The Internet of Things through IPv6
Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 4 3 96
A.J. Jara, L. Ladid and A. Skarmeta

The Internet of Things through IPv6:

An Analysis of Challenges, Solutions and Opportunities

Antonio J. Jara[1], Latif Ladid[2], and Antonio Skarmeta[3]

[1] Vice-chair, IEEE ComSoc IoT ETC

University of Applied Sciences Western Switzerland (HES-SO)

Sierre, Vallais, Switzerland

jara@ieee.org

[2] Chair, IEEE ComSoc IoT ETC

IPv6 Forum and University of Luxembourg

Luxembourg

latif@ladid.lu

[3] Vice-chair, IEEE ComSoc IoT ETC

University of Murcia

Murcia, Spain

skarmeta@um.es

1/31/2014

Abstract

The public IPv4 address space managed by IANA (http://www.iana.org) has been completely depleted by Feb 1st, 2011. This creates by itself an interesting challenge when adding new things and enabling new services on the Internet. Without public IP addresses, the Internet of Things capabilities would be greatly reduced. Most discussions about IoT have been based on the illusionary assumption that the IP address space is an unlimited resource or it is even taken for granted that IP is like oxygen produced for free by nature. Hopefully, the next generation of Internet Protocol, also known as IPv6 brings a solution. In early 90s,

IPv6 was designed by the IETF IPng (Next Generation) Working Group and promoted by the same experts within the IPv6 Forum since 1999. Expanding the IPv4 protocol suite with larger address space and defining new capabilities restoring end to end connectivity, and end to end services, several IETF working groups have worked on many deployment scenarios with transition models to interact with IPv4 infrastructure and services. They have also enhanced a combination of features that were not tightly designed or scalable in IPv4, such as IP mobility and ad-hoc services, catering for the extreme scenario where IP becomes a commodity service enabling lowest cost networking deployment of large scale sensor networks, RFID, IP in the car, to any imaginable scenario where networking adds value to commodity. For that reason, IPv6 makes feasible the new conception of extending Internet to consumer devices, physical systems and any imaginable thing, that can be benefited of the connectivity. IPv6 spreads the addressing space in order to support all the emerging Internet-enabled devices. In addition, IPv6 has been designed to provide secure communications to users and mobility for all devices attached to the user; thereby users can always be connected. This work provides an overview of our experiences addressing the challenges in terms of connectivity, reliability, security and mobility of the Internet of Things through IPv6. This paper describes the key challenges, how they have been solved with IPv6, and finally presents the future works and vision that describe the roadmap of the Internet of Things in order to reach an interoperable, trustable, mobile, distributed, valuable, and powerful enabler for emerging applications such as Smarter Cities, Human Dynamics, Cyber-Physical Systems, Smart Grid, Green Networks, Intelligent Transport Systems, and ubiquitous healthcare.

Keywords: IPv6, Internet of Things (IoT), M2M, 6LoWPAN, GLoWBAL IPv6.

1 Introduction

The number of things that are connected to the Internet is growing exponentially. This has led to defining a new conception of Internet, the commonly called Internet of Things.

Internet of Things ecosystems are composed, on the one hand, of so called smart objects, i.e., tiny and highly constrained physical devices in terms of memory capacity, computation capability, energy autonomy, and communication capabilities. On the other hand, Internet of Things is made up of identification tags and codes that allow identifying a specific thing in a unique and global way.

Several technologies are enabling these types of things.

First, dealing with smart objects we can find technologies such as 6LoWPAN for Wireless Sensor Networks (IEEE 802.15.4), Bluetooth Low Energy (IEEE 802.15.1) for Wireless Personal Area Networks, WiFi Low Power (IEEE 802.11) for Wireless Local Area Networks, and finally Long Term Evolution â€“ Advanced (LTE-A) for machine to machine communications in Wide Area Networks.

Second, for the identification of things the most extended technologies are barcode for the simple identification of a resource (e.g., product identifier), Quick Response (QR) or matrix barcodes for the extended identification of a resource (e.g., plain text and Universal Resource Locators (URLs)), Radio Frequency Identification (RFID) for the digital identification of resources with capabilities for multiple resource identification, identification out of line of sight, and extended identification capability. Finally, Near Field Communication (NFC) for the digital identification of resources through personal devices such as smart phones, and the establishment of peer-to-peer (P2P) communications.

Finally, other existing Internet technologies and devices such as smart phones, tablets, laptops, industrial technologies, appliances, and building automation are also considered part of the Internet of Things.

This new conception of extending Internet to any relevant thing is feasible thanks to the new version of the Internet Protocol (IPv6). IPv6 spreads the addressing space in order to support all the emerging Internet-enabled devices.

IPv6 has been designed to provide secure communications to users and mobility for all devices attached to the user; thereby users can always be connected.

IPv6 features are what have made it possible to think about connecting all the objects and to build the Internet of Things.

The objective of the Internet of Things is the integration and unification of all communications systems that surround us. Hence, the systems can get a total control and access to the other systems in order to provide ubiquitous communication and computing with the purpose of defining a new generation of services.

IPv6 is considered the most suitable technology for the Internet of Things, since it offers scalability, flexibility, tested, extended, ubiquitous, open, and end-to-end connectivity.

For that reason, some efforts are being carried out to provide mechanisms for enabling an IPv6 address for each one of the things; ranging from identification tags and legacy technologies to the mentioned emerging technologies to build smart objects. Thereby, the integration of multi-technology networks in a common all-IP network is reached.

For the first nature of devices, i.e., identification tags, and legacy technologies from building automation and industrial control the IPv6 Addressing Proxy technology has been proposed, and for the second nature of devices, i.e., emerging technologies such as Bluetooth Low Energy and to offer a lightweight integration of IPv6 header for global communications an optimization of 6LoWPAN, denominated GLoWBAL IPv6 has been proposed.

Thereby, Internet of Things is moving towards a more ubiquitous and mobile Internet-powered ecosystem.

Once all the things are IPv6 addressable, we can consider that they are also empowered with all the IP protocols, i.e., protocol for mobility such as MIPv6 and security such as IPSec. However, it is not feasible for all the things and resources integrated into the Internet of Things ecosystems to be associated with protocols designed with the considerations of devices with higher capabilities.

Internet of Things devices, the so-called smart objects, are energy and resource constrained, host based protocols require most of the signalling on end nodes and because the design features of the Internet of Things networks were not considered in the design issues of the host based protocols. For example, considering a network with the technology 6LoWPAN over IEEE 802.15.4, a 6LoWPAN node may run out of energy causing a fault in the network, this has restriction in size packets and this presents aggressive techniques to conserve energy by using of sleep schedules with long sleep periods, they just wake up to receive IPv6 signalling messages, this feature introduces delays in the reception of messages because they are not attended until that the node wakes up. Therefore, these delays, power restrictions, and packet size restrictions are not considered in the current IPv6 protocols.

Nevertheless, Mobility management and security continue being required for the Internet of Things.

Mobility management is a desired feature for the emerging Internet of Things. Mobility-aware solutions increase the connectivity and enhance adaptability to changes of location and infrastructure. Internet of Things is enabling a new generation of dynamic ecosystems in environments such as smart cities and hospitals.

Dynamic ecosystems require ubiquitous access to Internet, seamless handover, flexible roaming policies, and an interoperable mobility protocol with the existing Internet infrastructure. These features are challenges for Internet of Things devices due to their constraints. The work presented in [1, 2] analysis of the requirements, desirable features, existing solutions and proposes, on the one hand, detection of movement direction for IEEE 802.15.4 radios to offer a fast handover, and on the other hand, an efficient solution for constrained environments compatible with IPv6-existing protocols, i.e., Mobile IPv6.

Both solutions present a proper performance and solution, but the solution based on Lightweight Mobile IPv6 needs to be highlighted, since one of the major considerations for the Internet of Things is to offer scalable and inter-domain solutions that are not limited to specific application domains or infrastructure.

The integration and interoperability with the existing infrastructure is one of main requirements for mobility management in dynamic ecosystems, since mobile nodes require the capability to use other networks during roaming. For that reason, it is important to offer a highly compatible solution with available access points, routers and networks.

IPv6-based solutions are key enablers for the success of the Internet of Things interoperability, acceptance and integration.

In addition to the mobility, security is a high requirement for the Internet of Things. This close relationship between the cybernetic and the physical world enabled by the Internet of Things carries with it vulnerabilities in terms of security and privacy. Since vulnerability is now not simply limited to the hardware of our computer. as well it is also able to reach our energy systems, physical access control systems, and even when we cross the street in a smart city.

For that reason, security and privacy are considered as one of the major issues for the Internet of Things. Security is already considered as a big issue in the current digital society, and several solutions and mechanism have been built. Therefore, part of the path is already paved, the major challenge now is how to extend these mechanisms to the Internet of Things devices, define new mechanisms more focused on identity and privacy, and the most important challenge, how to make them scalable and feasible for a future with billions of devices interconnected to Internet.

Security is also an inherent requirement for the mobility management, since this offers the capability to redirect traffic to a new address and claim the identity of a node. Therefore, mobility opens a high number of vulnerabilities for the man in the middle attacks, identity supplantation, and data integrity. In order to avoid these vulnerabilities, we require the authentication of the mobile node such as is carried out in Mobile IPv6 with the trust relationship between the mobile node and its home agent.

In our previous works have been designed, developed and evaluated a scalable secure protocol for IPv6, i.e., IPSec.

IPSec support was mandatory with IPv6, but since its complexity and use for very specific use cases such as virtual private networks, tunnelling protection, and related IPv6 protocols, it has been considered to make it optional.

Although IPSec is not considered mandatory much more for IPv6 hosts, it continues being useful and relevant for IPv6-related protocols such as MIPv6. In particular, IPSec used by the MIPv6 protocols, where IPSec is used to protect the communications between the mobile node and the home agent.

IPSec presents two challenges, first, the cryptosuite which is to be used, and second the overhead from the IPSec headers. For the first issues, an optimization of the Elliptic Curve Cryptography to offer a suitable asymmetric key cryptography for constrained devices is presented, regarding the overhead; a lightweight integration of IPSec is analyzed.

The described evolution from the Internet of Things towards a ubiquitous and mobile Internet is having influence in several application areas and market sectors.

Security is a major requirement in clinical environments, since the security vulnerabilities directly affect patient health and privacy. For example, first, a Deny of Service (DoS) attack could stop continuous vital sign monitoring of a critical patient, consequently in case of anomalies, there would be no alarm. Second, impersonation attack could reply false information from a patient, e.g. informing that he is not in danger when he is. Therefore, the need for security mechanisms is clear to prevent the attacks and to minimize the adverse effects of such attacks in the healthcare market.

Internet of Things is considered one of the major communication advances in recent years, since it offers the basis for the development of cooperative services and applications. Extensive research using this concept in different areas, such as building automation, Intelligent Transport Systems, and in particular for healthcare, is being carried out. For example, its potential for mobile health applications has been reported in [3, 4], showing its potential identification capacities for drug identification, and its communication capabilities in offering ubiquitous therapy by providing wireless and mobility capabilities for personal devices and smart objects, in addition to allowing the collection of data anytime and anywhere.

This work analyses the developed enablers to exploit the aforementioned Internet of Things capabilities in order to build a communication architecture that allows to exploit the IPv6 potential for the Internet of Things.

2 Why an Internet of Things?

The Internet of Things (IoT) [5], or Machine-to-Machine (M2M), is one of the main drivers for the evolution of the Internet towards the Future Internet.

Nowadays, sensors, actuators and devices (so-called things), are connected to the Internet through gateways and platforms such as Supervisory Control and Data Acquisition platforms (SCADAs), panels, and brokers. These gateways and platforms

break the end-to-end connection with the Internet. For that reason, this initial approach is defined as an Intranet of Things [6].

The Intranet is being extended to smart things [7] with a higher scalability, pervasiveness, and integration into the Internet Core. This extension is leading to reach a real IoT, where things are first class citizens in the Internet, and they do not need to relay any more on a gateway, middleware, proxy, or broker.

IoT requires both an architecture and products that allow for the extension of Internet technologies, in order to reach a Future Internet of Things, Services and People.

IoT drives towards integrating everything into the Internet Core, this trend is the denominated Internet of Things. The integration of everything is motivated by the market wish to have all processes remotely accessible through an uniform medium â€“ while at the same time understanding that re-engineering an infrastructure to allow this for each application independently would be prohibitively costly and time-consuming. Moreover, the current evolution from uniform mass markets, to personalized ones, where the customization and user-specified adaptation is a requirement, makes the sort of uniform infrastructure found in the Internet, imperative. This allows many components to be re-used, and services to be shared, with correspondingly huge economies of scale and shortened implementation times.

IoT fills the gap between the needs arising from the evolution of the market, information, users, and things, by moving all of them to a common framework, the Internet. This is different from the current approach in such applications, where they are based on stand-alone and monolithic solutions designed for a narrow or -*stovepiped*- application domain. Users now require more flexibility and freedom. Offering a common framework allows choice among the available manufacturers, suppliers, service providers, delivery options, and payment services. While this obviates the need for standalone or proprietary solutions, it also requires a high level of integration.

IoT allows communication among very heterogeneous devices connected via a very wide range of networks through the Internet infrastructure. IoT devices and resources are any kind of device connected to Internet, from existing devices, such as servers, laptops, and personal computers, to emerging devices such as smart phones, smart meters, sensors, identification readers, and appliances.

In addition to the physical devices, IoT is also enriched with the cybernetic resources and Web-based technologies. For that purpose, IoT is enabled with interfaces based on Web Services such as RESTFul architecture and the novel protocol for Constrained devices Applications Protocol (CoAP) [8]. These interfaces enable the seamless integration of the IoT resources with information systems, management systems, and the humans. Reaching thereby a universal and ubiquitous integration among human networks (i.e., society), appliance networks, sensor networks, machine networks, and, in definitive, everything networks.

Due to the above mentioned potential, IoT is receiving a lot of attention from the academia and industry sectors.

IoT offers several advantages and new capabilities for a wide range of application areas. For example, nowadays IoT is finding applications for the development of *Smart Cities*, starting with the *Smart Grid*, *Smart Lighting* and transport with new services such as *Smart Parking* and the *Bicycle Sharing System* [9] for building sustainable and efficiently smart ecosystems.

The application of the IoT is not limited to high scale deployments such as the locations in Smart Cities, elsewhere it can also be considered for consumer

electronics, vehicular communications, industrial control, building automation, logistic, retail, marketing, and healthcare.

3 Key challenges

IoT and ubiquitous integration of clinical environments define complex design challenges and requirements in order to reach a suitable technology maturity for its wide deployment and market integration. From the beginning, IoT devices present inherited challenges since they are constrained devices with low memory, processing, communication and energy capabilities.

The first key challenge for a ubiquitous deployment is the integration of multi-technology networks in a common all-IP network to ensure that the communication network is reliable and scalable. For this purpose, IoT relies on the connectivity and reliability for its communications on Future Internet architecture and the IPv6 protocol to cover the addressing and scalability requirements.

The second key challenge is to guarantee security, privacy, integrity of information and user confidentiality. The majority of the IoT applications need to take into considerations the support of mechanisms to carry out the authentication, authorization, access control, and key management. In addition, due to the reduced capabilities from the constrained devices enabled with Internet connectivity, a higher protection of the edge networks needs to be considered with respect to the global network.

The third key challenge is to offer support for the mobility, since the Future Internet presents a more ubiquitous and mobile Internet. Mobility support increases the applicability of Internet to new areas. The most present nowadays are mobile platforms such as smart phones and tablets which enable a tremendous range of applications based on ubiquitous location, context awareness, social networking, and interaction with the environment. Future Internet potential is not limited to mobile platforms, else IoT is another emerging area of the Future Internet, which is offering a high integration of the cybernetic and physical world. Therefore, since the physical world is mobile and dynamic, IoT will require support mobile and dynamic ecosystems.

Mobility support in the IoT enables a global and continuous connection of all the devices without requiring the disruption of the communication sessions. For example, mobility management in hospitals is required since clinical devices can be connected through wireless technologies. Mobility offers highly valuable features such as higher quality of experiences for the patients, since this allows the patients to move freely, continuous monitoring through portable/wearable sensors, extend the coverage within all the hospital, and finally a higher fault tolerance since the mobility management allows the connection to adapt dynamically to different access points. Therefore, clinical environment is one of the main scenarios where the mobility for the IoT-based applications exploit these capabilities, in terms of fault tolerance influences directly in the life support, and continuous monitoring influences the quantity of data available which is required for real-time diagnostic.

Finally, other challenges are also arising from the application, economical, and technological perspectives. For example, from an application point of view are the requirements for processing large amounts of data for a growing number of devices, it is the so-called *Big Data*. From the economic points of view, the needs to provide economies of scale, i.e., new services based on existing modules in order to leverage the related platform investment. From the networking point of view to offer an end-

to-end support for Quality of Service (QoS), since the different IoT applications will present different requirements in terms of latency and bandwidth, for example, for clinical environments the traffic should be prioritized over other non-critical traffic coming from smart-metering.

The Figure 1 describes the key challenges to offer an Internet of Things. This covers from the integration of heterogeneous devices to the integration into a Web of Things.

Figure 1: Key challenges to offer an Internet of Things.

The following subsections describe in more detail the current status of the challenges in terms of heterogeneity, connectivity/reliability, security and mobility.

Heterogeneity

IoT started focusing on building blocks such as Radio Frequency IDentification (RFID), due to its capabilities of identifying the uniqueness of an object in the world. After that initial approach, the technology evolved and the IoT was not much more a metaphor for RFID capabilities, else it was feasible that the devices such as sensors and appliances were connected to the IoT. Thereby, it was giving birth to smart things and smart objects concepts, as an evolution of the devices located at the Wireless Sensor Networks (WSN) with IPv6 connectivity through protocols such as the mentioned 6LoWPAN [10].

IoT market is developing new technologies such as WiFi Low Power, Bluetooth Low Energy, IEEE 802.15.4g, and Near Field Communications (NFC), which are the evolution of the initial RFID and WSN (IEEE 802.15.4) towards very well-known and interoperable technologies with the new generation of personal devices such as laptops, tablets and smart phones.

IoT deployments are not limited to RFID, WSN and the mentioned emerging technologies; the majority of the IoT scenarios and ecosystems are composed of heterogeneous IoT devices based on different technologies with different capabilities such as legacy building automation technologies (e.g., BACnet, Konnex, X10), industrial devices based on industrial protocols (e.g., Control Area Network (CAN), M-BUS, Wireless M-BUS), smart grid technologies (e.g., smart metering), and smart cities technologies (e.g., parking pots, street lights, environmental sensors).

For example, deployments in clinical environments cover multiple types of devices ranging from passive things to active things. An IoT-based clinical environment can be composed of the wheelchairs, drugs and instruments that are tagged with RFID passive tags, and also of active things such as patient monitors, clinical devices, appliances, and personal devices (e.g., laptops, smart phones, tablets).

In conclusion, since IoT ecosystems will be composed of a high range of technologies, a suitable support for the heterogeneity needs to be provided by the IoT communication architecture. The goals are firstly, to evaluate the capabilities of 6LoWPAN based on IEEE 802.15.4 for IoT applications and clinical environments. Second, to evaluate the capabilities of the IoT for emerging technologies such as NFC as an evolution of RFID, and Bluetooth Low Energy as an evolution of initial WSNs,

and finally, to develop a communication architecture that allows the integration of heterogeneous devices in a common environment.

Connectivity and reliability

The number of devices that are connected to the Internet is growing exponentially. This has led to defining a new conception of Internet, the commonly called Future Internet, which started with a new version of the Internet Protocol (IPv6) that extends the addressing space in order to support all the emerging Internet-enabled devices.

IPv6 is the fundamental technology for the IoT. It is estimated that several billion things will be connected by 2020. Unlike IPv4, IPv6 can address this number of objects. The IPv6 address space supports 2^{128} unique addresses (approximately $3.4*10^{38}$). Specifically, it can offer $1.7*10^{17}$ addresses on an area about the size of the tip of a pen. The advantages of the IPv6 integration in the IoT are not limited to a universal addressing space; its main advantages are to offer stable, scalable, extensive, and tested protocols for global end-to-end communication, device/service discovery, mobility, end-to-end security, and other relevant features such as stateless addressing auto-configuration, multicast addressing for group operations, and its flexibility for the application layer with technologies such as Web Services.

IPv6 has been designed to provide secure communications to users and all the devices attached to the them; thereby users are always connected.

IPv6 features are what have made possible thinking about connecting all the objects and build the IoT. The objective of IoT is the integration and unification of all communications systems that surround us. Hence, the systems can get a control and access total to the other systems for leading to provide ubiquitous communication and computing with the purpose of defining a new generation of services.

IoT is enabled by tiny and highly constrained devices, so-called smart objects. These devices have low-performance properties due to their constraints in terms of memory capacity, computation capability and energy autonomy. In addition, their communication capabilities present a low bandwidth, limited reachability because of the usage of hard duty cycles and consequently unstable connectivity for solution with a very low duty cycle and high power constraint.

These devices with constrained connectivity and communication capacity are what we can find, from some years ago, in the Low-power Wireless Personal Area Networks (LoWPANs).

The IETF working group has defined IPv6 over that LoWPANs (6LoWPAN) to extend Internet to smart devices [11]. 6LoWPAN offers the LoWPANs all the advantages from IP such as scalability, flexibility, well tested, extended, ubiquitous, open, and end-to-end connectivity.

It could be considered that 6LoWPAN devices are also empowered with IP protocols, i.e., protocol for mobility such as MIPv6, management such as SNMP, security such as IPSec, etc. However it is not feasible for 6LoWPAN devices to be associated with host-based protocols such as mobility, management, security etc. because 6LoWPAN nodes are energy and resource constrained. Host-based protocols require most of the signaling on end nodes and because the design features of 6LoWPAN network were not considered in the design issues of the host-based protocols. For example, a 6LoWPAN node may run out of energy causing a fault in the network. This has restrictions in size packets and presents aggressive techniques to conserve energy by using sleep schedules with long sleep periods, devices just

wake up to receive IPv6 signaling messages. This feature introduces delays in the reception of messages because they are not attended to until the node wakes up. Therefore, these delays, power restrictions, packet size restrictions etc. are not considered in the current IPv6 protocols.

The goal to solve the initial challenge for connectivity and reliability is to move toward the common addressing space of Internet (IPv6) to all the resources and devices available in an IoT ecosystem. In this manner, an Internet of Things can be reached.

Security

Security is a wide concept which covers everything from authenticity (ensuring that the end-user is who is claimed to be), authority (ensuring that the end-user is allowed to perform the requested action), integrity (the data received is exactly the same data transmitted), and confidentiality (communication is not understandable for intermediary users, even when an intruder is in the network). These concepts are satisfied through a set of protocols, algorithms and cryptographic primitives.

The IoT security has been one of the most discussed and yet pending issues, even after of the existence of protocols for IPv6 network security such as IPSec, and for datagrams (i.e., UDP or CoAP) such as DTLS. Security for the IoT is not excessively extended and deployed because of the difficulties in configuring (IPSec) for end users and the lack of scalable certificate management for DTLS. Consequently, the majority of the Internet traffic continues being transmitted in plain text, i.e., unprotected.

For that reason, one of the initial actions in order to carry out an effective deployment of autonomous and unassisted IoT deployments that satisfies the scalability and self-management requirements from the IoT is the development of protocols for authentication and key management.

Specifically, on the one hand, the protocol for the authentication and key management at the network layer such as the Protocol for Carrying Authentication for Network Access (PANA) [12] is being considered by the research institutions and also industrial alliances, such as the ZigBee Alliance for their ZigBee IP stack [13].

On the other hand, the IPSec set of protocols (i.e., Internet Key Exchange (IKE) and Encapsulation Security Protocol (ESP)), and another protocols at the medium access layer such as 802.1x, are also being considered. All of these share the usage of the Extensible Authentication Protocol (EAP) to transport the security credentials.

Therefore, the challenge is not limited to the protocol, else the EAP scheme needs to be optimized in terms of a proper support of the required cryptographic primitives by the constrained device, i.e., symmetric cryptography algorithm to protect the packet, hash function to ensure the integrity and authenticate of the packet, and finally asymmetric cryptographic algorithm to carry out the key exchange and initial authentication.

Some initial works for the IoT have been proposed for IPSec [14], where several pending problems have been found, since for example a low version of the symmetric cryptography with 32-bit keys is used, such as AES-CBC-32, which are very weak. In addition, this relies on pre-shared keys for IPsec, which is not very scalable. Therefore, it does not solve the scalability and self-management requirements.

In order to satisfy these requirements, a Key Management Protocol (KMP) can be considered, that allows keys to be refreshed periodically (therefore maintaining acceptable security levels). Specifically, an automatic key exchange mechanism is

required; thereby, each node can keep track of the security associations (SA) that specify how a particular IP flow should be treated in terms of security.

The most extended KMP is IKE. A very simple approach of IKE has been defined in [15], which does not satisfy all the requirements and functionality for a full SA establishment.

Other issues from IPSec is that the overhead caused by a IPsec packet (the extra bytes on the IP header) can force the packet to be fragmented (the link layer payload that includes the extra IPsec bytes becomes bigger than the maximum size of a 802.15.4 packet), thus an extra packet must be sent to the link layer and the energy/network overhead will become bigger. In addition, this overhead problem is worse with the ESP mode of IPSec, since the internal headers of IPv6 and UDP are encrypted and consequently cannot be compressed.

In addition to IPSec, the majority of works from the CORE Working Group in IETF are focused on the integration of security through the transport layer security solutions such as DTLS for CoAP. DTLS is the default security for CoAP.

A pre-shared key mode (PSK) is also considered by CoAP, with the aforementioned problems regarding the lack of scalability for this pre-establishment of the security credentials.

CoAP also offers a very interesting approach based on RawPublicKey, i.e., a solution based on the use of an asymmetric key pair, but without an X.509 certificate metadata. This approach is highly relevant since it can manage the identity issues mentioned in the introduction section, in order to verify the authenticity of the device and its link with the manufacturer. For example, the Certification Authority (CA) of the public key can also indicate the list of identities of the nodes, with which it can communicate. It can thereby indicate the entities which are trustworthy in the initial verification and bootstrapping phase.

CoAP also considers certificates, i.e., X.509 certificate that binds it to its Authority Name and is signed by some common trust root, e.g., the manufacturer.

In order to optimize DTLS for smart objects, DTLS 1.2 [16] offers the schemes to re-use the cryptographic hardware support by the majority of the IEEE 802.15.4 transceivers for the symmetric cryptography, i.e., AES CCM. In addition, considers the usage of Elliptic Curve Cryptography (ECC) for the asymmetric cryptography. Thereby, making it more suitable for these constrained devices.

Nowadays, DTLS is being considered by the Smart Energy profile for ZigBee alliance (SE 2.0), and it is also being considered as an adaptation of DTLS 1.2 in the IPSO Alliance based on the subset allowed by RFC6347.

In addition to the solutions presented, there is security support over the current Internet architecture based on IPv6 in the network layer and UDP/TCP for the transport layer, where the security is based on IPSec for IPv6 and DTLS/TLS for UDP/TCP respectively. Also two solutions from the IETF to support the ID/Locator split have been defined. The first, HIP, has been developed by the Host Identity Protocol (HIP) Working Group, a group mainly focused on improving security of the Future Internet, and the HIP Diet EXchange (HIP DEX) [17], which has been optimized for constrained environments such as the Internet of Things. HIP offers in a single mechanism the capabilities for authentication and establishment of the communication.

Therefore, the goals to solve for the security support are, first, to optimize cryptographic primitives for the described protocols. Specially, ECC for the asymmetric cryptography. Second, to analyze and evaluate the impact of IP security

protocol (IPSec) for constrained devices. Finally, to analyze the possibilities for novel protocols that satisfies the scalability and self-management requirements.

Mobility

Mobility presents several challenges for the efficiency of networks and protocols, since mobility protocols have to deal with inherent characteristics of IoT such as hard duty cycles (i.e., long sleep period), reduced energy and processing capabilities, and constrained bandwidth.

Mobility management is composed of two fundamental phases, on the one hand, the movement detection in order to be aware of the device changing its location and consequently will require linking to an alternative network, on the other hand, the signaling and control messages required to be aware of changing locations, (i.e., network and locator), to the networks and clients relative to the device in movement.

Movement detection is solved through active scan, passive overhearing of messages from other protocols, or specific signaling from the mobility protocol.

Mobility signaling is being solved in different ways mainly split into two trends, on the one hand, a trend based on an evolutionary research following the IPv6-based approach and current Internet architecture, and on the other hand, a clean-slate, where new architectures are proposed that require major changes in the existing protocols and networking philosophy.

The clean-slate trend is based on new concepts such as ID/Locator split architectures such as those presented in LISP [18], developed by the Locator ID Separation Group (LISP) Working Group which is focused on improving the scalability of the routing for the Future Internet, and HIMALIS presented in [19].

HIMALIS architecture offers lightweight mobility management based on the ID/Locator split concept. The ID/Locator split architecture employs two different values, one for identification (*ID*) and another for location (*Locator*). Therefore, the device changes its Locator in the network layer when the device changes its position in the network topology. The most relevant aspect of this split is that the Locator changes without requiring upper layers to change the ID, thereby ensuring that established communication sessions associated with the ID are not interrupted by mobility.

These kinds of architectures present the advantage that mobility is directly supported by the separation of the session identification with the locator of the device, which is the problem of the current Internet architecture. Previous works for the IoT have been focused on this approach, the main issue is that the overhead for 6LoWPAN devices is increased since there is the need to transport one additional header for the identification layer. These types of solutions are very relevant from the research point of view, but they present the main inconvenience of not being feasible, since the current hardware and infrastructure deployed is not ready for this kind of approach.

For that reason, the other trend is the evolutionary research approach; this follows the current Internet architecture for the management of the identification and location, i.e., IPv6 continues being used for *Identification* of the session in the transport and application layers, and *Locator* of the devices for routing in the network layer. These solutions allow continuing using the existing infrastructure and overcome the problem using a similar concept to the ID/Locator split but in an implicit way. Specifically, the main protocol following the evolutionary approach is Mobile IPv6 (MIPv6). MIPv6 uses two IPv6 addresses, fist, the initial address of the device, commonly

denominated Home Address is used as identifier, and second, the new address in the visited network, commonly called care-of address, is used as locator.

MIPv6 protocol provides the signaling messages and IPv6 header extensions to manage the binding between these two addresses. In addition, this defines the security mechanisms and networking requirements in order to avoid the identity supplantation and man-in-the-middle attacks.

The main concerns of MIPv6 is that it presents a high overhead for the data packets when the mobile node is in roaming, since this needs to include the destination option to specify its Home Address in case of applied route optimization or build an IPv6 tunnel which requires an additional IPv6 header. Both cases require a high overhead.

The second problem with Mobile IPv6 is that IPSec is mandatory in order to protect the communications between the mobile node and the home agent. Such as mentioned, the trust relationship between the mobile node and the home agent is a fundamental requirement of MIPv6, since all the security of the binding update for the mapping between the care-of address and home address, and additional security processes such as the return routability for the route optimization are based on this trust relationship.

Therefore, the goals for the mobility support are, first, to design new techniques for fast movement detection. Second, to design and evaluate a lightweight implementation of MIPv6 to offer a secure and efficient mobility management for the IoT.

4 IPv6-based solutions

The described challenges, in terms of connectivity, reliability, security, and mobility, can be addressed through IPv6 solutions. Specifically, the Figure 2 presents the technologies considered to satisfy the previously challenges through the IPv6-based technologies.

Figure 2: Key challenges to offer an Internet of Things.

4.1 Connectivity and reliability

The bases of the Internet of Things is provide connectivity and reliability.

In order to satisfy these requirements, the interconnection framework has relied on Internet technology, in particular IPv6. Since, IPv6 is the main enabler for extending the Internet of Things to the Future Internet.

The work presented in [20] presents how the architecture has been powered by the IPv6 connectivity in order to provide an homogeneous, scalable, and interoperable medium for integrating heterogeneous devices built on technologies such as 6LoWPAN, Bluetooth Low Energy, legacy devices and identification technologies.

In more detail, our works have proposed two novel solutions to enable ubiquitous connectivity and reliability, on the one hand, GLoWBAL IPv6 presented in [21], and on the other the IPv6 Addressing Proxy for legacy technologies presented in the Chapter [22, 23].

GLoWBAL IPv6 has been proposed to optimize global addressing involving smart devices such as that found in low power wireless personal area networks (LoWPAN). GLoWBAL IPv6 has the further advantage of providing efficient addressing and integration to both IEEE 802.15.4 sensor devices, which do not offer native support for 6LoWPAN, and also to other technologies which do not support IPv6 communication capability into their stacks.

GLoWBAL IPv6 defines an Access Address/Identifier (AAID) to reduce the overhead from the network and transport headers. AAID simplifies IPv6 and UDP communication parameters (source and destination addresses/ports, originally 36 bytes long) to a single 4-byte communication identifier augmented by one byte for the *Dispatch* header, totaling 5 bytes for the GLoWBAL IPv6 header. Thus, the IPv6/UDP headers are significantly reduced. This mechanism achieves an efficient frame format for global communications in networks that do not have native support for IPv6.

An example of its potential is described. Let take a heterogeneous device with a Bluetooth Low Energy interface, such as a smart phone with also Internet connectivity through the cellular network interface. GLoWBAL IPv6 fills the IPv6 addressing requirement for any smart thing connected to the smart phones through the Bluetooth Low Energy network by acting as the mapping protocol between the Local Network (capillary network) and the wide-area network (cellular network) using appropriately constructed IPv6 addresses. , Consequently this smart phone can efficiently enable with IPv6 through GLoWBAL IPv6 to the smart things connected through its Bluetooth Low Energy interface. But, GLoWBAL IPv6 is not a suitable solution for all devices that need to be enabled IPv6, since all the devices do not offer programming capabilities such as a smart phone or a gateway. Examples of these devices can be found in the inherited legacy technologies from the industrial and building automation markets. These markets present a rather fragmented set of technologies. Each technology comes with a set of fit-for-purpose sensors and their respective application environments which lack efficient interoperability among them. Some associations of manufactures have been formed to build common technology frameworks, e.g., Konnex (KNX) for building automation. While such *de facto* standards present widespread adoption to date, this does not discourage use of other relevant protocols such as the emerging ZigBee and the older X10. Due to this fragmentation, the support of this heterogeneity in order to shift towards a common access and communication framework based on IPv6 is also considered.

For that reason, an additional solution has been proposed to embrace all existing native addressing schemes. This solution has defined IPv6 mappings for each native addressing scheme by use of an IPv6 Addressing Proxy which handles the translations between an IPv6 address and its corresponding technology addressing, i.e. the native addressing depends on the technology.

IPv6 Addressing Proxy provides a transparent mechanism for the users and devices to map the different addressing spaces from each legacy technology to a common IPv6 addressing space. Specifically, the IPv6 addressing proxy is a technology-dependent mechanism for mapping each device to the different sub-networks built under the IPv6 prefix addresses provided by the Internet Service Provider. The IPv6 addressing proxy enables IPv6 addressing to all the devices regardless of the device technology thus offering a scalable and homogeneous solution to interact with devices which do not support IPv6 addressing. The IPv6 addressing proxy has been implemented in a multi-protocol card, and its performance,

scalability and interoperability through a protocol built over IPv6 has been evaluated successfully.

4.2 Scalable security and mobility

First, IPv6 supports connectivity and reliability with the heterogeneous resources thanks to the presented interconnection framework and the IPv6 features. Then, the communication architecture is required to offer higher communication capabilities such as security and mobility. For that reason, the next goal has been to support scalable security and mobility.

Mobile IPv6 (MIPv6) is the protocol founded on IPv6 to support mobility. MIPv6 uses two IPv6 addresses, the initial address of the device, denominated Home Address, as identifier (ID), and the new address in the visited network, denominated care-of address, as Locator.

MIPv6 protocol provides the signaling messages and IPv6 header extensions to manage the binding between these two addresses. In addition, this defines the security mechanisms and networking requirements in order to avoid the identity replacement and man-in-the-middle attacks.

The feasibility of MIPv6 for constrained devices such as that considered for the IoT was initially analyzed in the work presented in [1]. These works concluded that MIPv6 presents a high overhead for the data packets when the mobile node is in roaming, since this needs to include the destination option to specify its home address in case of route optimization applied or build an IPv6 tunnel which requires an additional IPv6 header.

In addition, IPSec is analyzed in [24, 25], as IPSec is mandatory for MIPv6 in order to ensure the trust relationship between the mobile node and the home agent. This communication protection between the mobile node and the home agent is a fundamental requirement of MIPv6, since all the security of the binding update for the mapping between the care-of address and home address, and additional security processes such as the return routability for the route optimization are based on this trust relationship.

IPSec presents the difficulty that encapsulates an IPv6 packet inside another. The problem with this encapsulation is that the inner header cannot be compressed and optimized. Therefore, the overhead coming from the inner header (40 bytes) cannot be waived. For that reason, the works carried out in [24, 25], analyzes the impact of MIPv6 with IPSec over 6LoWPAN networks and the conclusion is that the unique way to offer an interoperable integration of the mobility with MIPv6 is without route optimization and using IPSec only for tunneling/encapsulation. Consequently the inner header can also be compressed. However, this approach presents security vulnerabilities in the case that the application layer is not secure. For that reason, this work also analyzes the suitability of IPSec ESP to provide security to the encapsulated packet in order to avoid any security vulnerabilities.

4.3 Application protocol

During the last few years the promoters of the IoT, from academia and industry, have been focused on empowering these constrained devices with the protocols and functions of Internet-enabled devices.

The initial steps, the constrained capabilities of the IoT devices and differences between IPv6 design issues, have led to develop lightweight versions of the existing

protocols. These lightweight versions have the advantage that they continue being interoperable/translatable to the full implementations. For example, a lightweight implementation of the IP stack such as uIP [26] and header compression through the 6LoWPAN protocol [27] have been developed in order to reach Internet connectivity. In addition, as a generic and wide supported application protocol, Web Services through RESTFul architecture have also been adapted for the IoT devices with lightweight and compressed protocols such as the Constrained Application Protocol (CoAP) [8, 28]. CoAP is an equivalent to HTTP but considers the constraint issues of the IoT devices, with the capability to be mapped to HTTP and offer at least an equivalent potential, for some scenarios it is even able to offer higher capabilities, since it has been designed with the IoT-related scenarios and requirements in mind.

IPv6 and WebServices offer the primitives to build application protocols for different use cases, as the final purpose of the communication architecture is its usage and exploitation for different applications and use cases. However, this requires definition on top of CoAP/IPv6 a description of the resources from the different application and used cases. For this purpose, application profiles and guidelines such as the Open Mobile Alliance Lightweight Device Management for M2M (OMA LWM2M) [29] in the context of the oneM2M for cellular networks, and IPSO Application Guidelines [30] for capillary networks are being defined.

5 Future works and vision

This work has described the key components to reach the evolution of connectivity, reliability, support for heterogeneity, security and mobility.

This section describes the ongoing and future works to continue enhancing the potential of the IoT and its application in eHealth/mHealth and emerging areas such as Smart Cities.

5.1 Towards an interoperable Internet of Things

The evolution of the IoT in order to build interoperable ecosystems is yet in progress.

The first goal of the IoT has been to offer interconnectivity to everything, i.e. connect things to the Internet. Once connectivity is achieved we need to cope with heterogeneity and enable a seamless interoperability among the different entities. For this purpose, the existing heterogeneous islands of devices have been focused on moving towards IPv6. Specifically, this integration at the connectivity level is reached with solutions such as 6LoWPAN [27], and the contributions from our previous experiences such as GLoWBAL IPv6 and the IPv6 Addressing Proxies.

After connectivity is reached, then a common protocol for the transport and application layer is required. The most extended application in the Internet is the World Wide Web, and consequently the data transfer protocol designed for the Web, i.e., the Hypertext Transport Protocol (HTTP). The capabilities of offering an homogeneous application protocol in HTTP have been squeezed by the Web Services during the last decade. Nowadays, technologies such as Hypertext Markup Language (HTML), for the representation of resources, and JavaScript, for building logic and intelligence, are making its potential even greater. For example, HTML5 and JavaScript enable everyday desktop applications over the Web, at the same time, providing a road on which to interoperate and exchange information among different applications. For that reason, the next step in the IoT had been to connect things to the Web, thereby conceiving the so-called Web of Things.

The new protocols such as Constrained Application Protocol (CoAP) and other lightweight versions of HTTP make interaction with resources from constrained devices through Web clients such as browsers, feasible. This Web-based interaction offers to the Internet of Things the simplicity and flexibility that the Web offers nowadays.

The Web of Things is allowing different things and systems to interact together. As a result, it composes more complex services and solutions. These interactions are enabled through the definition of application programming interfaces (API) over HTTP or CoAP protocol. Consequently, the applications give leverage to the HTTP protocol in order to provide the interface for publishing data updates into the system, for retrieving data updates from the system, and in general, exchange of information.

The data can be encoded with different envelopes, semantics and metadata. For example, the data can be encapsulated in plain text, over complex structures such as XML/EXI or simpler but yet organized structures such as JSON. In addition, they can be represented with different format and units, and finally they can offer additional information.

The current market of the IoT is focused on deployments that are connected vertically, i.e. stovepiped, to the specific sensors and applications for which they have been designed in order to address specific requirements and target a specific use case. However, the IoT requires horizontal integration of multiple capabilities and resources towards a larger ecosystem.

Therefore, IoT is not only a vehicle for communication, but also is about integration and interoperability, and to this end, semantic is the major driver.

The challenge after the Web of Things, is to build a Semantic Web of Things (SWoT) in order to ensure a common understanding as a result of which resources would be able to cooperate, be shared, linked, and combined in order to build complex services with higher intelligence and context aware. Thus, the Internet of Things will provide added value to the existing and emerging markets, which would exploit the huge potential of everything connected being controllable and providing continuously (i.e. every time) data from everywhere.

The SWoT is, on the one hand, the fusion of the trends of the IoT for moving towards Web technologies with protocols such as CoAP, REST architecture and the Web of Things concept, and on the other hand, the evolution of the Web with the Semantic Web technologies.

SWoT promises a seamless extension to the IoT allowing integration of both the physical and digital worlds. SWoT is focused on providing wide scale interoperability that allows the sharing and re-use of these things. Consequently, the use cases and markets of the IoT will not be held back to vertical solutions or pre-established use cases. In fact, these deployed infrastructures and available data can target other secondary markets and use cases, since the data that they are collecting and managing can be of importance in providing data analysis (aggregated, anonymity, processed information, e.g. for Smart City administration). They provide a major understanding of the primary markets, since they can be contrasted and extended with the available third party data.

Therefore, the challenges to move from the IoT/WoT towards the SWoT are several, some of these are to define a common description that callow data to be universally understandable create extensible annotations, i.e. from minimal semantic descriptions towards more elaborate ones, and agree on a catalogue of semantic descriptions.

These challenges can be addressed only in an ideal ecosystem, since several products will develop unique features that will be out of the scope of the existing standards and each manufacturer is associated with a different standard organization, and the standards landscape related to M2M is very large. Nowadays in numbers, the Global Standards Collaboration Machine-Machine Task Force (GSC MSTF) identifies 143 organizations with a direct or indirect interest in M2M standardization [31].

The ongoing work looks into the convergence of the emerging standards, of the capillary and cellular networks, towards an interoperable IoT ecosystem.

First, the standards considered for cellular networks have been initialized by the European side with the ETSI M2M and extended globally with the oneM2M initiative, which is already offering the OMA Lightweight Device Management Protocol.

Second, the standards considered for capillary networks are supported by organizations such as the Internet Engineering Task Force with solutions such as CoAP, which is supported by industry alliances such as IPSO Alliance, with the IPSO OMA Web Objects Application Guidelines. The capillary networks present major heterogeneity and other standards for offering a lightweight reliable messaging transport protocol for the IoT such as the Message Queuing Telemetry Transport (MQTT) protocol. This protocol is optimized to connect physical world devices and events with enterprise servers and other consumers supported by OASIS and Eclipse Foundation [32], and other private standards such as the ZigBee-IP solution for Smart Energy (SE 2.0) supported by the ZigBee Alliance [13].

Other activities and projects are the W3C with the SSN-XG ontology for offering a semantic layer for the IoT, the European Research Cluster on the Internet of Things (IERC), and its projects such as OpenIoT, IoT.est, and SPITFIRE where the capabilities of RDF, OWL and classic semantic technologies for the IoT have been explored.

Since the current environment regarding semantic is quite fuzzy, the future work requires reaching a more homogeneous and clear standards ecosystem, where the manufacturers and vendors can determine what to apply to where in the different IoT use cases.

5.2 Towards a distributed trust and security

The future work should be focused on solutions to carry out IoT/M2M trust verification, through a mechanism such as capabilities-based access control [33, 34]. Consequently, novel scenarios based on temporal access to resources can be defined. For example, a house proprietor with an access control solution (e.g. a smart door lock) is able to offer temporal access to his neighbour so as to go everyday at anytime from 15:00 to 18:00 in order to feed the pets and irrigate the plants.

The mechanisms required to offer secure solutions that make usage of the IoT capabilities feasible during usual human activities and behaviors, where devices and physical resources are involved, needs to be enhanced. As a result, these new mechanisms and solutions will facilitate the introduction of the IoT as part of the Internet-powered society.

The communications between IoT-devices and humans present two different ways to be satisfied, the first, an integration of the required communication technologies and capabilities in personal devices such as Smart Phones. Following this approach, the potential of WiFi Low Power, Bluetooth Low Energy, and Near Field

Communication could be exploited. Thus, the smart object can talk with the personal device through the same medium technologies, i.e. WiFi Low Power, Bluetooth Low Energy, etc. However this approach presents high requirements such as compatibility in the medium technology between the personal device and the smart object. Consequently it is limiting the availability and success of these solutions.

For that reason, the other approach is the exploitation of the common and abstracted communication medium with IP technology. In this case, the personal device and the objects can be connected to the Internet through any communication interface, and communication between them is based on the end-to-end feature of the IP technology. As a result, it is not required that the smart object and the personal device use similar technology to establish the communication.

These distributed security scenarios, based on both IP abstracted technology and direct interaction, are being explored with the techniques such as the capability-based token mentioned.

5.3 Towards a ubiquitous and mobile Internet of Things

IoT and M2M are being enabled and developed from the capillary and the cellular points of view. Until now, mobile IoT for the capillary networks with the lightweight Mobile IPv6 protocol has been explored.

However, a mobile IoT based on cellular networks to also provide ubiquitous access and mobility between different networks can also be defined.

The mobile IoT based on capillary networks present challenges in terms of the availability of coverage in a wide scale, and the lack of agreements among different network access providers involved.

For that reason, the IoT based on cellular networks perspective is also gaining attention, since this provides a wider range of coverage, and homogeneous technology worldwide (regulated by the 3GPP Alliance). In particular, the last version of the Long Term Evolution-Advanced (LTE-A) standard defines how to integrate IoT/M2M devices.

The inconvenience of the cellular networks continue to be the requirement of a subscription (i.e. dependence with a network access provide), higher power consumption, and higher costs.

For that reason, mobility protocols with vertical handoff among different technologies, i.e. between capillary and cellular networks need to be explored, in order to provide the best trade-off in terms of communication costs, availability and reliability.

These kind of signaling protocols between cellular and capillary networks are becoming a reality, thanks to the convergence of both with the Open Mobile Alliance (OMA) Lightweight Device Management Protocol (LWM2M).

Therefore, a set of objects for the mobility-related signaling can be defined, which can be supported by the solutions promoted from the cellular vendors and manufacturers (i.e. oneM2M Alliance), and from the capillary vendors and manufacturers (i.e. IPSO Alliance).

5.4 Towards a valuable Internet of Things

Finally, the major challenge for the Internet of Things is to demonstrate its value to the end-customers.

The potential of the end-to-end connectivity and convergence with the Internet and Web protocols are providing, from the developing and engineering perspective, highly valuable advantages.

Some of these advantages are the reduction of costs for the development of solutions thanks to the re-usage of existing technologies; major interoperability thanks to common communications technology; major control and monitoring capabilities; a major number of possibilities to compose services based on cybernetic and physical resources, and major flexibility.

However, even when this list of advantages could be considered sufficient motivation to justify the value of the IoT, it continues to not be enough from the consumers perspective, since none of them are directly related to perceptible values by the end user.

All of them provide big opportunities to develop and offer a solution that can breakthrough the market. However, the killer solutions or applications based on the IoT, which demonstrate to the consumers the potential of the IoT, are yet to come.

In my opinion, the two trends to build this value powered by the IoT potential can be based on an evolve approach, or in a totally novel value proposal.

Regarding the evolve approach, the IoT can offer the same solutions that nowadays are being offered by existing technologies but with major simplicity for usage, interaction and understanding. For example, current industrial automation solutions (e.g., SCADA) are featured by a complex set-up process, where a set of skills and training is required. The potential of the IoT is to set-up these physical devices through more understandable platforms such as smart phones, remotely through Internet-based solutions, and even automatic configuration based on the smart capabilities of smart objects to come. For example, some of their smart capabilities are the potential to discover other devices, exchange messages with control and monitoring systems, and set-up automatically a big part of the conventionally required parameters.

An example of this approach is what our ongoing work is offering with the developed Smart Driver for lighting in Smart Cities. The Smart Driver is featured by being a power supplier with Internet connectivity and processing capabilities. These new two features offer the potential to set-up current, voltage, and logic scheduling directly from any IP-enabled device without requiring the set-up with specific and complex solutions, while the device is connected to a proprietary software or device.

The other approach is to offer a novel value proposal, which is inspired in the potential of the data. One of the advantages of this new capability to connect with everything is the potential capability to collect data from everything in a major frequency on a temporary basis. Consequently, this data with proper data mining, a.k.a. Big Data tools, will offer solutions that were not feasible before.

For instance, following the example of street lighting, the data gathered from each street light is not limited to the control of the street light, it can also offer additional data from humidity, temperature, nose, quality of air, motion, etc. Thus, novel solutions such as noisy maps and pollution maps can be built to evaluate the quality in the different zones before renting or buying a house.

In addition to the sensors that can been integrated in the Smart Driver itself, these Smart Objects present endless possibilities, since they can be also seen as the infrastructure to connect and communicate to any device.

Therefore, the integration of the Internet and IoT-related capabilities in a street light that initially could be motivated to optimize power consumption, simplify the set-up, and enable the remote and monitoring platforms, is also converted into a big

opportunity to build a nerve for the rest of the devices. This nerve can provide connectivity to the parking pots, citizens' devices, cars, gardens, and in short, any of the entities that are part of the city ecosystem.

The smart lighting solution described for smart cities pursue the goal of offering major power consumption reduction, and a major awareness about air and acoustical pollution in order to carry out the proper actions to enhance sustainability.

Another example based on eHealth/mHealth is the interconnection among different devices. For example, for patients with diabetes type 1, devices for Continuous Glucose Monitoring (GCM) and also insulin pumps to provide the insulin therapy are provided nowadays.

These devices are starting to be able to interact between each other, but without any action, only to show the data to the user, due to the lack of intelligence in both them.

IoT enables the insulin pump and the GCM to interact with intelligence devices such as a smart phone, swatch, and even with a backend system deployed in the cloud that can offer a calculus of the insulin therapy based on the patient's health record, evolution, and in short Big Data from the patient. Consequently, the loop between monitoring, therapy and user can be closed in a smarter and simpler way, and consequently avoid that the user needs to introduce manually the insulin dosage in the insulin pump multiple times per day.

These mHealth-based solutions pursue the goal of offering to patients with chronic diseases a major level of freedom with respect to their illness, and quality of life. All these new interaction models, knowledge, and improvement of the existing solutions are some of the ways that we can start building and probing the value of the IoT. In short, the IoT is another enabler to continue improving both quality of life and experiences, and planet sustainability.

6 Conclusions

IoT defines the basis to reach a ubiquitous and mobile integration of the clinical environments with support for large scale connectivity from different physiological sensors, integration with information systems, and its homogeneous access through Internet and Web technologies from consumer devices such as tablets, smart phones, and laptops.

This paper has presented the contributions carried out to move from a conceptual IoT to a real one through the potential of IPv6 technology.

The communication architecture for the Internet of Things is composed of the key components to enable security, mobility, and end-to-end connectivity/reliability.

For the integration of everything, it needs to be considered all the rage of IoT technologies, such as 6LoWPAN (IEEE 802.15.4), Bluetooth Low Energy (IEEE 802.15.1) and Near Field Communication (NFC).

These technologies require protocols such as GLoWBAL IPv6 and the IPv6 Addressing Proxy, for the inclusion of all the resources and devices available in the IoT ecosystem to the common addressing space from Internet (IPv6). Thereby, an Internet of Things can be reached.

In addition to the support of the addressing, IPv6 also offers the possibility to provide a scalable security and mobility.

For this purpose, the protocols Mobile IPv6 (MIPv6) for mobility, and IP Security (IPSec) for security have been defined, but both protocols have required a lightweight

version of MIPv6 with support to IPSec in order to make it suitable for the IoT ecosystems.

In definitive, the conclusion is that smart phones, personal data terminals, and other mobile computing devices are still far from what a future IoT will require to connect services, people, and things. But, full IPv6 integration is the first step towards this destination. As next steps one envisages support for mobility, multi-homing, discovery techniques, and management solutions in order to make things more autonomous and to enable a communications era based on the ***Future Internet of Things, Services and People***.

Acknowledgments

This research was conducted during the PhD Thesis of Antonio J. Jara in the Intelligent Systems and Networks group, of the University of Murcia, Espinardo, Spain, awarded for its excellence as a research group in the frame of the Spanish "Plan de Ciencia y Tecnología de la Región de Murcia" from the "Fundación Séneca" (04552/GERM/06). The authors would like to thank the European Project "Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling heterogeneous components interoperability (IoT6)" from the FP7 with the grant agreement no: 288445, and the Spanish ministry, for education, social politics and sport, for sponsoring this research activity with the grant FPU program (AP2009-3981).

References

url@samestyle

[1] A. Jara, R. M. Silva, J. Silva, M. Zamora, and A. Skarmeta, "Mobile IPv6 over Wireless Sensor Networks (6LoWPAN) Issues and feasibility," in *Proc. of the 7th European Conference on Wireless Sensor Networks (EWSN'10), Coimbra, Portugal*, February 2010.

[2] A. J. Jara, R. Silva, J. S. Silva, M. A. Zamora, and A. F. Skarmeta, "Mobile IP-based Protocol for Wireless Personal Area Networks in Critical Environments," *Wireless Personal Communications*, vol. 61, no. 4, pp. 711–737, 2011.

[3] A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, "Interconnection Framework for mHealth and Remote Monitoring Based on the Internet of Things," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 47–65, 2013.

[4] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, "An initial approach to support mobility in hospital wireless sensor networks based on 6lowpan (hwsn6)," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 1, no. 2/3, pp. 107–122, 2010.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[6] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's INTRAnet of things to a future INTERnet of things: a wireless-and mobility-related view," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 44–51, 2010.

[7] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, January 2010.

[8] Z. Shelby, K. Hartke, and C. Bormann, "Constrained application protocol (CoAP)," IETF Internet-draft (work in progress), March 2013, http://tools.ietf.org/html/draft-ietf-core-coap-14.
[9] J. FroehlichJon, J. Neumann, and N. Oliver, "Measuring the pulse of the city through shared bicycle programs," *Proc. of the 2008 International Workshop on Urban, Community, and Social Applications of Networked Sensing Systems (UrbanSense'08), Raleigh, North Carolina, USA*, pp. 16–20, November 2008.
[10] J. Vasseur, C. P. Bertrand, F. Watteco, B. Aboussouan, V. Marketing, G. E. Gnoske, A. K. Pister *et al.*, "A survey of several low power Link layers for IP Smart Objects," http://www.ipso-alliance.org/wp-content/media/low\s\do5(p)ower\s\do5(l)ink\s\do5(l)ayer.pdf, June 2010, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #6.
[11] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*. plus 0.5em minus 0.4emWiley, 2009.
[12] R. Marin-Lopez, F. Pereniguez-Garcia, A. F. Gomez-Skarmeta, and Y. Ohba, "Network access security for the internet: protocol for carrying authentication for network access," *IEEE Communications Magazine*, vol. 50, no. 3, pp. 84–92, 2012.
[13] D. Sturek, "ZigBee IP stack overview," 2009, zigBee Alliance.
[14] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Thingsâ€"a comparison of link-layer security and IPsec for 6LoWPAN (Online First, DOI: 10.1002/sec.406)," *Security and Communication Networks*, 2012.
[15] S. Raza, T. Voigt, and V. Jutvik, "Lightweight IKEv2: A Key Management Solution for both the Compressed IPsec and the IEEE 802.15. 4 Security," in *Proc. of the 2012 IETF Workshop on Smart Object Security, Paris, France*, March 2012.
[16] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," IETF RFC 6347, January 2012, http://www.ietf.org/rfc/rfc6347.txt.
[17] P. Nie, J. Vähä-Herttua, T. Aura, and A. Gurtov, "Performance analysis of HIP diet exchange for WSN security establishment," in *Proc. of the 7th ACM symposium on QoS and Security for Wireless and Mobile Betworks (Q2SWinet'11), Miami, Florida, USA*. plus 0.5em minus 0.4emACM, October-November 2011, pp. 51–56.
[18] D. Farinacci, D. Lewis, D. Meyer, and V. Fuller, "The Locator/ID Separation Protocol (LISP)," IETF RFC 6830, January 2013, http://www.ietf.org/rfc/rfc6830.txt.
[19] V. P. Kafle and M. Inoue, "HIMALIS: Heterogeneity inclusion and mobility adaptation through locator id separation in new generation network," *IEICE Transactions on Communications*, vol. 93, no. 3, pp. 478–489, 2010.
[20] A. J. Jara, S. Varakliotis, A. F. Skarmeta, and P. Kirstein, "Extending the Internet of Things to the Future Internet through IPv6 support (Online First, DOI: 10.3233/MIS-130169)," *Mobile Information Systems*, http://iospress.metapress.com/content/WGJ522G068321467.
[21] A. J. Jara, M. A. Zamora, and A. Skarmeta, "Glowbal IP: An adaptive and transparent IPv6 integration in the Internet of Things," *Mobile Information Systems*, vol. 8, no. 3, pp. 177–197, 2012.
[22] A. J. Jara, P. Moreno, A. Skarmeta, S. Varakliotisy, and P. Kirstein, "IPv6 addressing proxy: Mapping native addressing from legacy

communication technologies and protocols to IPv6 and the Internet of Things," in *Proc. of the 3rd International Conference on the Internet of Things (IoT'12), Wuxi, China*, October 2012, pp. 1–6.
[23] ------, "IPv6 addressing Proxy: Mapping native addressing from legacy technologies and devices to the Internet of Things (IPv6)," *Sensors*, vol. 13, no. 5, pp. 6687–6712, May 2013.
[24] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, "Lightweight MIPv6 with IPSec support (Online First, DOI: 10.3233/MIS-130171)," *Mobile Information Systems*, http://iospress.metapress.com/content/N82J053850436262.
[25] ------, "Lightweight mobile ipv6: A mobility protocol for enabling transparent ipv6 mobility in the internet of things," *Globecom 2013, Atlanta*.
[26] A. Dunkels, "uIP-A free small TCP/IP stack," 2002, http://www.sics.se/adam/uip.
[27] J. Hui and P. Thubert, "Compression format for IPv6 datagrams over IEEE 802.15.4-based networks," IETF RFC 6282, September 2011, http://www.ietf.org/rfc/rfc6282.txt.
[28] M. Castro, A. J. Jara, and A. Skarmeta, "Architecture for improving terrestrial logistics based on the web of things," *Sensors*, vol. 12, no. 5, pp. 6538–6575, 2012.
[29] N. Chu, D. Raouf, B. Corlay, M. Ammari, N. Gligoric, S. Krco, N. Ognjanovic, and A. Obradovic, "OMA DM v1. x compliant Lightweight Device Management for Constrained M2M devices," http://openmobilealliance.org/about-oma/ work-program/m2m-enablers/, 2013.
[30] Z. Shelby and C. Chauvenet, "The IPSO Application Framework," IPSO Draft: draft-ipso-app-framework-04 (work in progress), August 2012, http://www.ipso-alliance.org/wp-content/media/draft-ipso-app-framework-04.pdf.
[31] GSC MSTF, "Preliminary list of global organizations, groups, assoications, fora, and other entities with a direct or indirect interest in M2M standardization," 2011, http://www.gsc16.ca/english/documents/openplenary/GSC16-PLEN-42a1r1.xlsx.
[32] E. G. Davis, A. Calveras, and I. Demirkol, "Improving Packet Delivery Performance of Publish/Subscribe Protocols in Wireless Sensor Networks," *Sensors*, vol. 13, no. 1, pp. 648–680, 2013.
[33] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Mathematical and Computer Modelling*, vol. 58, no. 5/6, pp. 1189–1205, 2013.
[34] J. L. Hernandez-Ramos, A. J. Jara, L. MarÄ±n, and A. F. Skarmeta, "Distributed Capability-based Access Control for the Internet of Things," *Journal of Internet Services and Information Security (JISIS)*, vol. 3, no. 3/4, November 2013.

[Sorry. Ignored `\begin{biography} ... \end{biography}`]

[Sorry. Ignored `\begin{biography} ... \end{biography}`]

[Sorry. Ignored `\begin{biography} ... \end{biography}`]