Wireless Protocols for Critical IoT

UE Critical IoT and Factory of the futur

Katia Jaffrès-Runser

ENSEEIHT, kjr-at-n7.fr

Département Sciences du Numérique
3ème année - Parcours SEmbIIoT

2020-2021

Course structure

1. Wireless networks in Industry
   - Wireless in Industry
2. Wireless protocols and Determinism
   - WiFi and determinism
   - Bluetooth and determinism
   - 802.15.4 and determinism
3. TSCH - Time Slotted Channel Hopping
4. IP over TSCH : 6TiSCH.
   - 6TiSCH protocol stack
   - Allocation of slots
5. Routing for low power and lossy networks
   - RPL protocol
   - Trickle timer
6. Elements of 5G for Industry

Course structure

1. Wireless networks in Industry
   - Wireless in Industry
2. Wireless protocols and Determinism
   - WiFi and determinism
   - Bluetooth and determinism
   - 802.15.4 and determinism
3. TSCH - Time Slotted Channel Hopping
4. IP over TSCH : 6TiSCH.
   - 6TiSCH protocol stack
   - Allocation of slots
5. Routing for low power and lossy networks
   - RPL protocol
   - Trickle timer
6. Elements of 5G for Industry

Wireless networks in Industry

Wireless networks are present in the industry for many years, now, but mostly to carry non time-sensitive data :

- Internet access (cloud, web, email)
- Administration, sales, finance, etc.

Wireless networks :

:-) offer easy access to the network to mobile users, and a

:-) offer simplified deployment for the company.

:-(are prone to data loss (interference, collisions, etc.)

:-(may more vulnerable to security attacks

Wireless networks in Industry

Factory of the future

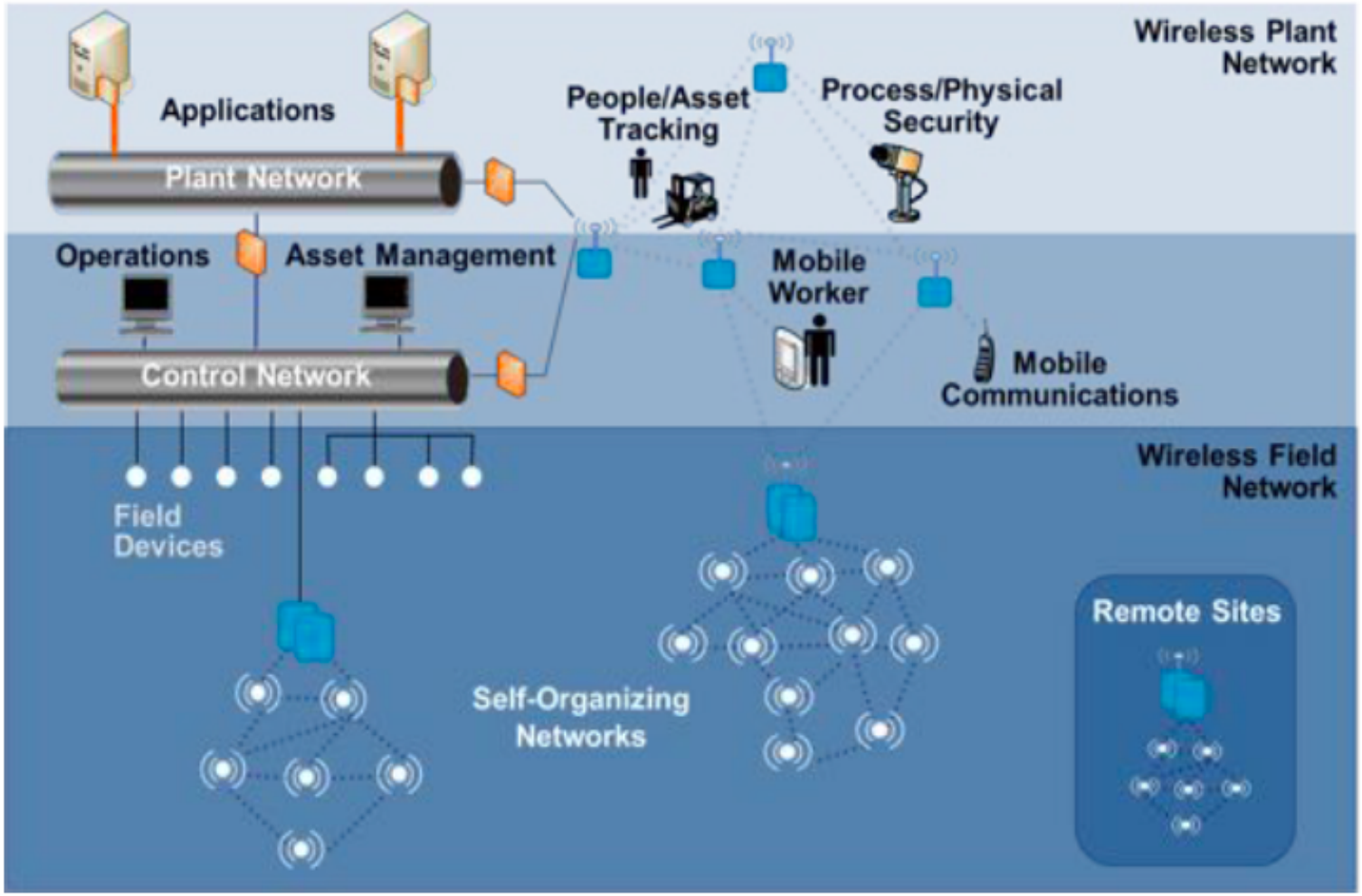
Currently, networks deployed in plants, factories, hospitals, etc. are meant to **converge to Internet**.
This to :

- Optimize processes at short term (predictive maintenance, production planning, etc.)
- Gather enough data to better invest its assets and improve productivity on the long term.

In this context, wireless networks will be deployed to monitor production using the new ** *Internet of Things - IoT* ** technologies.

Wireless networks in Industry

Networking in operational technology



Source : Pascal Thubert, Cisco [5]

Industrial IoT (IIoT) : expected benefits of 1%

Table 1: Industrial Internet: The Power of 1 Percent

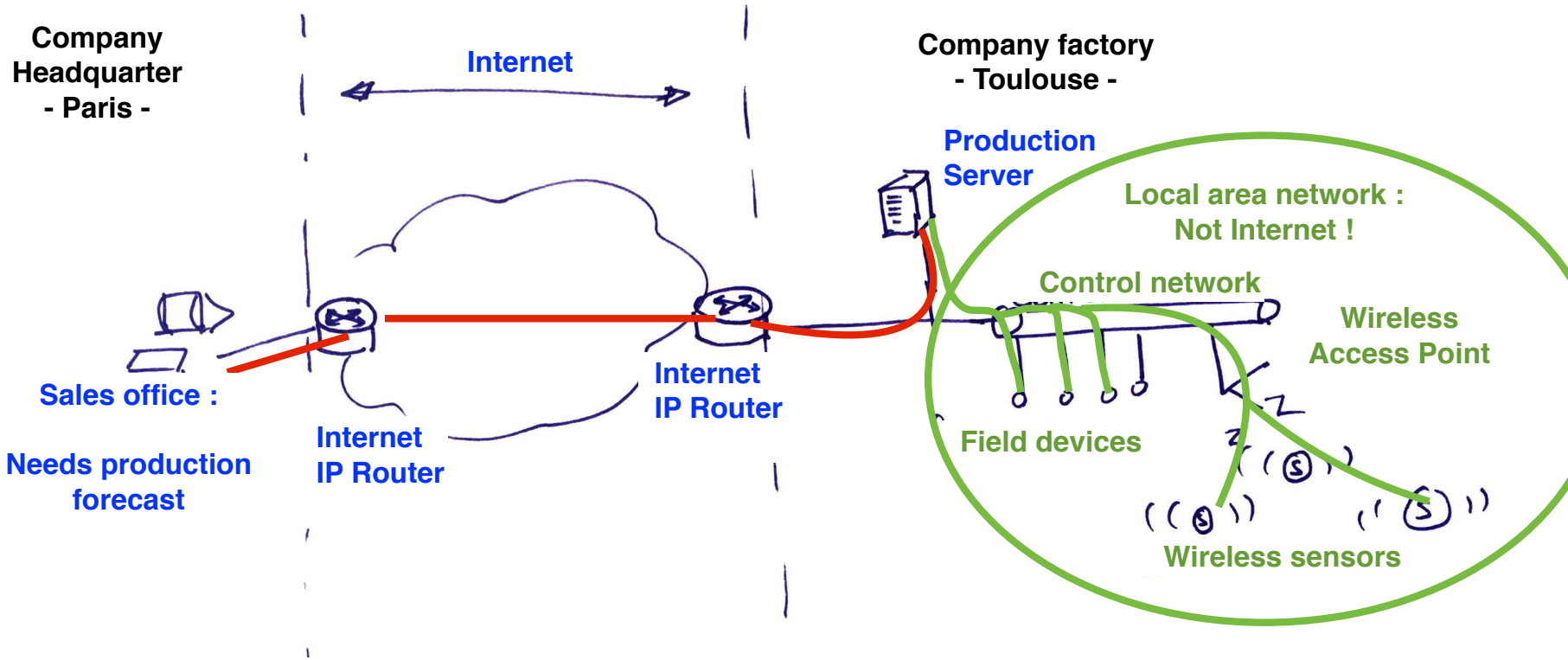
What if... Potential Performance Gains in Key Sectors			
Industry	**Segment**	**Type of Savings**	**Estimated Value Over 15 Years** (Billion nominal US dollars)
Aviation	Commercial	1% Fuel Savings	$30B
Power	Gas-fired Generation	1% Fuel Savings	$66B
Healthcare	System-wide	1% Reduction in System Inefficiency	$63B
Rail	Freight	1% Reduction in System Inefficiency	$27B
Oil & Gas	Exploration & Development	1% Reduction in Capital Expenditures	$90B

Note: Illustrative examples based on potential one percent savings applied across specific global industry sectors.
Source: GE estimates

Source : GE Automation [4]

Before Industrial IoT

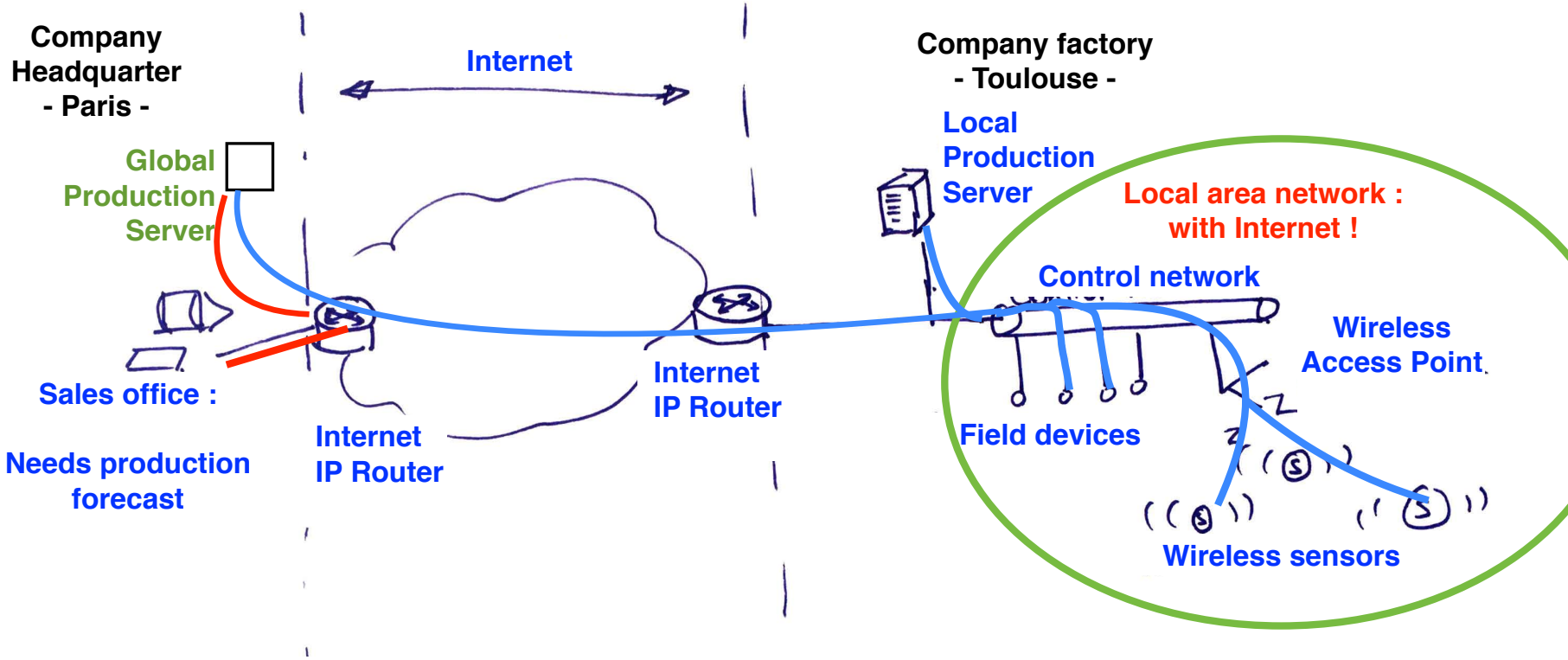
Production networks were isolated from Internet



Field devices are connected to field buses (CAN, TTP-C, etc.) discussing with production servers.

With Industrial IoT

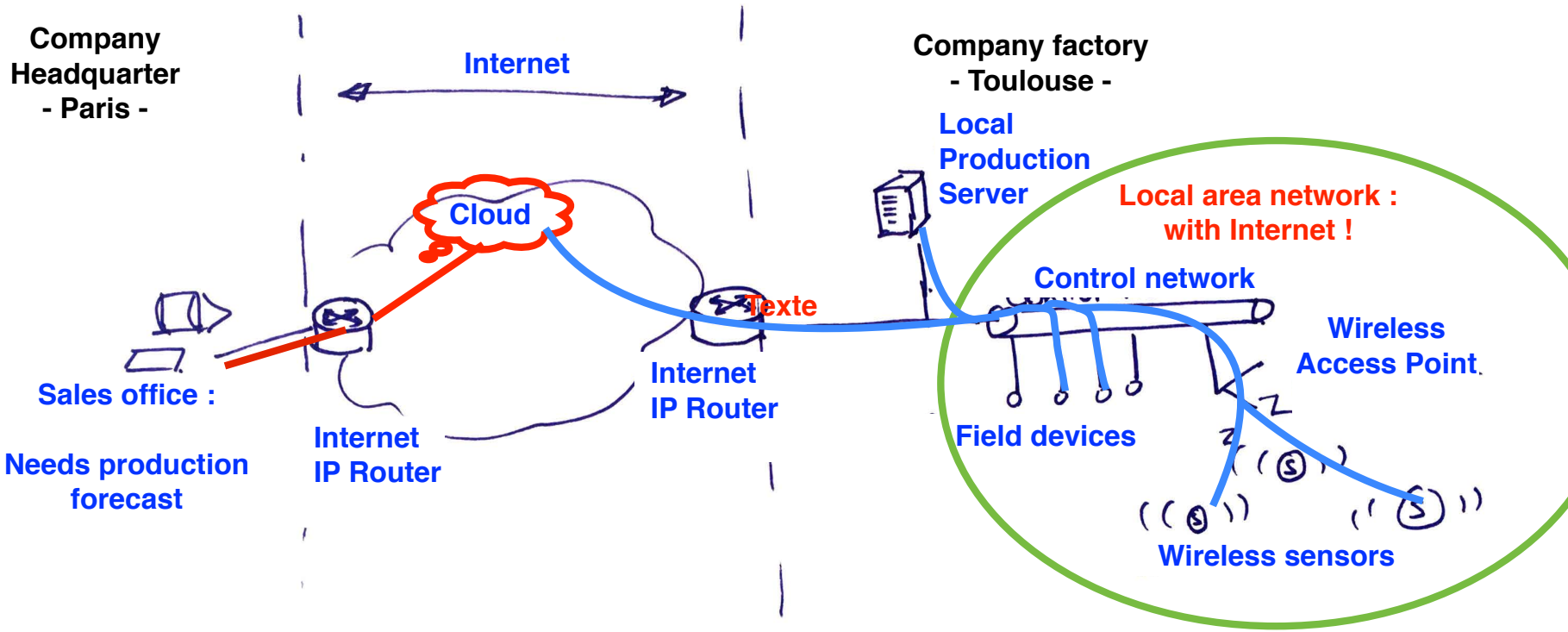
Production networks will be ** integrated ** to Internet



Field devices have an IP address as well and can understand IP protocol. The layer 2 (MAC protocol) may be a legacy field bus, but most often newer ones that are better suited to carry IP messages.

With Industrial IoT and Cloud IoT Platform

Production networks and the ** Cloud **



Here, production data not located in the enterprises' premises : all data is collected in an IoT platform in the Cloud.
Elastic storage and advanced services are offered by this IoT platform to simplify the server setup to companies.

Industrial Internet of Things (IIoT)

To converge these networks to IP, we have to keep them as efficient as of today but with IP connectivity :

- Make **IP more efficient** in this context (small data, QoS provision, offer determinism, etc.) ;
- Address **numerous objects** using IPV6, and thus compress the 40 bytes fixed header to carry the 2 or 4 bytes of raw data.
- Offer {determinist / non-determinist} {wired / wireless IP} connectivity, and inter-connect all technologies on the factory floor.

Industrial IoT

Networking in operational technology

Two types of services :

1. Control loops and movement detection : *Deterministic*, fixed latency and ressource allocation, static multipath, currently wired (CAN, TTEthernet, TSN, DetNet) but wireless is considered in research.
2. Large scale monitoring : *Stochastic*, self-healing, distributed routing, currently use wireless solutions (6TiSCH, WirelessHART, etc.).

Wireless protocols for real-time

Requirements

For real-time operations, a protocol has to offer :

- Determinism : always offer the same service guaranty in terms of **end-to-end latency** that has to be **upper bounded** ;
- **Extremely low data loss** rates ;
- Transport of **unicast or multicast** data streams of **different bandwidth**.
- Offer **differentiated services** to maybe carry both real-time flows with non real-time ones.

Wireless protocols for real-time

Requirements : the case of wireless protocols

For real-time operations, a protocol has to offer :

- Determinism : always offer the same service guaranty in terms of **end-to-end latency** that has to be **upper bounded**
  Requires a time slotted medium access for MC flows ;
- [DIFFICULT] Extremely low data loss rates ;
- Transport of **unicast or multicast** data streams of **different bandwidth**.
- Offer **differentiated services** to possibly carry both real-time flows with non real-time ones.

Inherent complexity of wireless

Challenges

Complexity of transferring data in wireless originates from :

- **Hidden Node problem**
  Received power is strongly attenuated. Attenuation is inversely proportional to the square of the distance between source and destination : $P_r = P_t \frac{1}{k.d^n}$, with $n \geq 2$.
  Thus, some nodes in the network may not hear an ongoing communication, and start emission after listening to the medium and thinking no-one is sending.
- **Inside network Interference**
  As these nodes start transmission, they add interference (seen as noise) to the ongoing communication, and the signal at the receiver can't be demodulated. This is also called a **collision**.
  Moreover, interference is additive, thus the power created by multiple ongoing communications can interfere another one (say C), even if individually, each ongoing communication doesn't interfere communication C.

Inherent complexity of wireless

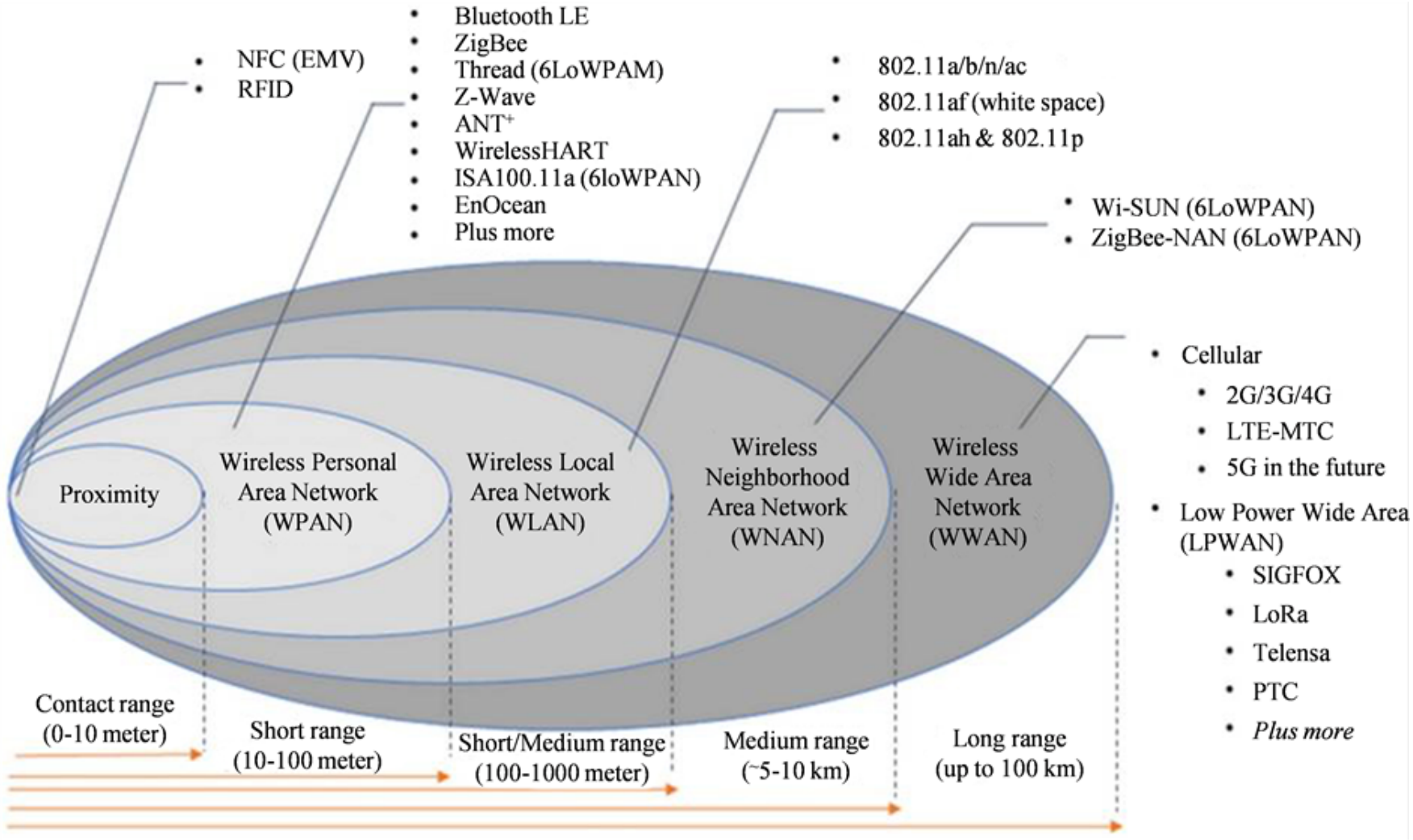
Challenges

- **Outside network interference :**
  Transmissions of nodes that belong to other networks using the same frequency bands causes interference as well.
  This type of interference is particularly difficult to forecast as you have no control over it.

Course structure

1. Wireless networks in Industry
   - Wireless in Industry
2. Wireless protocols and Determinism
   - WiFi and determinism
   - Bluetooth and determinism
   - 802.15.4 and determinism
3. TSCH - Time Slotted Channel Hopping
4. IP over TSCH : 6TiSCH.
   - 6TiSCH protocol stack
   - Allocation of slots
5. Routing for low power and lossy networks
   - RPL protocol
   - Trickle timer
6. Elements of 5G for Industry

Plethora of wireless technologies !



source : http ://file.scirp.org/Html/1-4000110_65802.htm#txtF3

In numbers

Nom	WiFi	Bluetooth	ZigBee
Standard	IEEE802.11	IEEE802.15.1	IEEE802.15.4
Range (free space)	125m	100m	10-100m
Data rate	450 Mbps 802.11n	up to 2Mbps	250 kbps
Lifetime (AA)	4-8h / 50h idle	60h in activity	60h / few days idle

Nom	6TiSCH/TSCH	LPWAN
Standard	IEEE802.15.4 e	SigFox, LoRa
Range (free space)	10-100m	100 km
Data rate	250 kbps	27 kbps
Lifetime (AA)	similar to ZigBee	10-20 years

Main types of wireless architectures

- Star architecture
  - A central access point that controls communications and connects stations to core network ;
  - Stations can't talk directly together, they an only talk to the central access point.
- Meshed architecture
  - Multi-hop communications ;
  - Part of the nodes can route messages ;
  - Requires a routing protocol.
- Hybrid architecture
  - Several controllers forming a mesh network ;
  - Each controller is the controller of stations in a star topology.

Wireless and Determinism : challenges

- Physical layer : account and mitigate the negative effects of pathloss, fading, external interference.
- Medium access : hidden / exposed terminal - determinism is necessary in the MAC protocol (TDMA, polling, token-based) - synchronisation service.
- Routing : multi-hop / mesh to reduce energy ; multi-path to improve reliability ; control congestion at relay nodes.

Off-the-shelf wireless solutions for real-time IoT ?

Are mainstream technologies suited for determinism ?

What about these technologies :

- IEEE802.11 (aka WiFi) ?
- IEEE802.15.1 (aka Bluetooth) ?
- IEEE802.15.4 (aka Zigbee) ?

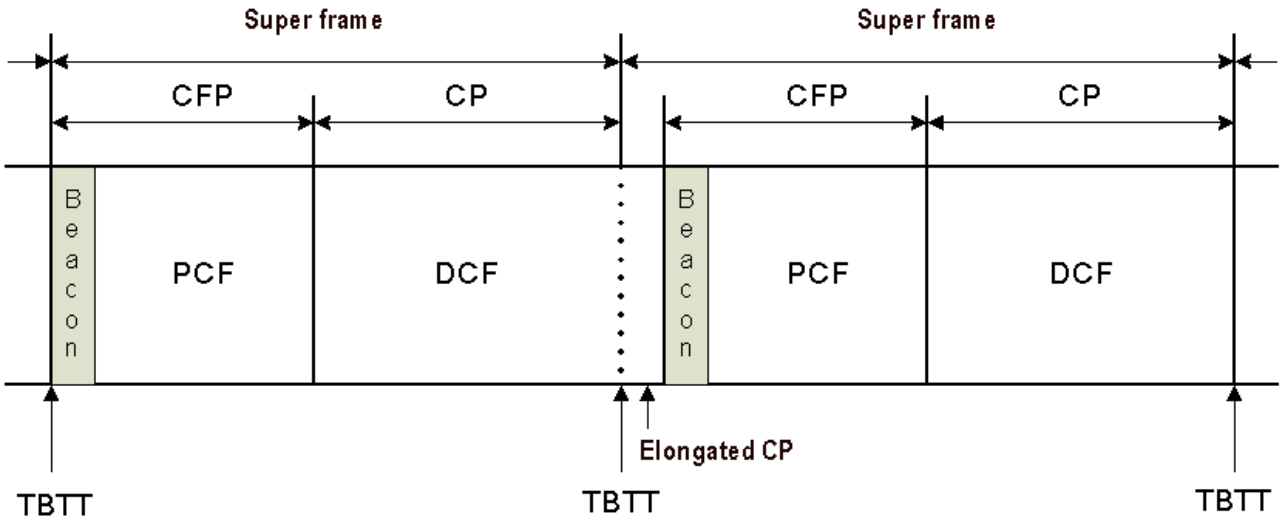
WiFi - IEEE802.11

In short

- Several standard evolutions : IEEE802.11a, b, g, e...
- ISM 2.4GHz - spread spectrum DSSS / **OFDM**
- MAC protocol defines two modes of operations :
  - DCF : Distributed coordination function
  - PCF : Point coordination function - Barely available in commercial products
- DCF : CSMA/CA with exponential backoff : [non-deterministic by design]
  - IFS : Inter-Frame Space
  - CCA : Clear Channel Assignment
  - RTS/CTS : combat hidden terminal problem

PCF mode

- Works for PCF stations, and coexists with DCF-only stations.
- Creates a period of time where the access point leads all communications by polling all PCF-enabled stations.
- Time is a sequence of super-frames of variable size divided into :
  - *Contention Free Period* (CFP) where AP polls all PCF stations ;
  - *Contention Period* (CP) where regular DCF is used.
- CFP starts with a beacon that announces PCF mode start, and makes DCF-only stations be quiet for PCF duration.



WiFi and determinism

PCF mode and determinism

Points in favor :

- Polling of stations is deterministic : only one station speaks
- DCF-only stations can't access the channel.

Points against :

- A PCF station that wants to access CFP has to request it during the CP period [possible loss or delayed request].
- CFP starts only when the beacon of the AP has won channel access over all possible DCF stations.
  [Non-deterministic start time of CFP].
- High emission power (20dB) : increased multi-path.

WiFi and determinism

Improved MAC protocols for QoS

Introduced in IEEE802.11g amendment

- HCF (*Hybrid Coordination Function*) : Time slot allocation by controller, but points agains not solved.
- EDCF (802.11e) : introducing QoS in DCF but still non-deterministic.

Bluetooth - IEEE802.15.1

- Architecture
  - 1 piconet : 1 controller of up to 7 stations
  - 1 controller can belong to up to 4 piconets, but controls only one piconet
  - Set of piconets = scatternet
- Physical Layer : GMSK at 1Mbits/s (v1.2) à 24Mbits/s (v3.0)
- Link layer (L2CAP) offers 2 possible services :
  - ACL : Asynchronous Connection Less
    ARQ, 6 types of paquets (encoded or not)
  - SCO : Synchronous Connection Oriented
    Real time : a periodic reservation of time slots. No ACK
- MAC layer : controller polls its stations in TDMA mode.
  Slots of $T_{slot} = 625\mu s$, in duplex mode :
  - Controller transmits in *odd* time slots ;
  - Station responds in *even* time slots if polled by the controller in previous slot.

Bluetooth and Frequency hopping

Frequency hopping

For out of band interference mitigation and piconet cohabitation (piconets aren't sync'ed).

- Frequency band divided into 79 channels of 1MHz ;
- Channel change every time slots - (i.e. every 625μs).
- Channel sequence known from all devices.

Version 1.2 : AFH : Adaptive Frequency Hopping

- Exclusion of channels with high frame loss rate

Bluetooth and Determinism

Points in favour

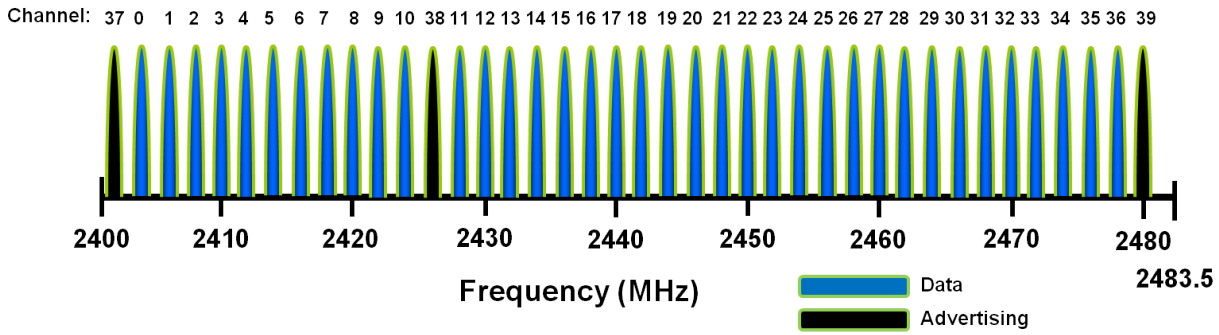
- TDMA with polling.
- Adaptive frequency hopping

Points against

- Device pairing takes time (non deterministic) : needs to find the current channel to communicate with the controller,
- Piconets are small (max 8 nodes)
- Scatternets are not sync'ed - messages can be lost.

Changes w.r. to Bluetooth

Faster connection of the devices to the controller.

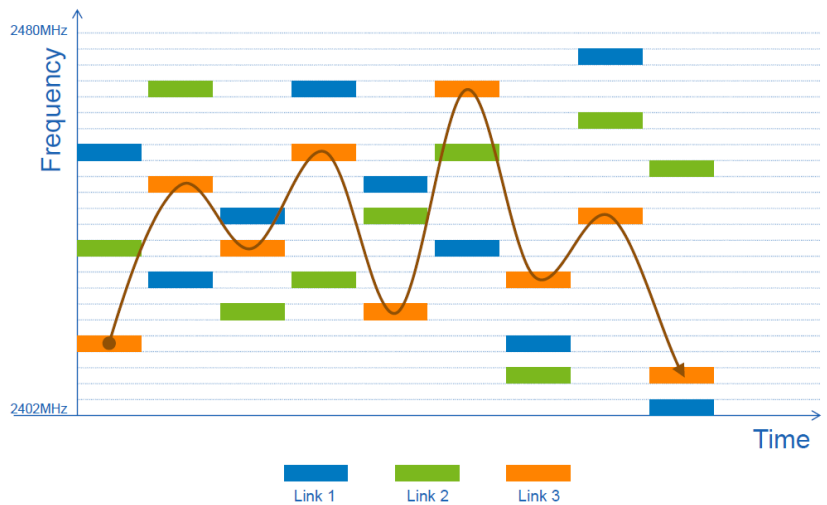


- Frequency band divided into 40 channels of 1MHz ; channel change every 625μs time slot.
- New **advertising mechanism** :
  - 2 types of nodes : **advertiser** node and **scanner**.
  - The advertiser beams `ADV_IND` messages on channels 37, 38 or 39.
  - The scanner device chooses the advertiser it wants to connect to by listening to these 3 channels.
  - Scanner device requests connection with `CONNECT_IND` frame that contains frequency hopping sequence information.

Source : `http://microchipdeveloper.com/wireless:ble-phy-layer`

Changes w.r. to Bluetooth

- 1 Mbps to 2 Mbps data rate per link, 40-300m range, up to 10mW.
- Client/Server : Client is the controller that polls the server (sensor). Sensor exposes state.
- Asynchronous connection-less MAC, used for low latency, fast transactions (i.e. $3ms$ from start to finish).
- Frequency hopping : $f_{n+1} = (f_n + h) \mod 37$,



where $h \in \{5, \ldots, 16\}$ assigned at connection for each link. Adaptive Frequency Hopping is performed as well.

BLE and Determinism

Points in favour

- TDMA with polling.
- Adaptive frequency hopping
- Reduced connection and pairing operations thanks to advertising channels

Network extension

- Bluetooth Mesh extension : offers a message-flooding service across a meshed network topology.

Course structure

1. Wireless networks in Industry
   - Wireless in Industry
2. Wireless protocols and Determinism
   - WiFi and determinism
   - Bluetooth and determinism
   - 802.15.4 and determinism
3. TSCH - Time Slotted Channel Hopping
4. IP over TSCH : 6TiSCH.
   - 6TiSCH protocol stack
   - Allocation of slots
5. Routing for low power and lossy networks
   - RPL protocol
   - Trickle timer
6. Elements of 5G for Industry

IEEE802.15.4 for sensor networks

Design objectives

1. Interconnect sensors with wireless to retrieve their data.
2. Energy savings : lifetime extension - several years with AA battery
3. Simple hardware (small MCU, low memory) : simple networking operations

Consequences

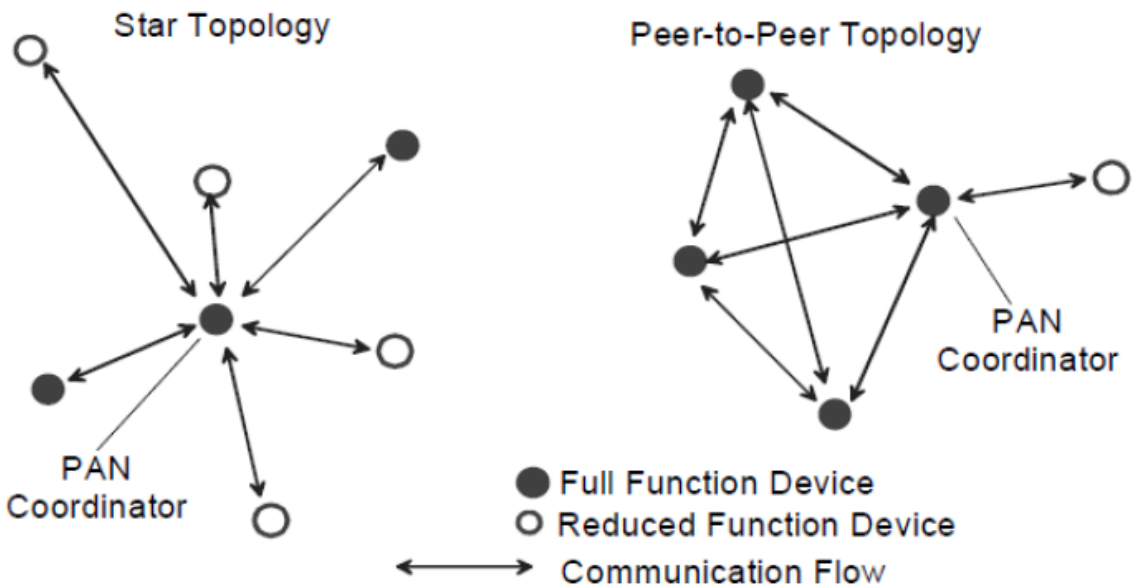
1. Small payload : maximum **127 bytes**.
2. Power from 0 to 10dBm (1 to 10mW)
3. Long inactivity period. Collect data every minute or hour.
4. Simple modulation/PHY layer, low speed : **250kbps**.

IEEE802.15.4 for sensor networks

Tailored for sensor networking

Originally leveraged by the ZigBee consortium (2000's). Works as well in ISM 2.4GHz / 925 MHz.

- Types de terminaux :
  - FFD (*Full Function Devices*). Controller, talks to RFDs and FFDs.
  - RFD (*Reduced Function Devices*). Only talks to FFD.
- An FFD and its associated devices creates a **Personal Access Network (PAN)**. The FFD initiating the PAN is the PAN coordinator.



Extended mesh topology

Several PANs are interconnected using FFDs. The first PAN coordinator is in charge of the complete cluster tree management.

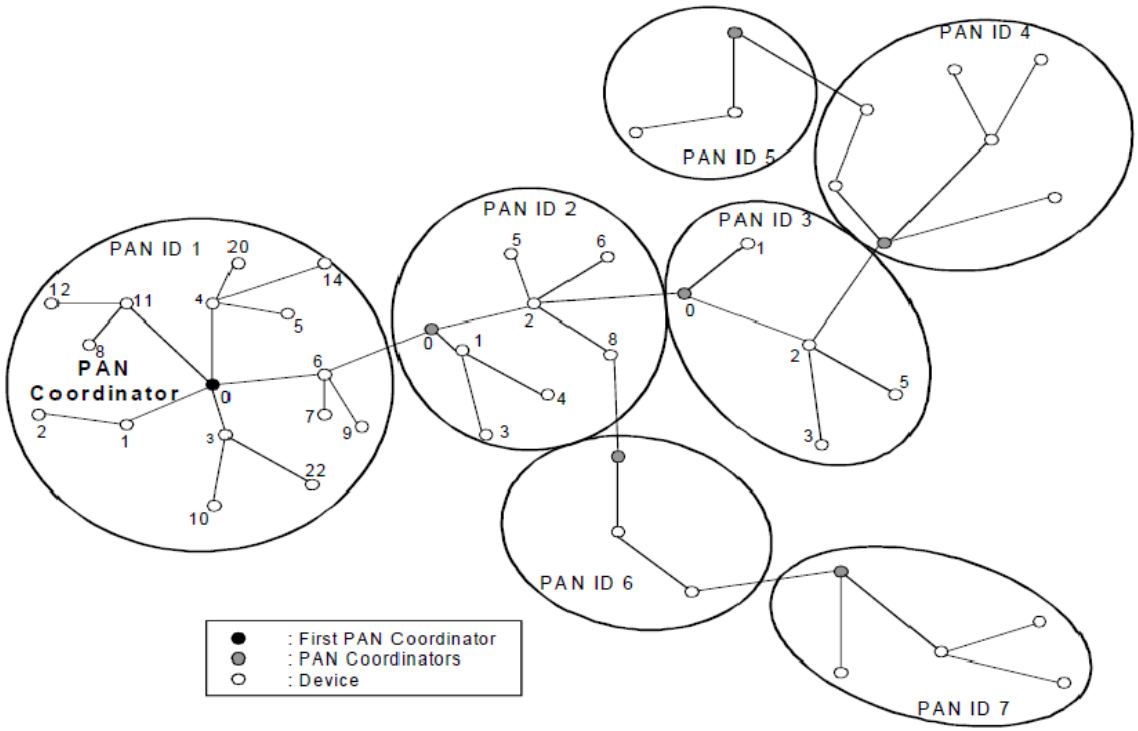


Figure 5-2—Cluster tree network

Each line represents a parent-child relationship in this figure.

Medium access for low power

Most of the traffic is converge-cast : data of sensors converges to the PAN coordinator.

- Defines different modes :
  - Beacon-enabled modes, where beacons emitted by the PAN coordinator delimit operations.
  - Non-beacon mode, where nodes use unslotted CSMA/CA with exponential backoff.

Unslotted CSMA/CA - Frame

A frame is emitted in non-beacon mode :

- by the device to the PAN coordinator when she needs it.
- by the PAN coordinator to the device after the device requests access to a pending frame.

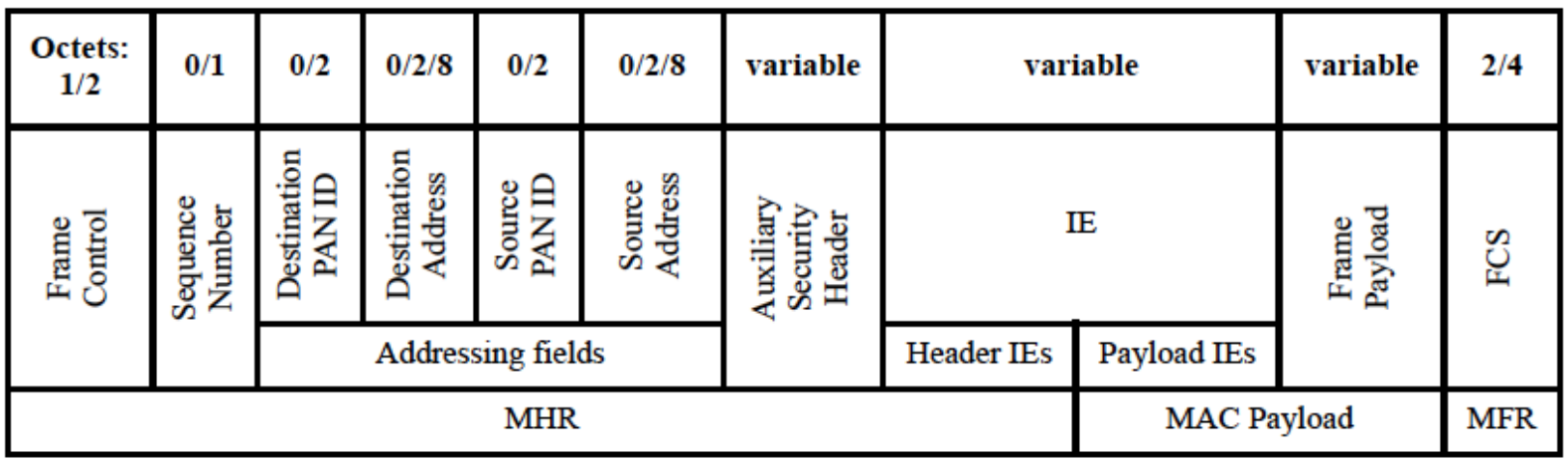


Figure 7-1—General MAC frame format

An Information Element (IE) is a key/value pair representing either control data (header IE) or payload (payload IE).

Beacon enabled modes

Several modes exist, :

- **Super-frame with Guarantied Time Slots (GTS).**
- DSME multi-superframe structure.
- **TSCH slotframes : Time Slotted Channel Hopping.**
- RFID (radio frequency identification blink)
  etc...

We will detail the GTS mode (legacy) and the TSCH mode in this class.

Duty-cycling

All modes may offer portions of time where nodes are **inactive** for **energy saving** purpose. During inactivity, devices can go to deep sleep mode. It is usually characterised with the **duty cycle** of the radio, i.e. the percentage of time the radio is up (transmission or reception).

IEEE802.15.4 - beacon enabled modes

The super-frame structure of GTS mode.

It is composed of a Contention Access Period (CAP), a Contention Free Period (CFP) and an inactivity period (optional).
A GTS is allocated by the PAN coordinator to the devices requesting access in the previous super-frame CAP period using CSMA/CA.

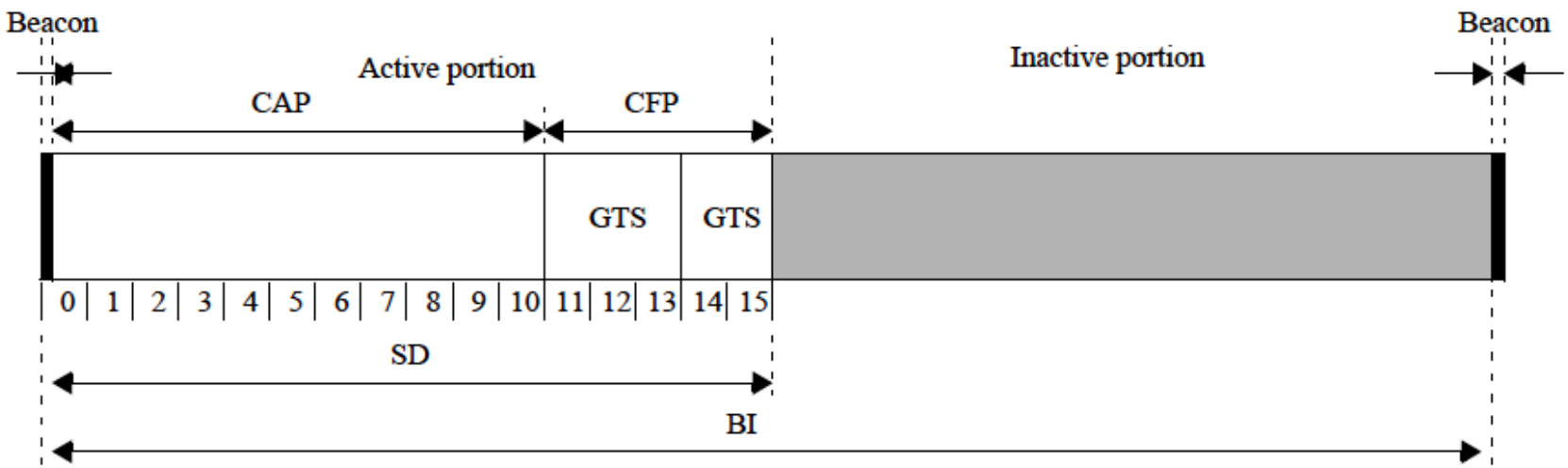


Figure 6-1—An example of the superframe structure

A GTS can last several slots.

IEEE802.15.4 - beacon enabled modes

Beacons.

They are sent periodically over time by a PAN coordinator to :

- offer new nodes the opportunity to enter the network.
- advertise the PAN Id, PAN coordinator address, the Beacon Interval (BI), the Superframe Duration (SD), the GTS allocation, etc.
- synchronise the network (count superframe number, include IE with timing information)

IEEE802.15.4 - beacon enabled modes

Octets: 2	1	4/10	variable	2	variable	variable	variable	2/4
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	Superframe Specification	GTS Info	Pending address	Beacon Payload	FCS
MHR				MAC Payload				MFR

Figure 7-5—Beacon frame format

The Enhanced Beacon frame is differentiated from the Beacon by the frame version being set to 0b10. The MAC frame for the Enhanced Beacon frame shall be formatted as illustrated in Figure 7-6.

Octets: 2	0/1	variable	variable	variable		variable	2/4
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	IEs		Beacon Payload	FCS
				Header IEs	Payload IEs		
MHR				MAC Payload			MFR

Figure 7-6—Enhanced Beacon frame format

IEEE802.15.4 - beacon enabled modes

If FFD X belongs to 2 PANs, and coordinates one of them

FFD X has to maintain timing such as to avoid the emission of a super-frame that overlaps with its parent's super-frame.

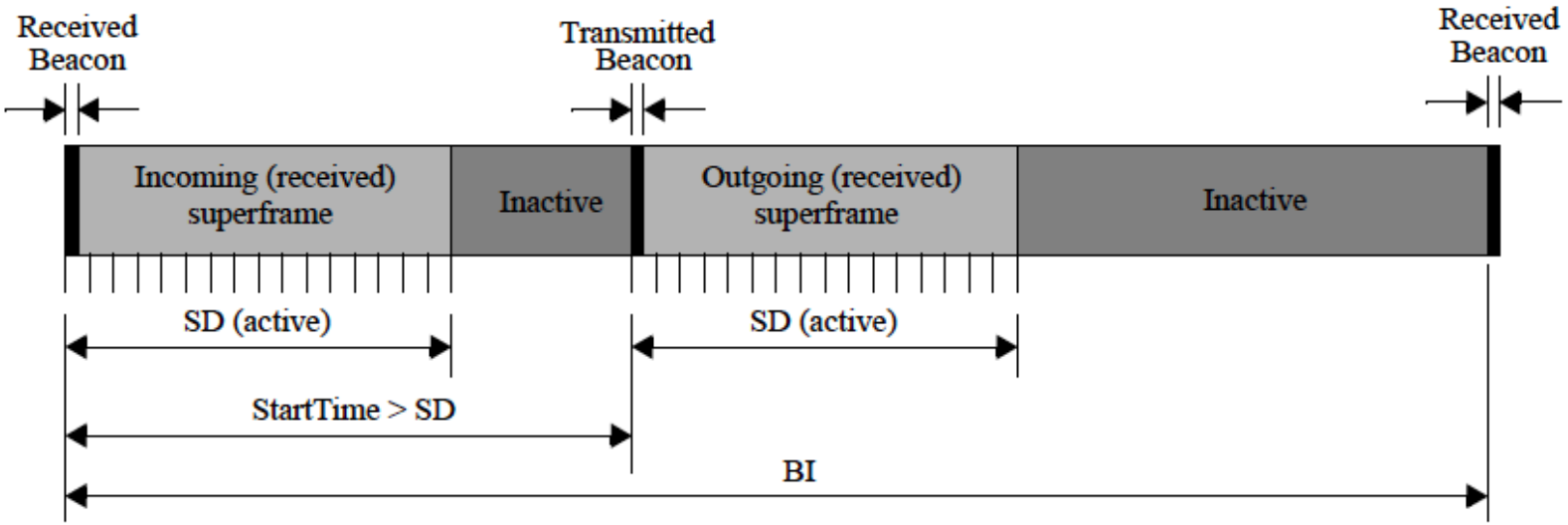


Figure 6-2—The relationship between incoming and outgoing beacons

The StartTime of the super-frame of X must be set after the activity period of its parent's super-frame.

IEEE802.15.4 GTS mode and Determinism

Points in favour

- Transmission in GTS are deterministic.
- Reduced energy expenditure.
- Mesh topology.

Points against

- No frequency hopping.
- Request for GTS in made with CSMA/CA in the CAP. Non-deterministic channel access :-(

Course structure

1. Wireless networks in Industry
   - Wireless in Industry
2. Wireless protocols and Determinism
   - WiFi and determinism
   - Bluetooth and determinism
   - 802.15.4 and determinism
3. TSCH - Time Slotted Channel Hopping
4. IP over TSCH : 6TiSCH.
   - 6TiSCH protocol stack
   - Allocation of slots
5. Routing for low power and lossy networks
   - RPL protocol
   - Trickle timer
6. Elements of 5G for Industry

Chronology

Towards a deterministic wireless MAC

- 1997 : Smart Dust vision
- 2004 : First wireless sensor network standard : IEEE802.15.4, non-beacon and GTS modes.
- 2007 : WirelessHART, industrial standard. First time-slotted commercial solution
- 2009 : ISA.100.A (US version of Wireless HART)
- 2011 : IEEE802.15.4e - TSCH mode.

IEEE802.15.4e is now included in the 2015 version of IEEE802.15.4.

IEEE802.15.4**e** : Time Slotted Channel Hopping

The "e" amendment

- Offers a deterministic link layer to sensor networks,
- Released in Feb. 2012, and included in the 2015 version of the 802.15.4 standard,
- Known as *TiSCH* for
  - Time Slotted
  - Channel Hopping
- Still 127 bytes payload max, 0-10dBm power & same PHY layer.
- Data rate
  - of 250 kbits/s in the 2450 MHz, 915 MHz, 780 MHz or 2380 MHz bands
  - of 100 kb/s when operating in the 868 MHz band

TSCH mode : Time Slotted Frequency Hopping

A time-triggered solution for wireless.

- Nodes are synchronised with microseconds accuracy to define :
  - a time slot of typically 10ms duration
  - with a guard interval of 1ms

Each slot :

- is numbered with an *Absolute Slot Number* (ASN) since the start of the network
- allows the transmission of a 127byte maximum DATA frame with ACK, at 250kbps.

Time Slotted Channel Hopping

Transmission in a slot

The duration for a timeslot is enough for emitting a frame of size max and an optional ACK.

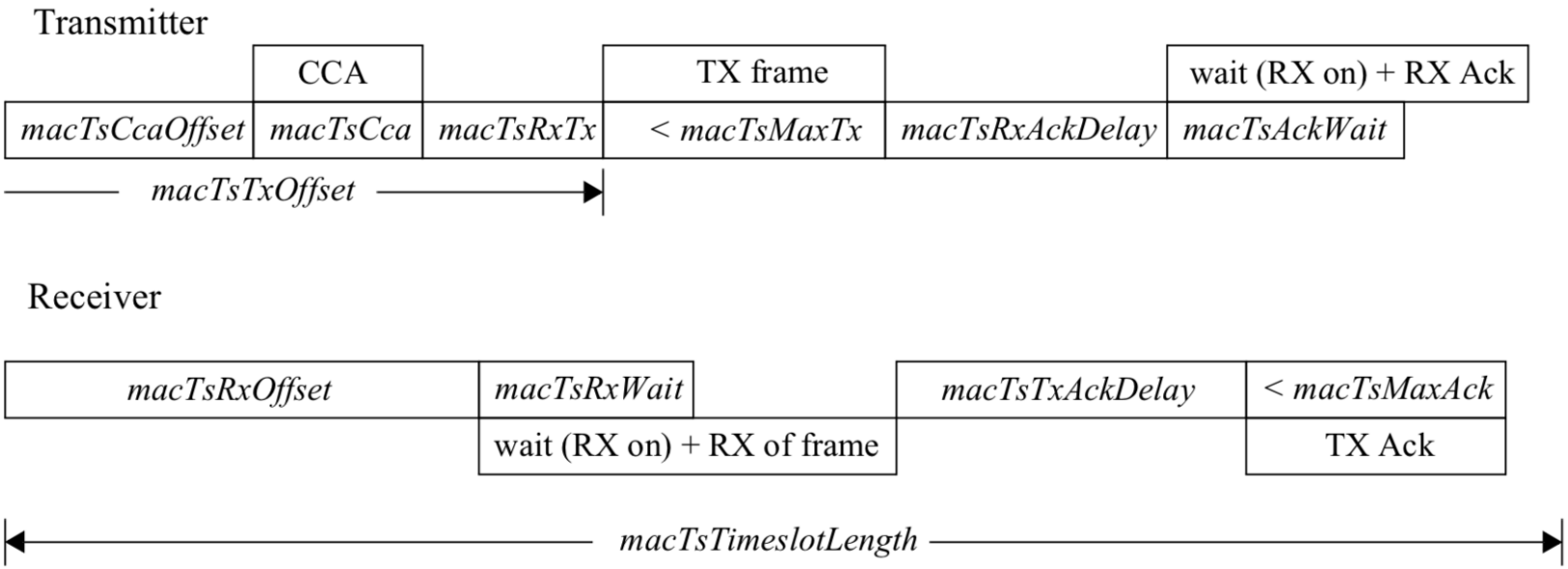


Figure 6-30—Timeslot diagram of acknowledged transmission

At 250kbits/s, it takes around 4ms to send one 127 byte-long frame.

TSCH mode : Time Slotted Frequency Hopping

Medium Access Control

A time slot can be

- **shared** : the slot is shared between multiple communications. Access is handled with a CSMA/CA protocol.
- **guaranteed** : the slot is assigned to a **unidirectional communication** between a transmitter and a receiver node.

TSCH mode : Time Slotted Frequency Hopping

The slotframe

Time slots are grouped into a slotframe of fixed size. The slotframe size is known from all nodes and advertised in the beacons emitted by the PAN coordinators. (cf. 6.2.6 in IEEE802.15.4(2015))

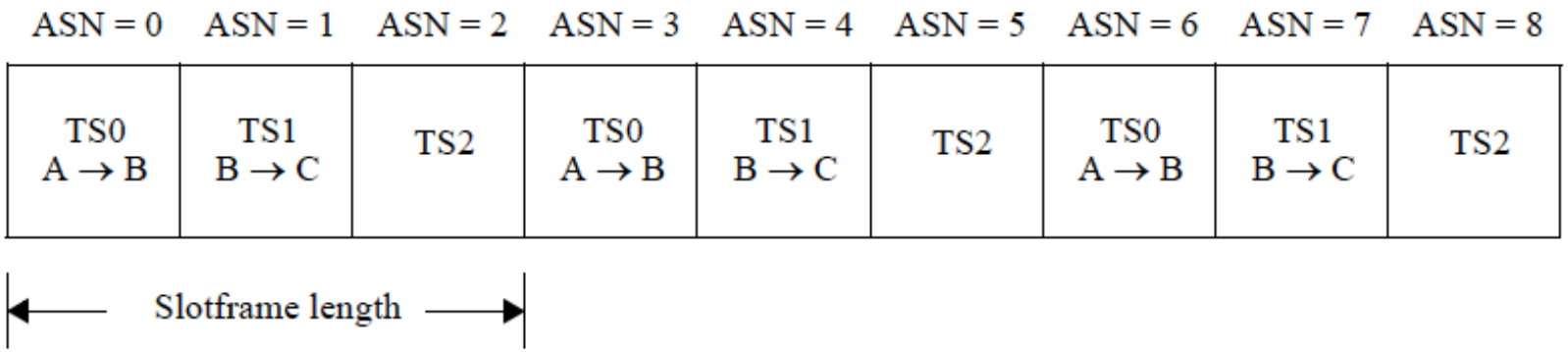


Figure 6-9—Example of a three time-slot slotframe

The slotframe is stored in a *macLinkTable* that lists all active timeslots and the type of link (TX only, TX/RX, TX shared, etc.).

TSCH mode : Time Slotted Frequency Hopping

Channel hopping

There are 16 channels in the 2400–2483.5 MHz band.
They are used for channel hopping to increase robustness against external interference and persistent multi-path fading in industrial environments.
Each slot is assigned the following channel identifier :

$$CH = Sequence[(ASN + ChannelOffset)\%SequenceLength]$$

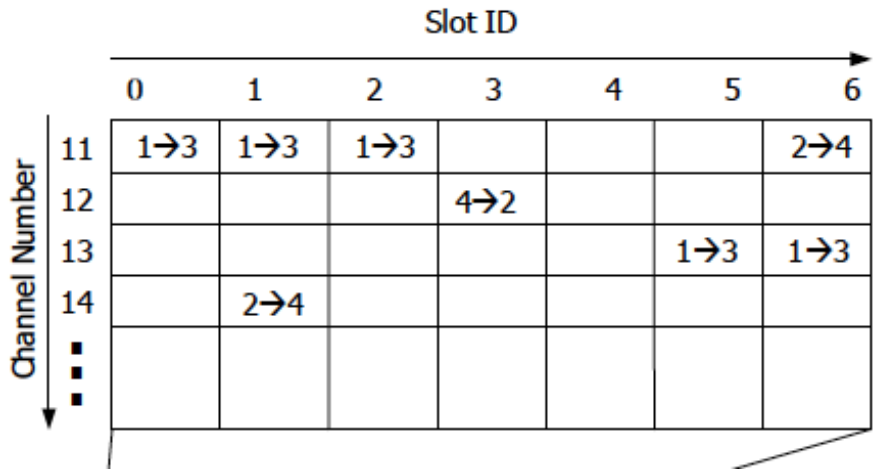
- *Sequence* is a table listing the channel identifier sequence in use (e.g. [10, 15, 17, 21] for example)
- *SequenceLength* the size of the Sequence table.
- *ChannelOffset* allows for **different channels to be used in the same ASN** for the given hopping *Sequence*.

TSCH mode : Time Slotted Frequency Hopping

A communication link

An active slot in the slotframe is call a **link**. It is thus caracterized by :

- its **slotframe ID**,
- its **timeslot** number in the slotframe (not the ASN)
- its **channel offset**
- its **mode** : TX, TX/RX, TX Shared, RX Shared.



In this figure, the channel number represents the channel offset. Node 1 is using the links (0,11), (1,11), (2,11), (5,13), (6,13) to transfer 5 frames of DATA.

TSCH mode : Time Slotted Frequency Hopping

Enhanced beacons in TSCH

Here beacons are Enhanced Beacons as they carry **Information Elements** :

- **TSCH slotframe and link IE** : Initial link and slotframe information (e.g. slotframe size) so new nodes know when there are shared timeslot and guaranteed timeslots.
- **TSCH timeslot IE** : when to expect a frame to be transmitted and when to send an ACK within a slot
- **Channel hopping IE** : identification of the channel hopping sequence in the network
- **TSCH synchronization IE** : information used for association of new nodes,

Node association

A node may hear several extended beacons, emitted by different nodes in the network. It has to chose the one it is using to synchronise to the network :

For example, after having received the first EB, a node may listen for at most `MAX_EB_DELAY` *seconds until it has received EBs from* `NUM_NEIGHBOURS_TO_WAIT` *distinct neighbors.*

It may select the time parent to attach to using the **Join Metric** which varies between 1 and 255. This metric represents the distance to the global PAN coordinator. It has to be directly fed by the routing protocol (RPL for instance).

TSCH mode : Time Slotted Frequency Hopping

TSCH synchronization IE

7.4.4.2 TSCH Synchronization IE

The TSCH Synchronization IE Content field shall be formatted as illustrated in Figure 7-50.

Octets: 5	1
ASN	Join Metric

Figure 7-50—TSCH Synchronization IE Content field format

The ASN field contains the ASN corresponding to the timeslot in which the enhanced beacon is sent. The ASN is used as the Frame Counter for security operations if enabled.

- ASN is the Absolute Slot Number,
- **Join Metric is an important field** used by a node to select the PAN coordinator it connects in the association process. It picks the one with the lowest metric.

TSCH mode : Time Slotted Frequency Hopping

Node association procedure

When a new node wants to join the network,

1. It scans the channels for beacons for a fixed duration or until a given number of beacons has been recorded.
2. Selects the PAN coordinator with the lower join metric.
3. Stores info from all IEs (e.g. *synchronization IE*, *slotframe and link IE*, etc).
4. Executes the schedule :
   - Listens to all advertising links (TX Shared) for higher layer control operations
   - Sends/receives DATA in TX/RX slots if it is either transmitter or receiver.
   - Synchronizes slot boundaries in each slot with Timekeeping set to 1.
   - Listens for beacons to maintain a list of visible PAN Coordinators.

Course structure

1. Wireless networks in Industry
   - Wireless in Industry
2. Wireless protocols and Determinism
   - WiFi and determinism
   - Bluetooth and determinism
   - 802.15.4 and determinism
3. TSCH - Time Slotted Channel Hopping
4. IP over TSCH : 6TiSCH.
   - 6TiSCH protocol stack
   - Allocation of slots
5. Routing for low power and lossy networks
   - RPL protocol
   - Trickle timer
6. Elements of 5G for Industry

6TiSCH initiative

Connecting a mesh network to IP.

In order to push the data to the central PAN coordinator, additional operations are required :

- Find a route that adapts to channel conditions and congestion to transfer data to the coordinator,
- Allocate timeslots to each part of the routes,
- Carry IP information to reach each sensor from the Internet : carry address, and other elements of the IP header.
  Fragment / Reassembly messages.

The 6TiSCH Architecture.

Connecting a mesh network to IP.

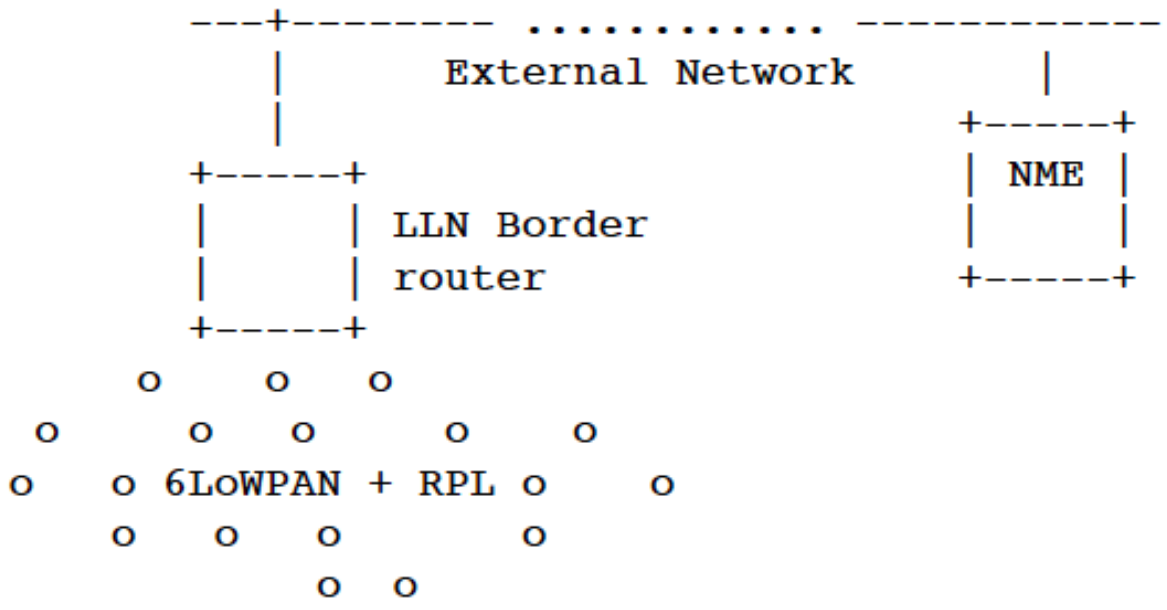


Figure 3: Basic Configuration of a 6TiSCH Network

LLN = global PAN coordinator,
NME = Network Management Entity,
RPL = Routing Protocol for LLNs.

The 6TiSCH Architecture

Connecting a mesh network to IP.

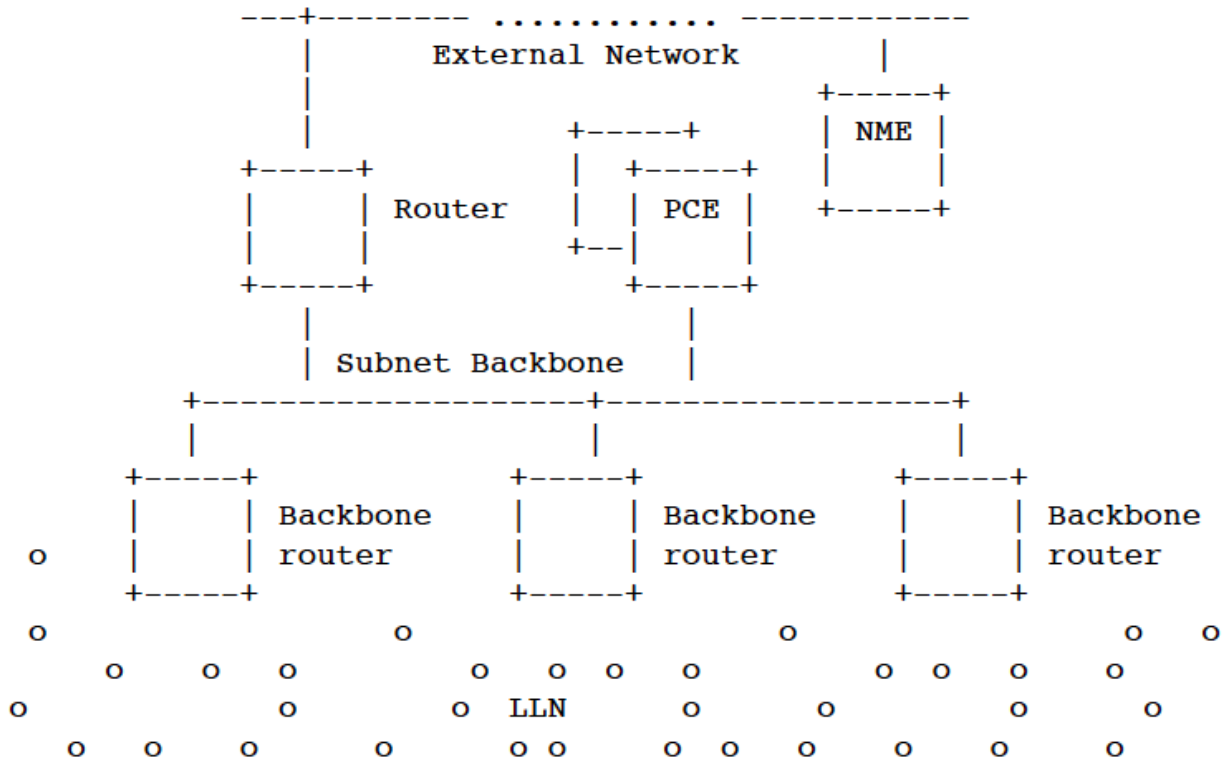


Figure 4: Extended Configuration of a 6TiSCH Network

PCE = Path Computation Element

Proposed protocol stack

A **deterministic protocol stack** designed for real-time monitoring control operations in industry.

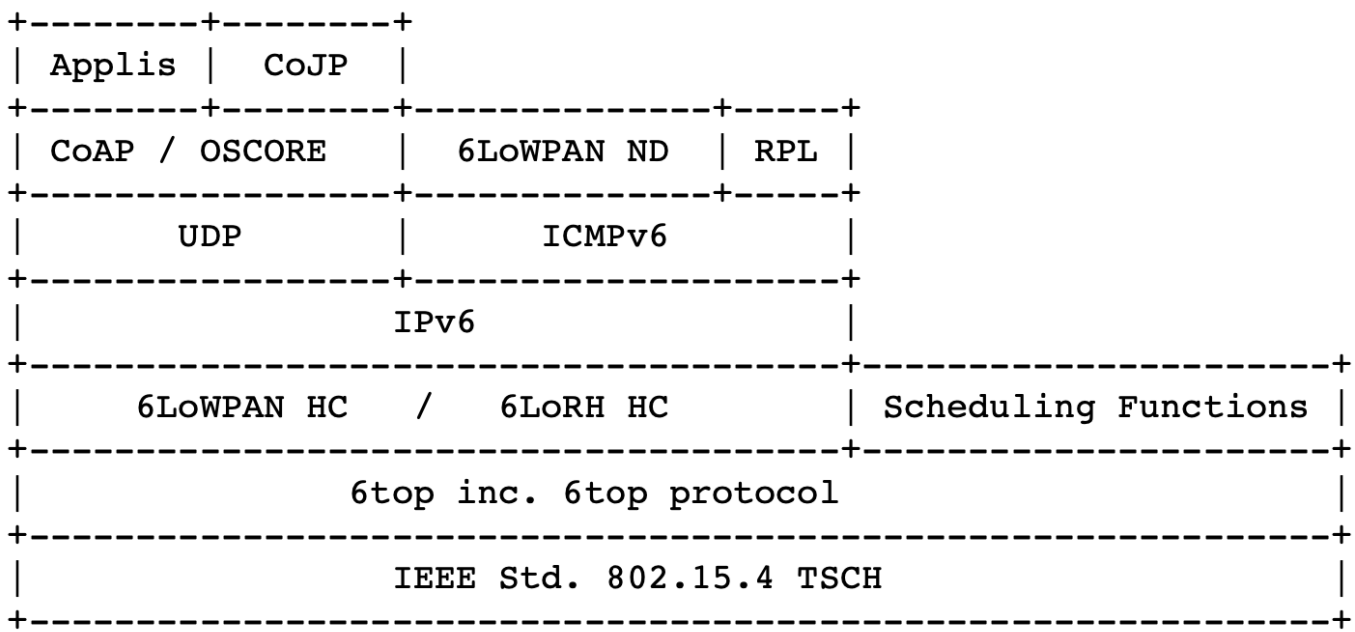


Figure 4: 6TiSCH Protocol Stack

Protocols and IETF RFCs

Routing protocol : RPL

- IETF ROLL working group for Routing Over Low power and Lossy networks :

RFC 6550 *RPL* Routing protocol for LLNs
RFC 6551 *RPL Routing metrics* specifications
RFC 6552 *RPL Of0* Objective function 0 specification
RFC 6206 Trickle algorithm

All available at `https://datatracker.ietf.org/`

Protocols and IETF RFCs

IPv6 over 802.15.4

- IETF 6LoWPAN working group for encapsulating IPv6 frames in 802.15.4 :

RFC 4919 *6LowPANs* problem statement for IP over 802.15.4
RFC 4944 *6LowPANs* standard for IPv6 packet in 802.15.4

All available at `https://datatracker.ietf.org/`

Protocols and IETF RFCs

Scheduling the links in TSCH

- 6TiSCH working group working on a link allocation layer between RPL and IEEE TSCH :

Draft [draft-ietf-6tisch-architecture-28] Protocol architecture of 6TiSCH
RFC 7554 *6TiSCH problem statement*
RFC 8480 *6Top Protocol (6P)* for on-demand slot allocation
RFC 8180 A *minimal 6-TiSCH* implementation

All available at `https://datatracker.ietf.org/`

Allocation of slots

TSCH is not in charge of deciding which slot is to be given to a unidirectional DATA communications. This is the task of a higher layer protocol :

- WirelessHART
- ISA100.11a
- 6Top from 6TiSCH

This allocation can be static (WirelessHART, ISA100.11a) or on-demand (6TiSCH). A static allocation is calculated by a network manager that floods the calculated allocation in the network using shared slots.

6top Protocol (6P)

If a node A wants to add a link with B in the schedule :

- it contacts B to request the provision of it using a 6Top ADD transaction. In this request, A lists how many links it needs (NumCells $= 1$ here), and proposes a list of cells that it sees as free in the her view of the slotframe.
- B answers with the list of cells it has selected (list of size NumCells). Selection is made using a *Scheduling Function (SF)* that is implementation dependent.

6top Protocol (6P)

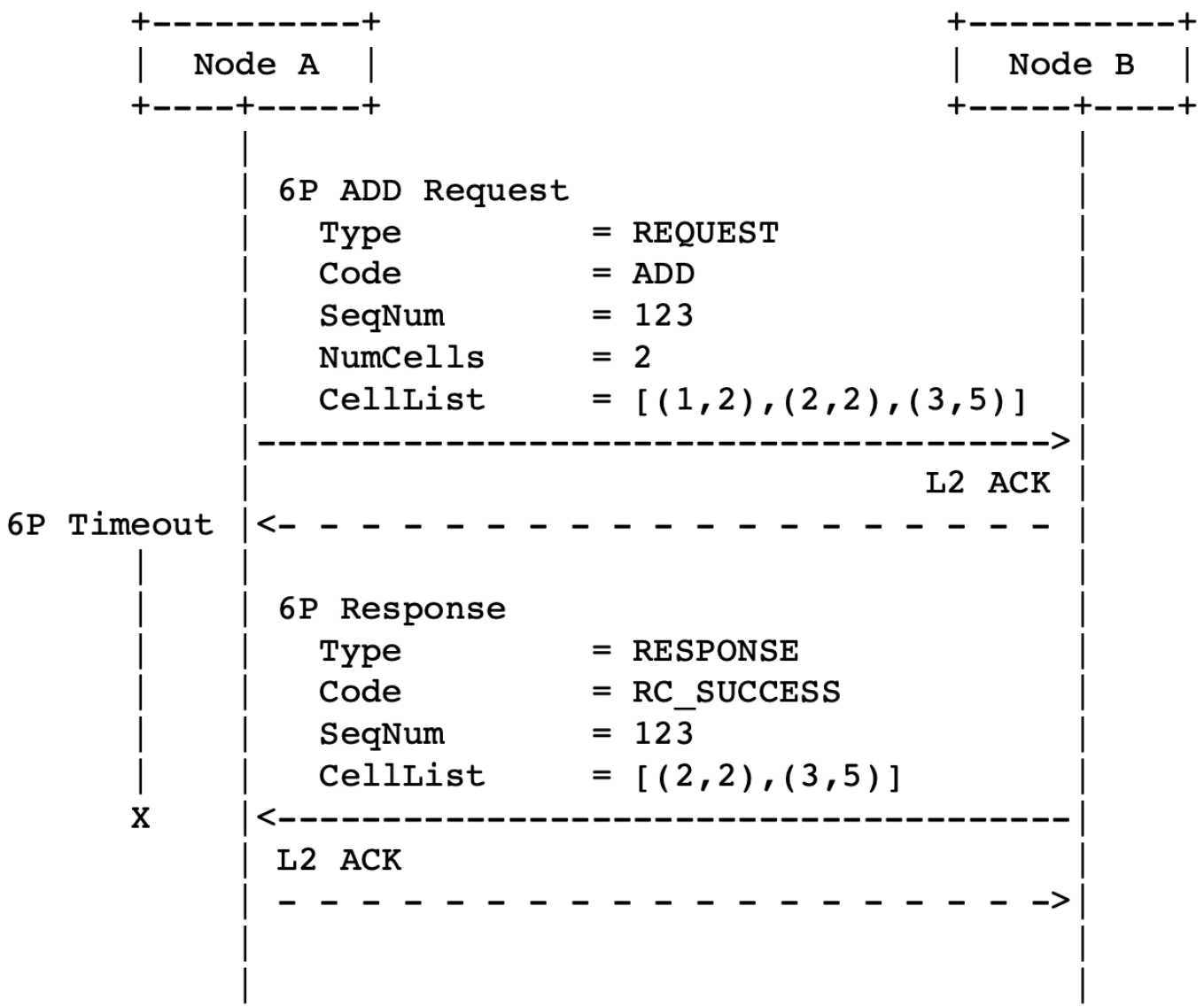


Figure 4: An example 2-step 6P Transaction.

Course structure

1. Wireless networks in Industry
   - Wireless in Industry
2. Wireless protocols and Determinism
   - WiFi and determinism
   - Bluetooth and determinism
   - 802.15.4 and determinism
3. TSCH - Time Slotted Channel Hopping
4. IP over TSCH : 6TiSCH.
   - 6TiSCH protocol stack
   - Allocation of slots
5. Routing for low power and lossy networks
   - RPL protocol
   - Trickle timer
6. Elements of 5G for Industry

RPL : Routing Protocol for LLN

Description

LLN are network made of low power, low memory, low processing nodes over a lossy communication channel (wireless).

- Traffic is multipoint to point (converge-cast) to the sink node
- RPL separates the packet processing and forwarding (RFC 6550) from the optimisation objective (RFC 6552).
- Follows a gradient routing principle

RPL : Routing Protocol for LLN

Definitions

- DAG : Directed Acyclic Graph, a directed graph with no loops
- DODAG : A Destination oriented DAG, a DAG with a unique destination for all paths (sink)
- DODAG_root : Destination node of the DODAG
- DODAG_id : Identifier of a DODAG
- Up direction : Towards the DODAG root
- Down direction : Away from the DODAG root
- When A –> B is a communication from A to B, we have :
  - B the *Parent* node
  - and A the *Child* node.
  - If B sends to A : Down direction
  - If A sends to B : Up direction

RPL : Routing Protocol for LLN

Rank of a node

- It increases in the down direction.
- It decreases in the up direction.
- Lowest rank node is the DODAG root.
- Computed based on the DODAG's optimisation function. It is in general proportional to the distance to the DODAG root.

DODAG construction

The DODAG root regularly floods a **DIO** control message : **DODAG Information Object**. Every time a node received a DIO, it :

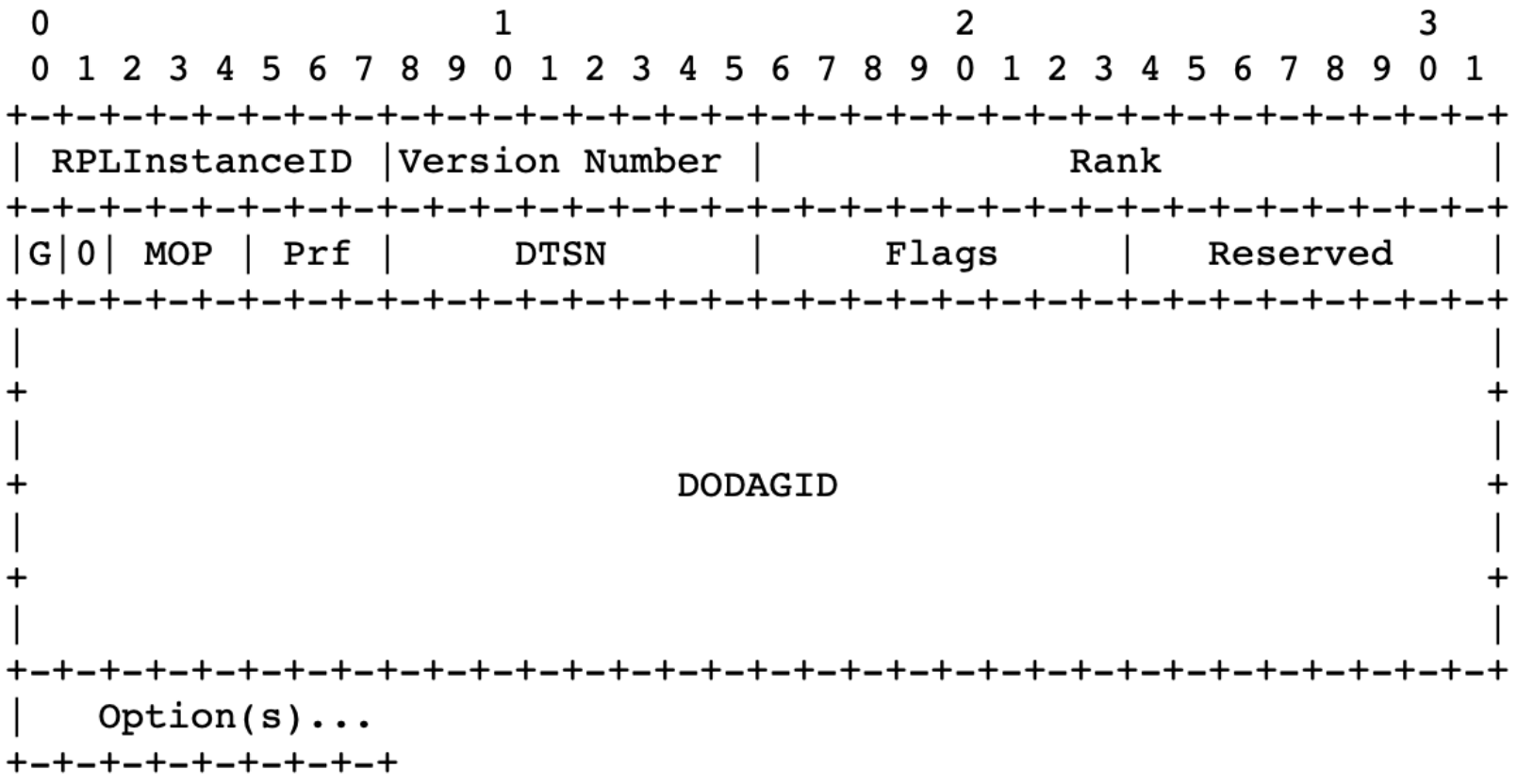
- reads the Rank of the node that has sent the DIO.
- reads the link or node metrics that are stored in its IE fields (hop count, energy, throughput, ETX etc..).
- calculates its Rank w.r. to this DIO :

$$NewRank = ReceivedRank + OF(metrics)$$

- If $NewRank < CurrentRank$, I add the emitter of the DIO in a set of parent nodes.
- Update the most preferred parent. This preferred parent is **next hop** for any Up direction DATA transfer.
- Transmit a DIO with NewRank according to Trickle algorithm.

DIO control message

DIO is a RPL control message, of type 1.



Example with Optimisation Function 0

ROLL working group has proposed a default optimisation function OF0 in the RFC 6552 :

$$R(N) = R(P) + (3 * ETX - 2) \times MinHopRankIncrease \qquad (1)$$

where :

- $R(P)$ is the rank of a parent node ;
- $MinHopRankIncrease = 256$;
- ETX is the number of transmission attempts required to transfer a frame over one hop.
- DODAGroot has rank of 256.

ETX is the expected number of transmissions on a lossy link. It's the inverse of the frame success rate.

Link between RPL and TSCH

How to select the RPL Parent as the TSCH PAN coordinator ?

A node joining a TSCH PAN that hears several Enhanced Beacons chooses the TSCH PAN that exposes the minimum **Join Metric** in the `synchronisation IE`.

In RPL, the rank is encoded on 2 bytes and the TSCH Join Metric on 1 byte.
To select the RPL Parent as TSCH PAN coordinator, the RPL rank is transformed into a Join Metric by :

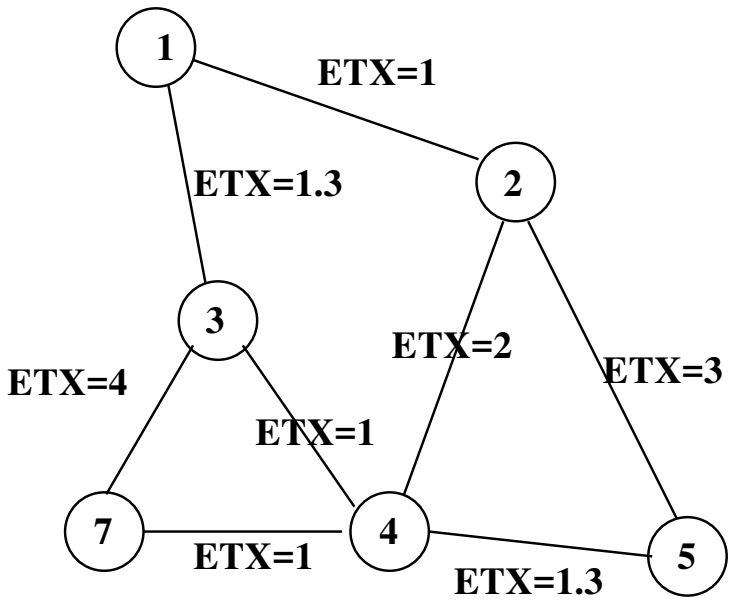
$$JoinMetric = RPLrank\%256$$

and broadcast in the beacon.

Once the joining node selects its new parent in TSCH layer,**it can negociate with 6P** a unidirectional link in the slotframe.

Exercice with Optimisation Function 0

The edges on this figure represent the connectivity of a sensor network. Each edge is labeled by the current ETX value measured by the pair of nodes.



RPL is deployed with OF0.

Exercice with Optimisation Function 0

1. We assume node 1 is selected as a DODAGroot and that its DODAGroot rank equals 0.
   Calculate the rank nodes 3, 4, 5 and 7 will eventually choose after receiving DIO messages from their neighbors.
2. Represent the DODAG, rooted at node 1, that will be used for routing by RPL.
3. If the rank is calculated by simply counting hops (i.e. $R(N) = R(P) + 1$), would RPL define the same DODAG as the one calculated with OF0 ? DODAGroot rank is still equal to 0.

RPL : Routing Protocol for LLN

Data transfer in the Up direction

Each node simply sends its data to its preferred parent.
There are alternatives where nodes send to their preferred parent AND their alternative parent.

Data transfer in the Down direction

The DODAG being oriented towards its root, there are :

- neither routes from the root to the rest of nodes in the down direction,
- nor routes from one node to another one.

Another mechanism is necessary if such routes are needed.

DAO control message

If a node has to be reached by other nodes, she sends a **Destination Advertisement Object - DAO** control message with :

- her IP address as 'target' address
- the `all-RPL-nodes` broadcast address as destination.
- and the `DAOsequence` field equal to 1.

DAO forwarding up

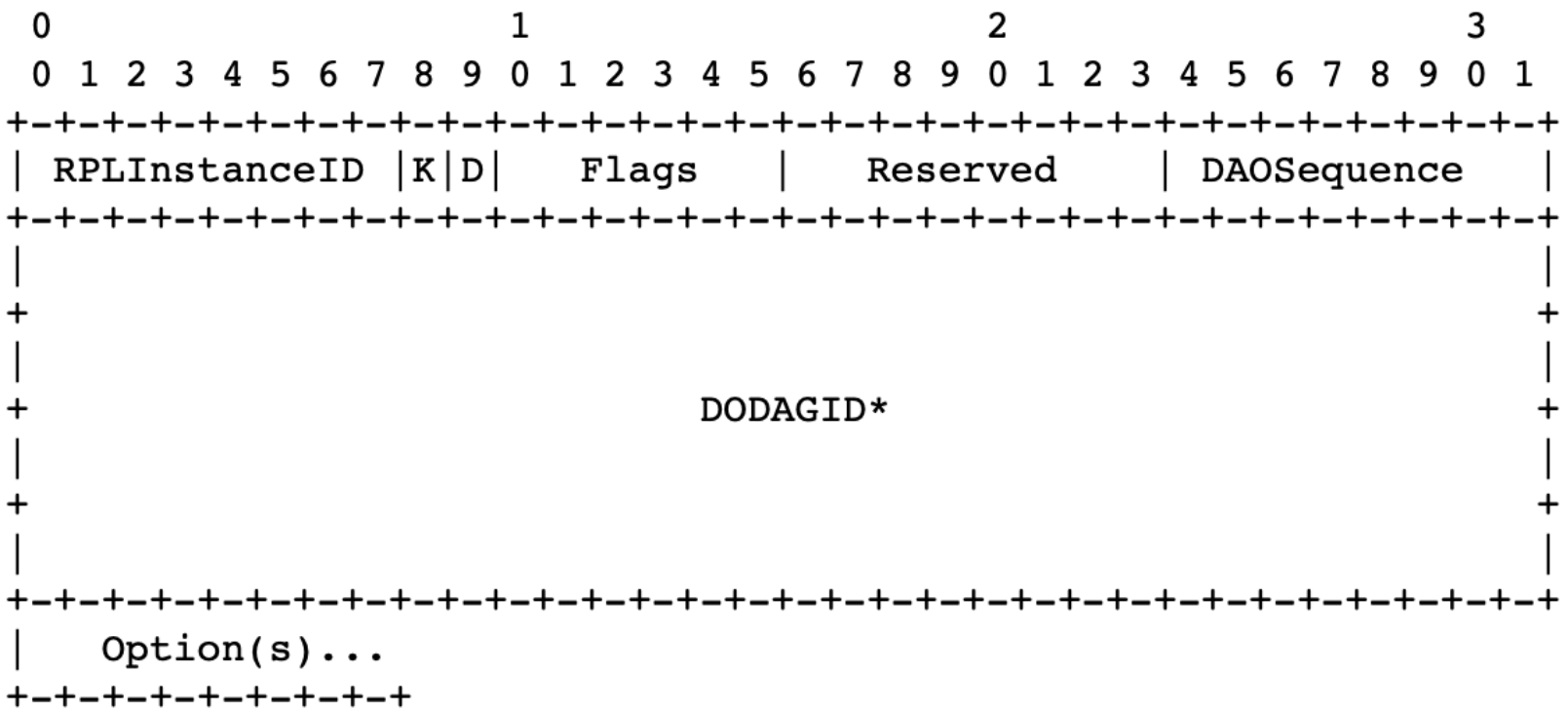
When a node receives a DAO message,

- She sets `DAOsequence = DAOsequence + 1`,
- She adds her address in the list of nodes that have already forwarded this DIO (an option field of DAO),
- She forwards it to her preferred parent, in the Up direction, towards the DODAG root.
- She may request an acknowledgement (DAO-ACK).

The DAO is eventually received by the DODAGroot that now knows a new path to the target node.

DAO control message

. Format of the DAO Base Object



Storing and non-storing modes

The DAO advertises the presence of its emitter to the nodes that forward it and to the DODAGroot node. This information can be stored in a **routing table**.

There are 2 different modes in RPL for storing these routing tables :

- Storing mode : all intermediary nodes maintain a routing table,
- Non-storing mode : only the DODAGroot has a routing table (that is populated with source routing).

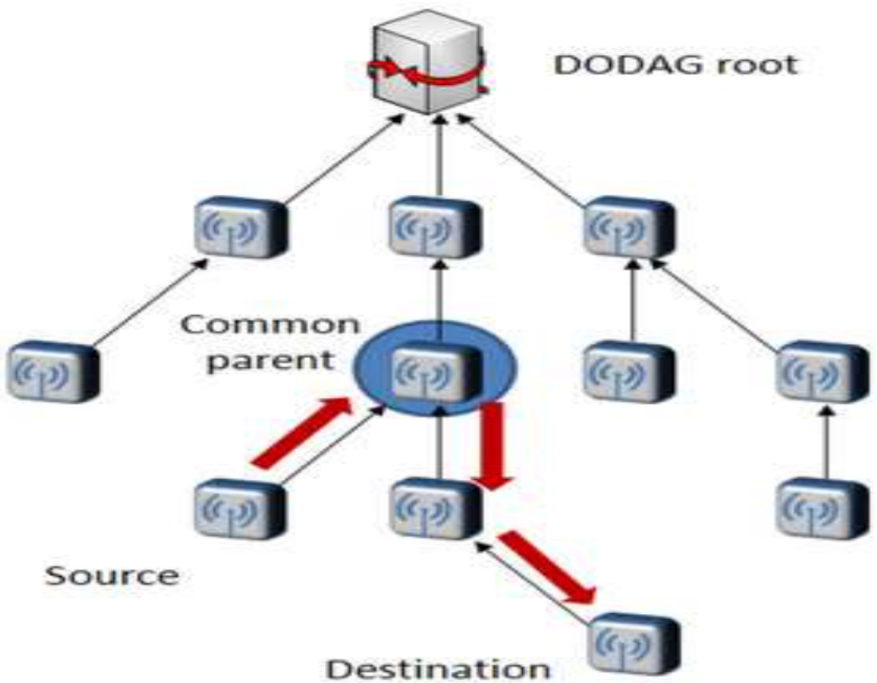
All modes are enforced by the `MOP` field of `DIO` messages.

RPL : Routing Protocol for LLN

Routing in **storing** mode

A node S sending data to a node D checks in its routing table if there is an entry towards D.

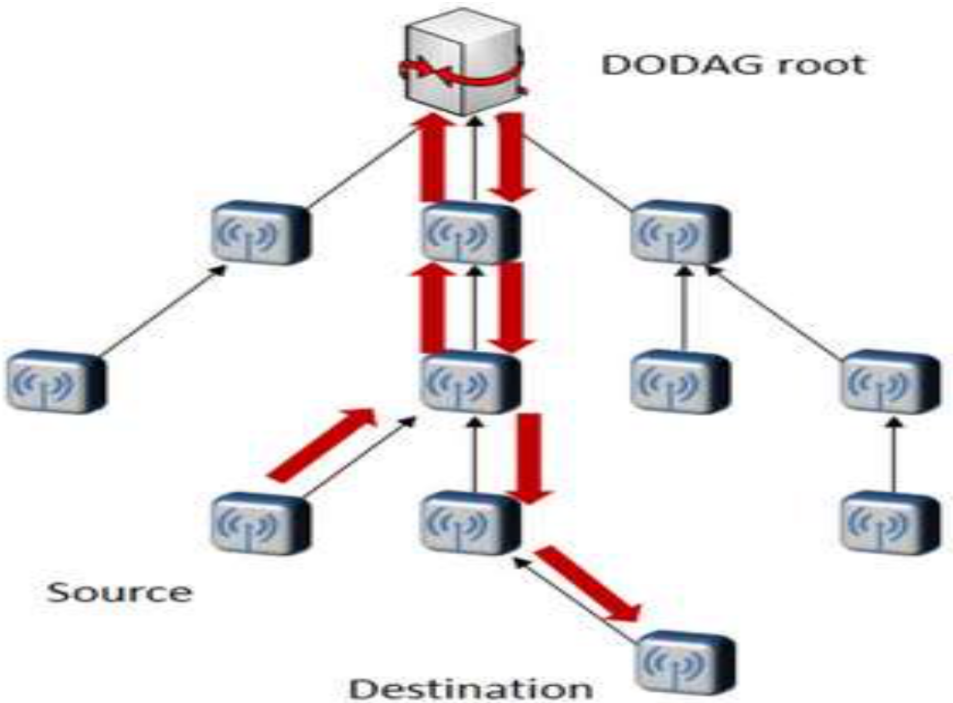
- If yes, she sends it **down** to next hop node in routing table.
- If no, she sends it **up to its preferred parent**.



RPL : Routing Protocol for LLN

Routing in **non-storing** mode

Data is always pushed up. Only the DODAGroot sends data messages down by writing the complete path in the data (source routing).



Loop detection

Nodes detect loops if :

- There is an inconsistency between the transfer direction (up/dowm) and the type of message received (DAO, DIO,etc)
- A node receives data going in up direction from a node with lower rank.

To ask for repair, a node may :

- send a **DIS** (DIO Information Sollicitation) to her parent. The parent node sends then a new DIO to trigger rank updates.
- send a **DIO poisoning** message, i.e. a DIO with `INFINITE_RANK` to notify its sub-DODAG that she's a bad choice as parent.

Trickle timer

Description

RFC 6206 introduces the Trickle algorithm which is here to govern how DAO or DIO messages are spread in the network.

Let's read the RFC : `https://tools.ietf.org/html/rfc6206`

Course structure

1. Wireless networks in Industry
   - Wireless in Industry
2. Wireless protocols and Determinism
   - WiFi and determinism
   - Bluetooth and determinism
   - 802.15.4 and determinism
3. TSCH - Time Slotted Channel Hopping
4. IP over TSCH : 6TiSCH.
   - 6TiSCH protocol stack
   - Allocation of slots
5. Routing for low power and lossy networks
   - RPL protocol
   - Trickle timer
6. Elements of 5G for Industry