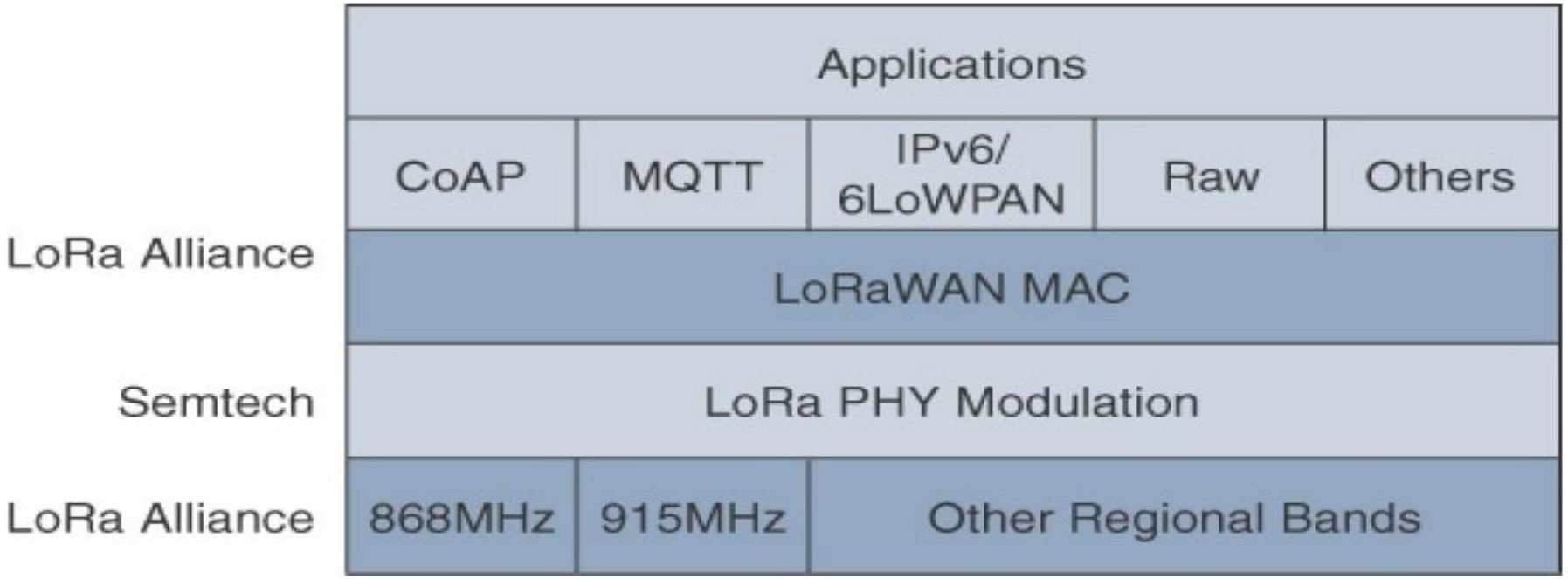
Physical and Link Layers Protocols- LoRaWAN

- LoRaWAN
  - LoRaWAN is an example of an unlicensed-band Low-Power Wide-Area (LPWA) technology.
  - LPWA particularly well adapted for long-range and battery-powered endpoints.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- LoRaWAN

- LoRaWAN Layers



- nal frequency

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN-Standardization and Alliances

- Initially, LoRa was a physical layer, or Layer 1, modulation that was developed by a French company named Cycleo. Later, Cycleo was acquired by Semtech (in 2012).
  - Semtech LoRa as a Layer 1 PHY modulation technology is available through multiple chipset vendors.
  - Semtech has licensed its LoRa intellectual property (ip) to other chip manufacturers, such as HopeRF, Microchip, Dorji, etc.

- Optimized for long-range, two-way communications and low power consumption, the technology evolved from Layer 1 to a broader scope through the creation of the LoRa Alliance.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN-Standardization and Alliances

- To differentiate from the physical layer modulation known as LoRa, the LoRa Alliance uses the term LoRaWAN to refer to its architecture and its specifications that describe end-to-end LoRaWAN communications and protocols.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRa Specification

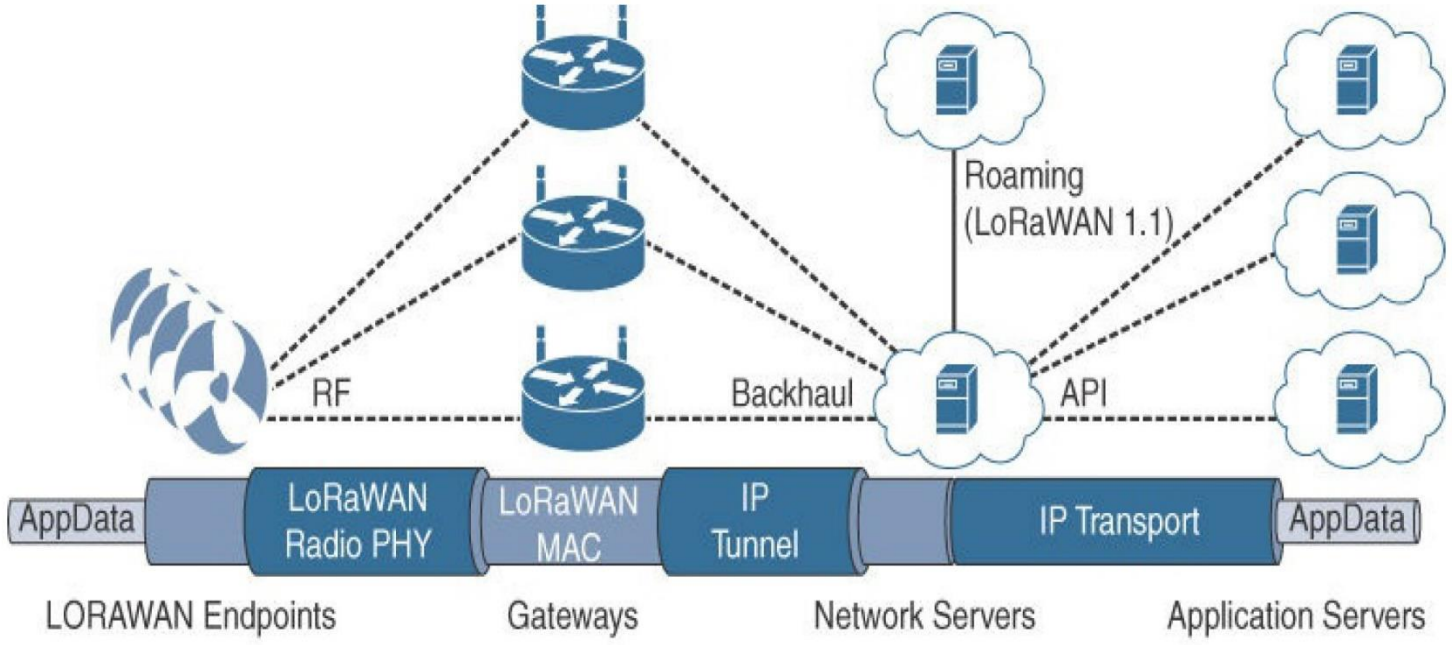
- The range between LoRa sender and receiver depends on the environment the equipment operates in. Indoor coverage largely depends on the type of building material used.

Urban areas (towns & cities)	2-5
Rural areas (country sides)	5-15
Direct Line of Sight	>15

- Some notable records: Andreas Spiess, ground to ground connection: 212 km (= 131.73 miles) Weather balloon to ground connection: 702.67 km (= 436.61 miles)

LoRaWAN- Topology

- LoRaWAN
  - Topology
    - Star of stars



* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN- Topology

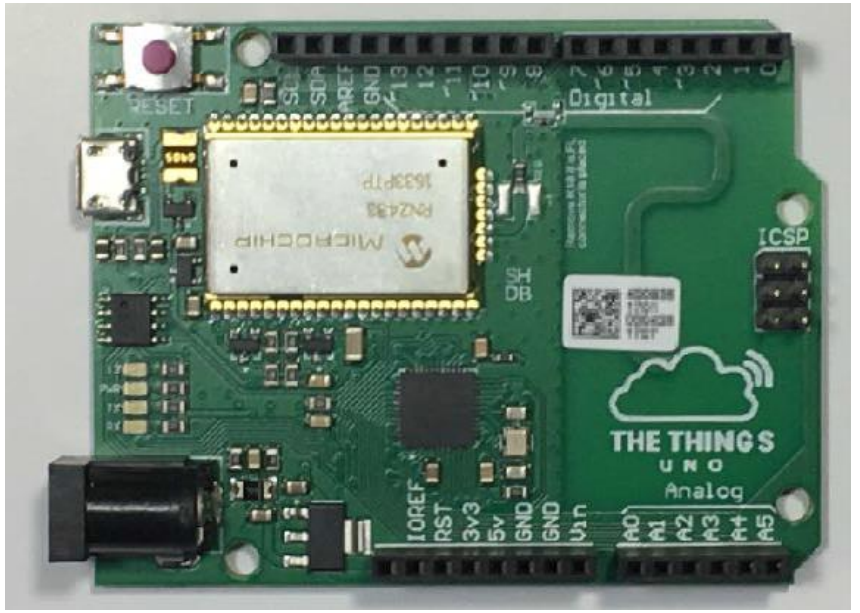
- **End-devices:**
  - Perform the communication gateways using LoRa and LoRaWAN technologies.
- **Gateways (i.e., base stations):**
  - Dispatch the LoRaWAN frames from the end devices to a network server using a back-haul interface with higher throughput, usually via Ethernet, 3G/4G, satellite or Wi-Fi.
- **The Network Server:**
  - Decodes the packets sent by the devices, performing security checks and adaptive data rate, thus generating the control data that should be sent back to the devices.
- **Each Application:**
  - Receives data from the network server. It should decode the security packets and uses the information to decide the action in the application.

LoRaWAN- Topology

- LoRa is an acronym for Long Range and it is a wireless technology where a low powered sender transmit small data packages (0.3 kbps to 5.5 kbps) to a receiver over a long distance.
- A gateway can handle hundreds of devices at the same time.

The Things Gateway

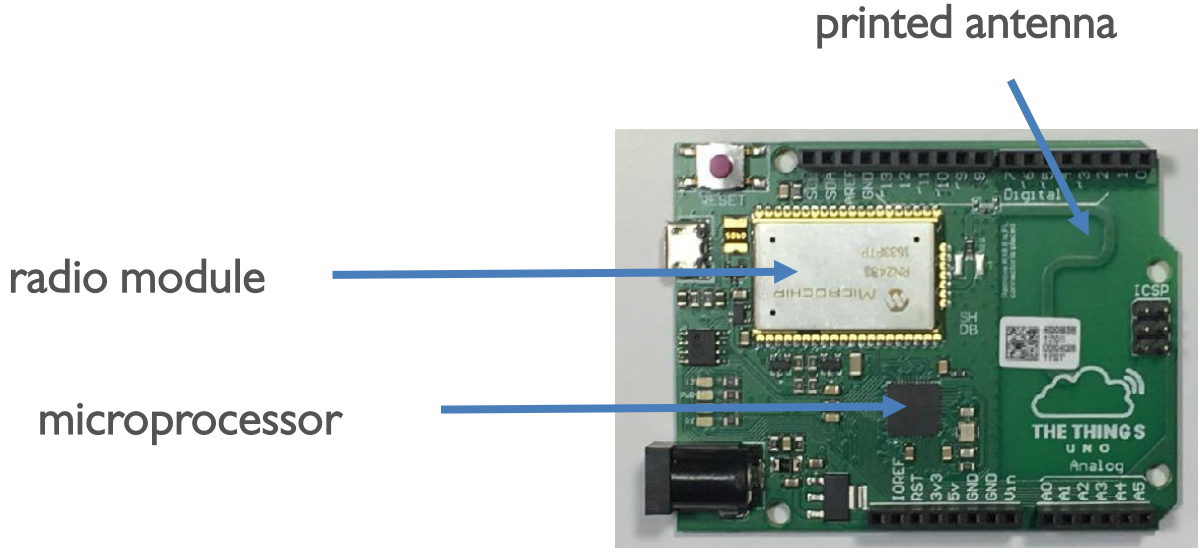
(gateway / concentrator)



The Things Uno (end node)

LoRa End-Node

- A LoRa end node consists of 2 parts:
  - A radio module with antenna.
  - A microprocessor to process for example the sensor data.
- End nodes are often battery powered.
- A LoRa device (end node) has a wireless transceiver. If this device also has sensors, this device acts as a remote sensor. Such a device is called a mote, short for remote.



LoRa Gateway

- A LoRa gateway consists of 2 parts:
  - A radio module with antenna.
  - A microprocessor to process the data.

- Gateways are mains powered and connected to the Internet.

- Multiple gateways can receive data from the same end node.

- The gateways can listen to multiple frequencies simultaneously

LoRaWAN: Specification

- The most **critical factors** in a LPWAN are:
  - Network architecture;
  - Communication range;
  - Battery lifetime (low power);
  - Robustness to interference;
  - Network capacity (maximum number of nodes in a network);
  - Network security;
  - One-way vs two-way communication;

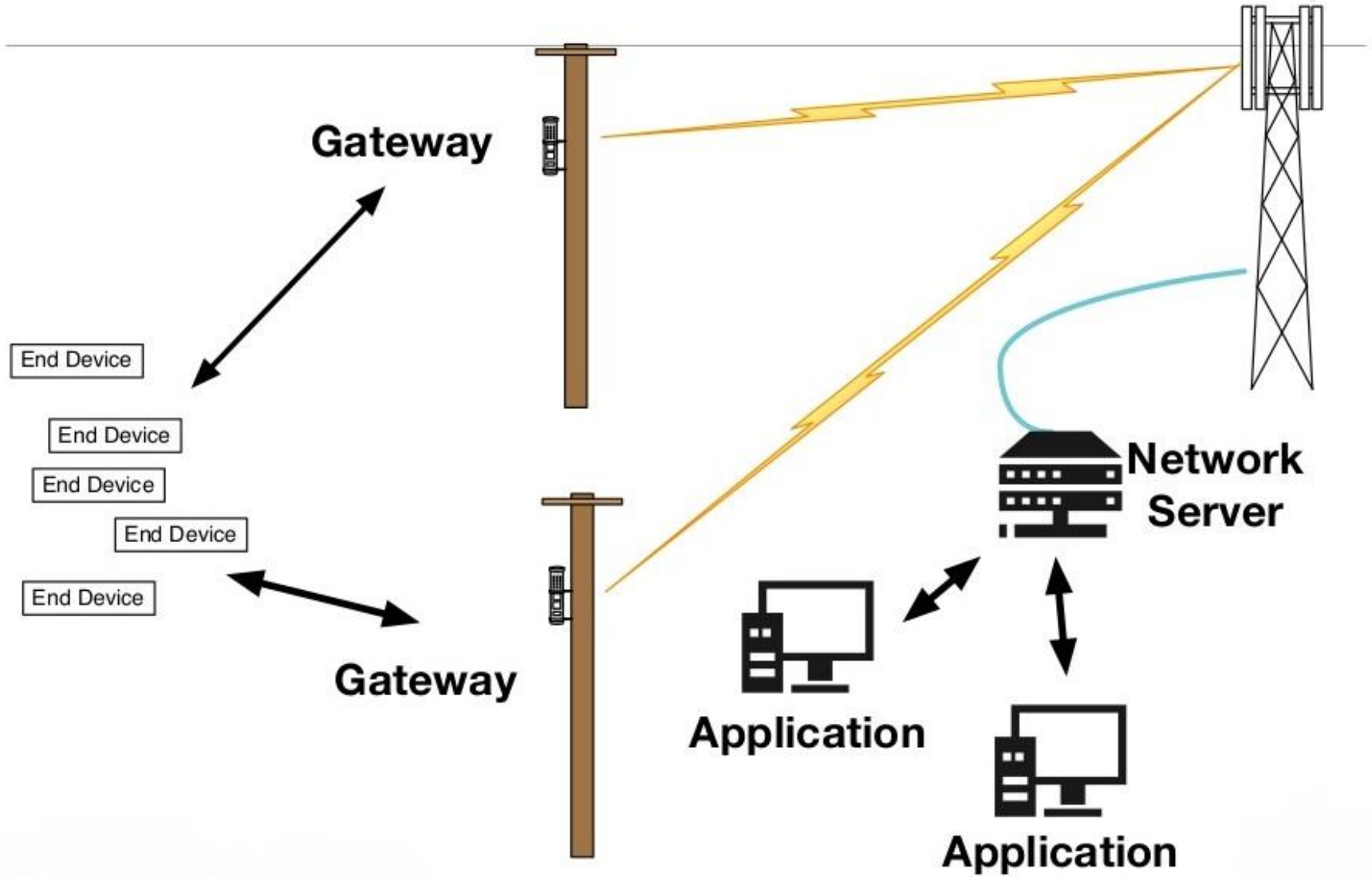
Characteristic	LoRaWAN
Topology	Star on Star
Modulation	SS Chirp
Data Rate	290bps - 50kbps
Link Budget	154 dB
Packet Size	20-256 bytes
Battery lifetime	8 ~ 10 years
Power Efficiency	Very High
Security/Authentication	Yes (32 bits)
Range	2-5 km urban 15 km suburban 45 km rural
Interference Immunity	Very High
Scalability	Yes
Mobility/Localization	Yes

LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities, Inatel, 2017

LoRaWAN- How It Works?

- **End Node**
  - broadcast its data to every gateway in its vicinity.
- **Gateways:**
  - Forward this packet to the network server. It is only a protocol convertor.
- **Network Server:**
  - Collects the messages from all gateways and filters out the duplicate data and determines the gateway that has the best reception.
  - Forwards the packet to the correct application server where the end user can process the sensor data.
- Optionally the application server can send a response back to the end node.
  - When a response is sent, the network server receives the response and determines which gateway to use to broadcast the response back to the end node.

LoRaWAN- Topology



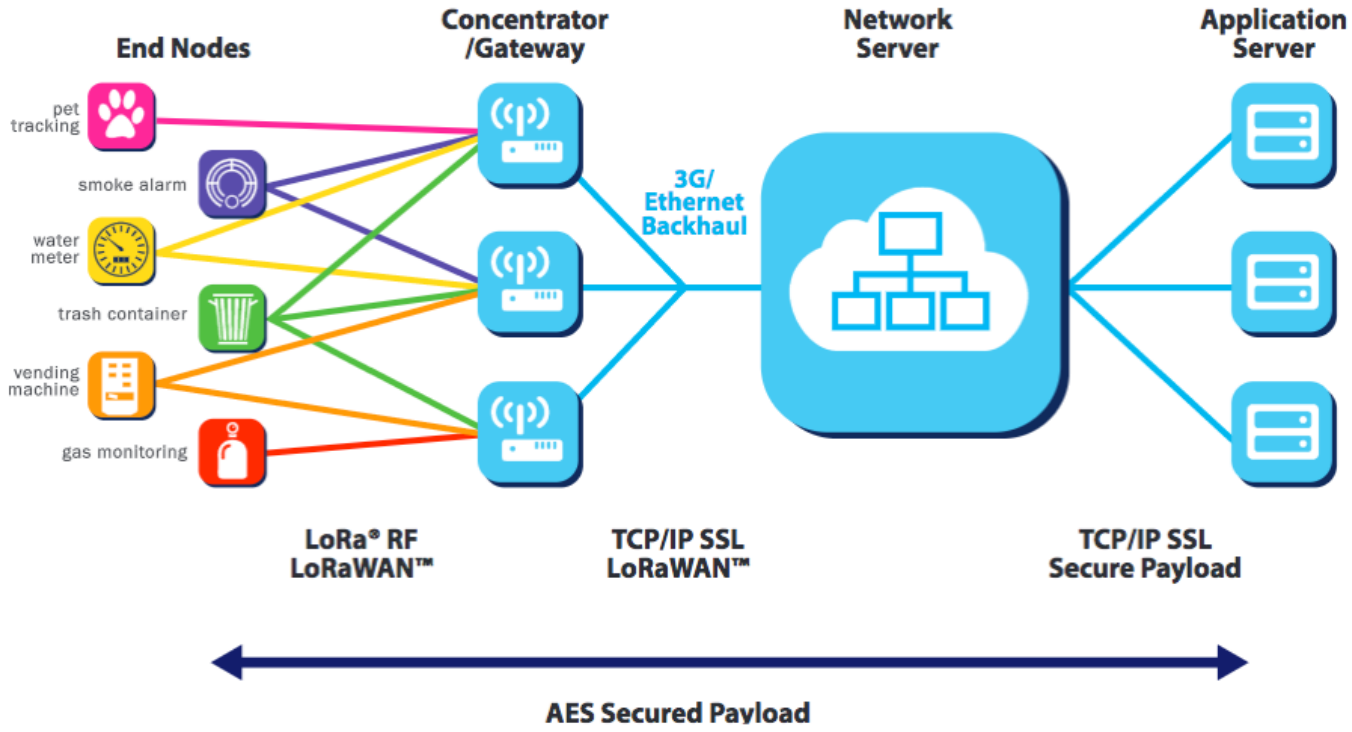
LoRaWAN- Topology

- LoRaWAN network architecture is deployed in a star topology.
- End nodes are not associated with a particular gateway. Rather, when a node sends data, it is typically received by multiple gateways.
- Each of these gateways, in turn, forwards the received data toward the cloud-based network server using some backhaul technology.
- The network server is responsible for all complex and intelligent functions:
  - it manages the network, filters redundant received data, performs security verification, schedules acknowledgments through the most optimal gateway, and performs adaptive rate control, etc.
- A key feature of this architecture is that no handover mechanism is required from one gateway to another to support the mobility of end nodes.
  - Therefore, it is straightforward to enable IoT asset tracking applications.
- Another key feature is the built-in access redundancy, where the failure of a gateway or path toward the network server is handled by sending redundant copies of data packets

LoRaWAN- Topology

- LoRaWAN network architecture is deployed in a star topology.

- The communication between the end node and gateway is bidirectional which means the end node can send data to the gateway but it can also receive data from the gateway.

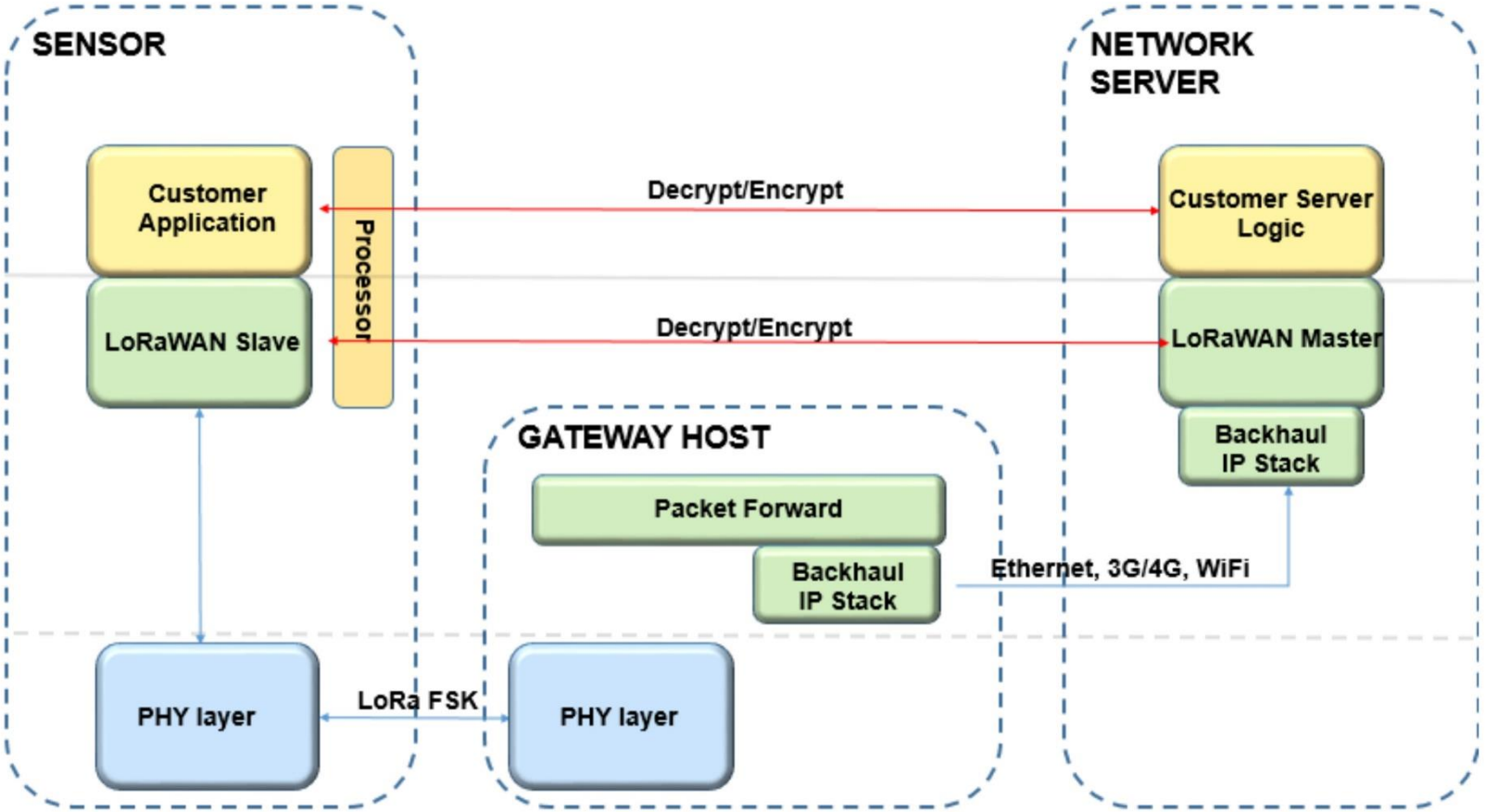


LoRaWAN- Topology

- LoRaWAN- LoRa gateway
  - A LoRa gateway is deployed as the center hub of a star network architecture.
  - It uses multiple transceivers and channels and can demodulate multiple channels at once or even demodulate multiple signals on the same channel simultaneously.
  - LoRa gateways serve as a transparent bridge relaying data between endpoints, and the endpoints use a single-hop wireless connection to communicate with one or many gateways.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN Protocol



LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities, Inatel, 2017

Few Use Cases Using LoRa Technology

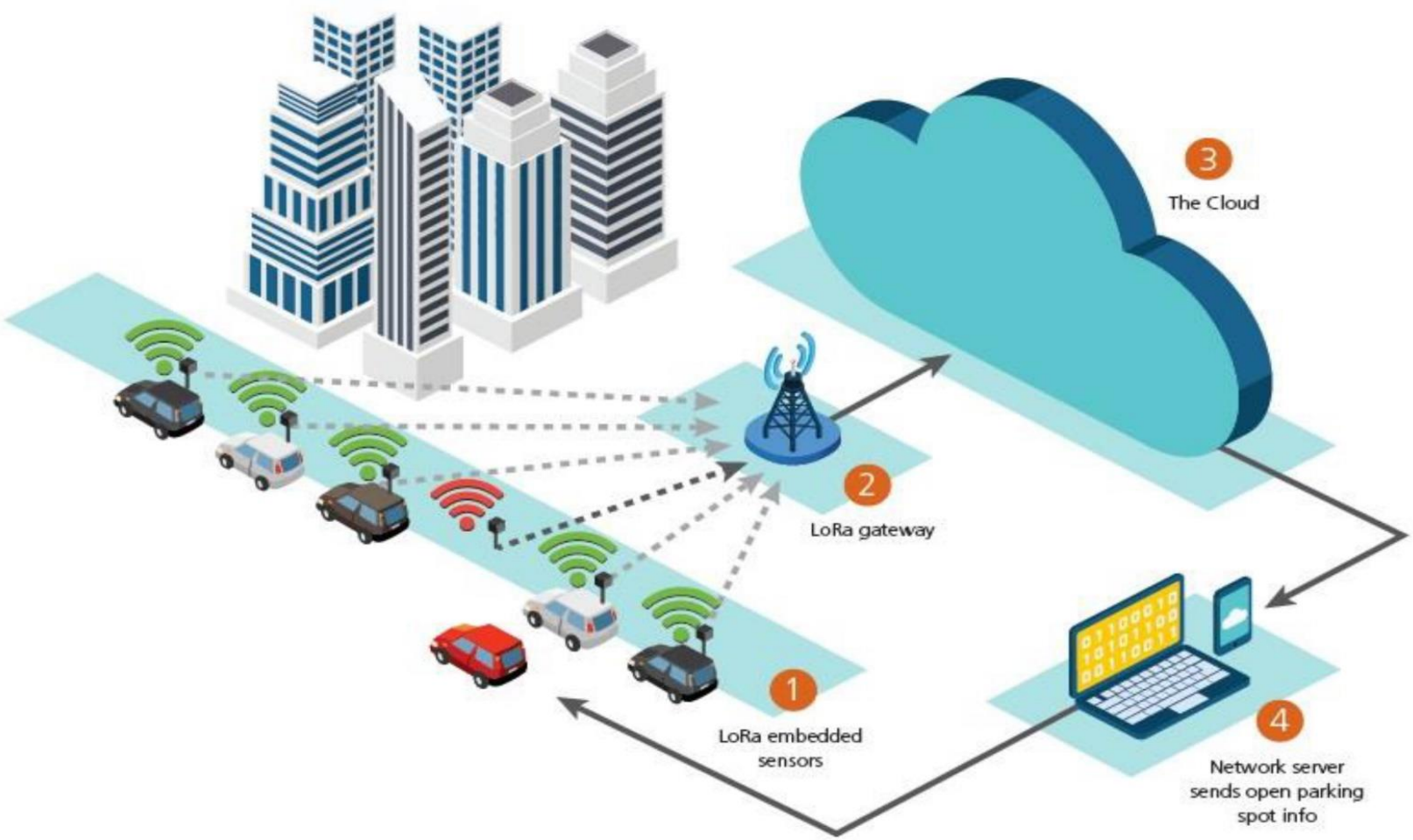
- **Smart utilities**
  - Power transformer monitoring
  - Water level monitoring
  - Utility meter
  - Fuel monitoring (monitoring fuel levels in fuel tanks for heating houses)
- **Health & Hygiene**
  - Temperature / humidity monitoring
  - Environmental monitoring
  - Waste management (monitoring waste level in waste bins)

Few Use Cases Using LoRa Technology

- **Safety**
  - Smart lightning
  - Water level monitoring
  - Radioactivity level monitoring
  - Dike monitoring (prevent peat dikes from drying out)
- **Efficiency**
  - Asset management (e.g. tracking containers, pallets, etc.)
  - Fleet management (e.g. tracking cars, vans, trucks, etc.)
- **Agriculture**
  - Monitoring animal welfare
  - Monitoring plant growing conditions

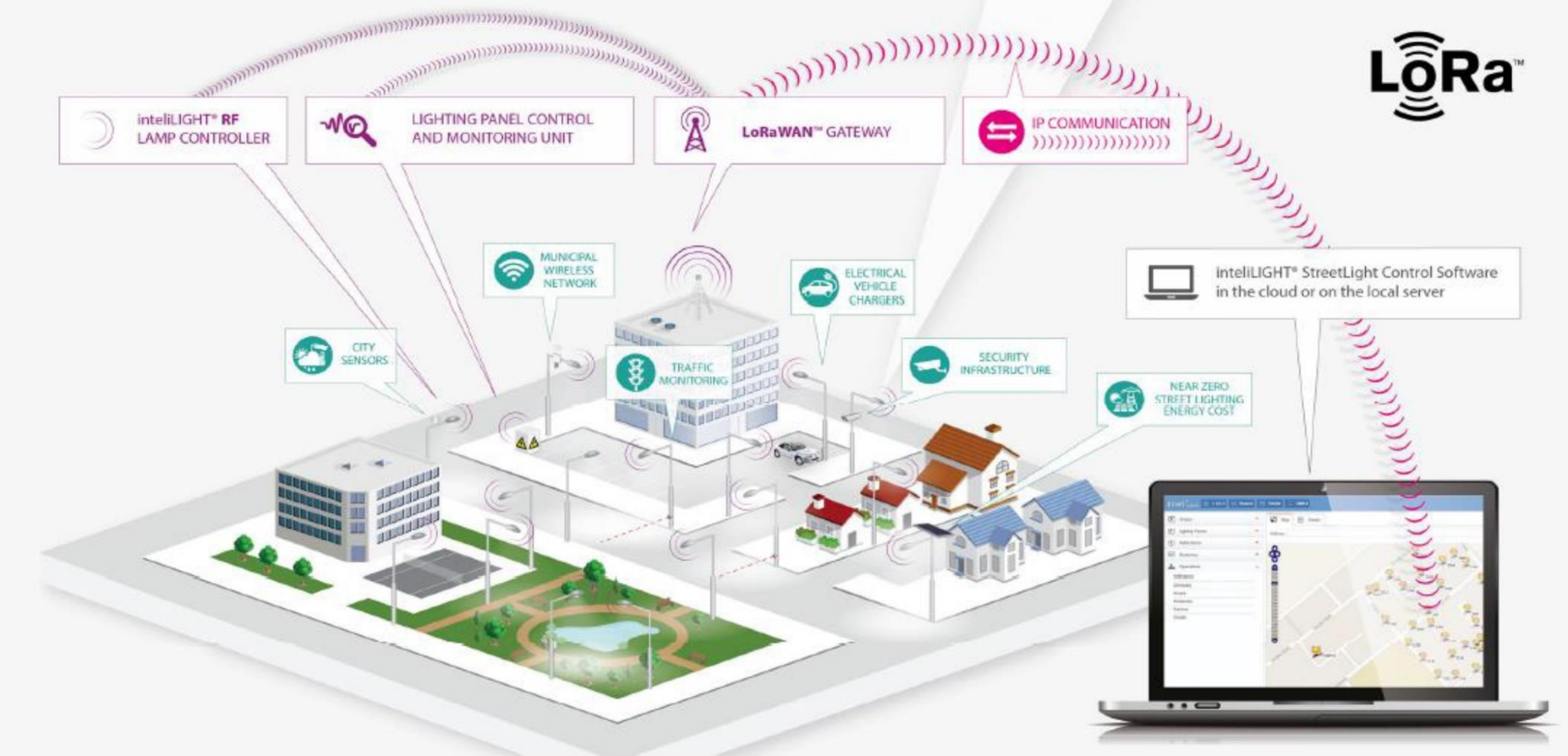
Few Use Cases Using LoRa Technology

LoRaWAN Use Case- Parking Occupancy



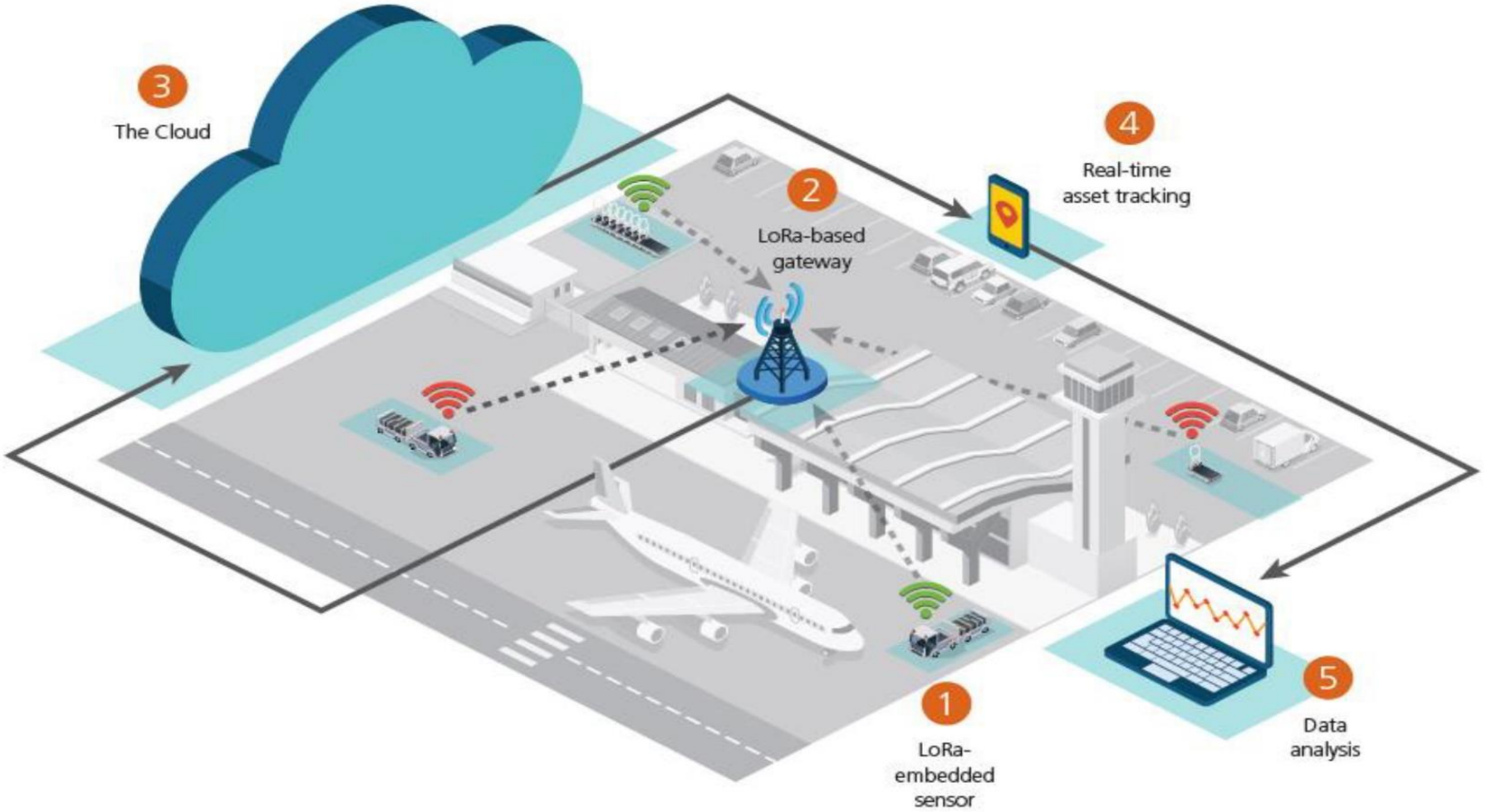
IOT and LORAWAN, Quaenet, 2018

LoRaWAN Use Case- Smart Lighting



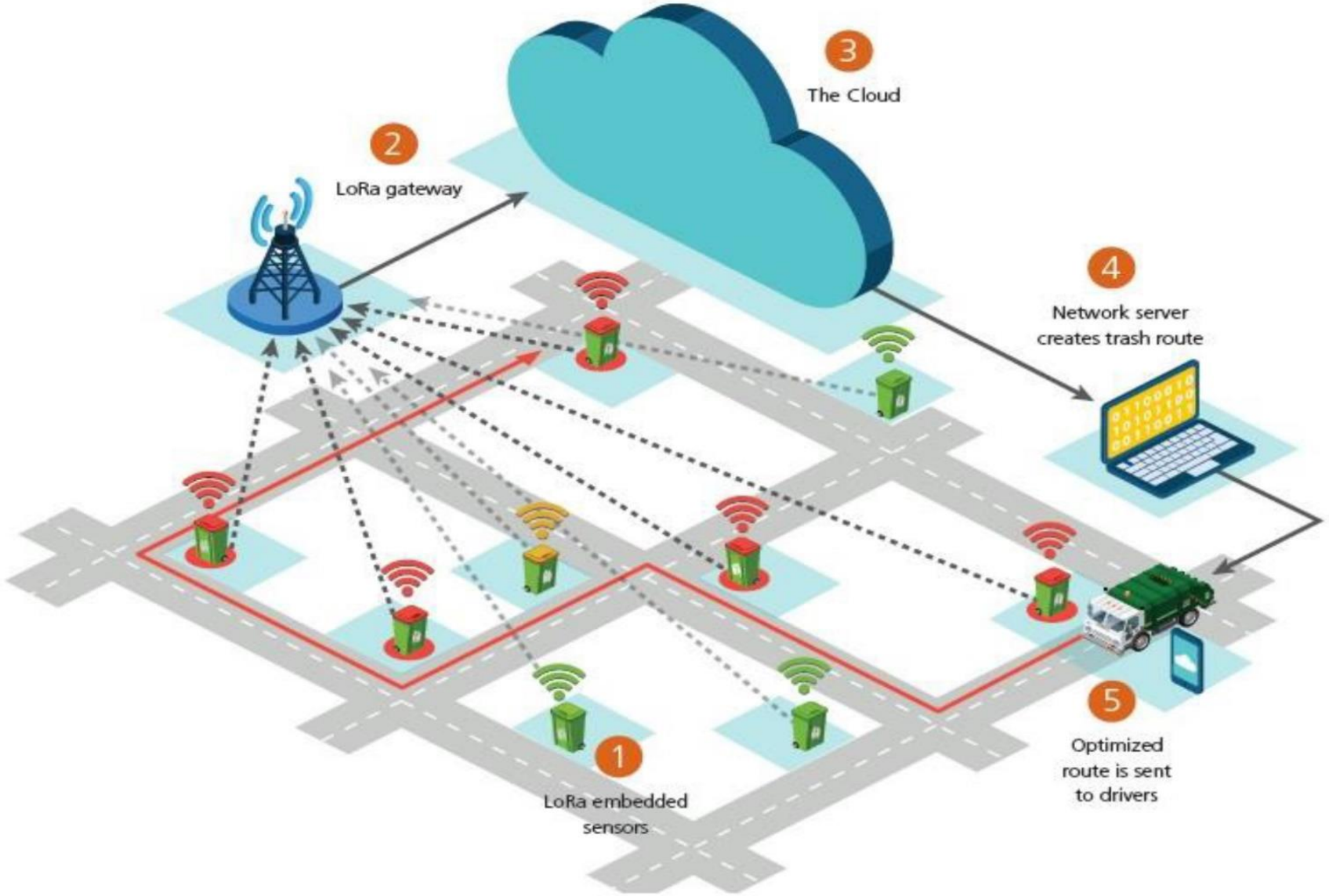
IOT and LORAWAN, Quaenet, 2018

LoRaWAN Use Case- Asset Management

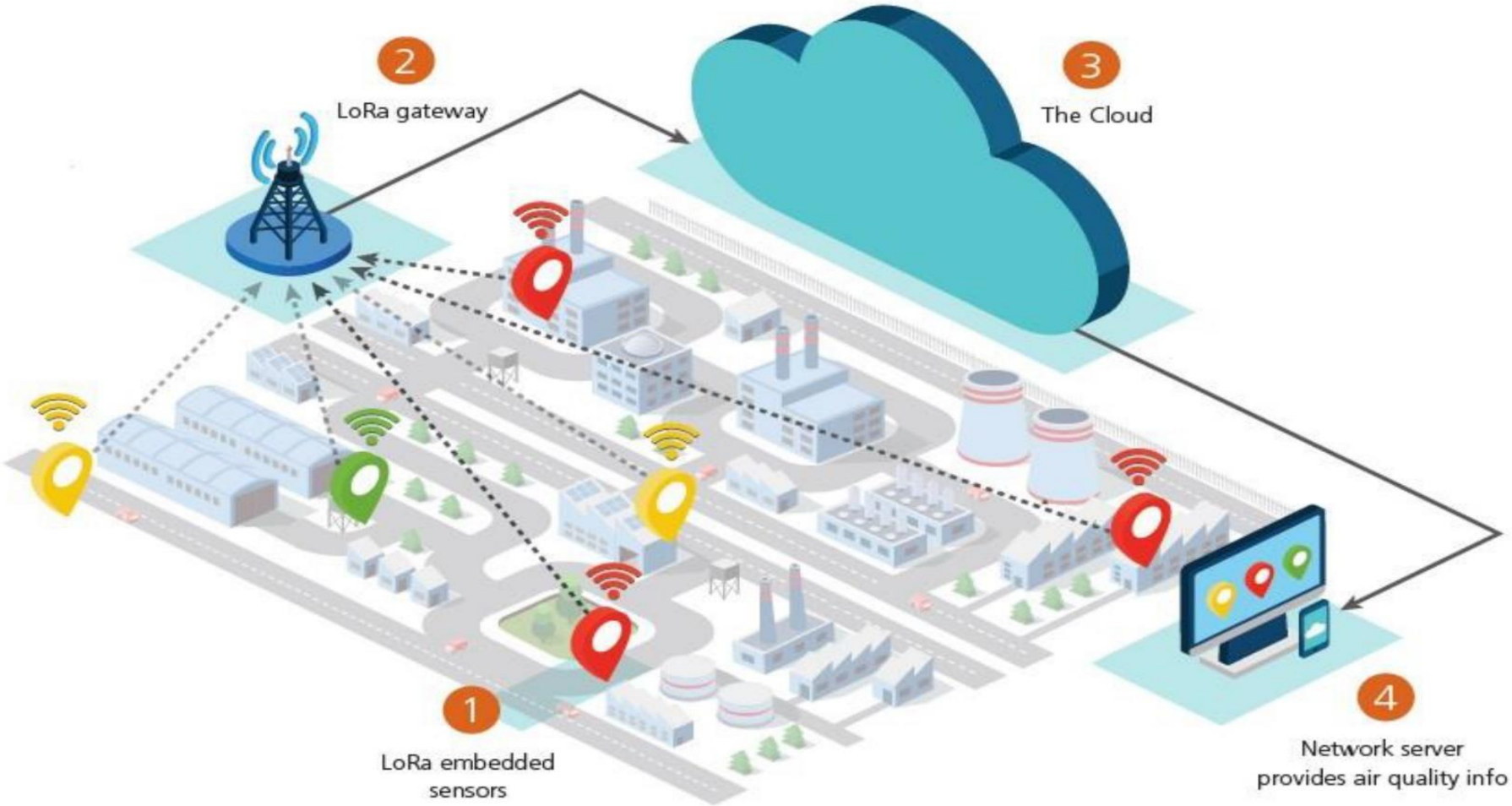


IOT and LORAWAN, Quaenet, 2018

LoRaWAN Use Case- Smart Waste Management

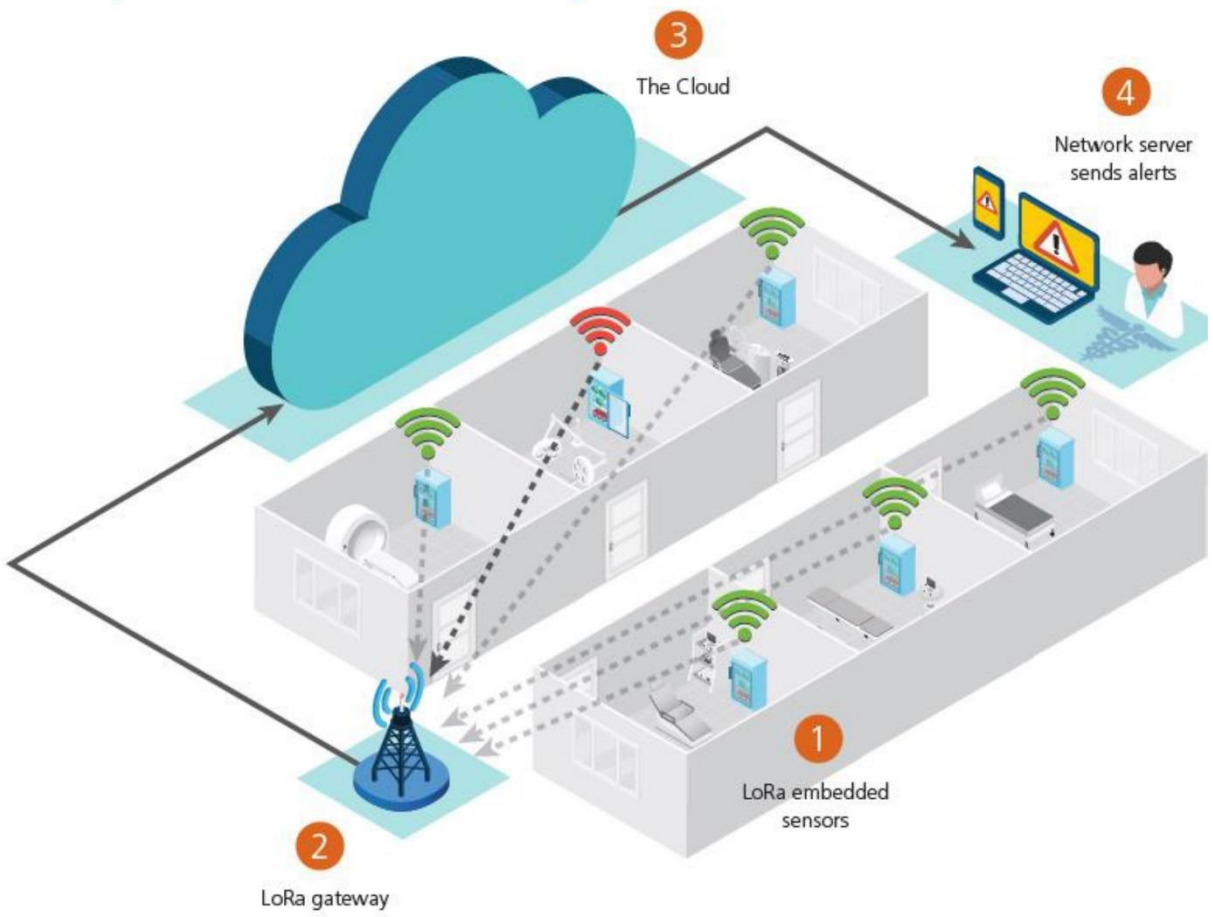


LoRaWAN Use Case- Smart Environment



IOT and LORAWAN, Quaenet, 2018

LoRaWAN Use Case- Cold Storage Monitoring



IOT and LORAWAN, Quaenet, 2018

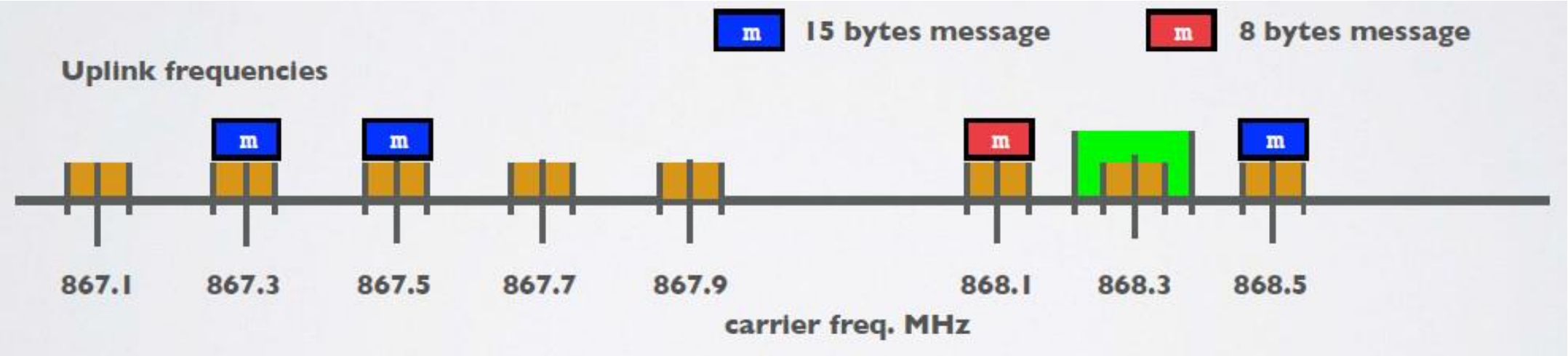
LoRaWAN- Physical Layer

- LoRaWAN 1.0.2 regional specifications describe the use of the main unlicensed sub-GHz frequency bands of
  - 433 MHz,
  - 779–787 MHz,
  - 863–870 MHz,
  - and 902–928 MHz,
  - as well as regional profiles for a subset of the 902–928 MHz bandwidth
    - For example, Australia utilizes 915–928 MHz frequency bands, while South Korea uses 920–923 MHz and Japan uses 920–928 MHz.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

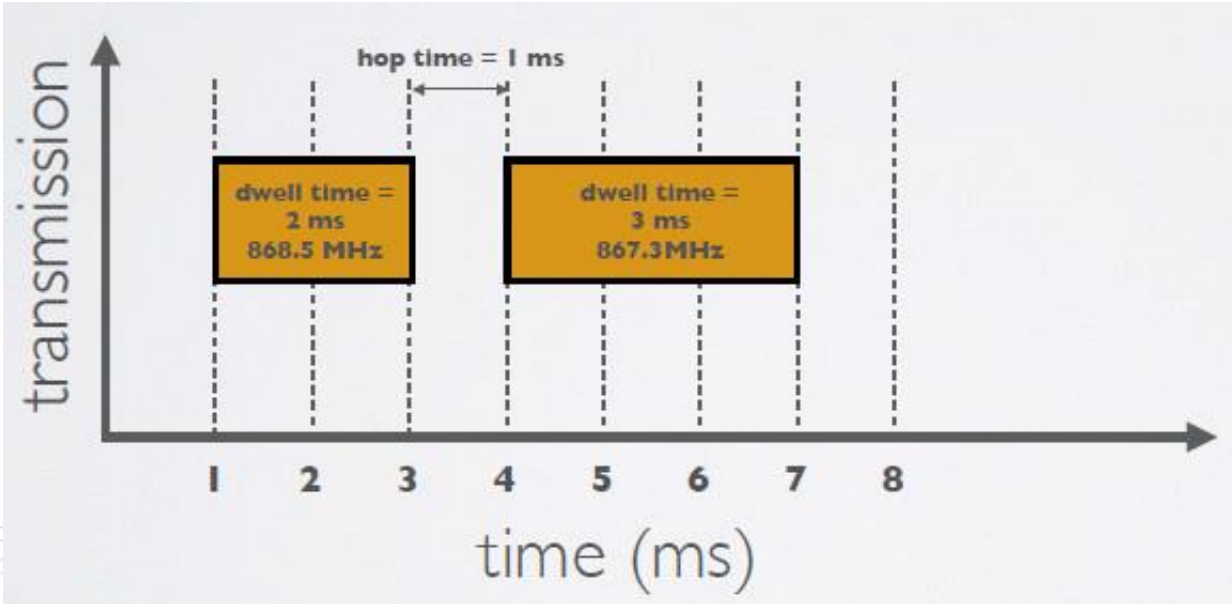
Changing Frequency for Every Transmission

- An end device changes channel in a pseudo-random fashion for every transmission. Changing frequencies makes the system more robust to interferences.
- For example in Europe for uplink transmissions 8 different frequencies are used.



Dwell Time & Hop Time

- Dwell time (or transmit time) is the amount of time needed to transmit on a frequency.
- Hop time is the amount of time needed to change from one frequency to another in which the radio is not transmitting



ISM Band and Duty Cycle

- In Europe when using the ISM band frequencies (863 MHz - 870 MHz) users must comply to the following rules:
  - For uplink, the maximum transmission power is limited to 25mW (14 dBm).
  - For downlink (for 869.525MHz), the maximum transmission power is limited to 0.5W (27 dBm)
  - There is an 0.1% and 1.0% duty cycle per day depending on the channel.

- Besides these ISM band rules, the network service provider (for example The Things Network) can also add additional restrictions.

Time on Air (ToA)

- When a signal is send from a sender it takes a certain amount of time before a receiver receives this signal. This time is called Time on Air (ToA).

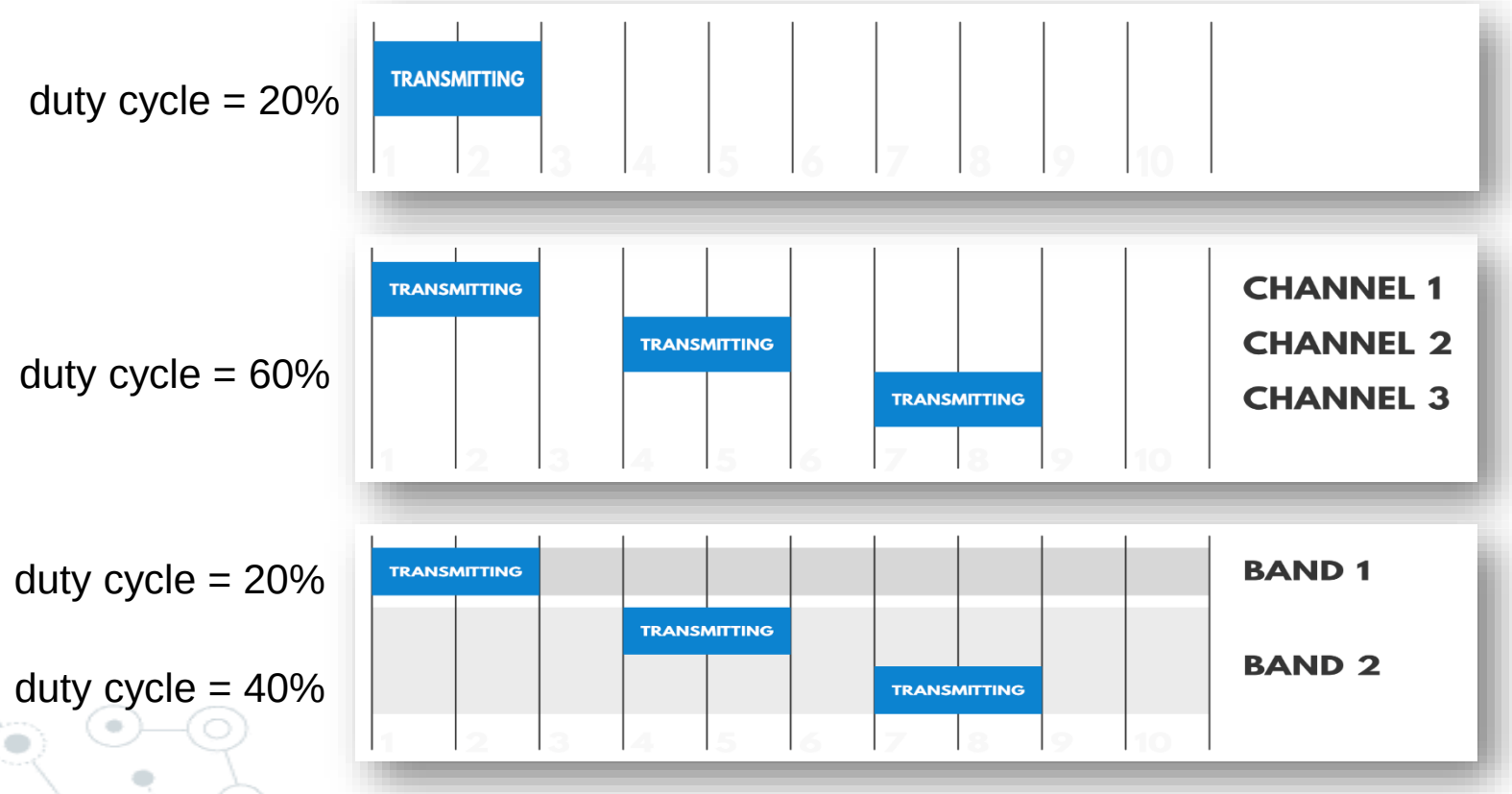
Time on Air (ToA)

- Duty cycle is the proportion of time during which a component, device, or system is operated. The duty cycle can be expressed as a ratio or as a percentage.

- As mentioned previously in Europe there is a 0.1% and 1.0% duty cycle per day depending on the channel.

Duty Cycle

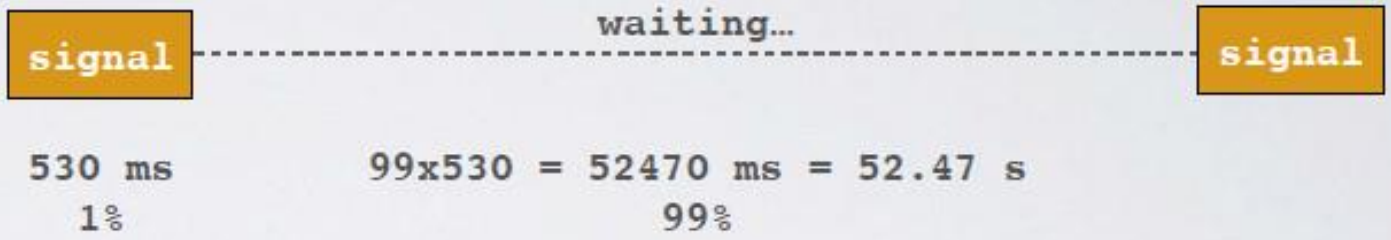
- Duty-cycle regulations in the ISM bands: The maximum time each device may occupy the channel



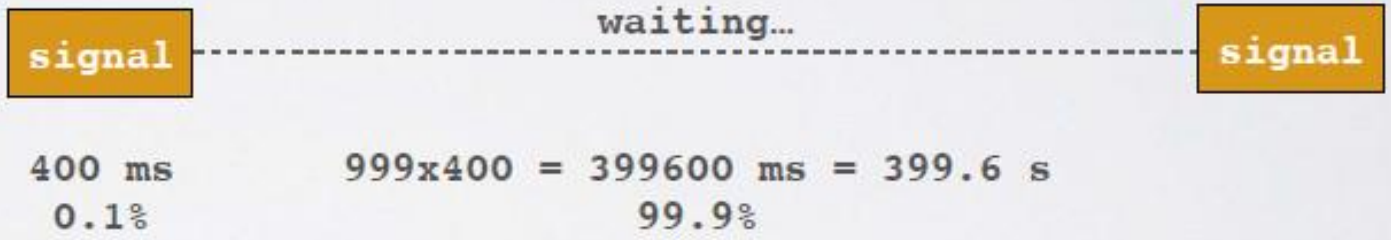
[8] ” Duty Cycle for LoRaWAN Devices”, https://www.thethingsnetwork.org/docs/lorawan/duty-cycle.html

Duty Cycle

For example:
Time on Air = 530 ms
Duty cycle = 1%



For example:
Time on Air = 400 ms
Duty cycle = 0.1%



Duty Cycle

- Each device must be silent in the sub-band for a minimum off-period:

$$T_s = T_a(\frac{1}{d} - 1)$$

where

  - d is the maximum duty-cycle in a sub-band, and
  - T_a is the packet transmission time, known as Time On Air

- Examples: Let assume $d = 0.01$ (1%, as in EU 868 MHz ISM band)
  - For duty-cycle $T_s = 1\ hour = 3600\ s$, we have:

$$3600 = T_a(100 - 1) = 3600 = T_a 99 \longrightarrow T_a = 36.36\ Sec$$

    - i.e., a maximum transmission time of 36.36 sec/hour in each sub-band for each end-device
  - For a use-case with packet transmission time of $T_a = 56\ ms$, we have:

$$T_s = 56(100 - 1) = 5.544\ sec$$

    - For every 56 ms transmission, the sub-band is not available for 5544 ms (a transmission of 56 ms per 5544 ms in each sub-band for each end-device)

[9] Ferran Adelantado,Xavier Vilajosana,Pere Tuset-Peiro,Borja Martinez,and oan Melia, “Understanding the limits of LoRaWAN”, IEEE Communications Magazine, 8 September 2017, Vol.55

LoRaWAN- Physical Layer

- Semtech LoRa modulation is based on chirp spread spectrum modulation, which trades a lower data rate for receiver sensitivity to significantly increase the communication distance.

- It allows demodulation below the noise floor, offers robustness to noise and interference, and manages a single channel occupation by different spreading factors.

- An important feature of LoRa is its ability to handle various data rates via the spreading factor.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN- Physical Layer

- Semtech LoRa modulation is based on chirp spread spectrum modulation, which trades a lower data rate for receiver sensitivity to significantly increase the communication distance.

- It allows demodulation below the noise floor, offers robustness to noise and interference, and manages a single channel occupation by different spreading factors.

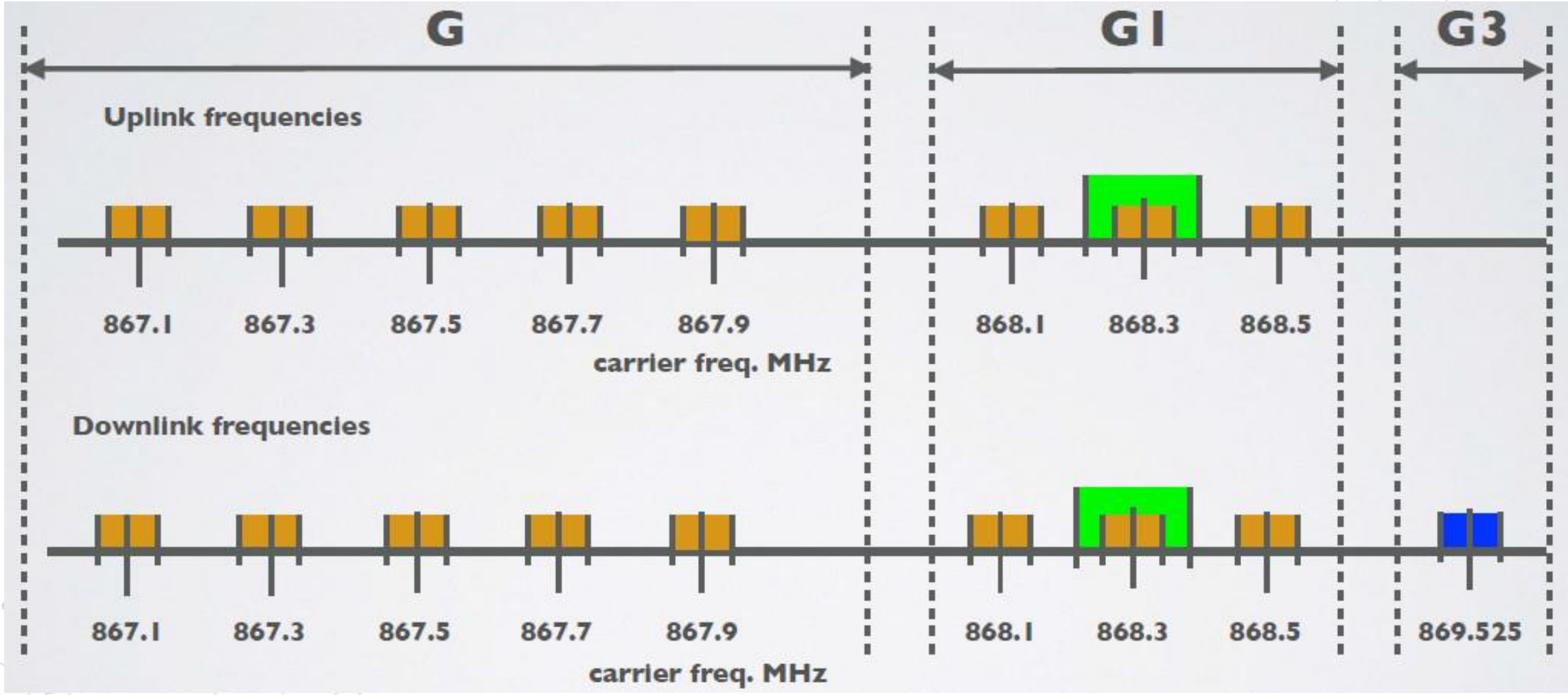
- An important feature of LoRa is its ability to handle various data rates via the spreading factor.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN- Physical Layer

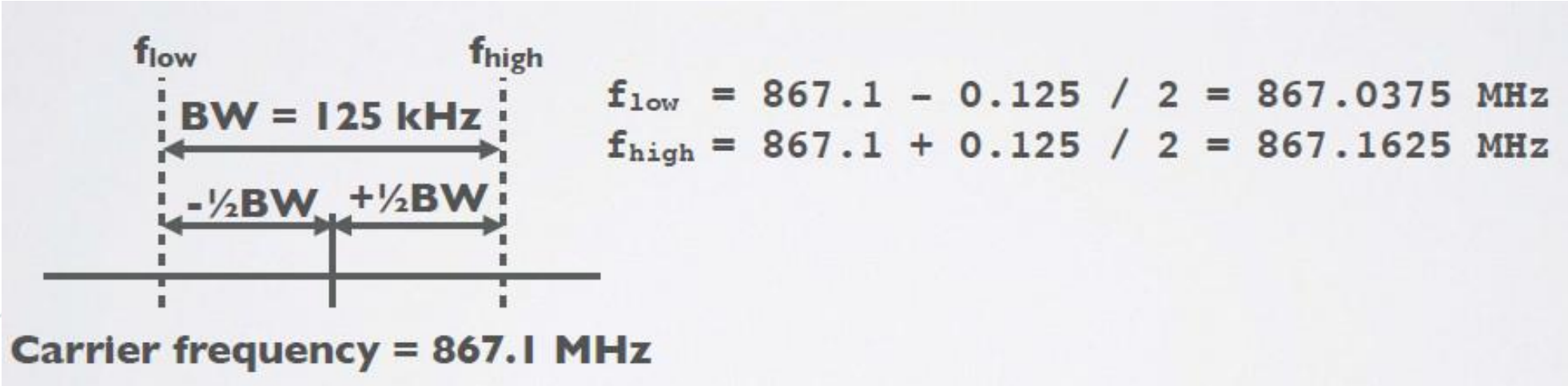
- In most cases LoRaWAN uses LoRa modulation.
  - LoRa modulation is based on Chirp spread- spectrum technology, which makes it work well with channel noise, multipath fading and the Doppler effect, even at low power.
- The data rate depends on
  - bandwidth
  - spreading factor
- LoRaWAN can use channels with a bandwidth of either 125 kHz, 250 kHz or 500 kHz, depending on the region or the frequency plan.
- The spreading factor is chosen (SF7 to SF12) by the end-device and influences the time it takes to transmit a frame.

LoRaWAN- Physical Layer: EU863-870 Frequency and Sub-bands

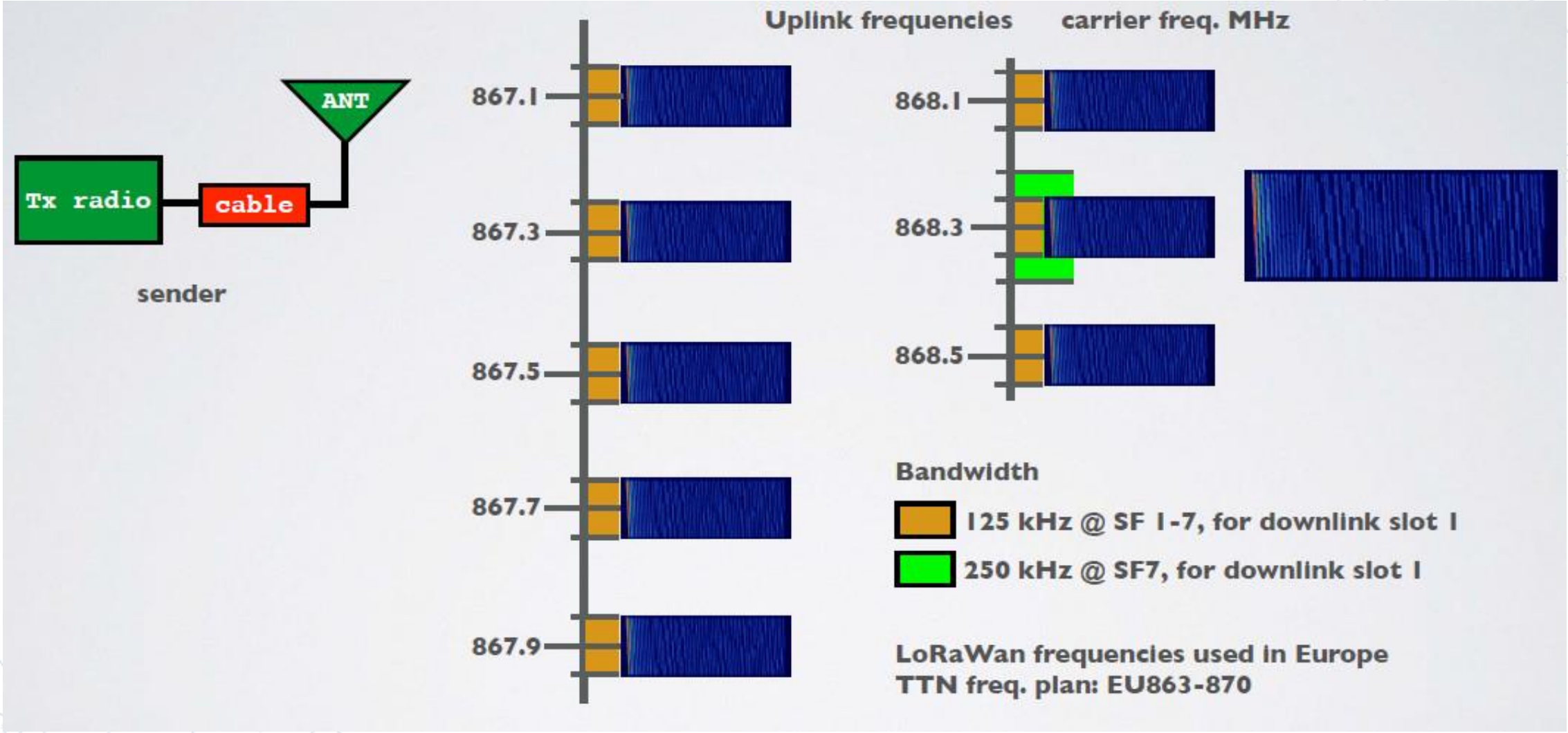


LoRaWAN- Physical Layer: Bandwidth

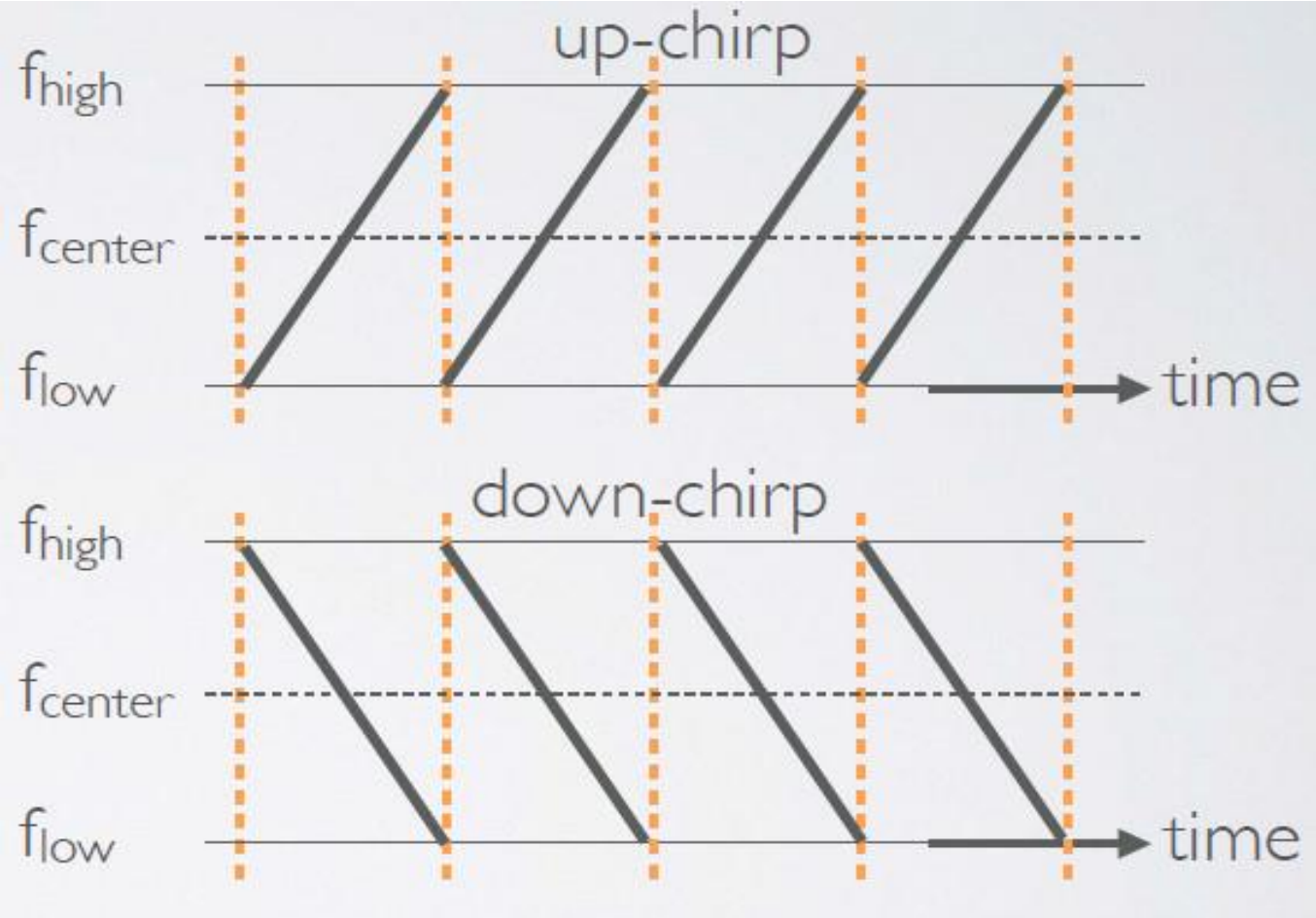
- LoRaWAN only uses the following bandwidth ranges: 125 kHz, 250 kHz and 500 kHz. Which of these 3 ranges are actual used depends on the region or frequency plan. For example in Europe only the bandwidths 125kHz and 250 kHz are used.
- The relationship between bandwidth and carrier frequency can be seen in the figure below.

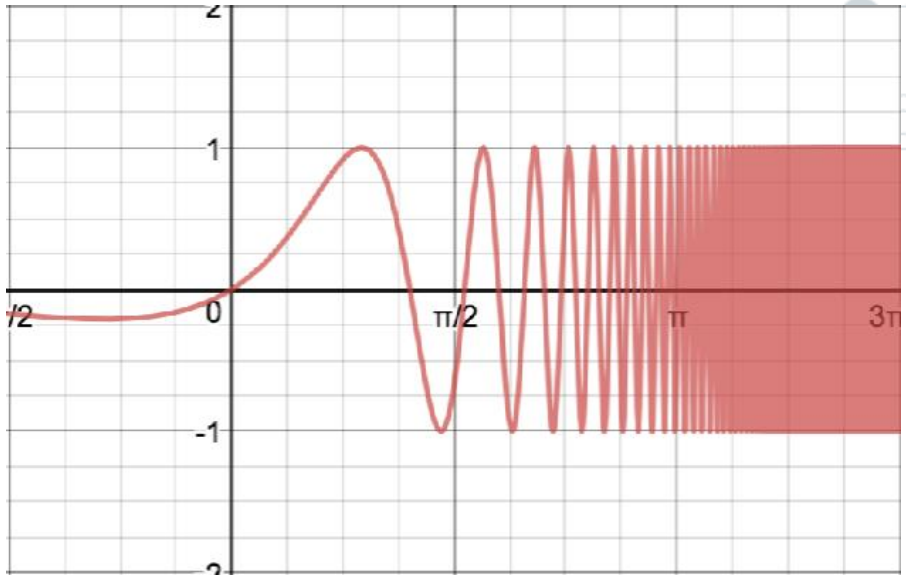


LoRaWAN- Physical Layer: Carriers Frequency and Bandwidth



LoRaWAN- Physical Layer: Chirps

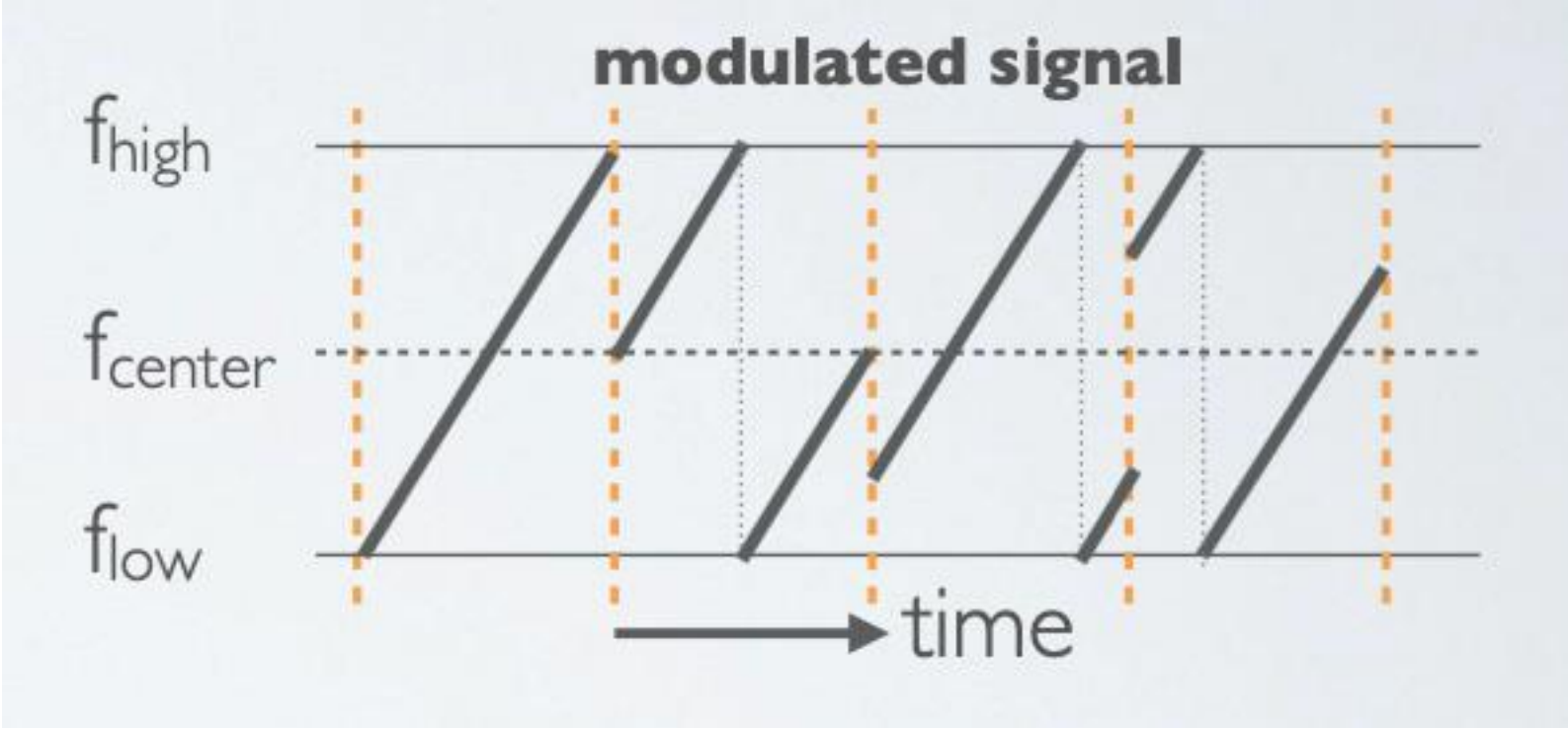




Example of an up-chirp where the frequency increases in time.

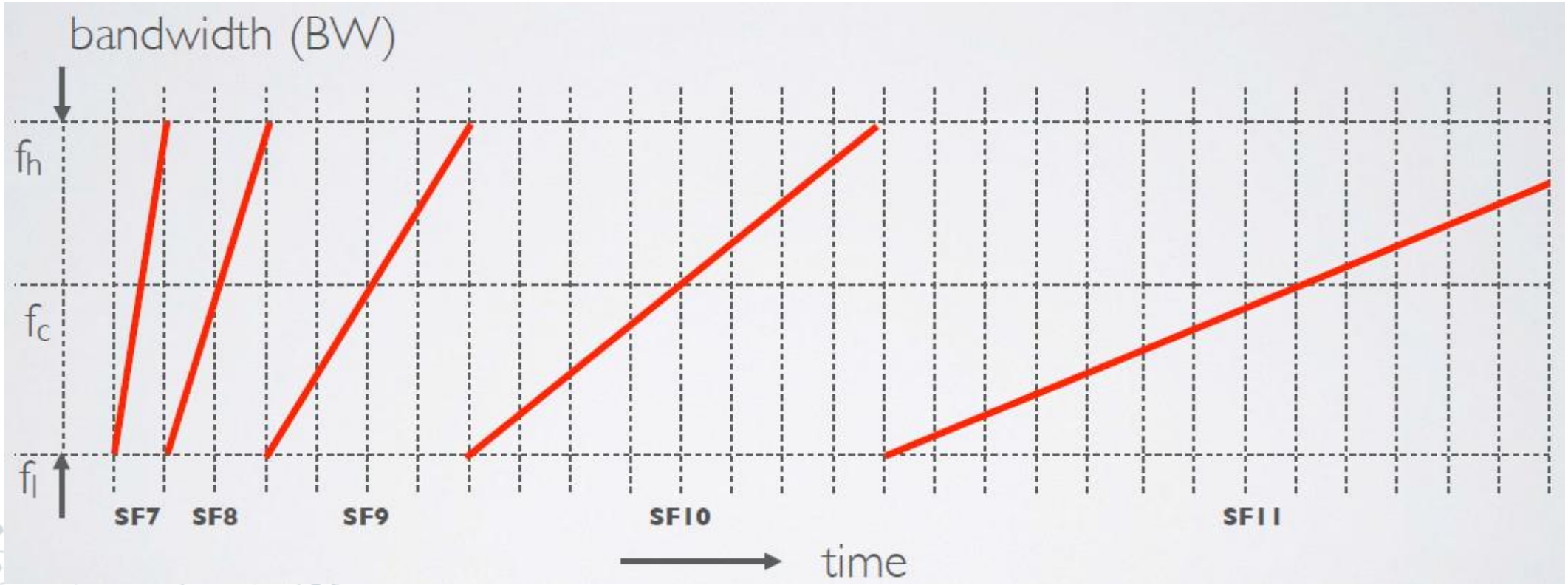
LoRaWAN- Physical Layer: Chirps

- The chirps are cyclically-shifted, and it is the frequency jumps that determines how the data is encoded onto the chirps, aka LoRa modulation.



LoRaWAN- Physical Layer

- An overview of symbol durations with respect to different Spreading Factors.
- If the SF increases by one the symbol duration doubles.

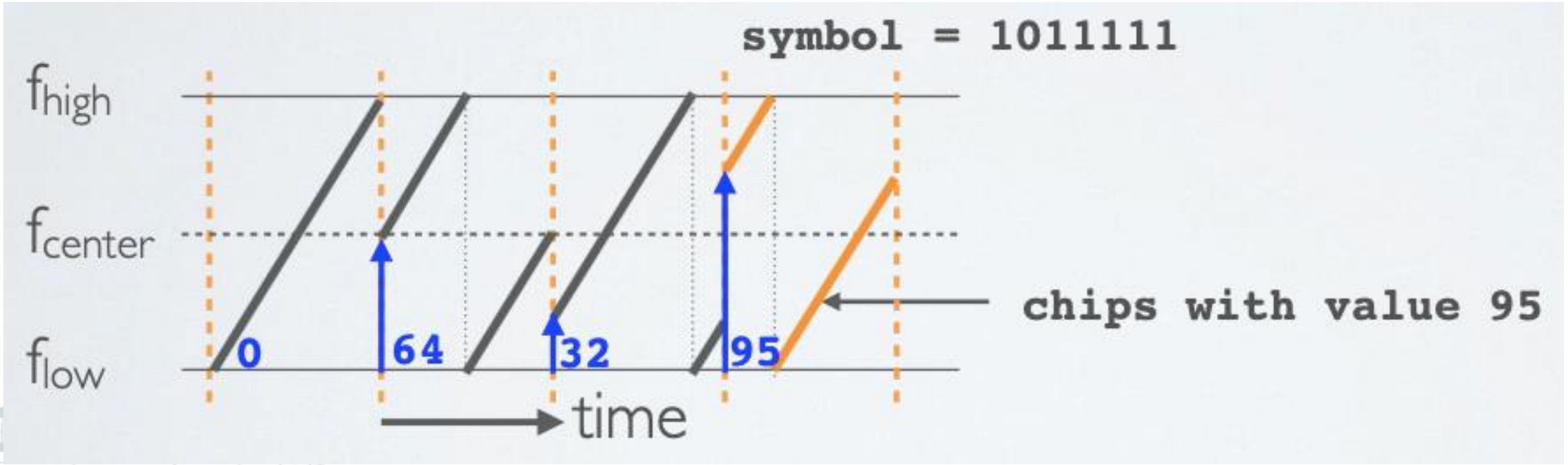


LoRaWAN- Physical Layer

- A symbol represents one, or more bits of data, for example: Symbol = 1011111 (decimal = 95)
- In the example above the number of raw bits that can be encoded by the symbol is 7. This is the same as saying: Spreading Factor (SF) = 7
- The symbol has 2^{SF} values. If SF=7, the values ranges from 0 - 127.
- The symbol value is encoded onto a sweep signal (up-chirp).

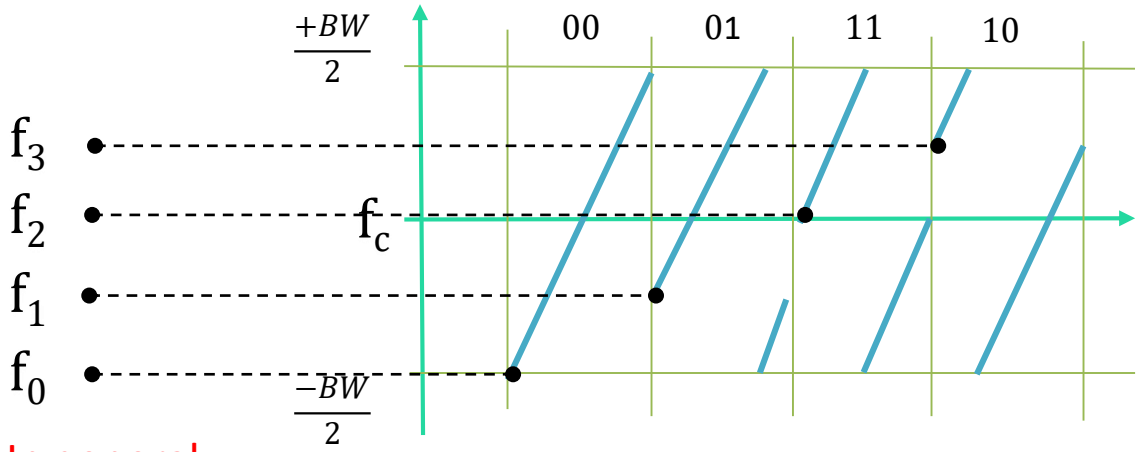
LoRaWAN- Physical Layer

- The sweep signal is divided into 2SF steps or chips.
- For example if the symbol is: 1011111 (decimal value = 95), the number of raw bits that can be encoded by this symbol is 7 (SF=7) and the sweep signal is divided in 2SF = 27 = 128 chips.



Technical overview CSS as a modulation for Long Range Communication

Example with $SF = 2$



$SF = 2$

The number of symbols $2^2 = 4$

each stating with different a frequencie of the set f_0, f_1, f_2, f

The number of bit carried by each chrip symbol = $\log_2 4$

In general

Spreading Factor = sf

The number of symbols: 2^{sf} each stating with different frequencies

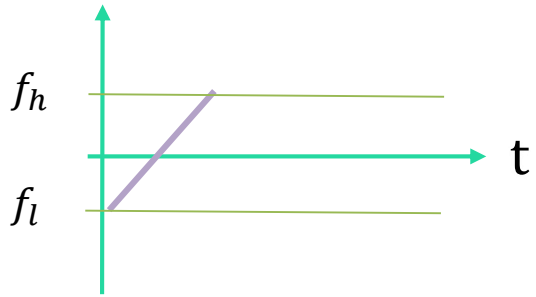
Frequencies = $f_0, \ldots, 2^{sf}$

The number of bit carried by each chrip symbol = $\log_2 s^{sf} = sf$

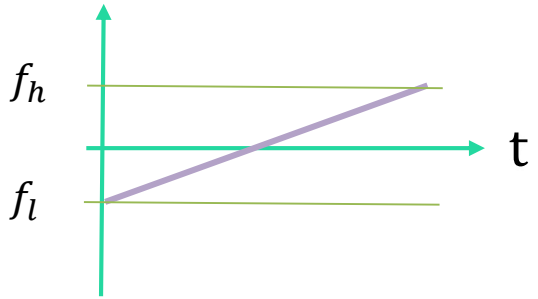
[7] V. Talla, M. Hessar, B. Kellogg, A. Najafi, J. R. Smith, S. Gollakota, “LoRa Backscatter: Enabling The Vision of Ubiquitous Connectivity”, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2017/9/11.

Technical overview CSS as a modulation for Long Range Communication

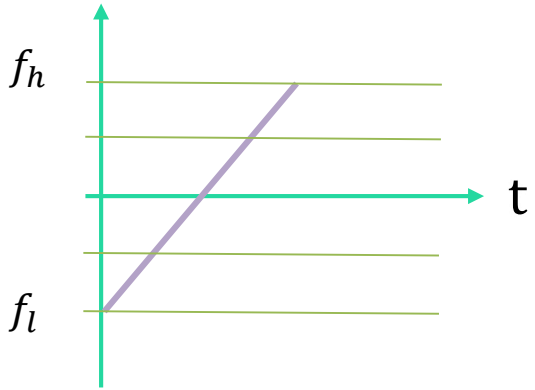
$SF = 7 \quad BW = 125kHz$



$SF = 8 \quad BW = 125kHz$



$SF = 8 \quad BW = 250kHz$



Spreading Factor $= sf$

The number of symbols: 2^{sf}

The number of bit carried by each chrip symbol $= \quad \log_2 2^{sf} = sf$

$$symbol\ time(s) = \frac{2^{sf}}{BW}$$

$$symbol\ rate(s) = \frac{BW}{2^{sf}}$$

$$bit\ rate(s) = \frac{BW}{2^{sf}} sf$$

[7] V. Talla, M. Hessar, B. Kellogg, A. Najafi, J. R. Smith, S. Gollakota, "LoRa Backscatter: Enabling The Vision of Ubiquitous Connectivity", Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2017/9/11.

LoRaWAN- Physical Layer

- The Data Rate Story: There are three physical factors:
  - **transmission power**,
  - **bandwidth**
  - **spreading factor**

- If you lower the tx power, you'll save battery, but the range of the signal will obviously be shorter.

- The other two factors (spreading factor and bandwidth) combined form the data rate. This determines how fast bytes are transmitted.

LoRaWAN- Physical Layer

- Bandwidth is interchangeable with chip rate:
-
- BW = **R_c** = chip rate (chips/s)
- For example: if BW = 125 kHz, then BW = R_c = 125000 chips/s
- The Symbol Rate (R_s) is calculated as follow: **R_s (symbols/sec) = BW / 2^{SF} = R_c / 2^{SF}**
- For example: If BW = 125 kHz, SF=7, then R_s = 125000 / 2^7 = 977 symbols/sec
- The symbol duration or sweep time is calculated as follow: **T_s(sec) = 2^{SF} / BW**

LoRaWAN- Physical Layer

- If you increase the data rate (make the bandwidth wider or the spreading factor lower) you can transmit those bytes in a shorter time.

- Making the bandwidth 2x wider (from BW125 to BW250) approximately allows you to send 2x more bytes in the same time.

LoRaWAN- Physical Layer

- Spreading Factor
  - Devices with a low spreading factor (SF) achieve less distance in their communications but transmit at faster speeds, resulting in less airtime.
  - A higher SF provides slower transmission rates but achieves a higher reliability at longer distances.
- Making the spreading factor 1 step lower (ex. from SF10 to SF9) allows you to send 2x more bytes in the same time.
  - Lowering the spreading factor makes it more difficult for the gateway to receive a transmission, as it will be more sensitive to noise.
  - You could compare this to two people taking in a noisy place. If you're far from each other, you have to talk slow (SF10), but if you're close, you can talk faster (SF7)

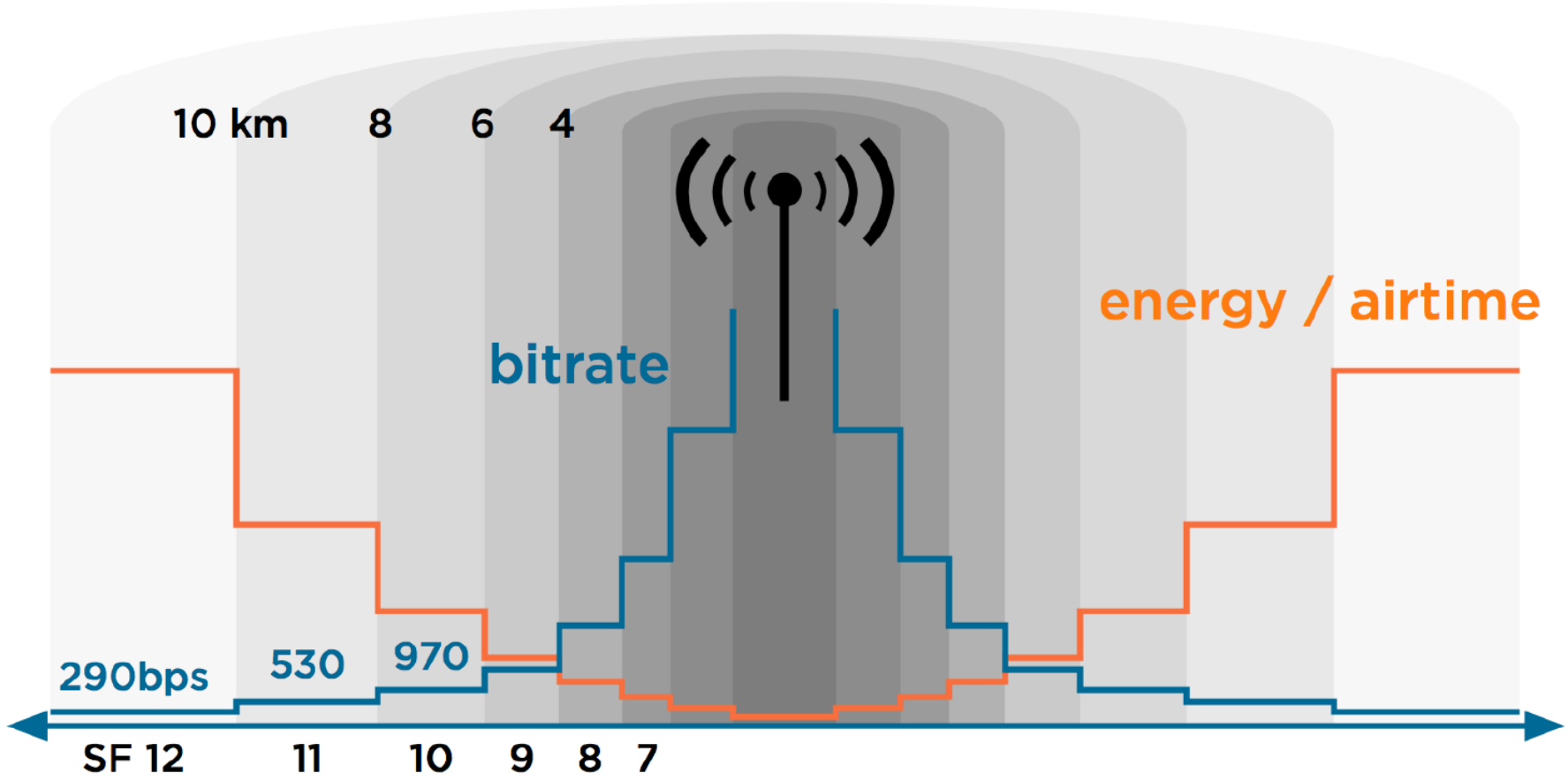
* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN- Physical Layer

Spreading factor (at 125 kHz)	Bitrate	Range (indicative value, depending on propagation conditions)	Time on Air (ms) For 10 Bytes app payload
SF7	5470 bps	2 km	56 ms
SF8	3125 bps	4 km	100 ms
SF9	1760 bps	6 km	200 ms
SF10	980 bps	8 km	370 ms
SF11	440 bps	11 km	740 ms
SF12	290 bps	14 km	1400 ms

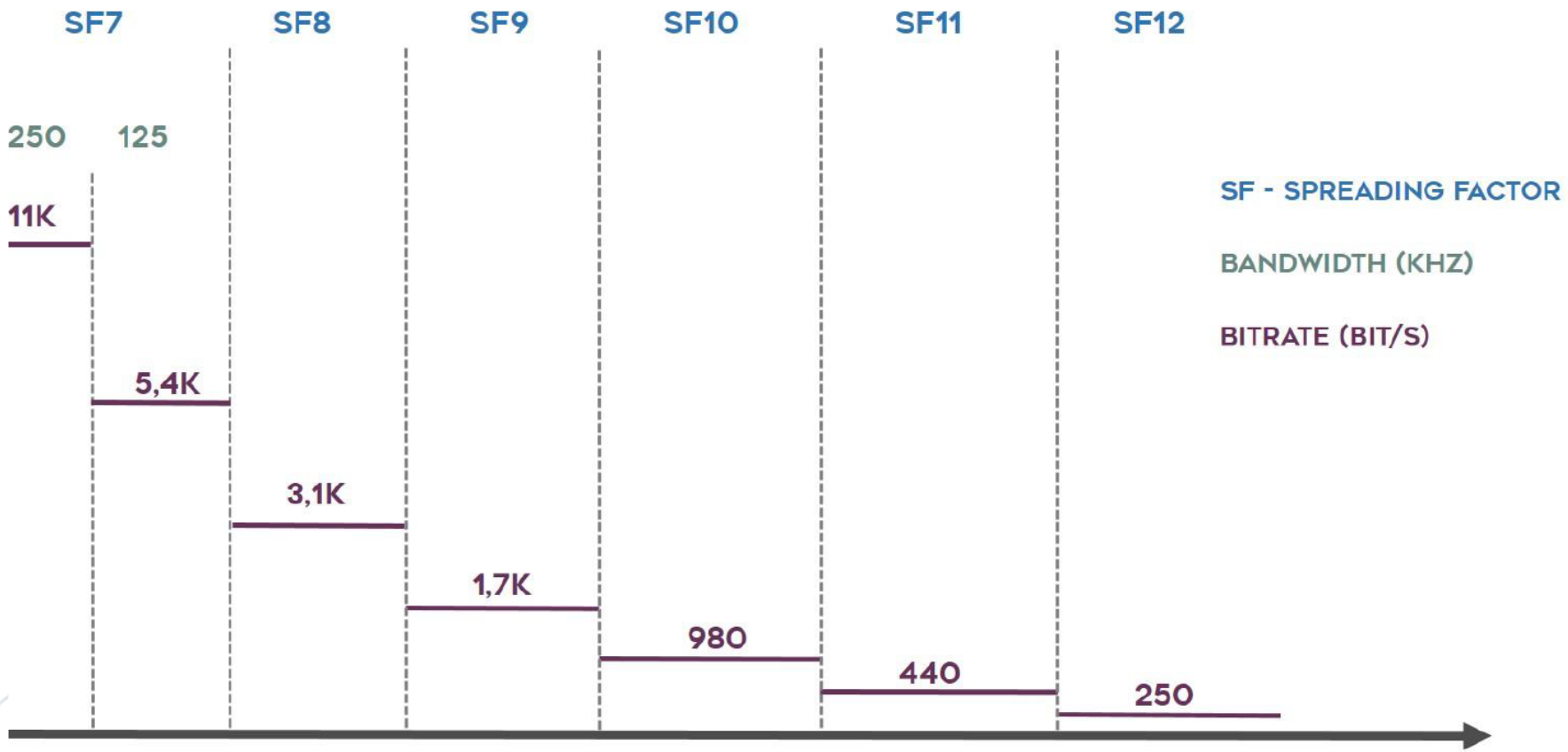
(with coding rate 4/5 ; bandwidth 125Khz ; Packet Error Rate (PER): 1%)

LoRaWAN- Physical Layer



http://www.linuxembedded.fr/2017/12/introduction-a-lora/

LoRaWAN- Physical Layer



LoRaWAN- Adaptive Data Rate

- Adaptive Data Rate (ADR) is a mechanism for optimizing data rates, airtime and energy consumption in the network.

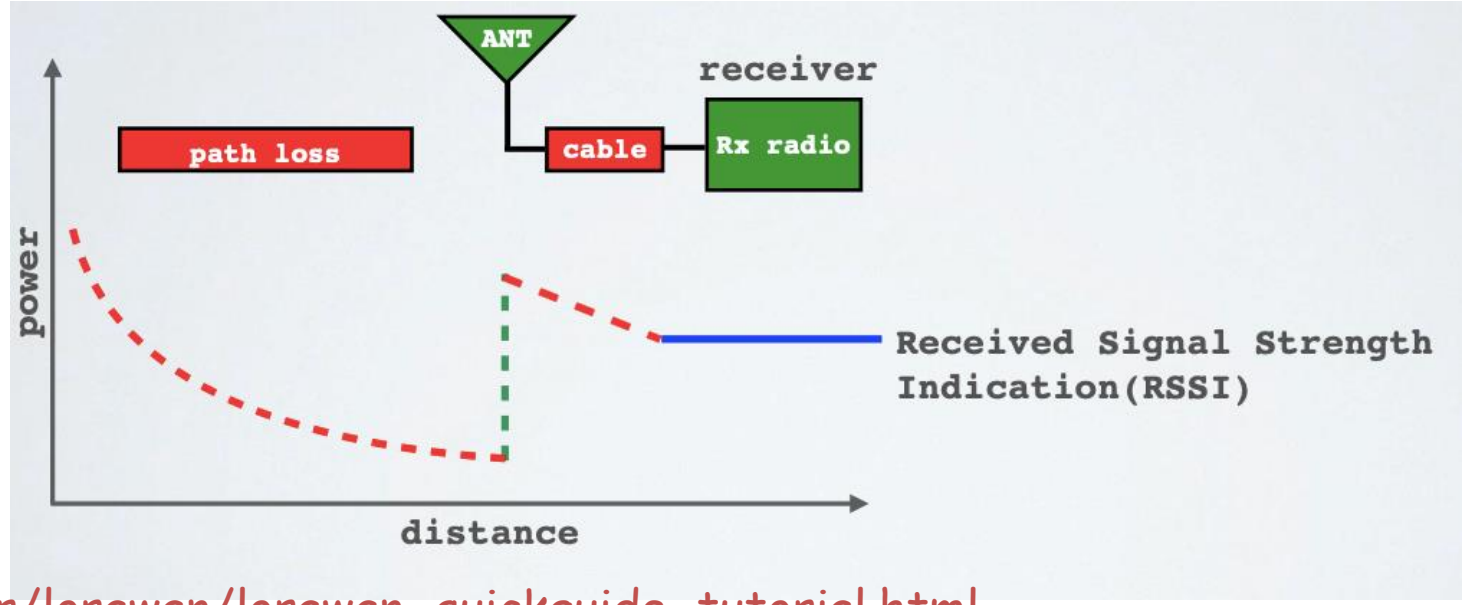
- End devices decide if ADR should be used or not, not the application or the network.

Adaptive Data Rate

- The LoRaWAN protocol defines the Adaptive Data Rate (ADR) scheme to control
- the uplink transmission parameters of LoRa devices:
  - Spreading Factor (SF)
  - Bandwidth (BW) Transmission parameters
  - Transmission power
- Whether the ADR functionality will be used is requested by the end nodes by setting the ADR flag in the uplink message. If the ADR flag is set, the network server can control the end node's transmission parameters.
- ADR should only be used in stable Radio Frequency (RF) situations where end nodes do not move. Mobile end nodes which are stationary for longer times can enable ADR during those times.

LoRaWAN- Physical Layer

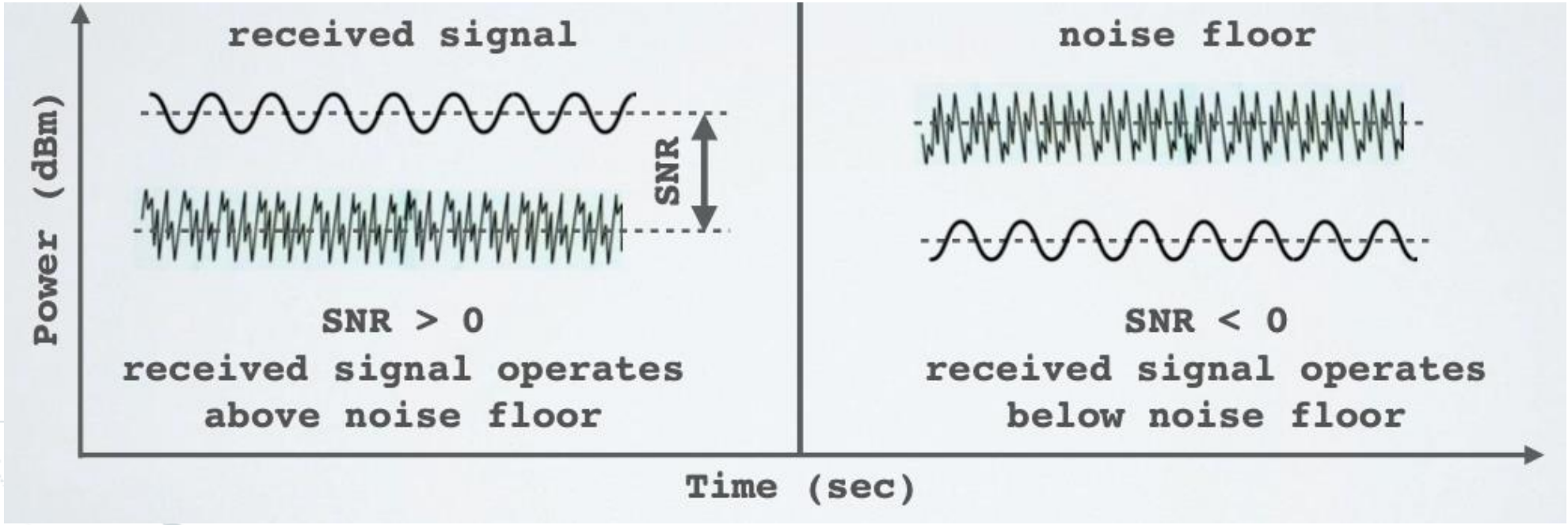
- The Received Signal Strength Indication (RSSI) is the received signal power in milliwatts and is measured in dBm. This value can be used as a measurement of how well a receiver can "hear" a signal from a sender.
- The RSSI is measured in dBm and is a negative value. The closer to 0 the better the signal is.



* https://www.mobilefish.com/developer/lorawan/lorawan_quickguide_tutorial.html

LoRaWAN- Physical Layer

- Signal-to-Noise Ratio (SNR) is the ratio between the received power signal and the noise floor power level.
- The noise floor is an area of all unwanted interfering signal sources which can corrupt the transmitted signal and therefore re-transmissions will occur.
- Typical LoRa SNR values are between: -20dB and +10dB



LoRaWAN- MAC Layer

- LoRaWAN- MAC layer
  - This layer takes advantage of the LoRa physical layer and classifies LoRaWAN endpoints to optimize their battery life and ensure downstream communications to the LoRaWAN endpoints.
  - The classes of LoRaWAN devices:
    - **Class A**: This class is the default implementation. Optimized for battery-powered nodes, it allows bidirectional communications.
    - **Class B**: A Class B node or endpoint should get additional receive windows compared to Class A, but gateways must be synchronized through a beaconing process.
    - **Class C**: This class is particularly adapted for powered nodes.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN- MAC Layer

- Class A
  - UL anytime, DL only at well-defined slots after UL
  - Battery-powered sensors
- Class B
  - UL anytime, DL at scheduled slots
  - Battery-powered actuators
- Class C
  - UL and DL anytime
  - Mains-powered devices.

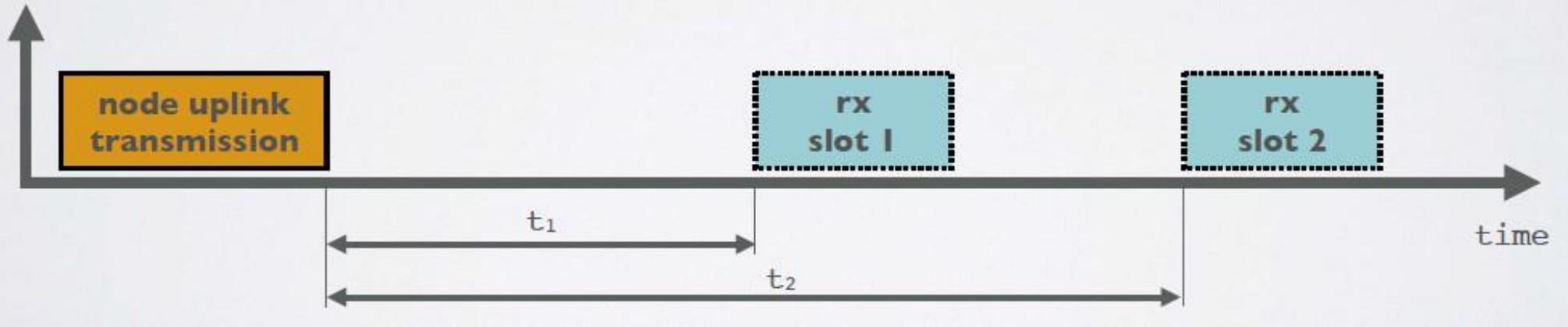
LoRaWAN Device Classes

- The LoRaWAN specification defines three device classes:

Class	Description
A(II)	Battery powered devices. Each device uplink to the gateway and is followed by two short downlink receive windows.
B(eacon)	Same as class A but these devices also opens extra receive windows at scheduled times.
C(ontinuos)	Same as A but these devices are continuously listening. Hence these devices uses more power and are often mains powered.

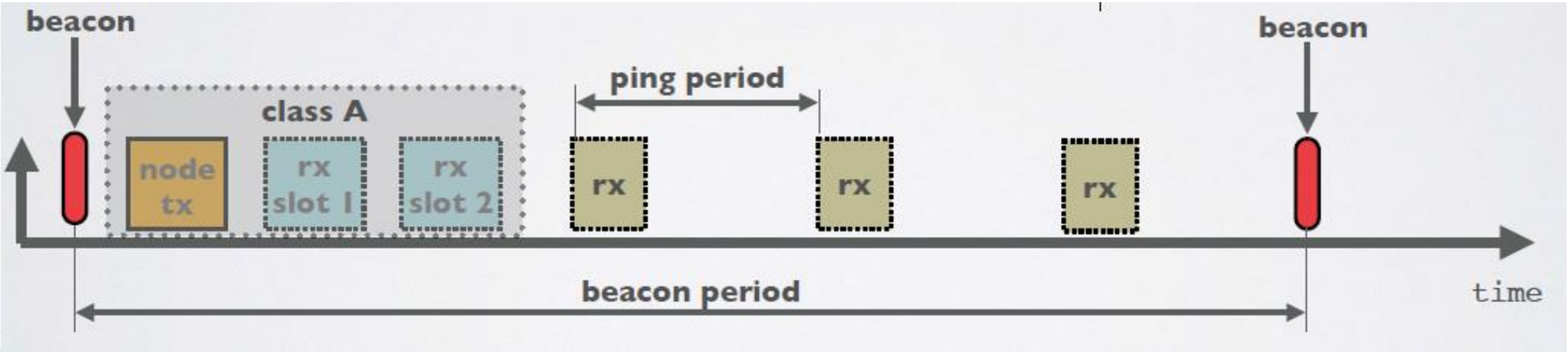
CLASS A

- At any time an end node can broadcast a signal. After this uplink transmission (tx) the end node will listen for a response from the gateway.
- The end node opens two receive slots at t1 and t2 seconds after an uplink transmission. The gateway can respond within the first receive slot or the second receive slot, but not both.
- Class B and C devices must also support class A functionality.



CLASS B

- In addition to Class A receive slots, class B devices opens extra receive slots at scheduled times.
- The end node receives a time synchronized beacon from the gateway, allowing the gateway to know when the node is listening.
- A class B device does not support device C functionality.

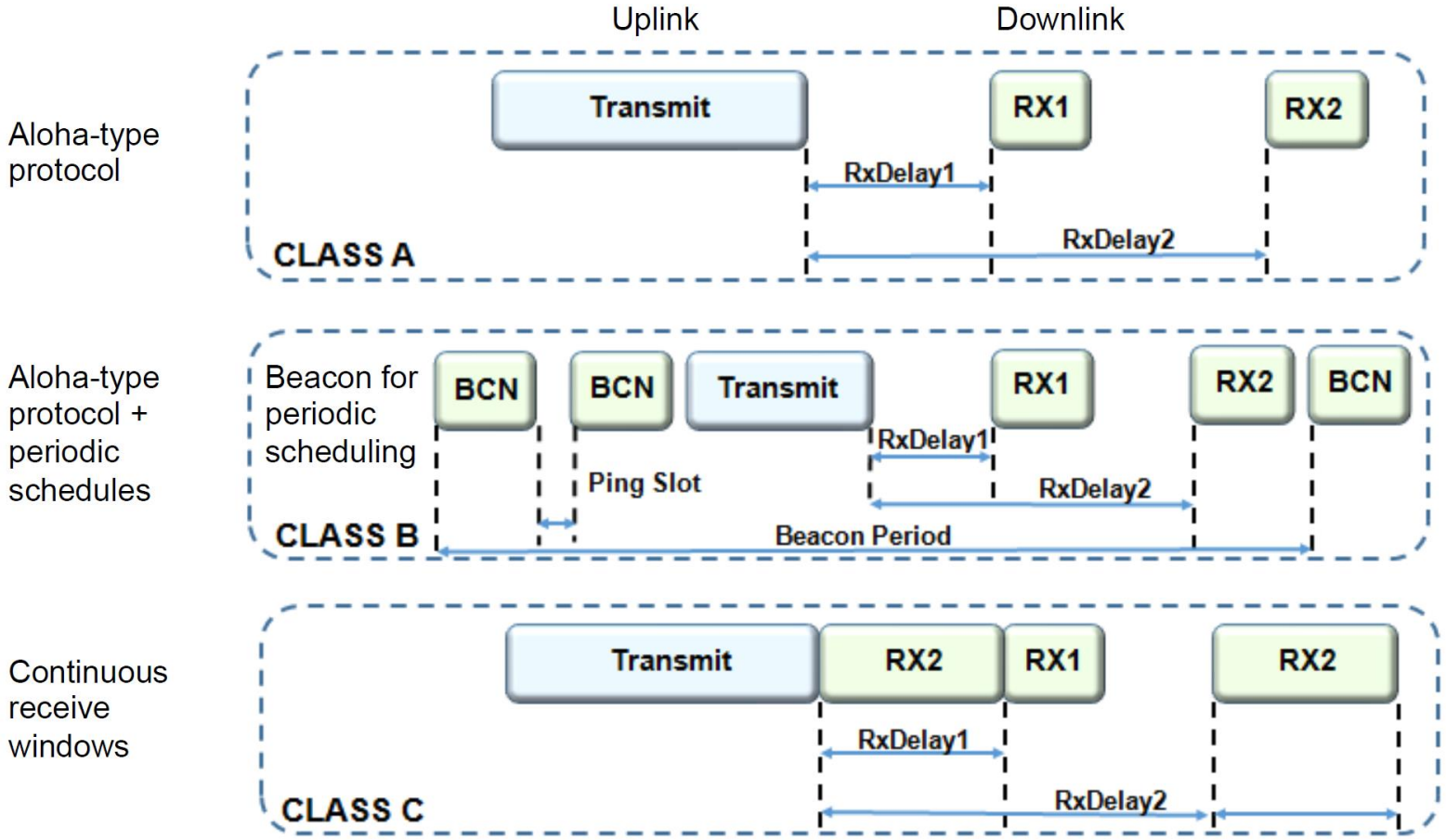


CLASS C

- In addition to Class A receive slots a class C device will listen continuously for responses from the gateway.
- A class C device does not support device B functionality.

LoRaWAN Device Classes

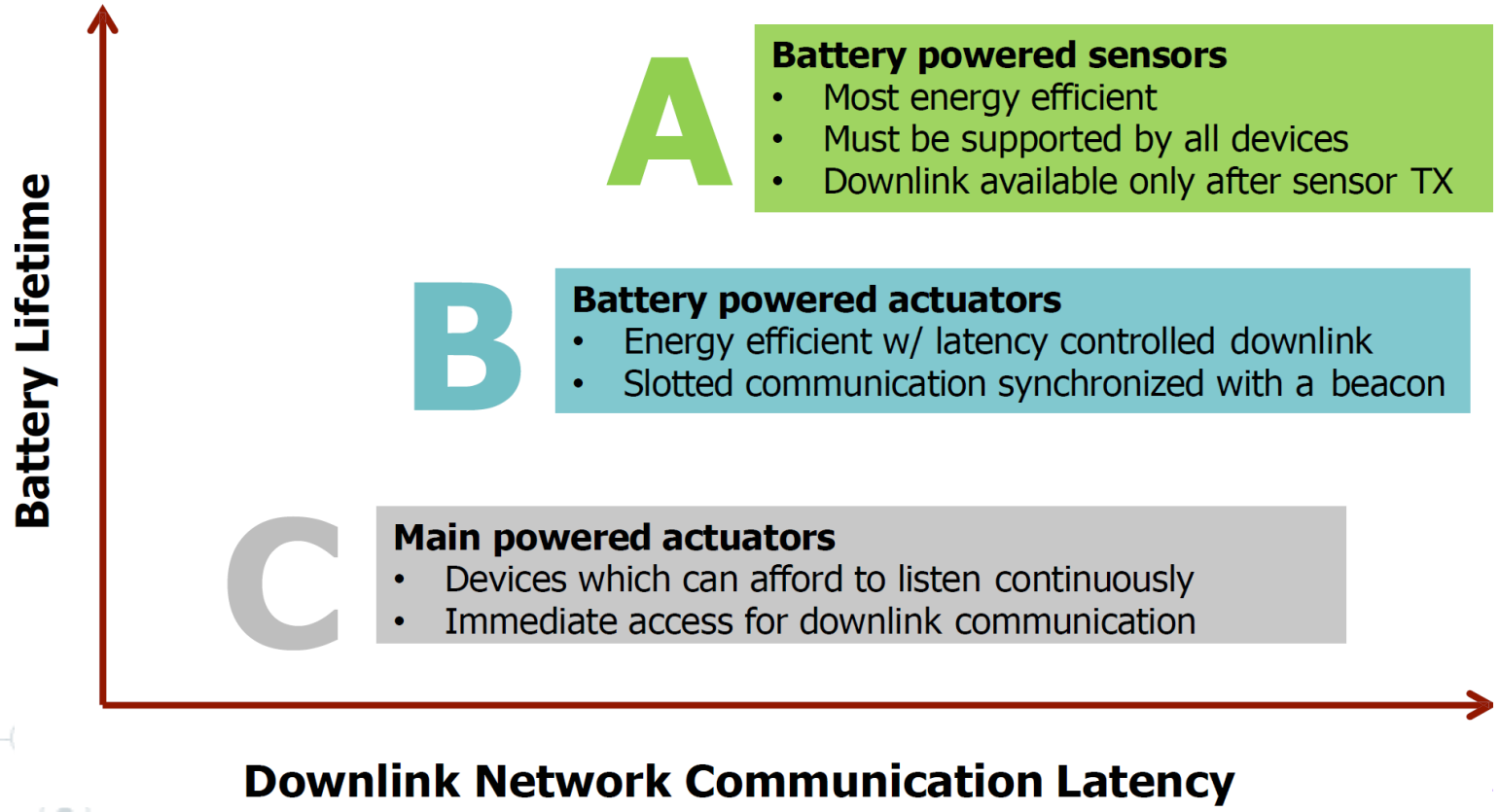
- LoRaWAN Protocol End-Device Classes



J. Silva, etl, LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities, 2th Int. Multidisciplinary Conf. on Computer and Energy Science, 2017

LoRaWAN Device Classes

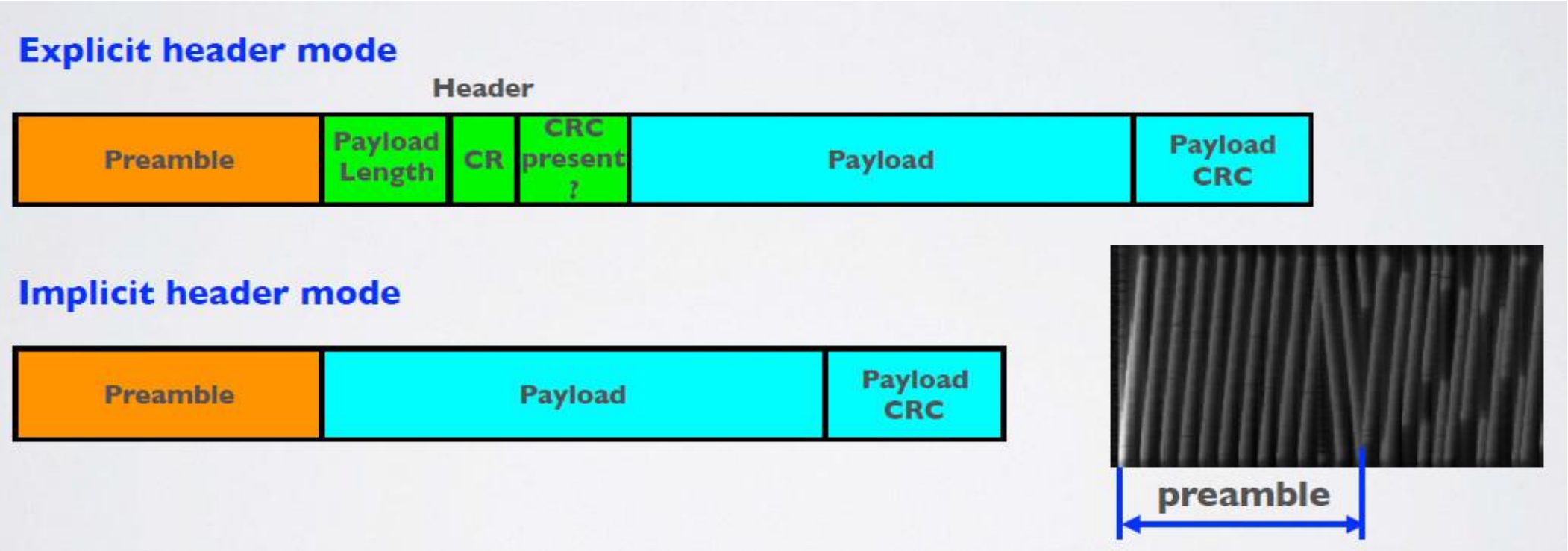
- LoRaWAN Protocol End-Device Classes



J. Silva, etl, LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities, 2th Int. Multidisciplinary Conf. on Computer and Energy Science, 2017

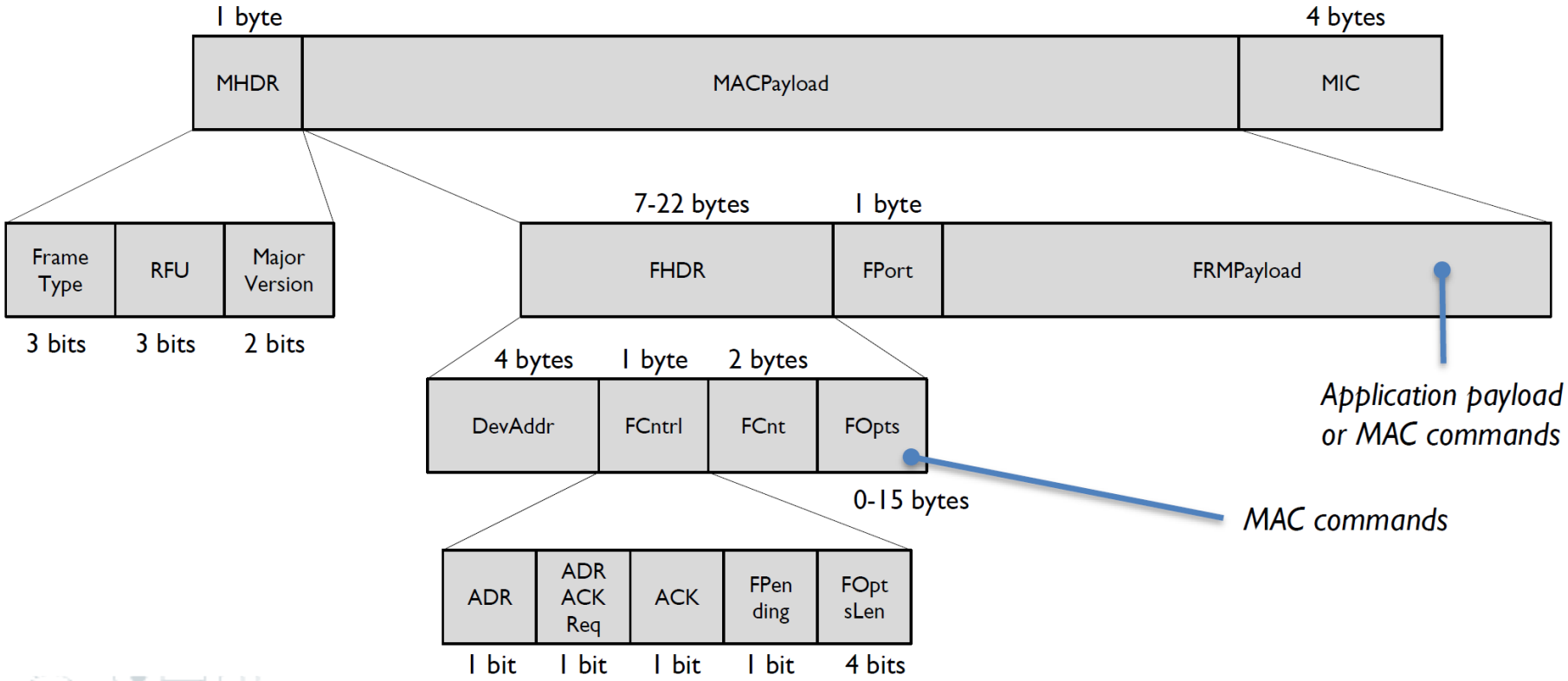
LorRa Packet Format

- The LoRa packet comprises of three elements: Preamble, header (optional) and payload.



LorRa Frame Format

- The LoRa packet comprises of three elements: Preamble, header (optional) and payload.



LorRa Packet Format

- There are two types of LoRa packet format modes:
  - **Explicit header mode:**
    - Includes a short header that contains information about the payload length, coding rate and whether a CRC is used in the packet.
      - CRC stands for Cyclic Redundancy Check and is used to detect errors in digital data.
  - **Implicit header mode**
    - Where the payload, coding rate and CRC presence are fixed. In this mode the header is removed from the packet thus reducing transmission time.
      - In this case the payload length, error coding rate and presence of the payload CRC must be manually configured on both sides of the radio link.

LorRa Packet Format

- **The preamble** is used to detect the start of the packet by the receiver.

- **The header** (only in explicit header mode) is the default mode of operation. It provides information on the payload:

  - The payload length in bytes.

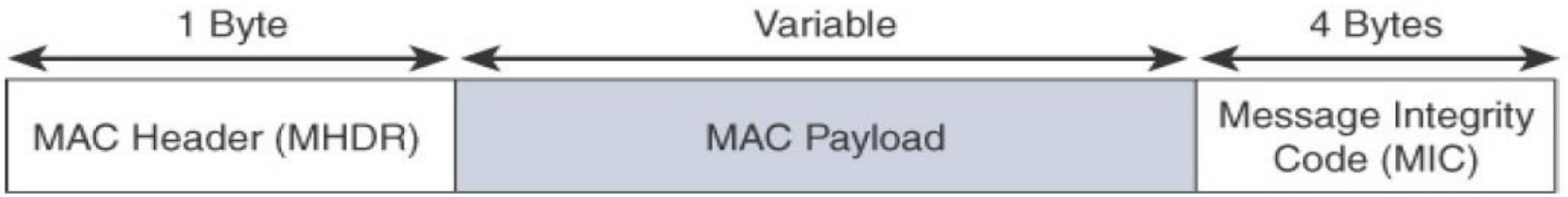
  - The forward error correction code rate.

  - The presence of an optional 16 bits CRC for the payload.

- **The payload** is a variable-length field that contains the actual data coded at the forward error correction code rate either as specified in the header in explicit mode or fixed in implicit mode. An optional payload CRC may be appended.

LoRaWAN- MAC Layer

- LoRaWAN- MAC layer
  - LoRaWAN messages, have a
    - The MAC payload size depends on the frequency band and the data rate, ranging from 59 to 230 bytes for the 863–870 MHz band and 19 to 250 bytes for the 902–928 MHz band.



* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Direct Communication Between Devices

- The LoRaWAN protocol does not support direct communication between end nodes.

- If you want direct communication between LoRa devices without the use of gateways, use the RadioHead Packet Radio library for embedded microprocessors. It provides a complete object-oriented library for sending and receiving packet sized messages via a variety of radios such as LoRa on a range of embedded microprocessors: https://www.airspayce.com/mikem/arduino/RadioHead/

RadioHead does not have an official GitHub repo but several people have cloned the Radiohead library on GitHub.

LoRaWAN- Security

- LoRaWAN considers two layers of security, one for the network and another for the applications.

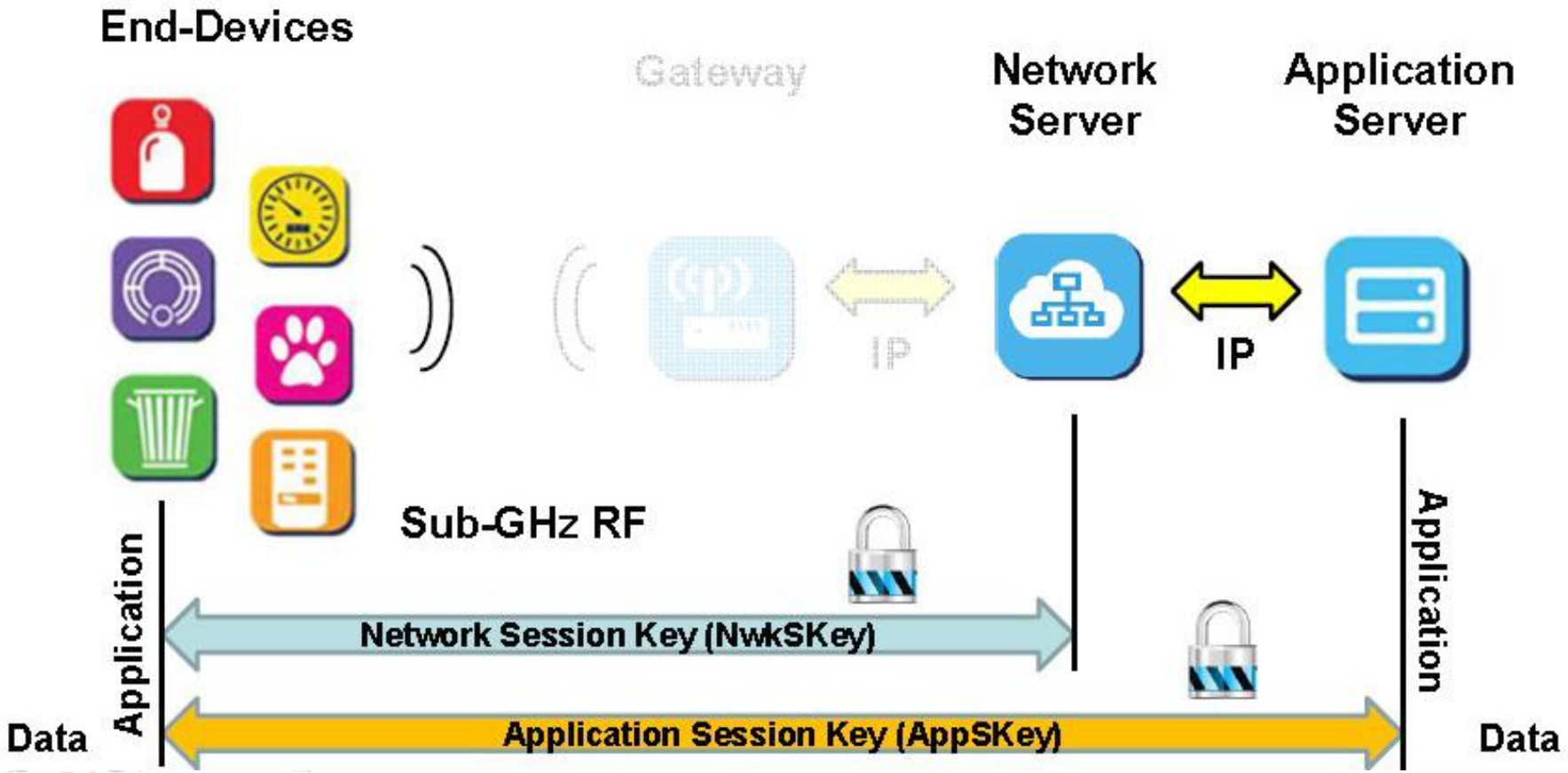
- Each end-device has key assignments done by device manufacturers or the application owners.
  - **Other systems use** a **single key** for **encryption** and **authentication**, compared to LoRaWAN.

- Authentication and encryption are separate, so it is **possible** to **authenticate packets** and **provide integrity protection**.

J. Silva, etl, LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities, 2th Int. Multidisciplinary Conf. on Computer and Energy Science, 2017

LoRaWAN- Security

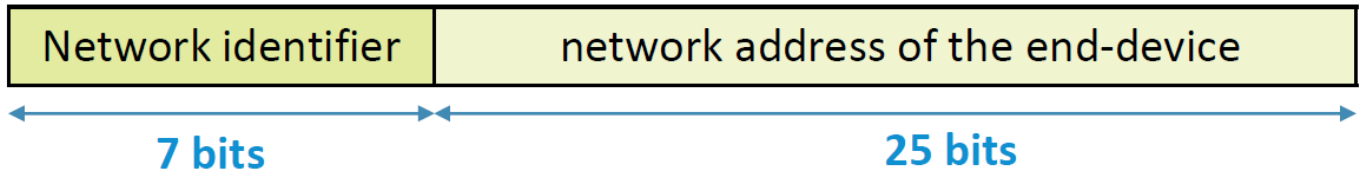
- Logical data Flow:



J. Silva, etl, LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities, 2th Int. Multidisciplinary Conf. on Computer and Energy Science, 2017

IoT wireless technologies overview

- **End-device address (*DevAddr*):**



- **Application identifier (*AppEUI*):** A global application ID in the IEEE EUI64 address space that uniquely **identifies the owner of the end-device**.

- **Network session key (*NwkSKey*):** A key used by the network server and the end-device to calculate and verify the message integrity code of all data messages to ensure data integrity.

- **Application session key (*AppSKey*):** A key used by the network server and end-device to encrypt and decrypt the payload field of data messages.

LoRaWAN- Security

- The first layer, called “network security” but applied at the MAC layer, guarantees the authentication of the endpoints by the LoRaWAN network server.
  - Also, it protects LoRaWAN packets by performing encryption based on AES.

- Each endpoint implements a network session key (NwkSKey), used by both itself and the LoRaWAN network server.
  - The NwkSKey ensures data integrity through computing and checking the MIC of every data message as well as encrypting and decrypting MAC-only data message payloads.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN- Security

- The second layer is an application session key (AppSKey), which performs encryption and decryption functions between the endpoint and its application server.

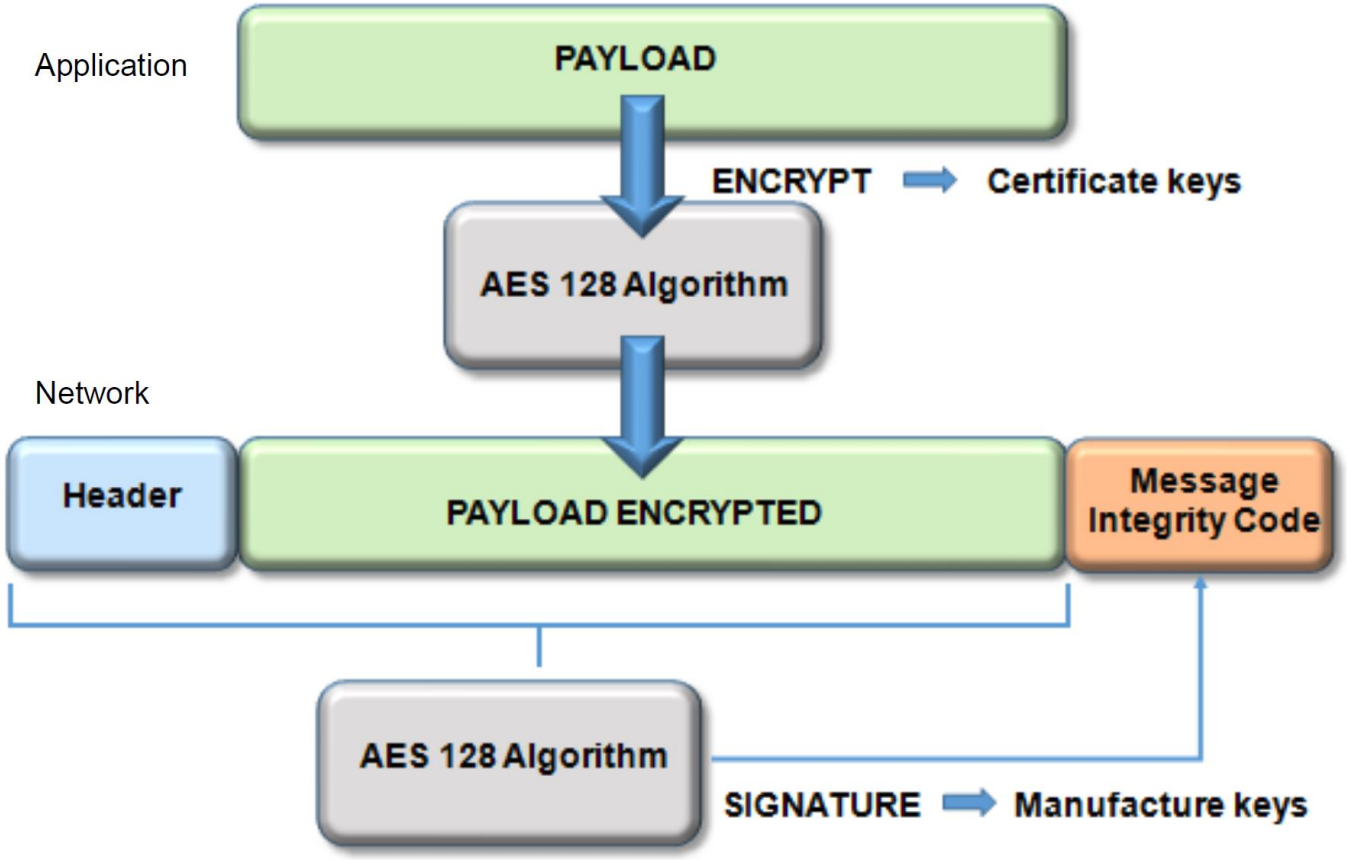
- Furthermore, it computes and checks the application-level MIC, if included. This ensures that the LoRaWAN service provider does not have access to the application payload if it is not allowed that access.

- Endpoints receive their AES-128 application key (AppKey) from the application owner. This key is most likely derived from an application specific root key exclusively known to and under the control of the application provider.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN- Security

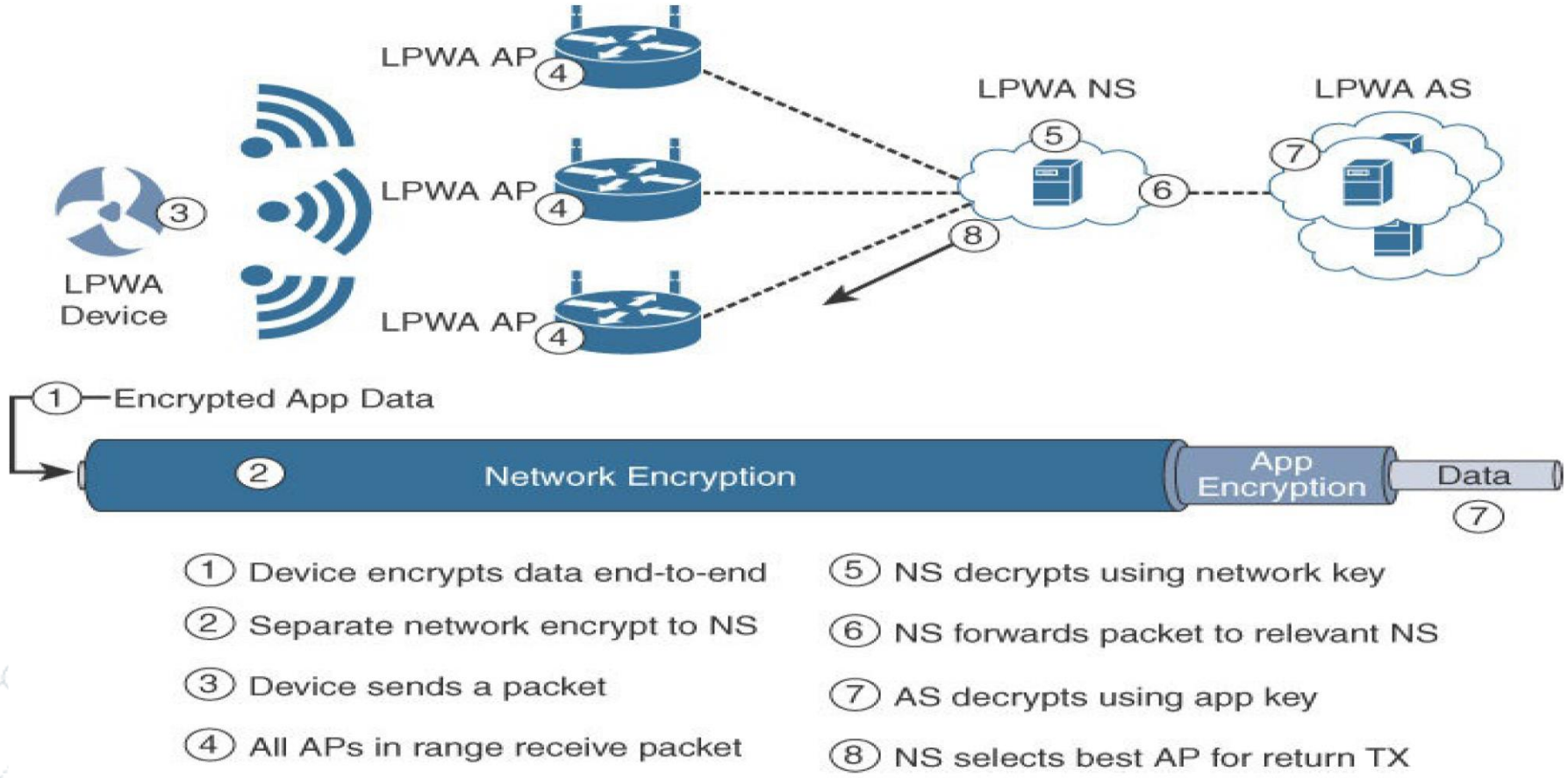
- LoRaWAN endpoints must implement two layers of security:



J. Silva, etl, LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities, 2th Int. Multidisciplinary Conf. on Computer and Energy Science, 2017

LoRaWAN- Security

- LoRaWAN endpoints must implement two layers of security, protecting communications and data privacy across the network.



* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN- Security

- LoRaWAN endpoints attached to a LoRaWAN network must get registered and authenticated. This can be achieved through one of the two join mechanisms:

- **Activation by personalization (ABP):**
  - Endpoints don't need to run a join procedure as their individual details, including DevAddr and the NwkSKey and AppSKey session keys, are preconfigured and stored in the end device.
  - The same information is registered in the LoRaWAN network server.

- **Over-the-air activation (OTAA):**
  - Endpoints are allowed to dynamically join a particular LoRaWAN network after successfully going through a join procedure. The join procedure must be done every time a session context is renewed.
  - During the join process, which involves the sending and receiving of MAC layer join request and join accept messages, the node establishes its credentials with a LoRaWAN network server, exchanging its globally unique DevEUI, AppEUI, and AppKey.
  - The AppKey is then used to derive the session NwkSKey and AppSKey keys.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

LoRaWAN- OTAA Activation Method

- In OTAA, a device is given a DevEUI, an AppEUI and an AppKey. The AppKey is used to generate the session keys, NwkSKey and AppSKey.

- To activate, the device sends a join request and uses the join response to derive the session keys NwkSKey and AppSKey

- The device may store those keys and continue to use them to communicate. If they are lost or the network chooses to expire them, the device must re-join to generate new keys.

LoRaWAN- OTTA Activation Method

- **Pros:**
  - Session keys are only generated when required, so cannot be compromised prior to activation.
  - If the device changes to a new network, it can re-join to generate the new keys - rather than having to be re-programmed.
- **Cons:**
  - A scheme is required to pre-program each device with a unique DevEUI and AppKey, and the correct AppEUI.
  - The device must support the join function and be able to store dynamically generated keys.

LoRaWAN- ABP Activation Method

- In some cases you might need to hardcode the DevAddr as well as the security keys in the device. This means activating a device by personalization (ABP).
  - This strategy might seem simpler, because you skip the join procedure, but it has some downsides related to security
  - In ABP (Activation By Personalisation), a device does not need a DevEUI, an AppEUI or an AppKey.
- Instead the session keys NwkSKey and AppSKey are preprogrammed into the device and the device is pre-registered on the network.
  - When the device wants to communicate, it does so using the session keys without having to use a join procedure first.

LoRaWAN- ABP Activation Method

- **Pros:**

  •The device does not need the capability or resources to perform a join procedure.

  •The device does not need to decide whether a join is necessary at any point, since it is never necessary.

  •No scheme is necessary to specify a unique DevEUI or AppKey

- **Cons:**

  • The scheme must be secure to prevent the keys being obtained or derived by rogue parties.

  • If the device is compromised at any time, even before activation, the keys may be discovered.

  • Network settings cannot be specified at join time.

  • Events that warrant a change of keys (for example, moving to a new network, the device being compromised, or the keys being expired) require a re-programming of the device..

LoRaWAN- Battery Lifetime

- Synchronization network usually **consumes** significant **energy**. In LoRaWAN, nodes are asynchronous and communicate via **events** or in pre**scheduled** opportunities.

- The **ADR** (Adaptive Data Rate) scheme is used for LoRa network infrastructures for manage the individual **data rates** and **maximize** the **battery life** of **each connected device** through RF output.

- A recent research study performed by **Scientific Research Publishing**, Inc revealed that **LoRaWAN** showed an **advantage of 3 up to 5-fold in the energy economy compared** to all the **others LPWAN** technologies.