1

Wireless Sensor Networks

1

2

Recall: Short range wireless application areas

	Voice	Data	Audio	Video	State
Bluetooth ACL/HS	x	Y	Y	x	x
Bluetooth SCO/eSCO	Y	x	x	x	x
Bluetooth low energy (BLE)	x	x	x	x	Y
Wi-Fi	(VoIP)	Y	Y	Y	x
Wi-Fi Direct	Y	Y	Y	x	x
ZigBee	x	x	x	x	Y

State =
low bandwidth, average/low latency data

Low Power

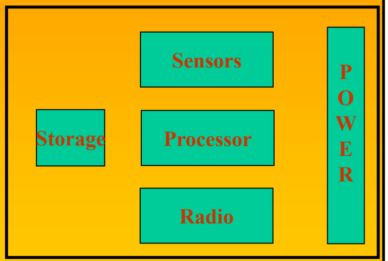
2

What are wireless sensor networks (WSNs)?

- A wireless sensor network (WSN) is a wireless network using sensors to cooperatively monitor physical or environmental conditions
- Networks of typically small, battery-powered, wireless devices (often MANY, sometimes heterogeneous)
  - On-board processing,
  - Communication, and
  - Sensing capabilities.

Or…

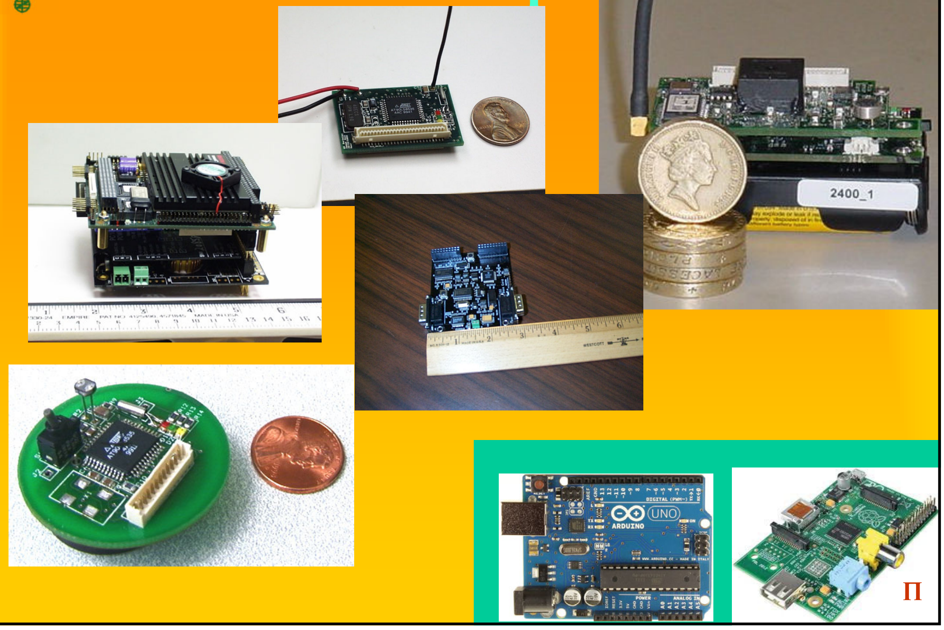
- ➢ Wireless sensing + Data Networking!
  - ➢ Group of sensors linked by wireless media to perform distributed sensing tasks



WSN device schematics

3

Sensor Nodes and platforms

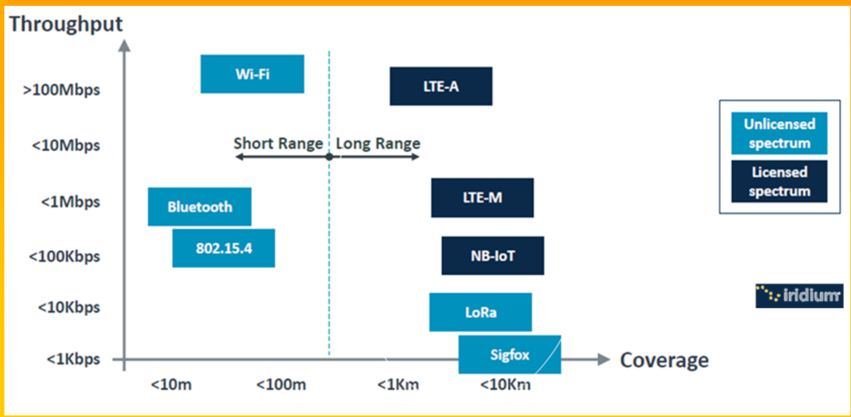


4

5

IoT Wireless Connectivity

As with wireless in general, multiple standards with different properties



5

6

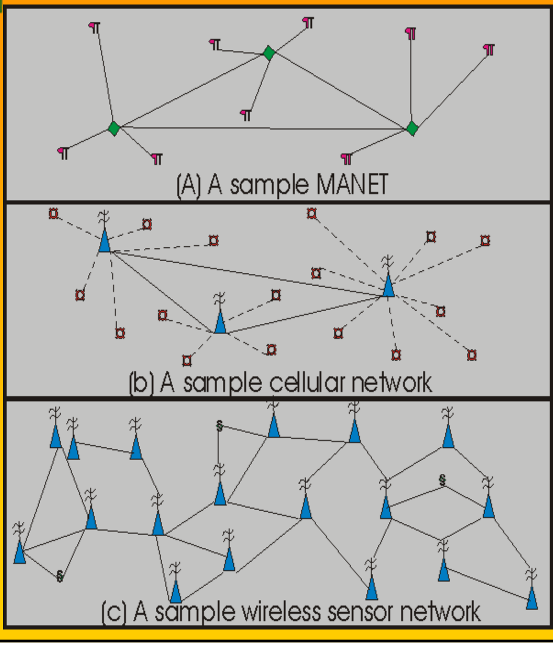
MIoT and HIoT are different

- IoT has multiple scenarios, from human-oriented to machine-oriented, and from industrial to forest environments
- WSN need to adapt to these environments.

	Manufacturing IoT	Consumer IoT
Goal	Manufacturing-industry Centric	Consumer Centric
Devices	Machines, Sensors, Controllers, Actuators, Smart meters	Consumer devices and Smart appliances
Working Environment	Harsh (vibration, noisy, extremely high/low temperature)	Moderate
Data rate	High (usually)	Low or average
Delay	Delay sensitive	Delay tolerant
Mission	Mission-critical	Non-mission-critical

6

Types of wireless Networks



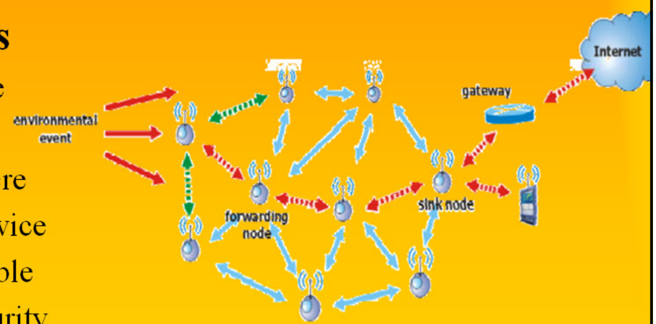
WSN can explore the architecture and protocol concepts both of MANETs (mobile ad-hoc networks) and of celular networks.

7

8

Wireless Sensor Network

- **Focus on:**
  - Ubiquitous Computing
  - Ubiquitous Network Society
  - (often) Human-centric
- **Ubiquitous**
  - Anytime
  - Anyone
  - Anywhere
  - Any Device
  - Affordable
  - All Security
  - Any Information/Service



8

Challenges in WSN's

- Energy and Power Consumption
- Self-organization
- Communication Heterogeneity
- Adaptability
- Security
- Scalability

9

Design Challenges

Why are WSNs challenging/unique?

- Typically, severely energy constrained.
  - Limited energy sources (e.g., batteries).
  - Trade-off between performance and lifetime.
- Self-organizing and self-healing.
  - Remote deployments.
- Scalable.
  - Arbitrarily large number of nodes.

10

Design Challenges

- **Heterogeneity.**
  - Devices with varied capabilities.
  - Different sensors.
  - Hierarchical deployments.
- **Adaptability.**
  - Adjust to operating conditions and changes in application requirements.
- **Security and privacy.**
  - Potentially sensitive information.
  - Hostile environments.

11

Sensor Network MAC Protocols

- **The major sources of energy wastage are:**
  - Collisions – *interfering packets*
  - Overhearing – *hearing more than required from a packet*
  - Control packet overhead – *control versus data*
  - Idle listening – *hearing for nothing*

Typical solutions in wireless MACs (compare LATER with WiFi)

- **Carrier Sensing**
  - Only during low traffic load.
- **Contention**
  - RTS-CTS only during high traffic load.
- **Backoff**
  - Backoff in application layer is desired other than in MAC layer.

Achieving good scalability and collision avoidance capability is necessary.

12

Challenges

1. Energy Efficiency:

- Sensor nodes are not connected to any energy source.
- Energy efficiency is a dominant consideration no matter what the problem is.
- Many solutions, both hardware and software related, have been proposed to optimize energy usage.

2. Ad hoc deployment (adaptability):

- Most sensor nodes are deployed in regions which have no infrastructure.
- We must cope with the changes of connectivity and distribution.

13

Challenges

3. Unattended operation:

- Generally, once sensors are deployed, there is no human intervention for a long time.
- Sensor network must reconfigure by itself when certain errors occur.

4. Dynamic changes (self-healing and scalability)

- As changes of connectivity due to addition of more nodes or failure of nodes, Sensor network must be able to adapt itself to changing connectivity, to arbitrary large numbers of nodes

5. Security

- Both Sensors and Actuators carry sensitive information in an hostile environment

14

15

802.15.4 and Zigbee

15

What is ZigBee?

- **Technological Standard Created for Control and Sensor Networks**
  - **Based on the IEEE 802.15.4 Standard**
  - **Centered in small radios**
- **Created by the ZigBee Alliance**
  - **200+ members**
- **History**
  - ***May 2003: IEEE 802.15.4 completed***
  - **December 2004: ZigBee specification ratified**
  - **June 2005: public availability**

16

What Does ZigBee Do?

- **Designed for wireless controls and sensors**
  - Operates in Personal Area Networks (PAN's) and device-to-device networks
  - Connectivity between small packet devices
  - Examples: control of lights, switches, thermostats, appliances, etc.

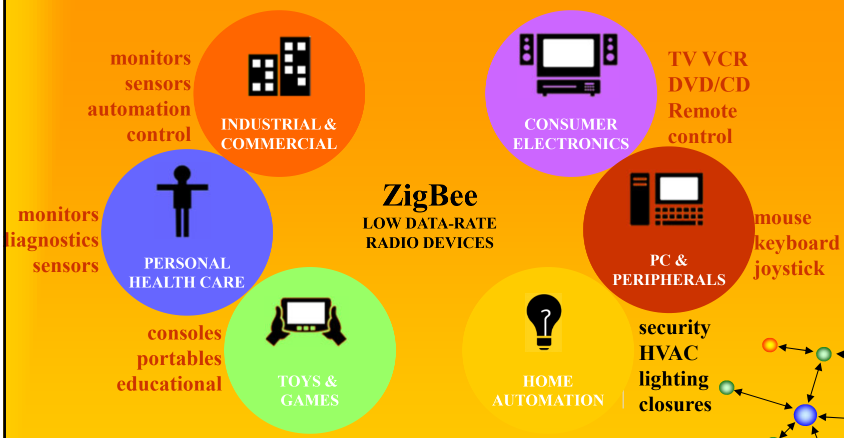
Zigbee?

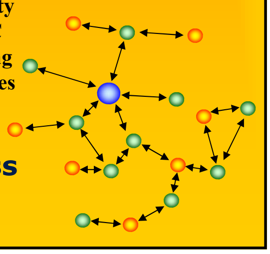
- Named for erratic, zig-zagging patterns of bees between flowers
- Symbolizes communication between nodes in a mesh network
- Network components "seen as analogous" to queen bee, drones, worker bees

17

18

ZigBee network applications





- **Just everything you can imagine for wireless sensor nodes or in general short range communications**

18

ZigBee and Other Wireless Technologies

Market Name Standard	ZigBee™ 802.15.4	--- GSM/GPRS CDMA/1xRTT	Wi-Fi™ 802.11b	Bluetooth™ 802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2^{64})	1	32	7
Bandwidth (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

Source: http://www.zigbee.org/en/about/faq.asp

19

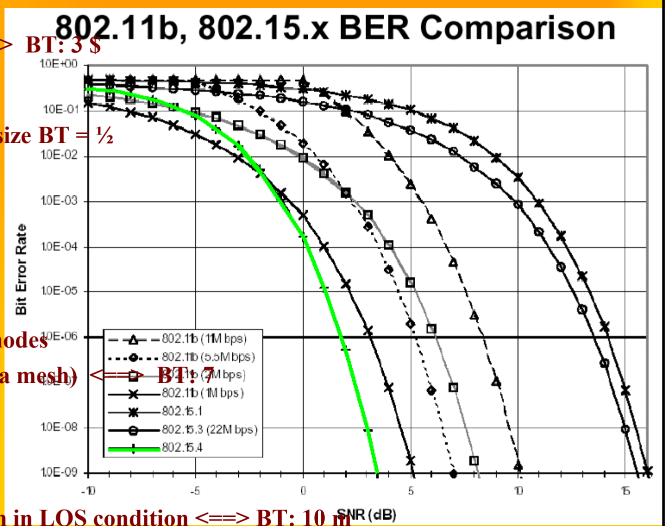
Why do we need another "WPAN" standard?

Lower:

- Power consumption
  - ZigBee: 10mA <==> BT: 100mA
- Production costs
  - ZigBee: 1.1 $ <==> BT: 3 $
- Development costs
  - Codesize ZB/codesize BT = ½
- Bit-error-rate (BER)

Increasing:

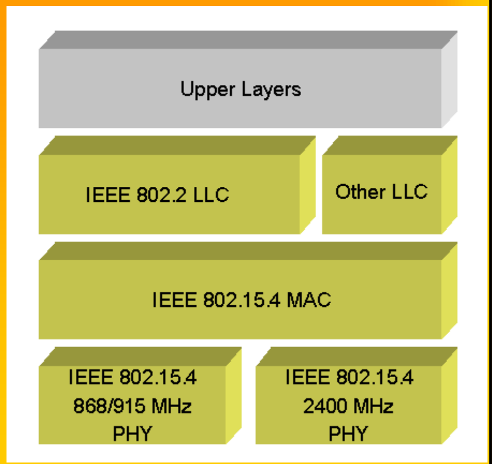
- Sensitivity
- flexibility
  - No. of supported nodes
  - ZigBee: 65536 (in a mesh) <==> BT: 7
- Security
- Latency requirements
- Range
  - ZigBee: up to 75 m in LOS condition <==> BT: 10 m



20

IEEE 802.15.4 - Overview

- Low Rate WPAN (LR-WPAN)
  - E.g. Sensor networks
- Simple and low cost
  - Fully handshake protocol
- Low power consumption
  - Years on lifetime using standard batteries
- Different topologies
  - Star, peer-to-peer, combined
- Data rates: 20-250 kbps
  - Low latency support
- Operates at different frequencies
  - 868 Mhz, 915 Mhz, 2.4 GHz

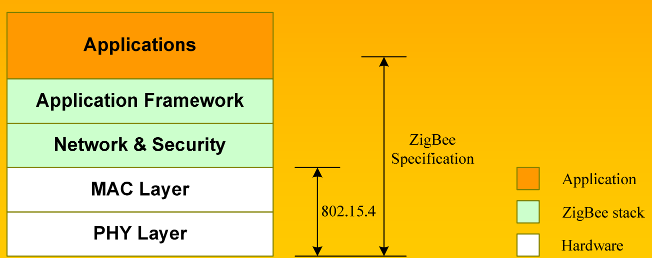


21

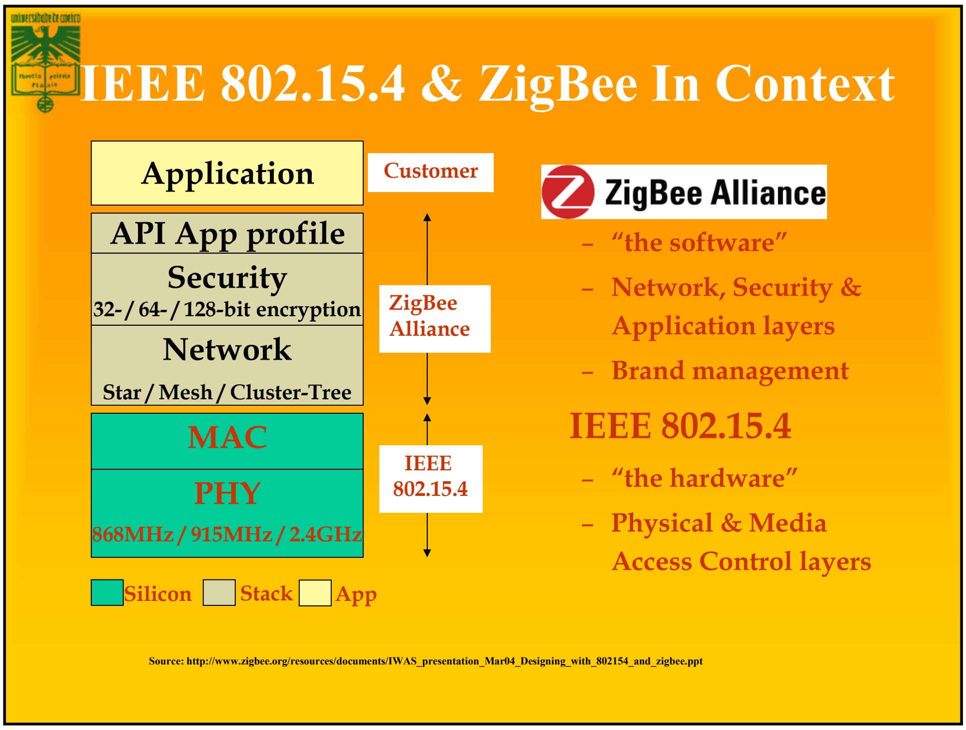
22

ZigBee/802.15.4 architecture

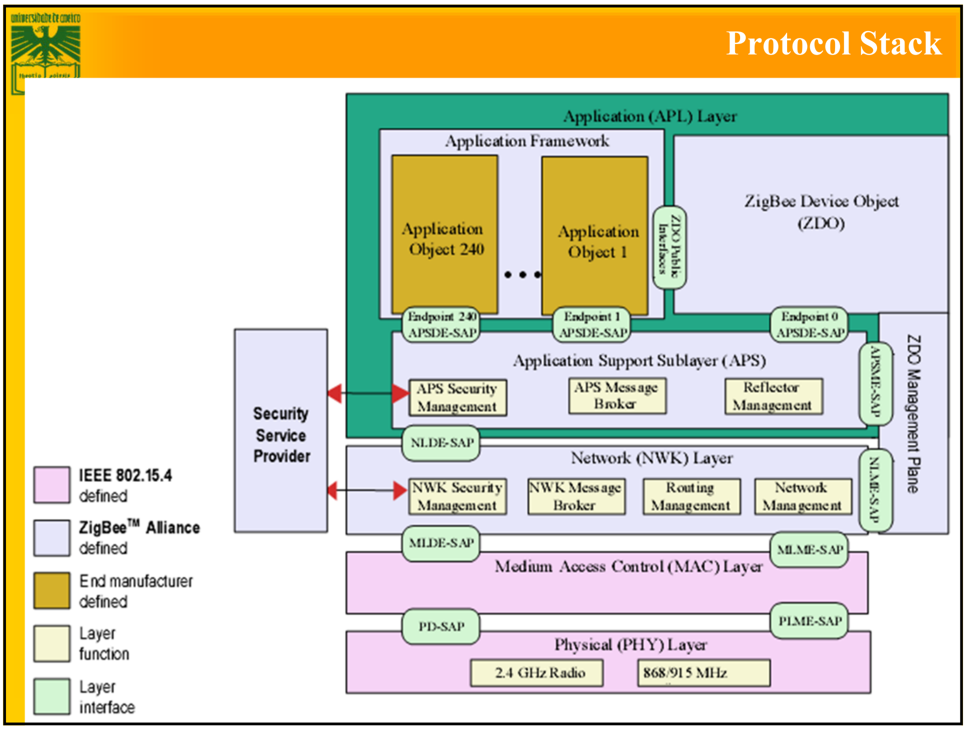
- ZigBee Alliance
  - 45+ companies: semiconductor mfrs, IP providers, OEMs, etc.
  - Defining upper layers of protocol stack: from network to application, including application profiles
  - First profiles published mid 2003
- IEEE 802.15.4 Working Group
  - Defining lower layers of protocol stack: MAC and PHY



22


IEEE 802.15.4 & ZigBee In Context
Application
API App profile
Security
32- / 64- / 128-bit encryption
Network
Star / Mesh / Cluster-Tree
MAC
PHY
868MHz / 915MHz / 2.4GHz
Silicon
Stack
App
Customer
ZigBee Alliance
IEEE 802.15.4
ZigBee Alliance
– "the software"
– Network, Security & Application layers
– Brand management
IEEE 802.15.4
– "the hardware"
– Physical & Media Access Control layers
Source: http://www.zigbee.org/resources/documents/IWAS_presentation_Mar04_Designing_with_802154_and_zigbee.ppt

23


Protocol Stack
Application (APL) Layer
Application Framework
Application Object 240
Application Object 1
ZDO Public Interfaces
ZigBee Device Object (ZDO)
Endpoint 240 APSDE-SAP
Endpoint 1 APSDE-SAP
Endpoint 0 APSDE-SAP
Application Support Sublayer (APS)
APS Security Management
APS Message Broker
Reflector Management
APSME-SAP
ZDO Management Plane
Security Service Provider
NLDE-SAP
Network (NWK) Layer
NWK Security Management
NWK Message Broker
Routing Management
Network Management
NLME-SAP
MLDE-SAP
MLME-SAP
Medium Access Control (MAC) Layer
PD-SAP
PLME-SAP
Physical (PHY) Layer
2.4 GHz Radio
868/915 MHz
IEEE 802.15.4 defined
ZigBee™ Alliance defined
End manufacturer defined
Layer function
Layer interface

24

How ZigBee Works

- Topology
  - Star
  - Cluster Tree
  - Mesh
- Network coordinator, routers, end devices
- 2 or more devices form a PAN/WSN

25

How ZigBee Works

- States of operation
  - Active
  - Sleep
- Devices
  - Full Function Devices (FFD's)
  - Reduced Function Devices (RFD's)
- Modes of operation
  - Beacon
  - Non-beacon
- Traffic types
  - Intermittent
  - Repetitive
  - Periodic

26

IEEE 802.15.4: Traffic-Types

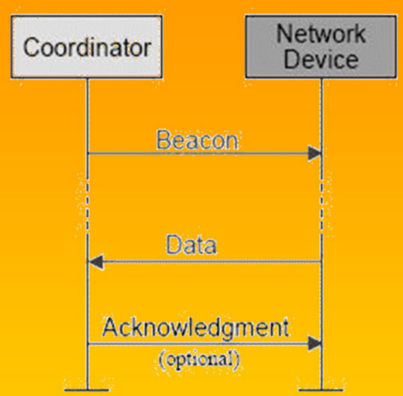
- **Data is periodic**
  - application dictates rate (e.g. sensors)
- **Data is intermittent**
  - application or stimulus dictates rate (optimum power savings), e.g. light switch
- **Data is repetitive (fixed rate a priori)**
  - device gets guaranteed time slot (e.g. heart monitor)

27

IEEE 802.15.4: Traffic-Modes

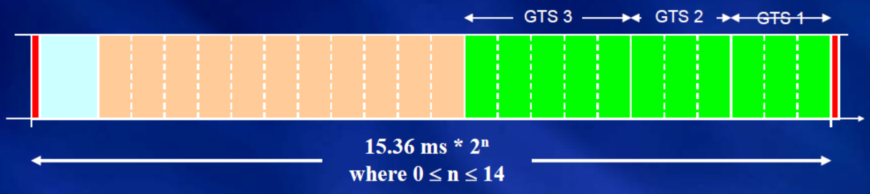
Beacon mode:

- beacon sent periodically
- Coordinator and end device can go to power save
- Lowest energy consumption
- Precise timing needed
- Beacon period (ms-m)



28

Beacon Mode



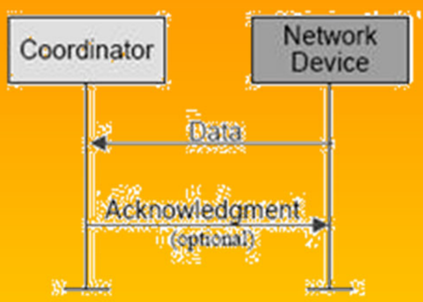
Network beacon	Transmitted by network coordinator. Contains network information, frame structure and notification of pending node messages.
Beacon extension period	Space reserved for beacon growth due to pending node messages
Contention period	Access by any node using CSMA-CA
Guaranteed Time Slot	Reserved for nodes requiring guaranteed bandwidth.

29

IEEE 802.15.4: Traffic-Modes

Non-Beacon mode:

- **coordinator/routers have to stay awake (robust power supply needed)**
- **heterogeneous network**
- **asymmetric power**



30

ZigBee Node-Types

ZigBee Coordinator (ZBC) (IEEE 802.15.4 FFD)

- only one in a network
- initiates network
- stores information about the network
- all devices communicate with the ZBC
- routing functionality
- bridge to other networks

ZigBee Router (ZBR) (IEEE 802.15.4 FFD)

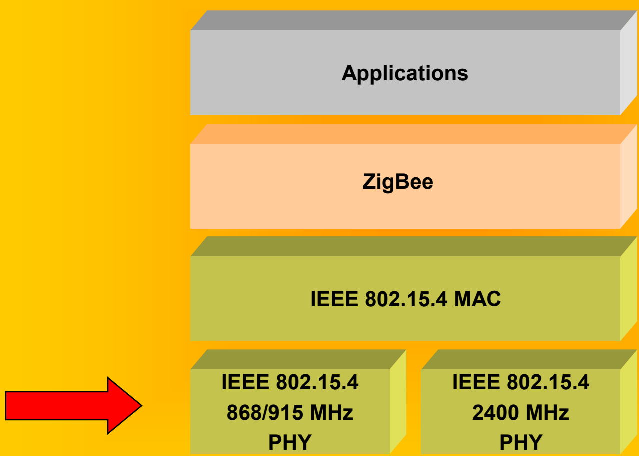
- optional component
- routes between nodes, network backbone
- extends network coverage
- manages local address allocation/de-allocation

ZigBee End Device (ZBE) (IEEE 802.15.4 RFD)

- optimized for low power consumption
- cheapest device type
  - sensor would be deployed here

31

802.15.4 / ZigBee Architecture



- Packet generation
- Packet reception
- Data transparency
- Power Management

32

33

IEEE 802.15.4 basics

- **802.15.4 is a simple packet data protocol for lightweight wireless networks**
  - **Channel Access is via Carrier Sense Multiple Access with collision avoidance and optional time slotting**
  - **Message acknowledgement and an optional beacon structure**
  - **Multi-level security**
  - **Works well for**
    - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics
  - **Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries**

33

34

802.15.4 General characteristics

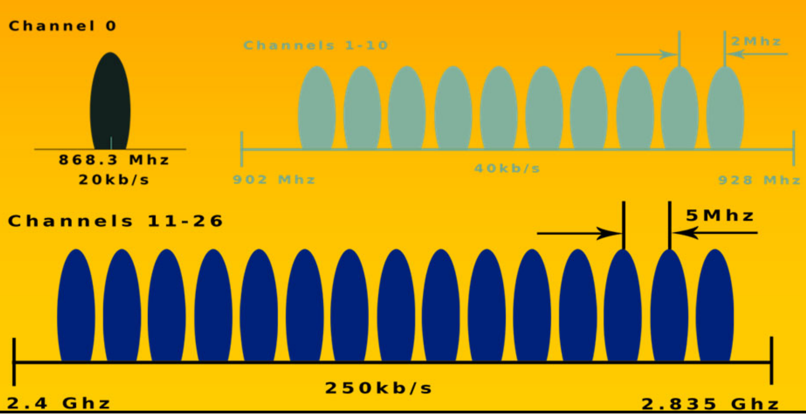
- Data rates of 250 kbps , 20 kbps and 40kpbs.
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- CSMA-CA channel access, with CCA detection
- Dynamic device addressing.
- Fully handshaked protocol for transfer reliability.
- Low power consumption.
- 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz ISM band and one channel in the European 868MHz band.
- Extremely low duty-cycle (<0.1%)

34

802.15.4 frequency bands

Operates in Unlicensed Bands

- ISM 2.4 GHz Global Band at 250kbps
- 868 MHz European Band at 20kbps
- 915 MHz North American Band at 40kbps



35

36

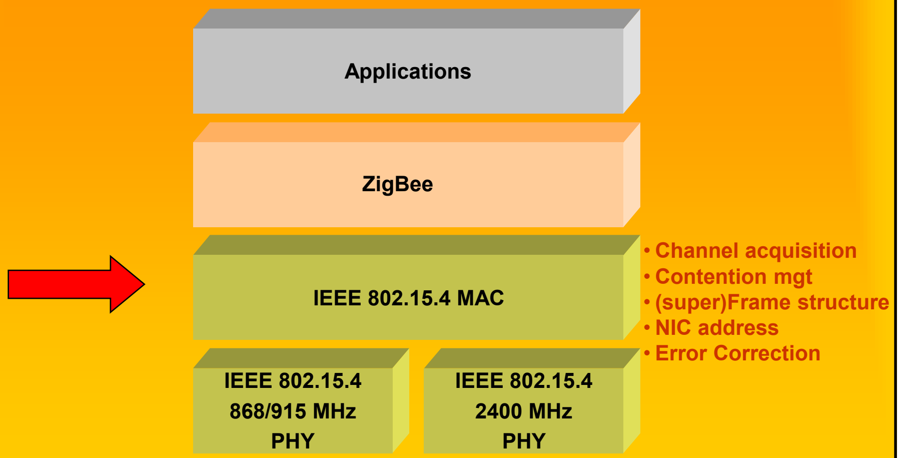
PHY frame structure

- PHY packet fields
  - Preamble (32 bits) – synchronization
  - Start of packet delimiter (8 bits) – shall be formatted as “11100101”
  - PHY header (8 bits) –PSDU length
  - PSDU (0 to 127 bytes) – data field

Sync Header		PHY Header		PHY Payload
Preamble	Start of Packet Delimiter	Frame Length (7 bit)	Reserve (1 bit)	PHY Service Data Unit (PSDU)
4 Octets	1 Octets	1 Octets		0-127 Bytes

36

802.15.4 Architecture (MAC)

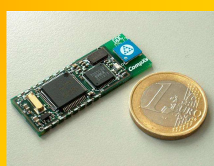


37

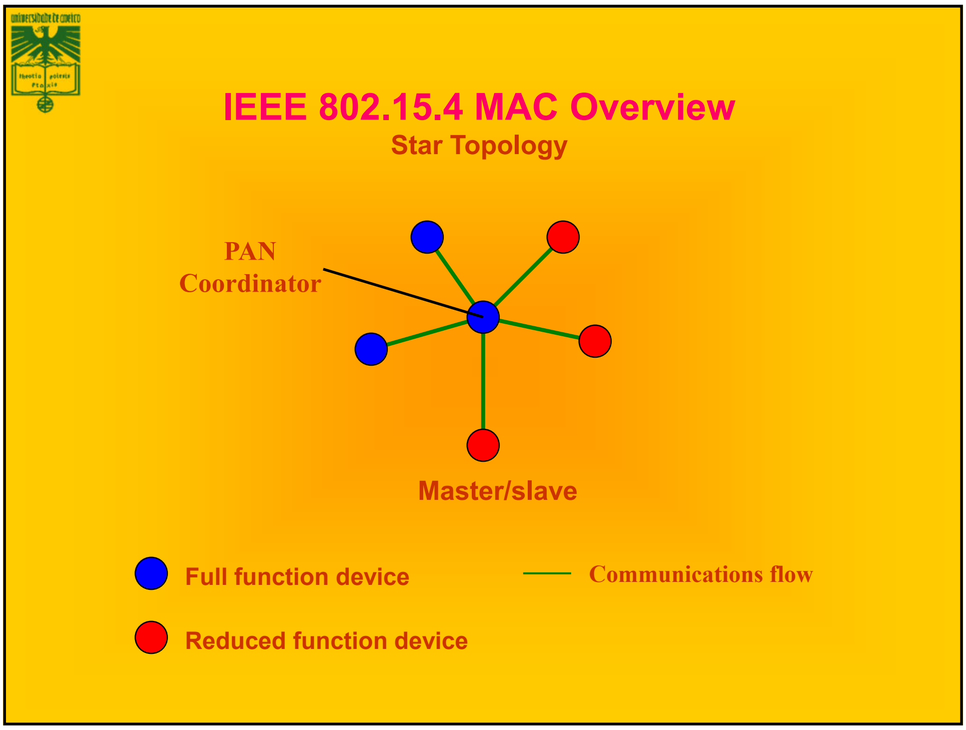
IEEE 802.15.4 MAC Overview

Device Classes

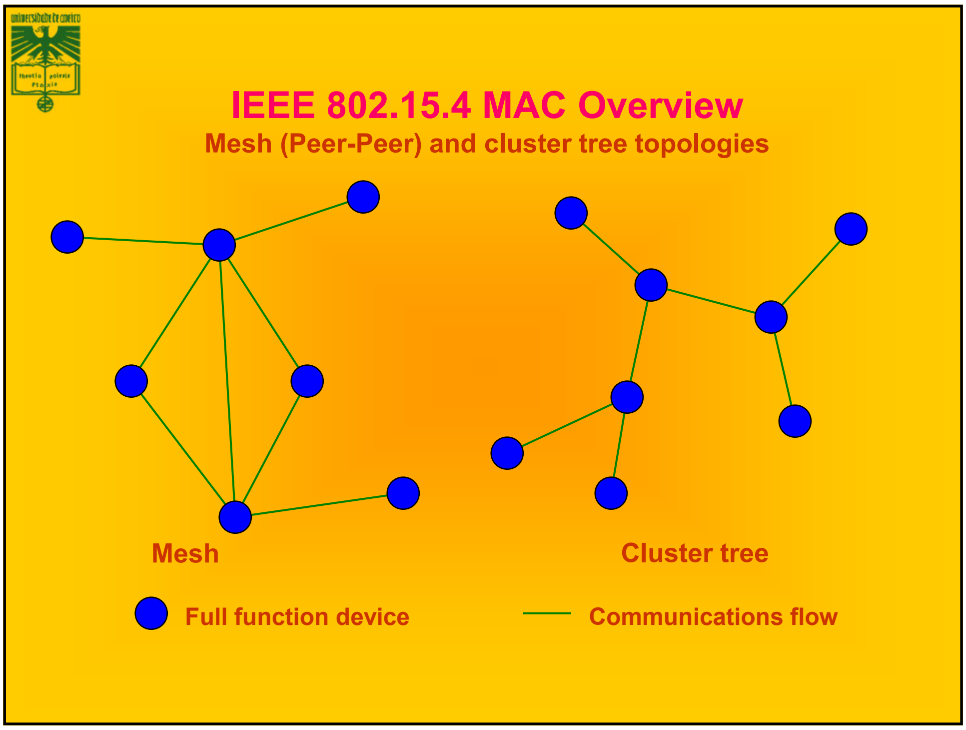
- **Full function device (FFD)**
  - Any topology
  - Network coordinator capable
  - Talks to any other device
  - The FFD can operate in three modes serving
    - Device
    - Coordinator
    - PAN coordinator
- **Reduced function device (RFD)**
  - Limited to star topology
  - Talks only to a network coordinator
    - Cannot become a network coordinator
  - Very simple implementation



38


universidade de aveiro
theoria poiesis praxis
IEEE 802.15.4 MAC Overview
Star Topology
PAN
Coordinator
Master/slave
Full function device
Communications flow
Reduced function device

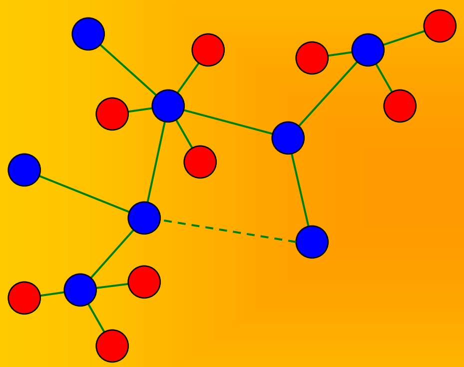
39


universidade de aveiro
theoria poiesis praxis
IEEE 802.15.4 MAC Overview
Mesh (Peer-Peer) and cluster tree topologies
Mesh
Cluster tree
Full function device
Communications flow

40

IEEE 802.15.4 MAC Overview

Combined Topology



Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

May have a mesh structure in some cases as well

Full function device

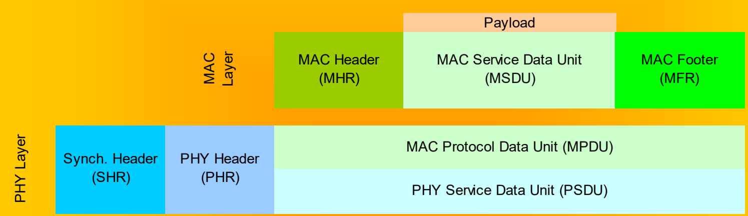
Reduced function device

Communications flow

41

IEEE 802.15.4 MAC Overview

General Frame Structure



4 Types of MAC Frames:

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

42

MAC layer

Managing PANs

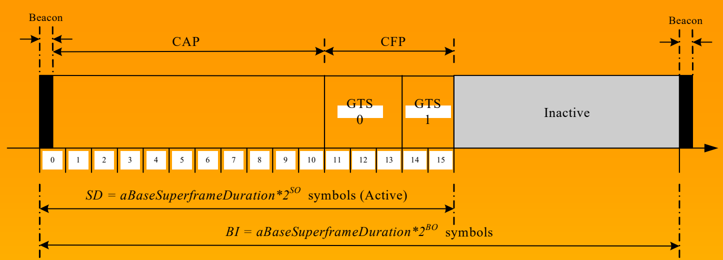
- **Channel scanning (ED, active, passive, orphan)**
- **PAN ID conflict detection and resolution**
- **Starting a PAN**
- **Sending beacons**
- **Device discovery, association/disassociation**
- **Synchronization (beacon/nonbeacon)**
- **Orphaned device realignment**

Transfer handling

- **Transaction based (indirect transmission)**
  - **Beacon indication**
  - **Polling**
- **Transmission, Reception, Rejection, Retransmission**
  - **Acknowledged / Not acknowledged**
- **GTS management**
  - **Allocation/deallocation/Reallocation**
  - **Usage**

43

Superframe



- **A superframe is divided into two parts**
  - **Inactive: all devices sleep**
  - **Active:**
    - Active period will be divided into 16 slots
    - 16 slots can further divided into two parts
      - » Contention access period
      - » Contention free period

44

44

45

Superframe

- Beacons are used for
  - starting superframes
  - synchronizing with associated devices
  - announcing the existence of a PAN
  - informing pending data in coordinators
- In a beacon enabled network,
  - Devices use the slotted CAMA/CA mechanism to contend for the usage of channels
  - FFDs which require fixed rates of transmissions can ask for *guarantee time slots (GTS)* from the coordinator

45

46

GTS concepts

- A guaranteed time slot (GTS) allows a device to operate on the channel within a portion of the superframe
- A GTS shall only be allocated by the PAN coordinator
- The PAN coordinator can allocated up to seven GTSs at the same time
- The PAN coordinator decides whether to allocate GTS based on:
  - Requirements of the GTS request
  - The current available capacity in the superframe

46

47

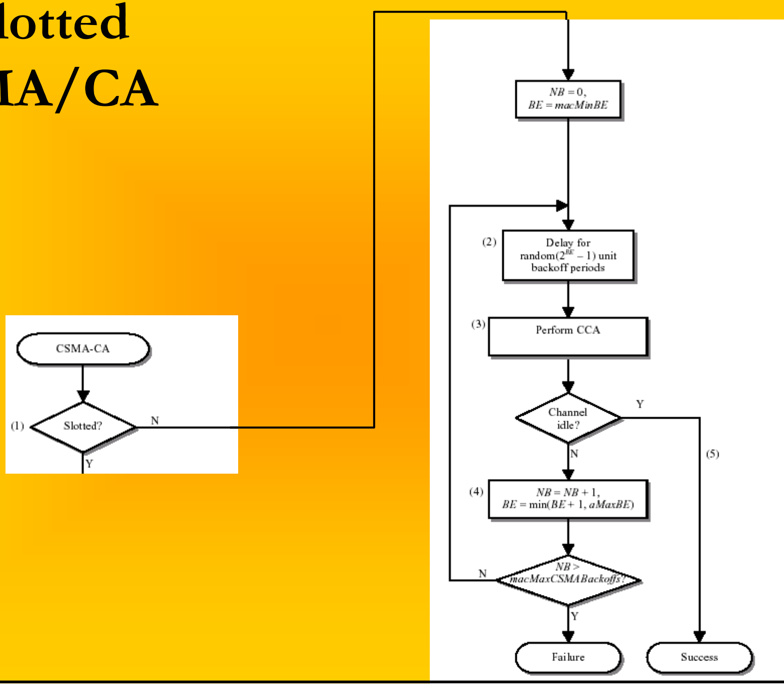
Channel access mechanism

- **Two type channel access mechanism:**
  - **In non-beacon-enabled networks → unslotted CSMA/CA channel access mechanism**
  - **In beacon-enabled networks → slotted CSMA/CA channel access mechanism**

47

48

Unslotted CSMA/CA



48

49

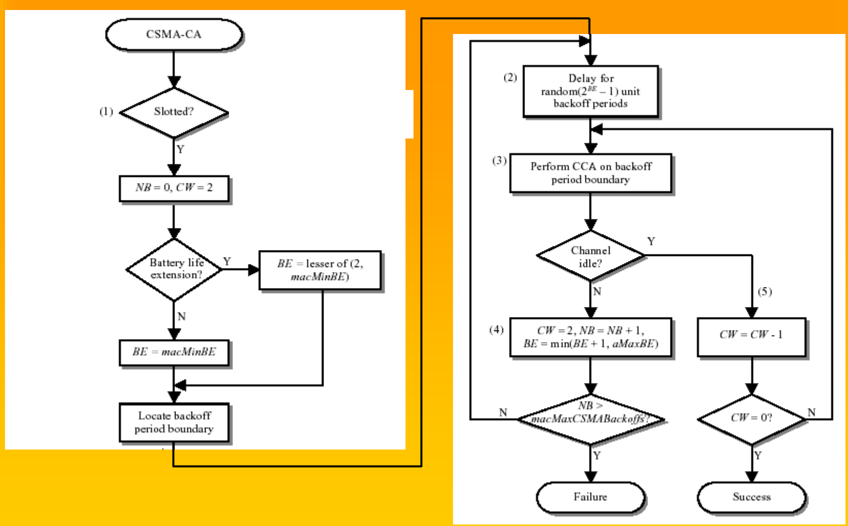
CSMA/CA algorithm

- **In slotted CSMA/CA**
  - **The backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries of the PAN coordinator**
    - i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission
  - **The MAC sublayer shall ensure that the PHY layer commences all of its transmissions on the boundary of a backoff period**

49

50

Slotted CSMA/CA

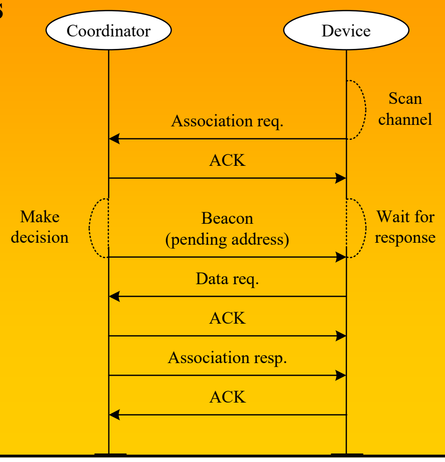


50

51

Association procedures

- A device becomes a member of a PAN by associating with its coordinator
- Procedures



51

52

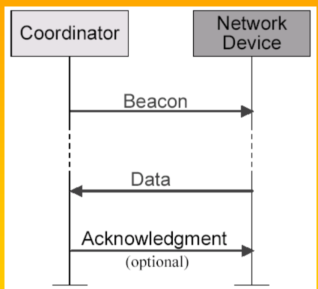
Association procedures

- In IEEE 802.15.4, association results are announced in an indirect fashion
- A coordinator responds to association requests by appending devices' long addresses in beacon frames
- Devices need to send a data request to the coordinator to acquire the association result
- After associating to a coordinator, a device will be assigned a 16-bit *short address*.

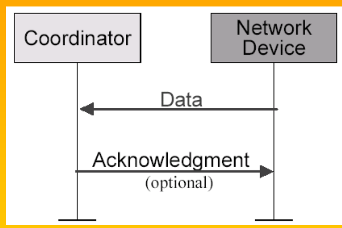
52

Data transfer model (device to coordinator)

- **Data transferred from device to coordinator**
  - **In a beacon-enable network, device finds the beacon to synchronize to the superframe structure. Then using slotted CSMA/CA to transmit its data.**
  - **In a non beacon-enable network, device simply transmits its data using unslotted CSMA/CA**



Communication to a coordinator
In a beacon-enabled network



Communication to a coordinator
In a non beacon-enabled network

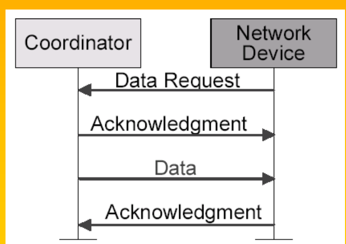
53

53

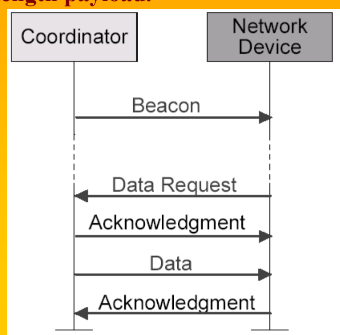
54

Data transfer model (coordinator to device)

- **Data transferred from coordinator to device**
  - **In a beacon-enable network, the coordinator indicates in the beacon that the data is pending. Device periodically listens to the beacon and transmits a MAC command request using slotted CSMA/CA if necessary.**
  - **In a non-beacon-enable network, a device transmits a MAC command request using unslotted CSMA/CA. If the coordinator has its pending data, the coordinator transmits data frame using unslotted CSMA/CA. Otherwise, coordinator transmits a data frame with zero length payload.**



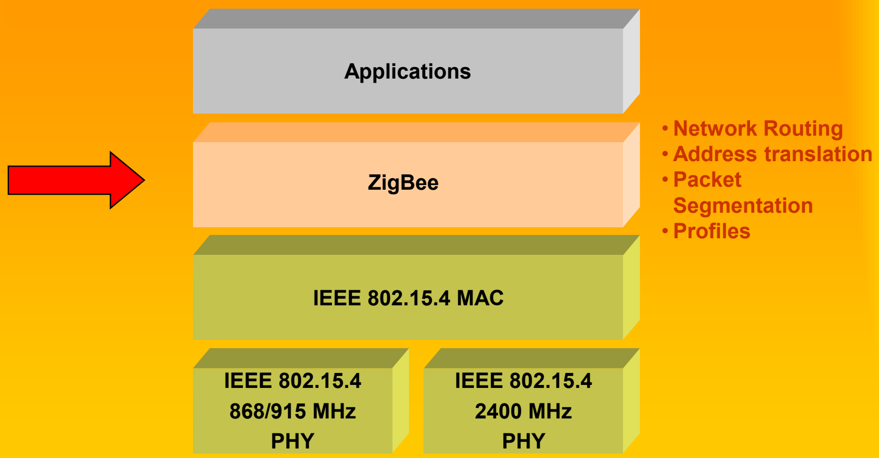
Communication from a coordinator
in a non beacon-enabled network



Communication from a coordinator
In a beacon-enabled network

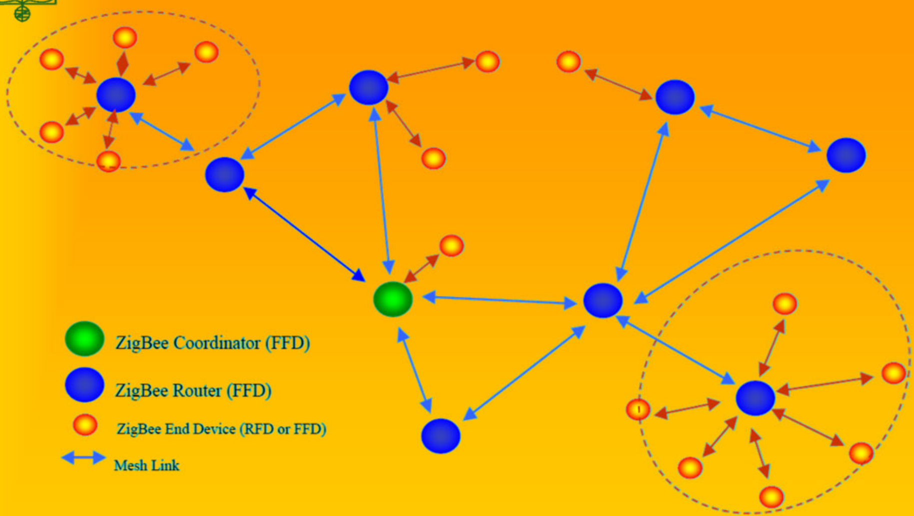
54

802.15.4 Architecture



55

Combined topologies: Mesh Topologies

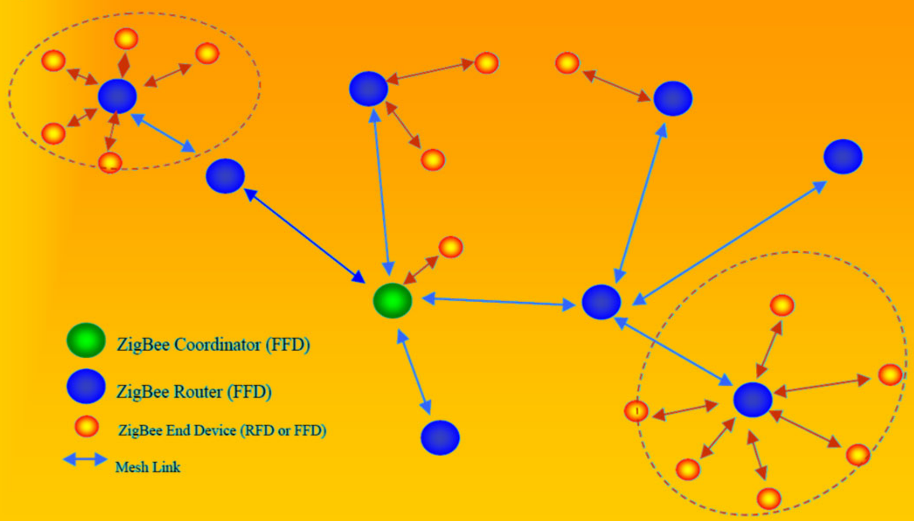


In a mesh network, regular beacons are not allowed.

Devices in a mesh network can only communicate with each other by peer-to-peer transmissions

56

Combined Topologies: Tree



In a tree network, the coordinator and routers can announce beacons.

57

58

Device addressing

- **Two or more devices communicating on the same physical channel constitute a WPAN which includes <u>at least one FFD (PAN coordinator)</u>**
- **Each independent PAN will select a unique PAN identifier**
- **All devices operating on a network shall have unique 64-bit extended address (IEEE 802.15.4). This address can be used for direct communication in the PAN**
- **The network address can use a 16-bit short address, which is allocated to the child routers by the PAN coordinator when the device associates**
- **256 sub addresses may be allocated for subunits**

58

59

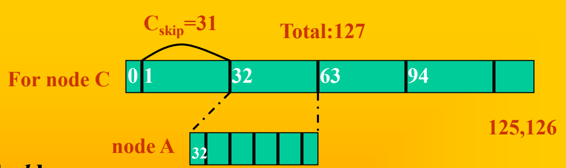
Address assignment in a ZigBee network

- In ZigBee, network addresses are assigned to devices by a distributed address assignment scheme
- ZigBee coordinator determines three network parameters to set the allocations
  - the maximum number of children (C_m) of a ZigBee router
  - the maximum number of child routers (R_m) of a parent node
  - the depth of the network (L_m)
- A parent device utilizes C_m, R_m, and L_m to compute a parameter called C_{skip}
  - which is used to compute the size of its children's address pools

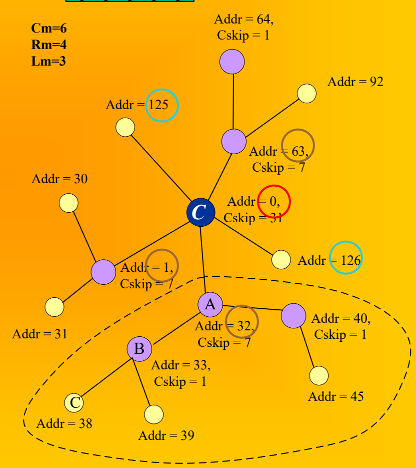
$$Cskip(d)=\begin{cases}1+Cm\cdot(Lm-d-1), & \text{if } Rm=1 \quad\cdots\cdots\cdots\cdots\text{(a)}\\ \dfrac{1+Cm-Rm-Cm\cdot Rm^{Lm-d-1}}{1-Rm}, & \text{Otherwise} \quad\cdots\cdots\cdots\cdots\text{(b)}\end{cases}$$

59

60



- If a parent node at depth d has an address A_{parent},
  - the nth child router is assigned to address $A_{parent}+(n-1)\times C_{skip}(d)+1$
  - nth child end device is assigned to address $A_{parent}+R_m\times C_{skip}(d)+n$



60

61

ZigBee routing protocols

- **In a tree network**
  - **Utilize the address assignment to obtain the routing paths**
- **In a mesh network**
  - **Two options**
    - Reactive routing: if having routing capacity
    - Use tree routing: if do not have routing capacity
- **Note:**
  - **ZigBee coordinators and routers are said to have *routing capacity* if they have routing table capacities and route discovery table capacities**

61

62

Summary of ZigBee network layer

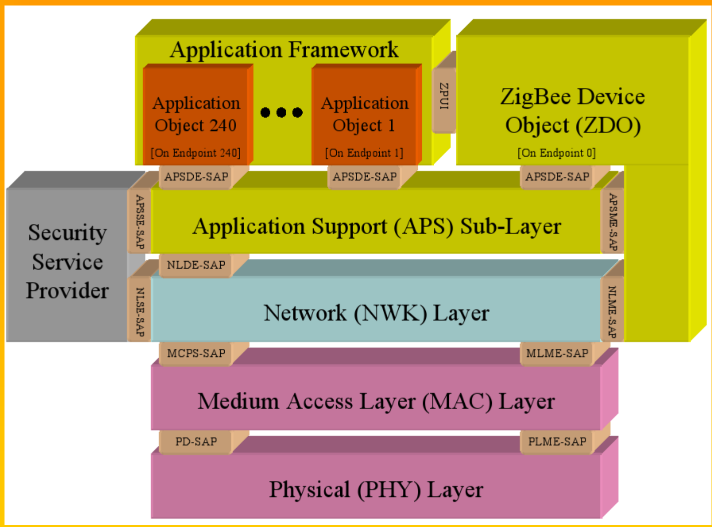
- **Pros and cons of different kinds of ZigBee network topologies**

	Pros	Cons
Star	1. Easy to synchronize 2. Support low power operation 3. Low latency	1. Small scale
Tree	1. Low routing cost 2. Can form superframes to support sleep mode 3. Allow multihop communication	1. Route reconstruction is costly 2. Latency may be quite long
Mesh	1. Robust multihop communication 2. Network is more flexible 3. Lower latency	1. Cannot form superframes (and thus cannot support sleep mode) 2. Route discovery is costly 3. Needs storage for routing table

62

ZigBee – Short range comunication

Application Level



63

ZigBee – Short range comunication

Application Layer

ZigBee defined Objects (ZDO):

- **provides common function for applications**
- **Initializes APS, NWK-Layer and Security Service Specification**
- **offers services like device-/service-descovery, binding and security management**
- **assembles information about the network**
- **for ZBC/ZBR -> e.g. binding table**

Command	Addressing	
	Request	Response
End device bind	Unicast to ZC	Unicast
Bind	Unicast to ZC or Src	Unicast
Unbind	Unicast to ZC or Src	Unicast

64

ZigBee Profiles

Profiles:

Definition of ZigBee-Profiles
- describes a common language for exchanging data
- defines the offered services
- device interoperatbility across different manufacturers
- Standard profiles available from the ZigBee Alliance
- profiles contain device descriptions
- unique identifier (licensed by the ZigBee Alliance)

65

66

ZigBee vs BLE

- Business comparison:
  - ZigBee is older. It has gone through some iterations
  - ZigBee has market mindshare, but not a lot of shipments yet.
  - Market barriers: connectivity – ZigBee is not in PCs or mobile phones yet.
- Technical comparison:
  - Zigbee is low power; Bluetooth LE is even lower. Detailed analysis depends on specific applications and design detail, no to mention chip geometry.
  - ZigBee stack is light; the Bluetooth LE/GATT stack is even simpler
- Going forward:
  - ZigBee has a lead on developing applications and presence
  - BLE has improved technology, and a commanding presence in several existing markets: mobile phones, automobiles, consumer electronics, PC industry
  - Replacing “classic Bluetooth ” with “dual mode” devices may bootstrap this market quickly

66

67

Wide Area Wireless Sensor Networks

WWSN

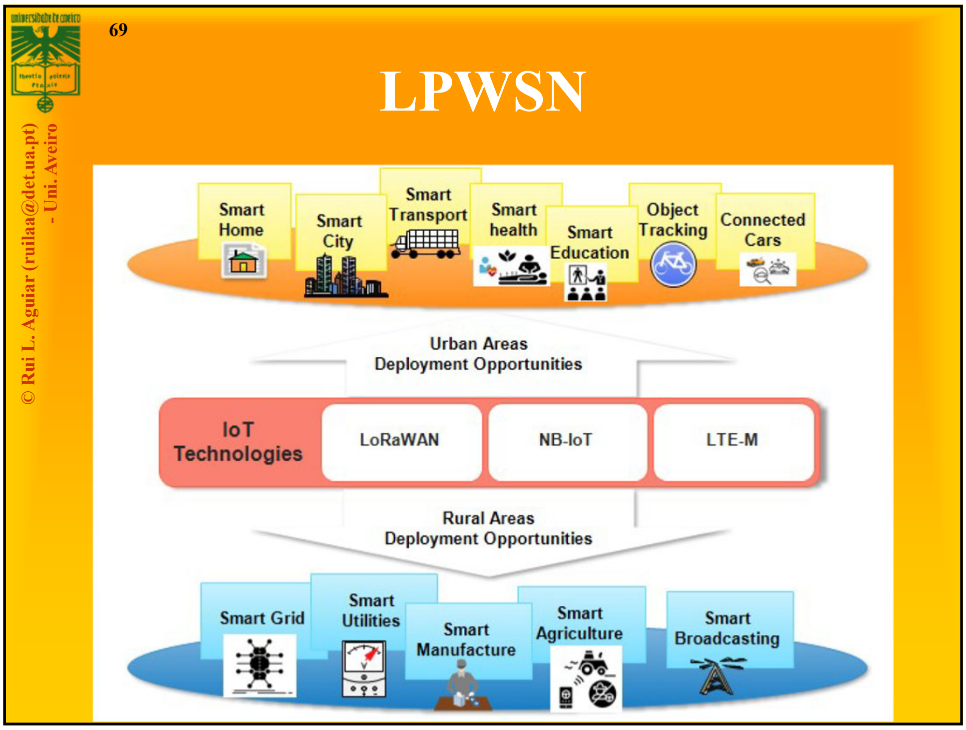
67

68

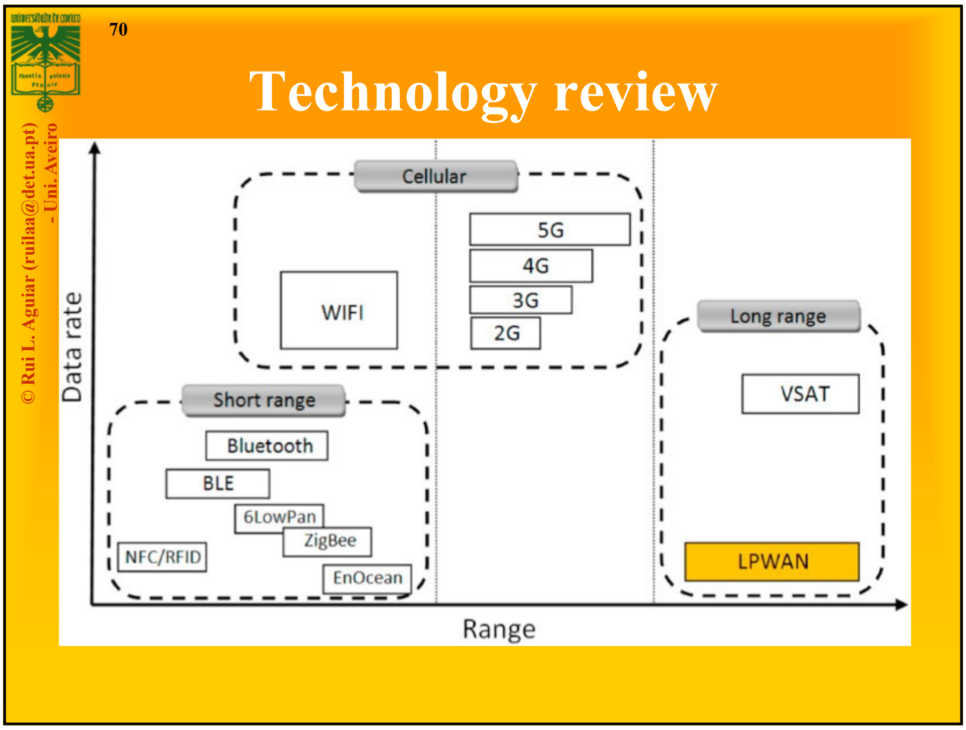
What is this?

- **WWSN – wide area wireless sensor networks**
- **LPWSN – low power wireless sensor networks**
- **Technologies for sensor networks in wide areas**
  - **either for low power, or for geography**
  - **Typically: Sigfox, LoRa, cellular (LTE-M, NB-IoT)**

68


69
LPWSN
© Rui L. Aguiar (ruilaa@det.ua.pt) - Uni. Aveiro
Smart Home
Smart City
Smart Transport
Smart health
Smart Education
Object Tracking
Connected Cars
Urban Areas
Deployment Opportunities
IoT Technologies
LoRaWAN
NB-IoT
LTE-M
Rural Areas
Deployment Opportunities
Smart Grid
Smart Utilities
Smart Manufacture
Smart Agriculture
Smart Broadcasting

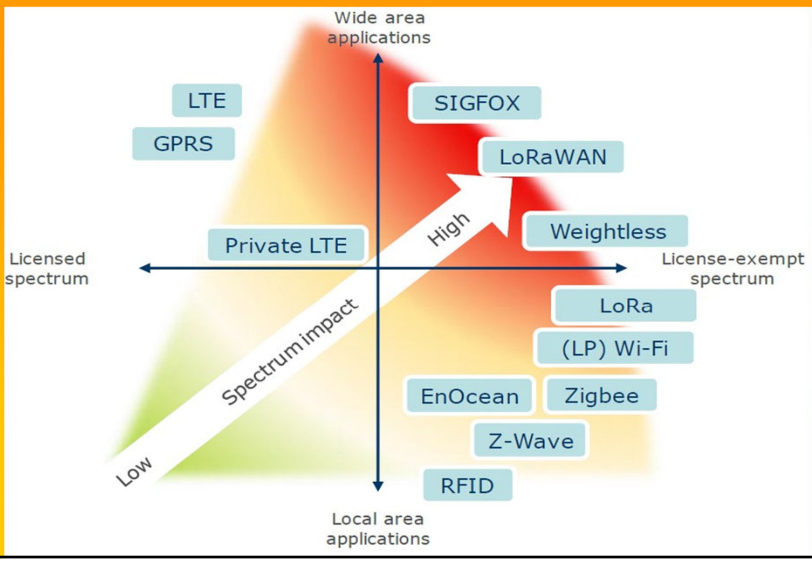
69


70
Technology review
© Rui L. Aguiar (ruilaa@det.ua.pt) - Uni. Aveiro
Cellular
5G
4G
3G
2G
WIFI
Long range
VSAT
LPWAN
Short range
Bluetooth
BLE
6LowPan
ZigBee
NFC/RFID
EnOcean
Data rate
Range

70

71

Licensed vs licensed-exempt



71

72

Overview of LPWAN

Overview of LPWAN technologies: Sigfox, LoRa, and NB-IoT.

	Sigfox	LoRaWAN	NB-IoT
Modulation	BPSK	CSS	QPSK
Frequency	Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia)	Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia)	Licensed LTE frequency bands
Bandwidth	100 Hz	250 kHz and 125 kHz	200 kHz
Maximum data rate	100 bps	50 kbps	200 kbps
Bidirectional	Limited / Half-duplex	Yes / Half-duplex	Yes / Half-duplex
Maximum messages/day	140 (UL), 4 (DL)	Unlimited	Unlimited
Maximum payload length	12 bytes (UL), 8 bytes (DL)	243 bytes	1600 bytes
Range	10 km (urban), 40 km (rural)	5 km (urban), 20 km (rural)	1 km (urban), 10 km (rural)
Interference immunity	Very high	Very high	Low
Authentication & encryption	Not supported	Yes (AES 128b)	Yes (LTE encryption)
Adaptive data rate	No	Yes	No
Handover	End-devices do not join a single base station	End-devices do not join a single base station	End-devices join a single base station
Localization	Yes (RSSI)	Yes (TDOA)	No (under specification)
Allow private network	No	Yes	No
Standardization	Sigfox company is collaborating with ETSI on the standardization of Sigfox-based network	LoRa-Alliance	3GPP

	Spectrum cost	Deployment cost	End-device cost
Sigfox	Free	>4000€/base station	<2€
LoRa	Free	>100€/gateway >1000€/base station	3–5€
NB-IoT	>500 M€ /MHz	>15 000€/base station	>20€

72

73

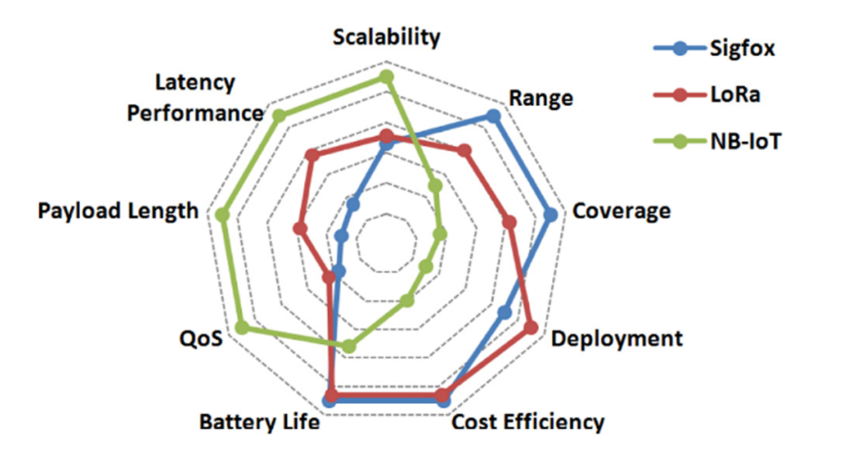
Network Items	SigFox [48]	LoRaWAN [45]	NB-Fi [49]	NB-IoT [26]	LTE-M [50]
Bandwidth	100 Hz	250 kHz & 125 kHz	50 Hz–25.6 kHz	200 kHz	200 kHz
Modulation	BPSK	CSS	DBPSK	QPSK	QPSK
Standardisation	SigFox/ETSI	LoRA Alliance	WAVIoT	3GPP	3GPP
Max. Data Rate	100 bps	50 kbps	25 kbps	200 kbps	200 kbps
Bidirectional	HD	HD	FD & HD	HD	HD
Architecture	SoS	SoS	SoS	SoS	SoS
Frequency	ISM-bands	ISM-bands	ISM-bands	LTE-bands	LTE-bands
Payload	UL-12 B & DL-7 B	243 B	240 B	1600 B	256 B
Security	AES-128	AES-128	AES-256	LTE Enc	LTE Enc
Interference	High	High	High	Low	low
Urban Range	10 km	5 km	10 km	1 km	1 km
Rural Range	40 km	20 km	40 km	4 km	4 km

Note: B—bytes; SoS—star-of-stars; UL—uplink; DL—downlink; Enc—encryption.

73

74

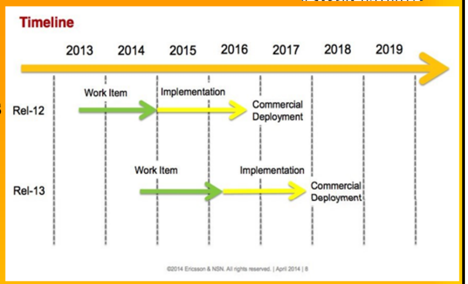
Comparison Radar



74

LTE-M - Overview

- Evolution of LTE optimized for IoT
- Low power consumption and autonomous
- Easy Deployment
- Interoperability with existing LTE networks
- Coverage up to 11 Km
- Max Throughput ≤ 1 Mbps



- ✓ First released in Rel.12 in 2 Q4 2014
- ✓ Optimization in Rel.13
- ✓ Specifications completed in Q1 2016
- ✓ Available since 2017

75

Evolution from LTE to LTE-M

3GPP Releases	8 (Cat.4)	8 (Cat. 1)	12 (Cat.0) LTE-M	13 (Cat. 1,4 MHz) LTE-M
Downlink peak rate (Mbps)	150	10	1	1
Uplink peak rate (Mbps)	50	5	1	1
Number of antennas (MIMO)	2	2	1	1
Duplex Mode	Full	Full	Half	Half
UE receive bandwidth (MHz)	20	20	20	1.4
UE Transmit power (dBm)	23	23	23	20

Release 12

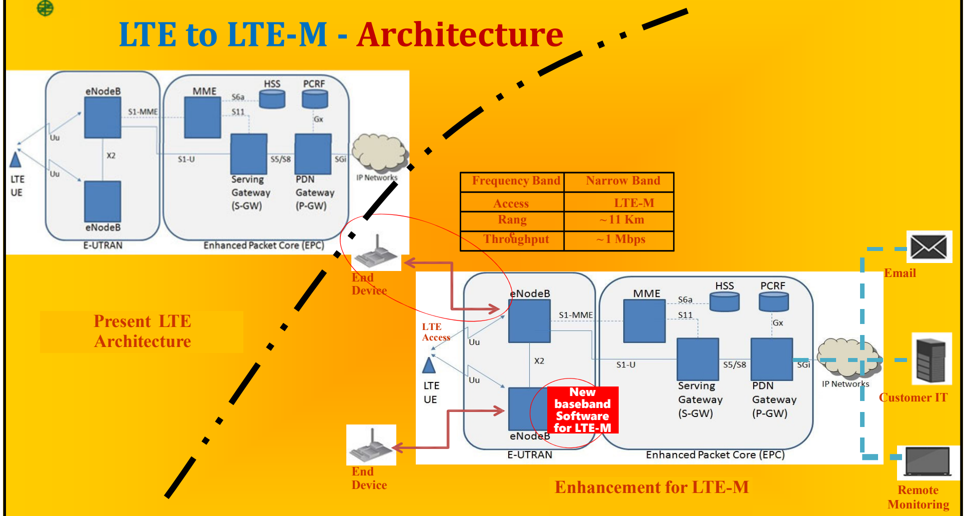
- New category of UE ("Cat-0"): lower complexity and low cost devices
- Half duplex FDD operation allowed
- Single receiver
- Lower data rate requirement (Max: 1 Mbps)

Release 13

- Reduced receive bandwidth to 1.4 MHz
- Lower device power class of 20 dBm
- 15dB additional link budget: better coverage
- More energy efficient because of its extended discontinuous repetition cycle (eDRX)

76

LTE to LTE-M - Architecture



Frequency Band	Narrow Band
Access	LTE-M
Rang	~11 Km
Throughput	~1 Mbps

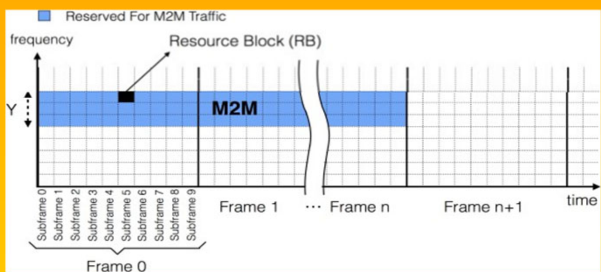
The only change neeeded is proper updates in the control of the baseband.
LTE-M is a simple exploitation over an operational LTE network

77

LTE-M

- Licensed Spectrum
- Frequency Bands: 700-900 MHz for LTE

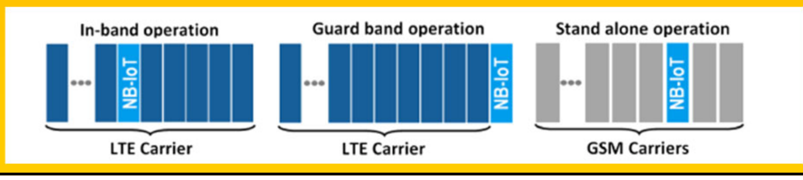
  (Lower frequencies for higher coverages)
- Some resource blocks are allocated to IoT on LTE bands



78

NB-IoT

- Defined in R13, another mode instead of LTE-M
- Bandwidth – 200KHz
  - One resource block in GSM/LTE
- Based in LTE protocol, stripped down
  - OFDMA(down)/FDMA(up), QPSK
  - 200kbps (down)/20kbps(up)
- Three modes of operation



79

NB-IoT

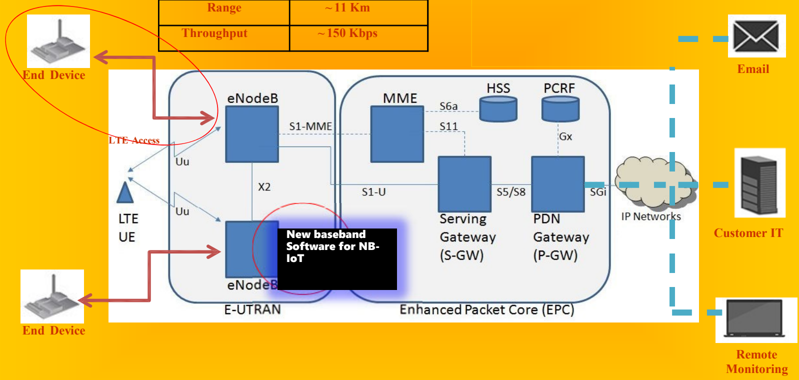
- **Uses LTE design extensively** e.g. DL: FDMA, UL: SC-FDMA
- **Lower cost than MTC:** Narrow band: supports 180 KHz channel
- **Long battery life:** 10 years with 5 Watt Hour battery (depending on traffic and coverage needs)
  - **Extended coverage:** 164 dB maximum coupling loss or link budget (at least for standalone) in comparison to GPRS link budget of 144dB and LTE of 142.7 dB
  - **Low Receiver sensitivity** = -141 dBm
- **Support for massive number of devices:** at least 50.000 per cell
- **3 modes of operation:**
  - **Stand-alone**: *stand-alone carrier, e.g. spectrum currently used by GERAN (GSM Edge Radio Access Network) systems as a replacement of one or more GSM carriers*
  - **Guard band:** *unused resource blocks within a LTE carrier's guard-band*
  - **In-band:** *resource blocks within a normal LTE carrier*

80

NB-IoT - Architecture

HD-FDD
p/2 BPSK, Class 3 (23 dBm)
p/4 QPSK Class 5 (20 dBm)

Frequency Band	Ultra Narrow Band
Range	~11 Km
Throughput	~150 Kbps

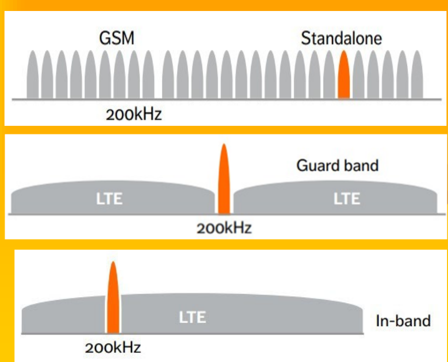


Tagain, the idea is to explore the LTE network, but with more scope in terms of frequencies.

81

NB-IoT – Spectrum & Access

Designed with a number of deployment options for licensed GSM, WCDMA or LTE spectrum to achieve efficiency



Stand-alone operation

Dedicated spectrum. Ex. by re-farming GSM channels

Guard-band operation

Based on the unused RB within a LTE carrier's guard-band

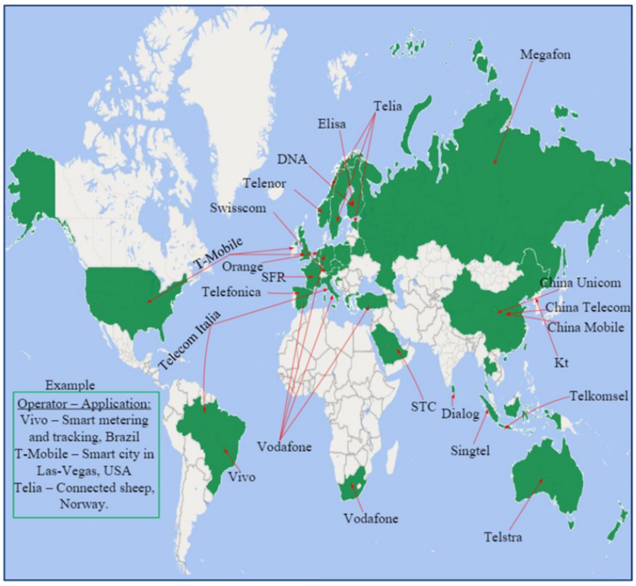
In-band operation

Using resource blocks within anormal LTE carrier

82

83

NB-IoT (@2019)



83

84

Cellular technologies

- **Two strategies, for different scenarios**
  - **No MIMO for lower end device energy.**

	LTE-M	NB-IoT
Peak data rate	384 kbps	<100 kbps
Latency	50-100 ms	1.5 – 10 seconds
Power consumption	Best at medium data rates	Best at very low data rates
Mobility	Yes	No, stationary only
Voice	Yes	No
Antennas	1	1

84

SigFox

- **Provide and maintain a PAID connectivity platform**
  - **Ultra Narrow Band: 100Hz per message**
  - **Ultra Low Bit rate: 12 byte messages, 140 messages per day (max!)**
  - **Long Range: ~50KM**
  - **Sensors lasting 10 years**
  - **Only provides connectivity, access control and a broker**
- **Business Model: connectivity service for alarms, smart meters, etc..**
- **As with the cellular technologies, SigFox sells a consumer service**

85

86

SigFox

- **Low Power Wide Area Sensor Network (LPWASN)**
- **Thousands of millions sensors ☺**
  - **A million sensors per access point ;)**
- **Proprietary ☹ comercial**
  - **You have to use its access infrastructure (built with operators) and software**
  - **Open market for the endpoints**
- **30-50km range in rural areas, and 3-10km range in urban**
  - **Ultra narrow band, 868 (EU) or 902 (US) frequency (MHz)**
  - **Low energy consumption**
- **Dedicated network deployed by SigFox across different countries**
  - **Often as subcontracting to local companies in the country.**

86

87

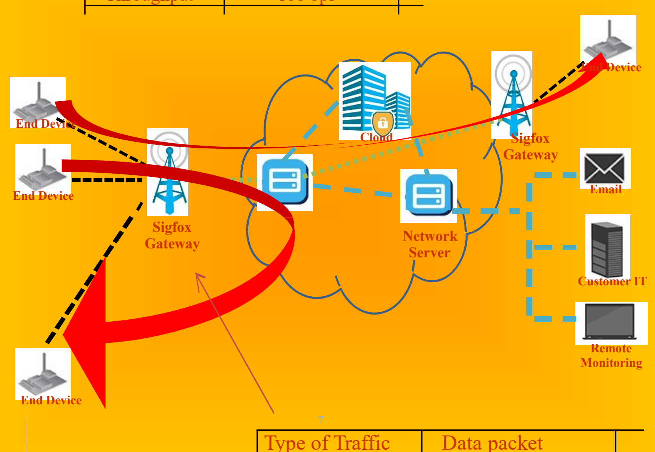
SigFox

- Strong duty cycle limitations
  - Common in the IoT
- Each device can send up to 140 messages per day
  - Payload: 12 octets (~96 bytes)
  - Datarate: up to 100bps
  - Duty cycle: the time occupied by the operation of a device, which operates intermittently
- Sigfox exploits this:
  - When a device has a message to be sent, the Sigfox interface wakes up, and the message is transmitted uplink
  - Then, the device listens for a short duration, if there is data to be sent to it
  - This is good for data acquisition scenarios, but not so good for command-and-control situations
- Use cases:
  - Businesses exploring smart meters, smoke detectors, security alarms

87

Sigfox - Architecture

Frequency Band	Ultra Narrow Band
Range	~ 13 Km
Throughput	~ 100 bps



Type of Traffic	Data packet
Payload	~ 12 Bytes
Security	No security
Time on air	Up to 6 seconds

88

89

LoRa

- Stands for "Long Range"
- Network to be used in long-lived battery-powered devices scenarios
- Semi-proprietary
  - Parts of the protocol are well documented, others not
  - Proprietary: the radio part (sub-licensing is possible)
  - Users can install their own separate gateways
- LoRa means two different (but related) things:
  - "LoRa": a physical layer that uses Chirp Spread Spectrum (CSS) modulation
  - "LoRaWAN": a MAC layer protocol

89

90

LoRa (the physical layer ☺)

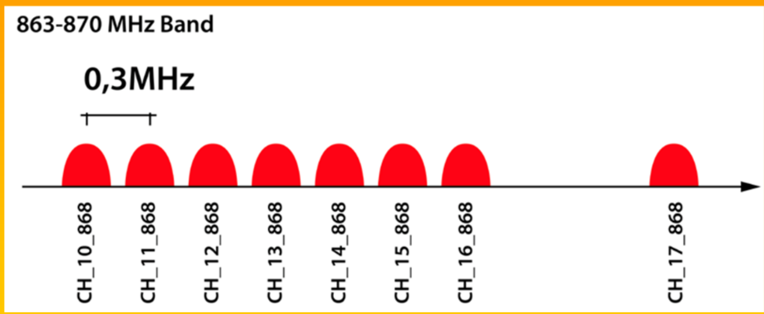
- Developed by Semtech
  - physical layer is proprietary
- Low-range, low-power and low-throughput
- Operates on 433-, 868- (EU) or 915 (US) MHz bands
- Payload from 2 to 255 octets (2Kb)
  - Depends on configuration parameters
- Datarate: up to 50Kbps

90

91

LoRa (the physical layer ☺)

- **In Europe, 8 channels with a bandwidth of 300KHz are used**



Source: Libelium

91

92

LoRa Physical Layer

- **Modulation**
  - **(changing a signal, the carrier, in a way that allows it to contain information to be transmitted)**
- **LoRa uses a proprietary Spread-Spectrum modulation technique: Chirp Spread Spectrum (CSS)**
  - (A chirp is a signal in which frequency raises or lowers with time)
  - **Tries to increase range by:**
    - Sending information with more power (within regulated values - <14dBm or 25mW)
    - Or by lowering the data rate
  - **Increases link budget**
  - **Increases immunity to in-band interference**
- **This, along with Forward Error Correction techniques, contribute to extend the range and robustness of radio communication links**
  - **Compared to FSK**

92

93

LoRa Physical Layer

- The Bandwidth (kHz), Spreading Factor and Coding Rate are design variables that allow a system to optimize the trade-off between
  - Occupied bandwidth
  - Data rate
  - Link budget
  - Interference immunity
- By using software, it is possible to combine these values to define a transmission mode

93

94

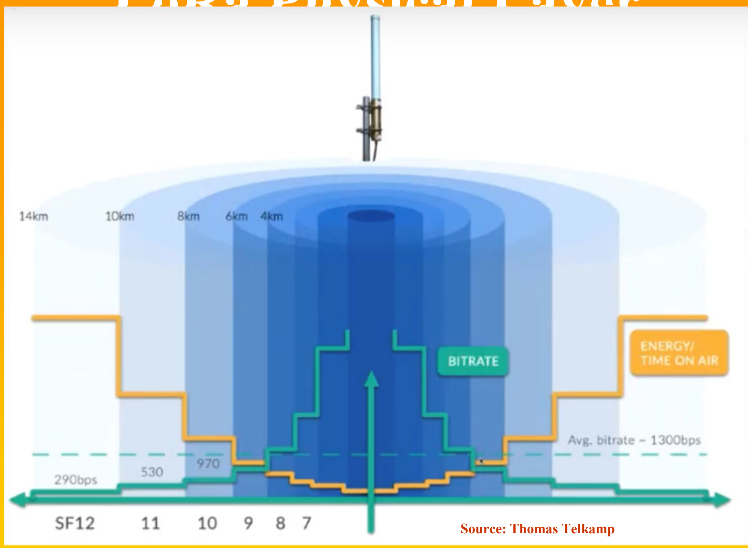
LoRa Physical Layer

Mode	BW	CR	SF	Sensitivity (dB)	Transmission time (ms) for a 100-byte packet sent	Transmission time (ms) for a 100-byte packet sent and ACK received	Comments
1	125	4/5	12	-134	4245	5781	max range, slow data rate
2	250	4/5	12	-131	2193	3287	-
3	125	4/5	10	-129	1208	2120	-
4	500	4/5	12	-128	1167	2040	-
5	250	4/5	10	-126	674	1457	-
6	500	4/5	11	-125,5	715	1499	-
7	250	4/5	9	-123	428	1145	-
8	500	4/5	9	-120	284	970	-
9	500	4/5	8	-117	220	890	-
10	500	4/5	7	-114	186	848	min range, fast data rate, minimum battery impact

94

95

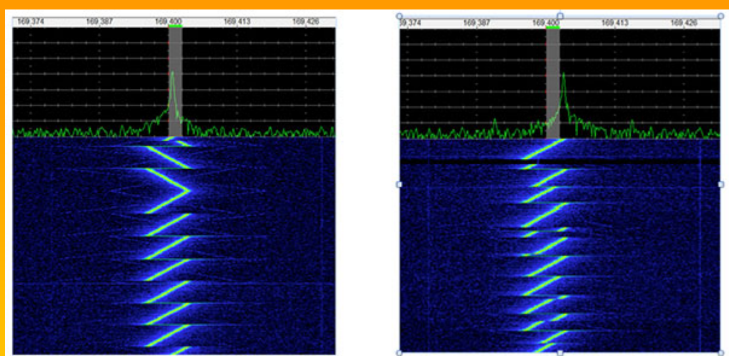
LoRa Physical Layer



95

96

LoRA Physical Layer



Bandwidth

Source: Link Labs

96

97

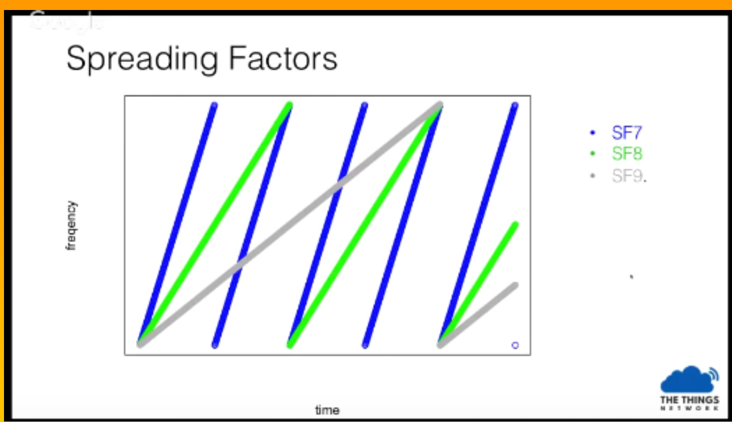
LoRa Physical Layer

- **Has different Spread Factors (SF7 to SF12)**
  - **Spread factors can set the modulation rate and tune the distance**
  - **They indicate how fast or slow is the chirp (how many chirps you get per second) → <u>how much data you can encode per second</u>**
    - The higher the SF, the lower the datarate
    - Each SF is 2x slower than the one before
    - <u>The slower you send your data, the farther you can send it</u>
    - <u>The higher the SF, the more energy is required (time on air)</u>
      - <u>The interface has more time to decode and sensititviy is increased</u>
- **This helps on scaling the network**
  - **Closer nodes receive data much faster**
  - **Air is ”cleared” for other nodes to transmit**
  - **By adding more gateways, devices get nearer to them, applying the above**

97

98

LoRa Physical Layer



Source: Thomas Telkamp

98

99

LoRa Physical Layer

- For a 125kHz bw (configurable by design)

Spreading Factor	Symbols/second	SNR limit	Time-on-air (10 byte packet) - ms	Bitrate - bps
7	976	-7.5	56	5469
8	488	-10	103	3125
9	244	-12.5	205	1758
10	122	-15	371	977
11	61	-17.5	741	537
12	30	-20	1483	293

99

100

LoRa Physical Layer

- Bandwidth
  - Show how wide is going to be the transmission signal
  - 3 options: 125 kHz, 250 kHz or 500 kHz
  - Greater reach: 125 kHz
  - Greater transmission speed: 500 kHz
  - Less bandwidth = more airtime = more sensitivity = more battery consumed

100

101

LoRa Physical Layer

- **Coding Rate**
  - **4 options: 4/5, 4/6, 4/7 and 4/8**
  - **Meaning:**
    - Every 4 useful bytes are going to be encoded by 5, 6, 7 or 8 transmission bits
  - **Smaller coding rate: 4/8**
  - **Lower coding rate = more airtime**

101

102

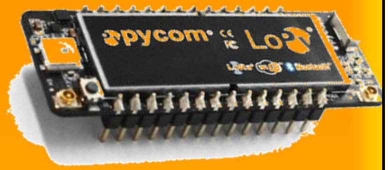
LoRa Physical Layer

- **Spreading Factor**
  - **Number of chips per symbol used in data treatment before the transmission signal**
  - **7 options: 6, 7, 8, 9, 10, 11 and 12**
  - **Greater Spreading Factor = Greater Range = more air time**

102

103

LoRa Physical Layer - Practical



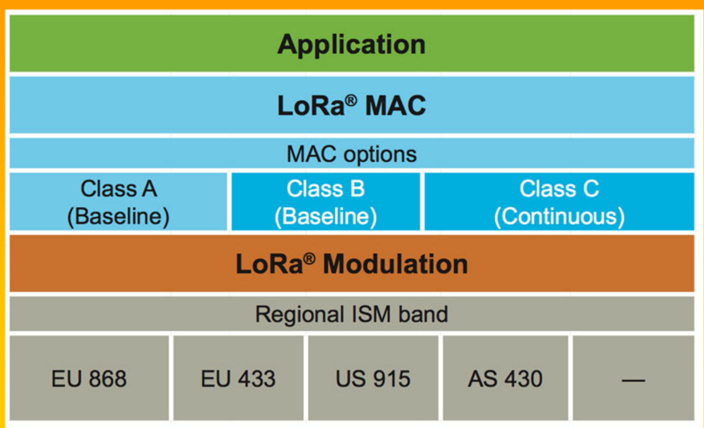
- **On the LoPy**
  - **Method**
    - lora.init(mode, * , frequency=868000000, tx_power=14, **bandwidth=LoRa.BW_125KHZ**, sf=7, preamble=8, **coding_rate=LoRa.CODING_4_5**, power_mode=LoRa.ALWAYS_ON, tx_iq=False, rx_iq=False, adr=False, public=True, tx_retries=1, device_class=LoRa.CLASS_A)
- **Bandwidth: LoRa.BW_125KHZ / LoRa.BW_250KHZ / LoRa.BW_500KHZ**
- **SF: sf=6 / sf=7 / sf=8 / sf=9 / sf=10 / sf=11 / sf=12**
- **Coding Rate: LoRa.CODING_4_5 / LoRa.CODING_4_6 / LoRa.CODING_4_7 / LoRa.CODING_4_8**

103

104

LoRa Stack

Different classes of devices



104

105

LoRaWAN

- MAC mechanism for controlling communications between end devices and LoRaWAN gateways. For all devices, it manages:
  - Communication frequencies
  - Data rate
  - Power
- Open Standard developed by the LoRa Alliance

105

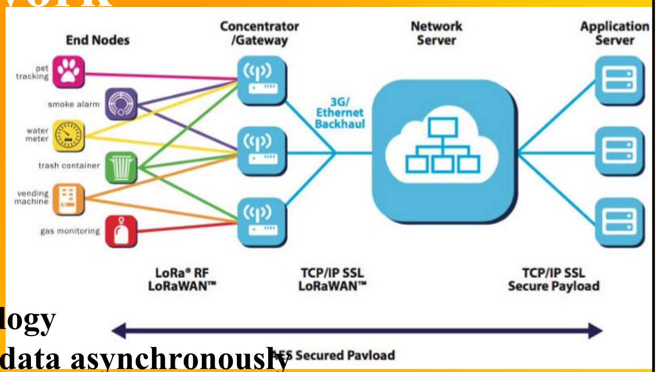
106

LoRaWAN

- Adaptive Data Rate
  - The network tells the node at which data rate it can send data
    - Manages the SF for each end-device
    - Explores the possibilities of the technology at the physical layer (as discussed before)
  - The aim is to:
    - Optimize for fastest data rate versus range
    - Maximize battery life
    - Maximize network capacity

106

LoRA Network



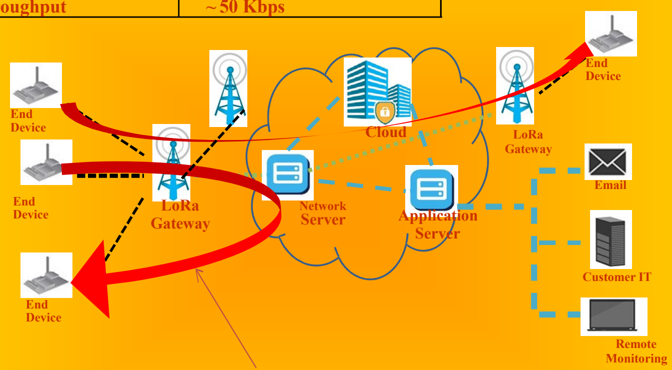
- **Star of stars topology**
- **Devices transmit data asynchronously**
  - **Data is received by multiple gateways**
  - **Each gateway forwards received data to a centralized network server, using a backhaul link (Ethernet or cellular)**
  - **The network server:**
    - Filters duplicate packets
      - Packet with the strongest signal gets decoded
    - Realizes security checks
    - Manages the network

Source: semtech.com

107

LORA - Architecture

Modulation	LoRa RF (Spread Spectrum)
Range	~ 15 Km
Throughput	~ 50 Kbps



Type of Traffic	Data packet
Payload	~ 243 Bytes
Security	AES Encryption

108

109

LoRaWAN

- **Typically, there is no node-to-node direct communication**
  - **LoRaWAN allows this by having 2 gateways and a network server in between the nodes**
- **However, most end-device vendors also include (for testing, mostly) a raw form of LoRa**
  - **Allows peer-to-peer communication between nodes**
  - **Contains only the link layer protocol**
  - **Only allows a very small number of nodes in a topology**
    - There is no packet management

  (useful for a first try with LoRa)

109

110

LoRaWAN

- **Components**
  - **End-Device**
    - Devices (low-power) that communicate with the LoRa Gateway
    - They are not associated to a particular gateway.
    - They are, however, associated to a Network Server.
  - **Gateway**
    - Intermediate devices that relay packets between end-devices and a network server.
    - Linked to the Network server via a higher bandwidth backhaul network.
    - They add information about the quality of reception, when forwarding a packet from an end-device to a network server.
    - They are transparent to the end-devices.
    - There are multiple gateways in a network
    - Multiple gateways can receive the same packet transmitted from the same end-device
  - **Network Server**
    - Decodes and de-duplicates packets sent from devices.
    - Generates packets to be sent towards devices
    - Choses the appropriate gateway to send packets to a specific end-device

110

111

LoRaWAN

- **End-Device Duty Cycle**
  - **Besides transmission frequency, duty cycle regulations apply**
  - **Delay between successive frames sent by a device**
  - **1% limitation for end-devices**
    - Device has to wait 100x the time it took for it to send the message, in order to be able to send again in the same channel
  - **Gateways: 10%**

111

LORA – Device Classes

Classes	Description	Intended Use	Consumption	Examples of Services
A (« all »)	Listens only after end device transmission	Modules with no latency constraint	The most economic communication Class energetically.. Supported by all modules. Adapted to battery powered modules	• Fire Detection • Earthquake Early Detection
B (« beacon »)	The module listens at a regularly adjustable frequency	Modules with latency constraints for the reception of messages of a few seconds	Consumption optimized. Adapted to battery powered modules	• Smart metering • Temperature rise
C (« continuous »)	Module always listening	Modules with a strong reception latency constraint (less than one second)	Adapted to modules on the grid or with no power constraints	• Fleet management • Real Time Traffic Management

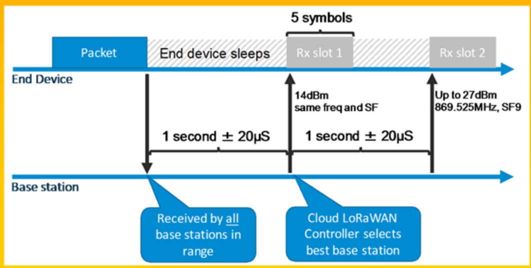
Any LoRa object can transmit and receive data

112

113

LoRaWAN

- **End-devices classes**
  - **Class A – bi-directional**
    - Lowest power consumption
    - Devices schedule uplink transmissions according to their requirements, with a small variation before transmission.
    - Each uplink transmission is followed by two short downlink receive windows
      - Downlink transmissions at any other time have to wait until the next uplink transmission
      - Less flexibility for downlink

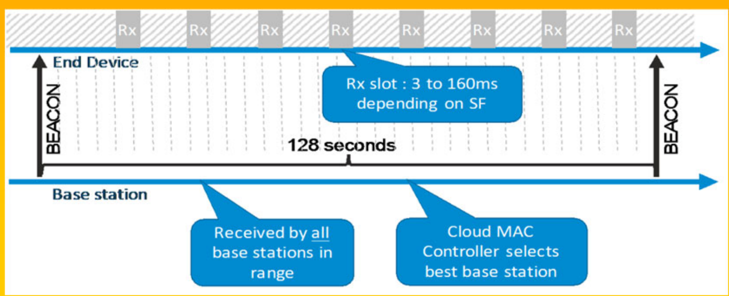


113

114

LoRaWAN

- **End-devices classes**
  - **Class B – bi-directional with scheduled receive slots**
    - Devices open more receive windows at scheduled times
    - There is a synchronized beacon from the gateway to the network server, indicating when the device is listening

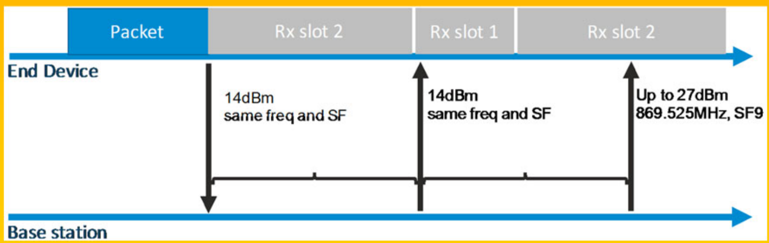


114

115

LoRaWAN

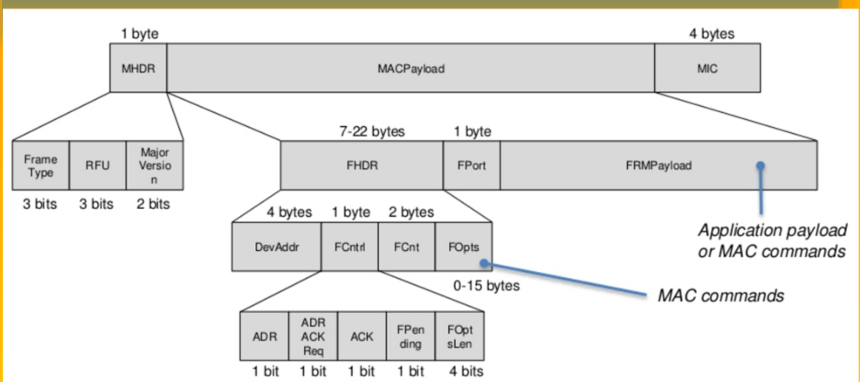
- **End-devices classes**
  - **Class C – bi-directional with maximal receive slots**
    - Greatest power consumption
    - Almost continuous receiving windows
      - Server can initiate transmission almost anytime



115

116

LoRaWAN - Payload



Source: Stephen Pharrell

116

117

LoRaWAN

- *DevAddr* - short address of the device.
- *FPort* - multiplexing port field.
- *FCnt* - frame counter.
- *MIC* - cryptographic message integrity code
- *MType* - message type (uplink, downlink, confirmed (requires an ACK, …).
- *Major* - LoRaWAN version
- *ADR* and *ADRAckReq* - data rate control adaptation mechanism by the network server.
- *ACK* - acknowledges the last received frame.
- *Fpending* - indicates that there is still data to be sent by the network server (end-device is required to send another message to open a receive window).
- *FOptsLen* - length of the *FOpts* field in bytes.
- *FOpts* - contains MAC commands on a data message.
- *CID* - MAC command ID.
- *Args* -optional arguments of the command.
- *FRMPayload* - payload, encrypted using AES with a key length of 128 bits.

The minimal size of the MAC header is 13 bytes; its maximal size is 28 bytes.

There is no destination address on uplink packets, or source address on downlink packets.

117

118

LoRaWAN

- MAC Commands
  - Allows the network to customize end-device parameters
- Checks
  - Link status (this can be send by the end-device itself)
  - Device battery
  - Device margin (SNR)
- Settings
  - Datarate
  - TX power
  - TX and RX channels
  - RX timing
  - Repetition
  - Duty cycle
  - Dwell time

118

119

LoRaWAN

- **End-Device Connection to a network**
  - **Also known as *Activation***
- **This process provides the end-device with:**
  - **End-device address (*DevAddr*): An identifier composed by the network identifier (7bit) and by the end-device's network address (25bit)**
  - **App identifier *(AppEUI):* Unique identification of the end-device owner**
  - **Network Session Key (*NwkSKey*): A key used by both the network server and end-device to verify and ensure message integrity**
  - **App Session Key (*AppSKey*): A key used by both the network server and end-device to encrypt the payload of received messages**
- **Note on security:**
  - **LoRaWAN protocol security is based on 802.15.4**
    - AES-128

119

120

LoRaWAN

- **To activate the device, there are two procedures:**
  - **Over-the-Air Activation (OTAA)**
    - *Join-Request* and *Join-Response* messages are exchanged in each new session, allowing the end-devices to obtain the network and application session keys
  - **Activation By Personalization (ABP)**
    - The devices have both keys already stored internally

120

The Things Network

- Built in a crowdsourced manner by companies and enthusiasts
  - Low density coverage, mostly in larger cities (3 GW in Aveiro)
  - 1-2Km range in cities, 10km in open space
- Provides a Free connectivity service, and broker with APIs
- Composed by:
  - Nodes: owned by companies and citizens, send data to Gateways
  - Gateways: owned by companies and citizens, interface with TTN
  - TTN Servers: Hosted by TTN, routing data to/from user apps

121

122

LoRaWAN vs NB-IoT

(ruilaa@det.ua.pt) - Uni. Aveiro

Table 5. NB-IoT vs. LoRaWAN average power consumption, latency, and throughput.

Features	NB-IoT	LoRaWAN
Joining network	3 mAh	1 mAh
Uplink message (44 bytes)	1.8 mAh	100 µAh
UE class	Cat NB1	A
Data rate (20 bytes)	0.6–4 bps	
Frequency	28 Mhz	EU868 MHz

122