Towards a Fully-Fledged Validation of 5G NetApps

Rafael Direito
Instituto de Telecomunicações
Universidade de Aveiro
Aveiro, Portugal
rdireito@av.it.pt

Diogo Gomes
Instituto de Telecomunicações
Universidade de Aveiro
Aveiro, Portugal
dgomes@av.it.pt

***Abstract*—The lack of testing and validation mechanisms for 5G Network Applications poses a severe challenge in ensuring their correct behavior and in reducing their time to market. This work addresses the intricate complexities of validating such Applications and defines some research questions related to this research field. These questions focus on problems that are still unresolved, and based on them we establish future directions for solving such intricate research problems.**

***Index Terms*—Network Applications, Validation, DevOps, Automation, 5G, NFV**

I. Introduction

Network Function Virtualization (NFV) is one of the key enablers of 5G networks, facilitating upgrades on network services and providing them with more reliability and scalability [1]. Even though 5G Network Applications (NetApps) are in high demand, it still lacks tools to validate that their behavior is the expected one. Since NFV scenarios highly differ from traditional network scenarios, one must rely on something other than the well-established certification methodologies that target the traditional scenario [2]. Thus, new validation and certification processes targeting the new network paradigms (e.g., NFV) arise.

DevOps methodologies may be employed to validate Virtualized Network Functions (VNFs). Although initially intended for software solutions, DevOps principles can also be applied in validating VNFs, since these are almost entirely virtualized and thus heavily depend on software rather than hardware [3]. However, even relying on DevOps methodologies, validating VNFs is a complex process due to these entities' broader scope of configurations. Moreover, the validation of 5G NetApps (offered as VNFs) must consider a plethora of different aspects, ranging from the assurance that a particular application can be orchestrated in a specific infrastructure, to more fine-grained performance and security validations, for example [3]. Hence, the complexity in validating such applications.

However, in the face of full-scope VNF validation methodologies, it is possible to ensure the performance, reliability, availability, security, and functional correctness of those Network Functions (NFs). These methodologies, if correctly applied, will enable the massive diffusion of 5G Network Applications. This work presents an overview of what was already achieved concerning NetApps validation methodologies and processes. Furthermore, it intends to propose future directions in this research field. Regarding its organization, this paper is structured as follows. Section II provides some context on NetApp validation methodologies. Then we move to present a brief State of the Art (SotA) on such methodologies on Section III. Based on the presented SotA, we formulate some research questions in Section IV, and provide meaningful insights to establish future direction in our research (Section V).

II. NetApps Validation

Many organizations recognize that new validation and certification methodologies for 5G NetApps and services are required. As examples of these organizations, one may point out the European Telecommunications Standards Institute (ETSI) and the European Commission (EC). ETSI heavily contributes to the standardization of NFV technologies, while the EC continuously pushes for innovative actions toward establishing validation and certification processes to certify NFV-based solutions. As a result, the EC committed substantial monetary amounts to sponsor several research projects to solve these problems. 5GTANGO, 5G-EVE, 5GinFIRE, VITAL-5G, EVOLVED-5G, 5G-IANA, and 5GASP are examples of such research projects, which tackle the many intricate scopes of the validation and certification of NetApps.

Due to the intricate complexity of a NetApp validation process, we opt to decompose it into separate stages. The first stage (Stage 1) is the onboarding of both NetApp and testing artifacts to an orchestration platform capable of instantiating and managing these artifacts. During this phase, compliance testing is performed to validate that the NetApp complies with all aspects required for successful onboarding. Then, we move to Stage 2: pre-deployment testing. Pre-deployment tests ensure that the NetApp can be correctly and securely orchestrated. If the NetApp passes these tests, then it can be deployed. When a NetApp is instantiated, we reach Stage 3: post-deployment testing. In the post-deployment testing phase, one shall conduct a series of experiments to evaluate the functional behavior of a NetApp, its security, its performance, its scalability and reliability, its capacity to interact with the 5G system correctly, etc. Alongside this phase, Stage 4 begins: the gathering of specific Network and NetApp-level metrics. Such metrics are necessary to evaluate the behavior of a NetApp further and to estimate its impact on a 5G infrastructure. After every test comprised by Stage 3 has been performed, Stage 5 may start - the validation of the obtained testing results and the collected metrics. Finally, if Stage 5 is successful, a NetApp can be certified and pushed to a certified NetApp store, making it available to be instantiated in an operator's 5G infrastructure - Stage 6. We now move on to address the SotA regarding some of the phases we defined.

III. NetApps Validation - State Of The Art

This paper does not aim to present a full-blown SotA on the validation of 5G Network Applications. Thus, this section only addresses the most complex aspects of a NetApp validation process. According to the stages we previously defined, these aspects are related to Stages 1, 2, 3, and 4.

A. Stage 1 and Stage 2

Concerning Stage 1 and Stage 2, the solutions achieved in 5GTANGO, 5G-EVE, and 5GASP are the most complete.

In the onboarding process defined in 5GTANGO, NetApp developers must onboard their NetApp descriptors alongside the tests that shall be performed to validate the NetApp. The NetApp descriptors must follow the 5GTANGO-defined schemas, which are backward compatible with ETSI's defined package format. This aspect is validated during the onboarding process. The validation of the descriptors evaluates (i) their syntax (if they follow the defined schemas), (ii) their integrity, and (iii) the validation of Network Services' topology. Furthermore, additional custom rules can be defined to validate the onboarded descriptors [3]. Before onboarding the NetApp descriptors, NetApp developers must sign them. This enables 5GTANGO to link a NetApp's validation results to their descriptors. Since the developers signed these, if anything is updated in the descriptors, the link between the validation results and the descriptors will become invalid [3]. However, 5GTANGO's onboarding approach suffers from a crucial drawback, which is the fact that all developers must onboard their own tests. Given that many tests can be reused to test different NetApps, these could already be onboarded to the 5GTANGO's Verification and Validation (V&V) platform. The developers would only need to invoke them [2]. This approach was employed in 5GASP's onboarding methodologies.

Even though 5GASP's onboarding portal does not validate the onboarded NetApp descriptors, which is a drawback, it provides a vast pool of tests already onboarded to its ecosystem and can be used by all developers. This way, NetApp developers may rely on these tests to validate their NetApps. Furthermore, they can also onboard their tests to complement the tests already offered by 5GASP [4].

5G-EVE demands that NetApp developers onboard their Testing Artifacts alongside the NetApp descriptors, which must be defined using technology-agnostic information models. Concerning the Testing Artifacts, 5G-EVE makes it possible for the developers to onboard (i) Test Case Blueprints, (ii) Experimental Blueprints, (iii) Experiment Descriptors, and (iv) Context Blueprints. Such artifacts allow 5G-EVE to create several validation contexts where the NetApp is validated in different network conditions [5], which is a highly relevant asset of the 5G-EVE project.

Finally, one should also mention EVOLVED-5G since it also improved the NetApp onboarding processes by creating a collection of security tests that ensures the security of all onboarded artifacts.

B. Stage 3

Concerning the post-deployment testing process, most approaches are centered on validating (i) the NetApp's performance, (ii) the interoperability between the NetApp's VNFs, and (iii) the functional behavior of a NetApp [2]. To perform such validations, 5GTANGO relies on a test creation Software Development Kit (SDK). The SDK allows NetApp developers to develop and perform several test cases using Python [3]. Besides this approach, 5GTANGO allows developers to use TTCN-3[1] to implement the desired tests. Moreover, Packetdrill[2] and Switchyard[3] are also tools that are employed to create tests that 5GTANGO can execute.

On the other hand, 5G-EVE defines test cases as a collection of SSH commands that shall be executed on a specific VNF. Even though such an approach enables complete flexibility in defining such tests, this approach is far from ideal. If a Small and Medium-Sized Enterprise (SME) wishes to validate its NetApp on 5G-EVE's platform, it may refrain from doing so since it will have to share the credentials of its NetApp's VNFs with the 5G-EVE platform. By providing access to such credentials, the SME may risk exposing trade secrets, such as the code running inside each VNF. Despite that, 5G-EVE presents a severe advantage compared to other NetApp validation systems. By relying on Context Blueprints, 5G-EVE can generate several NetApp descriptors addressing several network topologies, which enables to validate a NetApp under different infrastructure conditions [5]. For instance, through 5G-EVE's Context Blueprints, one may create a scenario where the network performs poorly by introducing components that will delay packets flowing from one VNF to another. However, the creation of these scenarios is not performed automatically. The developers must constantly upload new Context Blueprints to create new NetApp descriptors. After the descriptors are generated, the developer may use them to request the orchestration of his NetApp and its validation [5]. Such a process can be tedious; thus, an automated approach is required to sustain this testing approach.

5GASP's approach relies on Robot Framework[4] tests to evaluate the functional behavior of a NetApp and its security. Such tests must be onboarded alongise the NetApp artifacts to 5GASP's NetApp Onboarding and Deployment Service (NODS) [4].

Finally, EVOLVED-5G builds upon all approaches previously presented, introducing the concept of 5G readiness tests. These tests validate the interaction between a NetApp and the 5G System. As an initial approach for implementing these tests, EVOLVED-5G developed a Network Function

[1] http://www.ttcn-3.org/

[2] https://github.com/google/packetdrill

[3] https://switchyard.jboss.org/

[4] https://robotframework.org/

Exposure (NEF) emulator [6]. NetApps expected to interact with the NEF are redirected to this emulator, which will collect information on all the interactions between the NetApp and itself. This information will then be used to validate the NetApp during what we defined as Stage 5.

C. Stage 4

5G-EVE heavily relies on metrics to validate NetApp-specific Key Performance Indicators (KPIs). These metrics encompass application metrics and infrastructure metrics. Infrastructure metrics are collected from the infrastructure where a NetApp is instantiated, while the application metrics are gathered through the execution of SSH commands on the NetApp's VNFs [7]. Once again, we must reinforce that requiring SSH access to gather application metrics may pose some concerns to the organizations that wish to validate their NetApps in the 5G-EVE platform.

Contrastingly to 5G-EVE, 5GTANGO only makes available infrastructure metrics. These are collected through several probes deployed in the infrastructure where a NetApp is instantiated. The metrics mainly encompass (i) metrics from the Virtual Infrastructure Manager (VIM), (ii) metrics related to the transport network, and (iii) metrics on the service platform itself [3]. A similar approach is also found in the EVOLVED-5G project [8]. Finally, the 5GASP project also provides the monitoring and validation of infrastructure metrics, which are collected through a similar approach as the one employed by 5GTANGO. However, 5GASP presents an advantage that is not seen, to the best of our knowledge, in any other NetApp validation mechanism. 5GASP allows NetApp developers to provide VNF-level endpoints from where application metrics can be obtained. The developers must list these endpoints in their Testing Descriptor, and the 5GASP system will then rely on them to collect application-level metrics that can then be employed to validate a NetApp.

IV. Research Questions

When analyzing the previously presented approaches, one notices that different research projects focused on solving different issues. While 5G-EVE proposes a highly valuable approach to test NetApps under different network conditions (through 5G-EVE's Context Blueprints), it does not propose any tests to validate the interaction between a 5G NetApp and the 5G System. Contrastingly, EVOLVED-5G is heavily focused on developing 5G readiness tests to evaluate those interactions. Thus, the main issue regarding NetApp validation methodologies is that it still lacks a system able to fully perform a wide-scope validation of NetApps. Furthermore, other issues arise when considering the complexity of onboarding all artifacts to a NetApp validation system and configuring the validation process. Nowadays, considering all available approaches, it is still very complex to configure these validation processes. Hence, there is a need to simplify the onboarding of the NetApp and testing artifacts to the validation system and develop more straightforward mechanisms to configure the NetApp testing processes.

This section focuses on raising Research Questions (RQs) that point out future directions in enabling better and simpler NetApp validation methodologies.

A. RQ1 – How to orchestrate a full-scope NetApp validation process?

A full-scope NetApp validation process involves the orchestration of both NetApp and a plethora of testing agents and artifacts. NetApps may rely on private virtual networks for the communication between their VNFs. Most times, these networks are configured and created through the NS Descriptors (NSDs) of a NetApp, which poses a severe challenge when one wishes to validate the interactions that occur inside those private networks, since a static Testing Agent will not be able to observe such interactions. To address this issue, the Testing Agents must be orchestrated on-demand and have access to all networks on which a NetApp relies upon. Furthermore, a similar situation occurs when one wishes to deploy Monitoring Probes or Stimulation Agents to perform NetApp profiling. Thus, to avoid any change in the NetApp artifacts onboarded by the developers, as occurs in 5G-EVE [7], the orchestration process must comprise 2 phases: the NetApp orchestration phase and the Testing VNFs orchestration phase. The latest phase relies on the outputs of the NetApp orchestration phase, and it is during this phase that the Testing Agents, Monitoring Probes, Stimulation Agents, and all remaining Testing VNFs are orchestrated.

Furthermore, the orchestration layer of the NetApp validation solution, should refrain from employing specific and custom schemas to define NetApp's components. The NetApp orchestrator must comply with the schemas supported by the most common Management and Orchestration (MANO) frameworks, such as ONAP and OSM, for instance. This enables NetApp developers to transparently validate their NetApps without creating specific and redundant descriptors to onboard them to the validation platform. Thus, simplifying the process of onboarding NetApps and Testing Artifacts to the validation platform.

B. RQ2 – How to make available transparent NetApp profiling mechanisms?

5G-EVE presented a novel VNF profiling mechanism [5]. This mechanism relies on the Context Blueprints onboarded by NetApp developers to generate different NSDs, that are used to test NetApp under different network conditions. However, when a developer wishes to perform a new test under different network conditions, he/she must onboard a new Context Blueprint and generate a new NSD [5]. This is troublesome. Firstly, it is a tedious process where no automation is involved. Secondly, because the 5G-EVE platform will regenerate the NetApp descriptors initially onboarded by the developer. This is an issue since, in the presence of an unsuccessful test, the NetApp developer may state that the fault relies on the 5G-EVE platform, blaming an incorrect descriptor regeneration as the culprit for the failed validation process. As an alternative approach, we suggest providing VNF profiling by employing

Software Defined Networking (SDN) technologies. Such an approach would rely on directly instantiating the descriptors onboarded by the developers. After instantiating the NetApp, a validation process would be conducted in an optimal network performance scenario. This would serve as the baseline for the VNF profiling tests. After this step, SDN would be employed to create scenarios that mimic different network conditions. This process would be transparent to the developer, and no action would be needed from him. Furthermore, the logs of the SDN controller would be collected, which, alongside the baseline tests, would make it possible to verify that the VNF profiling tests were properly conducted.

C. RQ3 – Which tests should be considered when validating a 5G NetApp?

As previously stated, different approaches to the problem of validating a NetApp focused on different test scopes. While 5G-EVE, 5GTANGO, and 5GASP heavily focused on validating the functional behavior of a NetApp, EVOLVED-5G opted to pursue the validation of a NetApp's interaction with the 5G system. Thus, currently, no single validation system provides all the tests required to validate a NetApp fully. Due to this, one must study all the testing scopes that may be involved in NetApps validation processes. We suggest addressing the following aspects: (i) integration tests to validate the interoperability of the NetApp, (ii) performance tests, (iii) security-related tests, (iv) General Data Protection Regulation (GPDR) and user license validation tests, (v) Health-check validation tests, and (vi) 5G readiness tests. Furthermore, we also propose the creation of a NetApp Validation Test Store – an archival comprising a plethora of NetApp-related tests and where NetApp developers could freely onboard new tests they may see as useful for the 5G community. All NetApp developers could then (re)use these tests to validate their NetApps.

Even though EVOLVED-5G is actively working on 5G readiness tests, these are still trivial, and there is the need to elaborate further on the aspects that should be validated when evaluating the interaction between a NetApp and the 5G system. An approach that could contribute to this issue is the development of 5G User Equipment (UE) emulators whose behavior could be controlled programmatically. Such an approach would enable mimicking the interaction between the NetApp and its end clients. Another approach is the development of emulators for the 5G Core NFs, such as the approach presented in [6].

V. Research Methodology and Future Directions

Based on the previously presented Research Questions, in this Section, we present our Research Methodology and establish future directions to solve the intricacies related to the validation of NetApps. The first step to enable better NetApp validation methodologies relies on investigating all scopes that must be address during the validation process, so it is possible to design an architecture capable of supporting all those scopes. Thus, an extended and detailed SotA analysis must be performed to raise all requirements of a NetApp Validation System. Moreover, the SotA analysis must also address the different testing scopes that should be considered when validating a NetApp.

Having a better understanding of the challenges laying ahead, the second task of our research is the development of an orchestrator capable of coping with all the requirements and problems identified during the SotA analysis. This orchestrator shall enable a straightforward onboarding of both NetApps and testing artifacts and provide the functionalities addressed in Research Question 1. Furthermore, such orchestrator must also support pre-deployment validation mechanisms, which shall verify if a NetApp is compliant with the defined models and standards, if the NetApp is secure, and if it can be deployed successfully.

The third task of our research work is the development of a pool of tests addressing testing scopes that must be considered when validating a NetApp. The development of such tests will enable a proper validation of our orchestration and validation methodologies. Furthermore, a Test Store shall also be developed to store all tests that our NetApp Validation System may rely upon.

Acknowledgment

This work was supported by the European Horizon 2020 Programme for research, technological development and demonstration under Grant 101016448 (5GASP).

References

[1] M. Touloupou, E. Kapassa, A. Mavrogiorgou, and D. Kyriazis, "Towards optimized verification and validation of 5g services," in *2019 Sixth International Conference on Software Defined Systems (SDS)*, 2019, pp. 5–10.

[2] M. Peuster, S. Schneider, M. Zhao, G. Xilouris, P. Trakadas, F. Vicens, W. Tavernier, T. Soenen, R. Vilalta, G. Andreou, D. Kyriazis, and H. Karl, "Introducing automated verification and validation for virtualized network functions and services," *IEEE Communications Magazine*, vol. 57, no. 5, pp. 96–102, 2019.

[3] P. Twamley, M. Müller, P.-B. Bök, G. K. Xilouris, C. Sakkas, M. A. Kourtis, M. Peuster, S. Schneider, P. Stavrianos, and D. Kyriazis, "5gtango: An approach for testing nfv deployments," in *2018 European Conference on Networks and Communications (EuCNC)*, 2018, pp. 1–218.

[4] K. Trantzas, C. Tranoris, S. Denazis, R. Direito, D. Gomes, J. Gallego-Madrid, A. Hermosilla, and A. Skarmeta, "Implementing a holistic approach to facilitate the onboarding, deployment and validation of netapps," in *2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, 2022, pp. 261–267.

[5] M. Femminella, M. Pergolesi, and G. Reali, "Simplification of the design, deployment, and testing of 5g vertical services," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, 2020, pp. 1–7.

[6] D. Fragkos, G. Makropoulos, A. Gogos, H. Koumaras, and A. Kaloxylos, "Nefsim: An open experimentation framework utilizing 3gpp's exposure services," in *2022 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, 2022, pp. 303–308.

[7] W. Nakimuli, G. Landi, R. Perez, M. Pergolesi, M. Molla, C. Ntogkas, G. Garcia-Aviles, J. Garcia-Reinoso, M. Femminella, P. Serrano, F. Lombardo, J. Rodriguez, G. Reali, and S. Salsano, "Automatic deployment, execution and analysis of 5g experiments using the 5g eve platform," in *2020 IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 372–377.

[8] F. Setaki, I. Mesogiti, E. Theodoropoulou, G. Lyberopoulos, H. Koumaras, D. A. Guillen, J. G. Rodrigo, G. Avdikos, I. Margaritis, E. Kafetzakis, Y. Karadimas, and D. Tsolkas, "The netapps certification environment for 5g and beyond vertical ecosystems: The evolved-5g approach," in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 1182–1187.