Zigbee Communication Protocol

A case study

# Introduction

ZigBee is a short-range, energy-efficient wireless communication protocol based on the IEEE 802.15.4 standard and is maintained by a consortium of companies, universities and government agencies.

The ZigBee protocol came with the Zigbee Alliance in 2002 and now exists in different versions : ZigBee (2004/2006/2007), ZigBee PRO which defines an additional stack and features (2007/2012), ZigBee 3.0 and specific protocols such as ZigBee IP, ZigBee RF4CE, ZigBee Green Power. The Zigbee Alliance, as a non-profit association, develops open global Zigbee standard for use in the Internet of Things consumer, commercial and industrial applications. It includes companies like Amazon, Samsung, Huawei, Qualcomm, Toshiba, Silicon Labs, Philips etc. Today, Zigbee 3.0 is one of the most common wireless standards implemented in IoT devices.

Zigbee has data rates of 250 kb/s, 40 kb/s and 20 kb/s depending on the implementation. It is a Peer-to-Peer network, that is to say that different nodes can communicate with each other in a star or mesh pattern. End devices are most often low latency devices. Zigbee is a fully handshaked protocol, which increases transfer reliability. Despite this, Zigbee is a low power consumption type of communication protocol due to it’s relatively low data rate. Zigbee operates within different configurable frequency bands of operation : 16 channels in the 2.4GHz ISM\* band, 10 channels in the 915MHz ISM band and 1 channel in the European 868MHz band. This last band is particularly useful to shield from interference, as not many local networking devices operate on this band.

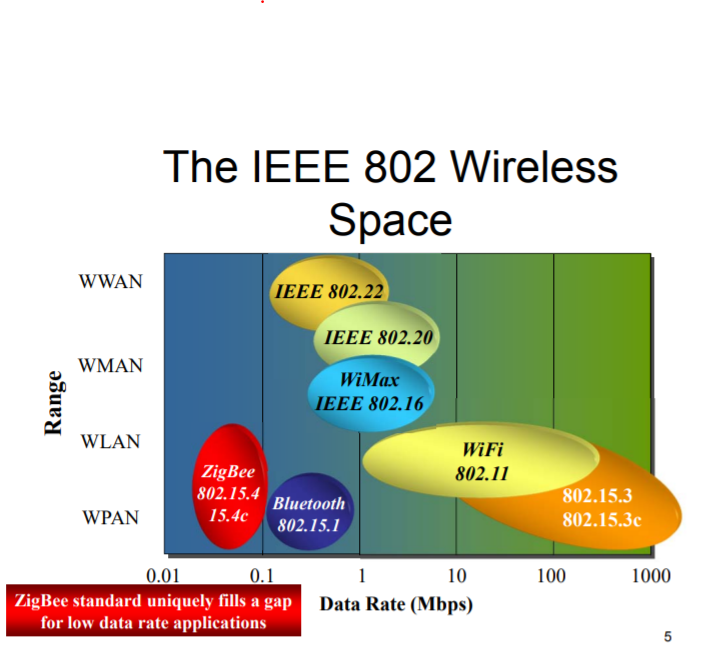
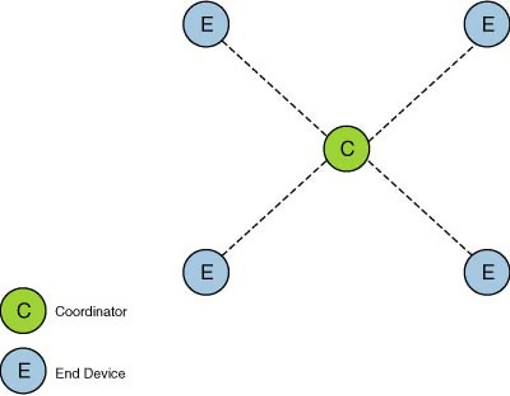


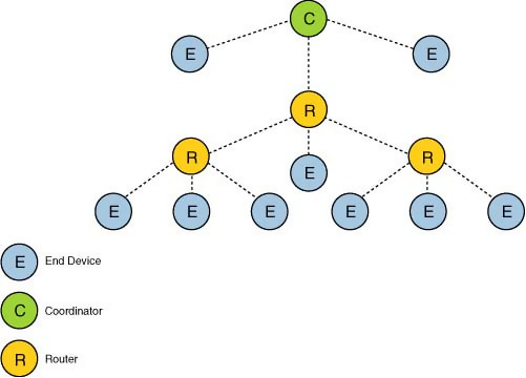
Fig 1 The 802 space : https://blog.formatis.pro/zigbee

Zigbee occupies a unique position within the 802 wireless space. These considerations aside, we will now look into the topology of the Zigbee protocol.

Below are three possible networking configurations using Zigbee:

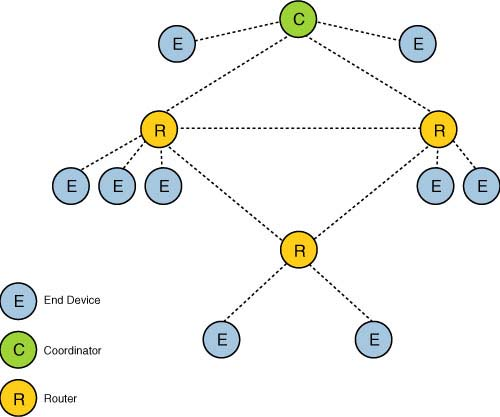
The *Star Topology* is the most simple networking option. In this topology, the coordinator is responsible for routing the packets in the network. End devices can communicate only via the coordinator. Star topology has the weakness of having a single point of failure but is the easiest to put into place. packets go through at most two hops to reach their destination.

Fig 2 : Star Topology, source 1 in bibliography



The *Tree Topology* uses a hierarchical routing strategy. An end device can be a child to a coordinator or a router and can communicate to another end device only via a router or a coordinator. This topology has the risk of an end device being unreachable if a parent node shuts down. It is a multihop topology.

Fig 2 : Tree Topology, source 1 in bibliography



*Mesh Topology* allows full peer-to-peer communication. It has a single coordinator, multiple routers to extend the network, and end devices. This topology has the advantage of being self-healing, meaning during transmission, if a path fails, the node will find an alternate path to the destination. Devices can be close to each other so that they use less power. However mesh routing uses a more complex routing protocol than a star topology and is also more expensive.

Fig 3 : Tree Topology, source 1 in bibliography

Let’s now look into how the protocol is actually implemented, by looking into the Zigbee stack and how Zigbee is put into place using the physical layer, the MAC layer while considering the aspects of security and power consumption.

# 

# Physical layer usage for the Zigbee protocol

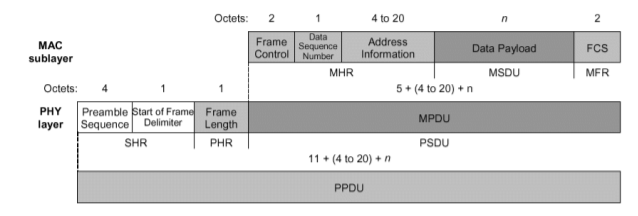
1. IEEE 802.15.4 standard

The physical layer of the zigbee protocol has several tasks. It can activate or deactivate transceivers, a low duty cycle saves energy and some components can last a few years with a small battery. PHY listens to channels and declares availability or not. This layer permits transmitting and receiving data. The signal can reach 30m inside and up to 100m outside.

As the zigbee protocol is based on the IEEE 802.15.4 standard, there are two different physical layers. The first one is 868 MHz (in Europe) or 915 MHz (in US and Australia). The second used worldwide, 2.5 GHz. Each bandwidth has different characteristics. Here is a board presenting the differences.

| Bandwidth | 868 MHz | 915 MHz | 2.5 GHz |
| --- | --- | --- | --- |
| Channels | 1 | 10 | 16 |
| Channel spacing | - | 5 MHz | 5 MHz |
| Rate | 20 kbps | 40 kbps | 250 kbps |

1. Zigbee PHY packet structure



The packet structure of the PHY layer begins with a preamble sequence on 4 octets. This sequence is only composed of zeros (32 zeros). This preamble is used for synchronization, timer receiving recovery. Next, there is a SFD (Start Frame Delimiter) on 1 octets, the purpose is to segregate the preamble and the frame length which follow, it indicates the end of the synchronization field. Then there is the PSDU, which contains several elements including the payload. The PSDU can not exceed 127 bytes.

1. Modulation

Zigbee uses the OQPSK modulation to transmit the signal. *Offset quadrature phase-shift keying* (*OQPSK*) is a variant of phase-shift keying modulation using four different values of the phase to transmit. It is sometimes called *staggered quadrature phase-shift keying* (*SQPSK*).

The aim is to modulate two waves, with different phases, then we transmit the sum of the two waves. With four possible phases, QPSK can encode two bits per symbol.

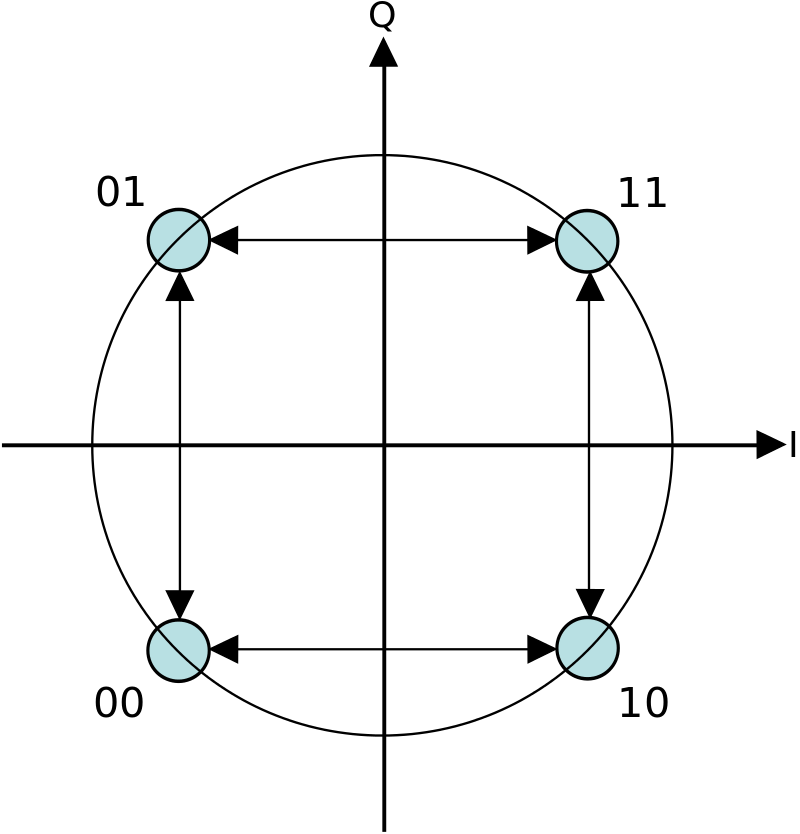
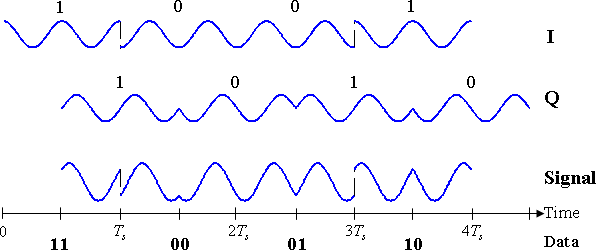


fig1. Timing Diagram for OQPSK fig2. Constellation Diagram

In the constellation diagram shown, we can see that this will limit the phase-shift to no more than 90° at a time. This yields much lower amplitude fluctuations than non-offset QPSK and is sometimes preferred in practice.

# 

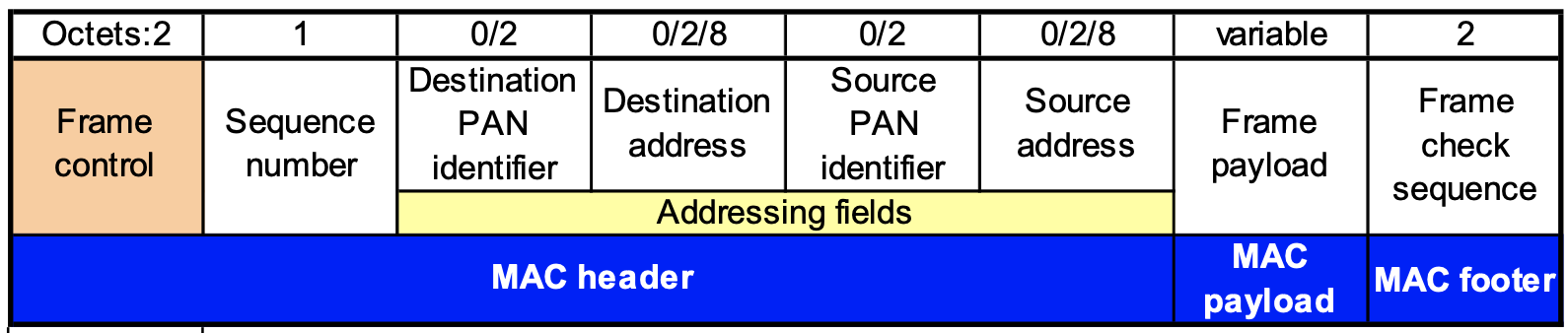
# MAC layer usage

Zigbee is built on the Medium Access Control (MAC) sub-layer defined in the IEEE 802.15.4 standard. It is located between the physical and network layers. It enables the transmission of MAC frames through the use of the physical channel.

The MAC layer performs **multiple functions** :  
→ Transfers data to the network layer and vice versa; transfers data to the physical layer and vice versa  
→ Manages access to the physical channel and network beaconing.   
→ End device association and dissociation  
→ In the coordinator, offers optional guaranteed time slot (GTS) for each device accessing the network (in beacon-enabled mode)  
→ Generates the beacon frame in a coordinator (if operating in beacon-enabled mode)  
 ***Beacon*** *: special frame sent by the PAN coordinator in order to synchronize with other units*→ Supports device security  
→ Lowers power consumption through beacon enabled mode since units can be put to “sleep” between being “woken up” by beacons.  
→ Provides carrier-sense multiple access with collision avoidance (CSMA/CA) as the access method for the network  
→ Offers an AES-128 security  
→ Provides a reliable connection between two MAC layers by using an acknowledgment thus providing a reliable data transfer

It is a simple but flexible protocol for which there are two IEEE 802.15.4 Device classes : FFD (Full function device) and RDF (Reduced function device). The former can use any topology, is capable of PAN coordinating and implements a complete protocol set, while the latter is limited to star topology or end-device in a peer-to-peer network, cannot become a PAN coordinator and implements a reduced protocol set.

It uses a simple structure of frame and there are 4 types of MAC Frames (Data Frame, Beacon Frame, Acknowledgement Frame and MAC Command Frame), this is the general MAC Frame format:



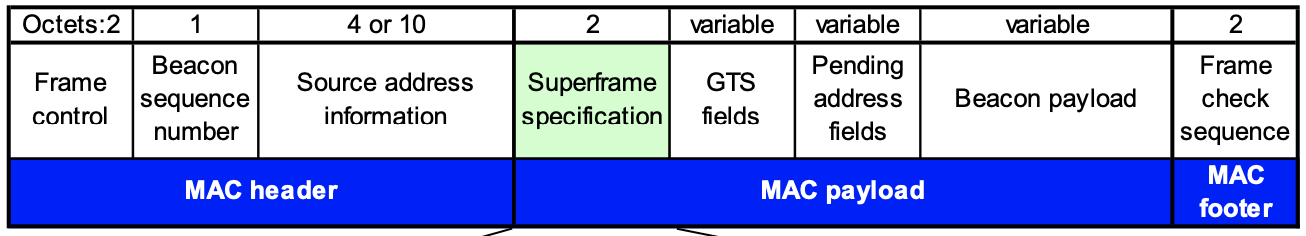
Generic MAC layer frame has a frame control field of 2 octets. It carries useful information such as frame type, source and destination addressing modes. Frame type specifies whether the frame is beacon frame,data frame, ACK of data, MAC command frame etc.

There are two 802.15.4 Channel access options : Non beacon network and beacon enabled network.

Non-beacon network is a simple, traditional multiple access system used in simple peer and near-peer networks. It uses standard CSMA-CA communications, and provides a positive acknowledgement for successfully received packets.

Beacon-enabled network has a network coordinator that transmits beacons at predetermined intervals. The superframe may be split between contention access period, contention free period (containing guaranteed time slots (GTS)), and inactive period. The beacon mode is also powerful for controlling power consumption in extended networks. It allows all clients in a local piece of network the ability to know when to communicate with each other. Finally, the PAN coordinator manages the channel and arranges the calls.

**Beacon Frame Format :**

****

# Security considerations of the Zigbee protocol

The level of security offered by the ZigBee security architecture depends on the protection of symmetric keys, the protection mechanisms used, and the proper implementation of cryptographic mechanisms and security policies.

ZigBee uses some of the security features of the 802.15.4 standard which are detailed in the previous article. It extends the functionality of this standard by using :

* 128-bit AES encryption keys;
* definition of different keys to secure communications: Master, Link, Network;
* use of the CCM algorithm;
* use of a Trust Center (TC);
* security that can be customised per application.

Although several security protections are present on the MAC layer of the 802.15.4 standard, the ZigBee protocol also integrates security considerations in the network and applicative layers.

A 128-bit AES key is used to encrypt/decrypt packets. All devices that are allowed to join the network must have a copy of this key. A sequence number is usually associated with the key to identify the instance.

Each router that has to transfer an encrypted packet must first check whether the packet is valid. To do this, the router decrypts the packet and checks its integrity. If the packet is valid, it encrypts the packet again before forwarding it to the next router or to the end equipment.

The ZigBee Trust Center (ZTC or TC) is usually the coordinator (ZC) of the network, but can also be a dedicated device. It is trusted by all other devices and is responsible for the following security features

* trusted manager: to authenticate devices wishing to join the network;
* network manager: to maintain and distribute network keys;
* configuration manager: to enable end-to-end security between devices.

3 types of keys are used by ZigBee to ensure the security of exchanges:

* Link Key: key only shared between two devices to protect frames on the APS layer;
* Network Key: key used to perform network layer actions (routing, request to join the network, etc.) and to prevent illegitimate insertion of a device;
* Master Key: used to share the initial secret between two devices when they perform the key establishment procedure (SKKE) to generate the Link Key.

In order to establish the keys, several methods can be used by manufacturers such as pre-installation on the equipment or transport as well as establishment: equipment negotiates with the trust centre to establish the keys without them being transported. This happens using one of these three techniques:

* SKKE (Symmetric-Key Establishment) ;
* CBKE (Certificate-based Key Establishment);
* ASKE (Alpha-secure Key Establishment).

The SKKE exchange generates the Link Key based on the Master Key. Therefore, if the Master Key is compromised, publicly known or left as a default, the Link Key establishment is also compromised.

Although these safeguards are sufficient for protection against various attacks, not all of them are necessarily implemented by manufacturers, which creates multiple threats to devices using this protocol. That said, Zigbee provides solid security for a WPAN protocol thanks to built in functionalities.

# 

# Power consumption of Zigbee protocol

1. Zigbee : a low consumption protocol

As we said, the Zigbee protocol is used for sensor networks because of his low energy consumption for a maximum data rate of 250kB/s (at 2.4GHz but can also work at 868 Mhz in Europe and 915Mhz in Australia and America with lower theoretical data rates). In order to evaluate power consumption of a Zigbee-based sensor network you need to consider the system which is not only based on your sensor nodes and gateway but also rely on the routers to work.

How is he saving energy? Using some features of IEEE 802.15.4

• Duty-cycle control using superframe structure (Beacon order and superframe order, coordinator battery life extension)

• Indirect data transmission

• Devices may sleep for extended period over multiple beacons

• Allows control of receiver state by higher layers

The idea is to set the right duty cycle for your application so you can save energy since the standby mode consume really low power :

1. Exemple of consumption in WSN network (2.4GHz and CC2530 ZigBee development kit) :

To illustrate the efficiency of Zigbee protocol we can look for consumption of a sensor node in a simple WSN counting 7 sensors, 1 router and 1 gateway :

-In power mode : during a couple of seconds when turning on your sensor try to establish connection with the router and gateway before communicating periodically with it. The power consumption during this time is around 0.2A. The time of power mode will grow with the complexity of the WSN.

-Reporting data without acknowledgement (only MAC ACK) : around 10^-4 J during 0.01 s

-Reporting data with acknowledgment : add 10^-3J for 0.100 sec (default time).

But we can also interest us on the consumption of the router, since all the nodes routing th or “hoping” the message need to be powered :

-In power mode : Preparing configuration and finding route to gateway it consumes 0.0566 J for 1 second.

-After power up : Average around 0.3A.

With this information and knowing that ZigBee messages are 128 bytes long and a maximum of 100 bytes for the payload (without security option) we can approximate the energy per byte to 10^-7J/Bytes for transmitting + 0.2A during the power up time. This is for the sensor node at the end of the network but all the nodes transmitting (router and coordinator )the message need to be awake thus, they can’t have energy limitations.

1. Comparison with other protocols

In order to get some comparaison, Zigbee tends to consume a bit more than BLE, but nearly 5 times less than wifi, a protocol transmitting much more data, as we can see on the energy test made bellow with an ESP82 device :

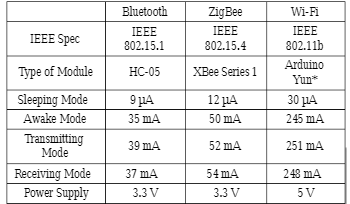


Figure 1. Comparison of consumption of ESP82 with different protocols

It is also important to note that the topology of the sensor network can also impact the energy consumption : star, mesh or tree topology are 3 different topologies allowed with ZigBee.

# Conclusion

This report allows us a better understanding of the ZigBee protocol based on the IEEE 802.15.4. He is the first protocol from a consortium with such a low power consumption and integrating all the features useful for a Wireless Sensor Network. Today, he is a bit less used in industries with the appearance of BLE which is used for the low range applications since he has a better rendement. He is a good solution to work with routers that don’t have consumption constraints and a final sensor node in standby most of the time. It is also quite easy to implement since it can reconfigure itself automatically and dynamically allowing around 65000 nodes and a network with a size of a couple of kilometers.

Bibliography

ZigBee Wireless Sensor and Control Network, Ata Elahi, Adam Gschwender, Oct 29, 2009, Pearson. ISBN-10: 0-13-713485-1, ISBN-13: 978-0-13-713485-4

Song, Jiaying; Tan, Yen Kheng (2012). *[IEEE 2012 IEEE International Conference on Communication Systems (ICCS) - Singapore, Singapore (2012.11.21-2012.11.23)] 2012 IEEE International Conference on Communication Systems (ICCS) - Energy consumption analysis of ZigBee-based energy harvesting wireless sensor networks. 468–472.* doi:10.1109/ICCS.2012.6406192

*Comparative Study of Communication Interfaces for Sensors and Actuators in the Cloud of Internet of Things* Olaide O. Kazeem, Olubiyi O. Akintade\*, Lawrence O. Kehinde Department of Electronic and Electrical Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria

A Effective Method for Properties Access in MAC Layer of ZigBee, January 2011Communications and Network 03(03):149-152, DOI:10.4236/cn.2011.33018, Qi-Yong Pan

<https://www.researchgate.net/publication/271292667_A_Effective_Method_for_Properties_Access_in_MAC_Layer_of_ZigBee>

Smain Femmam, ... Laurent George, in *Building Wireless Sensor Networks*, 2017

<http://www-soc.lip6.fr/~hassan/msc57_zigbee_2011_2012.pdf>

<https://www.rfwireless-world.com/Terminology/QPSK-vs-OQPSK-vs-pi-4QPSK.html>

<https://en.wikipedia.org/wiki/Phase-shift_keying#Offset_QPSK_(OQPSK)>

<http://robert.cireddu.free.fr/SIN/Protocole%20ZigBee.pdf>

Zigbee functional descriptor graphic

<https://mmbnetworks.atlassian.net/wiki/spaces/SKB/pages/39518242/Zigbee+Network+Concepts>