IoT6 – Moving to an IPv6-Based Future IoT*

Sébastien Ziegler[1], Cedric Crettaz[1], Latif Ladid [2], Srdjan Krco[3], Boris Pokric[3], Antonio F. Skarmeta[4], Antonio Jara[4], Wolfgang Kastner[5], and Markus Jung[5]

[1] Mandat International, Geneva, Switzerland
{iot6,sziegler}@mandint.org
[2] University of Luxembourg, Luxembourg, Luxembourg
latif@ladid.lu
[3] Ericsson, Belgrade, Serbia
srdjan.krco@ericsson.com
boris.pokric@gmail.com
[4] University of Murcia, Murcia, Spain
{skarmeta,jara}@um.es
[5] Vienna University of Technology, Vienna, Austria
{k,mjung}@auto.tuwien.ac.at

Abstract. IoT6 is a research project on the future Internet of Things. It aims at exploiting the potential of IPv6 and related standards to overcome current shortcomings and fragmentation of the Internet of Things. The main challenges and objectives of IoT6 are to research, design and develop a highly scalable IPv6-based Service-Oriented Architecture to achieve interoperability, mobility, cloud computing integration and intelligence distribution among heterogeneous smart things components, applications and services. The present article starts by a short introduction on IPv6 capabilities for the Internet of Things and information on the current deployment of IPv6 in the world. It continues with a presentation of the IoT6 architecture model and its concept of service discovery. Finally, it illustrates the potential of such IPv6-based architecture by presenting the integration of building automation components using legacy protocols.

Keywords: IoT, M2M, IPv6, CoAP, architecture, interoperability, building automation.

1 Introduction

The Internet of Things is exponentially growing towards an ecosystem interconnecting tens of billions of smart things. Simultaneously, the Internet Protocol version 6 (IPv6) is scaling up the Internet to an almost unlimited number of globally reachable addresses. IoT6 is a 3 years FP7 European research project on the Internet of Things. It aims at exploiting the potential of IPv6 and related standards (6LoWPAN, CORE, COAP, etc.) to address current needs of the Internet of Things, considering how the IPv6 features like addressing, security, mobility and autoconfiguration could help the deployment of IPv6 sensor based solution allowing E2E communication on the IoT ecosystem. Its main challenges and objectives are to research, design and develop a

* Invited Paper.

A. Galis and A. Gavras (Eds.): FIA 2013, LNCS 7858, pp. 161–172, 2013.

highly scalable IPv6-based Service-Oriented Architecture. Its potential will be researched by exploring innovative forms of interactions such as:

- Information and intelligence distribution.
- Multi-protocol interoperability with and among heterogeneous devices.
- Device mobility and mobile phone networks integration, to provide ubiquitous access and seamless communication.
- Cloud computing integration with Software as a Service (SaaS).
- IPv6 - Smart Things Information Services (STIS) innovative interactions.

The main outcomes of IoT6 are recommendations on IPv6 features exploitation for the Internet of Things and an open and well-defined IPv6-based Service Oriented Architecture enabling interoperability, mobility, cloud computing and intelligence distribution among heterogeneous smart things components, applications and services, including with business processes management tools.

2 IPv6 Capabilities for the Internet of Things

Global Internet human users are currently estimated at 2.4 Billion and are further projected to climb to 3.0 Billion by 2015. More significantly, the number of Internet connected objects has overpassed the number of connected human beings, and is expected to expend far beyond the human population, with 20 to 50 Billion interconnected smart things. Over the last decades, the Internet Protocol version 4 (IPv4) has emerged as the mainstream protocol for networking layer. However, this protocol was not designed for the Internet of Things (IoT) and is inherently limited to about 4 Billion addresses. At the global level, IANA has entirely exhausted its IPv4 addresses allocation on the 3rd Feb 2011; and two out of five RIRs (Regional Internet Registries) have achieved their address allocation limit in April 2011 by APNIC and in August 2012 by RIPE. The Internet Protocol version 6 (IPv6) has been adopted by IANA and the RIRs to overpass the IPv4 limitations and to address the growing demand. IPv6 provides 2^{128} unique Internet addresses, or 3.4×10^{38} addresses, which corresponds to over 6.67×10^{17} unique addresses per square millimeters of Earth surface. It also provides new features enabling an easier configuration of devices, data streaming compliance, improved security, and effective peer-to-peer connections avoiding Network Address Translation (NAT) barriers. All those elements contribute to turn IPv6 into a natural candidate for the addressing and networking of a globally connected Internet of Things. Many devices are already interconnected through the Internet Protocol, including printers, sensors, lighting, healthcare systems, smart meters, video cameras, TVs and heating control systems. The emergence of IPv6-related standards specifically designed for the IoT, such as 6LoWPAN, CoAP, and CoRE[14][15], has enabled highly constrained devices to become natively IP compliant. IPv6 is being referred to by a growing number of IoT and Machine-to-Machine (M2M) related standards, such as oneM2M, OMA Lightweight M2M, or the IEEE 802.15.4g protocol, which will support Advanced Metering Infrastructure (AMI) for smart cities deployments.

3 IPv6 Worldwide Deployment

The potential of IPv6 to interconnect the future IoT depends on its effective deployment. Thus, it is important to consider its current evolution. Year 2012 has indicated a clear shift towards a global IPv6 deployment across the world. Google has reached 1% of users connecting over IPv6 [1] and over 22% of the top 500 web sites are already IPv6 compliant [2]. In Europe, IPv6 adoption is gaining significant momentum with RIPE NCC having announced its final /8 allocation policy for IPv4 address pool in August 2012. It is reinforced by the European Commission action plan for the deployment of IPv6 [3]. On a percentage basis, Romania is leading the deployment with 8.43% per cent adoption [4] rate followed by France at 4.69%. In North America, IPv6 adoption rate is at 1.97%. It translates into an estimated IPv6 user base of 3.5 million users, the largest base of IPv6 users in the world. In Asia and Pacific, countries like China, Japan and South Korea are proactively supporting the deployment of IPv6 with IoT applications. In March 2000, Japanese Telecommunications Company NTT became the world's first ISP to offer IPv6 services to the public. Millions of smartphones, tablets and other devices in homes, offices and public spaces throughout Japan rely on the country's long-standing IPv6 network. Japan ranking highly at 2.04% user penetration on IPv6. China launched its five-year plan for early IPv6 adoption in 2006. The program, known as the China Next Generation Internet (CNGI) project, has been instrumental in helping the country build the world's largest IPv6 network, which has been showcased at the 2008 Olympic Games in Beijing. Its expansive next-generation network connects millions of devices, users, and security and transportation systems throughout the country. In 2004, South Korea initiated widespread migration, making it one of Asia Pacific's earliest adopters of the next-generation Internet protocol. The policy, established by the Ministry of Information and Communication, required the mandatory upgrade to IPv6 in the public sector by 2010. Indian authorities aim to achieve major transitions on dual stack across the industry by 2017 and plans to achieve complete IPv6 ready status by 2020 [5]. The rest of the Asia Pacific region of Hong Kong ,Singapore, Thailand, Malaysia, Sri Lanka and Indonesia are at a nascent stage of IPv6 adoption and have got started on IPv6 initiatives with mandates for IPv6 transition around 2015-16 timeframes. Africa being a late entrant into the technology landscape also has the advantage of direct IPv6 implementation. According to AfriNIC, IPv4 allocations have been on the decline and countries have started taking up IPv6. Kenya and South Africa are leading in IPv6 allocations. In Latin America, countries such as Brazil, Argentina, Venezuela, Columbia, Chile and Peru are beginning their IPv6 transition.

It results form the current stage, that IPv6 is not fully deployed yet. However, the current evolution tends to provide an extensive worldwide IPv6 network able to address and interconnect an unlimited number of smart things across all the continents.

4 IoT6 Architectural Model

Over the years, a number of projects have specified various versions of IoT architectures, basing them on the specific requirements the projects were addressing (SENSEI

[6], HOBNET [7], iCORE[29], BUTLER [30]etc.) Due to a large heterogeneity of application domains and consequently the requirements, the approaches to the architecture specification differed between the projects resulting in more or less different architectures comprised of a number of components and protocols. The diversity of the architectures was soon recognized by the community as one of the factors limiting the progress in the domain which resulted in more coordinated efforts driven by the IERC (Internet of Things European Research Cluster) aiming at specifying a common, harmonized reference IoT architecture. Significant roles in this effort have the IoT-A and IoT-I projects [8]. The former has extensively analysed IoT application domains to identify requirements and devise a reference architecture model that can be used for specification of reference architectures and architecture instantiations suitable for specific systems. The latter project analysed the IoT-A architecture reference model, compared it to other relevant architectures and validated its applicability in a range of application scenarios [9].

Other important coordinated effort that should be noted is the FI-PPP program and the FI-WARE architecture [10]. There, a detailed architecture of a Future Internet platform has been designed taking into account inputs from numerous European organizations, also covering in the process the IoT functionality as an important aspect of the Future Internet. Further to this, a large and significant effort has been invested in the framework of the ETSI M2M Technical Committee, and more recently oneM2M alliance [11] resulting in corresponding ETSI technical specifications for M2M architecture.

The aim of the IoT6 architecture is to enable a highly scalable IPv6-based Service-Oriented Architecture to achieve interoperability between different communication technologies and interaction with application based services like cloud based services, intelligent information processing, application specific visualization and integration with business processes and workflows. The approach selected towards definition of the IoT6 architecture is to leverage the on-going related activities by extending, enhancing and modifying different architectural components with a particular focus on the communication layer. This focus on the communication layer comes from the project focus on IPv6 as the main integrating point for various IoT devices, underlying technologies as well as higher layer services and applications. The goal was not only to use IPv6 as a pure transport protocol, but to leverage the embedded IPv6 features to enable functions currently implemented using higher layer protocols. This approach complements well other IoT architecture efforts as these mainly focus on higher layers and do not address the details of the communication layer, but usually assume IP or any other communication paradigm.

Having this in mind, based on the requirements analysis of several application domains and similar efforts done in other projects as well as the IoT reference architecture model proposed by the IoT-A project and IoT architectures designed by FI-WARE and ETSI M2M, the initial IoT6 architecture was designed. To a large extent, the IoT6 architecture adopts the existing solutions and provides novel proposals on the communication layer. These proposals facilitate utilization of IPv6 addressing schemes across IoT devices, including those that do not natively support IPv6 and leverage DNS (Domain Name System) functionality to provide resource and service registration and discovery. To that end, service discovery is conducted through the

IPv6 network-based information systems that are already deployed, such as the domain name system with service discovery (DNS-SD). In the same manner, a resource directory serving a local domain can be replaced with a multicast DNS (mDNS), thus providing the required functionality by exploiting and extending the IPv6 functions only [12].

Figure 2 shows the IoT6 architecture model indicating different network domains. IoT devices (sensors and actuators) can be found at the bottom of the architecture stack outlined in Figure 1. There are two distinct types of devices: IoT6 compliant and non IoT6 -compliant or legacy devices. The IoT6 compliant devices can be IPv6-enabled IoT devices or IoT devices based on protocols such as 6LoWPAN and the proposed GLoWBAL IPv6 [13], CoAP [14] and CoRE [15]. protocols. The non-IoT6 compliant devices are based on other, non-IP communication protocols, as well as IPv4-based devices. The non-IoT6 compliant devices require gateways or proxies to be connected to the rest of the IoT6 system in order to adapt the native protocols, functionality and addressing to IPv6 through a transparent mechanism. IoT6 Local Area Network (LAN) provides connectivity mechanisms to IoT devices taking into account their specific protocols and technology and making them available to the rest of the IPv6 powered environment in terms of discovery, access and management. The IoT6 wide area network (WAN) enables the interconnection of multiple IoT6 LANs and IoT6 backend servers and creates the overall IoT6 core infrastructure. This infrastructure offers access to the IoT devices from the application-level layer consisting of different services such as Software as a Service (SaaS), Smart Things Information Service (STIS), Web and mobile applications to mention a few examples [16].

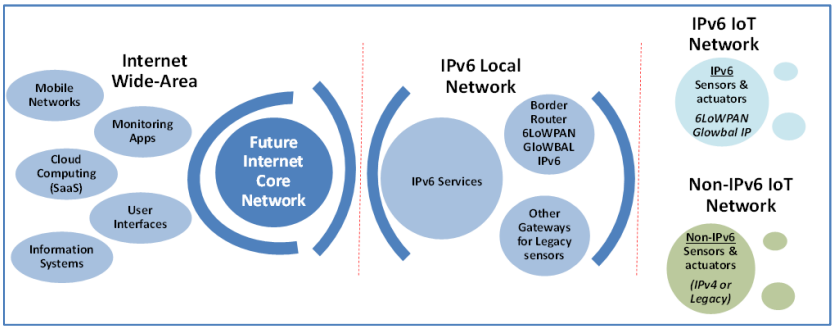

Fig. 1. High-level IoT6 architecture indicating network domains

A more detailed architecture is shown in Figure 2 indicating the component level view. These components take into account the three level of entities indicated in figure 1, covering the upper layer the Internet Wide-Area servies, the middle layer the local IPv6 services like half-gateways, and finally the lower layer the IoT sensor area with the possible integration of legacy system. As can be seen, it builds largely on the ETSI oneM2M and FI-WARE IoT architectures and adds specific solutions on the communication layer. It comprises components from the FI-WARE architectural

model as well as service discovery components such as Resource Directory (digrectory), specific protocol adapters accommodating DNS-SD, mDNS, CoAP Resource Directory, and its own IoT6 stack API (discovery API) support. There are distinct types of device (sensor) clusters, namely ETSI M2M clusters, large IPv6 clusters, small IPv6 clusters, RFID clusters, and other clusters (IPv4, proprietary, legacy technologies, etc.). As for the ETSI M2M clusters and others, the existing service discovery mechanism supports CoRE Resource Directory. It is based on DNS-SD and mDNS with appropriate protocol adapters providing the full set of required functionality. The focus of the subsequent analysis related to the service discovery is on the IPv6 sensor clusters using the DNS-SD and mDNS methodology.

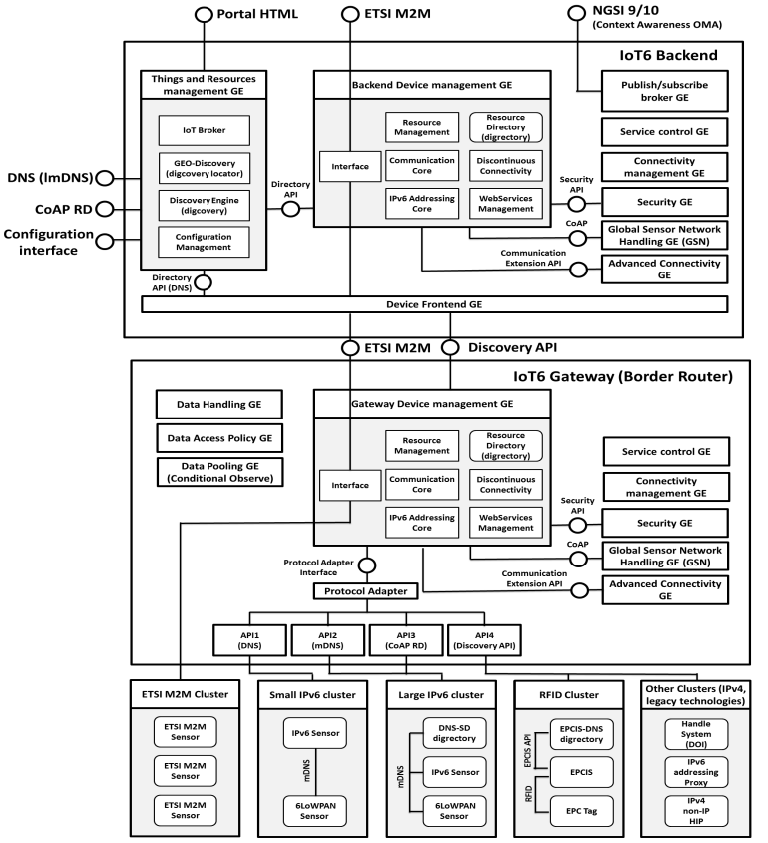

Fig. 2. Detailed IoT6 reference architecture

5 Resources Repository and Service Discovery

A key requirement for any IoT architecture is to provide adequate service discovery and registries. This becomes even more challenging, when it is supposed to encompass

the actual heterogeneity of the IoT. IoT6 has designed a concept of "*Digcovery*", which is illustrated in Figure 3. This presents how the different technologies involved in the Internet of Things ecosystem such as Smart Objects, RFID tags, and legacy devices, are integrated into different directories named "*digrectories*". These *digrectories* are managed through DNS-queries extended with an elastic search engine in order to make it scalable at the same time it offers a centralized point, called "*digcovery core*", to manage and discover them.

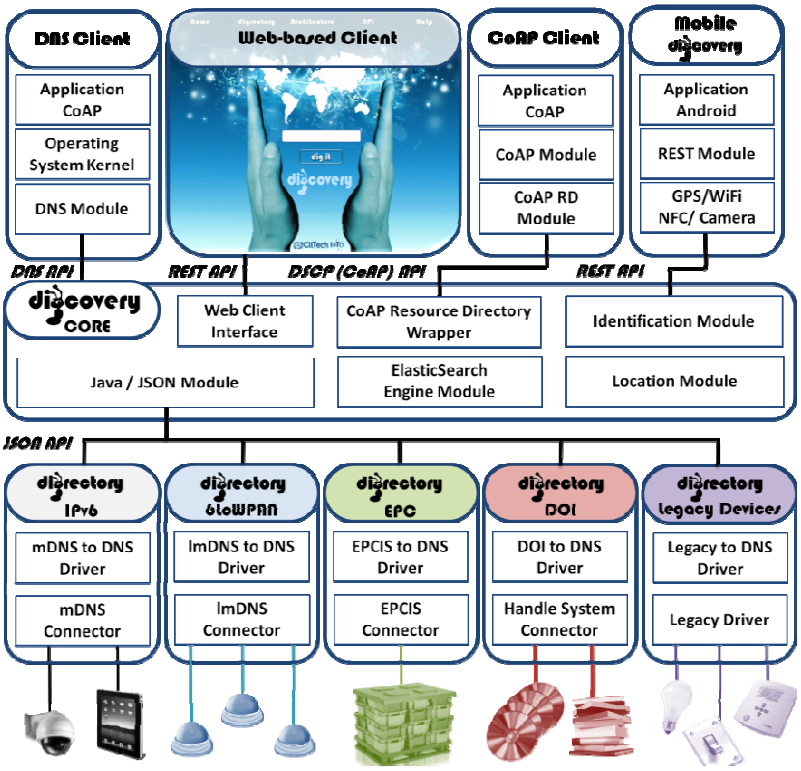

Fig. 3. IoT6 Digcovery ecosystem

All the resources and services are mapped to a common ontology and description, based on existing ontologies and profiles from the IP-enabled Smart Objects Alliance (IPSO) [17, 18], and oBIX from the Building Automation area. It will also consider emerging profiles developed by standardization bodies such as the Open Mobile Alliance (OMA) [19]. These semantic layer interfaces have been integrated into the DNS-SD types, in order to reach a common semantic description accessible through DNS and powered with the universal IPv6 capabilities to carry out the discovery resolution.

This also presents how to interoperate with the discovery architecture through other interfaces different to DNS such as RESTful architecture with data structured in

JSON format. JSON has been chosen for the interoperability with all the resources, since it is considered by the Working Groups from the IETF such as the Constrained Resources (CoRE) Working Group, and the Constrained Management (COMA) Working Group as the most suitable protocol to structure the data for constrained resources, leaving other formats such as XML optional.

The IoT6 architecture uses a RESTful interface based on CoAP [20] developed by the IETF CoRE Working Group. This enables the integration of constrained devices with an overhead of only 4 bytes and a functionality optimized for the observation of resources [21], application-layer fragmentation [22], and mapping with the HTTP-based RESTful architecture.

Specific solutions have been developed to enable look-up and queries over *digcovery,* exploiting ElasticSearch and enabling queries on various *Digrectories* with context awareness, based on location or resource types [ref]. The proposed architecture enables organized and context-based queries over heterogeneous and distributed registries of resources and services.

The platform can use Domain Name Servers (DNS) in order to exploit existing IP-based technologies, protocols and mechanisms. It can also use a Web-based platform to access and register resources through a RESTful architecture. However, the IoT6 architecture can integrate other repositories such as HANDLE [23], for the mirroring of the objects with Digital Object Identifiers (DOI), or EPCIS for RFID tags.

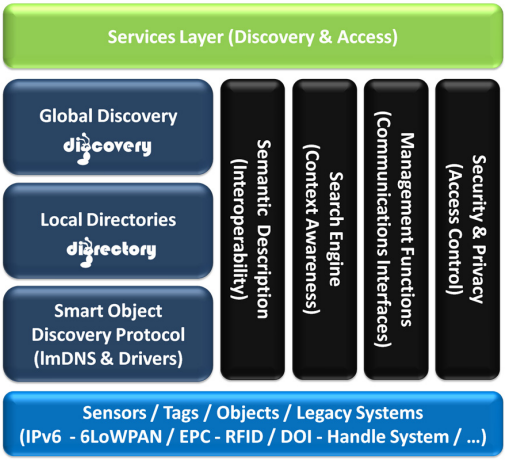

Fig. 4. Digcovery components

6 Building Automation Components Integration

Building automation components constitute a particularly interesting domain of IoT to test an IPv6-based architecture, due to their extensive use of heterogeneous communication protocols. Buildings have to provide supportive conditions for people to work

and relax. The underlying demands are best tackled through an appropriate design of the building and its structure as well as technical infrastructure. The task of building automation systems (BAS) is to provide automatic feedback control, central and remote monitoring and access to underlying building services. These building services primarily address the energy intensive areas of heating ventilation and air conditioning (HVAC) and lighting/shading. Besides, dedicated systems for the domains concerning security and safety exist. On the way to intelligent buildings and smart homes, cross-domain integration is of particular relevance. As a next step, it is desirable to integrate existing building automation technologies into an information infrastructure aiming at use case scenarios and applications that are part of the IoT.

Building automation systems follow the well-known automation pyramid with functions dedicated for the field, automation and management level. Meantime, progress in computer engineering progress allows intelligent field devices to take over functions of the automation layer. This has led to a 2-tier architecture of underlying control networks with a field and a backbone layer. While at the field level robust fieldbus networks are deployed, Ethernet and IP communication is already prevalent at the management level.

Over the last three decades, many different protocols for the use in building automation have emerged. Ideally an all-in-one solution that allows total control of all conceivable scenarios within a building would be desired. However, even despite the long timespan of their development, not one specific protocol has yet emerged that covers all relevant domains. Rather, many different protocols co-exist. Some of them aim at the control of multiple domains (e.g. BACnet, KNX, LonWorks), while others exclusively offer tailored functions for a specific area (e.g. lighting: DALI, blinds and shutters: SMI). Another particular class of technologies are wireless standards such as ZigBee, EnOcean, Z-Wave and KNX-RF to name just a few [24].

Integration of this heterogeneity of technologies within the building automation domain is already challenging. A further integration within the future Internet of Things is even a more thrilling task. For the desired interconnection, various approaches can be taken. These have their individual benefits and shortcomings, but all of them aim at providing a homogeneous view on the underlying heterogeneous protocols and systems. While an integration of systems is beneficial in several ways, it is also the case that several challenges still need to be solved on the road to an integrated system. Since the management tier of BAS already provides IP communication, for the integration Web service based approaches seem a reasonable choice. Here OPC Unified Architecture (OPC UA) [25], open Building Information Exchange (oBIX) [26] or Building Automation Control Network / Web Services (BACnet/WS) [27] come into play which either facilitate SOAP or RESTful Web services (or both) for their protocol bindings. These technologies also define and care for information models that can be used for an abstract data representation of the different involved technologies.

Recent research favors the use of RESTful Web services and IPv6 even on most constrained devices and within constrained wireless networks aiming at providing the deepest possible integration and interoperable end-to-end communication within the future Internet of Things. The constrained application protocol (CoAP) together with

optimization technologies like 6LoWPAN and EXI allow to deploy sensors and actuators with Web service based protocol stacks.

While Web service interfaces at centralized servers are a feasible solution, within the IoT6 project a solution has been created that combines existing integration approaches with the recent advances for constrained RESTful environments using a protocol stack based on IPv6, CoAP, EXI and oBIX [28]. IPv6 acts a common network layer for end-to-end communication. By means of CoAP, RESTful Web service interface are realized. EXI is used to compress the exchanged XML messages in order to keep the payload of frames exchanged within (wireless) links as low as possible to avoid message fragmentation. Finally, oBIX supports an object model that can be used to model domain specific contracts for different device types. It further provides a standardized XML schema that is required for optimal EXI encoding.

Currently, this protocol stack is deployed within the IoT6 project on one hand on constrained devices and on the other hand on a gateway that offers a central or per-device interfaces based on the protocol stack for existing building automation devices (e.g. KNX, BACnet, ZigBee). These interfaces are then further integrated into the overall IoT6 architecture.

7 Conclusion

After one year of research, IoT6 has demonstrated a good compliance between IPv6 and the various IoT domains requirements, including tags, sensors, building automation, mobile phones and building automation components. A comprehensive IPv6-based architecture for the IoT has been designed and will be tested through practical use cases implementations. IoT6 will continue researching and exploring IPv6 features for the integration of a heterogeneous and fragmented IoT. In parallel, IPv6 starts to be globally deployed across the World and a growing number of IoT and M2M related standards are now clearly referring to IPv6 for their networking layer. It seems to be of good auguries for a possible global convergence and interconnection of the future IoT through IPv6.

References

1. Google IPv6 statistics, `http://www.google.com/ipv6/statistics.html`
2. According to a study made by Lars Eggert, IRTF Chair– IPv6 Deployment Trends
3. Advancing the Internet: Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe, European Commission communication, `http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/communication_final_27052008_en.pdf`
4. IPv6 Observatory, `http://www.ipv6observatory.eu`

5. National IPv6 Roadmap Policy version 2, http://www.dot.gov.in/ipv6 and National Telecom Policy 2012, http://www.dot.gov.in/ntp/NTP-06.06.2012-final.pdf
6. SENSEI European research project (Integrating the Physical with the Digital World of the Network of the Future), Pervasive and Trusted Network and Service Infrastructures: ICT-2007.1.1: The Network of the Future, Contract no. 215923, http://www.sensei-project.eu
7. Hobnet European research project, http://hobnet-project.eu
8. Internet of Things Architecture, IoT-A, http://www.iot-a.eu
9. IoT6 European research project, Deliverable D1.5: "IoT6 Reference Model", White Paper (2012), http://www.iot6.eu
10. FI-WARE Internet of Things (IoT) Services Enablement, http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_Internet_of_Things_(IoT)_Services_Enablement
11. ETSI M2M Communications, http://www.etsi.org/website/technologies/m2m.aspx
12. Jara, A.J., Martinez-Julia, P., Skarmeta, A.F.: Light-weight multicast DNS and DNS-SD (lmDNS-SD): IPv6-based resource and service discovery for the Web of Things. In: International Workshop on Extending Seamlessly to the Internet of Things (2012)
13. Jara, A.J., Zamora, M.A., Skarmeta, A.F.: GLoWBAL IP: an adaptive and transparent IPv6 integration in the Internet of Things. In: MobiWIS 2012, The 9th International Conference on Mobile Web Information Systems, Niagara Falls, Ontario, Canada, August 27-29 (2012)
14. Constrained Application Protocol (CoAP), draft-ietf-core-coap-11 (July 16, 2012), https://datatracker.ietf.org/doc/draft-ietf-core-coap/
15. Constrained RESTful Environments (CoRE), http://tools.ietf.org/wg/core
16. Kim, S.H., Im, J., Byun, J., Lee, K., Kim, D., Ziegler, S., Crettaz, C., KAIST, Mandat International: Initial IoT6 integrations have been validated with IoT-SaaS integration between Mandat International and RunMyProcess, and STIS integration with KAIST (October 2012)
17. Dunkels, A., Vasseur, J.: IP for Smart Objects, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper, N. 1, IPSO Alliance (2008)
18. Shelby, Z., Chauvenet, C.: The IPSO Application Framework, draft-ipso-app-framework-04, IPSO Alliance, Interop Committee (2012)
19. Tian, L.: Lightweight M2M (OMA LWM2M), OMA Device Management Working Group (OMA DM WG), Open Mobile Alliance - OMA (2012)
20. Shelby, Z., Hartke, K., Bormann, C., Frank, B.: Constrained Application Protocol (CoAP), Constrained Resources (CoRE) Working Group, Internet Engineering Task Force (IETF), work in progress, draft-ietf-core-coap-13 (2012)
21. Li, S.T., Hoebeke, J., Jara, A.J.: Conditional observe in CoAP, Constrained Resources (CoRE) Working Group, Internet Engineering Task Force (IETF), work in progress, draft-li-core-conditional-observe-03 (2012)
22. Shelby, Z.: Embedded web services. IEEE Wireless Communications 17(6), 52–57 (2010), doi:10.1109/MWC.2010.5675778
23. Sun, S., Lannom, L., Boesch, B.: RFC3650 - Handle System Overview. IETF Standards (2003)

24. Kastner, W., Neugschwandtner, G.: Data communications for distributed building automation. In: Embedded Systems Handbook, 2nd edn., vol. 2, pp. 29–34. CRC Press, Boca Raton (2009)
25. OPC Unified Architecture Specification, OPC Foundation (2009)
26. oBIX Version 1.1 Working Draft 06, OASIS (2010)
27. Addendum c to ANSI/ASHRAE Standard 135-2004, BACnet - A data communication protocol for building automation and control networks, American Society of Heating, Refrigerating and Air-Conditioning Engineers (2004)
28. Jung, M., Weidinger, J., Reinisch, C., Kastner, W., Crettaz, C., Olivieri, A., Bocchi, Y.: A transparent IPv6 multi-protocol gateway to integrate Building Automation Systems in the Internet of Things. In: Proceedings of the IEEE International Conference on Internet of Things (iThings 2012), Besancon, France (November 2012)
29. iCORE EU Project, `http://www.iot-icore.eu/`
30. BUTLER EU Project, `http://www.iot-butler.eu`