

IoT App Development



LoRa and LoRaWAN Technology

Dr. Manas Khatua

Associate Professor, Dept. of CSE, IIT Guwahati

E-mail: manaskhatua@iitg.ac.in

“All Birds find shelter during a rain. But Eagle avoids rain by flying above the Clouds” – **APJ Abdul Kalam**

IoT Access Technologies

- there are many IoT technologies in the market today



LoRaWAN

LoRaWAN is a wireless networking protocol **published in 2015**.

For more details: <https://lora-alliance.org/>

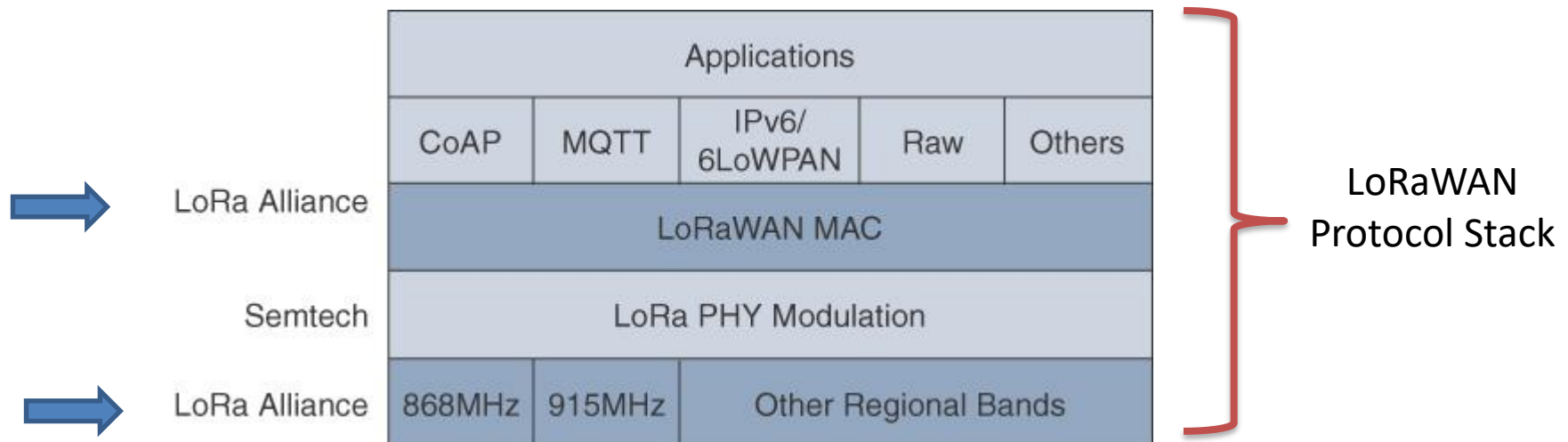
LPWA Technology

- A new set of wireless technologies has received a lot of attention from the industry, known as
 - **Low-Power Wide-Area** (LPWA) networking technology
- **unlicensed-band** LPWA technology
 - LoRaWAN
- **licensed-band** LPWA technology
 - NB-IoT and Other LTE Variations



LoRa Alliance

- Initially, **LoRa** was a **PHY layer modulation scheme**
 - developed by a **French company “Cycleo”**; Later, Cycleo was acquired by **Semtech**.
 - Semtech LoRa**: PHY modulation technology available by multiple chipset vendors
- The **LoRa Alliance** is a technology alliance committed to
 - enabling large scale deployment of **Low-Power Wide Area Networks** (LPWAN) IoT
 - publishing **LoRaWAN** specifications for LPWAN
- LoRaWAN** is a premier solution for global LPWAN deployments at present
 - Its MAC-layer protocol built on top of LoRa PHY

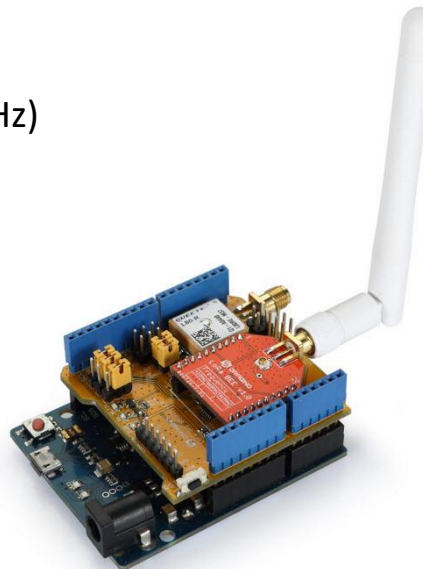


LoRa PHY layer

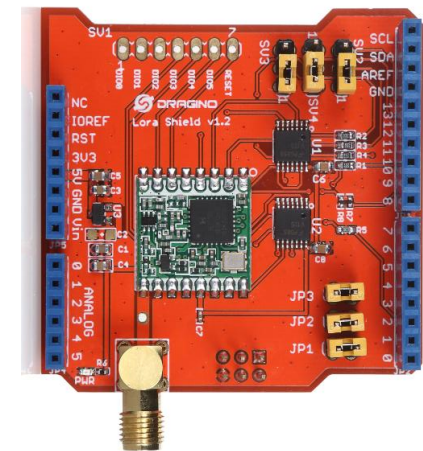
- Semtech LoRa PHY
- Uses a variation of **chirp spread spectrum** (CSS) modulation
 - it allows demodulation below the noise floor.
So, offers **robustness to noise and interference**
 - manages a single channel occupation by different **spreading factors** (SFs)
- Main **unlicensed** sub-GHz frequency bands
 - 433 MHz
 - 779–787 MHz
 - 863–870 MHz (**In India**: 868 MHz)
 - 902–928 MHz



LoRa Module: **SX1276**
868MHz band



LoRa GPS Shield
with Arduino



LoRa Shield for Arduino

LoRaWAN MAC layer

- LoRaWAN endpoints are classified into **three classes**.

Class A:

- this is default implementation
- optimized for battery-powered nodes
- allows bidirectional communications
- two receive windows** are available after each transmission

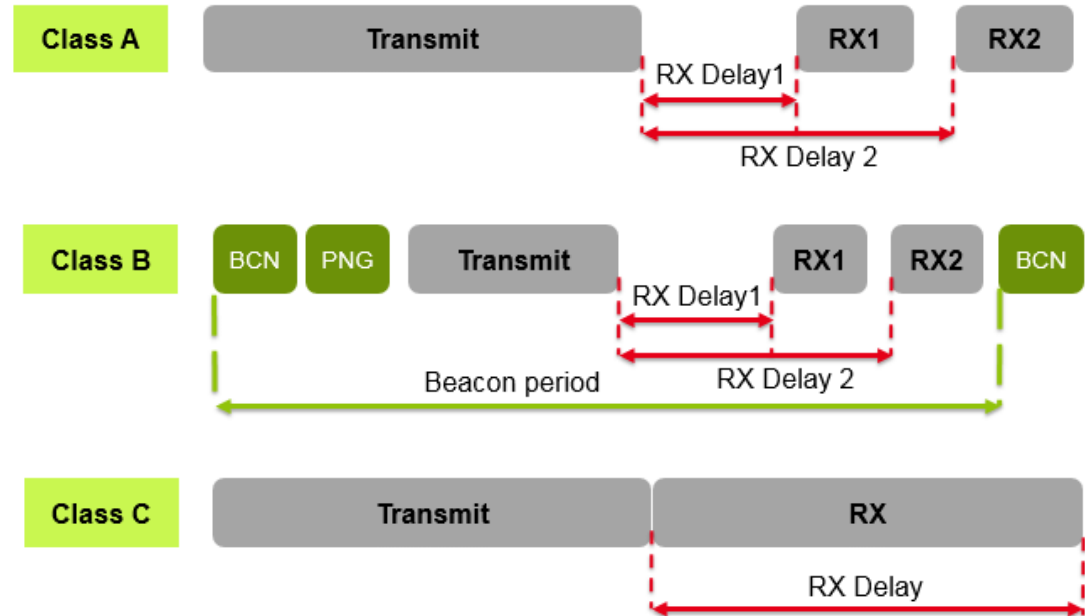
Class B:

- Class B node should get **additional receive windows** compared to Class A controlled by BCN
- gateways are **synchronized** through a **beaconing process**
- “**ping slots**”, can be used by the network infrastructure to initiate a **downlink communication**

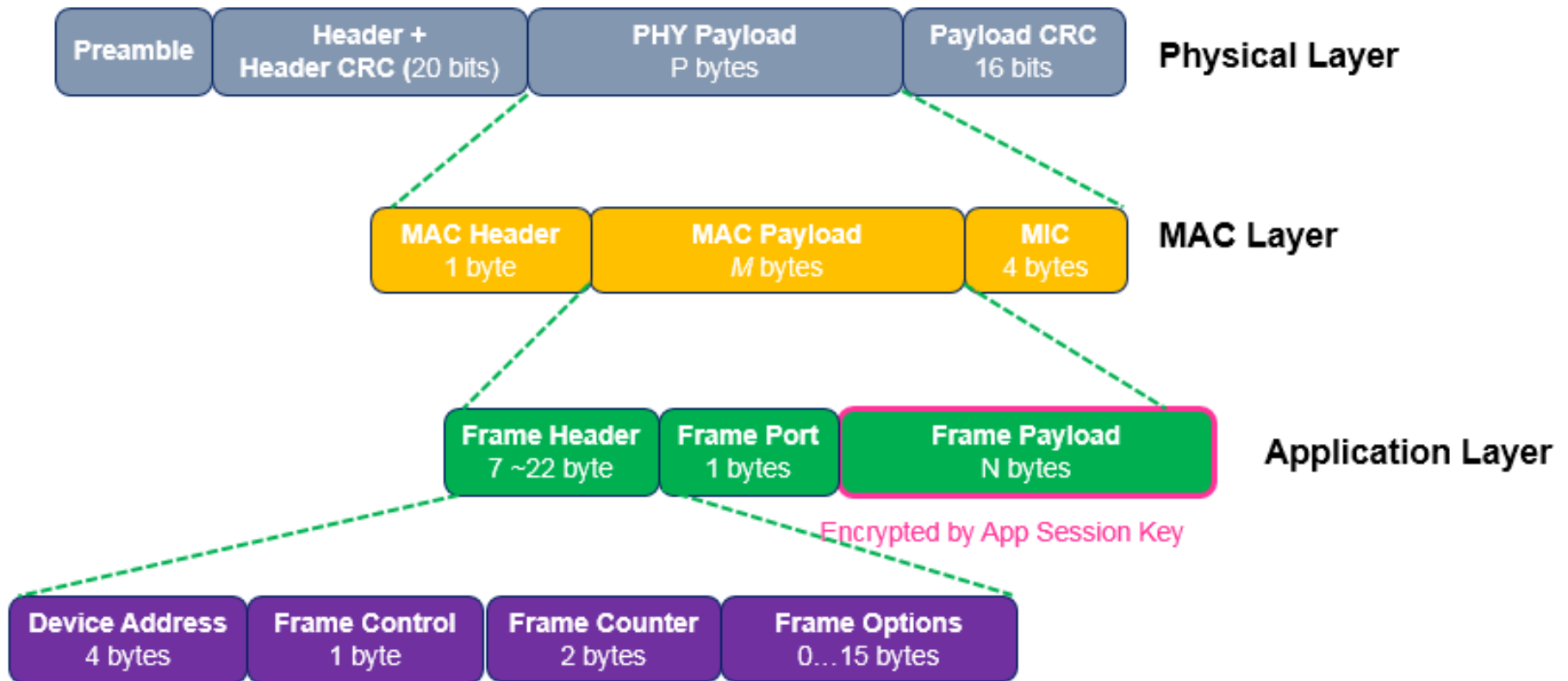
Class C:

- This class is particularly adapted **for powered nodes**
- enables a node to be **continuously listening** by keeping its receive window open when not transmitting

Uplink Transmission



LoRaWAN MAC Frame Format



Node Addressing: endpoints are also known by their **32-bit end device address**

- 7 bit for **network** + 25 bit for **devices**

LoRaWAN Address Space



- LoRaWAN uses a number of **identifiers for devices**, **applications** and **gateways**.
 - **DevAddr** - 32 bit device address (non-unique)
 - **DevEUI** - 64 bit end-device identifier, EUI-64 (unique)
 - **AppEUI** - 64 bit application identifier, EUI-64 (unique)
 - **GatewayEUI** - 64 bit gateway identifier, EUI-64 (unique)
- In LoRaWAN , **DevEUI** is assigned to the device by the chip manufacturer or the authorized owner.
- However, **all local communication is done with a dynamic DevAddr**
 - of which **7 bits** are fixed **for the Network**, leaving **25 bits** can be assigned to **individual devices**.

* EUI-64 (**Extended Unique Identifier**) has a method we can use to automatically configure IPv6 host addresses.

LoRaWAN Gateway

- LoRa **gateway** is deployed as the **centre hub** of a **star network architecture**.
- It uses **multiple transceivers** and **channels**
 - It can **demodulate multiple channels** at once
 - It can also **demodulate multiple signals** on the same channel simultaneously
- LoRa **gateways** serve as a **transparent Bridge** relaying data between endpoints
- The **endpoints** use a **single-hop** wireless connection to communicate with one or many gateways
- **Data rate** varies depending on the **frequency bands** and **adaptive data rate** (ADR)
 - **ADR** is an algorithm that **manages data rate and radio signal** for each endpoint.

Dragino
LoRa Gateway Device



Cont...

- LoRa has the ability to handle various data rates via **spreading factor (SF)**
- **Best practices:**
 - Use **adaptive data rate (ADR)** for **fixed endpoints**
 - Use **fixed data rate** or **spreading factor (SF)** for **mobile endpoints**

LoRaWAN Data Rate

Example

- Low SF → high data rate, less distance
- High SF → low data rate, longer distance

Configuration	863–870 MHz bps	902–928 MHz bps
LoRa: SF12/125 kHz	250	N/A
LoRa: SF11/125 kHz	440	N/A
LoRa: SF10/125 kHz	980	980
LoRa: SF9/125 kHz	1760	1760
LoRa: SF8/125 kHz	3125	3125
LoRa: SF7/125 kHz	5470	5470
LoRa: SF7/250 kHz	11,000	N/A
FSK: 50 kbps	50,000	N/A
LoRa: SF12/500 kHz	N/A	980
LoRa: SF11/500 kHz	N/A	1760
LoRa: SF10/500 kHz	N/A	3900
LoRa: SF9/500 kHz	N/A	7000
LoRa: SF8/500 kHz	N/A	12,500
LoRa: SF7/500 kHz	N/A	21,900

LoRaWAN Security



- LoRaWAN supports to protect communication and data privacy across the network
- LoRaWAN **endpoints** must implement two layers of security
 - **Network security** applied in MAC layer
 - **Authentication**: do **authentication** of the endpoints
 - **Confidentiality**: **encrypt** LoRaWAN packets using **AES**
 - Each endpoint implements a **network session key** (NwkSKey)
 - **Integrity**: The NwkSKey ensures **data integrity** using **message integrity code** (MIC) of every data packet
 - **Data security** applied at the end points (end device / application server)
 - second layer of security by an **application session key** (AppSKey)
 - performs encryption / decryption **between the Endpoint and its Application server**.
 - it computes and checks the **application-level MIC**
- LoRaWAN **service provider** **does not have access to the application payload** if it is not allowed

LoRaWAN Node Registration



- LoRaWAN endpoints attached to a LoRaWAN network must get **registered and authenticated**.
 - **Activation by personalization (ABP)**
 - Endpoints **don't need to run a join procedure**
 - Individual details (e.g. NwkSKey and AppSKey keys, and DevAddr) are **preconfigured** and **stored in the end device**.
 - This 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.
 - During the join process, the node **establishes its credentials** with a LoRaWAN network server, exchanging its globally unique DevEUI, AppEUI, and AppKey.
 - AppKey is then used to **derive the session keys**: NwkSKey and AppSKey.

Thanks!



Figures and slide materials are taken from the following sources:

1. David Hanes *et al.*, “IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things”, 1st Edition, 2018, Pearson India.