Applied Wireless Electronics

Grzegorz Budzyń

Lecture 3:
Wireless data transfer – ZigBee

Choose yourself and new technologies

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!

Wrocław University of Technology

EUROPEAN SOCIAL FUND

Project co-financed from the EU European Social Fund

Plan

- Introduction
- Simple solutions
- High performance solutions

Introduction

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!
Wrocław University of Technology
EUROPEAN SOCIAL FUND
Project co-financed from the EU European Social Fund


Building


Energy


Health


Home


Telecom

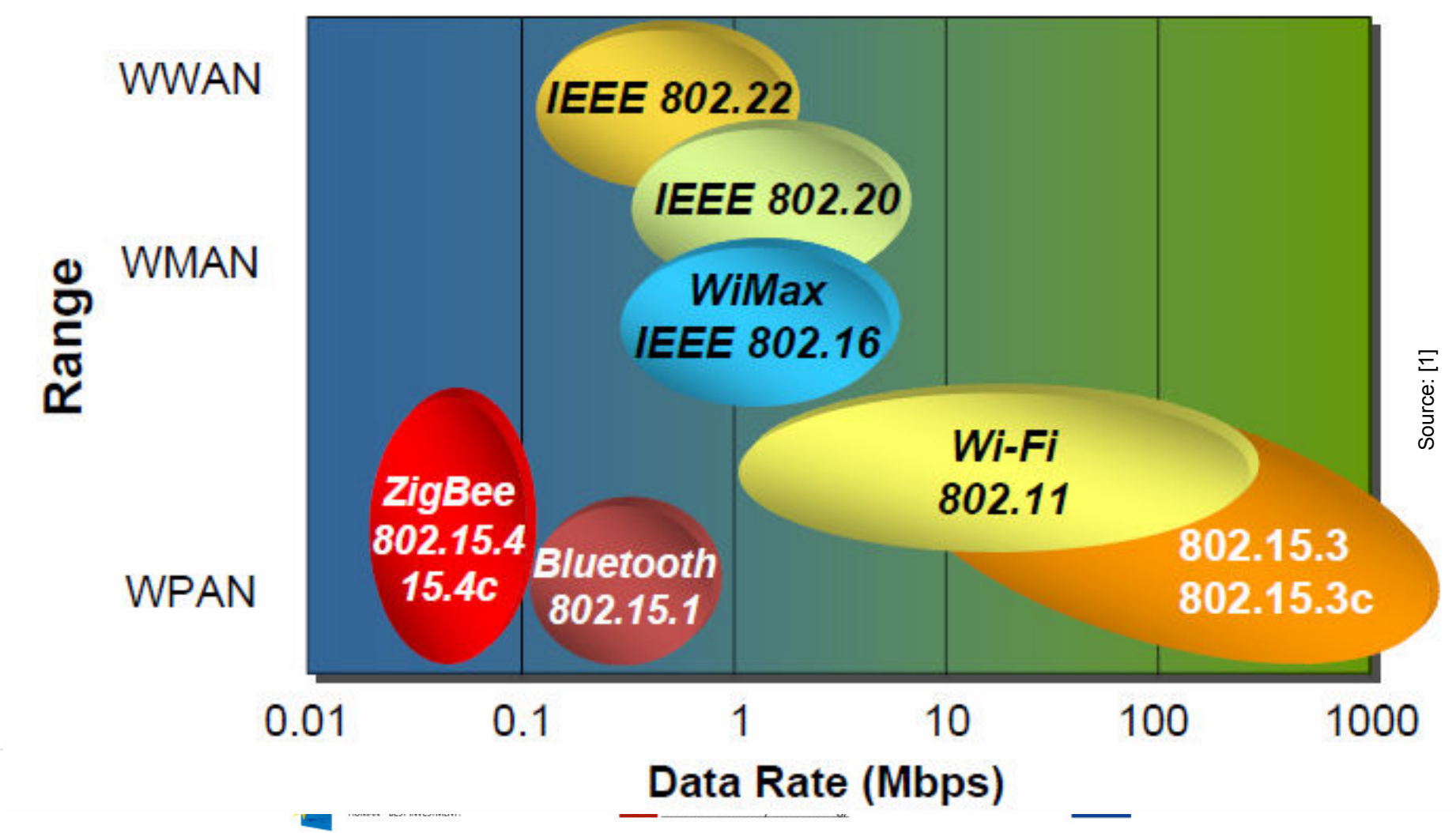
Introduction

- The popularity of wireless data transfer is increasing rapidly
- Reliable wireless communication is a very difficult issue – electromagnetic environment is noisy and very crowded
- Thanks to the effect of scale on the market there are available ready and cheap wireless data transfer devices

Introduction

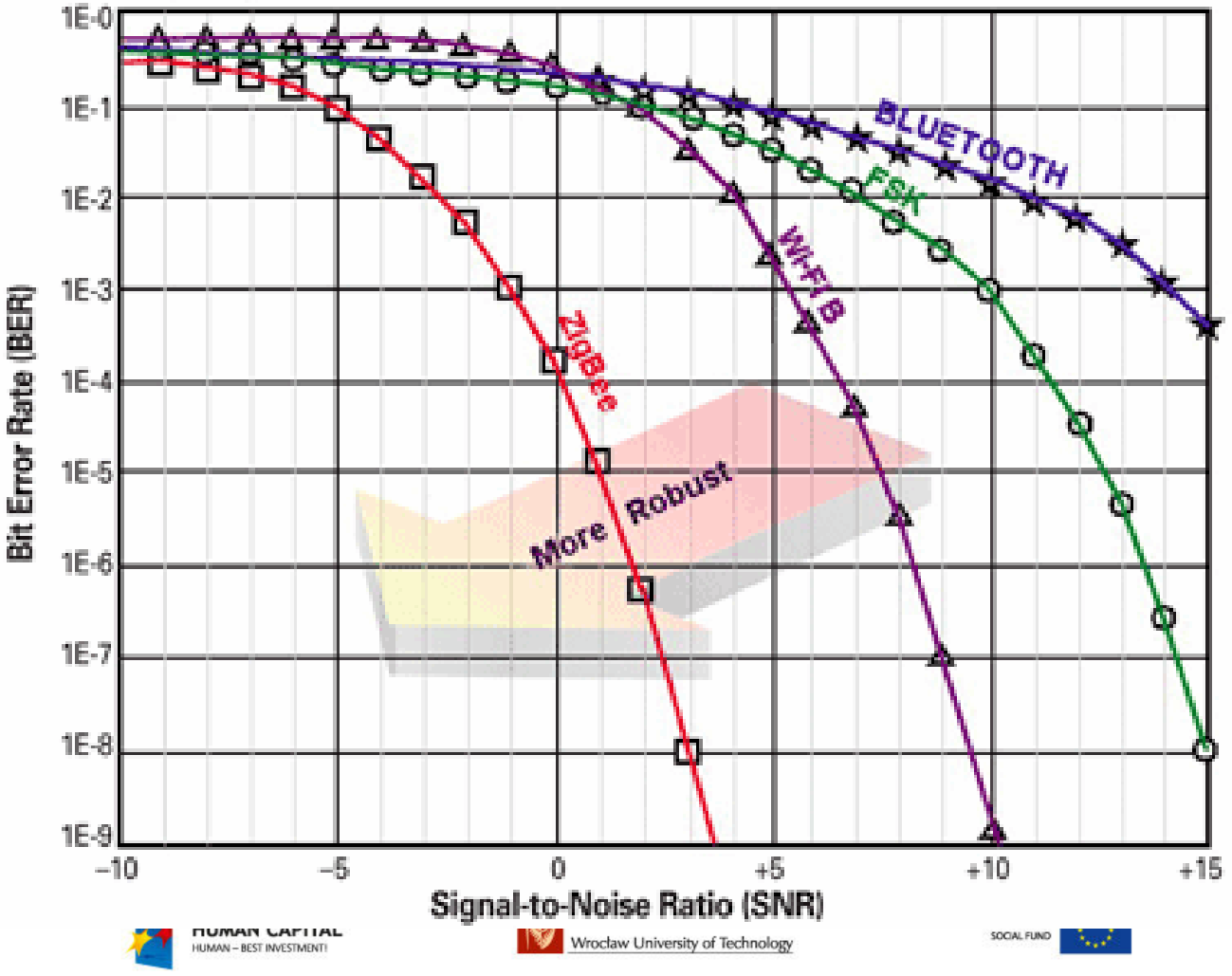
- Solutions available on the market allow for transmission rates from single bytes/sec to hundreds MB/s
- Available ranges: from meters to kilometers
- Available frequency ranges are limited by international and local regulations. In Europe most common ranges are: 433 MHz, 868MHz, 2.4 GHz

Introduction



Source: [1]

Introduction



Source: [1]

ZigBee vs Bluetooth

- ZigBee looks like Bluetooth but is simpler
- ZigBee has a lower data rate
- ZigBee spends most of the time snoozing
- The operational range of ZigBee is 10-75m (10m for Bluetooth, ClassII)
- ZigBee is slower than Bluetooth (250kbps vs 1Mb)
- ZigBee uses simpler protocol
- Upto 254 nodes possible (8 nodes in BT)
- Rapid wake up of ZigBee nodes (15ms, 3s in BT)

ZigBee
IEEE 802.15.4

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!
Wrocław University of Technology
EUROPEAN SOCIAL FUND
Project co-financed from the EU European Social Fund

ZigBee – general characteristic

- Dual PHY (2.4GHz and 868/915 MHz)
- Data rates of 250 kbps (@2.4 GHz), 40 kbps (@ 915 MHz), and 20 kbps (@868 MHz)
- Optimized for low duty-cycle applications (<0.1%)
- CSMA-CA channel access
  - Yields high throughput and low latency for low duty cycle devices like sensors and controls

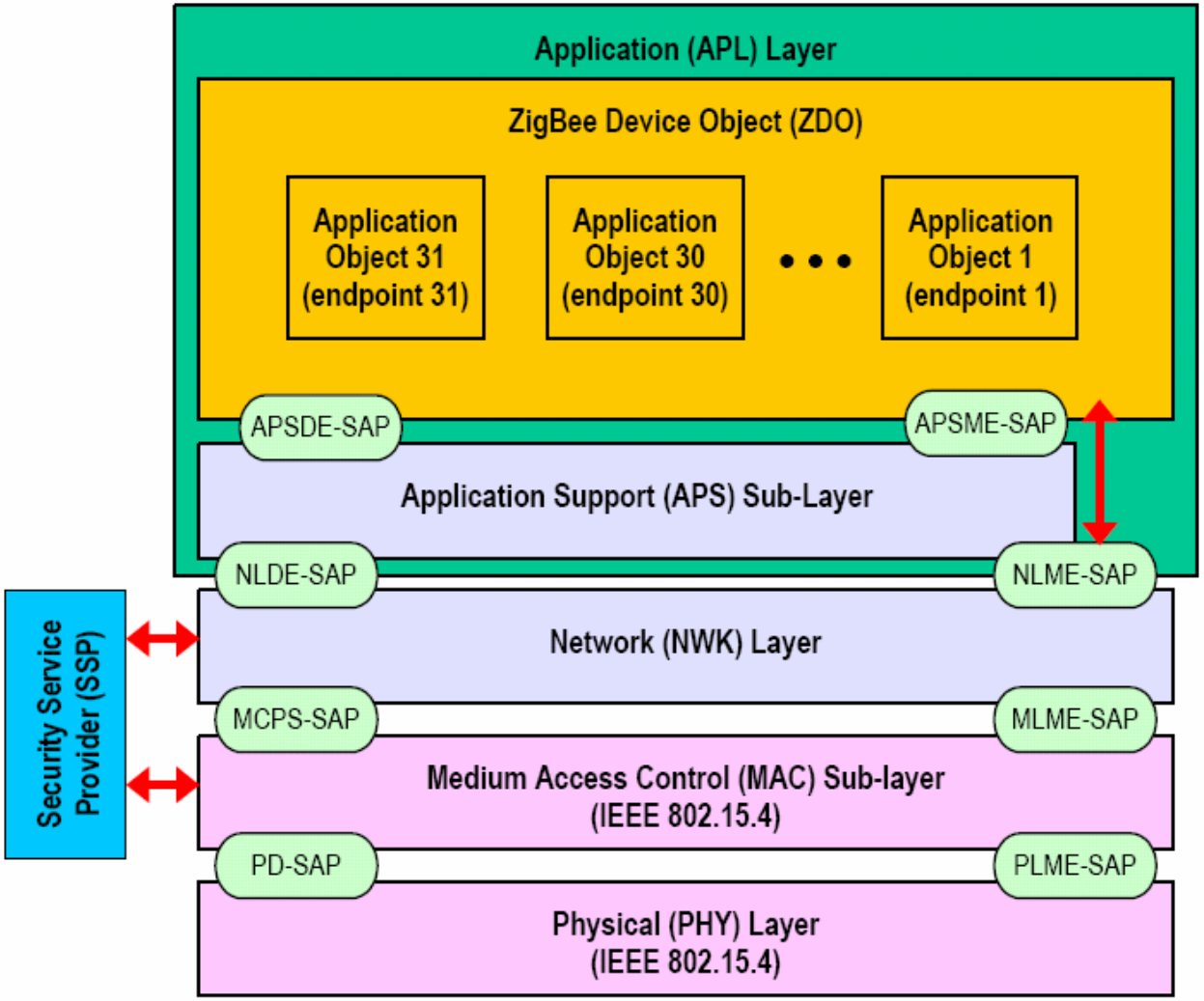
ZigBee – general characteristic

- Low power (battery life multi-month to years)
- Multiple topologies: star, peer-to-peer, mesh
- Addressing space of up to:
  - 18,450,000,000,000,000,000 devices (64 bit IEEE address)
  - 65,535 networks

ZigBee – general characteristic

- Optional guaranteed time slot for applications requiring low latency
- Fully hand-shaked protocol for transfer reliability
- Range: 50m typical (5-500m based on environment)

ZigBee – general characteristic



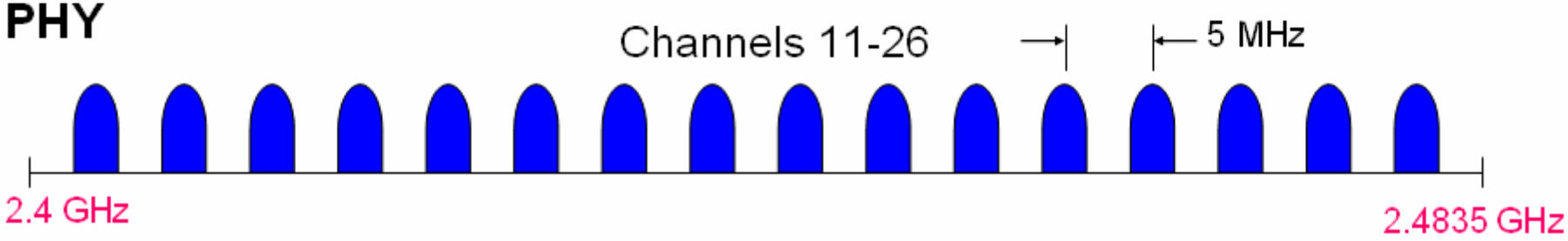
Source: [1]

ZigBee – Frequency range

868MHz / 915MHz PHY

Source: [2]

2.4 GHz PHY



802.15.4 PHY

- Frequency bands and data rates

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
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

ZigBee/IEEE802.15.4

- Typical Traffic Types Addressed:
  - Periodic data
    - Application defined rate (e.g., sensors)

Periodic data can be handled using the beaconing system whereby the sensor will wake up for the beacon, check for any messages and then go back to sleep.

ZigBee/IEEE802.15.4

- Typical Traffic Types Addressed:
  - Intermittent data
    - Application/external stimulus defined rate (e.g., light switch)

Intermittent data can be handled either in a beaconless system or in a disconnected fashion. In a disconnected operation the device will only attach to the network when it needs to communicate saving significant energy.

ZigBee/IEEE802.15.4

- Typical Traffic Types Addressed:
  - Repetitive low latency data
    - Allocation of time slots (e.g., mouse)

Low latency applications may choose to the guaranteed time slot (GTS) option. GTS is a method of QoS in that it allows each device a specific duration of time each Superframe to do whatever it wishes to do without contention or latency.

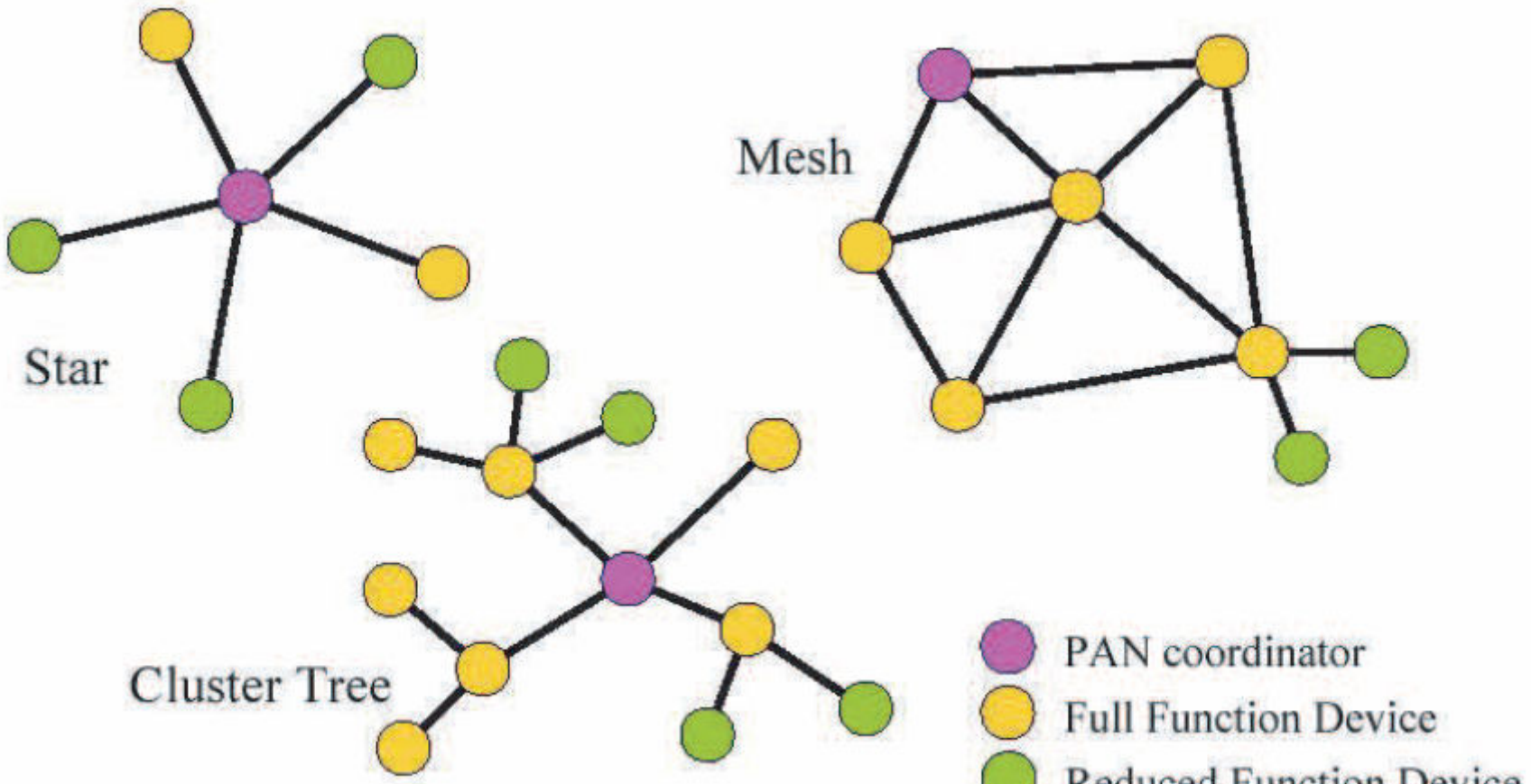
ZigBee – Device classes

- Full Function Device:
  - Works in any topology
  - Capable of being Network Coordinator
  - Talks to any other deivce
  - Can talk to any other device
- Reduced Function Device:
  - Limited to star topology
  - Cannot become a Network Coordinator
  - Talks only to a Network Coordinator
  - Very simple implementation

ZigBee – Device classes

- An IEEE 802.15.4/ZigBee network requires at least one full function device as a network coordinator, but endpoint devices may be reduced functionality devices to reduce system cost.
  - All devices must have 64 bit IEEE addresses
  - Short (16 bit) addresses can be allocated to reduce packet size
  - Addressing modes:
    - Network + device identifier (star)
    - Source/destination identifier (peer-peer)

ZigBee – network architecture



Source: [1]

ZigBee – Star topology

- Communication is established between devices and a single central controller (PAN coordinator)
- The PAN coordinator may be mains powered while the devices will most likely be battery powered
- After an FFD is activated for the first time, it may establish its own network and become the PAN coordinator
- Each start network chooses a PAN identifier, which is not currently used by any other network within the radio sphere of influence

ZigBee – Mesh topology

- Mesh topology is called peer-to-peer topology
- In contrast to star topology, any device can communicate with any other device as long as they are in range of one another
- Mesh network can be ad hoc, self-organizing and self-healing
- Network allows multiple hops to route messages from any device to any other device in the network

ZigBee – Cluster-tree topology

- Cluster-tree network is a special case of mesh network in which most devices are FFDs
- An RFD may connect to a cluster-tree network as a leave node at the end of a branch
- Any of the FFD can act as a coordinator and provide synchronization services to other devices and coordinators
- Only one of these coordinators however is the PAN coordinator

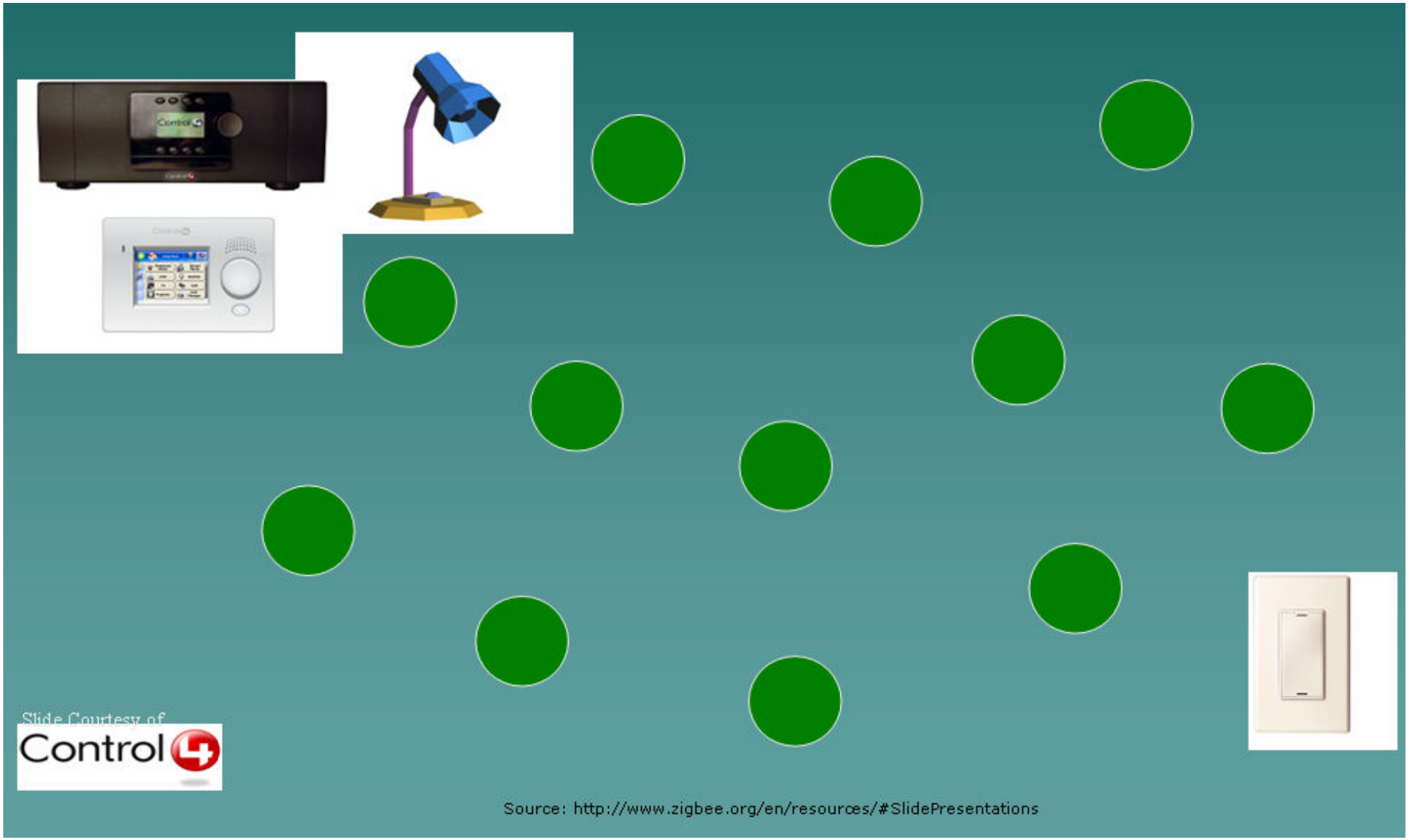
ZigBee – Cluster-tree topology

- The PAN coordinator forms the first cluster by establishing itself as the cluster head (CLH) with a cluster identifier (CID) of zero, choosing an unused PAN identifier, and broadcasting beacon frames to neighboring devices
- A candidate device receiving a beacon frame may request to join the network at the CLH
- If the PAN coordinator permits the device to join, it will add this new device as a child device in its neighbor list

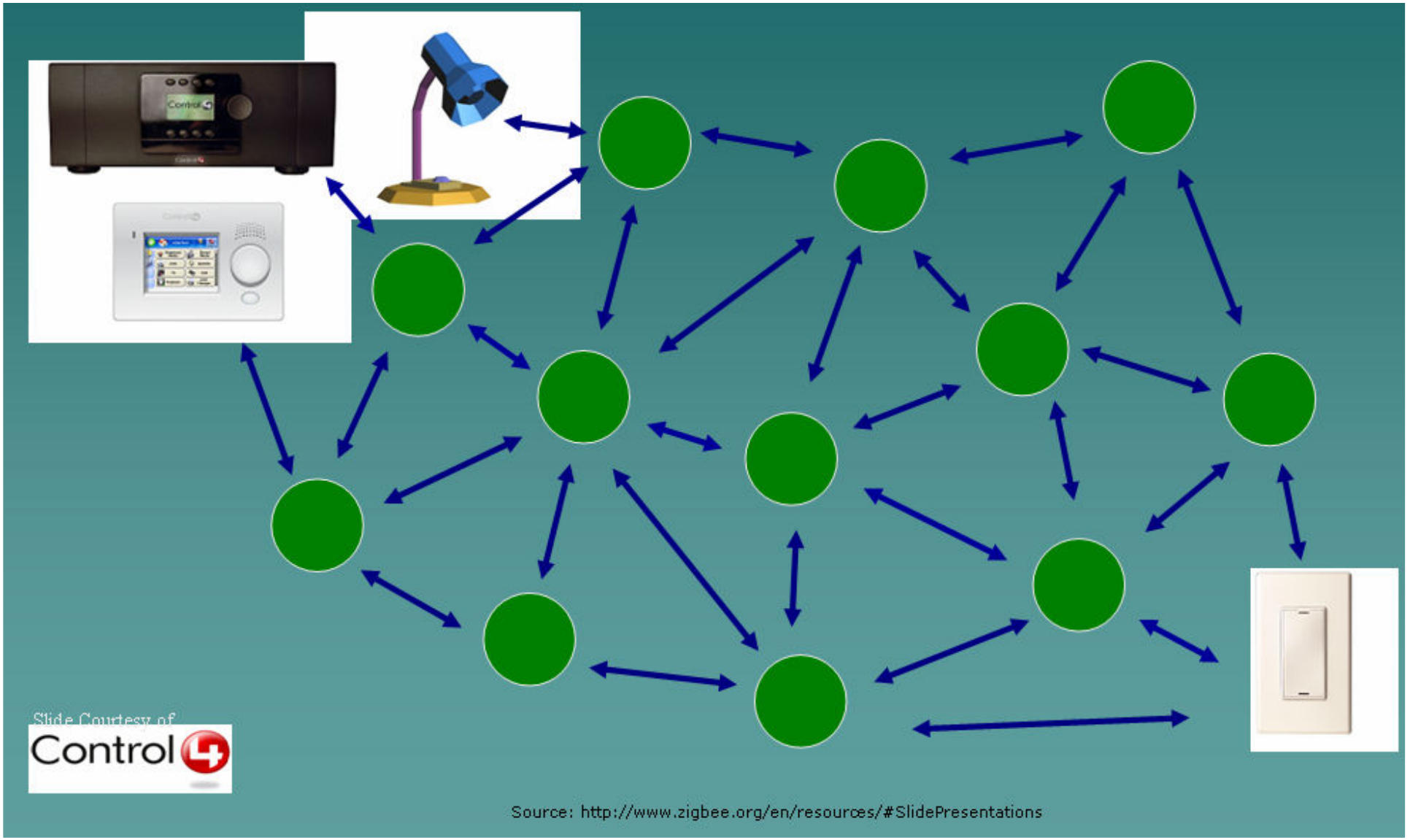
ZigBee – Cluster-tree topology

- The newly joined device will add the CLH as its parent in its neighbor list and begin transmitting periodic beacons such that other candidate devices may then join the network at that device
- The advantage of this clustered structure is the increased coverage area at the cost of increased message latency

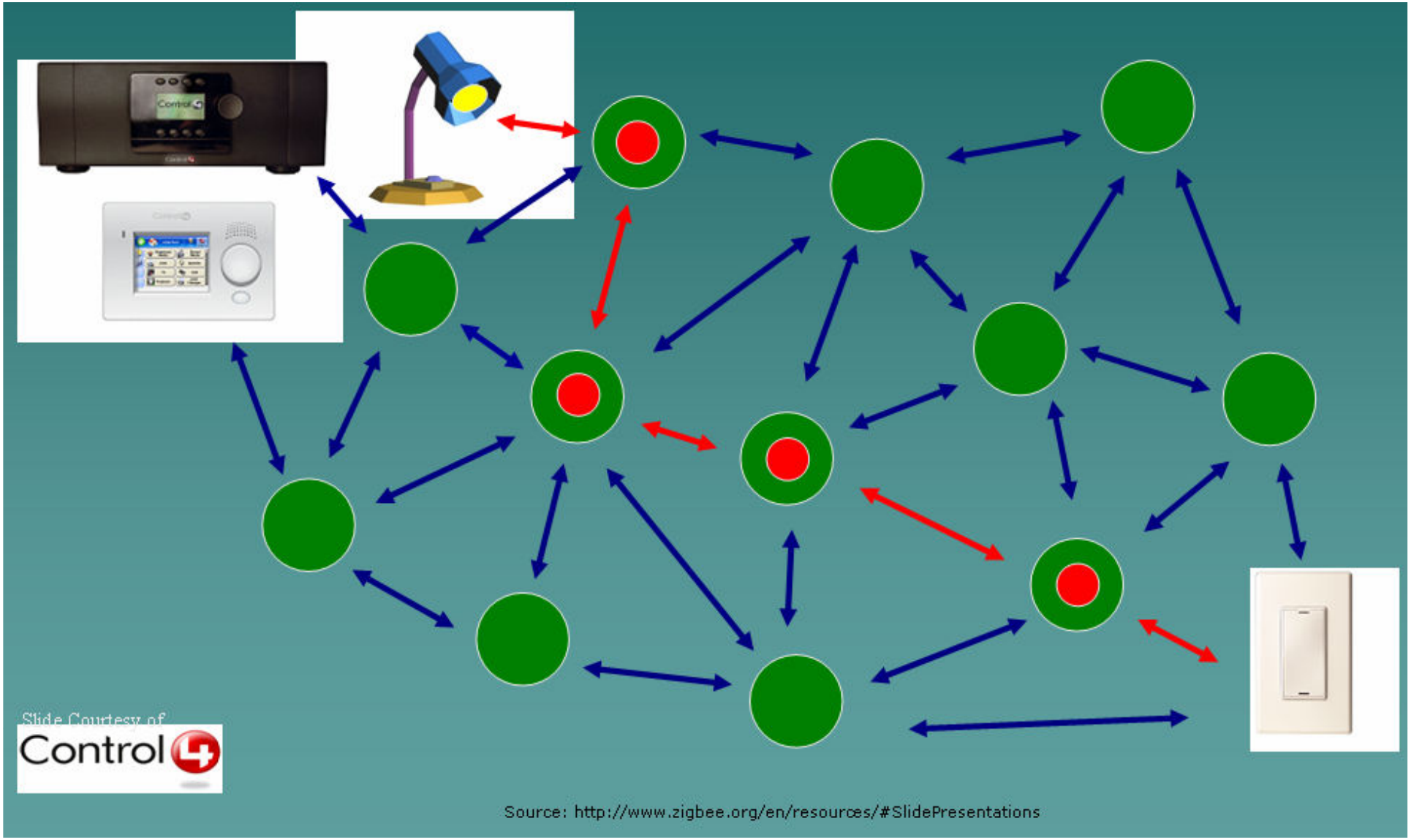
ZigBee – how it works



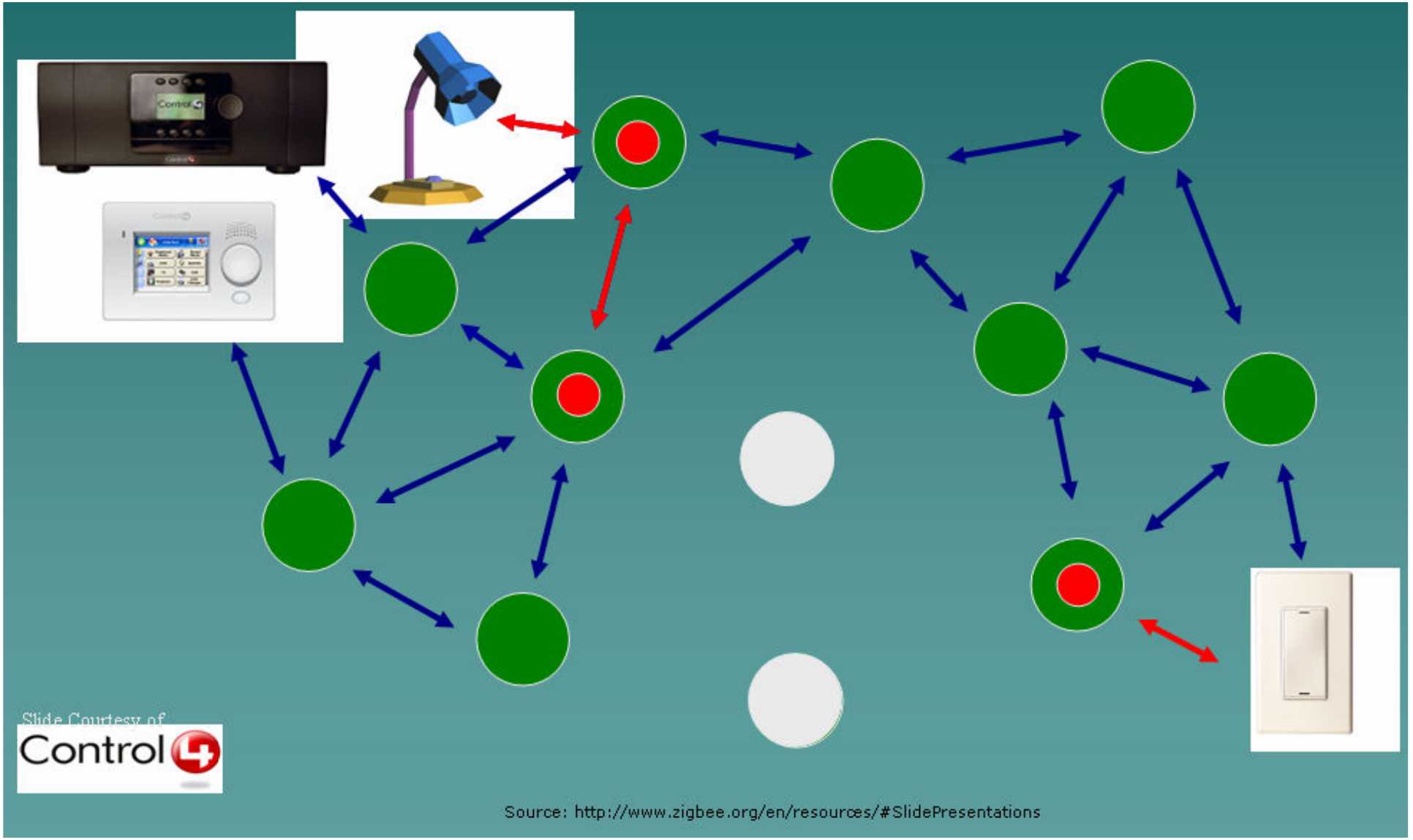
ZigBee – how it works



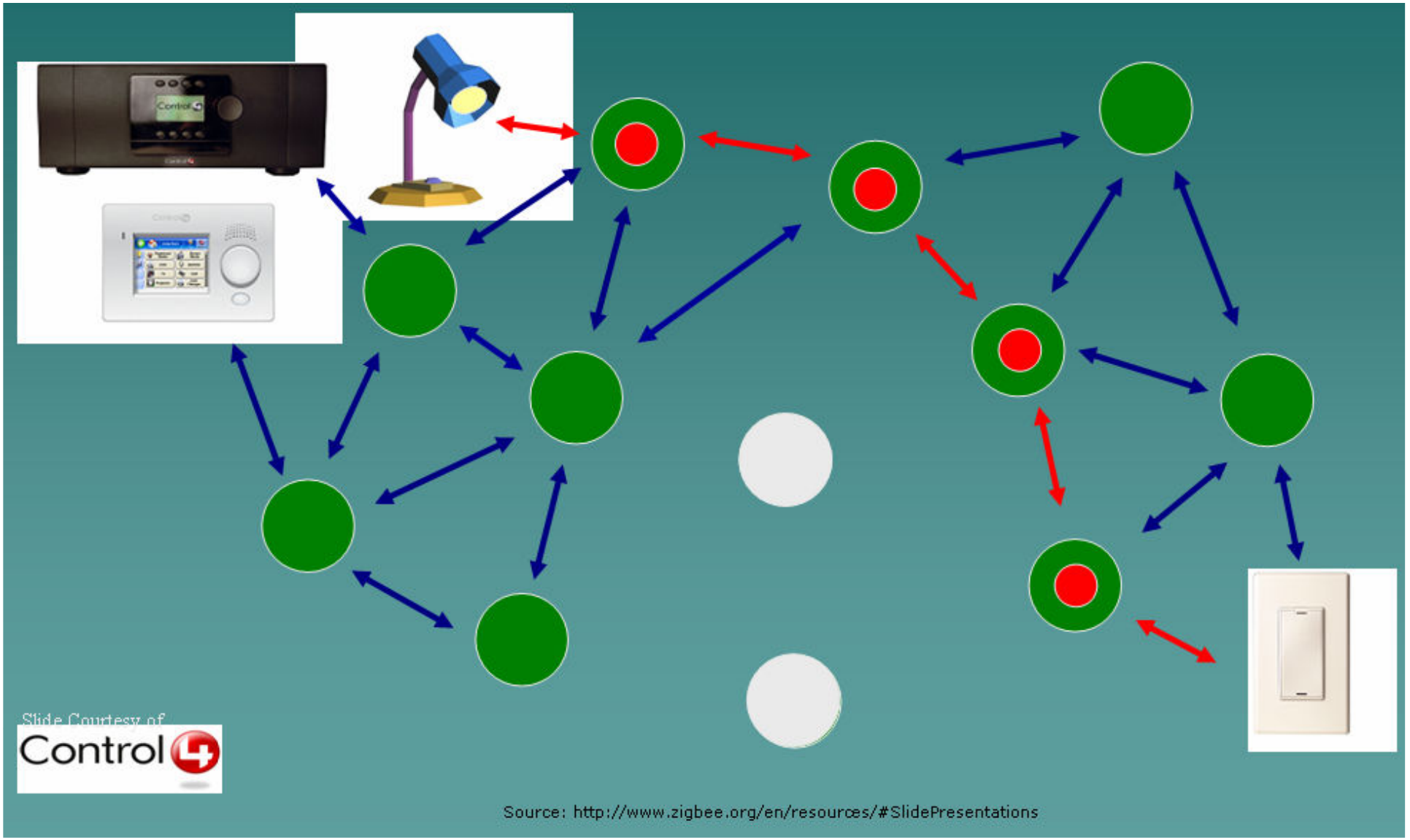
ZigBee – how it works



ZigBee – how it works



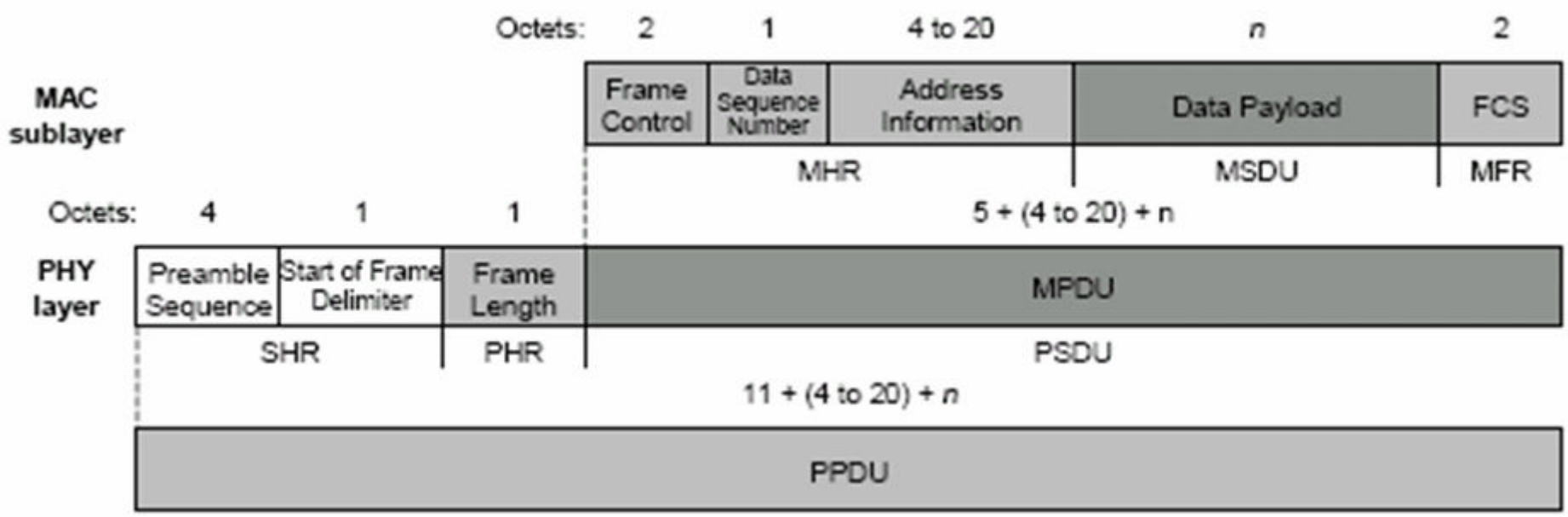
ZigBee – how it works



MAC layer frame structure

- The IEEE 802.15.4 MAC defines four frame structures:
  - A **beacon** frame, used by a coordinator to transmit beacons.
  - A **data** frame, used for all transfers of data.
  - An **acknowledgment** frame, used for confirming successful frame reception.
  - A MAC **command** frame, used for handling all MAC peer entity control transfers.

MAC layer frame structure



- In summary the total overhead for a single packet is 15 -31 octets (120 bits); depending upon the addressing scheme used (short or 64 bit addresses).

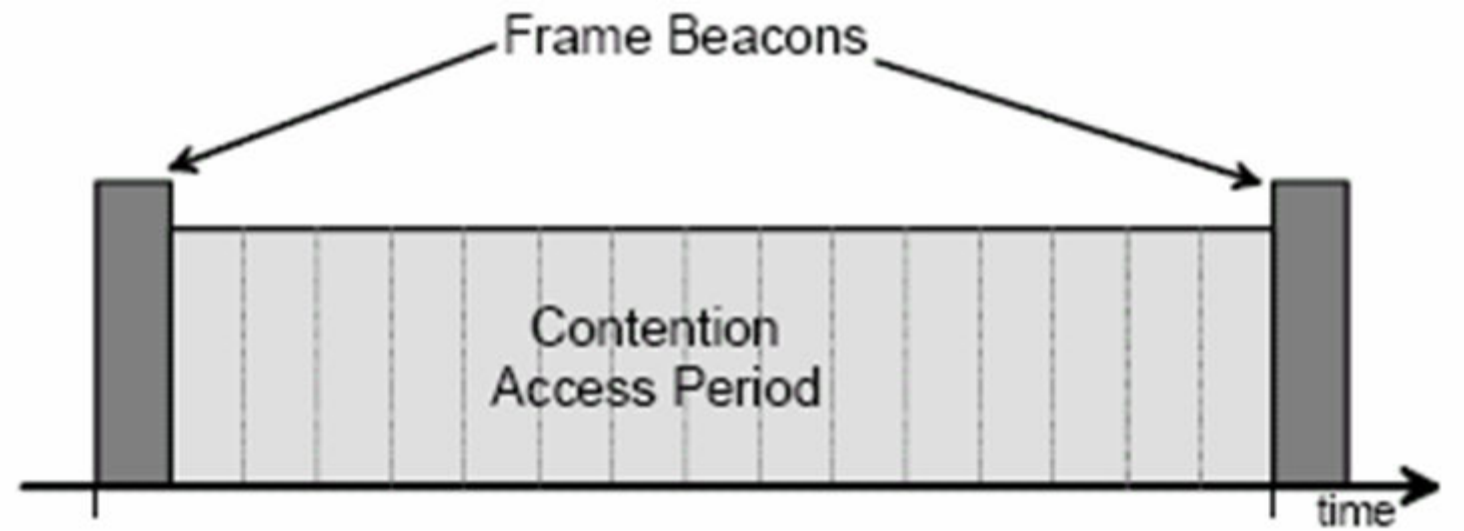
MAC layer frame structure

- The Physical Protocol Data Unit is the **total information** sent over the air - adds the following overhead:
  - Preamble Sequence 4 Octets
  - Start of Frame Delimiter 1 Octet
  - Frame Length 1 Octet
- The MAC adds the following overhead:
  - Frame Control 2 Octets
  - Data Sequence Number 1 Octet
  - Address Information 4 – 20 Octets
  - Frame Check Sequence 2 Octets

ZigBee – Super Frame Structure

- The superframe usage is optional
- The superframe format is defined by the network coordinator
- The superframe is bounded by network beacons, is sent by the coordinator and is divided into 16 equally sized slots.
- The beacon frame is transmitted in the first slot of each superframe

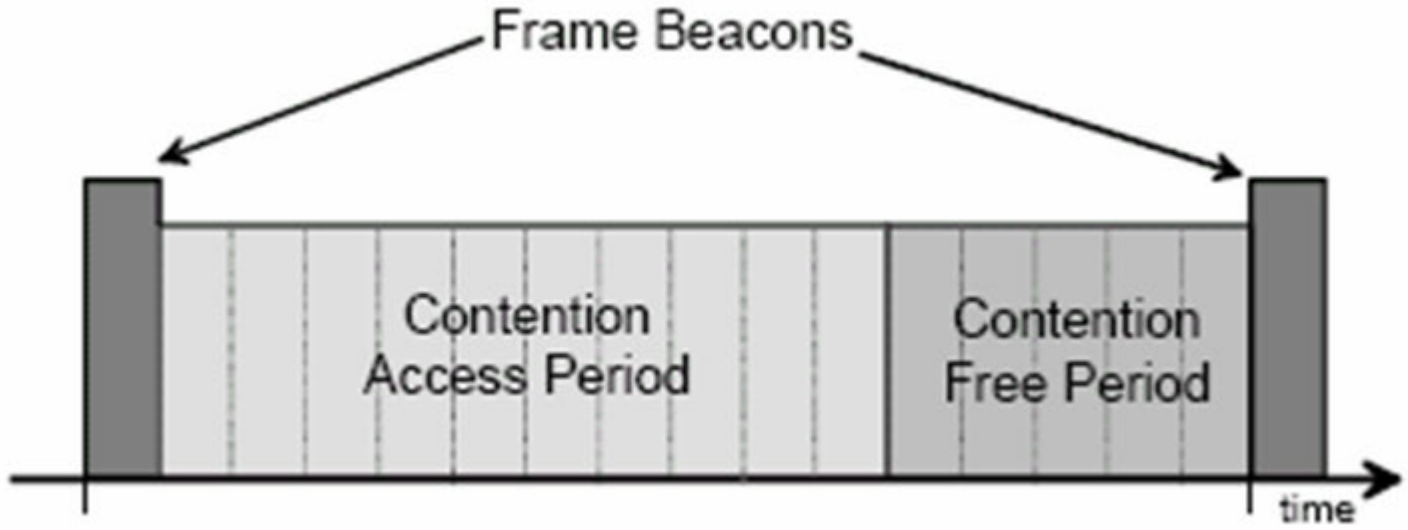
ZigBee – Super Frame Structure



- The beacons are used to synchronize the attached devices, to identify the PAN, and to describe the structure of the superframes
- Any device wishing to communicate during the contention access period (CAP) between two beacons shall compete with other devices using a slotted CSMA-CA mechanism

ZigBee – Super Frame Structure - GTS

- For low latency applications or applications requiring specific data bandwidth, the PAN coordinator may dedicate portions of the active superframe to that application – these are called guaranteed time slots (GTSs)



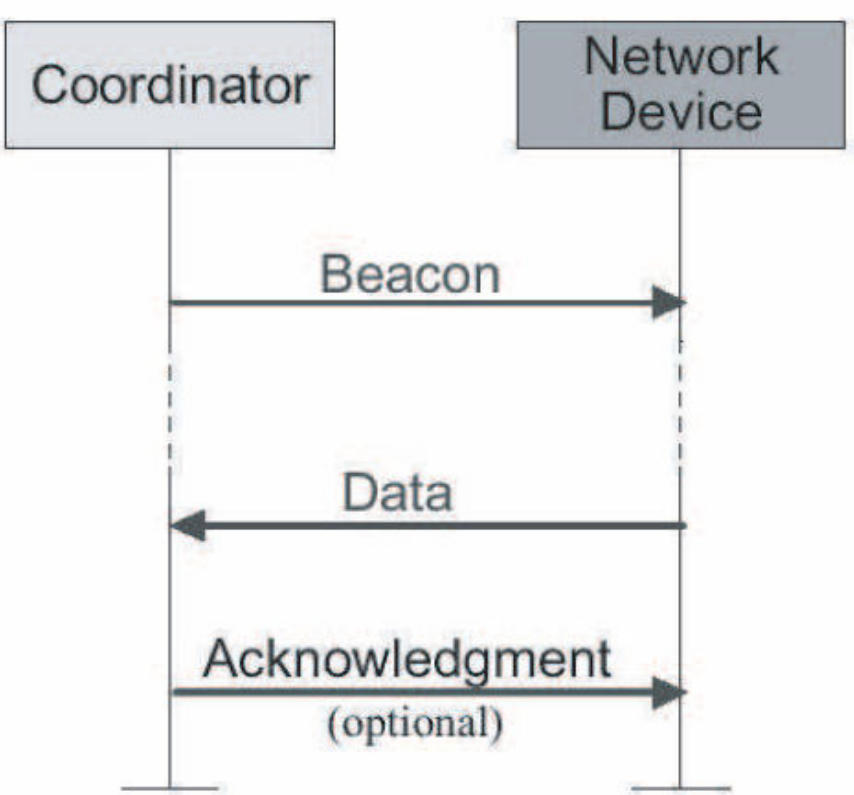
ZigBee – Super Frame Structure - GTS

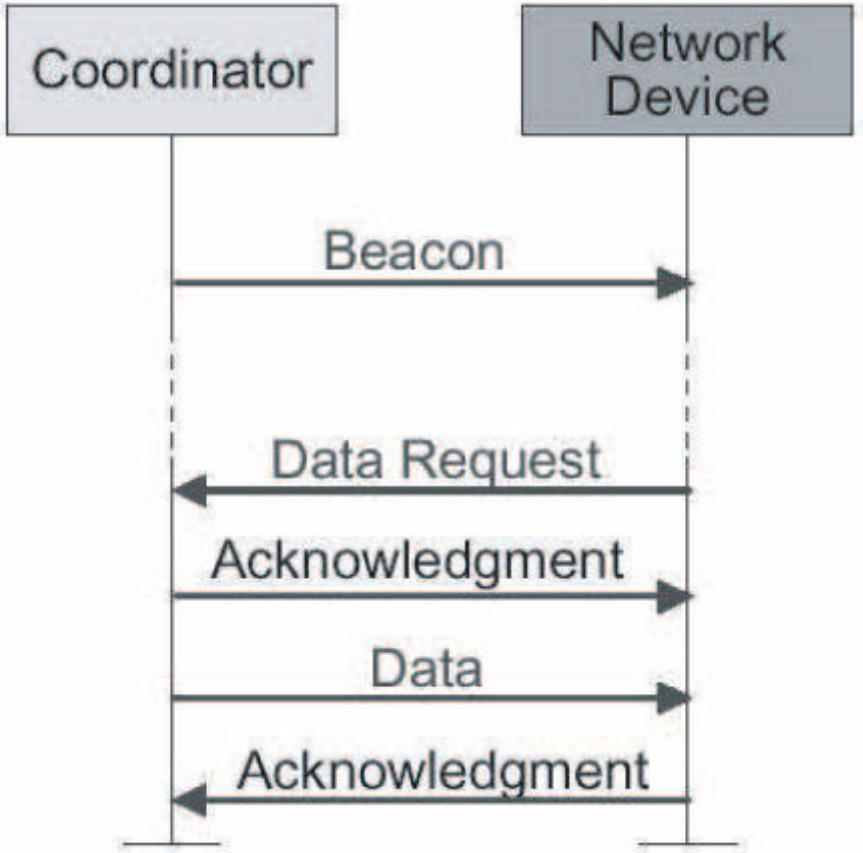
- The guaranteed time slots comprise the contention free period (CFP), which always appears at the end of the active superframe
- The PAN coordinator may allocate up to seven of these GTSs and a GTS may occupy more than one slot period
- A sufficient portion of the CAP shall remain for contention based access of other networked devices or new devices wishing to join the network
- All contention based transactions shall be complete before the CFP begins

ZigBee – Beacon mode

- Beacon mode is a fully coordinated mode in that all the device know when to coordinate with one another
- In this mode, the network coordinator will periodically "wake-up" and send out a beacon to the devices within its network
- This beacon subsequently wakes up each device, who must determine if it has any message to receive
- If not, the device returns to sleep, as will the network coordinator, once its job is complete

ZigBee – Beacon mode

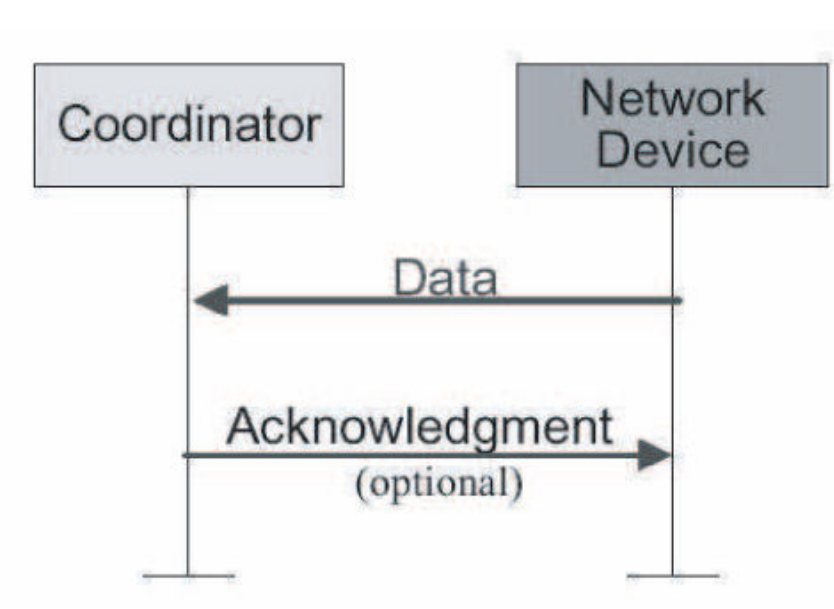


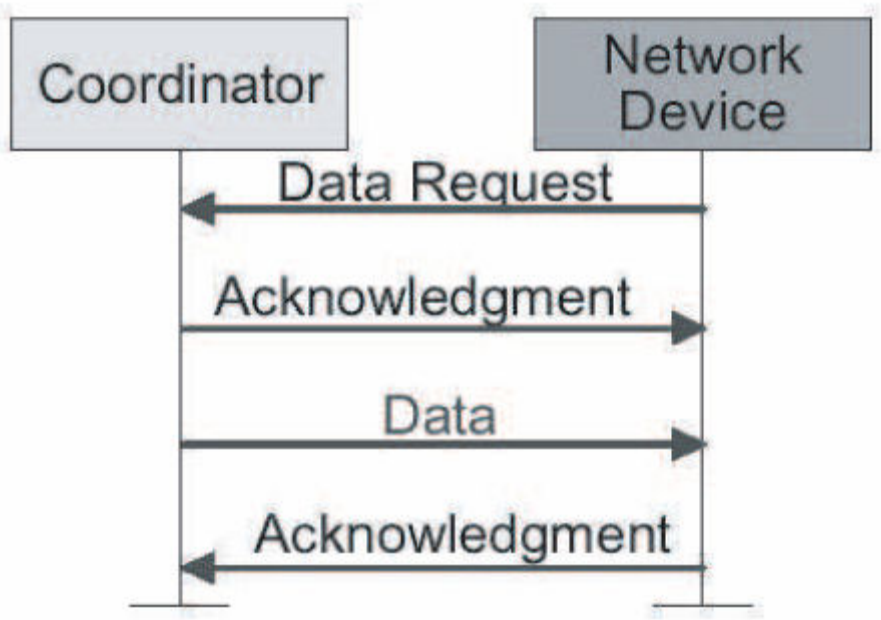


ZigBee – Non-Beacon mode

- Non-beacon mode, is less coordinated than beacon mode, as any device can communicate with the coordinator at will
- This operation can cause different devices within the network to interfere with one another
- The coordinator must always be awake to listen for signals, thus requiring more power

ZigBee – Non-Beacon mode





ZigBee – Security

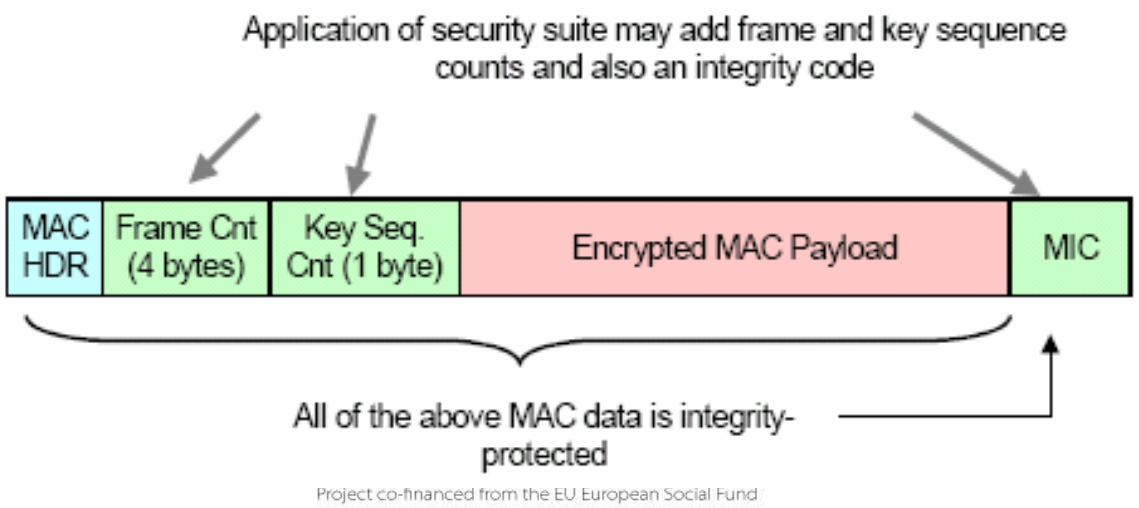
- When security of MAC layer frames is desired, ZigBee uses MAC layer security to secure:
  - MAC command,
  - beacon,
  - acknowledgement frames
- ZigBee may secure messages transmitted over a single hop using secured MAC data frames
- For multi-hop messaging ZigBee relies upon upper layers (such as the NWK layer) for security

ZigBee – Security

- The MAC layer uses the Advanced Encryption Standard (AES) as its core cryptographic algorithm
- The MAC layer does the security processing
- The upper layers, which set up the keys and determine the security levels to use, control processing

ZigBee – Security

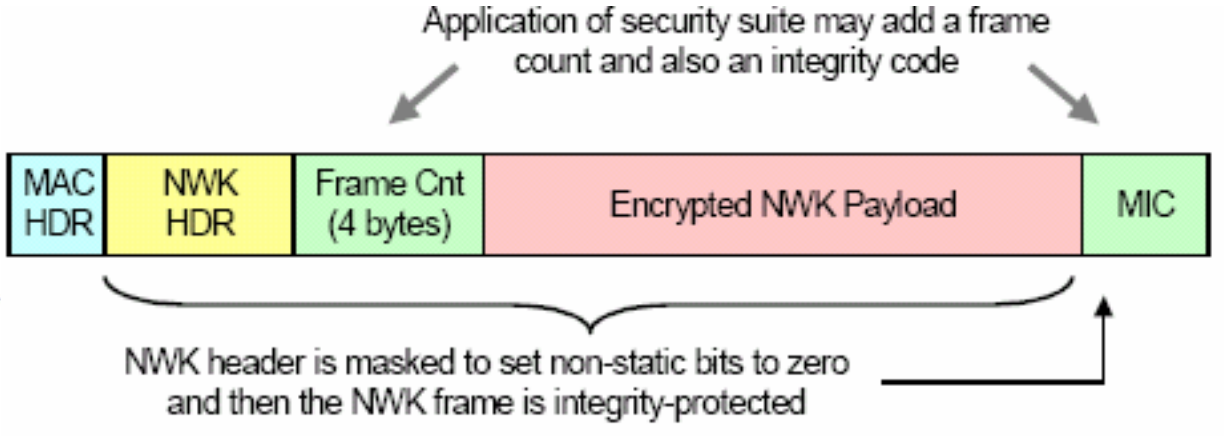
- If integrity is required, the MAC header and payload data are used in calculations to create a Message Integrity Code (MIC)
- If confidentiality is required, the MAC frame payload is also left appended with frame and sequence counts



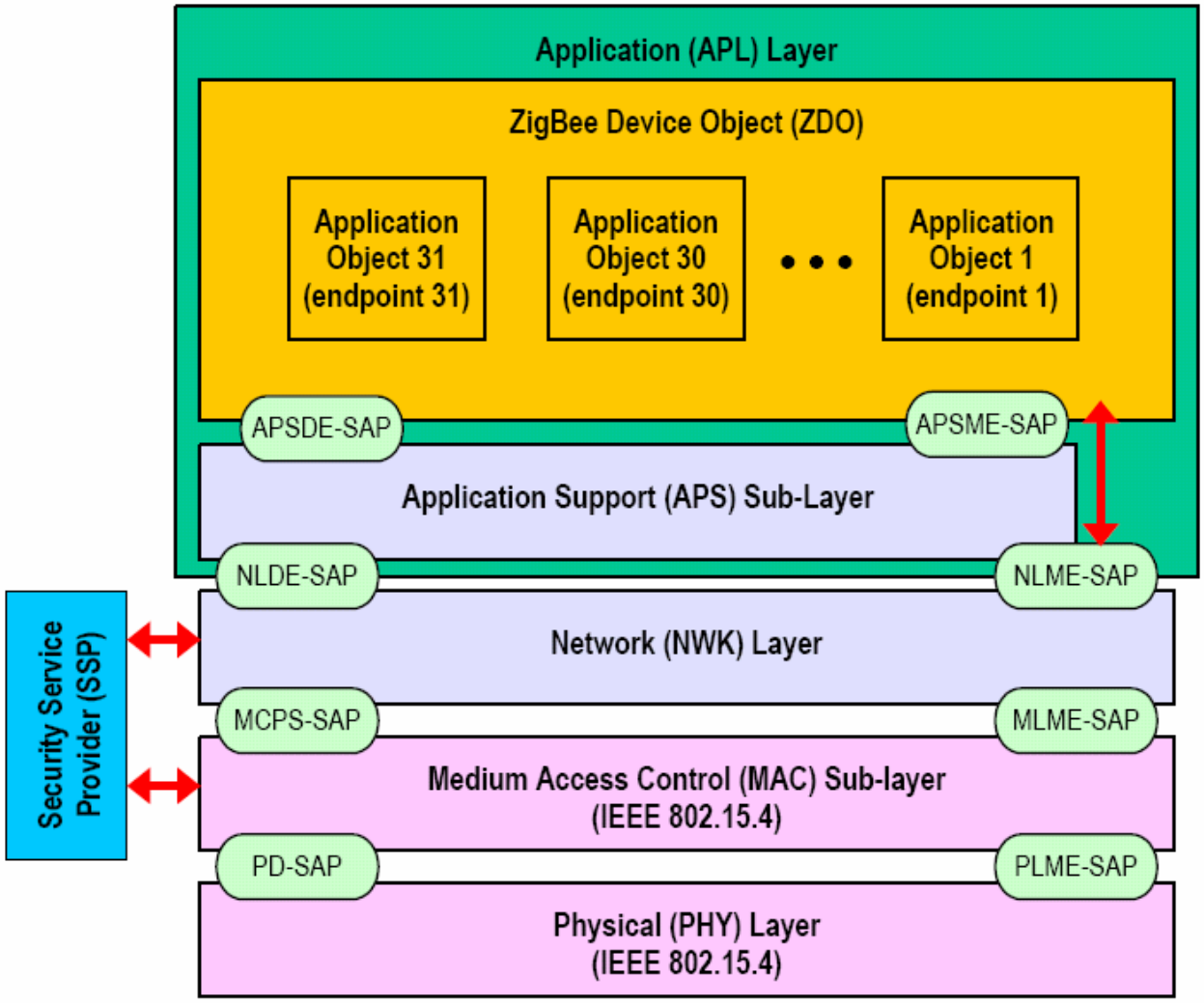
Project co-financed from the EU European Social Fund

ZigBee – Security

- When the NWK layer transmits (receives) a frame using a particular security suite it uses the Security Services Provider (SSP) to process the frame
- The SSP looks at the destination (source) of the frame, retrieves the key associated with that destination (source), and then applies the security suite to the frame



ZigBee – software architecture



Source: [1]

ZigBee Stack – System Requirements

- 8-bit μC, e.g., 80c51

- Full protocol stack <32k
- Simple node only stack ~6k
- Coordinators require extra RAM
  - node device database
  - transaction table
  - pairing table

ZigBee Stack – Network layer

- The responsibilities of the ZigBee NWK layer 1/2:
  - **Starting a network:** The ability to successfully establish a new network.
  - **Joining and leaving a network**: The ability to gain membership (join) or relinquish membership (leave) a network.
  - **Configuring a new device:** The ability to sufficiently configure the stack for operation as required.

ZigBee Stack – Network layer

- The responsibilities of the ZigBee NWK layer 2/2:
  - **Addressing:** The ability of a ZigBee coordinator to assign addresses to devices joining the network.
  - **Synchronization within a network:** The ability for a device to achieve synchronization with another device either through tracking beacons or by polling.
  - **Security:** applying security to outgoing frames and removing security to terminating frames
  - **Routing:** routing frames to their intended destinations.

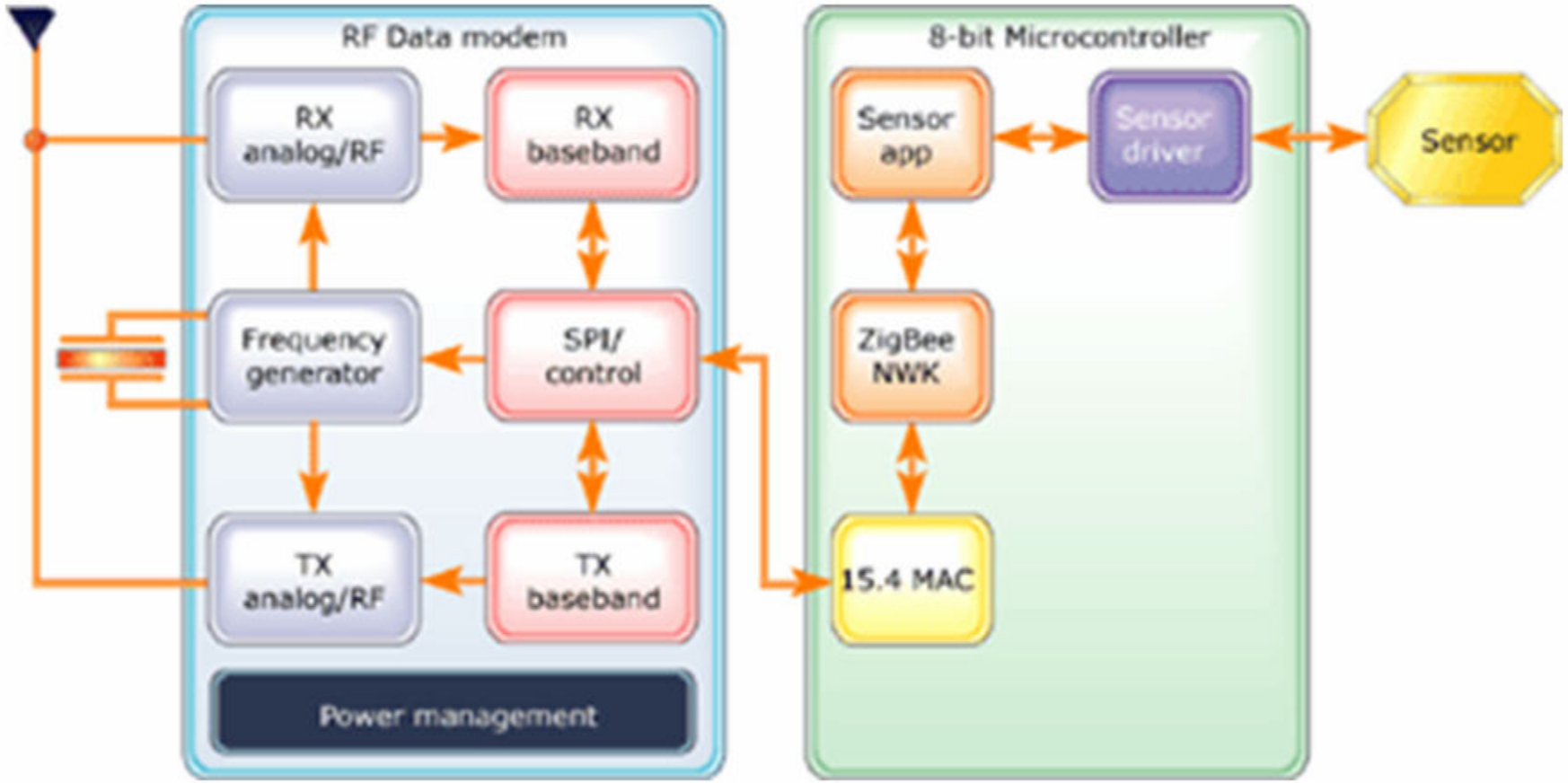
ZigBee Stack – Application layer

- The APL layer consists of:
  - APS sub-layer (application support) – responsible for:
    - maintaining tables for binding, which is the ability to match two devices together based on their services and their needs
    - forwarding messages between bound devices

ZigBee Stack – Application layer

- The APL layer consists of:
  - the ZDO (ZigBee Device Object) – responsible for:
    - defining the role of the device within the network (e.g., ZigBee coordinator or end device)
    - initiating and/or responding to binding requests
    - establishing a secure relationship between network devices
  - the manufacturer-defined application objects:
    - Definition of

ZigBee – device block diagram



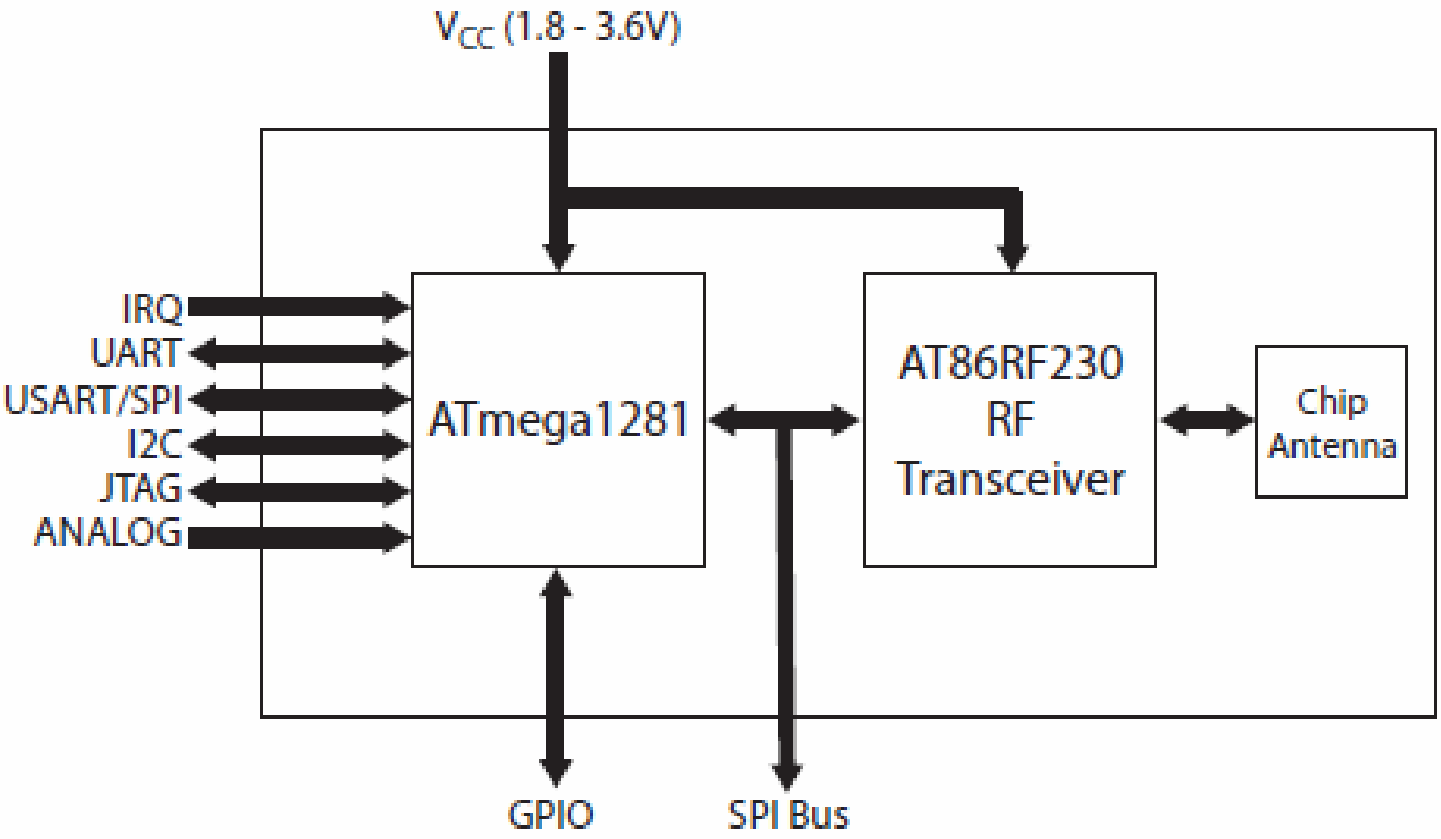
Source: [1]

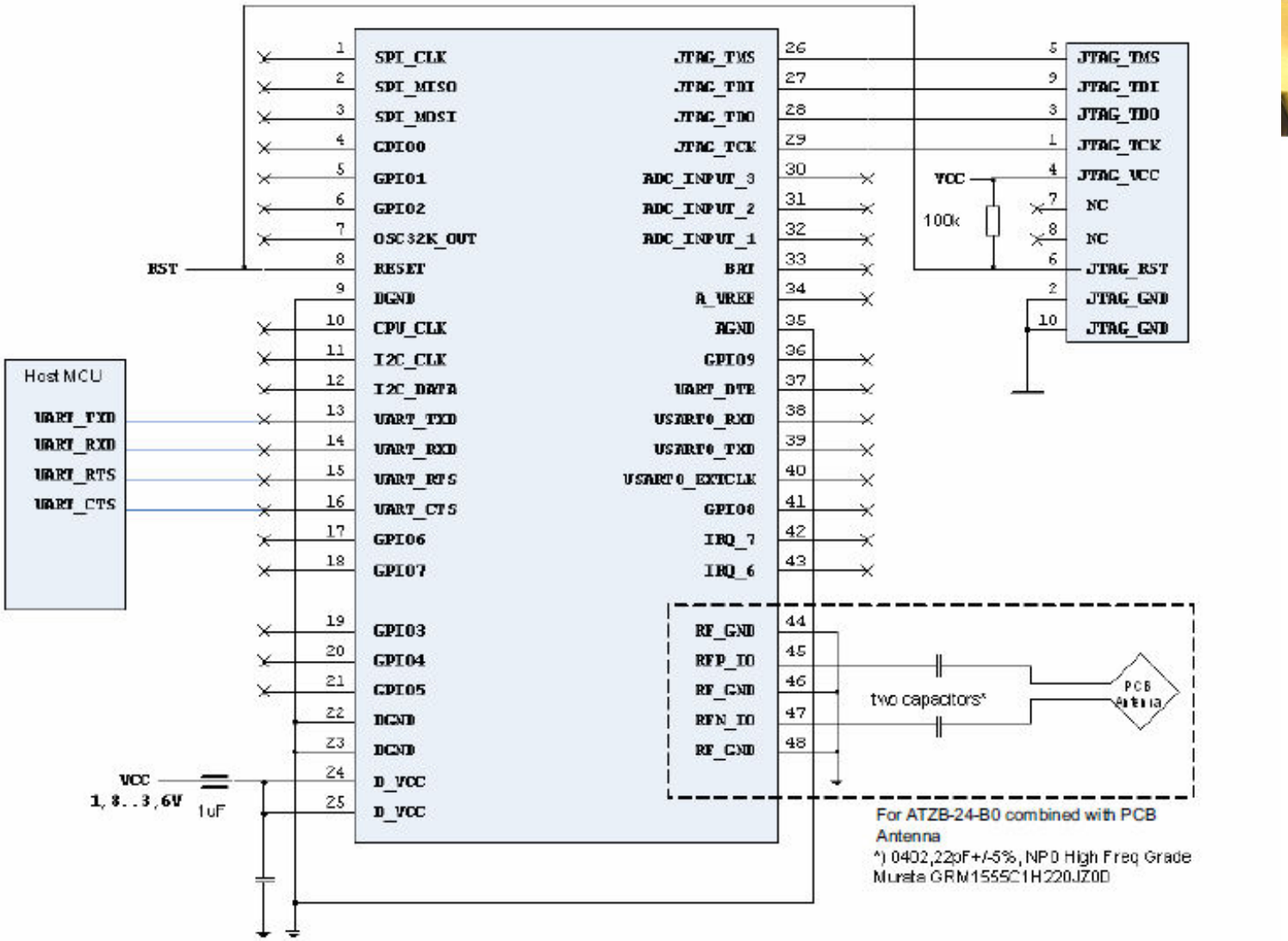
ZigBee – application examples

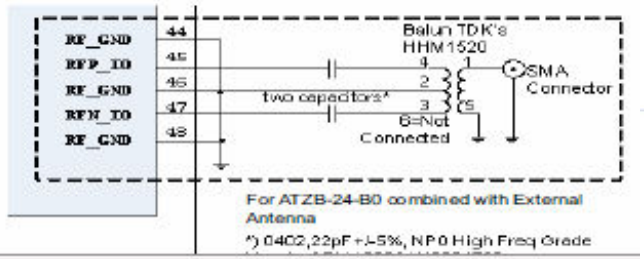
ZigBit – Main features

- Small dimensions
- Affordable price
- High reception sensitivity (-101dBm)
- Output power up to +3dBm
- Very small supply current: sleep <6μA, transmission <20mA
- RF part integrated with 8-bit ATMega1281 MCU
- Integrated antenna
- Works in 2.4 GHz range

ZigBit – Block diagram




SPI_CLK
SPI_MISO
SPI_MOSI
GPIO0
GPIO1
GPIO2
OSC32K_OUT
RESET
DGND
CPU_CLK
I2C_CLK
I2C_DATA
UART_TXD
UART_RXD
UART_RTS
UART_CTS
GPIO6
GPIO7
GPIO3
GPIO4
GPIO5
DGND
DGND
D_VCC
D_VCC
JTAG_TMS
JTAG_TDI
JTAG_TDO
JTAG_TCK
ADC_INPUT_3
ADC_INPUT_2
ADC_INPUT_1
BAT
A_VREF
AGND
GPIO9
UART_DTR
USART0_RXD
USART0_TXD
USART0_EXTCLK
GPIO8
IRQ_7
IRQ_6
RF_GND
RFP_IO
RF_GND
RFN_IO
RF_GND
RST
Host MCU
UART_TXD
UART_RXD
UART_RTS
UART_CTS
VCC
1,8..3,6V
1uF
VCC
100k
JTAG_TMS
JTAG_TDI
JTAG_TDO
JTAG_TCK
JTAG_VCC
NC
NC
JTAG_RST
JTAG_GND
JTAG_GND
two capacitors*
PCB Antenna
For ATZB-24-B0 combined with PCB Antenna
*) 0402,22pF+/-5%, NP0 High Freq Grade
Murata GRM1555C1H220JZ0D


RF_GND
RFP_IO
RF_GND
RFN_IO
RF_GND
two capacitors*
Balun TDK's HHM1520
SMA Connector
6=Not Connected
For ATZB-24-B0 combined with External Antenna
*) 0402,22pF+/-5%, NP0 High Freq Grade

Source: [5]

Thank you for your attention

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!
Wrocław University of Technology
EUROPEAN SOCIAL FUND
Project co-financed from the EU European Social Fund

References

[1] www.zigbee.org/en/resources

[2] Dvorak J., „IEEE 802.15.4 and Zigbee Overview”

[3] www.wikipedia.org

[4] Diamond C., et all, „ZigBee-Wireless Communications”, EE 418/518

[5] ZigBit modules documentation, www.atmel.com

[6] http://pages.cs.wisc.edu/~suman/courses/838/papers/zigbee.pdf

[7] Kinney P., „ ZigBee Technology: Wireless Control that Simply Works”, Communications Design Conference, 2003