Politechnika Białostocka

Białystok University of Technology
Faculty of Electrical Engineering

Erasmus+

LoRaWAN technology and its applications in IoT systems

Andrzej Zankiewicz, PhD

Agenda

Part 1: Introduction to Internet of Things

- General concept of Internet of Things (IoT)
- Typical workflow in the IoT system
- A survey of applications of Internet of Things systems
- Review of transmission technologies used in IoT systems

Part 2: Foundations of LoRa and LoRaWAN

- General information about LoRa and LoRaWAN
- Operation of the LoRa radio interface
- Structure of the LoRaWAN network
- Security aspects in the LoRaWAN network

Part 3: Practical demonstration of creating LoRaWAN IoT measurement application

- End user node
- LoRaWAN Gateway
- The Things Network
- Google Docs as a user application
- Combining all the above together

Part 1:
Introduction to Internet of Things

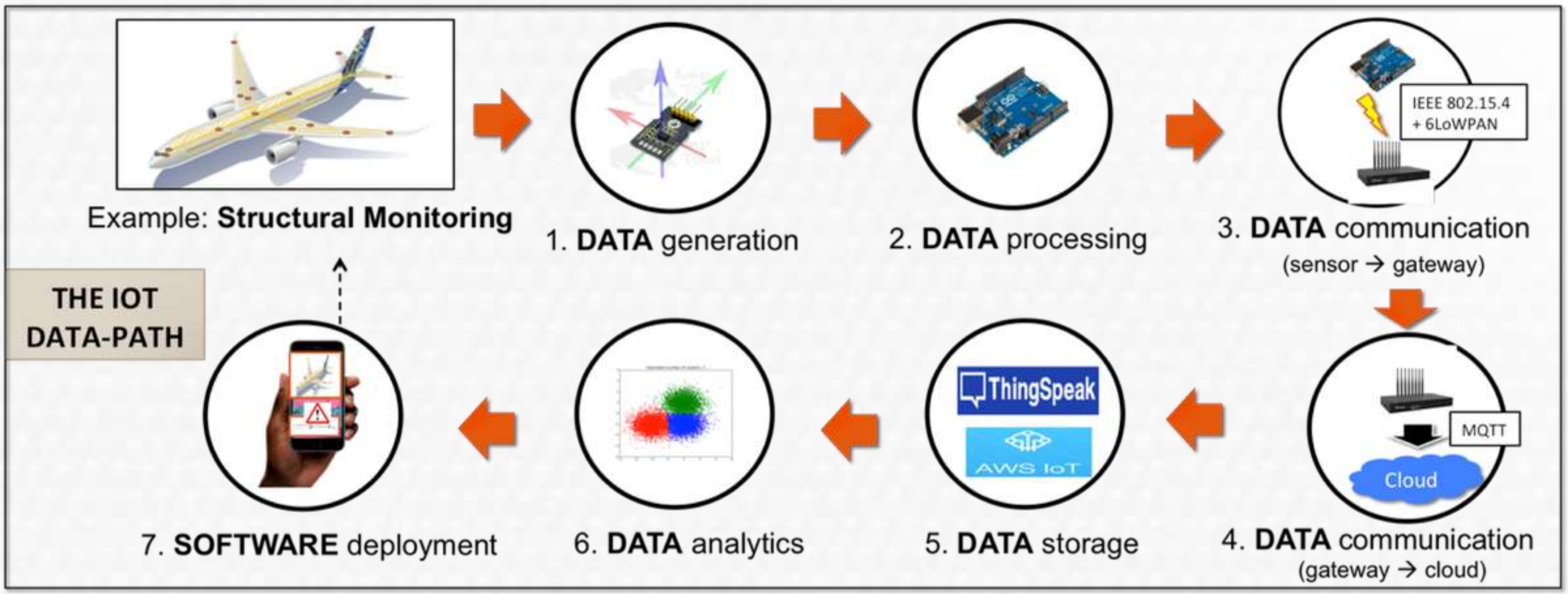
Introduction to Internet of Things

❑ General concept of Internet of Things (IoT)

- ✓ The Internet of things (IoT) describes physical objects (or groups of such objects) with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. (*Technical approach*)
- ✓ Interconnected devices with sensors and actuators more and more invisibly existed in the real world with processing and control moved to the virtual world. (*User experience point of view*)
- ✓ The IoT comprises many technologies working together to create a seamless link between real and virtual worlds that generates new qualities and benefits for our technical civilization. (*A bit philosophical*)

Introduction to Internet of Things

- Typical workflow in the IoT system: **from sensors to knowledge**



Source: https://site.unibo.it/

Introduction to Internet of Things

- A survey of applications of Internet of Things systems

Indoor Botanical Garden
Download »

Nationwide Smart Metering
Download »

Smart Island Management
Download »

Smart Water Leakage Detection
Download »

Smart Flood Monitoring
Download »

Soil Moisture
Download »

Smart Irrigation
Download »

Wireless Gas Level Monitoring
Download »

Water Management & Protection
Download »

Source: www.semtech.com

Introduction to Internet of Things

- A survey of applications of Internet of Things systems

Water Flow Monitoring
Download »

Waste Management
Download »

Tank Flow Monitoring
Download »

Smart Parking
Download »

Shipment Quality
Download »

Radiation Leak Detection
Download »

Predictive Maintenance
Download »

Precision Farming
Download »

Parking Management
Download »

Source: www.semtech.com

Introduction to Internet of Things

- A survey of applications of Internet of Things systems

Medical Fridge
Download »

Locating Stolen Vehicles & Cargo
Download »

Liquid Presence Detection
Download »

Industrial Temp
Download »

Indoor Air Quality
Download »

Home Security
Download »

Fleet Tracking
Download »

Fleet Management
Download »

Fire Detection
Download »

Source: www.semtech.com

Introduction to Internet of Things

- A survey of applications of Internet of Things systems

Fall Detection
Download »

Energy Management & Sustainability
Download »

Cattle Tracking
Download »

Agriculture Processing
Download »

Air Pollution Monitoring
Download »

Asset Tracking
Download »

Smart Lighting
Download »

Source: www.semtech.com

Introduction to Internet of Things

- A survey of applications of Internet of Things systems






Introduction to Internet of Things

- Review of physical transmission technologies used in IoT systems
  - ✓ **WPAN – Wireless Personal Area Network**
    - ✓ Bluetooth Classic (BR/EDR), Bluetooth Low Energy (BLE)
    - ✓ Technologies based on IEEE 802.15.4
      - ✓ Zigbee
      - ✓ WirelessHART
      - ✓ 6LoWPAN
      - ✓ IEEE 802.15.5
      - ✓ Thread
    - ✓ ANT (Dynastream Innovations)
    - ✓ WM-Bus
    - ✓ Z-Wave
  - ✓ **LPWAN – Low Power Wide Area Network**
    - ✓ LoRa, LoRaWAN
    - ✓ Sigfox
    - ✓ 3GPP technologies (mobile celluar services)
      - ✓ eMTC (LTE Cat M1)
      - ✓ NB-IoT (LTE Cat NB1)
  - ✓ **WLAN – Wireless Local Area Network –** Wi-Fi (IEEE 802.11)

Introduction to Internet of Things

- Review of logical transmission technologies used in IoT systems
  - **Protocols of data exchange**
    - 6LoWPAN
    - CoAP
    - MQTT
    - WebRTC
    - Cloud services
    - http, https
    - ……………

Part 2: Foundations of LoRa and LoRaWAN

Foundations of LoRa and LoRaWAN

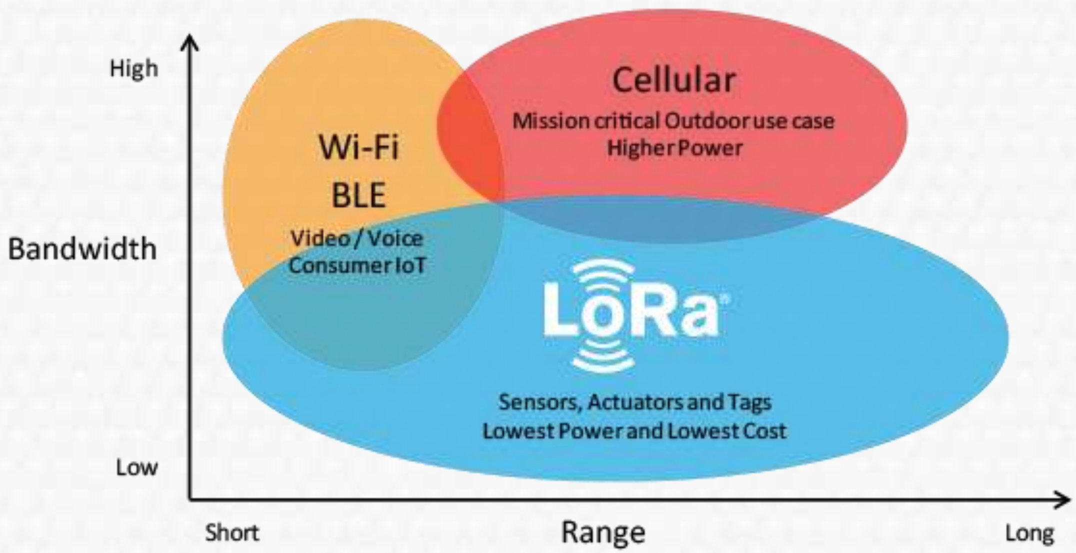
- In this part you will find out:
  - ✓ What are LoRa, LoRaWAN and what is the scope of their applications in comparison to other wireless communication techniques.
  - ✓ How LoRa radio interface operates.
  - ✓ What is the structure of the LoRaWAN network and what are functions provided by a particular parts in the LoRaWAN network.
  - ✓ How is the transmission in the LoRaWAN network secured.

Part 2: Foundations of LoRa and LoRaWAN

General information about LoRa and LoRaWAN

General information about LoRa and LoRaWAN

- LoRaWAN is an implementation of LPWAN (Low Power Wide Area Network), in which distributed remote nodes are connected using LoRa radio interfaces.
  - ✓ LPWAN is a type of a wide area network designed for communication over long distances at a low (compared to other available technologies) transmission rate with low energy consumption.



Source: semtech.com

General information about LoRa and LoRaWAN

- LoRaWAN is an implementation of LPWAN (Low Power Wide Area Network), in which distributed remote nodes are connected using LoRa radio interfaces.

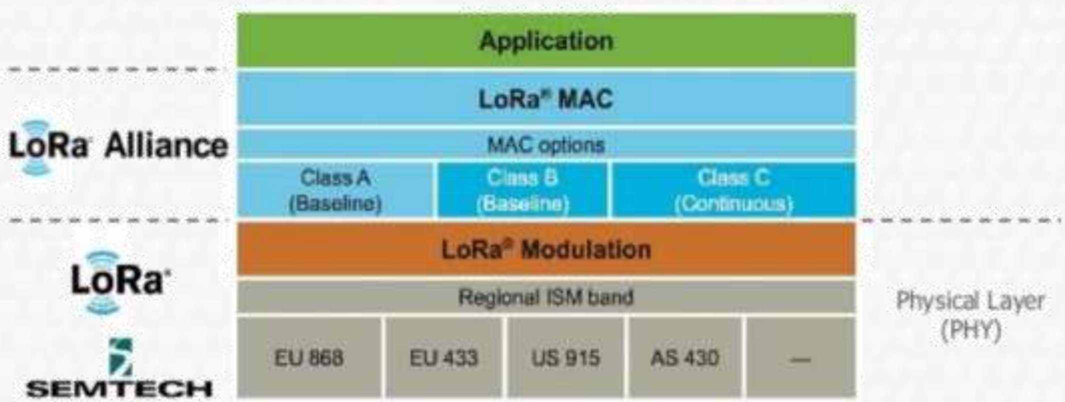
LoRa	LoRaWAN
Standard of implementation of a single radio link between two points (e.g. between a measuring sensor and a wide area network gateway). It is a proprietary solution from Semtech company.	A wide area network used for data delivering from end nodes (e.g. measurement sensors) to the user application. Communication from the application to the end nodes can also be available, but usually in limited form. The end nodes are connected using the LoRa radio interface. It is an open specification developed by LoRa Alliance®.

General information about LoRa and LoRaWAN

- Typical applications of LPWANs:
  - Data transmission from distributed battery-powered measuring sensors
    - Water, heat, gas and electricity meters, …
  - Transmission from sensor network hubs based on low-range technologies (e.g. Bluetooth Low Energy, ZigBee, Z-Wave)
- LPWAN networks can be implemented as private networks, as a service or infrastructure offered by operators (e.g. Sigfox network, LTE Cat-M1) and also can operate in a 'social' model (e.g. The Things Network)

General information about LoRa and LoRaWAN

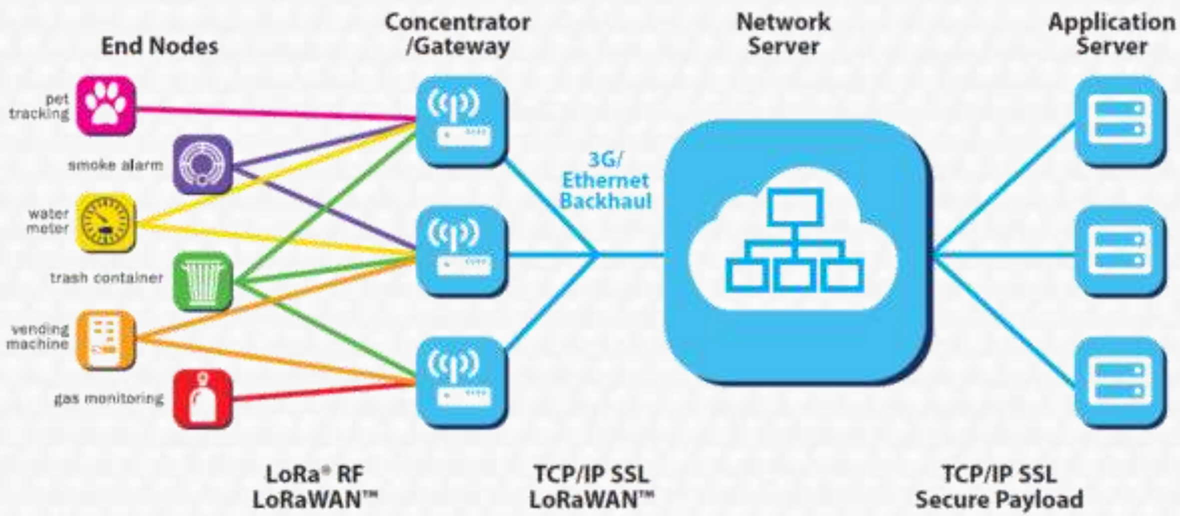
- The LoRaWAN system includes the following parts (layers):
  - ✓ LoRa PHY – physical layer protocol
    - ❖ Proprietary solution from Semtech company
  - ✓ LoRa MAC –MAC (*Medium Access Control*) layer protocol
    - ❖ Includes control of shared medium access and logical organization of transmission within the medium (including PDU creation, selection of a frequency channel, selection of transmission rate and power)
    - ❖ LoRa Alliance is responsible for its development and standardization that ensure mutual compatibility of devices from different manufacturers



Source:
LoRaWAN™ 1.0.3 Specification

General information about LoRa and LoRaWAN

- The LoRaWAN system includes the following parts (layers):
  - ✓ LoRa PHY – physical layer protocol
  - ✓ LoRa MAC –MAC (*Medium Access Control*) layer protocol
  - ✓ LoRa over TCP/IP
    - ❖ It performs the encapsulation of messages from end nodes in IP packets sent over the standard IP network (e.g. Internet) between the LoRa gateway and the network server (LNS - LoRa Network Server), which, among others, detects duplicate messages and provides information received from end nodes through standard IT solutions (e.g. SQL databases, APIs, …)



Source: lora-alliance.org

Part 2: Foundations of LoRa and LoRaWAN

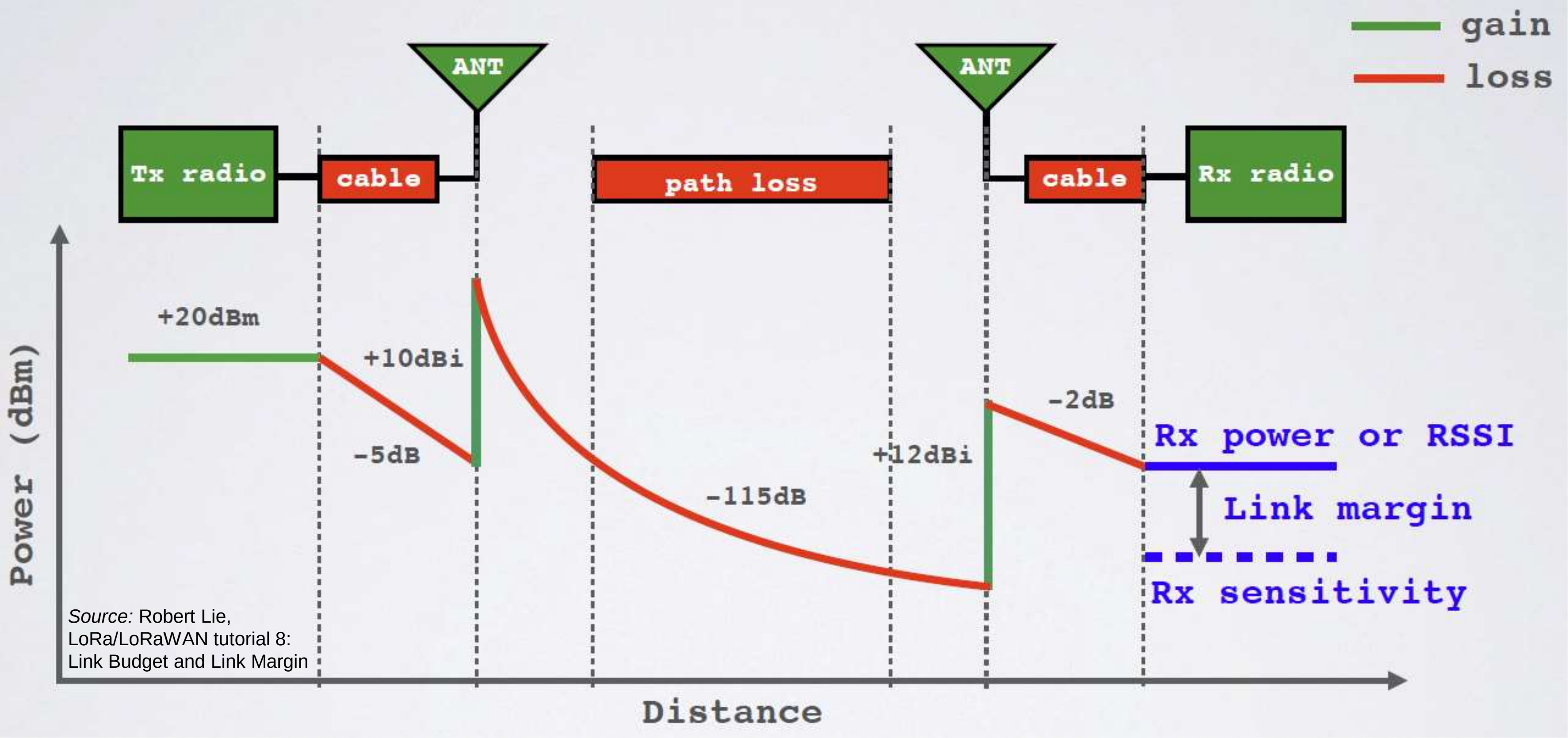
Operation of the LoRa radio interface

Operation of the LoRa radio interface

- The LoRa technology was developed by Cycleo of Grenoble (France), acquired by Semtech (USA) in 2012.
- The name LoRa comes from "Long Range" and emphasizes a key feature of the technology.
  - ✓ Range in urban conditions up to several km
  - ✓ Range in the open space up to several dozen km
    - ❖ Experimentally, a transmission distance of over 700 km was obtained: Osterwald (Germany) → Wrocław (Poland)
- LoRa PHY transmission is a proprietary solution based on patents currently owned by Semtech:
  - ✓ EP2763321A1 - Low power long range transmitter
  - ✓ US7791415B2 - Fractional-N synthesized chirp generator
  - ✓ The information is encoded in the values ot the frequency shift (FSK type) between successive chirp pulses

Operation of the LoRa radio interface

- LoRa PHY – transmission range
  - ✓ In radio communication systems, correct signal reception requires that the signal level at the receiver input should not be lower than the value of the receiver parameter defined as its sensitivity



Source: Robert Lie, LoRa/LoRaWAN tutorial 8: Link Budget and Link Margin

Operation of the LoRa radio interface

- LoRa PHY – transmission range
  - ✓ In radio communication systems, correct signal reception requires that the signal level at the receiver input should not be lower than the value of the receiver parameter defined as its sensitivity
  - ✓ The sensitivity of the receiver is the minimum signal power level at its input, at which correct reception is ensured (in the case of digital transmission it means the error rate below the assumed threshold value, e.g. 1%).
  - ✓ The receiver sensitivity is determined by the equation:
    Rx sensitivity = -174 dBm + $10\log_{10}(BW)$ + NF + SNR, where:

-174 dBm – the average noise power of an ideal receiver for each 1 Hz of bandwidth at temperature 290 K (it is k x T_o)

k –Boltzman's constant, T_o=290 K – temperature value defined by IEEE as close to typical "room" conditions)

BW – receiver bandwidth

NF – Noise Factor, noise level at the receiver output related to the ideal receiver

SNR - signal to noise ratio required for the correct detection

Operation of the LoRa radio interface

- LoRa PHY – transmission range
  - ✓ The receiver sensitivity is determined by the equation:

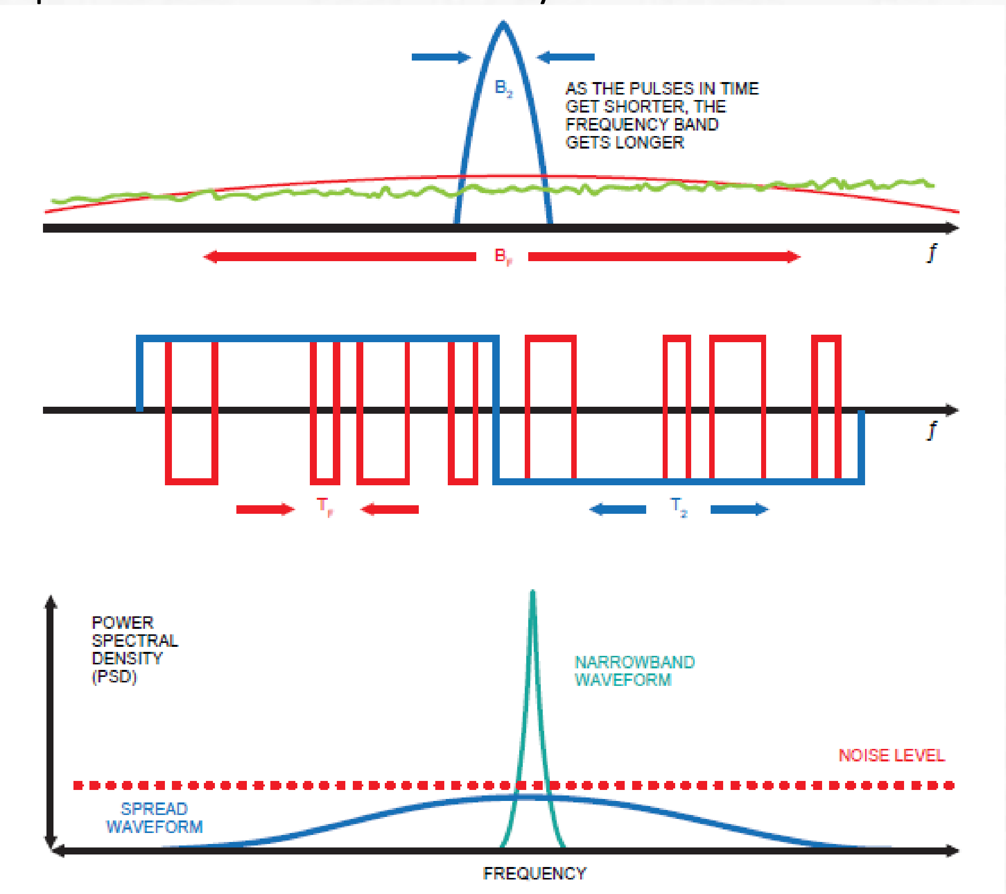
    Rx sensitivity = -174 dBm + $10\log_{10}$(BW) + NF + SNR

The higher the SNR, the lower ("worse") sensitivity of the receiver is and a stronger signal at the input is required for correct reception (that is, for the given transmission conditions and the given transmitter power, the transmission range will be shorter).

Conclusion: a large transmission range requires the use of a type of detection that requires the lowest possible signal level at the input

Operation of the LoRa radio interface

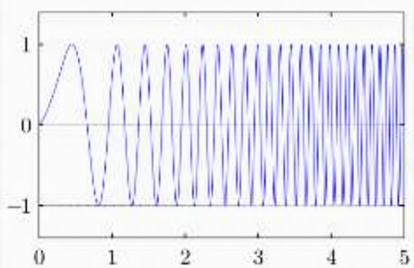
- LoRa PHY – transmission range
  - ✓ Proper detection at low signal levels can be provided e.g. by spread spectrum transmission systems.
  - ✓ They allow to obtaining a high value of the so-called the maximum link budget defined as the sum of transmitter power and receiver sensitivity



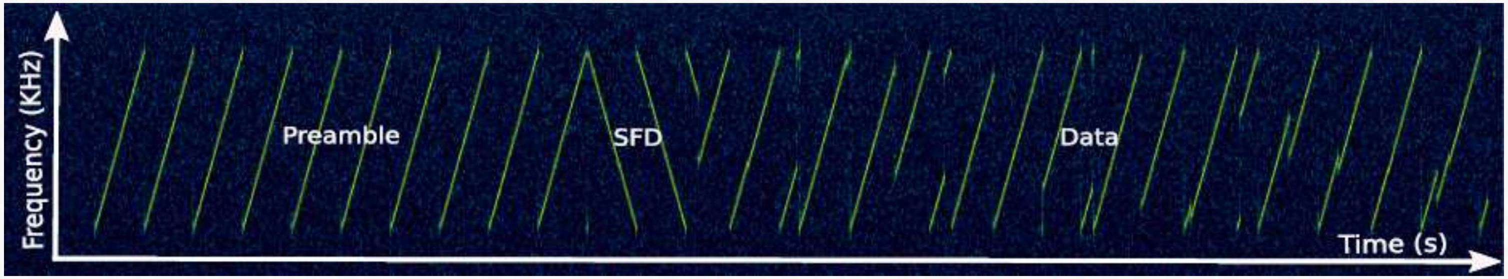
Source:
lora-developers.semtech.com

Operation of the LoRa radio interface

- LoRa PHY – physical layer protocol
  - ✓ Transmission is realized using the spectral spreading method Chirp Spread Spectrum (CSS)
  - ✓ CSS uses the so-called chirp which is a sinusoidal pulse with a frequency varying in a polynomial (in this case linear) manner, being a single modulation symbol



Source: Jansen Christian Liando, Known and Unknown Facts of LoRa: Experiences from a Largescale Measurement Study



Operation of the LoRa radio interface

- LoRa PHY – physical layer protocol
  - ✓ Physical transmission can take place at different rates described by the equation:

$$R_b = SF \cdot \frac{CR \cdot BW}{2^{SF}}$$

where:

R_b - transmission rate [b/s]

SF – Spread Factor – spectrum spreading factor, in this case also determines the number of bits encoded on one symbol (a single chirp pulse)

SF = {6 (not used), 7, 8, 9, 10, 11, 12)

BW – bandwidth (related to the range of the frequency sweep in the chirp pulse)

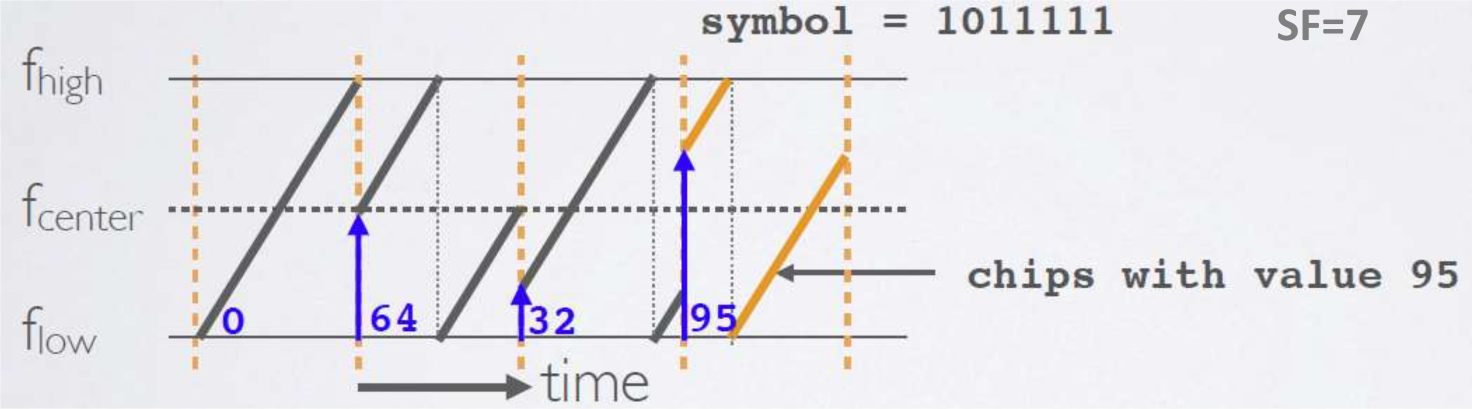
BW = {7.8; 10.4; 15.6; 20.8; 31.25; 41.7; 62.5; 125; 250; 500} [kHz]

CR – Coding Rate – the ratio of the number of data bits to the total number of bits transmitted in the radio transmission (additional bits are FEC correction codes)

CR = {4/5; 4/6; 4/7; 4/8}

Operation of the LoRa radio interface

- LoRa PHY – physical layer protocol
  - ✓ A full frequency change range is divided into 2^{SF} intervals (so-called chips)
  - ✓ The value of the currently transmitted symbol is encoded in the number of the interval from which the frequency sweep begins in the signal transmitting this symbol



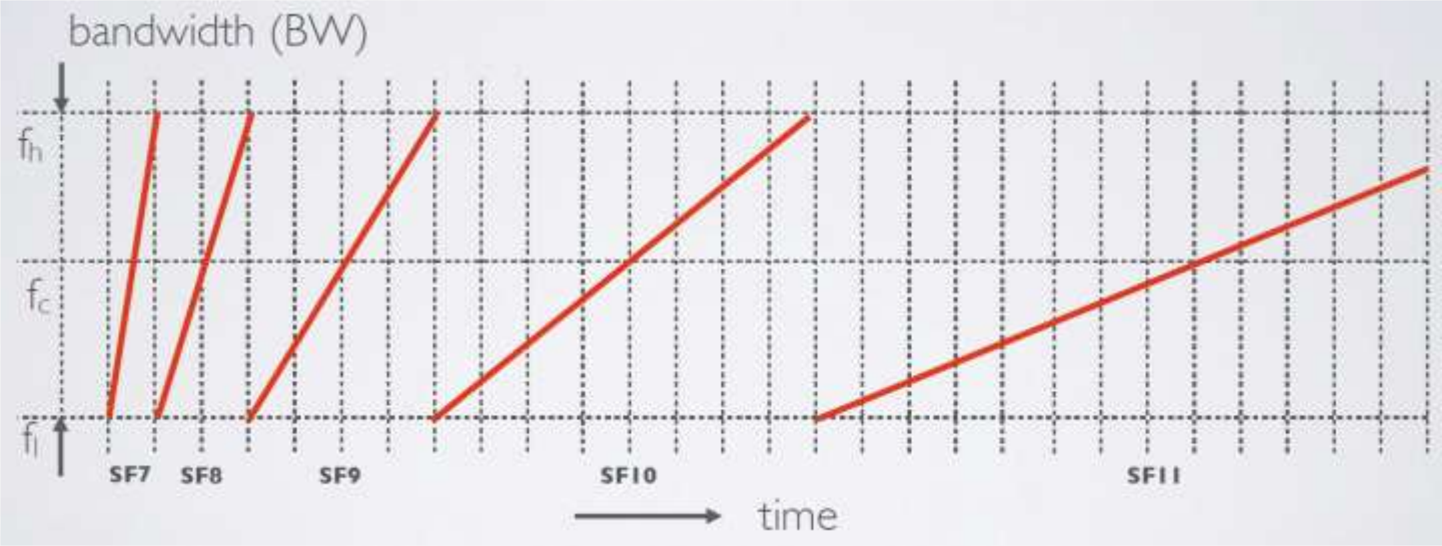
Source: Robert Lie,
LoRa/LoRaWAN tutorial 13: Symbol, Spreading
Factor and Chip

Operation of the LoRa radio interface

- LoRa PHY – physical layer protocol
  - ✓ The signal is created with dependency:

$BW = R_C$, where R_C – chip rate (chips/s)

which means that for a given SF, the slope (rate of change of frequency) does not depend on BW



Source: Robert Lie,
LoRa/LoRaWAN tutorial 15: Data Rate, Chip Rate, Symbol Rate, Chip Duration and Symbol Duration

Operation of the LoRa radio interface

- The use of LoRa modulation with spread spectrum CSS method allows for:
  - ✓ obtaining a high value of the so-called the maximum link budget defined as the sum of transmitter power and receiver sensitivity (without sign – the higher the better)

Maximum transmitter power = 14 dBm, receiver sensitivity (for BW=125kHz, SF=7) is **-125 dBm**, which gives a link budget of approx **141 dB**.

For comparison, the highest sensitivities of Wi-Fi receivers are at the level of -97 dBm.

SpreadingFactor (RegModulationCfg)	Spreading Factor (Chips / symbol)	LoRa Demodulator SNR
6	64	-5 dB
7	128	-7.5 dB
8	256	-10 dB
9	512	-12.5 dB
10	1024	-15 dB
11	2048	-17.5 dB
12	4096	-20 dB

Source: Semtech SX1276/77/78/79 Datasheet

RXS_LB	Sensitivity LoRa, RX boosted gain, split RF paths for RX and Tx, RF switch insertion loss excluded	BW = 10.4 kHz, SF = 7	-	–135	-	dBm
		BW = 10.4 kHz, SF = 12	-	–148	-	
		BW = 125 kHz, SF = 7	-	–125	-	
		BW = 125 kHz, SF = 12	-	–138	-	
		BW = 250 kHz, SF = 7	-	–122	-	
		BW = 250 kHz, SF = 12	-	–135	-	
		BW = 500 kHz, SF = 7	-	–118	-	
		BW = 500 kHz, SF = 12	-	–130	-	

Source: ST STM32WL55xx STM32WL54xx Datasheet (DS13293 Rev 1)

Operation of the LoRa radio interface

- The use of LoRa modulation with spread spectrum CSS method allows for:
  - ✓ obtaining a high value of the so-called the maximum link budget defined as the sum of transmitter power and receiver sensitivity,
  - ✓ no need to use a high-class reference clock (compared to DSSS),
  - ✓ avoiding interference when transmitting signals with different SFs in the same frequency channel (signals with different SFs are mutually orthogonal),
  - ✓ obtaining high resistance to multipath propagation and fading, which is particularly important in an urban environment,
  - ✓ low Doppler effect (for mobile devices).

Part 2: Foundations of LoRa and LoRaWAN

LoRa radio interface in the LoRaWAN

Operation of the LoRa radio interface

- LoRa PHY – physical layer protocol
  - ✓ The radio signal is transmitted in unlicensed ISM bands depending on regional regulations
    - ✓ Europe: 433 MHz, 868 MHz
    - ✓ USA, Australia, Brazil: 915 MHz (there are differences from country to country)
    - ✓ China: 470 MHz, 780 MHz
    - ✓ Detailed requirements are specified in the document„LoRaWAN Regional Parameters”

LoRa Alliance

RP002-1.0.0 LoRaWAN Regional Parameters

Contents

RP002-1.0.0 LoRaWAN Regional Parameters

Operation of the LoRa radio interface

❑ Frequencies in EU863-870MHz ISM Band

- ✓ The "LoRaWAN Regional Parameters" specification allows for individual choice of the frequency channels within the given radio band by the operator of a LoRaWAN network, although it defines the minimum set of three channels that all gateways must listen on.

Modulation	Bandwidth [kHz]	Channel Frequency [MHz]	FSK Bitrate or LoRa DR / Bitrate	Nb Channels	Duty cycle
LoRa	125	868.10 868.30 868.50	DR0 to DR5 / 0.3-5 kbps	3	< 1%

RP002-1.0.0 LoRaWAN Regional Parameters

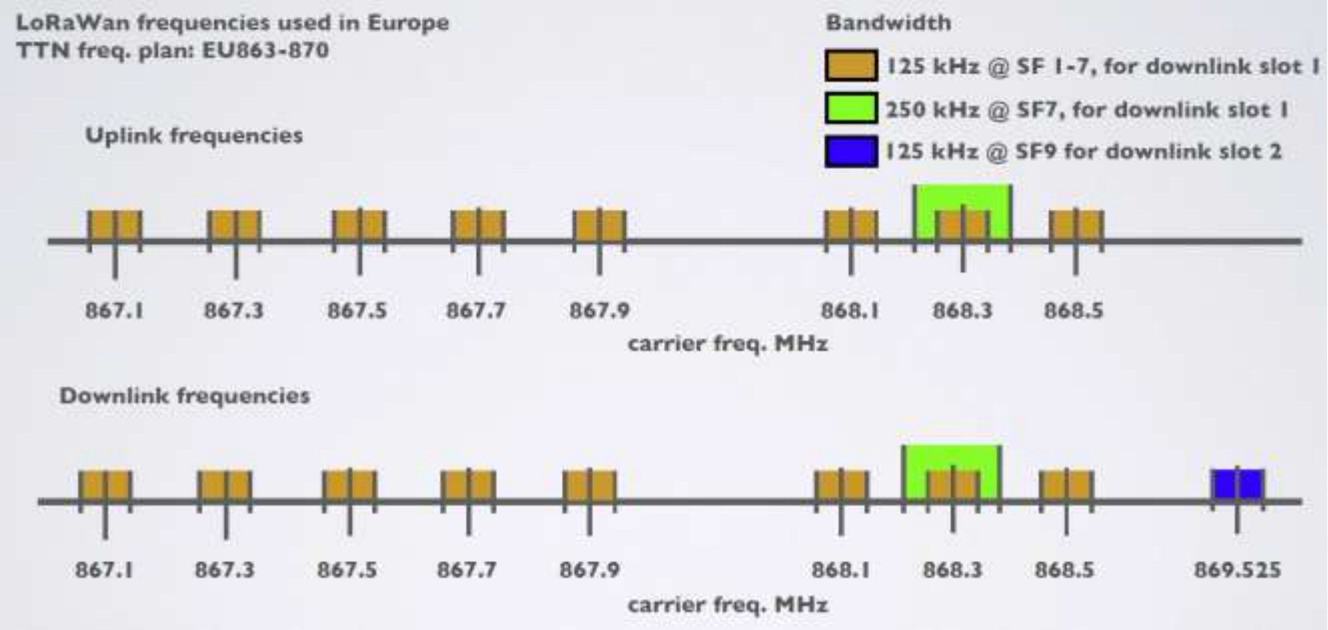
Operation of the LoRa radio interface

❑ Frequencies in EU863-870MHz ISM Band

✓ For example, in The Things Network on the EU863 band, the standard set of channels is as follows :

Uplink:

1. **868.1** - SF7BW125 to SF12BW125
2. **868.3** - SF7BW125 to SF12BW125 and SF7BW250
3. **868.5** - SF7BW125 to SF12BW125
4. **867.1** - SF7BW125 to SF12BW125
5. **867.3** - SF7BW125 to SF12BW125
6. **867.5** - SF7BW125 to SF12BW125
7. **867.7** - SF7BW125 to SF12BW125
8. **867.9** - SF7BW125 to SF12BW125
9. **868.8** - FSK



Downlink:

- Uplink channels 1-9 (RX1)
- **869.525** - SF9BW125 (RX2 downlink only)

Source: Robert Lie,
LoRa/LoRaWAN tutorial 11: Carrier Frequencies and Bandwidths

Operation of the LoRa radio interface

- Transmission rate and transmitter power

DataRate	Configuration	Indicative physical bit rate [bit/s]
0	LoRa: SF12 / 125 kHz	250
1	LoRa: SF11 / 125 kHz	440
2	LoRa: SF10 / 125 kHz	980
3	LoRa: SF9 / 125 kHz	1760
4	LoRa: SF8 / 125 kHz	3125
5	LoRa: SF7 / 125 kHz	5470
6	LoRa: SF7 / 250 kHz	11000
7	FSK: 50 kbps	50000
8..14	RFU	
15	Defined in LoRaWAN[1]	

[1] DR15 and TXPower15 are defined in the LinkADRReq MAC command of the LoRaWAN1.1 specification

TXPower	Configuration (EIRP)
0	Max EIRP
1	Max EIRP – 2dB
2	Max EIRP – 4dB
3	Max EIRP – 6dB
4	Max EIRP – 8dB
5	Max EIRP – 10dB
6	Max EIRP – 12dB
7	Max EIRP – 14dB
8..14	RFU
15	Defined in LoRAWAN

By default, the Max EIRP is considered to be +16 dBm.

Source:
LoRaWAN 1.1 Regional Parameters

Operation of the LoRa radio interface

- LoRa PHY – physical layer protocol
  - ✓ PHY layer packet format

PHY:

Size	8 Symbols	8 Symbols		*L* bytes (from PHDR)	2 Bytes
Packet Structure	Preamble	PHDR	PHDR_CRC	PHYPayload	CRC (uplink only)

  - ✓ In order to comply with the LoRaWAN specification, the PHY layer should use the following parameters:

Parameter	Uplink value	Downlink value
Preamble size	8 symbols	
SyncWord	0x34 (Public)	
Header type	Explicit	
CRC presence	True	False
Coding Rate	4/5	
Spreading Factor	Defined by the Datarate, specified in each region	
Bandwidth		
IQ polarization	Not-inverted	Inverted

RP002-1.0.0 LoRaWAN Regional Parameters

Data Rate (DR)	Physical bit rate [b/s]	Max Payload Size [bytes]
0	250	51
1	440	51
2	980	51
3	1760	115
4	3125	222
5	5470	222
6	11000	222
7	50000	222

Operation of the LoRa radio interface

ToA – Time on Air

- In the case of LoRa transmission, an important parameter is the time of transmission of a single PHY packet (medium busy time), called *ToA* (Time on Air)
- Compared to other systems (e.g. Wi-Fi), it may be relatively long
- Total *ToA* is the sum of the preamble transmission time and the PHY layer packet data :

  $ToA = T_{preamb} + T_{payload}$

  $T_{preamb} = (n_{preamb} + 4.25)\ T_s$

  n_{preamb} – the number of preamble symbols (for EU868 it is 8, 4.25 is the number of SFD symbols)

  $T_s = 2^{SF} / BW$ (duration of a single symbol)
- Example of ToA values for a payload of 20 bytes, CRC enabled, BW = 125 kHz, CR = 4/5

Higher SF means slower transmission and greater range, but also higher power consumption

SF	ToA [ms]
7	57
8	103
9	185
10	371
11	741
12	1319

Operation of the LoRa radio interface

- Data rate, transmission distance and power consumption

Higher SF means slower transmission and greater range, but also higher power consumption.

Data Rate (DR)	SF	Physical bit rate [b/s]	ToA [ms] (for 20 bytes)
0	12	250	1319
1	11	440	741
2	10	980	371
3	9	1760	185
4	8	3125	103
5	7	5470	57

RXS_LB	Sensitivity LoRa, RX boosted gain, split RF paths for RX and Tx, RF switch insertion loss excluded	BW = 10.4 kHz, SF = 7	-	–135	-	dBm
		BW = 10.4 kHz, SF = 12	-	–148	-	
		BW = 125 kHz, SF = 7	-	–125	-	
		BW = 125 kHz, SF = 12	-	–138	-	
		BW = 250 kHz, SF = 7	-	–122	-	
		BW = 250 kHz, SF = 12	-	–135	-	
		BW = 500 kHz, SF = 7	-	–118	-	
		BW = 500 kHz, SF = 12	-	–130	-	

Source: ST STM32WL55xx STM32WL54xx Datasheet (DS13293 Rev 1)

Operation of the LoRa radio interface

- Use of radio resources (Duty Cycle)
  - ✓ The Duty Cycle parameter determines the percentage of time that is taken by a radio transmission. For example, if we transmit for 1 second every 10 seconds, it is 10%.
  - ✓ In Europe, the permissible Duty Cycle (DC) factor is specified in the *Commission Implementing Decision (EU) 2017/1483 of 8 August 2017 amending Decision 2006/771/EC on harmonisation of the radio spectrum for use by short-range devices and repealing Decision 2006/804/EC (notified under document C(2017) 5464)* .

Operation of the LoRa radio interface

❑ Use of radio resources (Duty Cycle)

Band No	Frequency range	Restrictions
46a	863.0 – 865.0 MHz	EIRP < 25 mW, DC < 0.1%
47	865.0 – 868.0 MHz	EIRP < 25 mW, DC < 1%
47b	865.0 – 868.0 MHz	EIRP < 500 mW, DC < 2,5% Only for channels 865,6- 865,8 MHz, 866,2-866,4 MHz, 866,8-867,0 MHz, 867,4- 867,6 MHz
48	868.0 – 868.6 MHz	EIRP < 25 mW, DC < 1%
50	868.7 – 869.2 MHz	EIRP < 25 mW, DC < 0.1%
54	869.4 – 869.65 MHz	EIRP < 25 mW, DC < 0.1%
56b	869.7 – 870.0 MHz	EIRP < 25 mW, DC < 0.1%

✓ Particular LoRaWAN networks may additionally use their own limitations

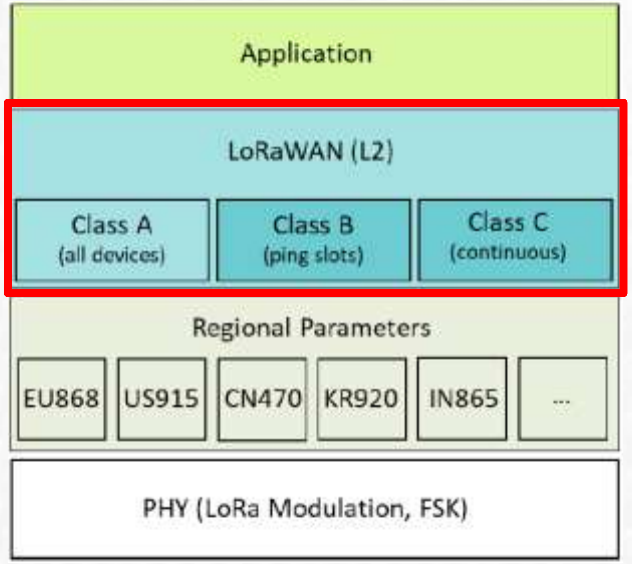
- ❖ For example, The Things Network has a Fair Access Policy that limits the uplink time to 30 seconds per node per day and to 10 downlink messages per node per day.

Part 2: Foundations of LoRa and LoRaWAN

LoRaWAN L2

LoRaWAN L2

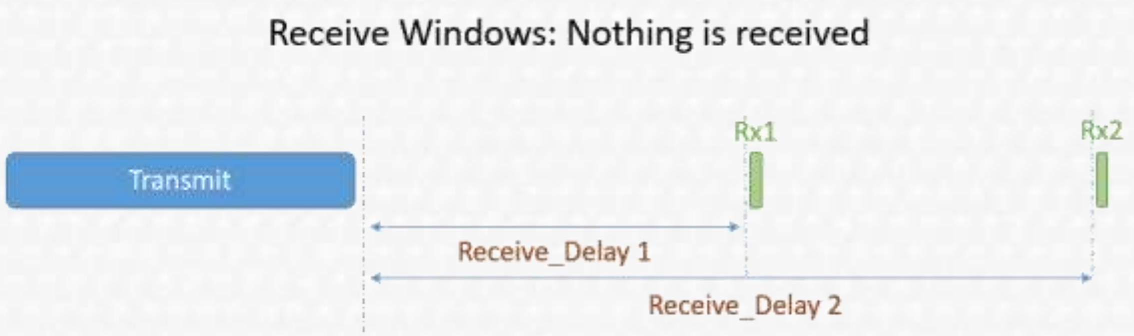
- LoRa – data link layer protocol (L2, Link Layer)
  - ✓ The LoRaWAN specification defines, among others, data link layer protocol (LoRaWAN L2, Link Layer)
  - ✓ LoRaWAN L2 provides logical organization of transmission between end nodes (e.g. sensors) and LoRa gateways
  - ✓ LoRaWAN L2 features include:
    - Encapsulation of transmitted data in frames
    - Support for downlink transmission modes
    - Management of frequency, power and bit rate
    - Transmission security (AES128-based encryption, authentication)



Source:
LoRaWAN™ 1.0.4 Specification

LoRaWAN L2

- LoRaWAN defines three transmission classes:
  - ✓ Class A: asynchronous communication
    - It is a basic class and its implementation is obligatory in all devices
    - The end device spends most of its time in sleep mode
    - The end device can start uplink transmission at any time
    - After each transmission from the end device to the gateway (uplink), two short transmission windows (about 1s) are opened in the downlink direction (RX1 and RX2).
    - The server cannot initiate a downlink transmission.
    - This is the most energy-saving mode.

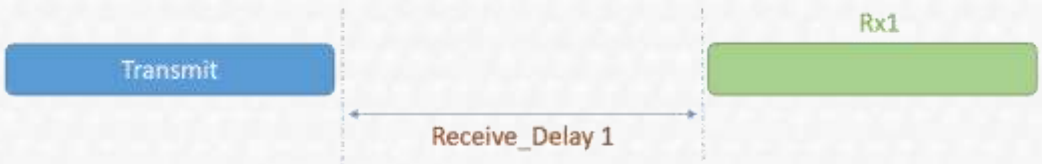


Source: lora-developers.semtech.com

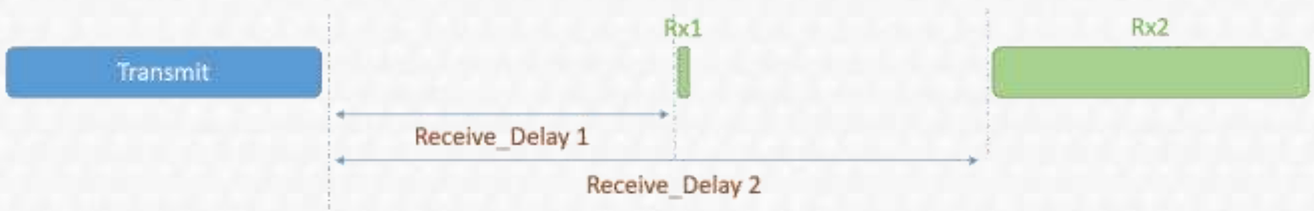
LoRaWAN L2

- LoRaWAN defines three transmission classes:
  - ✓ Class A: asynchronous communication
    - ❖ If no transmission is received in the Rx1 window, the device, after a short sleep period, opens the second window (Rx2).
    - ❖ The device will not initiate another uplink transmission until one of the conditions is met:
      - A message has been received in the Rx1 window
      - Waiting or transmission in the Rx2 window has ended

Receive Windows: Packet received in Rx1 window



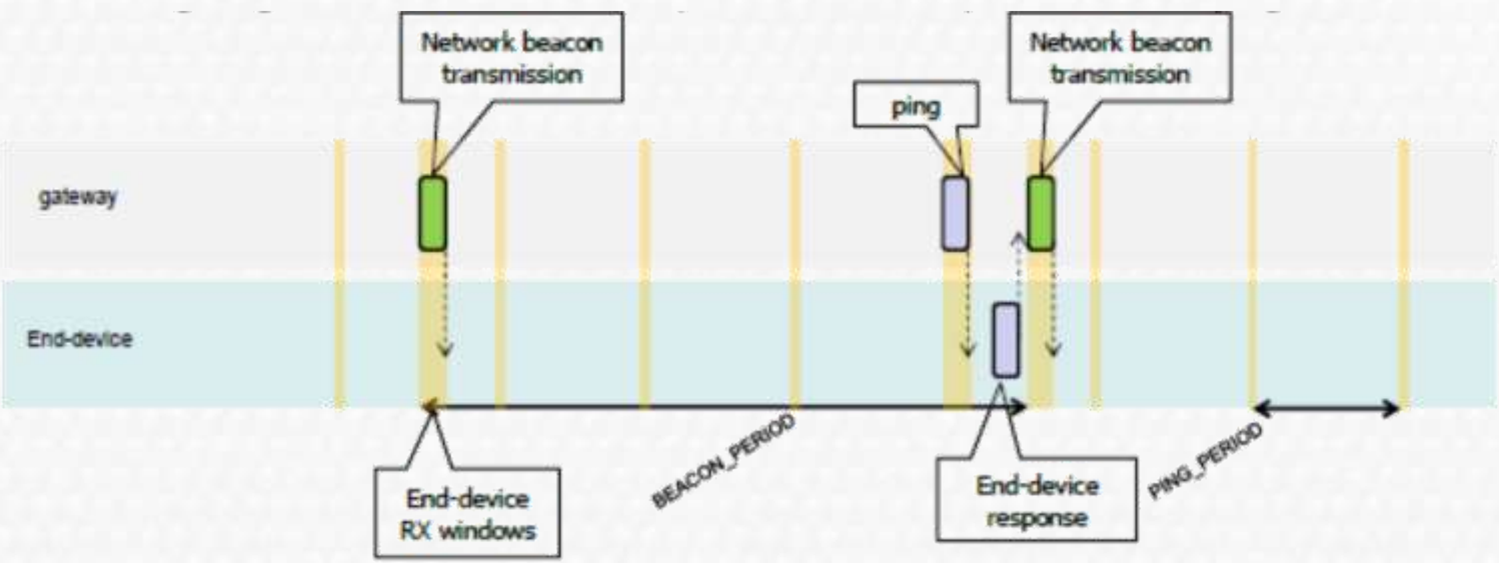
Receive Windows: Packet is received in Rx2 window



Source: lora-developers.semtech.com

LoRaWAN L2

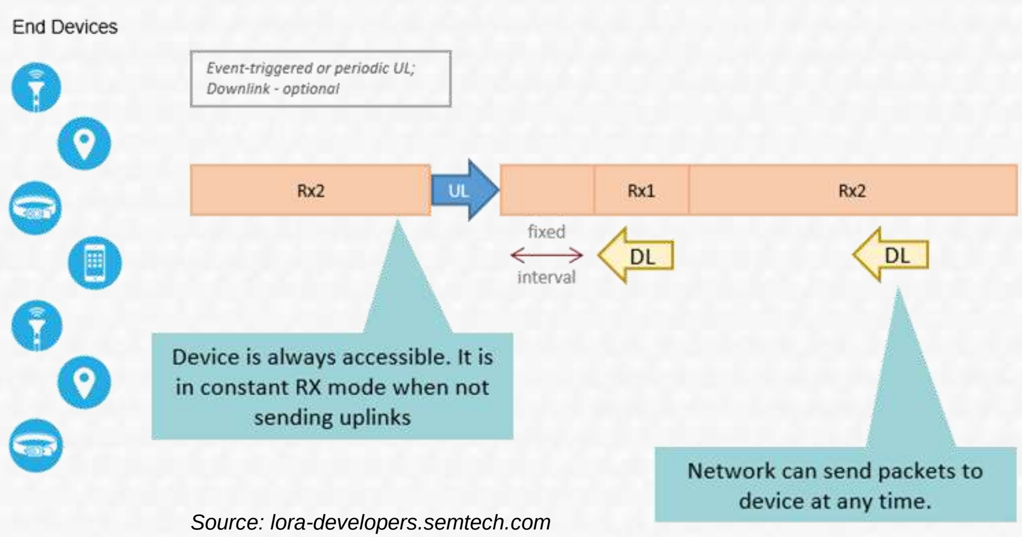
- LoRaWAN defines three transmission classes:
  - ✓ Class A: asynchronous communication
  - ✓ Class B: deterministic delay, synchronous communication
    - ❖ In addition to the mode as in class A (each device starts from class A), the end device cyclically opens the downlink window after receiving a Beacon message from the gateway (thanks to this the server knows when the device can receive data)



Source:
LoRaWAN™ 1.0.3 Specification

LoRaWAN L2

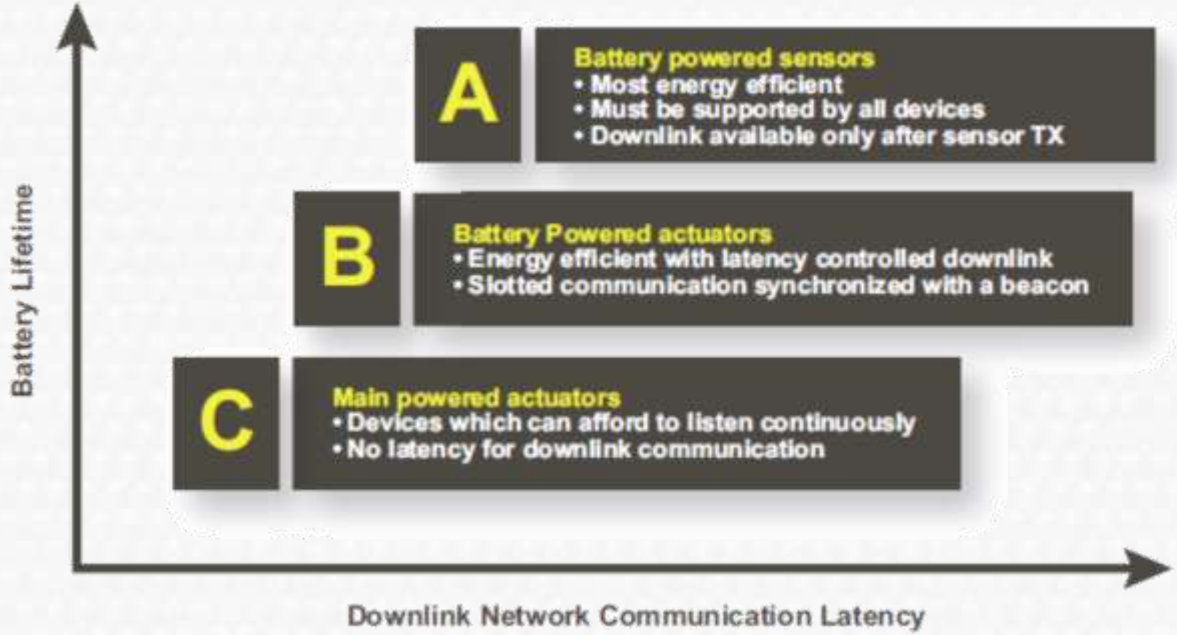
- LoRaWAN defines three transmission classes:
  - ✓ Class A: asynchronous communication
  - ✓ Class B: deterministic delay, synchronous communication
  - ✓ Class C: lowest delay, highest ability of downlink
    - The end device has the downlink window open almost all the time (it is closed only for the time of sending data)
    - Implementation is analogous to class A, but the Rx2 window is not closed until the next uplink transmission
    - Continuous power consumption by receiver
    - Class C is useful for updating the firmware of the device (FOTA)



Source: lora-developers.semtech.com

LoRaWAN L2

- ❑ LoRaWAN defines three transmission classes:
  - ✓ Class A: asynchronous communication
  - ✓ Class B: deterministic delay, synchronous communication
  - ✓ Class C: lowest delay, continuous power consumption by receiver



Source: lora-alliance.org

LoRaWAN L2

❑ LoRaWAN – types of messages

MAC Header (MHDR field)

Bits	[7:5]	[4:2]	[1:0]
MHDR	FType	RFU	Major

FType	Description
000	Join-Request
001	Join-Accept
010	unconfirmed data uplink
011	unconfirmed data downlink
100	confirmed data uplink
101	confirmed data downlink
110	RFU
111	Proprietary

Source:
LoRaWAN™ 1.0.4 Specification

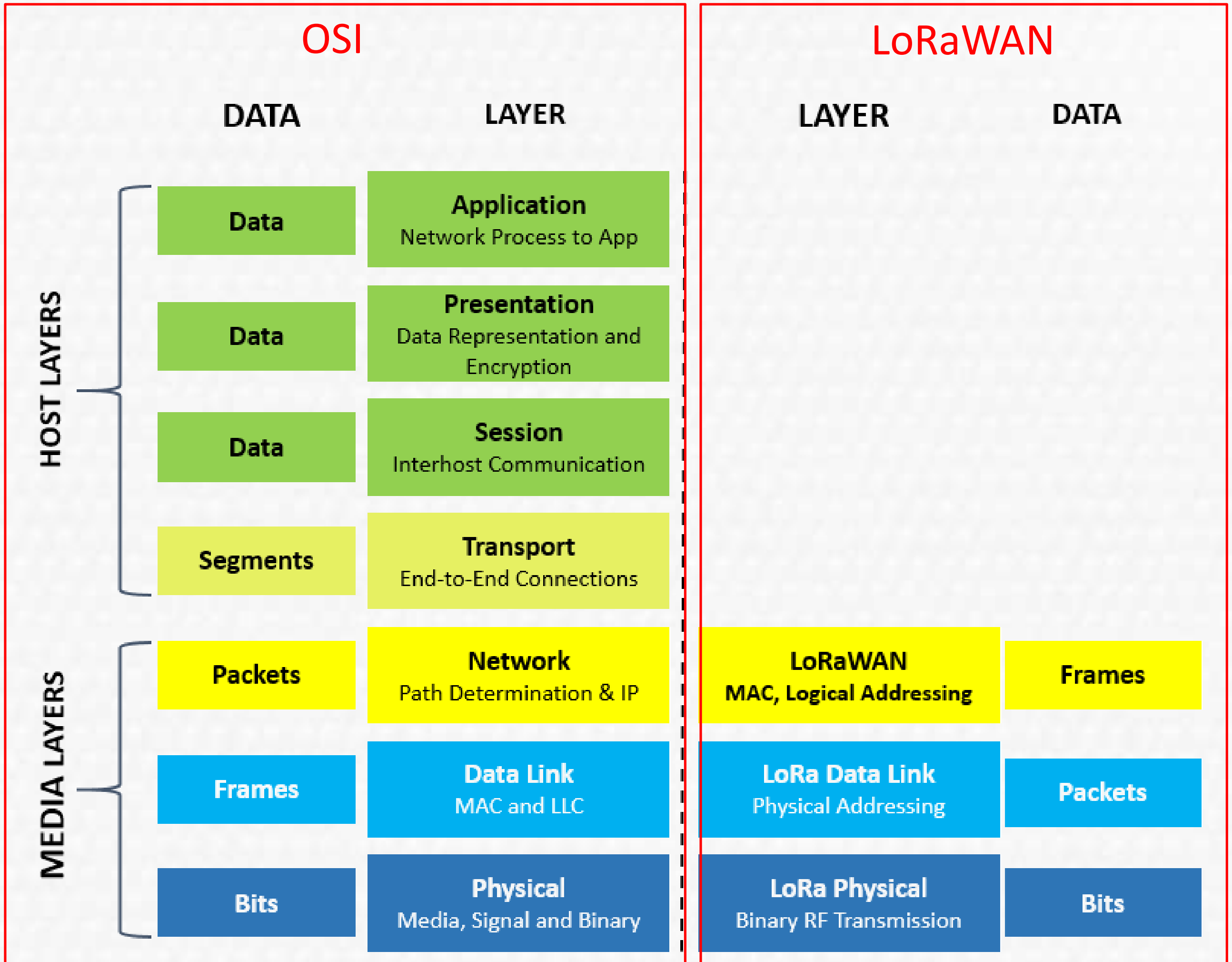
Join-request and *join-accept* messages – used to activate the device in over-the-air mode

Confirmed-data – receipt of the message must be acknowledged by the recipient
Unconfirmed-data – no confirmation of receipt of the message is required

The maximum message size (MAC Payload) depends on the transmission mode and ranges from 59 to 230 bytes (up to 250 assuming no repeater is used).

LoRaWAN L2

- LoRaWAN stack versus OSI stack



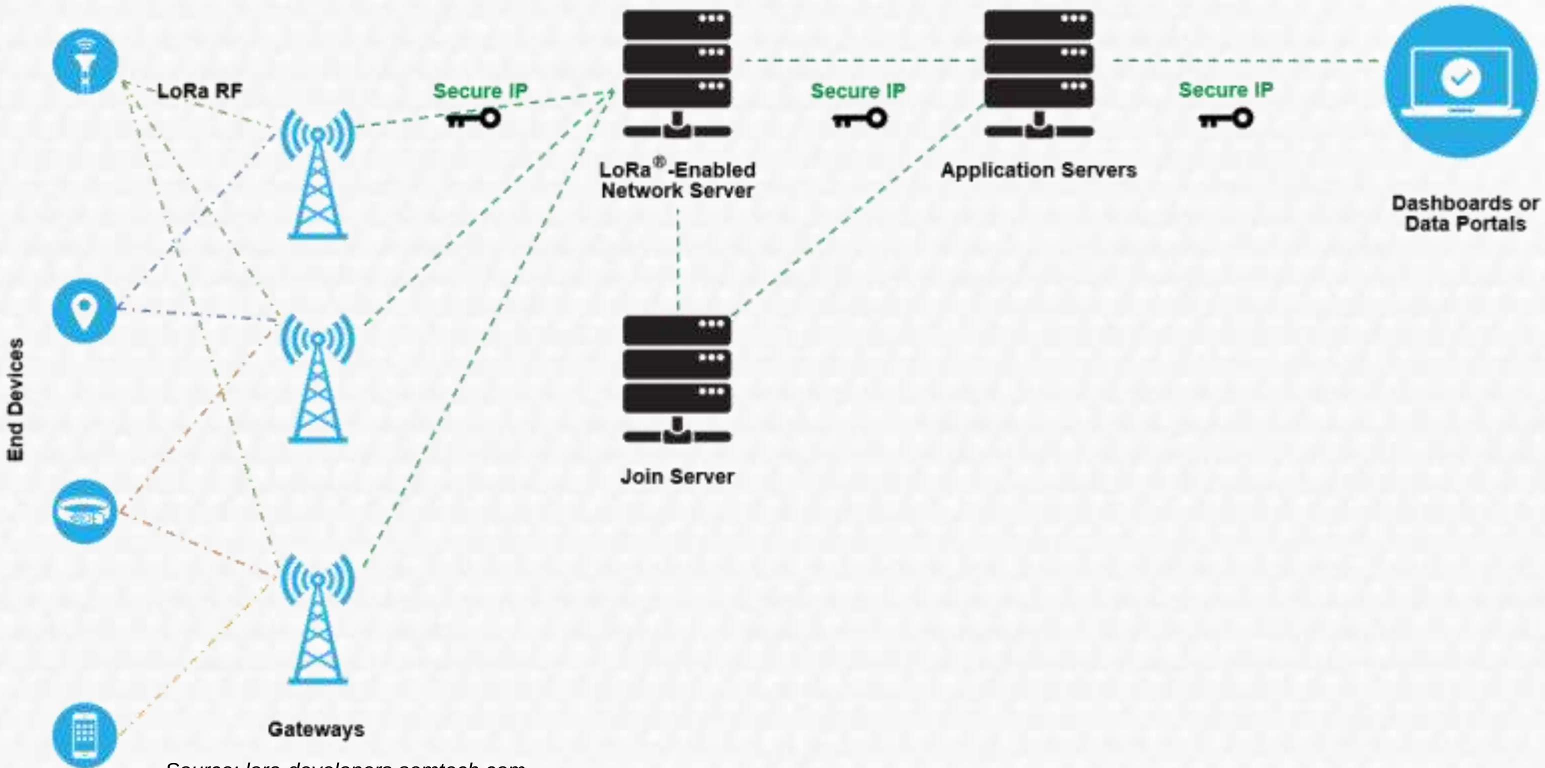
Source: *lora-developers.semtech.com*

Part 2: Foundations of LoRa and LoRaWAN

Transmission of messages in the LoRaWAN network

Transmission of messages in LoRaWAN

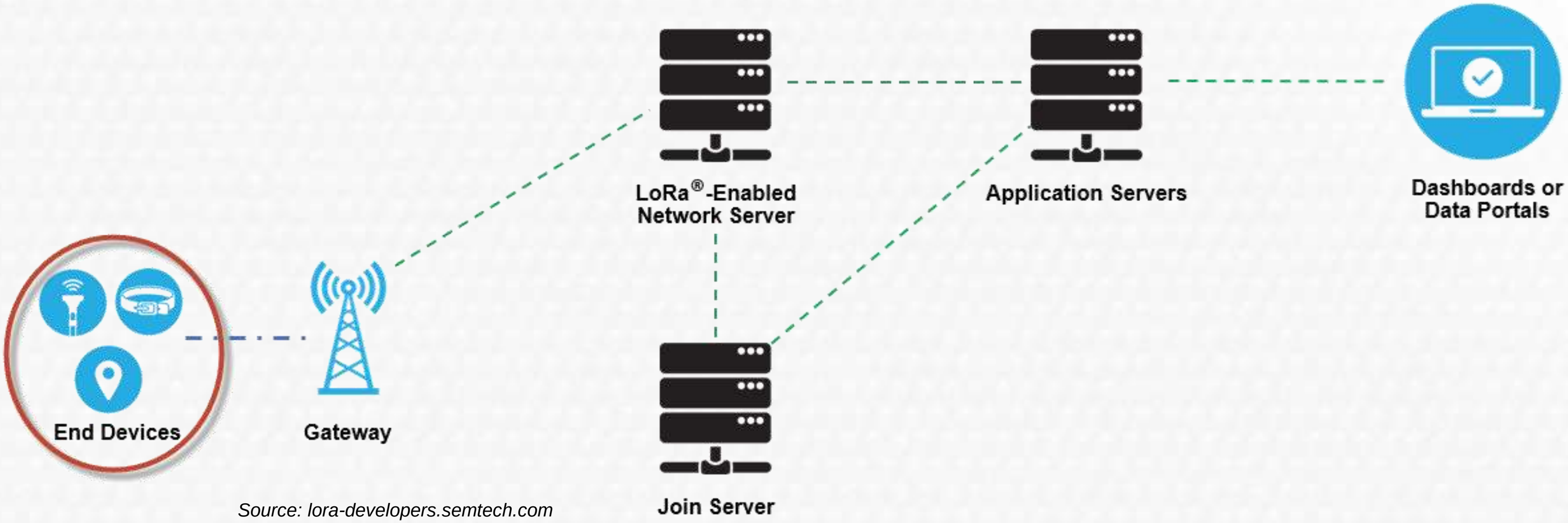
- There are four levels of devices in the structure of the LoRaWAN network:
  - ✓ End nodes
  - ✓ Gateways
  - ✓ Servers: LoRaWAN Network Server (LNS), Join Server, Application Server
  - ✓ Devices with a user interface



Source: lora-developers.semtech.com

Transmission of messages in LoRaWAN

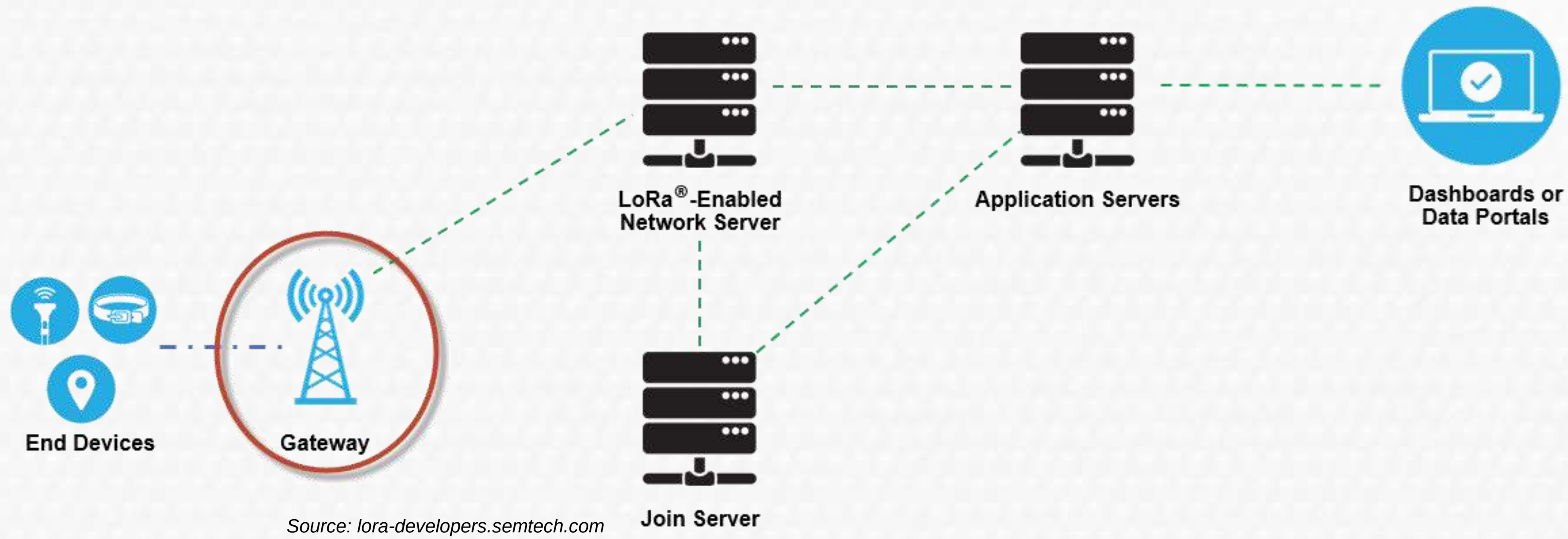
- There are four levels of devices in the structure of the LoRaWAN network:
  - ✓ End nodes (end devices)
    - ❖ These are sensors or actuators that communicate wirelessly with the gateway using LoRa radio interface
    - ❖ During production unique identifiers are saved in end devices which allow for safe activation of the device in the network and secure communication



Source: lora-developers.semtech.com

Transmission of messages in LoRaWAN

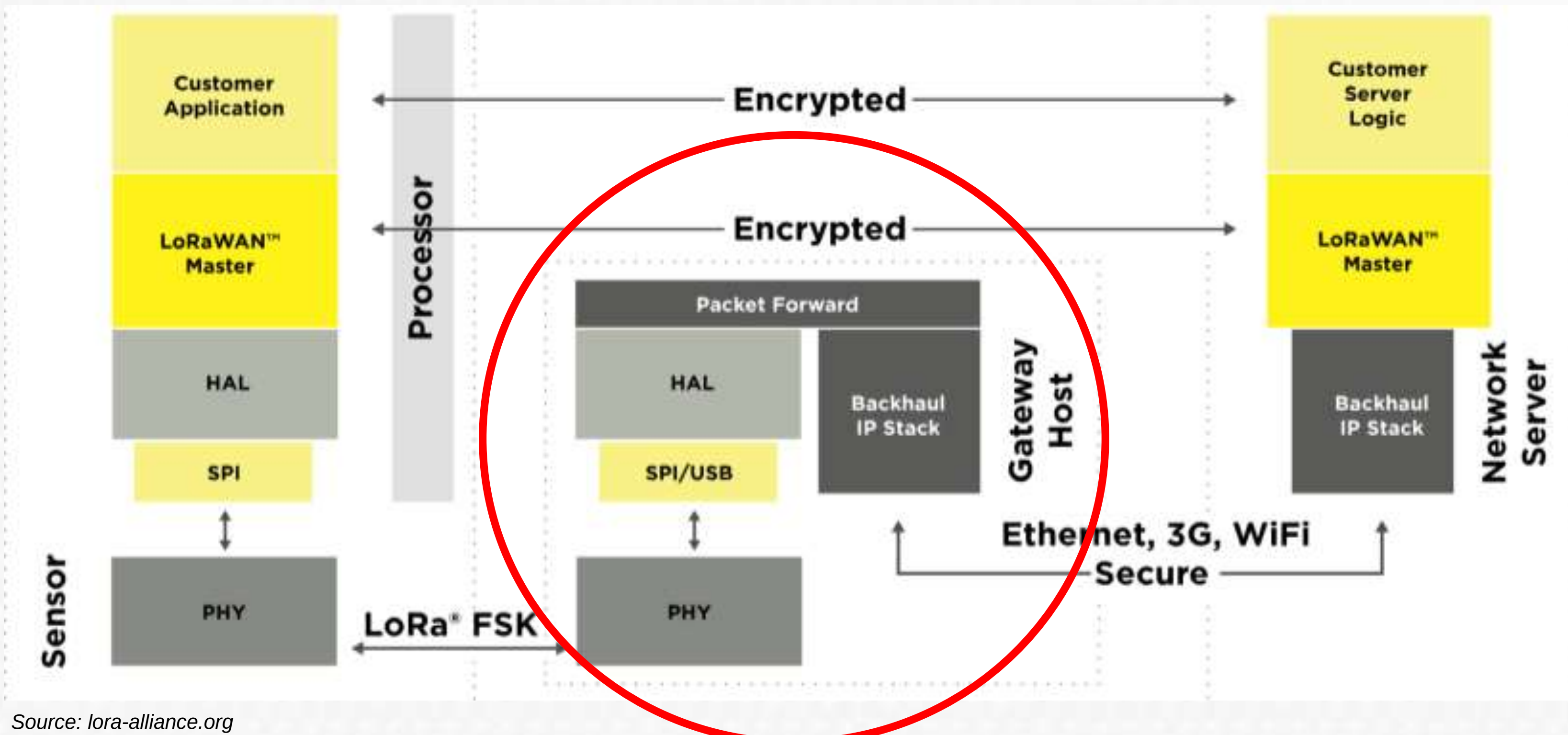
- There are four levels of devices in the structure of the LoRaWAN network:
  - ✓ Gateways
    - ❖ The gateway receives messages from end devices within its range via LoRa wireless communication, checks their CRC sum and transmits them to the LNS server (LoRaWAN Network Server) with additional data such as RSSI level and a time stamp.
    - ❖ An end device is not associated with a particular gateway and can contact multiple gateways within its range.
    - ❖ The packet sent by the end device can be received by many gateways. It can reduce a packet loss but LNS server must provide deduplication.



Source: lora-developers.semtech.com

Transmission of messages in LoRaWAN

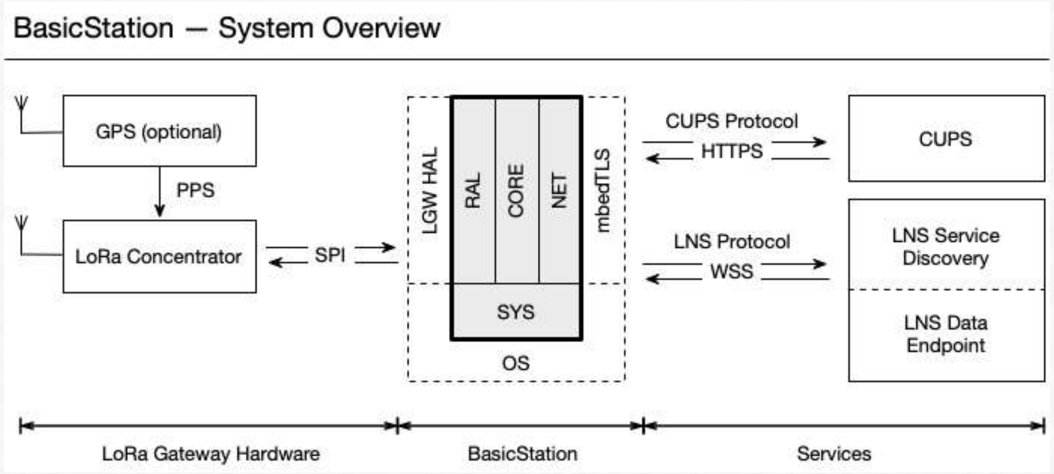
- LoRa gateway runs a Packet Forwarder process which communicates with:
  - ✓ LoRa interface circuit (usually through the HAL layer) to send and receive messages and to configure the interface
  - ✓ LoRaWAN Network Server (via the IP network) to transmit data received from end devices and to receive MAC commands and data for end devices



Source: lora-alliance.org

Transmission of messages in LoRaWAN

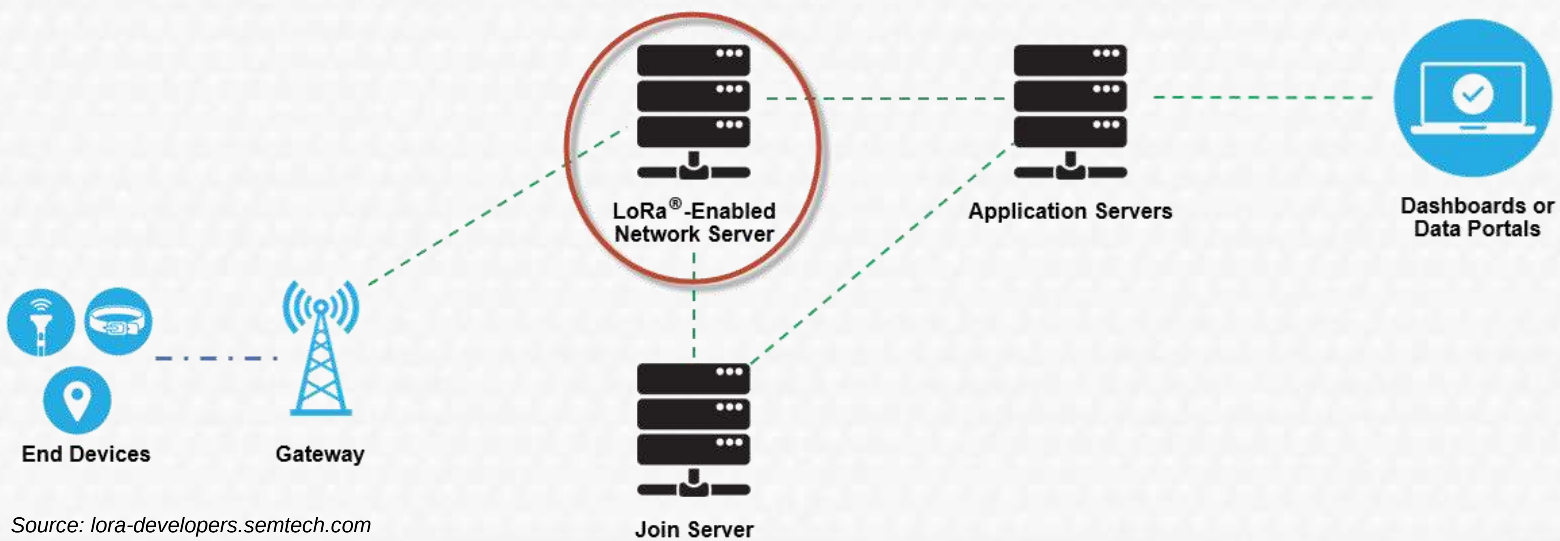
- Packet forwarder is usually provided by the gateway manufacturer or server operator (e.g. The Things Network).
- For example on The Things Network platform you can use the following packet forwarder solutions:
  - ✓ Semtech UDP Packet Forwarder – practically for all types of gateways
  - ✓ TTN Packet Forwarder – more modern solution, but available for a limited number of gateways - currently development of this software has been stopped
  - ✓ Semtech Basics Station – a modern solution, available for an increasing number of gateways. In addition to the functionality of communication with the LNS server (via websockets) it also provides remote configuration management and device updates (via CUPS - Configuration and Update Server).



Source: https://doc.sm.tc/station/

Transmission of messages in LoRaWAN

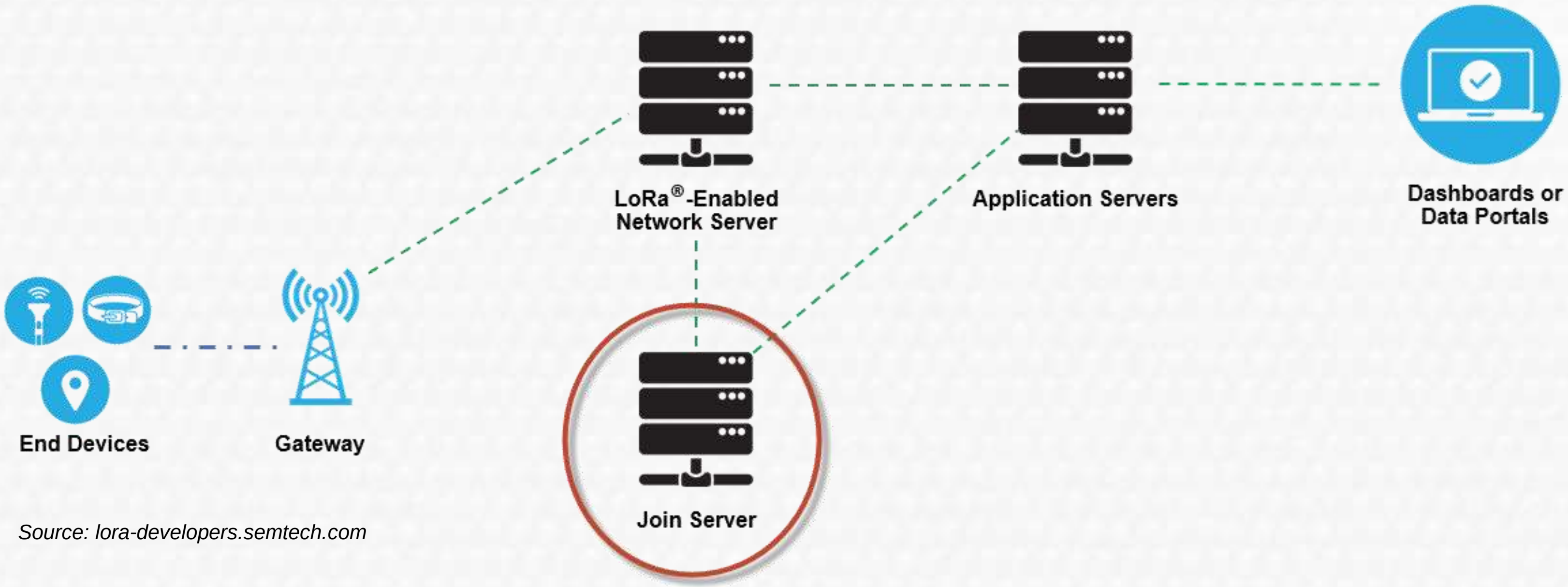
- There are four levels of devices in the structure of the LoRaWAN network:
  - ✓ LoRaWAN Network Server (LNS)
    - LNS manages the entire network, dynamically determines network parameters depending on the current conditions and sets up an encrypted AES-128 connection between the end device and the application (LNS does not have access to application data).
    - Checks the correctness of the frame authentication codes and the frame counter.
    - Confirms received messages (in confirmed mode)
    - Responds to MAC Layer (L2) Request messages from end devices
    - Forwards data to the appropriate application servers (uplink)
    - Queues data from application servers to end devices
    - Forwards Join-request and Join-accept messages between end devices and Join Server



Source: lora-developers.semtech.com

Transmission of messages in LoRaWAN

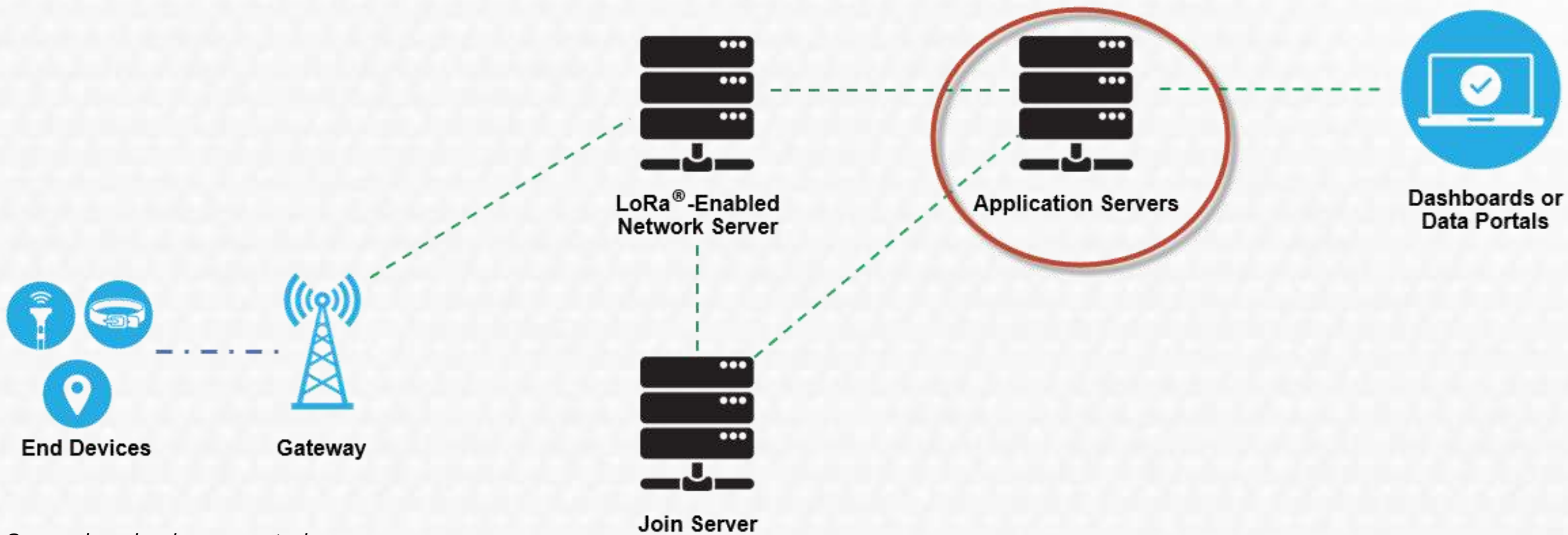
- There are four levels of devices in the structure of the LoRaWAN network:
  - ✓ Join server
    - Manages the over-the-air end device activation process in order to add them to the LoRaWAN network.
    - Stores information allowing for the processing of *join-request* requests and generation of *join-accept* responses.
    - Designates application and network session keys
    - Informs LNS which application server will be associated with a particular end device



Source: *lora-developers.semtech.com*

Transmission of messages in LoRaWAN

- There are four levels of devices in the structure of the LoRaWAN network:
  - ✓ Application servers
    - ❖ They are responsible for communication with end devices in order to exchange (mainly receive) and process application data according to the requirement of the particular application.
    - ❖ Forwards processed data to the dashboard or data portals with user interface.



Source: *lora-developers.semtech.com*

Part 2: Foundations of LoRa and LoRaWAN

Security aspects in the LoRaWAN network

Security aspects in the LoRaWAN network

- Fundamental requirements for secure communication: **confidentiality, integrity, availability**
- Security threats in LoRaWAN network
  - ✓ Wiretapping of communications (sniffing)
    - ❖ LoRa radio level
    - ❖ TCP/IP network level
  - ✓ Unauthorized connection to the network
  - ✓ Jamming of radio signal
- Communication security means included in the LoRaWAN specification
  - ✓ OTAA, ABP activation procedures (end node authentication)
  - ✓ Protection of communication integrity between the end device and the LNS server
  - ✓ Encryption of communication between the end device and the application server

Security aspects in the LoRaWAN network

Creating a secure communication channel

- Fundamental requirements for secure communication: **confidentiality, integrity, availability**
- **Confidentiality** can be ensured by **encryption** → for symmetric ciphers a common secret (encryption key) must be present on both sides
- **Integrity** of communication can be ensured by **secure authentication** (proving of identity) using:
  - A digital certificate issued by an authority trusted by the other side
    - ✓ PKI infrastructure is required
  - Verification of the common secret in a way that makes it impossible to obtain it by a third party (e.g. by eavesdropping on communication): a challenge-response method can be used here, in which party A generates a random request and sends it to party B, which then encodes it using the common secret and sends it back back to side A. Side A compares the received response with the self-encoded challenge (or decrypts the response and compares it with the sent challenge)
    - ✓ Encoding can be realized using encryption algorithm (ciphers) or authentication codes (e.g. MAC, HMAC) based on hash functions
    - ✓ Both parties must have a common secret agreed in an authenticated manner.

Security aspects in the LoRaWAN network

Creating a secure communication channel

- Secure agreement (exchange) of a common secret can be achieved through:
  - Its exchange through a separate secure communication channel (OOB – Out-of-Band):
    - e.g. manual configuration on all devices, sending by letter, dictating over the phone and so on
  - Generating the secret by side A, encrypting it with the public key of side B and sending it to side B
    - ✓ PKI infrastructure is required to validate the public key
  - Key exchange using Diffie-Hellman or similar algorithm
    - ✓ In the version without additional authentication of public numbers, this method is vulnerable to Man-in-the-Middle attack.

Security aspects in the LoRaWAN network

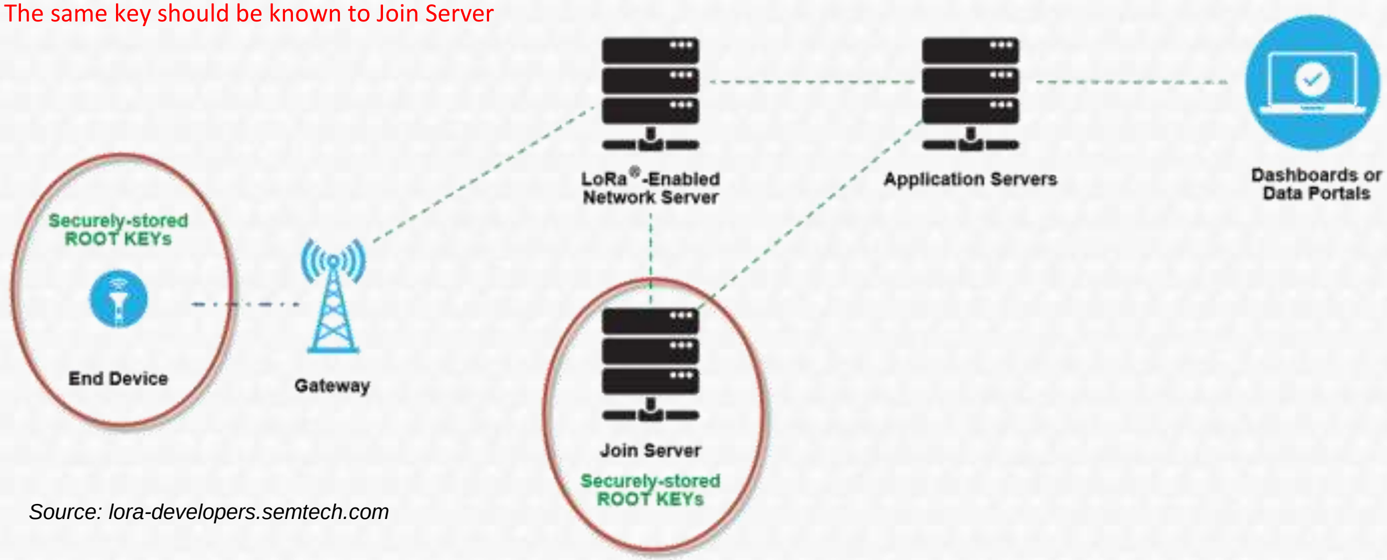
- LoRaWAN – activation of end devices
- In order for the end node to become an element of a particular LoRaWAN network, the procedure of its activation must be carried out
  - ✓ This provides control which end devices can join the network and then communicate with specific applications
- Activation of end devices in the LoRaWAN network can be carried out in two modes:
  - ✓ Over-The-Air Activation (OTAA)
  - ✓ Activation by Personalization (ABP)

Security aspects in the LoRaWAN network

- LoRaWAN – activation of end devices
- Nevertheless of the activation method (OTAA or ABP) this process results in the following parameters stored in the memory of the end device:
  - ✓ Device address (DevAddr)
    - A 32-bit address identifying the device on a given network
    - It consists of the *N*-bit network prefix (AddrPrefix, *N* = 7 ... 25) derived from the unique identifier of the LNS server (NetID, specified in the document "LoRaWAN Backend Interfaces Specification") and the (32-*N*) bit network address of the device (NwkAddr)
    - AddrPrefix allows to identify the LNS that has assigned a given DevAddr
    - DevAddr is a non secret parameter
  - ✓ Network session key (NwkSKey)
    - ✓ An individual network key assigned to a given device and its specific session in the network
    - ✓ NwkSKey is used by LNS and the end device to calculate the Message Integrity Code (MIC) of data sent in frames (it is also used to encrypt data in MAC-only frames with Fport = 0)
    - ✓ The NwkSKey should be stored in the device in a manner that is protected against unauthorized reading
  - ✓ Application session key (AppSKey)
    - ✓ Individual application session key for a given device
    - ✓ Used by application server and end device to encrypt and decrypt data in application-specific frames
    - ✓ AppSKey should be stored on the device in a manner that is secured against its unauthorized reading

Security aspects in the LoRaWAN network

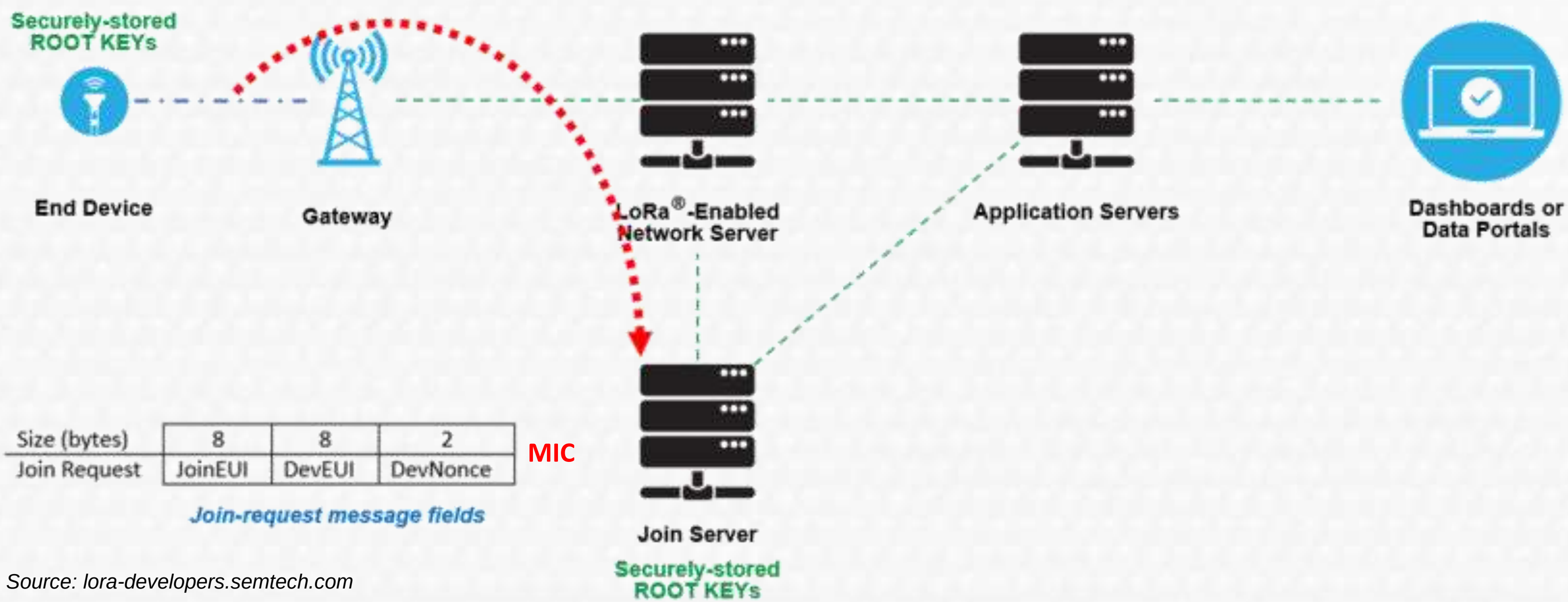
- Activation of end devices using the Over-The-Air Activation method (OTAA)
  - ✓ The following parameters should be pre-configured in the end device:
    - ✓ ***DevEUI*** – globally unique device identifier (in IEEE EUI64 format) – non secret
    - ✓ ***JoinEUI*** – a global application ID in the IEEE EUI64 address space that uniquely identifies the Join-Server that is able to assist in the processing of the Join procedure (previously the name **AppEUI** was used) – non secret
    - ✓ ***AppKey*** – the main key (root key) of the AES-128 encryption algorithm assigned to a given end device – secret
      - ❖ The same key should be known to Join Server



Source: lora-developers.semtech.com

Security aspects in the LoRaWAN network

- OTAA activation process is performed using the *Join-Request* and *Join-Accept* messages, which securely (by using the hash function and encryption) connects the device to the network by providing it with the *NwkSKey* and *AppSKey* session keys and the *DevAddr*.
  - ✓ In the first step, the device sends the *Join-Request* message to the Join Server with *JoinEUI*, *DevEUI* and *DevNonce*.
  - ✓ *DevNonce* is a 16-bit value representing a "counter" of device activation. When initializing the device, *DevNonce* = 0 is assumed and this value is increased by 1 with each subsequent activation. Since Join Server remembers the current *DevNonce* value and does not allow activation with lower values, the device should keep the current *DevNonce* value permanently.
    - ❖ If the device in its life cycles may exceed 65,536 activations, it should be planned to configure many *JoinEUI*s.
  - ✓ The frame with the *Join-Request* message contains the MIC authentication code calculated with the ***AppKey***.



Source: lora-developers.semtech.com

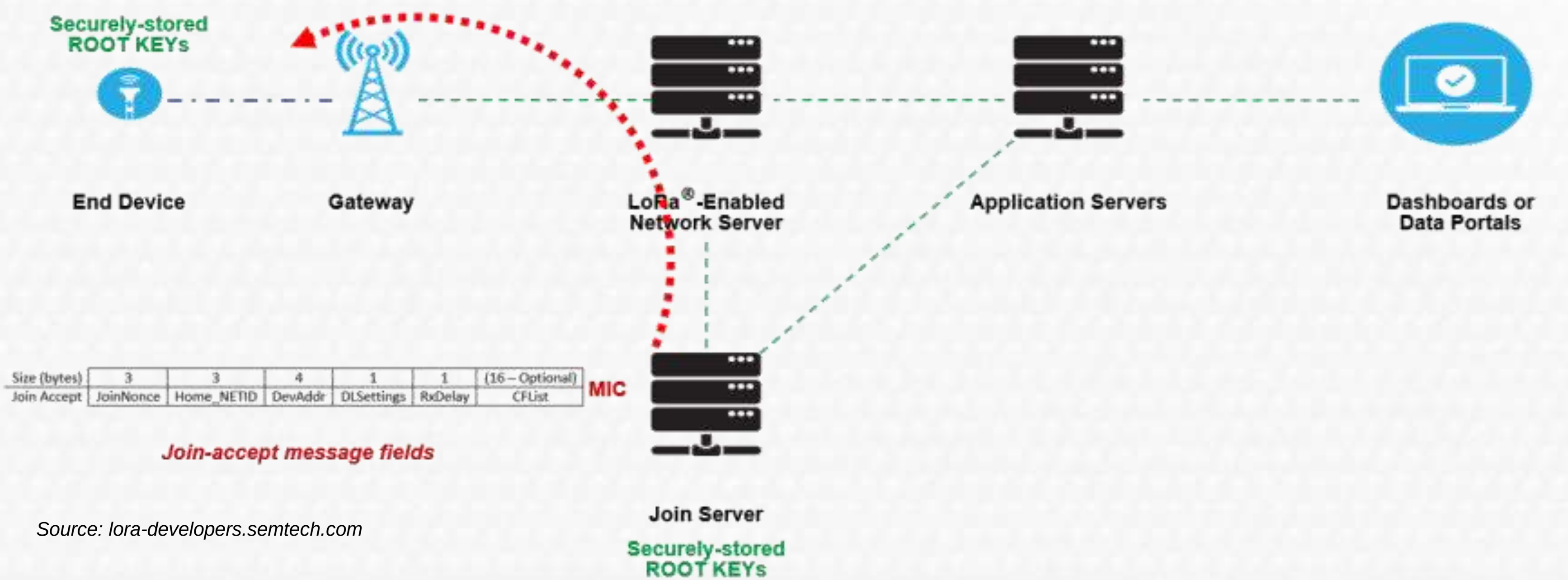
Security aspects in the LoRaWAN network

❑ Activation of end devices using the Over-The-Air Activation method (OTAA)

- ✓ The second step: Join Server verifies the received activation request and if the device is authorized to join the network, sends the *Join-Accept* message containing, among others, *JoinNonce* (a 24-bit counter managed by JS)
- ✓ The third step: End device computes the *NwkSKey* and *AppSKey* session keys according to the equations:

  NwkSKey = aes128_encrypt(AppKey, 0x01 | JoinNonce | NetID | DevNonce | pad_{16})

  AppSKey = aes128_encrypt(AppKey, 0x02 | JoinNonce | NetID | DevNonce | pad_{16})
- ✓ The frame with the Join-Accept message contains the MIC authentication code calculated with the ***AppKey***
- ✓ OTTA activation is performed every time the session context is lost



Source: lora-developers.semtech.com

Security aspects in the LoRaWAN network

- LoRaWAN – Activation by Personalization (ABP)
  - ✓ ***NwkSKey*** and ***AppSKey*** and the ***DevAddr*** address are statically configured on the device instead of ***DevEUI***, ***JoinEUI*** (***AppEUI***), and ***AppKey***

Over-The-Air Activation	**Activation by Personalization**
▪ The end device has pre-set parameters that allow for the generation of individual session keys. ▪ Session keys are valid for a given device activation in the network and after its disconnection (or loss of the session context) they lose their validity. ▪ The device may have saved parameters for activation in various LoRaWAN networks. ▪ This is the recommended activation method that provides effective protection against any breach attempts.	▪ Data (keys) securing communication of the device are permanently stored in it at the production stage and their possible change is difficult to carry out in a safe manner. ▪ One advantage is the immediate network readiness of the device without a separate dynamic activation procedure. ▪ Devices are permanently assigned to a given network (NetID is part of the device address). ▪ It is a simplified, less secure, activation method (e.g. for resource-constrained devices).

Security aspects in the LoRaWAN network

- ❑ OTAA, ABP activation procedures (end node authentication)
- ❑ Protection of the integrity of communication between the end device and the LNS server with the use of MIC codes calculated using the NwkSkey
  - ✓ The MIC (Message Integrity Code) is calculated in accordance with the RFC 4493 specification on a message containing all the fields contained in the frame:

```
msg = MHDR | FHDR | FPort | FRMPayload
CMAC = aes128_cmac(NwkSKey, B0 | msg)
MIC = CMAC[0..3],
```

where block B_0 is defined as below:

Size (octets)	1	4	1	4	4	1	1
B_0	0x49	4 × 0x00	Dir	DevAddr	FCntUp or FCntDown	0x00	len(*msg*)

Source: LoRaWAN™ 1.0.4 Specification

len(msg) is the length of the frame in bytes

Dir is 0 for uplink and 1 for downlink

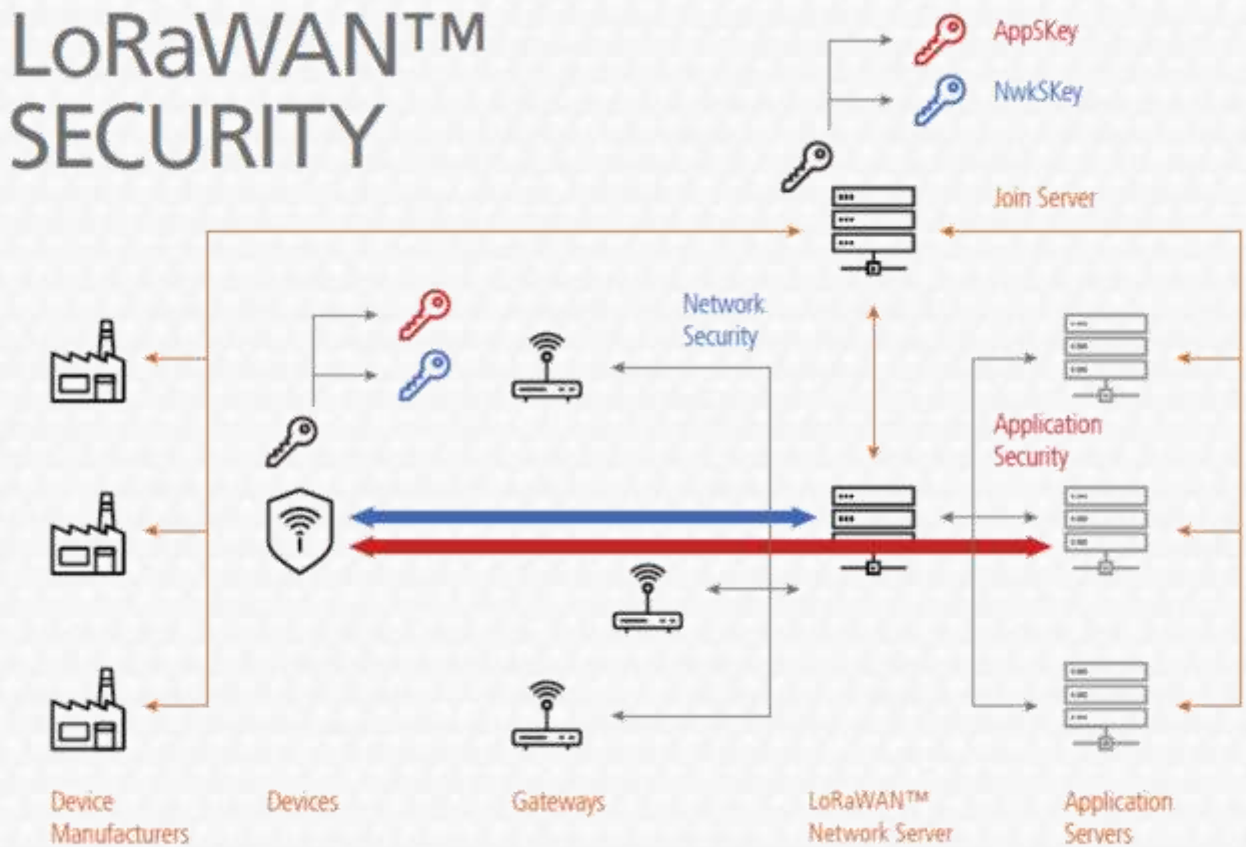
Security aspects in the LoRaWAN network

- ❑ OTAA, ABP activation procedures (end node authentication)
- ❑ Securing the integrity of communication between the end device and the LNS server with the use of MIC codes calculated using the NwkSkey
- ❑ Encryption of communication between the end device and the application server or LNS through a symmetric AES-CTR cipher with a 128-bit key
  - ✓ The plaintext (pld) constituting the frame payload (FRMPayload) is encrypted prior to the MIC calculation
  - ✓ The encryption scheme is based on the general algorithm described in IEEE 802.15.4/2006 770 Annex B
  - ✓ An AES cipher with a 128-bit key is used
  - ✓ The key used for encyption (*K*) depends on the FPort used in the frame:
    - ✓ For FPort=0 the *K* is a *NwkSKey* (this FPort is used by LNS to send MAC layer commands)
    - ✓ For FPort=1…255 the *K* is a App*SKey* (these FPorts are used for application data)

FPort	***K***
0	NwkSKey
1..255	AppSKey

Security aspects in the LoRaWAN network

- ❑ OTAA, ABP activation procedures (end node authentication)
- ❑ Securing the integrity of communication between the end device and the LNS server with the use of MIC codes calculated using the NwkSkey
- ❑ Encryption of communication between the end device and the application server or LNS through a symmetric AES-CTR cipher with a 128-bit key



Source: *LoRaWAN Security Whitepaper*

Part 2: Foundations of LoRa and LoRaWAN

Conclusion

Conclusion

- LoRaWAN can provide long distance low rate communication in urban and rural areas for outdoor and indoor applications

- LoRaWAN is suitable for:
  - ✓ Gathering small amount of data from distributed battery-powered sensors
    - smart cities, homes and buildings, communities, agriculture, metering and utilities, healthcare, environment, and supply chain and logistics
  - ✓ Control of distributed main-powered actuators
  - ✓ Limited control of distributed battery-powered actuators

- LoRaWAN is not suitable for:
  - ✓ Internet access
  - ✓ Real-time communication
  - ✓ Massive data transmission (e.g. multimedia streaming, security cameras)

How to learn more

- ❑ Semtech LoRa® Developer Portal
  https://lora-developers.semtech.com/
  - ✓ LoRaWAN Academy
  - ✓ Hands-on labs

- ❑ LoRa Alliance® Portal
  https://lora-alliance.org/
  - ✓ Resource Library
    - ❖ Technical Specifications
    - ❖ Technical Recommendations

- ❑ The Things Network
  https://www.thethingsnetwork.org/
  - ✓ The Things Network consists of an inclusive and open community of people, companies, governments and universities who are learning, experimenting and building with The Things Stack to realize LoRaWAN solutions

Part 3:
Practical demonstration of creating LoRaWAN IoT measurement application

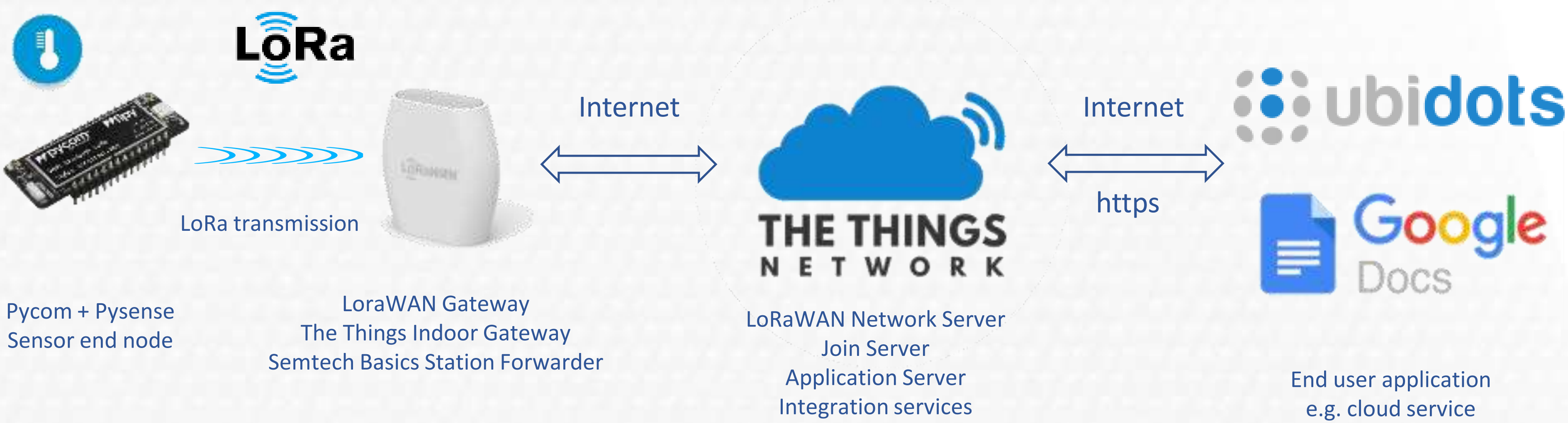
LoRaWAN application for the IoT system

- In this part you will learn:
  - ✓ What practical problems can be solved using LoRaWAN network.
  - ✓ How to create LoRaWAN end node firmware in MicroPython language.
  - ✓ How to use The Things Network in your own project.
  - ✓ How to create user application on the base of Google Docs service.

Part 3:
Practical demonstration of creating LoRaWAN IoT measurement application

Application structure

LoRaWAN application for the IoT system

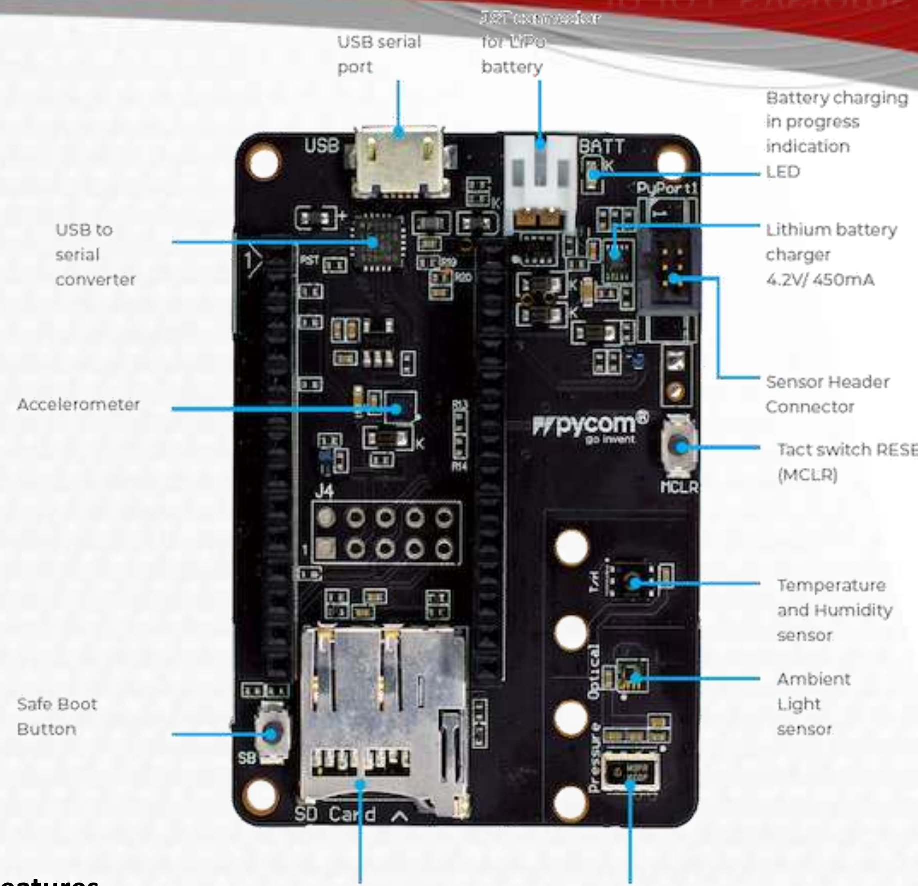


Part 3:
Practical demonstration of creating LoRaWAN IoT measurement application

Used components

LoRaWAN application for the IoT system

End node: Pycom FiPy + Pysense



Features

- Five Networks: WiFi, BLE, cellular LTE–CAT M1/NB1, LoRa and Sigfox
- Powerful CPU.
- Can also double up as a Nano LoRa gateway
- MicroPython enabled
- Fits in a standard breadboard (with headers)
- Ultra–low power usage
- World ready, one product covers all LTE–M bands

Features

- Ambient light sensor
- Barometric pressure sensor
- Humidity
- 3 axis 12-bit accelerometer
- Temperature sensor
- Compatible with development board as WiPy, FiPy, GPy and LoPy
- Ultra-low power standby mode
- Powered via USB or LiPo Battery connector

Source: pycom.io/products/

LoRaWAN application for the IoT system

LoRaWAn Gateway

LoRa	
Chipset	Semtech SX1308
Channels	8 Channels
Receive Sensitivity	-140/-135 dBm (EU/US)
Transmit Power	Up to +27 dBm
LoRaWAN® Spec Version	V.1.0.3
Packet Forwarder	LoRa Basics Station
Wi-Fi	
SoC	ESP8266
Mode	802.11 b/g/n, Client Mode
Tx Power	+20 dBm
Frequency Bands	2.4 GHz
WAN/LAN ports	-
USB Port	USB Type-C (900 mA)
Security	WPA/WPA2
Dimensions	90*80*40 mm
Operating Temperature	0-40℃
Certification	CE/FC/IC/RCM/WPC/RoHS

LoRaWAN application for the IoT system

LoRaWAN Network Server
Join Server
Application Server
Integration services

The workbench to get you started with IoT.

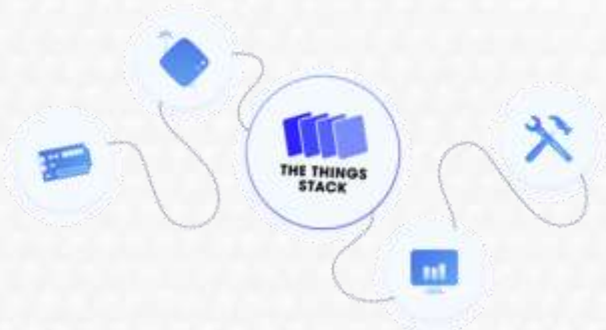
The Things Network provides a set of **open tools** and a **global, open network** to build your next IoT application at **low cost**, featuring **maximum security** and ready to **scale**.

Create a free account

Powered by The Things Stack.

The Things Stack is a **LoRaWAN Network Server** which is the critical component for any LoRaWAN solution. Used by thousands of companies and developers around the world, it securely manages **applications**, **end devices** and **gateways** and is built by **The Things Industries**.

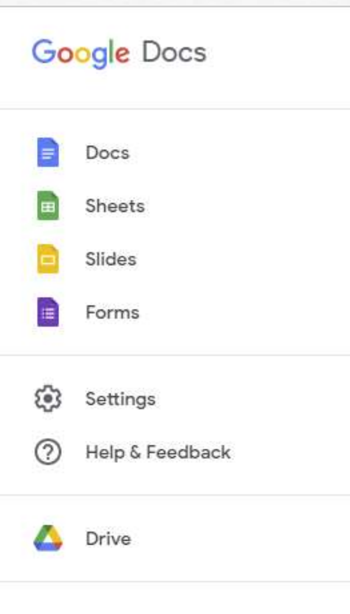
Learn more about The Things Stack

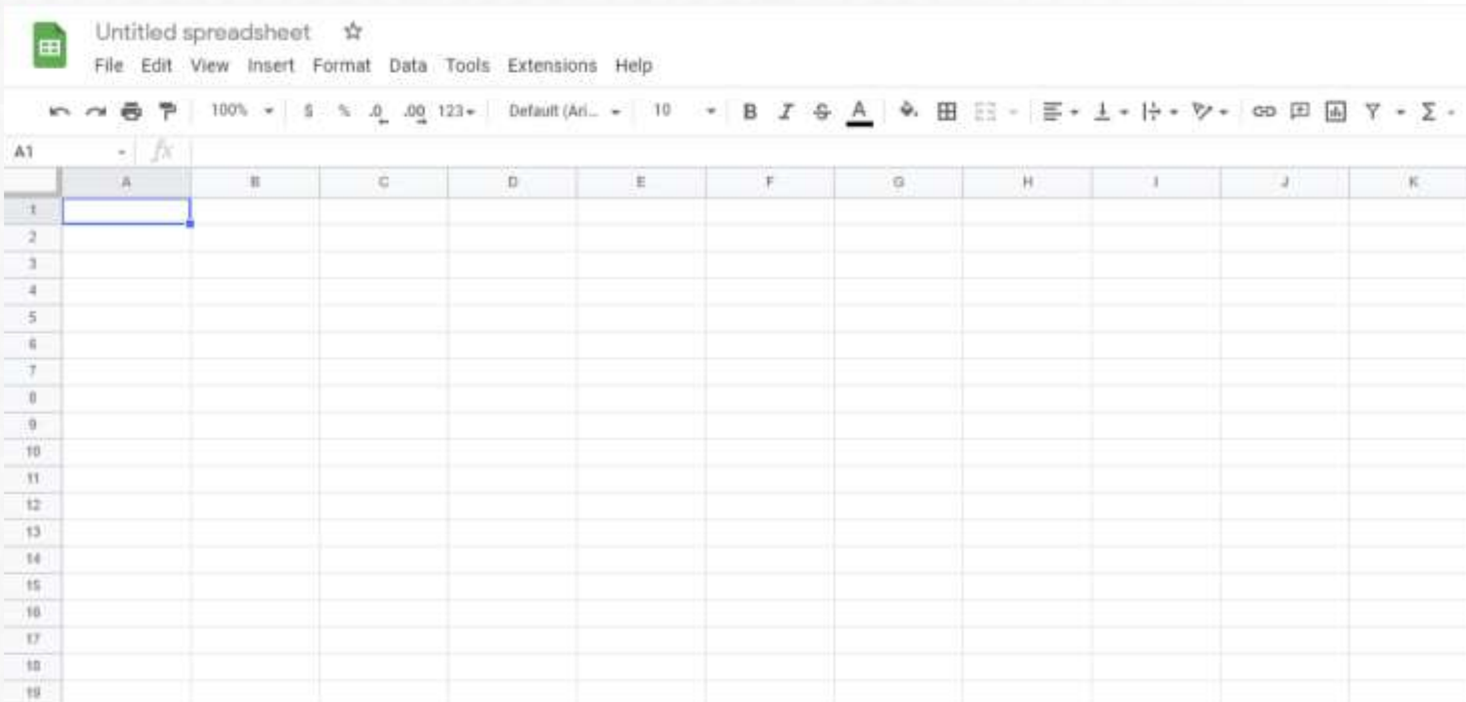


Source: thethingsnetwork.org

LoRaWAN application for the IoT system

End user application – Google Docs Spreadsheet



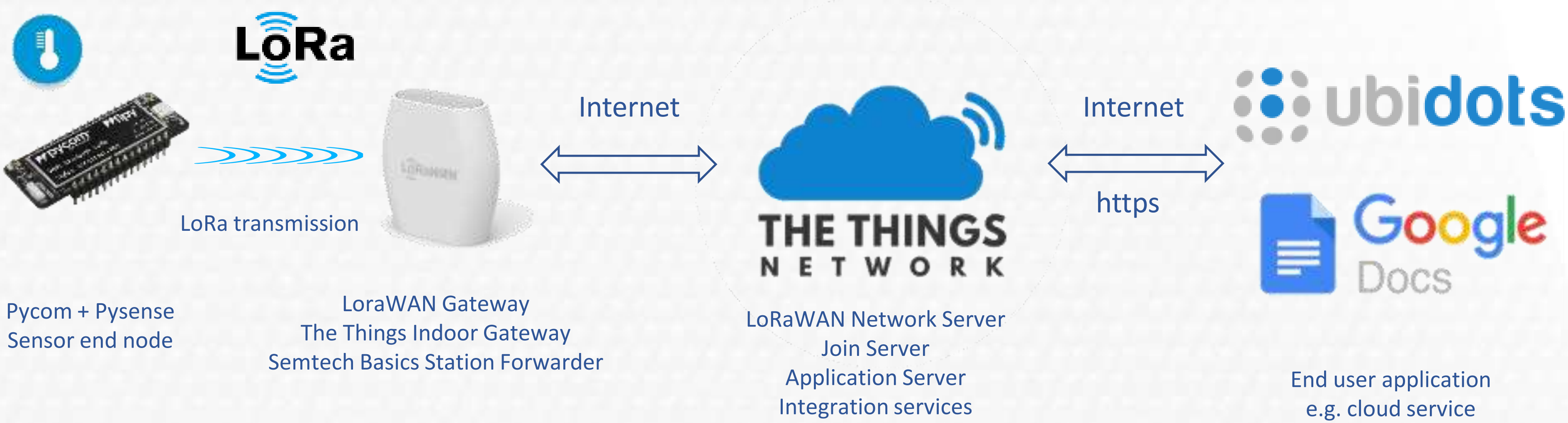


Source: docs.google.com

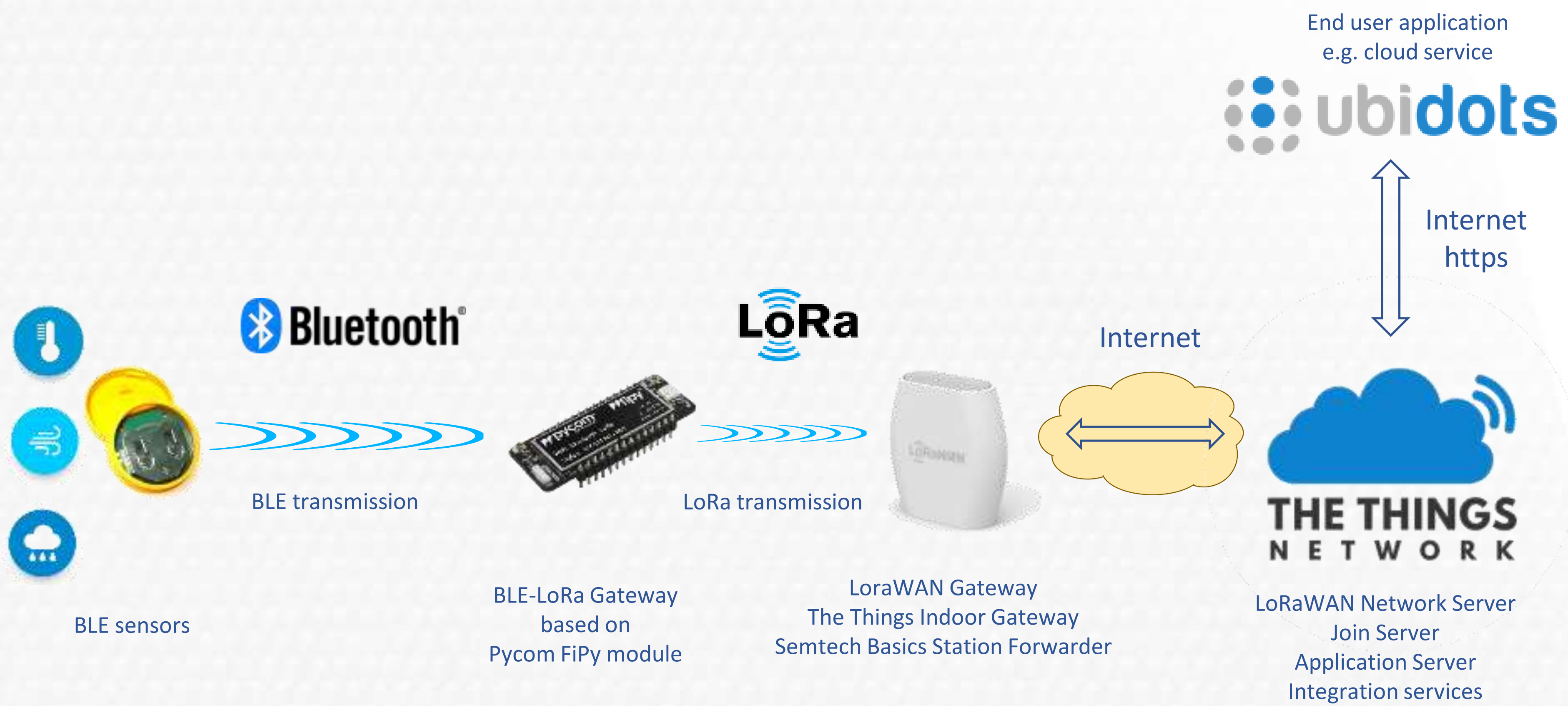
Part 3:
Practical demonstration of creating LoRaWAN IoT measurement application

Putting all things together

LoRaWAN application for the IoT system



LoRaWAN application for the IoT system



How to learn more

Thank You!