Internet of Things and Crowdsourcing – Towards a Multiple Integrating Model Based on the IoT Lab European Research Project

Sébastien Ziegler(✉)

Mandat International, Geneva, Switzerland
sziegler@mandint.org

Abstract. This article presents an initial set of results from the IoT Lab European research project on crowdsourcing and Internet of Things (IoT). It presents the interoperability challenges faced by the project and how it solved them, in order to provide a fully integrated experimental platform for multidisciplinary research combining the potential of the Internet of Things deployment together with richer end-user interactions. It gives an overview of its multiple integrations model, including with heterogeneous IoT, heterogeneous testbeds, crowdsourcing, virtual nodes, and other testbeds federations. It highlights the use of IPv6 as a global and strategic integration enabler.

Keywords: Internet of Things · Crowdsourcing · Interoperability · Crowd-sensing · Experiment · Testbed as a service · Pervasiveness · IPv6 · Interoperability · Multidisciplinary research · Virtual nodes · Testbed federation

1 Introduction and Project Presentation

There is a consensus on the fact that the Internet of Things will be massive and pervasive. It will play a growing role in many application domains, such as: environmental monitoring, transportation and mobility, waste management, energy efficiency and smart grid, water management, security, safety, assisted living, eHealth, etc.

Of course, developing and researching new IoT-related solutions requires addressing the usual technical requirements such as: scalability, reliability, Quality of Service, security, interoperability, portability, etc. Such requirements can be tested and validated in conventional research labs. However, an approach purely focused on technical requirements may lead to a missed target if the end-user perspective is not properly taken into account. In the IoT domain, end-user requirements are probably as much important as technical ones. Hence, understanding the end-user acceptance and satisfaction is critical.

IoT Lab (www.iotlab.eu) [1] is a European research project addressing this challenge, by developing a platform enabling researchers to work on both dimensions. It enables them to use IoT testbeds, including in public spaces, while collecting inputs from end-users through crowdsourcing and crowd-sensing.

IoT Lab is a 3 years FP7 European research project on the Internet of Things and crowdsourcing supported by the European Commission. IoT Lab is developing a research platform that combines Internet of Things (IoT) testbeds together with

B. Mandler et al. (Eds.): IoT 360° 2015, Part II, LNICST 170, pp. 403–414, 2016.
DOI: 10.1007/978-3-319-47075-7_45

crowdsourcing and crowd-sensing capabilities. It enables researchers to exploit the potential of crowdsourcing and Internet of Things testbeds for multidisciplinary research with more end-user interactions.

On one side, IoT Lab approach puts the end-users at the centre of the research and innovation process. The crowd is at the core of the research cycle with an active role in research from its inception to the results' evaluation. It enables a better alignment of the research with the society and end-users needs and requirements. On the other side, IoT Lab aims at enhancing existing IoT testbeds, by integrating them together into a testbed as a service and by extending the platform with crowdsourcing and crowd-sensing capacities.

To achieve such aims, the IoT Lab focuses its research and development of the following objectives:

- Crowdsourcing and crowd-sensing mechanisms and tools;
- Integration of heterogeneous testbeds together;
- Virtualization of testbed components and integration into a Testbed as a Service;
- Testing and validating the platform with multidisciplinary experiments;
- Research end-user and societal value creation through crowdsourcing;
- "Crowd-driven research".

The project also follows a multidisciplinary approach and addresses issues such as privacy and personal data protection through 'Privacy by Design' approach and built-in anonymity.

The consortium is aiming at maintaining the platform beyond the duration of the project in order to serve the research community. A non-for-profit association has been established to jointly maintain the platform and make it available to the research community.

2 Interoperability Challenges

In order to build an integrated experimental platform, IoT Lab has to overcome several interoperability barriers. These various barriers can be summarized and categorized as follow:

A. Intra-tesbed Heterogeneity

Many IoT testbeds are combining and using more than one IoT technology. This heterogeneity needs to be resolved in order to enable the testbed to be integrated into a common experimental platform. Any IoT testbed can be split into three fundamental levels with their corresponding building blocks:

- **The Southbound** composed of physical IoT devices: sensors, actuators, etc. It gathers the end-nodes of the IoT deployment.
- **The Middleware** composed of gateways and a network infrastructure enabling the various end-nodes to be centrally connected and integrated. In the smallest configuration, the middleware function will be provided by a simple gateway. In more complex cases, it can encompass hundreds of interconnected devices and equipment.

- **The Northbound** provides the API and interface enabling the applications and services to interact with the IoT testbed, including in our case the IoT Lab Testbed as a Service (TBaaS).

From the Northbound perspective, part of the communication protocol heterogeneity on the Southbound is usually hidden and ignored when the heterogeneity is limited to the lower layers of the protocol deicepile: when different physical layers are integrated into a common protocol stack, from the network layer upward. This is the case when combining wireless and wired technologies using a common protocol stack on top of the Internet Protocol network layer.

On the Southbound side, the issue emerges when the heterogeneity impacts the network layer and/or its upper layers. When it is the case, the heterogeneity may cause problem for the testbed integration. This heterogeneity can appear at various levels of the Open System Interconnection (OSI) model [2] and can be classified into three main categories:

- **Superficial heterogeneity:** The heterogeneity is limited to the application layer. Different systems are using the same protocol stacks up to the OSI presentation layer, but with distinct application layers and ontologies. In this case, the interoperability issue is often limited to data parsing on the gateway or server side.
- **IP-based heterogeneity:** The heterogeneity appears at a deeper level by combining different protocol stacks on a common IP layer. By impacting the session, transport and presentation layers, the interoperability becomes more complex than the Superficial heterogeneity.
- **Deep multi-protocol heterogeneity:** The heterogeneity impacts the complete protocol pile, including the network layer, by using and combining non-IP based standards and communication protocols such as EnOcean, X10, ZigBee or Z-Wave.

B. Inter-Testbed Heterogeneity

IoT Lab gathers several existing IoT testbeds, including:

- The smart campus of the University of Surrey, in the United Kingdom [3];
- A smart building and a smart office testbed run by Mandat International in Geneva, in Switzerland [4];
- A sensor network testbed from the University of Geneva, in Switzerland [5];
- A sensor and actuator testbed from the CTI in Patras, in Greece [6].

Moreover, Mandat International is interconnected with several distant testbeds, including the smart city of Santander in Spain [7].

Each testbed has its own genesis and will select a certain number of options in terms of architecture and configuration which will be specific and contextual. The natural consequence is a high heterogeneity in terms of architecture and technology deployment. One of the first challenges for IoT Lab has been to overcome this fragmentation by integrating the various resources together into a homogeneous and consistent addressing scheme and data plane.

Additionally, IoT testbeds being located in diverse regions may face diverse network connectivity profiles in terms of Quality of Service as well as in terms of Internet connectivity, including Internet Protocol version 6 (IPv6) availability from the Internet Service Providers (ISP).

C. Crowdsourcing-IoT Integration

Another axis of interoperability is related to the integration of IoT deployments with end-users interactions through their smart phones. In IoT Lab, the smartphone is used both as a source of human inputs (crowdsourcing) and embedded sensor data (crowd-sensing). Integrating both sources of data with IoT to enable direct interactions is another challenge.

D. Testbed Federation Interoperability

Finally, IoT Lab is designed to serve a research community, with a focus on the European FIRE research program [8]. In this context, it has to anticipate integration and interoperability requirements with other testbed federations, such as Fed4FIRE [9] and OneLab [10].

3 Technical Approach

IoT Lab has combined several approaches to overcome its multi cleaved environment.

A. Leveraging on IPv6 as an Integration Enabler

Since 1982, the Internet has benefited from the stable Internet Protocol version 4 (IPv4) [11]. Unfortunately, IPv4 only has a limited addressing capacity of about 4 billion theoretical public addresses (and fewer in practice). This corresponds to less than one public IP address per living adult on Earth, and less than one IP address per set of 10 IoT devices by 2020. The growing allocation of public Internet addresses started to cause concerns, leading to restricted public allocation policies and the introduction of Network Address Translation (NAT) mechanisms to provide end-users with private (and sometimes volatile) addresses. As a consequence, most users effectively became “Internet homeless”, unaware that they were sharing potentially volatile public Internet addresses with others (Fig. 1).

The continuous growth of the Internet convinced the IETF to design a .new protocol with a larger addressing scheme, standardized in 1998 as the Internet Protocol version 6 (IPv6) [12]. IPv6 is based on an addressing scheme of 2^{128} addresses, split by default in two parts: 64 bits for the network address and 64 bits for the host ID. IPv6 is now globally deployed and a growing number of Internet Service Providers (ISP) is offering IPv6 connectivity.

Enabling an IoT mote to access the Internet through a NAT and a shared public addresses is still doable, but enabling the reverse connection where a service wants to access an IoT mote from the Internet is quite less efficient if the mote doesn’t benefit from a unique public address. There is a rather large consensus in the IoT industry that we will reach over 50 Billion interconnected IoT devices by 2020 [13]. The exponential number of IoT devices to be connected highlights the inherent scalability limits of IPv4 as a global IoT addressing protocol.

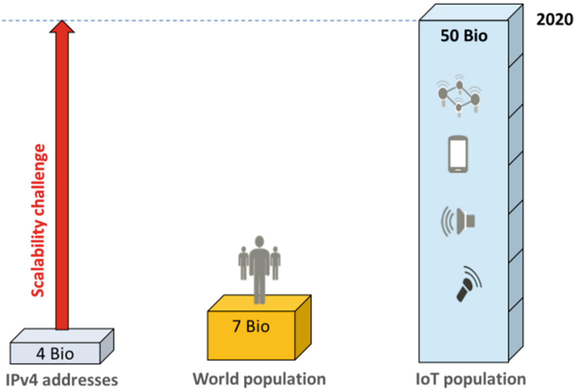

Fig. 1. IPv4 scalability challenge: highlighting the IPv4 addressing capacity gap.

UDG project [14] already demonstrated the ability to integrate all sorts of heterogeneous IoT protocols into an IPv6 addressing scheme. Online applications such as Turn It IPv6 enable IPv6-based control and addressing of non-IP devices [15].

Based on UDG results, the European research project IoT6 [16] designed a common IoT protocol stack based on IPv6 and 6LoWPAN for heterogeneous IoT integration [17–19]. In [20], the authors applied IoT6 model to testbeds and demonstrated multiple testbeds integration through IPv6. This integration was based on testbeds using similar technologies and directly integrated through IPv6.

In the case of IoT Lab, the problematic was more complex. The various testbeds were based on distinct technologies, with different levels of compliance with IPv6. Being distributed cross various countries, the corresponding ISP services offer was uneven too. We ended up with four distinct testbed profiles in terms of network configurations and connectivity,- all to be integrated together:

Case A - Local IPv6 integration, including with non-IP IoT devices:
In this case, the ISP constraints were avoided through a direct integration. However, the testbed included both IPv6 and non-IP IoT devices, using communication protocols such as KNX, ZigBee, EnOcean, BACnet and others. In order to integrate these heterogeneous devices, a UDG proxy has been used to generate consistent and scalable IPv6 addresses to the legacy devices.

Case B - Remote full end-to-end IPv6 compliance:
In this case (TB-B), the testbed integration was achieved through end-to-end IPv6 integration, including 6LoWPAN end nodes directly parsed into IPv6 addresses.

Case C - Remote IPv6 testbed through IPv4 ISP access:
In this case (TB-C), in order to overcome the lack of IPv6 connection at the ISP level, the testbed integration has been performed through v6 in v4 end-to-end tunneling, with a very limited latency impact.

Case D - Remote IPv4 testbed:
Finally, one of the testbed was fully and exclusively IPv4 based (TB-D). In this context, we decided to use a UDG proxy on the server side to map IPv6 addresses on top of the local IPv4 addresses.

The address definitions across the testbeds were maintained consistent by clearly separating the management of the Host ID on one side (IoT address) from the Network ID (Testbed address). This simple approach resulted in a consistent and highly scalable model, enabling the Testbed as a Service (TBaaS) to use a fully integrated and homogenized addressing scheme, including with mobile devices.

B. Multi-protocol Interoperability

In order to overcome the heterogeneity of communication protocols used in some of the testbeds, IoT Lab used the Universal Device Gateway (UDG) [21], a multi-protocol control and monitoring system developed by a research project initiated in Switzerland. It aimed at integrating heterogeneous communication protocols into IPv6. The UDG control and monitoring system enables cross protocol interoperability. It demonstrated the potential of IPv6 to support the integration among various communication protocols and devices, such as KNX, X10, ZigBee, GSM/GPRS, Bluetooth, and RFID tags. It provides connected device with a unique IPv6 address that serves as unique identifier for that object, regardless its native communication protocol. It has been used in several research projects, including by IoT6, where it has been used as an IPv6 and CoAP proxy for all kinds of devices.

In IoT Lab, the UDG platform has been used as a locally deployed proxy in the local testbed (TB-A in the Fig. 2) and as a cloud- based proxy in some other cases (TB-C and TB-D in the Fig. 2). However, for communication protocols which are non-compliant with the Internet Protocol, a local deployment was required.

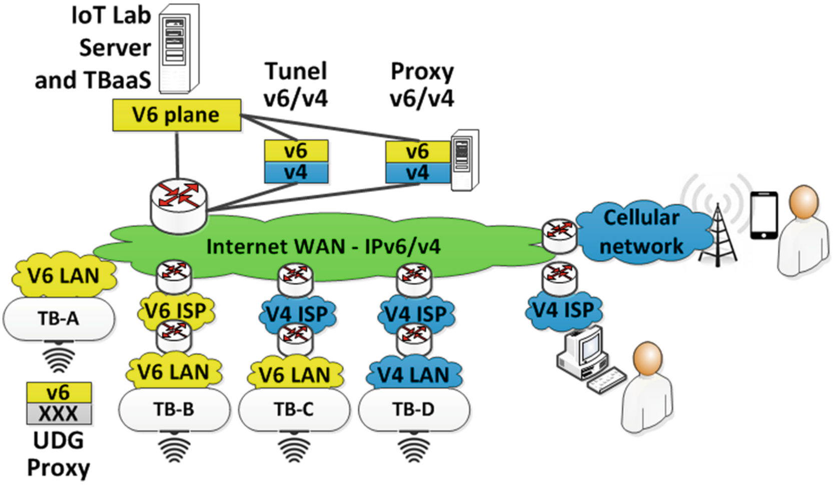

Fig. 2. IoT Lab IPv6-based network integration representing the four main testbed profiles.

C. Crowdsourcing and Crowd-sensing Tool

In the context of IoT Lab, the term "crowdsourcing" refers to direct interaction with participants from the crowd through surveys and other forms of interactions; "crowd-sensing" is understood as the interaction with the embedded sensors of the smart phones. In order to enable direct interactions with end-users, IoT Lab developed a dedicated smartphone application for crowdsourcing and crowd-sensing. This application enables end-users to share inputs and sensing data with researchers on a voluntary basis. The current version of the app is designed for Android environment and will be later extended to other smartphones. A public version of the application will be released in the last quarter of 2015 [22]. The question of IoT Lab application portability on other smart phone platforms is technically trivial and will be considered at a later stage.

D. Virtualizing Resources with a Testbed as a Service

In order to ease access and manageability, the IoT Lab resources are fully virtualized and integrated into a Testbed as a Service (TBaaS) represented in Fig. 3. This approach enables researchers to reserve resources for specific timeslots in order to perform their experiment. Beyond the conventional MySlice capacities, IoT Lab enables to select participants according to all sorts of criteria, including socio-economic profiles, ages and location.

The TBaaS is largely aligned with the Fed4FIRE architecture, including in terms of OML and Rspec specifications. This approach has been adopted for increased interoperability and for easier integration with other European testbeds in the future.

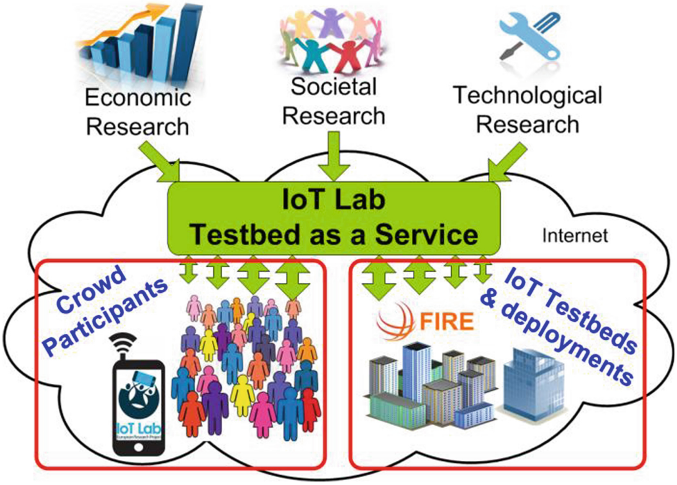

Fig. 3. IoT Lab 'testbed as a service' model combining crowdsourcing and IoT deployments into an online application enabling researchers to perform remote experiments.

E. Aligning on a de facto European Testbed Federation Standard

IoT Lab is closely linked to the FIRE programme of research supported by the European Commission aiming at supporting the research community with experimental infrastructure. In the context of the FIRE programme, several testbeds have been developed. One of the objectives of the European Commission is to interconnect and brings these various testbeds together. The lead project to support such federation is Fed4FIRE, which relied itself on previous research projects. Fed4FIRE has progressively selected and specified several open interfaces to enable such federations. In order to ease the integration with other testbeds, IoT Lab has decided to implement and provide Fed4FIRE compliant APIs.

F. Enabling Virtual and Physical Device Integration

One of the objectives of the IoT Lab project was to explore the potential of combining physical and virtual devices within the same platform. This objective has been implemented in the context of the project and enables researchers to emulate all sorts of nodes and to make them interact with real ones.

G. Privacy by Design Approach

Another key dimension of IoT Lab as a research project is its commitment to develop a fully privacy by design platform. It must find the right balance between the need for the researchers to access reliable and characterized resources, including socio economic profiles,- while ensuring a complete compliance with the European standards in terms of personal data protection. By following a holistic approach, this effort has enabled the consortium to develop a fully privacy-compliant platform by combining various methods, strategies and technology enablers.

4 Triple Paradigm Shift

A. Extending IoT Research to End-Users

Traditional IoT-related experiments are usually focused on the technical features and dimensions of IoT deployment. However, due to its ubiquitous and pervasive dimension, the IoT will require more and more end-user perspective to be taken into account. IoT Lab enables researchers to extend their experiments to this fundamental dimension: how are solutions accepted by end-users, where and what value they perceive in a given deployment, etc.

B. Pervasive Experiments

IoT Lab enables the researchers to perform experiments in all sorts of environments, including among others smart buildings and smart cities. A set of initial experiment has started to assess the potential of IoT and crowdsourcing to assess the level of smartness and sustainability of any city. This work is a direct contribution to the ITU Focus Group on Smart Sustainable Cities [23]. In other words, IoT Lab enables research to leak outside of traditional labs by exploring IoT deployments in real environment with real end-users providing real time feedbacks.

C. Crowd-Driven Research Model

Finally, IoT Lab is enabling and testing a new model of crowd-driven experiments. The key concept is to enable anonymous participants (the crowd) to suggest research topics and to rank them. According to the results, the favorite ideas will be proposed to researchers for selecting and implementing some of them. The results are expected to be shared with the participants (the crowd) in order to get their inputs and their assessment of the generated results. The idea is to explore the potential of a bottom-up research model on the IoT based on crowdsourcing and closer interactions between the researchers and potential end-users as illustrated in Fig. 4.

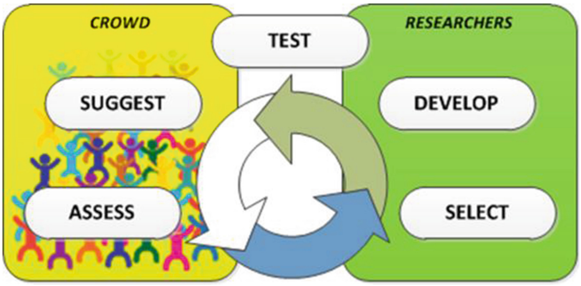

Fig. 4. Crowd-driven research model enabling anonymous end-users to trigger and drive experimentation process in cooperation with researchers.

5 Ongoing Experiments and Open Invitation

IoT Lab expects to support experimentally driven research, including multidisciplinary experiments. The initial version of the IoT Lab experimental platform is working and has been demonstrated at the World Summit on the Information Society (WSIS) [24].

At the present time, several experiments are in progress with targeted groups of end-users, including an experiment on energy efficiency in building, another one on a smart city deployment and the third one on the ITU Smart Sustainable Cities Key Performance Indicators (SSC KPI). Following an agile methodology, the first set of experiments enables the project to fine tune and to improve the designed tools.

In September 2015, the IoT Lab smart phone application will be released to the public. The objective will be twofold:

- Engaging the public (crowd) to join our community of participants to take art in experiments.
- Inviting researchers to use the IoT Lab platform for their own experiments. Any interested research team is welcome to contact us.

6 Conclusions – Towards a Quintuple Integration Model

In order to provide a completely integrated experimental platform combining IoT deployments with end-user interactions through crowdsourcing and crowd-sensing, IoT Lab had to overcome several interoperability barriers. Several IoT testbeds and a

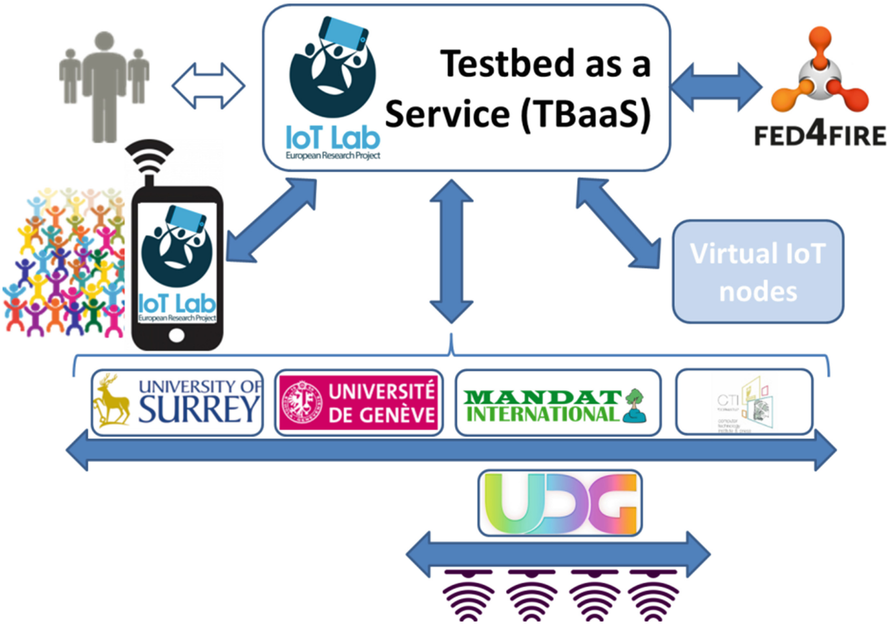

Fig. 5. IoT Lab six fold integration model represented by the blue arrows from the bottom and from left to right: heterogeneous IoT integration; heterogeneous testbeds integration through IPv6; crowdsourcing and crowd-sensing integration into the TBaaS; physical IoT testbeds integration into the TBaaS; virtual nodes integration; multiple testbed federations integration. (Color figure online)

potentially unlimited number of end-users are integrated together into a centralized and ubiquitously accessible Testbed as a Service (TBaaS).

As illustrated in Fig. 5, IoT Lab has applied and is further researching a six fold integration model by:

- Integrating heterogeneous IoT devices and communication protocols (including non-IP based protocols) integrated through the UDG technology;
- Integrating heterogeneous testbeds through IPv6 interconnection, proxy and aggregation;
- Integrating end-users through crowdsourcing and crowd-sensing capabilities enabled by the IoT Lab smart phone application;
- Integrating virtual IoT nodes with the physical ones for richer experiments;
- Integrating the IoT resources and testbeds into a Testbed as a Service in the Cloud, enabling all IoT Lab resources to be virtualized and to be accessible to researchers through remote access and control from anywhere.
- Integrating the platform with other testbed federations, such as Fed4FIRE, by using emerging de facto technologies for testbeds federation.

The IoT Lab platform is still in its improvement and fine tuning phase. It is open to partnerships with third parties research projects interested to test it and to join our effort for building a new experimental platform for the research community.

Acknowledgments. This article has been written in the context of the IoT Lab European research project of the 7th Framework Program supported by the European Commission. It is implemented by a consortium coordinated by Mandat International and gathering the Universities of Surrey, Geneva, Lulea, Southampton, as well as Dunavnet, Alexandra Institute, the Computer Technology Institute and Press "Diophantus", and the support of the Istituto Italiano per la Privacy. IoT Lab project work on interoperability also capitalized on other projects results, including IoT6 [16] and UDG [14].

References

1. IoT Lab is a European research project from the FP7 research programme. http://www.iotlab.eu
2. Open Systems Interconnection model developed by the International Standardization Orgaization: ISO/IEC 7498-1:1994. http://www.iso.org
3. University of Surrey. http://www.surrey.ac.uk
4. Mandat International. http://www.mandint.org
5. University of Geneva. http://www.unige.ch
6. CTI - Computer Technology Institute and Press "Diophantus". http://www.cti.gr
7. Smart Santanders. http://www.smartsantander.eu
8. Future Internet research in the ICT Programme. http://www.ict-fire.eu
9. Fed4FIRE is the main project aiming at federating European research testbeds. http://www.fed4fire.eu
10. OneLab. https://onelab.eu/
11. Postel, J.: Internet Protocol, RFC 791, Internet Engineering Task Force RFC 791, September 1981
12. Internet Protocol, Version 6 (IPv6), RFC 2460, IETF. https://www.ietf.org/rfc/rfc2460.txt
13. Ericson white paper 284 23-3149 Uen, More than 50 billion connected devices, February 2011. http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf
14. UDG is an IPv6-based multi-protocol control and monitoring system using IPv6 as a common identifier for devices using legacy protocols. It was developed by a Swiss research project and used by IoT6 for research purpose. More information on UDG ongoing developments. www.devicegateway.com
15. http://www.turnitipv6.com
16. IoT6 European research project. http://www.iot6.eu
17. Ziegler, S., et al.: IoT6 – moving to an IPv6-based future IoT. In: Winter, J., Ono, R. (eds.) The Future Internet. LNCS, vol. 17, pp. 161–172. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38082-2_14
18. Ziegler, S., Thomas, I.: IPv6 as a global addressing scheme and integrator for the Internet of Things and the Cloud
19. Ziegler, S., Palattella, M.R., Ladid, L., Krco, S., Skarmeta, A.: Scalable integration framework for heterogeneous smart objects, applications and services. In: Internet of Things – From Research and Innovation to Market Deployment. River Publishers Series in Communication (2014)

20. Ziegler, S., Hazan, M., Xiaohong, H., Ladid, L.: IPv6-based test beds integration across Europe and China. In: Leung, V.C.M., Chen, M., Wan, J., Zhang, Y. (eds.) Testbeds and Research Infrastructure: Development of Networks and Communities. Springer, Heidelberg (2014)
21. UDG is maintained by the UDG Alliance managed by Device Gateway and has been used by several European rsearch projects, including Hobnet, IoT6, EAR-IT and currently by IoT Lab. http://www.devicegateway.com
22. The application will be made available on the IoT Lab website. http://www.iotlab.eu
23. ITU Focus Group on Smart Sustanable Cities. http://www.itu.int/en/ITU-T/focusgroups/ssc/Pages/default.aspx
24. World Summit on the Information Society 2015. http://www.itu.int/net4/wsis/forum/2015/