IEEE 802.15.4 – 2006 standard

Evangéline BENEVENT

Università Mediterranea di Reggio Calabria
DIMET

IEEE 802.15.4 – 2006 standard

- Title of the IEEE 802.15.4 standard:

**Wireless Medium Access Control (MAC)
and Physical Layer (PHY) Specifications
for Low-Rate Wireless Personal Area Network (WPAN).**

www.ieee802.org

IEEE 802.15.4 – 2006 standard

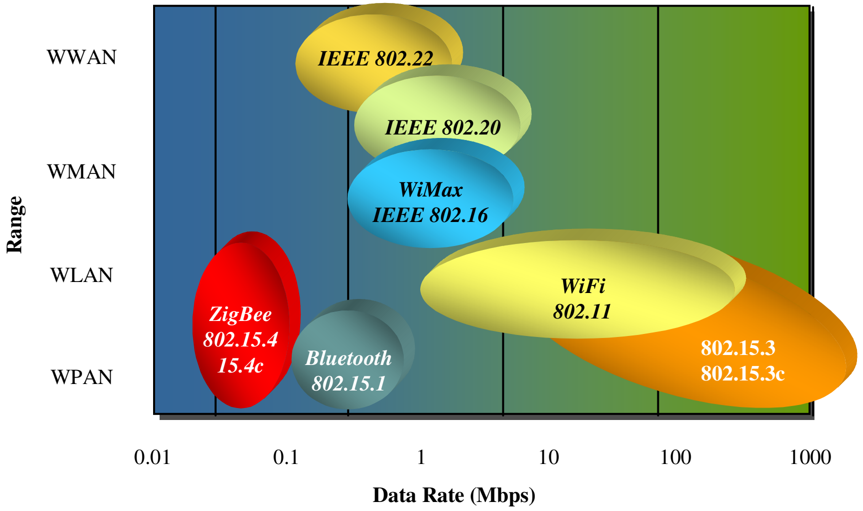
- Background and context
- General description
- PHY specification
- MAC sublayer specification

IEEE 802.15.4 – 2006 standard

- Background and context
- General description
- PHY specification
- MAC sublayer specification

IEEE 802.15.4 – 2006 standard

- Background and context
  - The IEEE 802 LAN/MAN standards committee develops local area network standards and metropolitan area network standards.
  - The IEEE 802.15 working group concerns Wireless Personal Area Network.
  - The IEEE 802.15.4 was chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity. It is operating in an unlicensed, international frequency band.

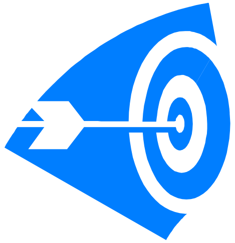


IEEE 802.15.4 – 2006 standard

- Background and context
  - Motivation for standard
    - The 802.15.4 standard was introduced by the IEEE to fill a **niche left by the existing wireless network standards**, which included:
      - IEEE 802.15.1: Bluetooth, which is relatively low-power, low-rate wireless network technology, intended for point-to-point communications,
      - IEEE 802.15.3: high-rate WPAN (Wireless Personal Area Network).
    - High-rate WPAN was driven by applications requiring high data rates and/or wide spatial coverage, often involving complex solutions with non-trivial power requirements. However, not all applications have such demanding needs – some network applications involve the infrequent exchange of relatively small amount of data over restricted areas (for example, a home temperature monitoring and control network). Such applications are diverse in nature and represent considerable **market potential.**

IEEE 802.15.4 – 2006 standard

- Background and context
  - Motivation for standard
    - Bluetooth was not designed for multiple-node networks, therefore the IEEE devised a WPAN standard based on a new set of criteria:
      - Very low complexity,
      - **Ultra-low power consumption,**
      - Low data rate,
      - Relatively short radio communication range,
      - Use of unlicensed radio bands,
      - Easy installation,
      - **Low cost.**
    - The IEEE 802.15.4 standard was born!



IEEE 802.15.4 – 2006 standard

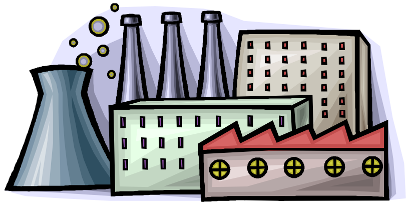
- Background and context
  - Motivation for standard

    - A central feature of the standard is the requirement for **extremely low power consumption.**
    - The motivation for this strict power requirement is to enable the use of battery-powered network devices that are completely free of cabling (no network or power cables), allowing them to be installed:
      - easily and cheaply (no costly cable installation needed),
      - possibly in locations where cables would be difficult or impossible to install.
    - However, low power consumption necessitates short ranges.

IEEE 802.15.4 – 2006 standard

- Background and context
  - Application areas

&



- The applications of IEEE 802.15.4 based networks are wide ranging, covering both **industrial and domestic use.**
- Essentially, for IEEE 802.15.4 to be used in a networking solution, the required **data rate** must be **low** (≤ 250 kbps) and the **maximum range** for communicating devices must be **short**.
- In addition, a device with an **autonomous power supply** (no power cables) must have an extremely low power consumption. If these criteria are met, IEEE 802.15.4 may provide the ideal networking solution, particularly when cost and installation are significant issues.

IEEE 802.15.4 – 2006 standard

- Background and context
  - Application areas
    - The main fields of application of IEEE 802.15.4 are:

HOME AUTOMATION

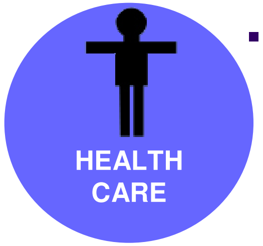
- Home automation and security: a wireless PAN provides a low-cost solution for electronic control within the home (for heating, ventilation, air-conditioning, lighting, doors, locks…). Another important application within the home is security – both intruder and fire detection.

CONSUMER PRODUCTS

- Consumer products: wireless PANs can be built into consumer electronics products. The most obvious example is to provide a common remote control for the various components of a home entertainment system (TV, audio…). Other examples are computer systems and toys, in which a wireless radio link may be used to replace a point-to-point cable link (such as between a mouse and a PC).

IEEE 802.15.4 – 2006 standard

- Background and context
  - Application areas
    - The main fields of application of IEEE 802.15.4 are:



- Healthcare: this field employs sensors and diagnostic devices that can be networked by means of a wireless PAN. Applications include monitoring during healthcare programs such as fitness training, in addition to medical applications.

- Vehicle monitoring: vehicles usually contain many sensors and diagnostic devices, and provide ideal applications for wireless PANs. A prime example is the use of pressure sensors in tires, which cannot be connected by cables.

IEEE 802.15.4 – 2006 standard

- Background and context
  - Application areas
    - The main fields of application of IEEE 802.15.4 are:

- Agriculture: wireless PANs can help farmers monitor land and environmental conditions in order to optimize their crop yields. Such networks can operate at very low data rates and latencies, but require wide geographical coverage – the latter issue is addressed by using network topologies that allow the relaying of messages across the network.

IEEE 802.15.4 – 2006 standard

- Background and context
  - Radio frequencies and data rates
    - IEEE 802.15.4 was designed to operate in unlicensed radio frequency bands. The unlicensed RF bands are not the same in all territories of the world, but IEEE 802.15.4 employs three possible bands, at least one of this should be available in a given territory. The three bands are centered on the following frequencies: 868, 915 and 2400 MHz.

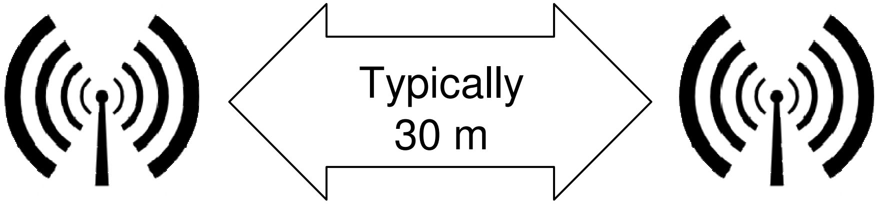
RF band	Frequency range	Data rate	Channel number(s)	Geographical area
868 MHz	868.3 MHz	20 kbps	0 (1 channel)	Europe
915 MHz	902-928 MHz	40 kbps	1-10 (10 channels)	America, Australia
2400 MHz	2405-2480 MHz	250 kbps	11-26 (16 channels)	Worldwide

IEEE 802.15.4 – 2006 standard

- Background and context
  - Radio frequencies and data rates
    - The 868 and 915 MHz frequency bands offer certain advantages such as fewer users, less interference, and less absorption and reflection, but the **2.4 GHz band is far more widely adopted** for a number of reasons:
      - Worldwide availability for unlicensed use,
      - Higher data rate (250 kbps) and more channels,
      - Lower power (transmit/receive are on for a shorter time due to higher data rate),
      - RF band more commonly understood and accepted by the marketplace (also used by Bluetooth and the IEEE 802.11 standard).
    - IEEE 802.15.4 includes **energy detection functionality** that can be used by higher software layers to avoid interference between radio communications.

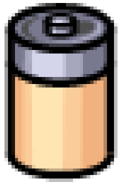
IEEE 802.15.4 – 2006 standard

- Background and context
  - Radio frequencies and data rates
    - The **range of a radio transmission** is dependent on the operating environment, for example, indoors and outdoors. With a standard device (around 0 dBm output power), a range of over 200 meters can typically be achieved in open air. In a building, this can be reduced due to absorption, reflection, diffraction and standing wave effects caused by walls and other solid objects, but **typically a range of 30 meters** can be achieved.
    - High power modules (greater than 15 dBm output power) can achieve a range of five times greater than a standard module.



IEEE 802.15.4 – 2006 standard

- Background and context
  - Achieving low power consumption
    - An important criterion of the IEEE 802.15.4 standard is the provision for building autonomous, low-powered devices. Such devices may be **battery-powered or solar powered**, and require the ability to go to sleep or shut down. There are many wireless applications that require this type of device.
    - **From a user perspective, battery power has certain advantages:**
      - Easy and low-cost installation of devices: no need to connect separate power supply,
      - Flexible location of devices: can be installed in difficult places where there is no power supply, and can even be used as mobile devices,
      - Easily modified network: devices can easily be added or removed, on a temporary or permanent basis.

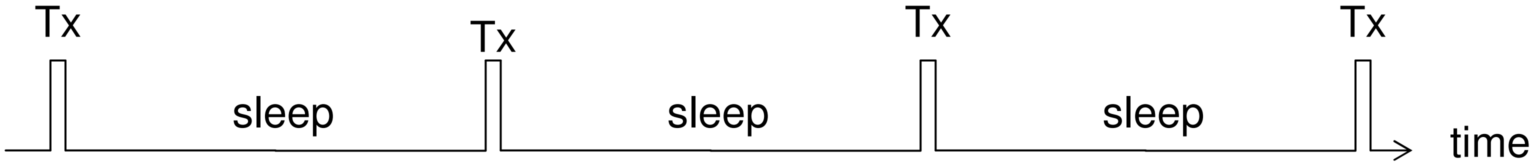


IEEE 802.15.4 – 2006 standard

- Background and context
  - Achieving low power consumption
    - A typical battery-powered network device presents significant technical challenges for battery usage. Since these devices are generally small, they use low-capacity batteries. Infrequent maintenance device is often another requirement, meaning long periods between battery replacement and the need for long life batteries. Battery use must therefore be carefully managed to **make optimum use of very limited power resources over an extended period of time.**
    - **Low duty cycle**: most of the power consumption of a wireless network device corresponds to the times when the device is transmitting. The transmission time as a proportion of the time interval between transmissions is called the duty cycle. Battery use is optimized in IEEE 802.15.4 devices by using extremely low duty cycles.

IEEE 802.15.4 – 2006 standard

- Background and context
  - Achieving low power consumption
    - **Low duty cycle**: this is helped by making the transmission times short and the time interval between transmissions long. In all cases, when not transmitting, the device should revert to a low-power sleep mode to minimize power consumption.



- **Modulation**: the modulation schemes used to transmit data (BPSK – Binary Phase Shift Keying – for 868/915 MHz, O-QPSK – Offset Quadrature Phase Shift Keying – for 2.4 GHz) minimize the power consumption by using a peak-to-average power ratio of one.

IEEE 802.15.4 – 2006 standard

- Background and context
- General description
- PHY specification
- MAC sublayer specification

IEEE 802.15.4 – 2006 standard

- General description
  - Specification of the PHY and MAC layer.
  - Low data rate: < 250 kbps.
  - Personal operating space: 10 m.

  - 2 device types in LR-WPAN:
    - FFD (full-function device), PAN coordinator, coordinator, device.
    - RFD (reduced-function device), can talk only with a FFD.

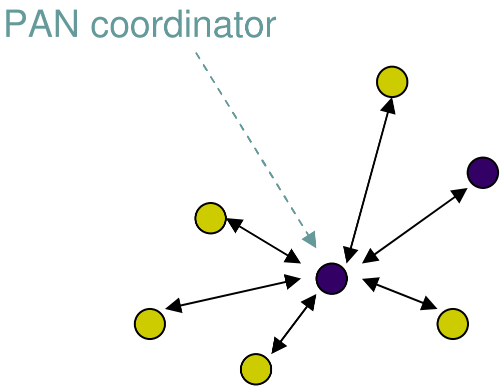
  - 2 topologies:
    - Star topology,
    - Peer-to-peer topology.

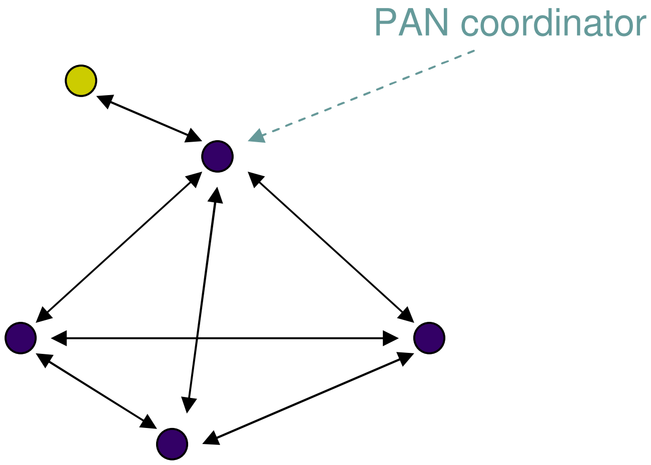
IEEE 802.15.4 – 2006 standard

- General description
  - Star topology:
  - Peer-to-peer topology:

🟣 FFD

🟡 RFD

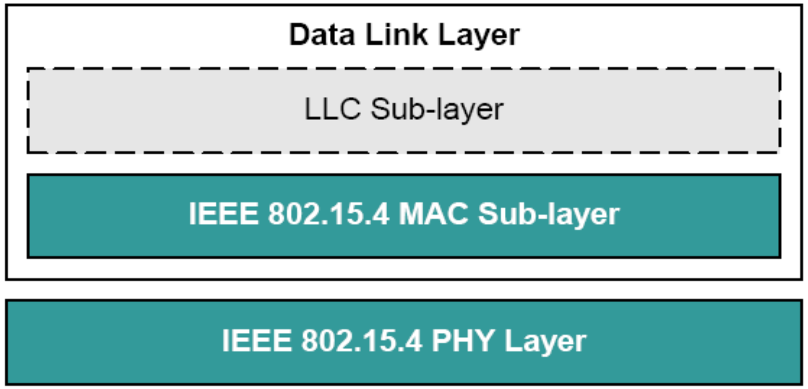




- PAN coordinator: mains powered.
- RFD: battery powered.

IEEE 802.15.4 – 2006 standard

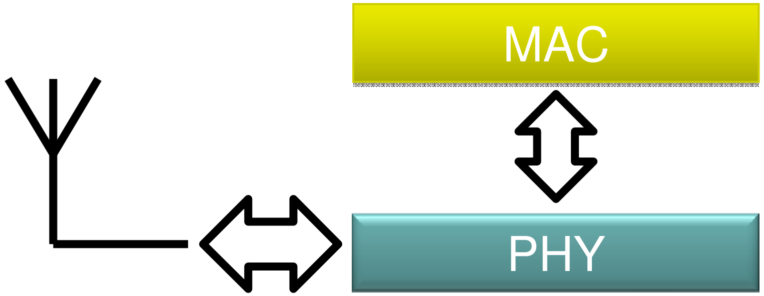
- General description
  - Architecture: OSI (open systems interconnection) 7-layer model.
  - LR-WPAN:
    - PHY layer: RF transceiver + low-level control mechanism,
    - MAC sublayer: access to the physical channel for all types of transfer,
    - Upper layers: network and application layer, outside the scope of this standard.



(LLC: Logical Link Control)

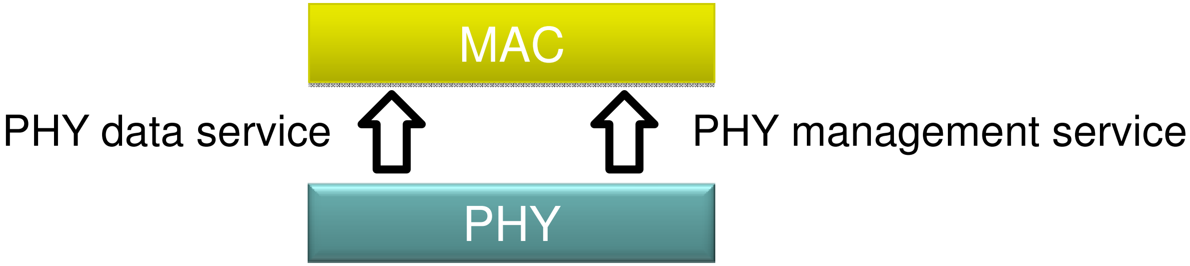
IEEE 802.15.4 – 2006 standard

- General description
  - Physical layer (PHY)
    - The PHY layer is concerned with the interface to the physical transmission medium (radio in this case), exchanging data bits with this medium, as well as exchanging data bits with the layer above (the MAC sublayer).
    - More specifically, its responsibilities towards the physical radio medium include:
      - Channel assessment,
      - Bit-level communications (bit modulation, bit demodulation, packet synch.).



IEEE 802.15.4 – 2006 standard

- General description
  - Physical layer (PHY)
    - The physical layer also offers the following services to the MAC sublayer:
      - PHY data service: provides a mechanism for passing data to and from the MAC sublayer,
      - PHY management service: provides mechanisms to control radio communication settings and functionality from the MAC sublayer.



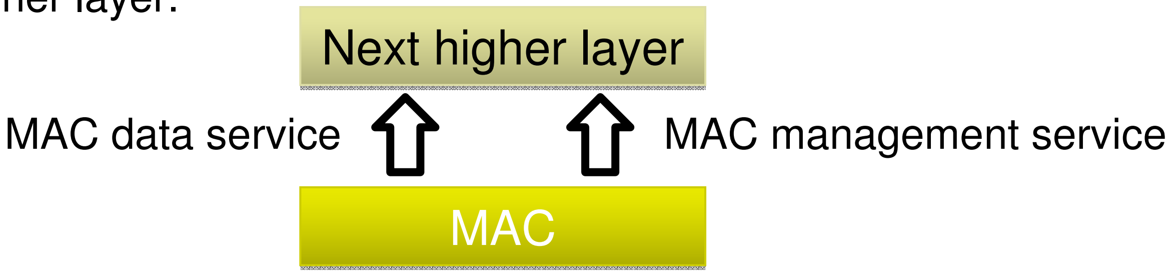
    - Information used to manage the PHY layer is stored in a database referred to as the PHY PIB (PAN Information Base).

IEEE 802.15.4 – 2006 standard

- General description
  - Medium Access Control (MAC) sublayer
    - The main responsibilities of the MAC sublayer are as follows:
      - Providing services for associating/disassociating devices with the network,
      - Providing access control to shared channels,
      - Beacon generation,
      - Guaranteed timeslot management (if applicable).

IEEE 802.15.4 – 2006 standard

- General description
  - Medium Access Control (MAC) sublayer
    - The MAC sublayer also offers the following services to the next higher layer:
      - MAC Data Service (MCPS): provides a mechanism for passing data to and from the next higher layer,
      - MAC Management Services (MLME): provides mechanisms to control settings for communication, radio and networking functionality, from the next higher layer.



    - Information used to manage the MAC sublayer is stored in a database referred to as the MAC PIB (MAC PAN Information Base).

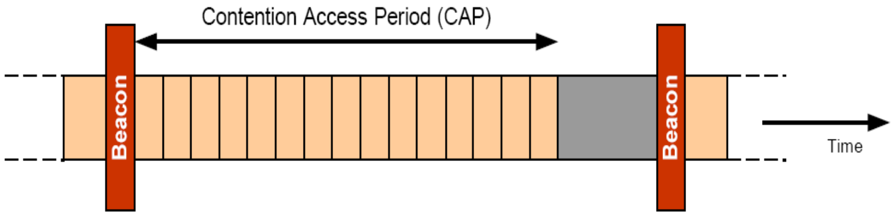
IEEE 802.15.4 – 2006 standard

- General description
  - Data frames and **acknowledgments**
    - Communications in an IEEE 802.15.4 network are based on a system of data and MAC command frames, and optional acknowledgments.
    - When a node sends a message to another node, the receiving node can return an acknowledge message. This simply confirms that it has received the original message and does not indicate that any action has been taken as a result of the message.
    - Acknowledgments are provided by the MAC sublayer.

IEEE 802.15.4 – 2006 standard

- General description
  - **Data transfer for a beacon enabled mode**
    - In this mode, the coordinator sends out a periodic train of beacon signals containing information that allows network nodes to synchronize their communications. A beacon also contains information on the data pending for the different nodes of the network.
    - Normally, two successive beacons mark the beginning and end of a **superframe**. A superframe contains **16 timeslots** that can be used by nodes to communicate over the network. The total time interval of these timeslots is called **Contention Access Period (CAP) during which nodes can attempt to communicate using CSMA/CA.**

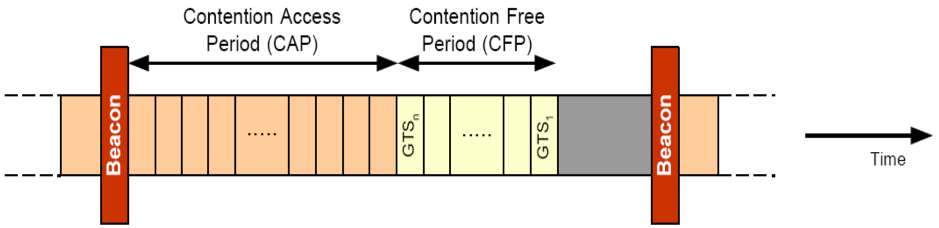
Superframe structure



IEEE 802.15.4 – 2006 standard

- General description
  - Data transfer for a beacon enabled mode
    - A node can also request to have particular timeslots (from the 16 available) assigned to it. These are consecutive timeslots called **Guaranteed Timeslots** (GTSs). They are located after the CAP and the total time interval of all GTSs (for all nodes) is called the Contention Free Period (CFP). Communication in the CFP does not require use of CSMA/CA. Use of GTSs reduces the CAP.
    - It is possible to have a dead period at the end of the superframe (before the next beacon). This allows network devices to revert to low-power mode for part of the time, and to save power.

Superframe with GTSs



IEEE 802.15.4 – 2006 standard

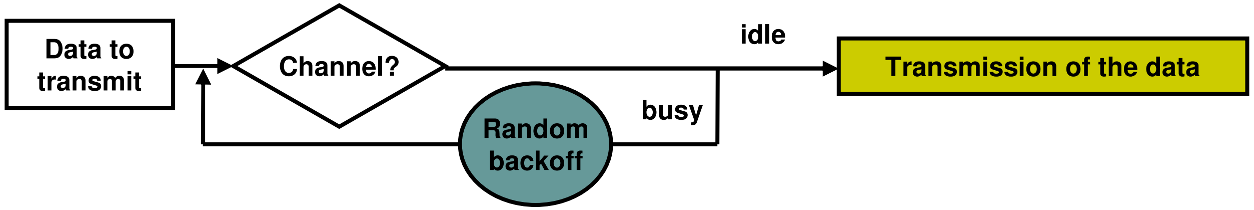
- General description
  - **Data transfer for non-beacon enabled mode**
    - In non-beacon enabled mode, beacons are not transmitted on a regular basis by the coordinator (but can still be requested for the purpose of associating a device with the coordinator).
    - Instead, communications are asynchronous – a device communicates with the coordinator only when it needs to, which may be relatively infrequently. This allows power to be conserved.
    - To determine whether there is data pending for a node, the node must **poll the coordinator** (in a beacon enabled network, the availability of pending data is indicated in the beacons).
    - Non-beacon enabled mode is useful in situations where only **light traffic** is expected between the network nodes and the coordinator. In this case, the use of regular beacons may not be needed and will waste valuable power.

IEEE 802.15.4 – 2006 standard

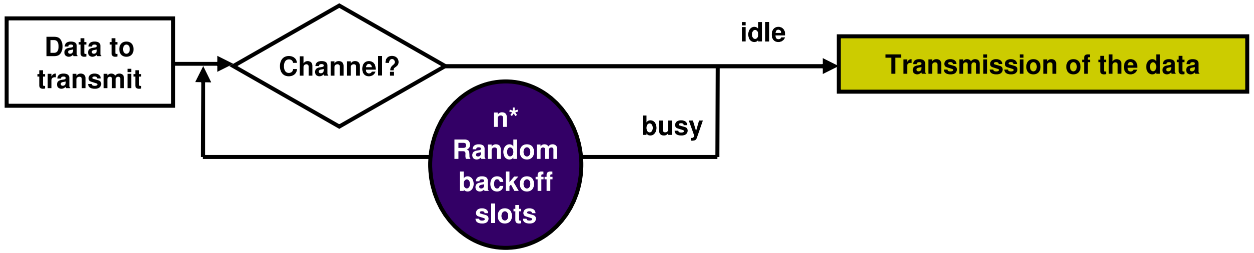
- General description
  - Channel access
    - When transmitting a packet across a network without using Guaranteed Timeslots, the **CSAM-CA** (Carrier Sense Multiple Access – Collision Avoidance) mechanism is implemented to minimize the risk of a collision with another packet being transmitted in the same channel at the same time by another node.
    - The transmitting node performs a **Clear Channel Assessment** (CCA) in which it first listens to the channel to detect whether the channel is already busy. It does not transmit the packet if it detects activity in the channel, but tries again after a random back-off period.
    - A Clear Channel Assessment is required by the MAC sublayer and is implemented by the PHY layer.

IEEE 802.15.4 – 2006 standard

- General description
  - Channel access
    - Unslotted CSMA-CA for nonbeacon-enabled PANs:



    - Slotted CSMA-CA for beacon-enabled PANs:



IEEE 802.15.4 – 2006 standard

- General description
  - Robustness: 3 mechanisms
    - CSMA-CA mechanism (Carrier Sense Multiple Access with Collision Avoidance)
    - Frame acknowledgement
      - If the originator does not receive an acknowledgement after some period, it assumes that the transmission was unsuccessful and retries the frame transmission. If an acknowledgement is still not received after several retries, the originator can chose either to terminate the transaction or to try again.
      - When the acknowledgement is not required, the originator assumes the transmission was successful.
    - Data verification
      - In order to detect bit errors, an Frame Check Sequence (FCS) mechanism, employing a 16 bit Cyclic Redundancy Check (CRC) is used to protect every frame.

IEEE 802.15.4 – 2006 standard

- General description
  - Security
    - A number of security services are included in the IEEE 802.15.4 standard. These are provided by the MAC sublayer which offers three security modes:
      - Unsecured mode,
      - ACL (Access Control List) mode,
      - Secured mode.
    - ACL mode
      - In ACL mode, a node is able to select the other network nodes with which it is prepared to communicate. This is achieved using an Access Control List, maintained in the device, which contains the addresses of nodes with which communication is allowed. The source node of an incoming message is compared against the list, and the result is passed to the higher layers which decide whether to accept or reject the message.

IEEE 802.15.4 – 2006 standard

- General description
  - Security
    - Secured mode
      - In secured mode, seven security suites are available, each incorporating a different combination of the following security options. In each case, an AES (Advanced Encryption Standard) algorithm is used.

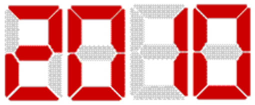
- Access control: this service is as described above for ACL mode, except messages which come for unauthenticated sources are not passed up to the higher layers.

- Encryption: data is encrypted at the source and decrypted at the destination using the same key. Only devices with the correct key can decrypt the encrypted data. Only beacon, command and data payloads can be encrypted.

IEEE 802.15.4 – 2006 standard

- General description
  - Security
    - Secured mode

- <u>Integrity</u>: this service adds a Message Integrity Code (MIC) to a message, which allows the detection of any tampering of the message by devices without the correct encryption/decryption key.



- <u>Sequential freshness</u>: a frame counter is added to a message, which helps a device to determine how recent a received message is. The appended value is compared to a value stored in the device (which is the frame counter value of the last message received). This value only indicates the order of messages and does not contain time/date information. This protects against replay attacks in which old messages are later re-sent to a device.

IEEE 802.15.4 – 2006 standard

- Background and context
- General description
- PHY specification
- MAC sublayer specification

IEEE 802.15.4 – 2006 standard

- PHY specification
  - Operating frequency range:
    - 3 bands:
      - 868-868.6 MHz (e.g., Europe),
      - 902-928 MHz (e.g., North America),
      - 2400-2483.5 MHz (worldwide).
  - 3 modulations:
    - BPSK (Binary Phase-Shift Keying),
    - ASK (Amplitude Shift Keying),
    - O-QPSK (Offset Quadrature Phase-Shift Keying).

IEEE 802.15.4 – 2006 standard

- PHY specification
  - Features of frequency bands:

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868-868.6	300	BPSK	20	20	Binary
	902-928	600	BPSK	40	40	Binary
868/915 (optional)	868-868.6	400	ASK	250	12.5	20-bit PSSS
	902-928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868-868.6	400	O-QPSK	100	25	16-ary orthogonal
	902-928	1000	O-QPSK	250	62.5	16-ary orthogonal
2450	**2400-2483.5**	**2000**	**O-QPSK**	**250**	**62.5**	**16-ary orthogonal**

IEEE 802.15.4 – 2006 standard

- PHY specification
  - Channels assignment:

Channel page (decimal)	Channel page (binary) (b_{31}, b_{30}, b_{29}, b_{28}, b_{27})	Channel number(s) (decimal)	Channel number description
0	00000	0	Channel 0 is in 868 MHz band using BPSK.
		1-10	Channels 1 to 10 are in 915 MHz band using BPSK.
		11-26	**Channels 11 to 26 are in 2.4 GHz band using O-QPSK.**
1	00001	0	Channel 0 is in 868 MHz band using ASK.
		1-10	Channels 1 to 10 are in 915 MHz band using ASK.
		11-26	Reserved.
2	00010	0	Channel 0 is in 868 MHz band using O-QPSK.
		1-10	Channels 1 to 10 are in 915 MHz band using O-QPSK.
		11-26	Reserved.
3-31	00011-11111	reserved	Reserved.

IEEE 802.15.4 – 2006 standard

- PHY specification
  - Physical service specification
    - **Tasks** of the PHY layer:
      - Activation and deactivation of the RF transceiver,
      - Energy detection (ED),
      - Link Quality Indication (LQI),
      - Channel selection,
      - Clear Channel Assessment,
      - To transmit/receive packets:

Interface between MAC layer and physical radio channel

IEEE 802.15.4 – 2006 standard

- PHY specification
  - Physical service specification: **primitives**

Primitives for the PHY data service	Request	Confirm	Indication
PD-DATA	√	√	√

Primitives for the PHY management service	Request	Confirm	Indication
PLME-CCA	√	√	
PLME-ED	√	√	
PLME-GET	√	√	
PLME-SET-TRX-STATE	√	√	
PLME-SET	√	√	

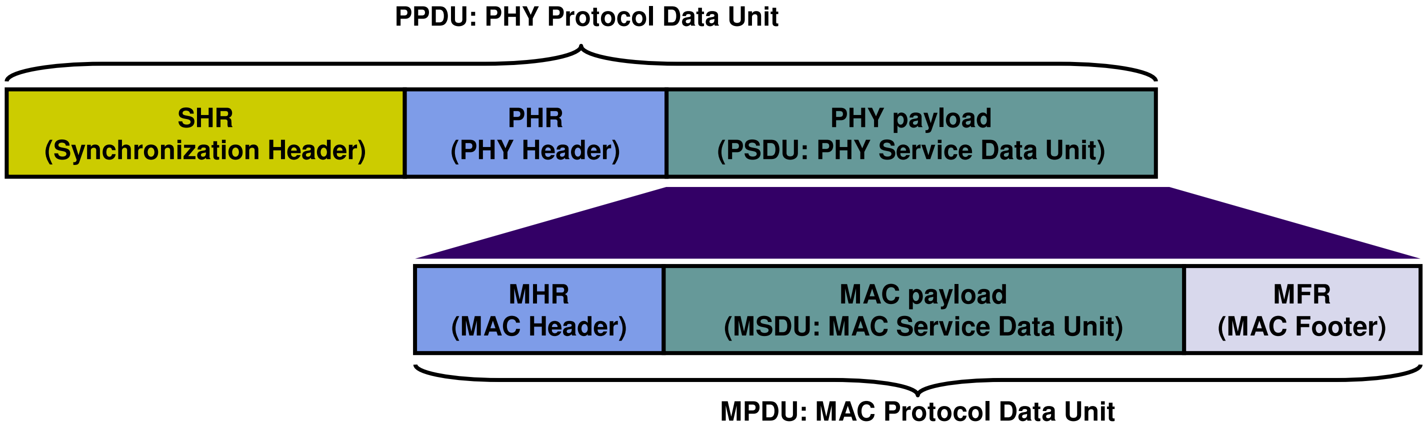
IEEE 802.15.4 – 2006 standard

- PHY specification
  - Physical service specification
    - Example of a primitive for the PHY data service:
      - PD-DATA.indication:

Semantics of the service primitive		**Description**
PD-DATA.indication	(psduLength, psdu, psduLinkQuality)	The primitive is generated by the PHY entity and issued to its MAC sublayer entity to transfer a received PSDU. This primitive will not be generated if the received psduLength field is zero or greater than *aMaxPHYPacketSize*. On receipt of this primitive, the MAC sublayer is notified of the arrival of an MPDU across the PHY data service.

IEEE 802.15.4 – 2006 standard

- PHY specification
  - PPDU format (PHY Protocol Data Unit):
    - Each PPDU packet consists of the following basic components:
      - A synchronization header which allows a receiving device to synchronize and lock onto the bit stream,
      - A PHY header which contains frame length indication,
      - A variable length payload which carries the MAC sublayer frame.


PPDU: PHY Protocol Data Unit
SHR
(Synchronization Header)
PHR
(PHY Header)
PHY payload
(PSDU: PHY Service Data Unit)
MHR
(MAC Header)
MAC payload
(MSDU: MAC Service Data Unit)
MFR
(MAC Footer)
MPDU: MAC Protocol Data Unit

IEEE 802.15.4 – 2006 standard

- PHY specification
  - PPDU format (PHY Protocol Data Unit):
    - Length of the 2.4 GHz O-QPSK PPDU:

SHR (synchronization header)		PHR (PHY header)		PHY payload
Preamble	SFD (start-of-frame delimiter)	Frame length (7 bits)	Reserved (1 bit)	PSDU (PHY service data unit)
4 octets	1 octet	1 octet		0 to 127 octets
00…000	11100101			

IEEE 802.15.4 – 2006 standard

- PHY specification
  - PHY constants (2):
    - aMaxPHYPacketSize = 127 octets,
    - aTurnaroundTime: RX-to-TX or TX-to-RX max. turnaround time = 12 symbol periods (192 us).
  - PIB (PAN information base) attributes (8):
    - phyCurrentChannel,
    - phyChannelSupported,
    - phyTransmitPower,
    - phyCCAMode,
    - phyCurrentPage,
    - phyMaxFrameDuration,
    - phySHRDuration,
    - phySymbolsPerOctet.

IEEE 802.15.4 – 2006 standard

- 2.4 GHz PHY specification
  - Data rate: 250 kb/s.
  - Modulation and spreading:
    - Symbol = 4 bits,
    - Symbol-to-chip mapping (Table), chip = 32 bits,
    - O-QPSK modulation.

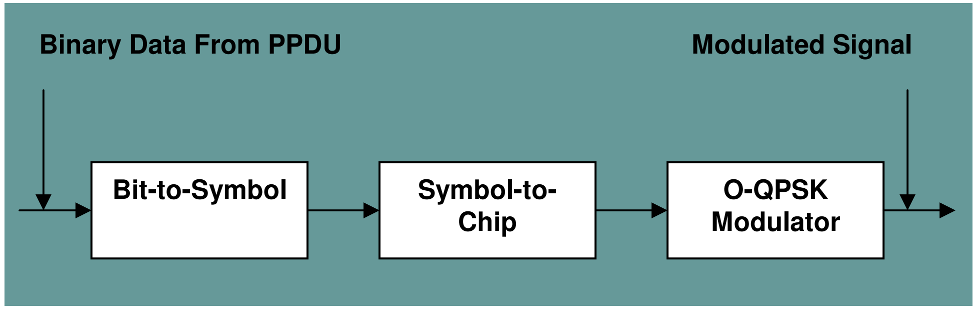
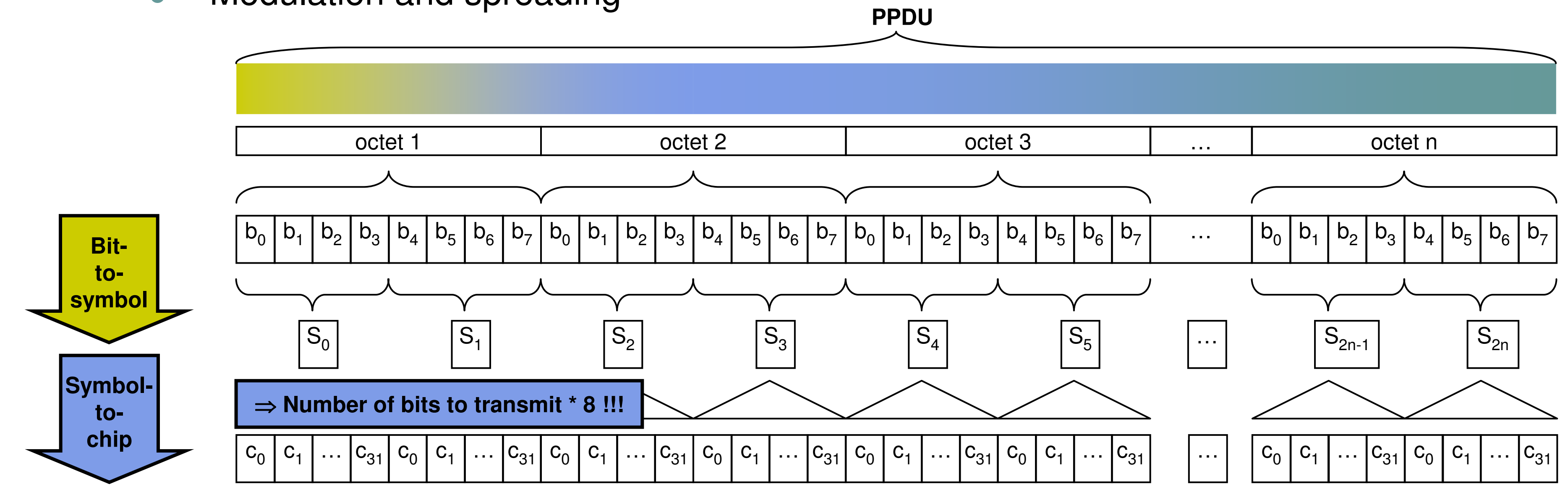


Table of symbol-to-chip mapping

Data symbol (decimal)	Data symbol (binary) (b_0 b_1 b_2 b_3)	Chip values (c_0 c_1 … c_{30} c_{31})
0	0 0 0 0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 0 0 0	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 1 0 0	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	1 1 0 0	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 0 1 0	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	1 0 1 0	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 1 1 0	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	0 0 0 1	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 0 1	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1
11	1 1 0 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 1 1	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 0 1 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	0 1 1 1	1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

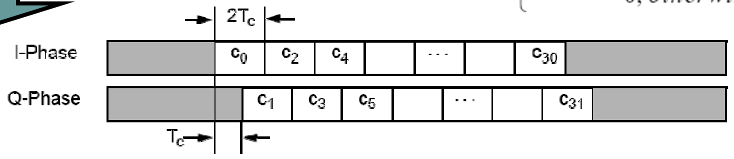
IEEE 802.15.4 – 2006 standard

- 2.4 GHz PHY specification
  - Modulation and spreading

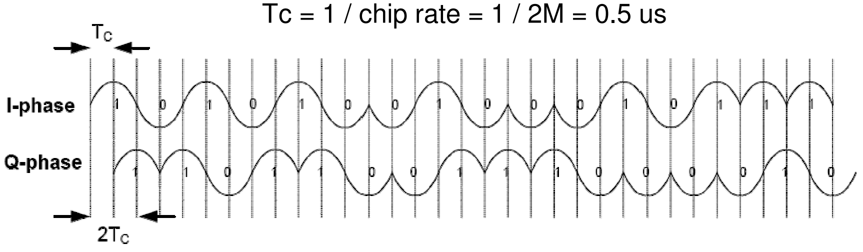


⇒ Number of bits to transmit * 8 !!!

Bit = half-sine pulse shape: $p(t) = \begin{cases} \sin\left(\pi \frac{t}{2T_c}\right), & 0 \le t \le 2T_c \\ 0, & otherwise \end{cases}$



Tc = 1 / chip rate = 1 / 2M = 0.5 us



IEEE 802.15.4 – 2006 standard

- Background and context
- General description
- PHY specification
- MAC sublayer specification

IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Tasks:
    - Generating network beacons if the device is a coordinator,
    - Synchronizing to network beacons,
    - Supporting PAN association and disassociation,
    - Supporting device security,
    - Employing the CSMA-CA (carrier sense multiple access with collision avoidance) mechanism for channel access,
    - Handling and maintaining the GTS (guaranteed time slot) mechanism,
    - Providing a reliable link between two peer MAC entities.

The MAC sublayer handles all access to the physical radio channel.

IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - MAC data service and MAC management service:

Primitives for MAC data service	Request	Confirm	Indication	Response
MCPS-DATA	√	√	√	
MCPS-PURGE	√	√		

Primitives for MAC management service	Request	Confirm	Indication	Response
MLME-ASSOCIATE	√	√	√	√
MLME-DISASSOCIATE	√	√	√	
MLME-BEACON-NOTIFY			√	
MLME-GET	√	√		

IEEE 802.15.4 – 2006 standard

- MAC sublayer specification

Primitives for MAC management service	Request	Confirm	Indication	Response
MLME-GTS	√	√	√	
MLME-ORPHAN			√	√
MLME-RESET	√	√		
MLME-RX-ENABLE	√	√		
MLE-SCAN	√	√		
MLME-COMM-STATUS			√	
MLME-SET	√	√		
MLME-START	√	√		
MLME-SYNC	√		√	
MLME-POLL	√	√		

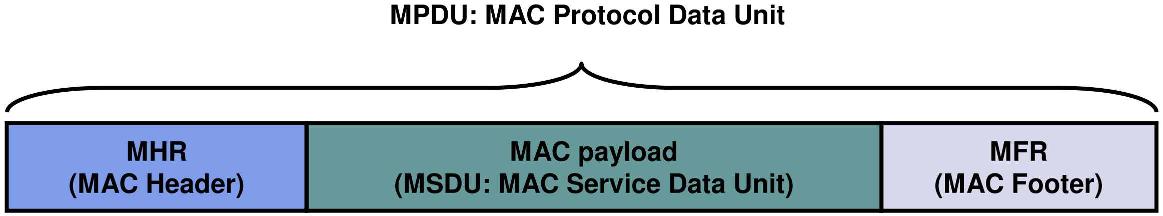
IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Example of a primitive of the MAC management service:
    - Beacon notification primitive: MLME-BEACON-NOTIFY.indication

Semantics of the service primitive		**Description**
MLME-BEACON-NOTIFY.indication	(BSN, PANDescriptor, PendAddrSpec, AddrList, sduLength, sdu)	The primitive is used to send parameters contained within a beacon frame received by the MAC sublayer to the next higher layer.

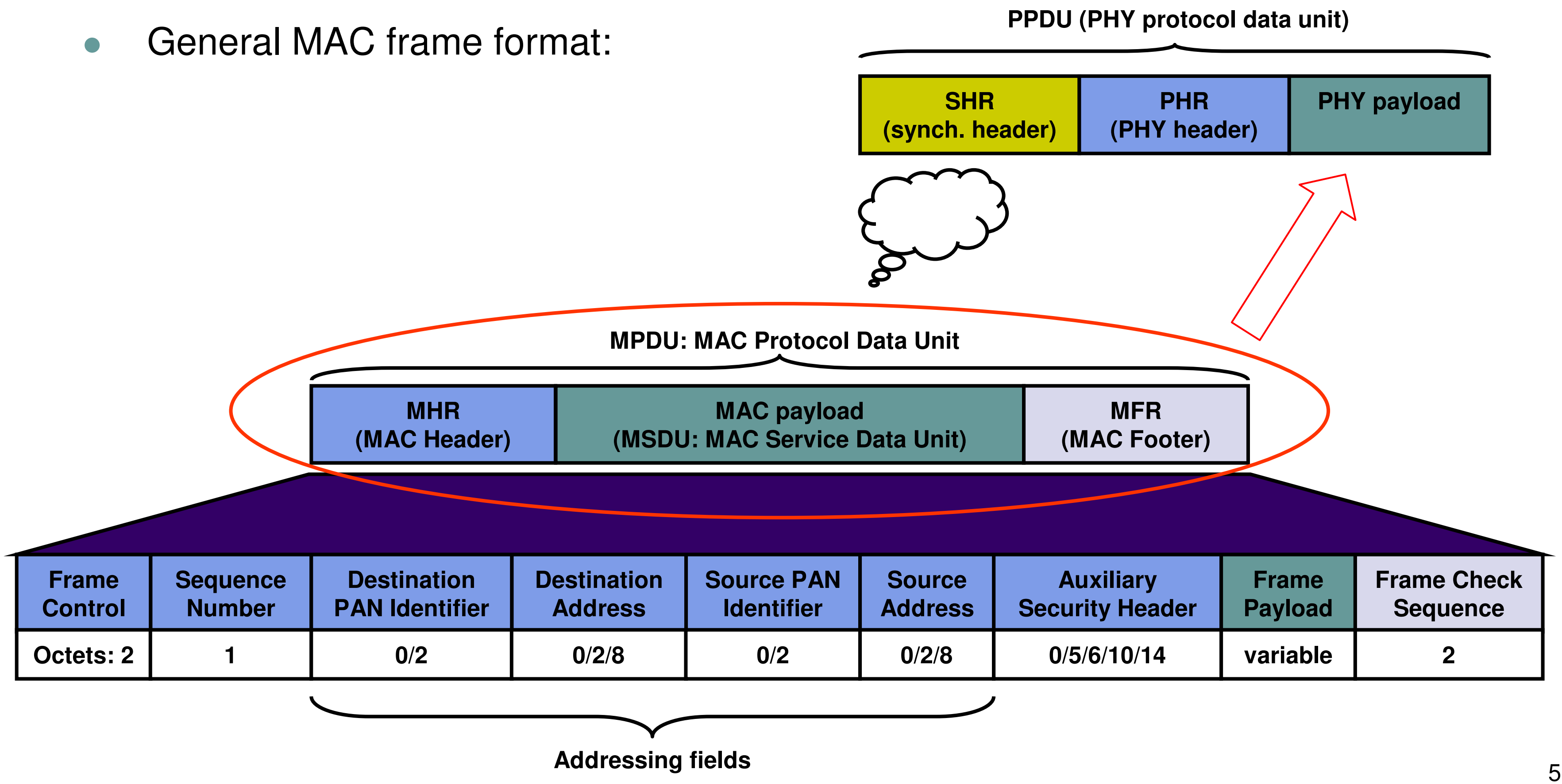
IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - MAC frame format:
    - 4 frame types:
      - Beacon,
      - Data,
      - Acknowledgment,
      - MAC command.
    - General MAC frame format:



IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - General MAC frame format:



PPDU (PHY protocol data unit)
SHR (synch. header)
PHR (PHY header)
PHY payload
MPDU: MAC Protocol Data Unit
MHR (MAC Header)
MAC payload (MSDU: MAC Service Data Unit)
MFR (MAC Footer)

Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Frame Payload	Frame Check Sequence
Octets: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	variable	2

IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Constants (15):

Constant	Description	Value
…	…	…
aExtendedAddress	The 64-bit (IEEE) address assigned to the device.	Device specific
aMaxBeaconPayloadLength	The maximum size, in octets, of a beacon payload.	*aMaxPHYPacketSize-aMaxBeaconOverhead*
aMaxLostBeacons	The number of consecutive lost beacons that will cause the MAC sublayer of a receiving device to declare a loss of synchronization.	4
aMaxMACSafePayloadSize	The maximum number of octets that can be transmitted in the MAC Payload field of an unsecured MAC frame that will be guaranteed not toe exceed *aMaxPHYPacketSize.*	*aMaxPHYPacketSize-aMaxMPDUUnsecured Overhead*
aMaxMACPayloadSize	The maximum number of octets that can be transmitted in the MAC Payload field.	*aMaxPHYPacketSize-aMinMPDUOverhead*
aMaxMPDUUnsecuredOverhead	The maximum number of octets added by the MAC sublayer to the PSDU without security.	25
aMaxSIFSFrameSize	The maximum size of an MPDU, in octets, that can be followed by a SIFS period.	18
aMinMPDUOverhead	The minimum number of octets added by the MAC sublayer to the PSDU.	9
aNumSuperframeSlots	The number of slots contained in any superframe.	16
…	…	…

IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Attributes (32):

Attribute	Identifier	Type	Range	Description	Default
…	…	…	…	…	…
macMaxBE	0x57	Integer	3-8	The maximum value of the backoff exponent, BE, in the CSMA-CA algorithm.	5
macMaxCSMABackoffs	0x4e	Integer	0-5	The maximum number of backoffs the CSMA-CA algorithm will attempt before declaring a channel access failure.	4
macMaxFrameTotalWaitTime	0x58	Integer	See eq.	The maximum number of (…) symbols in a nonbeacon-enabled PAN, to wait either for a frame intended as a response to a data request frame …	…
macMaxFrameRentries	0x59	Integer	0-7	The maximum number of retries allowed after a transmission failure.	3
macMinBE	0x4f	Integer	0-macMaxBE	The minimum value of the backoff exponent (BE) in the CSMA-CA algorithm.	3
…	…	…	…	…	…
macPromiscuousMode	0x51	Boolean	TRUE or FALSE	Indication of whether the MAC sublayer is in a promiscuous (receive all) mode. A value of TRUE indicates that MAC sublayer accepts all frames received from the PHY.	FALSE
macResponseWaitTime	0x5a	Integer	2-64	The maximum time, in multiples of *aBaseSuperframeDuration*, a device shall wait for a response command frame to be available following a request command frame.	32
macRxOnWhenIdle	0x52	Boolean	TRUE or FALSE	Indication on whether the MAC sublayer is to enable its receiver during idle periods. …	FALSE
…	…	…	…	…	…

IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Device management:

How does an IEEE 802.15.4 based network deal
with devices joining and leaving the network?

- PAN coordinator selection
  - All networks must have one and only one PAN coordinator.
  - This must be an FFD.
  - The selection of the PAN coordinator is the first step in setting up an IEEE 802.15.4 based network.
  - Once the PAN coordinator has been established, a PAN ID (identifier) must be assigned to the network. The PAN ID is assigned by the PAN coordinator taking into account the PAN IDs of any PAN coordinators that it can “hear”.

IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Device management:
    - Device association and disassociation

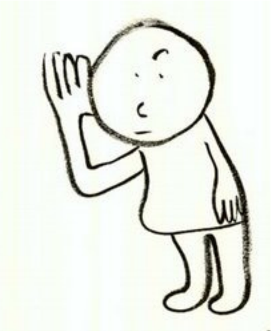
      - In order to join an IEE 802.15.4 based network, a device must first find a coordinator by conducting an active or passive channel scan.
      - The device can then send an association request to the coordinator, which acknowledges the request and then determines whether it has sufficient resources to add the device to its network. The coordinator will then accept or reject the association request.
      - The request to disassociate a device with a network can be made by either the coordinator or the device itself.

IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Device management:
    - Orphan devices
      - A device becomes an **orphan** if it loses communication with its coordinator.
      - An orphan device will attempt to rejoin the coordinator by first performing an orphan channel scan to find the coordinator – this involves sending out an orphan notification command across the relevant frequency channels.
      - On receiving this message, the coordinator checks whether the device was previously a member of its network – if this was the case, it responds with a coordinator realignment command.

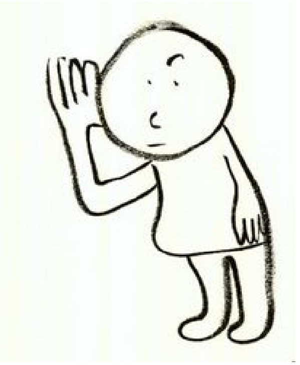
IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Channel management
    - IEEE 802.15.4 offers channel management facilities concerned with allocating channels, ensuring channel availability for transmission and protecting channels from nearby interfering transmissions.
    - IEEE 802.15.4 can scan the channels in a given frequency band, allowing the higher layers to select the appropriate channel.
      - When a network is set up, the channel of operation within the relevant frequency band must be chosen. This is done by the PAN coordinator. IEEE 802.15.4 provides an **energy detection scan** which can be used to select a suitable channel (normally the quietest channel).



IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Channel management
    - When a new device is introduced into a network, it must find the channel being used by the network. The new device is supplied with the PAN ID of the network and performs either of the following scans:



      - **Active channel scan** in which the device sends beacon requests to be detected by one or more coordinators, which then send out a beacon in response,
      - **Passive channel scan** (beacon enabled networks only) in which the device listens for periodic beacons being transmitted by a coordinator.

IEEE 802.15.4 – 2006 standard

- MAC sublayer specification
  - Device addressing
    - Each device in an IEEE 802.15.4 network can have two types of address:
      - **IEEE (MAC) address**: this is a **64-bit** address, allocated by the IEEE, which uniquely identifies the device – no two devices in the world can have the same IEEE address. It is also sometimes called the extended address.
      - **Short address**: this **16-bit** address identifies the node in the network and is local to that network (thus two nodes on separate networks may have the same short address). The short address may be allocated by a coordinator when a node joins a network.
    - The use of 16-bit short addresses rather than 64-bit IEEE addresses allows shorter packets and therefore optimizes use of network bandwidth.

IEEE 802.15.4 – 2006 standard

- Conclusion
  - The IEEE 802.15.4 defines the PHY layer and the MAC sublayer for Low Rate (< 250 kbps) Wireless Personal Area (10 m) Networks.
  - The standard was designed for very low-power application.
  - Three frequency bands are supported:
    - 868 MHz, Europe,
    - 915 MHz, USA,
    - 2.4 GHz, worldwide.
  - The PHY layer is responsible of the interface between the RF transceiver and the MAC sublayer, while the MAC sublayer ensures the access to the physical channels for all types of transfer.

For more details, see the website of the IEEE 802 LAN/MAN Standards Committee: www.ieee802.org and download the IEEE 802.15.4 standard.

IEEE 802.15.4 – 2006 standard

Evangéline BENEVENT

Università Mediterranea di Reggio Calabria
DIMET

Thank you for your attention