Zigbee

Wireless Sensors Networks

Onnig Brulez, Aude Jean-Baptiste, Romain Moulin, Marco Ribeiro Badejo

Table of contents

Introduction

Zigbee standardization

The reflexion for Zigbee started in 1998. Wireless protocols like Wifi and Bluetooth had already been standardized and Zigbee was created with the idea of being a low-power protocol for wireless personal area networks (LP-WPAN), and make a minimal use of the shared communication medium. The first drafts of the norm were submitted to IEEE in 2001. Then, in 2002, the Zigbee Alliance was created to promote Zigbee use. The norm 802.15.4, which standardizes the physical and MAC layers of Zigbee, was released in 2003.
The first commercial products including Zigbee, which is a full stack solution, were released in 2005.

Zigbee use cases

As a low-power protocol for WPAN, Zigbee has numerous applications, including in :

- smart homes & buildings
- industry
- autonomous cars
- smart cities

These applications are the main ones for quite every IoT protocol nowadays. We will see more in detail the functioning of the physical and MAC layers and if Zigbee keeps its promises of low power consumption.

Part 1: The physical layer

Physical Layer generalities

Zigbee is a wireless protocol, it uses electromagnetic waves to transmit its data. Zigbee can be used with 3 frequency bands depending on where you live : 868 MHz for Europe, 915 MHz for US / Australia and 2400 MHz worldwide.
On each band, a set number of channels is available for use : 1 for the 868MHz band, up to 13 for the 915MHz band and 16 for the 2400 MHz band

In indoor use or urban use, Zigbee range can go from 10 to 100 meters. Also it can theoretically support up to 65 000 nodes in a Zigbee network, which may vary due to various conditions such as network traffic, data rate, application requirements …

Modulation

For the modulation, we can have BPSK and O-QPSK. BPSK is a Phase digital modulation. The data is encoded through two values of phase with a phase shift of 180 degrees. It is reliable and easy to decode as there are not too many symbols possible.

O-QPSK is also a digital modulation. It is a variation of QPSK which uses 4 values of phase to encode the signal with a phase shift of 90 degrees between symbols. QPSK can shift as much as 180 degrees at a time while O-QPSK can only shift 90 degrees at a time. That means only one bit can change each time. It results in less amplitude fluctuation than QPSK and thus, enables decoding the received bits with a lower BER (bit error rate) and makes the overall transmission more reliable.

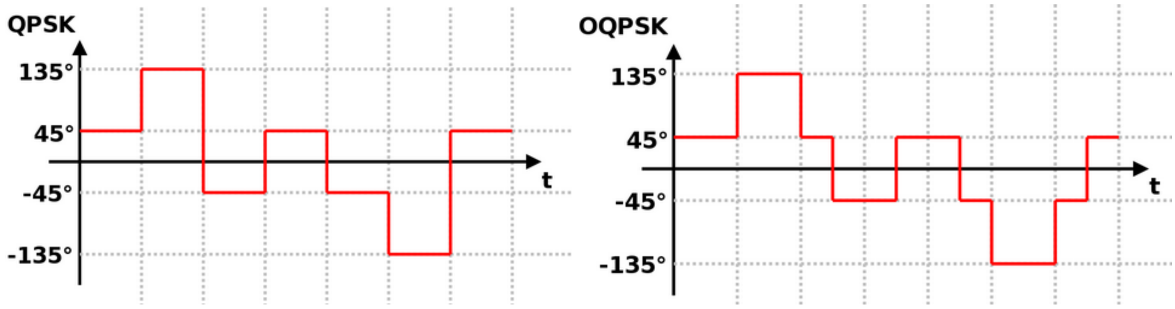

Figure 1: Phase shift response of QPSK and OQPSK signals

It also uses DSSS, which is Direct Sequence Spread Spectrum, it is a modulation technique used to reduce overall signal interference. It makes the signal use a wider bandwidth by combining it with a higher data rate spreading code. It spreads the signal across a wider frequency band and offers resistance to narrowband interference, offers a little bit of security, you need the spreading code used to modulate the signal to demodulate it and access the data.

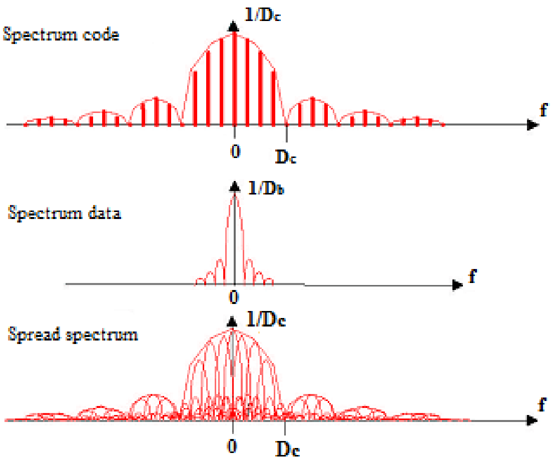

Figure 2: DSSS spreading example

DSSS is used in Zigbee because it makes Zigbee reliable even in environments with various wireless devices making it a good choice for applications such as home automation or IoT networks.

Frame Format

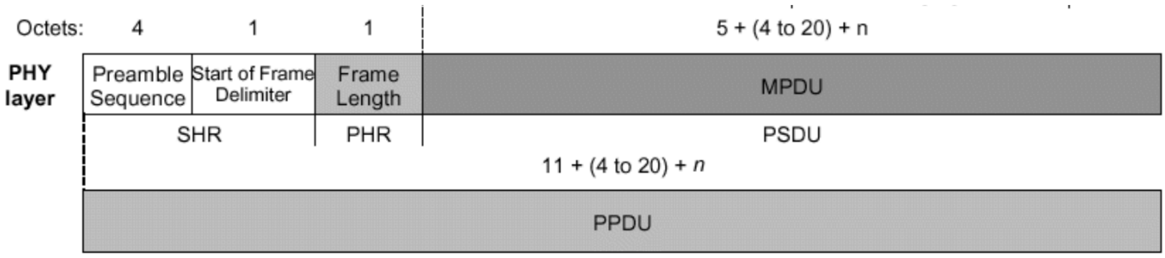

Figure 3: Zigbee's PHY Frame

- Preambule sequence is used for receiver timing recovery
- SFD indicates the end of the synchronization field
- Frame Length indicates the size of the PSDU
- The PSDU corresponds to the MAC frame which will be seen later on.

Part 2: The MAC layer

Mac Layer Generalities

As Zigbee follows the 802.15.4 norm, it implements the MAC layer specifications of the norm. Each frame is composed of 5 elements:

- The Frame control (2 bytes) : Specify the type of frame (Acknowledgement, data, beacon, command), the addresses types and the need of not for acknowledgement.
- Sequence number (1 byte) : Allows to detect frame loss or duplication
- Addresses (1-20 bytes) : Specify the source and destination addresses
- The data
- Control Sequence (2 bytes) : Define the CRC (Cyclic Redundancy Check) code to check the integrity of the frame

Because Zigbee is designed to be a low powered protocol, the bandwidth is limited. The MTU (Maximum Transmit Units) of a Zigbee frame is 127 bytes.

Frame Control	Sequence Number	Addresses	Data (Layer 3 PDU)	Frame Control

Figure 4: Zigbee's MAC frame

Medium Access

For the Medium access, Zigbee can operate in two modes.

A mode without coordination. In this mode, there is no coordinator, each node transmits when the medium seems available (no one is transmitting). It uses CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance). It is a common medium access protocol in wireless networks as it allows to limit the number of collisions. A collision in a wireless network is very

costly because it is hard for a node to detect a collision while transmitting.This operative mode is used for small networks with few devices where collisions are rare.
The difference with other wireless networks like wifi (802.11) is that we cannot reserve some resources for communication (RTS/CTS). Because Zigbee transmits short frames, the cost of implementing communication reservation is too high, that is why RTS/CTS is not available.

The other operational mode is with coordination. In this mode, a coordinator periodically sends beacons to every node to synchronize them. The coordinator also acts as a relay, if a node wants to send a frame, it will send it to the coordinator that will later transmit it to the destination. A beacon transmits information about the network as well as the message that the coordinator has received so the destination node can request this message. This allows a node to sleep between beacons when it does not need to send or receive anything and so, saving power.
Between two beacons, there is an active period and a passive period. During the passive period nothing happens. That allows every node to sleep for a moment. The active period is called a superframe. It is composed of 16 slots, the first one is always reserved for the beacon.
The rest of the superframe is divided in two parts, the CAP (Contention Access Period) which are the first slots of the superframe. During this period, nodes can contact the coordinator to send or ask to receive data. The protocol is CSMA/CA as in the first operative mode.
The remaining slots of the superframe compose the CFP (Contention Free Period). The coordinator can reserve slots for particular nodes (either to send or receive data) in order to give some bandwidth guaranties. The coordinator can make reservations for 7 nodes, each node can take one or more slots. It is important to note that the CAP part should never be empty as it allows nodes that do not need guarantees to still send data.

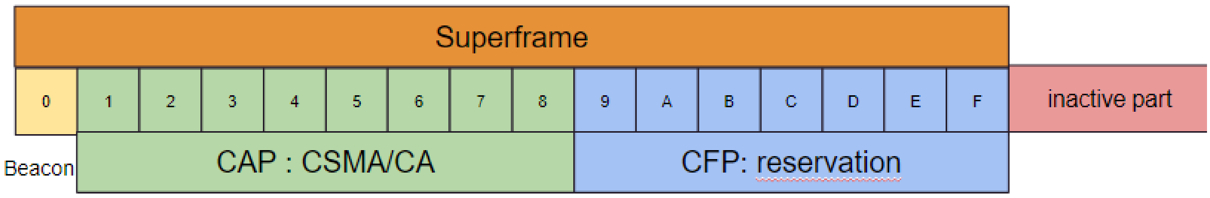

Figure 5: Zigbee's superframe with 7 slots reserved

LLC sublayer

The LLC sublayer comes between the MAC layer (Layer 2 in the OSI model) and the Network Layer (Layer 3). Its role is often to interface this two layers. A general LLC sublayer has 3 roles.

- Check the integrity of the frame : Zigbee's LLC layer does not have to do this part as it is already done in the MAC layer for the acknowledgement of the frames.
- Flow control : Zigbee implements stop and wait. It sends a frame and waits for the acknowledgement to send another frame.

- Address Convergence : Zigbee does not have to handle address convergence because Layer 2 and layer 3 addresses are the same. Indeed, Zigbee does not use IP as a layer 3 protocol but uses its own.

Part 3: The Network Layer

As mentioned in the previous part, the Zigbee Alliance introduced its own network layer for Zigbee's networks. The goal is to use a lighter protocol than IP that would be more suited for a low power and low bandwidth protocol.

The different types of nodes

In a Zigbee's network, there are 3 types of nodes :

- The Zigbee's Coordinator (ZC) : It is a unique central node for each network. It is the first node during the creation of the network. It acts as a coordinator described in part 2.
- The Zigbee's Routers (ZR) : It is a coordinator that will manage a small sub section of the network. It has to be associated with the ZC and/or other ZR. It then accepts connections from end devices. The ZRs relay the packets from the end devices using a routing protocol that we will define later.
- The Zigbee's End Devices (ZED) : It is simply the devices that need to send and/or receive data. They do not run any routing process.

The possible topologies of a Zigbee's network

Zigbee's network can be one of two types of topology.

- A tree topology : In this topology, every node is classified in a tree. The ZC is the root of the tree. Every node in the radio range of the ZC is associated with it and becomes layer 1 of the tree. The ones that are not in the radio range of the ZC connect to the nodes from the deeper layer of the tree. This process repeats until every node has a place in the tree.
- A meshed topology : With this topology, there is no logical link between nodes. The ZC stays the central node of the network but there are no rules for connection between ZRs.

Addressing in Zigbee's network

The Zigbee addressing scheme is only specified for the tree topology. In the case of the meshed topology, the addressing is free and chosen for the convenience of the upper layers. For the tree topology, the address of a node is defined depending on its depth in the tree.

Routing in Zigbee's network

Like the addressing scheme, the routing protocol depends on the topology of the network.

For the tree topology it is really simple. As the addressing scheme depends on the position in the tree, it is very simple for a node to know where to forward the packet depending on the destination address.
For the meshed topology, the routing strategy is similar to AODV (Ad-Hoc On Demand Distance Vector). When a destination node is not in the routing table, a node sends a path discovery message to every node in radio range which forwards the message to their own neighbors. When the destination ZR receives the path discovery, it replies to the ZR from which he received the message who sends it to the previous one until it reaches the source ZR. As this routing strategy is on demand, the nodes of the network do not keep in memory the topology of the network or the routes. This can lead to important routing traffic limiting the bandwidth.

Part 4: Zigbee energy consumption

Zigbee is a mature low-power protocol standard for supporting wireless smart device connectivity. Devices on wireless sensor networks need to support long battery life and a sufficient range and this is why Zigbee is used that much in IoT.

For the technicals information about Zigbee :
Operation frequency : 2.4GHz
Power transmission : -3.5dBm to +20dBm
Receiver sensibility : -92dBm

An important thing to know is that Zigbee can work in multiples states :

- Transmission : ~30mA (at 0 dBm)
- Receiving : 19 mA
- Standby : 1-2 µA
- Deep Sleep : < 1 µA

In reality, there is a consumption state, but a large part of it can be centralized as "Transmission" or "Receiving".

Mode	Current Consumption	Shortest	Longest
Sleep	1µA	?	?
Wakeup	9.5mA	1.5ms	3.7ms
Listen	30mA	360µs	340µs
Send Poll	34.5mA	760us	780µs
Listen for reply	30mA	520µs	500µs
Processing	9.5mA	460µs	500µs
Sleep	1µA	?	?
Total charge		71µC	93µC

Figure 6: Consumption in function of the Zigbee Mode on a ETRX35 Zigbee Module

The real advantage of using Zigbee is to use cycles sleep/wakeup. To give a clear example, a 1/100 cycle would mean on 100ms, you are sleeping 99ms and wake up for 1ms. It allows Zigbee to be a really low powered standard.
If we had to give a consumption/data rate ratio, it would really depend on the cycle ratio you would give to your Zigbee transmission.
We will suppose we are in a full transmission, so for a Zigbee module we will have :

- Average consumption in transmission mode : 30mA
- Voltage : 3V
- Transmission time : 1s

The energetic consumption is in Joules (J) and calculated with the formula **P = I x V x t**, where P is the power in **Watt** (**W**), I is the current in **Amperes** (**A**) and the voltage in **Volts** (**V**) and t the time in **seconds** (**s**).
For a 1 second transmission, the energy consumption would be :

Energy = 0,030A x 3V x 1s = 0,09 J

To get the ratio with the data rate, let's use the average bitrate with Zigbee : 250 kbps.

$$\text{Energy efficiency} = \frac{0{,}09\,J}{250\,000\,bps \times 1\,s} = 3.6\times10{-}7\text{J}$$

It lets us with an average consumption and an average transmission an Energy efficiency of **3.6×10^{-7} Joule / bit**.

Conclusion

Zigbee commercial and financial model

As previously said, Zigbee offers a full stack solution in which users can develop their own applications. Thus this model is particularly adapted to provide interoperability for users who choose Zigbee solutions. The CSA provides certifications that guarantee the interoperability of Zigbee devices.

The place of Zigbee in WSN and WPAN protocols today

In the world of WPAN standards, Zigbee is one of the most widely used and one of the more mature technologies. It is still in active development.

Choosing Zigbee for its low-power properties?

Zigbee keeps its promises of low-power consumption thanks to sleep / wakeup cycles. The actual power consumption by bit is **3.6×10^{-7} Joule**. The rest of the *Wireless Sensors Networks* presentations will allow us to compare this value to other WPAN protocols.
However, if you were to choose Zigbee, you should take into account that it does not implement security.

Sources

Zigbee official website: https://csa-iot.org/all-solutions/zigbee/

Technologie ZigBee / 802.15.4 - Protocoles, topologies et domaines d'application (Techniques de l'ingénieur): https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/reseaux-locaux-42292210/technologie-zigbee-802-15-4-te7508/

WPAN standards for IoT continue to develop use cases: https://www.techtarget.com/iotagenda/feature/WPAN-standards-for-IoT-continue-to-develop-use-cases

Zigbee standard Smart Energy datasheet: https://csa-iot.org/wp-content/uploads/2022/01/docs-07-5356-18-0zse-zigbee-smart-energy-profile-specification.pdf

ETRX35x ZIGBEE MODULES datasheet: https://www.silabs.com/documents/public/data-sheets/TG-PM-0516-ETRX35x.pdf

Zigbee PHY Layer : https://largo.lip6.fr/~hassan/msc57_zigbee_2011_2012.pdf

OQPSK Modulation : https://www.everythingrf.com/community/what-is-oqpsk-modulation

DSSS :
https://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum