MAI4CAREU
Master programmes in Artificial Intelligence 4 Careers in Europe

University of Cyprus

MAI650 Internet of Things

Vasos Vassiliou

September - December 2023

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CS6xx Internet of Things (8 ECTS)

Course purpose and objectives: The purpose of the course is to provide an overview on IoT tools and applications and to introduce to students hands-on IoT communication concepts through lab exercises.

Learning outcomes: Upon completion of this course, students will be able to explain the definition and usage of the term “Internet of Things” in different contexts. More specifically, the students will know how to apply the knowledge and skills acquired during the course to build and test a complete, working IoT system involving prototyping, programming and data analysis

Teaching methodology: interactive face-to-face lectures, group activities and discussions, in class/lab activities, student presentations and guest lectures or significant recorded public lectures

Assessment: Final exam (50%), midterm exam (20%) and assignments/project (30%).

Main text:

Rajkumar Buyya, Amir Vahid Dastjerdi, Internet of Things Principles and Paradigms, Morgan Kaufmann; 1st edition, 2016

J. Biron and J. Follett, "Foundational Elements of an IoT Solution", O'Reilly Media, 2016.

Other reading:

Jamil Y. Khan and Mehmet R. Yuce, Internet of Things (IoT) Systems and Applications, 2019, ISBN 9789814800297

David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, and Jerome Henry, IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, 2016, Cisco Press.

INTRODUCTION

IoT Communication Technology - Advanced

CONTENTS

1. Introduction
2. Communication and Network Protocols in IoT
3. System design: Challenges with various IoT network protocols
4. Build a LoRaWAN Network

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

INTENDED LEARNING OUTCOMES

Upon completion of this introductory unit, students will:

1. have detailed knowledge of the network access protocols
2. have detailed knowledge of how to interface with the platform of the IoT Network provider
3. have detailed knowledge of how to setup a private IoT network
4. be able to (skills):
    1. Exchange data with the core IoT network
    2. Program or use an edge computing system to send data to a carrier
    3. Apply design rules for low power bi-direction edge network devices
5. will (competences)
    1. be able to setup the infrastructure required for the data flow between edge devices and an IoT application development platform

Introduction

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Introduction

- Wireless networking is a very common and flexible way for IoT appliances to transfer information.
- All wireless radio technologies have their own characteristics for range, available bandwidth, and power consumption.
- Choosing the right radio technology for the right use case is important.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU Master programmes in Artificial Intelligence 4 Careers in Europe

Communication and Network Protocols in IoT

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Communication in IoT

- There are a large number of heterogeneous smart devices connecting to the Internet.
- Due to the constrained nature of the devices we have a lot of challenges related to the communication of the devices
- Important communication protocols: 6LoWPAN, LoRaWAN, NB-IoT

Communication Challenges

- Addressing
- Low power communication
- Routing
- Mobility

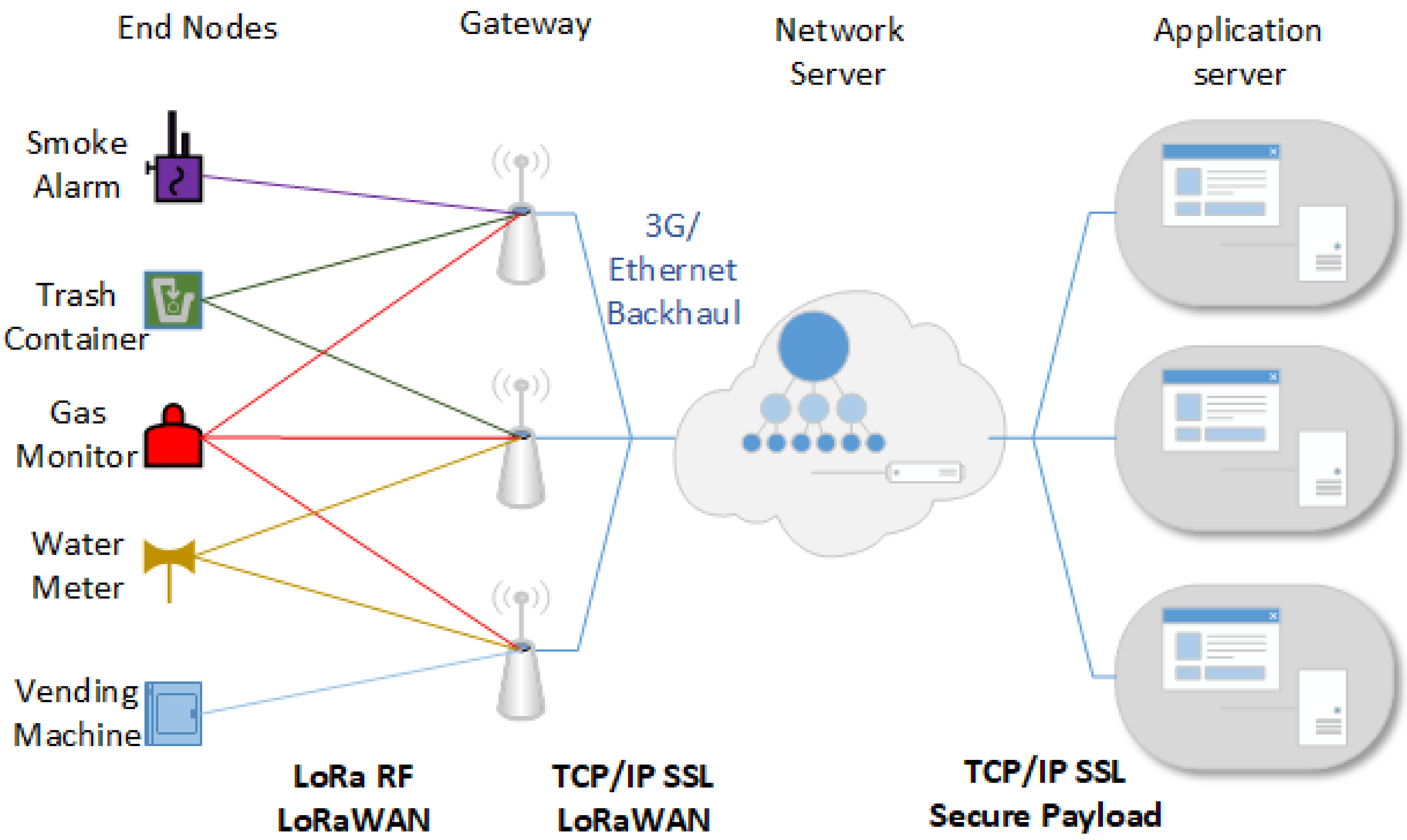
Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

LoRaWAN Communication

- LoRaWAN is an open standard architecture developed by LoRa Alliance
- Provide a medium access control mechanism and enable end-devices to communicate with one or more gateways
- LoRaWAN Alliance uses a star network topology, in which a gateway seamlessly relays messages between a Network Server (NS) and end-devices

LoRaWAN Architecture



Wael Ayoub, Abed Samhat, Fabienne Nouvel, Mohamad Mroue, Jean-Christophe Prévotet. Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs standards and Supported Mobility. 2018 25th International Conference on Telecommunications (ICT), Jun 2018, St. Malo, France

LoRaWAN

- The LoRaWAN Alliance specifications define three classes for an End-Device

- The three classes are:
  - Class A (Bi-directional)
  - Class B (Bi-directional with scheduled receive slots)
  - Class C (Bi-directional with maximal receive slots)

LoRaWAN Terminology

- Uplink = message from a LoRaWAN end-node to a LoRaWAN Network Server

- Downlink = message from a LoRaWAN Network Server to a LoRaWAN end-node

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

LoRaWAN

- Messages exchanged between the end-device and the Network and Application Servers use two security keys.

- Achieve security and integrity of the uplink and downlink messages

- Security keys:
  - Network Session Key (NwkSKey)
  - Application Session Key (AppSKey)

Network Session Key

- The Network Session Key (NwkSKey) is used for interaction between the Node and the Network Server (NS). This key is used to check the validity of messages (MIC check).

- Encrypts the whole frame (headers + payload) in case a MAC-command is sent. When data are sent, this key is used to sign the message which allows the NS to verify the identity of the sender.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

LoRaWAN

Application Session Key

- The Application Session Key (AppSKey) is used for encryption and decryption of the payload. The payload is fully encrypted between the Node and the Handler/Application Server component
- These keys are known only to the end-device and the network/application server. This means that another node or man-in-the-middle is not able to decode the packet payload.
- This key does not need to be known by the NS.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

LoRaWAN – Join the network

- A new End-Device can participate the LoRaWAN network only if it has been activated.

- Activation procedure requires 3 types of information:
  - Device Address
  - Network Session Key
  - Application Session Key

LoRaWAN – Join the network

Device Address

- It consists of a 32-bit identifier which is unique within the network. This address is equivalent to an IP address on a TCP/IP network. It is present in each data frame. This key is shared between end-device, Network Server and Application Server.

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

LoRaWAN Activation

- The following two methods are used to deploy these keys:
  - Over-the-Air Activation (OTAA)
  - Activation by personalization (ABP)

- With either of these methods, the same keys are loaded into both the module and network server that allows end-to-end data security.

Over-the-Air Activation (OTAA) Procedure

- Over-the-Air Activation (OTAA) Procedure:
  - The end-device performs a join procedure to connect to a LoRaWAN network and exchange data.
  - End Device exchanges two MAC messages with the server:
    - Join request
    - Join accept.
  - During the join procedure, an ED is assigned a dynamic device address (DevAddr) and security keys are negotiated with it.
- In case the end device loses the connection, the procedure must be repeated.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Over-the-Air Activation (OTAA) Procedure

- Keys used during the Over-the-Air activation (OTAA:
  - application ID (AppEUI) and an application key (AppKey)
  - a device ID (DevEui) to derive the network session key (NwkSKey),
  - application session key (AppSKey) and the device address.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Activation By Personalization (ABP):

- Activation By Personalization (ABP):
  - The shared keys are stored in the end-device.
  - When the end-device is turned on for the first time, it can directly initiate the communication.
- Activation by personalization (ABP) uses both session keys directly, along with the DevAddr, to sign and encrypt the data packets. These must be configured both on the node and on the network server.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

LoRaWAN Data Exchange

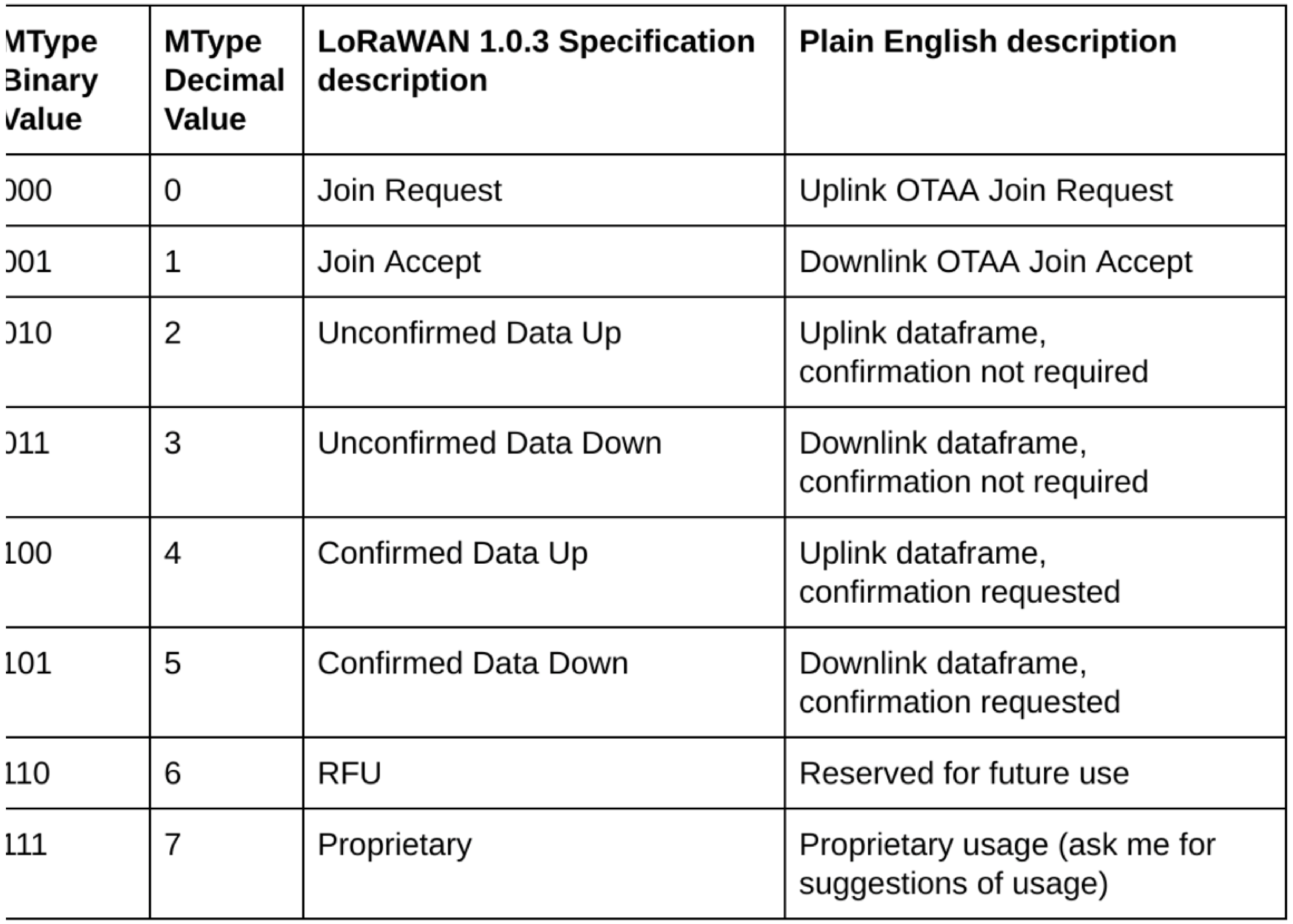
- By the time the end-device is activated it can starts to send/receive data messages.
- These messages are used to transfer both MAC commands and application data, which can both be combined in a single message.
- The data message can use the Adaptive Data Rate (ADR) scheme
- This scheme is used by the network or the End device application layer to manage, adapt, and optimize the data rate.
- If this scheme is not enabled, the network will not control the data rate even if the received RSSI is low.
- In this case, the device application layer is responsible for managing the data rate.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

LoRaWAN Data Exchange

- LoRaWAN confirmed/ unconfirmed message types



MType Binary Value	MType Decimal Value	LoRaWAN 1.0.3 Specification description	Plain English description
000	0	Join Request	Uplink OTAA Join Request
001	1	Join Accept	Downlink OTAA Join Accept
010	2	Unconfirmed Data Up	Uplink dataframe, confirmation not required
011	3	Unconfirmed Data Down	Downlink dataframe, confirmation not required
100	4	Confirmed Data Up	Uplink dataframe, confirmation requested
101	5	Confirmed Data Down	Downlink dataframe, confirmation requested
110	6	RFU	Reserved for future use
111	7	Proprietary	Proprietary usage (ask me for suggestions of usage)

Message types as outlined in LoRaWAN™ 1.0.3 Specification, page 16, section 4.2.1
(final release, March 20, 2018, V1.0.3)

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

LoRaWAN Frame Header

- Part of the LoRaWAN frame header.

- The Frame Header (FHDR) is a structure that immediately follows the MHDR in a LoRaWAN data frame.

- The FHDR contains the short device address of the end-device (DevAddr), a frame control octet (FCtrl), a 2-octets frame counter (FCnt), and up to 15 octets of frame options (FOpts) used to transport MAC commands.

Size (bytes)	4	1	2	0..15
FHDR	DevAddr	FCtrl	FCnt	FOpts

LoRaWAN ACK flag

- FCtrl, is the one that carries the ACK flag. The ACK flag is the third MSB of the FCtrl, for both uplink and downlink frames.

- If the ACK flag is set to 0, the sender indicates it has not previously received a message that required acknowledgment / confirmation.

- If the ACK flag is set to 1, the sender indicates it has received a message requiring an acknowledgment / confirmation, and is hereby providing the acknowledgment / confirmation.

LoRaWAN Confirmed Uplink message

- A confirmed uplink message is a message where the end device is requesting a LoRaWAN network to confirm the reception of its message.
- A message with MType set to 4 (‘100’ binary) is created and send uplink.
- If the end device receives a message which ‘ACK’ flag is set to 1, it will consider the original uplink message was delivered.
- If there is no message received, it means the network has not received the uplink.
- The end device decides how to react, but in most cases it should simply send the uplink again.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Confirmed Downlink message type

- A confirmed downlink message is a message where a LoRaWAN network is requesting a end device to confirm reception of its message.
- The Network Server creates a message with MType set to 5 (‘101’ binary), and sends downlink to the end device.
- The end device will transmit an acknowledgment in the next data uplink message.
- If the Network Server receives the next uplink message from that end-point without the ACK flag set to 1, it will consider the previous downlink message lost.
- If this happen, the Network Server can either perform a retransmission, or can inform the application and let the application decide how to react.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

NB-IoT

- NB-IoT is built from existing LTE functions

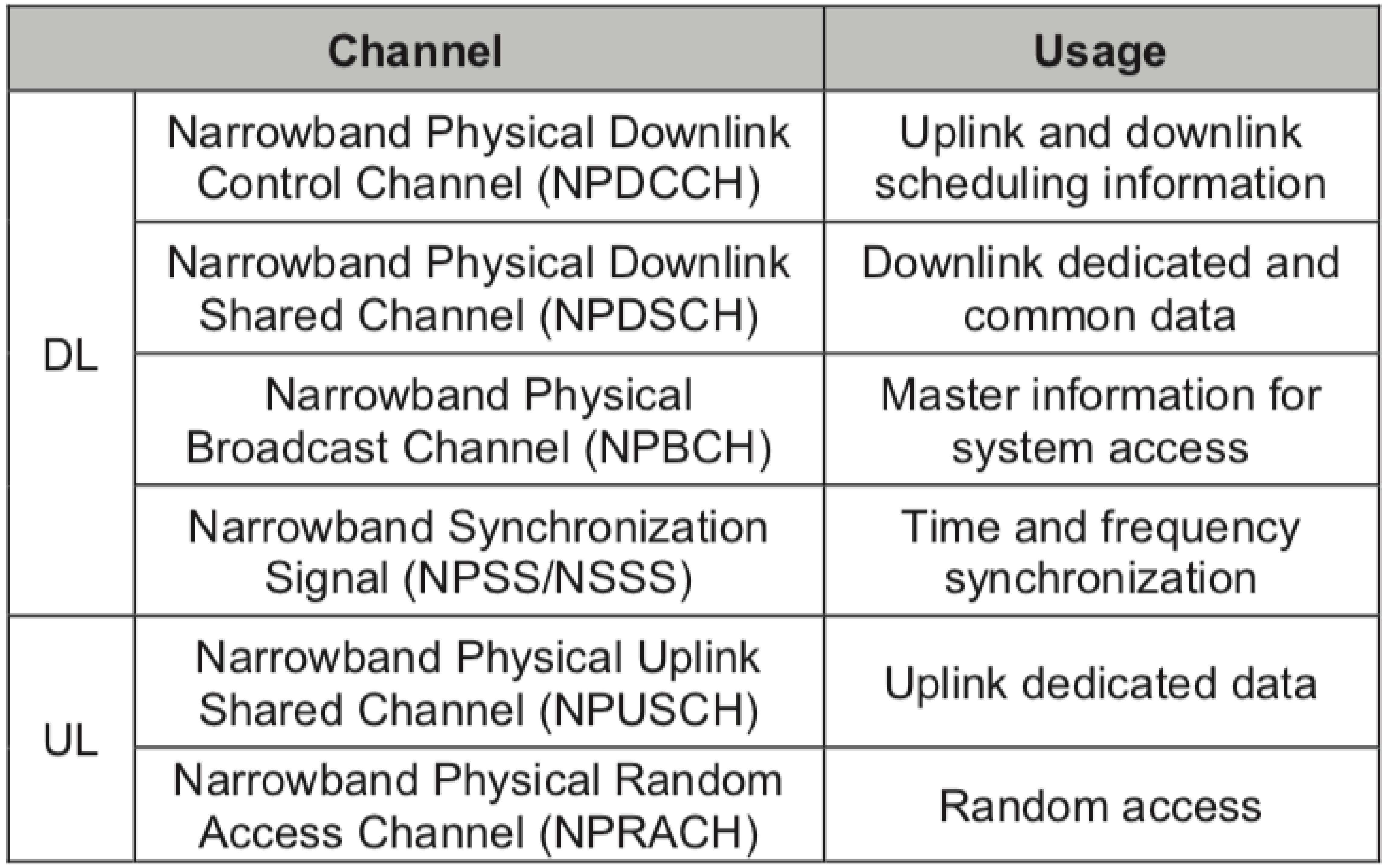
- Features of LTE that have been removed:
  - removing handover
  - carrier aggregation
  - measurements to monitor the channel quality
  - dual connectivity
  - real-time services

- Purpose: to keep it as simple as possible and to reduce device cost and minimize battery consumption.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

NB-IoT Downlink (DL) and uplink (UL) channels and signals



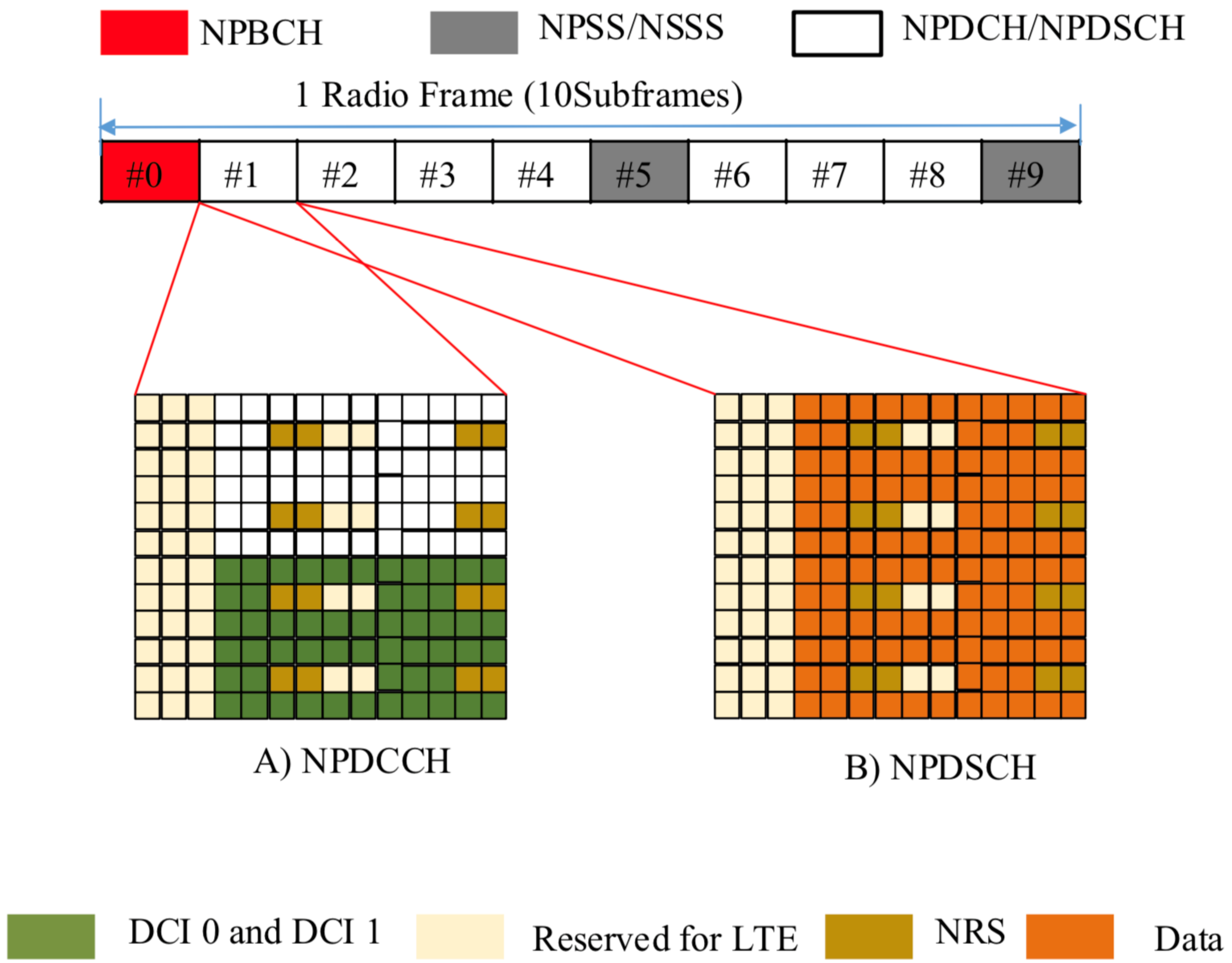
Channel		Usage
DL	Narrowband Physical Downlink Control Channel (NPDCCH)	Uplink and downlink scheduling information
	Narrowband Physical Downlink Shared Channel (NPDSCH)	Downlink dedicated and common data
	Narrowband Physical Broadcast Channel (NPBCH)	Master information for system access
	Narrowband Synchronization Signal (NPSS/NSSS)	Time and frequency synchronization
UL	Narrowband Physical Uplink Shared Channel (NPUSCH)	Uplink dedicated data
	Narrowband Physical Random Access Channel (NPRACH)	Random access

R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert and J. Koskinen, "Overview of narrowband IoT in LTE Rel-13," *2016 IEEE Conference on Standards for Communications and Networking (CSCN)*, Berlin, 2016, pp. 1-7

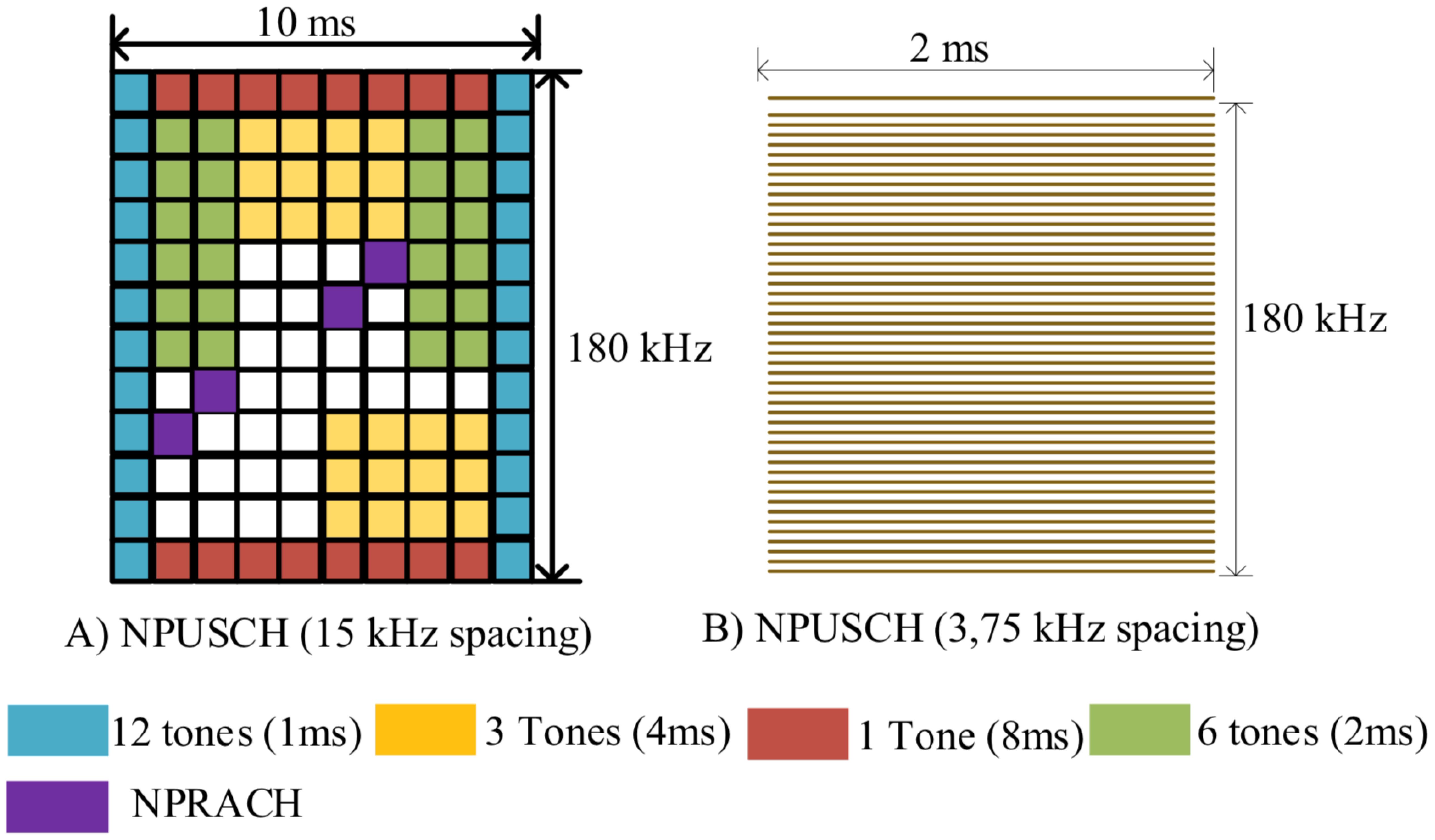
Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

NB-IoT Downlink Frame Structure



NB-IoT Uplink Frame Structure



A) NPUSCH (15 kHz spacing)

B) NPUSCH (3,75 kHz spacing)

NB-IoT Cell Acquisition and Synchronization

- Same process as LTE end devices where to associate a cell, it must performs a frequency and timing synchronization
- The end device obtains the center carrier frequency and the allocated slot and frame timing used for the cell acquisition.
- The end devices acquires Master Information Block (MIB) from NPBCH and System Information Block (SIBs) from the NPDCCH

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

NB-IoT Cell Acquisition and Synchronization

- In general, if MIB and SIB are properly decoded, cell ID, a subframe number, scheduling information, and system bandwidth can be detected successfully.

- In NB-IoT, the low complexity of devices may lead to poor synchronization and cell acquisition performance, especially due to carrier frequency offsets and poor channel estimation capacity.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

NB-IoT Procedures

- Other procedures supported:
- Random Access Procedure
- Channel Estimation and Error Correction
- Co-Channel Interference
- Radio Resource Allocation
- Link Adaptation
- Coverage and Capacity

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Communication in IoT

- Addressing: there is a need to uniquely identify the IoT devices.
- Due to the large number of devices a large addressing space is needed to cover the needs
- IP stack is needed
- 6LoWPAN could be one possible solution
- 6LoWPAN incorporates IPv6 to low power devices

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Low-power RF + IPv6 = 6LoWPAN

- Benefits:
  - include the easy interconnection with other IP networks,
  - the use of existing internet infrastructure,
  - the application of the well-known IP-based technologies to sensor networks,
  - reuse of existing power monitoring and diagnostic tools. The challenge in supporting IP protocols
- Problems:
  - lower power consumption,
  - low duty cycles,
  - limited bandwidth and reliability

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

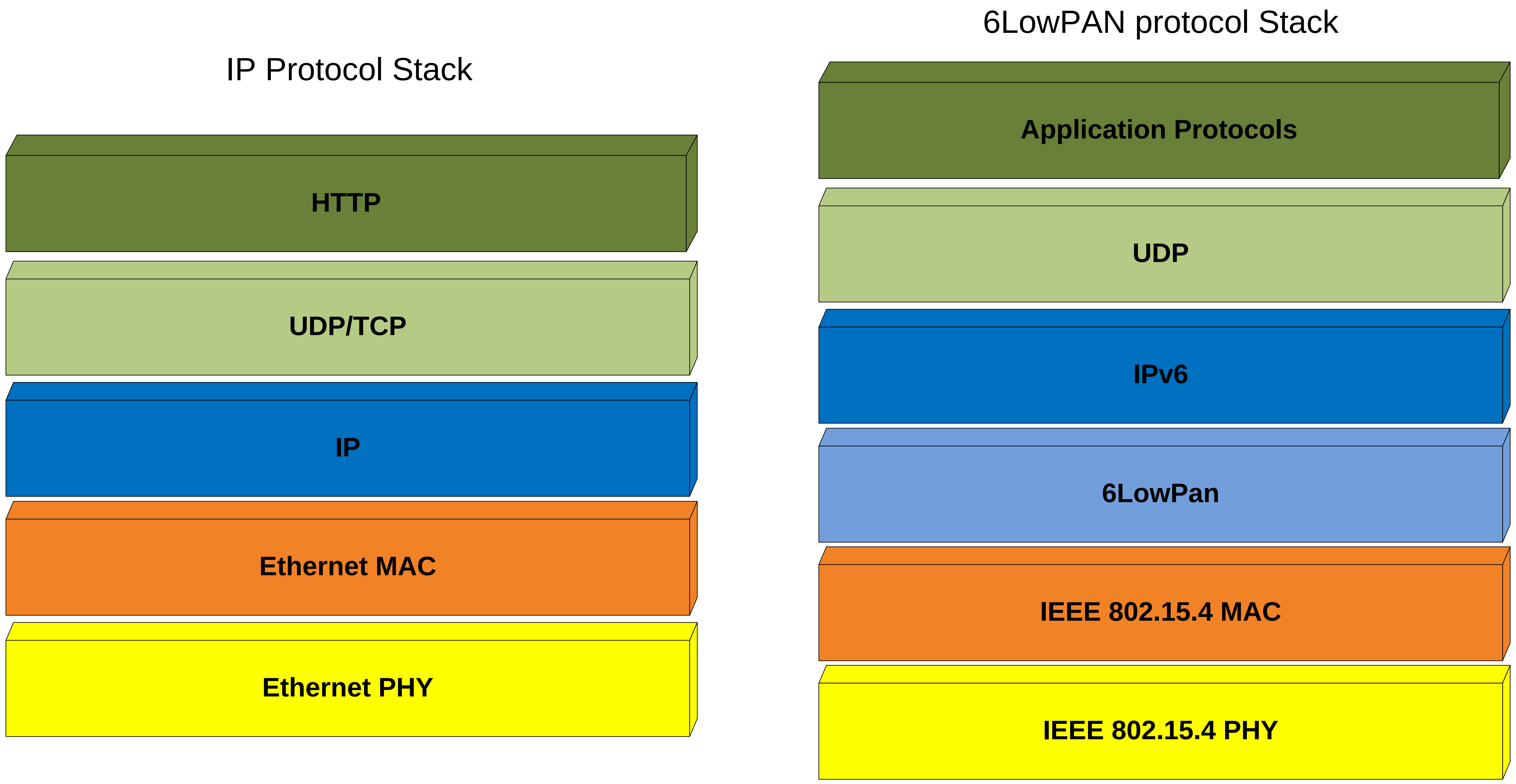
What is 6LoWPAN

- Low-power RF + IPv6 = 6LoWPAN
- Defined by IETF standards
- RFC 4919, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals”
- RFC 4944, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks”

Benefits of using IP in 6LoWPAN Technology

- The benefits of 6LoWPAN include:
  - Open, long-lived, reliable standards
  - Transparent Internet integration
  - Easy learning-curve
  - Established network management tools
  - Global scalability
  - Established security
  - End-to-end data flows

6LoWPAN architecture



6LoWPAN characteristics

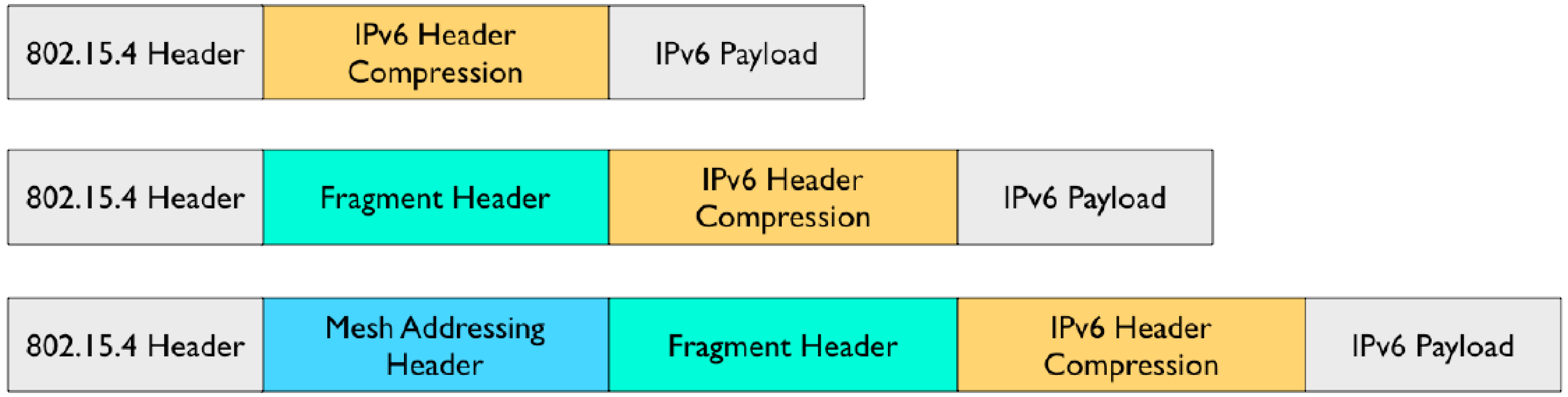
- As IEEE 802.15.4:
  - Small MTU size of 127 bytes
  - Low data rate of 250kbps
  - Operates in 2.4 GHz band
  - Short range communication
- Efficient header compression
- Network autoconfiguration using neighbor discovery
- Unicast, multicast and broadcast support
- Fragmentation
  - 1280 bytes IPv6 MTU -> 127 bytes 802.15.4 frames
- Support for IP routing (e.g. IETF RPL)
- Star and peer-to-peer (mesh) topologies

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Adaptation layer

- Responsible for:
  - Header compression
  - Fragmentation and Reassembly
  - L2 forwarding
- Headers



802.15.4 Header | IPv6 Header Compression | IPv6 Payload

802.15.4 Header | Fragment Header | IPv6 Header Compression | IPv6 Payload

802.15.4 Header | Mesh Addressing Header | Fragment Header | IPv6 Header Compression | IPv6 Payload

- Mesh addressing supports layer two forwarding
- Fragment supports IPv6 MTU
- IPv6 header to support IP routing

Addressing

- 3 types of addresses
  - 128-bits Global address: used for global communication.
  - 64-bits link local address: used for communication inside the same PAN
  - 16-bits short address: used for communication inside the same PAN

Fragmentation and Reassembly

- IP packets may be large, compared to 802.15.4 max frame size (1280 to 127 bytes)
- Big packets must be fragment to fit in a single 802.15.4 frame
- Each specifies tag, size, and position
- All fragments of an IP packet carry the same “tag”
- Do not have to arrive in order
- Time limit for entire set of fragments (60s)
- Fragmentation is undesirable because of the decoupling between lost of a fragment and retransmission of entire packet

Header compression

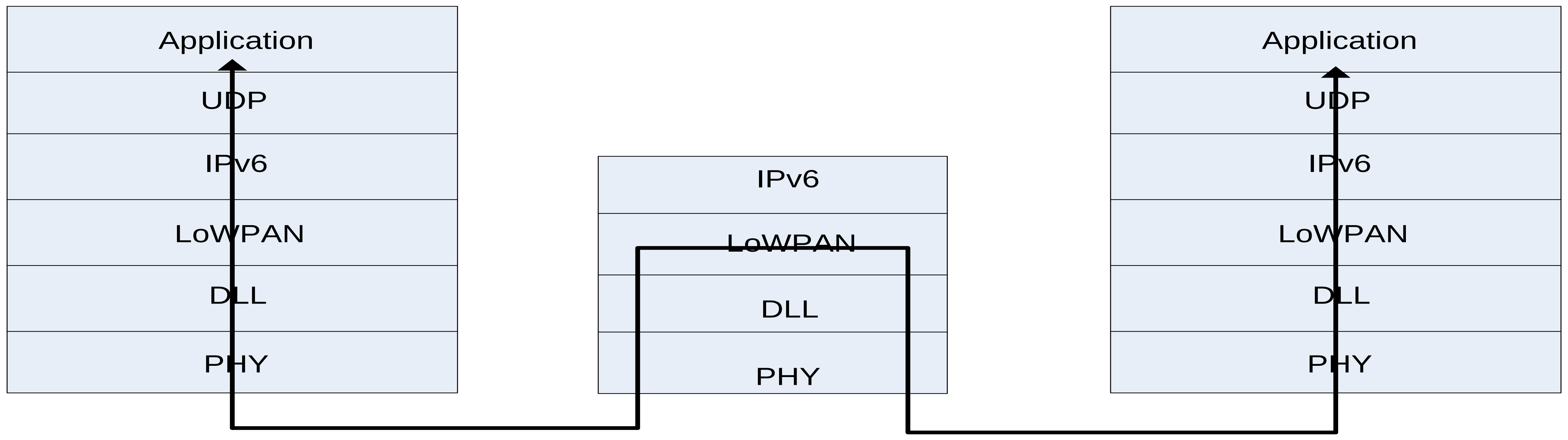
- IPv6 header is the largest header(40B ~ 32% of the 6LoWPAN MTU) + 8 bytes UDP header
- RFC 4944 defines HC1 stateless compression scheme for the IPv6 header
- The first byte of the IPv6 header used to identify compression (dispatch byte)
- This solution is optimal for link-local communication but routable addresses must be used when communicating with external devices. Best case of IPv6/UDP is 7 bytes
- New encoding format called IPHC
- Can compressed the IPv6/UDP header for global communication down to 10 bytes

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

6LoWPAN Routing

- Mesh under – L2 forwarding



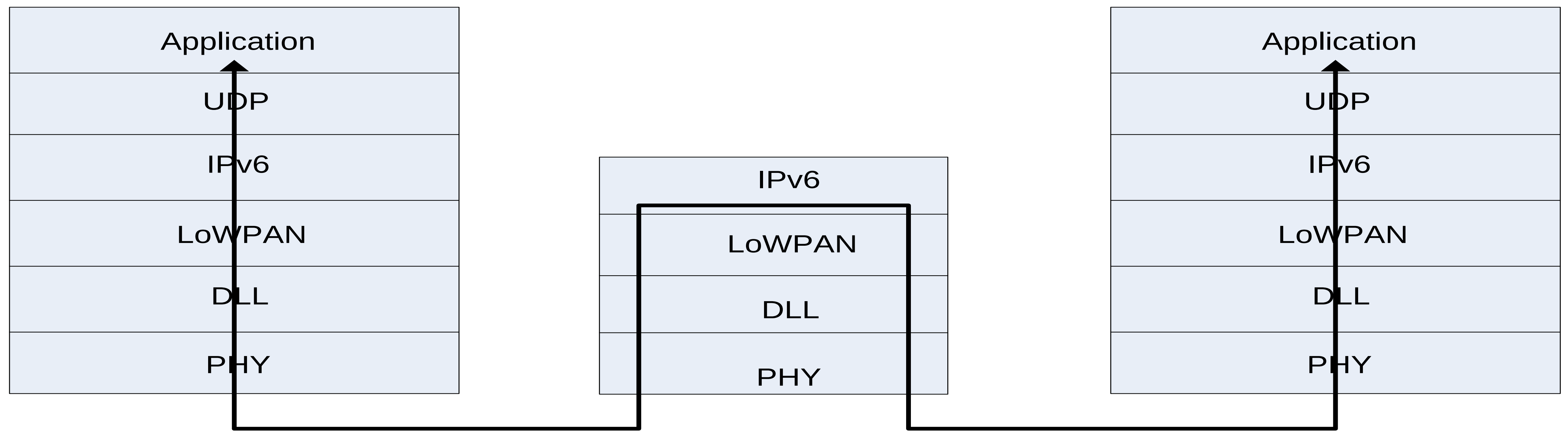
- 64-bit extended address or the 16 bit short address
- Hop by hop forwarding thus the originator address and the final destination node address are included on the 6LoWPAN header.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

6LoWPAN Routing

- Route over – IP routing



- Decisions are taken in the network layer where each node acts as an IP router.

Co-financed by the European Union
Connecting Europe Facility

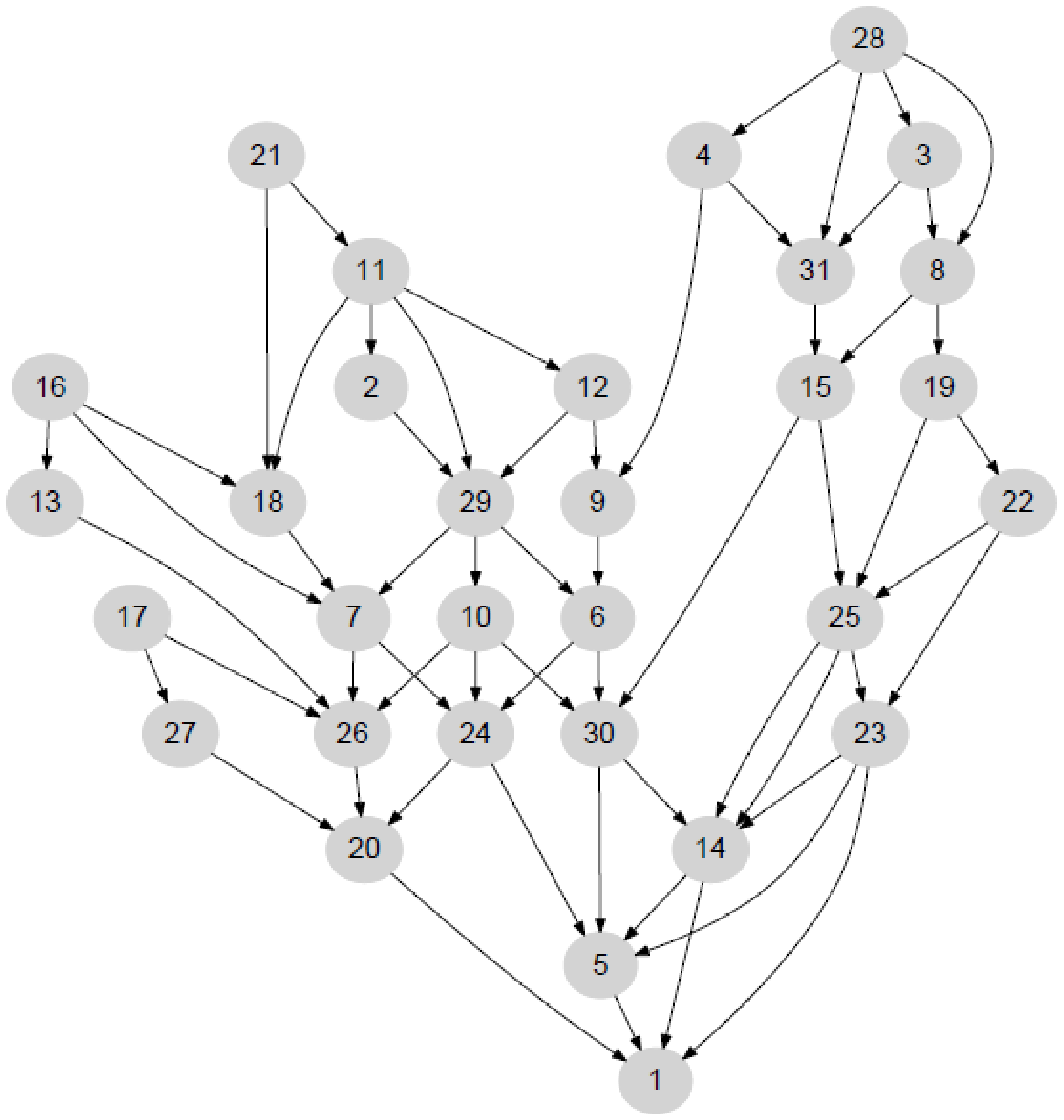
This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Routing - ROLL IETF Group

- Routing Over Low power and Lossy networks (ROLL)
  - Working group at the IETF
- Route over routing techniques
- Standardizing a routing algorithm for embedded apps until 2010
- Application specific requirements
  - Home automation
  - Commercial building automation
  - Industrial automation
  - Urban environments
- Analyzed all existing protocols
- Protocol in-progress called RPL “Ripple”- Proactive distance-vector approach

RPL “Ripple” routing protocol

- As IEEE 802.15.4:
  - Small MTU size of 127 bytes
  - Low data rate of 250kbps
  - Operates in 2.4 GHz band
  - Short range communication
- Efficient header compression
- Network autoconfiguration using neighbor discovery
- Unicast, multicast and broadcast support
- Fragmentation
  - 1280 bytes IPv6 MTU -> 127 bytes 802.15.4 frames
- Support for IP routing (e.g. IETF RPL)
- Star and peer-to-peer (mesh) topologies



Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

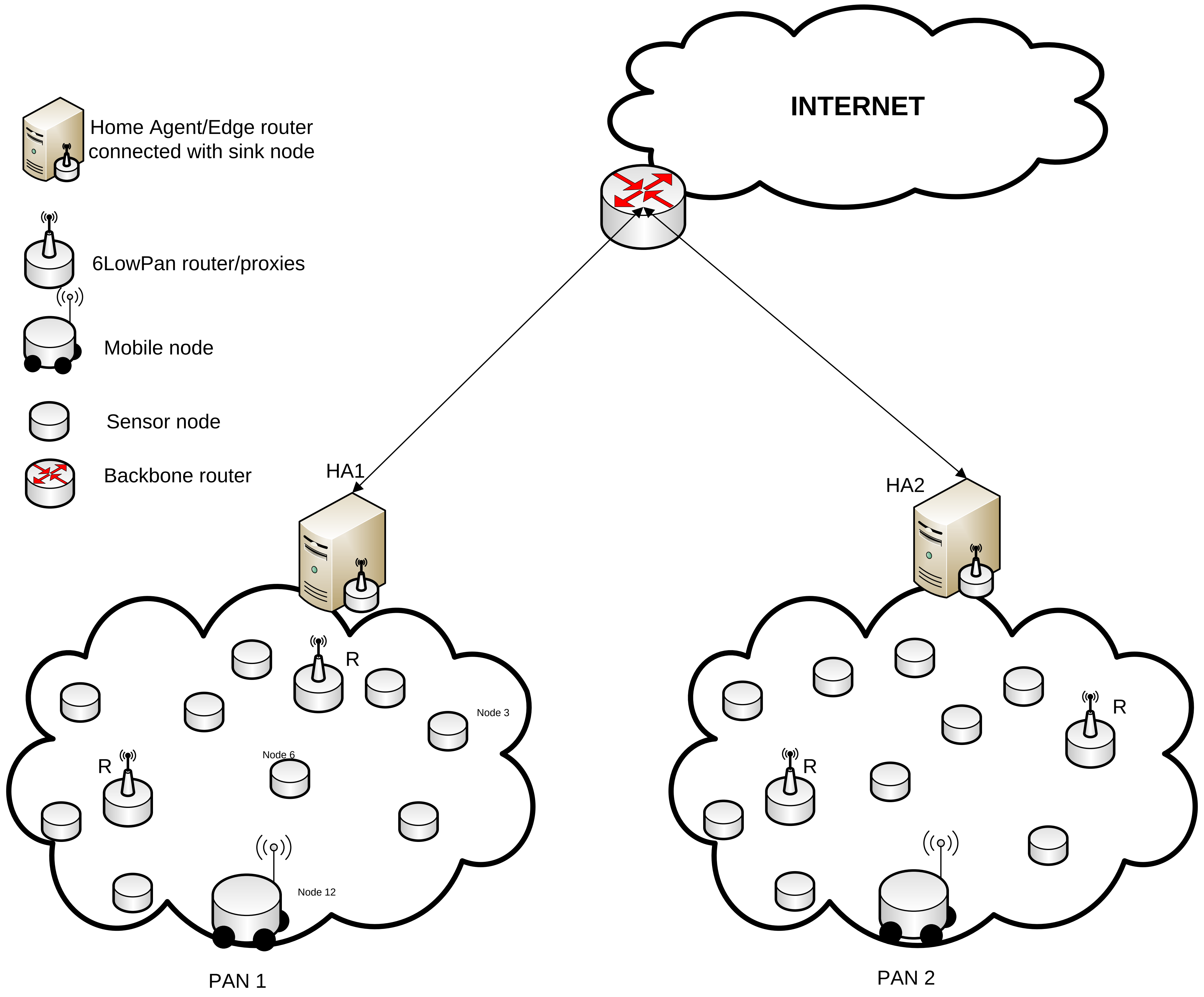
6LoWPAN Mobility Management

- Device movement within a single WPAN domain – Intra or Micro
- Device movement between multiple WPAN domains – Inter or Macro
- Single WPAN movement - NEMO

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

6LoWPAN Mobility Management



6LoWPAN Mobility Management

- “An Adaptation Model for Mobile IPv6 Support in lowPANs,” draft-silva-6lowpan-mipv6-00, 5/2009 (expired)
  - HC1 header compression scheme in order to compressed the MIPv6 mobility header from 6 bytes to 1 byte.

- “6LoWPAN architectural consideration for mobility”, draft-williams-6lowpan-mob-02.txt, work-in-progress, 2010
  - Network mobility support using the NEMO protocol
  - Gateways to support media conversion
  - They provide only some preliminary ideas.

System design: Challenges with various IoT Network protocols

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Special Topics

- Over the Air (OTA) upgrade

- Battery life

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Over the Air (OTA) upgrade

- OTA. Stands for "Over-The-Air." OTA refers to any type of wireless transmission of packages to a host.

- It is widely used to describe firmware or software updates distributed to IoT nodes.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Why to upgrade firmware/software

- Remember mirai attack?
- A DDoS attack with over 600 Gbps of traffic.
- Prime Target was IP Cameras with open telnet ports and default passwords.
- IoT will never be the same again after that.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Over the Air (OTA) upgrade

Problems

- Embedded/Factory software is often with bugs.
- Devices are connected to the Internet allowing vulnerabilities to be exploit by intruders.
- What if we would like to deploy new features, improve performance, make security patches etc?

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Over the Air (OTA) upgrade

Requirements

- Security:
  - There must be an adequate security level to prevent unauthorized access the device.
- Robustness:
  - In a way that the update will not cause any anomalies that would make the node unusable.
- Atomicity:
  - It has to be ensured that the update either will be installed completely or not at all

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

OTA Approaches

- When talking about OTA we have a number of frameworks to work with, the best strategies is aligned with the specifications of the hardware in need for the software update.

- Edge-to-cloud OTA updates: An ECU microcontroller installed in the edge devise can receive firmware OTA packages from a remote server. The package can include upgrades to both the microcontroller's underlying hardware capabilities (FOTA) and updates to applications running on those (SOTA).

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

OTA Approaches

OTA Approach-I

- Gateway-to-cloud OTA updates: An Internet-connected gateway, in charge of managing a set of local edge devices, can receive updates from a remote server. These updates can be aimed at improving all or some of the installed software applications, the app's host environment, and/or the gateway device's firmware.

OTA Approach-II

- Edge-to-gateway-to-cloud OTA updates: An internet-connected gateway manages a group of locally connected edge devices. These devices receive remote firmware updates via the gateway.

Battery Life

- IoT devices are intended to have a 10 years battery life to support massive deployment with limited human intervention.

- Key to achieve higher battery life:
  - Send small amounts of data
  - Send messages less frequently
  - Low Spreading factor (LoRaWAN)
  - PSM and extended Discontinuous Reception (DRX) in NB-IoT.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Battery Life

Small amounts of data

- When the device is made to send small data payload, it means it needs to be powered up for less time.
- Encoding of the data means also less bytes to be sent therefore less time the device is powered up.
- Avoid sending text.

- Example: “Humudity:65%” is 12 bytes
    - Convert 65 to hex and send only the value□ 1 byte

Battery Life

Less frequent

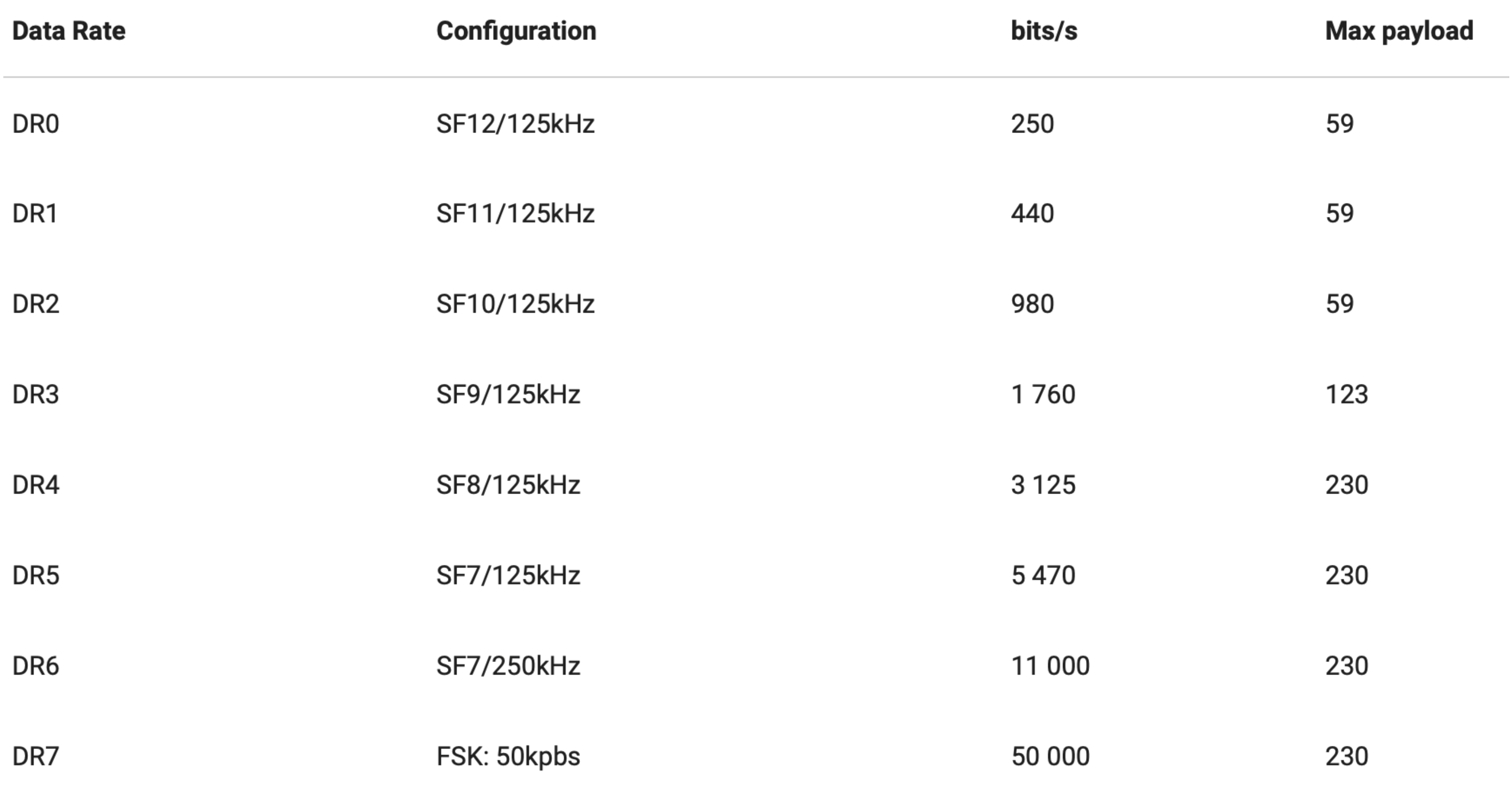
- Send messages less frequently, the device is in it's low power sleeping mode for a longer percentage of time so the battery will naturally last longer.

- When taking readings from sensors especially when you do not expect the values to change frequently, you need to reduce the frequency of the sending messages.

Battery Life

Low Spreading factor

- The spreading factor represents the rate on which the signal changes frequency.
- The spreading factor is expressed as a number ranging from 7 – 12, representing the speed of a frequency change in a chirp
- The spreading factor affects the data transfer rate and demodulation SNR. When data is spread more (a higher spreading factor), it can be demodulated with a lower SNR value.
- It’s clear that higher spreading factors will have a huge effect on battery life
- You want to use the lowest spreading factor as possible.



Data Rate	Configuration	bits/s	Max payload
DR0	SF12/125kHz	250	59
DR1	SF11/125kHz	440	59
DR2	SF10/125kHz	980	59
DR3	SF9/125kHz	1 760	123
DR4	SF8/125kHz	3 125	230
DR5	SF7/125kHz	5 470	230
DR6	SF7/250kHz	11 000	230
DR7	FSK: 50kpbs	50 000	230

Battery Life in NB-IoT devices

- Most significant features of battery-powered NB- IoT devices are:
  - **Power Saving Mode (PSM):** is a deep sleep operation for end device. The PSM mode is activated after the expiration of a timer, which determines for how long the end device will monitor paging before entering in PSM. In the deep sleep state, the device is unreachable by the network but stays registered to it. The energy consumption in this state can be minimized to a level that is even lower than the idle mode.
  - **Extended Discontinuous Reception (eDRX):** is defined in LTE release 13 and it provides longer inactive periods between reading, paging or controlling channels for the end device. Its difference with respect to PSM mode is that the node occasionally enters into receiving mode, waits for inbound messages and the device is reachable by network.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Build a LoRaWAN Network

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

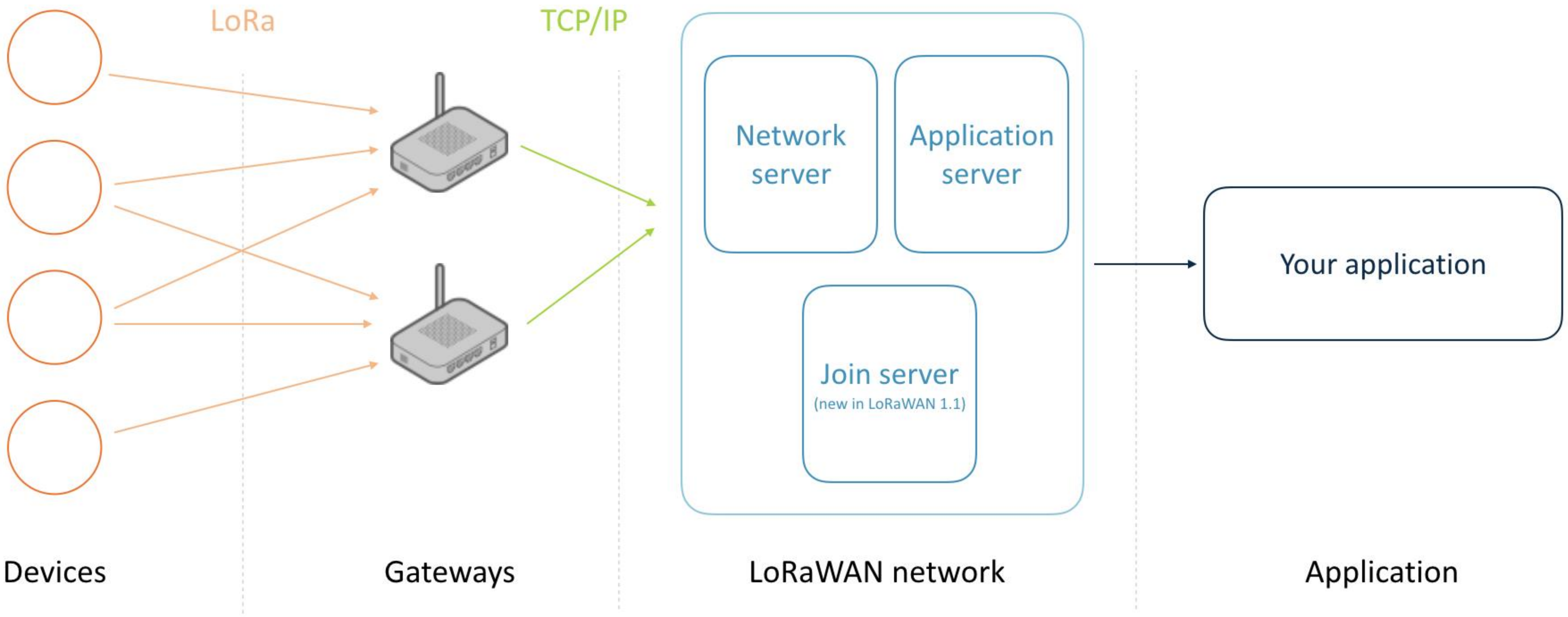
How to build LPWAN

- Components:
  - Hardware:
    - Devices
    - Gateways
  - Software:
    - Firmware
    - Network service
    - Application

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

LoRa Architecture



Devices

- Responsible to collect and transmit the data
- Indoor or outdoor devices
- Not associated with a specific gateway
- These devices could be for example sensors measuring air quality, temperature, humidity, location

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Devices

LoRaWAN CO2 Meter

Monitoring air temperature,
relative humidity and air pressure

Vehicle Detection Sensors

LoRaWAN™ ultrasonic 3D
waste sensor

PULSE SENSOR

Outdoor openings remote
control

LoRaWAN™ outdoor
environmental sensor

Water Level, Electrical
Conductivity and Temperature

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Gateway

- Scan the spectrum and capture LoRa packets
- Forward data to a network service that handles the packet
- Selection of gateway based on the:
  - Cost
  - Type of application
  - Configuration options
  - Features supported

Gateway

- Example of gateways:
  - Kerlink Wirnet station: great build quality and range with Cost of 1,200 euros
  - MultiTech conduit: suitable for smaller setups and cost of 450 euros
  - Raspberry Pi with an IMST iC880A concentrator: At about 150 euros suitable for small private networks
- Find more gateways here

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Lora Server

- Responsible to manage the state of the network.
- Monitors the devices active on the network
- Handle join-requests when devices want to join the network.
- When data is received by multiple gateways, LoRa Server will de-duplicate this data and forward it once to the LoRaWAN application-server.
- When an application-server needs to send data back to a device, LoRa Server will keep these items in queue, until it is able to send to one of the gateways.
- LoRa Server provides an API which can be used for integration or when implementing your own application-server.

Lora Application

- The end-application handles the application-payloads sent by the devices.

- It receives this data from LoRa Server, using one of the possible integrations (e.g. MQTT, HTTP or directly write to a database).

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Summary

- ❑ Introduction
- ❑ Communication and Network Protocols in IoT:
  - ❑ LoRAWAN
  - ❑ NB-IoT
  - ❑ 6LoWPAN
- ❑ System design: Challenges with various IoT Network protocols:
  - ❑ Battery Life
  - ❑ Over the Air (OTA) upgrade
- ❑ Build a LoRaWAN Network

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423