Outline

- A preliminary overview
- Propagation characteristics
- ISO-OSI Model
- Physical layer: modulation
- MAC layer:
  - Fixed resource assignment
  - Random access
    - Ethernet (CSMA/CD)
    - WiFi (CSMA/CA)
- Personal Area Networks
  - Bluetooth
  - **Zigbee**
- Cellular network dimensioning
- Cellular networks
  - From GSM (2G) to UMTS (3G)
  - LTE (4G)

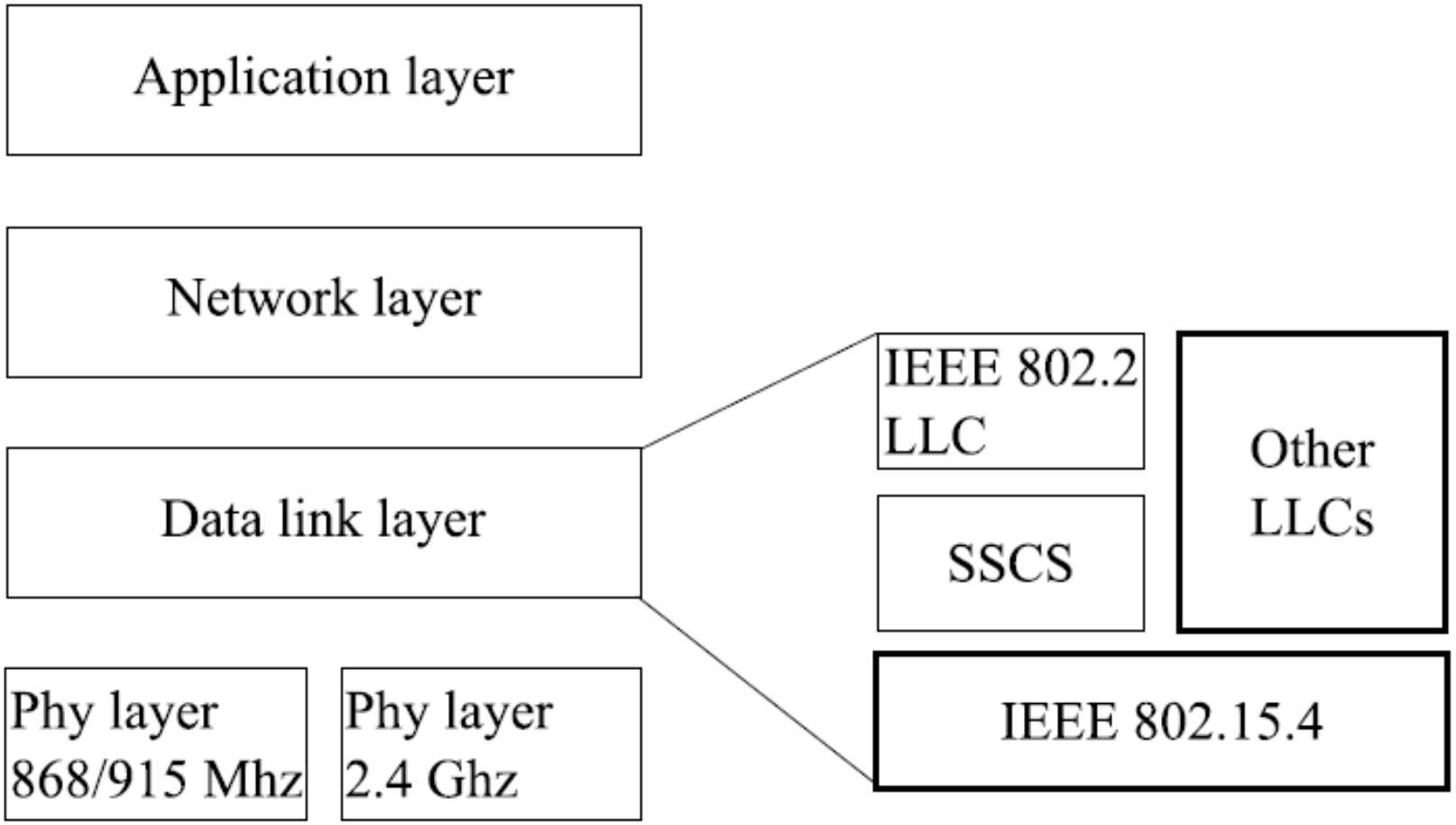
Zigbee

- Born in 2004—other versions in the next years.
- It can guarantee wireless data communication and, at the same time, high energy efficiency.
- It is explicitly designed for low-rate low-power PANs.
- First two layers of the ISO/OSI stack are derived from the IEEE 802.15.4 standard.
- Upon these, the other layers are defined by the ZigBee alliance.

IEEE 802.15.4: Main Functionalities

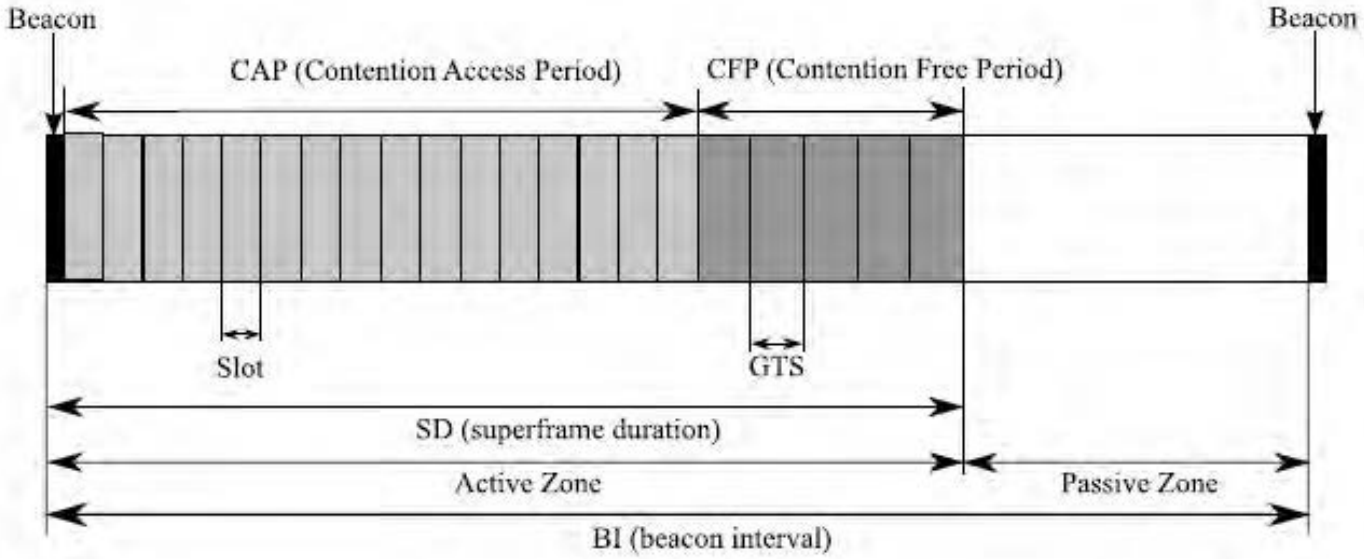
- Channel access management through a CSMA/CA mechanism.
- Reliable communication between two distinct MAC entities.
- Security management through a 128-bit symmetrical Advanced Encryption Standard (AES) key.
- Synchronization management through beacon packets.
- Support of (dis)association from the PAN.
- Management of Guaranteed Time Slots (GTS).

The ISO/OSI Stack of IEEE 802.15.4



Becon-Enabled Mode

- The use of beacon packets allows to synchronize the nodes.
- The time is divided into superframes.
- The nodes have, therefore, higher complexity, but duty cycle and channel access are better managed (GTSs).



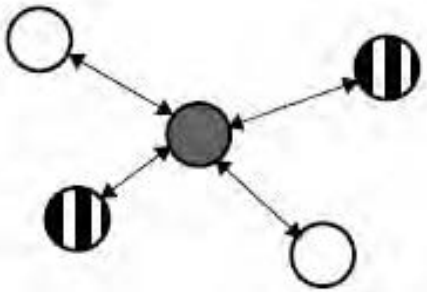
Beaconless Mode

- No synchronization between nodes.
- Nodes' structures are simpler, but, obviously the performance of beacon-enabled networks is better.
- The MAC protocol differs in terms of time management, synchronization, and packet retransmissions.

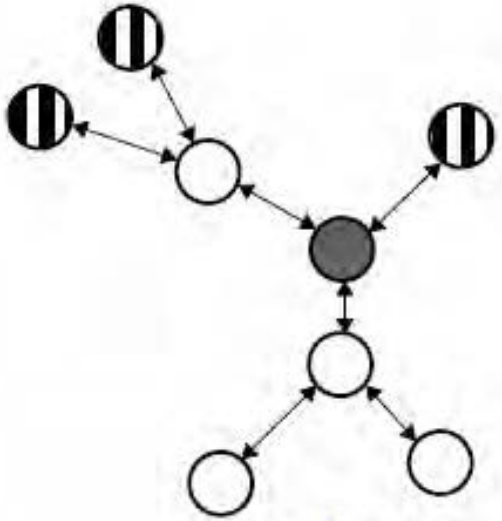
Network Topology

- Devices are grouped into PANs characterized by an identification number (PAN ID).
- At least one node is present and it has the role of coordinator.
- Coordinator tasks includes network initialization (e.g., PAN ID and parameter configuration), nodes' associations, and beacon transmission.
- Additional nodes are end devices with different functionalities.
- Nodes are logically divided into Full Function Devices (FFDs) and Reduced Function Devices (RFD).
- FFDs implement all functionalities of the ZigBee standard and can communicate with all other nodes in their transmission range.

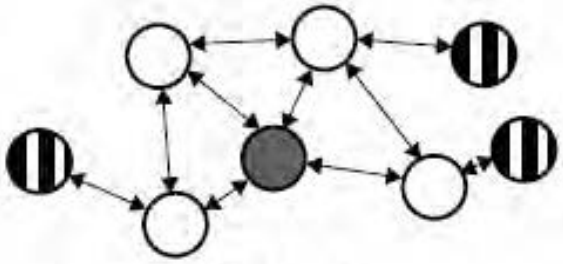
Allowed Topologies



Star



Cluster tree



Mesh

PAN Coordinator

FFD

RFD

Specifications

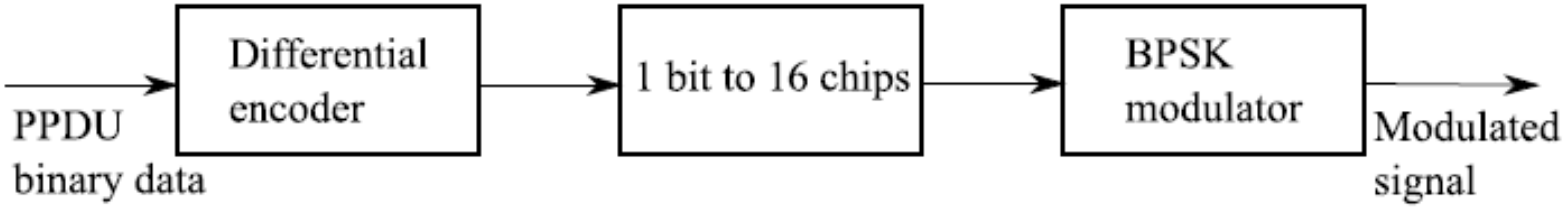
- Three operating frequencies: 868 MHz (Europe), 916 MHz (USA), and 2.4 GHz (worldwide available) $\Longrightarrow$ UNLICESED BANDS!!!
- Co-channel interference with Bluetooth, WiFi, etc.
- Channel allocation:

Channel number	Frequency (MHz)
$k = 0$	868.3
$k = 1, \ldots, 10$	$906 + 2(k - 1)$
$k = 11, \ldots, 26$	$2405 + 5(k - 11)$

- Transmission rates: 20 and 40 kbps (at 868 and 916 MHz, respectively), and 250 kbps (at 2.4 GHz) $\Longrightarrow$ LOW RATES!!!

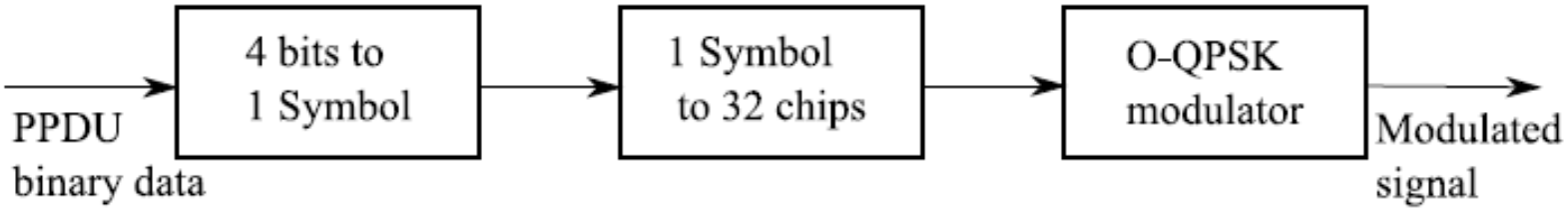
Modulation: 868 MHz and 916 MHz

- Differential encoding of the information bits.
- Direct Sequence Spread Spectrum (DSSS) expansion (factor 16).
- Binary Phase Shift Keying (BPSK) modulation before transmission.
- European and US bands differ for the chip rate.



Modulation: 2.4 GHz

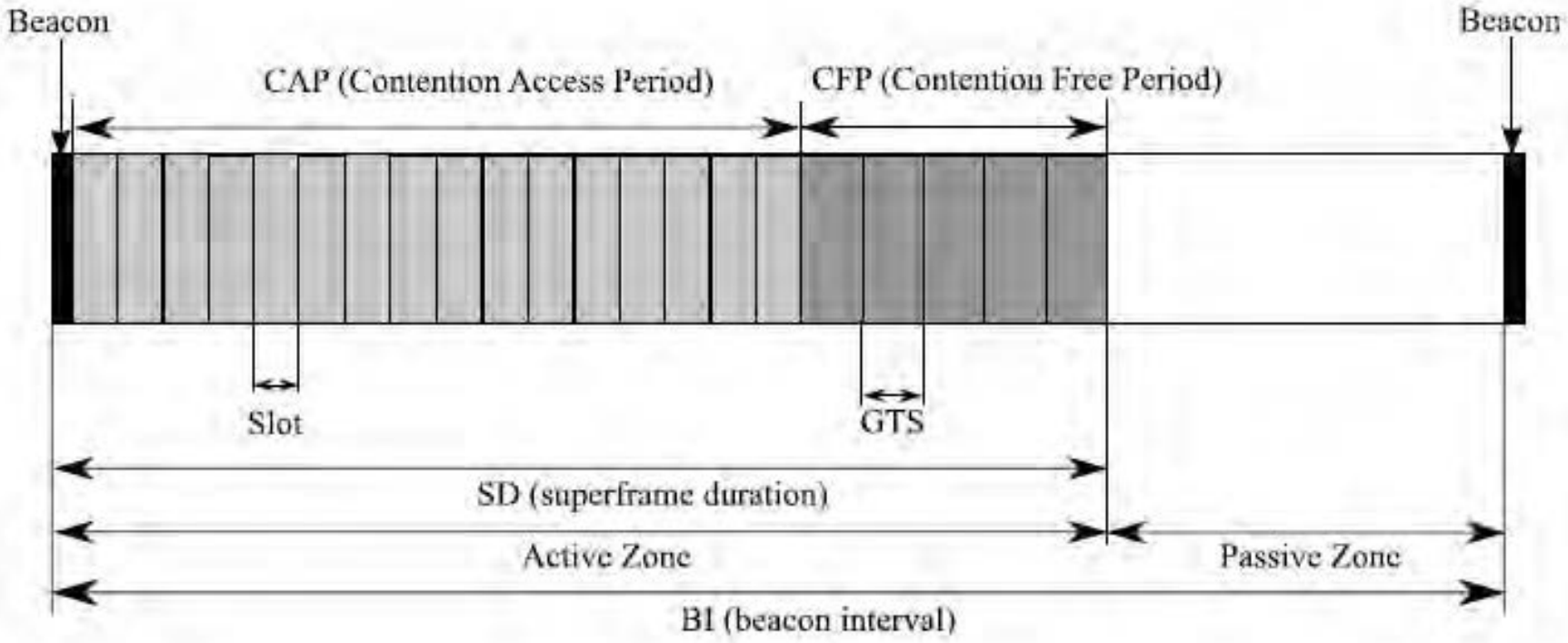
- 4 information bits are encoded with one of the 16 available symbols.
- DSSS spectral expansion (factor 32).
- Offset-Quadrature Phase Shift Keying (O-QPSK) modulation: odd indexes in the in-phase component and even indexes in the quadrature component.
- Lower error probability than WiFi.



Protocol

- The standard defines a Physical Protocol Data Unit (PPDU) with the following field.
  - Synchronization Header (SHR): 5 bytes used for the synchronization.
  - Physical Header (PHR): 1 byte used to carry the frame length.
  - Physical Service Data Unit (PSDU): contains the payload with maximum allowed length of 127 bytes.

Superframe Structure



Superframe Parameters

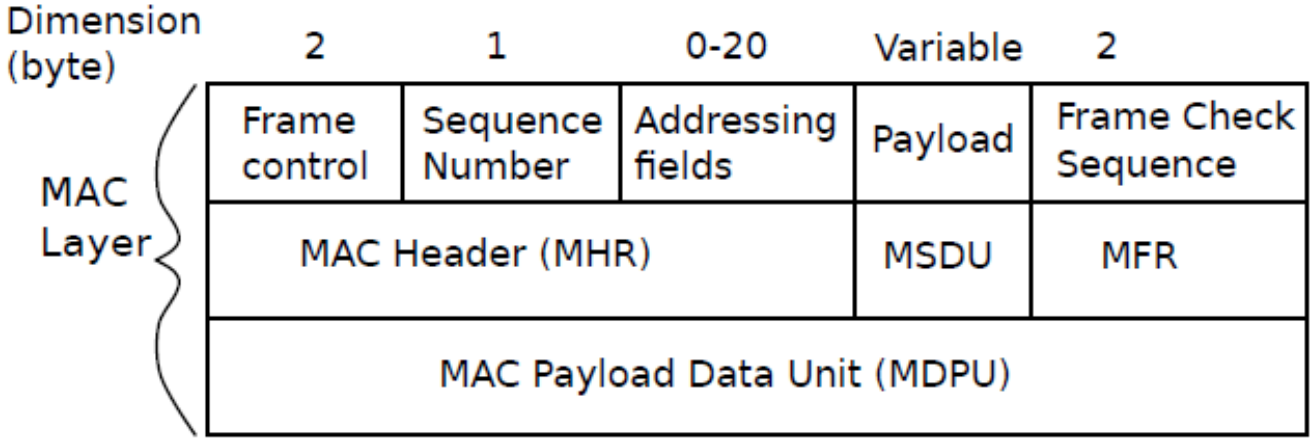
- The length is multiple of a physical modulated symbol $T_{\text{symb}} = 1.6\ \mu\text{s}$ (@ 2.4 GHz).
- $BI = d_{\text{SF}} \cdot 2^{BO}$, where BO (Beacon Order) is in the range [0,15]—15 corresponds to beaconless mode.
- $SD = d_{\text{SF}} \cdot 2^{SO}$, where SO (Superframe Order) is in the range $[0, BO]$. In the standard configuration, 16 slots are in the active zone with duration (in terms of physical symbols) equal to

$$d_{\text{sl}} = \underbrace{\text{aBaseSlotDuration}}_{\text{length when } SO = 0 = d_{\text{SF}}} \cdot 2^{SO}.$$

- Contention Access Period (CAP): the access is performed through CSMA/CA.
- Contention Free Period (CFP): the access is deterministic through a given number of GTSs.

Packet Format

- Beacons: used by the PAN coordinator to send beacons.
- Data: used by the higher levels for data transfer.
- Acknowledgement (ACK): used to confirm the correct receipt of a packet.
- MAC command: used to manage all control information.



CSMA/CA MAC Protocol: Unslotted Version

- The source node waits for a number of slots randomly generated in the interval $[0, 2^{BE_i} - 1]$.
- Once elapsed this time, the node verifies the channel status through a Clear Channel Assessment (CCA), i.e., the energy on the RF interface is measured over $8T_{\text{sym}}$.
- If the energy is above a threshold, the channel is busy; otherwise, it is assumed idle.
- If channel is idle, the node can transmit a packet in its queue. Otherwise, *NB* (number of backoff cycles for this packet) and *m* (maximum number of backoff cycles, denoted as backoff stage) are compared.
- If $NB = m$, the CSMA/CA is declared as failed. Otherwise, *BE* is incremented by 1. If $BE < BE_{\max}$, the procedure is repeated.

CSMA/CA MAC Protocol: Slotted Version

- The main difference is that all operations must be performed in the correspondence of a backoff boundary.
- CCAs of different nodes can collide. Therefore, two CCAs should be performed to prevent from collisions. However, this leads to waste in channel utilization.
- Obviously, in all cases collisions are still possible!!!

Performed Tasks

- Creation and management of the network.
- Choice of the network topology.
- Unicast and multicast routing of packets.
- Security management.
- Management of logical associations between the applications of different nodes (binding).

(ZigBee) Network Layer

- Provides functionalities for multihop communications, but it is not responsible for inter-PAN communications.
- Three classes of nodes are allowed:
  - router: optional node, which acts as a PAN coordinator at MAC level and it is able to relay packets according to the routing protocol;
  - coordinator: it has the same functionalities of a router, but it can set up the network and manage its parameters;
  - end device: it is the same of an end device at MAC level.
- All nodes hold also a neighborhood table, which contains information about all the surrounding nodes in their transmission range.

Routing Algorithms

- Hierarchical Algorithm. It is based on the fact that ZigBee nodes have a direct parent-child degree of kinship with at least another node in the network. However, it exploits sub-optimal paths, which cannot be modified, since no routing tables are held.

- Ad hoc based on Ad hoc On demand Distance Vector (AODV). It is a reactive protocol based on RREQ/RREP packets.

- Neighborhood routing. If the destination address is in the neighborhood table, a direct transmission is performed.

Network Topologies

- Star. No routers are present in the network, only a parent-child communication, and a maximum number of hops equal to two. Simpler but problems if links are not reliable.

- Tree. The PAN coordinator is the root, the routers create the branches, and the end devices are the leaves (no other nodes connected to them). Thanks to the beacon packets and the tree routing algorithm, this topology is energy efficient.

- Mesh. All nodes can communicate with all other nodes in the network, under the constraints given by the transmission range and routing capabilities. The main problem is that beacon mode cannot be employed.

Definitions

- Up to 240 application objects can be configured on each device.
- Each object is associated to an unambiguous number (end-point).
- The interoperability between applications is guaranteed by profiles.
- Data are defined by the couple ID-attributes.
- The operation of mutual associations between couples is denoted as binding.