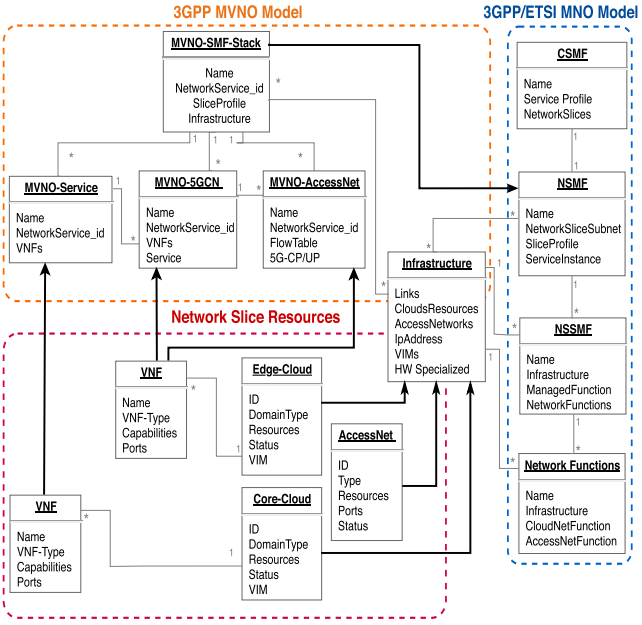

FIGURE 8. Example of MVNO slice information model.

infrastructure security is controlled by providing access credentials to tenants when performing resource reservations.

Similarly, at the VIM level, when an MNO reserves computational resources to register in the NFVO, it first interacts with infrastructure managers, such as OpenStack[1] for virtual machines (VMs) or Kubernetes[2] for containers. Then, the MNO associates the group of resources to a specific user by creating authorization credentials for accessing the resources. The authorization credentials are managed, stored, and provided by the MNO.

2) SERVICE ORCHESTRATION LAYER

The service orchestration layer comprises a network operator OSS/BSS, MNO SMF stack, MVNO SMF stack, third parties, and verticals as customers. A vertical manager can manage the resource layer using the MNO SMF stack when its management constraints are less strict. This case is not suitable for security and latency orchestration constraints. However, when the MVNO has stricter management constraints at the service layer, the MNO provides an independent SMF stack to control the resource orchestrator layer. In this case, the MVNO SMF stack can deploy virtualized network services through the different management systems described in the SIT file.

E. ORCHESTRATION INFORMATION MODEL

Fig. 8 shows a proposal for an MVNO network slicing orchestration object-oriented information model that provides customized management functionalities over the network slice by abstracting infrastructure and network function capabilities. The information model is depicted as a UML (unified modeling language) diagram describing the objects composing an MVNO slice and their capabilities and relations. Since the 3GPP network slice management model and ETSI NFV-MANO focus on a single centralized orchestration system, an extended information model that supports multitenancy concepts is defined in this work.

The MVNO SMF stack represents the abstraction of an orchestration system provided to an MVNO. It includes information on domain types, NF types, MANO platforms, SDN orchestrators, and network slices. The data are gathered from a group of resources allocated to the slice comprised of physical (e.g., access, transport, and cloud networks) and virtualized nodes (e.g., VNFs, PNFs, and MEC apps). Therefore, the information associated with the infrastructure object is usually related to computational resources, virtualization types, specialized hardware, links to interconnect ports inside and outside the domains, radio resources in 3GPP access networks, IP address pools, and the status of the nodes.

MVNO-AccessNet contains information related to the access networks. This information includes the access network protocols used for communication between the user's slice, capabilities, frequencies, and 5GCN identifiers that will be connected (e.g., PLMN-ID).

The MVNO-5GCN data information represents the network service deployed over cloud domains to enable users to access services through mobile networks according to the slice profiles requested by the MVNO. It contains information on 5G core network functions, NF types (e.g., VMs or containers) used to instantiate 5G network functions, tagged numbers of slice/service types (SSTs), and UE credentials for accessing different MVNO services. Additionally, this entity includes the cloud domain identifier where network functions are deployed and the network service identifiers to which they correspond.

The MVNO-Service defines a virtualized application as a network service deployed over any cloud domain. It contains information related to the identifiers of the slice profile, type of VNFs, cloud domains, and authorization certificates. This entity may include services such as MEC systems, MEC apps, and over-the-top services executed as VNFs. The flow rules to forward the user's traffic to these services can be made employing SDN controllers or DNS mechanisms.

Finally, the CSMF, NSMF, and NSSMF represent core information related to the list of service profiles, infrastructure resources, and network slices provided by the MNO in a multidomain and multitenancy context. They contain the data associated with the underlying physical network infrastructure and orchestration systems.

V. USE CASE: TELEOPERATED DRIVING

This section shows how the extensions proposed can be used by an MVNO to provide a vehicular cloud network service in a multidomain scenario. First, an overview of the MVNO scenario, together with some implementation details, is shown. Then, detailed workflows of the instantiation and deployment procedures of the MVNO use case are presented.

[1]https://www.openstack.org
[2]https://kubernetes.io

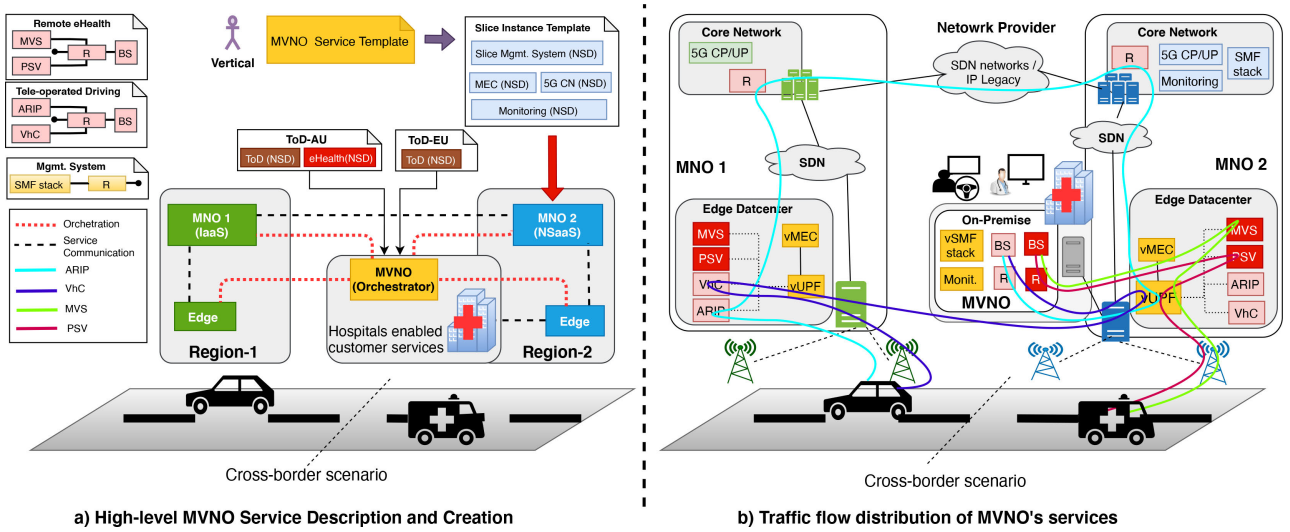

FIGURE 9. An MVNO providing and managing a vehicular cloud network service.

The workflows are divided into two procedures: the deployment of the MVNO SMF stack and the association among tenant and central SMF stacks.

A. VEHICULAR CLOUD NETWORK USE CASE

The automotive and telecommunications industries have joined forces to develop end-to-end solutions for future mobility and sustainable transport services. Different use cases have been defined with functional requirements that may demand divergent network behaviors [49]. Therefore, vehicular communications must face several technical issues (e.g., QoS, coverture, latency, roaming, handover, and service continuity) that must be solved. Thus, to cope with complex network demands, innovative technological approaches are being proposed [50].

Teleoperated driving (ToD) is one of the services envisaged in vehicular cloud networks for autonomous and nonautonomous cars within vehicle-to-everything (V2X) system communications. V2X supports four methods of communication: vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), vehicle-to-vehicle (V2V), and vehicle-to-network (V2N). The use case proposed in this work is related to the V2N model, where traffic flows with specific requirements sent to/from the vehicle components can be served by different types of network slices. Furthermore, it leverages the network slice management model proposed in this article to overcome some of the technical issues related to cross-domain scenarios in a novel manner.

Specifically, the use case focuses on implementing ToD services in a cross-border multidomain health care scenario. A health care company that owns a hospital in a particular region wants to offer two specific services to users in nearby areas: ToD service for elderly users (ToD-EU) to be transported to the hospital and ToD service for ambulance users (ToD-AU) that assists in car accidents. ToD-EU and ToD-AU are critical services.

To provide such services, the health care company, which does not own network infrastructure in the area, can exploit the benefits of an NSaaS. It must contact a third company acting as an MVNO (or even becoming an MVNO) to use the network resources offered by other network operators working in the regions. The MVNO must request the creation of the required network slices to the MNOs to deploy the service instances that will support the ToD service and guarantee its service continuity in each region. The management and orchestration of the services will be the service provider's responsibility (MVNO), although MNOs will provide the network resources.

Fig. 9 shows the overall description of the vehicular network service in a two-region cross-border scenario, showing the stakeholders involved in supporting the service's provision. The left view details the high-level requirements of the MVNO and presents the orchestration relationship between the different components of the scenario. The right view shows the distribution of the network functions instantiated in the network infrastructure provided by MNOs.

MNO-1 and MNO-2 are 5G network operators that provide coverage to region 1 and region 2, respectively (Fig. 9a). Both offer edge computing services and expose their network capabilities to deploy and manage functions that compose the vehicular network service.

The hospital is located in region 2 and uses MNO-2 as its internet service provider. The MVNO company owns an NFVI-enabled point of presence able to host computational services on premise.

Both MNOs can provide fully virtualized services implemented over their infrastructures or hired from third parties. In the use case scenario, MNO-2 will act as an NSaaS provider. The MVNO will be an NSaaS tenant of MNO-2,

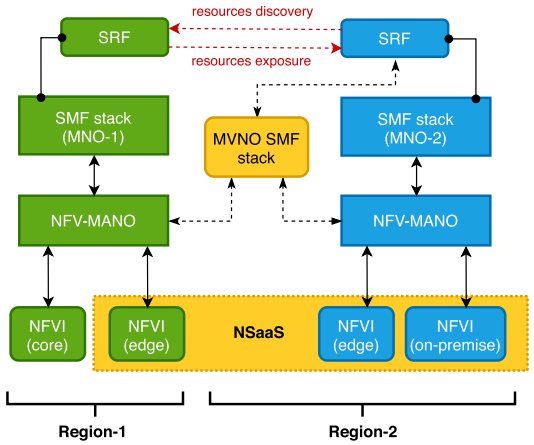

FIGURE 10. Discovery/exposure resources between MNOs through the SRF component.

requesting that it run all the dedicated services of the vehicular scenario (ToD-EU and ToD-AU). MNO-2 will be in charge of requesting the resources to MNO-1 needed in region 1 and reserving the resources it needs in region 2 to later deploy the VNFs for video streaming and vehicle control required for the ToD service in all administrative domains.

The NSaaS requested doe MNO-2 by the MVNO will include the service level management attribute described in Section IV-B in the NEST file. Accordingly, MNO-2 will deploy a dedicated SMF stack for the MVNO in the MVNO NFVI domain. This will ensure the reliability, security, and privacy of information for the MVNO.

The MVNO will control and orchestrate the physical and virtual resources detailed in the service profile created from the NEST. The service profile in this example is an SIT file composed of the management system (the SMF stack specified as an NSD), the 5GCN resources, the MEC system, and the monitoring NSDs.

Although MNO-1 has the capability to orchestrate its network infrastructure, in this scenario, it acts as an infrastructure as a service (IaaS) provider to allow third parties to use its network (e.g., access networks and transport networks as a service) and computational (e.g., NFVI as a service) resources. MNO-2 can discover the resources of MNO-1 through the communications between the SRF components of each MNO. For example, the SMF stacks of MNO-1 will expose the resources and MANO platforms that have registered. The SMF stack of MNO-2 will consume this information to enable the MVNO to control the resources from MNO-1, as shown in Fig. 10.

The ToD NS will include specific VNFs for processing application data (Fig. 9b). For example, a VNF for augmented reality image processing (ARIP) will process the video data streams coming from a car and apply visual computing models to add descriptions to the video images useful for the teleoperator. This service requires large amounts of bandwidth. Furthermore, a VNF for vehicle control (VhC) will operate a car's actuators. This function requires ultrahigh reliability with strict latency constraints. The traffic flows from each function arrive at the backend server (BS) VNF, where they are processed and presented in a unified way to the teleoperator. For the ToD-AU service, eHealth VNFs are added for remote paramedic assistance. These include VNFs for monitoring the vital signs (MVSs) captured by ambulance health tools and for processing streaming video (PSV) captured on cameras worn by paramedics. Since the traffic flows of remote vehicle actions (VhC VNFs) require strict latency constraints, the data flow must be resolved as a local breakout mode with core network functions deployed in the same edge site for both services.

In general, for this use case, the following assumptions are considered:

- The 5GCN is configured and linked to the appropriate radio resources by assigning the public land mobile network identifier (PLMN_ID).
- Service requirements are set as follows: reliability (99.9999%), data rate (32 Mbps for video and 10 Mbps for actuators), latency (10 ms for actuators and 100 ms for video), and coverage (1000 m).
- The services use a 3GPP SST with the value "4" that identifies the network slice of the MVNO. Conversely, for video streaming, remote-control, and eHealth services, they use service differentiator (SD) identifiers to steer the flows through the different VNFs.
- According to 3GPP TS.23.501, vehicular cloud network services use session and service continuity (SSC) mode 3 for protocol data unit (PDU) sessions. In the case of streaming video data streams, the user plane function (UPF) uses the uplink classifier (UL/CL) mode to achieve UPFs in the network cores in the data plane (DP).
- The MVNO stack controls the SDNs that interconnect the MNO-1 and MNO-2 providers.

B. USE CASE DEPLOYMENT WORKFLOW

An overview of the provisioning and deployment procedures of the MVNO SMF stack to control a vehicular cloud network is presented in Fig. 11. Besides, Fig. 12 shows the workflow for the registration, association, and configuration of MVNO network management functions with the central SMF stack of MNO-2. Below is a description of the steps.

Once MNO-2 has authenticated the MVNO client, the vertical requests information from the NSaaS catalogs through the CSMF entity (steps 1–2). Then, the instantiation request of the selected template is initiated. The template is translated into parameters set by the SIT and received by the NSMF (step 3). The NSMF reads the requirements and validates the resource information described in the SIT file (step 4).

Assuming that the MVNO SMF stack descriptors, 5GCN, monitoring, and MEC system are designed and onboarded, the NSMF communicates with each NSSMF to verify the availability of the necessary resources to instantiate the

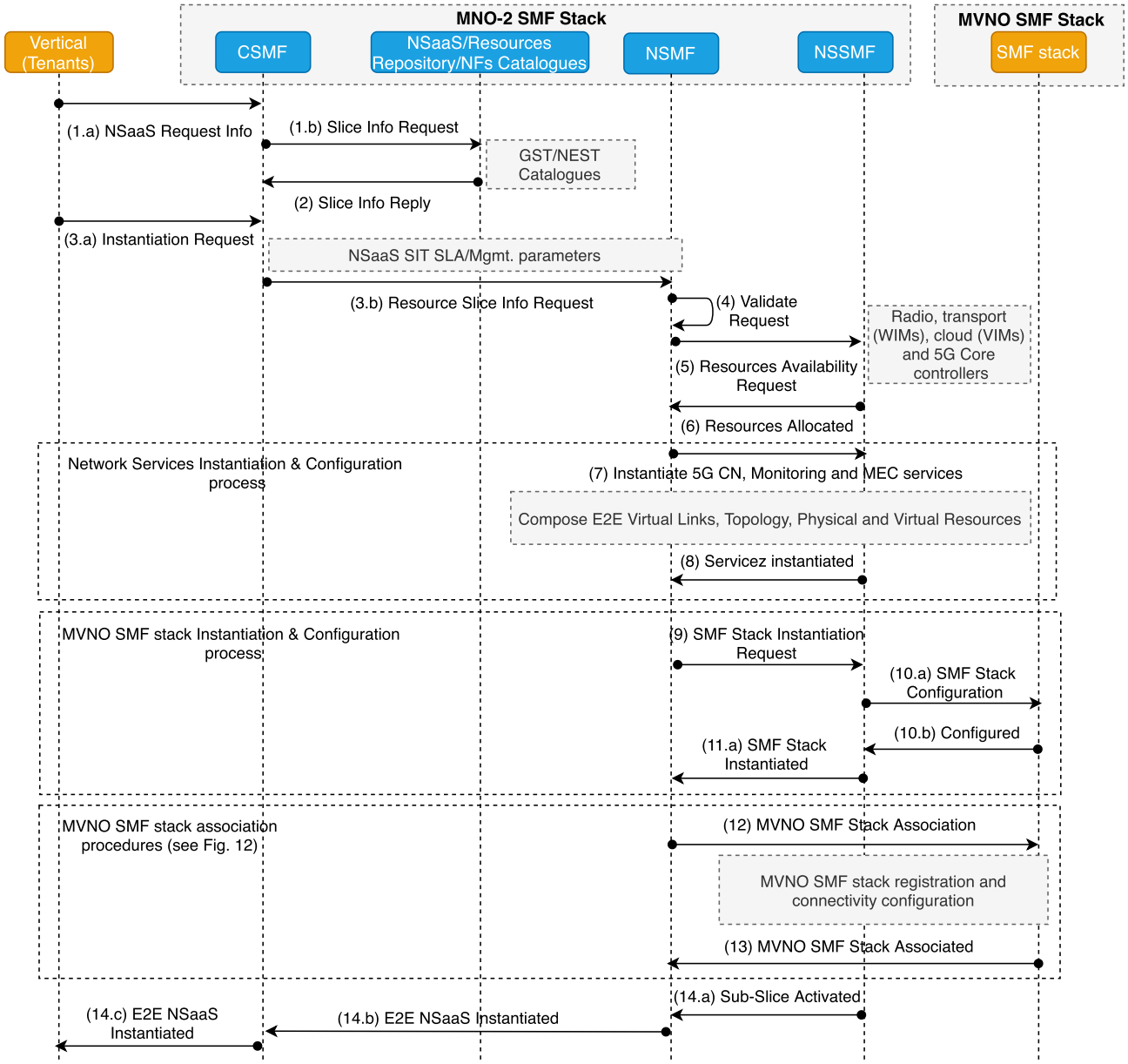

FIGURE 11. E2E NSaaS provision and MVNO SMF stack instantiation flow procedure.

required service (step 5). This step includes verifying the availability of MNO-1 resources based on the SLA previously established between both operators. Each NSSMF validates the request and reserves the infrastructure resources to be used by the NSaaS. For example, NSSMFs that control computing domains verify NFVI resource availability, VIM types (VM or container-based), and location (edge, core, and public). For access and transport networks, NSSMFs verify resource availability through specific controllers. The transport controller can consider the use of WIM functionalities. Furthermore, NSSMFs return an ACK to the NSMF with the physical network resources reserved and allocated (step 6).

Since the resources have been placed according to the SLA and management functionality negotiations defined in the SIT, the NSMF first starts the network service instantiation process (i.e., distributes the 5GCN, monitoring, and MEC systems as VNFs to the corresponding NSSMFs). NSSMFs perform the VNF packet onboarding process on each NFVO selected by the SIT and set the logical network topology by composing the E2E virtual links through the SDN controllers that manage the NFVI points-of-presence and transport networks (step 7). Orchestration and placement algorithms are performed to deploy the NSDs. Then, the NSMF starts the process of instantiating and configuring the virtual SMF stack (step 9). The NSSMF accesses the

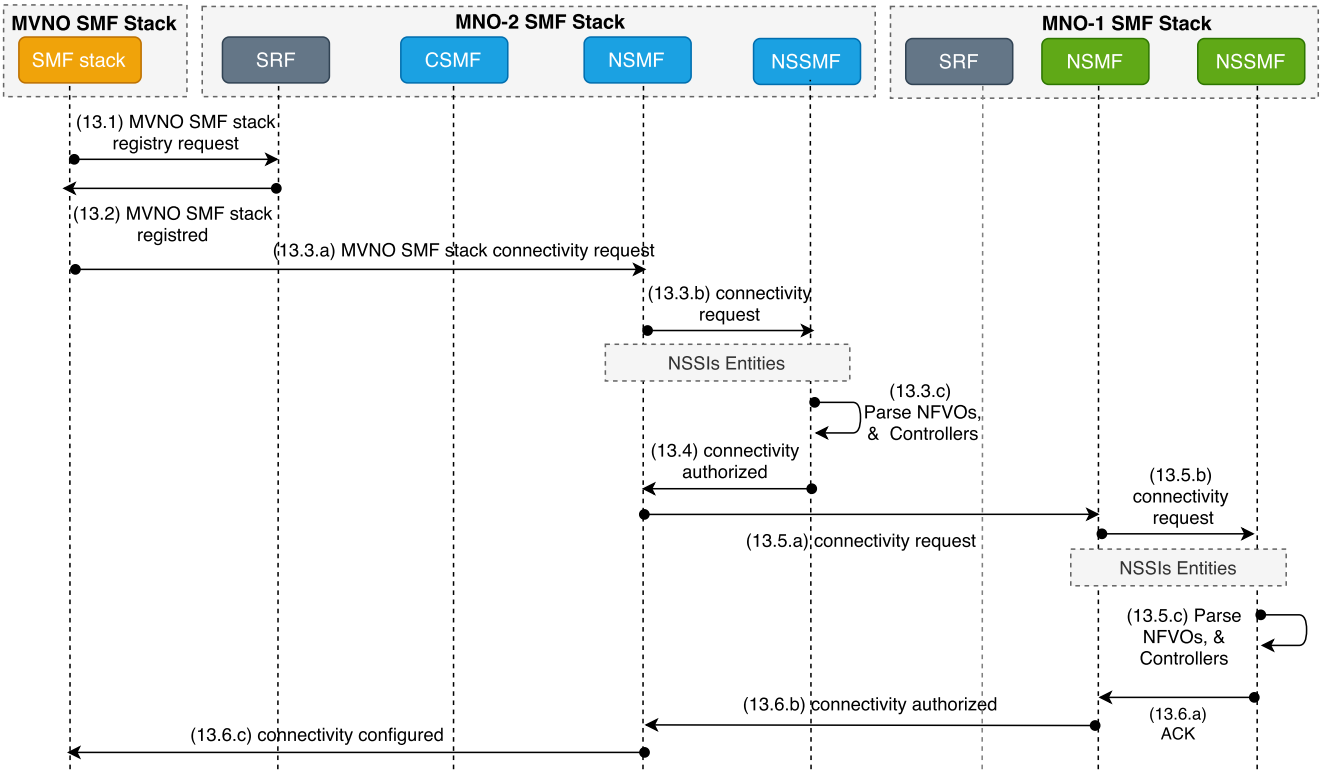

FIGURE 12. MVNO SMF stack registration and connectivity configuration workflow.

NFVI domain, where it will be instantiated. In this case, it communicates with the cloud deployed on the premises of the vertical via the corresponding NFVO.

It then performs the MVNO SMF stack network descriptor onboarding, deployment, and configuration procedures (step 10). Next, the NSSMF, in charge of managing the NFVI point of presence deployed on the premises of the vertical, returns the instantiation ACK (step 11). The NSMF starts the registration and association procedures between central (MNO-2) and vertical (MVNO) SMF stacks (step 12). The association and control activation procedures of the MVNO SMF stack are detailed in Fig. 12.

After the MVNO SMF stack has been instantiated (step 11), it sends a registration request message of its functions to the SRF component to access the services provided by the functions of the central SMF stack (step 13.1). The SRF entity validates and registers the MVNO stack components to its repository of active and enabled functions (step 13.2). Then, the MVNO SMF stack communicates with the NSMF of the central SMF stack to request access and connectivity configuration with the entities in charge of managing the NSSIs belonging to the MVNO (step 13.3.a). The NSMF forwards this request message to each NSSMF in its network infrastructure (step 13.3.b) and to the NSMF belonging to MNO-1 to validate the resources and provide access configuration to the NSSI entities instantiated in their domains (step 13.5.a). The connectivity request is established based on the access and service consumption permissions previously set with the SRF entity. Each NSSMF entity analyzes the availability of controllers, NFV-MANO, and NFVI systems on each network segment of MNO-1 and MNO-2, which the MVNO stack needs to access and manage. After access and control permissions are established, each NSSMF returns an authorized and accepted connectivity message to the central NSMF (MNO-2) (steps 13.4 and 13.6.b). The NSMF then forwards this message to the MVNO SMF stack, indicating that connectivity has been authorized and configured (step 13.6.c).

Finally, each NSSMF informs the NSMF that the slice subnet instances are configured and active. Then, the NSMF forwards this message to the CSMF to report to the vertical that the E2E NSaaS is instantiated and ready for use (step 14), as shown in Fig. 11.

Once the MVNO slice is instantiated, the MVNO SMF stack can onboard and deploy the ToD-EU and ToD-AU services (see Fig. 7). Each service is deployed with a single network slice template. Each slice template comprises NSDs with VNFs in the form of containers and VMs. In this light, the MVNO SMF stack starts the onboarding and deployment procedures. It possesses authorization certificates to access the cloud and network domains provided by the MNO. The NSMF divides the slice template according to the domain-type field specified in the descriptors and distributes the VNFs to the appropriate NSSMFs to deploy them through the corresponding NFVO platforms. In this scenario, they are deployed over the edge clouds of MNO-1

TABLE 3. Acronyms.

3GPP	3rd Generation Partnership Project	NSMF	Network Slice Management Function
5GCN	5G Core Networks	NSP	Network Slice Provider
ACK	Acknowledge	NSSI	Network Slice Subnet Instance
AN	Access Network	NSSMF	Network Slice Subnet Management Function
API	Application Programming Interface	ONF	Open Networking Foundation
ARIP	Augmented Reality Image Processing	OSS	Operational Support Systems
BS	Backend Server	PDU	Protocol Data Unit
BSS	Business Support Systems	PLMN	Public Land Mobile Network
CDN	Content Delivery Networks	PNF	Physical Network Function
CSC	Communication Service Customers	PSV	Processing Streaming Video
CSMF	Communication Service Management Function	QoS	Quality of Service
CSP	Communication Service Provider	REST	Representational State Transfer
E2E	End-to-End	SBI	Southbound Interface
eMBB	enhanced Mobile Broadband	SD	Service Differentiators
EPC	Evolved Packet Core	SDN	Software-Defined Networks
ETSI	European Telecommunications Standards Institute	SIT	Slice Instance Template
FCAPS	Fault, Configuration, Accounting, Performance and Security	SLA	Service Level Agreement
GSMA	Global System for Mobile Communications	SMF stack	Slice Management Function stack
GST	Generic Network Slice Template	SRF	SMF stack Register Function
IaaS	Infrastructure as a Service	SST	Slice/Service Type
ITU	International Telecommunication Union	TN	Transport Network
KPI	Key Performance Indicator	ToD	Teleoperated Driving
MANO	Management and Orchestration	ToD-AU	ToD Ambulance Users
MANOaaS	Management and Orchestration as a Service	ToD-EU	ToD Elderly Users
MEC	Multiaccess Edge Computing	UE	User Equipment
MECaaS	Multiaccess Edge Computing as a Service	UL/CL	Uplink Classifier
mMTC	massive Machine Type Communications	UML	Unified Modeling Language
MNO	Mobile Network Operators	UPF	User Plane Function
MVNO	Mobile Virtual Network Operator	URLLC	Ultra-Reliable Low-Latency Communications
MVS	Monitoring Vital Signs	V2I	Vehicle-to-Infrastructure
NBI	Northbound Interface	V2N	Vehicle-to-Network
NEST	NEtwork Slice Type	V2P	Vehicle-to-Pedestrian
NF	Network Function	V2V	Vehicle-to-Vehicle
NFV	Network Function Virtualization	V2X	Vehicle-to-Everything
NFVI	Network Function Virtualization Infrastructure	vCPE	Virtual Customer Premises Equipment
NFVO	Network Function Virtualization Orchestrator	VhC	Vehicle Control
NOP	Network Operator	VIM	Virtual Infrastructure Manager
NS	Network Service	VM	Virtual Machine
NSaaS	Network Slice as a Service	VNF	Virtual Network Function
NSC	Network Slice Customer	VNFD	Virtual Network Function Descriptor
NSD	Network Service Descriptor	WIM	Wide-area Infrastructure Manager
NSI	Network Slice Instance		

and MNO-2 providers, as well as over the on-premises of the MVNO. VNF chaining is performed via an NSSMF that sends the parameters and traffic policies to the SDN controllers. Similarly, the NSSMFs managing the access and transport networks translate the network service requirements to the appropriate configuration parameters that fulfill the SLA features defined in SIT. Once the services are deployed, the 5GCN controllers and the access network controllers establish the communication configurations and set up the required protocols within the V2N model.

VI. CONCLUSION

In this work, an agile NFV-based network slice management platform is proposed to support the customized management systems provided to particular verticals. The proposed service-based architecture extends the 3GPP network slice management model to solve reliability, scalability, and isolation requirements at the service orchestration level. This model works under the premise of providing management functions built as VNFs defined into a network service descriptor. The proposal addresses the management

and orchestration requirements for providing network slices in multitenancy and multidomain environments, starting from the premise of offering isolated management functions to each vertical. The virtualization of the management system is reached by the definition of a slice instance template with extended features that allow particular verticals (e.g., the MVNO) to play the role of a network operator in an agile way. Finally, the SMF stack should implement intelligent mechanisms to enable a seamless computing continuum in future works. These mechanisms should be in charge of performing service migration, redirection, and traffic balancing procedures without the intervention of an operator.

In the same way, to maintain a standard information model for orchestration and lifecycle management of VNFs and MEC systems, the SMF stack platform should implement mechanisms to generate flexible descriptors adapted to different platforms. In this work, some insights into how to address this challenge are provided.

APPENDIX

Table 3 lists the acronyms used in this work.

REFERENCES

[1] *International Mobile Telecommunication Vision—Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond*, document ITU-R M.2083 MT, 2015.

[2] GSMA. (2017). *An Introduction to Network Slicing*. [Online]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

[3] *Technical Specification Group Services and System Aspects; Telecommunication management: Study on Management and Orchestration of Network Slicing for Next Generation Network (Release 15)*, document TR 28.801 V15.1.0, 3GPP, 2018.

[4] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018, doi: 10.1109/COMST.2018.2815638.

[5] S. Sharma, R. Miller, and A. Francini, "A cloud-native approach to 5G network slicing," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 120–127, Aug. 2017, doi: 10.1109/MCOM.2017.1600942.

[6] *Network Functions Virtualisation (NFV) Release 3: Reliability: Report on NFV Resiliency for the Support of Network Slicing*, document GR NFV-REL 010 V3.1.1, ETSI, 2019.

[7] G. Bernini, P. G. Giardina, S. Spadaro, F. Agraz, A. Pages, J. Cabaca, P. Neves, K. Koutsopoulos, and A. Matencio, "Multi-domain orchestration of 5G vertical services and network slices," in *Proc. IEEE Int. Conf. Commun. Workshops*, Dublin, Ireland, Jun. 2020, pp. 1–6, doi: 10.1109/ICC-Workshops49005.2020.9145221.

[8] X. Zhou, R. Li, T. Chen, and H. Zhang, "Network slicing as a service: Enabling enterprises' own software-defined cellular networks," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 146–153, Jul. 2016, doi: 10.1109/MCOM.2016.7509393.

[9] J. X. Salvat, L. Zanzi, A. Garcia-Saavedra, V. Sciancalepore, and X. Costa-Perez, "Overbooking network slices through yield-driven end-to-end orchestration," in *Proc. 14th Int. Conf. Emerg. Netw. Exp. Technol.*, Dec. 2018, pp. 353–365, doi: 10.1145/3281411.3281435.

[10] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, May 2017, doi: 10.1109/MCOM.2017.1600935.

[11] A. Cardenas and D. Fernandez, "Network slice lifecycle management model for NFV-based 5G virtual mobile network operators," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Leganes, Spain, Nov. 2020, pp. 120–125, doi: 10.1109/NFV-SDN50289.2020.9289883.

[12] A. Kaloxylos, "A survey and an analysis of network slicing in 5G networks," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 60–65, Mar. 2018, doi: 10.1109/MCOMSTD.2018.1700072.

[13] X. Li, R. Casellas, G. Landi, A. de la Oliva, X. Costa-Perez, A. Garcia-Saavedra, and T. Deiss, "5G-crosshaul network slicing: Enabling multi-tenancy in mobile transport networks," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 128–137, Aug. 2017, doi: 10.1109/MCOM.2017.1600921.

[14] E. Kapassa, M. Touloupou, A. Mavrogiorgou, A. Kiourtis, D. Giannouli, K. Katsigianni, and D. Kyriazis, "An innovative eHealth system powered by 5G network slicing," in *Proc. 6th Int. Conf. Internet Things, Syst., Manage. Secur. (IOTSMS)*, Granada, Spain, Oct. 2019, pp. 7–12, doi: 10.1109/IOTSMS48152.2019.8939266.

[15] Q. Wang, J. Alcaraz-Calero, R. Ricart-Sanchez, M. B. Weiss, and A. Gavras, "Enable advanced QoS-aware network slicing in 5G networks for slice-based media use cases," *IEEE Trans. Broadcast.*, vol. 65, no. 2, pp. 444–453, Jun. 2019, doi: 10.1109/TBC.2019.2901402.

[16] L. M. C. Murillo and D. R. Lopez, "A network service provider perspective on network slicing," in *IEEE Softwarization: A Collection of Short Technical Articles*, 2018. [Online]. Available: https://sdn.ieee.org/newsletter/january-2018/a-network-serviceprovider-perspective-on-network-slicing

[17] S. Draxler, H. Karl, H. R. Kouchaksaraei, A. Machwe, C. Dent-Young, K. Katsalis, and K. Samdanis, "5G OS: Control and orchestration of services on multi-domain heterogeneous 5G infrastructures," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Ljubljana, Slovenia, Jun. 2018, pp. 1–9, doi: 10.1109/EuCNC.2018.8443210.

[18] Q. Wang, J. Alcaraz-Calero, M. Weiss, A. Gavras, P. M. Neves, R. Cale, and G. Bernini, "SliceNet: End-to-end cognitive network slicing and slice management framework in virtualised multi-domain, multi-tenant 5G networks," in *Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, Valencia, Spain, Jun. 2018, pp. 1–5, doi: 10.1109/BMSB.2018.8436800.

[19] *Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on Architecture Options to Support Multiple Administrative Domains*, document GR NFV-IFA 028 V3.1.1, ETSI, 2018.

[20] Guerzoni, "Analysis of end-to-end multi-domain management and orchestration frameworks for software defined infrastructures: An architectural survey," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 4, p. e3103, 2016. [Online]. Available: http://discovery.ucl.ac.uk/1519459/1/Galis_Guerzoni_et_al-2016-Transactions_on_Emerging_Telecommunications_Technologies.pdf

[21] A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, F. Ippoliti, and G. M. Pérez, "Dynamic network slicing management of multimedia scenarios for future remote healthcare," *Multimedia Tools Appl.*, vol. 78, no. 17, pp. 24707–24737, Feb. 2019, doi: 10.1007/s11042-019-7283-3.

[22] M. Shariat, Ö. Bulakci, A. De Domenico, C. Mannweiler, M. Gramaglia, Q. Wei, A. Gopalasingham, E. Pateromichelakis, F. Moggio, D. Tsolkas, B. Gajic, M. R. Crippa, and S. Khatibi, "A flexible network architecture for 5G systems," *Wireless Commun. Mobile Comput.*, vol. 2019, Feb. 2019, Art. no. 5264012, doi: 10.1155/2019/5264012.

[23] Fernandez, Vidal, and Valera, "Enabling the orchestration of IoT slices through edge and cloud microservice platforms," *Sensors*, vol. 19, no. 13, p. 2980, Jul. 2019, doi: 10.3390/s19132980.

[24] T. Taleb, P. A. Frangoudis, I. Benkacem, and A. Ksentini, "CDN slicing over a multi-domain edge cloud," *IEEE Trans. Mobile Comput.*, vol. 19, no. 9, pp. 2010–2027, Sep. 2020, doi: 10.1109/TMC.2019.2921712.

[25] C. Casetti, C. F. Chiasserini, T. Deiss, P. A. Frangoudis, A. Ksentini, G. Landi, X. Li, N. Molner, and J. Mangues, "Network slices for vertical industries," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Barcelona, Spain, Apr. 2018, pp. 254–259, doi: 10.1109/WCNCW.2018.8368981.

[26] F. Z. Yousaf, V. Sciancalepore, M. Liebsch, and X. Costa-Perez, "MANOaaS: A multi-tenant NFV MANO for 5G network slices," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 103–109, May 2019, doi: 10.1109/MCOM.2019.1800898.

[27] M. A. Habibi, B. Han, F. Z. Yousaf, and H. D. Schotten, "How should network slice instances be provided to multiple use cases of a single vertical industry?" *IEEE Commun. Standards Mag.*, vol. 4, no. 3, pp. 53–61, Sep. 2020.

[28] *Multi-Access Edge Computing (MEC): Framework and Reference Architecture*, document GS MEC 003 V2.1.1, ETSI, 2019.

[29] *Mobile Edge Computing (MEC): Deployment of Mobile Edge Computing in an NFV environment*, document GR MEC 017 v1.1.1, ETSI, 2018.

[30] *Network Functions Virtualisation (NFV); Management and Orchestration*, document GS NFV-MAN 001 V1.1.1, ETSI, 2014.

[31] *Technical Specification Group Services and System Aspects; System architecture for the 5G system (5GS); Stage 2*, document TS 23.501 V15.10.0, 3GPP, 2020.

[32] ETSI. (2018). *MEC in 5G networks*. [Online]. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[33] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018, doi: 10.1109/JIOT.2017.2750180.

[34] Q.-V. Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, L. B. Le, W.-J. Hwang, and Z. Ding, "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art," *IEEE Access*, vol. 8, pp. 116974–117017, 2020, doi: 10.1109/ACCESS.2020.3001277.

[35] A. Ksentini and P. A. Frangoudis, "Toward slicing-enabled multi-access edge computing in 5G," *IEEE Netw.*, vol. 34, no. 2, pp. 99–105, Mar. 2020, doi: 10.1109/MNET.001.1900261.

[36] L. Tomaszewski, S. Kukliński, and R. Kołakowski, "A new approach to 5G and MEC integration," in *Artificial Intelligence Applications and Innovations* (IFIP Advances in Information and Communication Technology), vol. 585, I. Maglogiannis, L. Iliadis, and E. Pimenidis, Eds. Cham, Switzerland: Springer, May 2020, pp. 15–24, doi: 10.1007/978-3-030-49190-1_2.

[37] V. Sciancalepore, F. Giust, K. Samdanis, and Z. Yousaf, "A double-tier MEC-NFV architecture: Design and optimisation," in *Proc. IEEE Conf. Standards for Commun. Netw. (CSCN)*, Berlin, Germany, Oct. 2016, pp. 1–6, doi: 10.1109/CSCN.2016.7785157.

[38] I. Sarrigiannis, E. Kartsakli, K. Ramantas, A. Antonopoulos, and C. Verikoukis, "Application and network VNF migration in a MEC-enabled 5G architecture," in *Proc. IEEE 23rd Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Barcelona, Spain, Sep. 2018, pp. 1–6, doi: 10.1109/CAMAD.2018.8514943.

[39] H.-C. Hsieh, J.-L. Chen, and A. Benslimane, "5G virtualized multi-access edge computing platform for IoT applications," *J. Netw. Comput. Appl.*, vol. 115, pp. 94–102, Aug. 2018, doi: 10.1016/j.jnca.2018.05.001.

[40] G. Cattaneo, F. Giust, C. Meani, D. Munaretto, and P. Paglierani, "Deploying CPU-intensive applications on MEC in NFV systems: The immersive video use case," *Computers*, vol. 7, no. 4, p. 55, Oct. 2018, doi: 10.3390/computers7040055.

[41] GSMA. (2019). *Generic Network Slice Template*. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.116-v2.0.pdf

[42] *5G; Management and Orchestration; Concepts, Use Cases and Requirements*, document TS 128 530 V15.0.0 TS 28.530 Version 15.0.0 Release 15), ETSI, 2018.

[43] *Technical Specification Group Services and System Aspects; Management and Orchestration; 5G Network Resource Model (NRM); Stage 2 and 3*, document TS 28.541 V16.1.0, 3GPPm 2019.

[44] Cisco. (2018). *Cisco Converged 5G xHaul Transport*. [Online]. Available: https://www.cisco.com/c/en/us/solutions/service-provider/mobile-internet/5g-transport/converged-5g-xhaul-transport.html

[45] *Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Network Service Templates Specification*, document GS NFV-IFA 014 V3.4.1, ETSI, 2020.

[46] *Mobile Edge Computing (MEC); Mobile Edge Management; Part 2: Application lifecycle, rules and requirements management*, document GS MEC 010-2 V1.1.1, ETSI, 2017.

[47] S. Clayman, F. Tusa, and A. Galis, "Extending slices into data centers: The VIM on-demand model," in *Proc. 9th Int. Conf. Netw. Future (NOF)*, Poznan, Poland, Nov. 2018, pp. 31–38, doi: 10.1109/NOF.2018.8597850.

[48] S. Clayman, F. Tusa, A. Galis, and L. M. Contreras, "WIM on-demand a modular approach for managing network slices," in *Proc. 6th IEEE Conf. Netw. Softwarization (NetSoft)*, Ghent, Belgium, Jun. 2020, pp. 395–403, doi: 10.1109/NetSoft48620.2020.9165342.

[49] 5GPPP. (2015). *5G Automotive Vision*. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf

[50] J. Mei, X. Wang, and K. Zheng, "Intelligent network slicing for V2X services toward 5G," *IEEE Netw.*, vol. 33, no. 6, pp. 196–204, Nov. 2019.

ANDRÉS CÁRDENAS (Member, IEEE) received the master's degree in network engineering and telematics services from the Universidad Politécnica de Madrid, Spain, where he is currently pursuing the Ph.D. degree with the Departamento de Ingeniería de Servicios Telemáticos (DIT). Additionally, he is currently a Software Network Researcher at the i2CAT Foundation. His current research interests include network slicing, network virtualization, software-defined networking, cloud computing, and 5G mobile networks.

DAVID FERNÁNDEZ received the M.S. degree in telecommunications engineering and the Ph.D. degree in telematics engineering from the Universidad Politeìcnica de Madrid (UPM), Spain, in 1988 and 1993, respectively. Since 1995, he has been an Associate Professor with the Department of Telematics Systems Engineering (DIT), UPM. His current research interests include software-defined networks, network virtualization, cloud computing datacenter technologies, and network security.

CARLOS M. LENTISCO received the M.S. and Ph.D. degrees in telecommunications engineering from the Universidad Politécnica de Madrid (UPM), Spain, in 2014 and 2019, respectively. He is currently an Assistant Lecturer with UPM, specializing in the fields of computer networking, multimedia services, and internet technologies. His current research interests include mobile broadcast services, virtualization, and software-defined networking.

RICARDO FLORES MOYANO (Member, IEEE) received the degree in electronic engineering from Universidad Politécnica Salesiana (UPS), in 2006, and the M.S. and Ph.D. degrees in telematics systems engineering from the Universidad Politécnica de Madrid (UPM), in 2013 and 2018, respectively. He is a full-time Professor with the Department of Computer Science Engineering, Universidad San Francisco de Quito (USFQ). His research interests include SDN, NFV, cloud networking, the future internet, and 5G networks.

LUIS BELLIDO received the M.S. and Ph.D. degrees in telecommunications engineering from the Universidad Politécnica de Madrid (UPM), Madrid, Spain, in 1994 and 2004, respectively. He is currently an Associate Professor with UPM, specializing in the fields of computer networking, internet technologies, and quality of service. His current research interests include mobile networks, multimedia applications, and virtualization.