The landscape of IoT protocols

practitioner's view

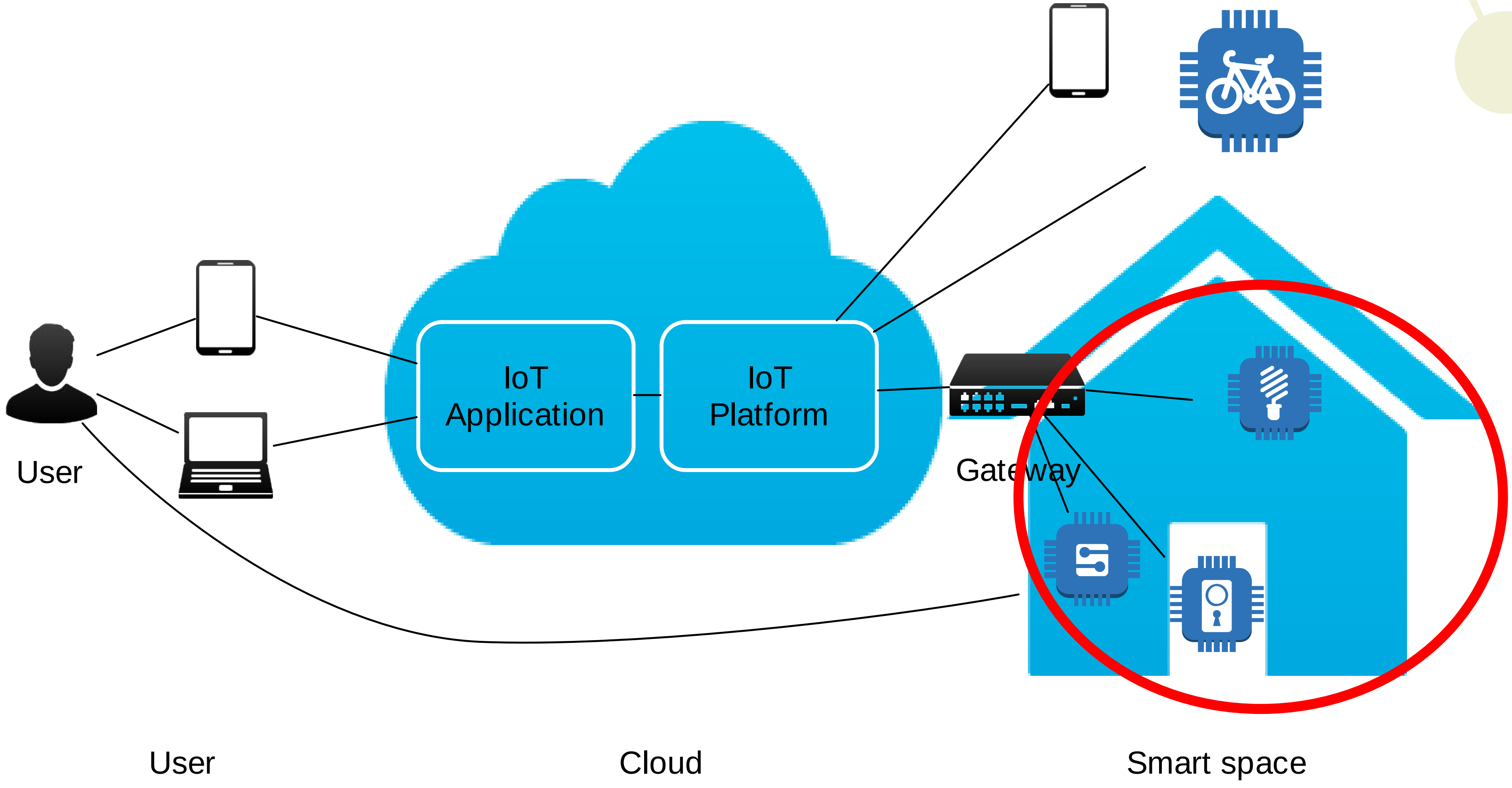
prof. Mario Kusek, University of Zagreb, FER

Grant agreement ID: 101079214

Outline

- Architecture of IoT system
- Protocol stack
- Essential properties of the physical layer and data link in IoT
- Standards
- Mid range: IEEE 802.15.4, ZigBee, Z-Wave, IEEE 802.11ah
- Long range: Sigfox, LoRa and LoRaWAN, LTE-M, NB-IoT

Architecture of IoT system



IoT protocol stack

TCP/IP

Application
Transport
Network
Dana link
Physical

IoT

COAP, MQTT
TCP/UDP
IPv4/IPv6
IEEE 802.15.4 Wi-Fi, WLAN NB-IoT,LTE-M

Network access
Device communication
M2M

Sensors/devices

Device communication

- Requirements
  - the greater the range
  - long-term battery life (low consumption, sleep mode)
  - low cost of the device
  - easy introduction into the system
  - support for mass application
  - small communication delay

Range

- Short range
  - IEEE 802.15.1 Bluetooth
    - BAN – body area network
    - certified to be used in contact with the body
  - IEEE 802.15.7 Visible Light Communications (VLC) – FSO (free space optics)
    - not used much in practice
- Mid range
  - wireless: IEEE 802.11 Wi-Fi, IEEE 802.15.4, 802.15.4g/e, ZigBee, IEEE 802.11ah (on the frontier of the long range), Z-wave, …
  - wired: IEEE 802.3 Ethernet, IEEE 1901.2 Narrowband Power Line Communications (PLC)
- Long range
  - mobile network: 2G – 5G (NB-IoT)
  - LPWA (Low-Power Wide-Area): LoRaWAN, Sigfox
  - wired: IEEE 802.3xx optics (*fiber*), broadband (xDSL), IEEE 1901-2010 - Broadband over PLC

Frequency spectrum (1)

- Unlicensed spectrum (ISM – industrial, scientific and medical):
    - 2.4 GHz used by:
        - IEEE 802.11b/g/n Wi-Fi
        - IEEE 802.15.1 Bluetooth
        - IEEE 802.15.4 WPAN
  - Advantages:
    - easier setup (no licenses required)
    - higher capacity (bit rate)
  - Disadvantages:
    - interference (a lot of devices on these frequencies)
    - closed space (walls, iron, ...) reduces the range
    - higher energy consumption

Frequency spectrum (2)

- Common frequencies below 1GHz for IoT applications:
    - 169 MHz – for meters (electricity, water, gas, ...)
        - usually required licence
    - 433 MHz, 868 MHz (EU), 915 MHz (USA)
        - it can usually be used for various applications: IEEE 802.15.4, IEEE 802.11ah, LoRaWAN, Sigfox, ...
    - 779–787 MHz only in China
        - za IEEE 802.15.4g i LoRaWAN
- Advantages:
    - greater range
    - lower energy consumption
    - through walls communication
- Disadvantages:
    - lower capacity
    - for some frequencies licence is needed

Energy consumption

- Requirements different for different battery-powered devices:
  - 10-15 years for meters (water and gas)
  - 5-7 years for smart parking sensors
  - 2-3 years for devices that can be regularly maintained (e.g. ENC - Electronic toll collection)

- How to achieve this?
  - some parts of the device are switched off during operation
    - devices "sleep" (do not consume energy or consume very little)
  - wireless communications that consume much less energy
  - optimized components that consume little energy

Power consumption - classification (1)

- RFC7228 https://tools.ietf.org/html/rfc7228
- **Classes of Energy Limitation**

Name	Type of energy limitation	Example Power Source
E0	Event energy-limited	Event-based harvesting (e.g. moving)
E1	Period energy-limited	Battery that is periodically recharged or replaced (e.g. solar)
E2	Lifetime energy-limited	Non-replaceable primary battery (e.g. ENC)
E3	No direct quantitative limitations to available energy	Mains-powered

Power consumption - classification (2)

- RFC7228 https://tools.ietf.org/html/rfc7228
- **Strategies of Using Power for Communication**

Name	Strategy	Ability to communicate
P0	Normally-off	Reconnect as needed. The main optimization is to reduce the reconnection energy.
P1	Low-power	Appears connected. Periodically plugged into the network. Period adjustment required.
P9	Always-on	Always connected. Optimization of circuitry (reduction of frequency or shutdown of individual parts)

Topology

- different technologies can have different topologies
- basic types:
  - star
  - peer-to-peer
  - tree
  - mesh

- examples:
  - WiFi – star around AP (*access point*)
  - IEEE 802.15.4, IEEE 1901.2a PLC – mesh
    - some nodes must relay messages

Mid range protocols

IEEE 802.15.4

- A standard that specifies wireless data transfer technologies for devices and networks of limited capabilities with a focus on low power consumption
  - low-rate wireless personal area networks (LR-WPANs)
  - PHY & Medium Access Control (MAC)
- Frequency range
  - 868.0-868.6 MHz (EU), 902-928 MHz (USA), 2.4-2.485 GHz (world)
- Max speed: 250 kbps
- Max power: ~1mW-100mW
- Frame: 127 bytes

IEEE 802.15.4 - standards

- The first standard 2003 (IEEE 802.15.4-2003), 2006, 2011, 2015
  - Frequencies and speed:
    - 2,4GHz, 16 channels, 250kb/s – the whole world
    - 915MHz, 10 channels, 40kb/s – North and South America
    - 868 MHz, 1 channel, 20kb/s – Europe, Middle East, Africa

- Other standards:
  - IEEE 802.15.4c-2009 – frequencies for China (314-316 MHz, 430-434 MHz, 779-787 MHz)
  - IEEE 802.15.4d-2009 – frequencies for Japan (950 - 956 MHz)
  - IEEE 802.15.4f-2012 – frequencies 433 MHz
  - IEEE 802.15.4e-2012 – support for ISA100.11a
  - IEEE 802.15.4g-2012 – support for Smart Grid and frequencies 902 - 928 MHz

IEEE 802.15.4

- Base for other standards:
  - ZigBee – defines higher layers
  - 6LoWPAN – compressed IPv6 over IEEE 802.15.4
  - ZigBee IP – ZigBee's evolution to use 6LoWPAN and RPL routing protocol
  - ISA100.11a – industrial automation (based on 6LoWPAN, IPv6 and UDP)
  - WirelessHART – time-synchronized, self-organized and self-healing mesh architecture
  - Thread – based on 6LoWPAN/IPv6, a safe and reliable mesh network for in-home product control

IEEE 802.15.4: device classes

- *Full-function device* (FFD)
  - supports all features
  - can receive, send and route packages
  - coordinator must be FFD
- *Reduced-function device (RFD)*
  - limited communication and hardware capabilities
  - end node in network
  - can consume small amount of energy and can sleep
  - can only communicate with FFDs
  - the end node can be RFD or FFD

ZigBee

- Over 300 companies participated in its standardization as part of the ZibBee Alliance
- Based on IEEE 802.15.4
- Designed for applications that require low connection speed, low power consumption, low delay, secure communication (128-bit AES encryption)
- The nodes can be activated from sleep state in a few milliseconds
- Supports 65000 nodes per network
- The established network is very robust and fault-resistant
- Easy network management
- Speeds up to 250kbps

ZigBee - application

- Building automation – security, HVAC, lights, locks, ...
- Personal health – patient supervision, fitness
- Industrial automation – resource management, control of near environment, energy management
- Home management – safety, HVAC, lights, locks, irrigation, ...
- Computer peripherals – mouse, keyboard, joystick
- Consumer electronics – remote controls for TV, VCR, DVD/CD

Z-Wave

- Developed by the private company Zensys (2005) Denmark
  - bought by Sigma in 2008 and sold to Silicon Labs in 2018
  - they're the only ones making chips
- Certification through Z-Wave Alliance - 1700 products from 300 manufacturers
- Application in a smart home
- Frekevencija <GHz (868 MHz Europe, 908 MHz USA)
- Maximum distance 30-100m (depends on obstacles) – Z-Wave Plus 167m
- Bit rate: 9.6-100 kbps
- Use AES 128 encryption
- One device can be powered for 10 years with a coin-sized battery

Z-Wave

- Network topology: mesh, max. 232 devices in one network
- Each network has its own Home ID — shared between devices
- Each device has its own Node ID.
- Device types:
    - Controller – has a Home ID set up and can't be changed – in the factory
        - Primary and secondary controllers
    - Slave – accept Home ID from the primary controller and the controller assigns them a Node ID
        - Can be a router in the network
- Each node maintains a list of neighbours
- Sending methods: single, multicast, broadcast
- Network healing can be initiated where the topology is rearranged

IEEE 802.11ah

- A variant of the most famous wireless protocol (WiFi)
- Standard published in 2016.
- Designed for IoT devices (lightweight variant that consumes little energy)
- Adjustment for frequencies below 1GHz
- Range: up to 1km
- Maximum speed: 100 kbps
- Redefined part in the physical and MAC layers

IEEE 802.11ah - application

- The 3 most important areas of application:
  - Sensors and meters
    - E.g. parking, environmental monitoring/agriculture, industrial processes, health and fitness, building automation
  - Data aggregation from industrial plants
    - Possible connection to IEEE 802.15.4g
  - Expand WiFi in an open space

IEEE 802.11ah – physical layer (PHY)

- Use unlicensed areas < 1GHz
  - 868–868.6 MHz – EMEAR (Europe, Middle East, Africa, Russia)
  - 902–928 MHz – North America, Asia and the Pacific
  - 314–316 MHz, 430–434 MHz, 470–510 MHz, 779–787 MHz – China
- Use OFDM modulation
- Channel width:
  - 2, 4, 8, 16 MHz – for computers, mobile phones, ...
  - 1 MHz for low throughput (sensors)

IEEE 802.11ah – data link layer (MAC)

- Optimized for < 1GHz frequencies
- Allows low consumption
- Multiple devices that can be connected (8192 per AP)
- MAC Header - Minimized
- Bulking and sectorization – sector antennas
- *Restricted access window (RAW)* – algorithm for collision avoidance
- *Target wake time (TWT)* – AP can define when a device can connect → reduced energy because the device can "sleep" in the meantime

Long range protocols

LPWAN – Low Power Wide Area Network

- Low power consumption
- Devices can run on battery
- Long distance communication (~x km)
- Lower communication frequencies → increased distance
- Lower data rate

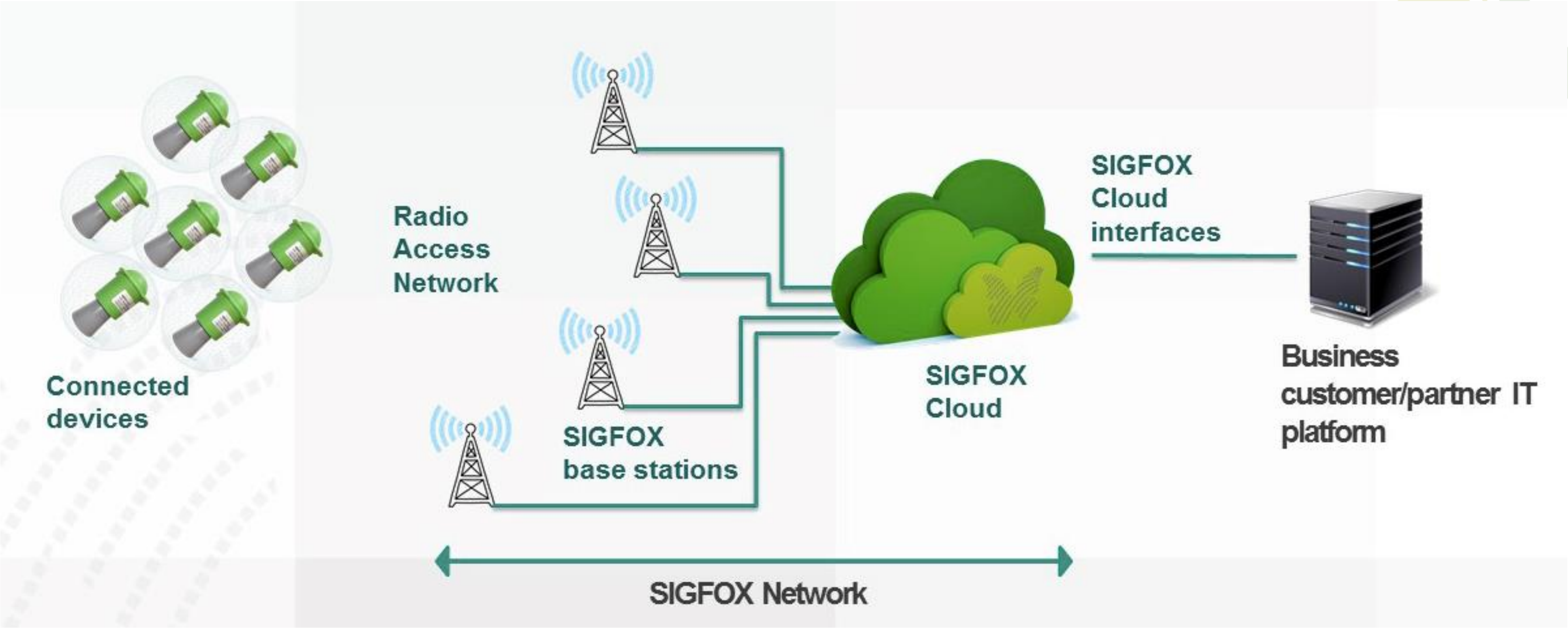
Sigfox

- Technology developed in 2009 in Toulouse, France
- Patented and closed technology
- Use unlicensed ISM band
- Constraints:
  - Up to 140 messages per device per day can be sent (duty cycle 1%, 6 messages/hour)
  - The size of the data transmitted by: 12 bytes (sending) and 8 bytes (receiving)
  - Transfer rate up to 100 bps (sending) and 600 bps (receiving)
- For communication in one direction from sensor to server (as a sensor network)

Sigfox – physical layer

- Ultra Narrow Band (UNB)
- Frequencies:
  - 868 MHz: Europe (regulatory document ETSI 300-200)
  - 902 MHz: North America (regulatory document FCC part 15)
- 333 channels, channel width 100 Hz
- Receiver sensitivity: -120 dBm/-142 dBm
- Transmitter power: +14 dBm, and in North America +22 dBm

Sigfox – topology

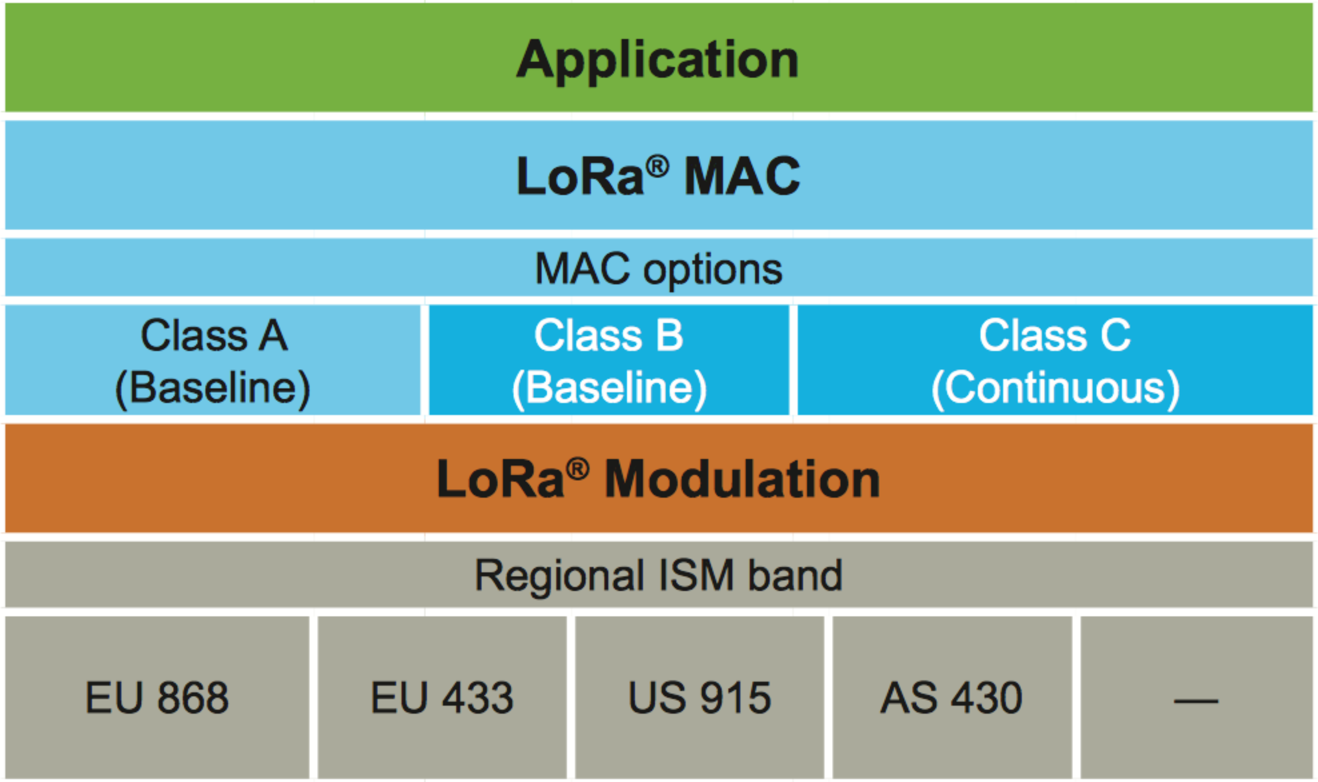


Izvor: https://ask.sigfox.com/storage/attachments/91-sigfox-network-architecture.jpg

LoRa and LoRaWAN

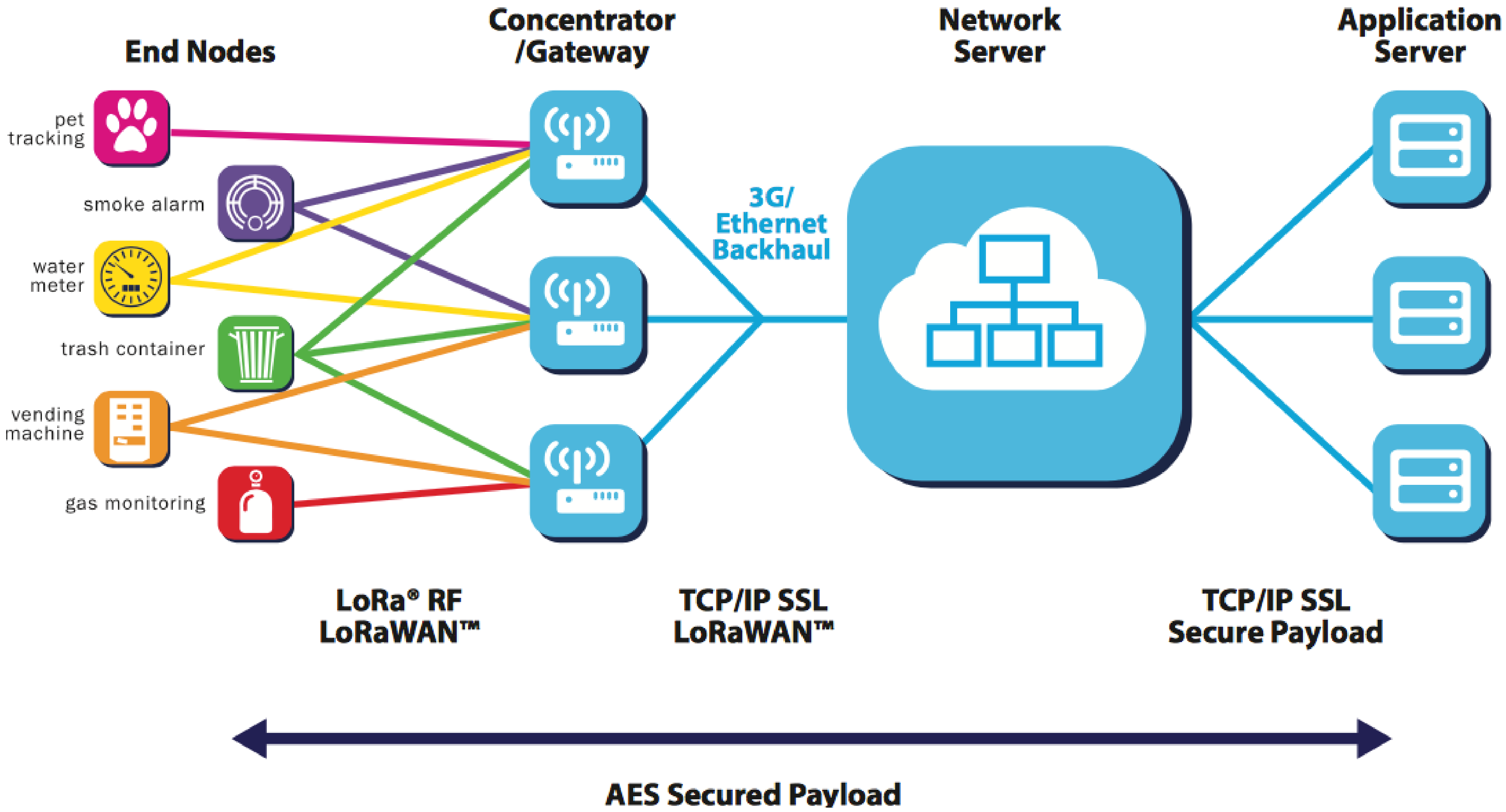
- LoRa – defines the physical layer
- LoRaWAN – defines the protocol and architecture of the system

LoRa – node architecture



Izvor: https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf

LoRaWAN – network architecture

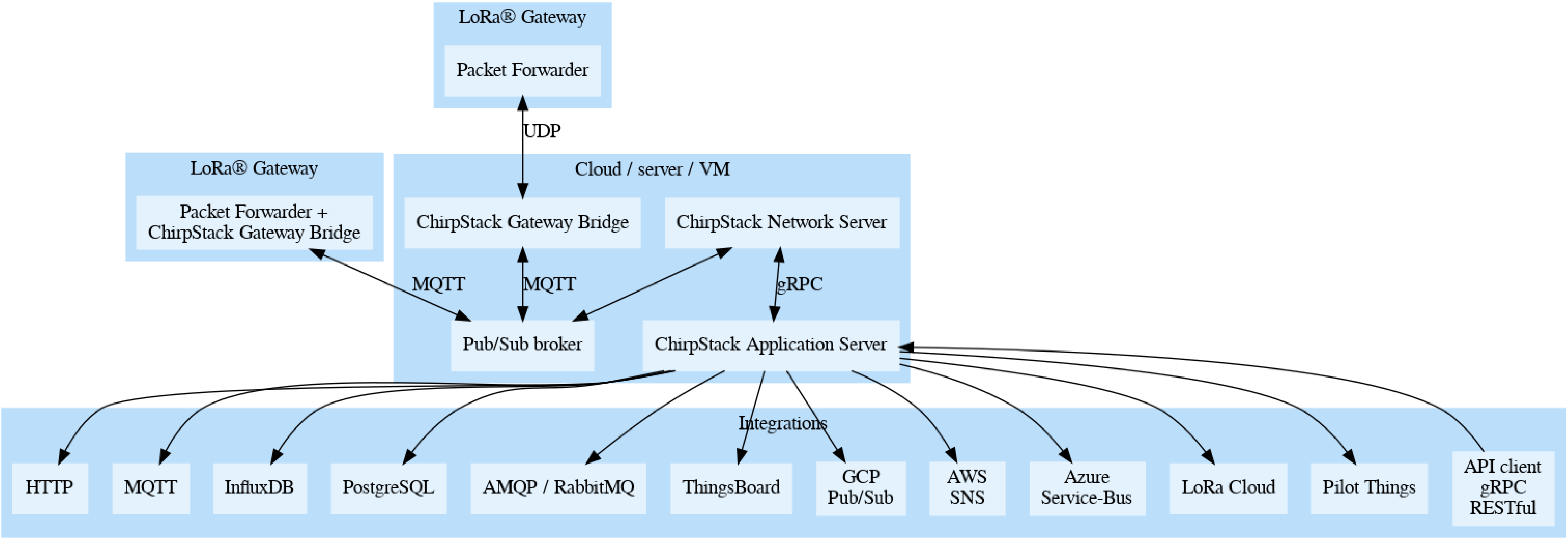


Izvor: https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf

ChirpStack

- LoRaWAN Network Server Open source stack
- components:
  - ChirpStack Gateway Bridge
    - for communication with gateway
  - ChirpStack Network Server
    - network server implementation
  - ChirpStack Application Server
    - application server implementation
  - ChirpStack Gateway OS
    - to perform the entire stack on the gateway running on the Raspberry Pi
    - based on Linux

ChirpStack - architecture



LoRa – device classes

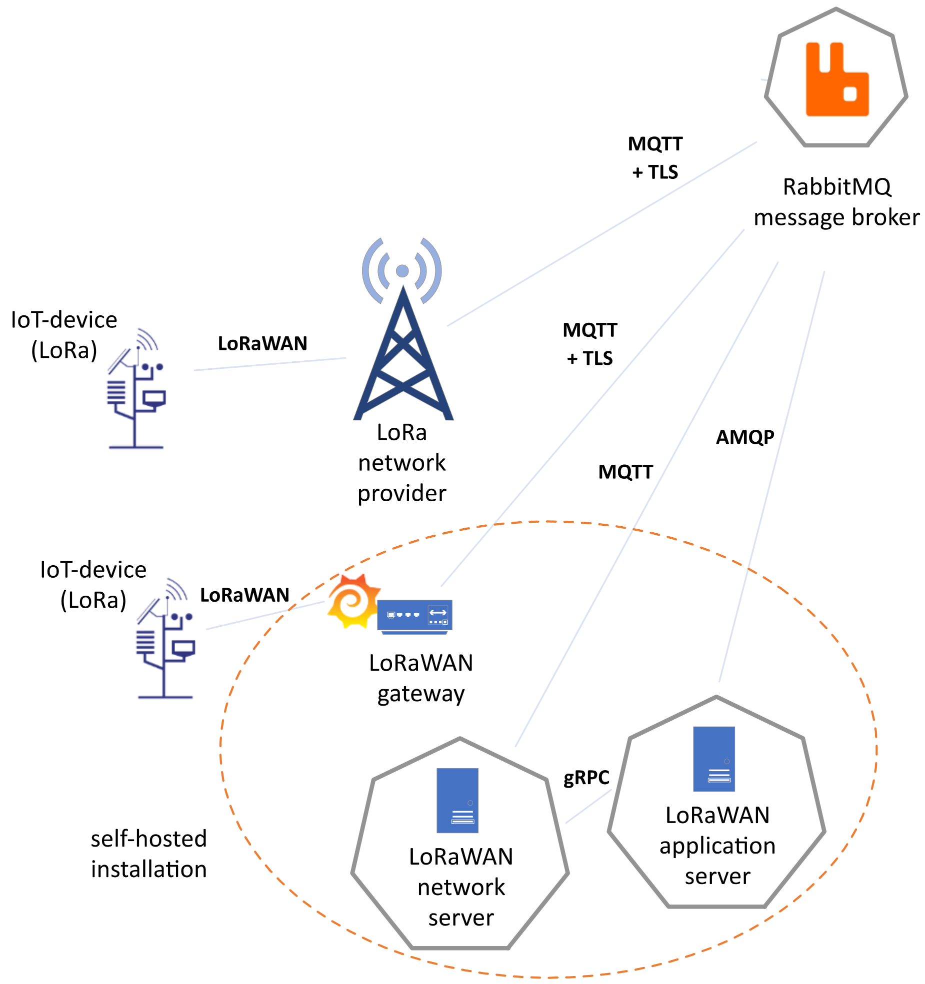
- Class A
  - Best for battery power
  - All devices on the network support this mode
  - Sending data to the device is possible only after successful sending
  - Use ALOHA mechanism
- Class B
  - Receiving over a scheduled period of time
  - Receives a sync signal from GW
- Class C
  - Continuously has an open receiving window
  - Receiving is stopped only when data is sent

Implementations

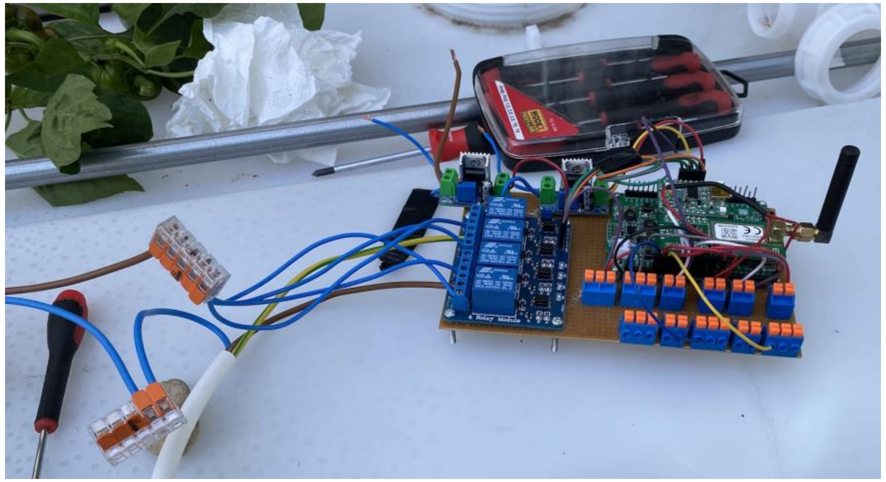
- Commercial:
  - Operators provide the network and charge for it:
    - OiV (Croatia), KPN (Netherlands), Orange (French), Unidata (Italy), …
    - Unidata (partner in the project symbIoTe) - operator of LoRaWAN network in Italy
    - https://www.i-scoop.eu/internet-of-things-guide/iot-network-lora-lorawan/
- Public:
  - Anyone can get involved and provide access
  - Up-to-date list https://www.thethingsnetwork.org
- Private:
  - Anyone can start their own private network

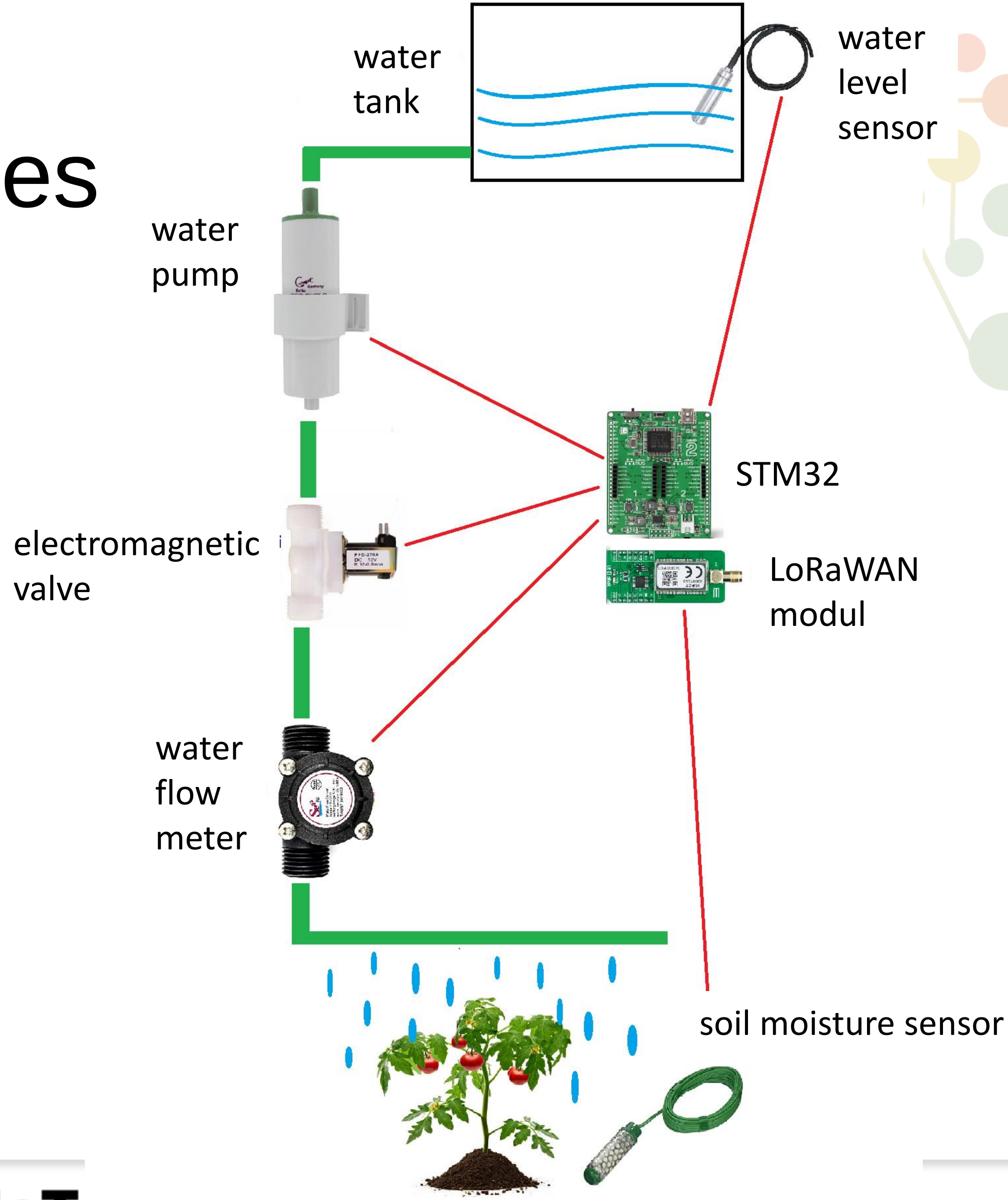
LoRaWAN implementation in IoT lab at FER

IoT-polje



Data collection and actuation with appliances in the urban garden





Mobile network
Standards and standardization bodies

- ITU – International Telecommunication Union
  - They define the goals and standards for devices that will be labelled with 4G or 5G
- 3GPP
  - Consortium defining technologies and upgrades
  - Everything is organized into releases:
    - Rel 8-9: LTE (2008, 2009)
    - Rel 10-12: LTE Advanced (2011, 2012, 2015)
      - Rel 12: **LTE-M (Cat 0)**
    - Rel 13-14: LTE Advanced Pro (2016, 2017)
      - Rel 13: **LTE Cat-M1 (eMTC), NB-IoT (LTE Cat-NB ili NB1)**
      - Rel 14: Vehicle-to-Everything (V2X), improvements for MTC, NB-IoT (NB2)
    - Rel 15: (2019) – improvements for MTC, 5G Vehicle-to-x service (V2X)
    - Rel 16: (2020) – 5G expansion (advanced V2X, Industrial IoT, URLLC), 5G Efficiency (power consumption)

LTE Cat 0 – Release 12

- Reduced bit rates to 1Mbps
- Half-duplex communication
- Introduces Power Save Mode (PSM)
  - Device can enter into a deep sleep and quickly wake up and connect
  - Can wake up and send data once a day
  - Maximum sleep period 12.1 days (depends on the network e.g. 2 or 4 hours)

LTE Cat-1 – Release 8

- Primarily used in the USA for M2M communication
- Higher speeds: 10Mbps (download), 5Mbps (sending)
- Can transmit audio and video
- Lower power consumption than 4G-LTE
- Can be switched to 3G or 2G

LTE Cat-M1 (eMTC or LTE-M) – Release 13

- eMTC – enhanced Machine Type Communication
- Reduced bandwidth from 20MHz to 1.4Mhz simpler devices, lower consumption
- Reduced power output by 50%
- Speeds of 375 kbps or 1 Mbps
- Application: V2V, sound
- Added mechanisms for the possibility of short sleep devices (10.24s) radio consumes 15μA on average
- PSM from Cat-0 applies here as well

NB-IoT (LTE Cat-NB or NB1) – Release 13

- Goals:
  - 10 years battery life with a capacity of 5 Wh
  - Additional coverage of space (+20 dB)
  - Module Price: ~$5
- Important changes:
  - Channel width only 180kHz → reducing module costs and power consumption
  - No audio or video transmission
  - There is no mobility between the cells
  - Maximum signal loss (MCL – max. coupling loss) 164 dB which is similar to LoRaWAN and Sigfox
    - Communication passes in basements and tunnels
    - Increased range by 7x outdoors
- Transmission speed: ~26kbps downlink, ~62kbps uplink
- Theoretically, it allows you to connect up to 200,000 devices per cell

NB-IoT (NB2) – Release 14

- Major upgrades:
  - more precise positioning: OTDOA and E-CID
  - added multicast
  - improved mobility
    - possible reconnection when we are connected, it is not necessary to go into idle mode
  - increased maximum speeds:
    - 127kbps *downlink*, 159kbps *uplink*
  - support for multiple (15) operators → increased device density 1M/km^2
  - new power class 14dBm → requires less battery

NB-IoT – the first installations 2017

- DT – launched in 8 EU countries (Germany, Netherlands, Austria, Croatia, Greece, Hungary, Poland, Slovakia)
  - Applications: tracking things, smart parking, smart meters
- T-Mobile US, Ericsson, Qualcomm
  - Applications: collection of sensor data (temp., humidity, gases, ...), flood alarming
- U-blox, PinMyPet, Huawei and operator Vivo: animal tracking
- China Mobile, ZTE – 200-site network testing
- Telia Norway – pilot project to track 1000 sheep in Norway

Conclusions

- Choosing protocol and technology depends on different constraints like:
  - Use case
  - Indoor or outdoor
  - Range
  - Type of power
  - Place (country and their regulations)
  - Subscription or self hosted
  - …