Zigbee protocols and features

Ali Molajani

September 6, 2020

1 Introduction

Zigbee is a one of the useful protocols in home automation Zigbee have it's own IEEE standard:IEEE 802.15.4 which lays down specification for low rate wireless personal area network Zigbee modules is could connect to most known boards and chips including AVRs and ARMs and also it is could work with raspberry pi & ardunio also.

2 About Zigbee it self

2.1 Abstract How To!

zigbee is low power & it has less handshaking protocol it's open-source and lots of companies build modules with zigbee standard one of problem of this protocol is "working with phone or other devices" and it is get connected using "**mesh method**" that means it makes a mesh of the exsiting devices to connect to the hub and then send data to cloud and then to your phone or your account.the more dvices you have the more reliable your network become.

but cosider this if you pay attention to your privacy the better idea is using local hubs (means not connected to internet).

other problem usually occurs is the products of diffrent companies aren't match with the others! that means if your zigbee network is using two companies products you have know that their network may not work with each other and they have their own network and hub! that means you have two sprated mesh with no connection.

Zigbee & WIFI both working in 2.45 GHz with is good in speed and scientificly safe for human health but the zigbee modules has much less prices in comparison with WIFI ones.

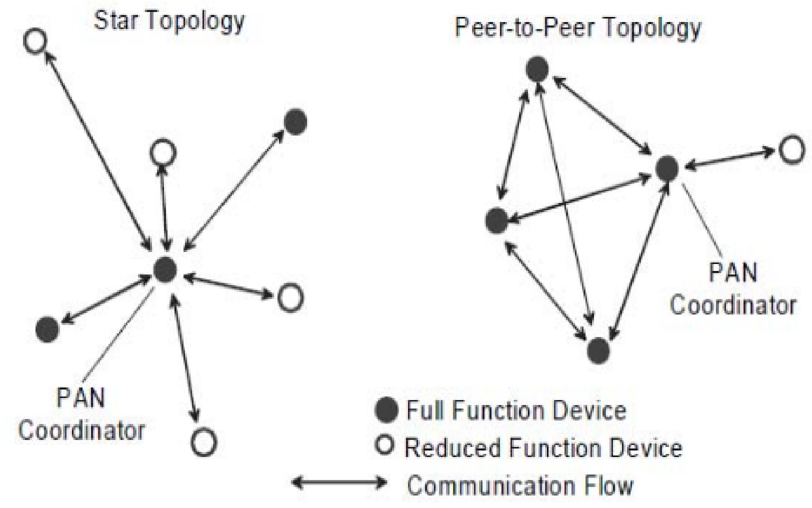
2.2 Source-Routing mesh Netwok (or alternativly:Wireless Adhoc Network)

this is the main idea of how mesh kind of networks handle. it is address the packet (the amount of data that is going to send in every cycle (this thing happens if we are talking about syncronous network)) to the next reciever. this job continues to reach the desired target. there is many talks about data frames and error correction that we ignore for now.

2.3 Elements

there are 2 main types of elements that listed below:

- FFD (Full-Function Device) the FFD is capable of all network functionalities and can operate in three different modes: it can operate as a PAN "*coordinator*" or it can serve simply as a device or as a "*network router*" that could participate in multihop routing of message .
- RFD (Reduced-Function Device) An RFD device is low on resources and memory capacity and it is capable of only very simple applications such as node or sense light and so on. in other word this type is the Zigbee End Device.

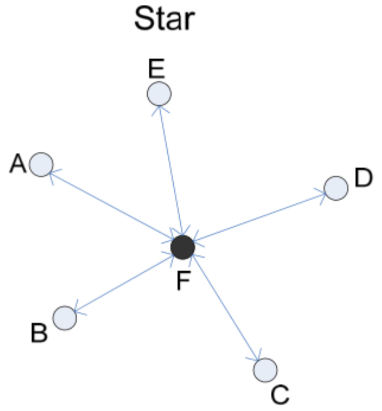


2.4 Zigbee Network Format

there is two most known format of network in zigbee:

2.4.1 Star

this network looks like below:



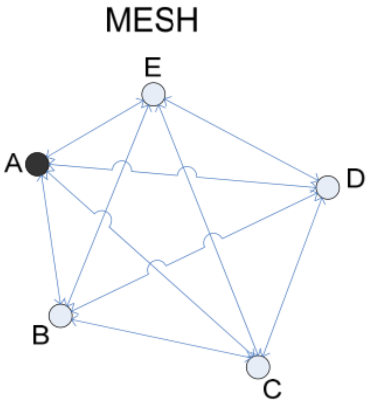
as we saw any component in the network directly connected to the coordinator (like WIFI or other wireless networks) this kind of network have some problems:

1. icreases the load of zigbee network when number of sensors increases :in a single home may be this thing is not a huge problem but when you are talking about a building with tousands of residents then this little thing becomes a big mess in your network. when you have thousands of client in different distances their delay is become different so may be you mess some of the commands also if your network load goes extremely high it could hurt your coordinator or your components so it is a important to choose the right format in case of use.

2. there is just one path to the coordinator for each of components :if we got an obstacle in the way of our signal it can destroy the packets so it's good to have another way to commiuunicate with coordinator.

2.4.2 Mesh (peer-to-peer)

most of zigbee networks looks like below:



in here your network is kind of multi hop network means there is more than one specific to commiuunicate with coordinator which is very important and in large network like a building there is no problem to connet whole building in single network. also need to place a repeater is reduced considerably so it is so efficient.

3 Wireless Protocol (802.11.n (a/b/g))

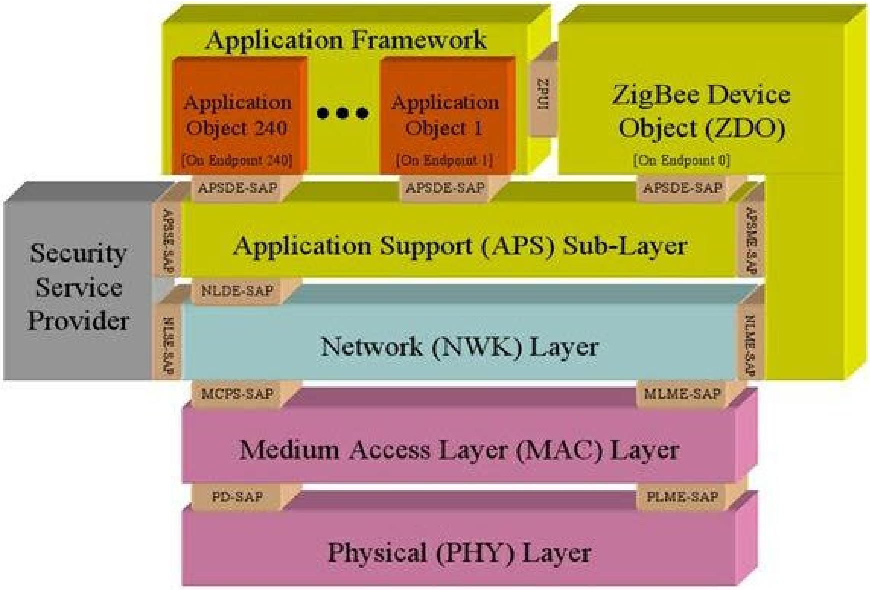
in this section we want to deeply diving into the zigbee protocols and network layers: in a normal wired or wireless network we have 7 network layers but in here because of change in architecture, layers and order of them are changed so in a normal network layer you got:

3.1 Network Protocol (includes other protocols)

1. Physical Layer :physical structure (for example for WIFI this is just air!)
2. Data Link Layer :data frames in here (our switches (keep in mind that switches working with MAC Addresses using CSMA-CA),bridges also ethernet mangement is in here)
3. Network Layer :packets built in this layer (for example in this layer your device could get IP)
4. Transport Layer :End-to-End connections (for example hand shaking protocols like TCP and UDP is in here)
5. Session Layer :Synch & send to port (for example in computer networks always servers uses port 67 this could be satisfied in here)
6. Presentation Layer :syntax layers (some useful protocols like SSH and SSL is in here)
7. Application Layer :End User Layer (normal HTTP or HTTPS sites we review)

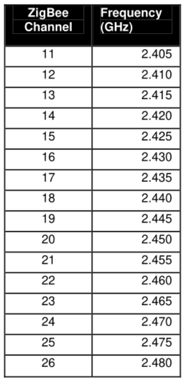
3.2 Zigbee Protocol

in Zigbee things goes a bit different:



3.2.1 Physical Layer

in first look it is not like normal network layer but now we want to know what are these layers exactly doing: IEEE 802.15.4 is for these two first layers thst is very great specification as i mentined before zigbee is working in 2.4 GHz ISM band at 250kb/s data rate. so in this layer we got the RF chips as interfaces and about channels we got from 11 to 26 so we can choose them in order not to have interface with WIFI signals also there is more option for this purpose that mentioned following.



ZigBee Channel	Frequency (GHz)
11	2.405
12	2.410
13	2.415
14	2.420
15	2.425
16	2.430
17	2.435
18	2.440
19	2.445
20	2.450
21	2.455
22	2.460
23	2.465
24	2.470
25	2.475
26	2.480

3.2.2 MAC layer

this layer is so similar to the second layer of normal networks but there is not that kind of handshaking so we got transmission retry,acknowlwdgement management and also CSMA-CA is available in here

3.2.3 Network Layer

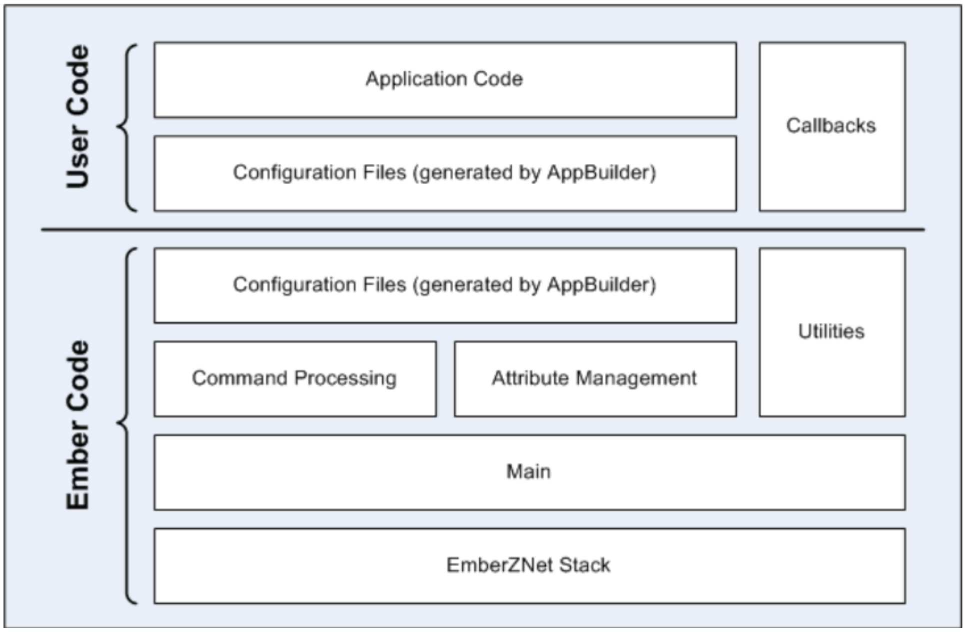
in this layer routing in our network is specified and we have to state the format of network. in here we are capable of transfering data with miltiple devices means ww could have multiple path (through other components or directly) to the destination. and it is called "*multiple hops*".

3.2.4 Application Support Sub-Layer

from here to end of the protocol is zigbee standard or it could be user defined in terms of need. this layer is connctor of next three layers which are the app.

3.2.5 Application Framework

the User App is defined on the top of the base app that called "*User Code*" and base code is named "*Ember Code*" that you could see thst below:



most often it is contains a embedded “C” code that can be configured by Appbuilder to implement any Zigbee cluster library (ZCL) application.

3.2.6 Zigbee Device Object (ZDO)

ZDO is a simple application running on endpoint0 in every zigbee device. ZDO, keeps track of the state of the ZigBee device on and off the network, and provides an interface to the ZDP (ZigBee Device Profile) , a specialized application profile for discovering, configuring, and maintaining ZigBee devices and services on the network. ZDP contains a set of commands for discovering various aspects about nodes in the network. Each ZDP request in BeeStack requires a destination address, which may be unicast or broadcast, as the zigbee specification allows.

3.2.7 Security Service Provider

zigbee now supports a single defined security mode called “**standard security**”. Various policies existes within that mode to control devices behave or inteact on the network. Earlier versions of zigbee standard utilized modes known as “**Residential Security**” and “**High Security**”. these have been deprecated.

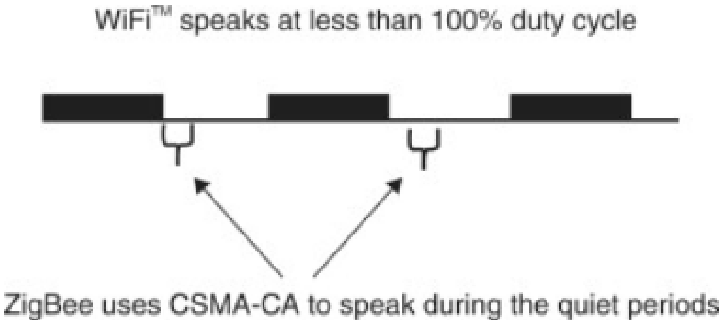
for example some of the well known companies uses 128-bit AES (Advanced Encryption Standards) encryption algorithms to achive desired security. (in order to make more transparent **hashes** in our daily computer usage is a very common example for AES encryption)

4 comparison of Zigbee VS WIFI

WIFI & Zigbee both working in same ferquency (chance of interferance?) but the major diffrent is in the type of connection. when you are speaking about WIFI you have one fixed **Access point** and all of your modules **directly** connect to that and also you are using "*TCP/IP*" handshaking format which is a regular format in our daily devices including our phones.

but when you are speaking about Zigbee things goes diffrent Zigbee uses something called "*mesh*" which means you have a centeral hub and every modules are connected to **otherone** then signal from one module send **trough the others** to the hub and also it doesn't have those heavy and complicated handshaking methods which needs more processing power and power consumption this heavy protocols some times fails in security which is one of the main aims (this is not mean these kind of protocols are useless) so you got **simpler chip** so you can reduce the cost.

the most important question could be asked here is **how zigbee perevents interferancing with WIFI signals?** well there is a very intersting mechanism preventing from that and that is: zigbee protocol could adapt it's network to the "*silent periods*" that means when WIFI duty cycle less than 100% zigbee is transfering data when WIFI is off so we could say that according to Zigbee Ailiance the "packet error rate" is 0% which is amazing in adition WIFI channels is usually is set to 1,6 or 11 but zigbee channels are 15,20,25 or 26 are always free from WIFI interferance.


WiFi™ speaks at less than 100% duty cycle
ZigBee uses CSMA-CA to speak during the quiet periods

5 comparison of Zigbee VS Zwave

Zwave is working in lower ferquency in comparison with Zigbee & WIFI and it have it's own company and driver. it is operating in 868.42 MHz in Europe and in North America is operating in 908.42 MHz which is considerably lower than zigbee. ferquency reduction not only affects the data transfer rate but also it affects the range of module usage across the home. connectivity is very simiular to zigbee and it is uses a “source-routed mesh network ”. in addition because of it’s proprietary software if you are a developer you have to buy the frimware to work with it. power consumption is near by zigbee which is good.

6 Power

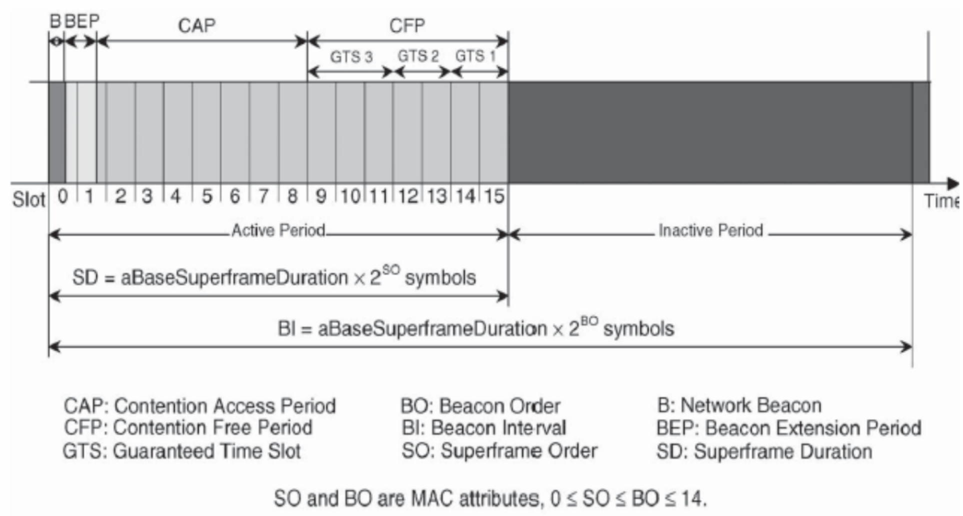
in terms of power zigbee consumes less power than WIFI & Z-wave but could we reduced it more? the answer is YES! in zigbee networks we got two mods that effectively affect the power usage :

6.1 Non-Beacon Network

a simple and traditional multi access system used in peer-to-peer and near-peer networks means you got CSMA-CA communication and when you connencted you recieve a positive acknowlwdgement for successfuly recieved packet.

6.2 Beacon-Enabled Network

this is means we are using superframe structure with idle time in other words your coordinator could goes sleep. means your coordinator is just when you actually need to transmit data. superframe beacon is depicted below:


B
BEP
CAP
CFP
GTS 3
GTS 2
GTS 1
Slot
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Time
Active Period
Inactive Period
SD = aBaseSuperframeDuration × 2^SO symbols
BI = aBaseSuperframeDuration × 2^BO symbols
CAP: Contention Access Period
CFP: Contention Free Period
GTS: Guaranteed Time Slot
BO: Beacon Order
BI: Beacon Interval
SO: Superframe Order
B: Network Beacon
BEP: Beacon Extension Period
SD: Superframe Duration
SO and BO are MAC attributes, 0 ≤ SO ≤ BO ≤ 14.

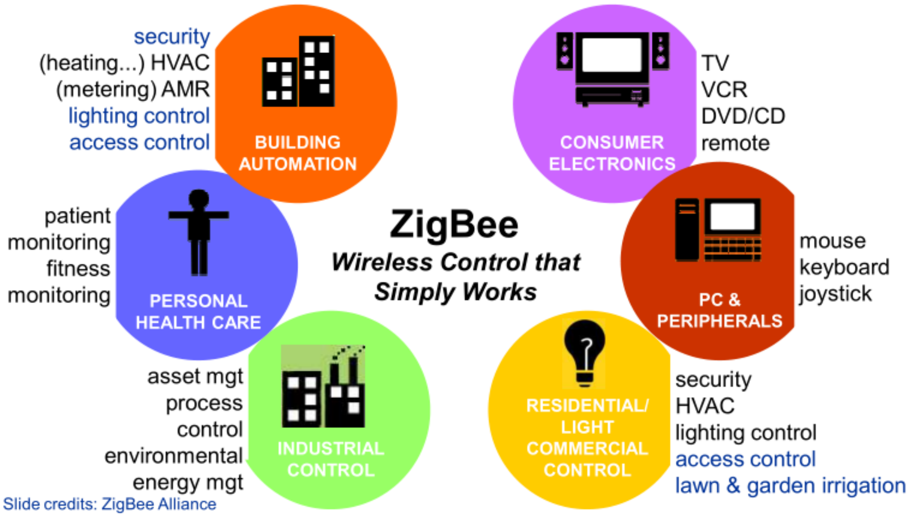
at the end i have to mention that if some End Device has no data to exchange the coordinator can switch their power off and it goes to sleep mode.

7 Security

one of the most important thins specially in home automation is the security. as i mentioned before zigbee could use hub to connect to internet or maybe your account. well it could be easily hijacked before!! but now you can make it more secure than before and also you can test your network to it could be hackded or not. for test there is an open-source tool called “ ZigDiggity ” this group developed the black hat app to test enviroment for zigbee. one of the very good options we got in zigbee is we can make our framework and handshaking (thanks to zigbee for being open-source!!) consider this any specfic company that provides zigbee network elements it would provide exclusive security frameworks that tested and secure as well.

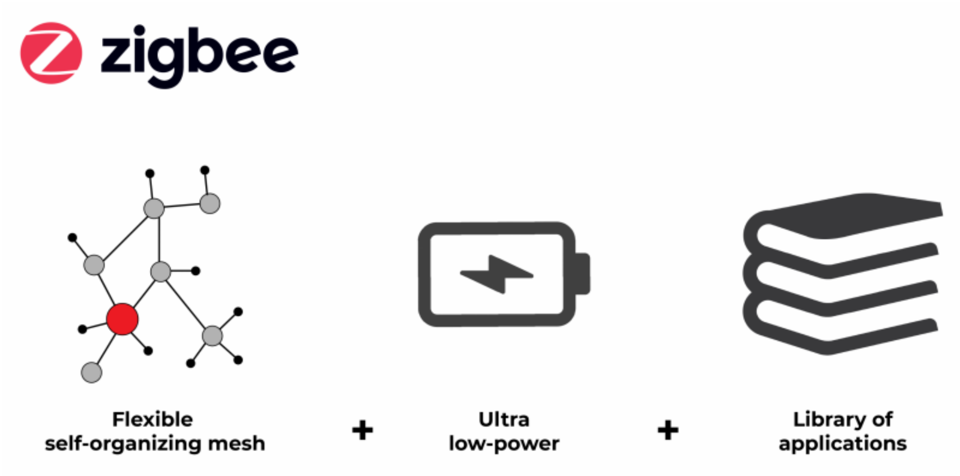
8 Other Usage

these days zigbee have lot more usage than home automation only that depicted below:



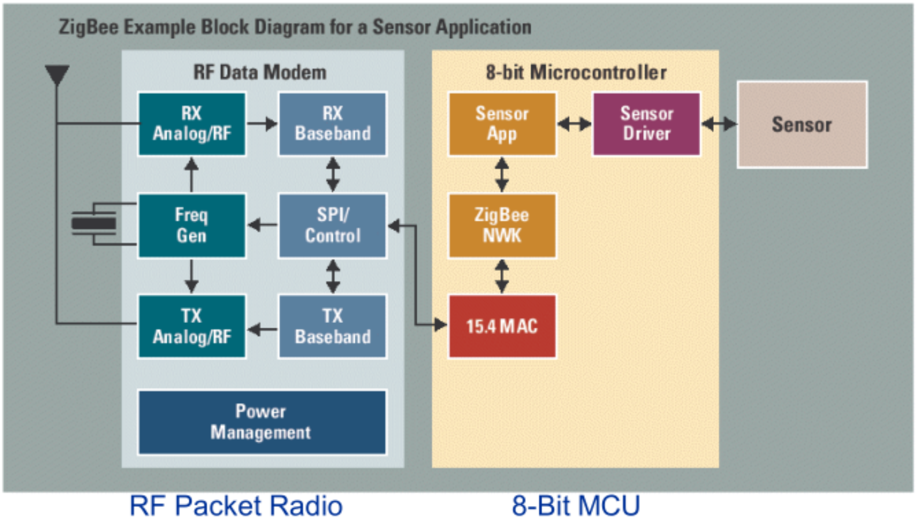
9 Conclusion

well zigbee is lowpower (thanks to the easier handshaking protocol!!) it uses mesh to connect to the hub and all other components. and one of the most important factors is cost and it is an advantage for zigbee.



10 How To Build a Zigbee Module!

everyone can build a zigbee module with the components below:



for MCU you can use any device in our case of study we are ganna use AVR atemga series from atmel those are 8-bit RISC AVR architecture microcontrillers. after MCU you need a 802.15.4 transceiver this is a kind of RF module that could commiunicate with other modules and zigbee hub that from here we just call it RF packet radio.

you could also buy a module that already contains the MCU and the RF packet radio that may be more economical because of integration.