The Internet of Things through IPv6:
An Analysis of Challenges, Solutions and Opportunities

by Antonio J. Jara, Latif Ladid and Antonio Skarmeta. An extract from their research project IoT6

Latif Ladid, IPv6 Forum President

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 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.

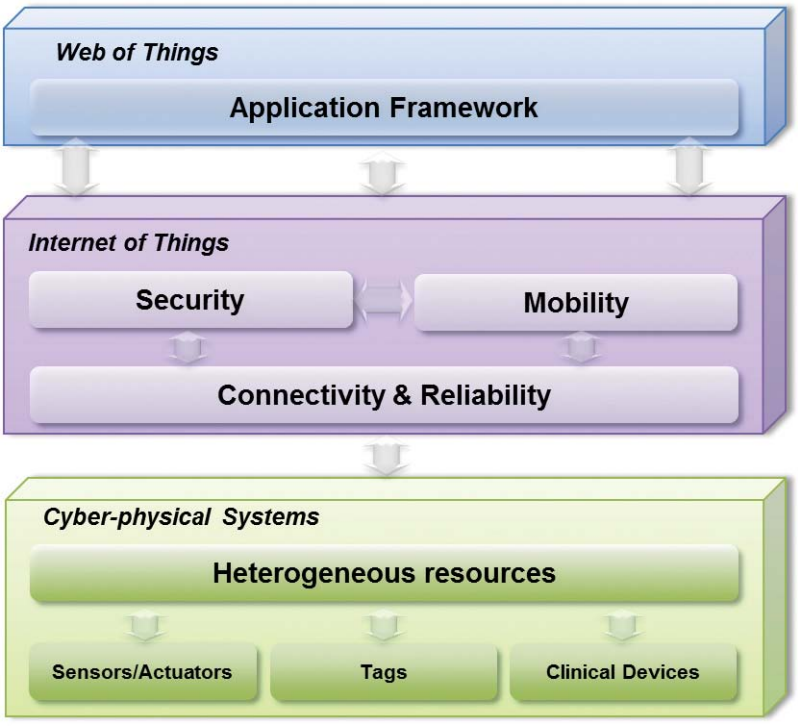
Once all the things are IPv6 addressable, we can consider that they are also empowered with all the IP protocols, i.e., protocol for mobility such as MIPv6 and security such as IPSec. However, it is not feasible for all the things and resources integrated into the Internet of Things ecosystems to be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

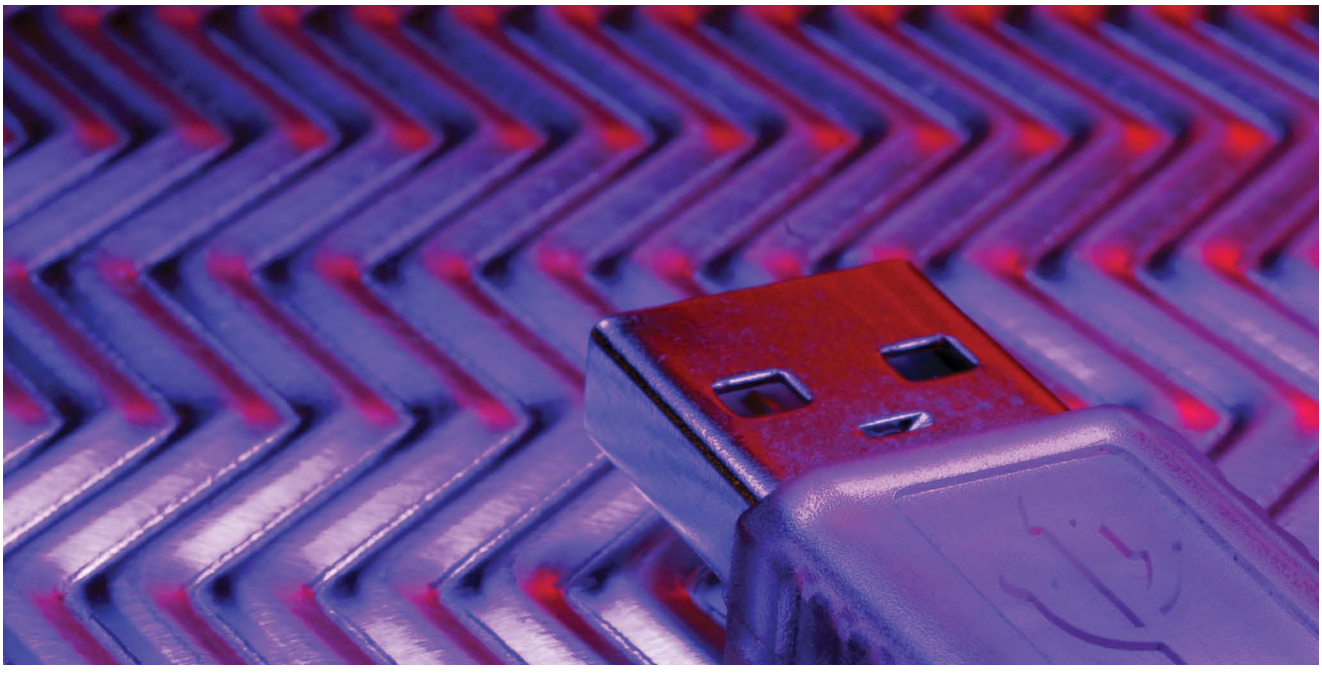
Security is also an inherent requirement for the mobility management, since this offers the capability to redirect traffic to a new address and claim the identity of a node. Therefore, mobility opens a high number of vulnerabilities for the man in the middle attacks, identity supplantation, and data 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.

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.

Authors: Antonio J. Jara: Vice-chair, IEEE ComSoc IoT ETC, University of Applied Sciences Western Switzerland (HES-SO), Sierre, Vallais, Switzerland, **jara@ieee.org**
Latif Ladid: Chair, IEEE ComSoc IoT ETC, IPv6 Forum and University of Luxembourg, Luxembourg, **latif@ladid.lu**
Antonio Skarmeta: Vice-chair, IEEE ComSoc IoT ETC, University of Murcia, Murcia, Spain **skarmeta@um.es**

For more information visit:
www.iot6.eu