American Journal of Mobile Systems, Applications and Services
Vol. 2, No. 1, 2016, pp. 13-31
http://www.aiscience.org/journal/ajmsas

Survey of the IEEE 802.15.4 Standard's Developments for Wireless Sensor Networking

Kalliopi Pantelaki*, Spyridon Panagiotakis, Andreas Vlissidis

Department of Informatics Engineering, Technological Educational Institute of Crete, Heraklion, Crete, Greece

Abstract

The concept of Internet of Things (IoT) has been grown rapidly in recent years. In IoT it is necessary to find ways that each node of such networks can be connected directly to the internet, with or without the intervention of a Gateway. From this point of view, the Wireless Sensor Networks keep a critical role in this technology. Due to that, appropriate standards have been created offering interoperable communication towards the Internet to power constrained devices, with most popular the family of the 802.15.4protocols. This paper surveys the current status of these standards and envisions their evolution towards a converged TCP/IP-based solution.

Keywords

802.15.4 Standard, ZigBee Protocol, 6LoWPAN Protocol, ZigBee IP Protocol, Smart Energy Profile 2.0 (SEP) Standard, Constrained Application Protocol (CoAP), ZigBee 3.0 Protocol

Received: September 16, 2015 / Accepted: October 21, 2015 / published online: January 11, 2016

1. Introduction

In addition to the great development of the Internet we all experience in our daily lives, recently also occurs the great development of Wireless Sensor Networks (WSN). Such a network is composed of many small computing nodes, inexpensive, with limited memory and processing power that do not consume much energy and have wireless communication capabilities.

Such networks are used, for example, to monitor and control residencies, offices, factories, to manage them remotely and/or collect data for environmental conditions. WSNs interconnected with the Internet can be accessed from anywhere. This is what is called Internet of Things (IoT). The use of the TCP/IP stack in these sensor networks seems at first to be an attractive idea, due to the capabilities and popularity the IP protocol provides. However, the TCP/IP suite has specifications that cannot fit into such networks of constrained devices. For example, its Network Layer is very complex and requires a lot of power resources. Also, the IP-based wireless networks have high data transmission speeds and apply at distances far greater than those WSN need. Thus, new protocols were developed to meet the new requirements from WSN networks.

At first, the 802.15.4 standard, developed by IEEE, specifies the Physical (PHY) and Media Access Control (MAC) layers for such Wireless, short-range Personal Area Networks (WPANs), leaving the upper layers to be developed according to the market needs. On top of 802.15.4, a plethora of protocols have been developed for the specification of its upper layers, with ZigBee, by ZigBee Alliance, and 6LoWPAN, by IETF, to be the most popular among them. The later includes the required mechanisms for the introduction of TCP/IP in WSNs enabling native interoperability of nodes with the Internet without proxies.

The purpose of this paper is to survey the new protocols used in wireless sensor networking. So, at first, the PHY and MAC layers of the 802.15.4 protocol are introduced. Then, we present the ZigBee and 6LoWPAN protocols, which express two completely different approaches built on top of 802.15.4.

* Corresponding author
E-mail address: ppopi25@yahoo.com (K. Pantelaki)

Finally, we pay attention on the ZigBee IP and the ZigBee Smart Energy 2.0 protocols, which attempt to harmonize the ZigBee with the Internet world, similar to the 6LoWPAN's approach. Some more protocol developments on top of 802.15.4, mainly for industrial use, are also described. To the best of our knowledge, this is the first survey paper that collects such information.

Wireless Sensor Networks

The wireless sensor networks are one of the most important technologies in 21st century. In a few years, sensors will be everywhere, in our houses, in the animals, even in the human body.

A wireless sensor network contains a large number of sensors that communicate wirelessly one to each other in order to exchange information or publish data to the internet. The sensors organize themselves in ad hoc manner.

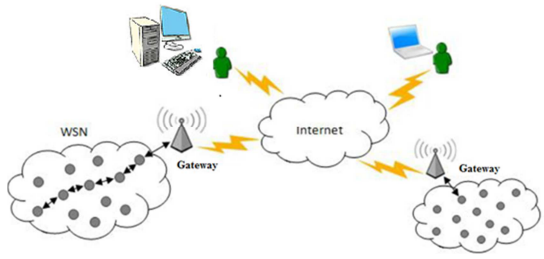

Figure 1. Wireless Sensor Networks.

If the users of the Internet want to obtain data from the corresponding sensor network they have to connect to the gateways. Then, the gateway translates Internet protocols into sensor protocols and relays the requests to the sensors in its network. The gateway then receives the answers from the relevant sensors by means of the proprietary sensor protocols and sends back the appropriate reply to the user using Internet protocols. This manner of access of a sensor network is not so efficient. The users can query the sensors only in the way that is allowed by the gateway. Another disadvantage is that the gateways and the sensors have to be from the same company in order to be compatible. Moreover, if new sensors need to be added then changes to the gateway happen [1] [2]. Figure 1 displays such a wireless sensor network.

These limitations raised the need for standardized, open solutions for network communication with the devices. Also, these new solutions have to be interoperable with the widely used protocols in the Internet, IP and HTTP. Such protocols are the IETF IPv6 over Low Power WPAN (6LoWPAN) protocol that operates over IEEE 802.15.4, the ZigBee IP protocol and the ZigBee over IEEE 802.15.4. All are specifically designed for transmitting short-range and low-speed data over wireless personal area networks (WPAN).

2. IEEE 802.15.4 Standard

2.1. IEEE 802.15.4 Overview

The IEEE standard 802.15.4 offers physical and Media Access Control (MAC) layers for low-cost, low-speed, low-power wireless, short-range personal area networks (WPANs). It only provides the MAC and PHY layers, leaving the upper layers to be developed according to the market needs. It can be used at the home networking, industrial networks, interactive toys etc.

- The standard versions of the 802.15.4 protocol are:

802.15.4 – 2003. Initial version using Direct Sequence Spread Spectrum (DSSS).It provided for two different PHYs - one for the lower frequency bands of 868 and 915 MHz, and the other for 2.4 GHz (ISM band).

802.15.4 – 2006. Revised version using both Direct Sequence Spread Spectrum(DSSS) with higher data rates and Parallel Sequence Spread Spectrum (PSSS).It also defined four new modulation schemes that could be used - three for the lower frequency bands, and one for 2.4 GHz.

802.15.4a – 2007. It added Direct Sequence Ultra-wideband (UWB) and Chirp Spread Spectrum (CSS) physical layers to the 2006 version of the standard (ranging support).

802.15.4c.It updates for 2.4 GHz, 868 MHz and 915 MHz, UWB and the China 779-787 MHz band.

802.15.4d It includes 2.4 GHz, 868 MHz, 915 MHz and Japanese 950 - 956 MHz band.

802.15.4e This version defines MAC enhancements to IEEE 802.15.4 in support of the ISA SP100.11a application.

802.15.4f This version will define new PHYs for UWB, 2.4 GHz band and also 433 MHz.

802.15.4g This version will define new PHYs for smart neighborhood networks. These may include applications such as smart grid applications for the energy industry. It may include the 902 - 928 MHz band [3] [4].

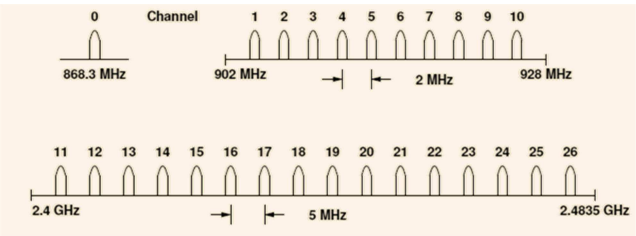

Figure 2. Operating frequency bands of 802.15.4.

2.2. IEEE 802.15.4 Physical Layer

The IEEE 802.15.4 physical layer is responsible for activation and deactivation of the radio transceiver, energy

detection within the current channel, link quality indication for received packets, clear channel assessment (CCA) for CSMA/CA, channel frequency selection, data transmission and reception.

The 802.15.4 protocol typically operates at one of the following license-free frequency bands: 868–868.6 MHz (Europe) with 20 Kbit/s data rate and 20 KBaud Rate, 902–928 MHz (America) with 40 kbit/s data rate and 40 KBaud Rate or 2,400–2,483.5 MHz (worldwide, ISM band) with 250 kbit/s data rate 62.5 KBaud Rate. The modulation used is the O-QPSK or BPSK.

The 802.15.4 protocol has 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz ISM band and one channel in the European 868MHz band. The figure 2 shows the form of the frequencies and channels at the physical layer.

The IEEE 802.15.4 is good against the noise. This happens because Direct Sequence Spread Spectrum (DSSS) is used to modulate the information before is sent to the physical layer. Each bit of information to be transmitted is modulated into 4 different signals. This process causes the total information to be transmitted to occupy a larger bandwidth but uses a lower spectral power density for each signal. This causes less interference in the frequency bands used and improves the Signal to Noise Ratio (SNR) in the receiver due to the fact that is easier to detect and decode the message which is being sent by the transmitter [5]. Figure 3 presents this technique.

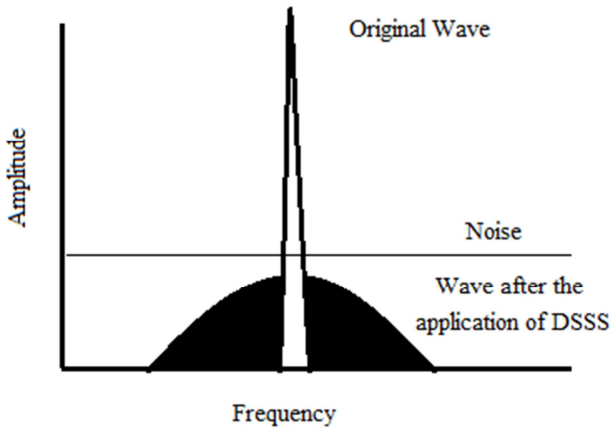

Figure 3. Direct Sequence Spread Spectrum technique.

Figure 4 shows the IEEE 802.15.4 physical layer frame structure. It consists of the fields:

_ Preamble (32 bits) for synchronization

_ Start of packet delimiter (8 bits) – shall be formatted as “11100101”

_ PHY header (8 bits)

_ PSDU (0 to 127 bytes) – data field

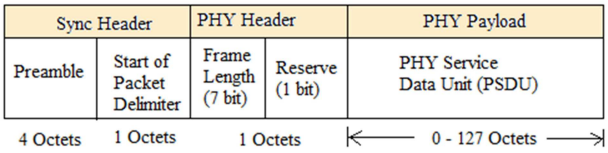

Figure 4. IEEE 802.15.4 PHY frame structure.

2.3. IEEE 802.15.4 MAC Sublayer

The MAC layer provides the control for the flow of frames that pass through the radio interface and are transmitted. The MAC layer also provides the interface to the higher layer protocol stacks of the application systems such as ZigBee, 6LoWPAN, etc.

When a device wants to send a packet, the MAC sublayer asks the PHY layer to check whether the medium is occupied by the Clear Channel Assessment for CSMA/CA method. If the PHY layer answers that another transmission is taking place, the MAC sublayer does not send the data and waits for a specified amount of time before it retries sending the packet. On the other hand, if the PHY layer determines that the medium is free then the MAC sublayer transmits the packet immediately. The MAC sublayer also provides acknowledgement of frame reception and validation of incoming frames.

The IEEE 802.15.4 protocol defines two types of devices: the full function devices (FFD) and reduced function devices (RFD).The FFD devices can coexist in a Personal Area Network (PAN), either as a coordinator or as a simple device. Even in the case of a PAN network consisting of only RFD devices, it is recommended the existence of even a FFD device that functions as a PAN coordinator.

Four different network operations are in 802.15.4: the star topology, the mesh and tree topology and the cluster topology.

Star Topology: This type of topology is simple. In this topology all the end devices of network are connected to the coordinator as shown in Figure 5. The coordinator handles all the traffic of the network and when it fails the network stops to function. In the case that the network includes a lot of nodes then the network efficiency is reduced. This topology has the advantage that the messages go through at most two hops to reach their destination.

Tree Topology: Figure 6 shows a tree topology. In this type of network the coordinator (FFD) is the root of the tree and initializes the network. The routers (FFD) or the end devices (RFD) can be connected to the coordinator and the network expands like a tree. The function of the router is to extend the network coverage. End devices (or child nodes) cannot connect with other end devices because these cannot relay the messages. Each end device is only able to communicate with its router or the coordinator. This topology allows the different roles of nodes. The packets travel from the source node to the connected router and from there to the other

routers until reach the destination node. The disadvantages of tree topology are: a) if a router becomes disabled, then the end devices that connect to that cannot communicate with other devices in the network. b) If two devices are located beside each other they cannot communicate directly.

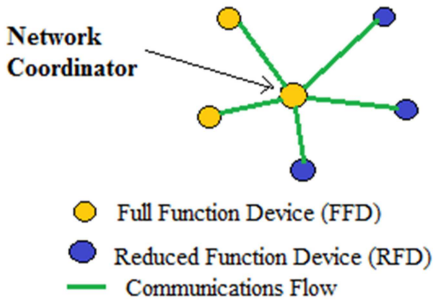

Figure 5. Star Topology.

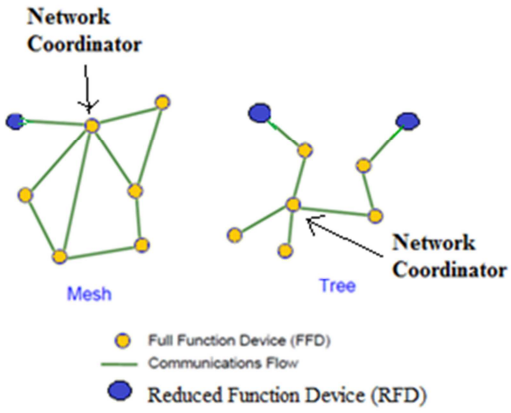

Figure 6. Mesh and Tree Topology.

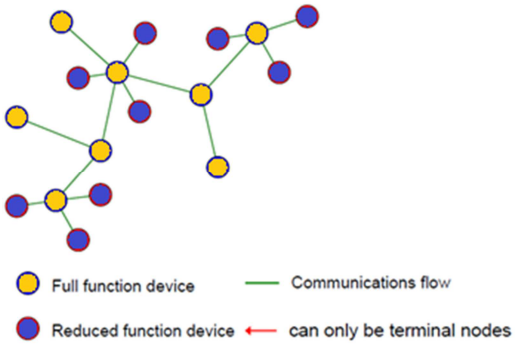

Figure 7. Cluster Topology.

Mesh Topology: A mesh topology shown in Figure 6. It consists of one coordinator, several routers, and end devices. In this topology messages pass through multiple hops to reach their destination. A mesh topology can find the solution if a path fails, since the nodes will find an alternative path to the destination (self-organisation). In this network is easy to add or remove devices.

In cluster topology we have a number of star topologies which connect each other (Figure 7). For example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

The 802.15.4protocol has an extremely low duty-cycle (<0.1%). This means that the transceiver can be sleeping most of the time (up to 99% on average) while the receiving and sending tasks can be set to take just a small part of the devices energy. So, low power consumption can be achieved.

The MAC layer defines four different frame types: Beacon frame, Acknowledgment frames, MAC command frames and Data frames. The beacon frames are used in the synchronization mechanism. The Acknowledgment frames (their use is optional) are used to identify emissions. The MAC command frames execute orders of the protocol, such as "connection request" or "data request". Finally, the data frames are used for all data transfers. The figure 8 shows the general frame structure of the IEEE 802.15.4protocol.

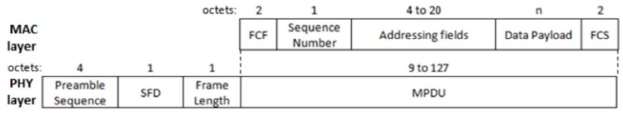

Figure 8. IEEE 802.15.4's general frame structure.

The 802.15.4 is good against collisions, because it uses two channel access techniques in order to avoid all the nodes start emitting at the same time: CSMA-CA and Time Domain Multiple Access (TDMA) using synchronization beacons and Guaranteed Time Slots (GTS). In the CSMA-CA method each node listens the medium prior to transmit. The Guarantee Time Slots (GTS) method uses a centralized node (PAN coordinator) which gives slots of time to each node so that anyone knows when to transmit. There are 16 possible time slots [5].

2.3.1. IEEE 802.15.4 Unslotted Mode

In the case that a node needs to communicate with the PAN coordinator, or a node with another node, then the sender uses CSMA/CA technique and the receiver sends an ACK if requested by the sender. Receiver needs to listen continuously and can't sleep. On the other hand if the PAN coordinator needs to communicate with a node, then the node polls the PAN coordinator whether data is available. The PAN coordinator sends an ACK followed by a data frame and the node sends an ACK if requested by the sender. Coordinator needs to listen continuously and can't sleep.

2.3.2. IEEE 802.15.4 Slotted Mode

The MAC layer is responsible for generating network beacons that allow devices to find an existing network. The beacons define the limits of superframes, help to the synchronization of the associated devices, send to all network devices the information of the existence of a PAN and inform

the coordinator about pending data [6].

Figure 9 shows the structure of a superframe. It is divided into two parts:

- Inactive: the channel is not used and all devices including the coordinator can sleep.
- Active: Consists of 16 slots. It can be further divided into two parts:
  - Contention access period (CAP), the channel can be accessed using normal CSMA/CA.
  - Contention free period (CFP) has Guaranteed Time Slots (GTS) assigned by the PAN coordinator to each node.

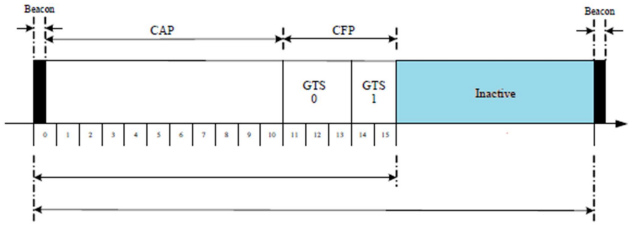

Figure 9. 802.15.4 Superframe.

3. ZigBee Technology

3.1. ZigBee Protocol Overview

The ZigBee wireless networking protocol is characterized by low data transfer speed, low energy consumption and costs and is used at applications which demand remote control. Therefore, this protocol provides communication with low cost and low energy consumption, without using high data transfer rates, such as the Bluetooth technology. The ZigBee protocol was developed by the ZigBee Alliance. The ZigBee Alliance is a group of companies that worked in cooperation to develop a network protocol which can be used in a variety of commercial and industrial low data rate applications [7]. The ZigBee wireless nodes transmit at a range of one to one hundred meters, depending on the power consumption demands of some applications. Also, the nodes transmit at frequencies that do not require authorization (at 868 MHz in Europe, 915 MHz in the Americas, Australia and the global 2.4 GHz ISM Band). The data transfer speed provided by the ZigBee protocol is 20 Kbps at 868 MHz, 40 Kbps at 915 MHz and 250 Kbps at 2.4 GHz.

3.2. ZigBee Versions

The standard versions of the ZigBee protocol [4] are:

ZigBee 2004.This is the original version of ZigBee (ZigBee 1.0) that was released in June 2005.

ZigBee 2006.This version of the ZigBee standard introduced the concept of a cluster library and was published in September 2006. The library is a set of standardised commands, organised under groups known as clusters with names such as *Smart Energy*, *Home Automation.*

ZigBee2007.This version was announced in October 2008 and contained two different profile classes.

ZigBee PRO .ZigBee PRO was the next version of the ZigBee 2007 release. It provided additional features required for robust deployments including enhanced security.

RF4CE. Radio Frequency for Consumer Electronics (RF4CE) was a standard that was used at audio-visual applications. It was released in 2009.

3.3. ZigBee Protocol Stack

The IEEE802.15.4 protocol focuses on the organization of the physical and MAC layers. The ZigBee protocol, on the other hand, is used to provide the upper layers of the protocol stack for interoperable data networks and security services [8]. So, it adds two more layers: the network layer and the application layer. Figure 10 shows the protocol stack.

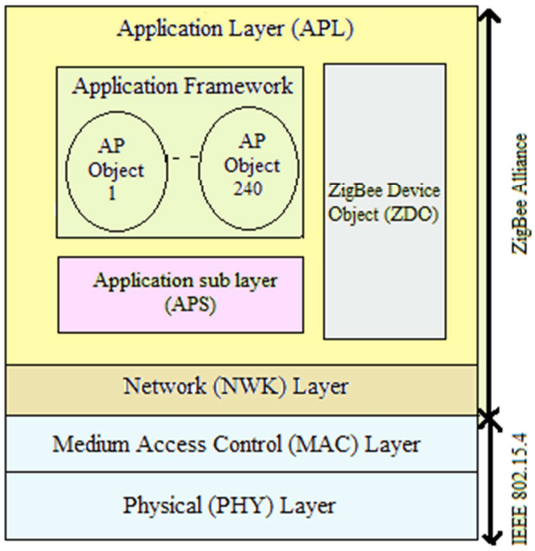

Figure 10. ZigBee Protocol stack.

Application Layer

The application layer contains the applications running on a ZigBee network, for example to control temperature, humidity or other atmospheric parameters. This layer makes the device useful to the user. A node can run more than one applications. These applications are characterized by a number from 1 to 240, which means that the maximum number of applications in a ZigBee device is 240. The application number 0 is reserved for a single application that is present in all the ZigBee devices. Application No. 255 is also reserved for transmitting a message to all the embodiments of a node. Finally, there is a special application in each ZigBee device, the ZigBee Device Object or ZDO.

This application provides function keys such as the definition of the type of a ZigBee device (end device, router and coordinator), the initialization of the network and participation in creation of a ZigBee network. That is, ZDO implements the control plane signaling.

In general, the characteristic operations of the application layer include the implementation of message exchange between applications, the initialization of the discovery of the network, the node's connection to it and the failure and recovery of ZigBee nodes.

Network Layer

The network layer implements characteristics of the ZigBee protocol such as the mechanism for self-organizing the network in case of an error. This layer provides network management, routing, recording of error messages and network security.

The operations of the network layer include the establishment of a network, participation in a network and the connection to it, assignment of an address, maintaining the adjacency matrix, the processes of mesh and tree routing, the implementation of broadcasting, the transmission and receipt of data, mobility and planning of beacons.

Security Plan

The security plan is spread among the network and application layers. In this, security mechanisms are implemented such as message encryption with AES. Another security feature is the timeout message defined by a counter field in each message. Using this counter field, a device can determine the age of a received message and prevent the possibility to record an old message that returns to the device (replay attack).

3.4. ZigBee Devices and Topologies

The ZigBee protocol separates devices into the following categories:

ZigBee coordinator. The coordinator is the root of the tree network, the more capable device and is responsible for its formation. There is always only one coordinator in each network. It requires continuous supply.

Router or ZigBee Full Function Device: routers can forward messages from other devices to their corresponding destinations. At the same time they can also perform the intended application running on the network. It requires continuous supply.

ZigBee End Device or Reduced Function Device: the end devices are very basic with few responsibilities and necessarily linked to a parent (router or coordinator). They send application messages, but they do not forward messages from other nodes. They spend much time asleep, saving thus energy from the batteries.

The ZigBee technology support three kinds of network topologies, similar to the IEEE 802.15.4 protocol: star, tree, and mesh networks (it is the topology that is used more often) [9]. The ZigBee technology does not support the cluster topology.

3.5. Data Transfer Model

ZigBee uses two modes for data transfer. These are the beacon and the non-beacon mode. The beacon mode is used when the coordinator works on batteries and the power saving is very important. The non-beacon mode is used when the coordinator is connected at the main power.

In a beacon-enabled network, a device receives the beacon from the coordinator, which is transmitted periodically, in order to be synchronized with him. Then it uses the super frame structure to send the data. If message transmission is completed, the device and the coordinator 'goes back to sleep' (inactive period of the super frame). In the beacon mode, all the devices in a mesh network know exactly when to communicate with each other. Figure 11 shows the function of the beacon mode [10] [11].

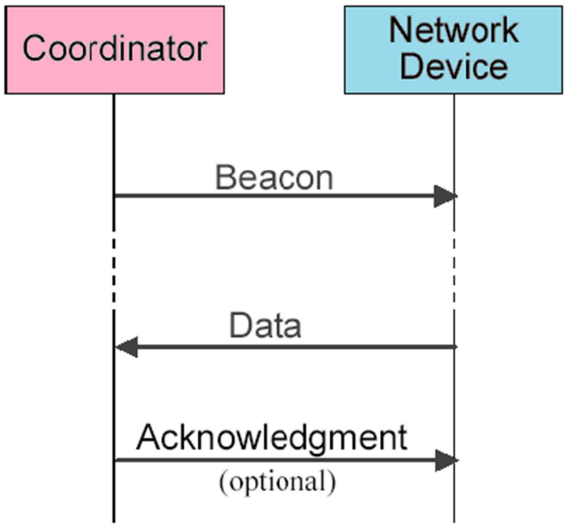

Figure 11. Beacon Network Communication.

In non - beacon mode all the end devices of the network are in 'the sleep mode' nearly always. The devices wake up at random intervals and confirm their presence in the network. If a device needs to send data then simply transmits its data to the coordinator which can always receive messages (it assumes the latter is always on main power). Of course, there is the case that a device needs to send data but the channel is busy. CSMA-CA resolves such issues. Figure 12 shows the function of the non - beacon mode [11].

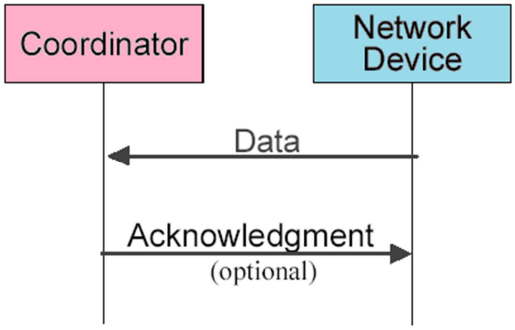

Figure 12. Non - Beacon Network Communication.

3.6. ZigBee Routing Protocols

The ZigBee routing algorithm depends on the topology used in the sensor network. So, in a tree network, when a router device receives a packet, it first checks if itself or one of its child end devices is the destination. If this is true then this device accepts the packet or forwards it to the designated child. Otherwise, this device relays the packet along the tree.

In mesh networks, route discovery is similar to the Ad hoc On Demand Distance Vector routing algorithm (AODV). The links with the lower cost are chosen into the routing path. The Route discovery procedure is a process that is based on a route request and route reply cycle and its metric is based on the number of hops between the two nodes wishing to communicate. When a source node wants to send data to a destination node, the source at first broadcasts a route request (RREQ) packet to its neighbors. Intermediate nodes will forward route request if they have routing capabilities and finally, any node which has a route to the destination or the destination itself will answer (unicast) with a route-reply (RREP) message to the source. If the source receives the route-reply, now it can send data to the destination. If an error occurs during the lifetime of route, a route-error (RRER) message is propagated in order to avoid the use of this broken link.

4. IPv6 over IEEE 802.15.4 (6LoWPAN)

4.1. General Characteristics

The most significant effort to integrate Internet Protocol (IP) into Wireless Sensor Networks comes from IETF, which created the group of 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network) protocols. The purpose of this group is to use the IPv6 protocol over the IEEE802.15.4 protocol, in order to exploit the opportunities provided by this protocol. The IPv4 addresses are not used for the reason that they are limited in number and a large number of small devices is going to need IP addresses. So the 6LoWPANprotocol starts by using IPv6 as the basic IP format. In this way, 6LoWPAN adopts a different approach unlike the other low power wireless sensor network solutions.

In RFC 4919 are established the advantages of using IP over 802.15.4 protocol. These are the following: The nature of IP networks which allow the use of existing infrastructure. The IP-based technologies already exist and are well-known. They have open and freely available specifications. There are already tools for diagnostics and management. IP-based devices can be connected readily to other IP-based networks, without the need for intermediate entities like translation gateways or proxies.
The RFC 4944 documents the 6LoWPAN protocol and describes the general characteristics of it [2]. These are:

- The 6LoWPAN protocol is an adaptation layer allowing to transport IPv6 packets over 802.15.4 links.
- It uses 802.15.4 in unslotted CSMA/CA mode.
- It is based on IEEE standard 802.15.4-2003.
- It supports:
  - Fragmentation / reassembly of IPv6 packets
  - Compression of IPv6 and UDP/ICMP headers
  - Mesh routing
  - Low processing / storage costs.

The IPv6 protocol requires a minimum MTU of 1280 bytes to keep up the frequent fragmentation of IP datagrams. Also the IPv6 forwarding routers, unlike IPv4 routers, do not support segmentation of outgoing packages. This means that packets should be sent with the correct size (MTU). The IEEE 802.15.4 protocol supports up to 127 bytes as maximum frame size. Therefore, 6LoWPAN protocol does not permit normally the transmission of large IP packets over such a network. In case the package does not fit in an 802.15.4 frame, it is fragmented into smaller parts. In addition, the 40 bytes IPv6 fixed header takes a significant part of the already small protocol data unit, leaving little room for IPv6 payload data. To solve these problems an adjustment layer, named 6LoWPAN adaptation layer, is situated between the data link layer and the network layer protocol stack. The adaptation layer provides three main services: packet fragmentation and reassembly, header compression and routing over data link layer (for multi-hop links) [1].

4.2. The 6LoWPAN Protocol Stack

Figure 13 illustrates the 6LoWPAN protocol stack. The physical layer converts data bits into signals that are transmitted and received over the air. This layer belongs to the IEEE 802.15.4 protocol. The data link layer includes the

media access layer (MAC) which provides access to the media, using features like carrier sense multiple access – collision avoidance (CSMA-CA) where the radio listens that no one else is transmitting before actually sending data over the air. This layer also handles data framing. The MAC layer is of the IEEE 802.15.4 protocol. The 6LoWPAN adaptation layer, providing adaptation from IPv6 to IEEE 802.15.4, also belongs to the link layer. The network layer addresses and routes data through the network, with the IPv6 and the RPL protocol. The transport layer is responsible to generate communication sessions between applications running on end devices. The transport layer allows multiple applications on each device to have their own communications channel. The TCP and UDP transport protocols are used at this layer. Also, it includes secure transport layers over TLS/DTLS. Finally, the application layer is responsible for data formatting. It also makes sure that data is transported in application-optimal schemes. The known HTTP protocol cannot be used in the 6LoWPAN systems due to the large overhead that it has. So, the industry developed alternative application protocols such as COAP which is defined by IETF in RFC 7252. It can inter-connect with HTTP easily via proxies [12].

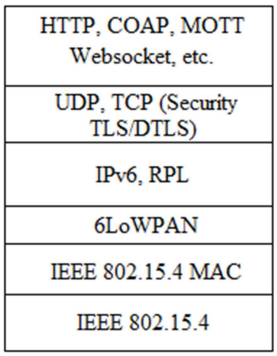

Figure 13. 6LoWPAN protocol stack.

Table 1. 6LoWPAN dispatch Codes.

Bit Pattern	Header Type	Description
00 xxxxxx	NALP	Not A LoWPAN Packet
01 000001	IPv6	Uncompressed IPv6 addresses
01 000010	LOWPAN_HC1	HC1 Compressed IPv6 header
01 010000	LOWPAN_BC0	BC0 Broadcast header
01 111111	ESC	Additional Dispatch octet follows
10 xxxxxx	MESH	Mesh routing header
11 000xxx	FRAG1	Fragmentation header (first)
11 100xxx	FRAGN	Fragmentation header (subsequent)

4.3. 6LoWPAN Protocol Frames

As mentioned above, the transport of IPv6 packets over LoWPAN networks is difficult due to the limited frame size of the IEEE 802.15.4 protocol. RFC 4944 defines that all6LoWPAN encapsulated datagrams transported over IEEE 802.15.4 are prefixed by an encapsulation header stack. Each header in the header stack contains a header type followed by zero or more header fields. The 6LoWPAN header provides three header forms: mesh addressing, fragmentation and header compression, in that order. Figure 14 shows some examples of the 6LoWPAN encapsulation header stack. These IPv6 datagrams are transmitted inside the payload field of an 802.15.4 data MPDU. The format of the header is defined by the 802.15.4 header field at the start of the frame. The first byte of the encapsulated header is called dispatch byte and it determines the next header. The Table 1 contains the different values of dispatch bytes [3]. The mesh address header is used to forward packets of multiple hops inside a 6LoWPAN network and it is not used when sending data over one hop only. The fragment header is used when the payload is too large to fit in a single IEEE 802.15.4 frame.

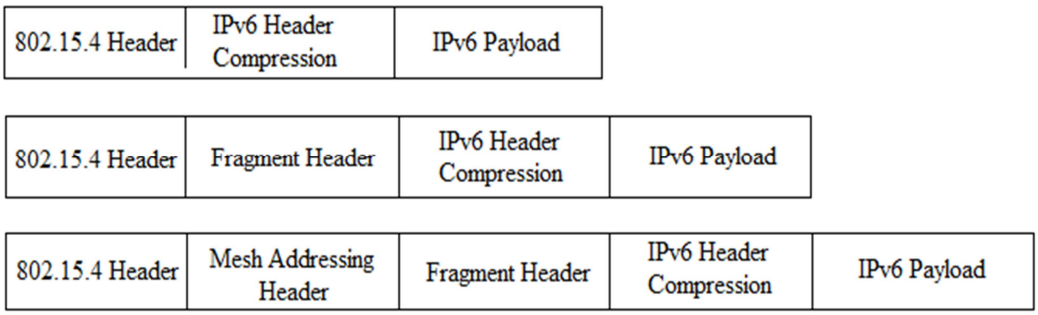

Figure 14. The three types of 6LoWPAN header.

4.4. 6LoWPAN Header Compression

One of the functions provided by the 6LoWPAN adaptation layer is header compression. The RFC 4944 describes the header compression techniques that can be used to compress IPv6 headers, so 6LoWPAN is able to transmit more data. The LOWPAN_HC1 is the main compression technique specified in RFC 4944. It is suitable for link-local IPv6 communication. This technique reduces the packet size by removing common areas. For example, the 6LoWPAN protocol always removes the area of Version by communicating via IPv6. Also, it compresses Traffic Class and Flow Label to a single bit when their values are both

zero. Another compression that the 6LoWPAN can do is the64-bit network prefix for the source and the destination addresses to one bit each when they carry the well-known link-local prefix. The 6LoWPAN protocol limits the values of the next field header field to two bits whenever the packet uses TCP, UDP and ICMPv6. HC1 compression has very low compression factors for global and multicast addresses. The RFC 4944 also defines the LOWPAN_HC2 compression for transport layer compression, which allows compressing UDP, TCP and ICMP headers. Headers of other transport layer protocols cannot be compressed by LOWPAN_HC2. There are also two new compression mechanisms, the LOWPAN_IPHC and LOWPAN_NHC, which are defined in RFC 6282. The LOWPAN_IPHC method compresses the Traffic Class and Flow Label individually. It uses shared-context information to elide the network prefix from IPv6 addresses, and supports multicast addresses. Contexts act as shared state for all nodes within the 6LoWPAN. The LOWPAN_NHC methods uses a next header identifier with variable length which could be used for future next header compressions in order to solve the problem of HC2 method that only compresses UDP, TCP and ICMPv6 headers.

Figure 15 illustrates an example of an uncompressed 802.15.4 frame with IPv6/UDP payload and Figure 16a illustrates how HC1 compression is used for the compression of IPv6 header. Figure 16b presents the case that both HC1 and HC2 compression mechanisms are applied. In this case, the compression removes the Version, Traffic Class, Flow Label, Payload Length, Next Header, and link-local prefixes from the IPv6 Source and Destination addresses [3].

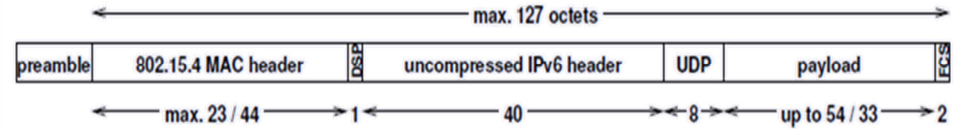

Figure 15. Uncompressed IPv6/UDP (Worst case scenario).

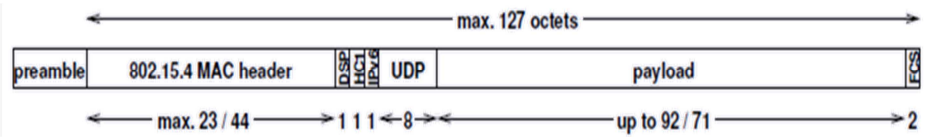

Figure 16a. Compressed Link –local IPv6/UDP.

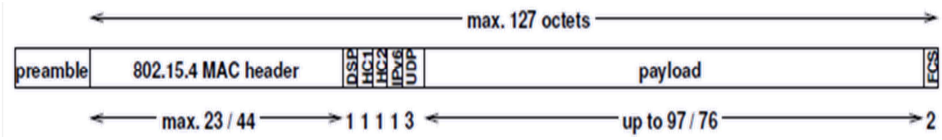

Figure 16b. Compressed Link –local IPv6/UDP with HC1 and HC2 compression (best case scenario).

- The Dispatch code is 01000001and indicates that no compression applies over the IPv6 datagram.

- Payload varies between 33 to 54 octets depending upon the security method (null or AES-CCM-128) that is adopted within the MAC header.

With null security the MAC header can be up to 25 octets. So, 127-25-40-8 = 54 octets (null security) for the payload.

With AES-CCM-128 the MAC header can be up to 25+21=46 octets. So, 127-46-40-8 = 33 octets (AES-CCM-128) for the payload.

- The header information-to-application payload ratio is very bad. Large amount of data cannot be transmitted.

- In Figure 16a the Dispatch code is 01000010 and indicates HC1compression.
- Figure 16b shows the maximum compression we can achieve for link -local addresses (does not work for global addresses).
- After the compression headers HC1 or HC1/HC2, non-compresssable header fields cannot be transmitted.

4.5. 6LoWPAN Fragmentation

The 6LoWPAN adaptation layer also provides the service of fragmentation and reassembly. Fragmentation is only necessary when the entire IPv6 packet does not fit within the standard IEEE 802.15.4 frame. The RFC 4944 defines that the fragmentation breaks a single IPv6 packet into smaller pieces and a fragmentation header is included in each piece. A first fragment carries a header that includes the datagram size (11 bits) and a datagram tag (16 bits). Subsequent fragments carry a header that includes the datagram size, the datagram tag, and the offset (8 bits). Time limit for reassembly is 60 seconds. When a fragment is lost the RFC 4944 requires the whole set of fragments to be resent. Figure 17 illustrates an example of the fragmentation (compressed link-local IPv6/UDP) [3].

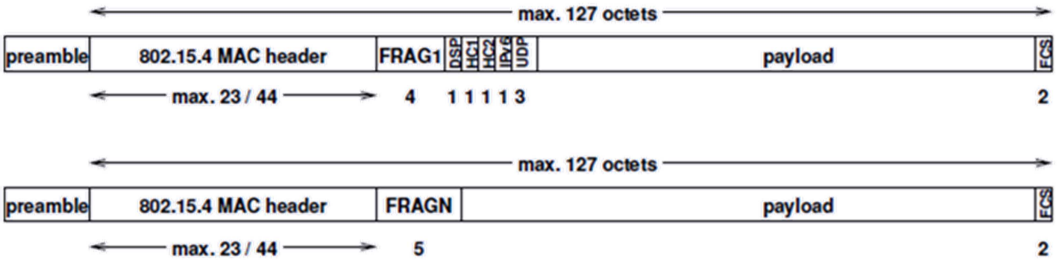

Figure 17. Fragmentation Example (compressed link-local IPv6/UDP).

4.6. 6LoWPAN Routing

Routing is the ability to send a data packet from one device to another device, sometimes over multiple hops. Traditionally, IP routing occurs at the network layer but 6LoWPAN technique supports the 6LoWPAN adaptation layer which is between the link and the network. So, it can do routing at both layers. Depending on what layer the routing mechanism is located, two categories of routing are defined: mesh-under and route-over. Mesh-under uses the layer-two (link layer) addresses (IEEE 802.15.4 MAC) to forward data packets. Route-over uses the layer three (network layer) addresses (IP addresses). Figure 18 shows the two routing categories.

Mesh-under routing uses link layer addresses to make forwarding decisions. Each forwarding layer 2 router along the path of a packet is expected to maintain its own forwarding table based on link layer addresses in order to make forwarding decisions based on these addresses. In a mesh-under network the only IP router in such a system is the edge router. One broadcast domain is established to ensure compatibility with higher layer IPv6 protocols. Broadcast messages are sent to all devices in the network, resulting in high network load. Mesh-under networks are best suited for small or local networks.

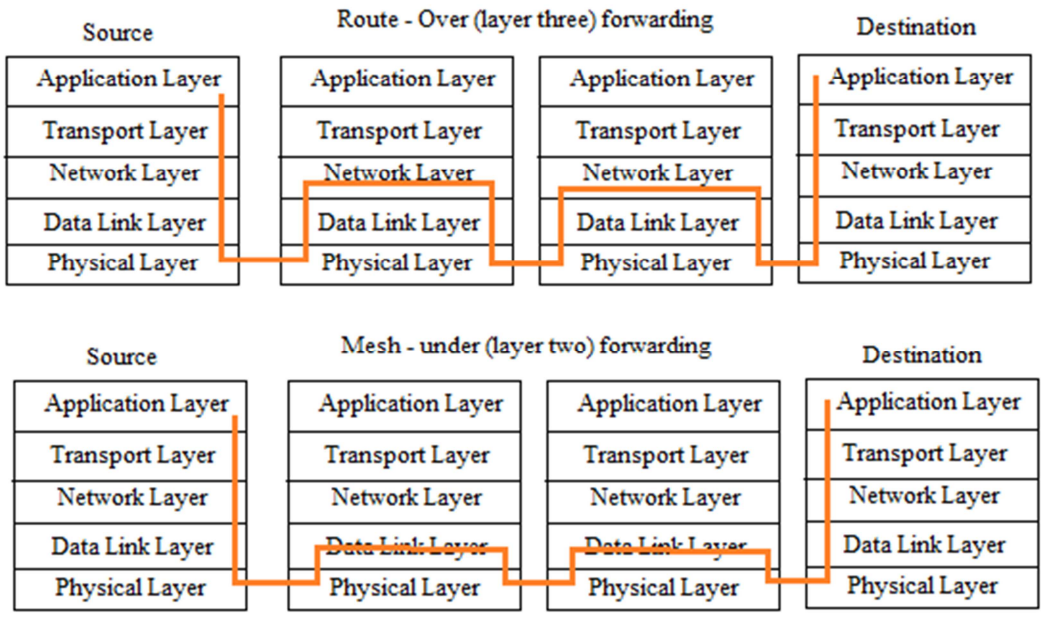

Figure 18. Routing categories.

In route-over networks the routing takes place at the IP level. Thus each hop in such networks represents one IP router. The most widely used routing protocol for route-over 6LoWPAN networks today is RPL [12] [13]. Section 5 is devoted to RPL

Table 2. 6LoWPAN Implementations.

Implementation	Operating System/Simulator	License	RFC4944	RFC6282	RFC6775
SICSLOWPAN	ContikiOS/Cooja Simulator	Open Source	X	X	X
BLIP (Barkley Low-power IP)	TinyOS	Open Source	X		
Arch Rock 6LoWPAN	TinyOS	Open Source	X		
NanoStack 6LoWPAN	FreeRTOS	Open Source	X	X	X
Hitachi	-	Commercial	X		
NS-3	Simulator	Open Source	X		

4.7. 6LoWPAN Implementations

Many organizations, companies and network simulators support the 6LoWPAN adaptation layer in their protocol stacks. Table 2 presents some of them [1].

4.8. 6LoWPAN Devices

A 6LoWPAN network consists of 6LoWPAN nodes (or hosts), 6LoWPAN routers and edge routers. The nodes send and receive packets, the routers perform routing within the 6LoWPAN network and edge routers perform routing between 6LoWPAN networks and other IP networks. A node can also be a sleepy device, waking up periodically to check its parent (a router) for data, enabling very low power consumption [12].

A 6LoWPAN IPv6 subnet includes all nodes that share the same IPv6 prefix covering all 6LoWPAN networks or extended 6LoWPAN networks. A 6LoWPAN network, defined by the nodes that share the same IPv6 prefix, typically having only one edge router, may be connected to other IP networks. An extended 6LoWPAN network can consist of more than one edge router nodes. The extended 6LoWPAN network uses a backbone link (based on Ethernet) to coordinate information routing over the 6LoWPAN network.

4.9. 6LoWPAN Neighbor Discovery Protocol

The 6LoWPAN Neighbor Discovery (ND) protocol is an extension of the IPv6 Neighbor Discovery Protocol. It is specifically designed for 6LoWPAN networks adding some new messages for fault tolerance, bootstrapping, header compression, etc [14].

When a node is put into operation for the first time, it has just a MAC address. Aiming to create an association with a 6LoWPAN network, it sends a Router Solicitation message and receives as response the Router Advertisement messages from local routers. The node can configure its IPv6 address from the information received in the Router Advertisement messages. Then, the node attempts registration to the edge router. The node sends a Neighbor Solicitation message with an Address Registration option to the edge router, in order to create a Neighbor Cache entry with a specific timeout. In case the edge router is a lot hops away from the node, the message is forwarded to the edge router via the local router. The edge router maintains a whiteboard with information about the state of neighboring nodes. This whiteboard is used for the detection of duplicate addresses in the network. Periodically, the node re-sends registration messages to the edge router, in order to update its entry at the whiteboard before it expires [15].

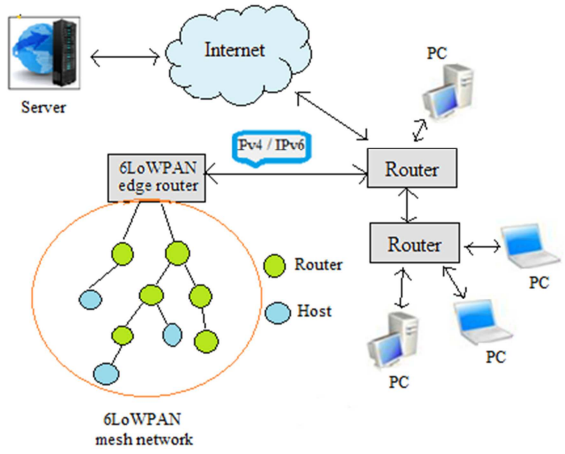

Figure 19. IPv6/IPv4 networking with a 6LoWPAN mesh network.

4.10. Example of a 6LoWPAN Network

Figure 19 illustrates a scenario of an IPv6/IPv4 network, including a 6LoWPAN mesh network. The 6LoWPAN network is connected to the IPv4/IPv6 network using an edge router. The edge router handles three actions: 1) the data exchange between 6LoWPAN devices and the Internet 2) local data exchange between devices inside the 6LoWPAN and 3) the generation and maintenance of the radio subnet (the 6LoWPAN network). Also, the edge router supports IPv6 translation mechanisms to interconnect the 6LoWPAN network with IPv4 ones. For this reason, the 6LoWPAN network is not required to implement IPv4.

5. The RPL Routing Protocol

A Low-power and Lossy Network (LLNs) is a network class in which routers and links are constrained. These routers usually work with limitations in computational power, memory and energy. The links are characterized by high rates of loss and low data rates. Such networks are comprised of tens to thousands of routers. The protocol used in these networks should provide support for point-to-point traffic flows (between nodes within the network), point-to-multipoint type (from a central control point in a subset of nodes in the network) and multipoint-to-point format (nodes within the network to a central control point). The RPL routing protocol (IPv6 Routing Protocol for Low-power and Lossy Networks) provides the mechanism by which these flows are supported. Nodes that implement the RPL protocol are able to independently and autonomously develop a network topology, install and calculate routes without any administrative interaction.

This protocol is based on Directed Acyclic Graph (DAG), which consists of one or more Destination Oriented DAGs (DODAGs) (Figure 20). The creation of the graph depends

on the traffic flow of the network. Specifically, for multipoint-to-point, traffic flow process is moving from the bottom upwards (towards the sink/root node). For point-to-multipoint, traffic flow goes from the sink node downwards. The graph is also used for avoiding loops [1] [3]. Additionally, as mentioned above, the support of point-to-point traffic flows is achieved by the sink node downwards.

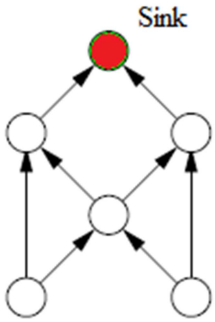

Figure 20. DODAG in RPL.

The RPL routing protocol uses routing metrics to calculate the shortest path. Thus, the graph is created, always choosing the shortest route. If a node, for whatever reason, is no longer accessible in the network, or a connection between two nodes is no longer available, the calculation and creation of different routes for all affected nodes is also supported. The RPL protocol uses three types of messages in order to maintain the DODAG. These are: the DIO (DAG Information Object), the DIS (DAG Information Solicitation) and the DAO (Destination Advertisement Object). The DIO message is broadcasted periodically from the nodes. The ratio of DIO messages depends on the stability or the routing inconsistencies of the network. A DIO carries information that allows a node to join a new DODAG, or to maintain an existing DODAG. The DIS message is used by a node to request a DIO from an RPL node. The DAO message propagates destination information upwards along the DODAG and a node chooses parents that minimize the path cost to the DODAG root [16].

6. Constrained Application Protocol (CoAP)

6.1. General Characteristics

In 2010, the IEFT organization formed a working group, called Effortless Constrained RESTful Environments (CoRE) in order to create a RESTful protocol a similar way as traditional web services, but suitable for networks and nodes with limited resources, such as the networks of wireless sensors. The specified protocol is the Constrained Application Protocol (CoAP). It is a specialized RESTful web transfer protocol for use by constrained networks and nodes.

Networks of limited resources such as 6LoWPAN support the fragmentation of IPv6 packets into small packets of data link layer, however, thus achieving a significant reduction in the probability of successful delivery of packets. One of the design goals of the CoAP protocol is to maintain low overhead messages, thereby reducing the need for fragmentation.

A lot of implementations of CoAP have appeared. These are Californium, jCoAP, CoAPy and Libcoap [17].

Characteristics of the CoAP protocol.

- Constrained machine-to-machine web protocol
- Representational State Transfer (REST) architecture
- Simple proxy and caching capabilities
- Asynchronous transaction support
- Low header overhead and parsing complexity
- URI and content-type support
- UDP binding
- Reliable unicast and best-effort multicast support
- Built-in resource discovery
- It provides a mapping to HTTP, allowing proxy servers to access CoAP resources via HTTP uniformly or an HTTP interface to be implemented as an alternative to the use of CoAP.
- Provides security through connection with DTLS (Datagram Transport Layer Security) [3].

6.2. CoAP Protocol Stack

Figure 21 shows the HTTP and CoAP protocol stacks.

CoAP physical Layer and Data Link Layer

The physical layer (PHY) and media access control (MAC) are determined from the IEEE 802.15.4 standard which is for low-rate wireless personal networks.

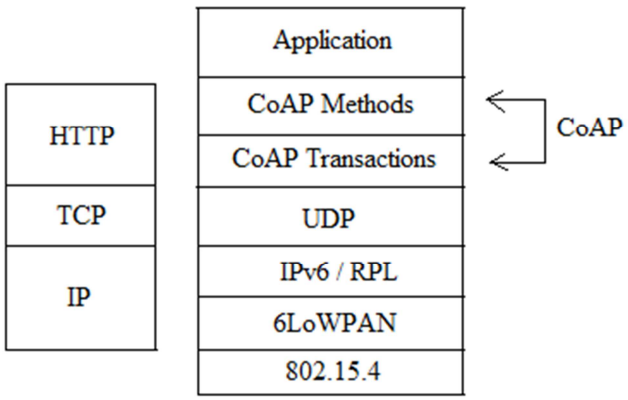

Figure 21. HTTP and CoAP protocol stacks.

CoAP Network Layer

This layer is specified from the IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) standard. Also, it uses the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) technology.

CoAP Transport Layer

HTTP is based on the Transmission Control Protocol (TCP) but is not suitable for the Low-Power and Lossy Networks (LLNs). CoAP is formed on the User Datagram Protocol (UDP) which has lower overhead and supports multicast.

CoAP Application layer

The CoAP transactions provide reliable UDP messaging, since UDP is an unreliable protocol, CoAP implements its own mechanisms in order to guarantee reliability to those applications that use it.

The interaction model of CoAP is similar to the well-known client -server one of HTTP. So, the methods of CoAP for the requests and responses resemble with the methods of HTTP.

The CoAP method calls may involve multiple CoAP transactions. The Roles at the transaction layer may change during a method request / response execution.

CoAP, for being able to run on constrained devices, it has a header overhead much smaller and it is a simpler protocol. So, it uses a 4-bytes base binary header that may be followed by compact binary options and payload [18][19].

6.3. CoAP Message Format

Figure 22 shows the CoAP Message Format. It comprises a 4-bytes binary header followed by one or more of the following optional fields: Token, Options and Payload [1]:

Version (Ver): A 2-bit unsigned integer indicating the CoAP version number. Messages that do not carry version number should be ignored.

Type (T): A 2-bit unsigned integer indicating if this message is of type Confirmable (0), Non-Confirmable (1), Acknowledgement (2) or Reset (3).

Token Length (TKL): A 4-bit unsigned integer indicating the length of the variable-length header. Larger values should not be sent and are treated as errors.

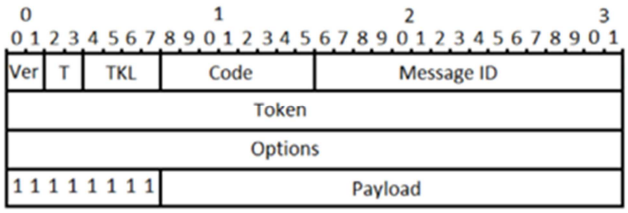

Figure 22. Message Format.

Code: An 8-bit unsigned integer indicating if the message carries a request (1–31) or a response (64–191), or is empty (0). (All other code values are reserved).

The CoAP interaction model is similar to the client/server model of HTTP. A client can send a CoAP request, requesting an action specified by a method code on a resource (identified by a URI) on a server. The CoAP server processes the request and sends back a response containing a response code and payload.

The methods that the CoAP supports are [3]:

GET: Retrieves information of an identified resource

POST: Creates a new resource under the requested URI

PUT: Updates the resource identified by an URI

DELETE: Deletes the resource identified by an URI

Message ID: A 16-bit unsigned integer in network byte order is used for the detection of message duplication, and to match messages of type Acknowledgement/Reset to messages of type Confirmable/ Non-confirmable.

The messages that the CoAP supports are:

CON:	This message is sent repeatedly using a predefined timeout time and waiting time exponential back-off between the missions of the message until the recipient to send Acknowledgement type message with the same identifier. On the other hand, if the receiver cannot process a message, it responds with a Reset message type.
NON:	A message that does not require are liable transport, such as a random measurement of a data stream of a sensor, can be sent as Non-confirmable (NON). Although no confirmation message is expected, these messages carry also an identifier or identifying duplicates. If the recipient cannot process the message, it replies with a Reset message type.
ACK:	Acknowledges that a CON has been received, may carry payload
RST:	Indicates that a CON has been received but some context is missing to process it.

Token: 0 to 8 bytes, as given by the Token Length field. The Token value is used to correlate requests and responses.

Options: The Option field can be followed by the end of the message, by another Option, or by the Payload Marker and the payload. The format of the Options field is shown in Figure 23 [3]:

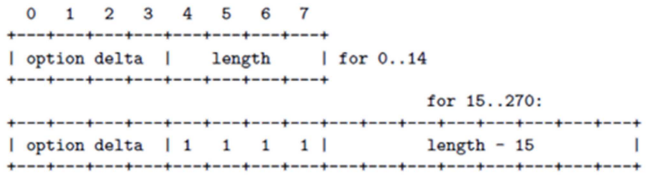

Figure 23. Option format.

The option delta is a 4-bit unsigned integer and it identifies the option type, encoded as the delta (difference) to the previous option code. The option code implies the type of the encoded data. URI parameters are carried in options.

Payload: The Payload Length is calculated from the datagram size. The absence of the Payload Marker (11111111) indicates zero-length payload.

7. ZigBee IP Protocol

7.1. General Characteristics

ZigBee IP is an open standard specified by the ZigBee Alliance based on the IPv6 specification for wireless sensor networks and remote control. The ZigBee IP protocol supports the operation of IPv6 on top of wireless mesh networks. It is suitable for low cost, low-power devices. It is designed to specifically support the ZigBee Smart Energy version 2 (SEP2) protocol. As a result of that, the standard allows the constrained devices to be part of the Internet of Things concept.

7.2. ZigBee IP Features

The features of the ZigBee IP protocol are:

- uses the IPv6 addressing scheme
- uses the IEEE 802.15.4 base standard to provide the low layer functionality.
- is specified for use in license free bands: 2.4 GHz (global); 868 MHz (Europe); 915 MHz (USA); 920 MHz (Japan).
- uses 6LoWPAN for header compression
- uses the IETF PANA for authentication
- uses the RPL protocol for routing
- uses the TLS and EAP-TLS for security
- uses the TCP and UDP transport protocols
- provides multicast capability. It enables service discovery using mDNS and DNS-SD protocols.
- Using the IPv6 protocol ZigBee IP is able to communicate end to end with devices in its own network or other networks with an ultimate connection [20].

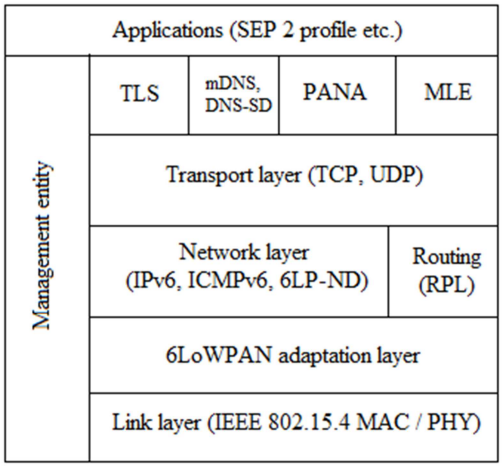

Figure 24. ZigBee IP protocol stack.

7.3. ZigBee IP Protocol Stack

Figure 24 illustrates the ZigBee IP's protocol stack [21].

The Physical Layer has the follow characteristics:

It uses the IEEE 802.15.4 PHY layer in 2.4GHz Global operation with:

– 250kbps data rate.

– DSSS (direct sequence spread spectrum).

It operates in regional, sub-GHz bands via 802.15.4g-2012.

Commonly available systems use FSK modulation with 50 – 200 kbps rate.

The link layer IEEE 802.15.4 MAC

It can discover the network using MAC beacons. A Node can find identifier, capacity and verifying information for the networks to be related with.

The Channel access scheme is CSMA/CA on the 2.4GHz band.

It supports battery operated sensor nodes. The parent node buffers packets for the sleepy nodes.

It uses the AES-128-CCM frame security for Privacy, Integrity and Replay protection.

The 6LoWPAN Adaptation Layer

It adapts IPv6 packets for transmission over 802.15.4 links. It applies header compression to reduce overhead and a fragmentation scheme to allow the transmission of large IPv6 packets over short 802.15.4 frames.

It supports the 6LoWPAN Neighbor discovery (RFC 6775) and optimizes it with:

• Reduced multicast signaling.

• Removes the need for transitive links.

• Supports duty-cycled nodes.

The Network and Transport Layers.

The Network layer supports the IPv6 and ICMPv6 protocols. For the transport layer it uses TCP for connection oriented sessions with HTTP(s) applications. The UDP is used for connection-less traffic and the support of applications as mDNS. The TLS 1.2 is used for end-to-end transport security.

Routing.

For routing protocol, the ZigBee IP standard uses the RPL protocol (RFC 6550), which supports multi-hop routing within the PAN, multiple upward and downward route options and loop avoidance and detection.

In Multicast transmissions, it supports UDP applications as mDNS and Mesh Link Establishments and controls flooding of packets within the PAN.

Access Control

The Authentication stack consists of PANA, EAP, and TLS protocols.

The Access control is achieved through a central server which supports PSK and ECC-256 cipher suites.

The Authenticated nodes can securely receive network security material, which can be updated periodically.

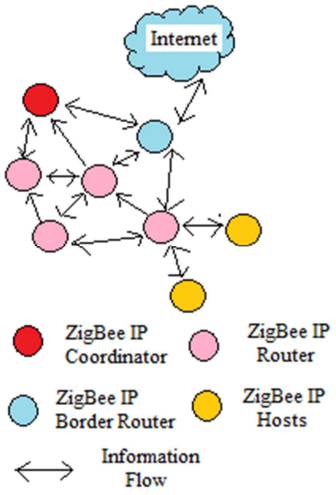

Figure 25. ZigBee IP network topology.

Mesh Management

It supports the Mesh Link Establishment (MLE*)* protocol based on UDP transport. It enables nodes to detect and maintain links with neighbor nodes. So:

– Detect new links and prune dead links

– Exchange bi-directional link quality metrics to detect asymmetric links

It propagates commissioning information into the network for channel updates, etc.

7.4. ZigBee IP Network Topology

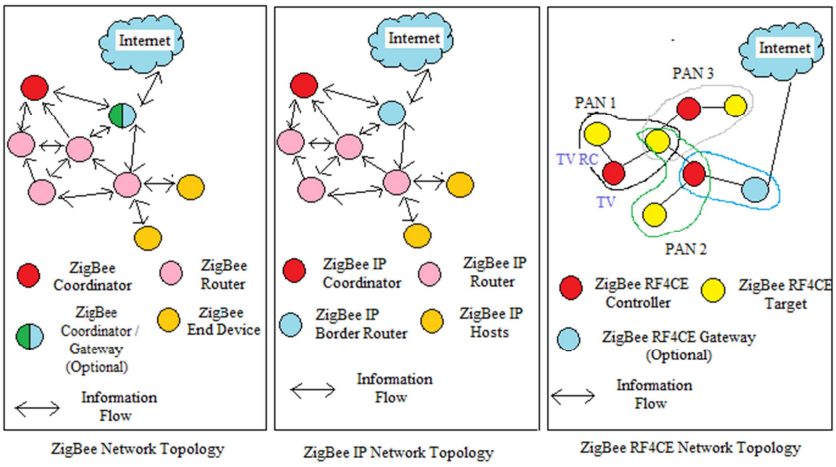

Figure 26. ZigBee network topology, ZigBee IP network topology and ZigBee RF4CE network topology.

Figure 25 illustrates the ZigBee IP network topology [22]. ZigBee IP networks consist of several device types: ZigBee IP Coordinator, ZigBee IP Routers and ZigBee IP Hosts. Coordinators control the formation and security of networks. Routers extend the range of networks. Hosts perform specific sensing or control functions. Manufacturers often create devices that perform multiple functions. So, in a smart home network, the coordinator may be a programmable communicating thermostat with advanced support for an in-home display. Devices such as smart plugs, thermostats and smart appliances could be configured as routing devices. Simple devices such as smart appliances and temperature sensors could be end devices [22] [23] [24]. Since all appliances have their own IP addresses based on IPv6, they can be directly connected to external networks. So all appliances can be not only controlled locally and centrally

through a remote control device at home but can be also controlled by a long-distance PC, which enters the home network by the edge router through the Internet.

Figure 26 juxtaposes [21] the ZigBee network topology, the ZigBee IP network topology and the ZigBee RF4CE network topology. The latter, addresses the need for one worldwide remote control standard capable of controlling multiple consumer electronic devices via RF for better user experience. Among them, only the ZigBee IP network topology has border routers for communication with the internet.

8. ZigBee Smart Energy 2.0 (SEP)

The Smart Energy Profile (SEP) 2.0 is an application protocol, developed by the ZigBee Alliance, running over the ZigBee IP stack. It has a well-defined semantic model with a secure HTTP architecture. SEP 2.0 can connect home automation devices, like thermostats, and gather data from them, which are then tied to smart phones that are also connected to the smart grid. Figure 24 presents SEP 2.0 over the ZigBee IP protocol stack.

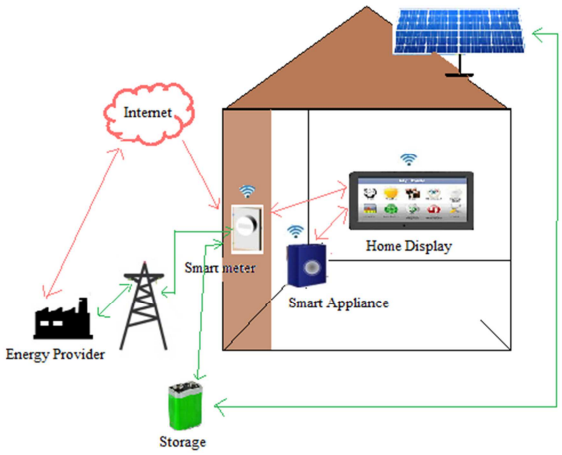

Figure 27. Typical smart home with the concept of the smart energy.

In the forthcoming years it is expected to find great use in the smart energy market, since it will help software developers to design advanced smart energy applications. The concept behind smart energy is of controlling energy use internally, within the home, and externally, from the home to outside connected devices, networks, and the smart grid itself, all with the goal for optimizing energy production, distribution, and usage. SEP 2 was selected by the United States National Institute of Standards and Technology (NIST) as a standard profile for smart energy management in home devices.

ZigBee IP with SEP 2.0 supports devices with long battery life, like gas or water meters, that need to run for years on single batteries. ZigBee IP lets battery-powered devices sleep for hours or even days, reducing battery use. A ZigBee node can wake up and communicate with other ZigBee devices and then return back to sleep. ZigBee IP also has meshing capability, which allows the signals to hop to other nodes on a network on their routes to their destinations. In addition, it allows the communication between indoor and outdoor devices, including exterior electric meters in metal enclosures [21], [25], [26], etc.

9. Smart Home Proposal

Figure 27 shows a typical smart home in which the concept of smart energy is applied. So, devices such as a washing machine, an in-home display and a power meter, all work collaboratively in order to make the home and power grid smarter.

The development of smart homes can be anymore a reality with the plethora of applications and sensors available. All consumer electronics and applications can collaborate, so the owner of a house can control and monitor almost all its functions for improving energy efficiency, access control, and security. These applications will operate and integrate over the same open communication standards (e.g. ZigBee or 6LoWPAN) and various sensor applications in order to create real Smart Homes without much human intervention.

The smart home applications that a smart home can include are:

Smart Home Applications

- Fire detection–Leak detection
- Home security - Access control
- Energy efficiency
- Lighting control
- Solar panel monitoring and control
- Temperature monitoring and HVAC control
- Energy Management

The Smart Home concept can be implemented in 3 phases [28]. Phase 1 includes the creation of the system of a RF-based remote control, according to the ZigBee RF4CE approach, for Set-Top Boxes. Such Set-Top-Boxes can also play the role of gateway for connection to the internet. During Phase 2 mostly an energy management system will be developed. But many other applications will be developed simultaneously, such as for lighting control, temperature monitoring, HVAC control and Energy efficiency. Finally, at Phase 3 the security system will be set up so we have an integrated environmental awareness. After that, the smart

house will be a part of the Internet of Things.

Figure 28 illustrates the interior [28] of a smart house. It is a figure of a typical house where we can apply the sensors and the applications in order to form a smart house. The three phases of implementation are illustrated with the corresponding colors.

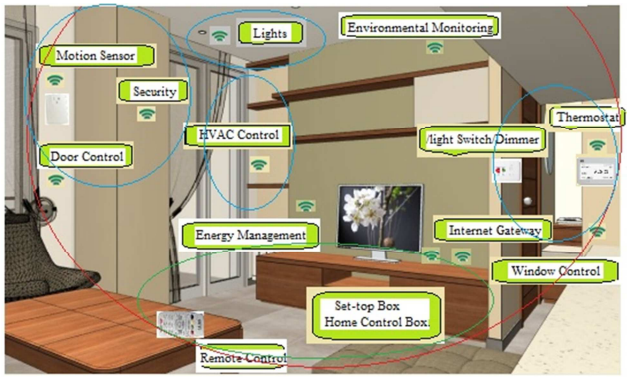

Figure 28. Smart Home.

10. Further Work

10.1. ZigBee 3.0 Protocol

The ZigBee Alliance currently carries out tests in order to release ZigBee 3.0, the new standard for ZigBee. This standard is designed to provide interoperability among the thousands of existing smart devices and give consumers and enterprises access to new products and services that work together harmoniously for the improvement of the everyday life. It is expected to be ratified by the end of 2015 [29] [30]. ZigBee 3.0 is based on IEEE 802.15.4 and uses ZigBee PRO networking to enable reliable communication for constrained devices. All current device types, commands and functionality defined in current ZigBee PRO standard is expected to be available in ZigBee 3.0 [31]. Figure 29 juxtaposes the ZigBee IP stack versus ZigBee Pro and ZigBee RF4CE [21].

	ZigBee RF4CE		ZigBee PRO							ZigBee IP
Application Standard	ZigBee Remote Control	ZigBee Input Device	ZigBee Building Automation	ZigBee Health Care	ZigBee Home Automation	ZigBee Light Link	ZigBee Retail Services	ZigBee Smart Energy 1.x	ZigBee Telecom Senders	ZigBee Smart Energy 2.0
Network	ZigBee RF4CE		ZigBee PRO							ZigBee IP
MAC	IEEE 802.15.4 - MAC									IEEE 802.15.4 - MAC
PHY	IEEE 802.15.4 Sub-GHz (specified per region)		IEEE 802.15.4 - 2.4 GHz (worldwide)							IEEE 802.15.4 2006 - 2.4 GHz or other

Figure 29. ZigBee IP stack versus ZigBee Pro and RF4CE.

The IEEE 802.15.4 standard, as we know covers the lower two levels of the OSI model (PHY and MAC layer). The previous ZigBee releases covered the application through network layers. ZigBee 3.0 is regarded to put special focus at the application layer. At the application layer, ZigBee 3.0 will support more than 130 devices from different places of the IoT, including building and home automation, like lighting, energy management, smart appliances, security, sensors and health care monitoring products.

10.2. Other Protocols of the 802.15.4 Family

Apart from the popular ZigBee and 6LoWPAN protocols, also the Wireless HART, ISA-SP100 and MiWi protocols use IEEE 802.15.4 as their PHY and MAC layer [1] [5].

Wireless HART: It is the wireless version of the HART (Highway Addressable Remote Transducer) protocol which is the most used in the automation and industrial applications which require real time. Wireless HART is a simple, reliable and secure protocol without the wiring costs. The implementation of it is very easy and keeps compatibility with existing HART devices, tools and systems. It supports star and mesh topologies. It is good against the electromagnetic interference. It operates at the license-free frequency band of the 2.4 GHz. In order to protect the network and the data of it uses several security techniques, such as industry standard 128-bit AES encryption and unique encryption key for each message. For the network protection, it uses channel hopping and it keeps reports authentication failures [32].

ISA - SP100: It also centers in the process and factory automation. It has been developed by the Systems and Automation Society (ISA). It is a simple and secure protocol. It is an open standard for anyone. Unlike the Wireless HART is supports multiple protocols (such as HART, Profi, Mod, FF, etc.) via a single wireless infrastructure. The implementation of it is very easy. It supports star and mesh topologies. It operates at the license-free frequency band of the 2.4 GHz. It uses channel hopping to support co-existence and increase reliability [33].

MiWi protocol: Its stacks are small foot-print alternatives to ZigBee, appropriate for cost-sensitive, low-power, low data rate and short-range wireless networking applications with limited memory. Its software is free. It supports star and mesh topologies, up to 8000 nodes and 64 hops. It has a simple architecture and it can form easily wireless networks [34].

11. Conclusions

The great development of the concept of IoT has as result the great development of wireless sensor networks. These new networks can communicate with the outside world through the internet Gateway, but this is an inefficient way. So, there was the need to create a new standard that will allow each sensor to communicate immediately with any other device located outside its own network. The solutions that are given to this end include the development of the 802.15.4standard'sfamily.

The aim of this survey work was to present the evolution of the 802.15.4 protocols. It was mainly taken into account ZigBee, 6LoWPAN, ZigBee IP and ZigBee smart energy 2.0. Also, a brief presentation of the RPL and COAP protocols was included, along with a smart home presentation.

We can say that 6LoWPAN is a pretty attractive solution because it is an IP-based protocol. However, it seems that ZigBee is more popular and has been adopted by many major industries. 6LoWPAN philosophy has been integrated by ZigBee Alliance into their own IP-based standard ZigBee IP [35].

The Smart Energy Profile 2.0 (SEP) is a standard which will be used in the smart energy market in the next years. With this protocol, one will be able to control his internal and external home energy consumption for optimized energy production, distribution, and usage.

References

[1] I. Ishaqal et al., 'IETF Standardization in the Field of the Internet of Things (IoT): A Survey'. *Mdpijournal*, vol. 2, pp. 235-287, April 2013.

[2] J. Rodrigues1 and P. Neves, 'A survey on IP-based wireless sensor network solutions', *INTERNATIONAL JOURNAL OF*COMMUNICATION *SYSTEMS*, pp. 963-981, 2010.

[3] J. Schonwalder, Internet of Things 802.15.4, 6LoWPAN, RPL, COAP, [On line]available from: http://cnds.eecs.jacobs-university.de/

[4] Radio-electronics.Com Homepage. Availablefrom:http://www.radio-electronics.com/info/wireless/ieee-802-15-4/wireless-standard- technology.php (accessed on 3 July 2015).

[5] Libelium Homepage. Available from: http://www.libelium.com/802-15-4-vs-zigbee/(accessed on 3 July 2015).

[6] J. T. Adams. 'An Introduction to IEEE 802.15.4'. IEEE, vol. 2, pp. 1-8, 2006.

[7] Digi,"Demystifying 802.15.4 and ZigBee", white Paper available on line from: www.digi.com

[8] P. Baronti. 'Wireless sensor networks: A surveyon the state of the art and the 802.15.4 and ZigBee standards'. *Elsevier*, vol. 30, pp. 1655-1695, May 2007.

[9] D. D. Vishwakarma. 'IEEE 802.15.4 and ZigBee: A Conceptual Study'. *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 1, pp. 477- 480, Sept. 2012.

[10] J. Kurose and K. Ross, 'Computer Networking A top - down approach', 6th ed., Pearson edition, 2008, pp.1-858.

[11] S.S.R. Ahamed. 'THE ROLE OF ZIGBEE TECHNOLOGY IN FUTURE DATA COMMUNICATION SYSTEMS'. *Journal of Theoretical and Applied Information Technology*, pp. 129-135, 2009.

[12] J. Olsson (2014), "6LoWPAN demystified", Texas Instruments.

[13] V. Kumar and S. Tiwari, '*Review Article:* Routing in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Survey'. *Journal of Computer Networks and Communications*, pp. 1- 10, 2012.

[14] Ukessys Homepage. Available from: http://www.ukessays.com/essays/computer- science/6lowpan-neighbor-discovery-protocol-computer-science-essay.php(accessed on 7 July 2015).

[15] M. Guines. *Embedded Internet and the Internet of Things WS 12/13*. [On line]. Available from: http://www.mi.fu-berlin.de/inf/groups/ag-tech/teaching/2012-13_WS/L_19528_Embedded_Internet_and_the_Internet_of_Things/06.pdf(accessed on 7 July 2015).

[16] Ko and A. Terzis. 'Connecting Low-Power and Lossy Networks to the Internet'. *IEEE Communications Magazine*, pp. 96- 101, April 2011.

[17] A. Ludovici et al. 'Tiny CoAP: A Novel Constrained Application Protocol (CoAP) Implementation for Embedding RESTful Web Services in Wireless Sensor Networks Based on TinyOS'. *J. Sens. Actuator Netw.* vol. 2, pp. 288-315, April 2013.

[18] M. Laine. 'RESTful Web Services for the Internet of Things'. pp. 1-3, 2011.

[19] W. Colitti, K. Steenhaut and N. De Caro. 'Integrating Wireless Sensor Networks with the Web', pp. 1-5, 2011.

[20] ZigBee (2010). The *ZigBee IP Stack IPv6-based stack for 802.15.4 networks.* [On line]. Available from: http://www.zigbee.org/what-is-zigbee/494-2/

[21] ZigBee (2013). *The New ZigBee IP specification: IPv6 Control for Low-Power*, *Low-Cost Devices* .[On line]. Available from: http://www.zigbee.org/what-is-zigbee/494-2/

[22] ZigBee Homepage. Available from: http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeeip/(accessed on 9 July 2015).

[23] Z. Zou et al. 'Smart Home System Based on IPV6 and ZIGBEE Technology'. *Elsevier*, vol. 15, pp. 1529-1533, 2011.

[24] C. Zhang, M. Zhang, Y. Su and W. Wang. 'Smart Home Design based on ZigBee Wireless Sensor Network', in proc. 7th International ICST Conference on Communications and Networking in China (CHINACOM), 2012 pp. 463-466.

[25] Green Tech Advocates Homepage. Available from: http://greentechadvocates.com/2013/04/04/zigbee-ip-smart-grid-meet-the-internet-of-things/. (Accessed on 10 July 2015).

[26] R. Simpson (April 2014). Smart Energy Profile 2.0 Overview ISO/IEC JTC 1/SC 25/WG 1. GE Digital Energy.

[27] EE Times webpage. Available from: http://www.eetimes.com/document.asp?doc_id=1280846. (Accessed on 11 July 2015).

[28] Green Peak webpage. Available from: http://www.greenpeak.com/Product/Products.html(accessed on 11 July 2015).

[29] ZigBee (2014). *ZigBee 3.0 – The Open, Global Standard for the Internet of Things.* [Online]. Available from: http://www.zigbee.org/zigbee-for developers/zigbee3-0/.

[30] ZigBee 3.0 Webpage. Available from: http://www.zigbee.org/zigbee-for-developers/zigbee3-0/(accessed on 15 July 2015).

[31] No Jitter Homepage. Available from: http://www.nojitter.com/post/240169469/the-next-zigbee-30(accessed on 15 July 2015).

[32] HART communication protocol Homepage. Available from: http://en.hartcomm.org/hcp/tech/aboutprotocol/aboutprotocol_what.html(accessed on 17 July 2015).

[33] ISA Homepage. Available from: https://www.isa.org/isa100/(accessed on 17 July 2015).

[34] Microchip Homepage. Available from: http://www.microchip.com/pagehandler/en-us/technology/personalareanetworks/technology/home.html(accessed on 17 July 2015).

[35] LSR Homepage. Available from: http://www.lsr.com/white-papers/zigbee-vs-6lowpan-for-sensor-networks(accessed on 17 July 2015).