Autonomous Private Mobile Networks: State of the Art and Future Challenges

Arturo Bellin, Marco Centenaro, Nicola di Pietro, Arif Ishaq, Daniele Munaretto, Daniele Ronzani, Andrea Spinato, Stefano Tomasin, and Fabrizio Granelli

***Abstract*—As mobile systems for private use are gaining momentum, the area of network management automation is bound to attract renewed attention from standardization organizations and vendors. Prominent examples of tasks that would benefit from network automation tools are provisioning, diagnosing, and healing. Nevertheless, due to the various network and service providers as well as stakeholders involved in the deployment of a non-public mobile system, the success of such automation heavily depends on a smooth and effective interoperability among the components of the overall system. In this paper, we review the state of the art of network operations, administration, and management in the context of mobile systems for non-public use, highlighting the differences with respect to traditional public networks. Then, we provide insights about the automated provisioning of an entire core network and a network slice subnet, both for private use, performed on a research testbed under continuous integration. Finally, we propose a list of future challenges in this research area.**

***Index Terms*—5G and beyond, non-public networks, private mobile networks, open ecosystem, 3GPP, ETSI, NFV, MEC, management and orchestration.**

INTRODUCTION

MOBILE communication networks for private use [1] – referred to as non-public networks (NPNs) within the fifth-generation (5G) mobile systems standardized by the 3rd Generation Partnership Project (3GPP) [2], [3, §5.30] – are attracting attention in both the academic and industrial research communities. NPNs aim at providing the technologies developed for public networks (such as 5G) to private entities or network tenants by restricting network access only to authorized terminals. For such reason they are expected to support a variety of *vertical industries*, e.g., Industry 4.0, smart grids, and public safety, with a combination of (dedicated) services, including (edge) cloud computing, mission-critical communication, Internet of Things (IoT), indoor communication and positioning. Two key enablers for a widespread adoption of NPNs are worth mentioning, that are i) the utilization of commodity hardware to host virtual mobile network functions and ii) open and standard interfaces to prevent vendor lock-in, thus opening up the market to new players, foster interoperability, and ease network management and orchestration. The former approach has been a general trend over the last decade with the advent of software defined networking and network function virtualization (NFV). The latter entails the concept of *openness* in different aspects and forms:

1) *Inter-subnetwork openness* – It ensures interoperability across domains, e.g., the radio access network and the core network.
2) *Intra-subnetwork openness* – The segmentation between control-plane network functions (NFs) and user-plane NFs within the 5G core network (5GC) as well as radio access network (RAN) protocol stack split enable interworking among (software) infrastructure providers.
3) *Security openness* – Thanks to the standardization of user equipment (UE) profiles and their authentication means, NPNs enable a private tenant to enforce thorough access control policies.
4) *End-to-end system orchestration openness* – The widespread adoption of network deployment approaches based on commodity hardware allows to focus on the management and orchestration of virtual NFs via standard interfaces.

The 3GPP and the European Telecommunications Standards Institute (ETSI) have been playing a crucial role to foster the creation of such an open ecosystem thanks to their standards related to 5G. This paper specifically focuses on the last openness factor, i.e., the overall orchestration of a non-public mobile system. Since most of the envisioned users of these systems are not experts in the mobile technology, it is reasonable to assume that the network automation means will need to evolve to incorporate the principles of zero-touch network and service management, so to build *autonomous NPNs*, needing (almost) no intervention from human operators – see, e.g., [4]. This objective can be achieved with the collaboration of all the involved vendors and stakeholders, especially the new ones that are entering the market of mobile network infrastructures for private entities – typically referred to as *private mobile networks*, without an *explicit label* on the intended use of the network. In the following, we aim at identifying the standardization framework for building an autonomous NPN, while highlighting the possible risk factors which may prevent to achieve this target.

In the rest of this manuscript, we first highlight how NPNs differ from public land mobile networks (PLMNs) in terms of standardization, functional requirements, system architectures, and governance. Then, we provide an overview of the NPN

A. Bellin and F. Granelli are with the Department of Information Engineering and Computer Science (DISI), University of Trento, 38150 Trento, Italy. A. Bellin is the corresponding author.

M. Centenaro, N. di Pietro, A. Ishaq, D. Munaretto, D. Ronzani, and A. Spinato are with the Research & Innovation Department, Athonet S.r.l., 36050 Bolzano Vicentino, Italy.

S. Tomasin is with the Department of Information Engineering (DEI), University of Padova, 35131 Padova, Italy.

communication and orchestration architectures. After that, we describe the ongoing activities on our research testbed, which integrates both proprietary and open-source tools to implement a management and orchestration framework for the 5GC of a private mobile network. Finally, we identify the future challenges for a widespread adoption of fully autonomous NPNs. This work significantly differentiates from [4] as it focuses on more low-level standardization aspects as well as practical issues concerning the system architecture and orchestration of NPNs.

A Comparison Between NPNs and PLMNs

Private Mobile Networks

Although NPNs have been clearly identified and defined in the recent 3GPP standardization, *private mobile networks* started to grow more than a decade ago leveraging fourth-generation (4G) mobile systems. They were defined as an isolated Long Term Evolution (LTE) network deployment with no interactions with a PLMN. As a matter of fact, almost all current deployments worldwide leverage the LTE technology, including, e.g., the systems operating in the USA on the Citizen Broadcast Radio System (CBRS) frequencies and following the specifications of the OnGo Alliance. Even some vertical markets can be still efficiently and reliably served by LTE systems for private use. This applies in particular to those related to critical communications for public safety, which traditionally require a dependable system, and have been considering this technology to replace the legacy Terrestrial Trunked Radio (TETRA) in the recent years. A dedicated PLMN identifier (ID) with Mobile Country Code (MCC) 999 has been assigned by the ITU-T to private mobile networks (regardless of their generation), while the Mobile Network Code (MNC) is left to the specific network deployment.

In other cases, the LTE technology cannot meet new application requirements, though. For example, when considering a network connecting control systems and physical actuators, latency and reliability requirements become very stringent. In this context, the ultra-reliable low-latency communications (URLLC) [3, §5.33], which significantly benefit from the new 5G air interface (the so-called New Radio) as well as leverage the enhanced 5GC uptime, are necessary. A huge expectation for private *5G* mobile networks thus comes from the Industry 4.0 sector, where URLLC can be combined with thorough access control and user equipment authentication [5], [6].

In order to allow the operation of multiple private networks in the same coverage area, the 3GPP formally specified a 5G system (5GS) for non-public use, giving rise to *NPNs* as an evolution of basic legacy private mobile networks. Specifically, two standard kinds of 5G NPNs are defined, namely the Standalone Non-Public Network (SNPN) and the Public Network Integrated NPN (PNI-NPN) [3, §5.30]. Both deployment options present different advantages, challenges, and use cases.

Standalone NPN

A SNPN is a 5GS for private use which leverages a novel approach for identifying such a network, that is, via the combination of a PLMN ID and a network identifier (NID). Such (combined) ID is broadcast by the RAN infrastructure to enable authorized UEs to discover the SNPN, thus starting the secured attach procedure which makes the difference with respect to a PLMN. Indeed, a UE that aims at connecting to the SNPN and access its functionalities must be enrolled using a dedicated subscriber list.

Typically, the SNPN is managed and operated entirely by a NPN operator (NPN-Op) that can be the enterprise customer itself or a delegated third-party company. As a matter of fact, in general a SNPN does not share any functionality with the PLMN; the RAN is the only infrastructure element that may be in common. In the latest 5G specifications (Rel-17 at the time of writing [3]), the 3GPP has specified features and characteristics of SNPNs concerning authentication (including via a external credential holder), access control, and onboarding of devices with default credentials.

A SNPN type of deployment provides a valid solution for an enterprise or organization that requires a fully customized configuration and a tight control over the mobile network: these needs also justify the additional overhead of setting up and managing an independent 5GS infrastructure. Another advantage in using SNPN is its strong perception of privacy of sensitive and proprietary data, which are handled locally accordingly to the company security policies.

Public Network Integrated NPN

In many use cases a certain degree of integration between the NPN and the PLMN can be desirable, especially when the private entity does not shoulder the burden of the entire NPN management. Two ways to support a NPN within the network of a PLMN operator (PLMN-Op):

1) via deployment of dedicated Data Network Names (DNN);
2) via deployment of dedicated network slices for non-public use, which may optionally leverage closed access groups (CAG) at access stratum level for access control purposes.

We observe that, in both cases,

- the RAN is shared between the PLMN and its NPN;
- some network functions may be shared between the PLMN and its NPN;
- the non-public users need to subscribe to the same PLMN ID as public users – it is up to the network to enforce user segregation in a correct fashion.

On the other hand, in case the PNI-NPN is supported via a network slice, a dedicated user plane function may be deployed close to the serving RAN, i.e., at the so-called edge cloud.

It is also worth mentioning that additional authentication means are provided to the private network tenants of a PNI-NPN, based on the tenant's own authentication servers, in order to ensure the enforcement of user access control policies by the PLMN-Op.

The Emerging Role of Hyperscalers

Unlike traditional mobile systems for PLMNs, 5G NPNs aim at reaching many independent customers, which are

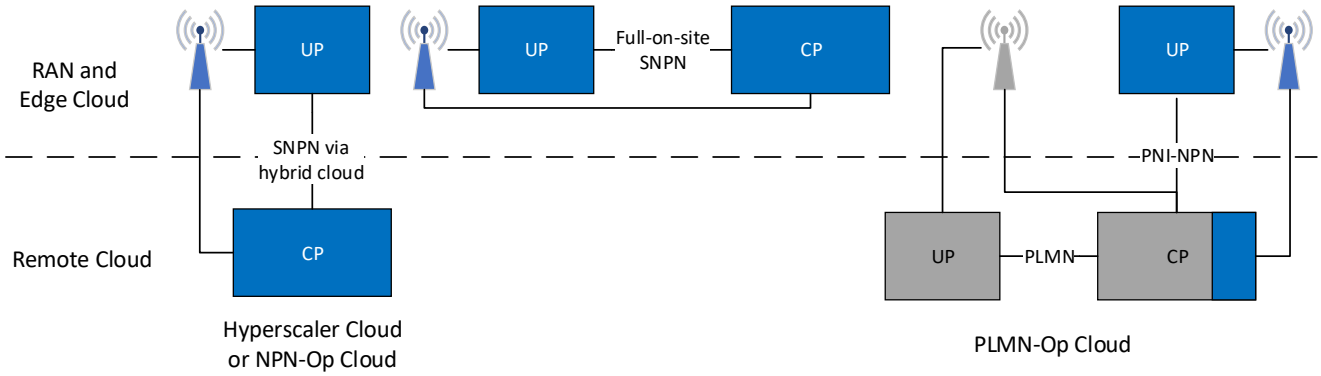


Fig. 1: 5G NPN deployment options. The left-most solution is the SNPN solution powered by the hybrid cloud. The one in the center is the full-on-site SNPN, where the entire SNPN is deployed at the edge cloud, in proximity of the RAN. Finally, the right-most solution is a PNI-NPN where the grey blocks represent the PLMN domain and the blue ones a private network slice comprising the central PLMN CP as well as dedicated user plane function at the edge.

typically much more than the amount of existing PLMN-Op. However, as opposed to a PLMN-Op, the NPN-Op are not technology experts in most cases: this is why new actors come into play. For example, the Regulatory Authorities now play an instrumental role by reserving spectrum portions for direct lease by private entities instead of allocating it to a handful of national operators. Especially in countries where the spectrum can be leased for private use, the traditional role of the PLMN-Op is challenged by independent system integrators and, lately, by *hyperscalers* such as, e.g., Amazon Web Services (AWS) and Microsoft, providing cloud, networking, and Internet services on a very large scale by offering organizations access to infrastructure as a service (IaaS).

As a matter of fact, (both public and private) cloud-based environments can be used for hosting the instances of virtual mobile core networks for SNPN deployments. In particular, as public cloud providers, the hyperscalers typically provide the private entities with a hybrid cloud environment, whereby a SNPN can be split between a remote site featuring non-critical NFs and an edge apparatus comprising the critical NFs.

The role of hyperscalers is yet to be fully unleashed, though they have already entered the mobile network market.[1] Specifically, their experience in the automation field (though not related to mobile networks) gives them an advantage, possibly pushing their proprietary solutions as *de facto* standards. Similarly to the case of PNI-NPNs, the private entity can leverage SNPN powered by hyperscalers to offload part of the network management. This comes at the price of sharing part of the 5G NFs with other tenants.

Summary and Observations

An overview of previously mentioned NPN configurations is provided in Fig. 1 and Table I. In particular, in the table we summarize each NPN configuration feature along with its degree of customizability and the management effort required from the point of view of the NPN-Op. A SNPN deployment provides a much higher level of customizability of the network that can be easily tailored to the needs of the customer and the constraints of the specific use case. As a trade-off, the NPN-Op is required to actively partake in the management of the infrastructure by establishing and maintain personalized configurations, network services and traffic policies. This burden can be partially taken by an hyperscaler. In contrast, by using pre-existing public infrastructures, a PNI-NPN deployment offers a lower operating expenditure (OPEX) and capital expenditure (CAPEX) solution as well as caters to private entities that do not have the expertise and technical know-how. It is the PLMN-Op that maintains most of the management responsibilities and customization options, with only a small set of capabilities that might be exposed to the private network tenant using specific APIs. In fact, a PLMN-Op is not likely to accept anyone else to orchestrate their infrastructure or accessing their proprietary management services with the risk of compromising nation-wide and mission-critical systems [2].

Focus on NPN Standardization

In this section, we describe the communication and management architectures of 5G NPNs from a standardization perspective.

NPN Communication Architecture

Since Industry 4.0 is considered as one of the prominent use cases [5], Fig. 2 shows the end-to-end (E2E) communication architecture of a 5G NPN for this purpose. It can be considered as an embodiment of a 5GS integrated with an edge computing infrastructure, as it comprises three domains accounting for i) RAN, ii) the 5GC, and iii) the ETSI multi-access edge computing (MEC) infrastructure [3]. Specifically, this 5GS can be considered either as a *private mobile network for non-public use*, isolated from the incumbent PLMN, if it uses a PLMN

[1]See, e.g., https://aws.amazon.com/it/private5g/. Last visited: January 2, 2024.

TABLE I: NPN configuration options, their relation with a PLMN, and respective impact on management and orchestration.

CONFIGURATION	RAN	CORE NETWORK	MEC PLATFORM	CUSTOMIZABILITY	MANAGEMENT EFFORT (FOR A NPN-OP)
SNPN	Shared w/ PLMN or dedicated	Dedicated (on site or via hybrid cloud)	Dedicated (on site)	Medium/High: NPN-Op can obtain customized network configurations based on its needs	Medium/High: SNPN owner needs to take care of network management (medium if assisted by hyperscaler)
PNI-NPN	Shared w/ PLMN	Shared w/ PLMN (network slice or dedicated DNN)	Shared w/ PLMN or dedicated (on site)	Low: most of the network is physically shared and partially logically shared, thus has feature constraints	Low: most of the network is centrally managed by the PLMN-Op

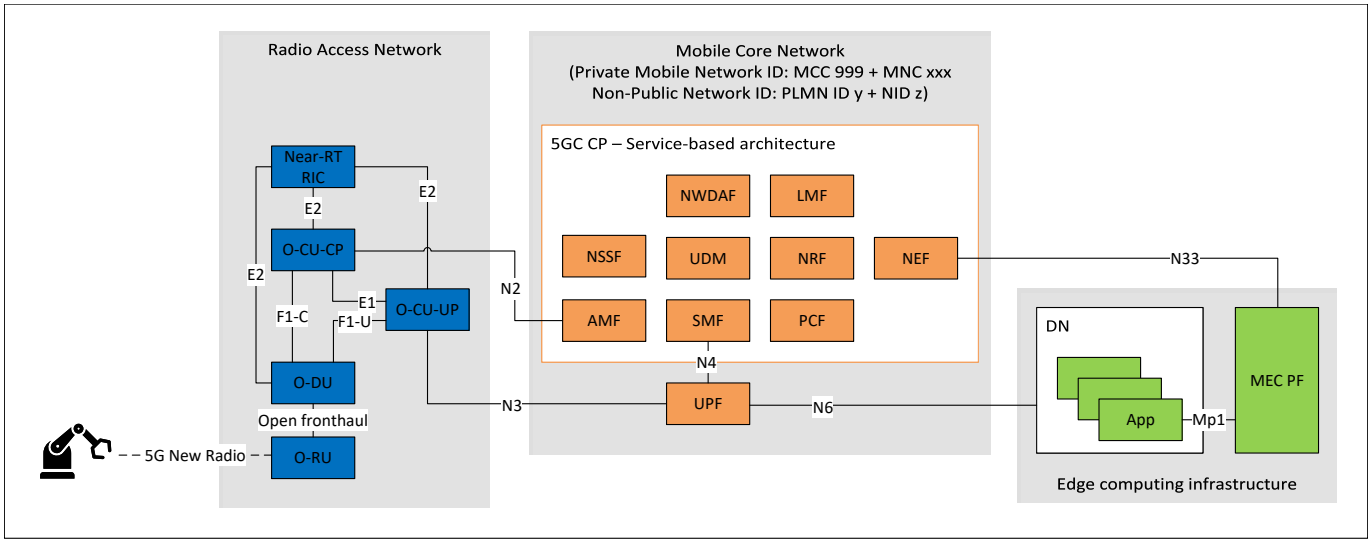


Fig. 2: E2E communication architecture for a generic 5G NPN. NF acronyms and reference points are those defined by the respective standards.

ID with MCC 999 or as a *NPN* if it uses a combination of PLMN ID and NID.

In the figure, two degrees of openness out of the four mentioned previously ones can be identified. About the inter-subnetwork openness, we notice that the N2/N3 reference points ensure the interworking between the RAN and the 5GC domains regardless the adopted network equipment [3]; the same holds for N6/N33 for the interworking between the 5GC and the MEC system [7]. On the intra-subnetwork openness, each of the three domains utilizes standard interfaces among blocks of the same color. At 5GC level, this is significantly simplified by the use of a service-based architecture among control-plane (CP) NFs. At RAN level, important steps forward have been taken with respect to the past. Despite being traditionally the most closed domain, due to the tight binding between hardware and software in radio equipment, the recent contributions brought by the O-RAN Alliance have been yielding a progressive decoupling between the radio software from the hardware. Novel RAN protocol stack split options across (open) remote units (O-RU), distributed units (O-DU), and centralized units (O-CU) were introduced, decomposing the monolithic radio equipment into modules that can effectively interwork with one another [8]. Finally, at MEC level the Mp1 reference point allows MEC applications to discover, advertise, consume, and offer MEC services from/to the MEC platform.

NPN Management Architecture

Considering the previous communication architecture, Fig. 3 shows a (simplified) overview of the respective E2E operations, administration, and management (OAM) architecture. Each of the three domains features a dedicated OAM system specified by the respective standard development organization, namely the 3GPP for the RAN and the 5GC [9] and the ETSI MEC industry specification group for the MEC system [10]. In particular, it is worth observing that the O-RAN Alliance specifies its service management and orchestration framework (SMO) by extending the 3GPP RAN OAM system with several features, including the non-real time RAN intelligent controller (non-RT RIC).

Note that three further domains, which are specific of the management architecture, are introduced in Fig. 3, namely the operations/business support system (OSS/BSS), the hardware infrastructure and the associated transport subnetwork, and the NFV management and orchestration (MANO) framework (in black, white, and grey, respectively). OSS/BSS provide means to the NPN-Op to manage the overall network by leveraging the OAM systems of the various communication domains. To this end, OSS/BSS exploits the NFV MANO framework specified by ETSI for the lifecycle management of the virtual network functions (VNFs). In fact, while the fault, configuration, accounting, performance, and security

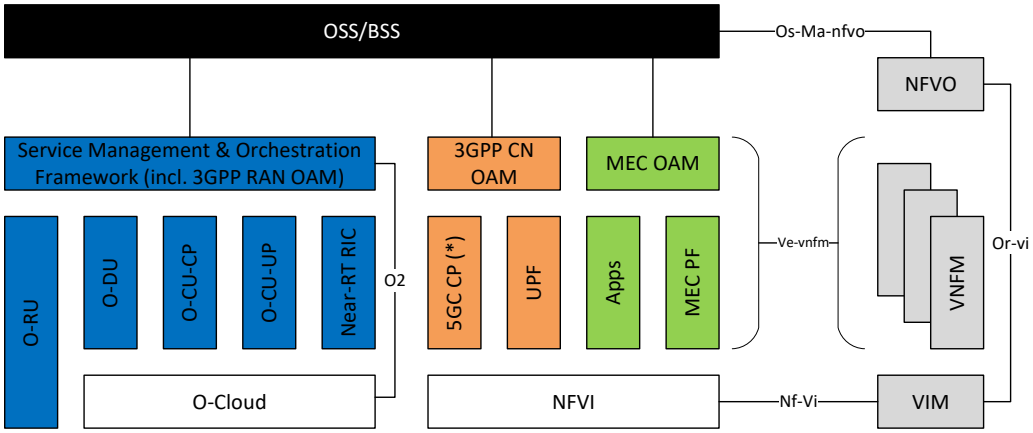


Fig. 3: E2E OAM architecture for the 5G NPN drawn in Fig. 2. Note that not all management entities are shown in this simplified representation. (*): the entire 5GC CP is shown as a unique software instance for graphical constraints only.

(FCAPS) of each VNF is performed by the respective element manager (or domain's OAM), the NFV MANO is responsible for, e.g., provisioning, diagnosing, and healing the virtual instances of VNFs, let them be hosted by virtual machines (VMs) or containers. Finally, all VNFs need to rely on an underlying physical infrastructure, consisting of hardware for computing, e.g., servers, and for the transport network, e.g., switches, routers, and firewalls. These elements are referred to as network function virtualization infrastructure (NFVI) in ETSI NFV and 3GPP, while O-RAN has introduced the concept of O-Cloud. In this respect, it is worth mentioning that, despite the O-Cloud is inspired to a NFVI [11], the two virtualization platforms may not be fully aligned because, e.g., of specific hardware requirements in terms of hardware acceleration needed by the RAN. As a consequence, interfaces between the orchestrator and the virtual infrastructure in O-RAN and ETSI NFV may not coincide in general, as captured in Fig. 3.

An open framework in terms of management architecture enables not only the interoperability among different network equipment vendors, but also the seamless exchange of the NFV orchestration infrastructure, let it be proprietary (e.g., VMware telco cloud automation[2]) or open-source, such as Open Source MANO (OSM) and Open Networking Automation Platform (ONAP) [12]. Moreover, we observe that an autonomous NPN relies on the interworking of all of these domain OAM systems. In this respect, the ETSI zero-touch network and service management (ZSM) industry specification group is working to accelerate the definition of the required end-to-end architecture and solutions.

Important Remarks

The presented architectures refer to an implementation of a 5G NPN for the Industry 4.0 vertical, thus they do not include all components typical of a mobile network for private use. For example, the IP Multimedia System (IMS) and Mission-Critical Push-to-talk (MCPTT), which are crucial enablers for indoor voice communications and public safety, are not shown in Fig. 2. Moreover, the means to integrate the NPN private network with legacy network technologies for private use, like Wi-Fi or Ethernet are missing [2].[3]

Fig. 3 does not fit all NPN setups as well. For example, for NPNs isolated from other systems or dedicated to public safety, dynamic management and orchestration is not of primary importance. Nevertheless, it is apparent that the standard OAM framework turns out to be quite complex, as each domain features independent functionalities, which eventually need to interwork together in order to build an effectively autonomous NPN. Moreover, the picture does not render the complexity caused by the possibly different entities managing the various domains thus exacerbating the problem. In the next section, we will highlight how these shortfalls jeopardize the effectiveness of a smooth E2E OAM of NPNs, also considering the new stakeholders introduced by the private mobile networks paradigm.

Testbed Activities

In order to study the evolution of NPN architectures and their management means towards zero-touch principles, we have been designing and continuously integrating a research and innovation testbed, inspired by the work done in [13].

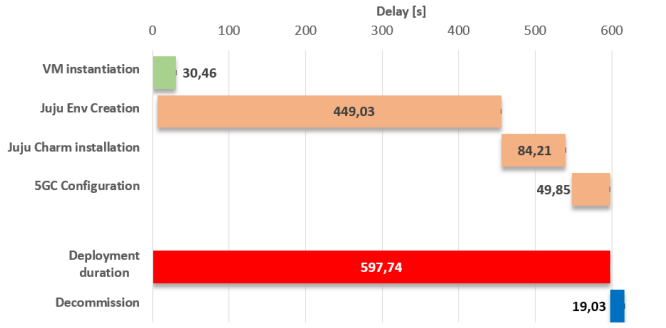
Testbed Architecture

At the time of writing, it comprises two physical machines:

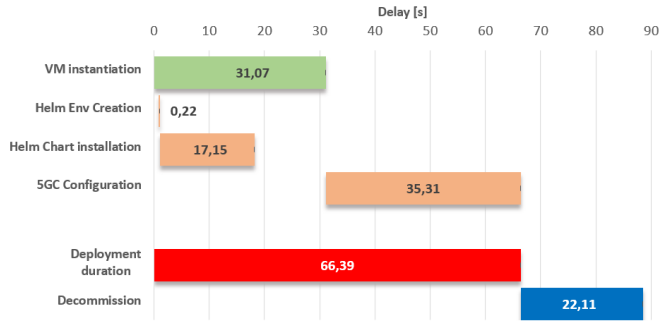
- a Dell PowerEdge R640 server based on two Intel(R) Xeon(R) Silver 4210R CP @ 2.40 GHz and 64 GB of memory, and
- a commodity Desktop PC equipped with an Intel(R) Core(TM) i7-2600 @ 3.40 GHz and 16 GB of memory running Ubuntu 20.04.

[2]https://telco.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-telco-cloud-automation.pdf. Last visited: January 2, 2024.

[3]We recall that a Rel-17-compliant SNPN shall not include non-3GPP access networks.



(a) Deployment using Juju charms



(b) Deployment using Helm charts

Fig. 4: Time delays associated with the 5GC deployments and erasure on the testbed.

The testbed aims at emulating a real world scenario wherein a NPN may be automatically deployed in different configurations and managed accordingly. In particular, the server node simulates a remote cloud datacenter, while the PC node simulates a constrained edge server deployed on the premises of the private entity or network tenant.

The infrastructure is fully virtualized as per ETSI NFV specifications. In particular, OpenStack[4] is utilized as NFVI and Virtual Infrastructure Manager (VIM). The NFVI is composed of the physical hardware resources, including storage, computing and networking, and by the virtualization layer which abstracts them and provides the virtual resources and environment wherein the VNFs carry out their lifecycle. The VIM is responsible for the management of the virtual resources allocated and used by the VNFs.

For the VNF managers (VNFMs) and NFV orchestrator (NFVO), an OSM[5] instance, deployed on a dedicated physical infrastructure, is utilized. OSM is an open source and community-led, ETSI-hosted project that provides a NFV MANO software stack aligned to the latest ETSI NFV information model and architecture. Recently, OSM was successfully tested for zero-touch automation purposes, being capable to support MEC and O-RAN use cases.[6]

[4]https://www.openstack.org/software/. Last visited: January 2, 2024.

[5]https://osm.etsi.org/. Last visited: January 2, 2024.

[6]See https://www.etsi.org/newsroom/press-releases/1863-2020-12-open-source-mano-release-nine-fulfils-etsi-s-zero-touch-automation-vision-ready-for-mec-and-o-ran-use-cases. Last visited on January 2, 2024.

Achieved Results

Within the testbed, we have been pursuing two main industrial research lines on autonomous NPNs:

1) automated SNPN deployment and configuration in both options shown in Fig. 1;
2) automated creation and configuration of a Network Slice Subnet (NSS), constituent part of a network slice for a PNI-NPN, composed of multi-vendor VNFs [14].

As for the former activity, the deployment automation of both hybrid cloud and full-on-site SNPN have been tested using OSM-compatible descriptors. Proprietary and open-source[7] 5GC implementations have been used for this activity. In particular, in Fig. 4 we show the average time delays for 10 consecutive 5GC full-on-site deployments and erasures on the Dell server using the Open5GS implementation. The same deployment has been tested using the two proxy charms alternatives offered by OSM, the former based on Juju bundles and the latter on Helm charts. The total deployment duration (in red) is the sum of the VM instantiation time (in green) and the configuration time of the VNFMs and the VNFs themselves (in orange). The configuration delay is the time necessary to create the environment in which to install and run the charm responsible for the 5GC configuration. This environment differs based on the type of proxy charm that is adopted. Juju uses a Linux container (LXC) while Helm uses a Docker container deployed on the same Kubernetes framework on which OSM is executed. The noticeable difference between the two charm options is mainly due to the fact that Helm is a much lighter and agile system while Juju requires several time-consuming steps before executing the charm. The first and most demanding one is the download of the LXC's cloud image followed by the update and upgrade of the installed packages, which take a substantial amount of time given the limited download speed available at the testbed (100Mbps). This time delay is an acknowledged limitation of OSM and, though mitigation strategies exist, they shall not be used in production environments.[8]

As for the latter activity, we have demonstrated the provisioning, configuration, and control of a NSS, as a part of a network slice supporting a PNI-NPN, using an implemented Network Management System (NMS) conforming to 3GPP OAM standards [14]. The NMS has been deployed on a separated physical infrastructure like OSM, and it interoperates with OSM itself as well as OpenStack to instantiate the NSS' constituent, multi-vendor NFs, that are, a NRF and a UDM, as shown in Fig. 5. The demonstration showed the feasibility of a standard-compliant system to manage the network slicing aspects of a 5GC and compatible with the combination of components from different vendors into an open environment (i.e., not subject to vendor lock-in). This study could be extended to the network slicing of the RAN, but this is left to future work.

[7]Specifically, Open5GS (see https://open5gs.org/) and Free5GC (see https://www.free5gc.org/).

[8]https://osm.etsi.org/docs/vnf-onboarding-guidelines/08-advanced-charms.html. Last visited: January 2, 2024.

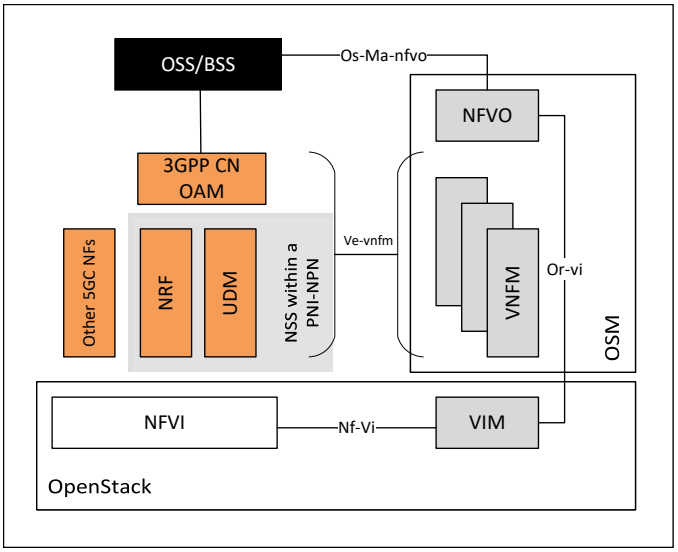


Fig. 5: Exemplary NSS and necessary 3GPP OAM/NFV MANO architecture needed for its automated creation and configuration.

Envisioned Future Challenges

A smooth OAM for 5G NPNs represent the key challenge for the effectiveness of mobile systems for private use. To face this challenge, NPNs need to embrace automation in network and service management and orchestration, so to be seamlessly integrated with the incumbent infrastructure of the NPN-Op as well as to implement extensive zero-touch management approaches. A few crucial challenges need to be faced in the coming years in this regard.

- *Automation easiness* – From the point of view of a NPN-Op, which is likely to be nonexpert of mobile telecommunications, the setup of the overall OAM system for a NPN may be not trivial. Many heterogeneous stakeholders such as the network infrastructure suppliers, the cloud providers, the NFV MANO providers, need to collaborate to build an holistic vision towards a solution of this problem. In this regard, the 3GPP has recently formalized the responsibilities regarding NPN management operations and roles assigned to them [15].
- *Normative work by SDOs* – On the other hand, the technical specifications enabling such an autonomated management need to be harmonized. In particular, the interworking between 3GPP OAM and ETSI NFV MANO which we started investigating in [14] as well as the simplification of ETSI MEC OAM deserves further attention from the involved SDOs. Our demonstration was limited to the configuration aspects, but fault supervision and performance monitoring are other essential functions of a management system.
- *New technological challenges* – The compatibility between public and private cloud infrastructure providers and the associated orchestration tools will be a key factor to preserve the openness of the NPN framework.

All in all, many things are yet to be done in the field of autonomous private mobile networks, but the effectiveness of such a paradigm highly depends strongly depends on the automation tools.

Acknowledgment

This work was supported in part by the European Commission under the projects FUDGE-5G (H2020-ICT-42-2020 call, grant n. 957242) and Affordable5G (H2020-ICT-42-2020 call, grant n. 957317). The views expressed in this contribution are those of the authors and do not necessarily represent the project.

References

[1] M. Wen *et al.*, "Private 5G Networks: Concepts, Architectures, and Research Landscape," *IEEE J. Sel. Topics Signal Process.*, pp. 1–1, 2021.
[2] J. Prados-Garzon *et al.*, "5G Non-Public Networks: Standardization, Architectures and Challenges," *IEEE Access*, vol. 9, pp. 153 893–153 908, 2021.
[3] *System architecture for the 5G System (5GS)*, 3GPP Tech. Spec. 23.501, Rev. 17.5.0, Jul. 2022.
[4] C. Monica, D. Teles, P. Ferro, and P. Antero Carvalhido, "Towards autonomous private 5G networks," Altice Labs, Whitepaper, Mar. 2021. [Online]. Available: https://www.alticelabs.com/wp-content/uploads/2021/10/WP_Towards-autonomous-private-5G-networks.pdf
[5] J. Ordonez-Lucena *et al.*, "The use of 5G Non-Public Networks to support Industry 4.0 scenarios," in *Proc. of 2019 IEEE Conf. on Standards for Commun. and Networking (CSCN)*, 2019, pp. 1–7.
[6] A. Aijaz, "Private 5G: The Future of Industrial Wireless," *IEEE Ind. Electron. Mag.*, vol. 14, no. 4, pp. 136–145, 2020.
[7] S. Kekki *et al.*, "MEC in 5G Networks," ETSI MEC ISG, Whitepaper, Jun. 2018. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf
[8] A. Garcia-Saavedra and X. Costa-Perez, "O-RAN: Disrupting the Virtualized RAN Ecosystem," *IEEE Commun. Standards Mag.*, pp. 1–8, 2021.
[9] *Management and orchestration; Architecture framework (Release 16)*, 3GPP Tech. Spec. 28.533, Rev. 16.4.0, Jun. 2020.
[10] *Mobile Edge Management; Part 1: System, host and platform management*, ETSI Group Spec. 010-1, Rev. 1.1.1, Oct. 2017.
[11] "O-RAN Use Cases and Deployment Scenarios," O-RAN Alliance, Whitepaper, Feb. 2020.
[12] G. M. Yilma *et al.*, "Benchmarking open source NFV MANO systems: OSM and ONAP," *Computer Communications*, vol. 161, pp. 86–98, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366420305946
[13] B. Nogales *et al.*, "Design and deployment of an open management and orchestration platform for multi-site NFV experimentation," *IEEE Commun. Mag.*, vol. 57, no. 1, pp. 20–27, 2019.
[14] A. Ishaq, D. Ronzani, A. Spinato, N. di Pietro, M. Centenaro, A. Bellin, and D. Munaretto, "Service-based management architecture for on-demand creation, configuration, and control of a network slice subnet," in *Proc. of the IEEE Int. Conf. on Network Softwarization (NetSoft)*, Milan, Italy, 2022, pp. 275–277.
[15] *Management of Non-Public Networks (NPN); Stage 1 and stage 2 (Release 17)*, 3GPP Tech. Spec. 23.501, Rev. 17.0.0, Mar. 2022.