Open Access

Open Journal of Internet of Things (OJIOT)
Volume 5, Issue 1, 2019

www.ronpub.com/ojiot
ISSN 2364-7108

Integrating a Smart City Testbed into a Large-Scale Heterogeneous Federation of Future Internet Experimentation Facilities: the SmartSantander Approach

Pablo Sotres, Jorge Lanza, Juan Ramón Santana, Luis Sánchez

University of Cantabria, Plaza de la Ciencia s/n, Santander 39005, Spain,
{psotres, jlanza, jrsantana, lsanchez}@tlmat.unican.es

ABSTRACT

For some years already, there has been a plethora of research initiatives throughout the world that have deployed diverse experimentation facilities for Future Internet technologies research and development. While access to these testbeds has been sometimes restricted to the specific research community supporting them, opening them to different communities can not only help those infrastructures to achieve a wider impact, but also to better identify new possibilities based on novel considerations brought by those external users. On top of the individual testbeds, supporting experiments that employs several of them in a combined and seamless fashion has been one of the main objectives of different transcontinental research initiatives, such as FIRE in Europe or GENI in United States. In particular, Fed4FIRE project and its continuation, Fed4FIRE+, have emerged as "best-in-town" projects to federate heterogeneous experimentation platforms. This paper presents the most relevant aspects of the integration of a large scale testbed on the IoT domain within the Fed4FIRE+ federation. It revolves around the adaptation carried out on the SmartSantander smart city testbed. Additionally, the paper offers an overview of the different federation models that Fed4FIRE+ proposes to testbed owners in order to provide a complete view of the involved technologies. The paper is also presenting a survey of how several specific research platforms from different experimentation domains have fulfilled the federation task following Fed4FIRE+ concepts.

TYPE OF PAPER AND KEYWORDS

Regular research paper: smart cities, IoT, testbed federation, future internet, Fed4FIRE, GENI, adaptation

1 INTRODUCTION

It goes without saying that experimentation is a fundamental part of research [49]. In this respect, many experimentation infrastructures have been rolled-out during the last ten years throughout the world in the field of Future Internet technologies [47][37][46]. These

This paper is accepted at the *International Workshop on Very Large Internet of Things (VLIoT 2019)* in conjunction with the VLDB 2019 conference in Los Angeles, USA. The proceedings of VLIoT@VLDB 2019 are published in the Open Journal of Internet of Things (OJIOT) as special issue.

testbeds' specific domains are heterogeneous, ranging from Software Defined Radio to Network Function Virtualization, Internet of Things (IoT), Optical Networks or Cognitive Networking. Most of the times, the access to these testbeds has been restricted to the specific research community supporting them. However, those that have proven to generate a larger impact have been those that have chosen more open policies. They have not only being able to attract more attention and to support a larger number of experiments, but also they have demonstrated a better evolution as they have been enriched through the feedback coming from their external users. Furthermore, when heterogeneous infrastructures come into play, the benefits and the potential generated from the combination of multiple platforms and technologies goes beyond the initial scope of the individual platforms. At the same time, the usage of common tools and protocols can help to lower the access barrier to experimenters that can design and execute more complex experiments that spans over different research domains, which can not be covered by a single experimental facility but only through the combination of some of them.

In this sense, enabling combined and seamless experimentation on Future Internet protocols, services and applications has been one of the main objectives of the Future Internet Research and Experimentation (FIRE) [36] and the Global Environment for Network Innovations (GENI) [31][40] initiatives. These two research programmes organized by the European Commission in Europe and the National Science Foundation in the United States, respectively have been promoting the deployment of experimental facilities and the execution of experiments on top of them. In particular, and under the FIRE umbrella, several different approaches have been carried out to explore the concept of testbed federation from different perspectives, achieving technical, syntactic and semantic interoperability between platforms from the same or different domains. Among all these projects, Fed4FIRE (Federation for FIRE) [5][34] and its continuation Fed4FIRE+ [7][35], emerge as the key projects to federate the heterogeneous platforms built during both FP7 and H2020 framework programmes targeting specific communities within the Future Internet ecosystem. Those two research projects have also established a tight collaboration with analogous ones funded by the GENI initiative. As a result, a common basis for infrastructure federation has been set up.

In this paper, we are presenting the most relevant aspects of the integration of a large scale testbed on the IoT domain within the Fed4FIRE+ federation. Specifically, SmartSantander [45] is an IoT-based smart city testbed deployed in the city of Santander (Spain). The different federation approaches that Fed4FIRE+ proposes to testbed owners will be reviewed and analysed in view of the specific features of different research infrastructures and, in particular, of a smart city testbed. Moreover, the different components and technologies involved on the integration of the SmartSantander testbed will be described.

The remainder of the paper is organized as follows: First, in section 2, an overview of Fed4FIRE+ basic concepts for heterogeneous infrastructure federation is presented. Then, an extensive analysis of how multiple research infrastructures from different experimentation domains have addressed the heterogeneous federation question is provided in section 3. After that, in section 4, the specific integration work carried out to federate SmartSantander platform into Fed4FIRE+ federation is provided. Finally, Section 5 will conclude the paper.

2 FED4FIRE+: FEDERATION OF FUTURE INTERNET EXPERIMENTATION FACILITIES

As it has been presented in the previous section, Fed4FIRE (2012-2016) was an Integrating Project under the European Union's 7th Framework Programme addressing the work programme topic "*Future Internet Research and Experimentation*". It was the largest federation of testbeds in Europe that allowed remote testing in numerous ICT areas. The facilities federated focused on different kinds of network related research (e.g. optical networking, wireless networking, software defined networking, etc.) or on different communities regarding services and applications (e.g. cloud computing, fog computing, data science applications, smart cities, etc.). As a result of this heterogeneity, the definition of the common federation framework and its architecture have been driven by representatives of the different FIRE communities.

H2020 Fed4FIRE+ (2017-2021) project has continued on the legacy from the Fed4FIRE project, with the clear objective to run and further improve Fed4FIRE's "best-in-town" federation of experimentation facilities for the FIRE initiative. Figure 1 shows a map of the current federated facilities that are managed by members of the Fed4FIRE+ project consortium. Nevertheless, additional testbeds can join and leave Fed4FIRE+ federation anytime without any restriction, as it has been the case of different testbeds that were federated during the previous project and either decided to opt out or evolved into a different direction with time.

The basic foundations of Fed4FIRE+ federation architecture are laid on [50] and [53], although an upgraded and extended description can be found on [52].

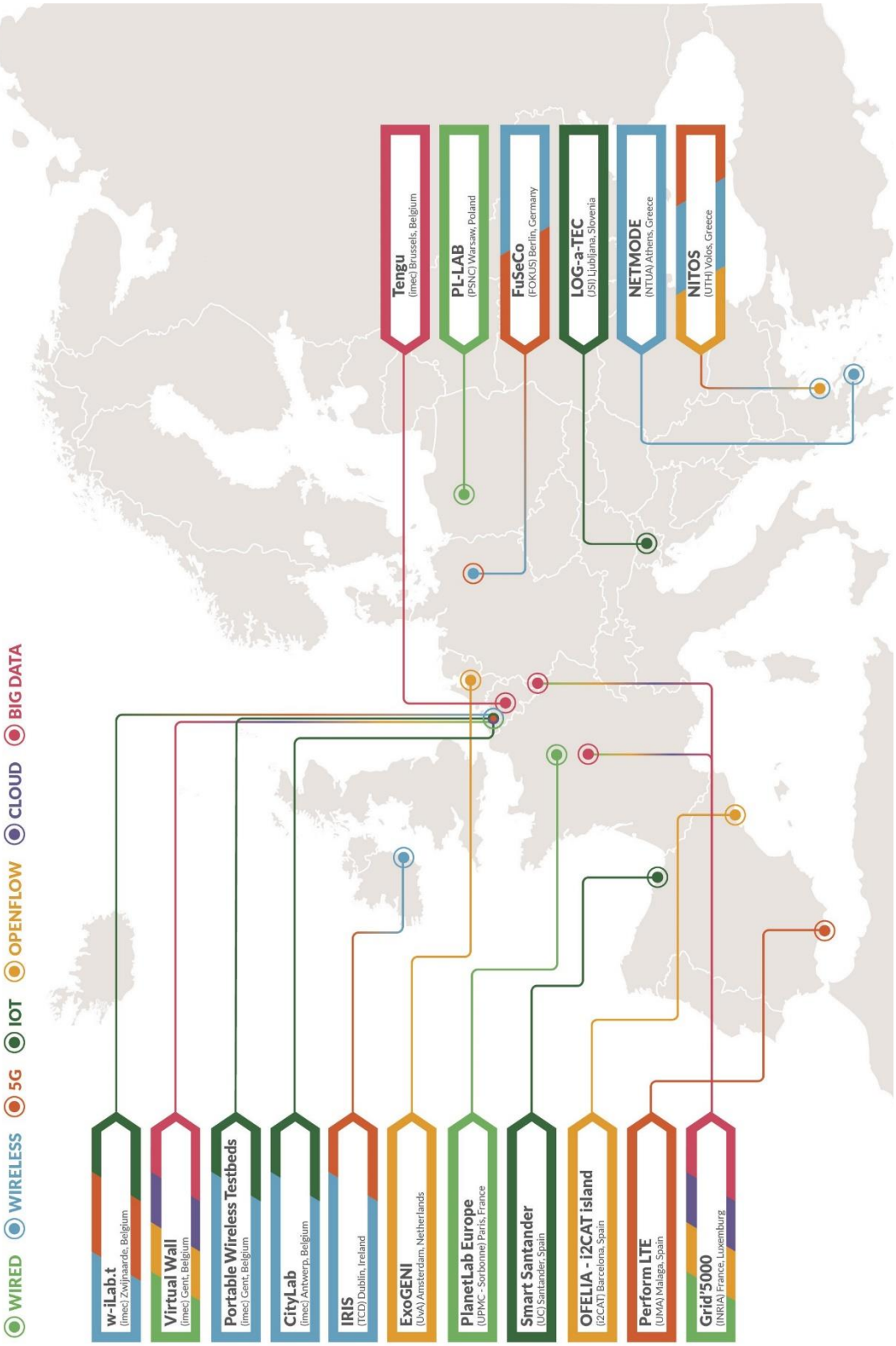

Figure 1: Fed4FIRE+ federated facilities [7]

Table 1: Fed4FIRE+ federation levels and models

		Testbed Interface for Experimenters	
		type A testbed	**type B testbed**
Federation Type	Associated Testbed	Testbed is mentioned on the Fed4FIRE+ website	
	Light Federation	Testbed can be controlled with its own API using Fed4FIRE+ credentials	
	Advanced Federation	Testbed can be controlled and combined with jFed using Fed4FIRE+ credentials	Testbed can be controlled and orchestrated through YourEPM tool using Speaks-For credentials, which are derived from Fed4FIRE+ ones

During the architecture definition, careful considerations were done to be aligned with the work in GENI. The objective was to enable worldwide research. As a result, it is interoperable with GENI and many others that have adopted the same framework (e.g. Korea, China, Brazil and Japan). An updated view of the status of all federated testbeds can be seen on [6].

The proposed federation architecture defines three main groupings on the experimentation life-cycle:

i) discovery, reservation and provision

ii) experiment control

iii) measurement and monitoring.

At the same time, it distinguishes two different types of testbeds which could be compatible with Fed4FIRE+:

- **type A:** those providing dedicated interactive access to their resources, hence with the need of granting individual access to each resource before being able to carry out the actual experimentation. Examples of this kind of testbeds are those providing resources which can be accessed through SSH, such as virtual machines (VM) or proxy resource controllers deployed at the testbed side or providing compatibility with the cOntrol and Management Framework (OMF) [44].
- **type B:** those providing a service with an API, either proprietary or standard, hiding the complexity of handling the individual resources behind an added-value service. Examples of this kind of testbeds are a service provider which offers a service to deploy Hadoop clusters for big data analysis or a service to read out sensor values of a Smart City, where the experimenter is not involved with the real sensors.

Finally, it also establishes different levels of federation, namely associated, light and advanced, based on the testbed commitment to adopt federated tools. From now on, we will only refer to advanced federation, which represents the highest Fed4FIRE+ federation level. For the sake of completion, Table 1 provides a summary of the implications of the different federation levels and types of testbed.

As the federation requirements for the two categories of testbeds are quite different, two different federation models have also been established, where protocols and tools used on each of the life-cycle management stage differs. Still, authentication schema based on X.509 certificates and a trust chain relationship is common for both of them, hence support for Fed4FIRE+ credentials is mandatory. The following subsections include an outline of the main protocols and tools proposed for each of the aforementioned federation models.

2.1 'Type A' Testbeds Federation Model

From a "type A" testbed perspective, the main requirement that needs to be fulfilled is to expose a *Slice-based Federation Architecture* (SFA) [43][30] interface. In practice, a software component known as the *Aggregate Manager* (AM) needs to be deployed at testbed side. This component implements the GENI AM API [10] and is used during the discovery, reservation and provision stages. It uses XML-RPC over SSL with client authentication based on X.509 certificates and *resource specification* XML files (RSpec) [24] as payloads. An external user can communicate with the testbed through the AM to get access to its resources.

Since FED4FIRE+ adopts the certificates-based mechanisms used by the GENI AM API for authentication and authorization [32], the federation also runs an identity provider and a PKI infrastructure to generate such credentials.

When dealing with federated experimentation and SFA communication, Fed4FIRE+ proposes the usage of a single tool, known as jFed [12], to interact with all the AMs of the different federated testbeds in an independent or combined way.

Experiment control is the life-cycle management step where testbeds can follow diverse strategies, depending on the functionality of the resources they provide. The most straightforward approach is to grant access to the individual resources through SSH by using a private/public key pair, which can be derived from the Fed4FIRE+ credential. Key distribution can be done as part of an AM API reservation operation. Those resources can be the actual ones provided by the testbed (e.g. a VM in a cloud testbed) or a gateway resource used to access the real ones provided by the testbed (e.g. an intermediate VM used to control the physical resources in a networking testbed). In addition, *Federated Resource Control Protocol* (FRCP) [8] can be used to interact with resource controllers deployed on the testbeds with access to the physical resources. In this case, either an A*dvanced Message Queuing Protocol* (AMQP) or an *Extensible Messaging and Presence Protocol* (XMPP) broker and a *Policy Decision Point* (PDP) component linked to the AM to verify the identity are also needed.

Finally, measurement and monitoring is based on *Orbit Measurement Library* (OML) streams [48][41], which are used for both experiment measuring and facility and infrastructure monitoring.

2.2 'Type B' Testbeds Federation Model

From a "type B" testbed perspective, the requirements for advanced federation are quite different to the ones mentioned in the previous subsection. In this scenario, the experimentation is based on added-value services and it is the service provider the one dealing with the whole experiment life-cycle under the hood. As a result, resource discovery, reservation management and interactions with the testbed, including experiment control and measurement, are offered in a way defined by the specific testbed manager. Still, support for Fed4FIRE+ credentials is compulsory, although the derived PKCS#12 version of the X.509 certificate is usually used in the context of client authentication with web services and APIs. This can be done with a proxy provided at the federation level without interfering the service API at all, or integrated as a part of the service itself.

Federated experimentation is tackled with the usage of service orchestration and, in particular, based on the YourEPM (*Your Experiment Process Model*) tool [29]. This tool retrieves all the available federated services from a central location known as *Service Directory* and retrieves its M2M description. For web services, this description is based on *RESTful API Modeling Language* (RAML) [23]. Thus, YourEPM can invoke the specific service API in an automated way. However, as this tool is also provided as a service, there is a security implication due to its interaction with other services and testbeds on behalf of an experimenter. For this reason, Fed4FIRE+ also implements the concept of chained *speaks-for* credentials already introduced by GENI in [32]. As a result, when any external tool (not only YourEPM) communicate to federated platforms on behalf of a user, it needs to use its own private key to establish a secure SSL connection together with the full chain of speaks-for credentials (from the tool up to the user, with any number of intermediate tools in between). This way, the targeted platform can validate the whole trust chain and perform authentication and authorization based on the original user's permissions. An interesting thing of this federation approach comes from the fact that YourEPM tool can also integrate a service on top of jFed CLI tool to communicate with SFA, hence extending the service composition to also include "type A" testbed resources.

Finally, even though experiment measurement mechanisms are defined by the testbed owner, the mechanisms for facility and infrastructure monitoring are also based on OML like in "type A" federated testbeds.

3 STRATEGIES FOR THE FEDERATION OF HETEROGENEOUS TESTBEDS INTO FED4FIRE+

As depicted on the previous sections, there are different considerations that a testbed manager need to carefully examine before taking an actual decision on the approach to follow to federate its platform within Fed4FIRE+. Nevertheless, there are already several testbeds from various research domains that have already faced them and successfully carried out the integration work in diverse ways. This section thoroughly surveys, from a practical point of view, different existing federation strategies and the specific testbeds that have adopted them.

The key factors on selecting a federation strategy are the kind of resources a testbed provide and how an experimenter interact with them. Yet, even within the same research domain, different testbeds often follow different approaches. Variations between them appear most of the times on the experiment control stage.

Indeed, facility and infrastructure monitoring are left out of the scope in this section as they are uniform across all the federation strategies.

First of all, wired cloud testbeds are ideal candidates to be federated. The reason behind it relies on the fact that SFA was initially designed with the experience from Emulab [4] and PlanetLab [20] in mind. The usage pattern is clear in this case, an AM is deployed to discover, reserve and provision VMs, and every VM can be controlled with an interactive SSH session. VM images support OML library for measurement collection, and specific applications can be instrumented to generate monitoring streams. Examples of testbeds federated following this pattern are Virtual Wall 1 & 2 [27], PlanetLab Europe [21] or PL-Lab [22], among others. In addition, some testbeds from different experimentation domains, such as some SDN testbeds, also provide cloud resources. This way, VMs with multiple network interfaces can be used to generate traffic loads inside a controlled private environment. i2CAT OpenFlow VTAM [19] is an example of testbeds following this strategy. Finally, a similar approach can also be applied on wireless, IoT and 5G testbeds with public IP connectivity offering control through interactive SSH sessions. This is the case, for example, of w-iLab.t [28], CityLab [2] or FuSeCo [9].

A second federation approach, which is only slightly different to the previous one in terms of deployed functional components in the testbed, is to provide a gateway machine acting as resource controller deployed on the platform side. Discovery, reservation, provision and experiment measurement remains the same. However, for experiment control the experimenter has to login on an intermediate machine using SSH and use specific software from that machine to control the real resources. By using this access schema, the provided resources are also secured, as they can run in the same private environment as they were running before federation and only the gateway machine needs to be publicly accessible from the outer world. In fact, this machine can be part of a private VPN, as long as the SSH gateway provided by the Fed4FIRE+ federation can be a permanent client of that VPN. Experiment measuring is still based on OML. Depending on the nature of the software used to control the resources three variants can be distinguished:

- **Use of bare tools or scripts.** This is the case of specialized domain specific testbeds, such as optical network testbeds like Ultraflow Access [39], or some wireless, 5G or IoT ones running in restricted environments like LOG-a-TEC [13] or Iris TCD [3].
- **Use of an OMFv6 Experiment Controller (EC).** OMFv6 provides a common experiment description language, known as OEDL, to describe an experiment, execute it and collect its results. OEDL can wrap the execution of tools and scripts, hence this variant can just be considered as an evolution of the previous one. Several wireless, 5G and IoT testbeds have adopted this approach, including PerformNetworks [33], LOG-a TEC, NITOS [42] or Netmode [15]. Yet, NITOS and Netmode make use of an extra layer, with an intermediate gateway used to provision their resources with a baseline image before accessing them using SSH [17][16].
- **Use of an OpenFlow EC.** This variant also builds on top of the first one, but it is specific for Software Defined Network (SDN) testbeds based on Openflow (e.g. i2CAT OpenFlow OFAM [19], Virtual Wall 2 or NITOS). In this case, the experimenter have access to a machine with a controller, or it can be installed during an interactive session.

A third federation approach consists on instrumenting the resources with an OMFv6 resource controller and provide access to them via a public messaging broker available to experimenters. This way, any machine with the proper credentials can execute an OEDL based experiment description from an EC. Examples of platforms that have adopted this federation strategy are BonFIRE [1] and NITOS, whose XMPP message broker is accessible from the internal gateway and visible from the public Internet also. The discovery, reservation, provision of resources and the experiment measurement remains the same as in the previous federation modality.

Even though the above federation strategies cover a great variety of possible scenarios, they assume that the resources to be used by the experimenter have almost no restrictions in terms of processing capacities or connectivity. However, resource-constrained testbeds need to be examined also. In some cases, providing direct and constant connectivity to testbed resources might not be feasible due to its specific nature. Restrictions based on computational power, battery consumption or connection availability imposes limitations on the kind of experiment control a testbed can offer. This is usually the case of low-power sensor based IoT testbeds. From “type A” testbed viewpoint, the federation approach is to deploy a GENI AM to support discovery, reservation an provision; and provide experiment control and measurement functionality out of band without using one of Fed4FIRE+ recommended options. Still, experiment measurement based on OML is highly advised whenever possible. Testbeds following this federation strategy are IoTLab [11], which uses CoAP, HTTP gateways and *Google Cloud Messaging* (GCM) to access sensor nodes; and SmartSantander

[45], whose integration is described in detail in this paper.

One important issue that might arise when a testbed decides to use one of the last two federation strategies is how to connect the credentials used to perform the first stages of the experiment lifecycle through the GENI AM to the security framework used for the experiment control operations. The BonFIRE testbed has successfully employed a PDP component for its integration but it remains as an open issue that each specific testbed has to address.

A remarkable aspect to be highlighted is the fact that some testbeds have themselves a heterogeneous mix of experimentation resources. Thus, their integration combine multiple of the abovementioned approaches to target different kind of resources. As an example, i2CAT OpenFlow testbed implements two different AM: VTAM and OFAM. The former provides virtualised computer nodes locally connected to an OpenFlow infrastructure that can be controlled through the latter. In this sense, once one or more VMs have been reserved using the VTAM, the network topology and the specific VM running the OpenFlow EC is linked using SFA operations through OFAM.

All the federation strategies described until the moment are applicable for the different flavours of "type A" testbeds. However, while SFA technology is used by the majority of the testbeds under Fed4FIRE+ umbrella, it is not applicable for all types of testbeds. When federating testbeds consisting on resource-constrained resources, enabling direct control of each of the underlying resources can be problematic at best. Moreover, all the analysed federation strategies are focused on manipulating resources in an individual way. Even if they can be combined in groups by using some extra tools, when experimentation implies hundreds or thousands of resources (a typical situation on IoT testbeds), having to individually control every device might be impractical. Furthermore, some testbeds only offer experimentation at a higher level, thus, using an SFA AM has simply no sense. Finally, some testbeds already have a pre-existent management solution that can be adapted without the need of deploying a new management stack.

These considerations justify the definition of a different federation model using service-oriented technologies for "type B" testbeds. The federation strategy in this case is straightforward: the testbed has to provide a web service supporting FED4FIRE+ credentials and be compatible with YourEPM orchestration tool, with all the implications that they impose as already explained on the section 2.2. There is no specific research domain which is better suited to be federated following this approach, it can be applied to multiple ones. Testbeds federated following this approach are varied in terms of the research domain to which they belong. For example, BonFIRE, a cloud testbed; Tengu [51], a big data experimental facility; or SmartSantander, a smart city one are using this approach.

All these federation alternatives are not self-excluding, just varied approaches that testbeds interested in joining the Fed4FIRE+ federation can explore and decide which of them suits better for offering their resources to the Fed4FIRE+ experimenters. In this sense, it is interesting to highlight the fact that some testbeds, for example BonFIRE and SmartSantander, have implemented two different federation approaches. Both have adapted their pre-existing, service-oriented, experimentation paradigm following the "type B" testbed federation model. In addition, they have also explored the more extended "type A" testbed federation alternative, trying to accommodate that paradigm to be used within the context of a resource-oriented experimentation one.

4 FEDERATION OF THE SMARTSANTANDER TESTBED IN FED4FIRE+

The SmartSantander testbed is an experimental test facility for the research and experimentation of architectures, key enabling technologies, services and applications for the Internet of Things in the context of a city (the city of Santander located in the north of Spain). The SmartSantander infrastructure enables a twofold approach in terms of experimentation: service and native experimentation. These two experimentation alternatives are referred as *Service Experimentation Layer* (SEL) and *Native Experimentation Layer* (NEL) respectively.

SEL experimentation consists on running experiments and/or applications based on the data gathered by SmartSantander sensor infrastructure and stored in a shared repository. Therefore, these services will be mainly based on data retrieval from this repository. This way, third parties will be able to provide added-value functionalities based on them, hiding the complexity of the SmartSantander infrastructure and only dealing with a high-level interface. In this sense, by using the data retrieved, service experimenters could run data mining procedures in order to infer more elaborated metrics and provide these extensions to, for instance, represent diagrams, maps, etc. On the other hand, NEL experimentation requires a thorough knowledge of the SmartSantander infrastructure and how the different nodes actually work. This type of experimentation is considered a low-level experimentation as it directly accesses the nodes and its hardware.

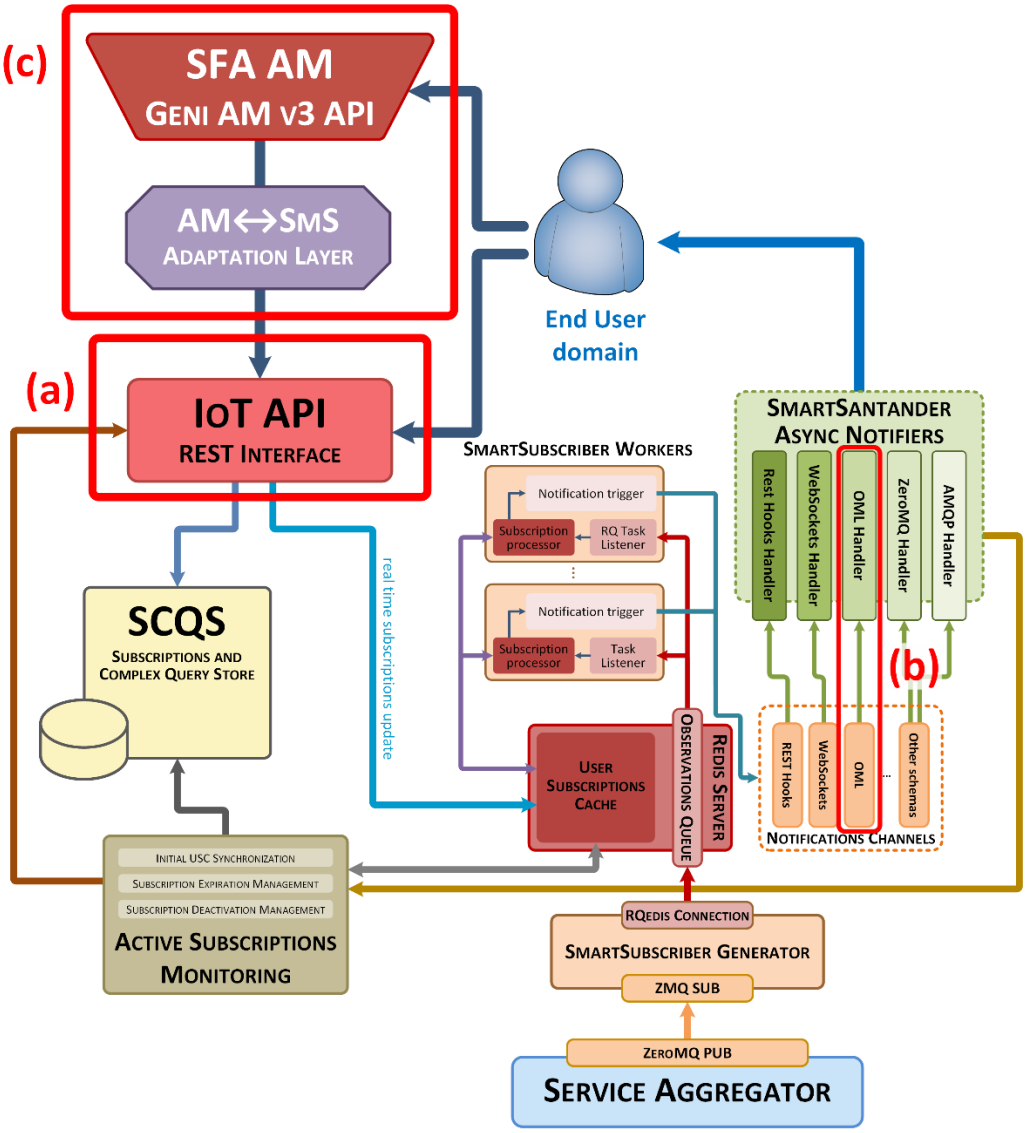

Figure 2: SmartSantander SEL federation components

Only the SEL services are federated as part of Fed4FIRE+. Access to the data is provided both through a near real time notification system based on subscriptions (asynchronous) and through direct access to historical datasets (synchronous). A detailed specification of these services can be found in [38].

In this section we delve into the specific integration work carried out to federate SmartSantander SEL platform into Fed4FIRE+ federation following two different patterns, first as a "type B" testbed federating the SmartSantander IoT API service; and also as a "type A" one, using SFA and OML to enable GENI AM based experimentation.

4.1 SmartSantander IoT API Federation as a "type B" Platform

SmartSantander service layer mainly enables the retrieval of real time measurements generated by the sensors deployed across the city of Santander. These nodes monitor different parameters such as traffic intensity, parking occupancy, temperature or pollutants, for example. Experimenters will use this data as an input for their developments to offer value-added services on top of a smart city.

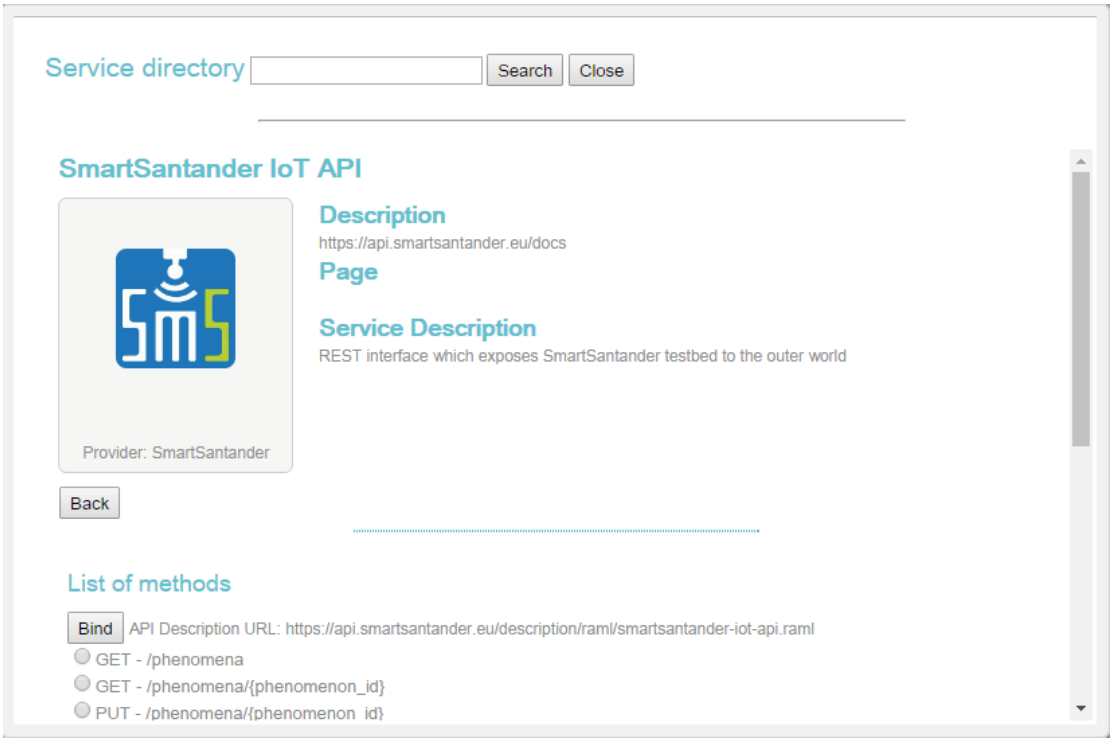

Figure 3: SmartSantander IoT API M2M description on YourEPM platform

The experimentation paradigm that SmartSantander offers, combined with the fact that most of the IoT devices deployed in the city of Santander are embedded devices with reduced computational capacity, makes SmartSantander testbed a perfect example of a "type B" platform. In particular, the boundaries between resource discovery, resource provisioning and experiment control stages of the life-cycle management are mostly blurred due to the data orientation of the SmartSantander SEL experimentation approach. First and foremost, resource discovery does not necessarily need to be based on the resource URN, hence, resources are not targeted in an individual form. Combination of geographic restrictions together with other information such as type of sensors can also be used without the need of knowing the exact resource that has generated the piece of information, or dataset, that the experiment requires. Moreover, multiple experimenters can be using at the same time the data that is being generated by a single resource. Thus, the concept of resource reservation does not apply. In addition, the experimenter does not need to have any particular control over the sensor behaviour. Instead, a user can "provision" its experiment by creating a subscription to a set of sensor measurements (or observations). As a result, information flow (experiment measurement stage) will start coming only when the specified criteria are met. In order to create a subscription the experimenter will have to include parameters regarding how and where he wants to be notified. Finally, most of the metrics that are calculated in SmartSantander SEL layer are derived from the collected sensor observations, so they do not suit with Fed4FIRE+ infrastructure monitoring concept. In practice, infrastructure monitoring mechanisms and experiment monitoring are equivalent.

This federation approach sits on top of the existing SmartSantander IoT API platform. As we will only focus on the specific components deployed to federate it under Fed4FIRE+ ecosystem, readers are referred to [49] for complete details about the SmartSantander IoT API. Figure 2 shows the different federation components (highlighted in red) introduced in SmartSantander SEL in order to complete the integration in Fed4FIRE+. Specifically, this subsection discusses those related to "type B" federation models, labelled in the figure as (a) and (b).

As explained in section 2, the fundamental functionality needed to achieve federation is to support the common trust and security schema used in Fed4FIRE+ ecosystem. As a matter of fact, this is enough to achieve the light federation status, meaning the offered resources provided by the testbed can't be controlled with federated tools but through their own tools using Fed4FIRE+ compatible credentials. Before this integration, SmartSantander IoT API authentication and authorization schema was only based on the usage

of a 128 bits randomly-generated key as part of an HTTP Basic authentication schema used inside an SSL session. Still, only server authentication was verified during the SSL handshake. In order to support Fed4FIRE+ X.509 credentials, a new version of this API supporting mutual authentication validation as part of the SSL handshake has been deployed (Figure 2a). Actually, as we are dealing with web authentication, the derived PKCS#12 version of the X.509 credential is used by the client.

The second requirement for federation is to be integrated with the Fed4FIRE+ facility monitoring system [6]. This means a Red/Amber/Green summary needs to be sent to a central OML Server. In addition, a periodic API test is established from a central location. In order to do so, a Python based script using OML4Py library [14] is periodically executed to gather the status of diverse SmartSantander SEL components and provide the required aggregated summary.

Besides, although it is not mandatory for this federation paradigm, Fed4FIRE+ recommends the adoption of OML streams as common data format for experiment measurement and monitoring. Taking this into account, this technology has also been adopted as one of the available mechanisms for sensor observation notifications in the SEL Asynchronous Service System (Figure 2b). As a result, a generic OML4Py based instrumented application has been developed to generate OML streams out of sensor observations. Therefore, experimenters can configure the destination OML server during the subscription definition. Of course, experimenters are free to choose any other available notification mechanism to gather sensor information in an asynchronous way (e.g. resthooks, websockets…).

Last but not least, the key important factor to consider SmartSantander SEL platform as an advanced federated testbed is to support combined heterogeneous experiments together with other research infrastructures. As detailed before, in the case of "type B" testbeds, this is achieved by providing compatibility with YourEPM orchestration tool.

For this purpose, SmartSantander IoT API needs to support Speaks-For credential validation so as to allow 3rd party services to speak on behalf of the real user. In this scenario, authentication is done using its Fed4FIRE+ credential together with a Speaks-For credential signed to that specific service by the user. As authorization is tied to the user, that request can then be authorized as if it were directly done using the experimenter's credential. Different approaches can be followed: a testbed can either decide to implement speaks-for validation itself or trust the Federation Proxy and avoid its complexity. In the case of SmartSantander SEL platform, a complete implementation has been done. As a result of the work carried out to support this security schema, an open source tool for Speaks-For credential management has been released [26].

Another relevant requirement to support service orchestration is to provide a RAML description of the service to allow M2M communication between YourEPM and that service. In this regard, the SmartSantander IoT API RAML description is available to be consumed at [25]. Figure 3 shows an excerpt of how this service is shown inside YourEPM platform.

As a consequence of all the described integration work, SmartSantander IoT API can not only be accessed used Fed4FIRE+ federated credentials, but new experiments can be created combining functionality offered by heterogeneous testbeds. As an example of such a scenario, an experiment combining a VM provided by BonFIRE testbed, which is used to deploy an OML server, and sensor information extracted from SmartSantander testbed can be seen on Figure 4.

4.2 SmartSantander IoT API Federation as a "type A" Platform

SFA architectural concepts, as already explained, better suits research facilities offering resource oriented experimentation paradigms. Nevertheless, despite the fact SmartSantander SEL experimentation model can't be fully mapped to "type A" federation concepts, an exercise to analyse and design such an experimentation layer on top of the existing platform has been done due to several reasons: first, it does empower SmartSantander integration with the rest of Fed4FIRE+ facilities; second, compatibility with SFA, hence with jFed experimentation tool, offers a good opportunity to reach different research communities. This subsection discusses the different components deployed within SmartSantander SEL platform in order to achieve advance level federation from a "type A" testbed perspective. Figure 5 shows a screenshot of a similar scenario as the one proposed on Figure 4 using jFed tool to combine different research infrastructures. In this case, the experiment combines virtualization resources (provided by Virtual Wall testbed) together with sensor information from a smart city platform (provided by SmartSantander testbed).

From an architectural perspective, the key components are those from Figure 2c. Still, as this second approach also builds on top of some of the components deployed on the testbed as a result of the "type B" integration, we refer to the previous subsection for the sake of completion. Examples of those reused components are the OML notifier stack for experiment measurement and monitoring (Figure 2b) as well as OML-based facility monitoring scripts.

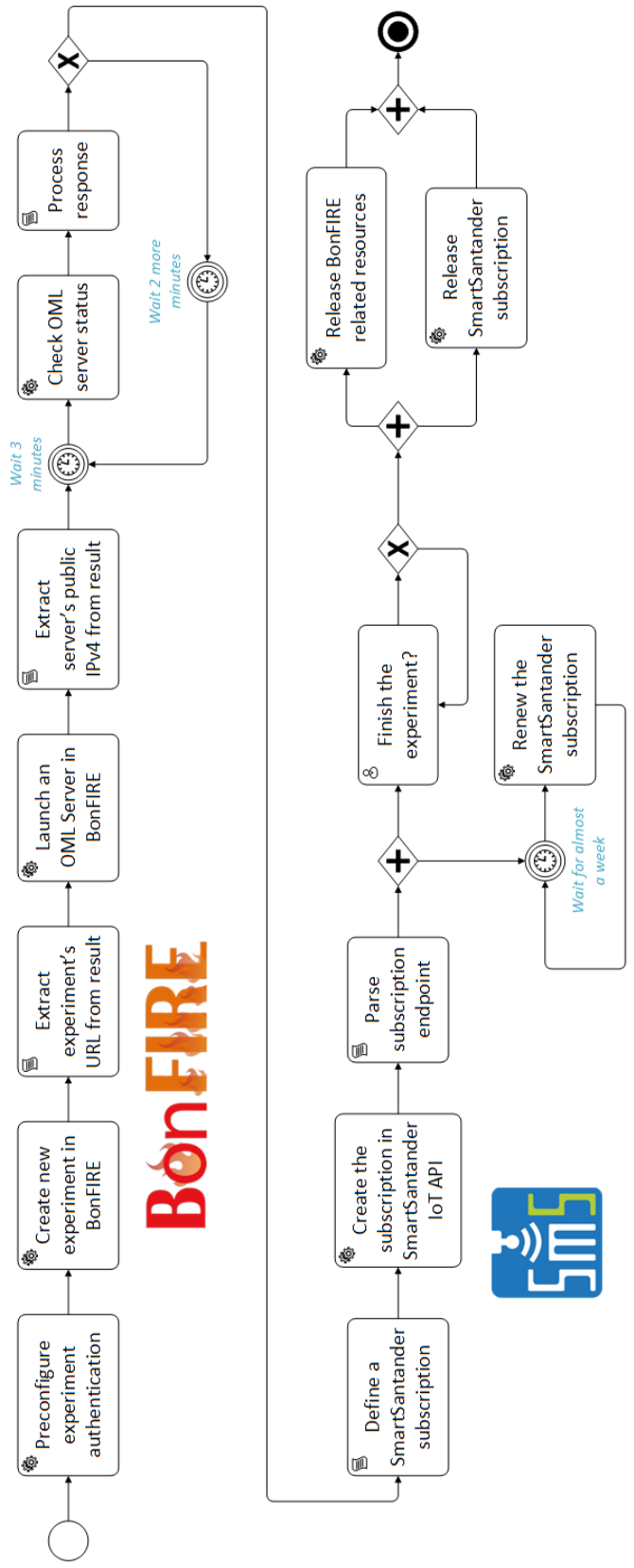

Figure 4: Simple smart city experiment scenario based on service orchestration with YourEPM

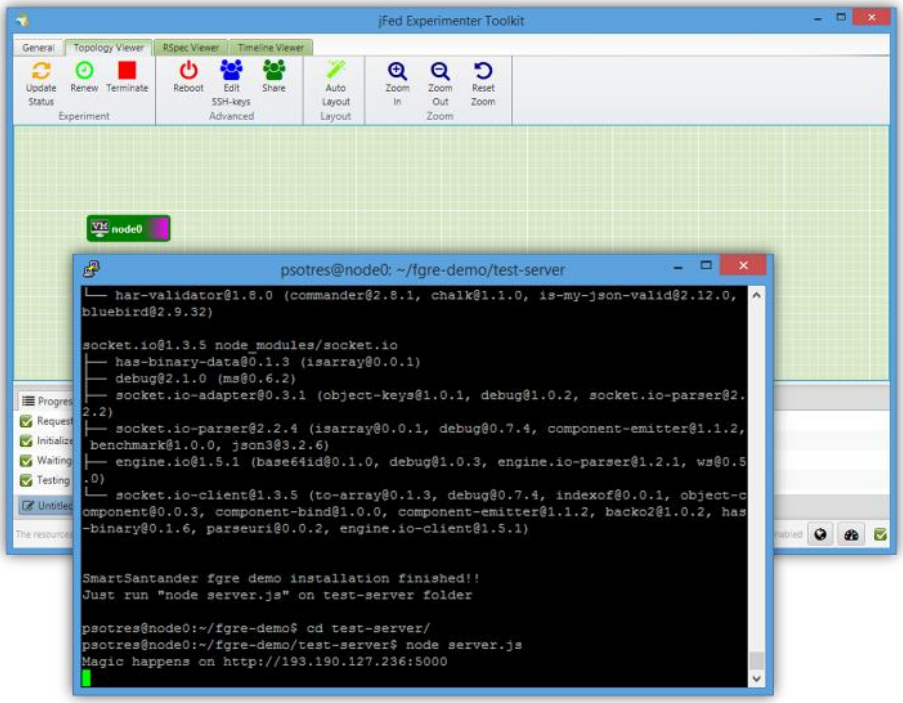

Figure 5: Usage of jFed to interact with SmartSantander SEL asynchronous platform

The integration of the SFA architectural concepts into SmartSantander have been carried out in two different steps. The first iteration, providing basic compatibility with GENI AM API v2 has been based on the SFAWrap framework [30], while the second one has been based on the GENI Reference Control Framework (GCF) [18]. The latter is considered to be the reference implementation of the GENI AM API v3.

During the first iteration, only a limited subset of all the different methods specified by the API were implemented. Therefore, only basic connectivity and testbed description through GetVersion() call were provided, whereas resource discovery and provision compatibility were left out of the scope due to the specific nature of the SmartSantander SEL experimentation model. Still, even without providing complete functionality, supporting a reduced version of the GENI AM API interface is valuable for facility monitoring within Fed4FIRE+.

The second integration iteration, on its side, have been focused on providing full life-cycle management through the GENI AM API v3 interface. However, due to the resource nature of this API, the functionality achieved when using the SmartSantander AM interface is not as rich as the one achieved with the service oriented IoT API interface. The fundamental idea for the integration is to take advantage of the resource provision stage to create SmartSantander asynchronous subscriptions based on RSpec contents. The drawback of this approach lies in the fact that, as RSpec description is organised by resources, subscriptions will always be resource based and flexibility decreases.

More specifically, the chosen approach is to consider every sliver in SmartSantander testbed as a single, resource based, subscription. Thus, every time an experimenter creates a new *sliver*, a new subscription is created via the SmartSantander IoT API. In addition, every resource addition or removal from a defined sliver results in a modification of its associated subscription. The stitching functionality to connect both domains is provided by the AM↔SmS adaptation layer, as depicted in Figure 2c. This component is in also in charge of subscription expiration or renewal whenever needed. Current functionality is restricted to the usage of the OML notifier component for experiment measurement, although this can be extended in the future.

From a practical perspective, SmartSantander sensing nodes can be discovered using a *ListResources()* operation which returns an *advertisement RSpec* to the client with all the available IoT sensors deployed across the city of Santander. After that, the experimenter can select as much IoT sensors as needed by producing the corresponding *request RSpec* and calling the *Allocate()* operation. For each sliver, the request RSpec also need to include the OML server endpoint acting as destination for the associated OML stream containing sensor observations. Actually, as any newly generated subscription is not enabled until the *Provision()*

operation is carried out, that endpoint information is only mandatory for the provision stage. *Describe()* operation can be used to check the sensing nodes included on a sliver, hence associated with a specific subscription, and *Update()* operation can then be used to modify the allocated subscription without deleting it. Finally, *Renew()*, *Delete()* and *Status()* operations are self explanatory.

5 SUMMARY AND CONCLUSIONS

This paper has presented the most relevant aspects of the adaptation of a large-scale IoT testbed into a heterogeneous federation context. In particular, the paper discusses the case of the SmartSantander platform, a smart city facility deployed in the city of Santander, Spain.

The applied federation concepts have been extracted from Fed4FIRE and Fed4FIRE+ EU projects, and are being applied in several testbeds from different research domains not only in Europe, but worldwide. An overview of these federation concepts and the different strategies that have been used for the integration of the testbeds that are part of the federation have been discussed. In this sense, a comprehensive analysis of the solutions adopted by several testbeds, under the Fed4FIRE+ umbrella, has been carried out. Interestingly, these testbeds enable experimentation on a wide range of Future Internet research areas.

The case of the SmartSantander testbed is particularly remarkable because the limitations associated to its experimentation model, particularly in terms of power consumption, direct connectivity, scale and programmability of the provided resources, have resulted in the definition of a service-oriented, federation approach that is quite unique within Fed4FIRE and Fed4FIRE+. In the case of the SmartSantander platform, these constraints have been overcome employing two different strategies. The reason for exposing two complementary solutions from which the experimenters can choose according to their preferences is the different quality of experience, in terms of provided functionality, that they offer. Both of them have led to equally valid solutions for the two experimentation communities that they target.

The challenge for smart city testbeds are to reach the critical mass of 3rd party service providers aiming at the creation of added-value services on top of the information extracted from different IoT sensors scattered across the city. Still, enabling smart city scenarios to be combined with diverse research infrastructures from different experimentation domains can result in a significant increase of the achieved impact.

ACKNOWLEDGEMENTS

This work was partially funded by the European project Federation for FIRE Plus (Fed4FIRE+) from the European Union's Horizon 2020 Programme with the Grant Agreement No. 732638 and by the Spanish Government (MINECO) by means of the projects ADVICE: Dynamic provisioning of connectivity in high density 5G wireless scenarios (TEC2015-71329-C2-1-R) and Future Internet Enabled Resilient Cities (FIERCE).

REFERENCES

[1] "Accessing BonFIRE for Fed4FIRE users" [Online]. Available: http://bonfire-dev.gforge.inria.fr/doc.bonfire-project.eu/integration/getting-started/fed4fire.html [Accessed: 29-Apr-2019].

[2] "CityLab testbed" [Online]. Available: https://doc.lab.cityofthings.eu/ [Accessed: 29-Apr-2019].

[3] "CONNECT's Testbed" [Online]. Available: https://iris-testbed.connectcentre.ie/ [Accessed: 29-Apr-2019].

[4] "Emulab" [Online]. Available: https://www.emulab.net/ [Accessed: 29-Apr-2019].

[5] "Fed4FIRE" [Online]. Available: https://old.fed4fire.eu/ [Accessed: 29-Apr-2019].

[6] "Fed4FIRE Federation monitor" [Online]. Available: https://fedmon.fed4fire.eu/ [Accessed: 29-Apr-2019].

[7] "FED4FIRE+" [Online]. Available: https://www.fed4fire.eu [Accessed: 29-Apr-2019].

[8] "Federated Resource Control Protocol (FRCP)." [Online]. Available: https://github.com/mytestbed/specification/blob/master/FRCP.md/ [Accessed: 29-Apr-2019].

[9] "FUSECO in Fed4FIRE+" [Online]. Available: https://www.fed4fire.eu/testbeds/fuseco/ [Accessed: 29-Apr-2019].

[10] "GENI aggregate manager API version 3" [Online]. Available: https://groups.geni.net/geni/wiki/GAPI_AM_API_V3 [Accessed: 29-Apr-2019].

[11] "IoTLab Fed4FIRE" [Online]. Available: https://gitlab.distantaccess.com/iotlab-fed4fire/fed4fire-documentation/ [Accessed: 29-April-2019].

[12] "jFed" [Online]. Available: https://jfed.ilabt.imec.be/ [Accessed: 29-Apr-2019].

[13] "LOG-a-TEC by SensorLab" [Online]. Available: http://log-a-tec.eu/overview.html [Accessed: 29-Apr-2019].

[14] "Native Python client library for the OML measurement framework" [Online]. Available: https://github.com/mytestbed/oml4py/ [Accessed: 29-Apr-2019].

[15] "Netmode testbed description" [Online]. Available: http://www.netmode.ntua.gr/main/index.php?option=com_content&view=article&id=103&Itemid=83 [Accessed: 29-Apr-2019].

[16] "Netmode testbed tutorial" [Online]. Available: http://www.netmode.ntua.gr/main/index.php?option=com_content&view=article&id=124&Itemid=89 [Accessed: 29-Apr-2019].

[17] "NITOS documentation" [Online]. Available: http://nitlab.inf.uth.gr/doc/ [Accessed: 29-Apr-2019].

[18] "Omni, stitcher, GCF sample aggregate manager, and other GENI tools" [Online]. Available: https://github.com/GENI-NSF/geni-tools/ [Accessed: 29-Apr-2019].

[19] "OpenFlow wired testbed - i2Lab" [Online]. Available: http://lab.i2cat.net/testbed-openflow-wired/ [Accessed: 29-Apr-2019].

[20] "PlanetLab: An open platform for developing, deploying, and accessing planetary-scale services" [Online]. Available: https://www.planet-lab.org/ [Accessed: 29-Apr-2019].

[21] "PlanetLab Europe in Fed4FIRE+" [Online]. Available: https://www.fed4fire.eu/testbeds/planetlab-europe/ [Accessed: 29-Apr-2019].

[22] "PL-Lab 2020" [Online]. Available: http://www.pllab.pl/fed4fire/ [Accessed: 29-Apr-2019].

[23] "RAML specification 0.8" [Online]. Available: https://github.com/raml-org/raml-spec/blob/master/versions/raml-08/raml-08.md [Accessed: 29-Apr-2019].

[24] "Resource specification (RSpec) documents in GENI" [Online]. Available: https://groups.geni.net/geni/wiki/GENIExperimenter/RSpecs [Accessed: 29-Apr-2019].

[25] "SmartSantander IoT API RAML description" [Online]. Available: https://api.smartsantander.eu/description/raml/smartsantander-iot-api.flat.raml [Accessed: 29-Apr-2019].

[26] "Speaks-For credential management tools" [Online]. Available: https://github.com/psotres/speaks-for/ [Accessed: 29-Apr-2019].

[27] "Virtual Wall - imec iLab.t" [Online]. Available: https://doc.ilabt.imec.be/ilabt/virtualwall/ [Accessed: 29-Apr-2019].

[28] "Wireless Testlab and OfficeLab - imec iLab.t" [Online]. Available: https://doc.ilabt.imec.be/ilabt/wilab/ [Accessed: 29-Apr-2019].

[29] "YourEPM documentation on Atos ARI FIRE Federation Tools" [Online]. Available: https://gitlab.atosresearch.eu/ari/atos_fire_federation_tools/wikis/yourepm-documentation [Accessed: 29-Apr-2019].

[30] J. Augé, "Tools to foster a global federation of testbeds," Computer Networks, vol. 63, pp. 205–220, 2014.

[31] M. Berman, J. S. Chase, L. Landweber, A. Nakao, M. Ott, D. Raychaudhuri, R. Ricci and I. Seskar, "GENI: A federated testbed for innovative network experiments," Computer Networks, vol. 61, no. 2014, pp. 5–23, 2014.

[32] M. Brinn, N. Bastin, A. Bavier, M. Berman, J. Chase and R. Ricci, "Trust as the toundation of resource exchange in GENI," in Proceedings of the 10th EAI International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities, 2015.

[33] A. Diaz, C. A. Garcia-Perez, A. Martin, P. Merino and A. Rios, "PerformNetworks: A testbed for exhaustive interoperability and performance Analysis for Mobile Networks," in Building the Future Internet Through FIRE, River Publishers, 2017, pp. 189–210.

[34] European Commission, "Federation for FIRE, projects from FP7 programme" [Online]. Available: https://cordis.europa.eu/project/rcn/105823/ [Accessed: 29-Apr-2019].

[35] European Commission, "Federation for FIRE plus, projects from H2020 programme" [Online]. Available: https://cordis.europa.eu/project/rcn/207030/ [Accessed: 29-Apr-2019].

[36] A. Gavras, A. Karila, S. Fdida, M. May and M. Potts, "Future internet research and experimentation: the FIRE initiative," ACM SIGCOMM Computer Communication Review, vol. 37, no. 3, p. 89, Jul. 2007.

[37] T. Huang, F. R. Yu, C. Zhang, J. Liu, J. Zhang and Y. Liu, "A Survey on large-scale software defined networking (SDN) testbeds: Approaches and

challenges," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 891-917, 2017.

[38] J. Lanza, P. Sotres, L. Sánchez et al., "Managing large amounts of data generated by a smart city internet of things deployment," International Journal on Semantic Web and Information Systems, vol. 12, no. 4, pp. 22–42, 2016.

[39] D. Larrabeiti, L. Kazovsky, G. Rodriguez, R. Aparicio, T. S. Shen and Shuang Yin, "Integrating a next-generation optical access network testbed into a large-scale virtual research testbed," in 2015 17th International Conference on Transparent Optical Networks (ICTON), 2015, pp. 1–6.

[40] R. McGeer, M. Berman, C. Elliott and R. Ricci. The GENI book. Springer. 2016.

[41] O. Mehani, G. Jourjon, T. Rakotoarivelo and M. Ott, "An instrumentation framework for the critical task of measurement collection in the future Internet," Computer Networks, vol. 63, pp. 68–83, 2014.

[42] K. Pechlivanidou, K. Katsalis, I. Igoumenos, D. Katsaros, T. Korakis and L. Tassiulas, "NITOS testbed: A cloud based wireless experimentation facility," 2014 26th International Teletraffic Congress (ITC), Karlskrona, 2014, pp. 1-6.

[43] L. Peterson, R. Ricci, A. Falk and J. Chase, "Slice-based federation architecture," working draft, Version 2.0, 2010. [Online]. Available: http://groups.geni.net/geni/raw-attachment/wiki/SliceFedArch/SFA2.0.pdf [Accessed: 29-May-2019].

[44] T. Rakotoarivelo, G. Jourjon, M. Ott and I. Seskar, "OMF: A control and management framework for networking testbeds," Operating Systems Review, pp. 54–59, 2009.

[45] L. Sanchez, L. Muñoz, J. A. Galache, P. Sotres, J. R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis and D. Pfisterer, "SmartSantander: IoT experimentation over a smart city testbed," Computer Networks, vol. 61, pp. 217–238, 2014.

[46] J. R. Santana, M. Maggio, R. Di Bernardo, P. Sotres, L. Sánchez and L. Muñoz, "On the Use of Information and Infrastructure Technologies for the Smart City Research in Europe: A Survey," IEICE Transactions on Communications, vol. E101.B, no. 1, pp. 2–15, 2018.

[47] M. Serrano, N. Isaris and H. Schaffers, Building the Future Internet through FIRE. River Publishers, 2017.

[48] M. Singh, M. Ott, I. Seskar and P. Kamat, "ORBIT Measurements Framework and Library (OML): Motivations, design, implementation, and features," in First International Conference on Testbeds and Research Infrastructures for the DEvelopment of NeTworks and COMmunities, 2005, pp. 146–152.

[49] S. H. Thomke, Experimentation matters : unlocking the potential of new technologies for innovation. Harvard Business School Press, 2003.

[50] W. Vandenberghe, B. Vermeulen, P. Demeester, A. Willner, S. Papavassiliou, A. Gavras et al., "Architecture for the heterogeneous federation of future internet experimentation facilities," in Future Network and Mobile Summit (FNMS), Lisbon, Portugal, 2013, pp. 1–11.

[51] T. Vanhove, G. Van Seghbroeck, T. Wauters, F. De Turck, B. Vermeulen and P. Demeester, "Tengu: An experimentation platform for big data applications," in Proceedings of IEEE 35th International Conference on Distributed Computing Systems Workshops, ICDCSW 2015, pp. 42–47, 2015.

[52] B. Vermeulen et al., "Fed4FIRE D2.9 – Final federation architecture," 2016. [Online]. Available: http://www.fed4fire.eu/wp-content/uploads/2016/10/d2-9-final-federation-architecture.pdf [Accessed: 29-May-2019].

[53] T. Wauters et al., "Federation of Internet experimentation facilities: architecture and implementation," in European Conference on Networks and Communications (EuCNC), Bologna, Italy, 2014, pp. 1–5.

AUTHOR BIOGRAPHIES

PABLO SOTRES received the Telecommunications Engineering degree from the University of Cantabria, Spain, in 2008. He is currently a Research Fellow with the Network Planning and Mobile Communications Laboratory, Communications Engineering Department, University of Cantabria. He has participated in several research projects on the smartcard, networking, security and IoT domains. During the latest years, he has been involved in various different international projects framed under the smart city paradigm, such as SmartSantander; and related to inter-testbed federation, such as Fed4FIRE, Fed4FIRE+, Wise-IoT and FED4SAE.

DR. JORGE LANZA is a senior researcher at the Network Planning and Mobile Communications Laboratory at the University of Cantabria (UC), Spain. He received his PhD in telecommunications engineering from University in 2014. He has participated in several research projects, national and international, with both private and public funding. Currently his research is focused on IoT infrastructures towards federating deployments in different locations using semantics technologies. In addition his work has included combined mobility and security for the wireless Internet.

JUAN RAMÓN SANTANA obtained his MSc in Telecommunication Engineering at the University of Cantabria in 2010. He is currently working as research fellow in the Network Planning and Mobile Communications Laboratory, a telecommunication research group from the same university. Prior to his current occupation, he worked on IoT solutions for the cattle industry. Since then, he has been involved in several Smart City international projects, from which we can highlight SmartSantander, carrying out the integration and deployment of the SmartSantander communication infrastructure. Beyond SmartSantander, he has been also working as work package leader in other EU projects, such as EAR-IT, FIESTA-IoT or FESTIVAL, an EU-Japan collaborative project. During his research work, he has co-authored more than 30 publications, including conferences, journals and book chapters. Among his research interests, we can include WSN (Wireless Sensor Networks) within the Smart City paradigm.

DR. LUIS SANCHEZ received both the Telecommunications Engineering and PhD degree from the University of Cantabria, Spain, in 2002 and 2009 respectively. He is Associate Professor at the Department of Communications Engineering at the University of Cantabria. He is active on IoT-enabled smart cities, meshed networking on heterogeneous wireless scenarios and optimization of network performance through cognitive networking techniques. He has a long research record working on projects belonging to the 5th, 6th, 7th and H2020 EU Framework Programs. He has authored more than 60 papers at international journals and conferences and co-authored several books. Dr. Sanchez often participates in panels and round tables discussing about innovation supported by IoT in Smart cities. He also acts as expert for French ANR (Agencie National Recherche) and Italian MIUR (Ministero dell'Istruzione, dell'Università e della Ricerca) reviewing and evaluating R&D proposals.