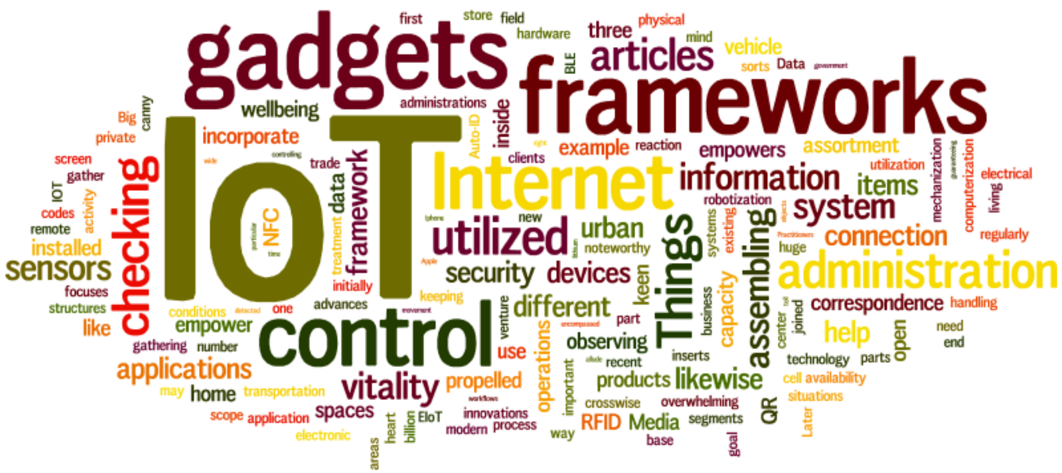
CS578: Internet of Things

Connecting Smart Objects



Dr. Manas Khatua

Assistant Professor

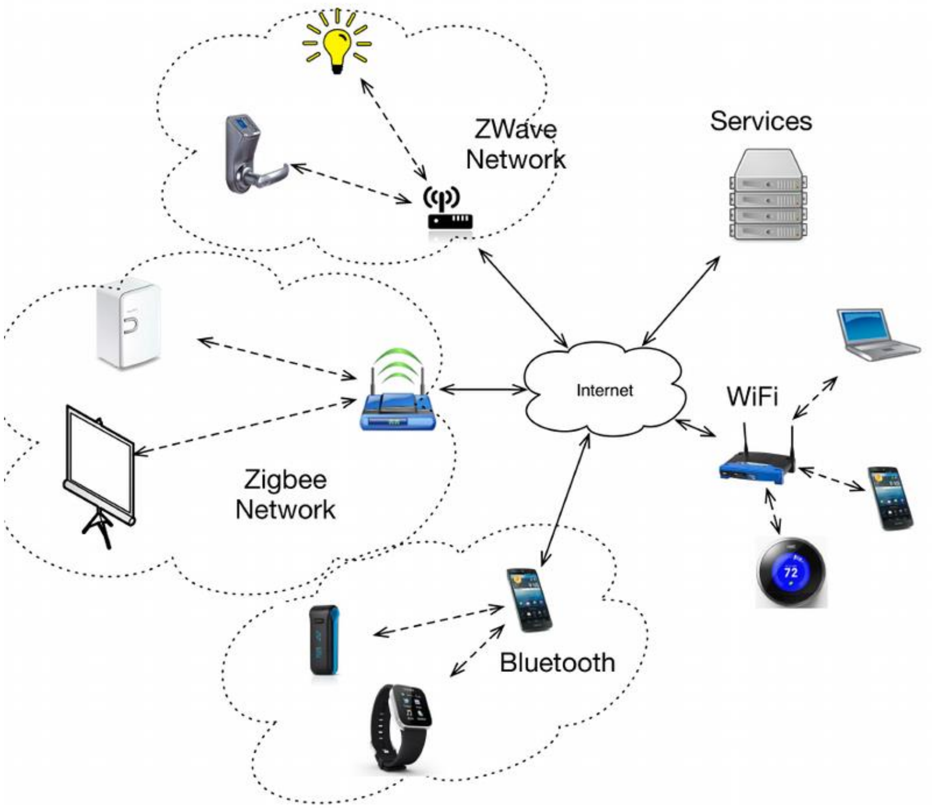
Dept. of CSE, IIT Guwahati

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**

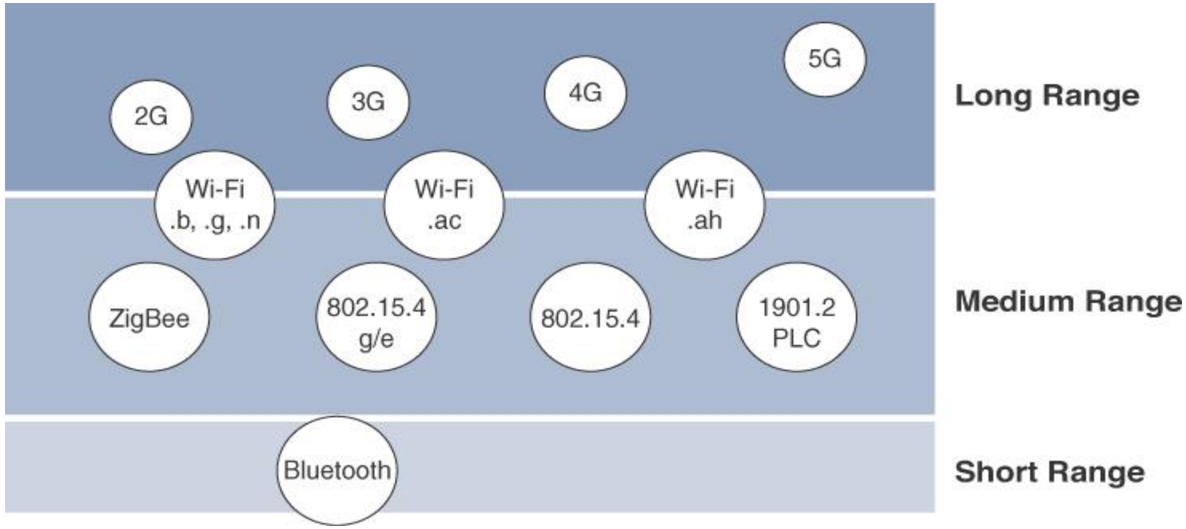
Communications Criteria

- A large number of wired and wireless access technologies are available
- Communication criteria describes the characteristics and attributes of access technologies
- Wireless communication is prevalent for smart object connectivity
  - eases deployment
  - allows smart objects to be mobile without losing connectivity



- Few basic criteria:
  - Range
  - Frequency bands
  - Power consumptions
  - Topology
  - Constrained devices
  - Constrained-node networks

Communication Range

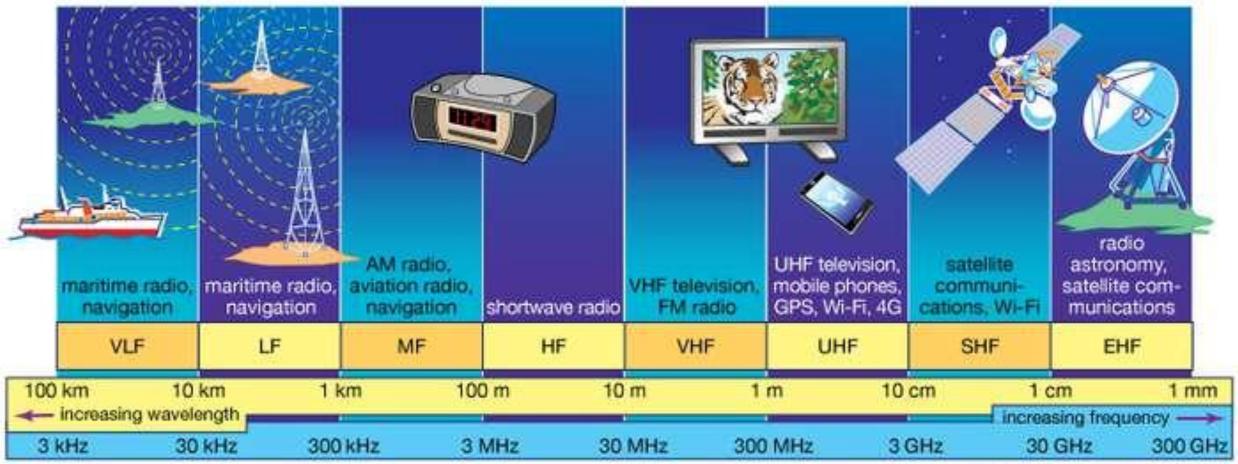


- **Short range**:
  - tens of meters of maximum distance between two devices
  - often considered as an alternative to serial cable
  - IEEE 802.15.1 Bluetooth, IEEE 802.15.7 Visible Light Communications (VLC)

- **Medium range**
  - tens to hundreds of meters between two devices
  - **Wireless** : IEEE 802.11 WiFi, IEEE 802.15.4 Low Rate WPAN, IEEE 802.15.4g Smart Utility Networks (SUN)
  - **Wired** : IEEE 802.3 Ethernet, IEEE 1901.2 Narrowband Power Line Communications (PLC)

- **Long range**
  - greater than 1 mile (1.6 km) between two devices
  - **Wireless** : 2G, 3G, 4G, Outdoor Wi-Fi (IEEE 802.11ah), Low-Power Wide-Area (LPWA) communications
  - **Wired** : IEEE 802.3 ethernet over optical fiber, IEEE 1901.2 Broadband PLC

Frequency Bands



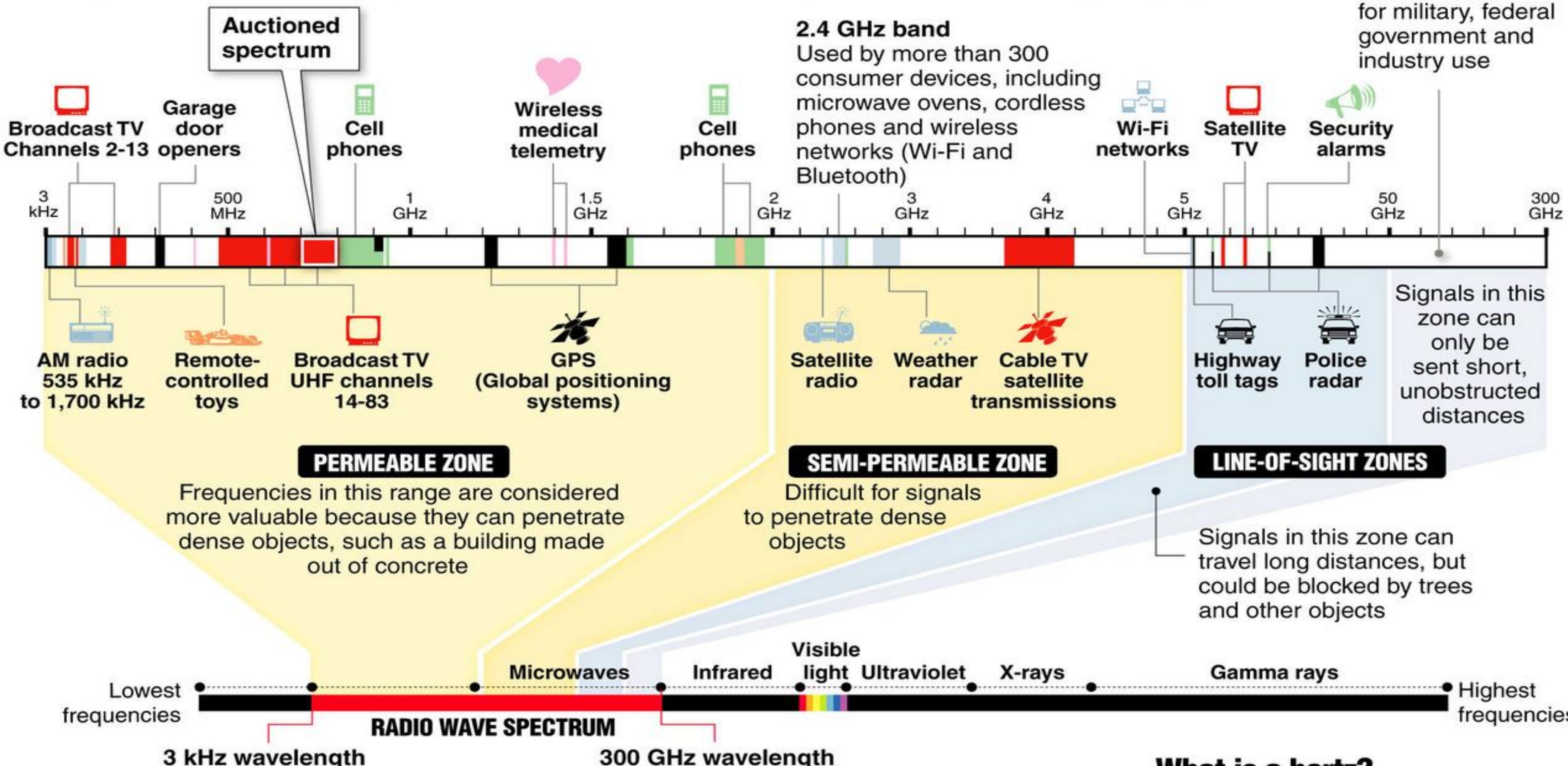
- Radio spectrum is regulated by countries and/or organizations (e.g. International Telecommunication Union (ITU), Federal Communications Commission (FCC))
- frequency bands leveraged by wireless communications are split between licensed and unlicensed bands.

- **Licensed**
  - applicable to long-range access technologies
  - users must subscribe to services
  - common licensed spectrum for IoT : Cellular (900-2100 MHz), NB-IoT (700-900 MHz), WiMax

- **Unlicensed**
  - industrial, scientific, and medical (ISM) portions of the radio bands
  - *Unlicensed* means that no guarantees or interference protections are offered
  - well-known ISM bands for IoT : 2.4 GHz, 5 GHz, 915 MHz for WiFi, BLE, ZigBee; 868 MHz for LoRa

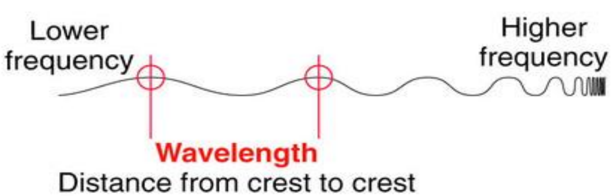
Inside the radio wave spectrum

Almost every wireless technology – from cell phones to garage door openers – uses radio waves to communicate. Some services, such as TV and radio broadcasts, have exclusive use of their frequency within a geographic area. But many devices share frequencies, which can cause interference. Examples of radio waves used by everyday devices:



The electromagnetic spectrum

Radio waves occupy part of the electromagnetic spectrum, a range of electric and magnetic waves of different lengths that travel at the speed of light; other parts of the spectrum include visible light and x-rays; the shortest wavelengths have the highest frequency, measured in hertz



What is a hertz?

One hertz is one cycle per second. For radio waves, a cycle is the distance from wave crest to crest

1 kilohertz (kHz) = 1,000 hertz

1 megahertz (MHz) = 1 million hertz

1 gigahertz (GHz) = 1 billion hertz

Source: New America Foundation, MCT, Howstuffworks.com
Graphic: Nathaniel Levine, Sacramento Bee

ISM Bands in India

ISM Bands - Industrial, Scientific and Medical

900MHz
vs.
2.4GHz
vs.
5GHz

900MHz

Advantages:

- More robust, less prone to interference
- Lower attenuation, travels further through more obstacles

Disadvantages:

- Low bandwidth prevents large data transfer, speed
- Components are larger at lower frequencies

2.4GHz

Advantages:

- Higher bandwidth allows large data transfer, speed
- Components are smaller, cheaper

Disadvantages:

- Congested band due to abundance of Wi-Fi, Bluetooth, microwaves, cordless phones
- Attenuates much more quickly, will not pass through metal

5GHz

Advantages:

- Higher bandwidth allows large data transfer, speed
- Less congested, few RF devices in this band

Disadvantages:

- Low transmit power limitations
- High attenuation in cables, requires very high gain antennas

- India also allow 865-867 MHz ISM band

Power Consumption

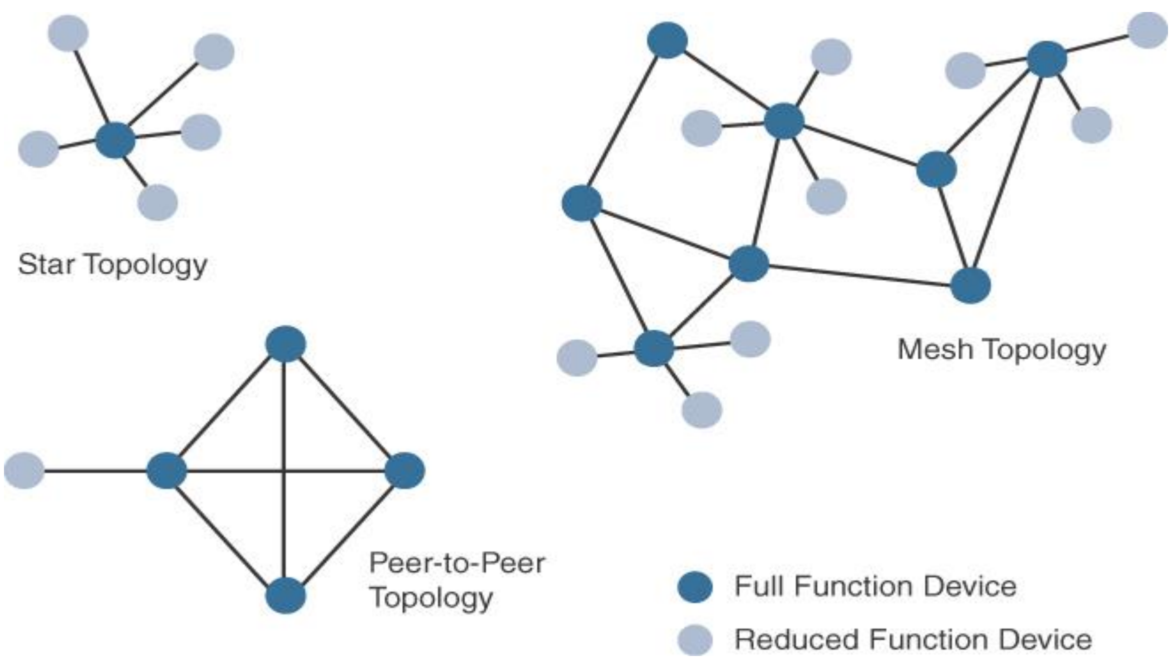
- Powered node
  - node has a direct connection to a power source
  - communications are usually not limited by power consumption criteria
  - ease of deployment is limited by the availability of a power source
  - makes mobility more complex
- Battery-powered nodes
  - bring more flexibility to IoT devices
  - batteries are small
  - batteries can be changed or recharged
  - IoT wireless access technologies must address
    - the needs of low power consumption
    - connectivity for battery-powered nodes

	Bluetooth	ZigBee	WiFi	LoRaWAN	NB-IoT
Standard	IEEE 802.15.1	IEEE 802.15.4	IEEE 802.11b	LoRaWAN	3GPP NB-IoT
Sleeping	9 µA	12 µA	30 µA	0.1 µA	3 µA
Awake/Idle	35 mA	50 mA	245 mA	1.4 mA	6 mA
Transmitting	39 mA	52 mA	251 mA	44 mA	220 mA
Receiving	37 mA	54 mA	248 mA	12 mA	46 mA
Power Supply	3.3 V	3.3 V	5 V*	3.3 V	3.6 V

* The ESP8266 module powered by 3.3 V could be used as WiFi module.

Topology

- **Three main topology** schemes are dominant:
  - star, mesh, and peer-to-peer
- For long-range and short-range technologies:
  - star topology is prevalent
- For medium-range technologies:
  - star, peer-to-peer, or mesh topology is common



- IEEE 802.15.4, 802.15.4g, and wired IEEE 1901.2a PLC are generally deployed as a mesh topology.
- Indoor Wi-Fi deployments are mostly star topologies

FFD: A node that implements the full network functions

RFD: The device can implement a subset of protocol functions to perform just a specialized part (communication with the coordinator).

Constrained Devices

- Constrained nodes have limited resources that impact their networking feature set and capabilities.
- RFC 7228 defines three classes for constrained nodes: Class 0, 1, 2

	RAM	Flash Storage	IP stack	Security Scheme	Example
Class 0	< 10 KB	< 100 KB	Not present	No	Push button
Class 1	> 10 KB	> 100 KB	Optimized IP stack	Light	Sensors
Class 2	> 50 KB	> 250 KB	Full IP stack	Yes	Smart meter

Constrained-Node Networks

- Constrained-node networks are often referred to as low-power and lossy networks (LLNs)

- Layer 1 and Layer 2 protocols must be evaluated in using the following characteristics:
  - data rate and throughput
  - latency and determinism
  - overhead and payload.

- Data rate & throughput:
  - data rates available from 100 bps to tens of megabits per second
  - actual throughput is less, sometimes much less, than the data rate
- Latency & determinism:
  - When latency is a strong concern, emergent access technologies such as Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e should be considered.
- Overhead & Payload
  - The minimum IPv6 MTU size is expected to be 1280 bytes.
  - the payload size for IEEE 802.15.4 is 127 bytes; payload in LoRaWAN may be from 19 to 250 bytes
  - So, the fragmentation of the IPv6 payload has to be taken into account by the link layer

IoT Access Technologies

- there are many IoT technologies in the market today

Sub-1GHz
LoRaWAN™
ZigBee®
WirelessHART
6LoWPAN
NB-IoT
HaLow 802.11ah
Bluetooth®
sigfox
NFC
Wi Fi
nwave
THREAD
Z WAVE®

IEEE 802.15.4 PHY and MAC

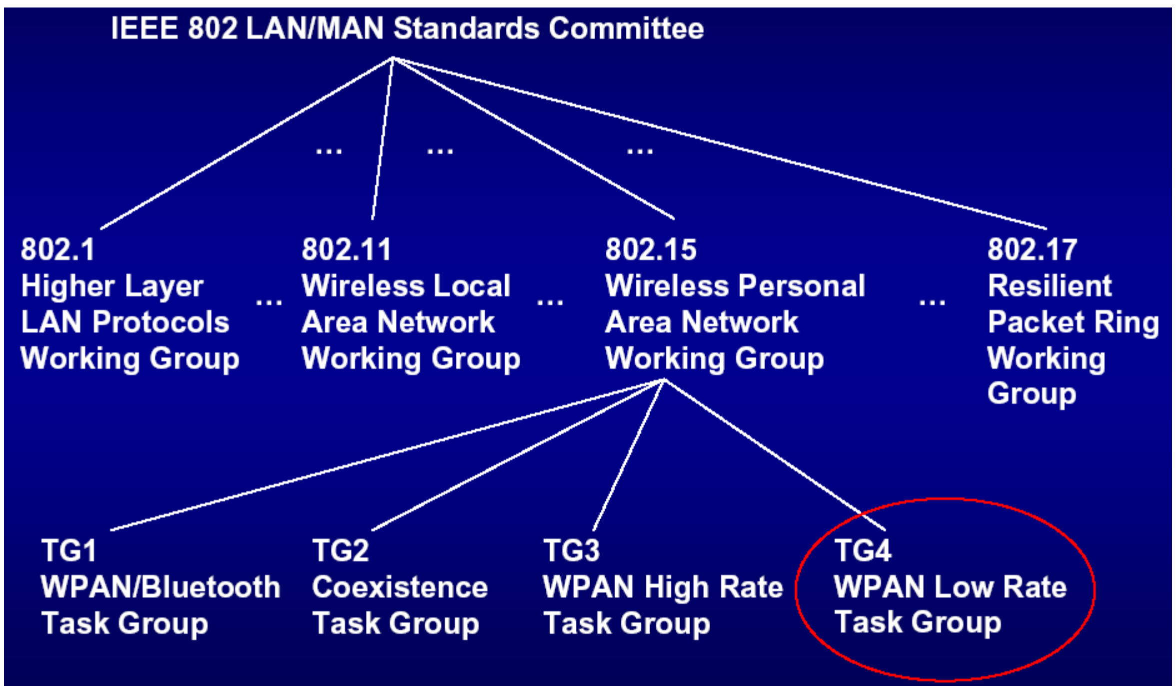
IEEE 802.15.4 is the IEEE standards for Low Rate Wireless Networks (or Low Rare Wireless Personal Area Networks). Latest version **published in 2015**.

For more details:
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7460875

IEEE 802.15 Task Group 4

- TG4 was formed to define low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN)

- standard has evolved over time:
  - IEEE 802.15.4-2003 ; IEEE 802.15.4-2006
  - IEEE 802.15.4-2011; IEEE 802.15.4-2015



- PAN
  - span a small area (e.g., a private home or an individual workspace)
  - communicate over a short distance
  - low-powered communication
  - primarily uses ad-hoc networking
  - could be wireless or wired (e.g. using USB)

IEEE 802.15.4

- IEEE 802.15.4 is a **wireless access technology** for
  - ✓ low-cost and low-data-rate devices
  - ✓ devices powered by batteries

- It enables easy installation using a compact protocol stack

- Several network communication stacks leverage this technology for many IoT use cases in both the consumer and business markets.

- Few applications:
  - ❖ Home and building automation
  - ❖ Automotive networks
  - ❖ Industrial wireless sensor networks
  - ❖ Interactive toys and remote controls

Cont…

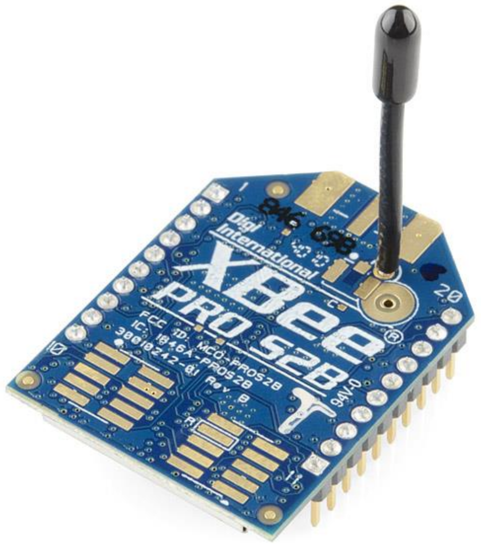
- Few well-known protocol stacks which leverage the IEEE 802.15.4:
  - **ZigBee**
  - **ZigBee IP**
  - **6LoWPAN**
  - WirelessHART
  - Thread
  - ISA100.11a

- **ZigBee** shows how 802.15.4 can be leveraged at the PHY and MAC layers, independent of the protocol layers above.

- Criticisms:
  - MAC reliability
  - unbounded latency
  - susceptibility to interference and multipath fading
  - lacks a frequency-hopping technique

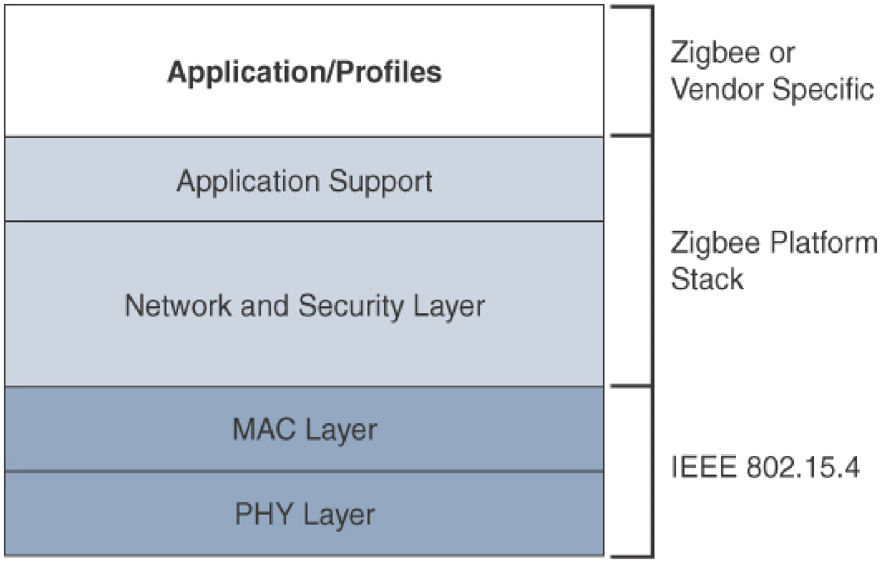
ZigBee

- ZigBee specification was ratified in 2004
- **ZigBee Alliance** is an industry group
  - ✓ certify interoperability between vendors
  - ✓ evolving ZigBee as an IoT solution
- ZigBee solutions are aimed at smart objects and sensors that have low bandwidth and low power needs.
- Well-known application domains:



Industrial and Commercial Automation	Smart Home Applications	Smart Energy
measuring temperature and humidity, and tracking assets	control lighting, thermostats, and security functions	smart meters, that can monitor and control the use and delivery of utilities, such as electricity and water

ZigBee Protocol Stack



- ZigBee predefines many application profiles for certain industries.
- Vendors can optionally create their own custom ones.

- The application support layer interfaces the lower portion of the stack, dealing with the networking of ZigBee devices, with the higher-layer applications

- ZigBee network & security layer provides mechanisms for network startup, configuration, routing, and securing communications.

- ZigBee utilizes the IEEE 802.15.4 standard at the PHY and MAC layers

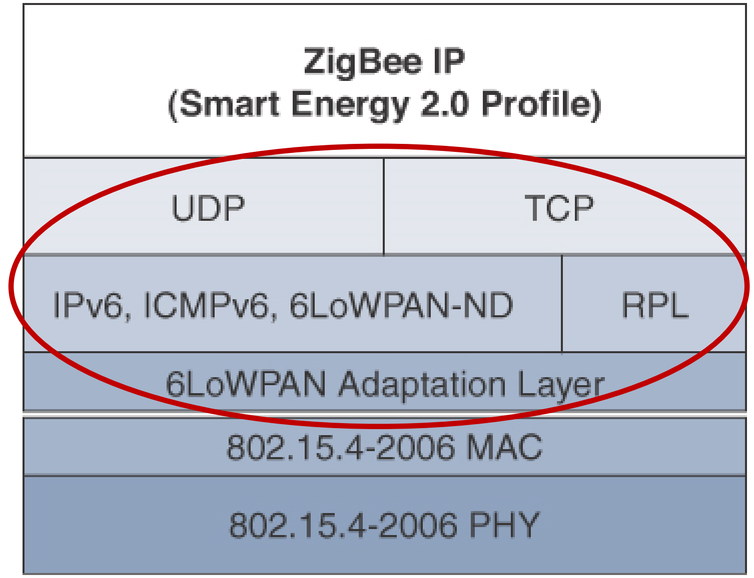
- ZigBee uses AODV routing across a mesh network

- ZigBee utilizes 128-bit AES encryption for security at the MAC layer

- It also provides security at the network and application layers.

ZigBee IP

- ZigBee has not provided interoperability with other IoT solutions or open standards
- ZigBee IP was created to embrace the open standards at the network and transport layers
- Open standards designed by IETF's work on LLNs, such as IPv6, 6LoWPAN, and RPL.
- ZigBee IP requires the support of 6LoWPAN's fragmentation and header compression schemes.
- ZigBee IP nodes support
  - IPv6,
  - ICMPv6,
  - 6LoWPAN,
  - Neighbour Discovery (ND), and
  - RPL for the routing of packets.

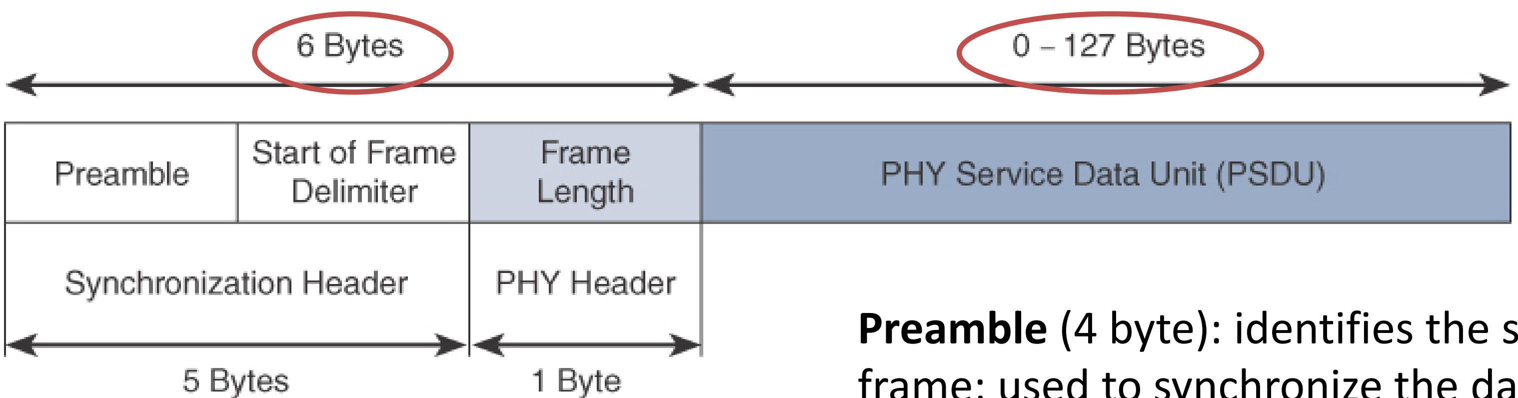


- ZigBee IP is a compelling protocol stack offering because it is based on current IoT standards at every layer under the application layer.

IEEE 802.15.4 PHY layer

- Physical layer transmission options in IEEE 802.15.4-2015
  - **2.4 GHz**, 16 channels, with a data rate of 250 kbps
  - **915 MHz**, 10 channels, with a data rate of 250 kbps
  - **868 MHz**, 3 channel, with a data rate of 100 kbps

- Modulation schemes
  - **OQPSK PHY :** Direct sequence spread spectrum (DSSS) PHY employing offset quadrature phase-shift keying (OQPSK)
  - **BPSK PHY :** DSSS PHY employing binary phase-shift keying (BPSK)
  - **ASK PHY :** parallel sequence spread spectrum (PSSS) PHY employing amplitude shift keying (ASK) and BPSK



IEEE 802.15.4 PHY Frame Format

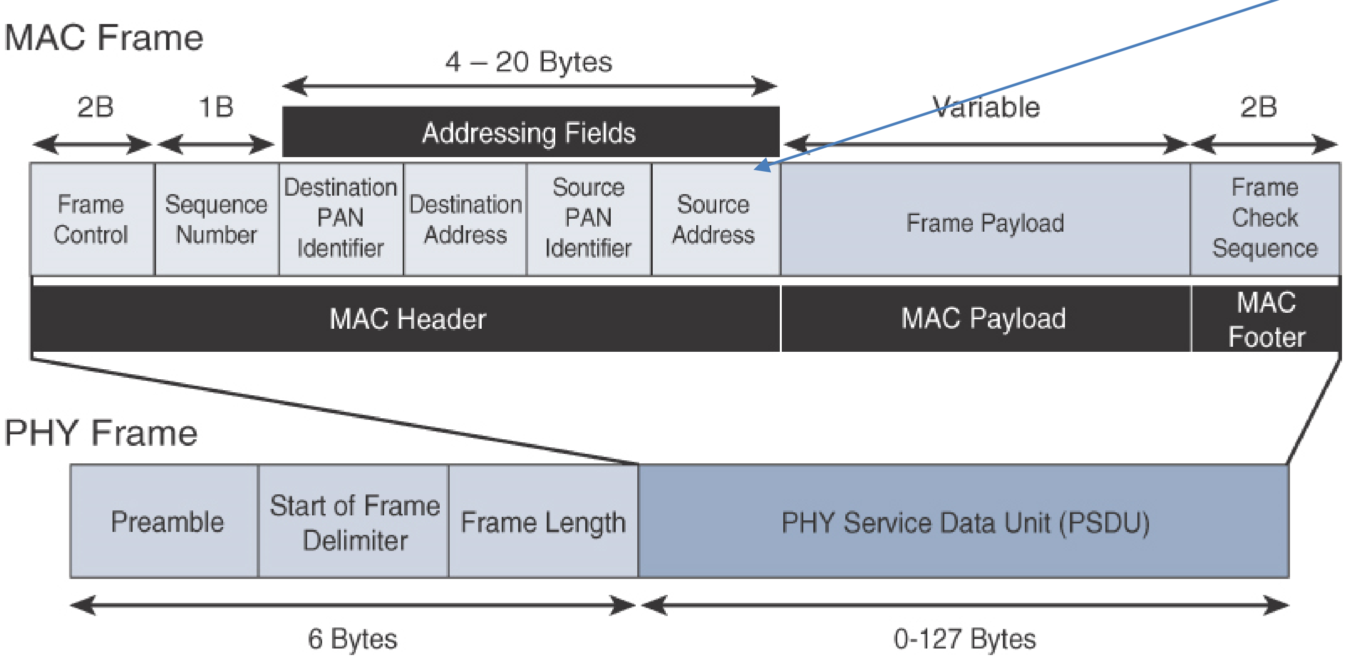
Preamble (4 byte): identifies the start of the frame; used to synchronize the data transmission

SFD (1 byte): informs the receiver about the starting point of frame content

IEEE 802.15.4 MAC layer

- MAC layer manages access to the PHY channel
  - defines how devices in the same area will share the frequencies allocated.
- Main tasks:
  - Network beaconing for devices acting as coordinators
  - PAN association and disassociation by a device
  - Reliable link communications between two peer MAC entities
  - Device security

16-bit short address
OR
64-bit extended address



- MAC frame types:
  - Data frame
  - Beacon frame
  - ACK frame
  - Command frame

Cont…

802.15.4 MAC header						MAC payload
Octets:2	1	0/2	0/2/8	0/2	0/2/8	variable
Frame Control	Sequence number	Destination PAN ID	Destination address	Source PAN ID	Source address	Frame payload

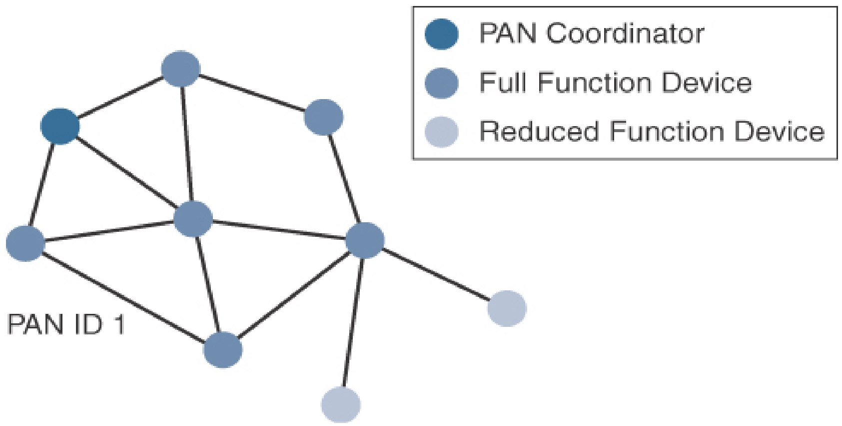
Bits: 3	1	1	1	1	3	2	2	2
Frame Type	Security enabled	Frame pending	ACK required	Pan ID Compress	**Reserved**	Dest addr mode	Frame Version	Src addr mode

-Values of the Frame Type subfield

Frame type value $b_2\ b_1\ b_0$	Description
000	Beacon
001	Data
010	Acknowledgment
011	MAC command
100–111	Reserved

Addressing mode value $b_1\ b_0$	Description
00	PAN identifier and address field are not present.
01	Reserved.
10	Address field contains a 16 bit short address.
11	Address field contains a 64 bit extended address.

Topology

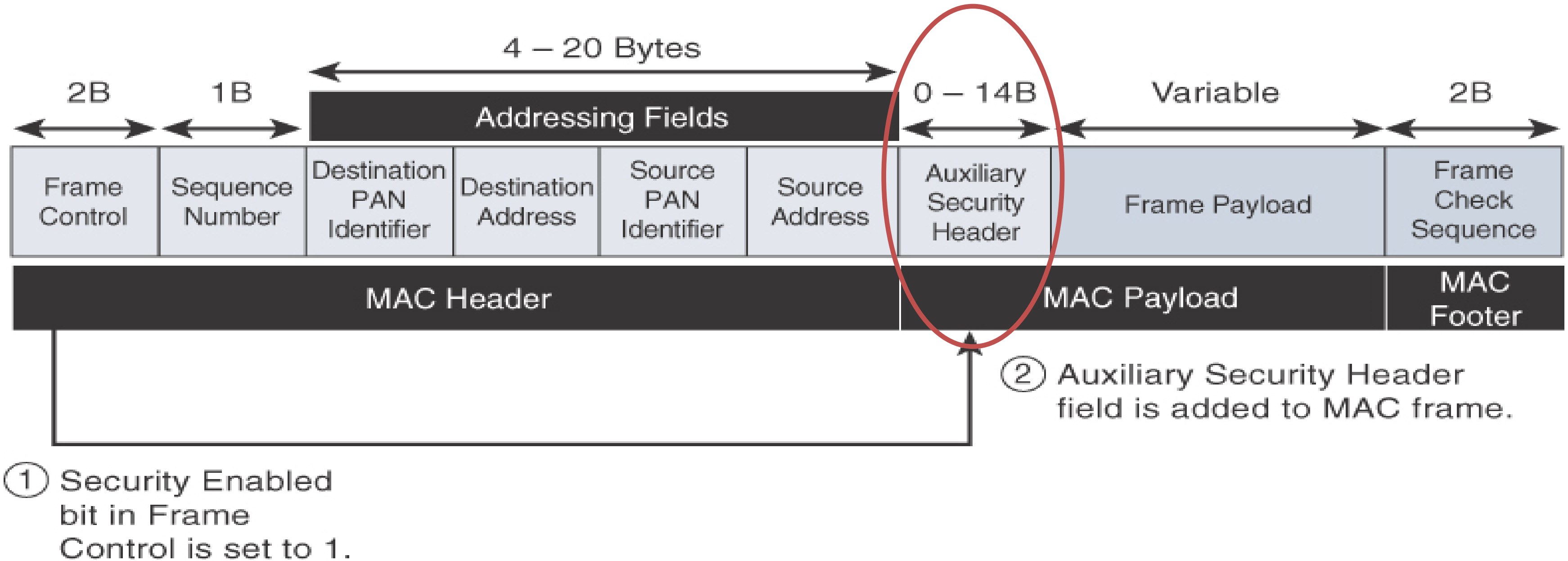


802.15.4 Sample Mesh Network Topology

- Topology for 802.15.4:
  - Star
  - Peer-to-Peer
  - Mesh

- IEEE 802.15.4 does not define a path selection for a mesh topology
  - ➢ Mesh-under: Path selection can be done at Layer 2
  - ➢ Mesh-over: Path selection can occur at Layer 3 in routing protocol

Security



- IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm
- Message integrity code (MIC), which is calculated for the entire frame using the same AES key, to validate the data that is sent

IEEE 802.15.4g
IEEE 802.15.4e

IEEE 802.15.4g & **IEEE 802.15.4e** are the PHY and MAC layer amendments of wireless personal area networks (IEEE 802.1.5.4) **published in 2012**.

For more details:
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6185525
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6471722

IEEE 802.15.4e & 802.15.4g

- **Disadvantages of IEEE 802.1.5.4**
  - MAC reliability
  - unbounded latency
  - multipath fading

- **IEEE 802.15.4e** amendment of 802.15.4-2011 expands the MAC layer feature set

  - to remedy the disadvantages of 802.15.4.
  - to better suitable in factory and process automation, and smart grid

  - Main modifications were:
    - frame format,
    - security,
    - determinism mechanism, and
    - frequency hopping

- **IEEE 802.15.4g** amendment of 802.15.4-2011 expands the PHY layer feature set

  - to optimize large outdoor wireless mesh networks for field area networks (FANs)
  - to better suitable in smart grid or smart utility network (SUN) communication

  - Main modifications were:
    - New PHY definitions
    - some MAC modifications were needed to support the new PHY

Wi-SUN PHY layer

- 802.15.4g-2012 and 802.15.4e-2012 led to **additional difficulty** in
  - achieving the **interoperability** between devices and mixed vendors
- Wi-SUN Alliance was formed to guarantee interoperability
- IEEE 802.15.4 maximum payload size of 127 bytes → 2047 bytes for SUN PHY.
  - Fragmentation is no longer necessary at Layer 2 for IPv6 packets
- Error protection was improved in IEEE 802.15.4g by the CRC from 16 to 32 bits.
- SUN PHY supports **multiple data rates** and **more channels** in ISM bands
- Modulation schemes:
  - **MR-FSK** : Multi-Rate and Multi-Regional Frequency Shift Keying
    - good transmit frequency
  - **MR-OFDM** : Multi-Rate and Multi-Regional Orthogonal Frequency Division Multiplexing
    - good data rate
  - **MR-O-QPSK :** Multi-Rate and Multi-Regional Offset Quadrature Phase-Shift Keying
    - cost effective design

802.15.4e MAC layer

- IEEE 802.15.4e amendment modifies: frame format, security, determinism mechanism, frequency hopping

- Physical layer for implementation could be Wi-SUN PHY

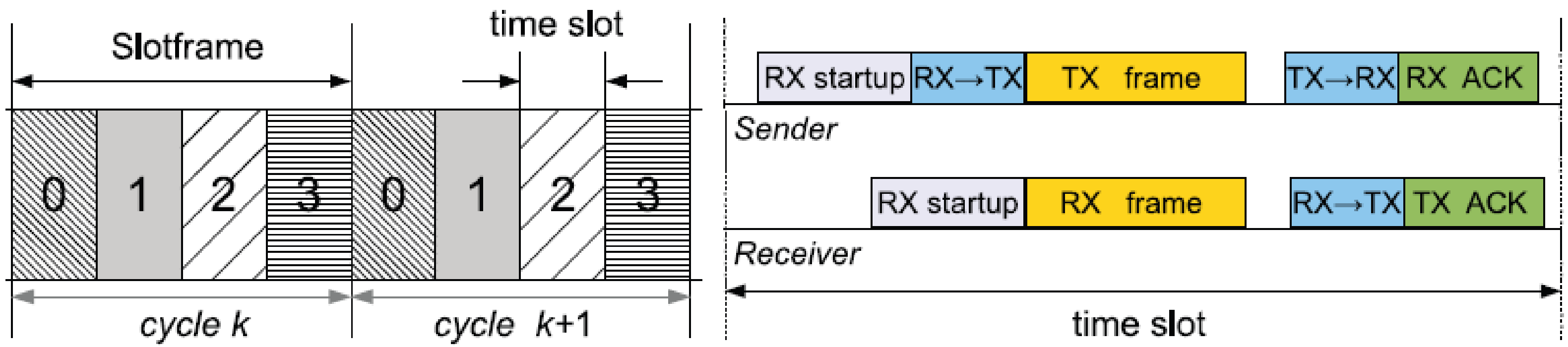
- **TSCH: Time Slotted Channel Hopping**
  - One type of MAC operation mode

  - guaranteed media access by time slotted access
    - time is divided in fixed time period – “time slots”
    - in a time slot, one packet and its ACK can be transmitted
    - multiple slots together form a “slot frame” which is repeated regularly
    - offers guaranteed bandwidth
    - offers predictable latency

  - provide channel diversity by channel / frequency hopping
    - reduce interference
    - increase robustness in noisy environment
    - increase network capacity by parallel communication via multiple cell

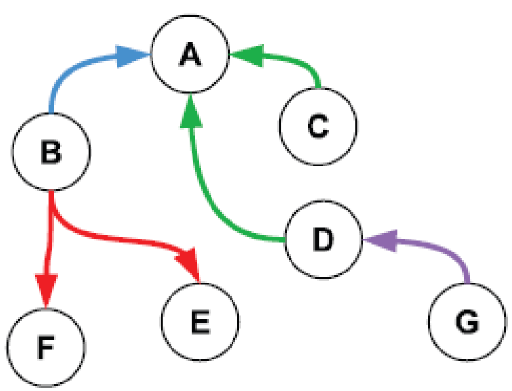
  - Transmitter and receiver maintain time & channel synchronization
    - by a global timeslot counter and a global channel hopping sequence list

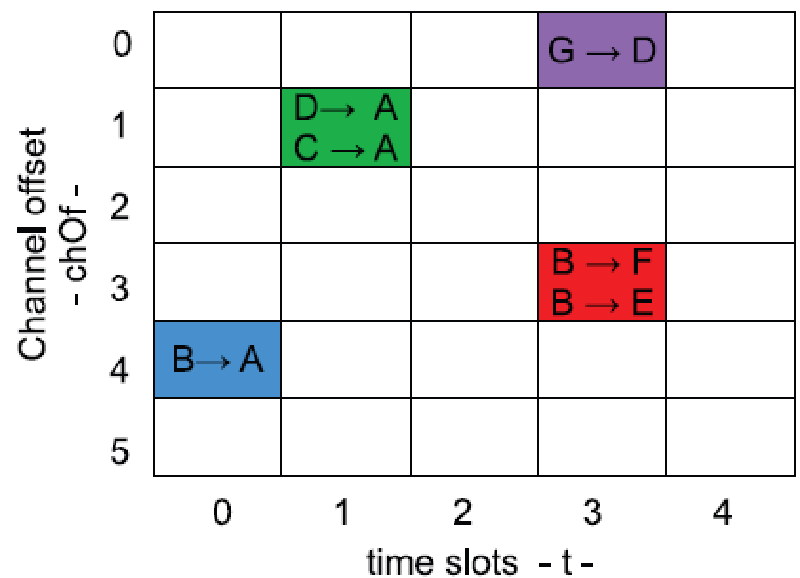
Cont…



(a) slotframe

(b) data frame and ACK transmission within a timeslot





Source: Palattella *et al.*, “Standardized Protocol Stack for the Internet of (Important) Things”, *IEEE Comm. Surv. & Tutor*, vol. 15, no. 3, 2013, pp. 1389–1406.

Cont…

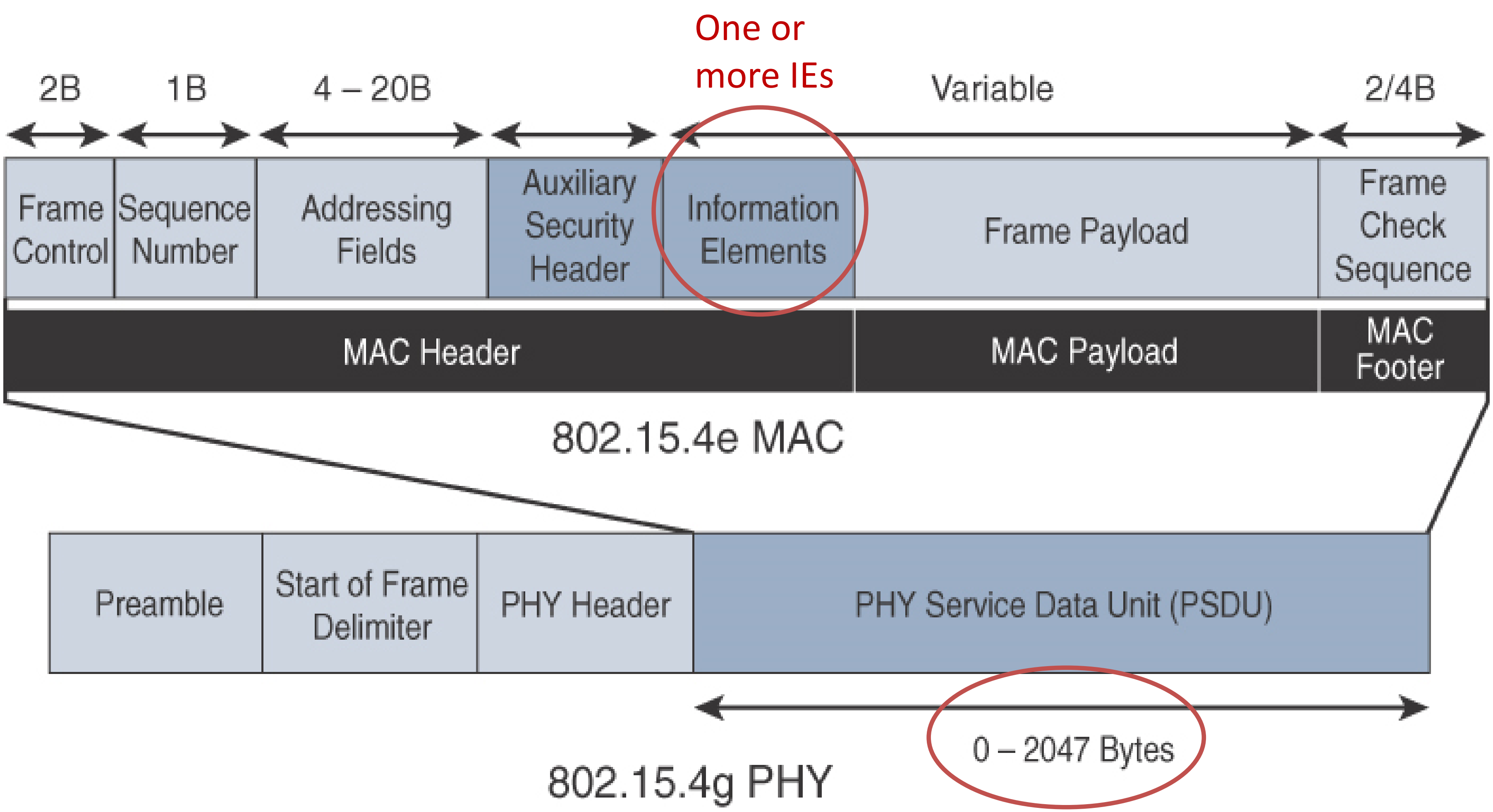
- **IE: Information Element**
  - allow for the exchange of information at the MAC layer
  - either as header IEs (standardized) and/or payload IEs (private)
  - carry additional metadata to support MAC layer services
    - IEEE 802.15.9 key management
    - Wi-SUN 1.0 IEs to broadcast and unicast schedule timing information,
    - frequency hopping synchronization information for the 6TiSCH architecture

- **EB: Enhanced Beacon**
  - allow the construction of application-specific beacon content
  - includes relevant IEs in EB frames
    - network metrics, frequency hopping broadcast schedule, and PAN information

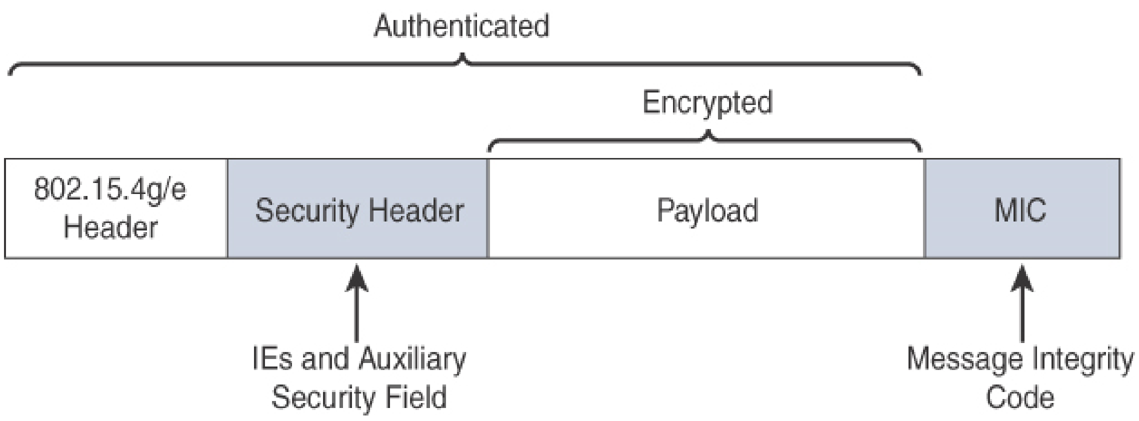
- **EBR: Enhanced Beacon Request**
  - allow the sender to selectively specify the request of information
  - EBRs leverages IEs to specify

- **Enhanced ACK**
  - allow for the integration of a frame counter for the frame being acknowledged
  - helps to protect against certain attacks

802.15.4e/g Frame Format

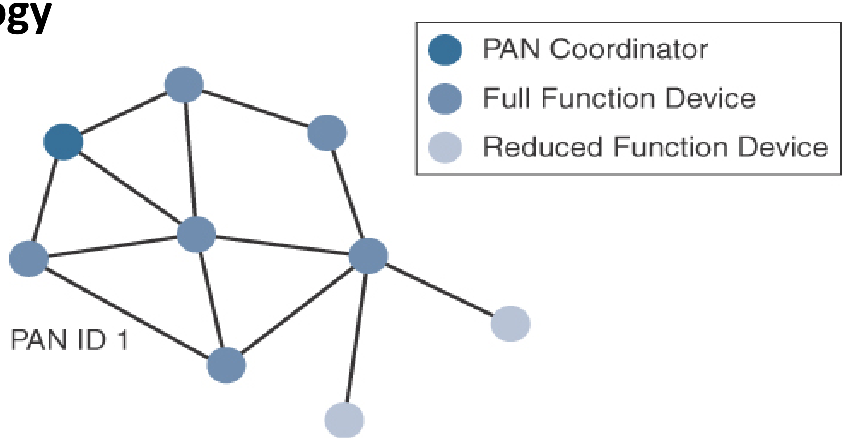


Security and Topology



- Encryption is done by AES with a 128-bit key
- Message integrity code (MIC) validates the data that is sent

Mesh Topology



- Battery-powered nodes with a long lifecycle requires
  - optimized Layer 2 forwarding or
  - optimized Layer 3 routing protocol

IEEE 802.11ah

IEEE 802.11ah is a wireless networking protocol **published in 2016**.

For more details: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7920364

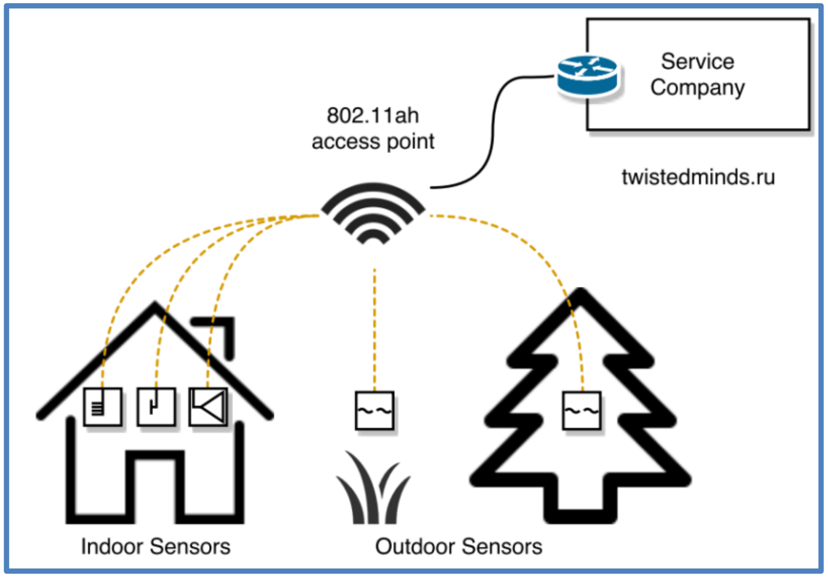
IEEE 802.11ah

- **Advantages** of WiFi
  - Most successful endpoint wireless technology
  - Useful for high data rate devices, for audio-video analytics devices, for deploying WiFi backhaul infrastructure

- **Disadvantages** of WiFi
  - Less signal penetration
  - Unsuitable for battery powered nodes
  - Unable to support large number of devices

- Wi-Fi Alliance defined a new technology called Wi-Fi HaLow
  - ❖ ah → **Ha**
  - ❖ Low power network → **Low**

- Main use cases for IEEE 802.11ah
  - ➢ Sensors and meters covering a smart grid
  - ➢ Backhaul aggregation of industrial sensors and meter data
  - ➢ Extended range Wi-Fi



802.11ah PHY layer

- Operating in unlicensed sub-GHz bands
  - 868–868.6 MHz for EMEAR (Europe, Middle East, Africa, and Russia)
  - 902–928 MHz for North America and Asia Pacific (India, Japan, Korea, …)
  - 314–316 MHz, 430–434 MHz, 470–510 MHz, 779–787 MHz for China

- OFDM Modulation

- Channels of 2, 4, 8, or 16 MHz (and also 1 MHz for low-bandwidth transmission)

- Provides one-tenth of the data rates of IEEE 802.11ac

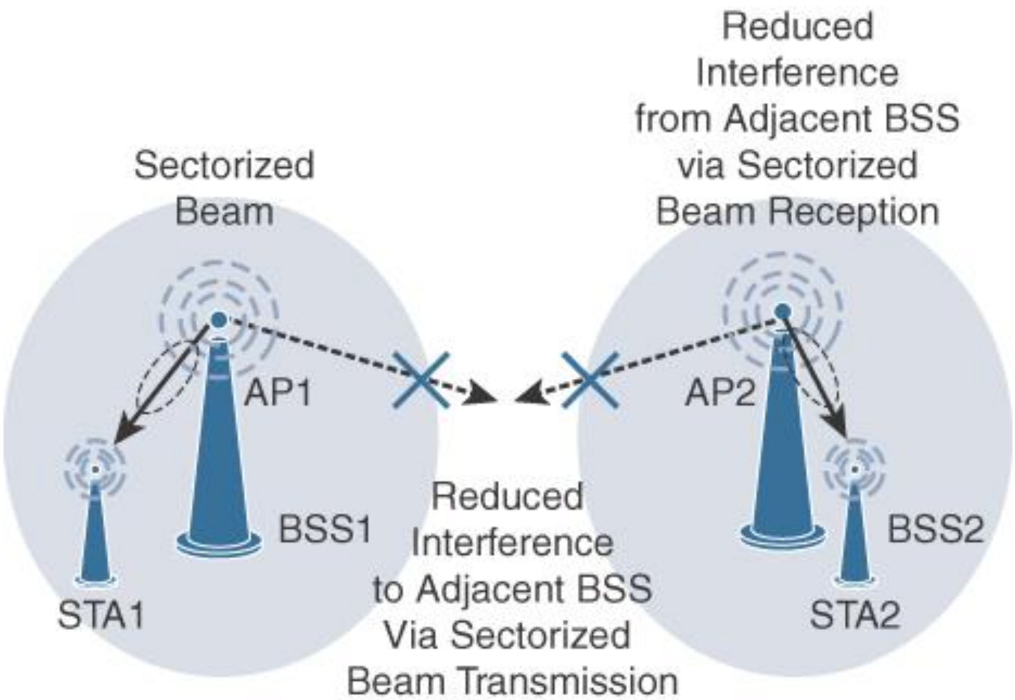
- Provide an extended range for its lower speed data
  - For data rate of 100 kbps, the outdoor transmission range approx 1 Km

802.11ah MAC layer

Enhancements and features

- Number of devices: Has been scaled up from 250 to 8192 per access point (AP).
- MAC header: Has been shortened
- Null data packet (NDP) support: to cover control and management frames.
  - It is only transmitted by a STA; It carry's no data payload.
- Restricted access window (RAW): increase throughput and energy efficiency by
  - dividing stations into different RAW groups.
  - Only the stations in the same group can access the channel simultaneously.
- Sectorization: partition the coverage area of a Basic Service Set (BSS) into sectors, each containing a subset of stations. it uses an antenna array and beam-forming technique.
  - reduces contention by restricting which group, in which sector, and at which time window.
  - to mitigate the hidden node problem; to eliminate the overlapping BSS problem.
- Target wake time (TWT): AP can define times when a STA can access the network
- Speed frame exchange: Enables an AP and endpoint to exchange frames during a reserved transmit opportunity (TXOP)
  - TXOP is the amount of time a station can send frames when it has won contention for the medium

802.11ah Topology



- Star topology
- Includes simple hops relay to extend its range
  - Max 2 hops
  - Client handle the relay operation

LoRaWAN

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

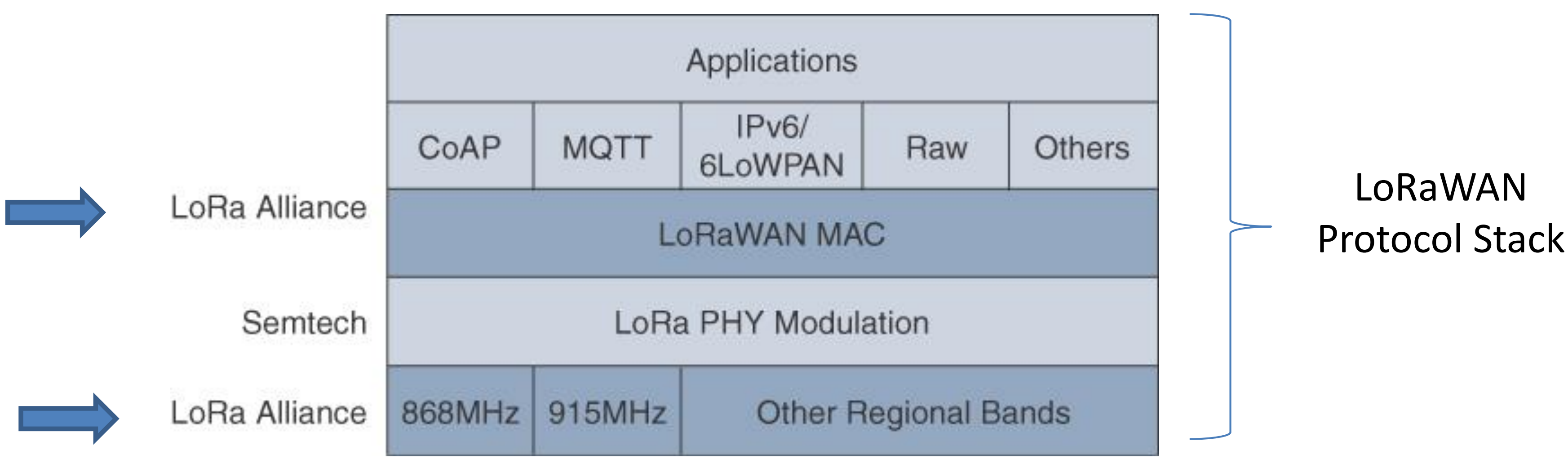
For more details: https://lora-alliance.org/sites/default/files/2018-07/lorawan1.0.3.pdf

LPWA Technology

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

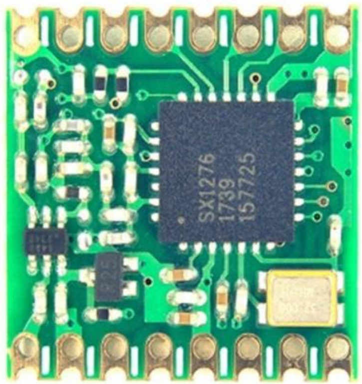
LoRa Alliance

- Initially, **LoRa** was a PHY layer modulation scheme
  - developed by a French company “Cycleo”; Later, Cycleo was acquired by Semtech.
- **Semtech LoRa**: Layer 1 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

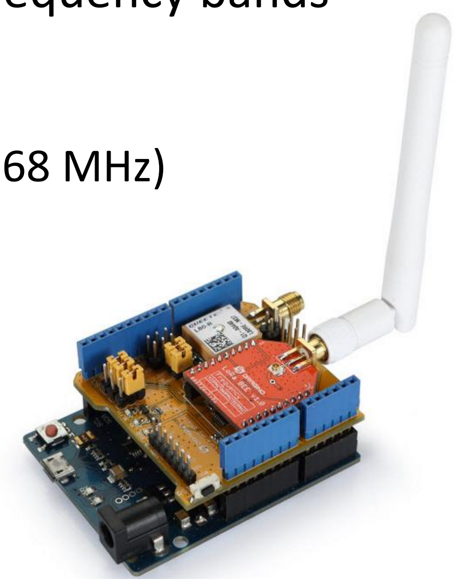


LoRaWAN PHY layer

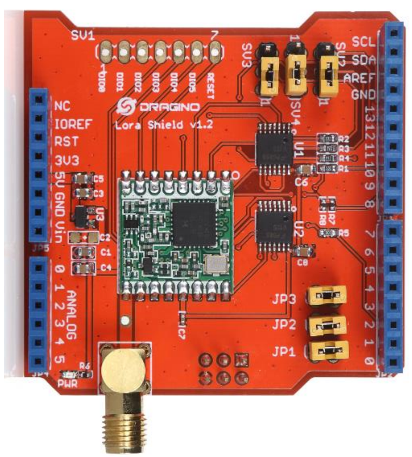
- Semtech LoRa PHY
- Uses **chirp spread spectrum** modulation
  - ➢ it allows demodulation below the noise floor, offers robustness to noise and interference
  - ➢ manages a single channel occupation by different spreading factors (SFs)
- Main unlicensed sub-GHz frequency bands
  - 433 MHz
  - 779–787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



LoRa Module: **SX1276**
868MHz band



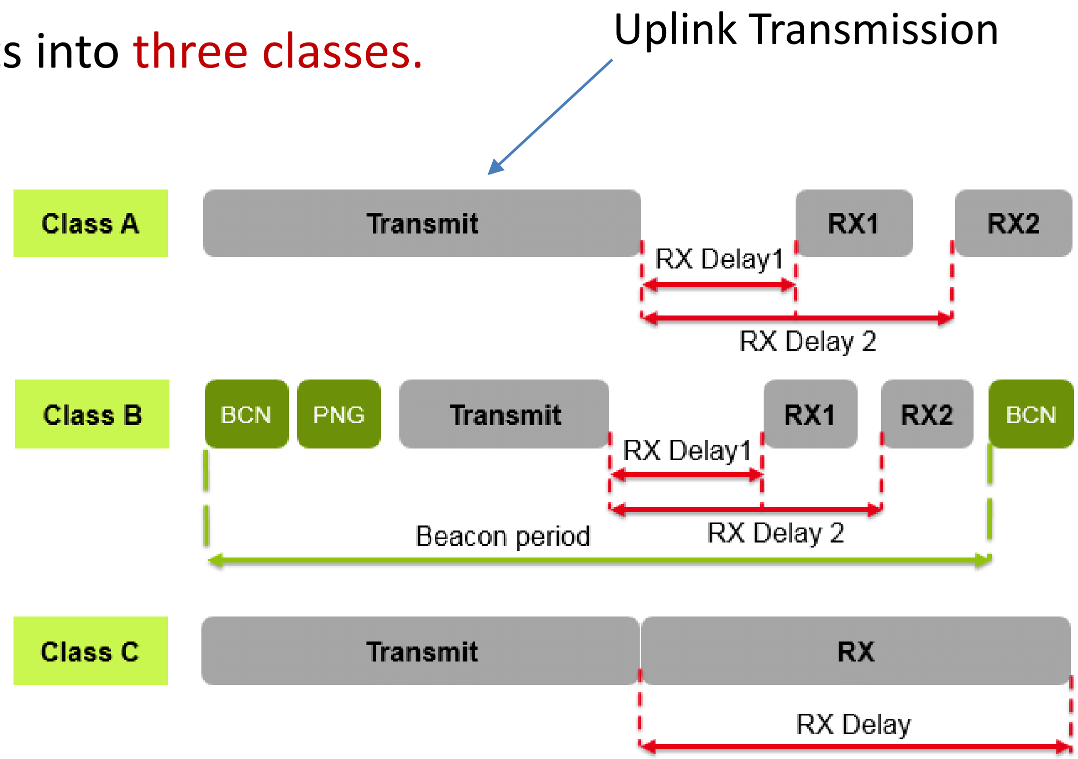
LoRa GPS Shield
with Arduino



LoRa Shield for Arduino

LoRaWAN MAC layer

- Classifies LoRaWAN endpoints 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

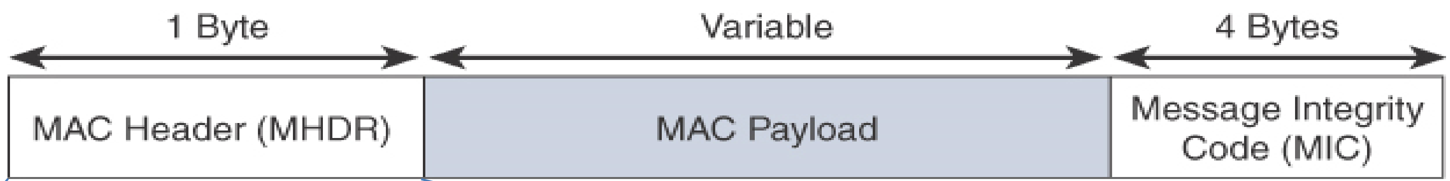
Class B:

- Class B node should get additional receive windows compared to Class A
- gateways must be synchronized through a beaconing process
- "ping slots", can be used by the network infrastructure to initiate a downlink communication

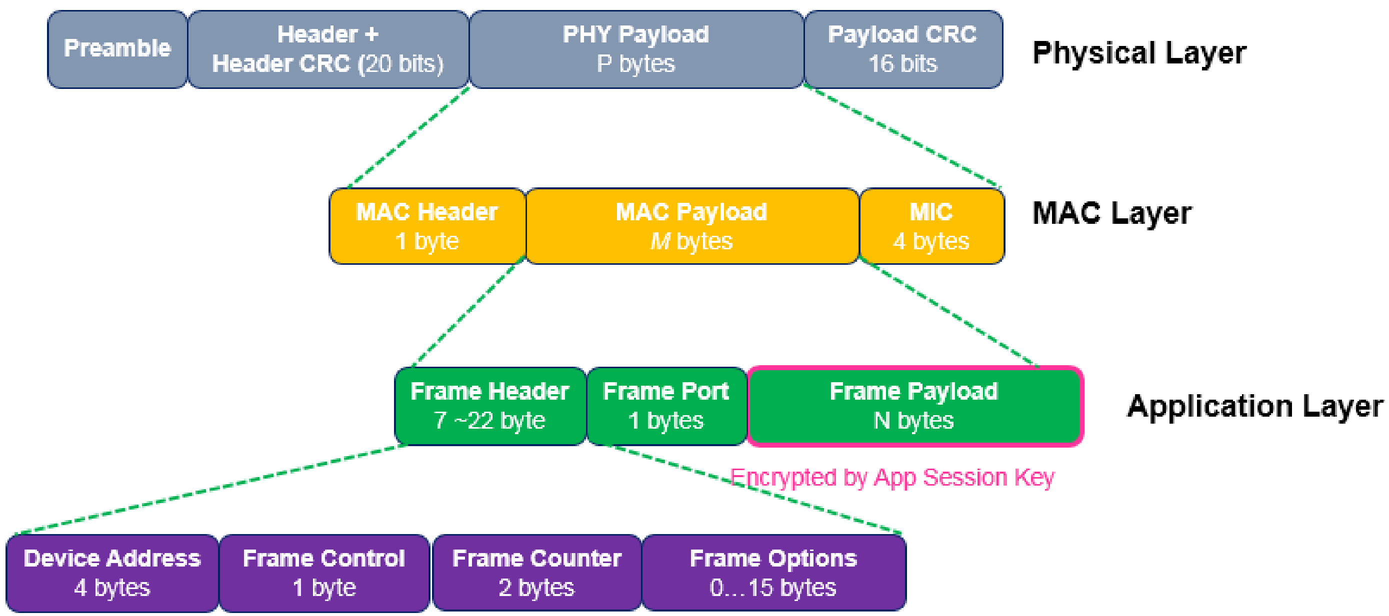
Class C:

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

LoRaWAN MAC Frame Format



Bit#	7..5	4..2	1..0
MHDR bits	MType	RFU	Major



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 knows a number of identifiers for devices, applications and gateways.
  - DevEUI - 64 bit end-device identifier, EUI-64 (unique)
  - DevAddr - 32 bit device address (non-unique)
  - AppEUI - 64 bit application identifier, EUI-64 (unique)
  - GatewayEUI - 64 bit gateway identifier, EUI-64 (unique)

- LoRaWAN devices have a 64 bit unique identifier (DevEUI) that is assigned to the device by the chip manufacturer.

- However, all communication is done with a dynamic 32 bit device address (DevAddr) of which 7 bits are fixed for the Network, leaving 25 bits that can be assigned to individual devices.

LoRaWAN Gateway

- LoRa **gateway** is deployed as the **center 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

Dragino LoRa Gateway

- **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.

Cont…

- LoRa has the ability to handle various data rates via spreading factor (SF)
- Best practices:
  - Use ADR for fixed endpoints
  - Use fixed data rate or spreading factor 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: protect communication and data privacy across the network
- LoRaWAN endpoints must implement **two layers of security**
  - Network security applied in MAC layer
    - authentication of the endpoints
    - protects LoRaWAN packets by performing encryption based on AES
    - Each endpoint implements a network session key (NwkSKey)
    - The NwkSKey ensures data integrity through computing and checking the message integrity code (MIC) of every data message
  - Data privacy applied at the end points (end device and application server)
    - second layer is an application session key (AppSKey)
    - performs encryption & decryption functions 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. DevAddr and the NwkSKey and AppSKey keys) 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.

NB-IoT
and
Other LTE Variations

NB-IoT

- Well-known Cellular Technology
  - GSM: Global System for Mobile Communications
  - GPRS: General Packet Radio Service
  - CDMA: Code Division Multiple Access
  - EDGE: Enhanced Data Rates for GSM Evolution
  - 3G/UMTS: Universal Mobile Telecommunications System
  - 4G/LTE: Long-Term Evolution
- Disadvantage
  - Not adapted to battery-powered small devices like IoT smart objects

- In 2015, 3GPP approved a proposal to standardize a new narrowband radio access technology called Narrowband IoT (NB-IoT)

- It address the requirement:
  - massive number of low-throughput devices,
  - low device power consumption,
  - extended coverage – rural and deep indoors
  - optimized network architecture.

- NB-IoT is addressing the LPWA IoT market opportunity using licensed spectrum
- New physical layer signals and channels are designed

- NB-IoT can co-exist with 2G, 3G, and 4G mobile networks

Comparison of Key Attributes

	WiFi	BLE	Thread	Sub-GHz: TI	SigFox	ZigBee	LoRa
Max. Data throughput	72 Mbps	2 Mbps	250 Kbps	200 Kbps	100 bps	250 Kbps	50 Kbps
Range	100 m	750 m	100 m	4 km	25 km	130 m	10 km
Topology	Star	P2P/ Mesh	Mesh/ Star	Star	Star	Mesh/ Star	Star of Star
Frequency	2.4 GHz	2.4 GHz	2.4 GHz	Sub-GHz	Sub-GHz	2.4 GHz	Sub-1GHz
Power consumption	1 Year (AA battery)	Up to years on a coin-cell battery for limited range					Few Years (AA battery)
IP at the device node	Yes	No	Yes	No	No	No	No
Deployed Devices	AP	smart phones	No	No	No	No	No

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.