Module IT.2301 - Internet of Things: Short Range Wireless Communications for IoT

Lina Mroueh
lina.mroueh@isep.fr

Institut Supérieur d'Electronique de Paris - Module IT.2301

Part I

Wireless Local Area Network (WLAN)
IEEE 802.11 WiFi

WiFi Overview

- Wi-Fi (Wireless Fidelity) is a wireless technology based on the **IEEE 802.11series of standards**, to provide wireless connectivity to fixed or mobile user devices.
- The 802.11 series of standards, are developed over the last 25 years by the US-based IEEE standards body.
- **CSMA-CA** is a key feature of the 802.11 standards to facilitate equitable spectrum access between multiple Wi-Fi systems even in highly contended environments.

Outline: WiFi

1. Releases and WLAN channels

2. Network architecture

3. Physical Layer in IEEE 802.11

4. MAC Layer in IEEE 802.11

Outline: WiFi

1. Releases and WLAN channels

2. Network architecture

3. Physical Layer in IEEE 802.11

4. MAC Layer in IEEE 802.11

Different IEEE 802.11 Protocols (1/)

Protocol	Release date	Frequency	Typical Data rate	Max Data rate
802.11a	1999	5GHz	1Mb/s	2 Mb/s
802.11b	1999	2.4GHz	6.5 Mb/s	11 Mb/s
802.11g	2003	2.4 GHz	25 Mb/s	54 Mb/s
802.11n	2009	2.4 GHz and/or 5GHz	200 Mb/s	450 Mb/s
802.11ac	2014	5GHz	433 Mb/s	1300 Mb/s

The most used standards are 802.11b, g and n.

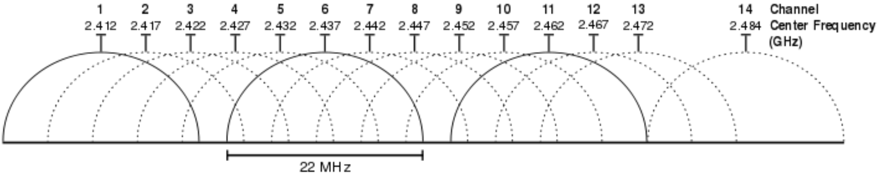
Different IEEE 802.11 Protocols (2/)

Protocol	Bandwidth	Modulation	Indoor range	Outdoor range
802.11a	20 MHz	OFDM	25 m	75 m
802.11b	22 MHz	DSSS	35 m	100 m
802.11g	20 MHz	OFDM	25 m	75 m
802.11n	20, 40MHz	MIMO-OFDM	50 m	125 m
802.11ac	20, 40, 80, 160 MHz	MIMO-OFDM	20 m	50 m

List of WLAN Channels

- IEEE 802.11 b, g and n operate in the 2.4 GHz ISM band and in the band of 5 GHz.
- Each range is divided into a multitude of channels.
- Countries apply their own regulations to the allowable channels, allowed users and maximum power levels within these frequency ranges.

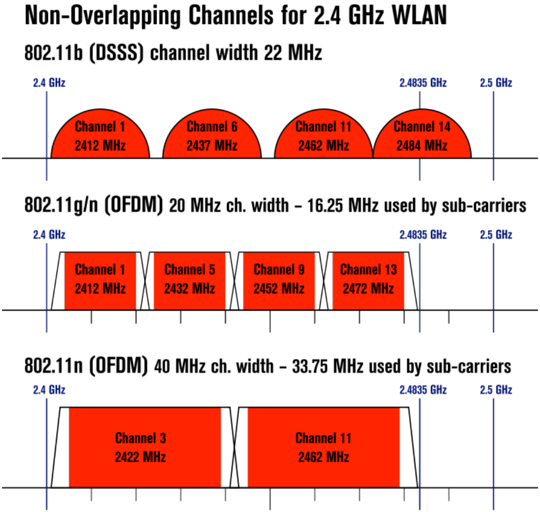
2.4 GHz WLAN 22 MHz Channels



- The available bandwidth of 2.4 GHz is divided into 14 partially overlapping channels, each 22 MHz wide.

- In Europe, only channels 1 to 13 are available with power restriction of 100 mW in France.

Non Overlapping Channels for 2.4 GHz WLAN Band



WLAN Channels for the 5 GHz Band

- In Europe, channel with 20 MHz of bandwidth are authorized in the 5 GHz band.

- Adjacent channels can be aggregated by 2 in 802.11n to increase the data rate.

- Authorized channels in the 5GHz are listed in the table, the carrier refers to the central frequency.

WLAN Channels for the 5 GHz Band

Channel	Carrier (GHz)
36	5.180
40	5.200
44	5.220
48	5.240
52	5.260
56	5.280
60	5.300
64	5.320
100	5.500
104	5.520

Channel	Carrier (GHz)
108	5.540
112	5.560
116	5.580
120	5.600
124	5.620
128	5.640
132	5.660
136	5.680
140	5.700
-	-

Outline: WiFi

1. Releases and WLAN channels

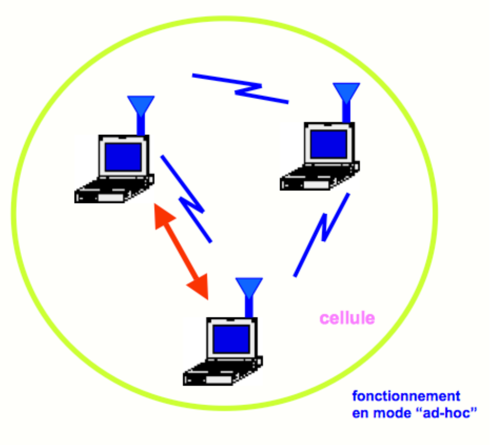
2. Network architecture

3. Physical Layer in IEEE 802.11

4. MAC Layer in IEEE 802.11

Ad hoc Architecture: Demo

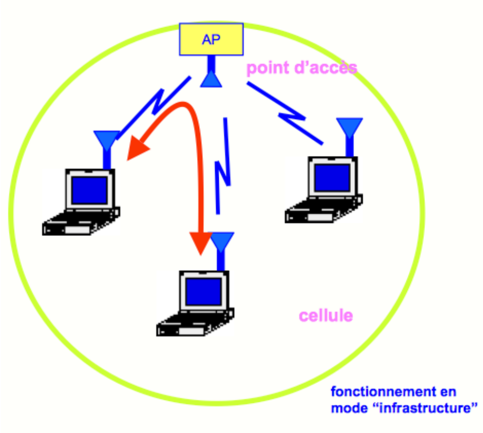
☞ Independent Basic Service Set (IBSS)



Infra-structured Architecture: Demo

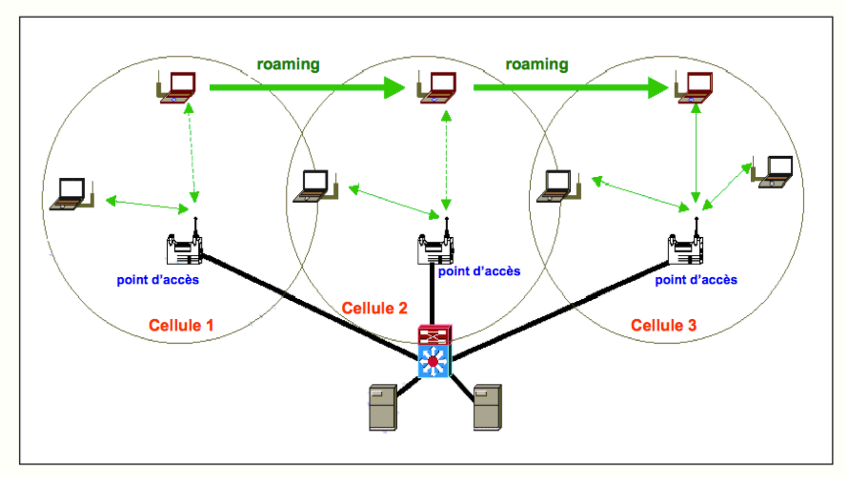
☞ Infra-structured BSS via an Access Point (AP).

Stations and AP operate in Time Division Duplex **TDD mode** and have **Half-duplex** communication.



Extended Basic Service Set (EBSS)

☞ Distribution System = Inter-AP connected via wired or wireless connection;



Basic Operations (1/)

- One 2.4 GHz channel is affected per AP and per BSS. An AP can be **bi-band** (two channels per BSS one in 2.4 GHz and one in 5GHz) in IEEE 802.11n.
- When powered on, a WiFi station will scan the available channels to discover active networks where beacons are being transmitted.
- It then selects a network, be it in ad hoc mode or infrastructured.

Basic Operations (2/)

- In the infrastructured case, it authenticates itself with the access point (AP) and then associates with it.

- Stations keep discovering new networks and may disassociate from the current one in order to associate with a new one (e.g., because it has a stronger signal).

- Stations can roam between networks that share a common distribution system, in which case seamless transition is possible.

Outline: WiFi

1 Releases and WLAN channels

2 Network architecture

3 Physical Layer in IEEE 802.11

4 MAC Layer in IEEE 802.11

Physical Layer of IEEE 802.11

1. **IEEE 802.11b**: 2.4 GHz, DSSS modulation.
2. **IEEE 802.11g**: 2.4 GHz, OFDM modulation.
3. **IEEE 802.11n**: bi-band 2.4 GHz and/or 5 GHz, carrier aggregation, OFDM, MIMO.
4. **IEEE 802.11ac**: 5 GHz, carrier aggregation, OFDM, MIMO, MU-MIMO.

1. IEEE 802.11b: Main Characteristics

- IEEE 802.11b operates only in 2.4 GHz band, divided into 13 overlapping channels of 22 MHz width;
- Channels 1, 6 and 11 are non-overlapping and can be used to cover large areas.
- IEEE 802.11b is based on DSSS modulation and CSMA-CA mechanism.

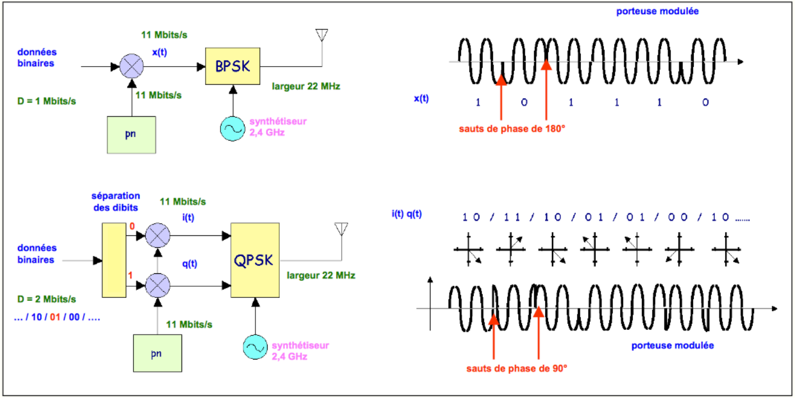
1. IEEE 802.11b: DSSS Modulation (1/)

- The channel width of IEEE 802.11b is 22 MHz. The effective bandwidth of the signal is 1 MHz. Two signals are considered with rate 1 Mbps or 2 Mbps.
- IEEE 802.11b uses the Barker sequence to spread a data signal with effective spectral occupation of 1 MHz into a spectrum of two-sided 11 MHz spectrum.
- Let $T_s = 1\mu$s be the one symbol duration. For BPSK modulation, the data rate is 1 Mbps and the effective signal bandwidth is 1 MHz.
- Using the same T_s with QPSK modulation (1 symbol = 2 bits), the data rate is 2 Mbps and the effective signal bandwidth is $B = \frac{1}{T_s} = 1$ MHz.

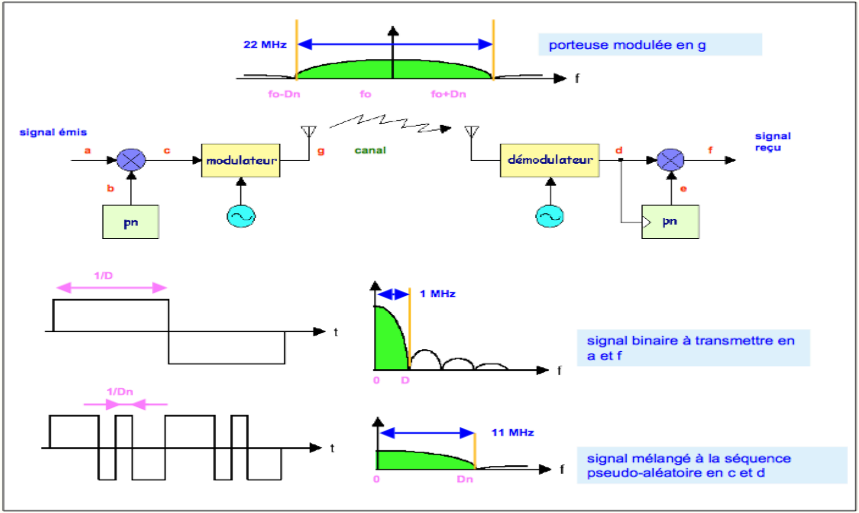
1. IEEE 802.11b: DSSS Modulation (2/)

- The Barker sequence replaces each symbol by 11 chips such that:
  $p_n = +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1;$
- The total duration of p_n is the same as the symbol one. The chip duration is however $T_c = T_s/11$.
- The bandwidth of the DSSS signal is therefore 2×11 MHz (two sided, with the symmetrical part).

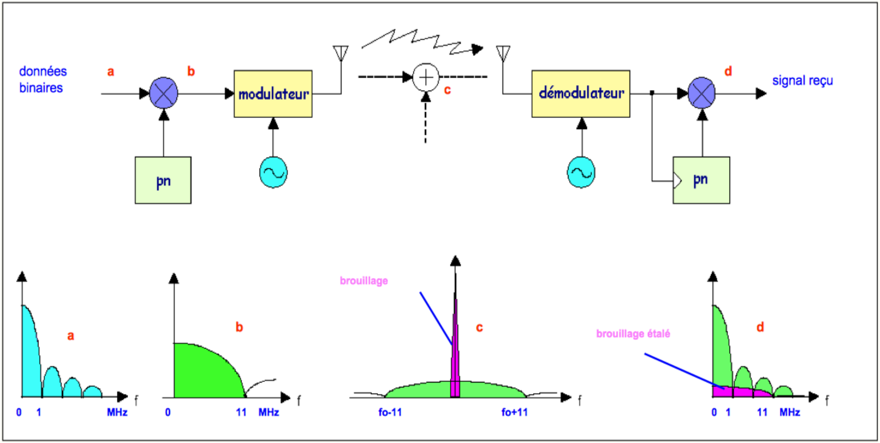
1. 1IEEE 802.11b: DSSS Modulation (3/)



1. IEEE 802.11b: DSSS Modulation (3/)



1. IEEE 802.11b: DSSS Modulation (4/)



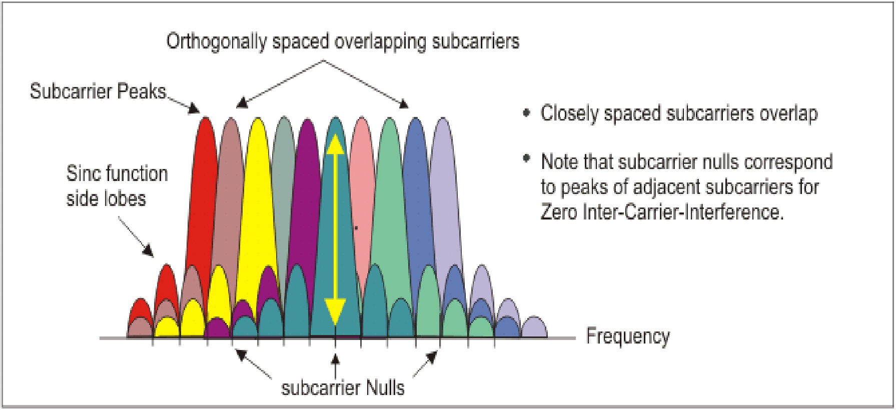
2. IEEE 802.11g: Main Characteristics

- IEEE 802.11g operates only in 2.4 GHz band, divided into 4 non-overlapping channels of 20 MHz width each;

- A BSS operating with WiFi 802.11g can only attribute one of the 2.4 GHz channels per BSS. 802.11g can coexist with the 802.11b one.

- IEEE 802.11g is based on OFDM modulation and CSMA-CA mechanism.

2. IEEE 802.11g: OFDM Modulation (1/)



- Closely spaced subcarriers overlap
- Note that subcarrier nulls correspond to peaks of adjacent subcarriers for Zero Inter-Carrier-Interference.

OFDM Signal Frequency Spectra

2. IEEE 802.11g: OFDM Modulation (2/)

- The OFDM signal decomposes the 20 MHz bandwidth into sub-channels that are orthogonal, no interference between subcarriers.

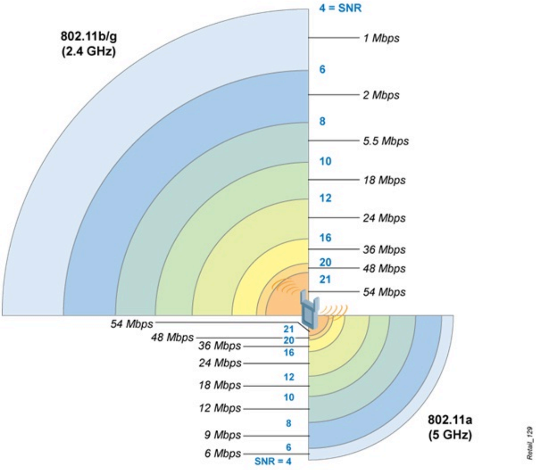
- OFDM uses a comb of $N_{\mathsf{FFT}} = 64$ subcarriers: 48 for data, 4 pilots, 12 null carriers, with a spacing of $\Delta f = 0.3125$ MHz.

  The useful bandwidth is then $0.3125 \times (48 + 4) = 16.25$ MHz.

- Each OFDM symbol is a packet containing 48 data symbols sent during 4μs. The symbol rate is therefore 12 Msymbol/s.

- Each symbol is protected with a convolutional code of either 3/4, 2/3, or 1/2 rate, using M-ary quadrature amplitude modulation (M-QAM) with M being 2, 4, 16, or 64.

2. IEEE 802.11g: Rate and SNR



Noise and average Interference floor can be set to -85 dBm

3. IEEE 802.11n: Main Characteristics

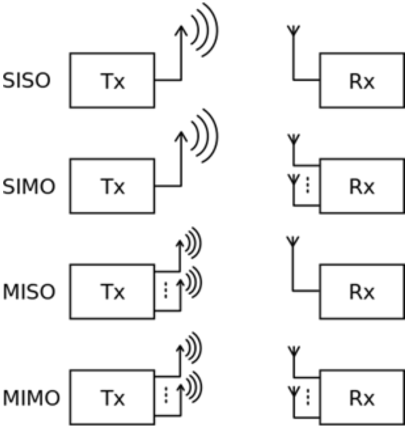
- IEEE 802.11n operates in 2.4 GHz band and or 5 GHz; An AP can be bi-band and this increases the number of simultaneously served stations.

- OFDM modulation used in IEEE 802.11g is used with 802.11n.

- In both bands, **carrier aggregation** can be used by grouping 2 adjacent carriers to increase the signal bandwidth and consequently the data rate.

- MIMO schemes are used to improve the data rate by enabling the exchange of multiple streams on the same radio resource.

3. IEEE 802.11n: MIMO (1/)



☞ **SISO**: Single Input Single Output; **SIMO**: Single Input Multiple Output; **MISO**: Multiple Input Single Output; **MIMO**: Multiple Input Multiple Output.

3. IEEE 802.11n: MIMO (2/)

- SIMO and MISO schemes improve the reliability of the transmission and reception by sending the data on independent faded paths: diversity gain.

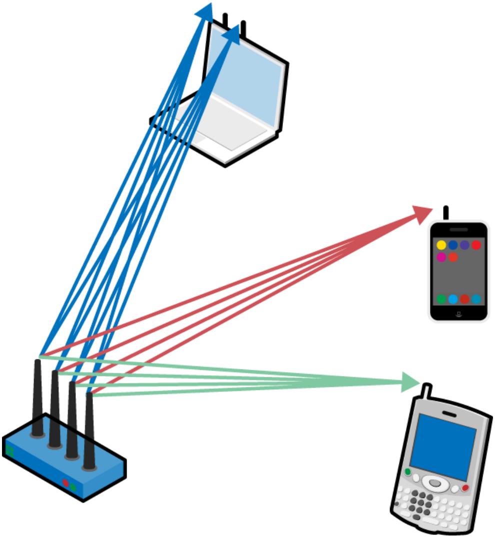
- In a $n_t \times n_r$ MIMO configuration, the simultaneously number of data symbols that can be transmitted is $\min(n_t, n_r)$.

- MIMO schemes achieve higher data rate, multiplied by a factor $\min(n_t, n_r)$ compared to the SISO rate.

4. IEEE 802.11ac: Main Characteristics

- IEEE 802.11ac operates in 5 GHz where 19 channels of 20 MHz are available;
- OFDM modulation is used in the 5 GHz band.
- **Carrier aggregation** can be used to increase the signal bandwidth and hence the data rate. This is performed by grouping 2, 4 or 8 carriers.
- MIMO schemes are used to improve the data rate by enabling the exchange of multiple streams on the same radio resource.
- MU-MIMO beamforming techniques are used at the AP to enable multi-user communication. The AP can exchange data with multiple users on the same radio resource.

4. IEEE 802.11ac: Multi-User MIMO-OFDM Modulation



☞ MU-MIMO increases the capacity of the BSS.

Outline: WiFi

1 Releases and WLAN channels

2 Network architecture

3 Physical Layer in IEEE 802.11

4 MAC Layer in IEEE 802.11

DCF and PCF

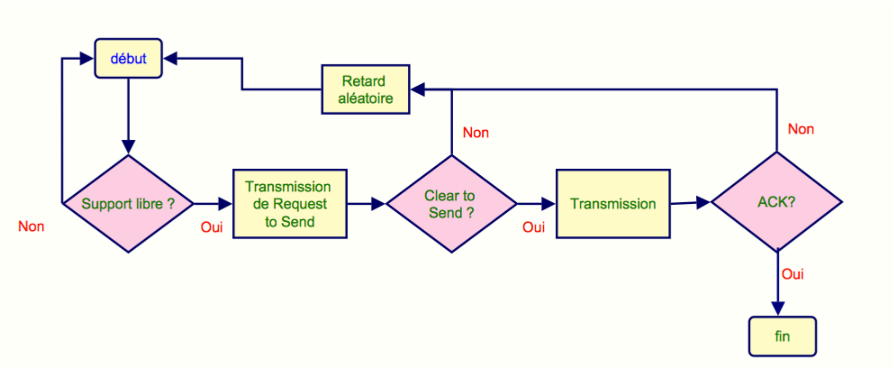
- Access to the transmission medium is controlled by means of a set of rules called a coordination function.

- Wi-Fi defines a **Distributed Coordination Function** (DCF) and a **Point Coordination Function** (PCF), the latter being optional.

- The fundamental Wi-Fi MAC protocol is the DCF, which is a CSMA-CA channel access method used in both ad hoc and infrastructured networks.

- PCF is an optional mode in which the point coordinator (PC), the AP, uses a round-robin policy to poll each station for data to be transmitted.

CSMA-CA protocol



References

The course was prepared based on several web references mainly:

- E. Ferro and F. Potori, Bluetooth and Wi-Fi Wireless Protocols- Survey and Comparison, IEEE Wireless Communication, 2005.
- M. Andersson, Short-range Low Power Wireless Devices and Internet of Things, 2014
- J. Burns, S. Kirtay, P. Marks, Future use of Licence Exempt Radio Spectrum, July 2015.
- Réseau Local, Lecture notes of Prof. Jean-Philippe Muller.
- L. Clavier, C. Loyez, Réseaux de capteurs autonomes - Couche physique et architectures matérielles, Techniques de l'ingénieur 2013.
- D. Trezentos, Standard pour réseaux WiFi sans fil: IEEE 802.11, Techniques de l'ingénieur 2002
- Wikipedia

Part II

Wireless Personal Area Network (WPAN)
Bluetooth

Why it is called Bluetooth?

- The word "Bluetooth" is taken from the 10th century Danish King **Harald Bluetooth**.
- King Bluetooth had been influential in uniting Scandinavian Europe during an era when the region was torn apart by wars and feuding clans.
- The Bluetooth name fits as this technology was developed in Scandinavia, and unites very differing industries under a common, simple wireless communication radio.

Outline: Bluetooth

1. Releases and Bluetooth Channels
2. Network Architecture
3. Physical Layer in Bluetooth
4. MAC Layer in Bluetooth
5. Bluetooth Low Energy

Outline: Bluetooth

1. Releases and Bluetooth Channels
2. Network Architecture
3. Physical Layer in Bluetooth
4. MAC Layer in Bluetooth
5. Bluetooth Low Energy

Bluetooth History

- The **IEEE 802.15.1** working group defined different versions of Bluetooth ratified with the year yyyy of standardization as IEEE standard 802.15.1-yyyy.

- **BDR** = Basic Data Rate; **EDR** = Enhanced Data Rate; **HS** = High Speed;
  BLE = Bluetooth Low Energy.

- The Bluetooth HS negotiates the transmission with IEEE 802.11 and the transmission is done via IEEE 802.11.

Bluetooth Releases

Bluetooth Version	Release Date	Data Rate	Range
V1.2 (BDR)	2003	732 kb/s	10 - 100 m
V2.1 (EDR)	2007	2.1 Mb/s	10 - 100
V3.0 (HS)	2009	25 Mb/s	10 - 100
V4.0 (BLE)	2010	0.3 Mb/s	10 - 100 m

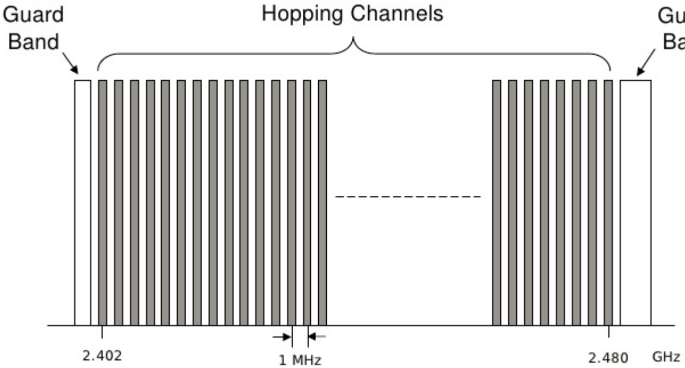
Bluetooth Channels

- Bluetooth devices use the unlincensed ISM 2.4 GHz band that is divided into 79 channels with 1-MHz of width each.

- The channels are accessed using an FHSS technique, with a signal rate of 1 Mb/s, using Gaussian shaped frequency shift keying (GFSK) modulation.

- The center of each channel is $(2402 + k)$ MHz with $k = 0 \ldots 78$ used without license and restricted indoor transmission power to 10 mW max and outdoor power 4 mW.

Bluetooth Channels

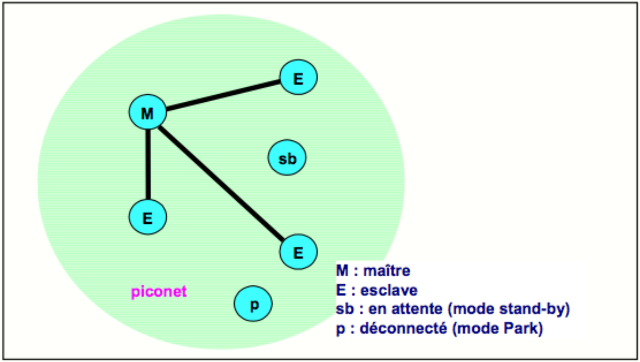


Outline: Bluetooth

1. Releases and Bluetooth Channels
2. Network Architecture
3. Physical Layer in Bluetooth
4. MAC Layer in Bluetooth
5. Bluetooth Low Energy

Network Topology (1/)

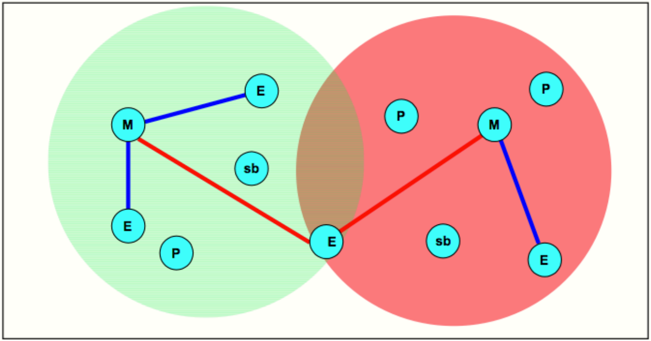
☞ Piconet = 1 master + up to 8 slaves (3 bits short address) and 255 devices in Stand-by mode (8 bits short address). One hopping sequence per piconet.



M : maître
E : esclave
sb : en attente (mode stand-by)
p : déconnecté (mode Park)

Network Topology (2/)

☞ Scatternet = Up to 10 piconet.



Basic Operations in Classical Bluetooth

- When a Bluetooth device is powered on, it tries to operate as one of the slave devices of an already running master device. It then listens for a master's inquiry for new devices and responds to it.
- The inquiry phase lets the master know the address of the slave; this phase is not necessary for already paired devices that have knowledge of each other's address.
- Once a master knows the address of a slave, it may open a connection toward it, provided the slave is listening for paging requests.
- If this is the case, the slave responds to the master's page request and the two devices synchronize over the frequency hopping sequence that is **unique to each piconet** and decided by the master.

Classical Bluetooth Discover and Association (1/)

- A synchronization between the master and the slave should be performed before any connection.

- The Bluetooth uses 32 **advertising channels** (divided into group A (resp. B) containing the lower (highest) 16 channels) to associate the two devices.

- In the discovery phase, the master transmits packets on the two group of advertising frequencies.

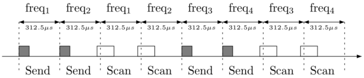
- The slave scans those frequencies at a slower rate, thus maximizing the probability of a correct reception.

Classical Bluetooth Discover and Association (2/)

- The master transmits two **inquiry packets** on two different frequencies during one regular transmission time slot of **625 μs**.

- During the next two time slots, the device **scans for a reply on these same two frequencies**, i.e. each scan occurs 625 μs after the corresponding send. The master spend 10 **ms** (= 16 × 0.625 ms) in transmitting and scanning each train.

- The device now proceeds to send and scan on the next pair of frequencies in the same fashion.



- Each train is repeated 256 times and the master swaps between train A and B every 2.56 seconds.

Classical Bluetooth Discover and Association (3/)

- Bluetooth devices that want to be discovered enter the inquiry scan substate and periodically scan for inquiry packets on the same 32 frequencies that the inquiring device is transmitting on.

- The frequency of each scanning device, known as its phase, cycles through the 32 frequencies in order, according to the value of its clock and changes every 1.28s.

- The scanning device listens continuously on its current frequency during an inquiry scan window of 11.25ms, long enough for the inquiring device to transmit on an entire train of 16 frequencies. The scanning device then sleeps, before scanning again.

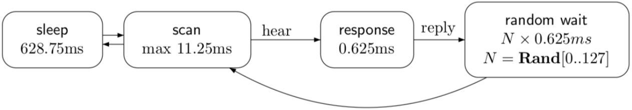
- If the scanning device successfully hears a message, by listening on the right frequency at the right time, it waits 625μs and then sends a reply (known as Frequency Hopping Synchronization (FHS) packet) on the same frequency.

Classical Bluetooth Discover and Association (4/)

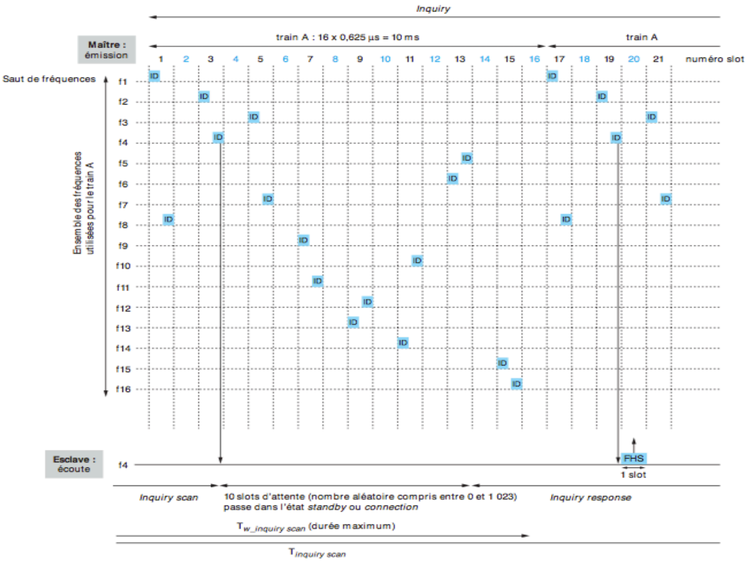
- This FHS packet contains the device's address and its clock offset. Using this information a link can be established.

- A contention problem arises when two devices in inquiry scan try to reply to the same inquiry packet. In this case, the two replies collide and are both lost.

- To avoid repetition of such a problem, after sending a reply, a device draws a random number $0 \leq N \leq 127$ and waits for $2N$ time slots before going back to the inquiry scan substate.



Example



10 slots d'attente (nombre aléatoire compris entre 0 et 1 023) passe dans l'état *standby* ou *connection*

Outline: Bluetooth

1 Releases and Bluetooth Channels

2 Network Architecture

3 Physical Layer in Bluetooth

4 MAC Layer in Bluetooth

5 Bluetooth Low Energy

FHSS Technique and Hopping Sequence (1/)

- Frequency hopping consists in accessing the different radio channels according to an extremely long pseudo-random sequence.

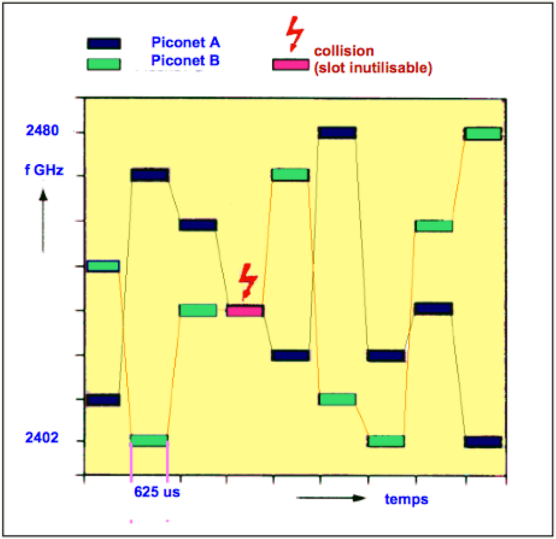
- The **hopping sequence** is generated from the **address** and **clock of the master station** in the piconet. Using this method, different piconets use different hop sequences.

- When entering a piconet, a slave waits for an Inquiry message from the master to learn the master's address and clock phase, and computes the hopping sequence.

FHSS Technique and Hopping Sequence (2/)

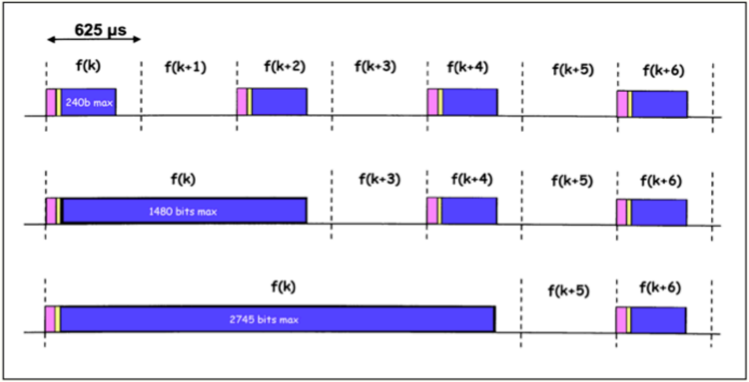
- The transmission channel **changes 1600 times per second**; this means that the transmission frequency remains unchanged for 625 μs long slots.
- The master station starts its transmissions in the even slots, the slaves in the odd ones. A message may last for **1, 3, or 5 consecutive slots**.
- The **channel** used to transmit **multi-slot messages** is the **same** one used as the first slot message: the hopping sequence does not advance with multislot messages.

FHSS Technique and Hopping Sequence (3/)



Packet Length and Data Rate

☞ Short Packet = 240 bits, 1time-slot; Medium Packet = 1480 bits, 3 time-slots; Long Packet = 2745 bits, 5 time-slots.



Data Rate in Classical Bluetooth

Packet way1/way2	**Size (bits)**	**Duration D**	**Data rate 1**	**Data rate 2**
Long/Short	2745 / 240	$6 \times 625\mu$s	732 kb/s	64 kb/s
Medium/Short	1480 / 240	$4 \times 625\mu$s	592 kb/s	96 kb/s
Long/Long	2745 / 2745	$10 \times 625\mu$s	439.2 kb/s	439.2 kb/s

Modulation in Classical Bluetooth

- The modulation used is the Gaussian Frequency Shift Keying (GFSK) with a data rate of R = 1 Mbit/s.

- For the Classical Bluetooth, a binary FSK modulation is used such that: $0 \rightarrow f_0 - \Delta f$ and $1 \rightarrow f_0 + \Delta f$.

- The modulation index is $\mathrm{MI} = \frac{2\Delta f}{R}$ is $0.28 \leq \mathrm{MI} \leq 0.35$ and this corresponds to $140 \leq \Delta f \leq 175$ kHz.

Modulation in Bluetooth EDR

- In the Bluetooth **Enhanced Data Rate** (EDR), higher order of modulation is used.

- Phase Shift Keying (PSK) modulation are used with 4 and 8 states: 4-Differential Quadrature PSK (DQPSK) or 8-Differential Phase Shift Keying (DPSK).

- 4**-DQPSK**: The phase $\varphi(t)$ at instant t is such that:

  $00 \rightarrow \varphi(t) = \varphi(t-1) + 90°$; $01 \rightarrow \varphi(t) = \varphi(t-1)$; $11 \rightarrow \varphi(t) = \varphi(t-1) + 180°$; $10 \rightarrow \varphi(t) = \varphi(t-1) + 270°$;

- The data rate is respectively multiplied by 2 with 4-DQPSK and 3 with 8-DPSK.

Transmission Power

Power Class	Max Power	Min Power	Range
Class 1	100 mW (20 dBm)	1 mW (0 dBm)	100 m
Class 2	2.5 mW (4 dBm)	0.25 mW (-6 dBm)	10 m
Class 3	1 mW (0 dBm)	NA	1 m
Class 4	0.5 mW (-3 dBm)	NA	0.5 m

- Most devices on the market are intended to replace short cables: they have fixed output power and usually fall into Class 1.

- Devices intended for general communications generally fall into Class 2 or Class 3 and have variable output power.

Sensitivity and Range

- The transmission power control is mandatory for equipments of class 1 and optional for other classes.
- The power control reduces the interferences and the power consumption.
- The receiver sensitivity defined by the standard is at least equal to -70 dBm.
- For a transmission power of 100 mW, the communication range is 100 m.

Outline: Bluetooth

1. Releases and Bluetooth Channels
2. Network Architecture
3. Physical Layer in Bluetooth
4. MAC Layer in Bluetooth
5. Bluetooth Low Energy

Centralized Polling Access

- In centralized case, one station acts as a master, while the other stations (slaves) only transmit when they are allowed by the master, which decides the transmission schedule
- **Pros:** Centralized schemes are simple and provide a single coordination point.
- **Cons:** The master is a single point of failure (and thus redundancy may be necessary) and a possible bottleneck.

Synchronous Connection Oriented (SCO) Links (1/)

- An SCO link provides guaranteed delay and bandwidth, apart from possible interruptions cause higher priority messages.
- A **slave** can open up to **three SCO links** with the same master, or **two SCO links** with different masters.
- A master can open up to three SCO links with up to three different slaves.
- SCO links provide constant bit rate symmetric channels, and are suitable to streaming applications (as average quality voice and music) with fixed symmetric bandwidth.

Synchronous Connection Oriented (SCO) Links (2/)

- SCO links provide limited reliability: no retransmission is ever performed, and no cyclic redundancy check (CRC) is applied to the payload.

- They are optionally protected with a 1/3 or 2/3 forward error correction (FEC) convolutional code.

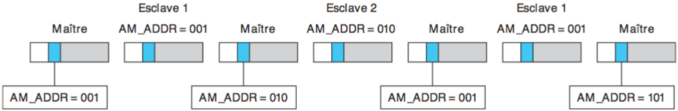
- Transmission of short package can be scheduled each 6 slots, and the corresponding data rate is 64 kb/s.

Asynchronous Connectionless Links (ACL)

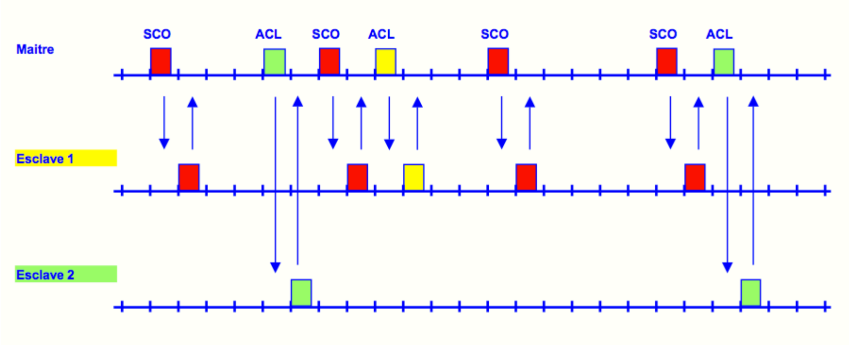
- ACL links are used for **non-real-time traffic**. A slave exchanges one packet at a time with the master according to a schedule between slaves, computed by the master.

- For ACL links, slaves have an Active Member Address (AM_ADDR) with 3 bits inside each piconet.

- Using this 3 bits AM_ADDR, the **Master transmits to** 7 **slaves**, the AM_ADDR = 000 is used to diffuse message in the whole piconet.



Asynchronous Connectionless Links (ACL)



Outline: Bluetooth

1 Releases and Bluetooth Channels

2 Network Architecture

3 Physical Layer in Bluetooth

4 MAC Layer in Bluetooth

5 Bluetooth Low Energy

Classical Bluetooth versus BLE

Technical Specification	Classic Bluetooth	Bluetooth Low Energy
Frequency	2400 to 2483.5 MHz	2400 to 2483.5 MHz
Modulation Technique	FHSS	FHSS
Modulation Scheme	GFSK	GFSK
Modulation Index	0.35	0.5
Number of channels	79	40
Advertising Channels	32	3
Channel Bandwidth	1 MHz	2 MHz
Application Throughput	0.7 - 2.1 Mbps	0.3 Mbps

Classical Bluetooth versus BLE

Technical Specification	Classic Bluetooth	Bluetooth Low Energy
Active slaves	n $\leq$ 7 in ACL mode	Unlimited
Average network setup speed	120 ms	6 ms
Range	10 to 100 m	10 to 100 m
Transmission Power	1W	0.1 to 0.5 mW
Battery Life	Days	Years
Voice	Capable	Not Capable

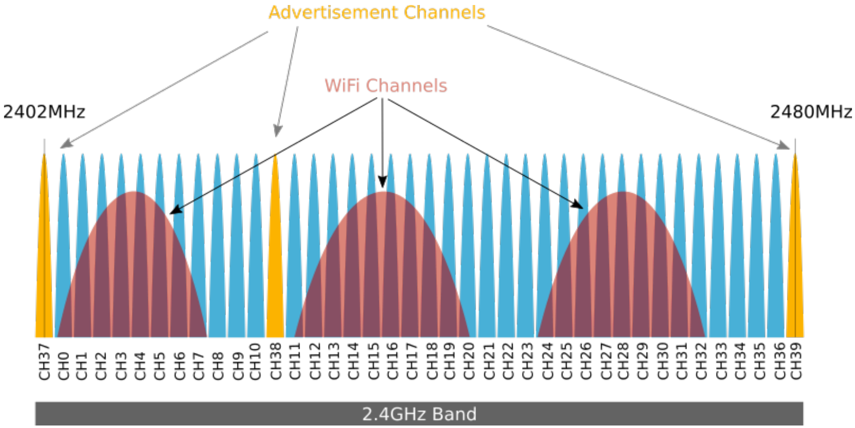
BLE Reduction of Power Consumption

- BLE's low power consumption is enabled by its very simple link layer, designed for quick connections.
- BLE chips spend most of their time asleep, only waking up to send data - a process that takes only few ms, compared to 100 ms with Classic Bluetooth.
- With fewer advertising channels, the chance is greater that another radio, broadcasting on one of the chosen frequencies, might be corrupting the signal.
- That's why BLE advertising channels are chosen between the non overlapping WLAN channels: so that no collision occurs between BLE and WiFi devices in these channels.

BLE Channels

- BLE uses only 40 channels, 2 MHz wide, while Classic Bluetooth uses 79 channels, 1 MHz wide.
- Only three Advertising channels, instead of 32 in the Classical Bluetooth case, are used for device discovery and connection setup.
- BLE minimizes time on air to reduce power consumption. BLE devices switch on for just 0.6 to 1.2 ms to scan for other devices using the three advertising channels.
- The power savings are significant: BLE consumes 10 to 20 times less power than Classic Bluetooth technology to locate other radios.

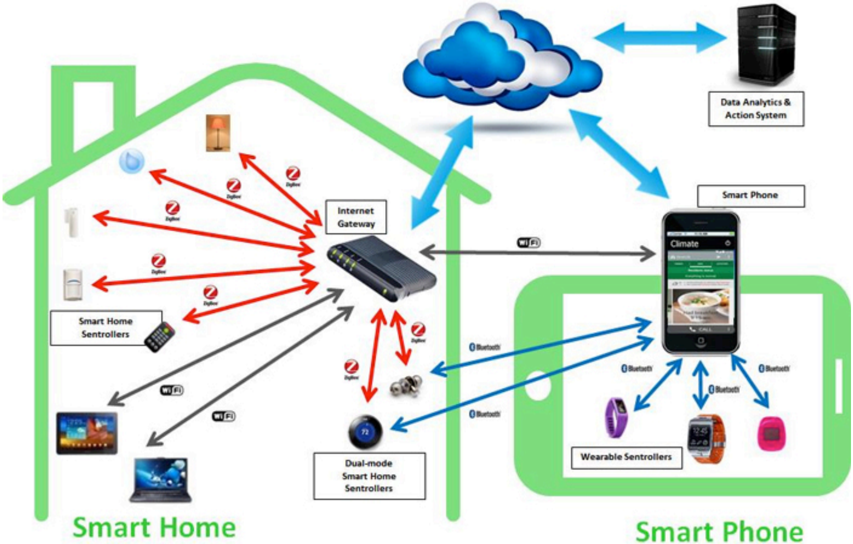
BLE Channels and Advertising Channels



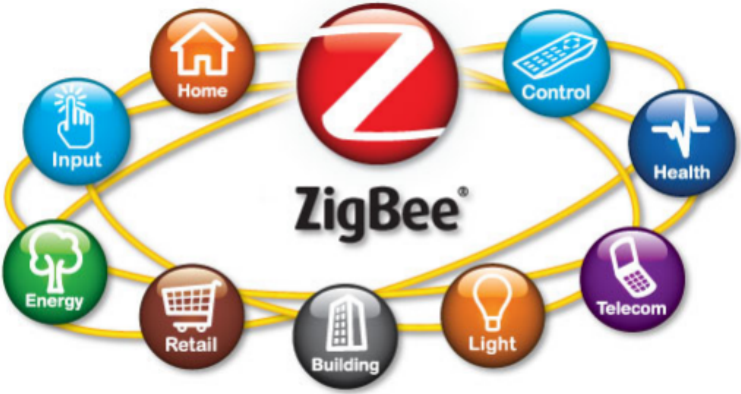
Part III

Wireless Personal Area Network (WPAN)
IEEE 802.15.4

Home Automation Network



IEEE 802.15.4/Zigbee Use Cases



Outline: IEEE 802.15.4

1. IEEE 802.15.4 Characteristics

2. Network Topology

3. IEEE 802.15.4 PHY Layer

4. IEEE 802.15.4 MAC Layer

Outline: IEEE 802.15.4

1. IEEE 802.15.4 Characteristics

2. Network Topology

3. IEEE 802.15.4 PHY Layer

4. IEEE 802.15.4 MAC Layer

IEEE 802.15.4

- In 2000, two standards groups, ZigBee, a HomeRF spinoff, and IEEE 802 Working Group 15, combined efforts to address the need for **low-power low-cost wireless networking** in the residential and industrial environments.

- In December of that year the IEEE New Standards Committee (NesCom) officially sanctioned a new task group to begin the development of a **low-rate wireless personal area network** (LR-WPAN) standard, to be called **802.15.4**.

- The goal of this group was to provide a standard with ultra-low complexity, cost, and power for low-data-rate wireless connectivity among inexpensive fixed, portable, and moving devices.

High-Level Characteristics

Property	Range
Raw data rate	868 MHz: 20 kb/s; 915 MHz: 40 kb/s; 2.4 GHz: 250 kb/s
Range	10 - 20 m
Latency	Down to 15 ms
Channels	868/915 MHz: 11 channels 2.4 GHz: 16 channels
Frequency band	Two PHYs: 868 MHz/915 MHz and 2.4 GHz
Addressing	Short 8-bit or 64-bit IEEE
Channel access	CSMA-CA and slotted CSMA-CA

Outline: IEEE 802.15.4

1 IEEE 802.15.4 Characteristics

2 Network Topology

3 IEEE 802.15.4 PHY Layer

4 IEEE 802.15.4 MAC Layer

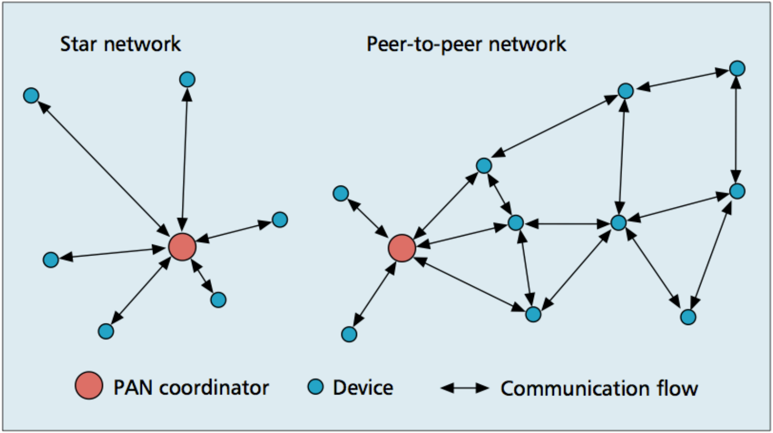
Network Topology

- The IEEE 802.15.4 draft standard supports multiple network topologies, including both **star** and **peer-to-peer** networks. The topology is an application design choice;

- PC peripherals require the low-latency connection of the star network, while perimeter security applications require the large-area coverage of peer-to-peer networking.

- Multiple address types, including both physical (i.e., 64-bit IEEE) and short (i.e., 8-bit network-assigned) are provided.

Network Topology



IEEE 802.15.4 Nodes Type

1. **Full-Function Device** (FFD) can serve as the coordinator of a PAN as it may function as a common node.

   FFD implements a general model of communication which allows it to talk to any other device: it may also relay messages. function as a common node.

2. **Reduced-Function Devices** (RFD) are extremely simple devices with very modest resource and communication requirements;

   RFD can only communicate with FFDs and can never act as coordinators.

Beacon Enabled Network

- The PAN coordinator transmit periodic beacons. Beacon intervals may range from 15.36 ms up to 251.7 s.

- A client registers with the coordinator and looks for messages. Messages are processed and when no messages are pending, the client returns to sleep, awaking on a schedule specified by the coordinator.

- Once the client communications are completed, the coordinator returns to sleep.
  - Low duty cycle operation with long beacon intervals requires precise timing which can be expensive;
  - Nodes only need to be active while a beacon is being transmitted.
  - Nodes may sleep between beacons, thus lowering their duty cycle and extending their battery life.

Non Beacon Enabled Network

- The PAN coordinator, powered from the main source, has its receiver on all the time and can therefore wait to hear from each of these stations.

- Remote units/clients wake up on a regular, yet random, basis to announce their continued presence in the network.

- When an event occurs, the sensor wakes up instantly and transmits the alert.

Outline: IEEE 802.15.4

1 IEEE 802.15.4 Characteristics

2 Network Topology

3 IEEE 802.15.4 PHY Layer

4 IEEE 802.15.4 MAC Layer

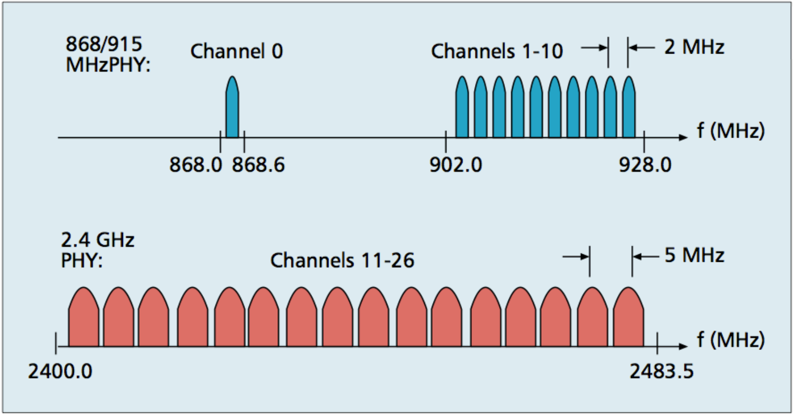
IEEE 802.15.4 Channels (1/)

Channel number	Center (MHz)	Width (MHz)	Region	Rate
k=0	868.3	2 MHz	EU, Japan	20 kb/s
k = 1, 2, . . . , 10	906 + 2(k - 1)	2 MHz	Only USA	40 kb/s
k = 11, 12, . . . , 26	2405 + 5(k - 11)	5 MHz	Worlwide	250 kb/s

IEEE 802.15.4 Channels (2/)

- Twenty-seven frequency channels are available across the three bands.
- The 868/915 MHz PHY supports a single channel between 868.0 and 868.6 MHz, and 10 channels between 902.0 and 928.0 MHz.
- The same hardware can be used for both bands that are close enough in frequency to lower manufacturing costs.
- The 2.4 GHz PHY supports 16 channels between 2.4 and 2.4835 GHz with ample channel spacing (5 MHz) aimed at easing transmit and receive filter requirements.

IEEE 802.15.4 Channels (3/)



Modulation in 868/915 MHz PHY

- The 868/915 MHz PHY uses a simple Direct Sequence Spread Spectrum (DSSS) approach in which each transmitted bit is represented by a **15-chip maximal length sequence** (m-sequence).

- Binary data is encoded by multiplying each m-sequence by +1 or -1, and the resulting chip sequence is modulated onto the carrier using binary phase shift keying (BPSK).

- Differential data encoding is used prior to modulation to allow low-complexity differentially coherent reception.

Modulation in 2.4 GHz PHY

- The 2.4 GHz PHY employs a 16-ary quasi-orthogonal modulation technique based on DSSS methods.

- Binary data are grouped into 4-bit symbols, and each symbol specifies one of 16 nearly orthogonal **32-chip pseudo-noise** (PN) sequences for transmission.

- PN sequences for successive data symbols are concatenated, and the aggregate chip sequence is modulated onto the carrier using Offset Quadrature Phase Shift Keying (O-QPSK) with half-sine pulse shaping.

Modulation Parameters

Frequency	Bit Rate	Symbol Rate	Modulation	Chip Rate	Chip
	(kb/s)	(kbaud)		(Mchip/s)	Modulation
868 MHz	20	20	BPSK	0.3	BPSK
915 MHz	40	40	BPSK	0.6	BPSK
2.4 GHz	250	62.5	16-ary orthogonal	2.0	O-QPSK

Sensitivity

- IEEE 802.15.4 currently specifies **receiver sensitivities** of **-85 dBm** for the **2.4 GHz PHY** and **-92 dBm** for the **868/915 MHz** PHY.

- These values include sufficient margin to cover manufacturing tolerances as well as to permit very low-cost implementation approaches.

- The best devices may be on the order of 10 dB better than the specification.

- The standard specifies that each device shall be capable of transmitting at least 1 mW, but depending on the application needs, the actual transmit power may be lower or higher (within regulatory limits).

Range

- Typical devices (1 mW) are expected to cover a 10-20 m range;
- A star network topology with good sensitivity and a moderate increase in transmit power, can provide a complete home coverage.
- For applications allowing more latency, mesh network topologies provide an attractive alternative for home coverage since each device needs only enough power (and sensitivity) to communicate with its nearest neighbor.

Co-existence Mechanisms

- Devices operating in the 2.4 GHz band must accept interference caused by other services operating in the band.
- IEEE 802.15.4 applications have relatively low quality of service (QoS) requirements, do not occur regularly, and perform multiple retries to complete packet transmissions.
- The excellent battery life requirement of IEEE 802.15.4 applications is achieved in the draft standard by the use of low transmit power and very low duty cycle operation.
- IEEE 802.15.4 devices sleep 99.9 percent of the time, and employ low-power spread spectrum transmissions, and are among the best neighbors in the 2.4 GHz band.

Packet Structure (1/)

- Each packet, or PHY protocol data unit (PPDU), contains a synchronization header (preamble plus start of packet delimiter), a PHY header to indicate the packet length, and the payload, or PHY service data unit (PSDU).

- The 32-bit preamble is designed for acquisition of symbol and chip timing, and in some cases may be used for coarse frequency adjustment.

- Within the PHY header, 7 bits are used to specify the length of the payload (in bytes). This supports packets of length 0-127 bytes.

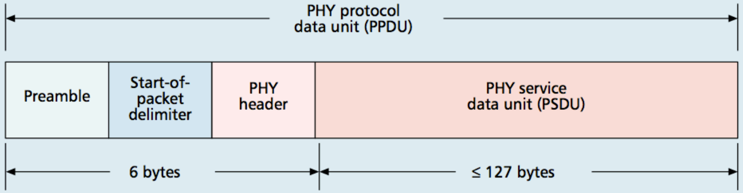
Packet Structure (2/)

- Typical packets sizes for home applications such as monitoring and control of security, lighting, air conditioning, and other appliances are expected to be on the order of 30-60 bytes.

- More demanding applications such as interactive games and computer peripherals, or multihop applications with more address overhead, may require larger packet sizes.

- Adjusting for the transmission rates in each band, the maximum packet durations are 4.25 ms for the 2.4 GHz band, 26.6 ms for the 915 MHz band, and 53.2 ms for the 868 MHz band.

Packet Structure (3/)


PHY protocol data unit (PPDU)
Preamble
Start-of-packet delimiter
PHY header
PHY service data unit (PSDU)
6 bytes
≤ 127 bytes

PHY packet fields:

- Preamble (32 bits) — synchronization
- Start-of-packet delimiter (8 bits) — signify end of preamble
- PHY header (8 bits) — specify length of PSDU
- PSDU (≤ 127 bytes) — PHY layer payload

Outline: IEEE 802.15.4

1 IEEE 802.15.4 Characteristics

2 Network Topology

3 IEEE 802.15.4 PHY Layer

4 IEEE 802.15.4 MAC Layer

CSMA-CA in a Non-Beacon Enabled Network Slotted

- When a device wishes to transmit in a non-beacon-enabled network, it first checks if another device is currently transmitting on the same channel.

- If so, it may back off for a random period, or indicate a transmission failure if unsuccessful after some retries.

- Acknowledgment frames confirming a previous transmission do not use the CSMA mechanism since they are sent immediately following the previous packet.

Slotted CSMA-CA in a Beacon Enabled Network Slotted

- In a beacon-enabled network, any device wishing to transmit during the contention access period waits for the beginning of the next time slot.
- It then determines if another device is currently transmitting in the same slot.
- If another device is already transmitting in the slot, the device backs off for a random number of slots or indicates a transmission failure after some retries.
- In addition, in a beacon-enabled network, acknowledgment frames do not use CSMA.

Questions?

References

The course was prepared based on several web references mainly:

- E. Ferro and F. Potori, Bluetooth and Wi-Fi Wireless Protocols- Survey and Comparison, IEEE Wireless Communication, 2005.
- Xavier Lagrange, Laurence Rouillé, Technologie Bluetooth, Techniques de l'ingénieur, 2007.
- Ed Callaway, Paul Gorday, Lance Hester, Jose A. Gutierrez, Marco Naeve, Bob Heile and Venkat Bahl Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks, IEEE In-Home Networking, 2002.
- Bluetooth, Lecture notes of Prof. Jean-Philippe Muller.
- Wikipedia