PART I

The Next Generation Internet with FIRE

1

European Challenges for Experimental Facilities

Hans Schaffers[1], Thanasis Korakis[2], Congduc Pham[3], Abdur Rahim[4], Antonio Jara[5] and Martin Serrano[6]

[1]Saxion University of Applied Sciences, Netherlands
[2]University of Thessaly, Greece
[3]University of Pau, France
[4]CREATE-NET, Italy
[5]HES-SO, Switzerland
[6]Insight Centre for Data Analytics Galway, Ireland

1.1 Evolution of Experimentation Facilities into Open Innovation Ecosystems for the Future Internet

There have been considerable changes in FIRE as a consequence of the evolving vision and the needs and interests of the industrial and scientific communities. Originally established from a core of networking testbeds and aimed at investigating fundamental issues of networking infrastructure, FIRE's mission has changed to deliver widely reusable facilities for the Future Internet community, resulting in the current emphasis on federation. Figure 1.1 provides an overview of representative testbeds that forms the European federated ecosystem.

New domains are coalescing within Future Networks, such as the Internet of Things, Internet of Services, Cyber-Physical Systems, Big Data and other areas, giving rise to new research and innovation challenges and demands to experimentation facilities. Interactions with communities such as Smart Cities, Cloud computing and Internet of Things already brought new perspectives into FIRE's portfolio. To some extent this is visible in the new Work Programme 2016–2017, in particular in relation to Internet of Things, where FIRE testbeds are considered to support technology validation before deployment

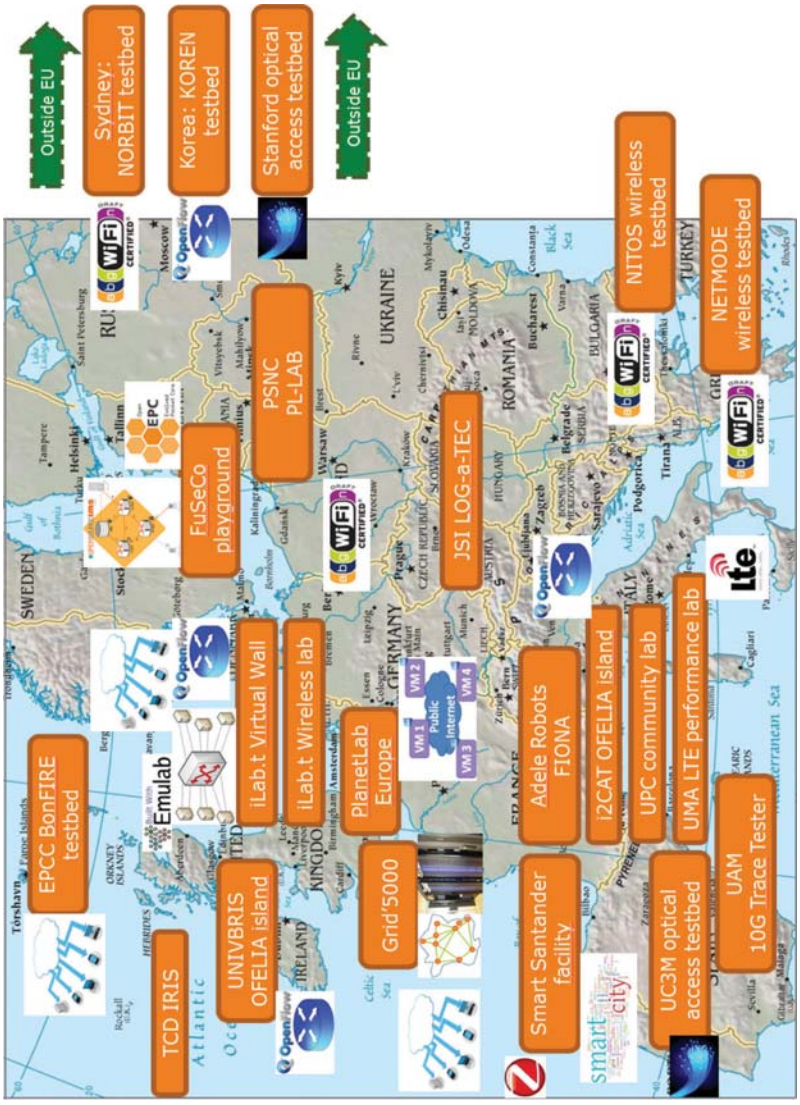

Figure 1.1 European federated testbeds ecosystem.

Source: FED4FIRE Project.

in field trials. AmpliFIRE identifies several key trends, such as the integration of a broad range of systems (cloud services, wireless sensor networks, content platforms, and mobile users) within Future Internet systems in large-scale, highly heterogeneous systems, to support increasingly connected and networked applications. This new emphasis calls for looser forms of federation of cross domain resources.

Whereas FIRE has become meaningful in the context of the Future Internet and its research community, FIRE also increasingly addresses the demand side of experimentation, the need to engage users and to support innovation processes. This way FIRE's evolution must find a balance between coherence and fragmentation in shaping the relation between facility building projects and research and experimentation – and increasingly innovation – projects. In this respect a specific development is how FIRE is increasingly shaped by new, flexible demand-oriented instruments such as Open Calls and Open Access, which demonstrates how customer "pull" is increasingly supplementing and balancing technology "push."

As experimenter needs and requirements are becoming more demanding, expectations are rising as regards how FIRE should anticipate the needs and requirements from SMEs, industry, Smart Cities, and from other initiatives in the scope of Future Internet such as Internet of Things and 5G. New types of service concepts for example *Experimentation-as-a-Service* aim at making experimentation more simple, efficient, reliable, repeatable and easier to use. These new concepts affect the methods and tools, the channels for offering services to new categories of users, and the collaborations to be established with infrastructure and service partners to deliver the services.

Thus it is expected that experimentation will increasingly be shaped by demand-pull factors in the period 2015–2020. These user demands will be based on four main trends:

- The Internet of Things: a global, connected network of product tags, sensors, actuators, and mobile devices that interact to form complex pervasive systems that autonomously pursue shared goals without direct user input. A typical application of this trend is automated retail stock control systems.
- The Internet of Services: internet/scaled service-oriented computing, such as cloud software (Software as a Service) or platforms (Platform as a Service).
- The Internet of Information: sharing all types of media, data and content across the Internet in ever increasing amounts and combining data to generate new content.

- The Internet of People: people to people networking, where users will become the centre of Internet technology—indeed the boundaries between systems and users will become increasingly blurred.

In order to contribute to these four fast moving areas, the FIRE ecosystem must grow in its technical capabilities. New networking protocols must be introduced and managed, both at the physical layer where every higher wireless bandwidth technologies are being offered, and in the software interfaces, which SDN (Software defined Networks) is opening up. Handling data at medium (giga to tera) to large (petabyte) scale is becoming a critical part of the applications that impact people's lives. Mining such data, combining information from separated archives, filtering and transmitting efficiently are key steps in modern applications, and the Internet testbeds of this decade will be used to develop and explore these tools.

Future Internet systems will integrate a broad range of systems such as cloud services, sensor networks and content platforms into large-scale heterogeneous systems-of-systems. There is a growing need for integration, for example integration of multi-purpose multi-application wireless sensor networks with large-scale data-processing, analysis, modelling and visualisation along with the integration of next generation human-computer interaction methods. This will lead to complex large-scale networked systems that integrate the four pillars: things, people, content and services. Common research themes include scalability solutions, interoperability, new software and service engineering methods, optimisation, energy-awareness and security, privacy and trust solutions. To validate the research themes, federated experimented facilities are required that are large-scale and highly heterogeneous. Testbeds that bridge the gap between infrastructure, applications and users and allow exploring the potential of large-scale systems which are built upon advanced networks, with real users and in realistic environments will be of considerable value. This will also require the development of new methodological perspectives for experimentation facilities, including how to experiment and innovate in a framework of collaboration among researchers, developers and users in real-life environments.

As we emphasize a focus on "complex smart systems of networked infrastructures and applications" within the experimentation, the unique and most valuable contribution of experimental facilities should be to "bridge" and "accelerate": create the testing, experimenting and innovation environment which enables linking networking research to business and societal impact. Testbeds and experiments are tools to address research and innovation

in "complex smart systems", in different environments such as cities, manufacturing industry and data-intensive services sectors. In this way, experimentation widens its primary focus from testing and experimenting, building the facilities, tools and environments towards closing the gap from experiment to innovation for users and markets.

1.2 Support, Continuity and Sustainability: The NITOS Testbed Example

1.2.1 NITOS Future Internet Facility Overview

University of Thessaly operates NITOS Future Internet Facility [http://nitlab.inf.uth.gr/NITlab/index.php/nitos.html], which is an integrated facility with heterogeneous testbeds that focuses on supporting experimentation-based research in the area of wired and wireless networks. NITOS is remotely accessible and open to the research community 24/7. It has been used from hundreds of experimenters all over the world.

The main experimental components of NITOS are:

- A **wireless experimentation testbed**, which consists of 100 powerful nodes (some of them mobile), that feature multiple wireless interfaces and allow for experimentation with heterogeneous (Wi-Fi, WiMAX, LTE, Bluetooth) wireless technologies.
- A **Cloud infrastructure**, which consists of 7 HP blade servers and 2 rack-mounted ones providing 272 CPU cores, 800 Gb of Ram and 22 TB of storage capacity, in total. The network connectivity is established via the usage of an HP 5400 series modular Openflow switch, which provides 10 Gb Ethernet connectivity amongst the cluster's modules and 1 Gb amongst the cluster and GEANT.
- A **wireless sensor network testbed**, consisting of a controllable testbed deployed in UTH's offices, a city-scale sensor network deployed in Volos city and a city-scale mobile sensing infrastructure that relies on bicycles of volunteer users. All sensor platforms are custom, developed by UTH, supporting Arduino firmware and exploiting several wireless technologies for communication (ZigBee, Wi-Fi, LTE, Bluetooth, IR).
- A **Software Defined Radio (SDR)** testbed that consists of Universal Software Radio Peripheral (USRP) devices attached to the NITOS wireless nodes. USRPs allow the researcher to program a number of physical layer features (e.g. modulation), thereby enabling dedicated PHY layer or cross-layer research.

- A **Software Defined Networking (SDN)** testbed that consists of multiple OpenFlow technology enabled switches, connected to the NITOS nodes, thus enabling experimentation with switching and routing networking protocols. Experimentation using the OpenFlow technology can be combined with the wireless networking one, hence enabling the construction of more heterogeneous experimental scenarios (Figure 1.2).

The testbed is based on open-source software that allows the design and implementation of new algorithms, enabling new functionalities on the existing hardware. The control and management of the testbed is done using the cOntrol and Management Framework (OMF) open-source software. NITOS supports evaluation of protocols and applications under real world settings and is also designed to achieve reproducibility of experimentation.

1.2.2 NITOS Evolution and Growth

The NITOS Future Internet facility has been developed and constantly expanded through the participation in several EU-funded FIRE projects. During these projects, the testbed has been enhanced with diverse hardware and software components, aiming to provide cutting-edge experimentation services to the research community, in an open-access scheme and remotely accessible, as well as augmented with user friendly orchestration of experiments. Below, we provide a brief overview of the key projects that assisted in the NITOS development.

OneLab2 (https://onelab.eu/) started in 2008, was the FIRE project that laid the foundations of the NITOS experimental facility. OneLab2

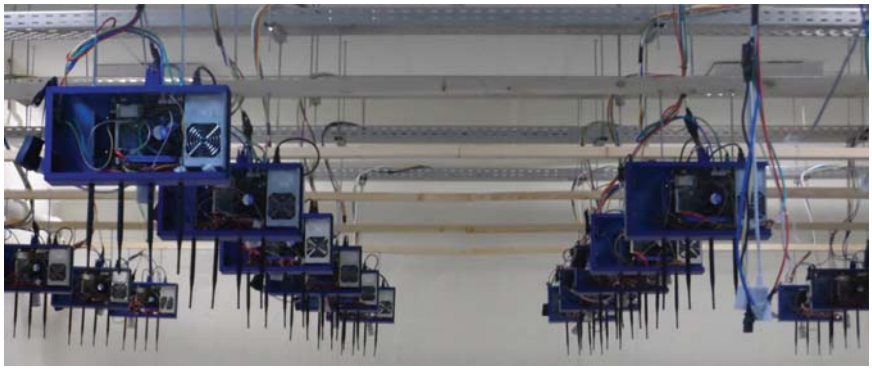

Figure 1.2 The NITOS Indoor deployment.

has developed one of the first pan-European experimental facilities, offering experimentation services involving both wired and wireless resources. During the project, the first tools for provisioning testbeds and conducting experiments were realized. Through OneLab2, NITOS was initially developed, operating with a small number of nodes, offering experimentation services involving open source WiFi networks and adopting the state-of-the-art OMF framework.

Following OneLab2, **OpenLab** (http://www.ict-openlab.eu) was one of the first projects to address testbed federation for both the control and experimental plane. By control we mean the way that the testbed resources are represented, reserved, provisioned and accessed, whereas by experimental we refer to conducting experiments over the testbeds. During OpenLab, NITOS testbed was extended with a large number of nodes and first steps towards federation were taken. In addition a WiMAX macroscale base station was installed, along with the respective end-clients, and a commercial LTE network was provisioned. Tools for enabling experimentation with a plethora of different components were implementing, by extending the OMF framework to support Wi-Fi, Wired, WiMAX and Software Defined Radio (SDR) components.

In **FIBRE** (http://www.fibre-ict.eu/) project, the first results of federation in Europe were extended in order to also cover Brazil. Moreover, focus was placed on Software Defined Networking (SDN), and its integration in the existing testbeds. Through FIBRE, NITOS was extended with OpenFlow enabled switches, and the extensions in the respective control and management tools for supporting them. In FIBRE, NITOS was one of the key European facilities, and following its paradigm, NITOS-like testbeds were installed at six different brazilian sites.

CONTENT was a project that investigated the integration and convergence of wireless resources, along with SDN-enabled wired and optical networks. During the project, NITOS was the key testbed where all the developments took place, and was extended with advanced frameworks for the configuration and management of the wireless resources. Aspects such as end-to-end network slicing, including both optical and wireless resources were examined, as well as network virtualization of the LTE and WiFi resources of the testbed.

NITOS is also one of the core wireless testbeds participating in the **Fed4FIRE** (http://www.fed4fire.eu/) project. NITOS has been developing for the project software dealing with the control plane federation of the testbeds (NITOS Broker), easing and unifying the federation of any NITOS-like testbed in Fed4FIRE.

In **CREW** (http://www.crew-project.eu/) NITOS testbed was extended with USRP devices for Software Defined Radio related research, whereas energy monitoring devices, with very high resolution were developed and installed at the testbed. These devices are able to measure the energy spent in the wireless transmissions in even a per packet basis, thus rendering them a valuable tool for energy minimization experimentally driven research.

In **SmartFIRE** (http://eukorea-fire.eu/) federation with South Korea was addressed. The project was coordinated by the NITOS team, and developed all the extensions in the testbed control and management frameworks that ease the federation of Korean testbed sites. The testbed was further expanded in terms of equipment, increasing the SDN capabilities and experiments that can be conducted.

Through the participation in **XIFI** (https://fi-xifi.eu/), NITOS was extended significantly with the integration of Cloud infrastructure in the testbed. The Cloud system is interconnected with the experimental resources of the testbed, thus enabling meaningful experiments including multiple technologies using Cloud processing and storage capabilities. Although the tools managing the Cloud infrastructure differed from the ones developed through FIRE projects, the NITOS team developed the appropriate drivers for their intercommunication.

Finally through **FLEX** (http://flex-project.eu) project, the testbed has been extended with commercial and open-source LTE infrastructure. NITOS team is coordinating the project, and is leading the development in all the control and management software for the LTE testbed components, as well as the uncontrolled and emulated mobility toolkits that are offered to experimenters.

After the completion of the aforementioned projects, NITOS has evolved into a truly heterogeneous Future Internet Facility providing a strong set of tools and hardware for experimental research. The tools that NITOS is offering are going beyond the existing 4G research and towards 5G, as the testbed is highly modular and can be tailored for supporting a very diverse set of experiments.

1.2.3 Facilitating User's Experience

The expertise of NITOS team on supporting experimenters, gained from the long experience on maintaining and managing the NITOS facility from 2008, led to the design and development of various tools and frameworks aiming at proactively assisting them and addressing possible issues before they arise.

Examples of such tools that have been designed, developed and extended in the context of the aforementioned EU-funded projects are the NITOS Portal (http://nitos.inf.uth.gr), the NITOS Documentation portal (http://nitlab.inf.uth.gr/doc/) and the NITOS Broker, which all targeted in operating, controling, managing and federating the facility to the most possible unobstructed way.

NITOS Portal

The NITOS Portal is the entry point for experimentation in NITOS Facility providing a wide range of web-based tools for discovering, reserving, controlling and monitoring testbed resources, including but not limited to the Scheduler, the Node Status tool, the Testbed Status tool, the Distance tool and the Spectrum Monitoring tool (Figure 1.3).

The **Scheduler** is a web-based tool that allows experimenters to discover and reserve resources from the testbed in order to conduct their experiments. Through this tool, experimenters are able to observe nodes' characteristics, filter them and finally reserve them based on their availability on time. They are also able to observe their current or future reservations in NITOS, in order to edit or cancel them. The **Node Status tool** allows a user to monitor and control the status (turn on/off and reset) of his/her reserved nodes and the **Distance tool** allows him/her to find out the physical distance between the nodes of the testbed. Finally the **Testbed Status tool** reports the functional state of each node of the three NITOS deployments together with their characteristics.

NITOS Documentation

NITOS provides a wide variety of use cases and tutorials online, on the Documentation portal of NITOS facility (http://nitlab.inf.uth.gr/doc). There is a basic tutorial with simple but detailed enough documentation, in order for every novice user to easily manage and configure NITOS resources and setup an experiment. In addition, for each of the specific testbeds that NITOS provides, for example the WiMAX or the LTE testbeds, there is a separate tutorial which guides users to the whole experimentation procedure. From the reservation of the proper resources to the configuration of them and the execution of the experiment. Finally, video tutorials can be found in the official YouTube channel of NITlab (https://www.youtube.com/channel/UCPfbZTgTk5gapcJbF85DI-w) for facilitating users during the experimentation process.

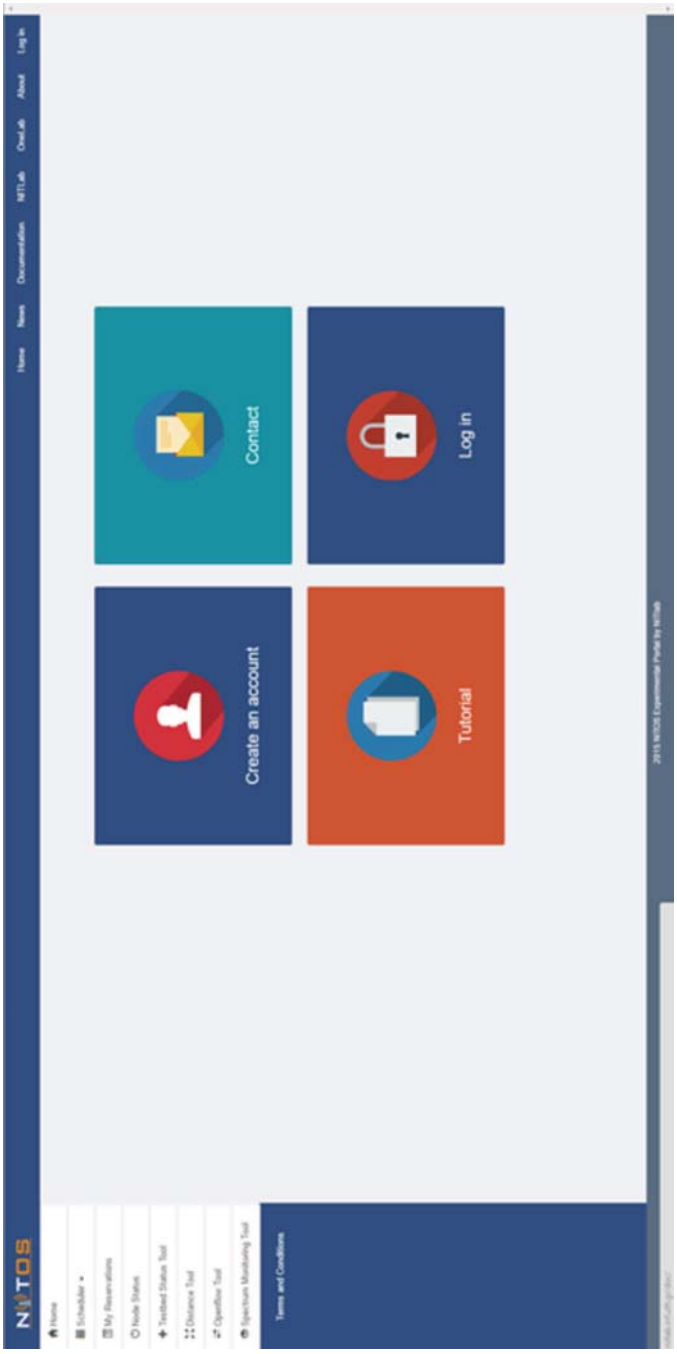

Figure 1.3 The NITOS testbed portal.

OMF Extensions

As mentioned before, the integration of a hardware extension in NITOS was constantly followed by the integration of this hardware to the control and management framework, namely the OMF [http://mytestbed.net/]. This way, all the heterogeneous hardware components were controllable through a single OMF script, enabling NITOS to effortlessly control every component, as well as combine diverse resources and design advanced experiment topologies.

In addition, the trend for the federation of experimental facilities in recent years, led to the design and implementation of the Broker entity [1] which is an OMF component responsible for controlling, managing and exposing properly the testbed's resources. It features all the necessary interfaces (XML-RPC, REST, FRCP [2], XMPP) for the federation of an OMF testbed with other heterogeneous facilities under the scope of SFA [3].

1.2.4 Exploitation of NITOS and Users Statistics

The NITOS facility attracts a large amount of research experimenters from all over the world, with a significant part coming from Industry and SMEs. More particular:

- Approximately 25% of the NITOS usage comes from Industry/SME.
- Approximately 75% of the NITOS usage comes from research institutions.

The distribution of the visitors based on their country is indicated in the following Figure 1.4:

Around 55% of the users are from EU countries, namely France, UK, Spain, Germany, Belgium, Italy and Greece, while 20% of them come from countries like US, Brazil, Australia, India, China, South Korea and Canada. Currently, NITOS counts around 500 subscribed experimenters who use the testbed in a daily basis.

Federation

The number of the NITOS users and the reservations for resources experienced significant increase upon the addition of the testbed in several federations, like OneLab [https://onelab.eu/] or the Fed4FIRE [http://www.fed4fire.eu/]. Currently NITOS is federated with facilities all over the world, including all the major EU facilities and testbeds in Brazil, South Korea and USA, providing heterogeneous resources to its users. This way, experimenters are able to form large-scale topologies including diverse resources, spanning from wireless nodes to OpenFlow switches, mobile robots, sensors and 4G equipment.

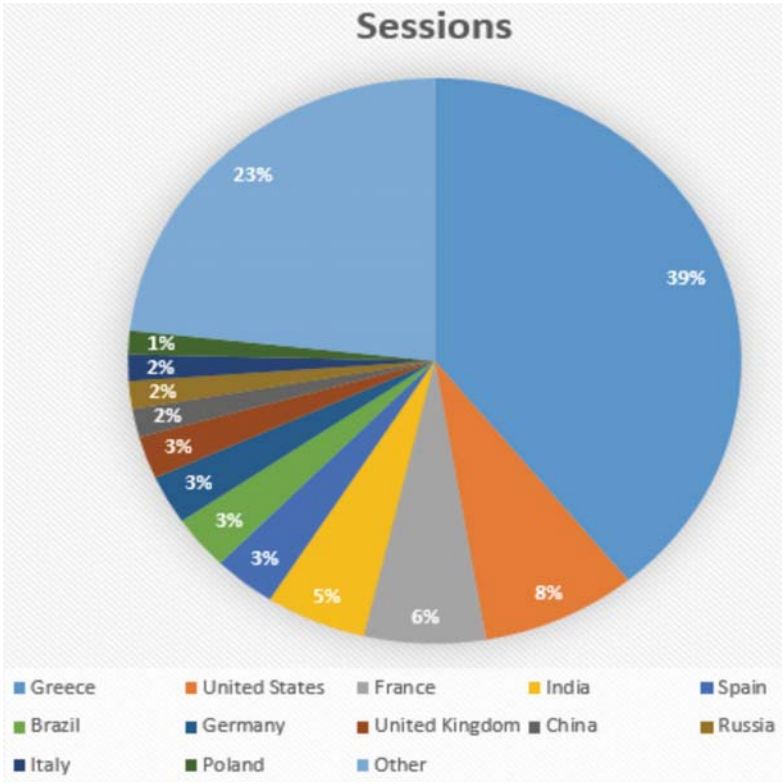

Figure 1.4 NITOS distribution in EUROPE.

Education

NITOS is deployed in Volos, Greece and specifically in University of Thessaly, thus it has very strong bonds with the University's community. During each semester, at least one course of the University is using NITOS. Students are conducting experiments using real resources, which enhance their overall knowledge on state-of-the-art wireless and wired network technologies and enables them to study and identify practical problems and solutions. In addition, NITOS is being frequently used in semester courses of the NYU Polytechnic School of Engineering.

Moreover towards the familiarization of the students with the testbed, Students Labs and "NITOS days" are often organized in the context of courses. These courses introduce NITOS portal and NITOS testbed to the participants, as well as other EU facilities and federations like OneLab, encouraging them to

create accounts and use them for experimentation. Finally, there is a variety of master thesis and PhD dissertations that take advantage of the testbed, publish experimental results and disseminate experimentation-driven research.

1.2.5 References

[1] D. Stavropoulos, A. Dadoukis, T. Rakotoarivelo, M. Ott, T. Korakis and L. Tassiulas, "Design, Architecture and Implementation of a Resource Discovery, Reservation and Provisioning Framework for Testbeds", to be presented in WINMEE, Bombay 2015, India, May 25, 2015.

[2] W. Vandenberghe, B. Vermeulen, P. Demeester, A. Willner, S. Papavassiliou, A. Gavras, M. Sioutis et al. "Architecture for the heterogeneous federation of future internet experimentation facilities." In Future Network and Mobile Summit (*FutureNetworkSummit*), 2013, pp. 1–11. IEEE, 2013.

[3] Peterson, L., R. Ricci, A. Falk, and J. Chase. "Slice-based federation architecture (SFA)" Working draft, version 2 (2010).

1.3 Experimentation: Vision and Roadmap

In Europe there are several initiatives that seek into the Future for establishing an ecosystem for Experimentation and Innovation. FIRE (Future Internet Research and Experimentation) seeks a synergetic and value adding relationships with infrastructures and stakeholders. GÉANT/NRENs and the FI-PPP initiatives related to Internet of Things and Smart Cities seek for the interactions with large deployments and big number of users. EIT Digital, the new 5G-PPP and Big Data PPP initiatives and the evolving area of Cyber-Physical Systems aims for defining ecosystems for large deployments. For the future, it is foreseen a layered Future Internet infrastructural and service provision model, where a diversity of actors gather together and ensure interoperability for their resources and services such as provision of connectivity, access to testbed and experimentation facilities, offering of research and experimentation services, business support services and more. Bottom-up experimentation resources are part of this, such as crowd sourced or citizen/community-provided resources. Each layer is transparent and offers interoperability. Research networks (NRENs) and GÉANT are providing the backbone networks and connectivity to be used by FIRE facilities and facilities offered by other providers.

European testbeds ecosystem core objective is to provide and maintain sustainable, common facilities for Future Internet research and experimentation, and to provide customized experimentation and research services. In addition, given the relevance of experimentation resources for innovation, and given the potential value and synergies that experimentation facilities offers to other initiatives, testbeds assume a role in supporting experimentally-driven research and innovation of technological systems. For this to become reality FIRE and other initiatives related to the Future Internet, such as 5G, should ensure sharing and reusing experimentation resources. FIRE should also consider opening up to (other) public and private networks, providing customized facilities and services to a wide range of users and initiatives in both public and private spheres. Specifically FIRE's core activity and longer term orientation requires the ability to modernize and innovate the experimental infrastructure and service orientation for today's and tomorrow's innovation demands. Really innovative contributions may come from smaller, more aggressive and riskier projects. Large-scale EC initiatives such as the 5G PPP, Big Data PPP and regarding the Internet of Things should have an influence on their selection and justification. Early engagement and dialogue among concerned communities is essential to accomplish this goal.

1.3.1 Envisioning Evolution of Experimentation Facilities into the Future

For setting out a transition path from the current FIRE facilities towards FIRE's role within a "Future Internet Ecosystem", four alternatives for future development patterns which equally represents the spectrum of forces acting upon FIRE's evolution have been defined:

- **Competitive Testbed as a Service**: set of individually competing testbeds offering their facilities as a pay-per-use service.
- **Industrial cooperative**: become a resource where experimental infrastructures (testbeds) and Future Internet services are offered by co-operating commercial and non-commercial stakeholders.
- **Social Innovation ecosystem**: A collection of heterogeneous, dynamic and flexible resources offering a broad range of facilities e.g. service-based infrastructures, network infrastructure, Smart City testbeds, support to user centred living labs, and other.
- **Resource sharing collaboration**: federated infrastructures provide the next generation of testbeds, integrating different types of infrastructures within a common architecture.

These future scenarios aim at stretching our thinking about how experimentation must choose its operating points and desired evolution in relation to such forces. Simplifying the argument, Experimentation evolution proceeds along two dimensions.

One dimension ranges from a coherent, integrated portfolio of activities on the one side to individual independent projects (the traditional situation), selected solely for their scientific and engineering excellence, on the other. A second dimension reflects both the scale of funded projects and the size of the customer or end-user set that future projects will reach out to and be visible to, ranging from single entities to community initiatives.

Some particular lines of FIRE's future evolution can be sketched as follows in Figure 1.5. **In the short term,** FIRE's mission and unique value is to offer an efficient and effective federated platform of facilities as a common research and experimentation infrastructure related to the Future Internet that delivers innovative and customized experimentation capabilities and services not achievable in the commercial market. FIRE should expand its facility offers to a wider spectrum of technological innovations in EC programmes e.g. in relation to smart cyber-physical systems, smart networks and Internet architectures, advanced cloud infrastructure and services, 5G network infrastructure for the Future Internet, Internet of Things and platforms for connected smart objects. In this role, FIRE delivers experimental testing facilities and services at low cost, based upon federation, expertise and tool sharing, and offers all necessary expertise and services for experimentation on the Future Internet part of Horizon 2020 (Figure 1.5).

For the **medium term**, around 2018, FIRE's mission and added value is to support the Future Internet ecosystem in building, expanding and continuously innovating the testing and experimenting facilities and tools for Future Internet technological innovation. FIRE continuously includes novel cutting-edge facilities into this federation to expand its service portfolio targeting a range of customer needs in areas of technological innovation based on the Future Internet. FIRE assumes a key role in offering facilities and services for 5G. In addition FIRE deepens its role in experimentally-driven research and innovation for smart cyber-physical systems, cloud-based systems, and Big Data. This way FIRE could also support technological innovation in key sectors such as smart manufacturing and Smart Cities. FIRE will also include "opportunistic" experimentation resources, e.g. crowd sourced or citizen- or community-provided resources.

In this time frame, FIRE establishes cutting-edge networked media and possibly Big Data facilities relevant to research and technology demands

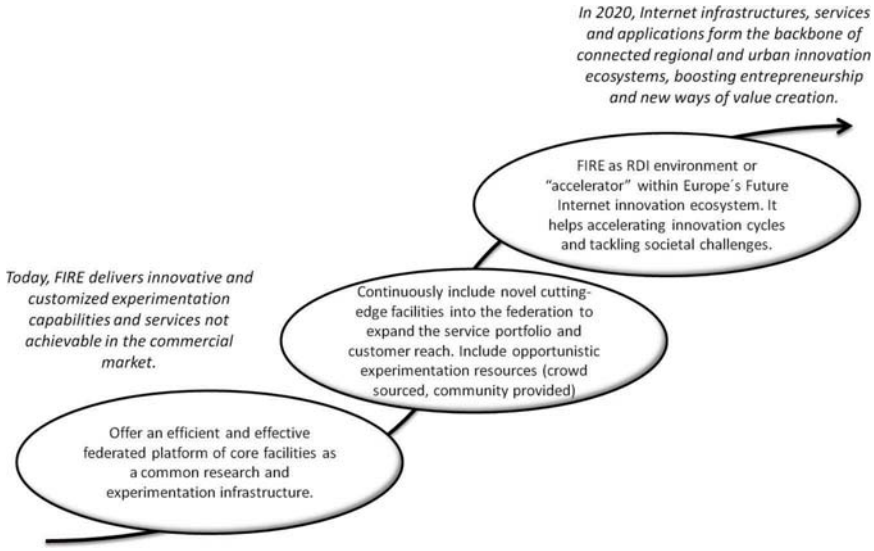

Figure 1.5 FIRE evolution longer term vision 2020.

to support industry and support the solving of societal challenges. Federation activities to support the operation of cross-facility experimentation are continued. A follow-up activity of Fed4FIRE is needed which also facilitates coordinated open calls for cross-FIRE experimentation using multiple testbeds. Additionally, a broker service is provided to attract new experimenters and support SMEs. This period ensures that openly accessible FIRE federations are aligned with 5G architectures that simplify cross-domain experimentation. Second, via the increased amount of resources dedicated to Open Calls, FIRE will create an Accelerator functionality to support product and service innovation of start-ups and SMEs. For this, FIRE will establish cooperation models with regional players and other initiatives. FIRE continues to implement professional practices and establishes a legal entity which can engage in contracts with other players and supports pay per use usage of testbeds.

For the **longer term**, by 2020, our expectation is that Internet infrastructures, services and applications form the backbone of connected regional and urban innovation ecosystems. People, SMEs and organisations collaborate seamlessly across borders to experiment on novel technologies, services and business models to boost entrepreneurship and new ways of value creation. In this context, FIRE's mission is to become the research, development and

innovation environment, or "accelerator", within Europe's Future Internet innovation ecosystem, providing the facilities for research, early testing and experimentation for technological innovation based on the Future Internet. FIRE in cooperation with other initiatives drives research and innovation cycles for advanced Internet technologies that enable business and societal innovations and the creation of new business helping entrepreneurs to take novel ideas closer to market.

In this timeframe it is envisaged that FIRE continues to add new resources that match advanced experimenter demands (5G, large-scale data oriented testbeds, large-scale Internet of Things testbeds, cyber-physical systems) and offers services based on Experimentation-as-a-service. The services evolve towards experiment-driven innovation. More and more FIRE focuses on the application domain of innovative large-scale smart systems. Implementing secure and trustworthy services becomes a key priority, also to attract industrial users. Responsive SME-tailored open calls are implemented, to attract SMEs. FIRE continues the accelerator activity by providing dedicated start-up accelerator funding. FIRE also takes new steps towards (partial) sustainability by experimenting with new funding models. Sustainable facilities are supported with continued minimum funding after project lifetime. FIRE community has achieved a high level of professional operation. FIRE contributes to establishing a network of Future Internet initiatives which works towards sharing resources, services, tools and knowledge and which is supported by the involved Commission Units.

Around 2020, FIRE thus may have evolved towards a core infrastructure for Europe's open lab for Future Internet research, development and innovation and FIRE has evolved into a technology accelerator within Europe's innovation ecosystem for the Future Internet. Clearly this implies that FIRE should achieve a considerable level of sustainability, possibly as (part of) the core infrastructure of a thriving platform ecosystem which creates technological innovations addressing business and societal challenges.

In summary, some of the key strategic objectives for FIRE proposed by AmpliFIRE are the following:

- For 2016: to increase its relevance and impact primarily for European wide technology research, but also to increase its global relevance.
- For 2018: to create substantial business and societal impact through addressing technological innovations related to societal challenges. To become a sustainable and open federation that allows experimentation on highly integrated Future Internet technologies; supporting networking and cloud pillars of the Net Futures community.

- For 2020: to become a research, development and innovation space that is attractive to both academic researchers, SME technology developers and industrial R&D companies, with emphasis on key European initiatives such as 5G, Big Data, Internet of Things and Cyber-Physical Systems domains.

1.3.2 Vision and Opportunities of OMA LwM2M/oneM2M and Its Role in the Monitoring and Deployment of Large Scale Unmanned Networks

OMA LwM2M improves existing functionality for device management and brings new features for the resource management tool through the provisioning of a standardized resources description based on OMA Objects. Homard platform acts as a horizontal application to enable the device management tool with the capabilities for remote firmware upgrade, remote maintenance, standard interface for subscription to events/data, access to statistics regarding communications/performance/status/devices health etc., and finally a standards description for the metadata of the nodes/devices (manufacturer, version, security, firmware etc.).

OMA LwM2M is a very relevant standard based on the experience and knowledge from the most validated and extended protocol for device management (firmware upgrade over the air, remote monitoring, remote reboot, maintenance etc.). In details, the operations offered by the device management platform Homard using OMA LwM2M protocol are:

- **Software Management**: enabling the installation, removal of applications, and retrieval of the inventory of software components already installed on the device and the most relevant firmware upgrade over the air.
- **Diagnostics and Monitoring**: enabling remote diagnostic and standardized object for the collection of the memory status, battery status, radio measures, QoS parameters, peripheral status and other relevant parameters for remote monitoring.
- **Connectivity and security**: allowing the configuration of bearers (WiFi, Bluetooth, cellular connectivity), proxies, list of authorized servers for remote firmware upgrade and also all the relevant parameters for enabling secure communication.
- **Device Capabilities**: allowing to the Management Authority to remotely enable and disable device peripherals like cameras, Bluetooth, USB, sensors (ultrasound, temperature, humidity, etc.) and other relevant peripherals from the nodes.

- **Lock and Wipe**: allowing to remotely lock and/or wipe the device, for instance when the device is lost (relevant for devices in open ocean, air etc.), or when the devices are stolen or sold. It enables the remote erase of personal/enterprise data when they are compromised.
- **Management Policy**: allowing the deployment on the device of policies which the client (node, device, sensor) can execute and enforce independently under some specific conditions, i.e., if some events happen, then perform some operations.

In addition to the functionalities, OMA LwM2M defines the semantics for the management objects. These objects have been defined with other standards organizations such as oneM2M and IPSO Alliance, which cooperate with OMA to avoid fragmentation and duplication that enables the semantic integration with the Management Objects. OMA LWM2M provides service providers with a secure, scalable, application-independent IoT control platform that provides control and security across multiple industries.

Thereby, this extension will also enable the integration into other initiatives such as oneM2M[1], which is the major initiative being led by ETSI and all the members from 3 GPP to enable a worldwide architecture for Internet of Things. It has a special focus on Semantic Web and interoperability. Therefore, Homard via the integration of OMA LwM2M support and oneM2M interworking will enable the openness of the platform towards possible future expansion through the integration with other IoT-based testbed infrastructures.

In addition, OMA LwM2M promotes the integration of a wide range of IoT enabled with OMA LwM2M for standardized management and data modelling based on Web Objects. OMA LwM2M and IPSO Alliance/OMA Web objects provide the capabilities for remote management and cloud computing integration. In addition, the OMA LwM2M clients are being supported in C and Java for integrating other sensors/nodes.

It is well known that there are an important number of IoT protocols with different adoption rate competing in the market as a consequence of the diversity of application domains in combination with the continuously increasing number of devices. In this direction, **oneM2M is an open standard that is based on the collection of the practices from the state of the art in a common framework** rather than the introduction of new approaches. In this way, oneM2M is gradually covering interoperability gaps and addresses

[1] OMA LwM2M is a key component from oneM2M [6, 7], it is the official device management component for oneM2M and it enablers interworking of the devices with oneM2M-based architectures.

pending difficulties using the global experience of IoT technologies. Lead by ETSI and the other SDOs such as ARIB, ATIS, CCSA, TIA, TTA and TTC, the oneM2M standard is totally coherent and has integrated outcomes from IETF, IPSO Alliance, IEEE, W3C and OMA, presenting a strong acceptability and maturity. oneM2M provides a well-defined service layer architecture as well as specifications for integrating existing IoT-specific technologies and standards such as CoAP, MQTT and OMA LwM2M.

1.3.3 Large Deployments with Low-power, Long-range, Low-cost

Internet of Things (IoT) devices are typically envisioned as the fundamental building blocks in a large variety of smart digital ecosystems: smart cities, smart agriculture, logistics&transportation... to name a few. However, the deployment of such devices in a large scale is still held back by technical challenges such as short communication distances. Using the traditional telco mobile communication infrastructure is still very expensive (e.g. GSM/GPRS, 3G/4G) and not energy efficient for autonomous devices that must run on battery for months. During the last decade, low-power but short-range radio such as IEEE 802.15.4 radio have been considered by the WSN community with multi-hop routing to overcome the limited transmission range. While such short-range communications can eventually be realized on smart cities infrastructures where high node density with powering facility can be achieved, it can hardly be generalized for the large majority of surveillance applications that need to be deployed in isolated or rural environments.

Future 5G standards do have the IoT orientation but these technologies and standards are not ready yet while the demand is already high. Therefore, and independently from the mobile telecom industry, recent modulation techniques are developed to achieve much longer transmission distances to a gateway without relay nodes to reduce the deployment cost and complexity. Rapidly adopted by many Machine-to-Machine (M2M) and IoT actors the concept of Low-Power Wide Area Networks (LPWAN), operating at much lower bandwidth, is gaining incredible interest. In addition, from a business perspective, the entry threshold for companies is much smaller with LPWAN than with traditional cellular technologies.

Some LPWAN technologies such as Sigfox$^{\mathrm{TM}}$ are still operator-based. However, other technologies such as LoRa$^{\mathrm{TM}}$ proposed by Semtech radio manufacturer can be privately deployed and used. Although direct communications between devices are possible with some technologies, most of IoT applications follow the gateway-centric approach with mainly uplink

traffic patterns. In the typical architecture for public large-scale LPWAN, data captured by end-devices are sent to gateways that will push data to well-identified network servers, see Figure 1.6. Then application servers managed by end-users could retrieve data from the network server. If encryption is used for confidentiality, the application server can be the place where data could be decrypted and presented to end-users.

The advantages of long-range transmission comes at the cost of stricter legal regulations as most of them operate in the sub-GHz, unlicensed bands (for both increased coverage and flexibility). In Europe, electromagnetic transmissions in the 863–870 MHz band used by Semtech's LoRa technology falls into the Short Range Devices (SRD) category. The ETSI EN300-220-1 document [1]\cite{etsi-EN300-220-1} specifies for Europe various requirements for SRD devices, especially those on radio activity. Basically, a transmitter is constrained to 1% duty-cycle (i.e. 36 s/hour) in the general case. This duty cycle limit applies to the total transmission time (referred to as time-on-air or air-time), even if the transmitter can change to another channel. In most cases, however, the 36 s duty-cycle is largely enough to satisfy communication needs of deployed applications. Note that this duty-cycle limitation approach is also adopted in China in the 779–787 MHz Band. US regulations in the 902–928 MHz Band do not directly specify duty-cycle but rather a maximum transmission time per packet with frequency hopping requirements.

1.3.3.1 LoRa technology

Although SigFox technology can have longer range than LoRa (40 kms have been reported for Sigfox while LoRa is typically in the range of 10 to 20 kms) when taking deployment flexibility into account, LoRa technology,

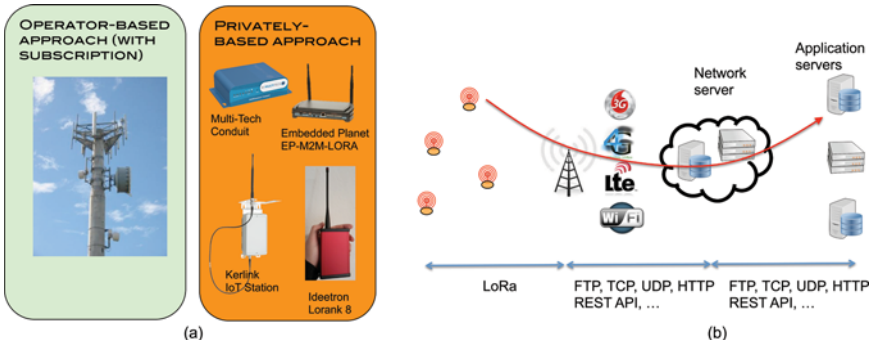

Figure 1.6

which can be privately deployed in a given area without any operator, has a clear advantage over Sigfox which coverage is entirely operator-managed.

Semtech's LoRa (LOng-RAnge) technology [2, 3]\cite{semtech-lora, Goursaud15} belongs to the spread spectrum approaches where data can be "spreaded" in both frequencies and time to increase robustness and range by increasing the receiver's sensitivity, which can be as low as –137 dBm in 868 MHz band or –148 dBm in the 433 MHz band. Throughput and range depend on the 3 main LoRa parameters: BW, CR and SF. BW is the physical bandwidth for RF modulation (e.g. 125 kHz). Larger signal bandwidth (currently up to 500 kHz) allows for higher effective data rate, thus reducing transmission time at the expense of reduced sensitivity. CR, the coding rate for forward error detection and correction. Such coding incurs a transmission overhead and the lower the coding rate, the higher the coding rate overhead ratio, e.g. with coding_rate = 4/(4+CR), the overhead ratio is 1.25 for CR = 1 which is the minimum value. Finally SF, the spreading factor, which can be set from 6 to 12. The lower the SF, the higher the data rate transmission but the lower the immunity to interference thus the smaller is the range. Figure 1.7 shows for various combinations of BW, CR and SF the time-on-air (ToA) of a LoRa transmission depending on the number of transmitted bytes. The maximum throughput is shown in the last column with a 255B payload. Modes 4 to 6 provide quite interesting trade-offs for longer range, higher data rate and immunity to interferences. Mode 1 provides the longest range.

1.3.3.2 LoRaWAN

Promoting the LoRa radio technology, the LoRa Alliance proposes a LoRaWAN [4]\cite{lorawan} specification for deploying large-scale, multi-gateways networks (star on star topology) and full network/application

				time on air in second for payload size of						
LoRa mode	BW	CR	SF	5 bytes	55 bytes	105 bytes	155 Bytes	205 Bytes	255 Bytes	max thr. for 255B in bps
1	125	4/5	12	0.95846	2.59686	4.23526	5.87366	7.51206	9.15046	223
2	250	4/5	12	0.47923	1.21651	1.87187	2.52723	3.26451	3.91987	520
3	125	4/5	10	0.28058	0.69018	1.09978	1.50938	1.91898	2.32858	876
4	500	4/5	12	0.23962	0.60826	0.93594	1.26362	1.63226	1.95994	1041
5	250	4/5	10	0.14029	0.34509	0.54989	0.75469	0.95949	1.16429	1752
6	500	4/5	11	0.11981	0.30413	0.50893	0.69325	0.87757	1.06189	1921
7	250	4/5	9	0.07014	0.18278	0.29542	0.40806	0.5207	0.63334	3221
8	500	4/5	9	0.03507	0.09139	0.14771	0.20403	0.26035	0.31667	6442
9	500	4/5	8	0.01754	0.05082	0.08154	0.11482	0.14554	0.17882	11408
10	500	4/5	7	0.00877	0.02797	0.04589	0.06381	0.08301	0.10093	20212

Figure 1.7

servers architecture as previously depicted in Figure 1.7. This specification defines the set of common channels for communications (10 in Europe), the packet format and Medium Access Control (MAC) commands that must be provided. In addition, LoRaWAN also defines so-called class A, B and C devices. Class A are bi-directional devices with each device's uplink transmission is followed by two short downlink receive windows for possible packets from the gateway. All LoRaWAN devices must at least implement Class A features. Class B and Class C devices are bi-directional devices with scheduled receive slots and bi-directional devices with maximal receive slots (nearly continuous listening) respectively. Class C devices consume a lot of power and few battery-operated applications can implement such behavior. Most of telemetry applications however use so-called Class A devices.

To optimize radio channel usage, Adaptive Data Rate (ADR) allows end-devices to use different spreading factor values depending on their distance to the gateway. By using a smaller spreading factor, the ToA is reduced therefore a larger amount of data can be sent within the 36 s of allowed transmission time.

When developed countries discuss about massive deployment of IoT using new LPWAN technologies, developing's countries are still far from being ready to enjoy the smallest benefit of it: lack of infrastructure, high cost of hardware, complexity in deployment, lack of technological eco-system and background, etc [5]\cite{IoT-newletter-zennaro}. For instance, in Sub-Saharan Africa about 64% of the population is living outside cities. The region will be predominantly rural for at least another generation. The majority of rural residents manage on less than few euros per day. Rural development is particularly imperative where half of the rural people are depend on the agriculture/micro and small farm business. For rural development, technologies have to support several key application sectors like water quality, agriculture, livestock farming, fish farming, etc.

Therefore, while the longer range provided by LPWAN is definitely an important dimension to decrease the cost of IoT, there are many other issues that must be addressed when considering deployment in developing countries: (a) Simplified deployment scenarios, (b) Cost of hardware and services and (c) Limit dependancy to proprietary infrastructures and provide local interaction models.

1.3.3.3 Simplified deployment scenarios

This typical LPWAN architecture depicted in Figure 1.6 can be greatly simplified for small, ad-hoc deployment scenarios such that those for agriculture/micro and small farm businesses, possibly in very remote areas.

Some LoRa and LoRaWAN community-based initiatives such as the one promoted TheThingNetwork^{TM} [6]\cite{TTN} may provide interesting solutions and feedbacks for dense environments such as cities but under simplified scenerios depicted in Figure 1.8 an even more adhoc and autonomous solution need to be proposed. In Figure 1.8, the gateway can directly push data to some end-user managed servers or public IoT-specific cloud platforms if properly configured.

Case A depicts a cellular-based and a WiFi Internet long-range gateway scenario. The Internet connection can be either privately owned or can rely on some community-based Internet access. Case B shows a no-Internet scenario where it is required that the gateway works in fully autonomous mode, capable of local interactions using standardized, consumer-market short-range technologies such as WiFi or Bluetooth.

Cost of Hardware and Services

The maturation of the IoT market is happening in many developed countries. While the cost of IoT devices can appear reasonable within developed countries standards, they are definitely still too expensive for very low-income sub-saharan ones. The cost argument, along with the statement that too integrated components are difficult to repair and/or replace definitely push for a Do-It-Yourself (DIY) and "off-the-shelves" design orientation. In addition,

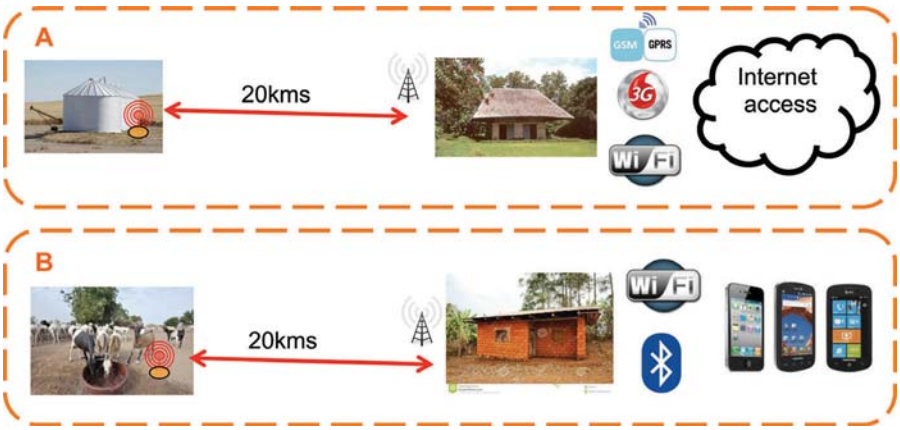

Figure 1.8

to be sustainable and able to reach previously mentioned rural environments, IoT initiatives in developing countries have to rely on an innovative and local business models. We envision mostly medium-size companies building their own "integrated" version of IoT for micro-small scale services. In this context, it is important to have dedicated efforts to design a viable exploitation model which may lead to the creation of small-scale innovative service companies.

The availability of low-cost, open-source hardware platforms such as Arduino-like boards is clearly an opportunity for building low-cost IoT devices from consumer market components. For instance, boards like Arduino Pro Mini based on an ATmega328 microcontroller offers an excellent price/performance/energy tradeoff and can provide a low-cost platform for generic sensing IoT with LoRa long-range transmission capability for a total of less than 15 euro. In addition to the cost argument such mass-market board greatly benefits from the support of a world-wide and active community of developers.

With the gateway-centric mode of LPWAN, commercial gateways are usually able to listen on several channels (e.g. LoRaWAN) and radio parameters simultaneously. For instance the LoRaWAN ADR mechanism may appear at first sight an interesting approach but it puts high complexity contraints on the gateway hardware as advanced concentrator radio chips, that alone cost more than a hundred euro, must be used. Besides, when a large number of IoT devices needs the longest range, the ADR mechanism provides only very small benefit.

Here, the approach can be different in the context of agriculture/micro and small farm business: simpler "single-connection" gateways can be built based on a simpler radio module, much like an end-device would be. Then, by using an embedded Linux platforms such as the Raspberry PI with high price/quality/reliability tradeoff, the cost of such gateway can be less than 45 euro.

Therefore, rather than providing large-scale deployment support, IoT platforms in developing countries need to focus on easy integration of low-cost "off-the-shelves" components with simple, open programming libraries and templates for easy appropriation and customization by third-parties. By taking an adhoc approach, complex and smarter mechanisms, such as advanced radio channel access to overcome the limitations of a low-cost gateway, can even be integrated as long as they remain transparent to the final developers.

Limit Dependancy to Proprietary Infrastructures and Provide Local Interaction Models

Data received on the gateway are usually pushed/uploaded to some Internet/cloud servers. It is important in the context of developing countries to be able to use a wide range of infrastructures and, if possible, at the lowest cost. Fortunately, along with the global IoT uptake, there is also a tremendous availability of sophisticated and public IoT clouds platforms and tools, offering an unprecedented level of diversity which contributes to limit dependency to proprietary infrastructures. Many of these platforms offer free accounts with limited features but that can already satisfy the needs of most agriculture/micro and small farm/village business models. It is therefore desirable to highly decouple the low-level gateway functionalities from the high-level data post-processing features, privileging high-level languages for the latter stage (e.g. Python) so that customizing data management tasks can be done in a few minutes, using standard tools, simple REST API interfaces and available public clouds.

In addition, with the lack or intermittent access to the Internet data should also be locally stored on the gateway which can directly be used as an end computer by just attaching a keyboard and a display. This solution perfectly suits low-income countries where many parts can be found in second markets. The gateway should also be able to interact with the end-user' smartphone to display captured data and notify users of important events without the need of Internet access as this situation can clearly happen in very remote areas, see case B in Figure 1.8.

Single-Connection Low-cost LoRa Gateway

Our LoRa gateway [7]\cite{pham-lcgw} could be qualified as "single connection" as it is built around an SX1272/76, much like an end-device would be. The low-cost gateway is based on a Raspberry PI (1B/1B+/2B/3B) which is both a low-cost (less than 30 euro) and a reliable embedded Linux platform. There are many SX1272/76 radio modules available and we currently tested with 6: the Libelium SX1272 LoRa, the HopeRF RFM92W & 95W, the Modtronix inAir9 & inAir9B, and the NiceRF SX1276. Most SPI LoRa modules are actually supported without modifications as reported by many users. In all cases, only a minimum soldering work is necessary to connect the required SPI pins of the radio to the corresponding pins on the Raspberry pin header as depicted in Figure 1.9. The total cost of the gateway can be less than 45 euro.

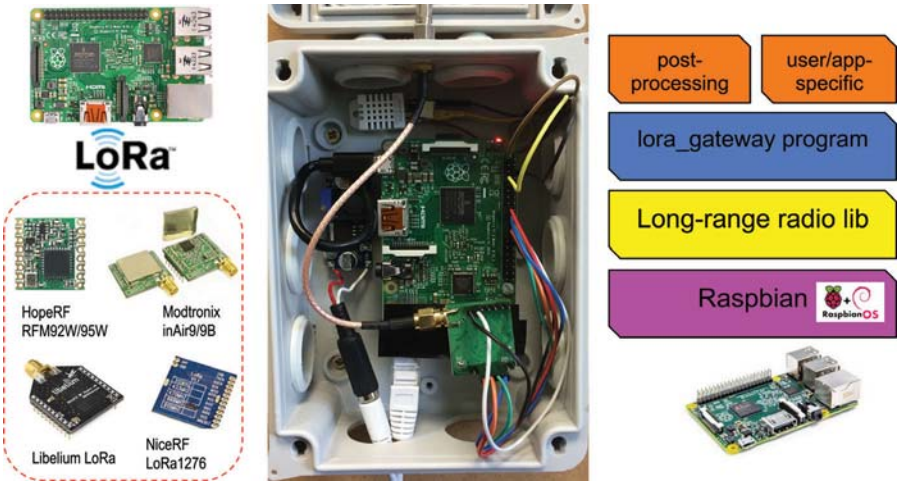

Figure 1.9

Together with the "off-the-shelves" component approach, the software stack is completely open-source: (a) the Raspberry runs a regular Raspian distribution, (b) our long range communication library is based on the SX1272 library written initially by Libelium and (c) the lora_gateway program is kept as simple as possible. We improved the original SX1272 library in various ways to provide enhanced radio channel access (CSMA-like with SIFS/DIFS) and support for both SX1272 and SX1276 chips.

We tested the gateway in various conditions for several months with a DHT22 sensor to monitor the temperature and humidity level inside the case. Our tests show that the low-cost gateway can be deployed in outdoor conditions with the appropriate casing. Although the gateway should be powered, its consumption is about 350mA for an RPIv3B with both WiFi and Bluetooth activated.

Post-Processing and Link with IoT Cloud Platforms

After compiling the lora_gateway program, the most simple way to start the gateway is in standalone mode as shown is Figure 1.10a. All packets received by the gateway is sent to the standard Unix-stdout stream.

Advanced data post-processing tasks are performed after the gateway stage by using Unix redirection of gateway's outputs as shown by the orange "post-processing" block in Figure 1.10b. We promote the usage of high-level language such as Python to implement all the data post-processing tasks

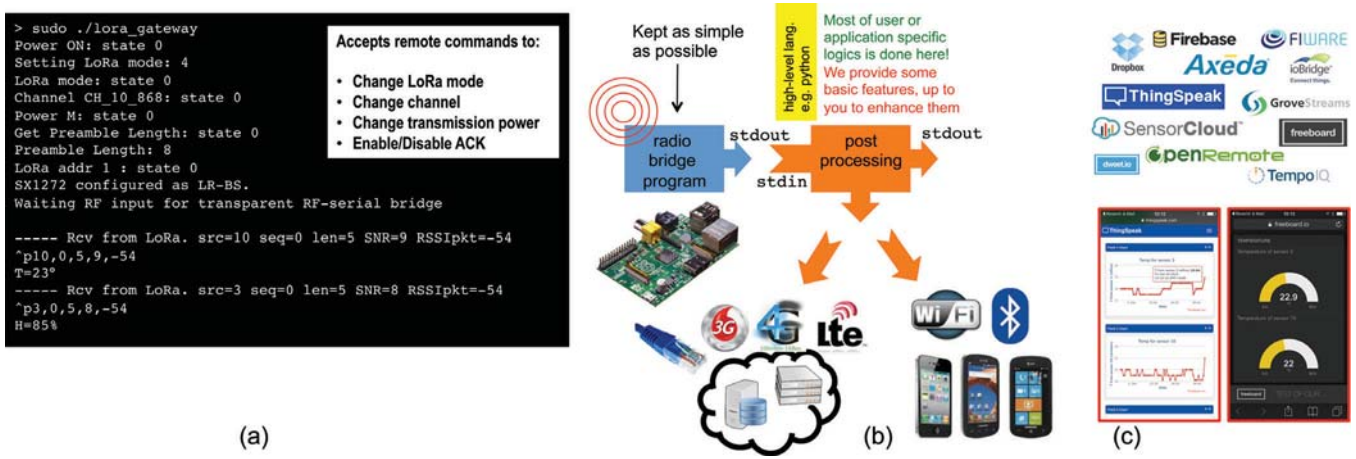
> sudo ./lora_gateway
Power ON: state 0
Setting LoRa mode: 4
LoRa mode: state 0
Channel CH_10_868: state 0
Power M: state 0
Get Preamble Length: state 0
Preamble Length: 8
LoRa addr 1 : state 0
SX1272 configured as LR-BS.
Waiting RF input for transparent RF-serial bridge
----- Rcv from LoRa. src=10 seq=0 len=5 SNR=9 RSSIpkt=-54
^p10,0,5,9,-54
T=23°
----- Rcv from LoRa. src=3 seq=0 len=5 SNR=8 RSSIpkt=-54
^p3,0,5,8,-54
H=85%
Accepts remote commands to:
• Change LoRa mode
• Change channel
• Change transmission power
• Enable/Disable ACK
(a)
Kept as simple as possible
high-level lang. e.g. python
Most of user or application specific logics is done here! We provide some basic features, up to you to enhance them
radio bridge program
stdout
stdin
post processing
stdout
3G
4G
lte
Wi Fi
(b)
Firebase
FIWARE
Dropbox
Axeda
ioBridge
ThingSpeak
GroveStreams
SensorCloud
freeboard
dweet.io
OpenRemote
TempoIQ
(c)

Figure 1.10

such as access to IoT cloud platforms and even advanced features such as AES encryption/decryption. Our gateway is distributed with a Python template that explains and shows how to upload data on various publicly available IoT cloud platforms. Examples include Dropbox™, Firebase™, ThingSpeak™, freeboard™, SensorCloud™, GrooveStream™ and FiWare™, as illustrated in Figure 1.10c.

This architecture clearly decouples the low-level gateway functionalities from the high-level post-processing features. By using high-level languages for post-processing, running and customizing data management tasks can be done in a few minutes. One of the main objectives of IoT in Africa being technology transfer to local developer communities, we believe the whole architecture and software stack are both robust and simple for either "out-of-the-box" utilization or quick appropriation & customization by third parties. For instance, a small farm can deploy in minutes the sensors and the gateway using a free account with ThingSpeak platform to visualize captured data in real-time.

Gateway Running Without Internet Access

Received data can be locally stored on the gateway and can be accessed and viewed by using the gateway as an end computer by just attaching a keyboard and a display. The gateway can also interact with the end-users' smartphone through WiFi or Bluetooth as depicted previously in Figure 1.8b. WiFi or Bluetooth dongles for Raspberry can be found at really low-cost and the smartphone can be used to display captured data and notify users of important events without the need of Internet access as this situation can clearly happen in very remote areas. Figure 1.11 shows our low-cost gateway running a MongoDB™ noSQL database and a web server with PHP/jQuery to display received data in graphs. An Android application using Bluetooth connectivity has also been developed to demonstrate these local interaction models.

Low-cost LoRa End-devices

Arduino boards are well-known in the microcontroller user community for their low-cost and simple-to-program features. These are clearly important issues to take into account in the context of developing countries, with the additional fact that due to their success, they can be acquired and purchased quite easily world-wide. There are various board types that can be used depen ding on the application and the deployment constraints. Our communication library supports most of Arduino boards as illustrated in Figure 1.12.


192.168.200.1
Access to the data from MongoDB
mongoDB
PHP
jQuery
Wi Fi
Isolated areas
Orange F
Bluetooth_raspi
Display data
Retrieve data in a csv file

Figure 1.11


Physical sensor reading
Physical sensor reading
Physical sensor reading
Activity duty-cycle, low power
Logical sensor management
Long-range transmission
Physical sensor management
Security
LoRa
LoRa radios that our library already supports
HopeRF RFM92W/95W
Libelium LoRa
Modtronix inAir9/9B
NiceRF LoRa1276

Figure 1.12

The Arduino Pro Mini, which comes in a small form factor and is available in a 3.3 v and 8 MHz version for lower power consumption, appears to be the development board of choice for providing a generic platform for sensing and long-range transmission.

Arduino Pro Mini clones can be purchased for less than 2 euro a piece from Chinese manufacturers with very acceptable quality and reliability level. Similar to the low-cost gateway, all programming libraries are open-source and we provide templates for quick and easy new behaviour customization and physical sensor integration for most of the Arduino board types.

For very low-power applications, deep-sleep mode are available in the example template to run an Arduino Pro Mini with 4 AA regular batteries. For instance, with a duty-cycle of 1 sample every hour, the board can run for almost a year, consuming about 146 uA in deep sleep mode and 93 mA when active and sending, which represents about 2 s of activity time. Our tests conducted continuously during the last 6 months show that the low-cost Pro Mini clones are very reliable.

Adding Advanced Radio Activity Mechanisms

The proposed framework leaves room for more research-oriented tasks as it actually provides a flexible framework for adding and testing new advanced features that are lacking in current LPWAN. For instance, while the LoRaWAN specifications may ease the deployment of LoRa networks by proposing some mitigation mechanisms to allow for several LoRa networks to coexist, it still remains a simple ALOHA system with additional tight radio activity time constraints without quality of service concerns. We briefly describe below 2 issues of long-range networks that are we currently study: improved channel access and activity time sharing for quality of service.

Improved channel access

A CSMA-like mechanism with SIFS/DIFS has been implemented using the Channel Activity Detection (CAD) function of the LoRa chip and can further be customized. A DIFS is defined as 3 SIFS. Prior to packet transmission a DIFS period free of activity should be observed. If "extended IFS" is activated then an additional number of CAD followed by a DIFS is required. If RSSI checking is activated then the RSSI should be below –90 dB for the packet to be transmitted. These features are summarized in Figure 1.13.

By running a background periodic source of LoRa packets, we observed that the improved channel access succeeds in reducing packet collisions. The current framework is used to study the impact of channel access methods

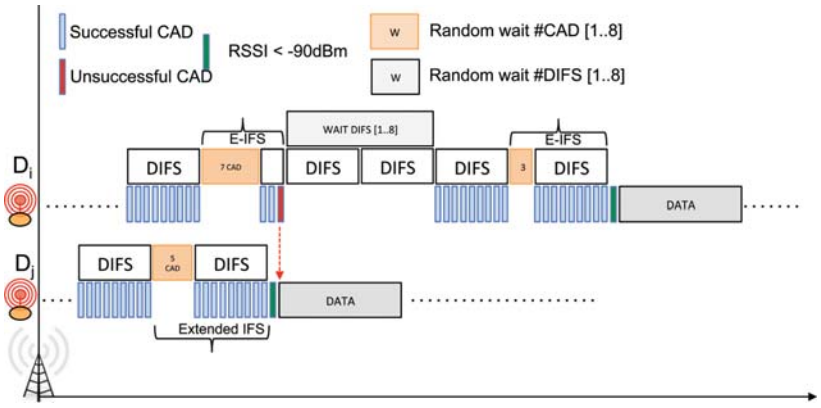

Figure 1.13

in a medium-size LoRa deployment when varying timer values due to the longer time-on-air.

Activity time sharing

We also propose and implement an exploratory activity time sharing mechanism for a pool of devices managed by a single organization [8]. We propose to overcome the tight 36 s/hour radio activity of a device by considering all the sensor's individual activity time in a shared/global manner. The approach we propose will allow a device that "exceptionally" needs to go beyond the activity time limitation to borrow some from other devices. A global view of the global activity time, G_{AT}, allowed per 1 hour cycle will be maintained at the gateway so that each device knows the potential activity time that it can use in a 1-hour cycle. Figure 1.14 shows how the deployed long-range devices Di sharing their activity time initially register (REG packet) with the gateway by indicating their local Remaining Activity Time l^{i}_{RAT0}, i.e. 36 s. The gateway stores all l^{i}_{RAT0} in a table, computes G_{AT} and broadcasts (INIT packet) both n (the number of devices) and G_{AT}. This feature is currently tested for providing better surveillance service guarantees.

Use Case: Fish Farming – Fish Pond Monitoring

With our WAZIUP partner Farmerline (http://farmerline.co/) we deployed a small number of our low-cost IoT sensor boards in a fish farm which operates several ponds of different sizes (http://www.kumahfarms.com/). This farm engages in pond culture and do both tilapia and catfish (Figure 1.15).

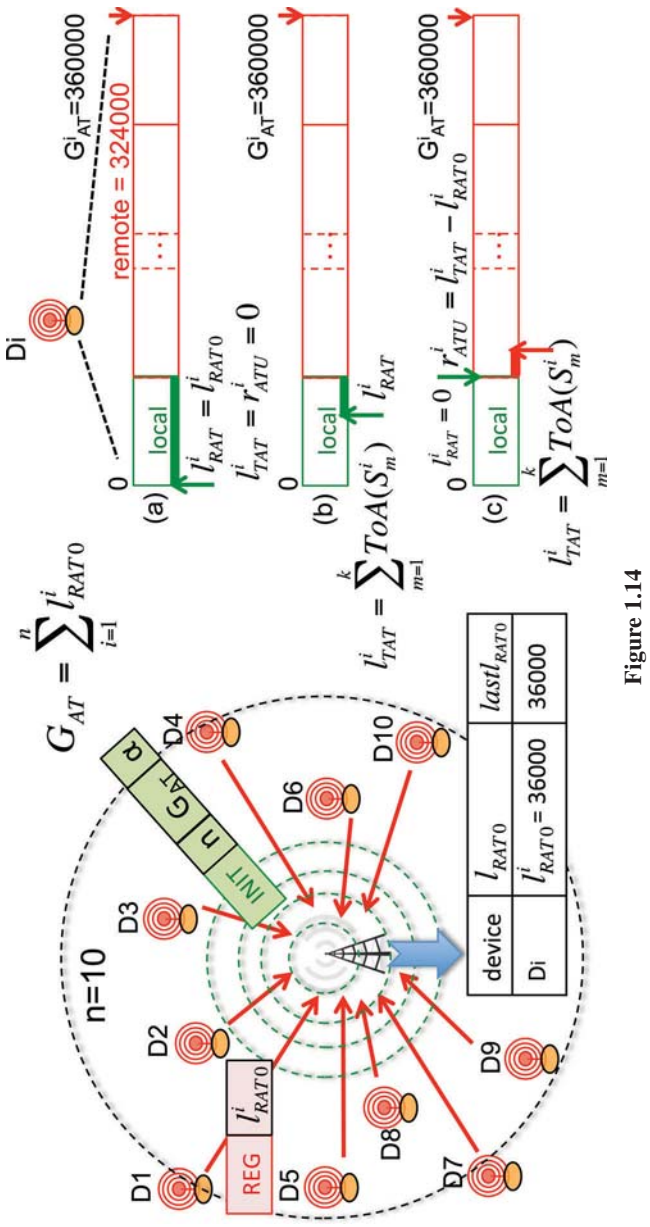
Di
G^i_{AT}=360000
remote = 324000
0
local
(a)
$l^i_{RAT} = l^i_{RAT0}$
$l^i_{TAT} = r^i_{ATU} = 0$
(b)
$l^i_{TAT} = \sum_{m=1}^{k} ToA(S^i_m)$
l^i_{RAT}
$r^i_{ATU} = l^i_{TAT} - l^i_{RAT0}$
$l^i_{RAT} = 0$
(c)
$l^i_{TAT} = \sum_{m=1}^{k} ToA(S^i_m)$
$G_{AT} = \sum_{i=1}^{n} l^i_{RAT0}$
n=10
D1
D2
D3
D4
D5
D6
D7
D8
D9
D10
REG
l^i_{RAT0}
INIT
n
GAT
r
device
Di
l_{RAT0}
l^i_{RAT0} = 36000
$lastl_{RAT0}$
36000

Figure 1.14

Figure 1.15

Their main needs is to get water quality indicators such as temperature and dissolved oxygen. 3 sensors are connected to the generic sensor board: a DHT22 ambient air temperature and humidity sensor, a PT1000 sensor for water temperature and an AtlasScientific DO sensor for water dissolved oxygen level. Using the generic activity duty-cycle module, the board will periodically read values on the 3 connected physical sensors every 3 minutes for our test scenario. The concatenated message string format is as follows: "TC/27.35/HU/67.5/WT/23.47/DO/10.42" where TC and HU are for the air temperature and humidity level from the DHT22, WT for water temperature from the PT1000 and DO for dissolved oxygen level from the AtlasScientific DO sensor. However, at the time of writing, we didn't receive the DO sensor yet so the DO values are emulated.

The gateway is installed on one of the farm's building and can have Internet access. The post-processing stage simply takes the message string to separate it into a list of fields: ['TC', '27.35', 'HU', '67.5', 'WT', '23.47', 'DO', '10.42']. The gateway then pushes data to the GroveStream cloud (with free account) which provides a very flexible framework where it is possible to create several data streams (e.g. TC/HU/WT/DO) per component (the sensor node) in a dynamic manner. Figure 1.16 shows for the 3 deployed sensors their data streams with a focus on the DO stream from sensor 9.

Figure 1.16 also shows the no-Internet connectivity scenario as illustrated previously in Figure 1.6 : the gateway also stores data from the various sensors in its local MongoDB database and acts as a WiFi access point and web server to display the sensed value (here, screenshot from an Android smartphone).

With the generic sensor board, with ready-to-use duty-cycle and low-power building blocks, deploying and setting the whole system was easy and quick. Regarding the physical sensor reading, each environmental parameter is wrapped in a Sensor class object that can implement pin reading and specific data conversion tasks to provide a usable value through a virtual

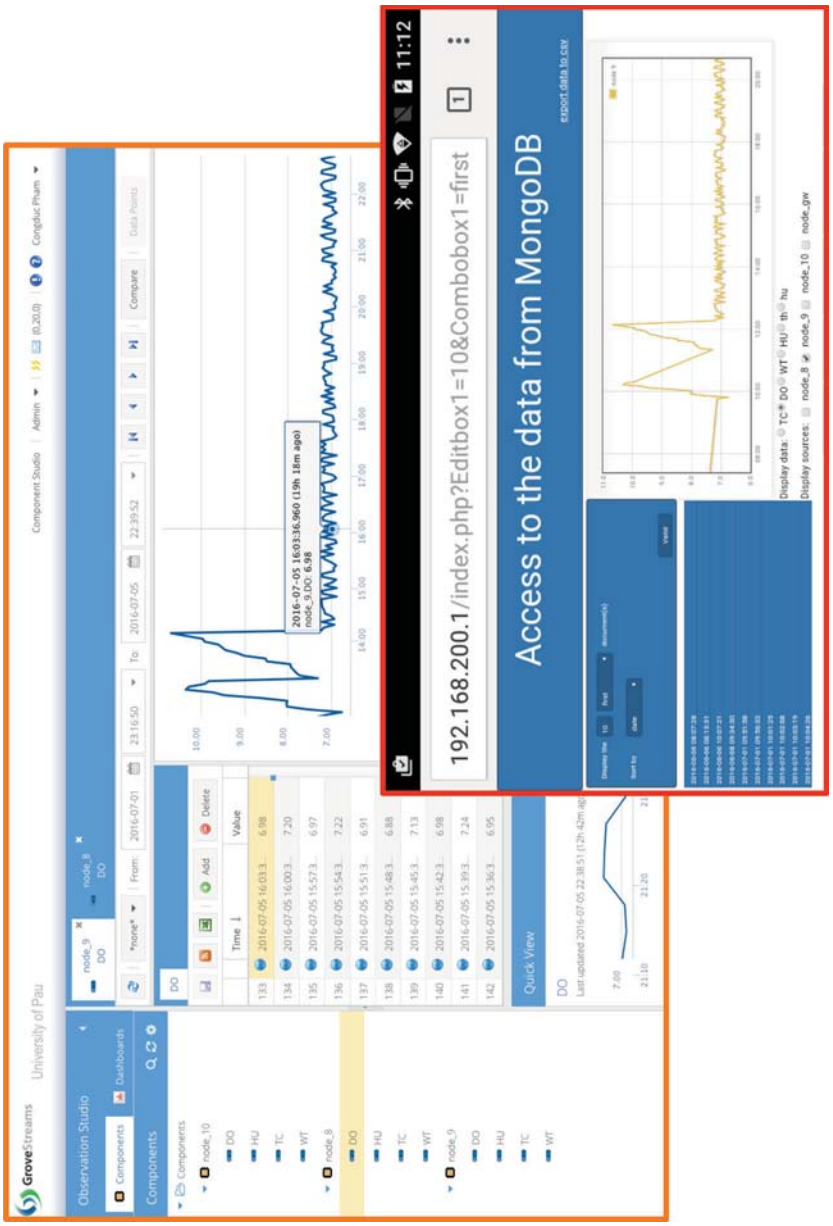
GroveStreams
University of Pau
Observation Studio
Components
Dashboards
Component Studio
Admin
Congduc Pham
Components
node_10
DO
HU
TC
WT
node_8
DO
HU
TC
WT
node_9
DO
HU
TC
WT
Add
Delete
Time
Value
Quick View
DO
Compare
2016-07-05 16:03:36.960 (19h 18m ago)
node_9.DO: 6.98
192.168.200.1/index.php?Editbox1=10&Combobox1=first
Access to the data from MongoDB
export_data_to_csv
11:12

Figure 1.16

get_value() method. For instance, the DHT22 sensor that provides 2 environmental parameters is represented by 2 different Sensor class objects. The sensor board will simply loop and call all get_value() methods of all connected sensors. At the gateway, the post-processing template written in Python can handle an arbitrary number of data streams therefore the whole post-processing stage was left unchanged for uploading data from the 3 physical sensors to our GroveStream cloud account.

1.4 Conclusions

FIRE has evolved into a diverse portfolio of experimental facilities, increasingly federated and supported by tools, and responding to the needs and demands of a large scientific experimenter community. Issues that require attention include the sustainability of facilities after projects' termination, the engagement of industry and SMEs, and the continued development of FIRE's ecosystem to remain relevant to changing research demands. A more strategic issue is to develop a full service approach addressing the gaps between ecosystem layers and addressing integration issues that are only now coming up in other Future Internet-funded projects. A related challenge is to expand the nature of FIRE's ecosystem from an offering of experimental facilities towards the creation of an ecosystem platform capable to attract market parties from different sides that benefit from mutual and complementary interests. Additionally, FIRE should anticipate the shifting focus of Future Internet innovation areas towards connecting users, sensor networks and heterogeneous systems, where data, heterogeneity and scale will determine future research and innovation in areas such as Big Data, and 5G and Internet of Things. Such demands lead to the need for FIRE to focus on testbeds, experimentation and innovation support in the area of "smart systems of networked infrastructures and applications".

To address the viewpoints identified by the FIRE community, the FIRE initiative should support actions that keep pace with the changing state-of-the-art in terms of technologies and services, able to deal with current and evolving experimenter demands. Such actions must be based upon a co-creation strategy, interacting directly with the experimenters, collecting their requirements and uncovering potential for extensions. FIRE must also collaborate globally with other experimental testbed initiatives to align with trends and share expertise and new facilities. Where major new technologies emerge, these should be funded as early as possible as new experimental facilities in the FIRE ecosystem.

This analysis leads to some recommendations regarding the future direction of FIRE, concisely summarized below.

- FIRE's strategic vision for 2020 is to be the Research, Development and Innovation environment for the Future Internet, creating business and societal impact and addressing societal challenges. Adding to FIRE's traditional core in networking technologies is shift of focus in moving upwards to experimenting and innovating on connected smart systems which are enabled by advanced networking technologies.
- FIRE must forcefully position the concept of experimental testbeds driving innovation at the core of the experimental large-scale trials of other Future Internet initiatives and of selected thematic domains of Horizon 2020. Relevant initiatives suitable for co-developing and exploiting testbed resources include the 5G-PPP, Internet of Things large-scale pilots, and e-Infrastructures.
- FIRE should help establish a network of open, shared experimental facilities and platforms in co-operation with other Future Internet initiatives. Experimental facilities should become easily accessible for any party or initiative developing innovative technologies, products and services building on Future Internet technologies. For this to happen, actions include the continuing federation of facilities to facilitate the sharing of tools and methods, and providing single access points and support cross-domain experimentation. Facilities also should employ recognized global standards. At the level of facilities, Open Access structures should be implemented as a fundamental requirement for any FIRE facility. To extend open facilities beyond FIRE, for example with 5G-PPP or Géant and NRENs, co-operation opportunities can be grounded in clear value propositions for example based on sharing technologies and experiment resources.
- FIRE should establish "technology accelerator" functionality, by itself or in co-operation with other Future Internet initiatives, to boost SME research and product innovation and facilitate start-up creation. The long-term goal of FIRE is to realize a sustainable, connected network of Internet experimentation facilities providing easy access for experimenters and innovators across Europe and globally, offering advanced experimentation and proof-of-concept testing. The number of SMEs and start-ups leveraging FIRE can be increased by offering professional highly supported facilities and services such as Experimentation-as-a Service, shortening learning time and decreasing time to market fort

experimentation. A brokering initiative should provide broker services across the FIRE portfolio or via exploitation partnerships. Additionally, community APIs should be offered to make FIRE resources more widely available.

- FIRE's core expertise and know-how must evolve: from offering facilities for testing networking technologies towards offering and co-developing the methodologies, tools and processes for research, experimentation and proof-of-concept testing of complex systems. FIRE should establish a lively knowledge community to create innovative methodologies and learn from practice.
- FIRE should ensure longer term sustainability building upon diversification, federation and professionalization. FIRE should support the transition from research and experimentation to innovation and adoption, and evolve from single area research and experiment facilities towards cross-technology, cross-area facilities which can support the combined effects and benefits of novel infrastructure technologies used together with emerging new service platforms enabling new classes of applications.
- FIRE should develop and implement a service provisioning approach aimed at customized fulfilment of a diverse range of user needs. Moving from offering tools and technologies, FIRE should offer a portfolio of customized services to address industry needs. FIRE should establish clear channels enabling interaction among providers, users and service exploitation by collaboration partners.

FIRE should become part of a broader Future Internet value network, by pursuing co-operation strategies at multiple levels. Cooperation covers different levels: federation and sharing of testbed facilities, access to and interconnection of resources, joint provision of service offerings, and partnering with actors in specific sectoral domains. In this FIRE should target both strong and loose ties opportunistic collaboration. Based on specific cases in joint projects, cooperation with 5G and Internet of Things domains could be strengthened.

Finally, FIRE should evolve towards an open access platform ecosystem. Platform ecosystem building is now seen critical to many networked industries as parties are brought together who establish mutually beneficial relations. Platforms bring together and enable direct interactions within a value network of customers, technology suppliers, developers, facility providers and others. Developer communities may use the FIRE facilities to directly work with business customers and facility providers. Orchestration of the FIRE platform

ecosystem is an essential condition. Steps towards forming a platform ecosystem include the encouragement of federation, the setting up open access and open call structures, and the stimulation of developer activities.

The concept of Low-Power Wide Area Networks (LPWAN), operating at much lower bandwidth, is gaining incredible interest in the IoT domain. In this contribution we presented several important issues when considering deploying low-power, long-range IoT solutions for low-income developing countries: (a) Simplified deployment scenarios, (b) Cost of hardware and services and (c) Limit dependancy to proprietary infrastructures and provide local interaction models. We described our low-cost and open IoT platforms for rural developing countries applications that addressed these issues. Targeted for small to medium size deployment scenarios the platform also privileges quick appropriation and customization by third parties.

References

[1] ETSI, "Electromagnetic compatibility and radio spectrum matters (ERM); short range devices (SRD); radio equipment to be used in the 25 MHz to 1000 MHz frequency range with power levels ranging up to 500 mw; part 1." 2012.

[2] Semtech, "LoRa modulation basics. rev.2-05/2015," 2015.

[3] C. Goursaud and J. Gorce, "Dedicated networks for IoT : PHY/MAC state of the art and challenges," EAI Endorsed Transactions on Internet of Things, Vol. 1, No. 1, 2015.

[4] LoRaAlliance, "LoRaWAN specification, v1.01," 2015.

[5] M. Zennaro and A. Bagula, "IoT for development (IOT4D). In IEEE IoT newsletter." July 14, 2015.

[6] TheThingNetwork, "http://thethingsnetwork.org/," accessed 13/01/2016.

[7] C. Pham, "A DIY low-cost LoRa gateway. http://cpham.perso.univpau.fr/lora/rpigateway.html and https://github.com/congducpham/lowcost loragw," accessed Apr 29th, 2016.

[8] C. Pham, "QoS for Long-Range Wireless Sensors under Duty-Cycle Regu lations with Shared Activity Time Usage", to appear in ACM Transaction on Sensor Networks (TOSN).