Communication Technologies for IoT

Sachin Chaudhari

Signal Processing and Communications Research Center (SPCRC)
International Institute of Information Technology (IIIT), Hyderabad
Email: sachin.chaudhari@iiit.ac.in

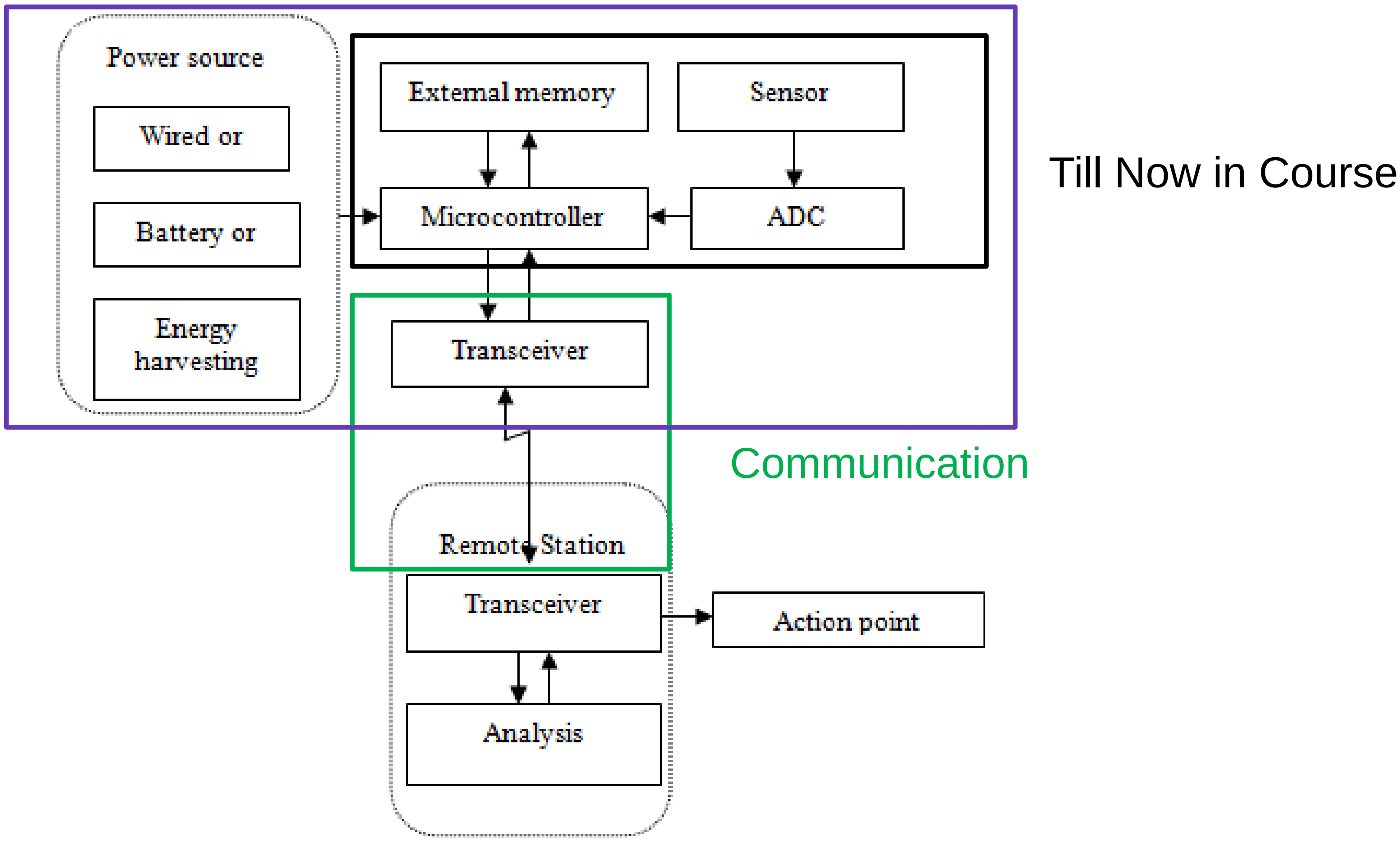
INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Embedded System Workshop and IoT Workshop, 11 October 2021

Outline

- Introduction
  - Basic issues
  - Scope of presentation
  - Basics of Communications (MAC)
- Different wireless technologies for IoT
  - IEEE 802.15.4 (Zigbee)
  - IEEE 802.11ah (WiFi)
  - Bluetooth
  - Cellular Technologies: LTE-M and NB-IoT
  - LoRaWAN
- Summary

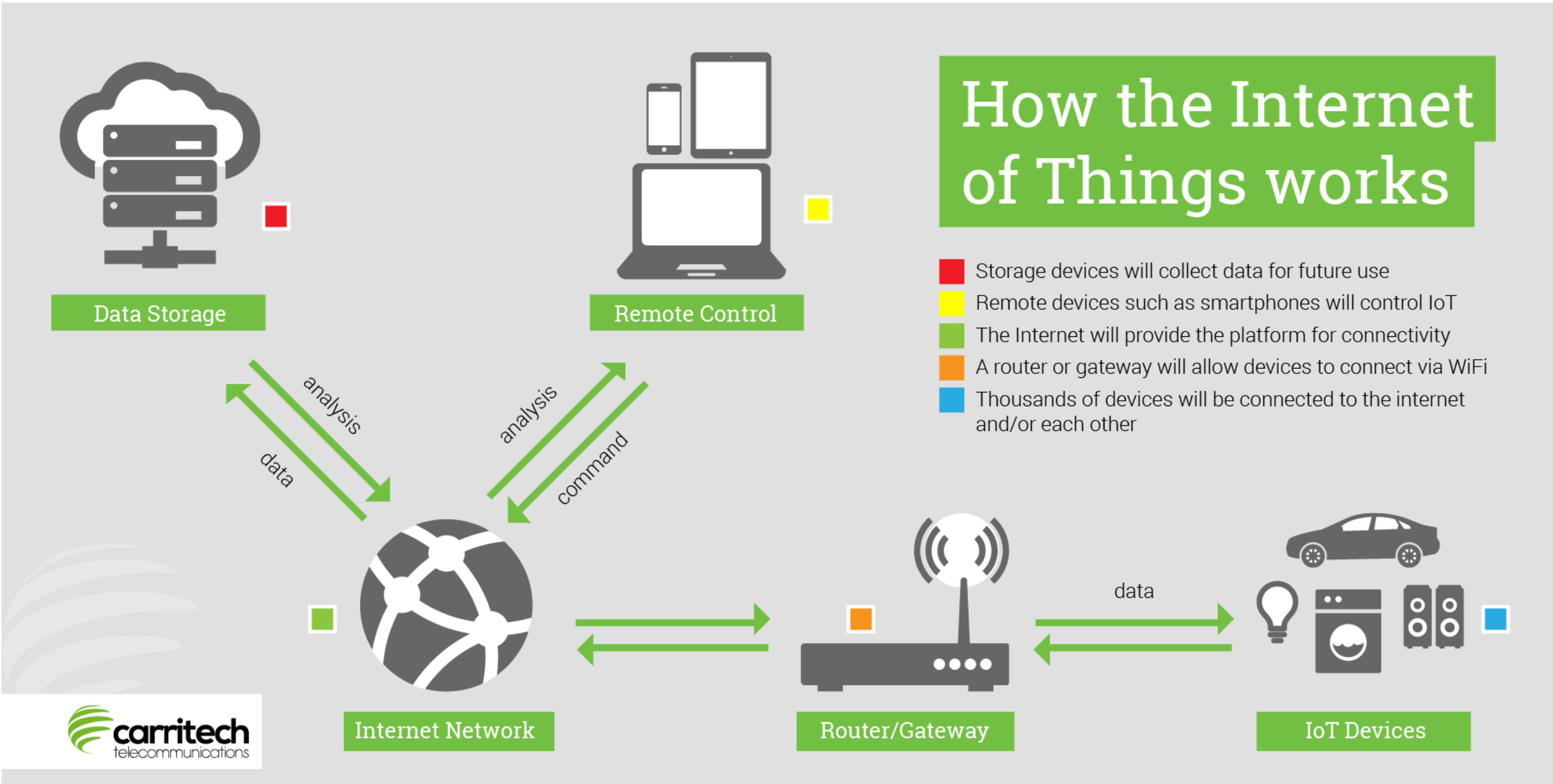
Block Diagram of Sensor Node



https://www.researchgate.net/publication/269310409_A_review_of_sensor_networks_Technologies_and_applications/figures?lo=1&utm_source=google&utm_medium=organic

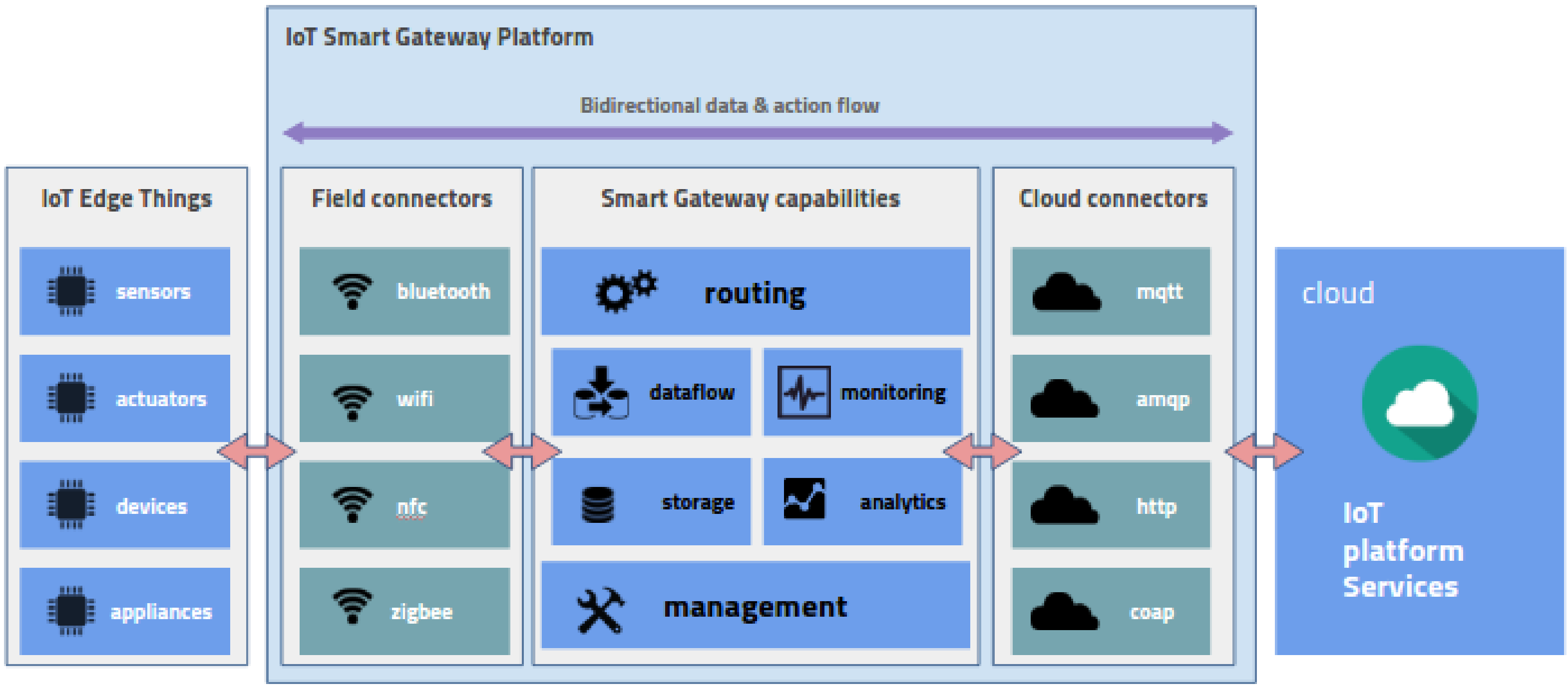
[Leverage: Intro to IoT] ***To be smart, a thing doesn't need to have super storage or a supercomputer inside of it . All a thing has to do is connect to super storage or to a super computer.***

How does IoT work?



Picture Credit: *http://www.carritech.com/news/internet-of-things/*

IoT Network Setup



Picture Credit: https:https://www.iotcentral.io/blog/the-iot-architecture-at-the-edge

Issues in IoT from Communication Perspective

[Not an exhaustive list!]

- Low power consumption
- Support large number of devices with low data rates
- Coverage
- Quality of service
- Low cost
  - Network/Private (DIY)
  - Licensed/Unlicensed
- Privacy and security
- Standardization for interoperability between different vendors

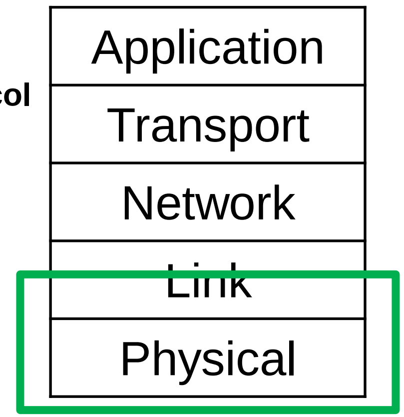
Scope of the Presentation

IoT PROTOCOLS

- The various protocols that are emerging:
  - **Infrastructure** (ex: 6LowPAN, IPv4/IPv6, RPL)
  - **Identification** (ex: EPC, uCode, IPv6, URIs)
  - **Comms / Transport** (ex: Wifi, Bluetooth, LPWAN)
  - **Discovery** (ex: Physical Web, mDNS, DNS-SD)
  - **Data Protocols** (ex: MQTT, CoAP, AMQP, Websocket, Node)
  - **Device Management** (ex: TR-069, OMA-DM)
  - **Semantic** (ex: JSON-LD, Web Thing Model)
  - **Multi-layer Frameworks** (ex: Alljoyn, IoTivity, Weave, Homekit)

Scope of the Presentation

Five-layer
Internet Protocol
stack



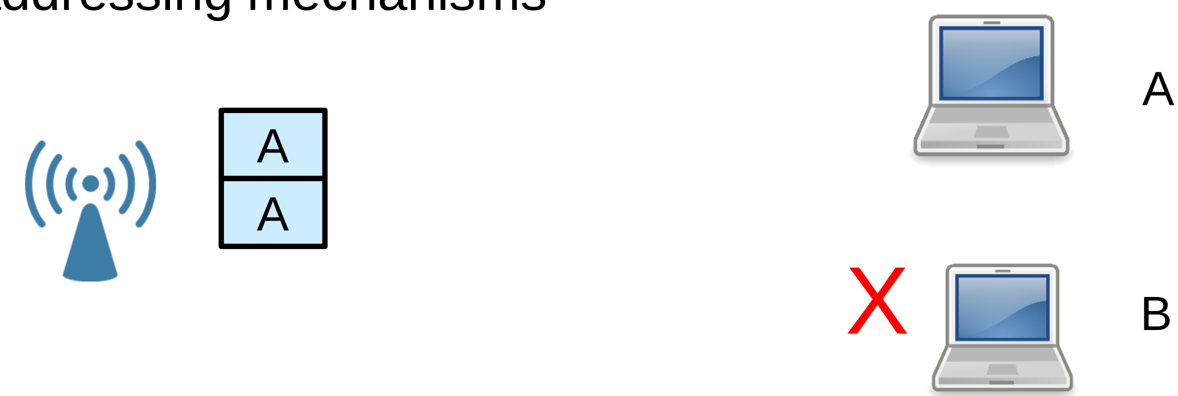
- Medium access control (MAC)
  - Provides channel access control mechanisms across a shared physical medium
  - Example: Aloha, CSMA/CA, TDMA, CDMA
  - Provides addressing mechanisms

- Physical Layer (PHY)
  - Defines the means of transmitting raw bits rather than logical data packets over a physical link/medium connecting two nodes on the same network
  - Signal processing of bits and physical signals: Modulation, Coding, Bit Interleaving, Synchronization, Carrier sensing and collision detection, etc.
  - Example: WLAN 802.11, LR-WPANs 802.15.4, Ethernet 802.3, Bluetooth 802.15.1

Medium Access Control (MAC)

- One of the two sublayers of data link layer
- Acts as an interface between the logical link control (LLC) and the network's physical layer
- Provides channel access control mechanisms across a shared physical medium

- Provides addressing mechanisms



Link Layer: *Various multiple access channels*

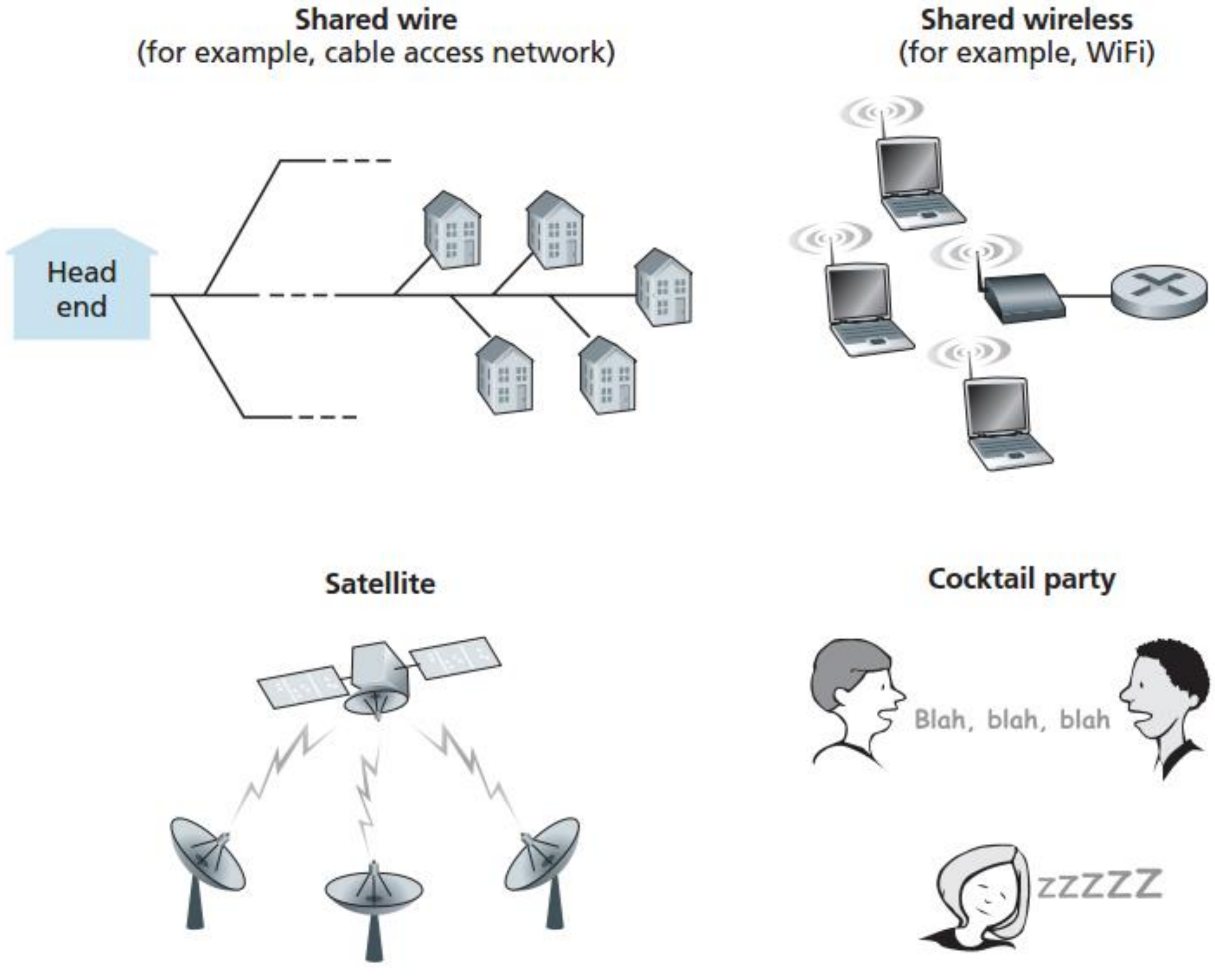


Figure 5.8 ♦ Various multiple access channels

Another Analogy: Roads

https://www.freepik.com/vectors/travel

Conversation Etiquettes

- ❑ Give everyone a chance to speak
- ❑ Don’t monopolize the conversation
- ❑ Don’t speak until you are spoken to
- ❑ Don’t interrupt when someone is speaking
- ❑ Don’t fall asleep when someone is speaking

Desirable Properties of MAC protocols

A MAC protocol for a broadcast channel of rate *R* bps should have following desirable properties

- When only one node has to send data, that node has throughput of *R* bps
- When *M* nodes have to send data, each of the nodes should have average rate of *R/M* bps
- The protocol is decentralized so that there is no master node with single point of failure
- The protocol is simple so that it is inexpensive to implement

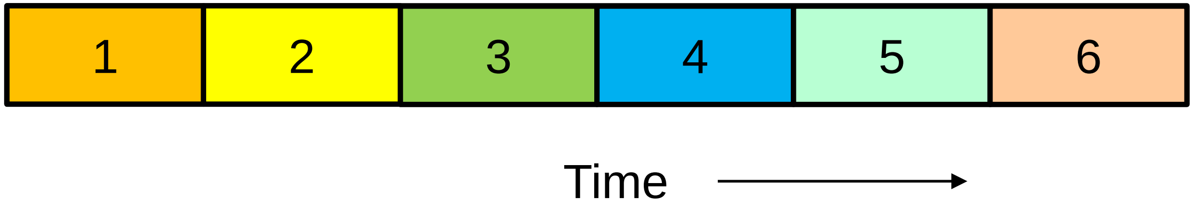
Types of MAC protocols

- Channel Partitioning Protocols (or Fixed Assignment Protocols)
  - TDMA, FDMA, CDMA, SDMA
- Random Access Protocols
  - Aloha, Slotted Aloha, CSMA/CA
- Taking Turn Protocols (or Demand Assignment Protocols)
  - Token Ring
  - Polling

Channel Partitioning Protocols

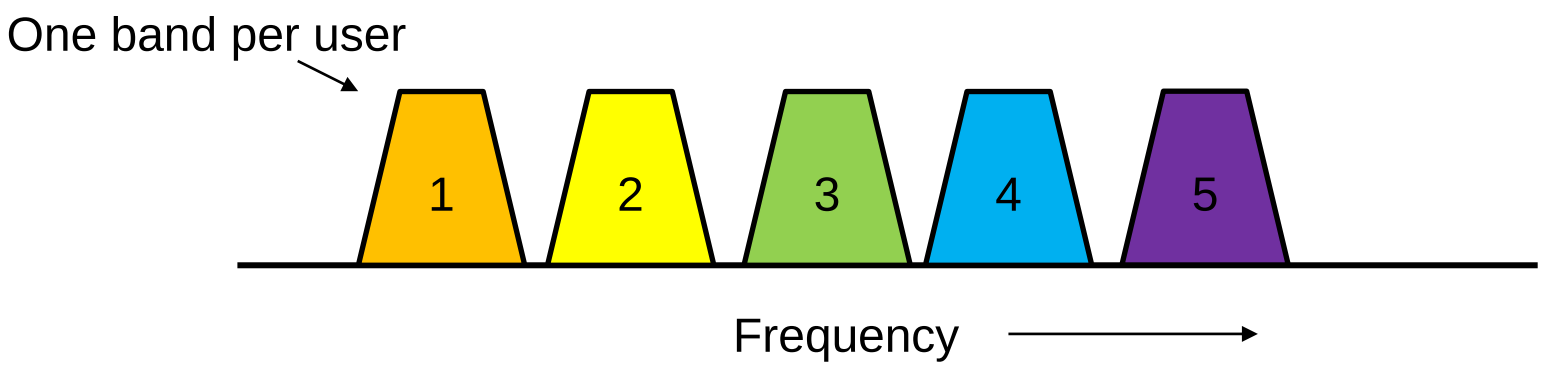
Time Division Multiple Access

- Time Division Multiple Access
  - TDMA is a digital technique that divides a single channel or band into time slots
  - Examples: T1 carrier systems (digital transmission of multiplexed telephone calls), 2G cellular system GSM



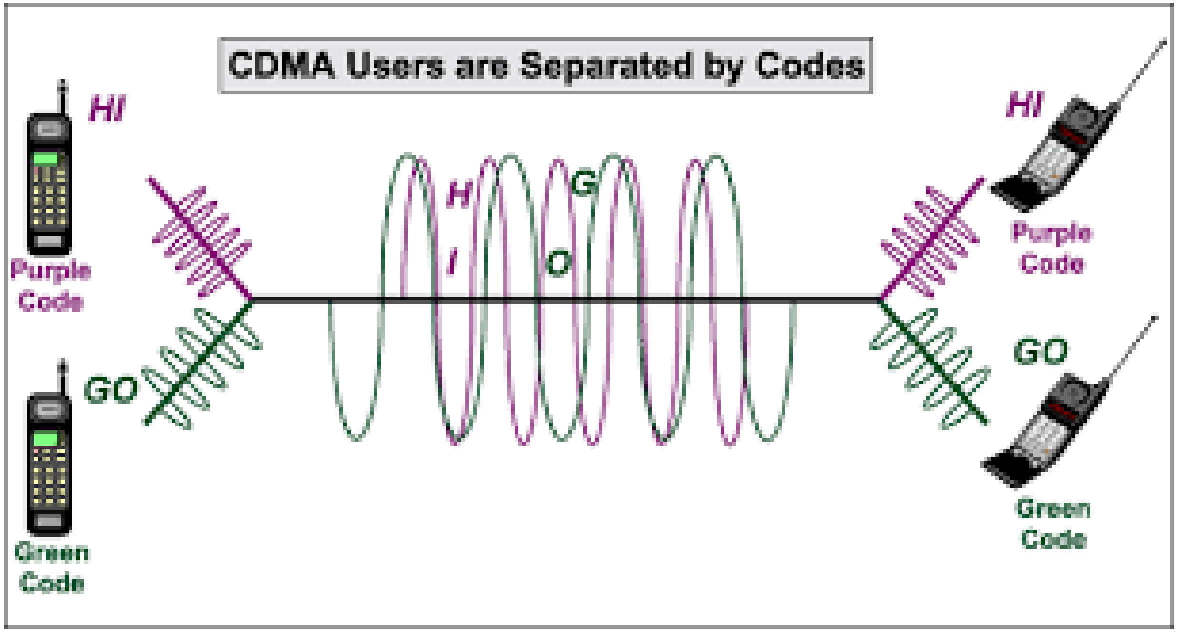
Frequency Division Multiple Access

- Frequency Division Multiple Access
  - FDMA divides the shared medium bandwidth into individual channels
  - Examples: Cable television system, FM stations



Code Division Multiple Access

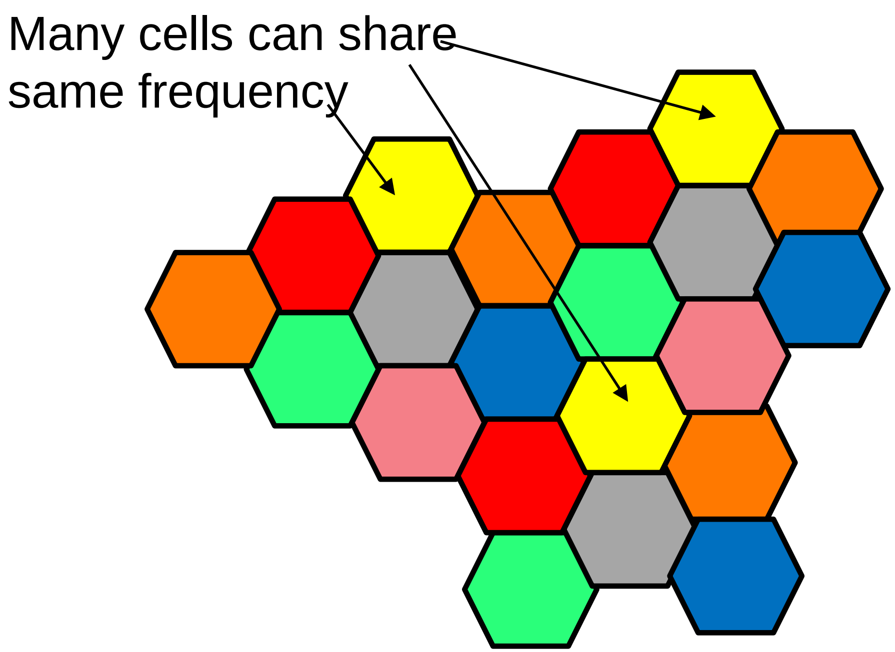
- Code Division Multiple Access
  - It is also known as spread spectrum because it takes the digitized version of an analog signal and spreads it out over a wider bandwidth at a lower power level.
  - Example: 2G IS-95, 3G (WCDMA)



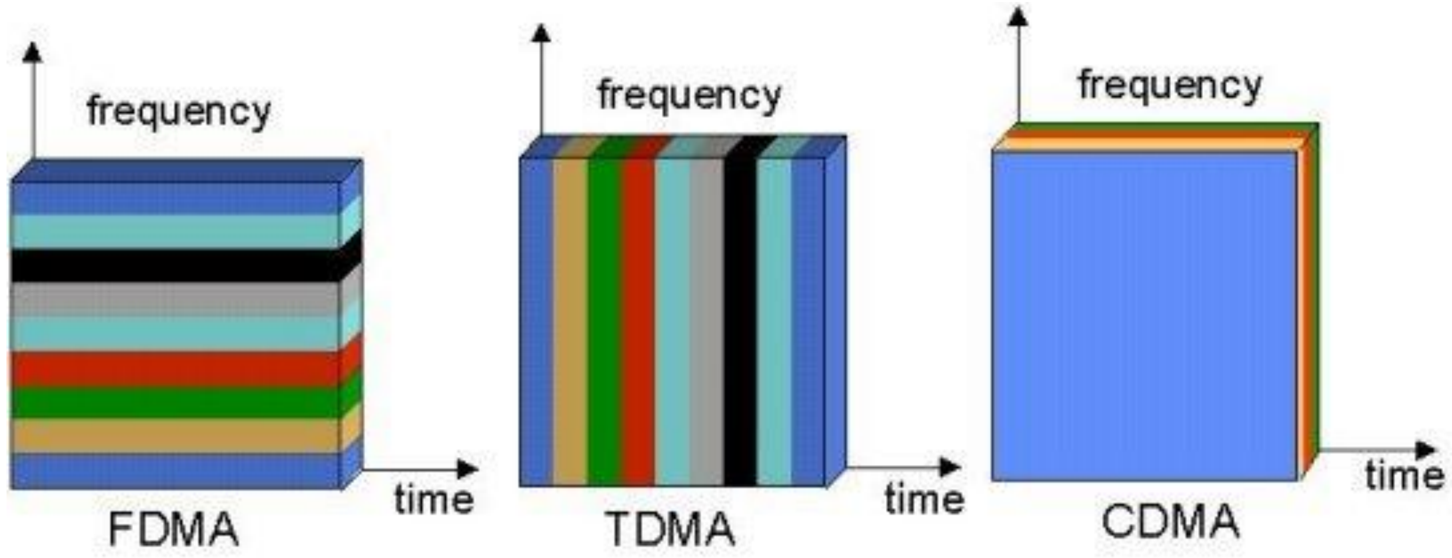
Source: http://www.electronicdesign.com/communications/fundamentals-communications-access-technologies-fdma-tdma-cdma-ofdma-and-sdma

Space Division Multiple Access

- Space Division Multiple Access
  - SDMA uses physical separation methods that permit the sharing of wireless channels. For instance, a single channel may be used simultaneously if the users are spaced far enough from one another to avoid interference. Known as frequency reuse, the method is widely used in cellular radio systems. Cell sites are spaced from one another to minimize interference.



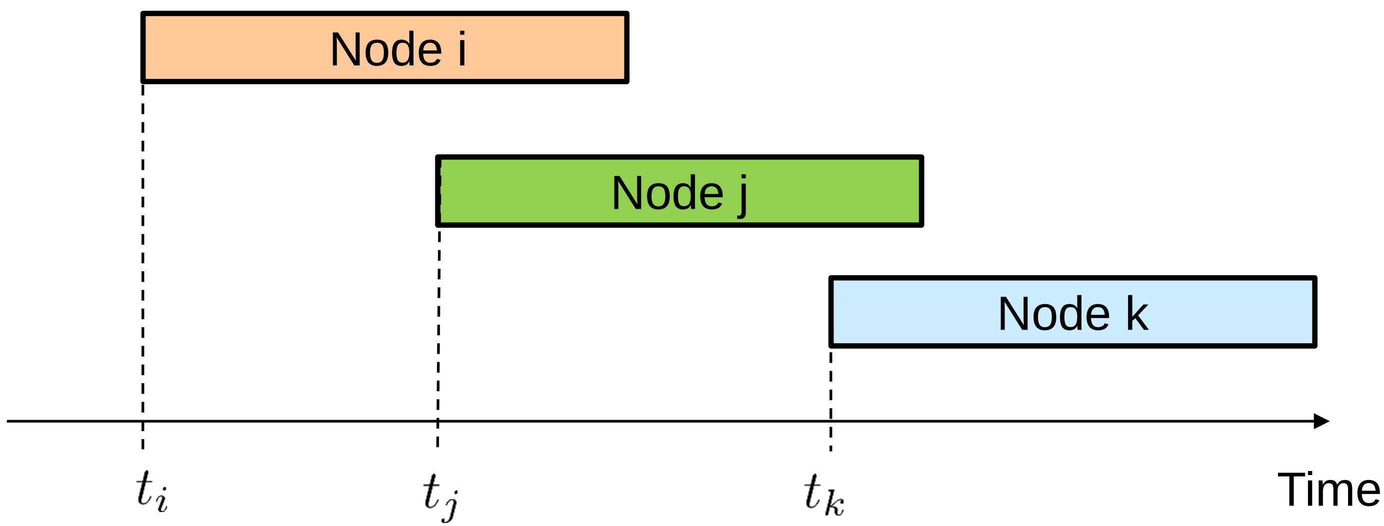
Difference between different TDMA/FDMA/CDMA



Random Access Protocols

Aloha

- When you have data, send it
- If data doesn't go through, resend it after random delay
  - Send with probability *p* or wait for one transmission frame with probability *1-p*
- Low efficiency:
  - Probability of success is $p(1-p)^{2(N-1)}$
  - 18.5% for large *N*
- Suitable only for light loaded network

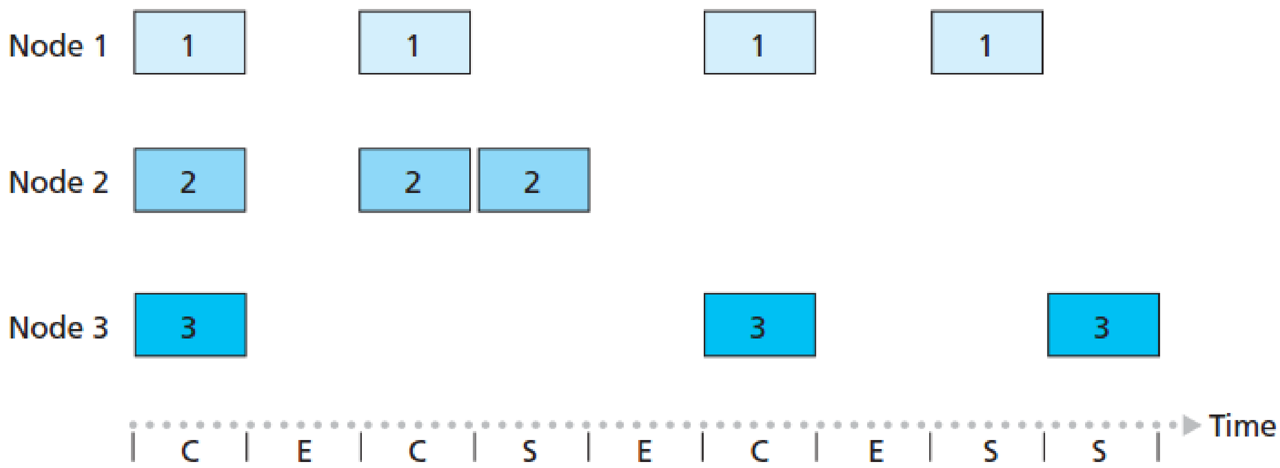


Aloha

- Unstable for certain channel conditions
  - Avalanche of retransmission attempts
- Nice animation
  - http://www.wirelesscommunication.nl/reference/chaptr06/aloha/alohplay.htm

Slotted Aloha

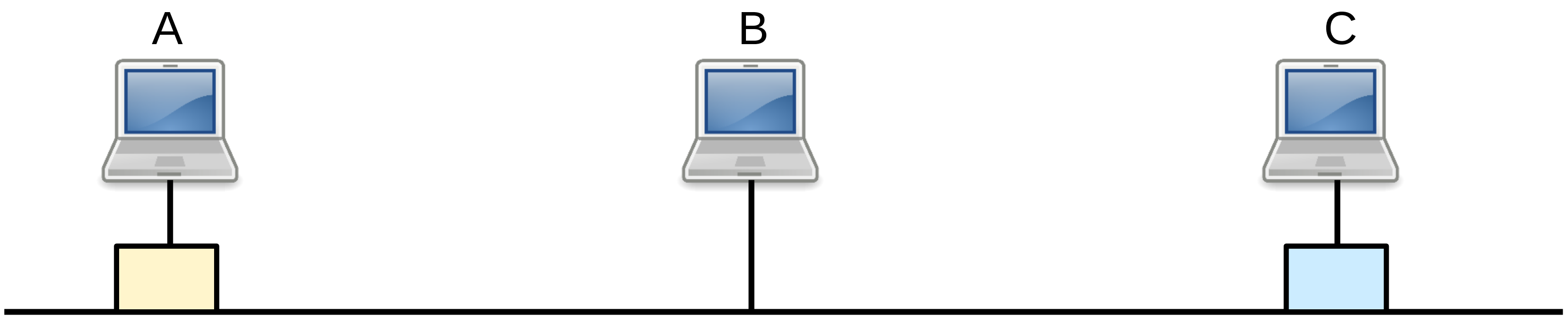
- Time is divided into equal time slots
- Sensor node can send data only at the beginning of a slot
- If have data to send, send at the start of slot. If collision, send in the next slot with probability *p* and do not transmit with probability *1-p*
- Requires time synchronization between nodes
- Efficiency: 37%; Better than Aloha but still low



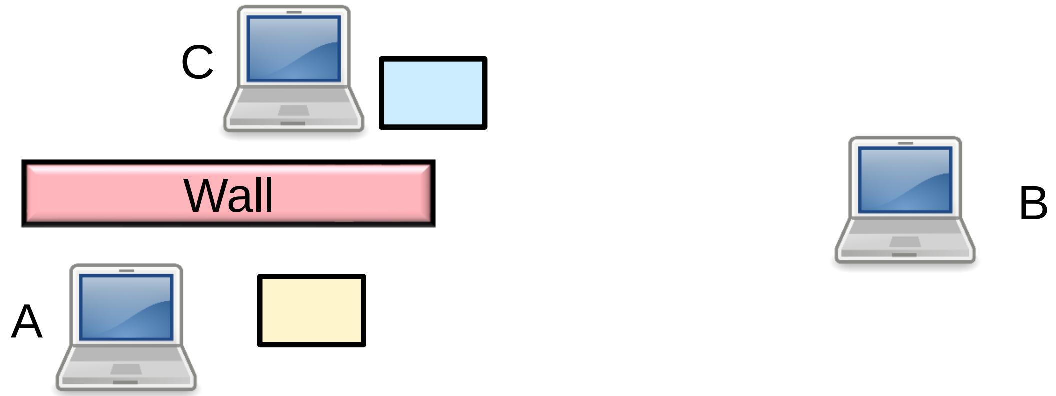
[Kurose2012]

Carrier Sense Multiple Access (CSMA)

- Listen before sending
- Send only if channel is idle
- Collisions can still happen (Hidden Node Problem)
- If collision, back-off for random delay and transmit again

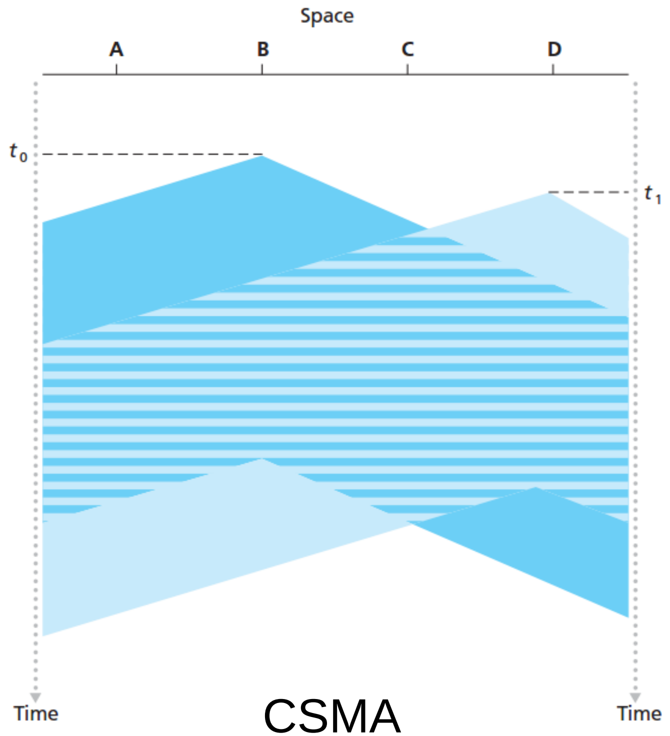


- Hidden Node Problem in Wireless Networks



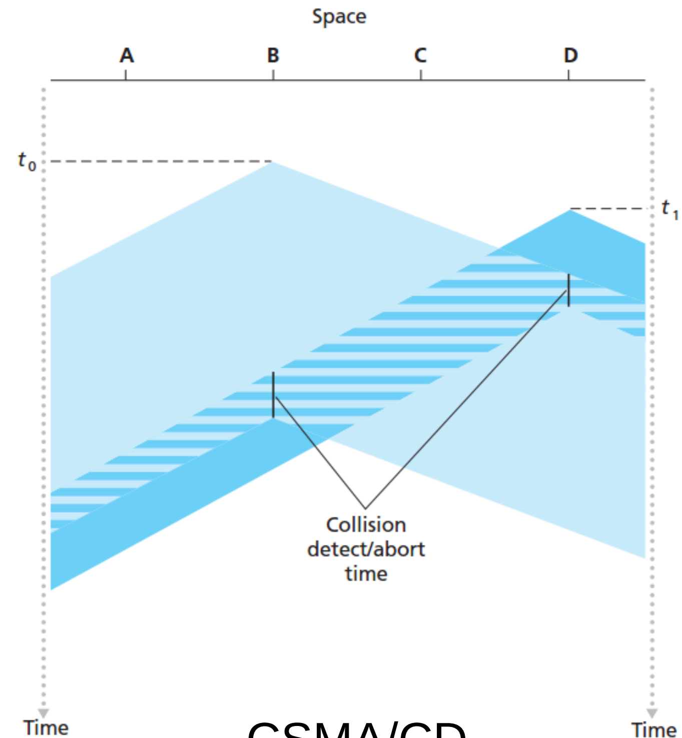
CSMA with collision detection (CD)

- Listen while transmitting!
- Stop transmitting as soon as collision is detected
- Wait for random duration before retry (binary exponential backoff)
- Improves CSMA performance at the cost of complexity
- Used in original Ethernet (wired LAN technology IEEE 802.3)



CSMA

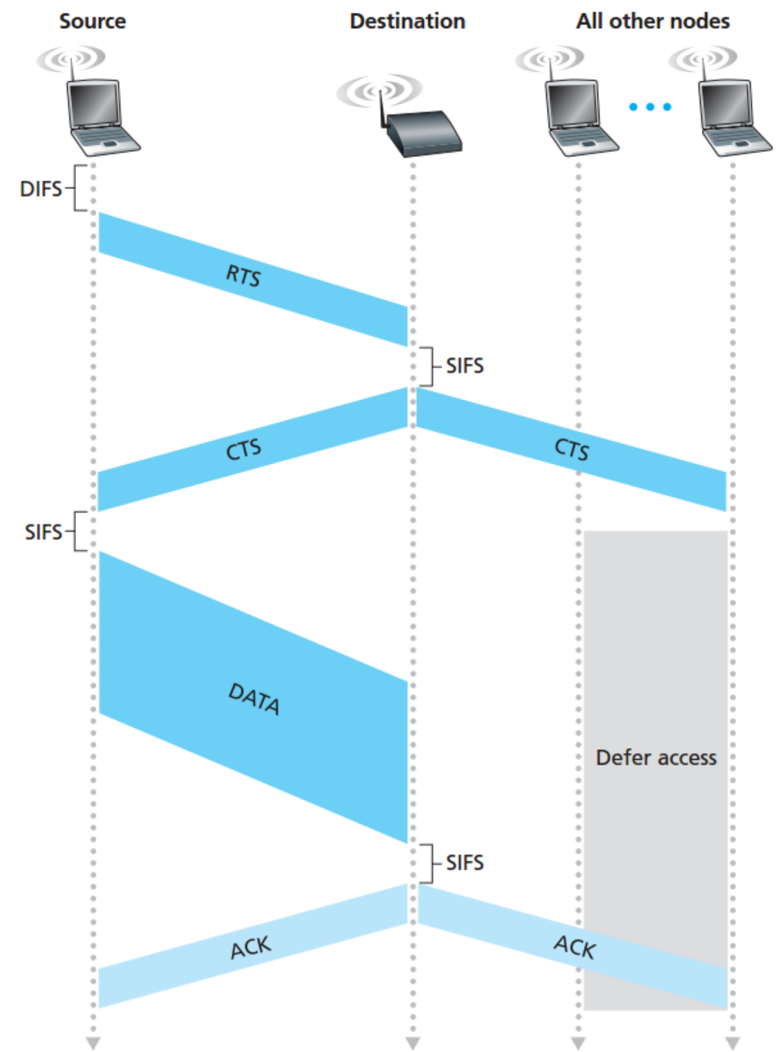
[Kurose2012]



CSMA/CD

CSMA with Collision Avoidance (CA)

- Use of ready to send (RTS) and clear to send (CTS)
  - In RTS/CTS access mode, prior to the data transmission the sending node will send a RTS packet to announce the upcoming transmission
  - When the destination node receives the RTS it will send a CTS packet after a short inter-frame space (SIFS) interval
  - Both the RTS and CTS packets are short control packets
- Used in most of the 802.11 (WLAN) technologies



[Kurose2012]

Demand Assignment Protocols
(or Taking Turn Protocols)

Motivation

- Problem with channel partitioning
  - Inefficient at low load (idle subchannels)
- Problem with contention-based protocols
  - Inefficient at high loads (collisions)

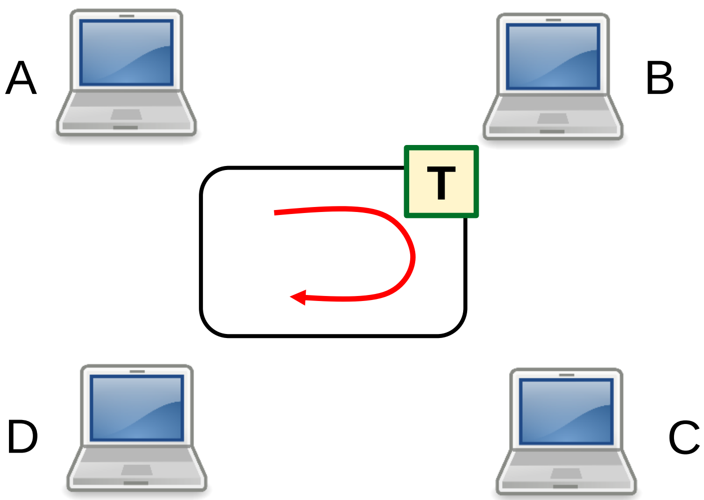
- Taking turn protocols
  - Can improve efficiency of channel partitioning and have no collisions
  - Can potentially also offer guaranteed bandwidth, latency, etc.

Polling Protocol

- One of the nodes becomes master node
- Master node polls each node in round-robin fashion
- Node polled can transmit up to maximum number of frames
- Eliminates the collisions that plague random access protocols and empty slots in channel partitioning protocols
- Issue of single point failure, delay in polling and instructing to send
- Example: used in Bluetooth and 802.15 protocols

Token Passing (or Token Ring)

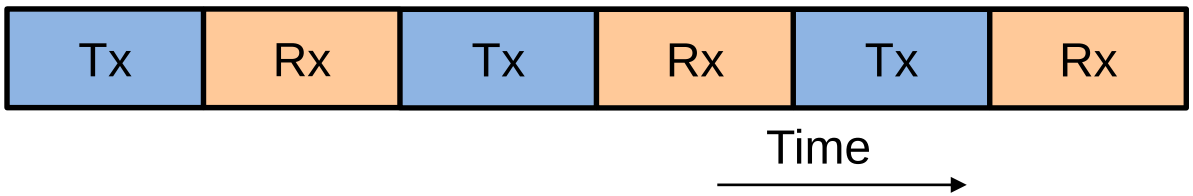
- A token is circulating in the ring and whichever node grabs that token will have right to transmit the data.
- This protocol provides fairness and eliminates collision
- Advantages: Decentralized and highly efficient
- Disadvantages: Node failure and node not releasing token
- Used in networks prior to Ethernet



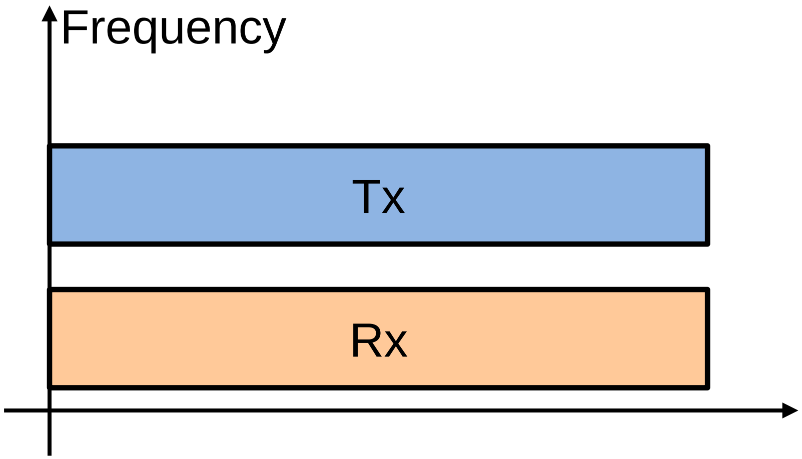
Few other things!

Duplexing Methods

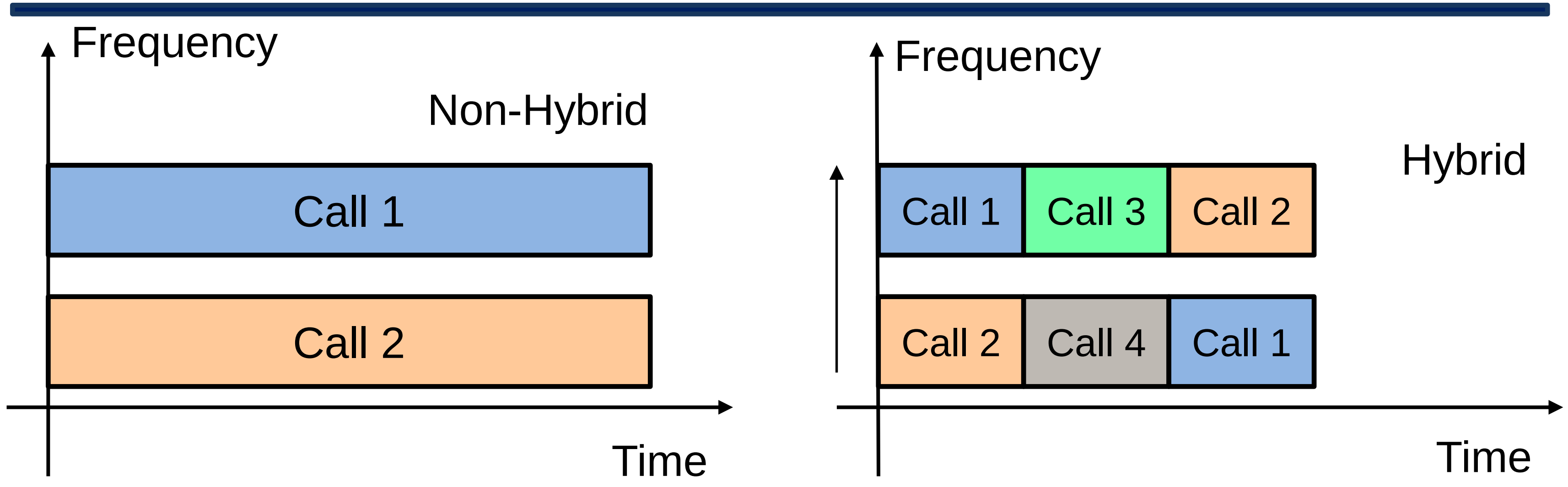
- Methods used for dividing forward and reverse communication channels, they are called as duplexing methods such as
  - Time division duplexing (TDD)



  - Frequency division duplexing (FDD)

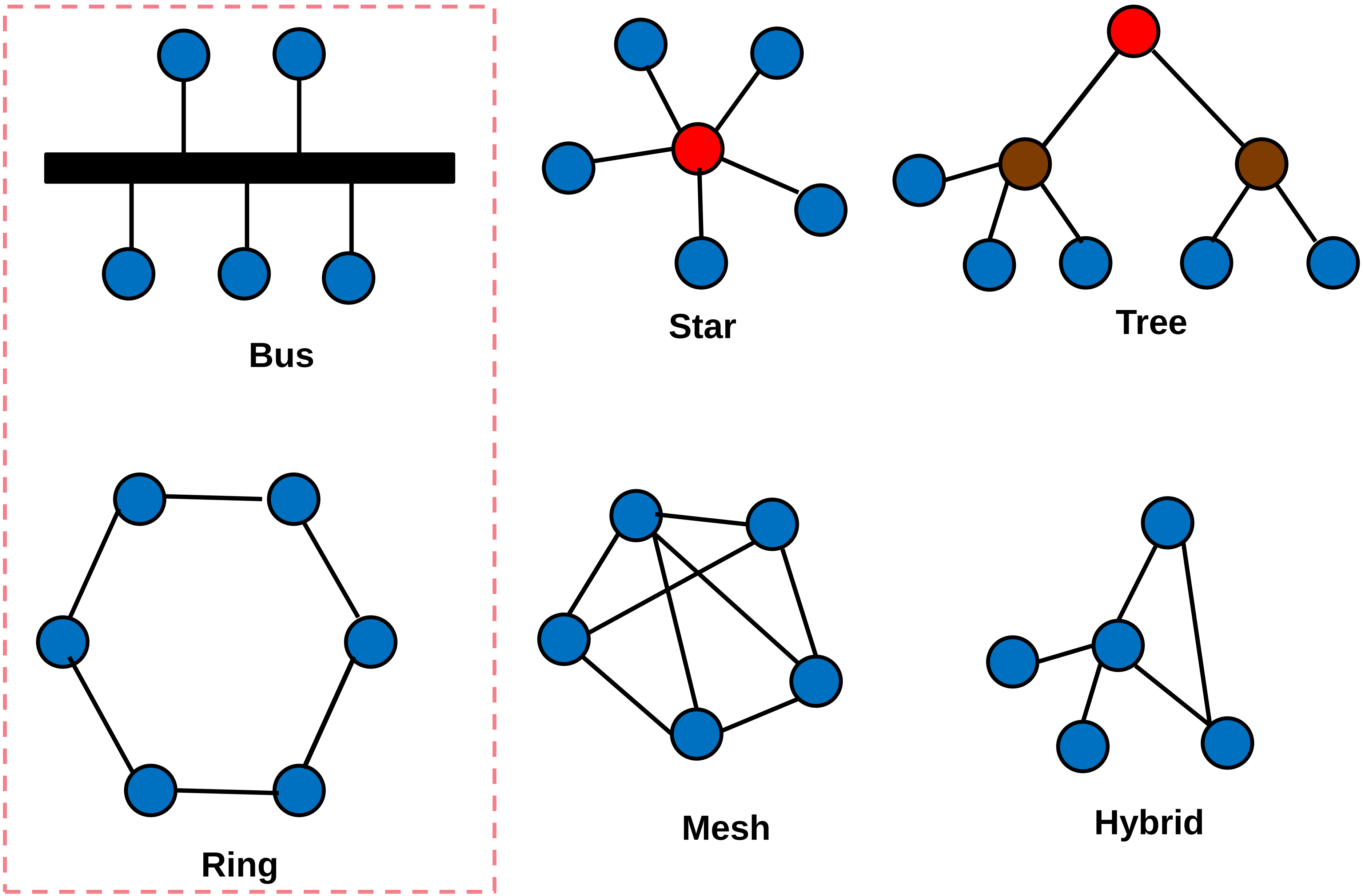


Hybrid Channel Access



- The GSM cellular system combines the use of FDD to prevent interference between outward and return signals with FDMA and TDMA to allow multiple handsets in a single cell.
- Bluetooth packet mode communication combines frequency hopping for shared channel access among several private area networks in the same room with CSMA/CA for shared channel access inside a medium
- IEEE 802.11b WLAN are based on FDMA and DS-CDMA for avoiding interference among adjacent WLAN cells or access points

Network Topologies



Factors contributing to energy waste/expense

- Energy consumption in transmission
  - Longer distances
  - Higher frequencies
  - More bandwidth

- Energy waste
  - Excessive overhead
  - Idle listening
  - Overhearing
  - Packet collisions and retransmissions

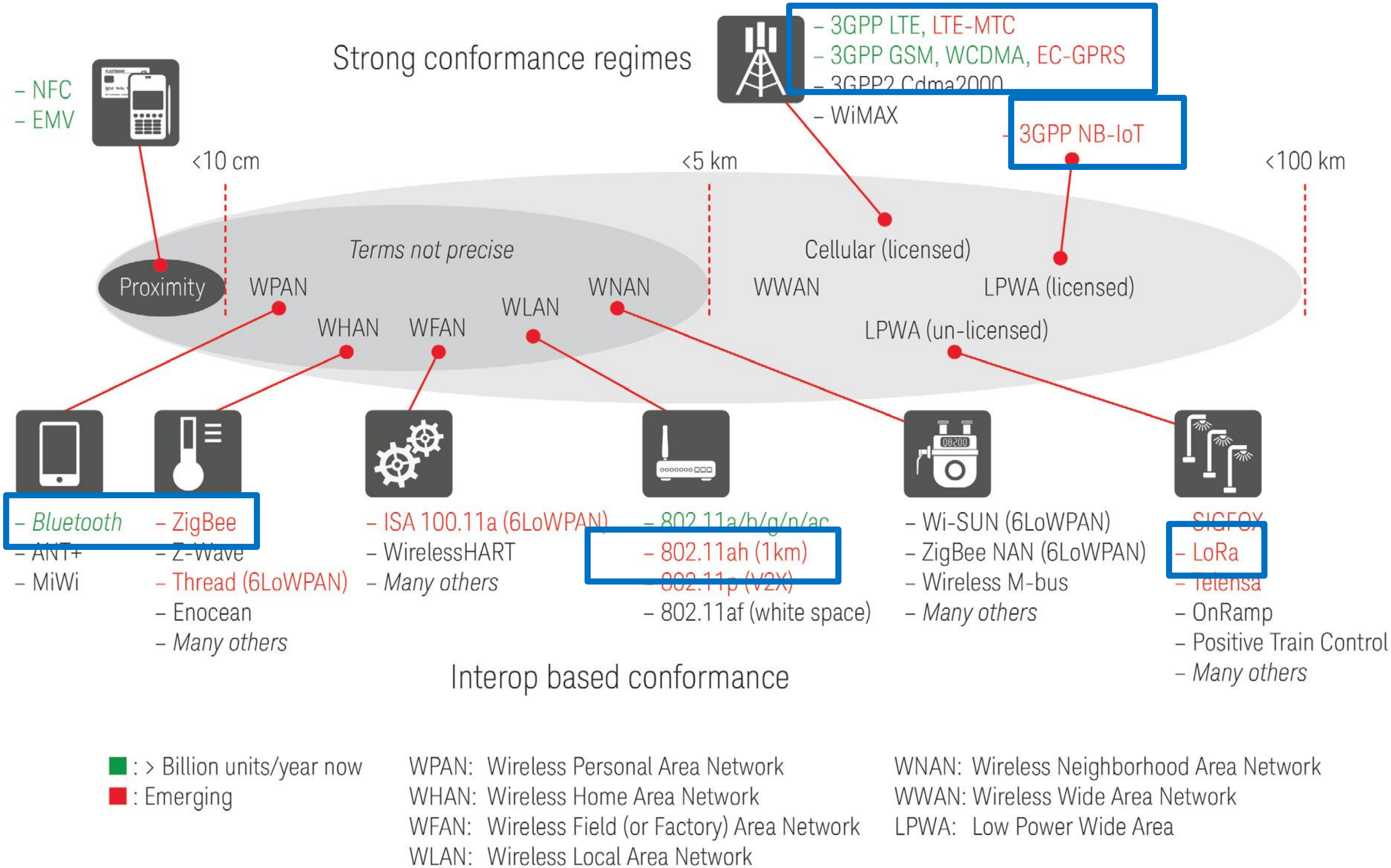
[Not exhaustive!]

Ways to Reduce Energy Waste/Consumption

- Reduced frequency/data rate/ bandwidth/ coverage
- Sleep
  - Low duty cycle
- Energy saving protocols
  - Schedule based (reduction in over-hearing and idle-listening)
    - Licensed spectrum; BLE
  - Contention based (less overhead and no need of synchronization)
    - Zigbee, WiFi
- Multihop and aggregation of data
- Signal processing
  - censoring, predictive filters
- Reduced overhead

Communication Techniques for IoT

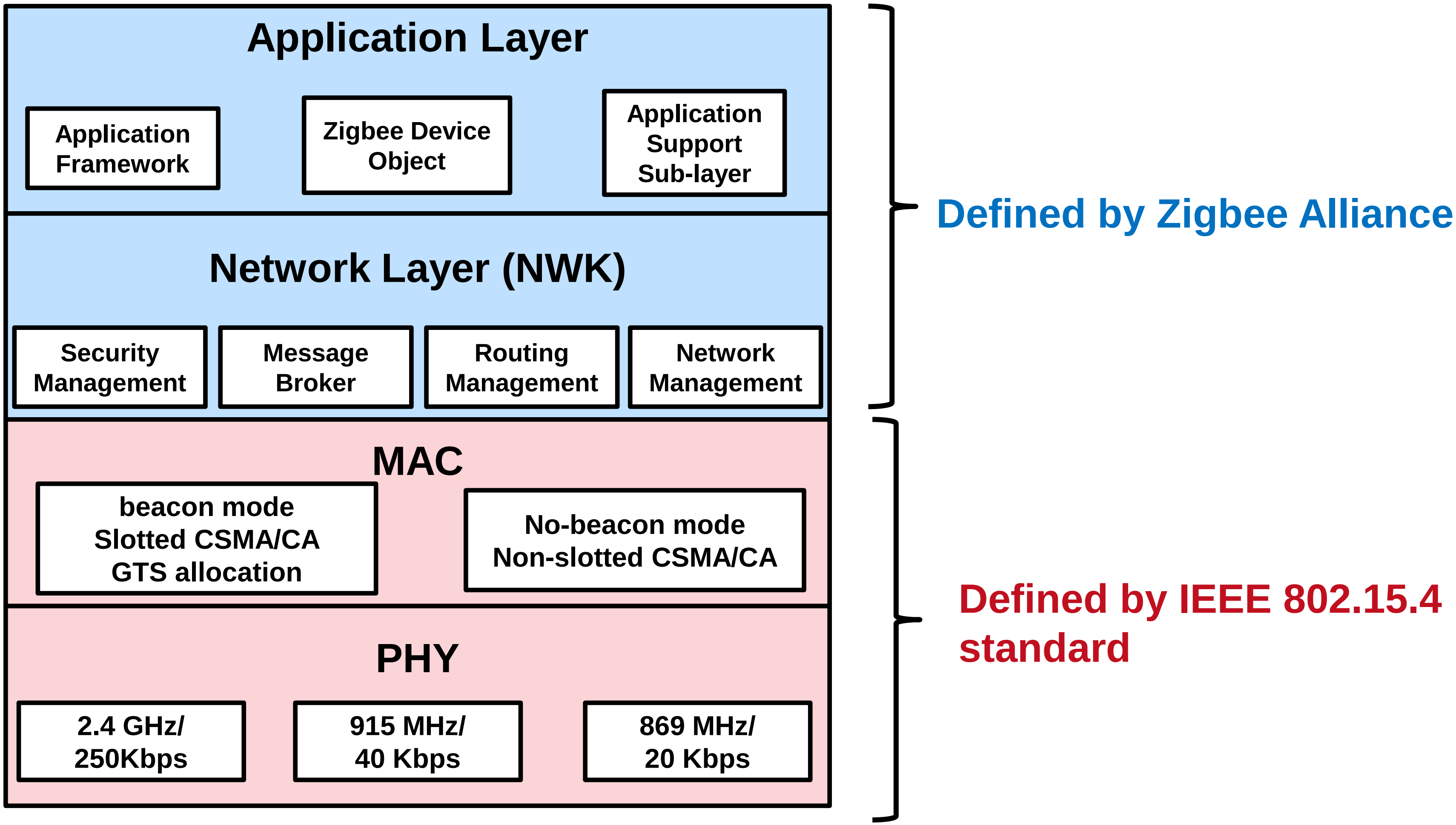
Communication Techniques for IoT



http://2yh5c119vtjz3yoo8229y5bs-wpengine.netdna-ssl.com/wp-content/uploads/2016/04/IoT-technologies-grouped-by-operating-range.jpg

IEEE 802.15.4

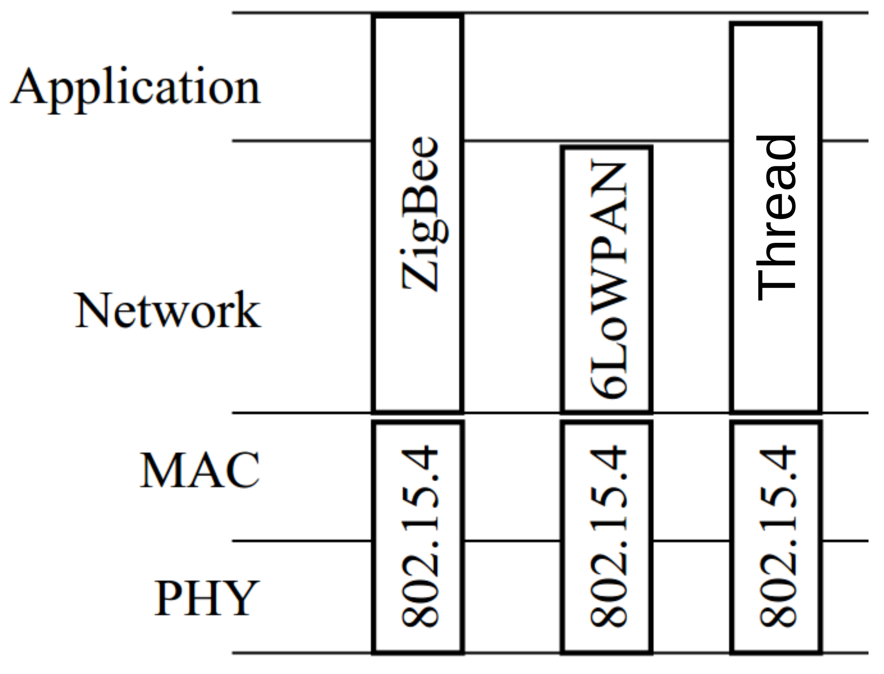
IEEE 802.15.4/Zigbee Protocol Stack



- Full protocol stack for low power, low rate and low cost wireless communications. Also applicable to Low rate WPAN – LR-WPAN.

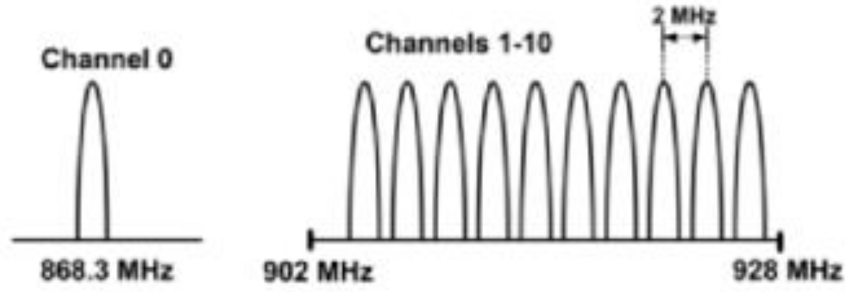
IEEE 802.15.4

- ❑ IEEE 802.15.4 defines the operation of low-rate wireless personal area networks (LR-WPANs)
- ❑ Widely used in wireless sensor-network (WSN) applications
- ❑ It specifies the physical layer (PHY) and media access control (MAC) for LR-WPANs
- ❑ Used by several "Internet of Things" protocols:
  - ➢ ZigBee, 6LowPAN, Thread, etc.



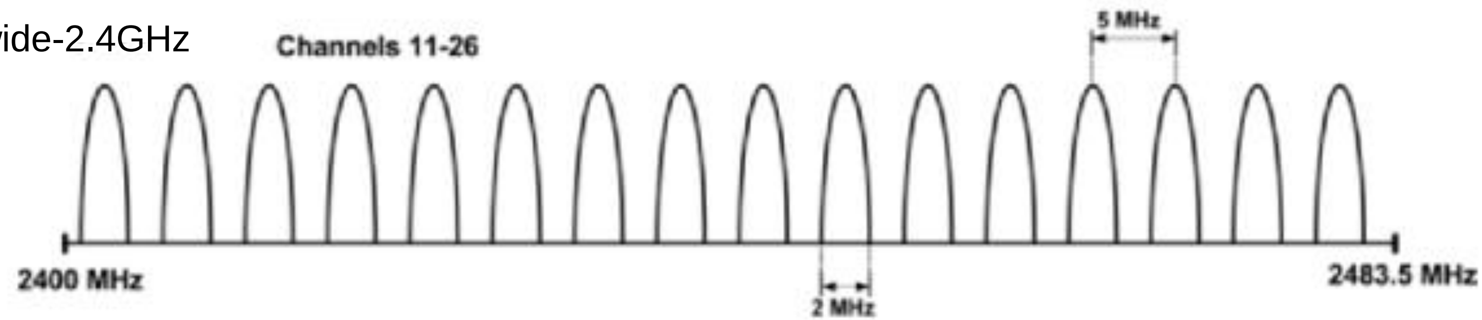
IEEE 802.15.4 PHY

Europe-868 MHz
USA – 915 MHz



[Koubaa2007]

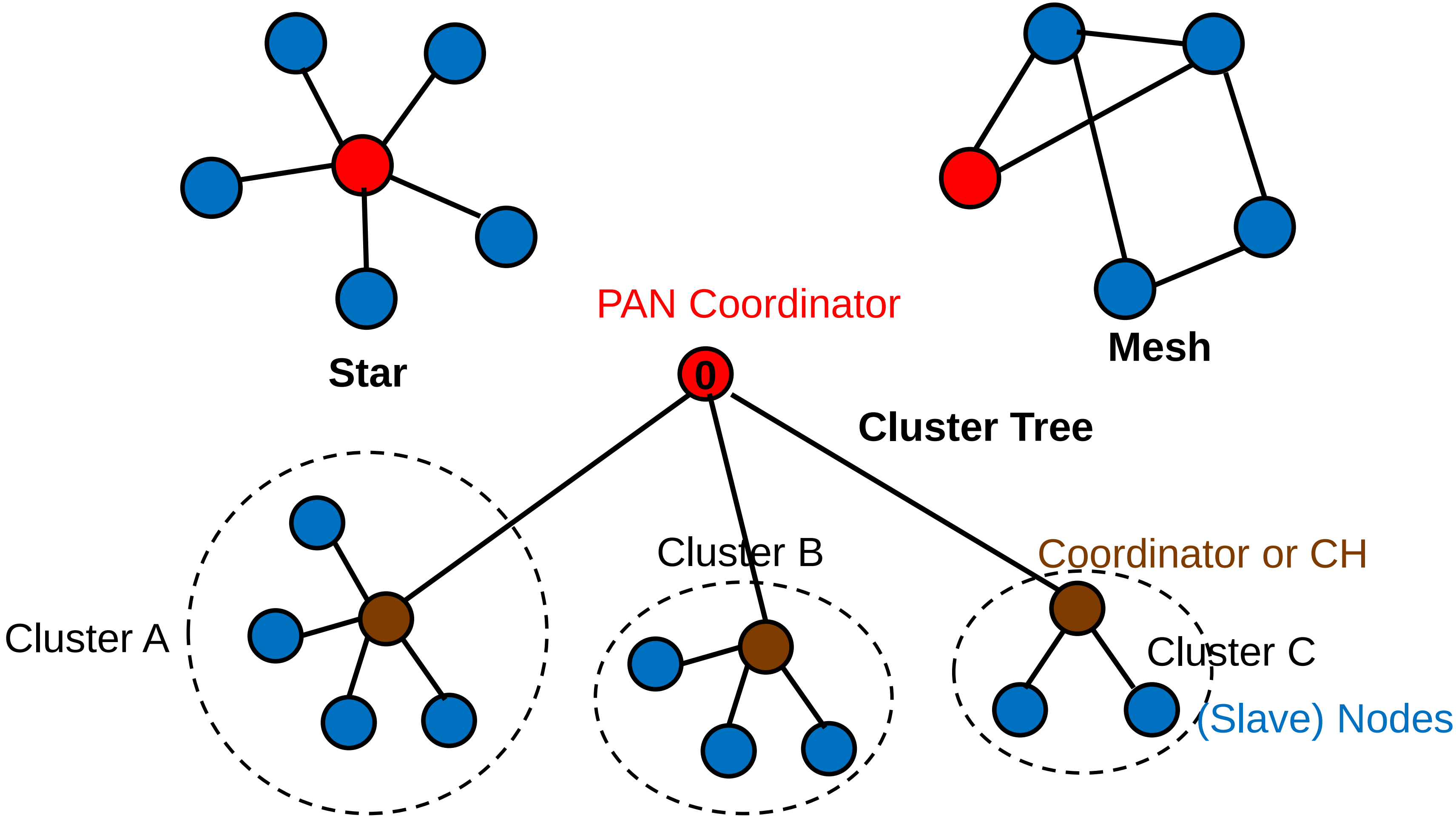
Worldwide-2.4GHz



Freq. band (MHz)	Spreading Parameters		Data Parameters		
	Chip rate (kchip/s)	Modulation	Bit rate (kbps)	Symbol rate (ksymbol/s)	Symbols
868	300	BPSK	20	20	Binary
915	600	BPSK	40	40	Binary
2400	2000	O-QPSK	250	62.5	16-ary

All bands are based on Direct sequence spread spectrum (DSSS)

Network Topologies



- 16 bit addresses support 65536 devices in a PAN. For clusters, 255 clusters with 254 nodes each
- Self recovering ability

MAC Layer: *Physical Device Types*

Two kind of devices in IEEE 802.15.4 based on complexity and capability

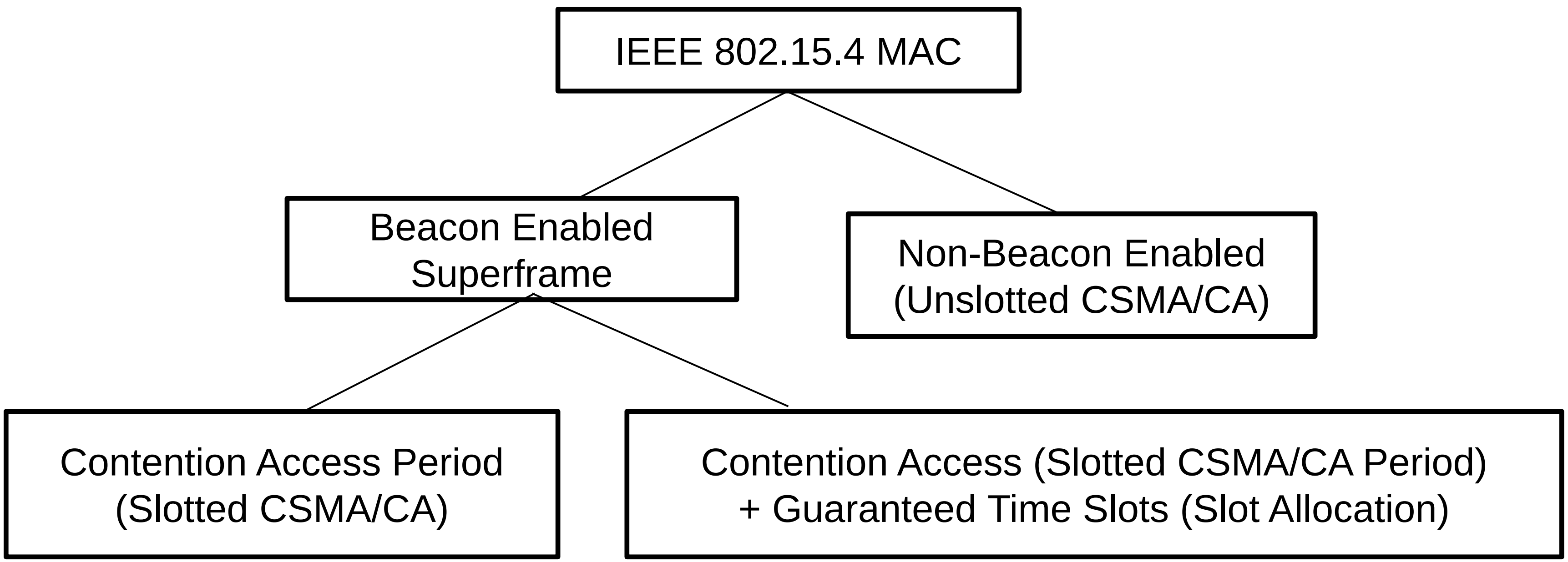
- Fully functional devices (FFD)
  - More resources
  - Multiple network responsibilities
- Reduced functionality devices (RFD)
  - Simple and low-cost device
  - Can only communicate with one FFD

MAC Layer features

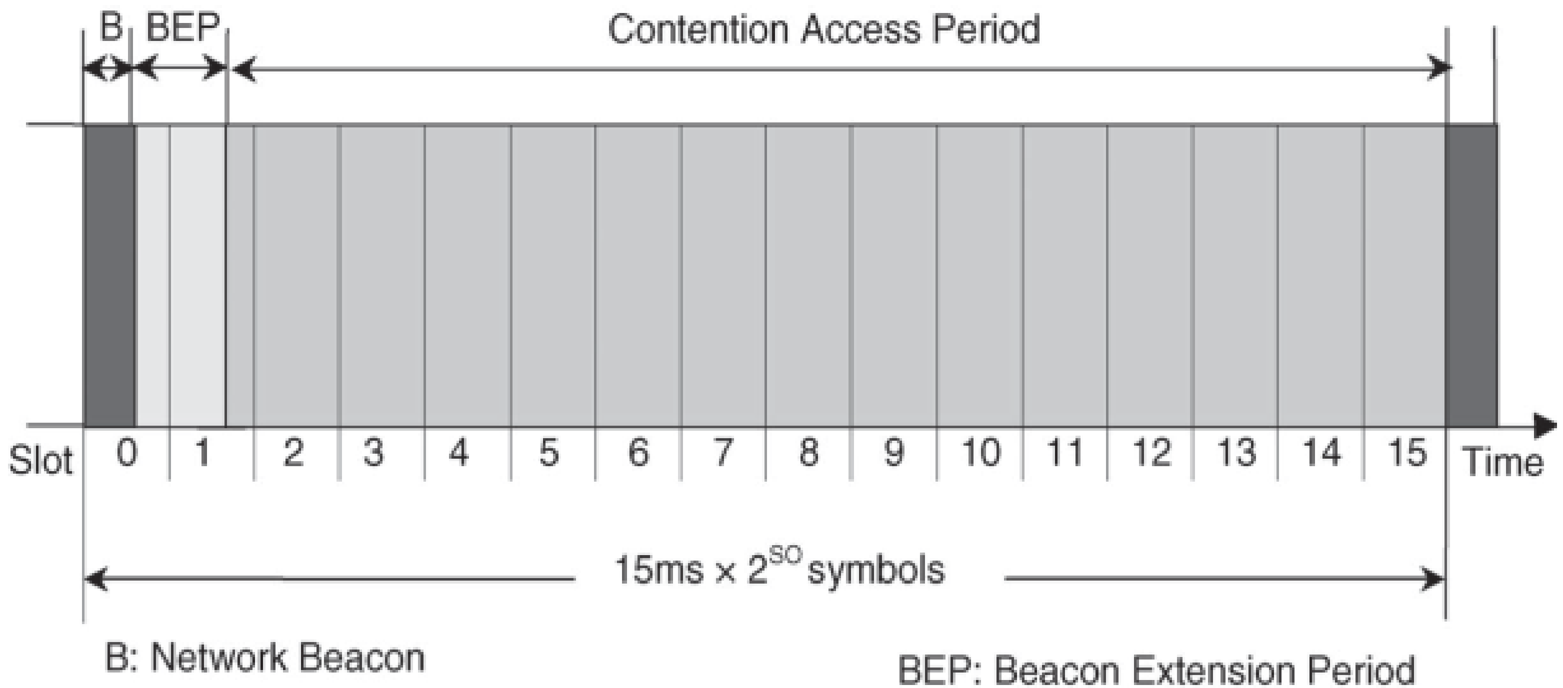
- Designed to support vast number of industrial and home applications for control and monitoring
- Enabling deployment of large number of devices with low cost and complexity
- Several features for flexible network configuration and low-power operation
  - Different topologies and network devices
  - Optional superframe structure with duty-cycle control
  - Both contention and scheduled based MAC protocols
  - Synchornized and non-synchronized operation
  - Efficient energy management
    - Adaptive sleep
    - Extended sleeping time
  - Flexible addressing scheme for large number of nodes

MAC layer functions

- Network association and disassociation
- Two modes of operation
  - Beaconing
  - Non-beaconing

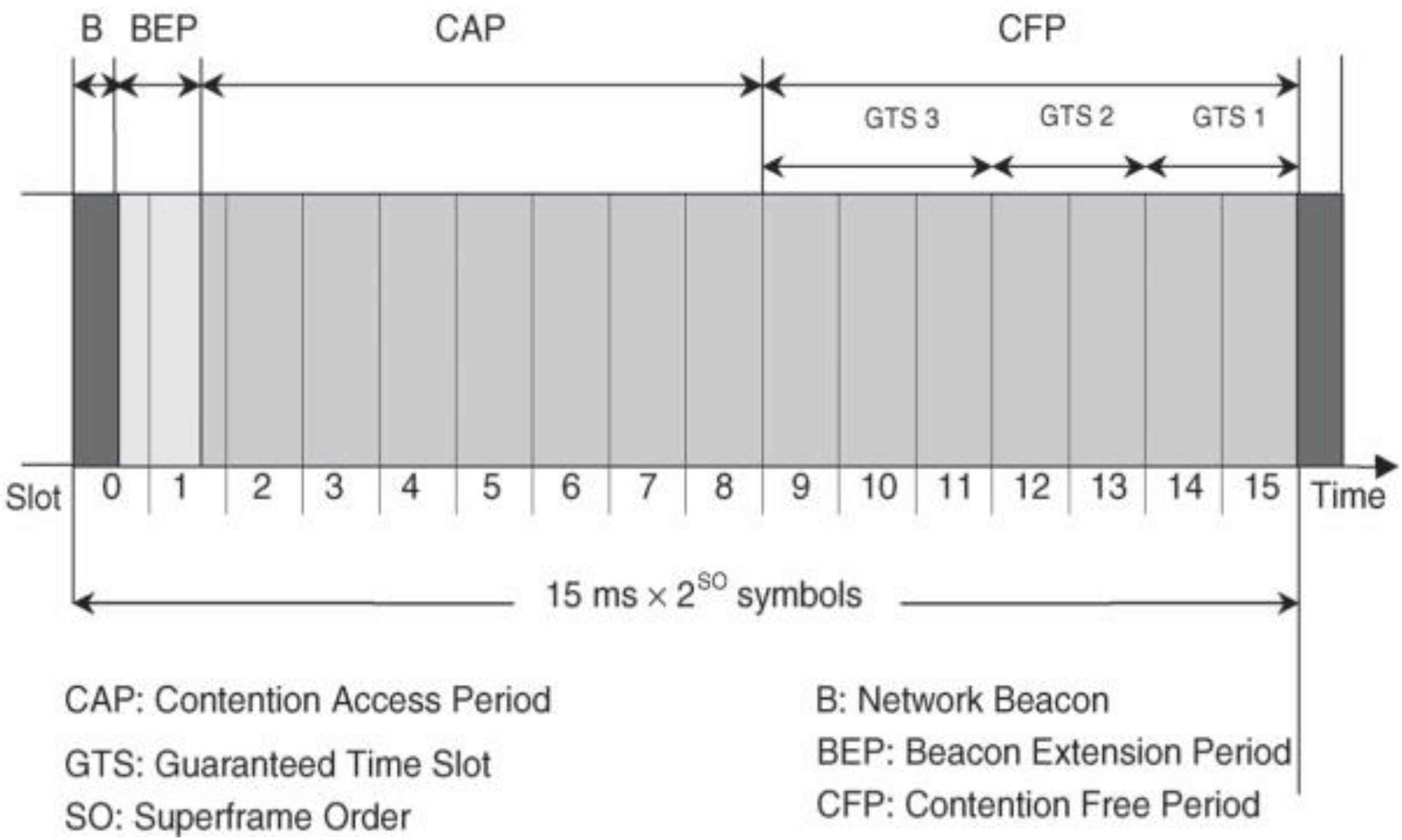


MAC: Superframe Structure



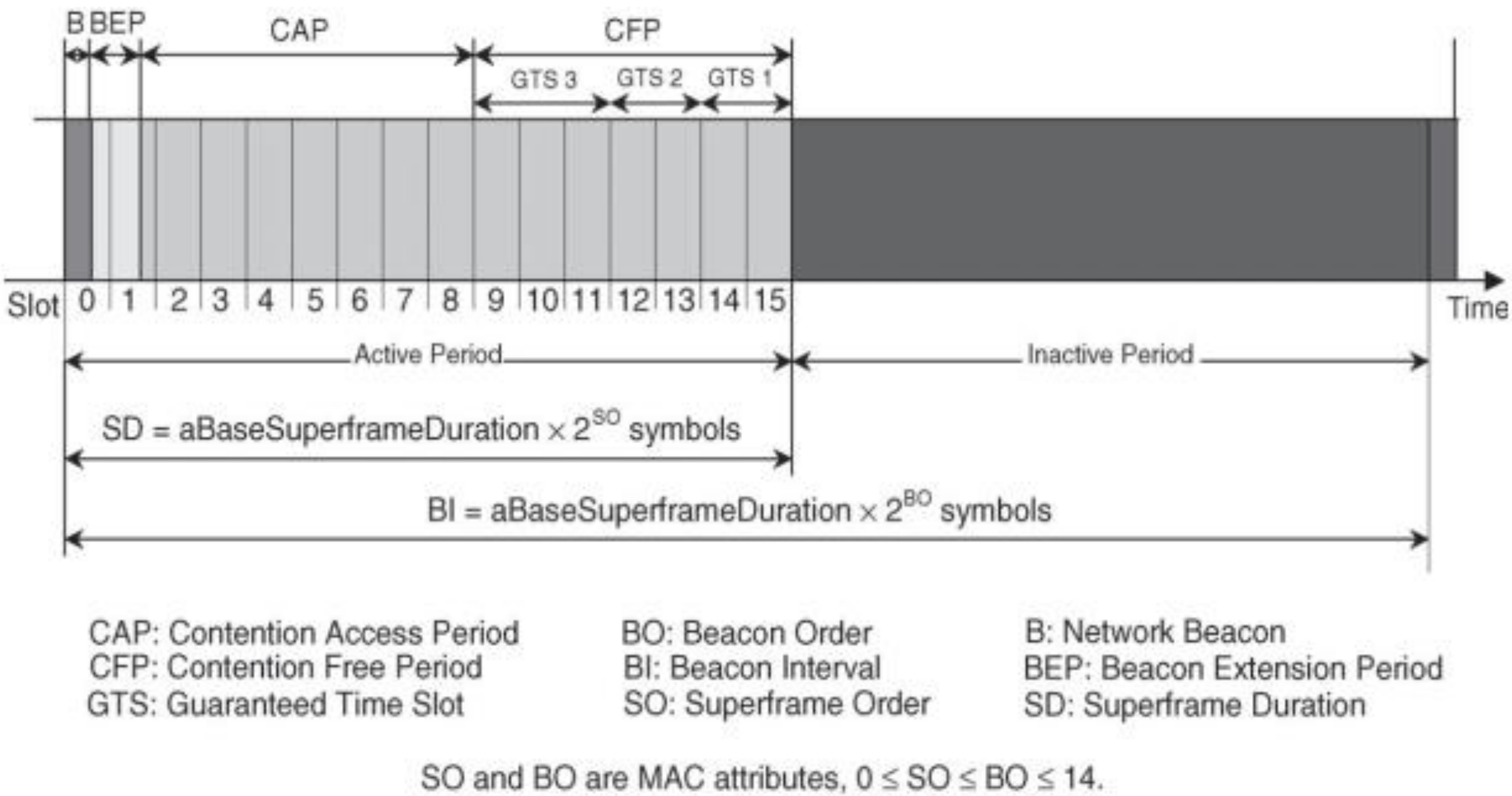
[Sohraby2007]

MAC: QoS Superframe Structure



[Sohraby2007]

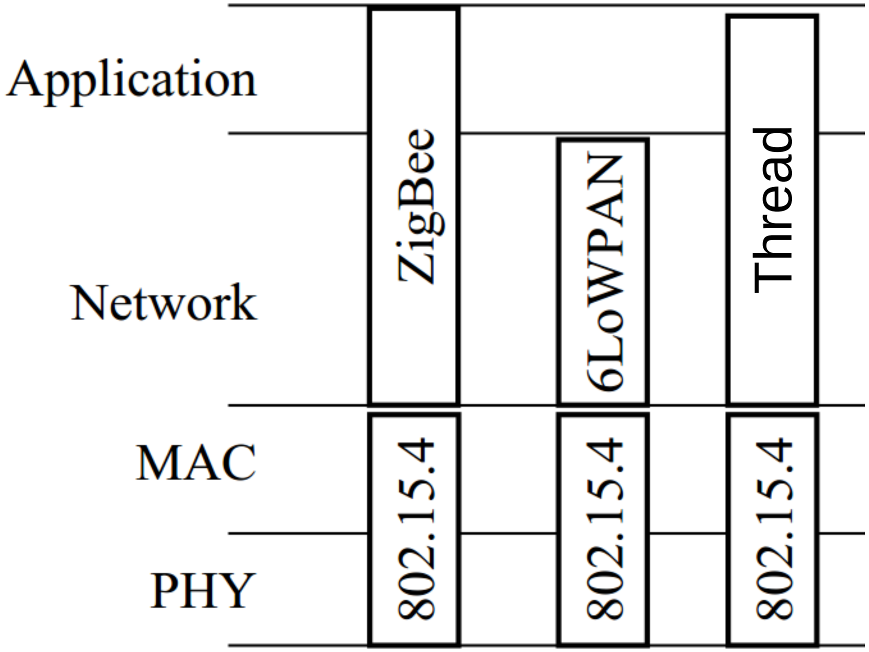
MAC: Superframe Structure with Energy Saving



[Sohraby2007]

802.15.4 only defines two layers

- Does not have IP address
- Used by several “Internet of Things” protocols
  - ZigBee, 6LowPAN, Thread



Zigbee IP

- Zigbee IP has been developed to enable full Internet connectivity of Zigbee devices using IPv6 protocol.
- Like the basic Zigbee specification, ZigBee IP builds on the IEEE standard 802.15.4. Essentially 802.15.4 provides the basic interface layers, while Zigbee IP provides the network and security layers and an application framework.
- ZigBee IP enables low-power devices to participate natively with other IPv6 enabled Ethernet, Wi-Fi and, HomePlug devices without the need for intermediate gateways.

Key IoT Features

Advantages

Source: Zigbee 3.0

- Low power
  - Zigbee (20 mJ per hour)
  - Zigbee Pro (Green Power: 20 microJ per hour)
- Large coverage of 1Km in Sub-GHz band
  - Even more for boosted modules (3.2 km for Xbee)
- Easy to install and maintain (mesh, self-healing, self-organization)
- Reliable (mesh, multiple channels, demonstrated interference tolerance, automated retransmissions)
- Supports thousands of nodes
- Low cost (many suppliers)
- Long battery life (years on AA battery)
- Secure (AES 128 bit)

Issues

- No mobility support, Scalability
- Less coverage area in 2.4 GHz band

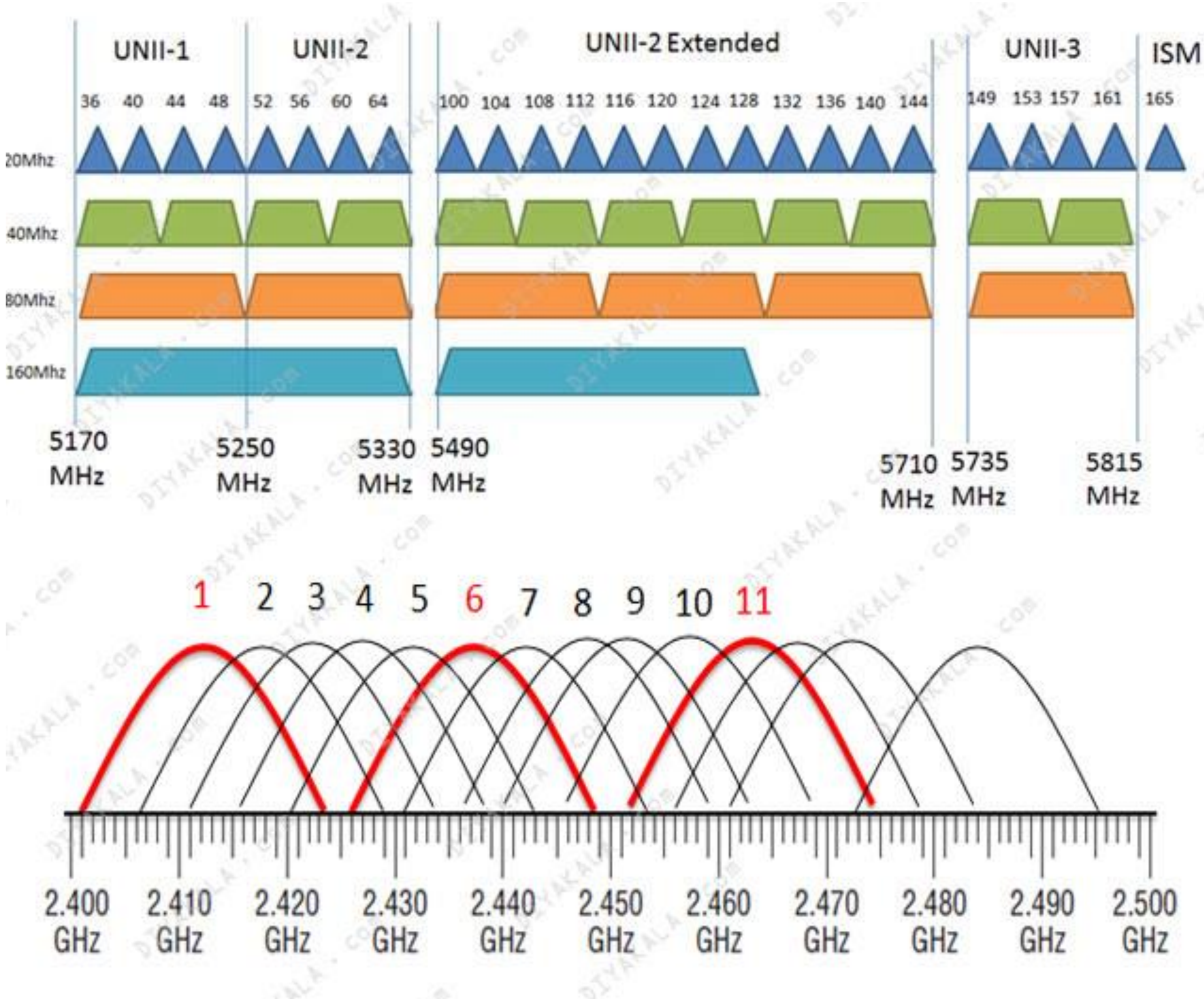
WiFi
(IEEE 802.11 family)

WLAN Standards

	2000	2004	2008 (4G)	2012	2016 (5G)	2020 (6G)
Standard	11b	11a/g	11n	11ac (wave1)	11ac (wave2)	11ax
MCS	Spread Spectrum	OFDM				OFDM (OFDMA)
Freq	2.4GHz	2.4GHz 5GHz				Same Freq (<7GHz)
Bandwidth	20MHz	20MHz	+40MHz	+80MHz	+160MHz	Same BW (+320M)
Multiple Antenna			MIMO Beamforming		MU-MIMO (DL)	MU-MIMO (UL)
PHY Rate	11Mbps	54Mbps	600Mbps (40M,4SS)	1.7Gbps (80M,4SS)	6.7Gbps (160M,8SS)	9.6GHz (160M,8SS)
MAC	CSMA/CA in DCF	Security QoS	Aggregation			BSS Management

https://www.wlanpedia.org/tech/overview/wlan-standard-in-ieee802-11/

WLAN Bandwidths



https://commons.wikimedia.org/wiki/File:Frequency-bandwitch-wifi-camera-wireless-camera.jpg

802.11ac (5G of WiFi) and 802.11ah (WiFi-Halow)

	802.11ac	802.11ah
Operating Bands	2.4 and 5 GHz	Sub 1-GHz
Spectrum available	100 + 150 MHz	26 MHz
Use Cases	Broadband wireless	Sensors and Meters Extended WiFi
Data Rate Requirement	20 Mbps - 3 Gbps	100 Kbps
Single Frame Size	Large (e.g., 1500 bytes)	Small (e.g., 100 bytes)
Traffic type	Video Streaming/ Large file transfer	Periodic packet transmission every few to tens minutes
Distance between devices	Up to 60 m	Up to 1 Km
Number of stations	3-20	8191
Location	Mostly indoor	Indoor and outdoor
Backward compatibility	Yes	No

[Park2015, Gonzalvez2016]

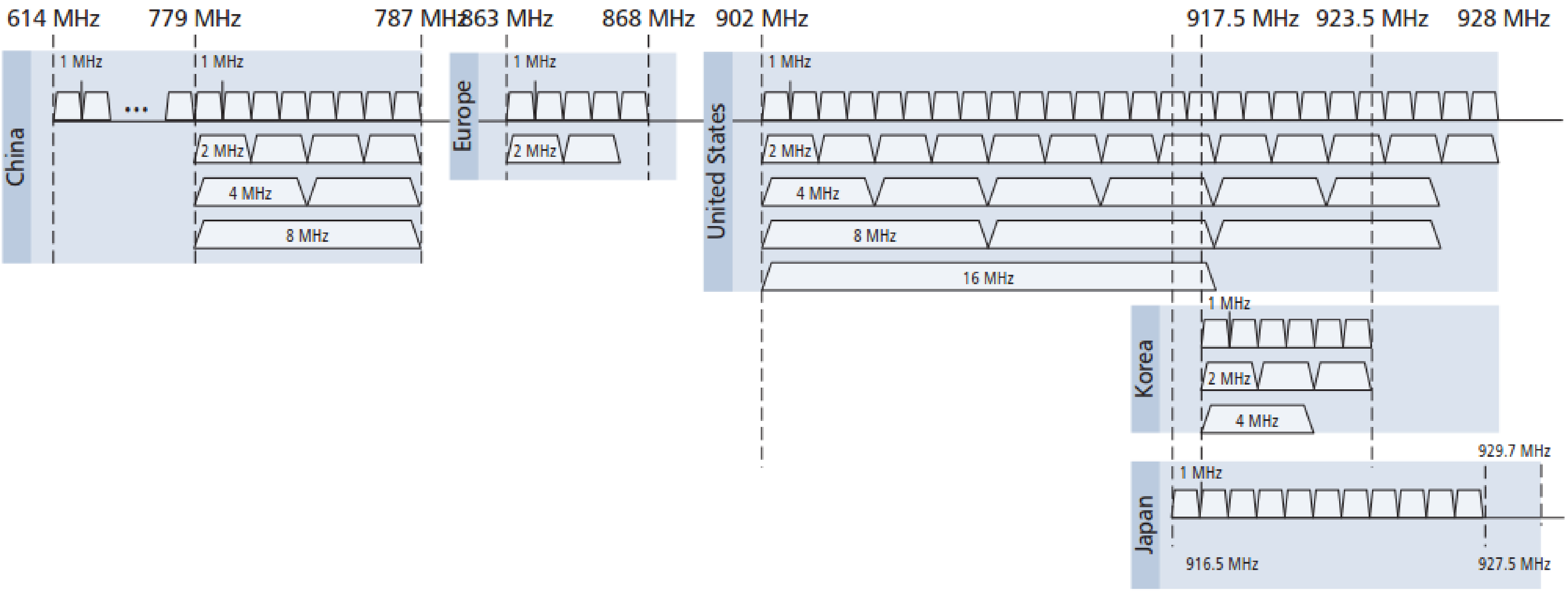
PHY parameters for 802.11ah

- Use of orthogonal frequency division multiplexing (OFDM)
- Basically adapted a scaled-down version of 802.11ac
  - Bandwidths of 20-160 MHz to 2-16 MHz
  - Same number of subcarrier
  - Increased symbol duration

[Park2015]

Parameters	Supported Values
Channel Bandwidthds	2, 4, 8, and 16 MHz
Modulation Schemes	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Code Rates	1/2 with 2 times repetition 1/2 , 2/3, 3/4 and 5/6 Convolution or low-density parity check (LDPC)
MIMO	Support up to 4 by 4
Data Rates	150 Kbps (1 MHz bandwidth, 1 spatial stream, BPSK, ½ coding rate, repetition) to 347 Mbps (16 MHz bandwidth, 4 spatial streams, 256 QAM, 5/6 coding rate)

Frequency Bands in Different Countries



[Park2015]

Link Budget Comparison

Parameters	Link budget enhancements of 900 MHz 802.11ah over 2.4 GHz 802.11n
Free space path loss	+8.5 dB
Noise bandwidth	+10 dB
Sub-total link budget gain	+18.5 dB
1 MHz channel width	+3 dB
Repetition coding	+3 dB
Total link budget gain	+24.5 dB

[Park2015]

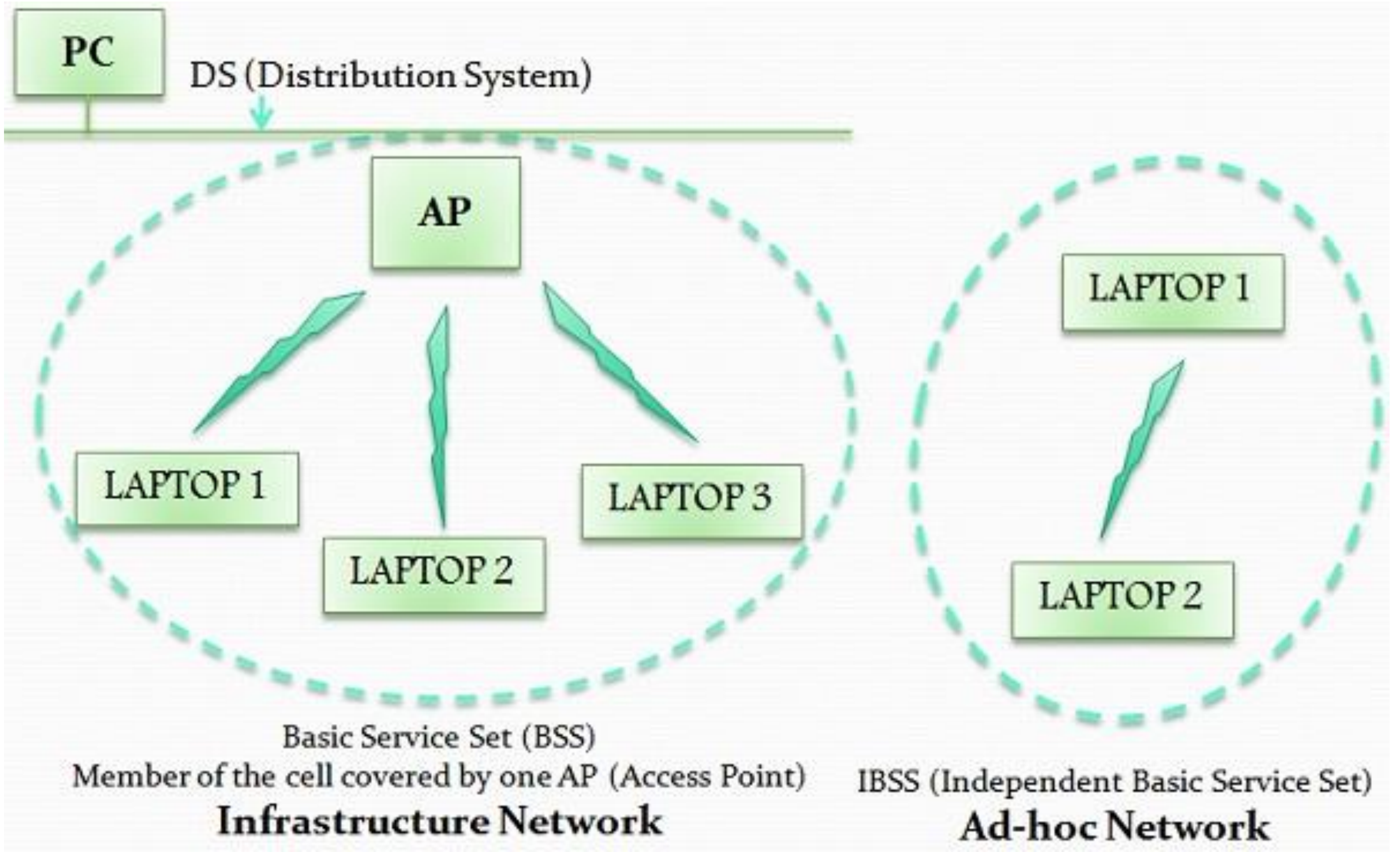
Low Power and Low Cost Support for Indoor Sensors:
This can reduce the transmit energy consumption and also lower the cost of an 802.11ah radio of a small sensor device.

IEEE 802.11 Network Topologies

Nodes as stations and cluster head as access point

- Basic service set (BSS) or Star
- Extended service set (ESS) or cluster tree
- Independent basic service set (IBSS)
  - Ad-hoc = Mesh without access point
- Mesh basic service set (MBSS)
  - (wired or wireless) Mesh of cluster heads (Hybrid)

IEEE 802.11 Network Topologies



https://techdifferences.com/difference-between-bluetooth-and-wifi.html

802.11ah MAC features

- Hierarchical association identifier
- Access scheme: Hybrid Coordination Function (HCF)
- Optional Restricted Access Window (RAW)
- Increased sleep time
- Target wake-up time
- Bidirectional transmission opportunity
- Short MAC frame
- Null data packet for ACK
- Synchronization frame operation
- And few more!

Increased Sleep Time

- In 802.11, the max sleep time is 18 hours without getting disassociated with the AP
- For 802.11ah, the max sleep time is redefined such that the station can sleep for approximately 5.2 years

Target Wakeup Time (TWT)

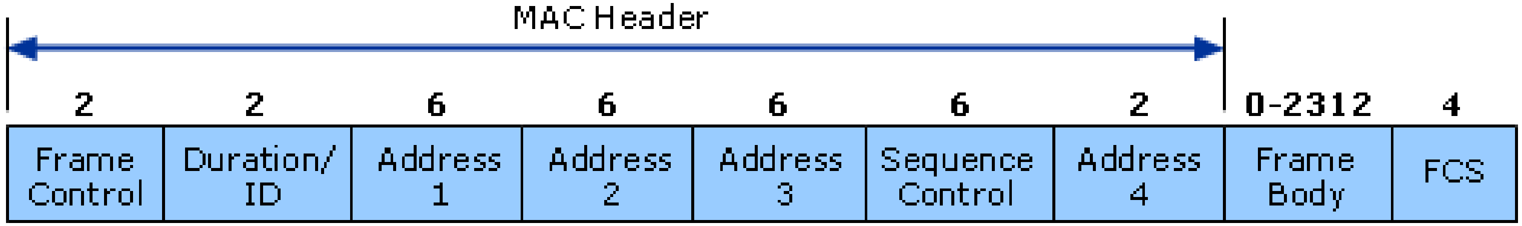
- 802.11
  - An AP buffers data destined for a station while the station is in sleep state
  - The station periodically wakes up at beacon transmission times and receives a beacon to see if there is any buffered data at the AP based on the information in traffic indication map (TIM)
  - If TIM indicates that there is data buffered at AP, it sends a PS-Poll frame to the AP to indicate the station is awake and is ready to receive the buffered data
  - The AP needs time to find the buffered data and has to contend for the medium: this indefinite latency makes the station consume energy waiting for the buffered data
- 802.11ah
  - Uses target wake-up time between an AP and a station so that the AP knows when the station will be awake
  - Removes the processing time and medium access latency

Bidirectional Transmission Opportunity

- Bidirectional transmission (BDT) allows an AP and a station to exchange one or more uplink and downlink packets in one TXOP.
- Packets are separated by short inter frame space (SIFS)
- In the BDT procedure, a station uses the More Data bit in the SIGNAL field of PHY preamble of a packet to indicate whether the station has more data to transmit following the current packet transmission.
- This reduces the number of contention-based channel accesses, improves channel efficiency by minimizing the number of frame exchanges required for uplink and downlink data frames, and enables stations to extend battery lifetime by keeping Awake-times short.

Short MAC Frame

- In 802.11n, the MAC header can be 30 bytes long



https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx

- For IoT application transmitting only 50 bytes of data infrequently, this is big overhead
- In 802.11ah, the length of header is reduced to 12 bytes

802.11ax (6G of WiFi)

- Convergence of high data rates and IoT applications
- Smarter access points for improved outdoor coverage with longer guard intervals
- Target Wake-up Time
- BSS coloring to reduce interference
- Only on 5 GHz
- Comparison with 802.11ac
  - 6 times speed, 7 times battery life with TWT, 4 times range
  - Support much more than 7 devices
- OFDMA instead of OFDM
- MU-MIMO
- 1024 QAM and 160 MHz bandwidth to give multi-giga bit data rates

Key IoT Features (802.11ah)

- High data rates
  - Can handle diverse range of applications including camera
- Longer range
- Scalable to thousands of nodes
- Widely used

Issues

- Most of the world is using 2.4 GHz
  - Problem for 802.11ah
  - Problem for 802.11ax
- 802.11ah available, but products are hardly there
  - Mostly using 802.11b/g/n
- Security
- High power consumption
- Roaming

Bluetooth Low Energy (BLE)

Bluetooth (IEEE 802.15.1 family) Versions

- Maintained by Bluetooth SIG
- **Bluetooth v1.2**
  - The v1.x releases laid the groundwork for future versions
  - Bluetooth v1.2 was the latest and most stable 1.x version.
  - Supported data rates of up to 1 Mbps (**Basic Rate (BR)**) using GFSK
  - 10 meter maximum range.
- **Bluetooth v2.1 + Enhanced Data Rate (EDR)**
  - The 2.x versions of Bluetooth introduced **enhanced data rate (EDR)**,
  - Data rates up to 3 Mbps using pi/4 QPSK and 8 DPSK
  - **Secure simple pairing (SSP)**
- **Bluetooth v3.0 + High Speed (HS)**
  - 24 Mbps speed with WiFi offloading in “+HS” versions
- **Bluetooth v4.0, v4.1, v4.2**
- **Bluetooth v5.0 Specifications launched in Dec. 2016**
  - 2 * data rate, 4 * range of BLE, 8 * broadcasting capacity
  - Backward compatible with classic as well as BLE

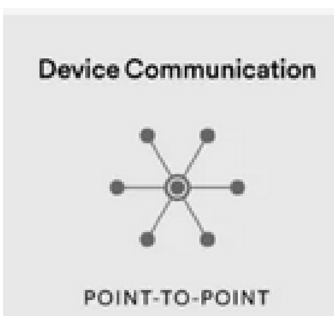
Bluetooth 4.0 and BLE

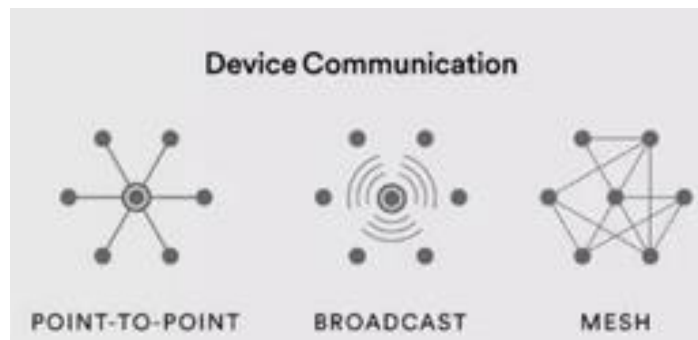
- **Bluetooth v4.0 and Bluetooth Low Energy**
  - Bluetooth 4.0 split the Bluetooth specification into three categories: **classic, high-speed,** and **low-energy**. Classic and high speed are backward compatible to Bluetooth versions v2.1+EDR and v3.0+HS respectively.
  - BLE is **Bluetooth Smart**
  - BLE + v4.0 classic is Bluetooth Smart Ready (can connect to both classic as well BLE)
- **Bluetooth low energy (BLE)**
  - BLE is a massive overhaul of the Bluetooth specifications, aimed at very low power applications. It sacrifices range (50m instead of 100m) and data throughput (0.27 Mbps instead of 0.7-2.1 Mbps) for a significant savings in power consumption.
  - Cannot carry voice. Only suited for intermittent data transmissions (no continuous data transmission)
  - Not backward compatible with Bluetooth classic
- **Bluetooth Mesh (2017)**

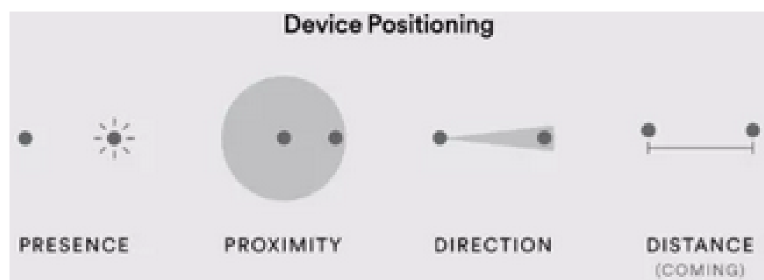
Comparison


Bluetooth® Classic
Solution Areas
AUDIO STREAMING
DATA TRANSFER


Bluetooth® Low Energy
Solution Areas
AUDIO STREAMING
DATA TRANSFER
LOCATION SERVICES
DEVICE NETWORKS


Device Communication
POINT-TO-POINT


Device Communication
POINT-TO-POINT
BROADCAST
MESH

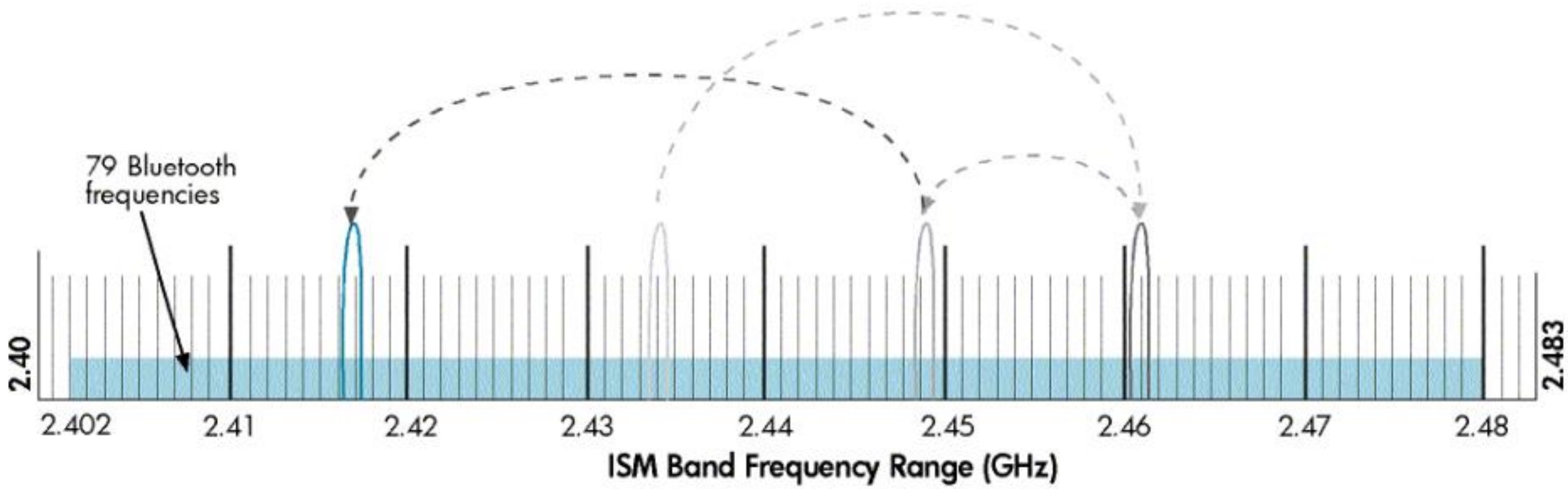

Device Positioning
PRESENCE
PROXIMITY
DIRECTION
DISTANCE
(COMING)

	Bluetooth Low Energy (LE)	Bluetooth Classic
Frequency Band	2.4GHz ISM Band (2.402 – 2.480 GHz Utilized)	2.4GHz ISM Band (2.402 – 2.480 GHz Utilized)
Channels	40 channels with 2 MHz spacing (3 advertising channels/37 data channels)	79 channels with 1 MHz spacing
Channel Usage	Frequency-Hopping Spread Spectrum (FHSS)	Frequency-Hopping Spread Spectrum (FHSS)
Modulation	GFSK	GFSK, π/4 DQPSK, 8DPSK
Data Rate	LE 2M PHY: 2 Mb/s LE 1M PHY: 1 Mb/s LE Coded PHY (S=2): 500 Kb/s LE Coded PHY (S=8): 125 Kb/s	EDR PHY (8DPSK): 3 Mb/s EDR PHY (π/4 DQPSK): 2 Mb/s BR PHY (GFSK): 1 Mb/s
Tx Power*	≤ 100 mW (+20 dBm)	≤ 100 mW (+20 dBm)
Rx Sensitivity	LE 2M PHY: ≤-70 dBm LE 1M PHY: ≤-70 dBm LE Coded PHY (S=2): ≤-75 dBm LE Coded PHY (S=8): ≤-82 dBm	≤-70 dBm
Data Transports	Asynchronous Connection-oriented Isochronous Connection-oriented Asynchronous Connectionless Synchronous Connectionless Isochronous Connectionless	Asynchronous Connection-oriented Synchronous Connection-oriented
Communication Topologies	Point-to-Point (including piconet) Broadcast Mesh	Point-to-Point (including piconet)
Positioning Features	Presence (Advertising) Proximity (RSSI) Direction (AoA/AoD) Distance (Coming)	None

https://www.bluetooth.com/bluetooth-technology/radio-versions

Frequency Hopping (Bluetooth)

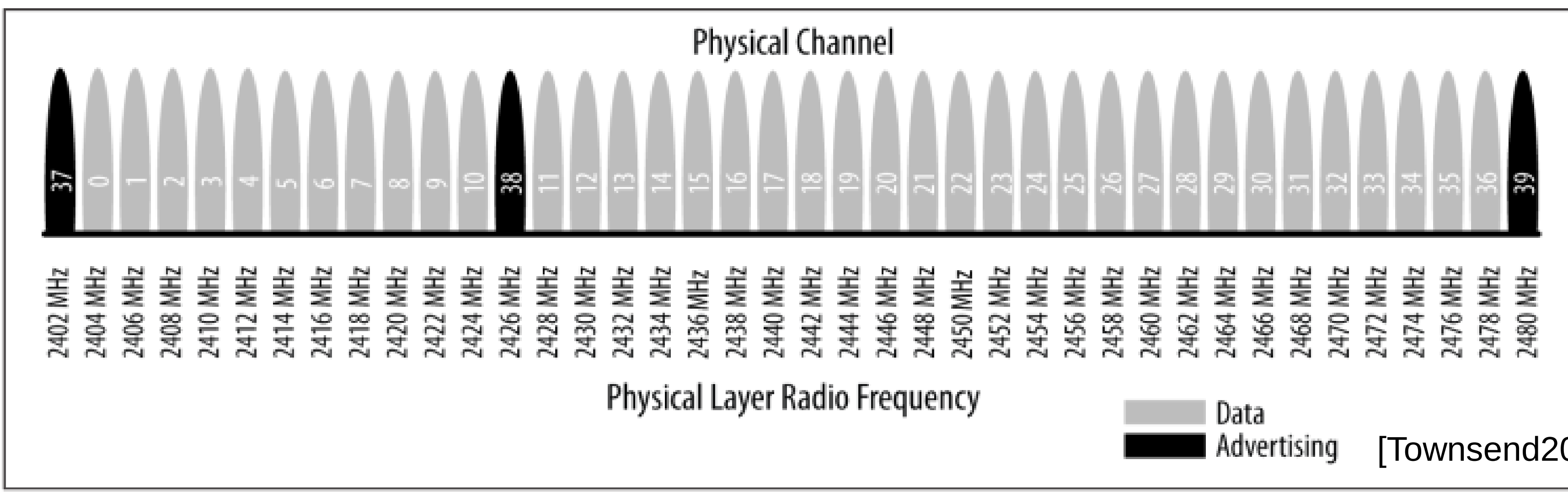
- Bluetooth devices hop between frequencies up to 1600 times per second or every slot of 625 microsecs
- This is primarily to minimize eavesdropping and interference from other networks that use the 2.4 GHz ISM bands
- The transmitter and receiver exchange a data packet at one frequency, and then they hop to another frequency to exchange another packet. They repeat this process until all the data is transmitted



http://h10032.www1.hp.com/ctg/Manual/c00186949.pdf

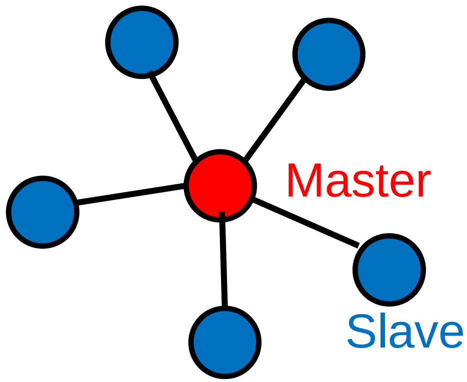
PHY Channels

- BLE operates in 2.4 GHz ISM band
  - In US, Europe, and rest of the world: 2.4 to 2.4835 GHz
  - Japan: 2.471 to 2.497 GHz
  - Spain: 2.445 to 2.475 GHz
  - France: 2.4465 to 2.4835 GHz
- BLE uses 40 channels of 2 MHz each
  - Channels are used for connection data and the last three channels (37-39) are used as advertising channels to set up connections and send broadcast data
  - Adaptive frequency hopping to avoid interference

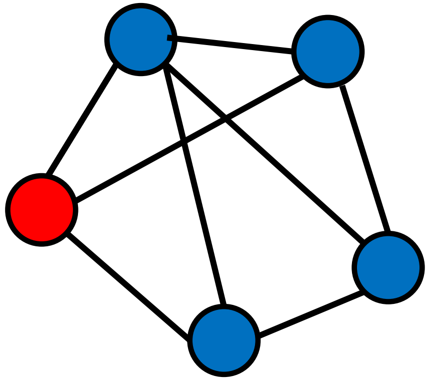


[Townsend2014]

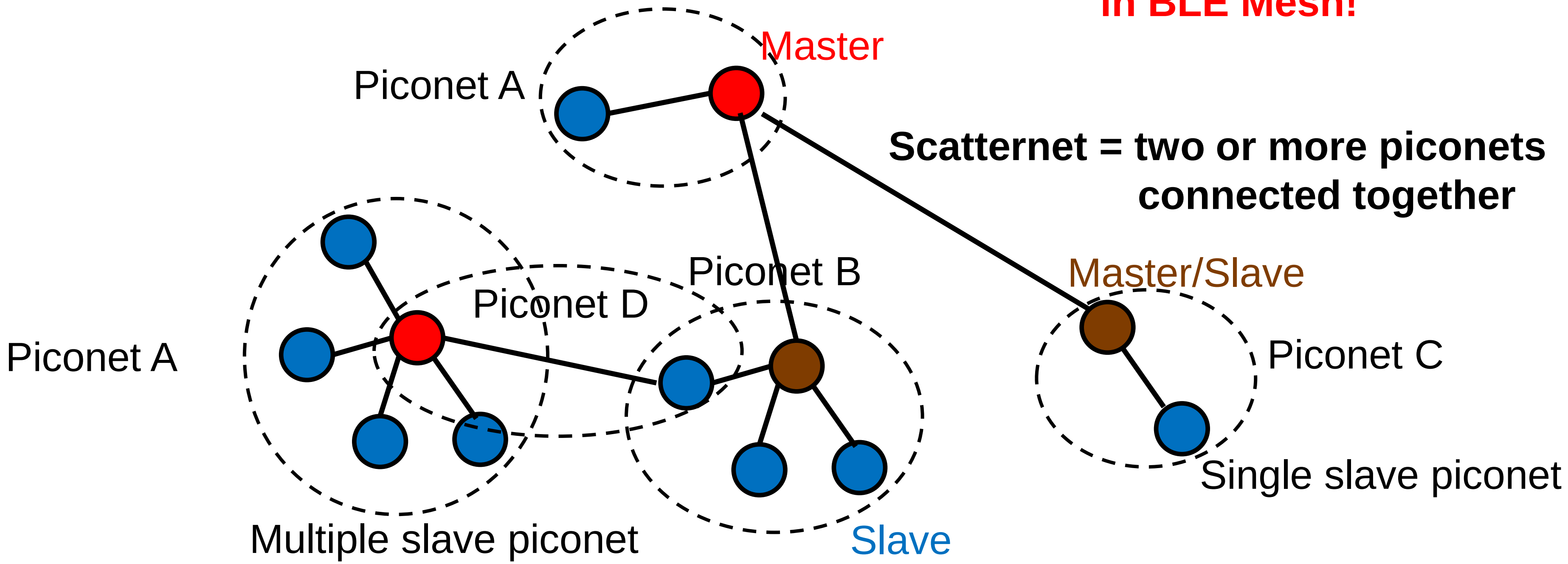
Network Topologies: Piconet and Scatternet



Piconet (Star)



Mesh now possible in BLE Mesh!



Scatternet = two or more piconets connected together

Key IoT features

Advantages

- Low power: years on button battery
- Small size and low cost
- Ubiquitous: most smartphones and tablets
- Security: AES 128 bit

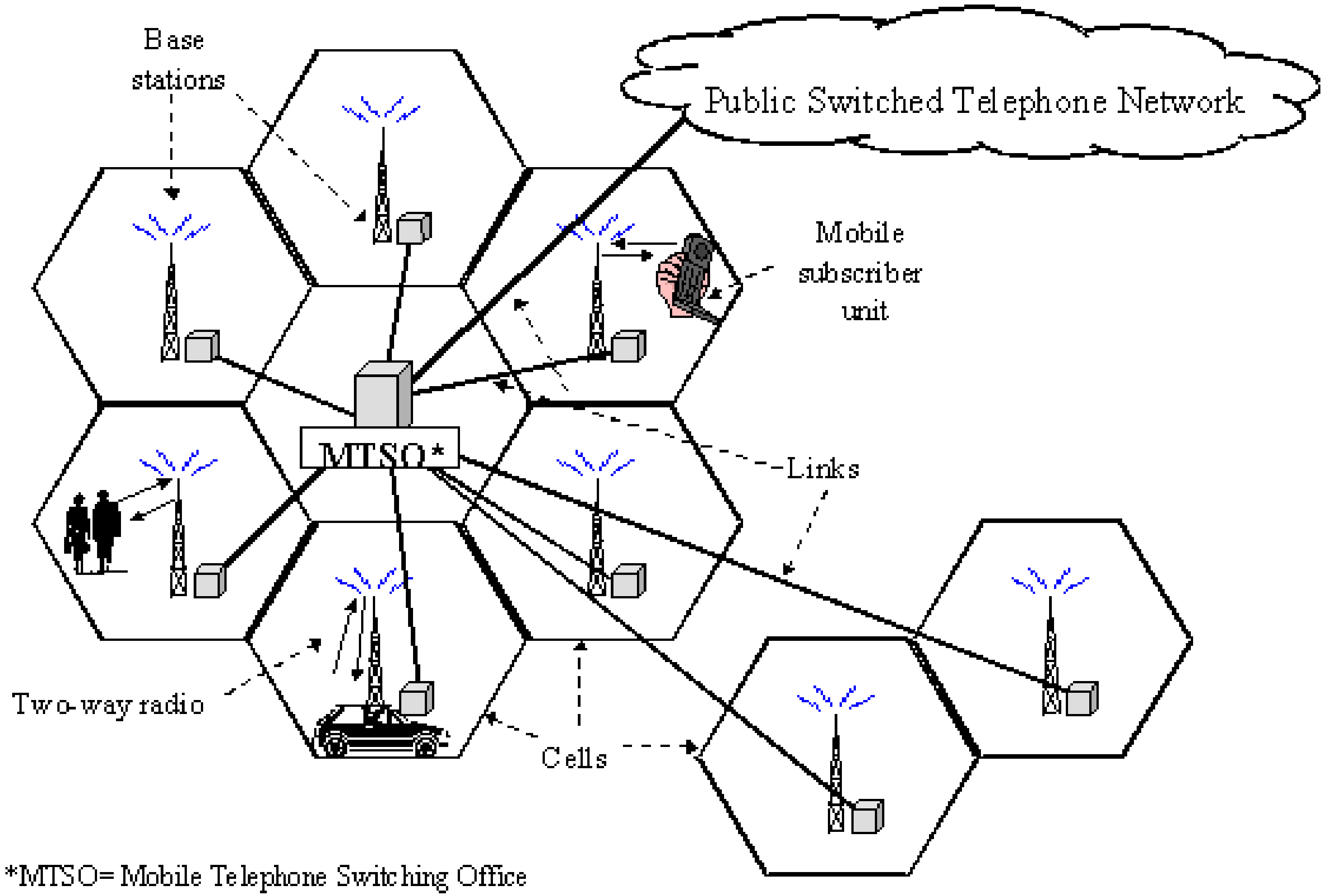
Issues

- Low range
- Low data rates: No voice or video capability
- Roaming

Cellular Technologies: 2G, 3G, 4G, 5G

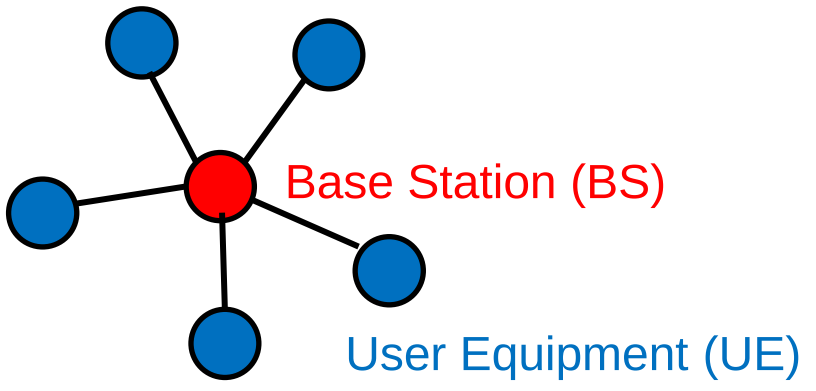
Cellular Architecture: an example of 2G

https://www.itu.int/osg/spu/ni/3G/technology/index.html



Good introduction to cellular communication: https://www.youtube.com/watch?v=1JZG9x_VOwA

Network Topologies: Star



Cat-1, Cat-0, eMTC, NB-IoT and EC-GSM-IoT

	LTE Cat 1	LTE Cat 0	LTE Cat M1 (eMTC)	LTE Cat NB1 (NB-IoT)	EC-GSM-IoT
3GPP Release	Release 8	Release 12	Release 13	Release 13	Release 13
Downlink Peak Rate	10 Mbit/s	1 Mbit/s	1 Mbit/s	250 kbit/s	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Uplink Peak Rate	5 Mbit/s	1 Mbit/s	1 Mbit/s	250 kbit/s (multi-tone) 20 kbit/s (single-tone)	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Latency	50–100ms	not deployed	10ms–15ms	1.6s–10s	700ms–2s
Number of Antennas	2	1	1	1	1–2
Duplex Mode	Full Duplex	Full or Half Duplex	Full or Half Duplex	Half Duplex	Half Duplex
Device Receive Bandwidth	1.08 – 18 MHz	1.08 – 18 MHz	1.08 MHz	180 kHz	200 kHz
Receiver Chains	2 (MIMO)	1 (SISO)	1 (SISO)	1 (SISO)	1–2
Device Transmit Power	23 dBm	23 dBm	20 / 23 dBm	20 / 23 dBm	23 / 33 dBm

LTE-M and NB-IoT enhanced in Release 14

http://www.3gpp.org/images/articleimages/iot_summary_large.jpg

Cat-1, Cat-0, eMTC, NB-IoT and EC-GSM-IoT

- Cat-1
  - IoT support in LTE 3G (Release 8)
  - Already standardized
  - Premium IoT applications

- Cat-0
  - IoT support in LTE-A 4G (Release 12)
  - Optimized cost as compared to Cat-1

- EC-GSM
  - IoT support in GSM networks
  - Extended Coverage

Cat-M1 (eMTC)

- IoT support in LTE-A 4G (Release 13)
- Compatible with existing LTE network (only software upgrade)
- 1.4 MHz bandwidth
- Supports mobility and voice-over LTE (VoLTE)
- Asset tracking and wearables

NB-IoT or Cat-M2

- Competing against Sigfox, LoRa (Release 13)
- Support of massive number of low throughput devices, ultra-low device cost, low device power consumption and optimized network architecture
- Improved indoor coverage
  - Power boosting
  - Repetition
- flexible spectrum: in-band and guard band in LTE; standalone deployment; GSM re-farming possible
- Not backward compatible with other 3G/4G devices
- No mobility support and not suitable for latency low applications
- LPWAN applications like smart metering

NB-IoT deployment

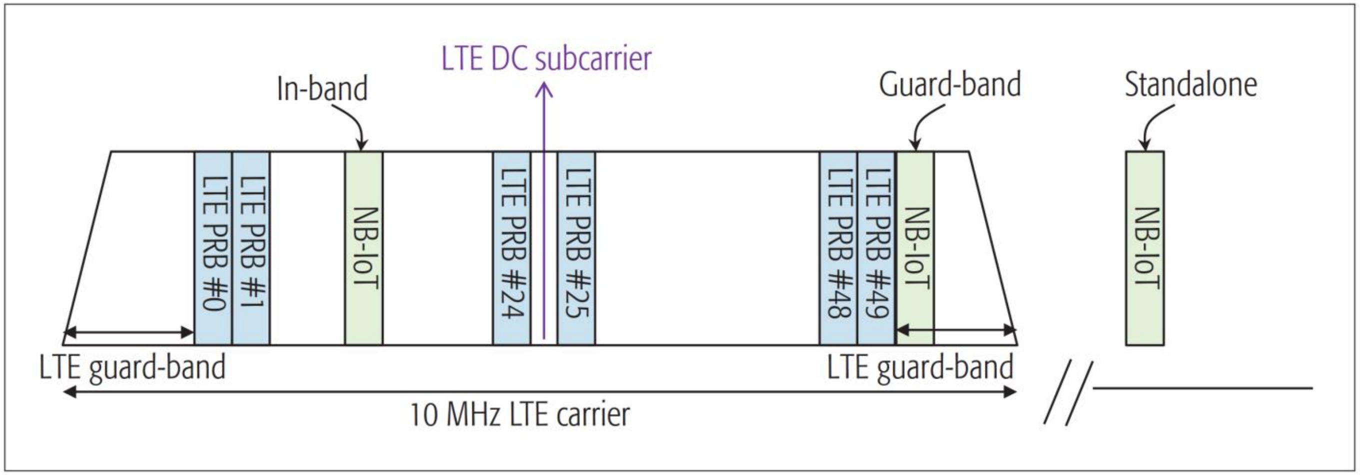


Figure 1. Examples of NB-IoT stand-alone deployment and LTE in-band and guard-band deployments.

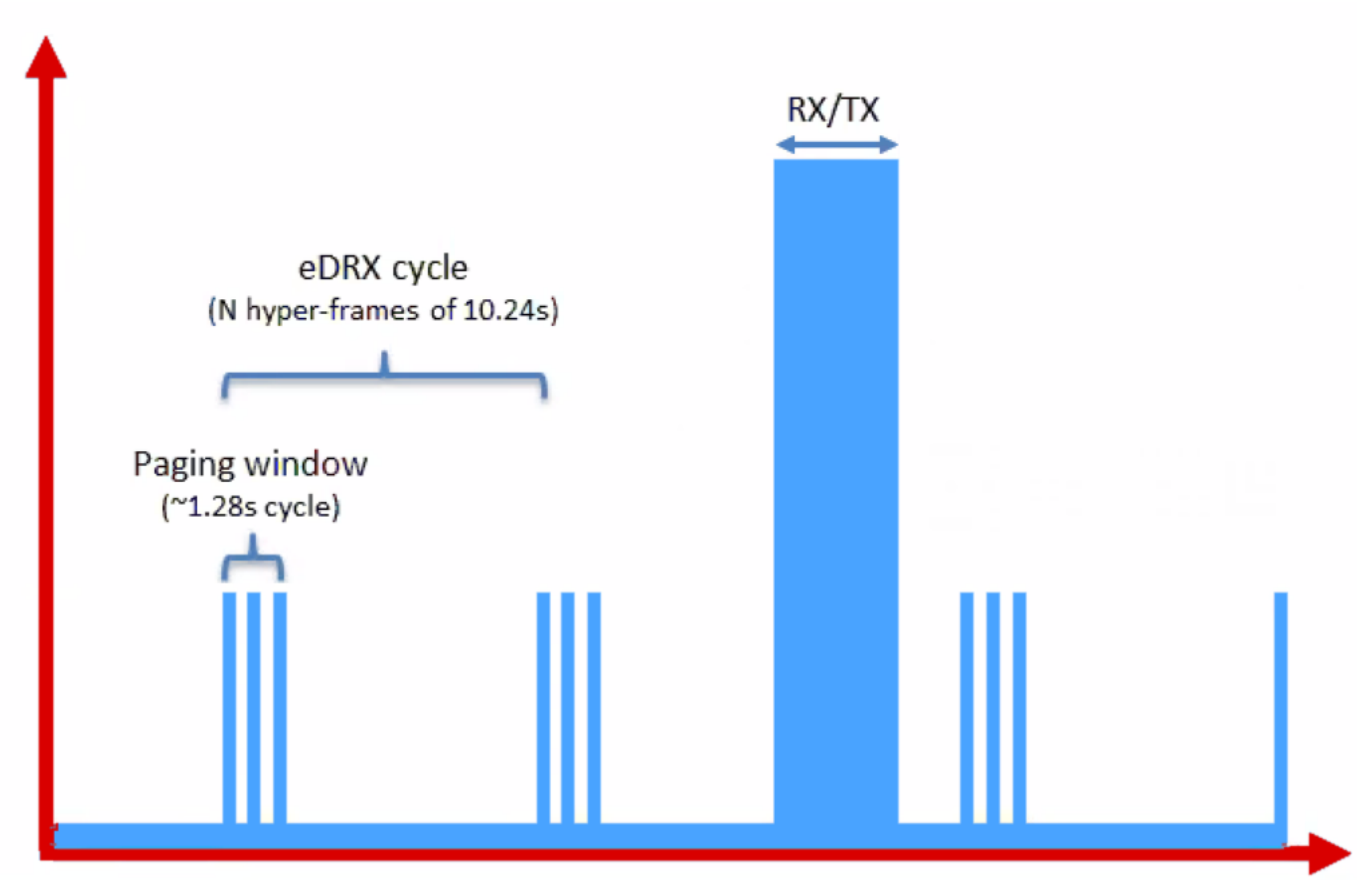
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7876968

Major Changes

- Ultra-low complexities
  - Half-duplex 1 receiver chain
  - Reduced peak data rates
  - Using simple modulation and coding
- Improved indoor coverage
  - Repetition
  - PSD boosting
- Support of massive number of devices
- Improved power efficiency
  - Power saving mode
  - Extended discontinuous reception

Extended Discountinous Reception (eDRX)

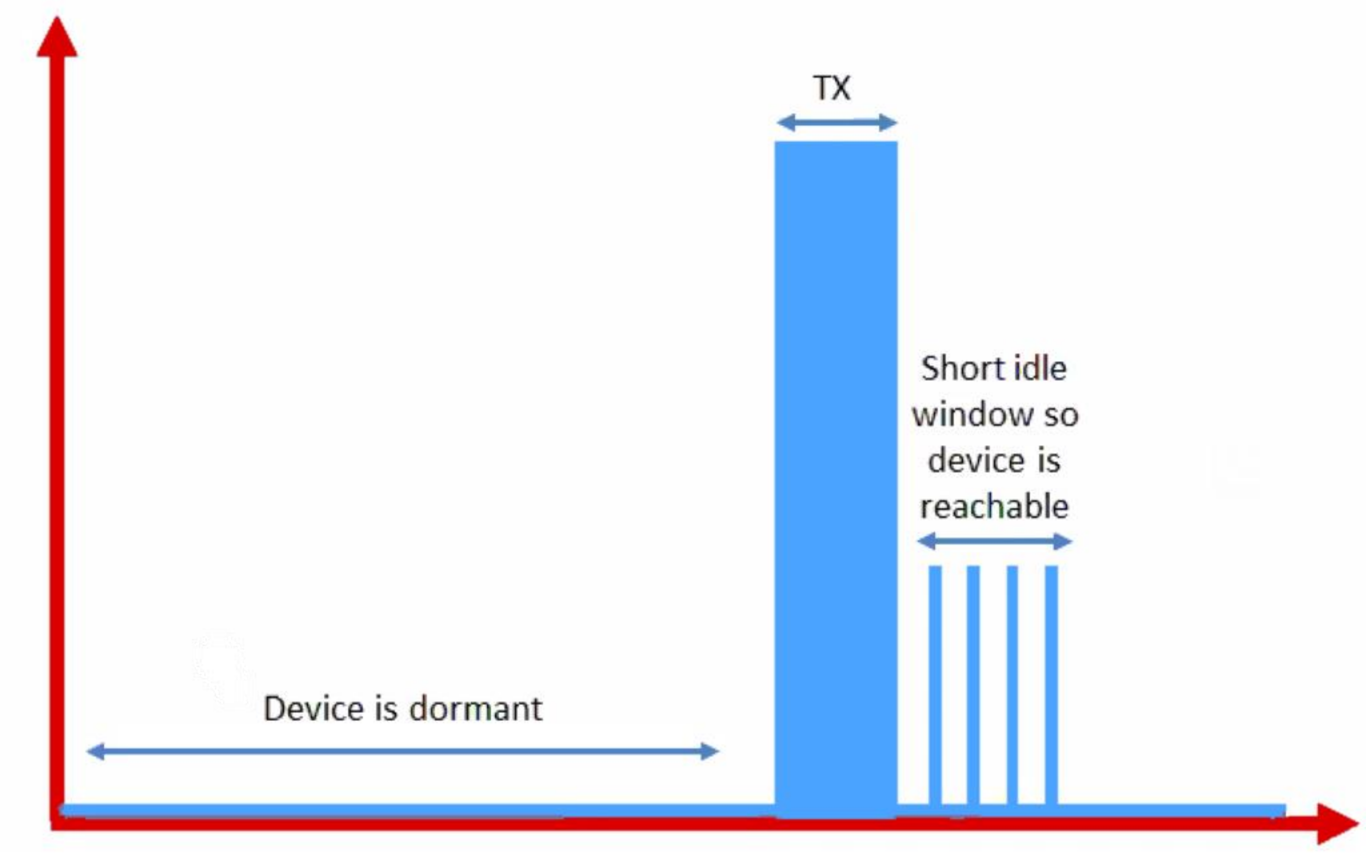
Node can skip several paging cycles



https://www.link-labs.com/blog/lte-e-drx-psm-explained-for-lte-m1

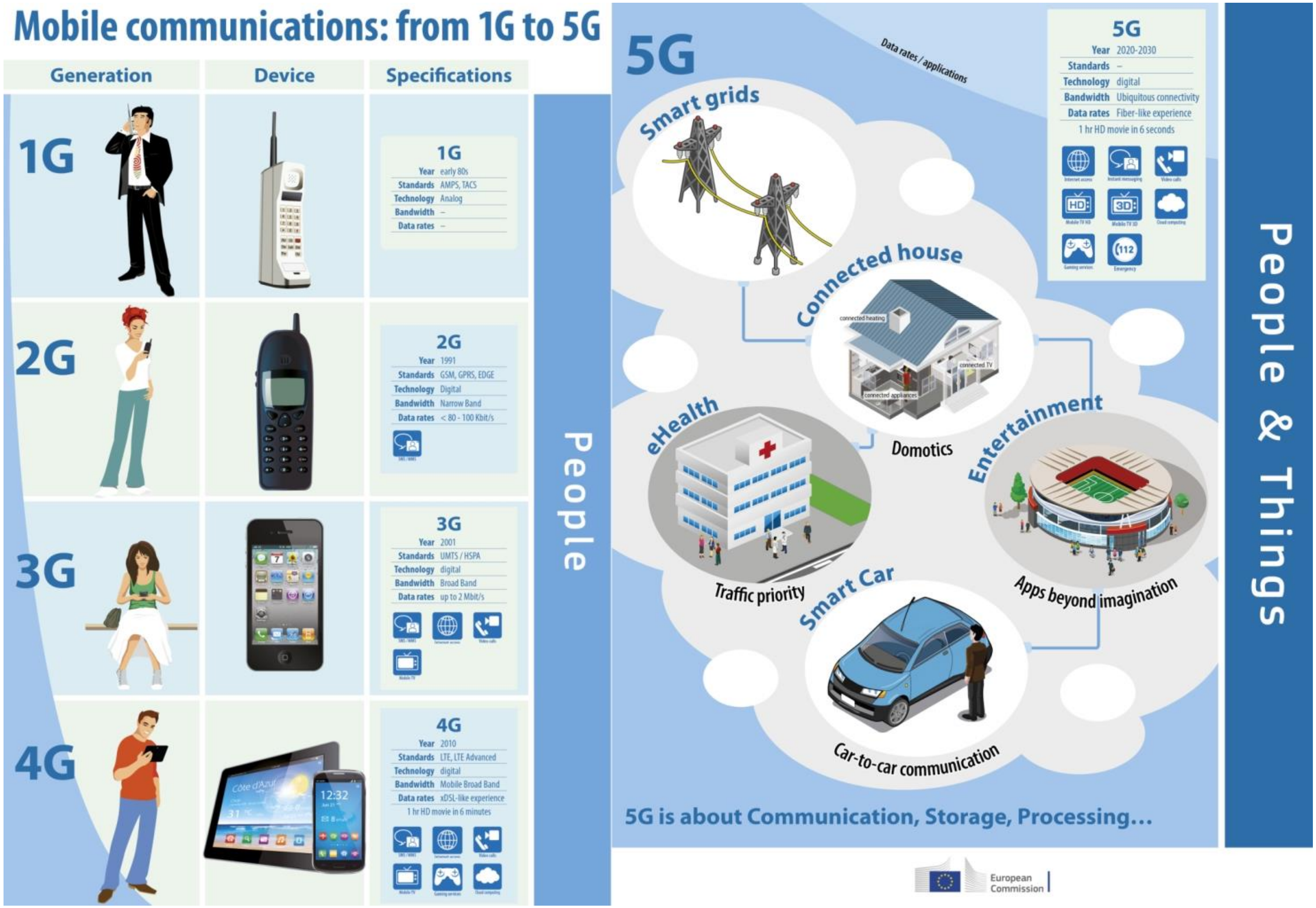
Power Saving Mode

PSM allows LTE-M devices to go idle without having to re-join the network when they wake up.



https://www.link-labs.com/blog/lte-e-drx-psm-explained-for-lte-m1

1G to 5G



https://www.ng-voice.com/the-evolution-of-wireless-generations/

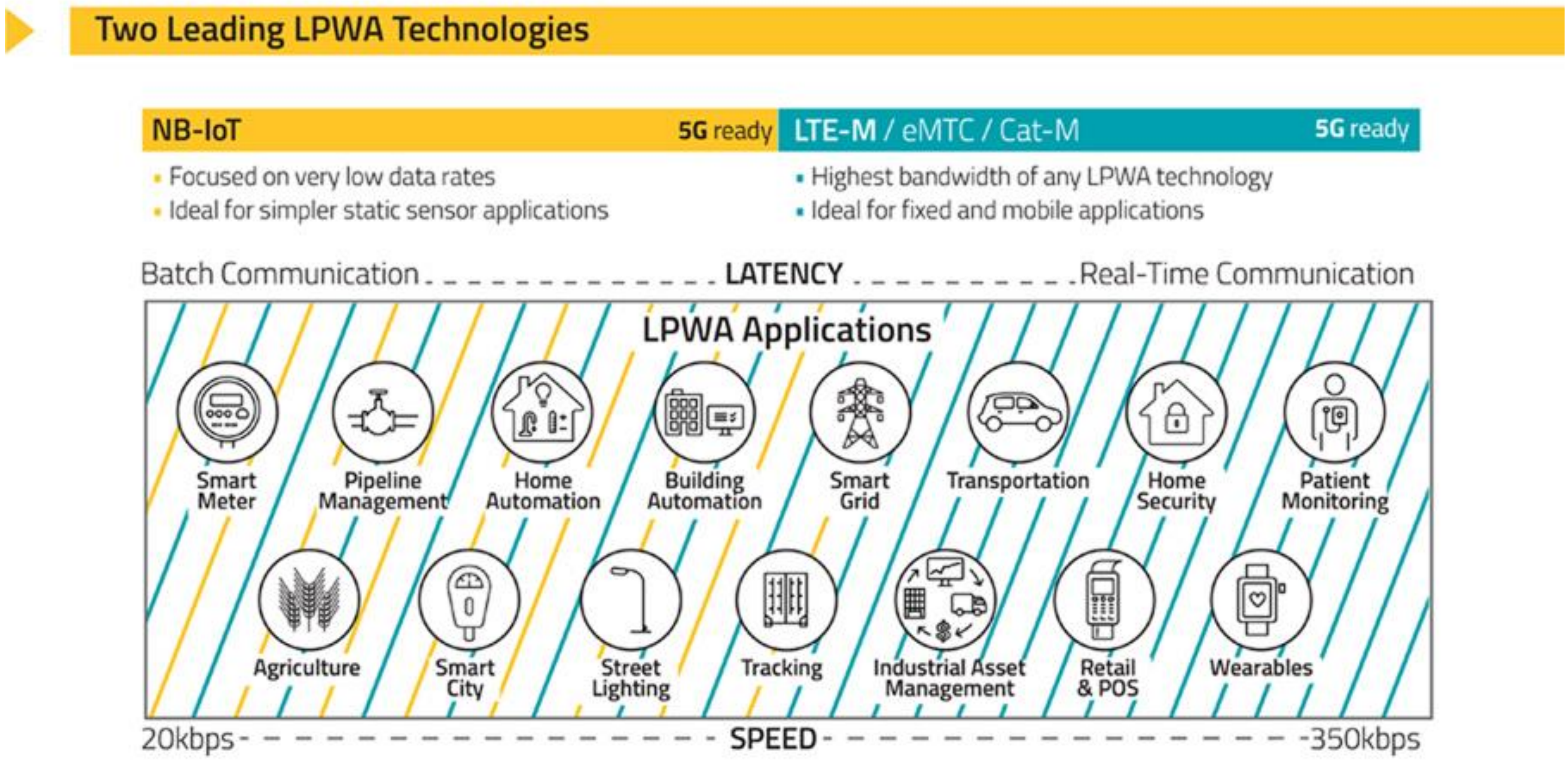
IoT in 5G Era

- ❑ **Mobile IoT/Massive IoT/LPWA:** improved network coverage, long device operational lifetime and a high density of connections. This is also known as mMTC (Massive MTC)
- ❑ **Enhanced Mobile Broadband:** improved performance and a more seamless user experience accessing multimedia content for human-centric
- ❑ **Critical Communications:** high performance, ultra-reliable, low latency industrial IoT and mission critical applications. This is also known as Critical IoT, URLLC (Ultra Reliable Low Latency Communications)

Source: GSMA

LTE-M and NB-IoT=Massive IoT

IoT in 5G era



https://www.iotforall.com/cellular-iot-explained-nb-iot-vs-lte-m/

Key IoT features

Advantages

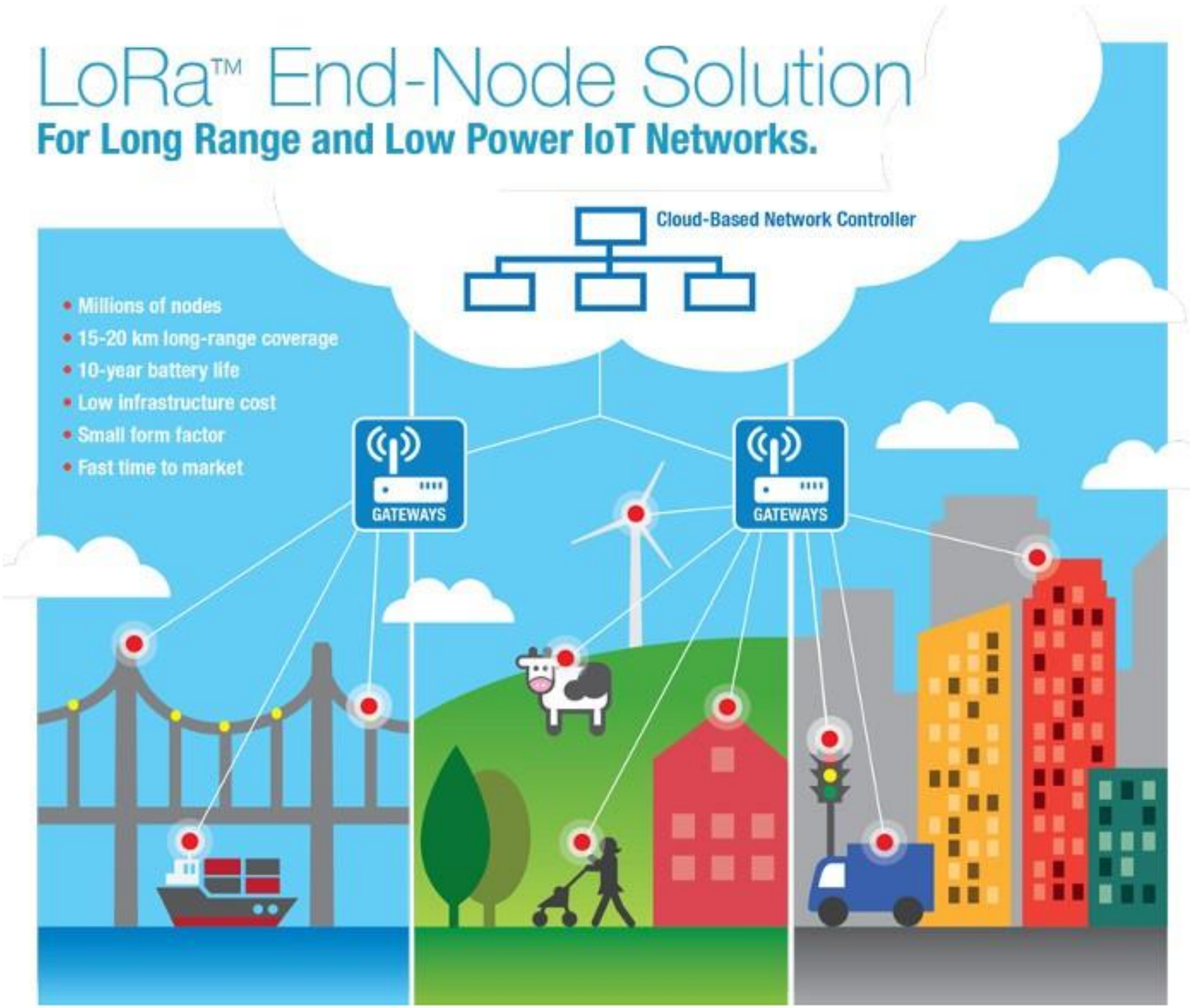
- Quality of service
  - Licensed band
  - Low latency
- Ubiquitous
- Security: SIM card protection + AES 256 bit (best)
- Great coverage: 2 km (LTE), 10 km (NB-IoT), 35 km (GSM)
- Global mobility and roaming support
- Scalable
- Connected even during power failure

Issues

- Cost: License, Capex and Opex, subscription
- High power
- Not possible to make your own network

LoRa and LoRaWAN

LoRaWAN


LoRa™ End-Node Solution
For Long Range and Low Power IoT Networks.
Cloud-Based Network Controller
Millions of nodes
15-20 km long-range coverage
10-year battery life
Low infrastructure cost
Small form factor
Fast time to market
GATEWAYS
GATEWAYS

LoRa PHY

- ❑ Chirp Spread Spectrum (FSK)

LoRa Parameters

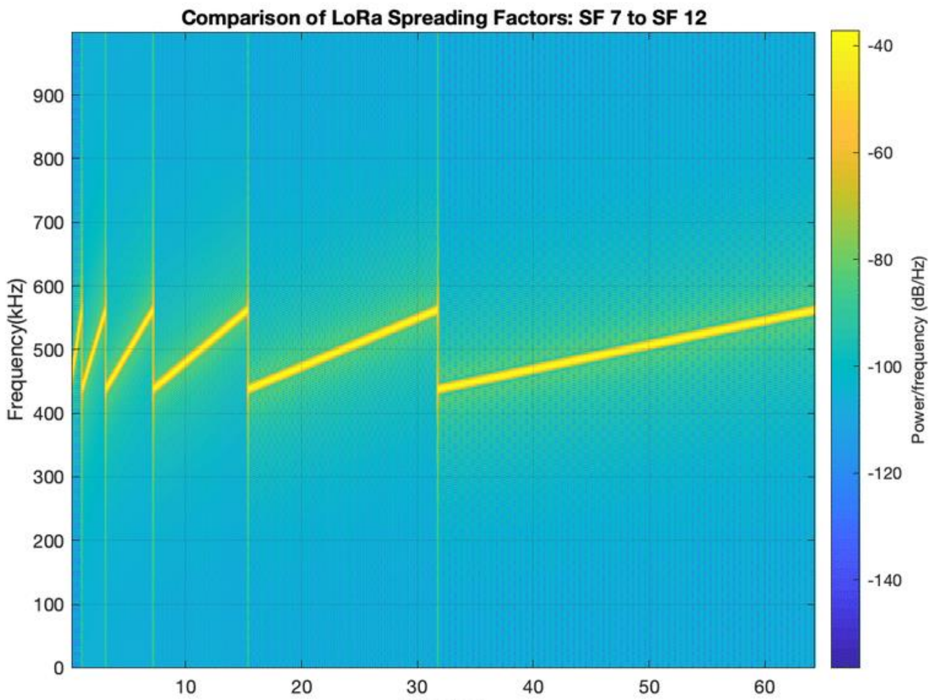
Parameter	Value Range	Explenation
frequency	863 - 870 Mhz / 902 – 928 MHz ...	The frequency used to transmit data
tx power	2 - 14 dBm / 5 – 20 dBm	Power used to transmit
bandwidth	125 / 250 / 500 KHz	Data bandwidth
spreading factor	7 - 12	Frequency spreading factor
coding rate	4/5, 4/6, 4/7, 4/8	Error correction data are (how many error correction bits)

- ❑ Communication between end-devices and gateways is spread over a range of frequency channels and data rates — LoRaWAN data rates range from 0.3 kbps to 50 kbps. Selecting the data rate is often a trade-off between message duration and communication range.

https://www.slideshare.net/alexandruradovici/lecture-6-wireless-sensors-lora-vs-lorawan

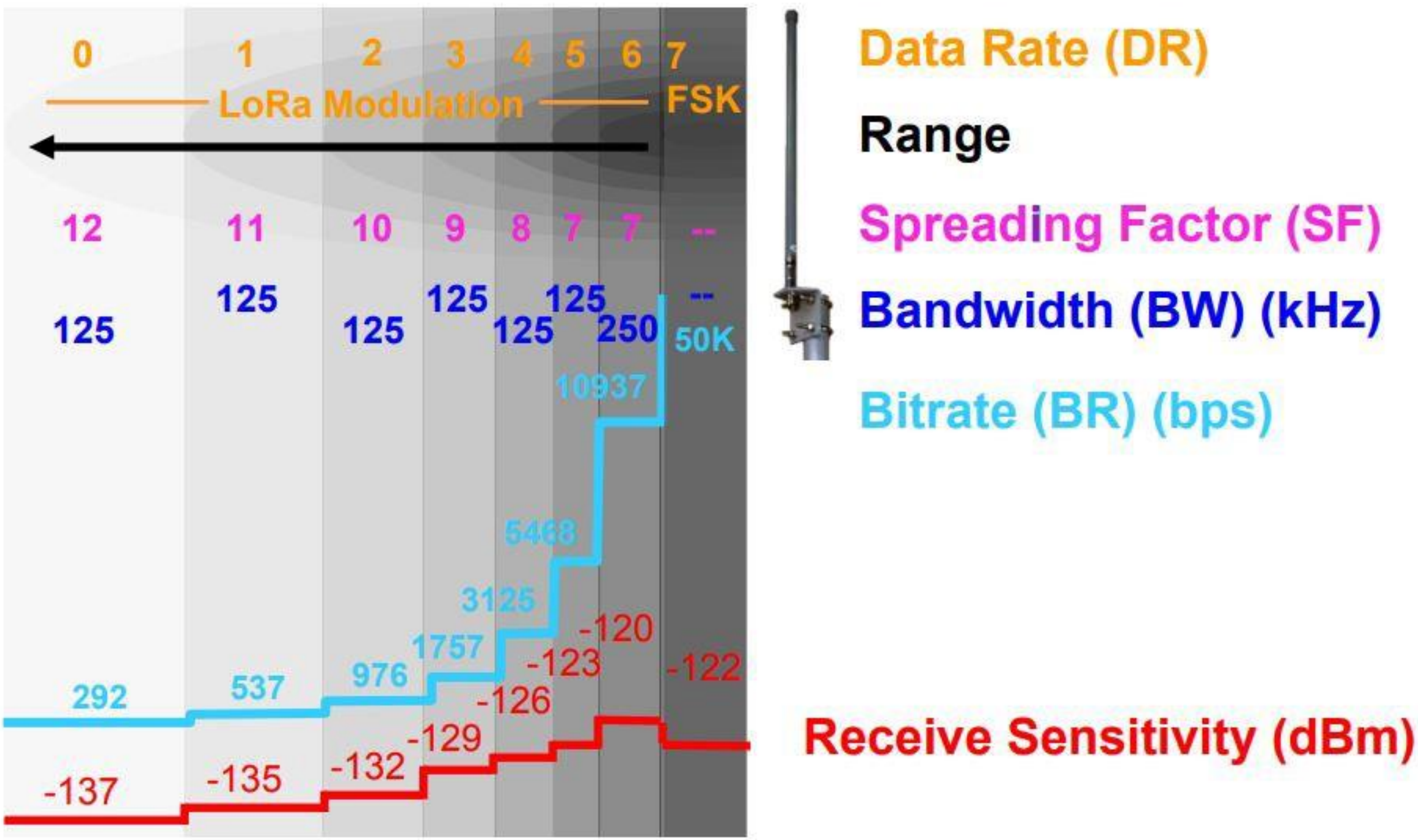
Chirp Spread Spectrum

- Chirp spread spectrum (CSS) is a spread spectrum technique that uses wideband linear frequency modulated chirp pulses to encode information
- The figure below shows that LoRa symbols are modulated over an up-chirp of a 125 kHz bandwidth, and SF 9 takes exactly twice the time of SF 8.



https://www.researchgate.net/figure/LoRa-uses-a-chirp-spread-spectrum-modulation-technique-The-figure-also-shows-that-LoRa_fig3_332151302

LoRa



0
1
2
3
4
5
6
7
LoRa Modulation
FSK
12
11
10
9
8
7
7
--
125
125
125
125
125
125
125
250
--
50K
10937
5468
3125
1757
976
537
292
-120
-123
-122
-126
-129
-132
-135
-137
Data Rate (DR)
Range
Spreading Factor (SF)
Bandwidth (BW) (kHz)
Bitrate (BR) (bps)
Receive Sensitivity (dBm)

LoRa

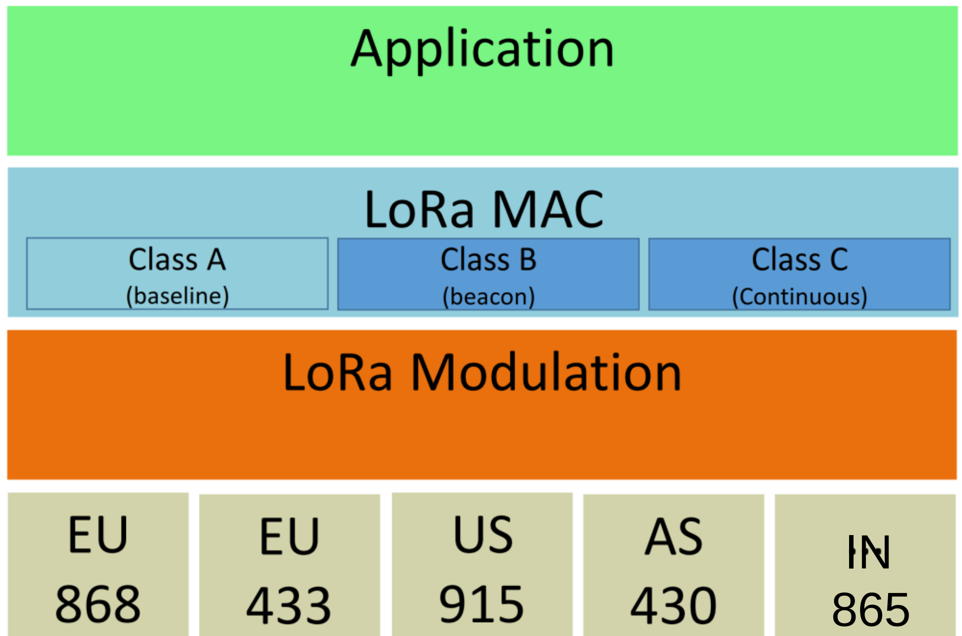
Modulation	Spreading factor	Bandwidth [kHz]	Maximum application throughput per channel [bps]	Maximum application layer throughput per end device per channel [bps]		
				10% duty cycle[1]	1% duty cycle[2]	0.1% duty cycle[3]
LoRa	12	125	146.1	14.61	1.46	0.15
LoRa	11	125	261.4	26.14	2.61	0.26
LoRa	10	125	584.2	58.42	5.84	0.58
LoRa	9	125	1359.2	135.92	13.59	1.36
LoRa	8	125	2738.1	273.81	27.38	2.74
LoRa	7	125	4844.7	484.47	48.45	4.84
LoRa	7	250	9689.3	968.93	96.89	9.69
GFSK	-	150	45660.4	1851.6[4]	456.6	45.66

https://www.researchgate.net/figure/Maximum-throughput-per-LoRaWAN-end-device-per-channel_tbl2_315119434

LoRaWAN

LoRaWAN
By LoRa Alliance
Or Symphony Link
(by Link Labs)

LoRa (Semtech)
CSS based



Application

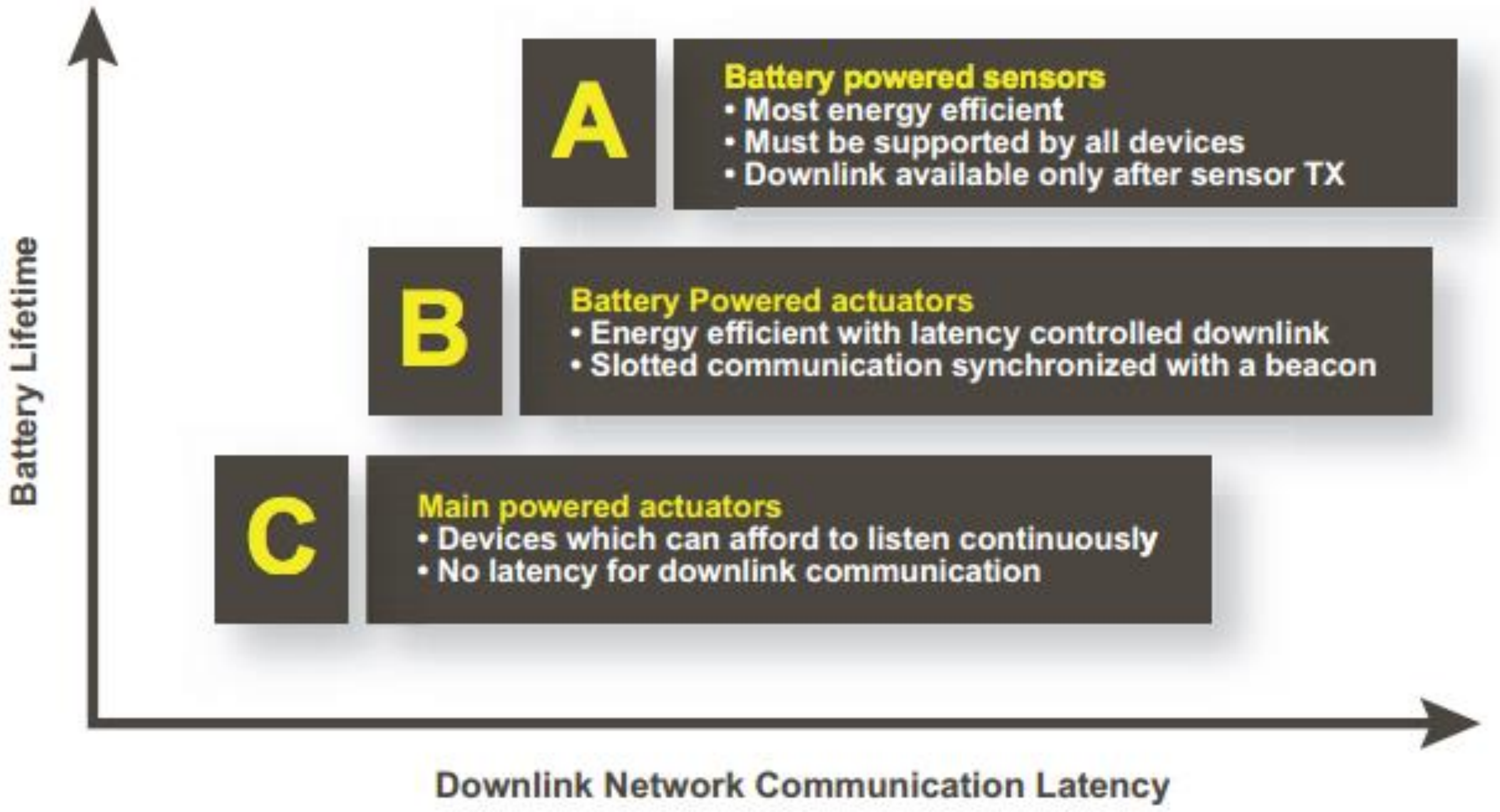
MAC

MAC options

Modulation

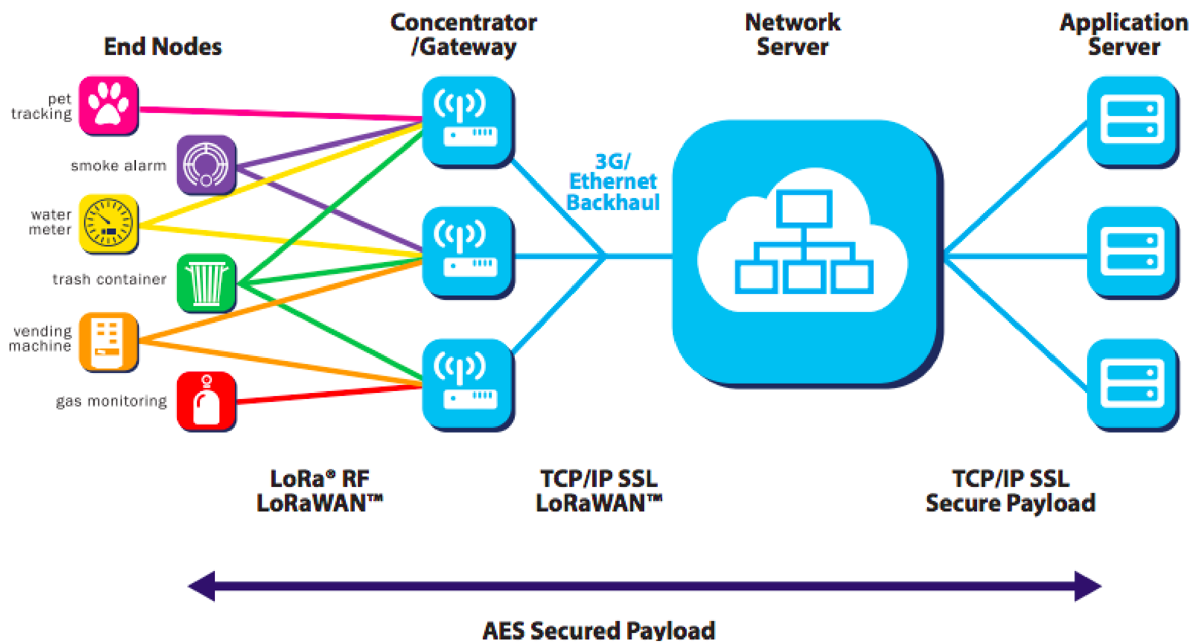
Regional ISM band

LoRaWAN classes



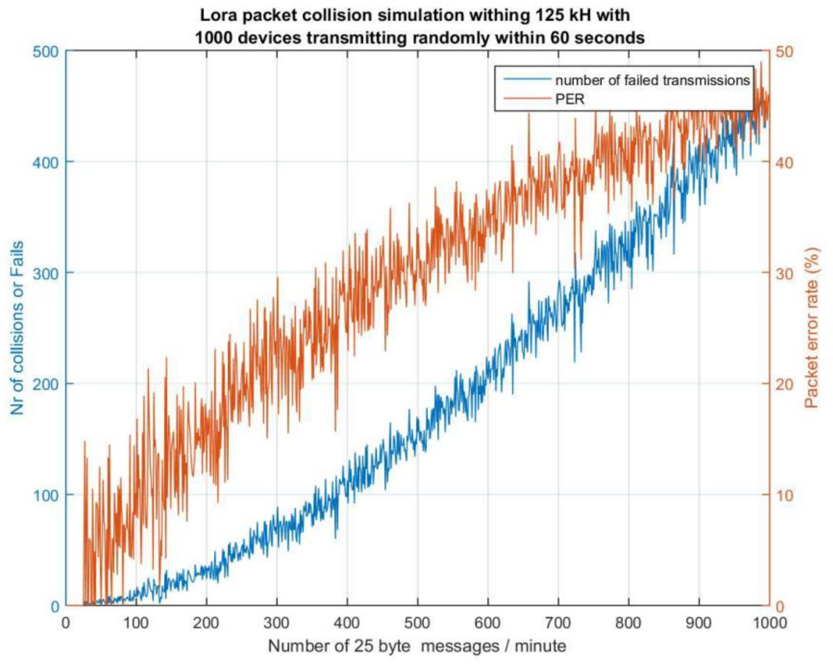
LoRaWAN

- LoRaWAN is a software layer above LoRa
  - Pure Aloha (18.4% efficiency) + CSS
  - Dumb Gateways and Smart Server: *Filters data at server*
  - Makes transmission reliable by allowing retransmissions
  - Transposes data on IP network
  - Adds security as LoRa does not have security



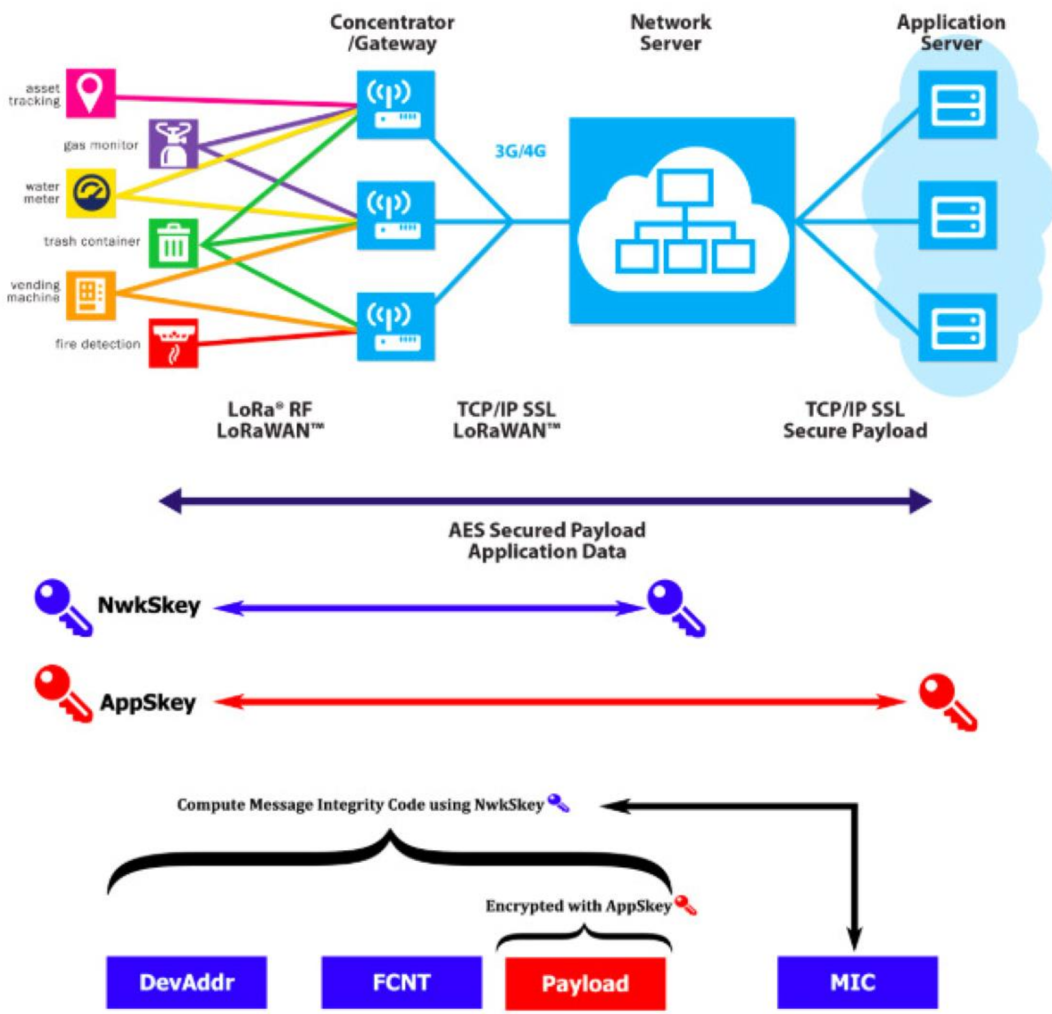
LoRaWAN

- Gateways listen on 8 frequencies on all spreading factor
- Collision prevented by maximum duty cycle



Source: https://sites.google.com/a/wesdec.be/mweyn/lpwan

LoRaWAN security



NwkSkey to guarantee the message integrity from the device to LoRa server

AppSKey to used for end to end AES-128 bit encryption from device to application server

IoT Features

Advantages

- Low powered sensors (Battery life of 2-5 years)
- Wide coverage area 1-10 Kms
- Low Costs
  - free(unlicensed) frequencies
- One gateway can support thousands of end devices
- Security: a layer of security for the network and one for the application with AES encryption.
- Fully bi-directional communication.
- LoRa Alliance: 500+ members companies including IBM and Cisco

Disadvantages

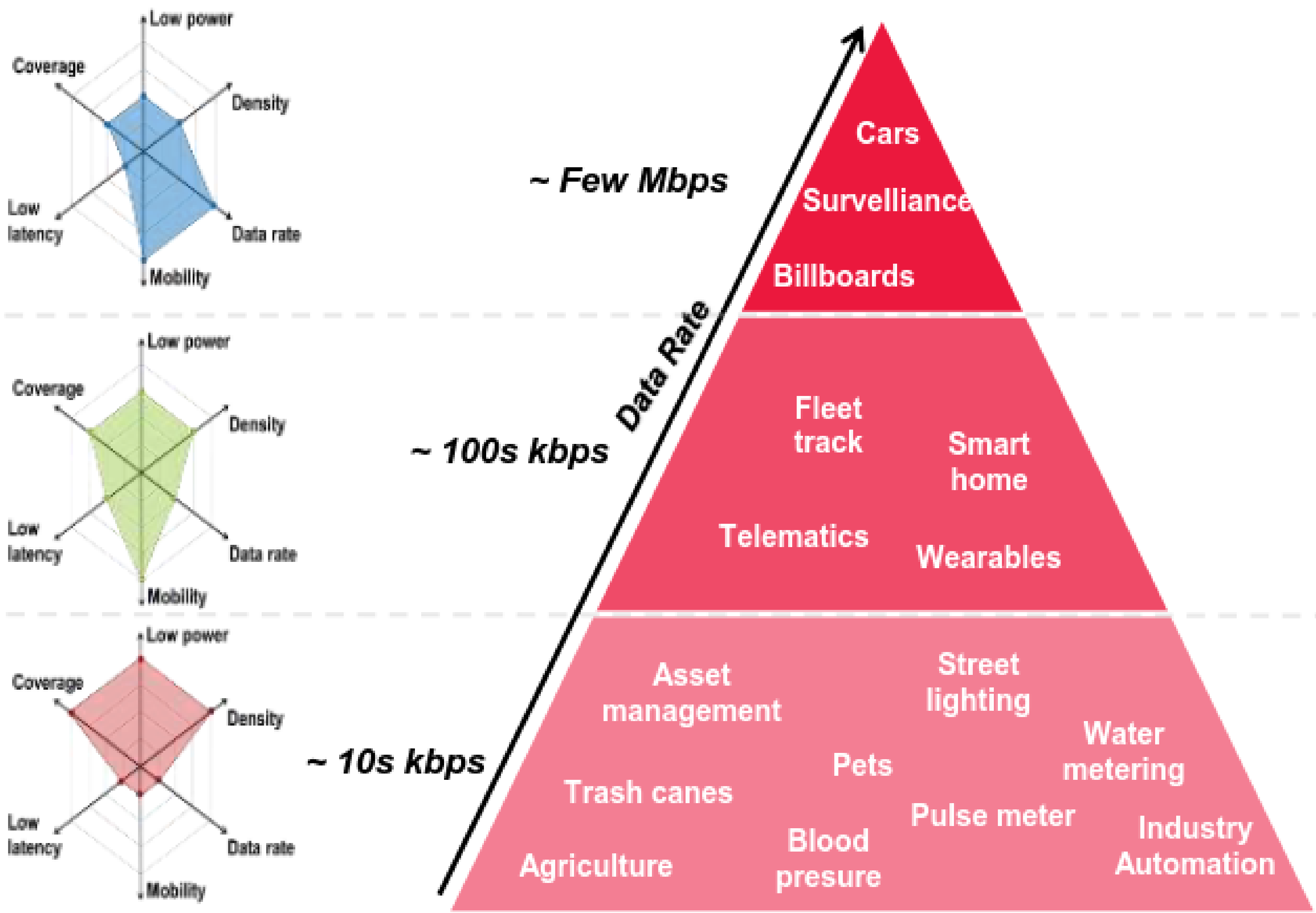
- Payload limited to 100 bytes
- Not for continuous or real-time monitoring (most of industry cases)
- Unlicensed frequency: crowding increases interference
- Low duty cycles (1% in EU)

	IEEE 802.15.4	IEEE 802.11ah	BLE	NB-IoT	LoRaWAN
Bands	868, 915 MHz 2.4 GHz (ISM)	900 MHz (ISM)	2.4 GHz (ISM)	Between 400-2200 MHz (Licensed Frequency)	868/915/433 MHz (ISM)
Topology	Star, Mesh, Cluster Tree	Star, Mesh, Cluster-Tree	Piconet, Scatternet, Mesh	Star	Star of Stars
Max. Range	1 Km	1 Km	100 m	10 Km in one cell	10 Km in one cell
Max.Power	100 mW	100 mW	100 mW	200 mW	25 mW
DIY	Yes	Yes	Yes	No	Yes
Max. Number of Nodes per cell	65536	8192	Unlimited	100K	50 K
Modulation	BPSK, O-QPSk + DSSS	OFDM	GFSK	QPSK	CSS
Channel Access	Slotted/Unslotted CSMA/CA + GTS	CSMA/CA + GTS + RAW	FH-TDD-TDMA Polling	HD-FDD TDMA+FDMA	Aloha
Data rates	20, 40 and 250 Kbps	150 Kbps- 347 Mbps	0.2-2 Mbps	20-250 Kbps	0.3-50 kbps
Power Saving	Sleep-Wake Schedule	Sub-1GHz TWT, Sleep-Wake, BDTO, Short MAC	Sniff, Hold, Park	PSM, low bandwidth, low duty cycle, eDRX	Target Application

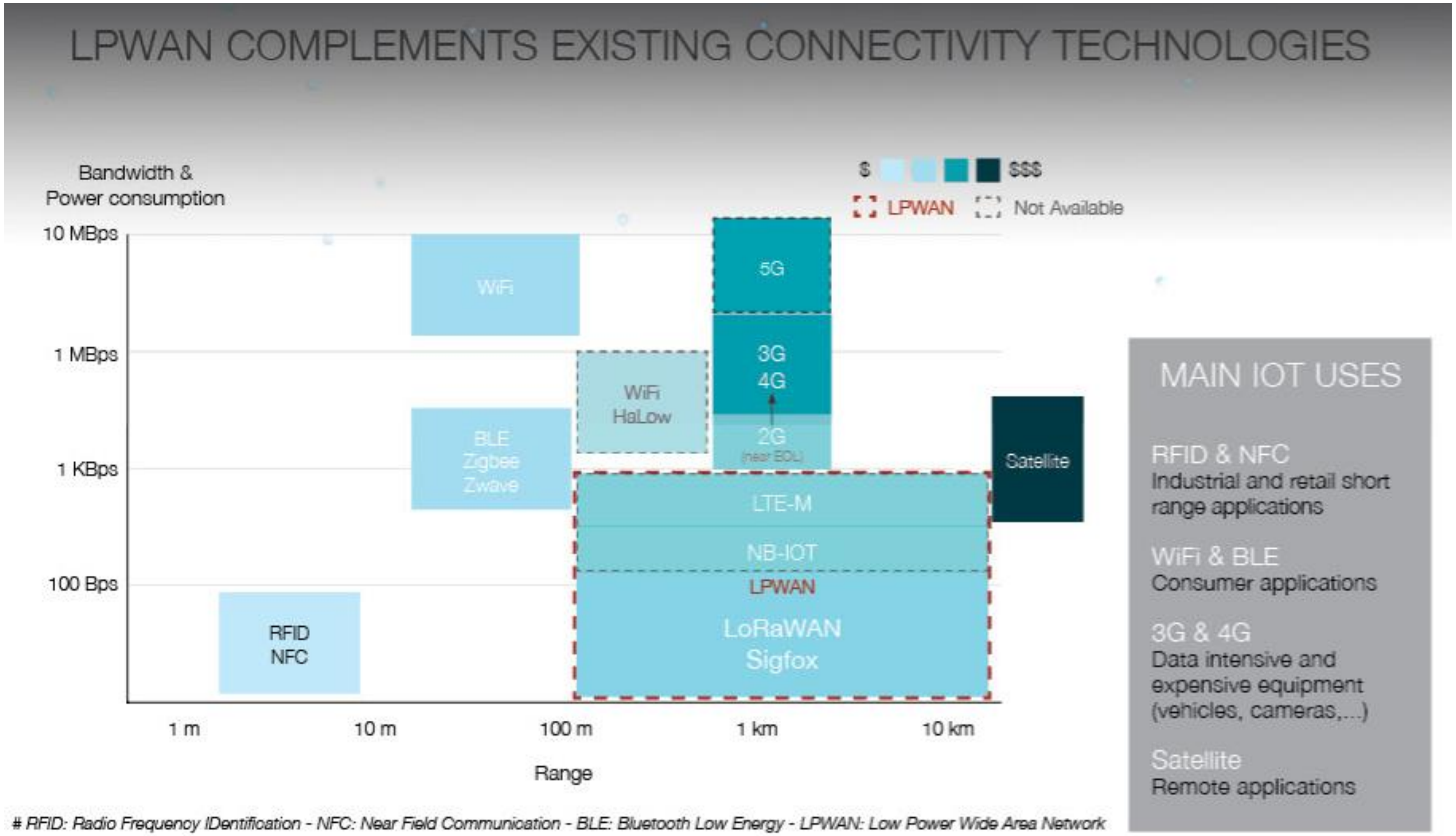
Summary: One size does not fit all!

Requirement

Devices per



Competing and Complementing!!!



https://www.iotforall.com/iot-connectivity-comparison-lora-sigfox-rpma-lpwan-technologies/

References

- [Kurose2012] J. Kurose and K. Ross, *Computer Networking, 5th edition,* Pearson, 2012
- [Sohraby2007] K. Sohraby, D. Minoli, and T. Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications,* Wiley, 2007
- [Koubaa2007] Anis Koubaa, Mário Alves and Eduardo Tovar, Time Sensitive IEEE 802.15.4 Protocol, *Sensor Networks and Configuration, pp.19-49*
- [Townsend2014] K. Townsend, C. Cufi, Akiba, R. Davison, *Getting Started With BLE,* O'Reily, May 2014
- [Gonzalez2016] V. Gonzalez et. Al. "IEEE 802.11ah: A Technology to face the IoT Challenge," Sensors, 2016
- [Park2015] M. Park, "IEEE 802.11ah: Sub-1-GHz license-exempt operation for the internet of things," *IEEE Communications Magazine*, September 2015.
- [Dohler2016] M. Dohler, et. al. "Internets of Things in 5G Era: Enablers, Architecture, and Business Models," *IEEE Journal on Selected Areas in Communications*, Vol. 34, No. 3, March 2016

References

- [Mekki2019] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, ”A comparative study of LPWAN technologies for large scale IoT deployment,” Science Direct, ICT express 5 2019.
- [IEEE802.11ax] Broadcom, *White paper on IEEE 802.11ax*, 17 Oct. 2018
- [Lea2018] P. Lea, *Internet of Things for Architects,* Packt, 2018
- [Yin2019] J. Yin et. al, “A Survey on Bluetooth 5.0 and Mesh: New Milestones of IoT,” ACM Trans. on Sensor Networks 15(3):1-29, May 2019

Thank You!

Questions?