# IEEE 802.15.4 and the Internet of things

Ketan Devadiga
Aalto University School of Science
e-mail: ketan.devadiga@aalto.fi

***Abstract*—Internet of things (IoT) is a paradigm in which everyday objects surrounding us will possess embedded computational capabilities and will be responsible for generating and sharing information. Basically, the IoT framework consists of a large number of low-power, low-cost devices which will be able to connect to each other and can be managed through some kind of mass device management system. An important aspect of the framework is the way the devices communicate with each other. IEEE 802.15.4 is a standard that defines the physical and medium access control (MAC) layers of a low-rate wireless personal area network(LR-WPAN). While IEEE 802.15.4 defines just the physical and MAC layer of the network stack, there have been other efforts such as ZigBee and 6LoWPAN that define the upper layers of the network stack.**

## I. Introduction

The IEEE 802 working group is responsible for developing standards for local area networks (LAN) and metropolitan area networks (MAN). The protocols and standards developed by IEEE 802 deals with the physical and data-link layer of the Open Systems Interconnection model (OSI model). The OSI model defines seven logical layers of a networking framework and was developed by International Organization for Standardization (ISO). The IEEE 802 divides the data-link layer into two sub-layers: Logical link control (LLC) and MAC layer. The IEEE 802 is responsible for many widely used standards such as the Ethernet (IEEE 802.3) and wireless LAN (IEEE 802.11). The IEEE 802.15.4 is a standard similar to IEEE 802.11. While the IEEE 802.11 defines standards for WLAN, the IEEE 802.15.4 is responsible for LR-WPANs. Since IEEE 802.15.4 just defines the bottom two layers of the stack, there has to be other standards that implement the upper layers. ZigBee and 6LoWPAN are some of these efforts that define the remaining upper layers over IEEE 802.15.4.

Section II gives an overview of the IEEE 802.15.4 standard. Section III and Section IV presents the ZigBee and 6LoWPAN specifications respectively. Section V provides some concluding remarks.

## II. IEEE 802.15.4

In this section, we briefly discuss the IEEE 802.15.4 standard. The original IEEE 802.15.4 standard was released in 2003. The original version supported two physical layers, one of them working in the 868 and 915 MHz frequency bands and the other working in the 2.4GHz band. Later on, there was another revision released in 2006, which improved the transfer speeds. Additional bands were added in the subsequent revisions.

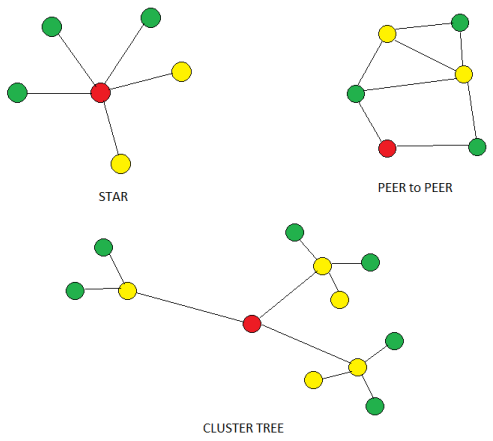


Fig. 1. Network Topologies

The IEEE 802.15.4 supports two classes of devices: Fully functional devices (FFD), which have full network functionalities and the Reduced functional devices (RFD), which possess limited functionalities. All personal area networks (PAN) consists of at least one FFD which acts as the PAN coordinator which is responsible for maintaining the PAN. RFDs are responsible for directly obtaining data from the environment and sending them to a PAN coordinator. Figure 1 shows the various topologies which a PAN can adopt. In the figure, the red devices are PAN coordinators, the yellow devices are FFDs but are not PAN coordinators and the green devices are RFDs. As seen from the figure, in a star topology, all devices directly interact with only the PAN coordinator. In a peer-to-peer topology, the FFDs can communicate with each other. In a cluster tree topology, the RFDs communicate with an FFD which in turn communicate with the PAN coordinator.

### A. Physical Layer

The original IEEE 802.15.4 standard released in 2003 adopted a wideband physical layer using Direct Sequence Spread Spectrum technique (DSSS). It provided physical layer operations in three frequency bands: the 868 MHz band, available in Europe, the 915 MHz band, available in US, and the 2.4 GHz ISM band, which is the unlicensed band available worldwide. Twenty seven channels were supported across these three bands. The 868 MHz band supported one channel, the 915 MHz band supported 10 channels and the 2.4 GHz band supported 16 channels. The three bands provide a

| Preamble | Delimiter | Header | Physical Data Service Unit (PSDU) |
|---|---|---|---|
| 4 bytes | 1 byte | 1 byte | <= 127 bytes |

Fig. 2. Physical layer packet structure

| Frame control | Sequence number | Dst Address | Src Address | Payload | Frame check sequence |
|---|---|---|---|---|---|
| 2 bytes | 1 byte | 0-20 bytes | | Variable | 2 bytes |

Fig. 3. MAC layer frame structure

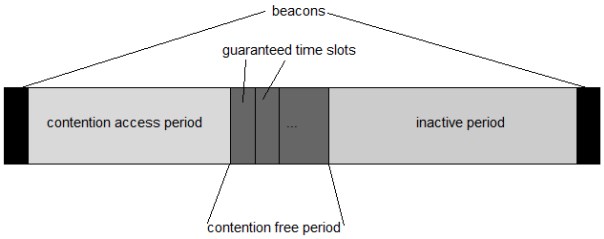


Fig. 4. Superframes in beacon-enabled networks

transmission rate of 20 kb/s, 40 kb/s and 250 kb/s respectively. In the later revisions that followed in 2006, 2007 and 2009, many additional bands were added.

The physical layer of the IEEE 802.15.4 is responsible for the following low level functions: data transfer and reception, energy detection of current channel, link quality indication and clear channel assessment. The energy detection of the receiver is used by the upper layer for their channel selection algorithm. Link quality indication (LQI) indicates the strength of the received signal. The clear channel assessment (CCA) is done based on one of the following three methods: energy detection, carrier sensing or a combination of carrier sensing and energy detection. Figure 2 shows the physical layer packet structure. The packet contains a synchronization header which is a combination of the preamble and the delimiter to indicate the start of an arriving packet. It also consists of a header that indicates the length of the payload followed by the payload. The preamble is used to get the symbol and chip timing and occasionally, for coarse frequency adjustments. Only seven bits of the header is used for specifying the length which gives a maximum length of 127 bytes for the MAC frame. Typical packet sizes for home applications are generally about 30-60 bytes whereas interactive applications require packets of larger sizes.

### *B. MAC Layer*

The MAC layer has the following features: association and disassociation, acknowledged frame delivery, channel access mechanism, frame validation, guaranteed time slot management, and beacon management. The general MAC format is shown in Figure 3. The frame control is the first field in the frame, which basically tells about the type of frame being transmitted, address format and also handles acknowledgments. There are four types of MAC frames: data frames, MAC command frames, acknowledgment frames and beacon frames. The size of the address field varies between 0-20 bytes. It might contain short 8-bit type addresses or 64-bit IEEE device addresses. The payload field is variable in size, but the size of the whole MAC frame has to be less than 127 bytes considering the size constraint of the physical layer payload. The sequence number field is used to match the acknowledgment frames. The frame check sequence is a 16-bit cyclic redundancy check (CRC) used to verify the integrity of the frame.

The IEEE standard supports two types of channel access mechanisms: non-beacon enabled and beacon-enabled. In case of non-beacon networks, the devices use unslotted carrier sensing multiple access with collision avoidance (CSMA-CA). In this mode, whenever a device wants to transfer data, it waits for a random backoff delay time, performs CCA and sends the data if the channel is found to be idle. If the channel is not idle, it waits for another random backoff delay time and repeats the process. In case of beacon-enabled networks, a slotted version of CSMA-CA is used. The concept of superframes is used in this method. Figure 4 shows a typical superframe. The PAN coordinator divides the time slots between two beacons into 16 time slots. The beacons contain information on how the data has to be transmitted during the time slots. The PAN coordinator provides dedicated bandwidth to certain devices during the contention free period (CFP) in terms of guaranteed time slots (GTS). Rest of the devices use CSMA-CA to transmit data during the contention access period (CAP). In this mode, the unit of the backoff delay time is set to the duration of the slot. Also, at the end of the backoff delay time, the devices wait till the beginning of the next time slot to perform CCA.

There are three types of security mechanisms in the IEEE standard: no security, access control lists (ACL) and symmetric key security. Each device can contain around 255 ACLs that can be used to control incoming and outgoing data. Advanced encryption standard (AES) is used to provide either confidentiality or integrity or both.

## III. ZigBee

The ZigBee alliance was established in 2002 to develop a standard protocol stack for low-cost, low-rate, low-power wireless devices. It uses the IEEE 802.15.4 standard to define its physical and MAC layer. The ZigBee alliance is a non-profit association of members aiming at the development of the standard and consists of various kinds of organizations including universities, equipment manufacturers, semiconductor companies etc.

Figure 5 shows the architecture of the ZigBee stack. From the figure, it can be seen that the physical and MAC layers are supported by the IEEE 802.15.4 standard. The network layer (NWK) is responsible for functions such as starting a network, joining and leaving a network, routing, configuration of new devices, addressing and security. The application layer

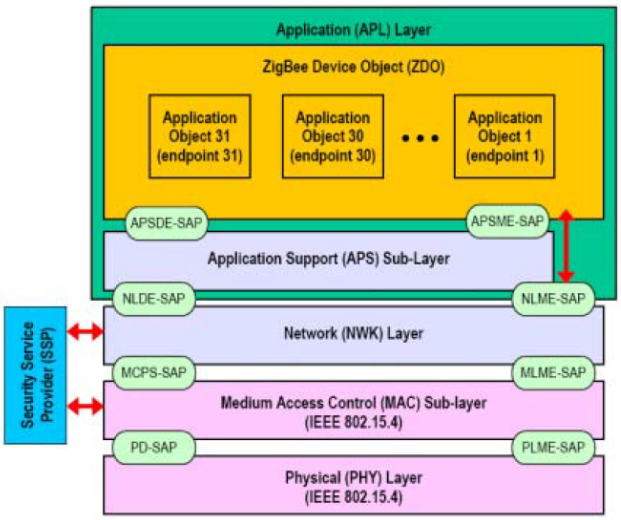


Fig. 5. ZigBee Stack [1]

is divided into application support sub-layer (APS), the ZigBee device object (ZDO) and the manufacturer defined application objects. Each application object contains software that is written by the application developer. Each application object has an end-point. For example, a remote control device will have an application object for each of its buttons. Suppose one of the button switches on a light bulb, then there has to be a binding that binds the end-point of that button and the end-point of the application object on the light bulb. These binding tables are maintained by the APS. Also, the APS is responsible for sending the message to the appropriate recipient end-point. A collection of these messages used for a particular application is called a profile. The ZDO is a special kind of application object that is present on all zigbee devices. Its task is overall device management including security policies and defining the role of the device. In addition to the MAC layer security provided by the IEEE 802.15.4, the zigbee stack provides its own security using the security services provider (SSP). It performs functions such as key establishment, key transport and authorization of devices.

## IV. 6LoWPAN

6LoWPAN is a protocol defined to enable IPv6 over IEEE 802.15.4 standard. It defines an adaption layer which employs header compression to reduce overhead, fragmentation to support the minimum MTU requirement of IPv6 and layer-2 forwarding. IPv6 packets require an MTU size of 1280 bytes. The maximum size of a MAC layer frame in IEEE 802.15.4 is 127 bytes which gives just 102 bytes for an IPv6 packet. If you take maximum security into consideration, that leaves just 81 bytes. Also, the IPv6 header is 40 bytes and the UDP header takes 8 bytes leaving 33 bytes for the application data. Hence, there is necessity of an adaption layer below IPv6 to provide fragmentation and reassembly so as to provide the MTU size required by IPv6.

In 6LoWPAN, all IPv6 packets i.e the IEEE 802.15.4 MAC layer protocol data units are encapsulated with lowpan encapsulation headers. The following types of headers are supported: dispatch header, mesh header and fragmentation header. The dispatch header defines the type of header that will follow. The mesh header indicates how to encode the hop limit and the link layer source and destination addresses. It is used to support layer-2 forwarding. The fragmentation header is used to support fragmentation and reassembly of payloads that cannot fit into an IEEE 802.15.4 MAC frame. These different headers can be stacked together in different combinations to support the needs of the network.

6LoWPAN uses two kinds of header compression: IPv6 header compression (HC1) and UDP header compression (HC2). In case of IPv6 headers, the following header fields are candidates for compression: version field, IPv6 interface identifiers, packer length, traffic class, flow label and the next header type. The only field that cannot be compressed is the hop limit. In case of UDP headers, the following fields can be compressed: source port, destination port and length. The UDP header checksum is the only field that cannot be compressed.

There can be security threats since mesh networking would be common in PANs. Adhoc routing might also be a cause for security threats. The RFC released by the working group [2] suggests to use link-layer security provided by IEEE 802.15.4 to reduce these threats. It is expected that the FFDs might communicate with off-link IPv6 peers. In such cases, usual mechanisms such as IPSec, TLS etc. should be used.

## V. Conclusion

IEEE 802.15.4 has proved to be a popular technology in case of wireless sensor networks. Though it is very similar to IEEE 802.11 (WLAN), there are certain differences that make it well suited in low-power networks. This makes it a suitable technology to be used in the internet of things framework. In comparison to 802.11, the following features makes it better suited for low-power networks: less data transmitted, less complex modulation, less frame overhead and better power management mechanisms. In case of 802.15.4, the RFDs are always in sleep mode and wake up periodically to request data from its coordinator. The coordinator stores the data till the specific RFD sends a request for the data.

The ZigBee alliance and the working group responsible for 802.15.4 worked in collaboration to develop the standard. In comparison, the 6LoWPAN specification was designed recently. The first draft of 6LoWPAN was released in 2007. The ZigBee alliance is an industry consortium supported by major players and has been quite successful. There are several examples of zigbee being used in commercial solutions. Though 6LoWPAN is a recently designed standard, it has some clear advantages over zigbee. By enabling IPv6 over 802.15.4, one can use tools that are already developed for configuring and debugging IP networks. Since the underlying technology is IP based, there exists several protocols and standards built over IP that can be explored to be employed with 6LoWPAN.

## REFERENCES


[1] P. Kinney, "Zigbee technology: Wireless control that simply works," October 2003.

[2] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," RFC 4944 (Proposed Standard), Internet Engineering Task Force, Sep. 2007, updated by RFC 6282. [Online]. Available: http://www.ietf.org/rfc/rfc4944.txt

[3] E. Callaway, P. Gorday, L. Hester, J. Gutierrez, M. Naeve, B. Heile, and V. Bahl, "Home networking with ieee 802.15.4:a developing standard for low-rate wireless personal area networks," *IEEE Communications Magazine*, August 2002.

[4] L. D. Nardis and M.-G. D. Benedetto, "Overview of the ieee 802.15.4/4a standards for low data rate wireless personal data networks," *4th workshop on Positioning, Navigation and Communication*, March 2007.

[5] G. Mulligan, "The 6lowpan architecture," *Proceedings of the 4th workshop on Embedded networked sensors*, 2007.