# Zigbee

## Protocol study

Maxime Arens, Vincent Erb, Baptiste Schersach
5ISS - A1

Tutor: Daniela Dragomirescu

## Contents

# 1 Introduction

Zigbee is a high level protocol, mainly used for communication between small, low-power devices. It is based on the IEEE 802.15.4 standard for physical and MAC layers, and developed by the Zigbee Alliance foundation, gathering huge industrial actors like Amazon, NXP or Comcast. The protocol was conceived in 1998 and standardized in 2003, so it is one of the early actors in the domain of IoT protocols. It is low-power, low-bandwidth and close proximity, so it aims at small-scale projects like home automation or medical device data collection.

# 2 Physical & MAC Layer

PHY (Physical Layer) Defines the physical operation of the Zigbee device including receive sensitivity, channel rejection, output power, number of channels, chip modulation, and transmission rate specifications. Most Zigbee applications operate on the 2.4 GHz ISM band at a 250 kb/s data rate.

MAC Manages RF data transactions between neighboring devices (point to point). The MAC includes services such as transmission retry and acknowledgment management, and collision avoidance techniques (CSMA-CA).

The ZigBee protocol uses the 802.15.4 standard to define the PHY and MAC layers, the frequency, signal bandwidth and modulation techniques are identical.

## 2.1 Generalities

COMPARISON OF THE BLUETOOTH, UWB, ZIGBEE, AND WI-FI PROTOCOLS

| Standard | Bluetooth | UWB | ZigBee | Wi-Fi |
|---|---|---|---|---|
| IEEE spec. | 802.15.1 | 802.15.3a * | 802.15.4 | 802.11a/b/g |
| Frequency band | 2.4 GHz | 3.1-10.6 GHz | 868/915 MHz; 2.4 GHz | 2.4 GHz; 5 GHz |
| Max signal rate | 1 Mb/s | 110 Mb/s | 250 Kb/s | 54 Mb/s |
| Nominal range | 10 m | 10 m | 10 - 100 m | 100 m |
| Nominal TX power | 0 - 10 dBm | -41.3 dBm/MHz | (-25) - 0 dBm | 15 - 20 dBm |
| Number of RF channels | 79 | (1-15) | 1/10; 16 | 14 (2.4 GHz) |
| Channel bandwidth | 1 MHz | 500 MHz - 7.5 GHz | 0.3/0.6 MHz; 2 MHz | 22 MHz |
| Modulation type | GFSK | BPSK, QPSK | BPSK (+ ASK), O-QPSK | BPSK, QPSK COFDM, CCK, M-QAM |
| Spreading | FHSS | DS-UWB, MB-OFDM | DSSS | DSSS, CCK, OFDM |
| Coexistence mechanism | Adaptive freq. hopping | Adaptive freq. hopping | Dynamic freq. selection | Dynamic freq. selection, transmit power control (802.11h) |
| Basic cell | Piconet | Piconet | Star | BSS |
| Extension of the basic cell | Scatternet | Peer-to-peer | Cluster tree, Mesh | ESS |
| Max number of cell nodes | 8 | 8 | > 65000 | 2007 |
| Encryption | E0 stream cipher | AES block cipher (CTR, counter mode) | AES block cipher (CTR, counter mode) | RC4 stream cipher (WEP), AES block cipher |
| Authentication | Shared secret | CBC-MAC (CCM) | CBC-MAC (ext. of CCM) | WPA2 (802.11i) |
| Data protection | 16-bit CRC | 32-bit CRC | 16-bit CRC | 32-bit CRC |

* Unapproved draft.
• Acronyms: ASK (amplitude shift keying), GFSK (Gaussian frequency SK), BPSK/QPSK (binary/quardrature phase SK), O-QPSK (offset-QPSK), OFDM (orthogonal frequency division multiplexing), COFDM (coded OFDM), MB-OFDM (multiband OFDM), M-QAM (M-ary quadrature amplitude modulation), CCK (complementary code keying), FHSS/DSSS (frequency hopping/direct sequence spread spectrum), BSS/ESS (basic/extended service set), AES (advanced encryption standard), WEP (wired equivalent privacy), WPA (Wi-Fi protected access), CBC-MAC (cipher block chaining message authentication code), CCM (CTR with CBC-MAC), CRC (cyclic redundancy check).

## 2.2 Bandwidth

Zigbee counts on the IEEE (Institute for Electrical and Electronics Engineers) who specify differents bandwidth and types of modulation Historically , these 3 are proposed:

2.4 GHz (worldwide): 250 kbit/s.
915 MHz (America and Australia): 40 kbit/s.
868 MHz (Europe): 20 kbit/s
Estimated range from 10 to 75 m, can be up to 1 500 with Zigbee PRO, with a power of 0 dBm (1 mW)

Pratically, it is more the 2.4GHz who is used for the obvious reason of the worldwide compatibility

## 2.3 Modulation

The Zigbee protocole uses the BPSK (Binary phase-shift keying) and also the OQPSK
Offset Quadrature phase shift keying (OQPSK) is another modulation technique, and it's a particularly interesting one because it actually transmits two

bits per symbol. In other words, a OQPSK symbol doesn't represent 0 or 1—it represents 00, 01, 10, or 11. It is possible because the carrier variations are not limited to only 2 states (0 or 1), like in ASK (Amplitude shift keying).We have 360 of phase to work with and four phase states, and thus the separation should be 360/4 = 90. So our four OQPSK phase shifts are 45, 135, 225, and 315.

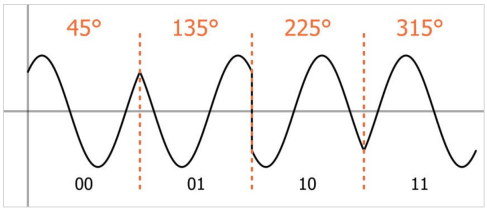


Figure 1: Different phase of QPSK

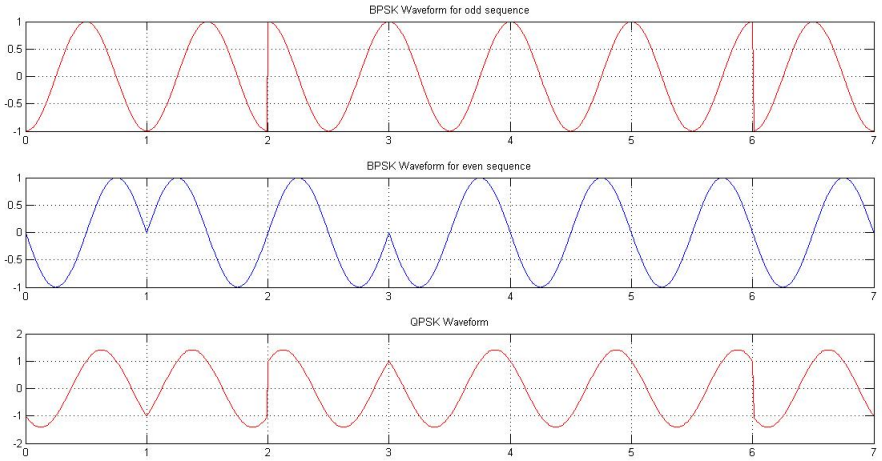


Figure 2: BPSK and QPSK waveforms

From 868MHz to 868,6 it uses BPSK
From 902MHz to 928MHz it also uses BPSK
In 2450 MHz it uses O-QPSK

## 2.4 Datarate

Data Rate : The raw, over-the-air data rate is 250 kbit/s per channel in the 2.4 GHz band, 40 kbit/s per channel in the 915 MHz band, and 20 kbit/s in the 868 MHz band as shown before.

## 2.5 Channel access & MAC layer

The Medium Acces Control layer is the interface between the physical and the network layer.

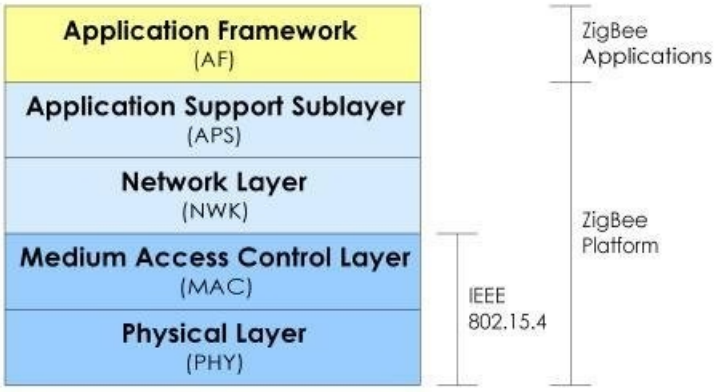


Figure 3: The Zigbee Architecture

The MAC layer implement various functions to handle and manage data by adding destination addresses and transmits options to the outgoing data frames.

We can list some functionalities of the MAC layer :

- For "Data Request" the data is formatted with a correct MAC header and physical header (with the frame length)
- For "Data Confirm" (transmit the status of the transmitted data), the MAC layer manage the validation and acknowledgment by sending a fail status if the frame exceeds or if there is no response to the transmitted data.
- The beacon generation and management (the "I'm here" function).
- The Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) to access the network.
- The Guaranteed Time Clot management (GTS) for real-time requirements of some devices.. . .

ZigBee channels exist in the same frequency band (2.4 GHz) as some Wi-Fi channels. As we can see below, ZigBee and Wi-Fi channels overlap a lot.

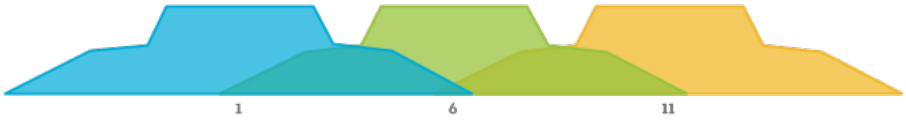


Figure 4: Wi-Fi channels

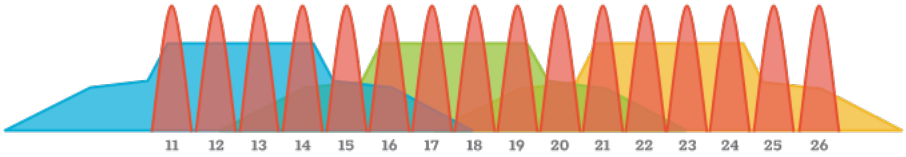


Figure 5: ZigBee channels

Because Zigbee has a low power spectral density compare to Wifi it's mostly Zigbee that suffers from this cohabitation.

In order to limit the interference, if you have control on the Wifi system responsible you can disable the 11 channel (yellow one) and use Zigbee channels 24 to 26 without interference.

## 2.6 Localization

Localization in wireless sensor networks is important because the source of incoming measurements is in itself an information.

Some algorithms like WCL (Weighted Centroid Localization) calculates the position of devices in a network by averaging the coordinates of known reference points.

Because Zigbee provides a quality indicator of a received packet (the Link Quality Indication) it is also possible to estimate a distance from a node to reference points (in addition to the use of the Received Signal Strength Indicator that the receiver can calculate).

# 3 Security

Zigbee was conceived with the importance of security in mind. However, trade-offs had to be made to keep the devices low-cost, low-energy and interoperable. Some parts of the standard's security controls are poorly implemented, which inevitably leads to security risks. In this section, we will highlight the main security mechanisms implemented and common attacks possible on the standard.

## 3.1 Security mechanisms

The Zigbee Alliance claims that their standard includes state-of-the-art security measures for wireless IoT. It uses a symmetric-key cryptography, meaning that the two parties must share the same key to communicate.
The encryption used is AES 128 bit, highly regarded and considered one of the best systems availbable today. Because it aims to be a low-cost protocol, Zigbee opts for an "open trust" model, where protection only exists between devices, but the different layers (Physical, MAC, Network, Application) all share the same key freely. This works with the assumption that the layer where originates a frame is responsible for its security.

Zigbee offers counter-measures to two important attacks:

- It includes a frame counter to stop replay attacks, where the attacker can record a message and try to re send it.
- It supports frequency agility, useful to avoid jamming attacks notably.

The protocol also proposes two network architectures to ensure security: First, a decentralized model where a router can establish a secured network if it does not find any already in place. Each router can issue network keys, and as nodes and routers join, they can exchange their keys. Second, the centralized model uses another device type, the "Trust center" (TC), holding the network key and establishing a secure connection with each node.

## 3.2 Weaknesses & Common attacks

Despite the best efforts to keep the protocol secure, well known attacks can be conducted on nodes, depending on hardware and application software present.

**Killerbee**
Killerbee is a python framework designed to exploit various vulnerabilities of the Zigbee standard. It offers many options, such as key sniffing, network traffic injection, packet decoding and manipulation, or even denial of service by crashing a device.

**Key sniffing**
Even without using a tool suck as Killerbee, it is possible to conduct key sniffing

on some infrastructures. Indeed, in centralized infrastructures using a TC, if the default link key from the TC has not been changed by the system administrator (ZigBeeAlliance09), you can decode all the traffic in clear.

**Worm attack on Philips Hue lightbulbs**
In 2016, a group of researchers conducted a coordinated attack on Philips Hue network using drones. They were able to turn lights on and off at a 400m distance, exploiting hard-coded keys in the network. The Zigbee Alliance claimed that the vulnerability was not part of their standard, but an implementation error from Philips. From this attack, we can see that even though the Zigbee Alliance tries its best to ensure the security of its standard, they do not have complete control over how other companies implement the protocol and some erroneous implementation can lead to security weaknesses.

# 4 Energy

In this section, we are going to look at the energy consumption from two perspectives. First, we are going to look at what Zigbee announces for its power consumption and some examples. Then, we will study the Energy per bit metric, which will give a more objective indication.

## 4.1 Power consumption and sleep mode

Zigbee is considered a low-power protocol. The Zigbee Alliance goes to great lengths to promote it, it is one of if not the most important element they want to put forward. It is designed to be used on battery-powered devices, so the focus is clearly justified.
The most important element that is highlighted is the sleep mode cycles and duration. Everything is done so that a device gets awake for the most limited time as possible, and directly goes back to sleep afterwards. This is done by different techniques, among which optimizing warmup time of the chip so that it can function as fast as possible for example.

## 4.2 Energy per bit

By combining and trying to optimize all the factors influencing the Energy per bit indicator, researchers managed to get it down to a very low level, going below 2mJ per bit.

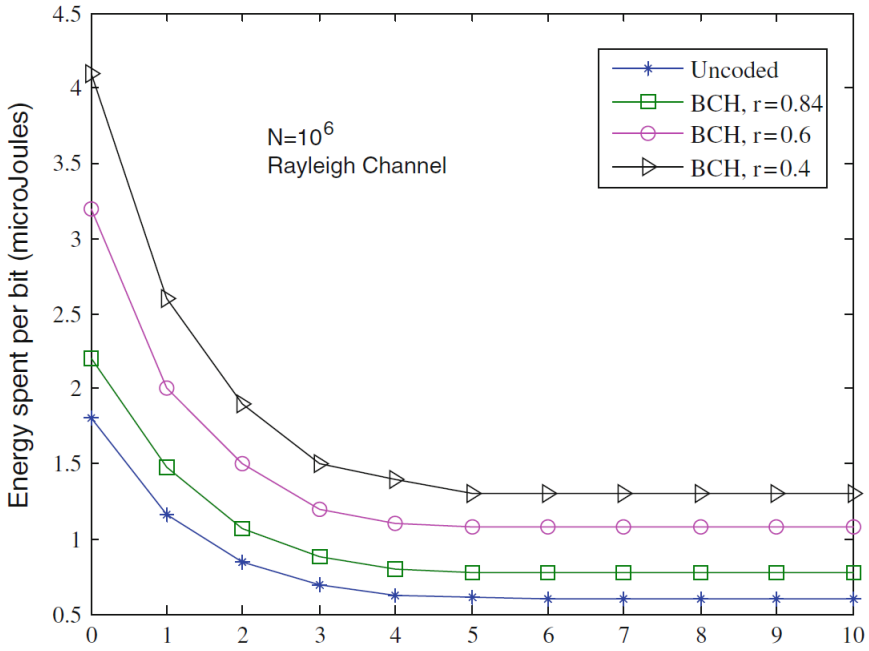


Figure 6: Energy per bit for different BCH coefficients [10]

# 5 Conclusion

ZigBee is a low consumption protocol used to connect devices on short distances. It's supposed to be easier and cheaper than bluetooth (a protocol with a similar use). As we saw the protocol is no exempt of weakness such as interference with Wi-Fi and security holes.

# References


[1] *(PDF) ROUTING SCHEMES FOR ZIGBEE LOW-RATE POWER PERSONAL AREA NETWORK: A SURVE*. URL: https://www.researchgate.net/publication/322519283_Routing_Schemes_for_ZigBee_Low-Rate_Power_Personal_Area_Network_A_Surve (visited on 01/07/2020).

[2] *802.15.4 power consumption - Recherche Google*. URL: https://www.google.com/search?client=firefox-b-d&q=802.15.4+power+consumption (visited on 01/07/2020).

[3] Laxmi Ashrit. *ZIGBEE Architecture (ZIGBEE Stack) - All Layers and its Functions*. en-US. Dec. 2018. URL: https://electricalfundablog.com/zigbee-architecture-zigbee-stack-layers/ (visited on 01/07/2020).

[4] Laxmi Ashrit. *ZIGBEE Architecture (ZIGBEE Stack) - All Layers and its Functions*. en-US. Dec. 2018. URL: https://electricalfundablog.com/zigbee-architecture-zigbee-stack-layers/ (visited on 01/07/2020).

[5] Nicolas Beilleau and Hassan Aboushady. "ZigBee IEEE 802.15.4 PHY Layer". en. In: (), p. 13.

[6] R Cireddu. "Protocole ZigBee". fr. In: (), p. 8.

[7] Ata Elahi and Adam Gschwender. "Introduction to the ZigBee Wireless Sensor and Control Network". In: Dec. 2009. URL: http://www.informit.com/articles/article.aspx?p=1409785&seqNum=7 (visited on 01/07/2020).

[8] Xueqi Fan et al. "Security Analysis of Zigbee". en. In: (), p. 18.

[9] Xueqi Fan et al. "Security Analysis of Zigbee". en. In: (), p. 18.

[10] Nicolas Fourty, Adrien van den Bossche, and Thierry Val. "An advanced study of energy consumption in an IEEE 802.15.4 based network: Everything but the truth on 802.15.4 node lifetime". en. In: *Computer Communications*. Special issue: Wireless Green Communications and Networking 35.14 (Aug. 2012), pp. 1759–1767. ISSN: 0140-3664. DOI: 10.1016/j.comcom.2012.05.008. URL: http://www.sciencedirect.com/science/article/pii/S0140366412001703 (visited on 01/07/2020).

[11] Ralf Grossmann et al. "Localization in Zigbee-based Sensor Networks". en. In: (), p. 8.

[12] *Phase-shift keying - Wikiwand*. URL: https://www.wikiwand.com/en/Phase-shift_keying (visited on 01/07/2020).

[13] Brian Ray. *A Bluetooth & ZigBee Comparison For IoT Applications*. en-us. URL: https://www.link-labs.com/blog/bluetooth-zigbee-comparison (visited on 01/07/2020).

[14] Daniel Vaquerizo-Hdez et al. "A Low Power Consumption Algorithm for Efficient Energy Consumption in ZigBee Motes". In: *Sensors (Basel, Switzerland)* 17.10 (Sept. 2017). ISSN: 1424-8220. DOI: 10.3390/s17102179. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5677289/ (visited on 01/07/2020).

[15] *ZigBee and WiFi Coexistence — MetaGeek*. URL: https://www.metageek.com/training/resources/zigbee-wifi-coexistence.html (visited on 01/07/2020).