30

Federated Experimentation Infrastructure Interconnecting Sites from Both Europe and South Korea (SmartFIRE)

Kostas Choumas[1], Thanasis Korakis[1], Jordi Ordiz[2], Antonio Skarmeta[2], Pedro Martinez-Julia[3], Taewan You[4], Heeyoung Jung[4], Hyunwoo Lee[5], Ted "Taekyoung" Kwon[5], Loic Baron[6], Serge Fdida[6], Woojin Seok[7], Minsun Lee[7], Jongwon Kim[8], Song Chong[9] and Brecht Vermeulen[10]

[1]University of Thessaly
[2]University of Murcia
[3]National Institute of Information and Communications Technology (NICT)
[4]Electronics and Telecommunications Research Institute
[5]Seoul National University
[6]University Pierre and Marie Curie
[7]Korea Institute of Science and Technology
[8]Gwangju Institute of Science and Technology
[9]Korea Advanced Institute of Science and Technology
[10]iMinds

30.1 Introduction

The main achievement of SmartFIRE [1, 2] is the design and implementation of a shared experimental facility spanning different testbeds, which are platforms located in Europe (EU) and South Korea (KR) and offered for conducting transparent and replicable testing of networking protocols and technologies. The SmartFIRE user is able to exploit a *federation* of testbeds, meaning that the testbeds are capable to operate both individually as well as in a unified and collaborative manner. Before SmartFIRE, the participating testbeds in the federation were able to provide diverse resources for experimentation,

including WiFi, WiMax and LTE enabled nodes, as well as virtual and physical OpenFlow switches and other SDN devices. However, the user of these infrastructures was not able to access them simultaneously and experiment on heterogeneous network environments that leverage on all the aforementioned resources. Now, the SmartFIRE testbeds have been significantly extended and federated in the experimental, as well as the control plane.

The federations on the experimental and control plane respectively mean the development and operation of simplified and user friendly interfaces, which take charge of the orchestration of the experimentation over all testbeds (experimental plane), as well as the reservation and provision of the resources of all testbeds (control plane). Both directions are supported by the leading experimental and control frameworks adapted by most global testbeds, which are the cOntrol and Management Framework (OMF) [3, 4] and the MySlice tool [5] that is based on the Slice Federation Architecture (SFA). The OMF framework, initially supporting control and experimentation in wireless testbeds, has been expanded in order to support SDN experimentation with OpenFlow switches and Click Modular Routers [7, 8], thus integrating wireless with OpenFlow testbeds [9]. Moreover, unique features, only existing in the KR testbeds have been integrated into OMF [10], unleashing the hidden potential of experimenting with novel resources. On the other hand, the developed SFA extensions enable the federation in the control plane allowing the assignment of multiple heterogeneous resources under a single slice, meaning an isolated set of resources that could be used together in one experiment.

The interconnection of the aforementioned EU sites takes advantage of the GEANT [11] network, while the respective KOREN/KREONET [12, 13] is utilized by the KR sites. The two disjoint networks are interconnected via the Trans-Eurasia Information Network (TEIN) [14] and the Global Ring Network for Advanced Application Development (GLORIAD) [15]. Last but not least, SmartFIRE really showcases its potential with the implementation of two representative use cases, designed to demonstrate the power of the EU-KR shared Future Internet experimental facility. The first experiment explores different mobility scenarios based on the Mobile Oriented Future Internet (MOFI) architecture [16], while the second experiment shows the benefits of an Information Centric Networking (ICN) architecture that achieves efficient content delivery. Finally, the large scaled federated facility is a significant promotion on the joint experimentation among EU and KR researchers, encouraging them to conceive and implement innovative protocols, able to take advantage of the current leading network technologies.

30.2 Problem Statement

The KR testbeds of SmartFIRE (OF@TEIN testbed of GIST, KREONET-Emulab of KISTI, MOFI testbed of ETRI, ICN-OMF testbed of SNU and Open WiFi+ testbed of KAIST) are geographically distributed in multiple sites throughout KR, including most of the well-known local facilities and sharing a minimum set of common SDN features, which are exploited towards the support of new networking protocols and architectures. Although they are able to offer individually an enriched environment for SDN experimentation, they do not share the same enhanced set of wireless experimentation capabilities with the EU testbeds. On the other hand, the EU testbeds of SmartFIRE (NITOS testbed of UTH, w-iLab.t testbed of iMinds and GAIA testbed of UMU) offer different aspects of wireless access networks, which are being controlled and operated in a common manner, participating also in other federations such as Fed4FIRE [17] and OpenLab [18]. However, they could improve significantly their experimentation diversity if they could be federated with the KR testbeds.

More specifically, the experimentation capabilities of all SmartFIRE testbeds, which are depicted in Figure 30.1, are presented below:

- Gwangju Institute of Science and Technology (GIST) offers OF@TEIN, which is an aggregated OpenFlow island consisting of 7 racks, located over 7 international sites. In the OF@TEIN testbed, similar to the GENI racks, a unique rack is designed and deployed to promote the international SDN research collaboration over the intercontinental network of TEIN. OF@TEIN aims at a) the design and verification of the racks (with domestic-vendor OpenFlow switch), b) the site installation and verification of the OF@TEIN network, and c) the design and development of

Figure 30.1 SmartFIRE testbeds.

the OF@TEIN experimentation tools. GIST provides also a cloud service based on OpenStack, offering virtualized resources.

- Korea Institute of Science and Technology Information (KISTI) offers an emulation based network testbed in the KREONET domain. It is called KREONET-Emulab and provides the opportunity for evaluation of several network protocols. Many network protocols, which cannot perform over KREONET due to unexpected hazard, can be freely tested in KREONET-Emulab. It consists of 42 powerful servers, each of them equipped with 5 network interfaces, one for the control and four for the experimentation. Each server can work as a router with 4 paths, and each network interface can be configured up to 1 Gbps.
- Electronic and Telecommunications Research Institute (ETRI) proposes the network architecture of MOFI. Following a completely different approach from the current IP networking, MOFI enables the development of networks with Future Internet support of mobile intrinsic environments. The evaluation of the MOFI architecture relies on the OpenFlow-based mobility testbed of ETRI. The mobility testbed is an aggregation island, consisting of four interconnected South Korean domain networks. Their interconnection is based on the KOREN networking infrastructure.
- Seoul National University (SNU) proposes the ICN-OMF architecture, as a result of the research on the development of content centric networking applying it to the OMF framework. In particular, ICN-OMF is the architecture for the development of ICN-based networks using Open-vSwitch and CCNx over virtual machines. It provides functionalities for in-network caching, as well as for their name-based forwarding. Additionally, SNU operates the ICN-OMF testbed which enables the experimentation on ICN.
- Korea Advanced Institute of Science and Technology (KAIST) provides a wireless mesh network, named Open WiFi+, which is a programmable testbed for experimental protocol design. It is located at the campus of the KAIST University and it consists of 56 mesh routers, 16 of them being deployed indoors and 40 outdoors, each of them equipped with three IEEE 802.11 b/g/n WiFi cards. Moreover, 50 sensor nodes are deployed at the same campus.
- University of Thessaly (UTH) provides the NITOS facility, which is open to the research community 24/7 and it is remotely accessible. The testbed consists of 100 powerful wireless nodes, each of them equipped with 2 WiFi interfaces, some of them being 802.11n MIMO cards and the rest 802.11a/b/g cards. Several nodes are equipped with USRP/GNU-radios,

cameras and temperature/humidity sensors. The nodes are interconnected through a tree topology of OpenFlow switches, enabling the creation of multiple topologies with software-defined backbones and wireless access networks. The testbed features programmable WiMAX and LTE equipment, fully configurable with an SDN backbone.

- iMinds supports the generic and heterogeneous w-iLab.t facility. It consists of two wireless sub testbeds: the w-iLab.t office and w-iLab.t Zwijnaarde. The w-iLab.t office is deployed in a real office environment while the testbed Zwijnaarde is located at a utility room. There is little external interference at the Zwijnaarde testbed as no regular human activity is present and most of its walls and ceiling are covered with metal. The majority of devices in w-iLab.t are embedded PCs equipped with WiFi interfaces and sensor nodes. Since the Zwijnaarde testbed was deployed more recently, the devices in this testbed are more powerful in terms of processing power, memory and storage.
- Universidad de Murcia (UMU) offers the research and experimentation infrastructure of GAIA. GAIA comprises several network nodes interconnected with different technologies. On the one hand, they are connected to the campus network through Gigabit Ethernet switches and thus they form the point of attachment to the Internet. On the other hand, they are connected to a CWDM network, which acts as backbone/carrier network and can be adapted to different configurations, depending on the specific requirements of each experiment. GAIA has also a wide wireless and WiMAX deployment along the campus. This, together with other smaller wireless deployments, allows the experimentation with many local and wide-range wireless technologies, including mobility and vehicle (V2V) communications.

Based on the individual experimentation capabilities of these testbeds, the main SmartFIRE goal was to operate an extended federated facility in KR and EU that could combine the strong points of the independent testbeds towards a joint infrastructure that could efficiently provide more research abilities for experimentation. The federated function and collaborative operation of all these testbeds could allow the experimentation with novel applications, under highly automated conditions, easily operated and managed. For example, the OpenFlow-based SDN is an emerging technology, which was supported by few testbeds before SmartFIRE, enabling the experimentation with content-centric architectures and protocols focusing only on the wired networking. SmartFIRE improved the capabilities of this experimentation environment by enabling the wireless support for all OpenFlow-enabled testbeds.

Except for the lack of diversity in the experimentation environments, coming from the fact that the SmartFIRE testbeds were not federated, another problem in the status before SmartFIRE was the adoption of different control and experimentation frameworks from these testbeds. The use of different frameworks made difficult the repeatability in the experiments description and execution. Before SmartFIRE, the researchers had to become familiar with the special tools used in each isolated testbed, in order to succeed conducting their experimentation. If they wanted to repeat their experimentation in another testbed with the same resources, they had to translate their experiment description to another accessible language for the tools of the other testbed. After SmartFIRE, the included testbeds are handled by common and widely adopted tools and frameworks that release the users from time-consuming learning curves and translations of experiment descriptions.

30.3 Background and State of the Art

Future Internet is the breakthrough innovation that changes our society in terms of economic, social, entertaining, informational, governmental or daily aspects. Many organizations and institutions are working for improving and upgrading the status of the nowadays Internet, facing a variety of inherent problems related to scalability, suitability, sustainability, energy efficiency, security, etc. Their efforts include the participation in various projects that introduce the fundamental redesign of the Internet architecture and protocols. These projects mostly support the development of large-scale experimental facilities and testbeds that provide easy experimentation in proposed theoretical formulations.

The Future Internet Research and Experimentation [19, 20] (FIRE) program, funded by the European Commission, and the Global Environment for Network Innovation [21] (GENI), funded by the National Science Foundation (NSF), are two leader projects that concentrate on the creation and functionality of large-scale testbeds that will provide insights and directions for the Future Internet evolution. Under these programs there are various testbeds that seek to provide researchers with well-dimensioned computing, storage, sensor and network resource slices.

The FIRE initiative in Europe aims at experimental research and funds projects to produce Future Internet research and experimentation facilities, like OpenLab and OFELIA [22]. OpenLab provides an open, both large-scale and sustainable federated testbed, including PlanetLab Europe, the NITOS wireless testbed and other federated testbeds like PlanetLab Korea

and PlanetLab Central. OFELIA is another program that provides OpenFlow-based experimentation capabilities to experimenters and researchers, spanning multiple OpenFlow-based islands in Belgium, Germany, Spain, Switzerland, UK, Italy and Brazil. Fed4FIRE is the newest effort to create a federation of all FIRE testbeds, providing easy access to them through a powerful and well accepted set of tools, which is elaborated in synergy with GENI.

OMF6 is the latest version of OMF, which is a generic framework included in the FIRE and GENI adopted tools and allows the definition and orchestration of experiments using shared resources from different federated testbeds. OMF6 is the successor of OMF5, which was originally developed for single wireless testbed deployments, but now it is extended to support multiple deployments and various features. Its architecture is modular consisting of different components endowed with the operation of the experiment orchestration and the resource control. As it is depicted in Figure 30.2, using a simple human readable experiment definition, OMF6 is supporting the whole experiment lifecycle, cooperating also with its accompanying framework, OMF Measurement Library (OML). The experimenter submits a simple script to the OMF6 Experiment Controller (EC) and the underlying functionality is responsible for setting up the resources, running the defined applications and collecting the results in an organized way.

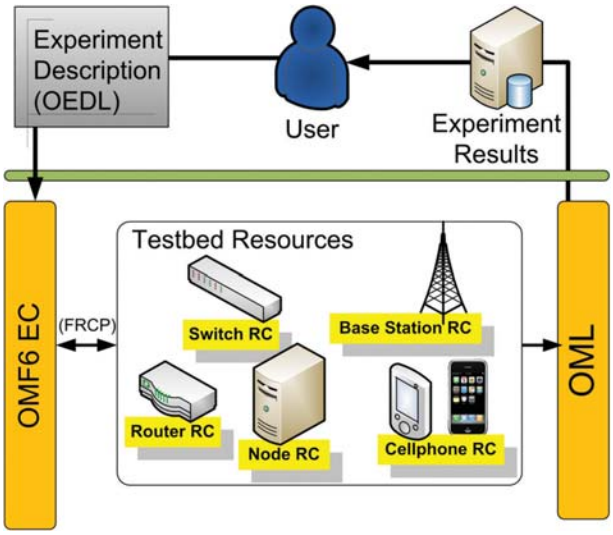

Figure 30.2 OMF6 architecture.

First, OMF6 provides a domain-specific language based on an event-based execution model to fully describe even complex experiments (OEDL). OMF6 also defines a generic resource model and concise interaction protocol (FRCP), which allows third parties to contribute new resources as well as develop new tools and mechanisms to control an experiment. It uses a standardized sequence of messages sent by the EC to the Resource Controllers (RCs) and vice versa. The RC is a daemon that behaves as a proxy between the EC and the resource, translating the messages of the EC to executable commands for the resource and vice versa. Testbed operators are able to use this flexible protocol to extend the experimenter's control on new testbed resources or even establish federations of testbeds, thus enhancing the experimentation ecosystem. In SmartFIRE, we took advantage of this feature in order to extend OMF6 support to OpenFlow and SDN resources, such as Click Modular Routers. In this way, there is one framework in the experimental plane that is able to coordinate the experimentation over network topologies with both wireless and SDN resources.

In the control plane, both FIRE and GENI have designed the Slice Federation Architecture (SFA), defining the interface that should provide each testbed want to be federated. The testbeds resources have to be described in RSpecs (Resource Description) and managed by a SFA Aggregate Manager (AM), which provides a SFA compatible interface. This interface enables the discovery, reservation, provisioning and releasing of all testbed resources in a unified and common way. MySlice is a software tool that interacts with the SFA interfaces and provides a portal, where the user is able to see the testbeds, as well as information about their location, status and resources (see Figure 30.3). The SFA and MySlice are already used by many FIRE projects, including OpenLab and Fed4FIRE, and they are also adopted by SmartFIRE.

30.4 Approach

As we have already mentioned, the set of KR and EU experimental infrastructures consists of five and three testbeds respectively, each one featuring unique characteristics. Except of expanding the OMF6 framework to support all these features, SmartFIRE did significant work to also extend the OpenStack [23] and ProtoGeni [24] frameworks. The extended OMF6 framework is now utilized by the SNU, KAIST, ETRI, UTH, iMinds and UMU testbeds, while the corresponding versions of OpenStack and ProtoGeni are exploited by the GIST and KISTI testbeds respectively. All these testbeds are federated in the control plane with use of the SFA based software of MySlice.

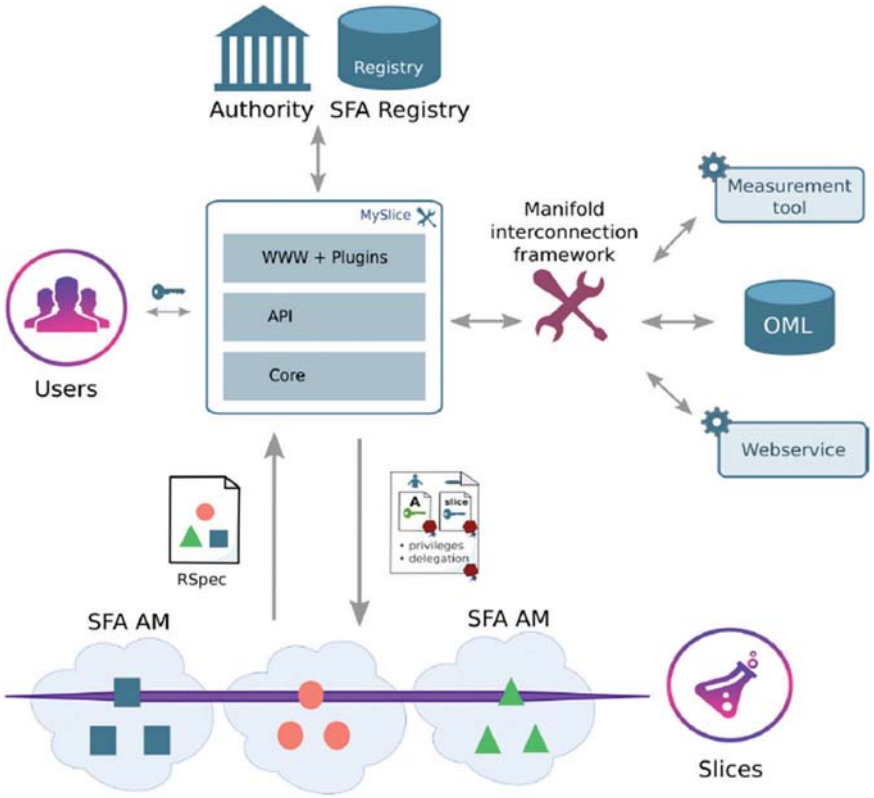

Figure 30.3 MySlice and SFA.

a) The contributions on the OMF6 framework are summarized below:

- **OMF6 extensions for ICN experimentation support**. ICN recently attracts much attention from researchers of Future Internet Architecture, due to its novel communication model, distributing/retrieving the contents by its name (i.e., "what") rather than accessing the location the contents resides ("where"). "Cisco's Visual Networking index: Global Mobile Data Traffic Forecast Update, 2013–2018" reported that the communication behavior of Internet has been shifted to publisher/subscriber model, which is more optimistic for content distribution/retrieval. However, the current IP-based Internet architecture is not designed to accommodate this communication model. With this motivation, ICN proposes to remedy the problems the Internet encounters (i.e., an inefficient communication model for contents distribution and retrieval) exploiting

the capabilities of SDN. Appropriate OMF6 extensions are required for enabling the configuration of ICN topologies with parameterized number of content publishers and subscribers.

- **Enabling experimentation on Mobility-based communication using OMF6**. GENI has noted that wireless/mobile will be the major access means for Future Internet. MOFI effectively realizes a seamless mobility architecture in the Future Internet. It utilizes Host Identifiers (HID) that represent "who is the user (human) or user's equipment (host)?" and Locators (LOC) that represent "where is the user or the equipment?". The HID is decoupled from the LOC. The enhanced OMF6 framework of SmartFIRE is able to control and manage domain networks that contain various Open-vSwitch (OvS) [25] resources as access routers and follow the MOFI architecture.
- **OMF6 support for new software and hardware resources, like**:
  - The OvS software that enables the creation of virtual switches with use of Linux operated computers. Although Open-vSwitch has been initially developed for managing wired networks by creating virtual switches, it can be efficiently used for managing wireless interfaces that are parts of such a switch.
  - The Click Modular Router is another long established software tool that its capabilities can be exploited for SDN development. More specifically, Click enables the development of Software Defined Routers with use of Linux operated computers. In [26], the authors present how they utilize Click and OMF6 to experiment with distributed loading shedding schemes.
  - The FlowVisor [27] software that enables the slicing of OpenFlow switches. FlowVisor will be used as the network virtualization layer, allowing for the physical network to be sliced by the control framework, and for each slice to be controlled by the OpenFlow controller associated with this slice. This feature is very crucial for testbed facilities with slicing mechanisms, enabling the simultaneous use of the included resources from multiple experimenters.
  - The Linux operated computers named M-Boxes, which enable the experimentation on virtual wireless topologies with use of Virtual Machines (VM) and OvS.
  - Wireless Access Points (AP) that are extended in order to be controlled even in terms of the utilized transmission power. The experimentation with wireless APs illustrates the big difference between the theoretical and actual performance of the protocols

for wireless networking. In the experimental research, the use of actual radio resources is becoming more and more important and the need for a real wireless environment testbed is increasing.

b) The contributions on SFA and MySlice are:

- **The development of the SmartFIRE portal**, which provides a graphical user interface that allows users to register, authenticate, browse all SmartFIRE testbeds resources, and manage their slices. This work was important to provide a unified and simplified view of many hidden components to the experimenter.
- **The definition of new RSpecs for the new SmartFIRE resources**. In this way the new resources can be viewed in the SmartFIRE portal. Of course, the RSpecs are reproducible and it is not needed to be defined again for the same type of resources used in another testbed.

c) Last but not least, the physical interconnection of the EU and KR testbeds and their federation in a unified experimentation platform that enables their control and management through a single framework.

30.5 Technical Work

30.5.1 ICN-OMF

Although there are lots of proposals investigating on architecture of ICN, their methodologies to evaluate and validate ideas still stay at unrealistic simulation or small-scale emulation. However, to become a new protocol deploying at the production networks, it should be validated and evaluated on real physical testbed, providing scalability, configurability, and low-cost to researchers. Thus, if there is a formulaic testbed for ICN, the experimenters can only focus on their own experiments without concerning cumbersome learning curves. SmartFIRE developed and deployed ICN-OMF, leveraging and extending OMF6 to control and manage globally dispersed ICN nodes (i.e., publishers, subscribers, or routers).

The experimenter is able to use OEDL to describe the ICN experiment, while the final ED is given to the EC which communicates with the ICN-RCs, as it is illustrated in Figure 30.4. The whole experimentation process is the same with the OMF6 one that was described before, with the only difference that all related parts are enhanced to support ICN experimentation. In particular, the ICN-RC is responsible for configuring the physical nodes by creating virtual switches and virtual machines behaving as ICN nodes on demand.

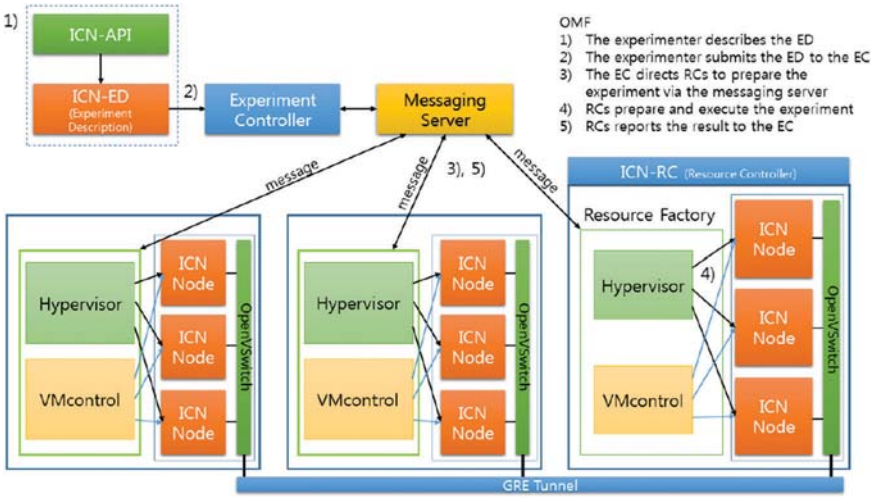

Figure 30.4 ICN-OMF framework.

Since ICN is a clean-slate network architecture that is not compatible with the current IP-based network, ICN networks are built as overlay networks. The CCNx open-source software is used, since it is one of the most well known candidates for ICN and it is widely used. SmartFIRE experimenters are able to utilize this framework in order to validate and evaluate their ideas in a convenient way.

30.5.2 MOFI-OMF

ETRI builds the MOFI testbed which consists of multiple domains interconnected through a global backbone network, such as Internet. All communication entities have one or more global HIDs that are necessary for the development of end-to-end communication channels. In the MOFI architecture, each domain network has multiple Access Routers (ARs) that take care of attached communication entities and one or more Gateways (GWs) that interconnect the domain networks through the backbone network. This network architecture is implemented with use of OpenFlow and SDN technologies. The ARs are based on the Open-vSwitch software and they are controlled by OpenFlow NOX controllers. These controllers are responsible for the domain networks, as well as the GWs that support the inter-domain communication.

In order the MOFI testbed to be operated and managed by OMF6, SmartFIRE extended OMF6 to control and manage the MOFI domain networks consisting of various resources such as the OvS based ARs and GWs.

As it is depicted in Figure 30.5, MOFI network domains are created with use of OvS instances which are configured by the corresponding RCs. The OvS instances are either the points of attachment for the hosts or the GWs that interconnect the domains. Both RCs and EC are able to support the description and control of specific MOFI components, which are identified and used by the experiments without the need to deploy the full networking stack on a generic resource. During the configuration phase of resources, OMF6 deploys specific links among the components, thus the switches and routers are connected to each other and to the hosts. Moreover, OMF6 manages the specification of low-level software components, such as kernel modules. This is addressed during the resource set-up phase so the general deployment of the networking element into the resource is sped up and the experiment definition is simplified. Network links should be supported as a special resource, which is not supported now, since the links are associated to the resources they are connected.

30.5.3 Open-vSwitch (OvS)

The creation of virtual OpenFlow switches relies on OvS, which is used in multiple commercial products and runs in many large scale production networks. Although OvS has been initially developed for managing wired networks by creating virtual switches, it can be efficiently used for managing

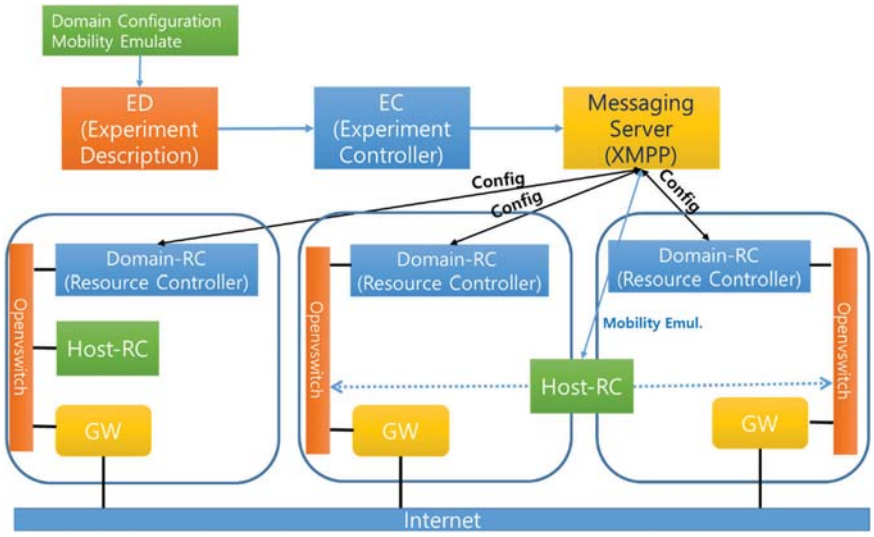

Figure 30.5 MOFI-OMF framework.

wireless interfaces that are parts of a switch. If such an interface is placed in OvS, the experimenter has the ability to intercept the traffic that is exchanged over the wireless interface as Ethernet based frames (since the wireless header is removed upon each packet reception by the wireless driver). Although this seems to be a time saving advantage for the researcher, it also poses many questions regarding the controllability of the SDN enabled wireless switch. To this aim, SmartFIRE enables a Simple Network Management Protocol (SNMP) agent process on the wireless nodes, which allows us to remotely configure the wireless interfaces in a software defined manner.

Based on these processes for creating wireless OpenFlow switches, SmartFIRE developed the corresponding extensions to the OMF6 framework that allow this functionality. The OMF RC entity is significantly extended, in order to be in charge of receiving the proper configuration messages and applying the corresponding settings to the resources. All the existing commands of the OvS API are supported by our extensions. Complementary to this, SmartFIRE developed the appropriate exchange messages among the OMF6 entities for instructing the RC to send the appropriate snmp-set commands for configuring the wireless interfaces, and the snmp-get commands for retrieving their status. Accordingly, the OMF EC entity, which is in charge of sending the appropriate messages to the RC based in the experiment description submitted by the user, has been extended to support this functionality.

The messages exchanged are based on the FRCP standardized by the OMF6 research community. With our extensions, the experimenter can now use the testbed framework to transparently create and configure virtual switches, combining even wireless resources, in large scale using a user friendly and human readable experiment description. An example of such a setup is the configuration of an OvS instance consisting of the wireless interface of a node, the initiation of an OpenFlow controller to control this switch, and multiple wireless clients to connect and generate traffic accordingly on the wireless network, in a single experiment definition. The aforementioned OMF6 extensions have been developed and evaluated using virtual switches combining several heterogeneous wireless technologies. Namely, our extensions support the concurrent operation and configuration of Atheros and Intel based Wi-Fi interfaces, Intel and Teltonika WiMAX interfaces and Huawei LTE interfaces in a single OpenFlow wireless switch.

30.5.4 Click Modular Router (Click)

Click Modular Router is another long established software tool that its capabilities can be exploited for SDN development. More specifically, Click

enables the development of Software Defined Routers with use of Linux operated computers. In Roofnet [28], Click developers investigated wireless connectivity issues and proposed a routing algorithm named after it. Their framework is extensible and well documented, enabling the implementation of many routing algorithms with significantly low effort. The alternative option for packet forwarding in a wireless mesh is the 802.11s protocol, that relies on a similar approach called path selection. Nonetheless, Click is much more flexible and extensible than the existing 802.11s implementations. Many testbeds utilize Click to implement wireless mesh networks, enforcing their computer resources to behave as wireless software defined routers.

Our extensions to support the Click framework have not been so straightforward as for the OvS framework. Since Click is a highly configurable tool, with many users being able to develop their own extensions of the supported functionality using Click elements or modules (as they are called by the supporting community). However, SmartFIRE follows a different approach in order to support as many as possible configurations. The corresponding RC is only responsible for executing the Click router in the user-space level with the appropriate arguments. The experimenter submits to the EC a configuration file that describes the desired Click settings. With this approach, the experimenters can now define new elements, which did not exist at the time that our developments took place, and use them to orchestrate their experimentation in large scale mesh networks. SmartFIRE has moved one step beyond in the extension of our framework and enabled OML support in the core Click system, responsible for capturing the output of Click execution and injecting the measurements in an OML database. Using our provided hooks in the Click version 1.8, the experimenter can easily support new measurements from the lately released elements.

30.5.5 FlowVisor

FlowVisor behaves as a network hypervisor, which enables the concurrent usage of an OpenFlow switch by multiple experimenters. FlowVisor is nothing more than a special purpose OpenFlow controller, which acts as a transparent proxy between any OpenFlow switch and multiple experimentation specific OpenFlow controllers. From the perspective of the OpenFlow switch, FlowVisor is its controller. It isolates parts of the underlying hardware switch and provides access to these subparts to experimentation specific controllers. Slicing might depend on several attributes of the switch, like for example the number of ports used, the physical switch memory or processing power utilized per controller instance. The slicing may also be based on the packet

flow characteristics, like the IP/MAC source and destination addresses or the VLAN tagging.

SmartFIRE extended OMF6 to control the FlowVisor process and allocate completely isolated OpenFlow switch slices upon a user's request. The slices are isolated based on the switch's physical ports, thus preventing each experimenter to interact with the traffic intended for another slice. When a user reserves testbed nodes attached to a physical switch, OMF6 transparently creates an OpenFlow slice, consisting of the ports where the reserved nodes are attached. As it is illustrated in Figure 30.6, with only the OMF6 functionality without the SmartFIRE extensions, each user reserves two nodes that share a wireless connection using an idle or non interfering with other users' wireless frequency. Our extensions take place at the wired OpenFlow enabled backbone connection of the nodes, and upon the node reservation set up the appropriate FlowVisor instance which abstracts the testbed switch that the two depicted nodes connect to.

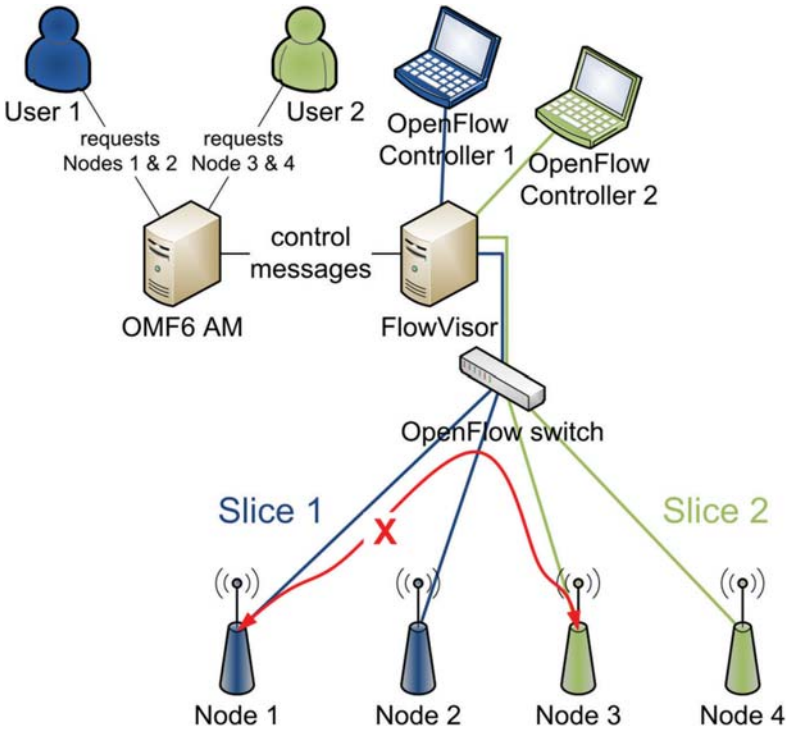

Figure 30.6 OMF6 extensions for FlowVisor.

30.5.6 Open WiFi+

SmartFIRE uses both commercial and open source APs to implement an experimentation environment close to the actual environment. Firstly, Open Wi-Fi+ was using commercial APs which can be found in the market. Secondly, by deploying the APs in a real office, SmartFIRE developed a Wi-Fi environment for experimentation under real world settings. Now, Open WiFi+ supports 8 APs, and the user is able to control each AP's transmission power. By using the power control, the user can change the wireless topology of his/her experiment.

30.5.7 SFA and MySlice

SFA has been designed as an international effort, originated by the GENI framework, to provide a secure common API with the minimum possible functionality to enable a global testbed federation. It provides a secure API that allows authenticated and authorized users to browse all the available resources and allocate those required to perform a specific experiment, according to the agreed federation policies. Therefore, SFA is used to federate the heterogeneous resources belonging to different administrative domains (authorities) to be federated.

The federation architecture adopted in SmartFIRE project is composed of 3 main components:

- Registry
- Aggregate Manager
- MySlice portal

The SFA Registry holds the certificate of the root authority of the federation. Its database is responsible for storing the users and their slices with the corresponding credentials. The project partners have decided to use a central Registry for the SmartFIRE federation. This component can also be federated with other Registries by exchanging certificates as a proof of trust relationship. The SmartFIRE federation is structured as a hierarchy of partner institutions. Each institution is responsible of its users and must validate the requests of new users belonging to their institution.

Another component of the SFA layer is the AM, which is required in each SFA-compliant testbed. The AM is responsible for exposing an interface that allows the experimenters authenticated by the Registry to browse and reserve resources of a testbed. The SFA AM exports a slice interface that researchers interact with to set up, control, and tear down their slices. Each testbed has

Table 30.1 AM Software used by SmartFIRE testbeds

Institution	Testbed	AM Software
UTH	NITOS	OMF-SFA Broker
UMU	GAIA	OMF-SFA Broker
SNU	ICN-OMF	OMF-SFA Broker
iMinds	w-iLab.t	OMF-SFA Broker
KISTI	KISTI-Emulab	ProtoGeni
KAIST	Open WiFi+	OMF-SFA Broker
ETRI	MOFI	OMF-SFA Broker
GIST	OF@TEIN	SFA Wrap

an AM, which relies on different software as shown in Table 30.1. But they all expose an SFA compliant API, allowing users to reserve resources across different testbeds.

MySlice was introduced by UPMC as a mean to provide a graphical user interface that allows users to register, authenticate, browse all the testbeds resources, and manage their slices. This work was important to provide a unified and simplified view of many hidden components to the experimenter. At the same time, it provides an open environment for the community to enrich the portal through various plugins specific to each testbed or environment. The basic configuration of MySlice consists on the creation of an admin user and a user to whom all MySlice users could delegate their credentials for accessing the testbed resources. In order to enable MySlice to interact with heterogeneous testbeds, MySlice has to be able to generate and parse different types of RSpecs; this task is performed by plugins. MySlice has been widely adopted by the community and is currently an international effort. As of today MySlice has been adopted by the following testbeds (or Projects): FIT (France), F-Lab (France), Fantaastic (EU), Fed4Fire (EU), Openlab (EU), FIBRE (Brazil), FORGE (EU), CENI (China), SmartFIRE (Korea) and III (Taiwan).

30.6 Results and/or Achievements

30.6.1 Multi-Domain, ID-Based Communications and Seamless Mobility with MOFI

One of the use cases proving the value of SmartFIRE platform is the mobility use case, which shows the service continuity using a video streaming application, when host moves and connects to different Access Routers (AR) and to different Gateways (GW) (as it is depicted in Figure 30.7. According to

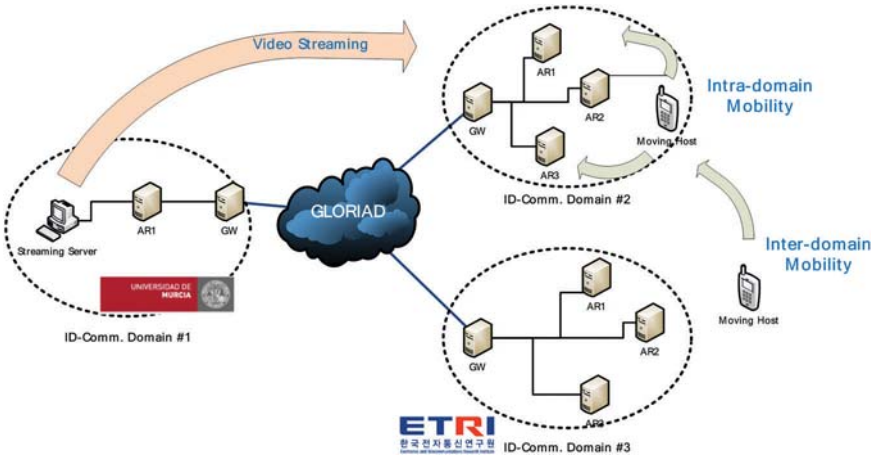

Figure 30.7 Seamless mobility scenario.

this use case, a video streaming server is deployed at UMU's domain network (Domain #1), while a video streaming client, which is a moving host, is located at one of the two ETRI's domain networks (Domain #3). The connection of both domains utilizes a dedicated Layer 2 intercontinental virtual link between UMU and ETRI. The video streaming application, which is installed in a server located in Domain #1, starts streaming to the client located in Domain #3, while the client moves to another AR whether in the same domain or to a different domain network (Domain #2). We have seen that video streaming service is provided continuously under this mobility scenario.

As we evaluate the above mobility scenario, the experimenter is able to continuously check the service by observing the experimentation messages, as it is depicted in Figure . This Figure 30.8 shows a connection between client and server. When the client moves to another domain, then the connection is lost for a while. After moving into another domain, the client registers its own Identifier to the new domain gateway by starting the HBR (Host Binding Request) process. The connectivity is resume soon and although video streaming is stopped for a while, after one second the client is able to deliver the streaming data smoothly.

In addition to the aforementioned mobility experiment, an extra experiment featuring multi screen streaming over the ID-based communication architecture of the MOFI testbed has been implemented. This experiment is designed to showcase the capabilities of the ID-based communication architecture for seamless service mobility. In particular, it focuses on a video

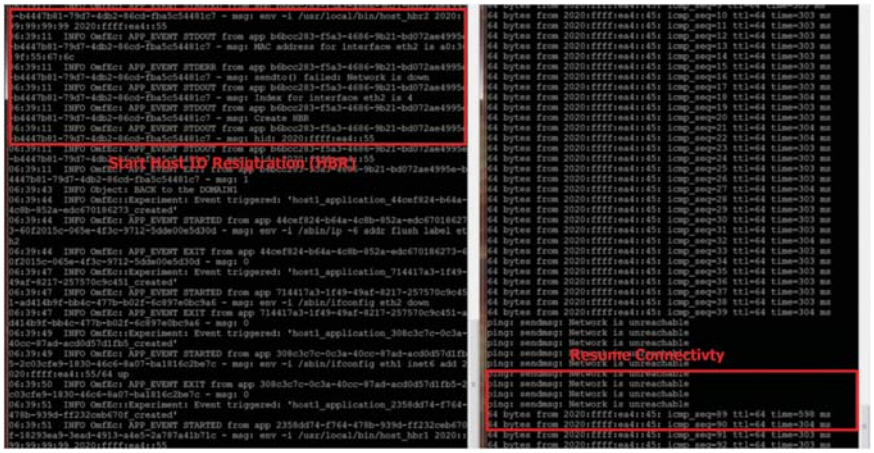

Figure 30.8 Experimentation messages for handover.

streaming service that is dynamically directed to different mobile hosts. The demonstrated service is called multi-screen streaming service and shows the opportunities of the Service ID (SID) concept (SID is used to uniquely identify an upper-layer application or service that is running on the host).

This experiment is depicted in Figure 30.9 and was also demonstrated at ICT 2015. A MOFI domain network is consisted of an AR, a GW, and various screens (such as Smart Phone, Tablet and PC monitor) equipped with USB

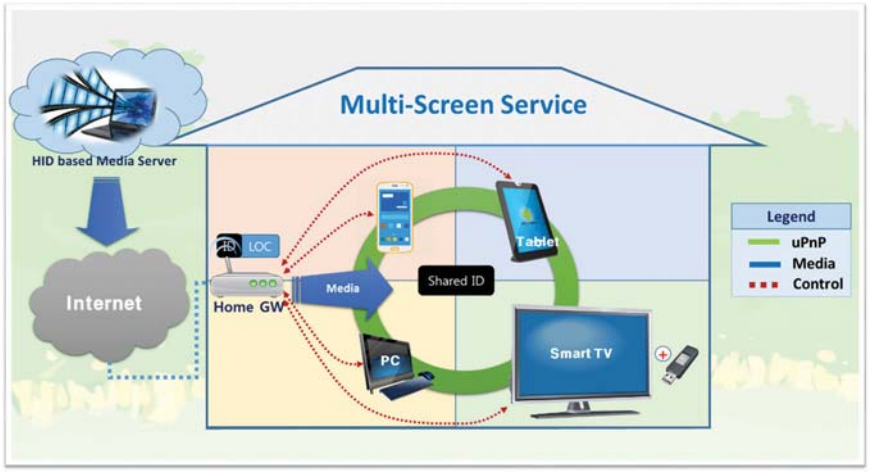

Figure 30.9 Seamless service mobility scenario as multi-screen service.

dongles that provide the processing power. In the service mobility scenario, when these screens are already connected to the MOFI domain network, they start negotiating for a common SID (Service IDentifier). During this experimentation, a daily scenario is emulated, where a user is coming back to home from his/her work. The video is first streamed to the smart phone. When the user enters the house, a new ID-based domain is available to the phone and various screens are discovered after the end of the SID negotiation process. These screens share the same SID, which corresponds to the original smart phone's HID. At this point, the smart phone selects another destination screen that will receive the ongoing video stream. Since the MOFI GW maintains a table that maps each screen's HID to its location, the selected screen is assigned the same HID and as a consequence, the video is directly forwarded to the desired screen through the GW.

SmartFIRE showcases two types of mobility scenario, named server mobility and service mobility. In server mobility scenario, the video stream is initiated between a server located in Spain and a video client located in ETRI, and the experimenter is able to observe the media data being streamed. In the intra-domain server mobility event (meaning the event when the server moves to another access router located within the same domain) there is no observable impact in the streaming session. On the other hand, in the inter-domain server mobility event (meaning the event when the server moves to another access router located in a different domain), it is a challenge to avoid the connection break due to the change of the destination address (which is the locator in the ID-based communication networks). In order to provide seamless streaming service, the SDN controllers that are in charge of mapping each host's HID to a specific locator, they update this mapping information and create the flows that will forward the traffic to the new location. After updating the mapping information, streaming data is forwarded to the new domain network to which the client is now attached. Thanks to the mapping the streaming service is provided in a non-disruptive way.

Secondly, the seamless service mobility scenario works in a pretty similar way to the above scenario without the procedure of synchronization for same SID. The video is initially streamed from the video server to the controller (smart phone). Then, the controller gets information that there are other screens within the Domain through uPnP. Discovered screens (tablet and PC monitor) are listed in the contoller. At the same time, the SID synchronization process is triggered in order to assign the smartphone's original HID forming a SID as group-ID. After that, the smart phone is able to choose a screen among a list of available screens to which the video streaming can be forwarded and displayed

at the screen. This is achievable thanks to the MOFI ID-based architecture and to the usage of SDN with which the same HID (ipv6 address in our case) can be assigned to multiple devices.

30.6.2 Content-Based Video Communications on Wireless Access Network

In this scenario, a content-based architecture is utilized, that is implemented using SDN technology (leveraging physical OpenFlow switches and nodes with virtual OpenFlow and Click Modular Router instances) on top of the UTH, SNU, KAIST and GIST testbeds. All these resources are controlled and managed with the support of the OMF6 tools developed by this project. The utilized resources are interconnected including Layer 2 intercontinental virtual links, based on the GEANT-GLORIAD-KREONET services. Wireless devices laying on UTH testbed are connected to a Content-based network on SNU, GIST and KAIST, where the IP addressing scheme is replaced by a novel one, based on content identifiers. The goal of this innovation is to use identifiers that specify only the content and not the location of this content, as the IP addresses do. Each piece of content is placed on multiple sides on the Content-based network developed on the aforementioned South Korean testbeds. The target of the Content-based architecture is the forwarding of the content from the most appropriate side to the requesting wireless device, while the streaming over the UTH wireless mesh is based on a Backpressure routing scheme.

We expected and proved that the time performance is much better when the data is cached. The in-network caching, which is an inherent feature of ICN, improves significantly the end-to-end delay of the video streaming from distributed South Korean sites to UTH. The interesting part of our experimentation is the trade-off between the time spent for the caches management and the reduction of the time delay in the packet forwarding. We showcase that the appropriate design and deployment of the Content-based and wireless access networks is fundamental for significant gains in terms of end-to-end delay in video streaming. In the following Figure 30.10, you can see the topology we created in the SmartFIRE testbed and we demonstrated in ICT 2015.

The results of our experimentation are very promising, since we observed significant improvements in terms of end-to-end delay in the video streaming. We showcase that the video streaming lasts for shorter time interval when more and more devices ask for the same video content, since the new devices

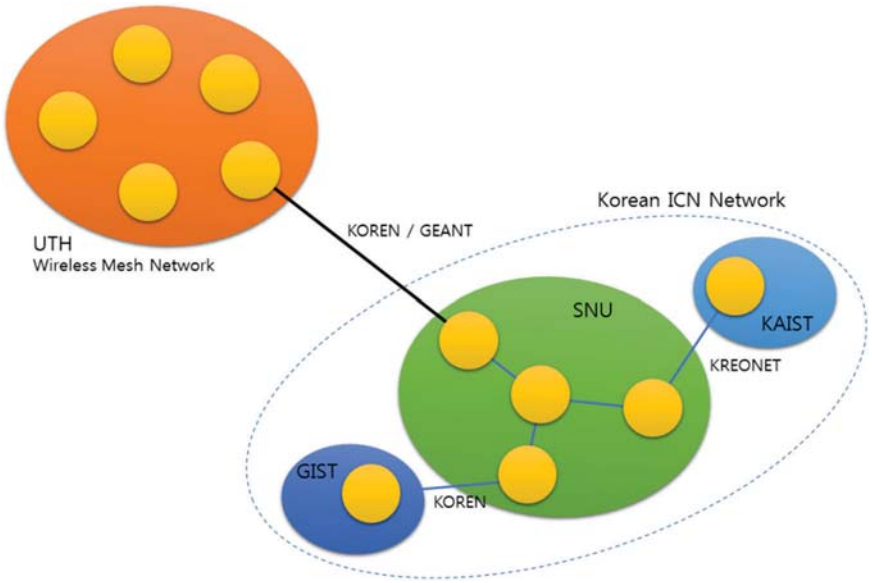

Figure 30.10 Topology of the experimentation on a content-based communication network.

requesting the same video are able to download from closer geographically caches. We measured the end-to-end delay for the video streaming by collecting and subtracting the timestamps of the video packets when they are generated and when they are delivered.

Figure 3.11 shows the end-to-end delay of the last request for a specific video content, when there is one WiFi device that requests for the same content. The requests are sent every 15 seconds. The y-axis shows the delay measured in milliseconds, while the x-axis shows the number of the requests that device has done.

Figure 30.11 End-to-end delay in the content-based communication network.

From the graph, we can see that the delay time is stable after the third request. It shows that after almost 30 seconds (2 requests), the content is completely cached in the ICN gateway, which is later used as a video streaming server. The time before, the content was being cached and could not be streamed from the closer ICN gateway, but it had to be downloaded from the remote video server. Having in mind that the length of the content (video) used in this experiment is seven seconds, we observe that the delay time after the third request is very short (less than one second). It is much lower than the delay of the first request, which is approximately 30 seconds. The graph illustrates the significant effect of the in-network caching in the end-to-end delay.

30.7 Discussion

The showcases presented as part of the results of the SmartFIRE project demonstrate the usefulness of a federated solution that interconnects multiple isolated and heterogeneous testbeds. We have shown how experiments can reinforce the research results obtained by two network approaches that have totally different natures.

On the one hand, the ID-based communications is a key research field in current networks. In fact it has been sometimes associated with the raise of SDN, which treats underlying network identifiers as such, identifiers, instead of using them to build some kind of addresses. The experiments showcased during the development of the SmartFIRE platform have supported the definition of specific requirements in terms of new interfaces to the OMF/SFA infrastructures and the specific support for heterogeneous resources, since MOFI resources have been exposed as network-level elements while other resources were exposed as lower-level elements. Moreover, the mobility requirements of the ID-based approach has supported the outcomes of setting up the wireless (and WiMAX) technologies within the SmartFIRE infrastructure. This has been translated into a better set of features and the extension of the kind of experiments supported by the final federated platform, enriching the FIRE ecosystem at the same time.

On the other hand, the experiment targeting content-based video communications has introduced another current research field, the ICN, and has related it to specific wireless scenarios. This has been the key to retrieve more requirements to apply to the SmartFIRE platform but, with valuable research results for the ICN community, it has also established the basement for a wider research initiative towards a wide research ICN platform for researching on video communications and their implications in wireless networks.

30.8 Conclusions

The current research efforts to study, analyze, find problems, and finally improve the Internet have to deal with the lack of real scenarios and infrastructures to experiment with. This makes it really difficult to achieve production ready solutions with a high degree of confidence. In order to improve this ecosystem, the experimentation driven research has been pushed to the network research field. It states the aspects that good research methodology [30] and results should meet in order to ensure they provide enough evidences to the research community, as well as the companies that will translate those results to products that impact to final users. In addition, the FIRE initiative has responded to this problem by establishing the objective of building a framework to support such kind of research. The SmartFIRE project has been incepted and developed with this objective in mind.

The federation of the SmartFIRE testbeds is the most outstanding result of the project's contributions. The physical interconnection of the testbeds, as well as the development of a common framework for controlling, managing, provisioning and reserving the testbeds' resources, enables the heterogeneous and large-scale experimentation in a unified and human-friendly platform.

This chapter has described the execution and final results obtained from the integration of the proof of concept experiments within the infrastructure provided by the SmartFIRE project. They have been used to get the most relevant requirements for such infrastructure in terms of resources and experimentation tools, and they have been used to improve even more the results of the project. This way, the showcases have also been used to evaluate, validate, and demonstrate the benefits provided by the resulting infrastructure. Also, they have shown enormous interest from the research community, especially from South Korea, so their execution and results have had good reception among them.

References

[1] SmartFIRE: K. Choumas, T. Korakis, H. Lee, D. Kim, J. Suh, T. Kwon, P. Martinez-Julia, A. Skarmeta, T. You, L. Baron, S. Fdida and J. Kim, "Enabling SDN Experimentation with Wired and Wireless Resources: The SmartFIRE facility", *Proceedings of CloudComp 2015*, Daejeon, South Korea, October 2015, (Best paper Award).

[2] SmartFIRE-link: SmartFIRE: Enabling SDN Experimentation in Wireless Testbeds exploiting Future Internet Infrastructures in South Korea and Europe, http://eukorea-fire.eu (accessed July 2016)

[3] OMF: Thierry Rakotoarivelo, Maximilian Ott, Guillaume Jourjon and Ivan Seskar, "OMF: a control and management framework for networking testbeds", *SIGOPS Oper. Syst. Rev.*, vol. 43, no. 4, pp. 54–59, January 2010.
[4] OMF-link: OMF: cOntrol and Management Framework, http://mytestbed.net (accessed July 2016)
[5] MySlice: MySlice: https://www.myslice.info (accessed July 2016)
[6] SFA: SFA: Slice-base Federation Architecture v2.0, http://groups.geni.net/geni/wiki/SliceFedArch (accessed July 2016)
[7] Click: E. Kohler, R. Morris, B. Chen, J. Jannotti and M. F. Kaashoek. "The Click Modular Router", ACM Trans. on Computer Systems, vol. 18, no. 3, pp. 263–297, August 2000.
[8] Click-link: Click: Click Modular Router, http://read.cs.ucla.edu/click/click (accessed July 2016)
[9] CNERT: K. Choumas, N. Makris, T. Korakis, L. Tassiulas and M. Ott, "Testbed Innovations for Experimenting with Wired and Wireless Software Defined Networks", *Proceedings of CNERT workshop of IEEE ICDCS 2015*, Columbus, Ohio, USA, June–July 2015.
[10] ICN-OMF: H. Lee, D. Kim, J. Suh and T. Kwon, "ICN-OMF: A Control, Management Framework for Information-Centric Network Testbed", *Proceedings of ICOIN 2015*, Siem Reap, Cambodia, January 2015.
[11] GEANT: GEANT: Pan-European Research and Education Network, http://www.geant.net/ Pages/default.aspx (accessed July 2016)
[12] KREONET: KREONET: Korea Research Environment Open NETwork, http://www.kreonet.re.kr/en_main (accessed July 2016)
[13] KOREN: KOREN: Korea Advanced Research Network, http://www.koren.kr/koren/eng/index.html (accessed July 2016)
[14] TEIN: TEIN: The Trans-Eurasia Information Network, http://www.tein.asia/tein4/index.do (accessed July 2016)
[15] GLORIAD: GLORIAD: Global Ring Network for Advanced Applications Development, http://www.gloriad.org/gloriaddrupal/index.php (accessed July 2016)
[16] MOFI: H. Jung, S. Koh, and W. Park, "Towards the Mobile Optimized Future Internet", *Proceedings of ACM CFI 2009*, Seoul, Korea, 2009.
[17] Fed4FIRE: Fed4FIRE: Federation for Future Internet Research and Experimentation, http://www.fed4fire.eu (accessed July 2016)
[18] OpenLab: OpenLab: http://www.ict-openlab.eu/home.html (accessed July 2016)

[19] FIRE: FIRE: Future Internet Research and Experimentation, https://www.ict-fire.eu (accessed July 2016)
[20] A. Gavras, A. Karila, S. Fdida, M. May and M. Potts, "Future internet research and experimentation: the FIRE initiative", *ACM SIGCOMM*, vol. 37, no. 3, pp. 88–92, July 2007.
[21] GENI: GENI: Exploring Networks of the Future, https://www.geni.net (accessed July 2016)
[22] OFELIA: OFELIA: OpenFlow in Europe: Linking Infrastructure and Applications, http://www.fp7-ofelia.eu (accessed July 2016)
[23] OpenStack: OpenStack: https://www.openstack.org (accessed July 2016)
[24] ProtoGeni: ProtoGeni: http://www.protogeni.net (accessed July 2016)
[25] OVS: Open vSwitch: http://openvswitch.org/ (accessed July 2016)
[26] K. Choumas, G. Paschos, T. Korakis and L. Tassiulas, "Distributed Load Shedding with Minimum Energy", *Proceedings of IEEE INFOCOM 2016*, San Francisco, CA, USA, April 2016.
[27] FlowVisor: Rob Sherwood, Glen Gibb, Kok-Kiong Yap, Guido Appenzeller, Martin Casado, Nick McKeown and Guru Parulkar, "Can the production network be the testbed?", *Proceedings of OSDI 2010*, Berkeley, CA, USA, 2010.
[28] John Bicket, Daniel Aguayo, Sanjit Biswas and Robert Morris, "Architecture and evaluation of an unplanned 802.11b mesh network", *Proceedings of ACM MobiCom 2005*, New York, NY, USA, 2005.
[29] A. Gavras, (ed.), "Experimentally driven research, white paper, On the existence of experimentally-driven research methodology, Version 1 (April 2010)", http://www.ict-fireworks.eu/fileadmin/documents/Experimentally_driven_research_V1.pdf (downloaded July 2012).
[30] A. Gavras, A. Bak, G. Biczók, P. Gajowniczek, A. Gulyás, H. Hrasnica, P. Martinez-Julia, F. Németh, C. Papagianni, S. Papavassiliou, M. A. Skarmeta, "Heterogeneous Testbeds, Tools and Experiments – Measurement Requirements Perspective, Measurement Methodology and Tools", *Lecture Notes in Computer Science*, vol. 7586, pp. 139–158, 2013.