Internet of Thing and Networks' Management : LNMP , SNMP , COMAN protocols

Hanane Lamaazi[1] , Nabil Benamar[1] , Antonio Jara[2] ,Latif Ladid[3] and Driss El Ouadghiri[1]
[1]University Moulay Ismail, Faculty of Science, Meknes
Meknes, Morocco
{Lamaazi.hanane; benamar73; dmelouad}@gmail.com
[2]University of Applied Sciences Western Switzerland (HES-SO)
Sierre, Vallais, Switzerland
anjejava@gmail.com
[3]IPv6 Forum and University of Luxembourg
Luxembourg
latif@ladid.lu

***Abstract*— Internet of Things (IoT) has attracted the attention of many researchers around the world given the improvement it brings to our daily lives in many areas such as health, environment, industry and the military. The main goal of this new technology is to make different devices communicating without the intervention of human both in data collection, service discovery, management and transfer of information. Of this it necessitates the use of systems, services and above all dedicated protocols, it does not involve creating new protocols but also to adapt or convert existing protocols to respond to its needs with the least loss. Furthermore, IPv6 technology is considered the most appropriate technology for the Internet of things, moving towards to its implementation on all devices because of its flexibility, scalability, mobility and security. However, there still some concerns in IoT that need more and deep research such as management problem for WSN and 6LoWPAN management protocols: LNMP, SNMP, and COMAN. In this paper, after introducing the concept of WSNs and 6LoWPAN, we have detailed network management systems designed for the IoT. Protocols, architecture and requirements were also analyzed.**

Index Terms: MANNA, management architecture, sensor network management, SNMP, management architecture, LNMP.

I. INTRODUCTION

Nowadays many devices that are connected to the Internet, and with the development of internet, the number continues to grow, which has led to the emancipation of a new paradigm, called internet of the future [1]. Hence the need for public addresses is an obligation to apply this new web design or so called Internet of Things (IoT). According to IANA 2 February 2011) [2], the blocks of IPv4 addresses are fully saturated, making it difficult to add new devices to the internet. So the application of a new version of IPv4 which is IPv6 has become indispensable. [3] This new version of IPv6 extends the address space so that it can support all devices that go to a connection via internet and then build the so-called internet of Things (IoT) [1]. IoT is based on intelligent devices which are very low performances constrain in terms of memory capacity, connectivity and communication is what we find in Low-Power Wireless Personal Area Networks (LoWPAN). To extend these smart devices on the Internet, the IETF has defined Pv6 LoWPAN (6LoWPAN). [1]
This definition (6LoWPAN) has inherited all of the LoWPAN the IP advantage, scalability, ubiquity, flexibility, etc. 6LoWPAN devices can also be associated with IP protocols, i.e., the mobility protocol such as MIPv6, and management such as SNMP, and security such as IPsec. [1]
Thanks to several IoT concept of smart object have seen birth, which represents an increase of device located in Wireless sensor networks (WSN) via protocols such as 6LoWPAN and IPv6 connectivity. [3] Such networks (WSN) also has great challenges in the internet world, considering its applications in various field such as military detection, emergency medical care, industry etc. [4]
Given the differences between the problems of design for IPv6 and low capacity devices for the IoT, Low power implementations of the IP stack has been developed, such as uIP, the compression header through the 6LoWPAN protocol to ensure Internet connectivity, as web services through an architecture based on protocols as Low Power and compressed such as CoAP (constrained Application Protocol), COMAN (the management of constrained networks and devices) and SNMP (Simple Network Management Protocol) . [1] Without forgetting LNMP protocol (LoWPAN Network Management Protocol) for 6LoWPAN based on Wireless sensor networks (WSN) [5]. In this article we will be focused solely on network management protocols because it is a major problem for current networks, taking into account their complexity.
Our paper is structured as follows: In Section 2, we present WSN and operation. Then in Section 3, we define the 6LoWPAN protocol and we will discuss the architecture of network management wireless sensor that will make the idea of section 4, in section 5 we proposed a discussion and we end with a conclusion that will make our section 6.

II. WIRELESS SENSOR NETWORKS

Wireless Sensor networks were born in military applications to detect the locations of the enemy and determine the combat zones to study them, with all these WSN applications is not limited to this area, it has spread to other larger such as environmental monitoring, industry and health and who posed

major challenges in terms of security, signal acquisition and coverage of communication [6]. The WSN is not only constrained to this domain, it also has a very important application is biofeedback, this application has to monitor health parameters (heartbeat, temperature….) by placing a sensor on the human body or through clothing [6], and it is perfectly the same principle of the IoT and M2M, since the communication is between the sensor and a receiver that requires the use of a connection for access remotely.

The wireless sensor networks (WSN) consist of the smart sensor nodes and base stations. These nodes serve to collect information from different backgrounds, such as ecosystems and battlefields, etc... And thereafter broadcast the information to one or more base station. The base stations act as a gateway between the nodes detection and the end-user. The applications of wireless sensor networks consider a network as a distributed system consisting of multiple sensor nodes and which operates autonomously. These applications are classified according to operational use, there are applications of data collection prompt sensor nodes to make the data to the base station periodically and event-applications require that the nodes send their data when an interesting event occurs. [7]

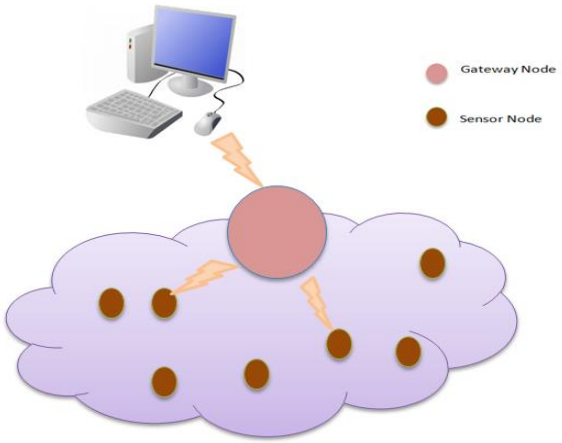

Figure 1. Sensor Wireless Architecture [8]

III. 6LoWPAN

The 6LoWPAN allows encapsulation and header compression for IPv6 datagrams. And that is what has made possible the integration of IPv6 in so-called smart objects, which is based on sensor networks. [9]

6LoWPAN characteristics have to be the defined as IPv6 networks and also as wireless sensor networks that contain a large number of nodes in limited ways. The 6LoWPAN is different from traditional behavior of IP and little work as a data-centric network. 6LoWPAN management requires restoration management needs for huge networks of large size and limited resources while providing IPv6 support. [5]

Current research IETF 6LoWPAN concerns the application of IPv6 on IEEE802.15.4 standard [10]. The lower layer 6LoWPAN adopts PHY (physical layer) and the standard IEEE802 .15.4. This standard allows the sending and receiving of the IPv6 packet size of 127 bytes and only a maximum data rate of 250 kbps [5]. The main market objectives 6LoWPAN is the wireless sensor networks (WSN) and the choice of the IPv6 for 6LoWPAN is to use as a networking technology. [10]

One of the objectives of the 6LoWPAN protocol is to find a solution to interconnect equipment LowPower to the Internet especially WSN via IPv6, why a 6LoWPAN architecture was proposed containing a 6LoWPAN gateway is a door to the outside and to enable communication between IPv6 clients and sensor nodes as it sends the data to a web server that allows to publish on the internet, also in the IPv6 layer, the 6LoWPAN gateway allows conversion between the IPv6 user and 6LoWPAN Devices [10].

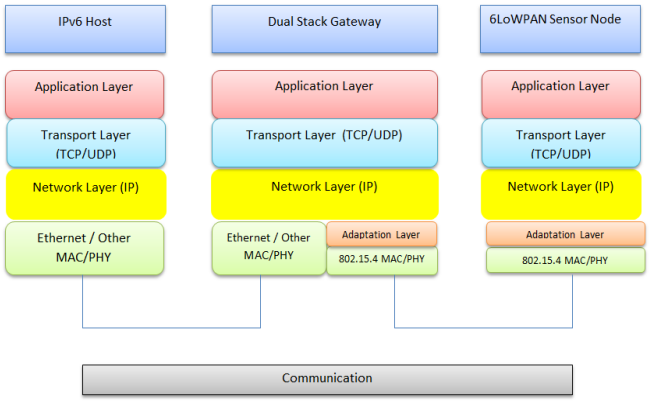

Figure 2: 6LoWPAN Gateway Structure

For new technologies, management is an important tool for any development, as for wireless sensor networks, the 6LoWPAN management is essential for verification of the availability of resources, operations, administration, etc.. And it also aims to use the Simple Network Management Protocol (SNMP) in these networks, which will allow it to reuse existing management tools [5].

IV. NETWORK MANAGEMENT SYSTEMS

Given the complexity of modern networks and large increases they know and the number of connected devices; control and management of these networks have become an indispensable necessity.

A. Sensor Network Management Framework

1. MANNA

MANNA (architecture management sensor) is based on a management policy that allows gathering dynamic information management system and performs functions and management services based on WSN models that keep the information about

the state of network. MANNA in several management function compose what is called a service management function example: connectivity discovery, discovery of nodes localization, surveillance coverage, etc. ... before performing a management service must know the type of information obtained from the WSN models. In addition MANNA adapts the behavior of WSN, but delays in WSN and uncertainties can affect the accuracy of the collected information management. [7].

B. Sensor Network Management Protocols

1. LNMP

LNMP (LoWPAN Network Management Protocol) is the combination of two architectures that enable the management of networks LoWPAN an operational architecture and other informational [5].

1.1 operational architecture

In the operational architecture, an entity 6LoWPAN performs the operation management in two stages: [5]

- Network discovery and device detection
- The actual management of available devices

- Network discovery

The large deployment of wireless sensor networks makes it difficult to manually discover "living" devices, why in the operating mode used in automatic discovery, this task network discovery is distributed through the 6LoWPAN and the coordinator is has delegated the task of discovering devices, which offers reduced cost of communication [5]. Here are the 3 levels defined by the operational architecture

A. End devices

Devices FFD (Full Function Devices) or RFD (Reduced Function Devices) [11], located behind the coordinator responding to the question of the coordinator during the verification of statements of devices. [5]

B. Coordinators

A coordinator is responsible for maintaining the state information of all the devices; it populates the list of devices notification, and the state table devices sending states, it allows the questioning of devices in the absence of state information of one of the device, and when a new connection from a terminal with the coordinator it adds the entry to the table [5].

C. Gateway

Well as coordinators tables are kept at the entrance. the status information received from the report coordinator these are filtered by gateway and implemented as an IP address and filled in the table states - that contains all IP addresses of devices available on the network - in its management information base (MIB), setting available via SNMP.

- Device Monitoring

Concerning requests for monitoring device status in 6LoWPAN, it is desirable that supports SNMP.
One of the objectives of 6LoWPAN networks is the implementation of SNMP protocol to be able to reuse all the existing management tools. The problem is that the maximum packet size of the physical layer is 127 bytes which means that SNMP can not be transported in 6LoWPAN networks because it is very cumbersome of point of view complexity and communication [5].
Between the context of local management and SNMP, the 6LoWPAN gateway acts as a proxy, as SNMP is supported only on the IPv6 network side. And on the 6LoWPAN gateway transported packets are converted to and from SNMP have a simplified format. The packet exchange is done as follows, each arrival request of NMS (Network Management System), the SNMP query is translated to a UDP request containing an ID and even when the gateway receives the response, and it is converted to SNMP size [5].

1.2 Informational Architecture

In addition to the objectives of reuse protocol such as SNMP, it is also important to support the Management Information Base (MIB) for 6LoWPANs networks, today many efforts aim to define the MIB for each layer to optimize 6LoWPAN perspective reuse and adaptability. [5]

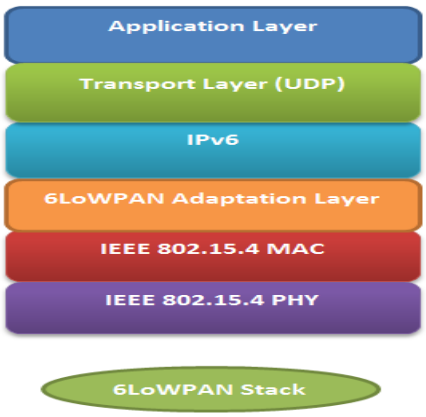

Figure 3: 6LoWPAN network stack

2. SNMP

Simple Network Management Protocol (SNMP) is a management protocol that was designed for TCP / IP networks. Series of RFC (Request for Comment) describes the SNMP protocol, it specifies and organizes information that is exchanged between the management and managed systems [8].
Management model based on SNMP consists of two essential element management system and an element management for the management system is composed of a Manager and database management, the system provides an interface with the human manager and for element management it consists of an agent, database management and a managed devices, this management component provides an interface with the management system and the managed device, as we shall see in the following figure. [12]

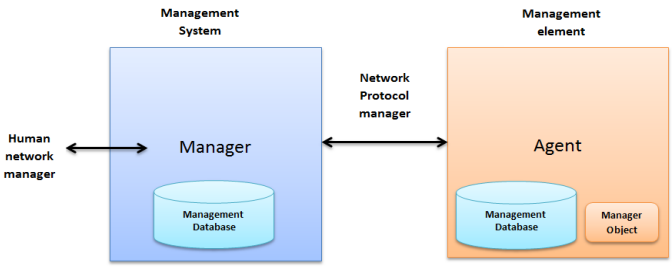

Figure 4. Management Model for SNMP[11]

3. COMAN

In this section we will give an idea of the scope of application and work in COMAN, there are several candidates for COMAN technologies, we will be limited on OMA-LwM2M; CoAP, we will descrire below.[13]

A. OMA-LwM2M

To enable activation and management of services M2M between the server LwM2M and LwM2M client, OMA Lightweight M2M aims to provide an agnostic protocol sub-layer adjacent. Currently a first version of catalyst is specified, there is provided a compact and lightweight protocol for devices and can forced, meet various requirements management. [13]
There are several overlapping OMA-LwM2M with COMAN requirements, we will quote a few:

- monitoring the energy states and appliances
- Logging
- authentication on the system and peripheral management
- controls access to the system and peripheral management

Good coordination between COMAN and OMA-LwM2M is recommended because it provides these chauvechement [13].

B. CoAP

The IETF has defined a binary protocol, easy to analyze and specially designed to constrained devices, which is the Constrained Application Protocol (CoAP), it used with lower-level protocols, but it is particularly adapted over the IPv6 and UDP also several projects have been made, the CoAP: [13]

- Allows use of all classes of devices seen its low complexity
- Designed to keep the server stateless
- Allows detection devices that its online with a simple ping CoAP.....

CoAP can meet several requirements COMAN: [13]

- Capability discovery
- Group-based provisioning
- Support for lossy links and unreachable devices
- Support of energy-optimized communication protocols

V. DISCUSSION

In this paper our work was to analyze different research in the field of the Internet of Things (IoT). This analysis is intended to be a simplification of the results and give a global vision of the IoT, its use, design, and requirements.
First we gave the idea on the implementation of the concept of the Internet of Things in wireless sensor networks and 6LoWPAN networks, as the adaptation of devices that allow the application of IoT beings present in all areas of life, with IPv6, as it has been confirmed in [6] [10].
Also it was shown that, given the complexity of these networks and constrains their use, it requires management to facilitate their use and implementation and results supported by its [9] [5] [10]. We have also presented different management protocols such as SNMP and LNMP and discussed their suitability with regards to the needs of the IoT, how they fit the structure of IPv6 [5].
Finally, we put the focus on a new protocol called COMAN, which is based on the response of candidate technologies such as CoAP and OMA-LwM2M, which has its own requirements and in turn, it responds to the needs of M2M and IoT, as it has been proven in [13].

VI. CONCLUSION

In this Article we presented the Internet of Things as a technology that includes other technology such as, the wireless sensor networks, the 6LoWPAN, as we presented how to control and manage a WSN with MANNA architecture (architecture management sensor networks), functioning and adaptation to sensor networks.
Given the complexity of networks of IoT and her constrained use, the challenges was to define protocols for managing networks of application of IoT as LNMP, SNMP, COMAN, for ease of deployment, which also allow respond the requirement of IoT and above all that can be applied with IPv6

protocol, in order to benefit from all its advantages, such as: security, mobility, flexibility and scalability, and it is also one of the challenges of IoT which aims to have all communication in IP.

REFERENCES

[1] Antonio J. Jara , David Fernandez, Pablo Lopez, Miguel A. Zamora and Antonio F. Skarmeta Clinical Technology Lab (CLITech), Research Institute for Oriented Information and Communications Technologies, Computer Sciences Faculty, University of Murcia, Regional Campus of International Excellence Campus Mare Nostrum, Murcia, Spain " Lightweight MIPv6 with IPSec support ,A mobility protocol for enabling transparent IPv6 mobility in the Internet of Things with support to the security, "

[2] http://www.zdnet.fr/actualites/ipv4-stock-d-adresses-epuise-dans-deux-jours-39757886.htm

[3] Antonio J. Jara1 , Latif Ladid2, and Antonio Skarmeta "The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities"

[4] Shangwei Duan and Xiaobu Yuan , School of Computer Science, University of Windsor, Canada "Exploring Hierarchy Architecture for Wireless Sensor Networks Managementé"

[5] Hamid Mukhtar, Kim Kang-Myo, Shafique Ahmad Chaudhry, Ali Hammad "LNMP- Management Architecture for IPv6 based lowpower Wireless Personal Area Networks (6LoWPAN)"

[6] Paulo Alexandre Correia da Silva Neves, Joel José Puga Coelho Rodrigues, « Internet Protocol over Wireless Sensor Networks, from Myth to Reality » , JOURNAL OF COMMUNICATIONS, VOL. 5, NO. 3, MARCH 2010

[7] Winnie Louis Lee , Amitava Datta , and Rachel Cardell-Oliver School of Computer Science & Software Engineering The University of Western Australia, "Network Management in Wireless Sensor Networks"

[8] Yi-Wei Ma 1, Jiann-Liang Chen 2, Yueh-Min Huang 1,3,* and Mei-Yu Lee 4 , " An Efficient Management System for Wireless Sensor Networks" Sensors 2010, 10, 11400-11413; doi:10.3390/s101211400

[9] Antonio J. Jara1, Socrates Varakliotis2, Antonio F. Skarmeta1, Peter Kirstein2 ," Extending the Internet of Things to the Future Internet through IPv6 support"

[10] Tariq ECH-CHAITAMI, Radouane MRABET, Hassan BERBIA "Interoperability of LoWPANs Based on the IEEE802.15.4 Standard through IPV6" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011

[11] http://fr.wikipedia.org

[12] IBM, AS/400 "Simple Network Management Protocol (SNMP) Support ",Version4,(https://publib.boulder.ibm.com/iseries/v5r2/ic2924/books/c4154120.pdf)

[13] http://www.ietf.org/id/draft-greevenbosch-coman-candidate-tech-03.txt