IoT Access Networks

ΕΠΛ 428: IOT PROGRAMMING

Dr. Panayiotis Kolios
Assistant Professor, Dept. Computer Science,
KIOS CoE for Intelligent Systems and Networks
Office: FST 01, 116
Telephone: +357 22893450 / 22892695
Web: https://www.kios.ucy.ac.cy/pkolios/

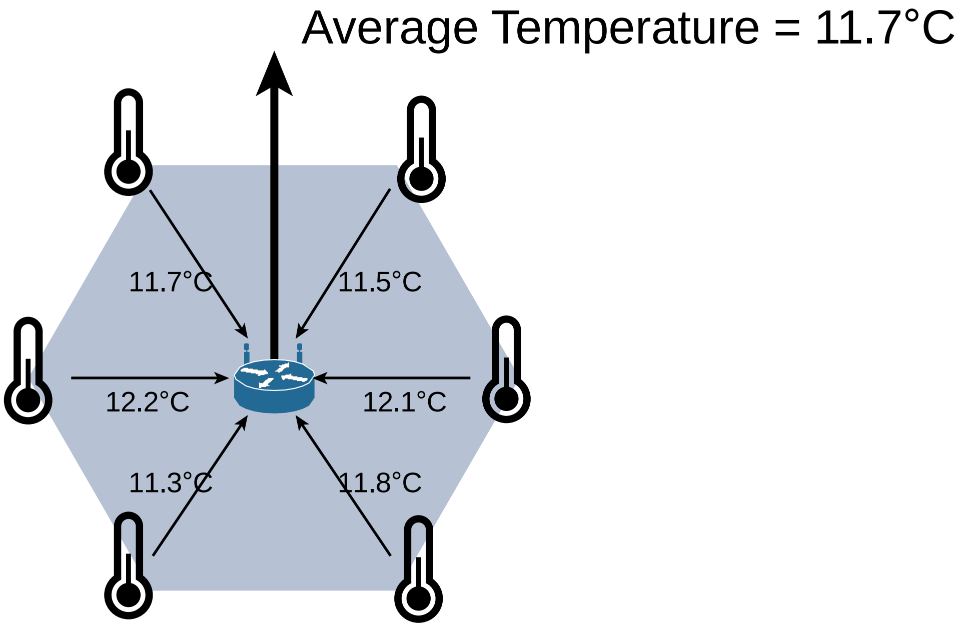
Πανεπιστήμιο Κύπρου

- Application requirements:
  - transmission range
  - data volume and frequency
  - sensor density and mobility
- Direct relationship between the network technology and the type of communication it can sustain
- Each technology is designed for certain use cases
  - Determined frequency band that was expected to be most suitable
  - The frame structure matching the expected data pattern (packet size and communication intervals)
  - Network topologies
- For IoT
  - May use existing technologies developed for other use cases
  - Employ new networking technologies

Πανεπιστήμιο Κύπρου

- Increasing the **throughput** and achievable **distance** typically comes with an increase in **power** consumption
- It may be tempting to simply choose the technology with the longest range and highest throughput. However, cost is a determining factor
- The amount of data to carry over a given time period along with correlated power consumption determines the wireless technology to be used

- Because many devices are low cost and correspondingly inaccurate, the ability to deploy smart objects redundantly allows for increased accuracy



- Data aggregation also results to reduced traffic over the network
  - Event-driven: Transmission triggered only at threshold/detection
  - Periodic: Transmission occurs at periodic intervals

Πανεπιστήμιο Κύπρου

COMMUNICATION CHARACTERISTICS

- **Range**: Power levels, signal propagation and distance
- **Frequency Bands**: licensed and unlicensed spectrum
- **Power Consumption**: Power source and use
- **Topology**: various layouts that may be supported for connecting multiple devices
- **Constrained Devices**: limitations of devices from a connectivity perspective
- **Constrained-Node Networks**: challenges that are often encountered with networks connecting IoT devices

COMMUNICATION RANGE

- Consider a transmitter node Tx and receiver Rx at a distance d apart
- Received power P_r (mW) decays proportionally to $^{1}/_{d^{n}}$ where n is the path loss exponent
- Free space propagation

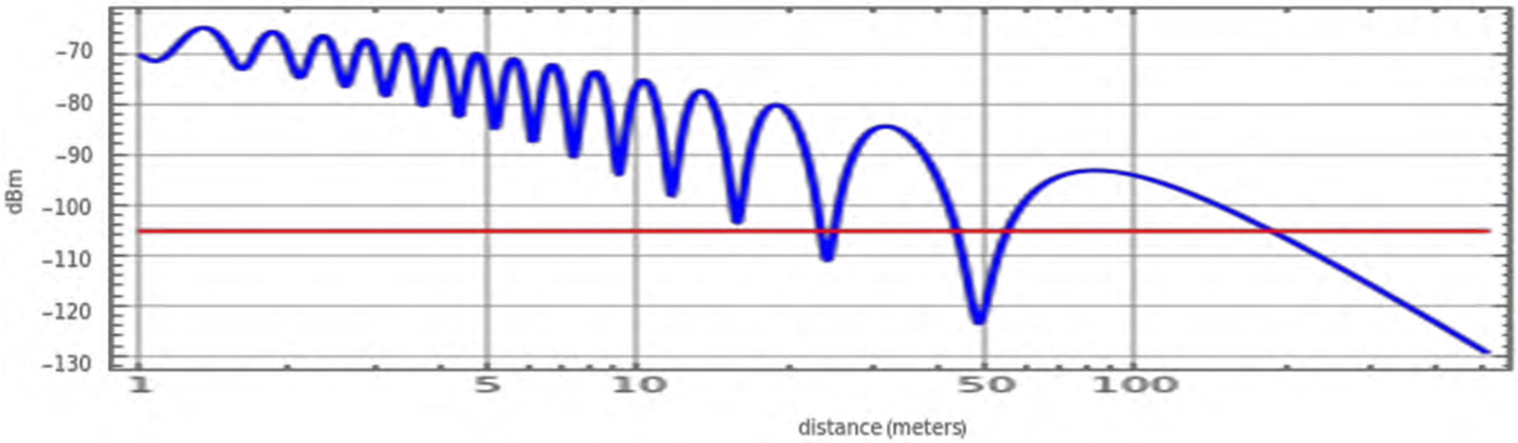
$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2$$

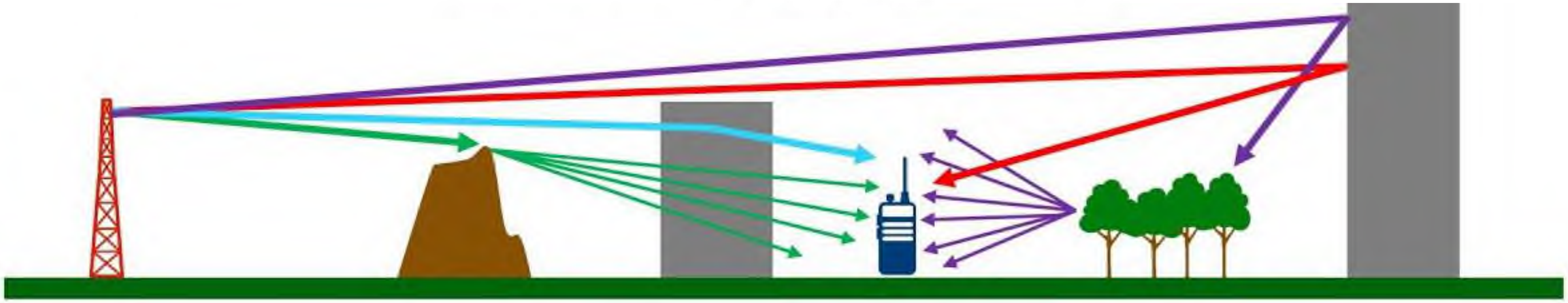
- where G_t and G_r are the transmitter and receiver antenna gains, respectively; P_t is the transmit power
- λ is the signal wavelength, $\lambda = c/f$ where $c = 3 \times 10^8\, m/s$ and f is the communication frequency
- term $\left(\frac{4\pi d}{\lambda}\right)^2$ is called the path loss L_P

Πανεπιστήμιο Κύπρου

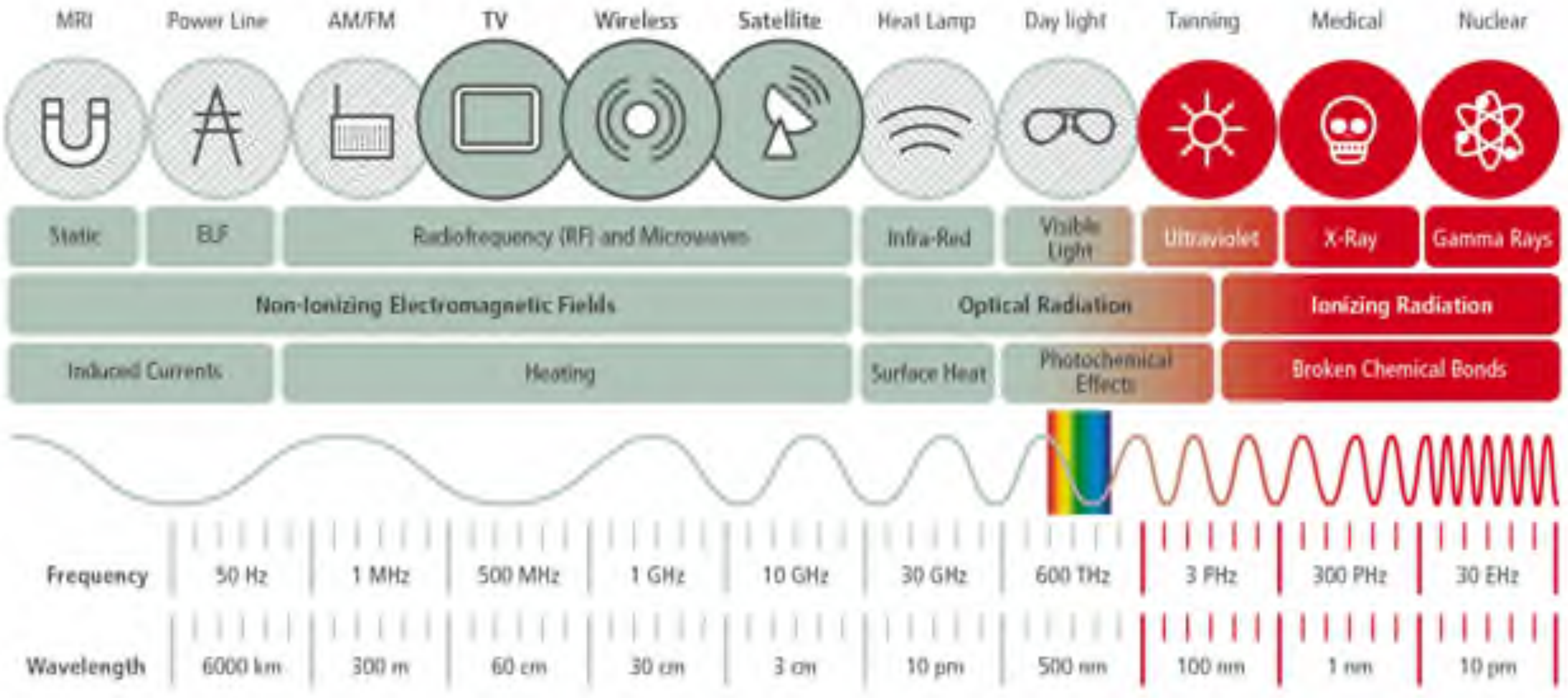
- In dB, the free space propagation expression becomes

$$\overbrace{P_r(dBm)}^{10\log_{10}P_r} = \overbrace{P_t(dBm)}^{10\log_{10}P_t} + \overbrace{G_t(dBm)}^{10\log_{10}G_t} + \overbrace{G_r(dBm)}^{10\log_{10}G_r} - \overbrace{L_p(dBm)}^{20\log_{10}\left(\frac{4\pi d}{\lambda}\right)}$$





FREQUENCY BANDS



Πανεπιστήμιο
Κύπρου

FREQUENCY BANDS

- Radio spectrum is regulated by countries and/or organizations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission (FCC)
- Define the regulations and transmission requirements for various frequency bands
- IoT access technologies use wireless communications in licensed and unlicensed bands
    - Licensed spectrum is generally applicable to long-range access technologies and allocated to infrastructures deployed by services providers, broadcasters, and utilities which guarantee QoS, e.g. NB-IoT
    - Unlicensed spectrum: industrial, scientific, and medical (ISM) portions of the radio bands. No guarantees or protections are offered (WiFi, Bluetooth, Zegbee)

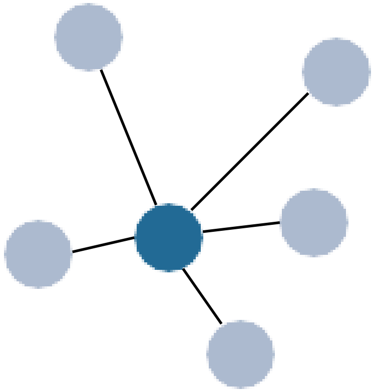
FREQUENCY BANDS

- Both license and unlicensed bands are regulated for:
  - Transmit power, duty cycle and dwell time, channel bandwidth, and channel hopping
- Unlicensed spectrum is simpler to deploy but can suffer from more interference because other devices may be competing for the same frequency in a specific area
- Tx frequency directly impacts range
  - Lower frequencies -> easier to penetrate obstacles or go around them
  - Lower frequencies -> lower data rate
- For example, in most European countries, the 169 MHz band is often considered best suited for wireless smart metering applications
  - good deep building basement penetration
  - the low data rate of this frequency matches the low volume of data that needs to be transmitted

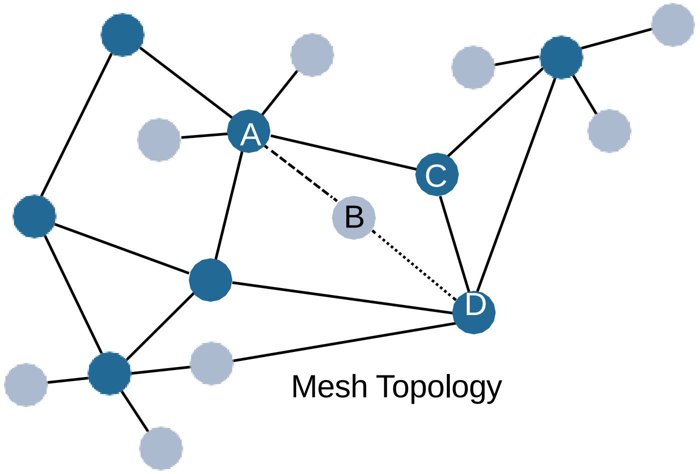
Power Consumption

- IoT needs low power connectivity for devices
- Led to the evolution of a new wireless environment known as Low-Power Wide-Area (LPWA)

- Some technologies offer flexible connectivity structures to extend communication possibilities
- **Point-to-point topologies**: These topologies allow one node to communicate with another node
- **Point-to-multipoint topologies**: These topologies allow one node to communicate with more than one other node
    - Several subtypes
        - Support both data collection and forwarding functions
        - Support also control actions (e.g. coordinator, gateways) to perform specific operations, and also interface with other networks or possibly other gateways



Star Topology



Mesh Topology

- **Start topology**: Coordinator collects data from other devices and performs control functions
- **Mesh topology**: a node can have more than one path to another node, can communicate with more than just one other node.
  - This communication can be used to directly exchange information between nodes or to extend the range of the communication link. In this case, an intermediate node acts as a relay
  - Another property of mesh networks is redundancy. The disappearance of one node does not necessarily interrupt network communications. Data may still be relayed through other nodes to reach the intended destination.

Πανεπιστήμιο
Κύπρου

CONSTRAINED DEVICES

- Heterogeneous devices in terms of computing, memory, storage, power, and networking
- Differentiating constrained IoT devices from servers, desktops or laptops, and smartphones is important for performance
- Constrained-node networks
  - low-power and lossy networks
  - network nodes must cope with the requirements from powered and battery- powered constrained nodes.

DATA RATE AND THROUGHPUT

- IoT data rates range from 100 bps (LORA) to Mbps (5G, WiFi)
- Shannon Capacity (theoretical maximum):

$$C = B\log_2(1 + SNR)$$

- where B is the channel bandwidth and SNR (signal to noise ratio) is the ratio of signal to noise power at the receiver
- Consider only thermal noise:

$$N = kTB$$

- where Boltzmann's constant k= 1.3803 × 10-23 J/K and temperature T (Kelvins) (Celsius + 273.15)

DATA RATE

	Example 1	Example 2	Example 3
Frequency	900MHz	2.4GHz	5GHz
Bandwidth	5MHz	10MHz	20MHz
Distance (m)	2000	500	300
Pathloss exponent	2	3.5	3.5
Thermal noise temperature	40°C	25°C	25°C
Atmospheric Attenuation (dB)	5		
Tx power (W)	0.2	0.15	0.15
Tx antenna Gain (dBi)	24	30	12
Rx power (dBm)			
Rx antenna Gain (dBi)	12	12	12
Other Losses (dB)	10	10	10
SNR (dB)			
Data Rate (bps)			

- Actual throughput, or “goodput,” is much lower
- Due to overheads of all the protocol layer data units (PDUs)
- TCP/IP assumptions
  - IPv4: minimum **20Bytes** overhead (without IP options)
  - TCP: minimum **20Bytes** overhead (without options)
- Data Link Layer assumptions
  - Maximum Transmission Unit (MTU) **1500 Bytes**
  - LLC overhead **26 Bytes**
  - On Ethernet additional **12 Bytes** for Interframe/Interpacket Gap
- Calculations:
  - 1GB file download
  - MTU – $\text{TCP}_{\text{overhead}}$ - $\text{IPv4}_{\text{overhead}}$ = **1460Bytes**
  - 1GB / 1460 = 684932 MTUs
  - **53MB** = 684932 * 78Bytes (overhead of TCP/IP + Datalink + Physical)
  - Total overhead **5.3%**

Πανεπιστήμιο Κύπρου

IoT ACCESS TECHNOLOGIES

- IoT access technologies:
  - **Standardization and alliances**: Technical bodies that maintain the protocols for a technology
  - **Physical layer**: The wired or wireless methods and relevant frequencies
  - **MAC layer**: Considerations at the Media Access Control (MAC) layer, which bridges the physical layer with data link control
  - **Topology**: The topologies supported by the technology
  - **Security**: Security aspects of the technology

IEEE 802.15.4

Πανεπιστήμιο Κύπρου

IEEE 802.15.4

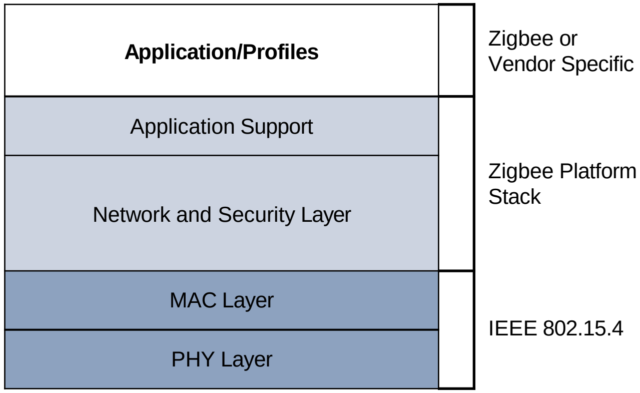
- WPAN wireless technology for low-cost and low-data-rate devices (defines PHY and MAC layer protocols)
- Common applications:
  - Home and building automation
  - Automotive networks
  - Industrial wireless sensor networks
  - Interactive toys and remote controls
- Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithm implemented
  - a device “listens” to check channel availability
  - If another device is transmitting, a wait time (which is usually random) occurs before “listening” again
- Frequency-hopping technique used in newer amendments to combat Interference and multipath fading

IEEE 802.15.4 PROTOCOLS

Protocol	Description
ZigBee	Defines upper-layer components (network through application) as well as application profiles. ZigBee also defines device object functions, such as device role, device discovery, network join, and security.
6LoWPAN	An IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers including header compression.
WirelessHART	A protocol stack that offers a time-synchronized, self-organizing, and self-healing mesh architecture, leveraging IEEE 802.15.4-2006 over the 2.4 GHz frequency band
Thread	Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home

ZigBee

- ZigBee specifies the network and security layer and application support layer that sit on top of the lower layers



Application/Profiles

Application Support

Network and Security Layer

MAC Layer

PHY Layer

Zigbee or Vendor Specific

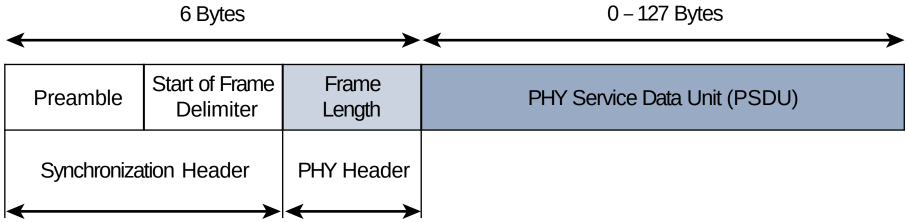
Zigbee Platform Stack

IEEE 802.15.4

- The ZigBee network and security layer provides mechanisms for:
    - Network startup, configuration, routing
    - Calculates routing paths in what is often a changing topology, discovering neighbours, and managing the routing tables as devices join for the first time
    - Security using Advanced Encryption Standard (AES) with a 128-bit key and also provides security at the network and application layers

IEEE 802.15.4 PHY LAYER

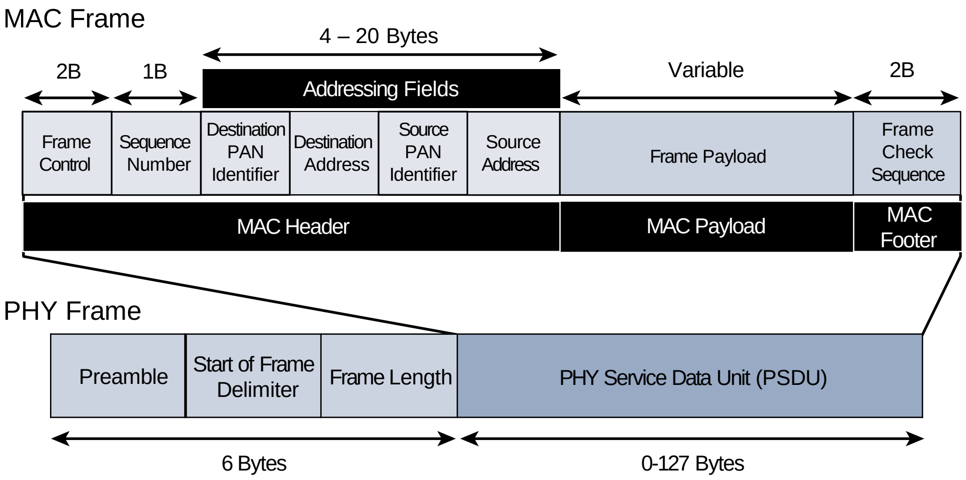
- Frequency band 2.4 GHz to sub-GHz frequencies in ISM bands
- Direct sequence spread spectrum (DSSS); a modulation technique in which a signal is intentionally spread in the frequency domain:
  - 2.4 GHz, 16 channels, with a data rate of 250 kbps
  - 915 MHz, 10 channels, with a data rate of 40 kbps
  - 868 MHz, 1 channel, with a data rate of 20 kbps



IEEE 802.15.4 MAC LAYER

- IEEE 802.15.4 MAC layer manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated
- At this layer, the scheduling and routing of data frames are also coordinated. The 802.15.4 MAC layer performs the following tasks:
  - Network beaconing for devices acting as coordinators
  - PAN association and disassociation by a device
  - Device security
  - Reliable link communications between two peer MAC entities
- Achieves these tasks by using predefined frame types
- Four types of MAC frames are specified:
  - **Data**: Handles all transfers of data
  - **Beacon**: Transmission of beacons from a PAN coordinator
  - **Acknowledgement** : Confirms successful reception of a frame
  - **MAC command**: Responsible for control communication

IEEE 802.15.4 MAC LAYER



MAC Frame

2B

1B

4 – 20 Bytes

Addressing Fields

Variable

2B

Frame Control

Sequence Number

Destination PAN Identifier

Destination Address

Source PAN Identifier

Source Address

Frame Payload

Frame Check Sequence

MAC Header

MAC Payload

MAC Footer

PHY Frame

Preamble

Start of Frame Delimiter

Frame Length

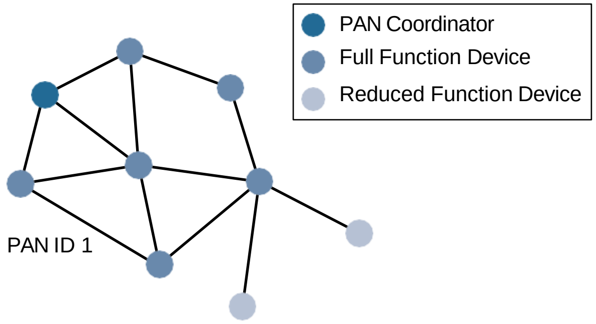
PHY Service Data Unit (PSDU)

6 Bytes

0-127 Bytes

102.15.4 TOPOLOGIES

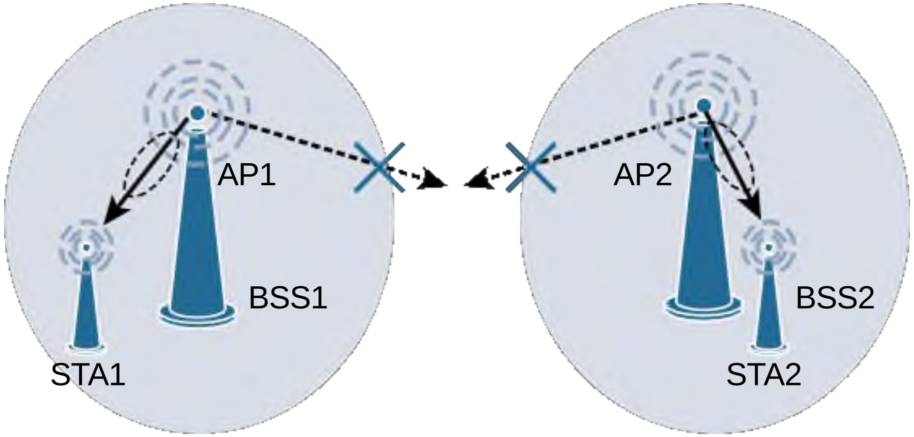
- Set up a star, peer-to-peer, or mesh topology
- Mesh networks extend connectivity. This allows nodes that would be out of range to leverage intermediary nodes to transfer communications
- Every 802.15.4 PAN should be set up with a unique ID
- All the nodes in the same 802.15.4 network should use the same PAN ID



- A minimum of one FFD acting as a PAN coordinator is required to deliver services that allow other devices to associate and form a cell or PAN

WIFI

- Key wireless access technology, for connecting:
  - endpoints such as fog computing nodes
  - high-data-rate devices
  - deploying Wi-Fi backhaul infrastructures
- WIFI originally Short range & Power hungry
- IEEE 802.11ah specified for IoT for sub-GHz long-range Wi-Fi
- Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithm implemented



IEEE 802.11 PHY

- In addition to unlicensed bands 2.4 & 5GHz, IEEE 802.11ah provides sub-GHz band operation at for example 868–868.6 MHz
- OFDM (orthogonal frequency division multiplexing) modulation. modulation scheme in which bits are carried by subsets of subcarrier frequencies
- Uses channels of 1, 2, 4, 8, or 16 MHz
- While the new IEEE 802.11ac achieves 1Gbps @ 5 GHz, 802.11ah provide an extended range, 100 kbps ~1km

IEEE 802.11 MAC

- MAC layer optimized to support
  - sub-GHz Wi-Fi
  - low power operation
  - a larger number of devices (8192 per AP)
- **MAC header**: Has been shortened to allow more efficient communication.
- **Null data packet (NDP) support**: Is extended to cover several control and management frames. Relevant information is concentrated in the PHY header and the additional overhead associated with decoding the MAC header and data payload is avoided. This change makes the control frame exchanges efficient and less power-consuming for the receiving stations
- **Grouping and sectorization**: Enables an AP to use sector antennas and also group stations (distributing a group ID) to reduce contention in large cells

- **Restricted access window (RAW)**: Is a control algorithm that avoids simultaneous transmissions when many devices are present and provides fair access
- **Target wake time (TWT)**: Access point schedules access to the network. Devices enter low-power state until their TWT time arrives.
- **Speed frame exchange**: Enables an AP and endpoint to exchange frames during a reserved transmit opportunity (TXOP).

IEEE 802.11 TOPOLOGY

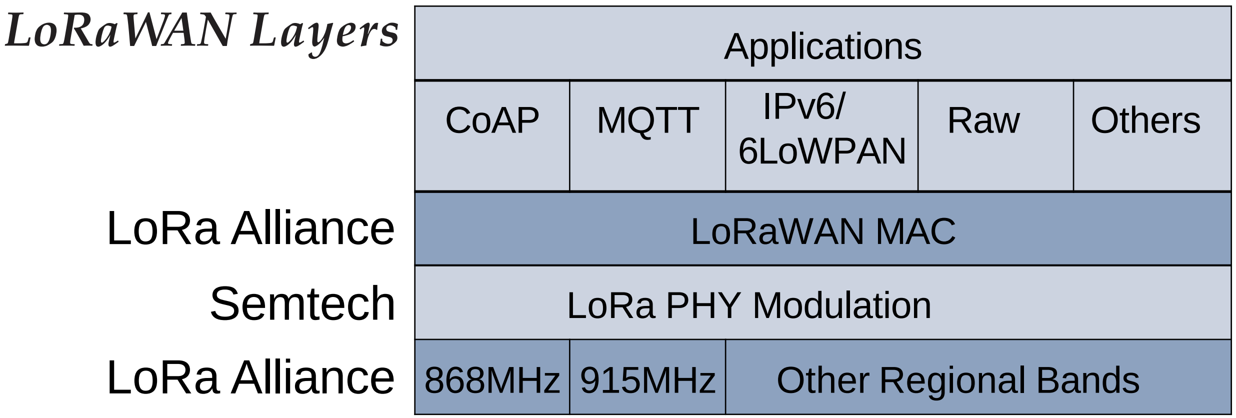
- Primarily a **star topology** but supports relay operation to extend its range. Devices can relay packets for other devices (2-hop or more)
- **Relays** can also employ higher modulation and coding scheme (MCS) achieving higher data rate. Higher MCS is reduced with increasing distance from the AP
- **Sectorization** is a technique that involves partitioning the coverage area into several sectors (using antenna arrays and beamforming) to get reduced contention

LORA/LORAWAN

Πανεπιστήμιο Κύπρου

LORA

- Low-Power Wide-Area (LPWA) technology
- Adapted for long-range and battery-powered endpoints
- Unlicensed-band LPWA technology
- Semtech defined **LoRa** = PHY modulation technology
- LoRa Alliance defined **LoRaWAN** = end-to-end architecture



LoRaWAN Layers

Applications

CoAP | MQTT | IPv6/ 6LoWPAN | Raw | Others

LoRa Alliance — LoRaWAN MAC

Semtech — LoRa PHY Modulation

LoRa Alliance — 868MHz | 915MHz | Other Regional Bands

LORA PHY

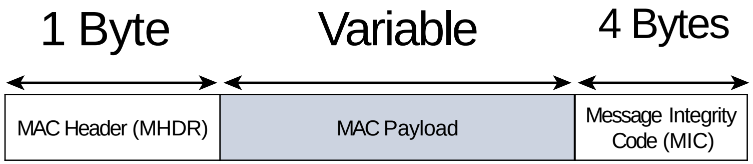
- Modulation based on chirp spread spectrum modulation,
  - Lower data rate but robustness to noise and interference
  - Higher receiver sensitivity to significantly increase the communication distance
  - Single channel occupation by different spreading factors enabling receive on multiple channels in parallel
- Use of unlicensed sub-GHz frequency bands
  - 433 MHz
  - 779–787 MHz
  - 863–870 MHz
  - 902–928 MHz

LORA PHY

- LoRa gateways operates per cell of a star topology
    - Uses multiple transceivers and channels and can demodulate multiple channels at once or even demodulate multiple signals on the same channel simultaneously
    - LoRa gateways can relay data between endpoints, and devices can communicate with one or many gateways simultaneously
- Data rate varies depending on the frequency bands and adaptive data rate (ADR)
- ADR is an algorithm that manages the data rate and radio signal
- The ADR algorithm ensures that packets are delivered at the best data rate possible and that network performance is both optimal and scalable
- Devices closer to the gateways with good signal transmit with higher data rates, which enables a shorter transmission time over the wireless network, and the lowest transmit power

LORAWAN MAC

- LoRaWAN defines three classes of devices:
  - **Class A**: default, optimized for battery-powered nodes, allows bidirectional communications & 2 receive windows after each transmission
  - **Class B**: get additional receive windows compared to Class A, but gateways must be synchronized through a beaconing process
  - **Class C**: adapted for powered nodes, enables a node to be continuously listening by keeping its receive window open when not transmitting
- LoRaWAN messages, have a PHY payload composed of a 1-byte MAC header, a variable-byte MAC payload, and a MIC that is 4 bytes in length
- MAC payload size depends on the frequency band and the data rate, e.g. 59-230 bytes @ 863–870 MHz

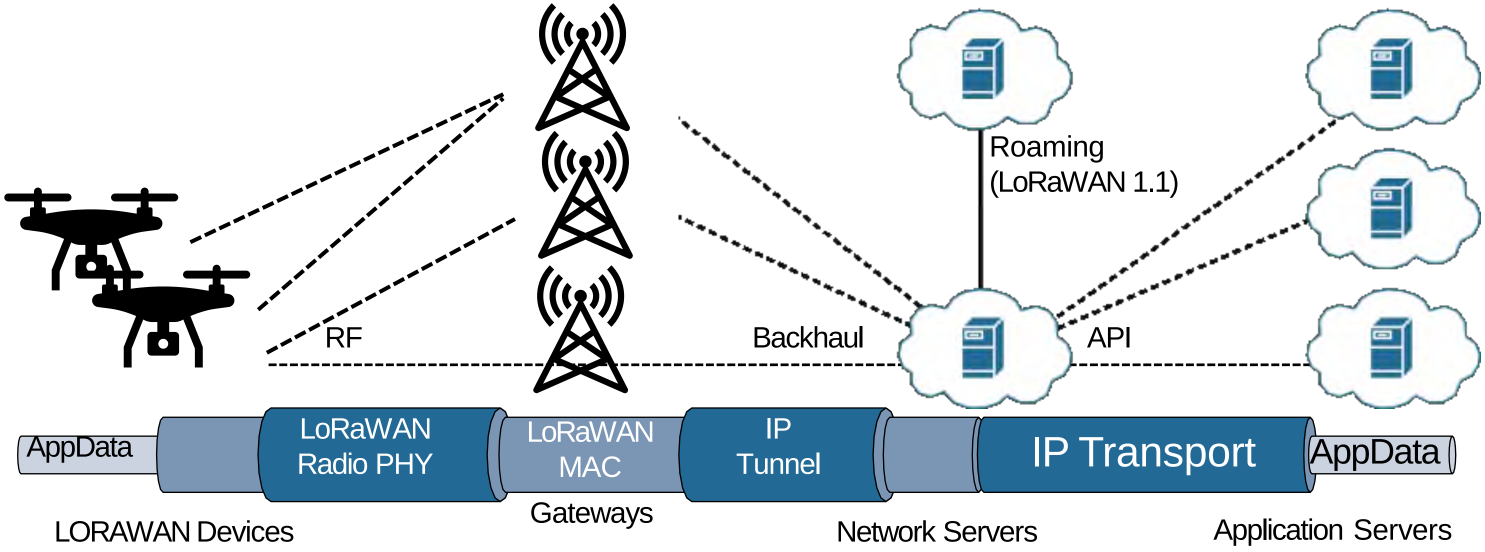


LORAWAN MAC

- LoRaWAN utilizes six MAC message types
  - join request and join accept messages for over-the-air (OTA) activation and joining the network
  - Confirmed data up/down must be acknowledged
  - Unconfirmed data up/down without acknowledgment
- Uplink messages are sent from endpoints to the network server and are relayed by one or more LoRaWAN gateways
- Downlink messages flow from the network server to a device though a single gateway
- LoRaWAN devices uniquely addressable through a DevEUI using IEEE EUI-64

LORAWAN TOPOLOGY

- Infrastructure consists of devices exchanging packets through gateways acting as bridges, and a central LoRaWAN network server
- Gateways connect to the backend network using standard IP connections, and devices communicate directly with one or more gateways



Πανεπιστήμιο Κύπρου

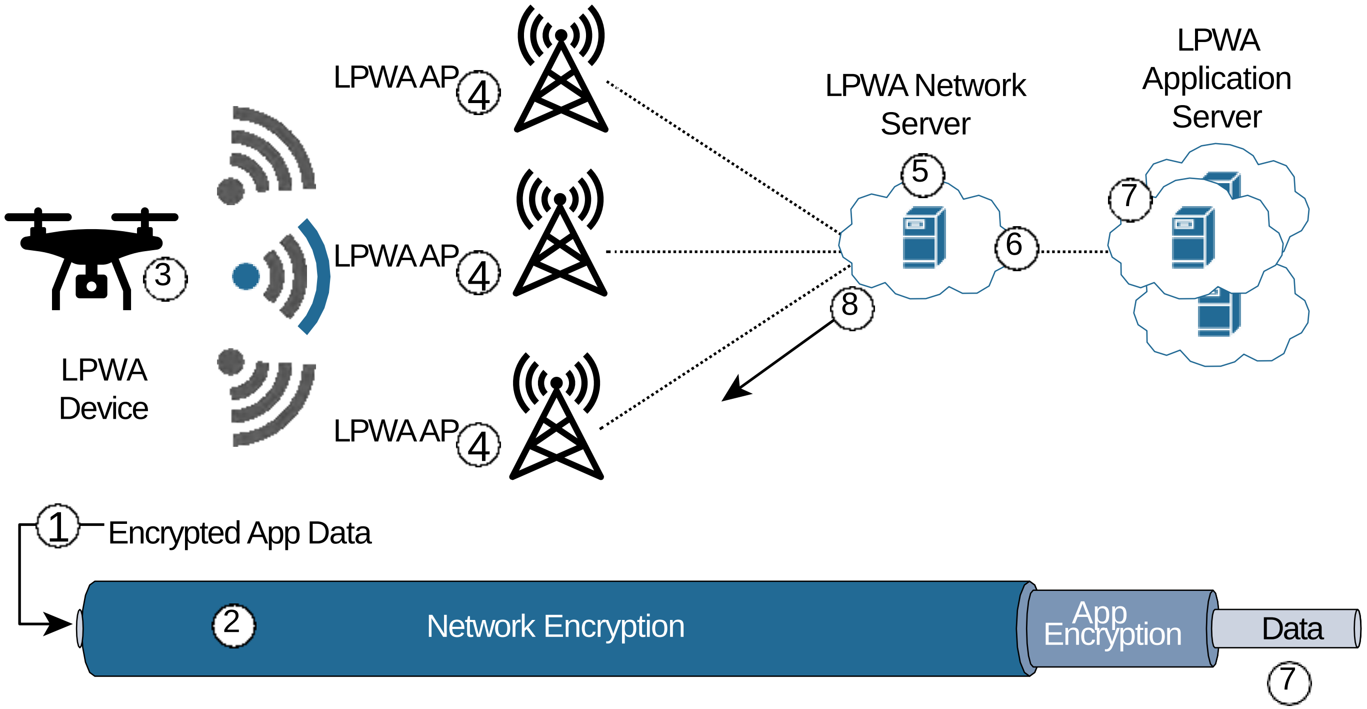
LORAWAN SECURITY

- Devices implement two layers of security

1. “network security” but applied at the MAC layer, guarantees the authentication of devices by the LoRaWAN network server. Also, it protects LoRaWAN packets by performing encryption based on AES
   - network session key (NwkSKey), used for data integrity through computing and checking the MIC of every data message as well as encrypting and decrypting MAC-only data message payloads
2. Application session key (AppSKey), which performs encryption and decryption functions between devices and application servers
   - Computes and checks the application-level MIC, if included.
   - AES-128 application key (AppKey) from the application owner

- Also LoRaWAN gateways can be protected using traditional VPN and IPSec technologies

LORAWAN SECURITY



1. Device encrypts data end-to-end
2. Separate network encrypt to NS
3. Device sends a packet
4. All APs in range receive packet
5. NS decrypts using network key
6. NS forwards packet to relevant NS
7. AS decrypts using app key
8. NS selects best AP for return TX

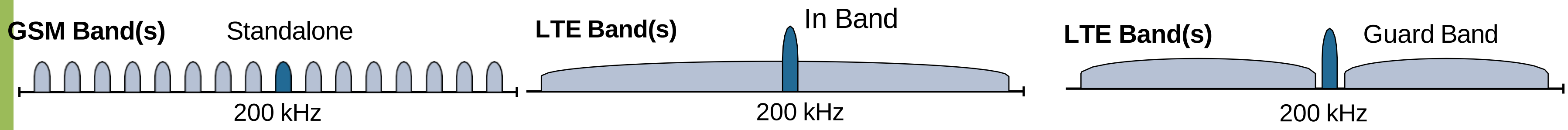
Πανεπιστήμιο Κύπρου

NB-IOT

Πανεπιστήμιο
Κύπρου

NARROWBAND IoT

- 3GPP (cellular alliance) develop NB-IoT to better address IoT requirements
  - low power consumption
  - large number
  - improved indoor coverage
  - optimized network architecture
- Three modes of operation
  - **Standalone**: Resuce of GSM carriers 900 MHz or 1800 MHz
  - **In-band**: Part of an LTE carrier frequency band allocated for NB-IoT
  - **Guard band**: NB-IoT carrier allocated between LTE or WCDMA bands



NARROWBAND IoT

- OFDMA access enabling multiple users to transmit low speed data simultaneously
- While traditional cellular networks define resource blocks with an effective bandwidth of 180 kHz
- NB-IoT, tone or subcarriers replace LTE resource blocks
  - The uplink channel can be 15 kHz or 3.75 kHz or multi-tone (n*15 kHz, n up to 12)
  - Layer 1, the maximum transport block size (TBS) for downlink is 680 bits, while uplink is 1000 bits.
  - Layer 2, the maximum Packet Data Convergence Protocol (PDCP) service data unit (SDU) size is 1600 bytes.
- NB-IoT operates in half-duplex frequency-division duplexing (FDD) mode with a maximum data rate uplink of 60 kbps and downlink of 30 kbps

Πανεπιστήμιο
Κύπρου