SoftFIRE: Constructing a Federated and Orchestrated Multi-Testbed Virtualisation Infrastructure

Serdar Vural
5GIC, University of Surrey, Guildford GU2 7XH, U.K
s.vural@surrey.ac.uk

Roberto Minerva
Trento CLC, EIT Digital, Brussels, Belgium
roberto.minerva@eitdigital.eu

***Abstract*—This paper presents a high-level view of the EU SoftFIRE project's network architecture, providing a description of the federation of multiple testbeds and the current version of the middleware architecture. Some lessons learned in building and using the platform are also presented.**

***Keywords*—virtualisation middleware, NFV, SDN, 5G, multi-site federated testbed, OpenStack, virtualisation experiments**

I. INTRODUCTION

The EU Project SoftFIRE[1] (Software Defined Networks and Network Function Virtualisation Testbed within FIRE+) [1] has the goal of bringing NFV and SDN capabilities to a completely virtualised and multi-site federated testbed platform that spans multiple countries in Europe. The testbed's foundational aim is to nurture an ecosystem of organizations willing to extend, consolidate, and possibly industrialise solutions in the realm of NFV/SDN solutions with a specific reference to their adoption in the 5th Generation (5G) mobile network architectures. SoftFIRE stresses out the importance of federation as a means: to create an open environment capable of encompassing several programmable solutions in the field of NFV/SDN (*programmability*), to identify and solve the interworking issues of the technologies (*interoperability*), and to create a security framework for supporting the needs of NFV/SDN providers (*security*). SoftFIRE regularly invites organisations via its Open Calls for experimenters and provides the selected organisations (experimenters) with the federated testbed as an Infrastructure as a Service (IaaS). This paper describes an overview of SoftFIRE's federated virtualised testbed, outlines its capabilities, and presents the experience in building a multi-site orchestrated federated testbed.

II. SOFTFIRE AND OTHER FEDERATED TESTBEDS

Several federated testbeds supporting virtualisation exist in various parts of the world, with differing scales and capabilities [2]. In this context, SoftFIRE's distinctiveness is to create a programmable environment addressing some important issues at the crossroads of research and industrialisation. Some issues tackled by the project are (*i*) co-existence of NFV and SDN, (*ii*) security within an integrated NFV/SDN environment, and (*iii*) the possibility for developers to quickly use the platform for creating their applications. The project is also offering the possibility to access physical radio resources.

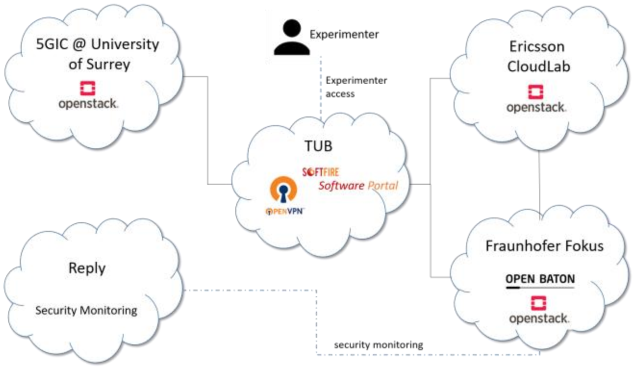
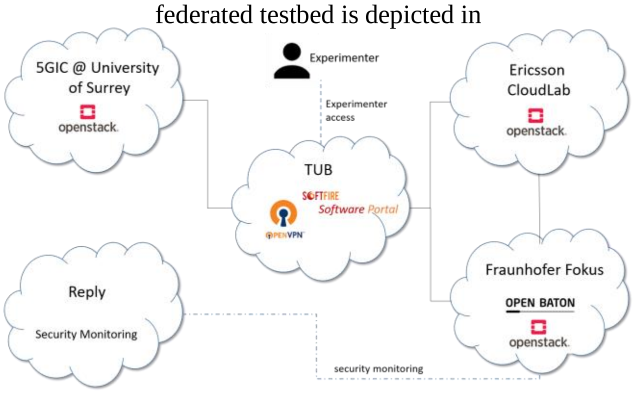


Figure 1: The SoftFIRE federated testbed.

Towards these goals, multiple testbeds have been integrated, providing a federated virtualisation platform to virtualisation experts and enthusiasts: (1) RMED Cloud Lab [3] from Ericsson, in Rome, Italy, (2) FUSECO Playground [4] from FOKUS Fraunhofer/TUB, in Berlin, Germany, (3) 5G Innovation Centre (5GIC) testbed [5] from University of Surrey (UoS), in Guildford, UK. Following its successful integration in 2016, the project is now expanding its testbed with the addition of Deutsche Telekom [6] testbed located in Berlin, Germany. Further expansion is planned in 2017, e.g. the integration of the ADS facility in Rome, Italy. A more detailed description of the component testbeds is available in [1]. The federated testbed is depicted in Figure 1. As can be seen, apart from the three testbeds, software solutions that provide secure connectivity and security monitoring services to the testbed are provided by Technical University of Berlin (TUB), and Reply Security, respectively. The component testbeds in SoftFIRE are connected via a Virtual Private Network (VPN), specifically OpenVPN [7], provided by TUB, which acts as the OpenVPN hub for SoftFIRE.



[1] This paper presents the work carried out by the entire SoftFIRE project, the authors gratefully acknowledge the input of the team.

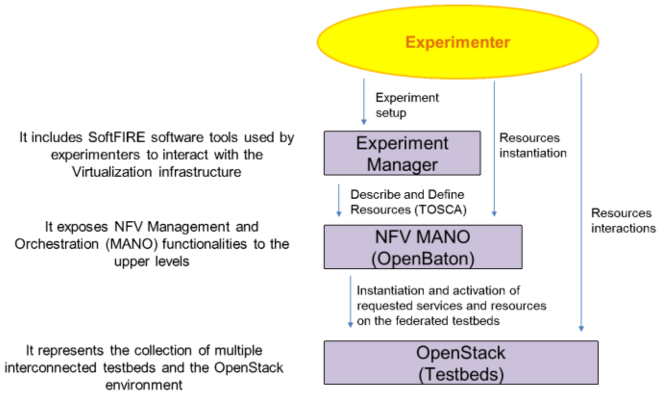

Experimenter
Experiment setup
Resources instantiation
Resources interactions
It includes SoftFIRE software tools used by experimenters to interact with the Virtualization infrastructure
Experiment Manager
Describe and Define Resources (TOSCA)
It exposes NFV Management and Orchestration (MANO) functionalities to the upper levels
NFV MANO (OpenBaton)
Instantiation and activation of requested services and resources on the federated testbeds
It represents the collection of multiple interconnected testbeds and the OpenStack environment
OpenStack (Testbeds)

Figure 2: The SoftFIRE Virtualization Architecture.

The VPN hub is capable of forwarding traffic between different SoftFIRE component testbeds. Access to the OpenVPN server is protected by certificates, which are automatically generated by the SoftFIRE Software Portal (SSP). This server provides network access to registered experimenters so they can directly interact with their NFVs.

III. The SoftFIRE Middleware

Figure 2 represents the high-level architecture of NFV virtualisation within SoftFIRE. The lower layer comprises of the tools and framework used to support virtualisation (e.g. OpenStack), the intermediate layer represents the orchestration capabilities of the platform supported by Open Baton [8], which is an ETSI NFV MANO-compliant [9] open source implementation. The upper layer is the set of tools and features needed to identify and support the experimenters and to map their requests on the available resources of the platform.

VIM implementation: OpenStack. All the SoftFIRE testbeds make use of OpenStack Newton [11]. It is a powerful virtual infrastructure manager (VIM), managing Compute, Networking, and Storage resources all over a datacentre. It also exposes its command line interface which provides developers and users with an extensive set of API commands. Through its dashboard and the API, it is possible to manage the Compute resources, create and configure Networks, and manage Storage resources.

Orchestration of the federated testbed: The Open Baton orchestrator is used to orchestrate various network services on the SoftFIRE federated testbed. Based on the ETSI MANO v1.1.1 specification [32], the orchestrator is designed to address the needs of cloud computing service providers as well as network operators, and is suitable for the virtualisation of various types of networks, such as 5G mobile networks. In particular, it enables dynamic deployment of core network functions and services. In its first year, using the Open Baton orchestrator hosted in Fraunhofer Fokus, the SoftFIRE federated testbed successfully demonstrated such dynamic deployment of 5G network services at its University of Surrey component testbed, to network operators, SMEs, and government representatives in multiple occasions. Open Baton can be easily installed on existing cloud-infrastructures like OpenStack. Each component testbed provides an individual installation of OpenStack, which enables Open Baton to control multiple Point of Presence (PoP), one per testbed. In this setup, each OpenStack instance is completely separated from and unaware of the presence of other component testbeds. Open Baton is the only access point at NFV MANO level, and manages all PoPs. This platform has been the basic infrastructure used by experimenters during SoftFIRE's first Open Call, which ended in February 2017; all the running experiments were executed and supported successfully.

IV. Lessons Learned

Interoperability and reliability issues are inevitable when integrating multiple heterogeneous networks; different component testbeds are likely to have different requirements, regulations, and restrictions. This requires not only development effort, but also IT support. An easy to use programming interface is essential to realise effective use of the platform by experimenters. The key point of consideration is the heterogeneity of experimenter needs; a federated testbed must have a minimal set of requirements, some basic capabilities exposed to experimenters, as well as a set of restrictions imposed on them. While providing ease of use of a wide range of programming capabilities, such interfaces must also enable certification, security, and isolation between users of the platform. Use of open source software is often challenging when different software pieces need to be integrated. The community support on such integration depends on different versions of the open source software pieces, which makes it difficult to realise their effective and timely integration. Furthermore, the integration of an infrastructure orchestrator with multiple OpenStack instances running at multiple sites is challenging, requiring considerable development effort towards providing suitable plugins, proxies, and managers. It is of utmost importance to plan how many experimenters/users are on the network and how many virtual machines exist, and the amount of resources consumed in aggregate and individually by different experimenters. Furthermore, security and safety mechanisms must be in place to protect the infrastructure from malicious users, and to avoid unintentional damage to experimenter software caused by improper use of the platform by experimenters. Although it has various challenges as outlined above, an integrated federated testbed paves the way to the future network function virtualisation realisations, such as operator control of a virtual mobile network with network slicing, or flexible and scalable multi-site virtual infrastructures to be provided by datacentre operators. Towards this, the SoftFIRE testbed has enabled a multi-site virtualisation platform – one of the most recent such deployments in the world readily used by experimenters.

References

[1] EU SoftFIRE project, https://www.softfire.eu/

[2] "Network Function Virtualization: State-of-the-Art and Research Challenges", Rashid Mijumbi, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck, Raouf Boutaba, IEEE Communications Surveys & Tutorials, vol 18, no 1, 236-262, September 2015,

[3] Ericsson RMED CloudLab, https://www.ericsson.com/portfolio/services-and-solutions/learning-services/education-centers/rmed

[4] Fraunhofer Fokus, FUSECO Playground, https://www.fokus.fraunhofer.de/go/en/fokus_testbeds/fuseco_playground

[5] 5G Innovation Centre (5GIC), University of Surrey, http://www.surrey.ac.uk/5gic

[6] Deutche Telekom testbed, https://www.telekom.com/en/company/special--5g-haus

[7] OpenVPN, https://openvpn.net/

[8] OpenBaton, https://openbaton.github.io/

[9] ETSI MANO specification, http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf

[10] OpenStack open source cloud computing software, https://www.openstack.org/

[11] OpenStack Newton, https://www.openstack.org/software/newton/

[12] Zabbix, http://www.zabbix.com/