Communications & Controls in IoT

WiSUN and BLE

Instructor: Sachin Chaudhari

Feb. 20, 2023

INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY
HYDERABAD

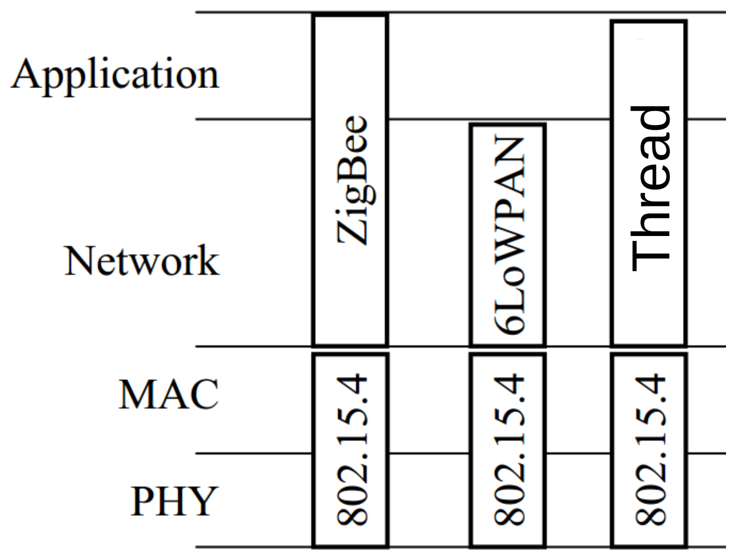
Recap

IEEE 802.15.4

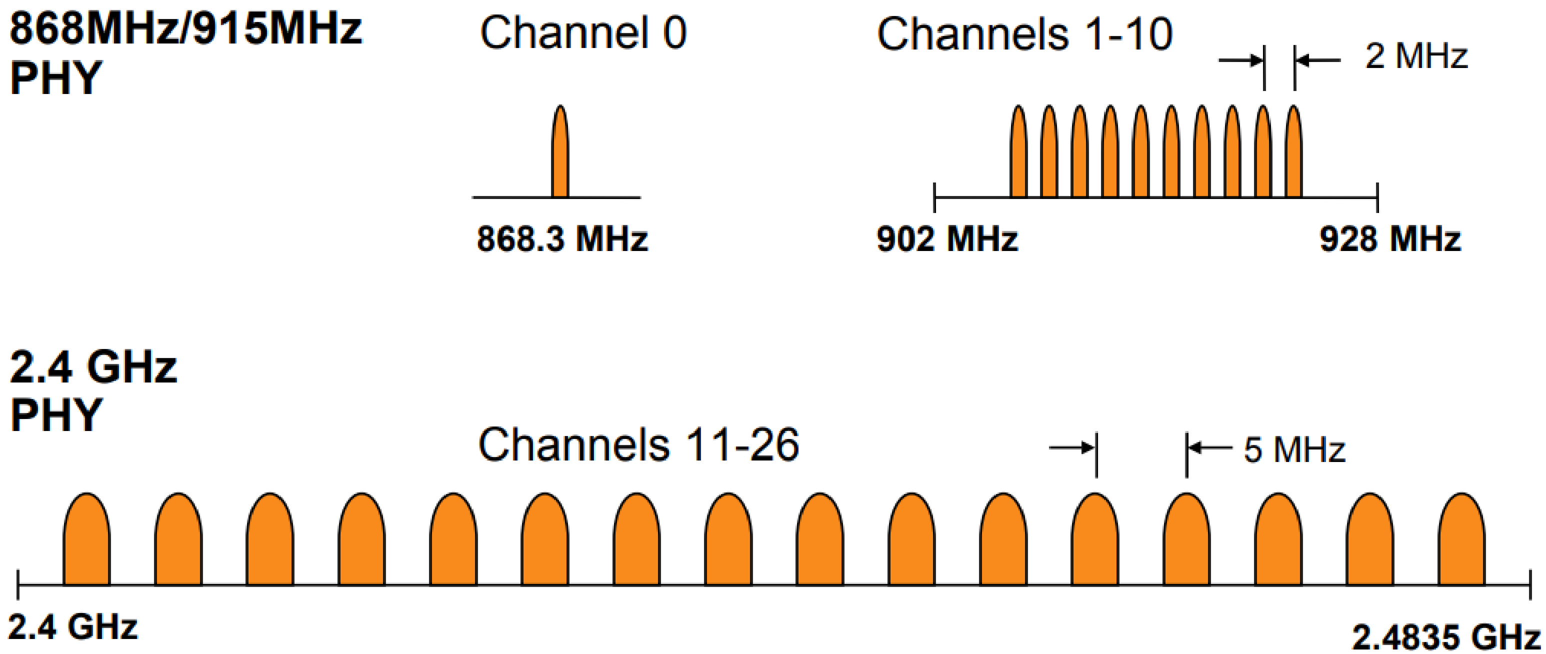
Ref: K. Sohraby, D. Minoli, T. Znati, *Wireless Sensor Networks,* Wiley, 2007

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
  - Vast number of industrial, home and medical applications
- It specifies the physical layer (PHY) and media access control (MAC) for LR-WPANs
- Does not have IP address
- Used by several “Internet of Things” protocols:
  - ZigBee, 6LowPAN, Thread, WiSuN etc.



Physical Layer (PHY): *Operating Frequency Bands*



https://people.eecs.berkeley.edu/~prabal/teaching/cs294-11-f05/slides/day21.pdf

PHY: *Modulation Parameters*

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

[Koubaa2007]

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

Additional Tasks of PHY of IEEE 802.15.4

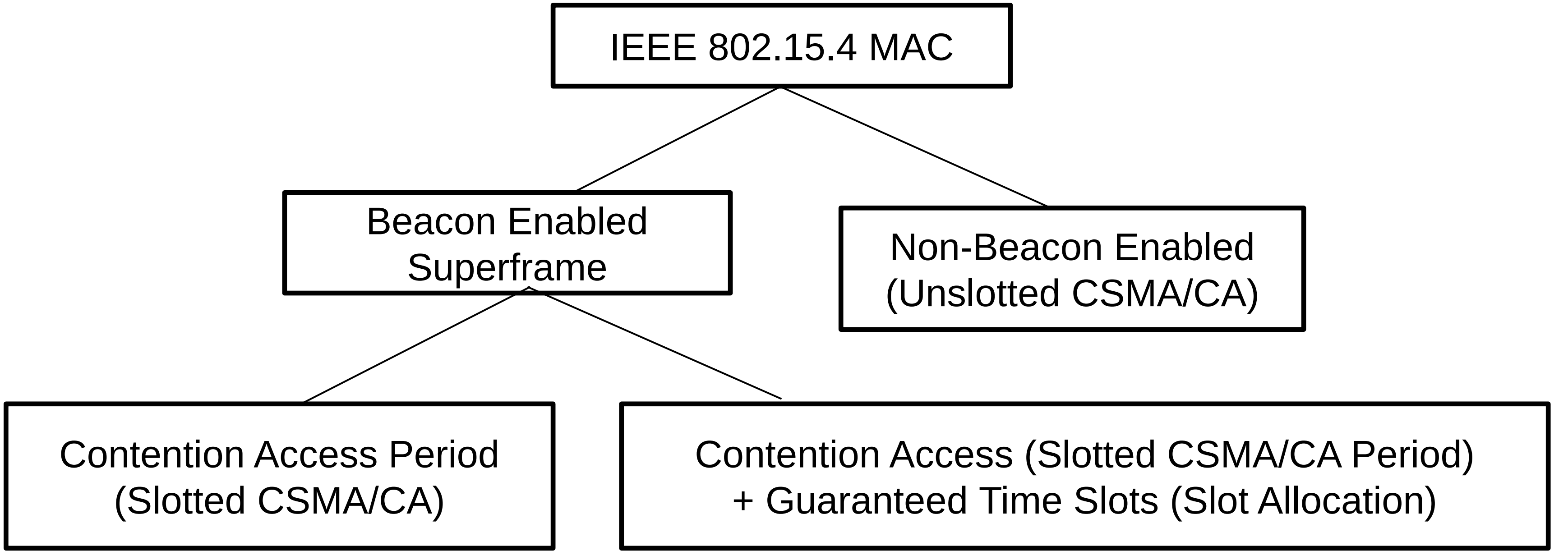
- **Activation and deactivation of the radio transreceiver**
  - Three states: Transmitting, receiving and sleeping
- **Receiver energy detection**
  - No decoding or signal identification
  - Required to understand if the channel is busy or idle
- **Link quality indication**
  - Using energy or SNR estimation or both
- **Clear channel assessment**
  - Energy detection or carrier sense or both
- **Channel frequency selection**
  - 27 channels

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
  - Synchronized 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



IEEE 802.15.4 Versions

- Since the first version in 2003, new amendments are constantly being introduced.
- Modifications
  - New country specific (frequencies, regulation)
  - New application and network specific:
    - SUN: Smart utility meter monitoring
    - LECIM: Low Energy Critical Infrastructure Monitoring
    - RFID: Radio Frequency Identification
    - RCC: Railway Communications and Control
    - TVWS: TV White Space
    - Medical
  - New PHY specific
    - OFDM, ASK, FSK, QAM, GMSK, MSK, OOK
  - New Protocols
    - TSCH, Aloha, PCA

L. Alkama, L. Medjkoune, "EEE 802.15.4 historical revolution versions: A survey", Springer Nature 2021

IEEE 802.15.4 Versions

Not in Syllabus for Exam

Versions	Date	Type of net-work	Max Data rate kb/s	Modulation Encoding	protocole used	Features
802.15.4e	2012	Industrial LR-WPAN	–	–	DSME LLDN TSCH	QoS, Security Minimizing collisions Deterministic yet flexible bandwidth Interference avoidance Multi-channel, multi-superframe High reliability of the system
802.15.4f	2012	RFID	250	MSK OOK PPM	ALOHA	Multi-year battery life Reliable communications Precision location
802.15.4g	2012	SUN	800	FSK BPSK QPSK QAM O-QPSK	CCA	Interference avoidance Security
802.15.4j	2013	MBAN	250	O-QPSK	–	Keeping a channelization scheme flexible
802.15.4k	2013	LECIM	–	BPSK O-QPSK FSK GFSK P-FSK P-GFSK	– CSMA/CA PCA ALOHA PCA	Reduction of collision probability Good transmit power efficiency Higher sensitivity Priority Forward error correction QoS, security

L. Alkama, L. Medjkoune, “EEE 802.15.4 historical revolution versions: A survey”, Springer Nature 2021

Today's Class

Wireless Smart Ubiquitous Network (WiSUN)
Field Area Networks (FAN)

Good References

- https://www.wi-sun.org/
- https://www.wi-sun.org/wp-content/uploads/Wi-SUN-Alliance-Comparing_IoT_Networks-r1.pdf

WiSUN Field Area Networks (FAN)

Field Area Network (FAN) provides connectivity to a large number of devices spread throughout a given geographic area

WiSUN-FAN

- An open specification based on the **IEEE 802.15.4g-2012** specification, as well as other IEEE 802 and IETF standards
- Application focus
  - smart cities
  - smart utilities
  - smart lighting
  - Mostly competing against LoRaWAN and NB-IoT
- Wi-SUN Alliance
  - Established in 2011
  - Manages the specifications and certifications to ensure interoperability
  - 300+ members
  - 100 million + devices worldwide
  - 150+ WiSUN certified products

IEEE 802.15.4g-2012: *WiSUN*

- Amendment made for Smart Metering Utility Networks (SUN)
- PHY
  - Support outdoor, low-data rate and wireless applications under multiple regulatory domain
  - Multiple PHY layers for targeting different markets and applications
  - Three alternate PHY provided
    - Multi-rate and multi-regional FSK (MR-FSK)
      - Good transmit power efficiency
    - Multi-rate and multi-regional OFDM (MR-OFDM)
      - Higher data rates in multipath fading channels
    - Multi-rate and multi-regional OQPSK (MR-OQPSK)
      - Same characteristics as previous versions

WiSUN Features

- Both star and mesh topologies are possible
  - Powerful use of mesh topology
    - One cluster of 5000 sensor nodes in 1 Km range
- Unlicensed band operation
- Leverages IPv6
- Can be designed for frequent communications
  - Every 10 secs
- Low latency of about 0.02-1 secs
- Data rates of upto 300 Kbps
- Coverage of 4 Km point-to-point using 1W non-directional antenna
- Security at multiple levels
  - Native public-key infrastructure (PKI) integration providing security certification capabilities for each device
- Networks designed for long lifecycle
  - Low power design (15-20 year battery target)
  - Backward and forward compatibility with different generations

WiSUN: Mesh topology

- Self-forming, self-healing
  - Easy to add new devices
  - Robustness against outages or node-failures
- Unlike Zigbee, designed for a much greater scale and several hops (around 30)
- With sufficient density, very robust against blockages and outages
- Coverage gaps can be filled with additional devices
- Star topology may encounter urban canyons and coverage gaps in urban environments
  - Electric meters cannot move to find reception

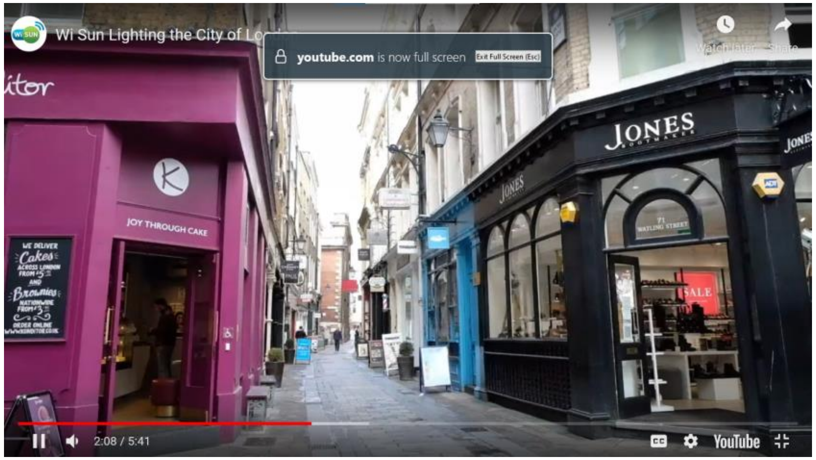
Star Networks

WiSUN

Comparison between Mesh and Star

	Mesh	Cellular (Star)
No. of devices	Many in same location	Few (<10) in one location
Coverage	Cellular coverage not there	Coverage available
Device communication	Device talk more frequently to neighbors	Devices mostly talk to cloud
Communication Frequency	More frequent	Less frequent

Use Case: *London Streetlights*



WiSun Lighting the City of London https://www.youtube.com/watch?v=3nQDSqx3S3w

Use Case: *London Streetlighting*

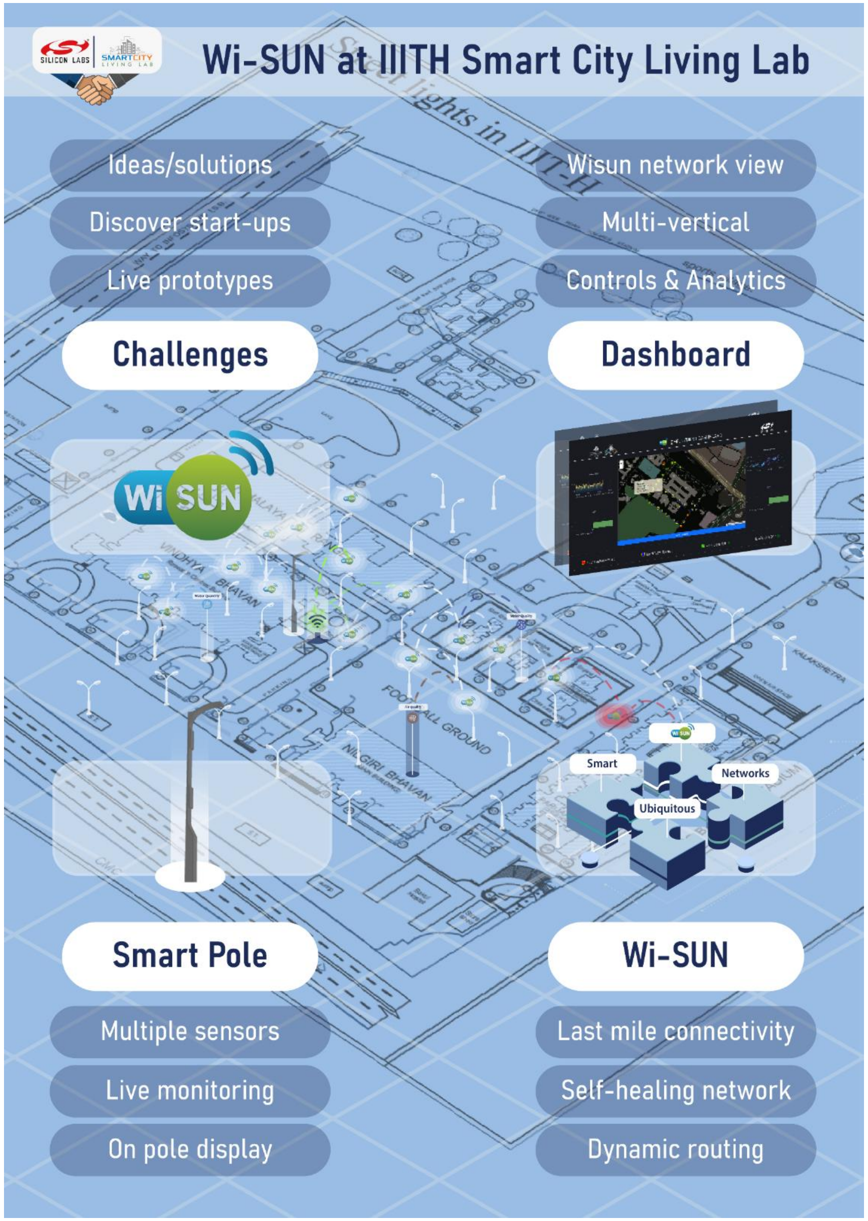
- Dynamic population in downtown
  - 9000 residents but 4,50,000 in peak times
- Narrow streets, alleys, tall buildings, and hidden areas
  - Unique and historical feel for London
  - Creates large urban canyons, where the tallest buildings sometimes block out the horizon
- LEDs and a Central Management System (CMS)
  - **Set the scene of its historic assets**
    - Use of the tunable settings of digital lighting that are not so easily achievable using analog lights
  - Reduction of maintenance and energy consumption costs
    - automated brightness adjustment to match lighting levels to environmental conditions, as well as to vehicle, bicycle, and pedestrian traffic.

Use Case: *London Streetlighting*

- Use of open standards so that any third-party devices can be integrated
  - traffic and parking monitoring, occupancy sensing, environmental monitoring, asset management, and lighting control
- Itron deployed 12,000 lights in two-years supported by 10 gateways
- UrbanControl's software-based security offerings to comply with the City's stringent requirements.

Use Case: *IIITH Streetlighting*

Wi-SUN Deployment in Collaboration With Silicon Labs



- RF Mesh – Enables Last Mile Connectivity for IOT Data
- Control through Dashboard
- Self Healing Network
- Interconnectivity through oneM2M

Questions?

Bluetooth

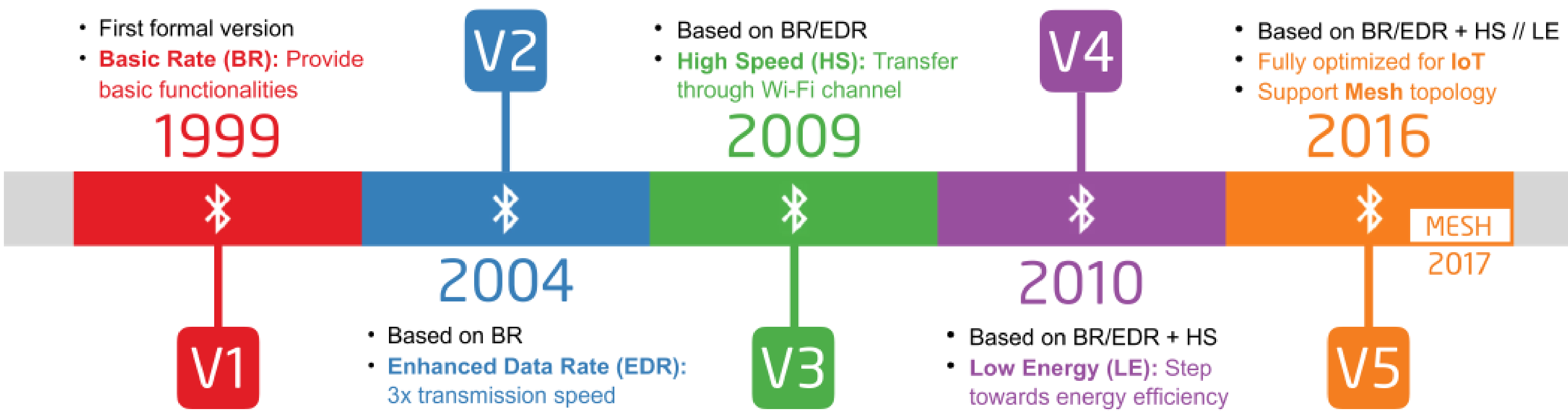
Good References

- [Lea2018] P. Lea, *Internet of Things for Architects,* Packt, 2018

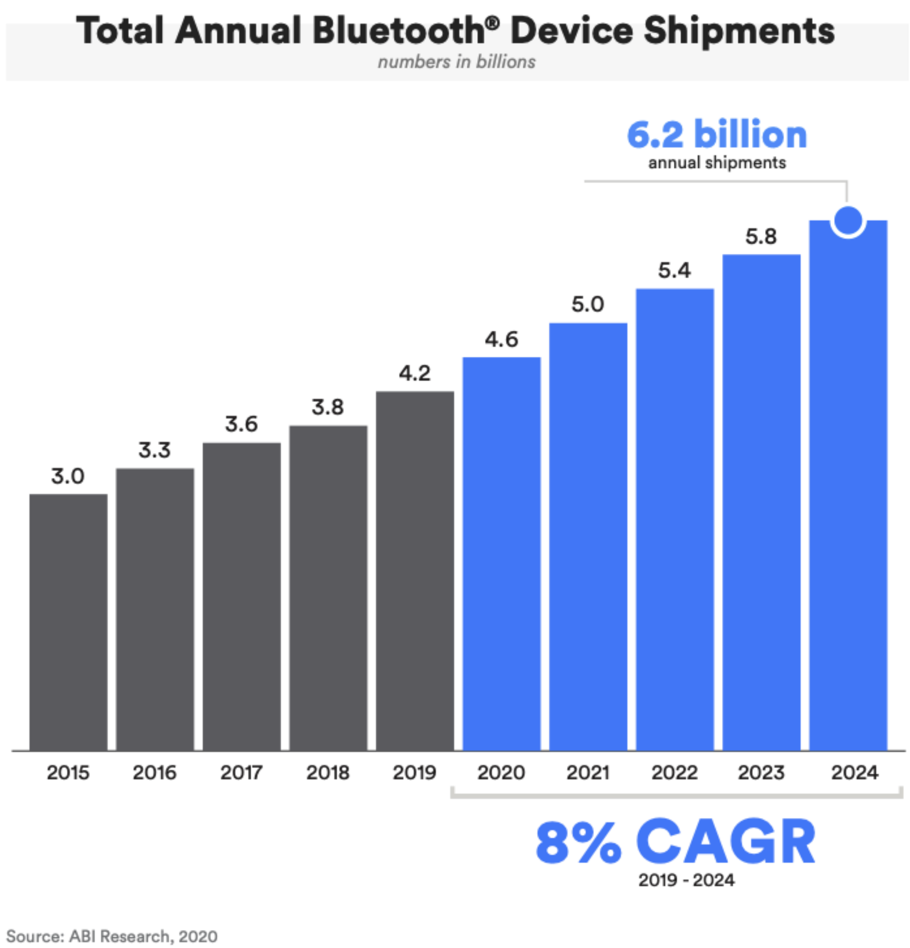
- [Yin2019] J. Yin et. al, "A Survey on Bluetooth 5.0 and Mesh: New Milestones of IoT," ACM Trans. on Sensor Networks 15(3):1-29, May 2019

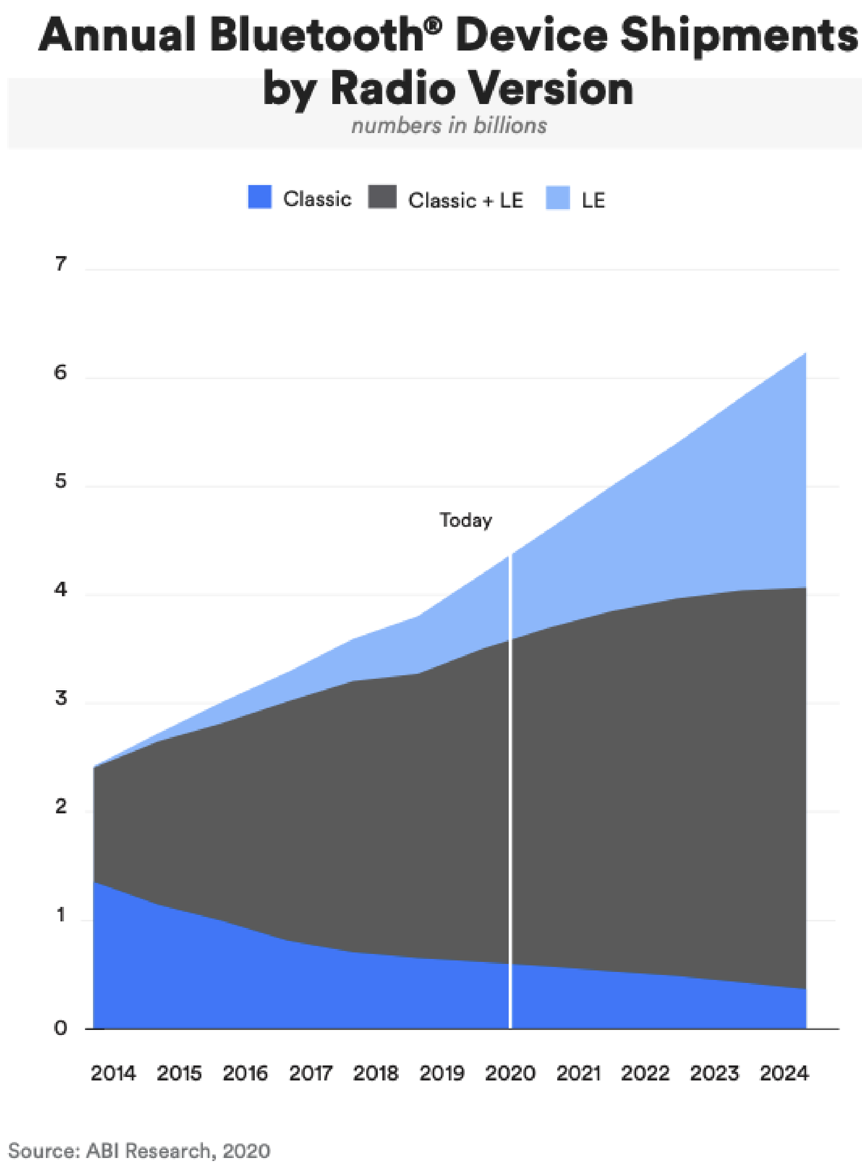
- https://www.bluetooth.com/

Bluetooth Versions



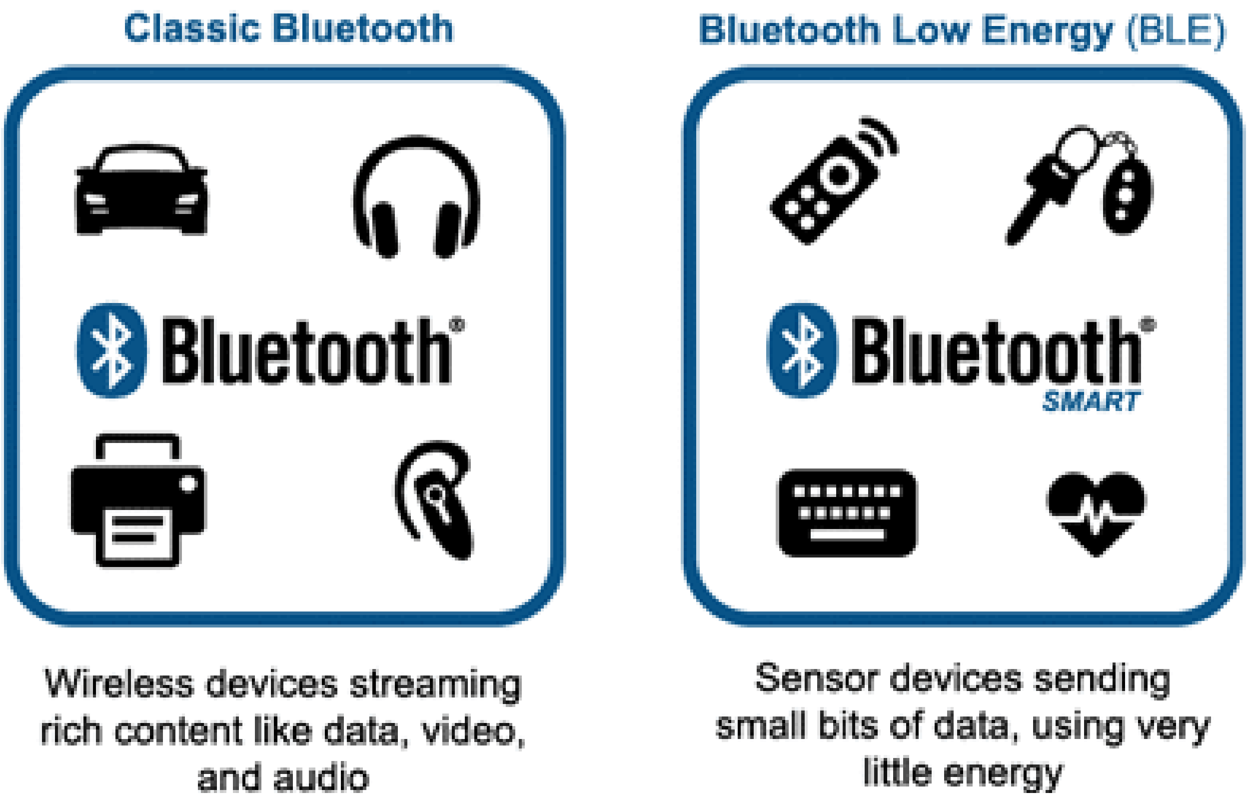
Bluetooth devices shipped every year





Outline

- Bluetooth
- Bluetooth Low Energy (BLE)



[Signils]

Introduction

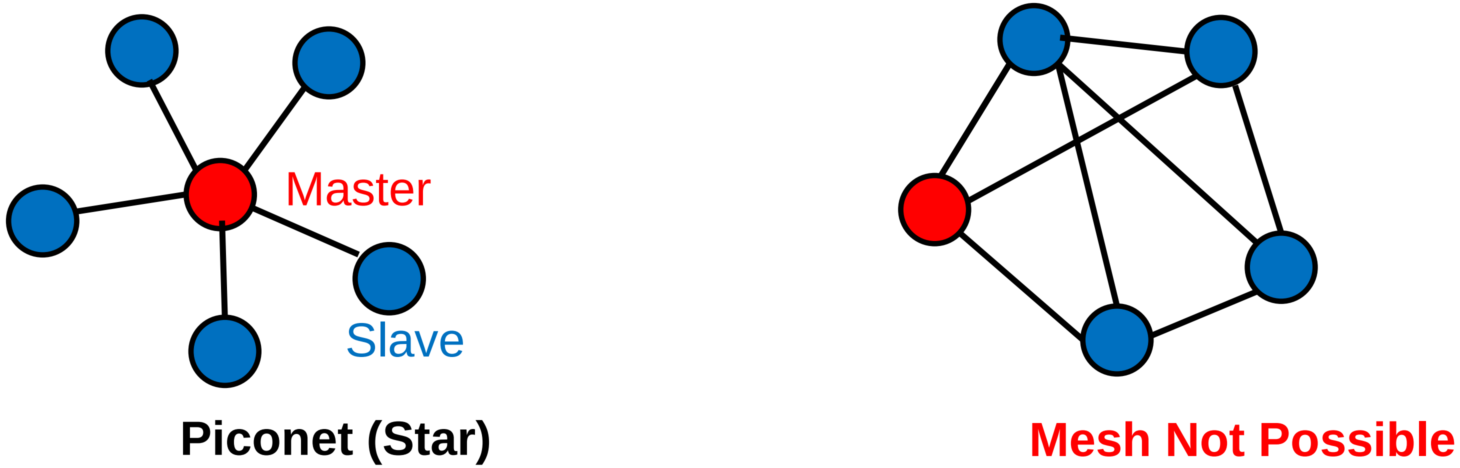
- Bluetooth is a standard wire-replacement communications protocol primarily designed for low-power consumption, with a short range based on low-cost transceiver microchips in each device. [wiki]

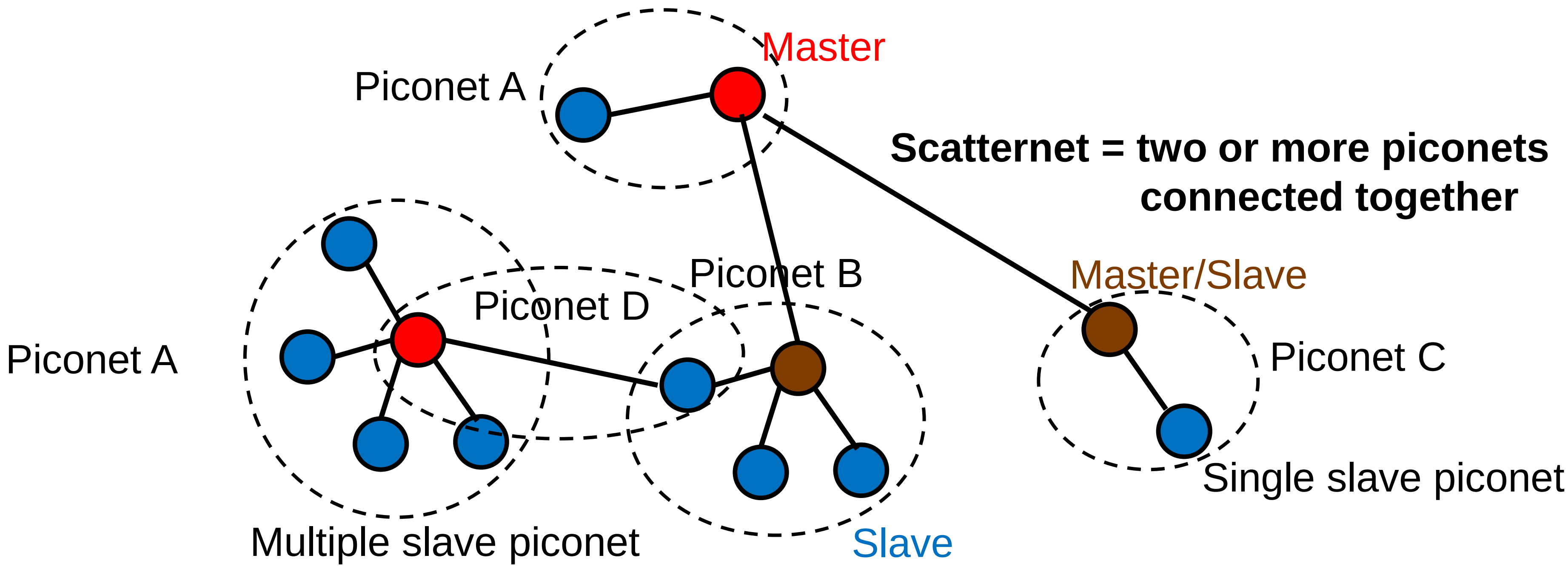
- Applications
  - Stream audio in devices including headsets and mobile phones, home stereos, MP3 players
  - Transfer data (meeting schedules, phone numbers), audio, graphic images and video from one device to the other provided they are Bluetooth compliant

- Earlier IEEE 802.15.1 standard (Now maintained by Bluetooth SIG)

- Why not use WiFi?

Network Topologies: Piconet and Scatternet





Physical Layer

Specification	Features Supported
RF Frequency	2.4 GHz
Transmit power	1 mW (min), 100 mW (max)
Data rate	1 Mbps
Distance	100 m (max)
RF bandwidth	220 KHz to 1MHz
Number of channels	23 (min) to 79 (max)
Topology	Up to 7 links in star configuration
Hopping rate	1600 hops per second
Access type	FH-TDD-TDMA

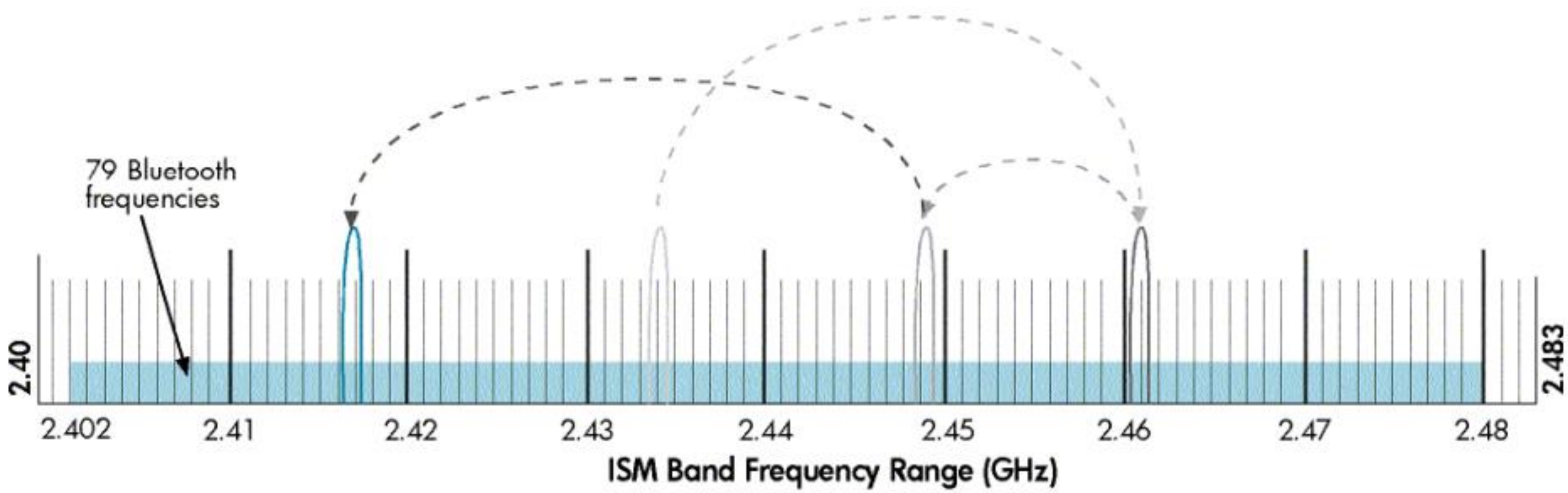
Frequency Allocation

- Bluetooth operates at 2.4 GHz ISM band.
- Following table defines Bluetooth frequencies used across the world.

Region	Frequency Range	RF Channels
In US, Europe, and rest of the world	2.4 to 2.4835 GHz	f = 2.402 + n MHz (n=0 to 78)
Japan	2.471 to 2.497 GHz	f = 2.473 + n MHz (n=0 to 22)
Spain	2.445 to 2.475 GHz	f = 2.449 + n MHz (n=0 to 22)
France	2.4465 to 2.4835 GHz	f = 2.454 + n MHz (n=0 to 22)

Frequency Hopping

- 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

Example of PN Sequence: 2, 5, 19, 31, 78, 43, 65, 7, 2, 5, 19, ….

Time Division Multiplexing

- Basic unit of operation is slot of 625 microsecs.
- In pre-connection stage (inquiry/page/scan), Tx and Rx can occur in half slots
- In connection state, Tx and Rx can occur in multiple slots: 1,3,5

Power Classes

Class number	Max Output Power (dBm)	Max Output Power (mW)	Max. Range
Class 1	20 dBm	100 mW	100 m
Class 2	4 dBm	2.5 mW	10 m
Class 3	0 dBm	1 mW	10 cm

Modulation Formats

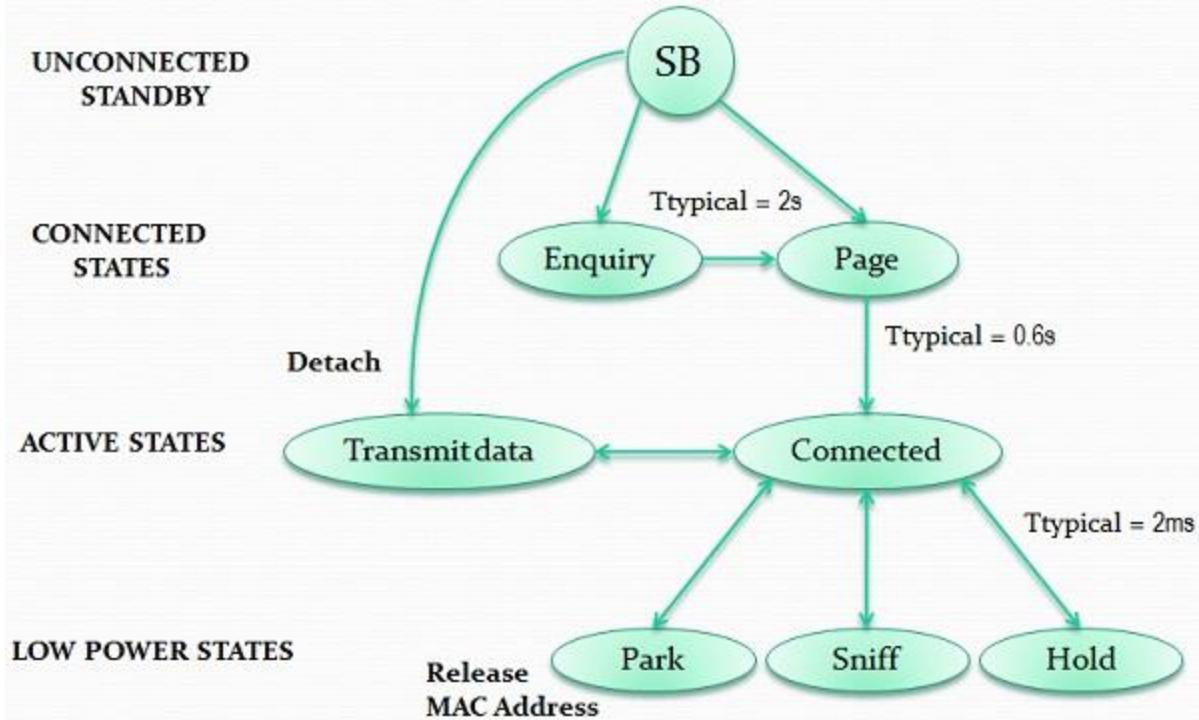
- The first version of the Bluetooth system used a **Gaussian Frequency Shift Keying (GFSK) modulation** types which was robust and reliable but not very efficient.
- Bluetooth systems from version 2.0 and above can use either **GFSK**, **pi/4 QPSK** or **D8PSK**.

Bluetooth Device Address

NAP (16 bits)	UAP (8 bits)	LAP (24 bits)

- 48 bit IEEE MAC address (BD_ADDR)
  - Lower address part (LAP) of 24 bits
  - Upper address part (UAP) of 8 bits
  - Non-significant address part (NAP) of 16 bits
- Globally unique!
- LAP and UAP of master are also used to determine frequency hopping sequence
- NAP is also used for encryption
- Bluetooth device may not have IP address!

States



- The connection establishment in Bluetooth is done in two phases- **Inquiry and page**
- Active devices are allocated a 3-bit **AMA (Active Member Address),** Parked devices are assigned an 8-bit **PMA (Parked Member Address)**, Standby devices do not need an address.

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

States

- Inquiry:
  - If two Bluetooth devices know absolutely nothing about each other, one must run an inquiry to try to **discover** the other. One device sends out the inquiry request, and any device listening for such a request will respond with its address, and possibly its name and other information.
- Paging
  - Paging is the process of forming a connection between two Bluetooth devices. Before this connection can be initiated, each device needs to know the address of the other (found in the inquiry process).
- Connection
  - After a device has completed the paging process, it enters the connection state. While connected, a device can either be actively participating or it can be put into a low power sleep mode

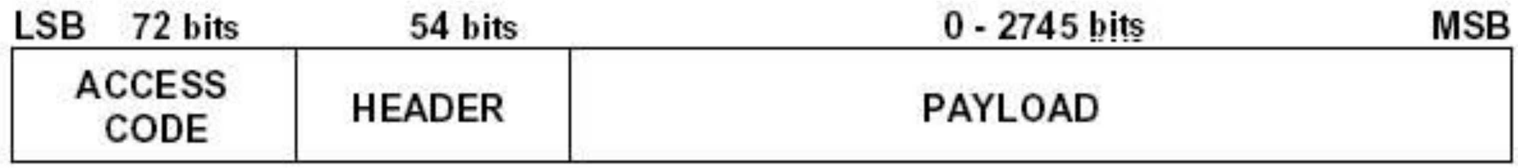
States..

- Connection States
  - Active mode
    - Listens for packet from master
    - Processes all packets from master
  - Sniff Mode
    - Listens to piconet less frequently in this mode
    - Device will sleep and only listen for transmissions at a set interval (e.g. every 100ms).
  - Hold Mode
    - Device temporarily sleeps for a defined period and then returns back to active mode when that interval has passed.
    - The master can command a slave device to hold.
  - Park Mode
    - Park is the deepest of sleep modes. A master can command a slave to “park”, and that slave will become inactive until the master tells it to wake back up
    - Releases AM_ADDR

Bonding Pairing

- Bonded devices **automatically establish a connection** whenever they’re close enough through two step process
- Pairing
  - Requires an authentication mechanism
  - Share information such as addresses, names, and profiles
  - Create temporary common security encryption key
- Bonding
  - information is stored in non-volatile memory
  - Creation and storage of permanent security keys

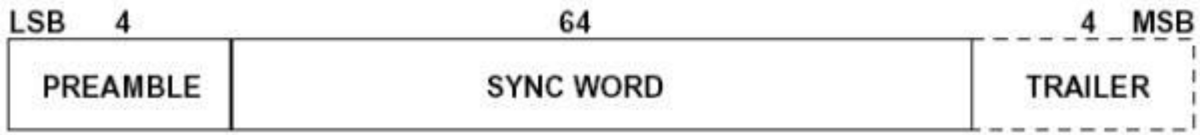
Packet Format



- Packet can contain
  - Access code
  - Access code and Header
  - Access code + Header + Payload

Packet Format

- Access code



  – Based on master’s identity and master’s system clock
  – Used for synchronization and identification
  – All packets in a piconet use the same access code
- Packet Header

  – Used for error correction, retransmission, and flow control information
  – AM_ADDR
    - 3-bit slave address
    - Temporary assigned while the slave is active and specific to piconet
    - Same in both directions
    - All zeros for broadcast

Bluetooth Low Energy (BLE)

Bluetooth Versions

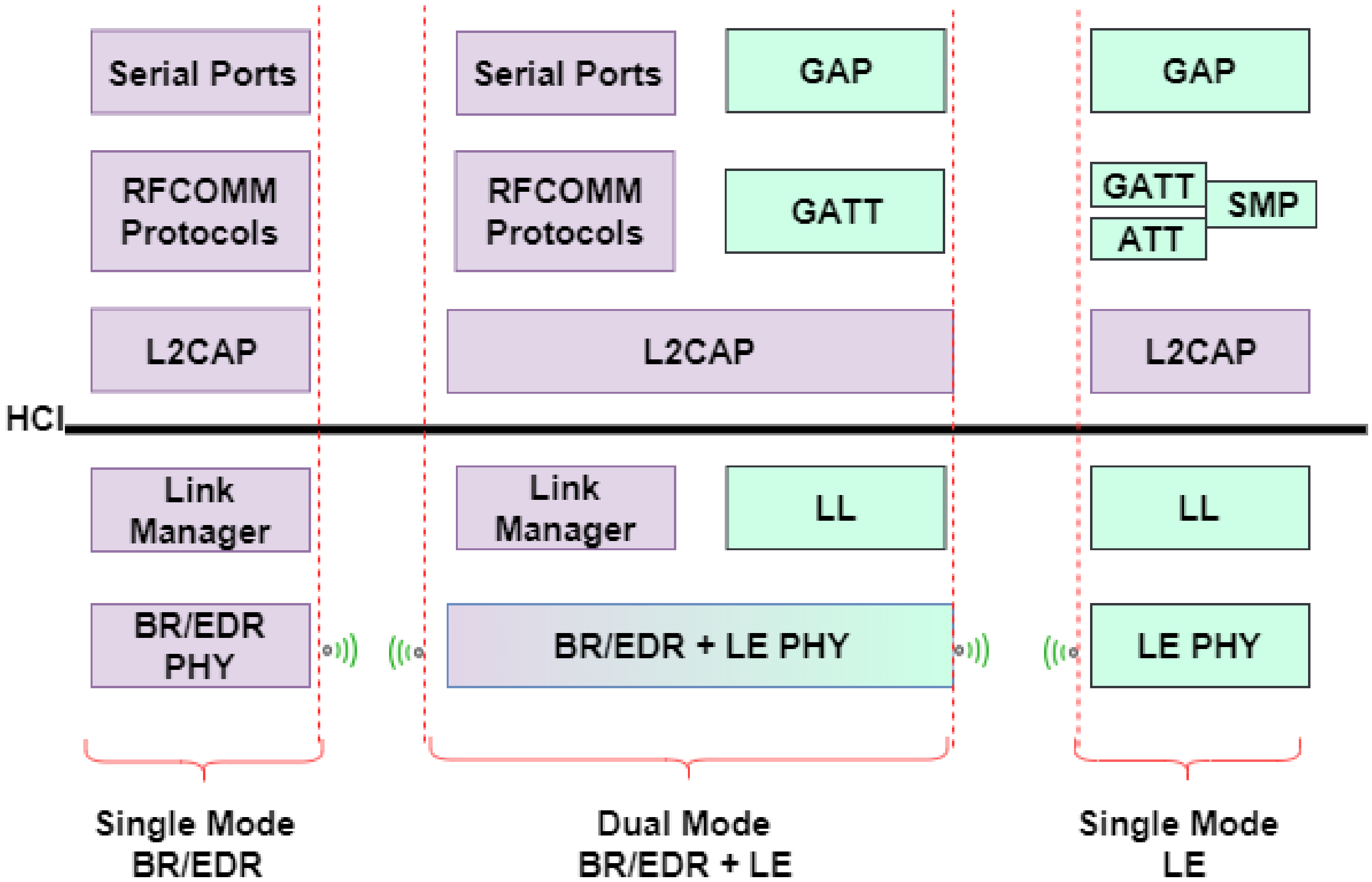
- Maintained by Bluetooth SIG
- **Bluetooth v1.2**
  - The v1.x releases laid the groundwork for future versions
  - Supported data rates of up to 1 Mbps (**Basic Rate (BR)**) using GFSK
  - 10 meter maximum range.
- **Bluetooth v2.1 + Enhanced Data Rate (EDR)**
  - The 2.x versions of Bluetooth introduced **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 (Dec. 2016)**
  - 2 * data rate, 4 * range of BLE, 8 * broadcasting capacity
  - Backward compatible with classic as well as BLE
  - V5.1 in Jan. 2019 and V.5.2 in Dec. 2019 (contains **LE Audio**), v5.3 (July 2021), v5.4 (Feb. 2023)

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.
    - Throughput is different than over the air data rate
  - Earlier versions could not carry voice. Only suited for intermittent data transmissions (no continuous data transmission)
    - V5 has LE Audio
  - Not backward compatible with Bluetooth classic
- **Bluetooth Mesh (2017)**

BLE protocol stack

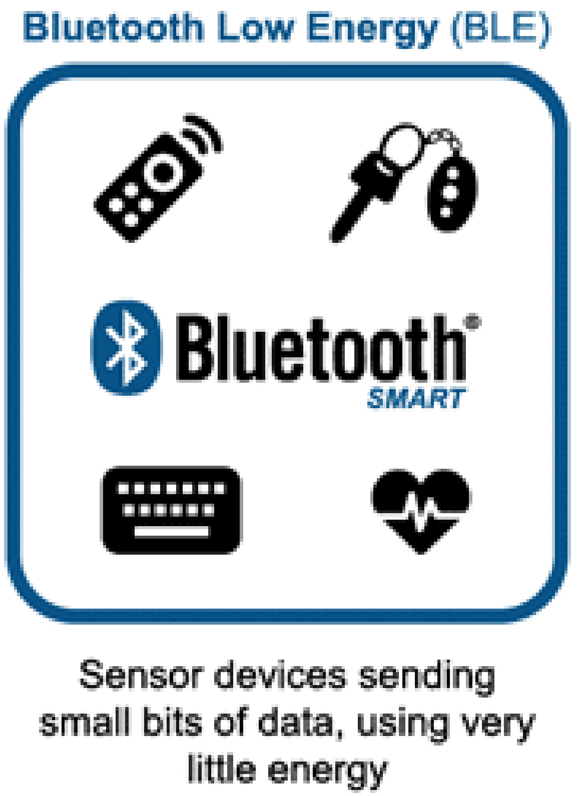
Not in Syllabus for Exam



https://www.mathworks.com/help/comm/ug/bluetooth-protocol-stack.html

Applications

- Smart home automation
  - Lighting
  - Thermostats
  - Door locks
  - Refrigerators
  - Smoke detectors
- Wearables
  - Sports and fitness bands
  - Smart watches
- Medical devices
  - Glucometer, Heart Rate Monitor
- Peripherals
  - Keyboards
  - Mouse
- Many more



Applications

Smart bulbs

Wireless Keyboards

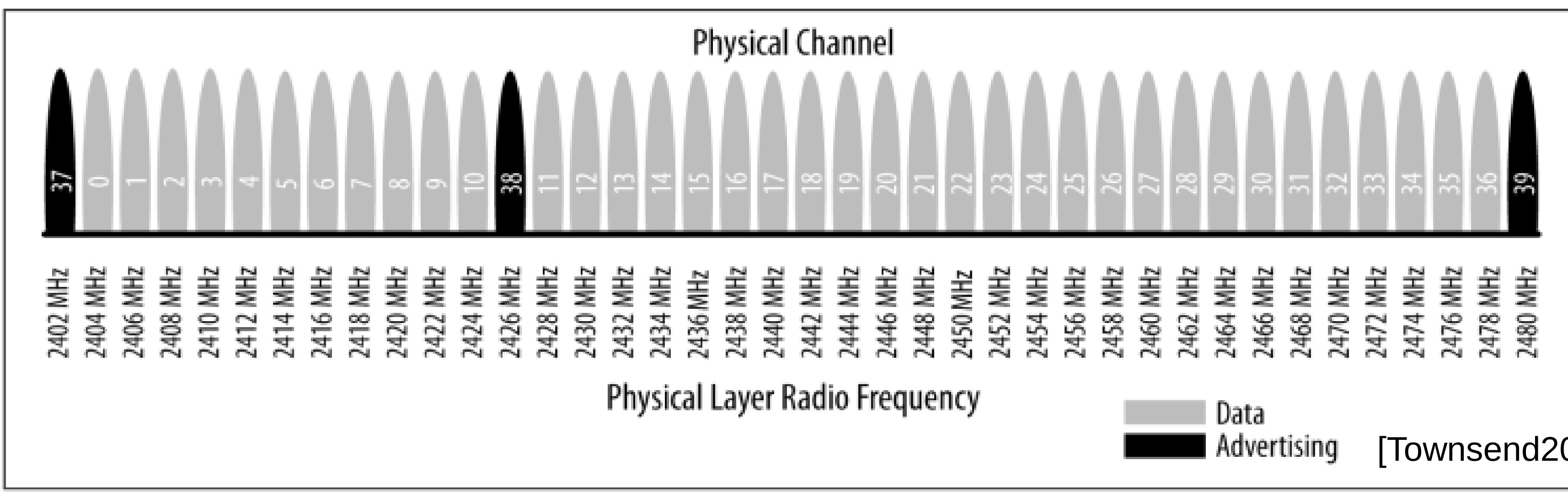
Smart Wearables

Smart Doorlocks

Batteryless
BLE Switches

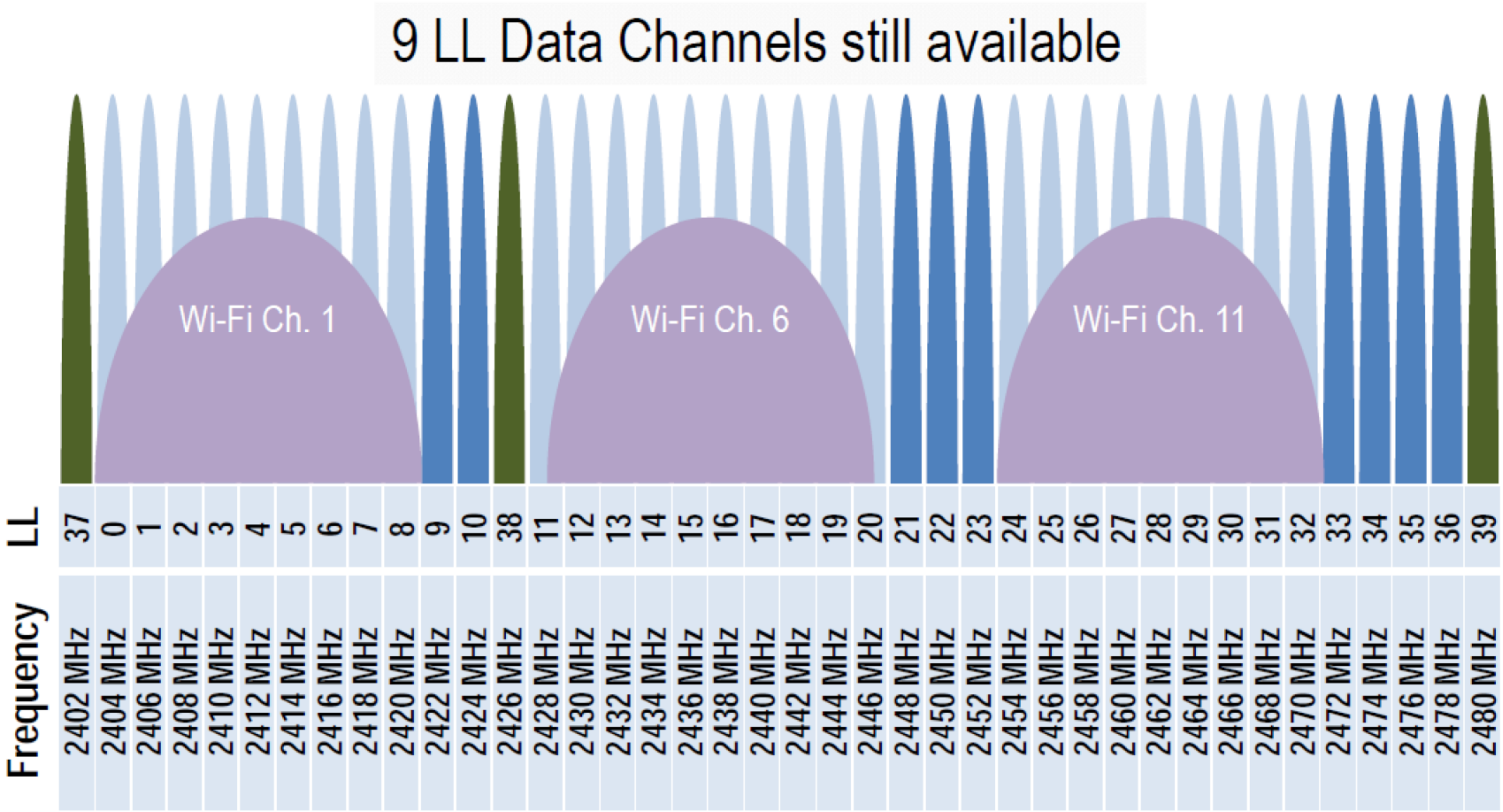
PHY Channels

- 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



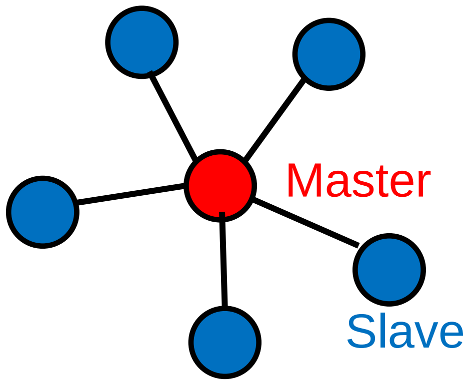
[Townsend2014]

Advertising channels avoid popular WiFi Channels

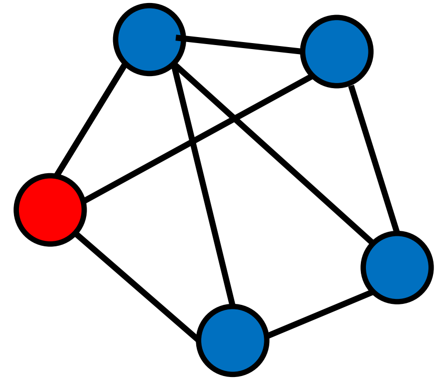


In Bluetooth 5.0, the other 37 channels can also be use as secondary advertising!

Network Topologies: Piconet and Scatternet

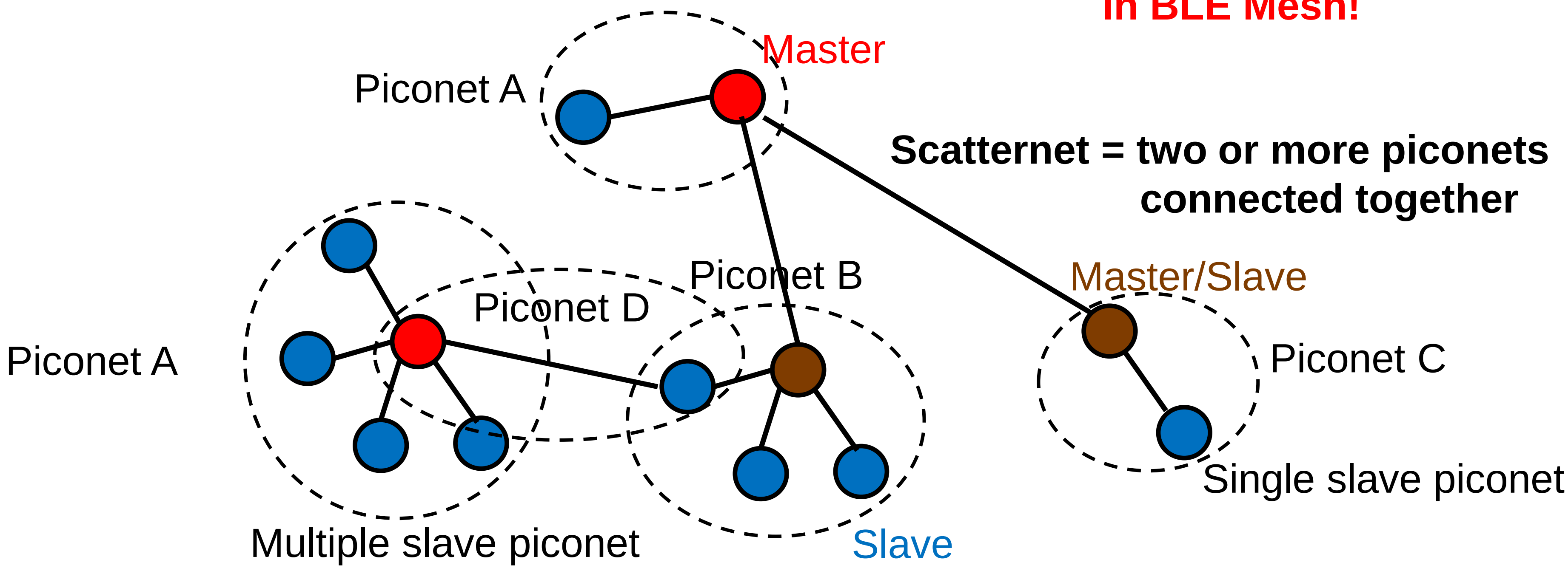


Piconet (Star)



Mesh now possible in BLE Mesh!

Scatternet = two or more piconets connected together



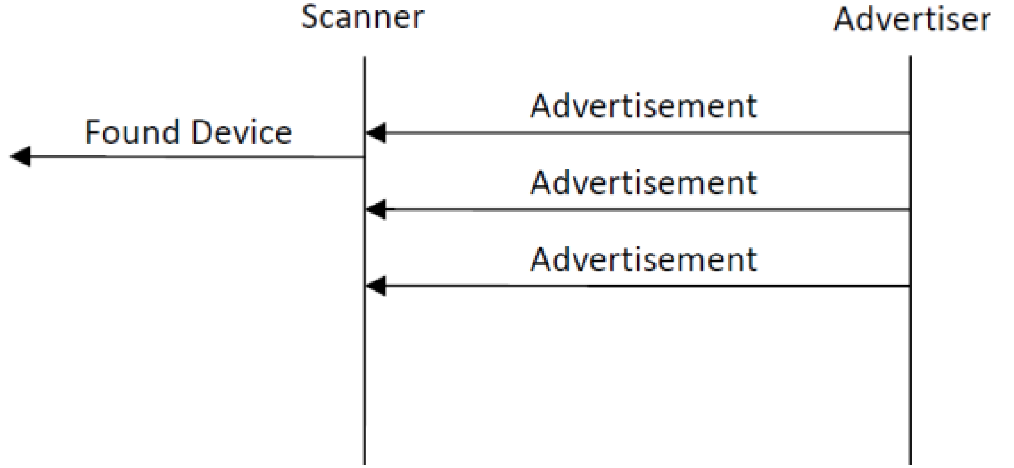
Link Layer Operations

- Advertising
- Scanning
- Connection

- BLE has only one packet format and two types of packets (advertising and data packets), which simplifies the protocol stack implementation immensely.

Advertising

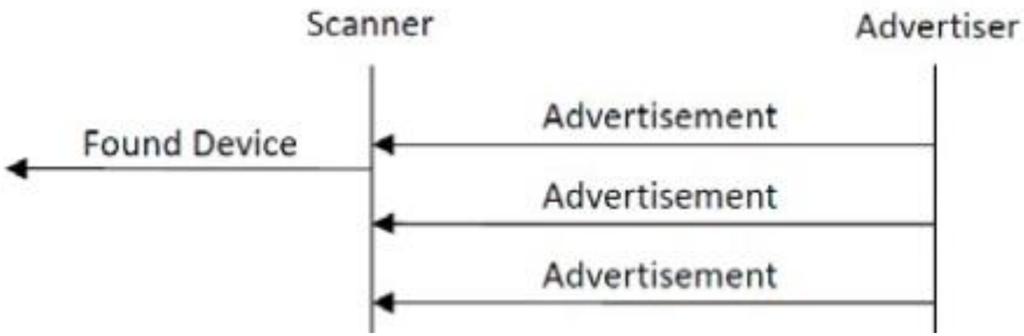
- Purpose
  - Enables devices to broadcast their presence
  - Broadcast data for applications that do not need the overhead of a full connection establishment
  - Discover devices and to connect to them
- Advertising device broadcasts packets on one or multiple advertising channels which remote devices can pick



[Silabs]

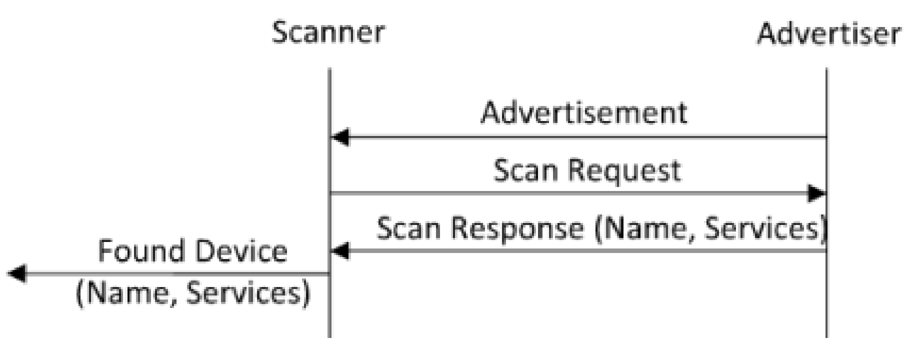
Scanning

- Passive scanning
  - Device simply listens to advertisement
  - Scans through the advertisement channels in round robin fashion



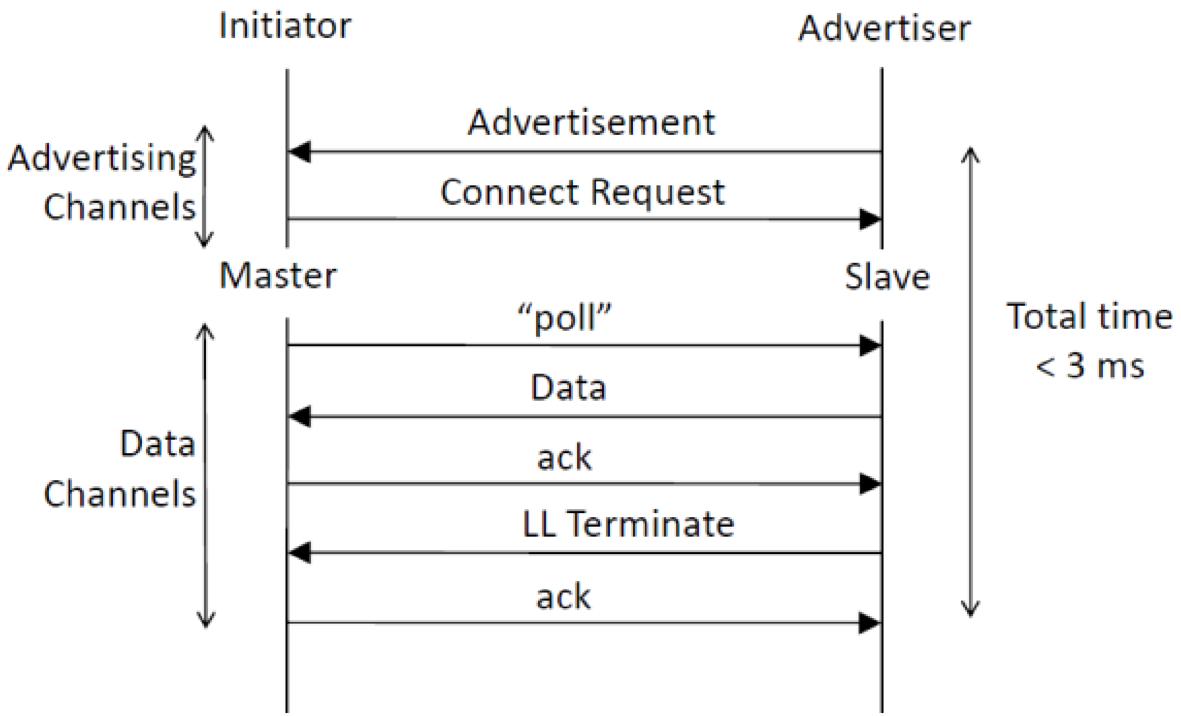
[Silabs]

- Active scanning
  - In addition to basic scanning, requests for more information



[Silabs]

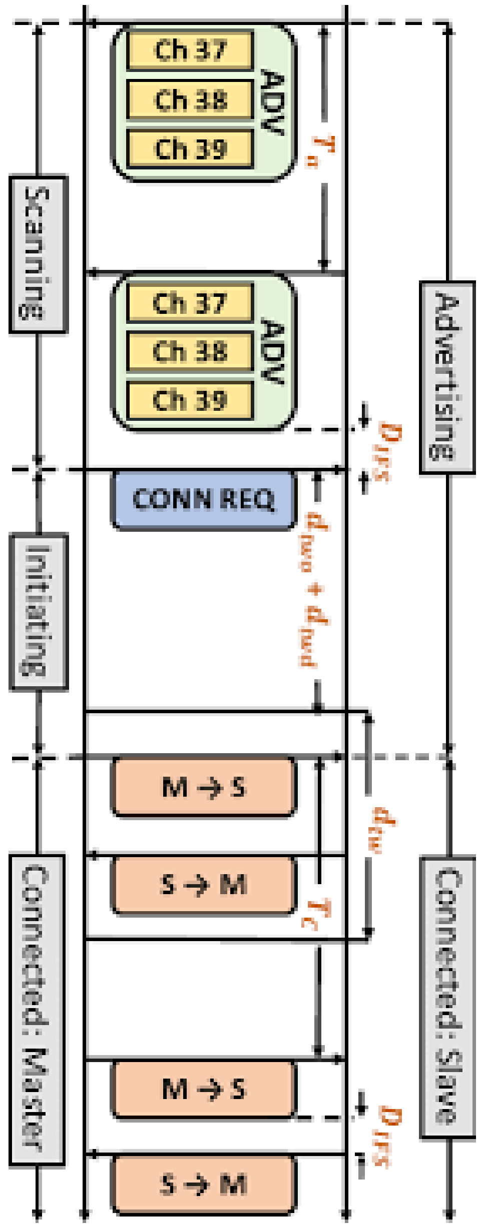
Connection Establishment



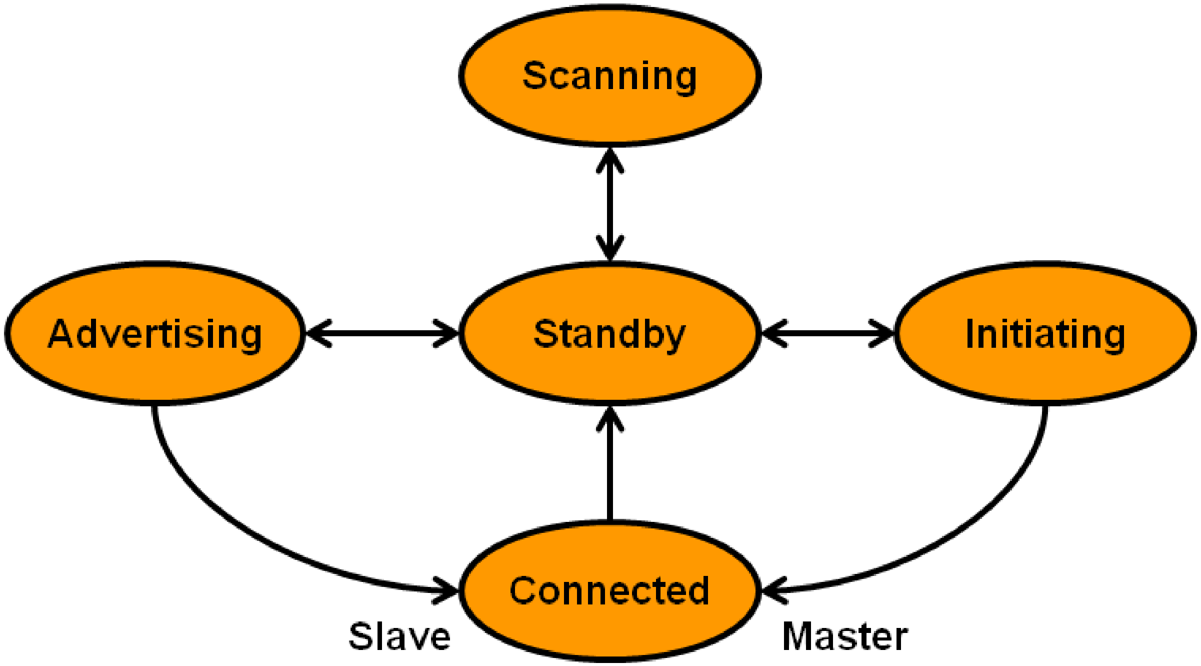
[Silabs]

- Reliable data transfer: use of CRC, acknowledgments and retransmissions
- Adaptive frequency hopping

Connection Establishment



Link Layer States



Bluetooth 5 enhancements

Not in Syllabus for Exam

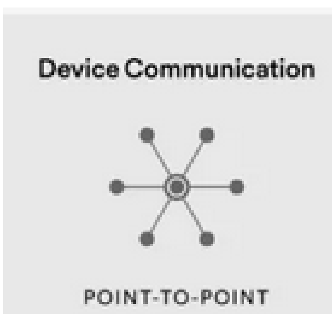
- New physical layers
  - LE Coded PHY
    - Longer range transmissions with no increase in power
  - LE 2M PHY
    - Higher data rates with 2M symbols per second
- Extended advertising
- Improved frequency hopping
  - New channel selection algorithm 2 (CSA2)
- Slot availability mask (SAM)
  - For BR/EDR

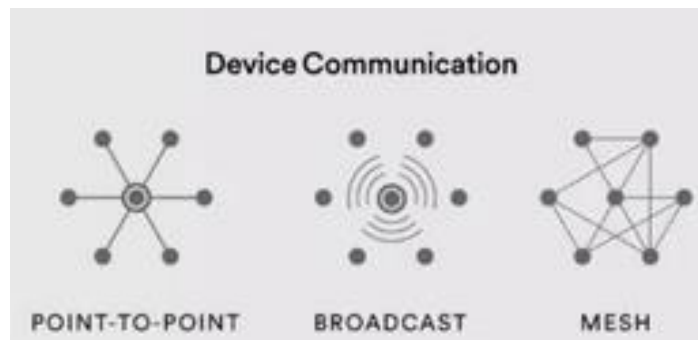
BLE 5: New PHY

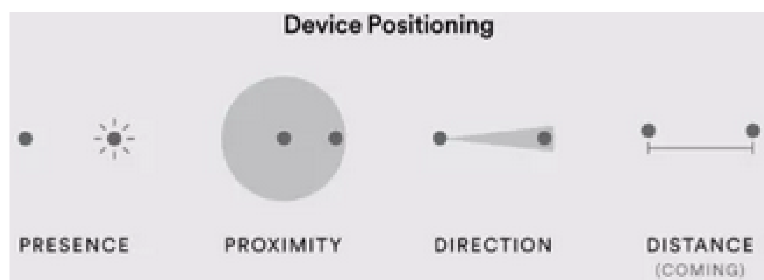
Not in Syllabus for Exam

	LE 1M	LE Coded S=2	LE Coded S=8	LE 2M
Symbol Rate	1 Ms/s	1 Ms/s	1 Ms/s	2 Ms/s
Protocol Data Rate	1 Mbit/s	500 Kbit/s	125 Kbit/s	2 Mbit/s
Approximate Max. Application Data Rate	800 kbps	400 kbps	100 kbps	1400 kbps
Error Detection	CRC	CRC	CRC	CRC
Error Correction	NONE	FEC	FEC	NONE
Range Multiplier (approx.)	1	2	4	0.8
Requirement	Mandatory	Optional	Optional	Optional

Comparison between classic and BLE







	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

Not in Syllabus for Exam

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

BLE Beacons

- Advertise some information on a periodic basis
  - Channels 37, 38. 39
- Only one way transmissions
  - Cannot connect or pair with other devices
    - Connection will stop advertising and no other device will be able to listen to them
  - Beacons cannot track user
  - Only the installed app can
- Beacons can transmit calibrated RSSI at one meter
- Period can be in the order of 100ms

Three use cases for beaconing

- Static point of interest
  - Distributing messages at the point of interest
  - Retail, Museum
  - Mobile payment through PoS
- Broadcasting telemetry data
  - In Eddystone, telemetry data regarding the beacon like battery level, time since power-on, advertisement count
- Indoor localization and geolocation services
  - Indoor positioning system
  - Key finder
  - Asset tracking and logistics

Key IoT features of BLE

Advantages

- Low power: years on button battery
- Small size and low cost (License free)
- Ubiquitous
- Connectivity to mobile phones
- Security: AES 128 bit

Issues

- Low range
- Low data rates: No voice or video capability
  - Now possible on low quality: https://www.youtube.com/watch?v=eqAFVi16l5E
- Roaming
- Security
  - Wearables, Smart locks: https://www.tomsguide.com/us/bluetooth-lock-hacks-defcon2016,news-23129.html

BLE Use Case: COVID-19 management

Reducing the Risk of COVID-19 Transmission Using Philips' Biosensor BX100 and Cassia's Bluetooth Gateways

- https://www.cassianetworks.com/wp-content/uploads/2020/09/Philips-and-Cassia-Networks-Case-Study.pdf
- Deployed in a major Dutch hospital
- 40 BLE paired simultaneously
- 300 meters coverage in open space for the AP
- Continuous patient monitoring

BLE Use Case: Avia Smart Lock

- Multipoint locks
- Home kit integration
- Uses BL654 BLE module
- Bluetooth 5
- AES-256 encryption with Diffie-Hellman pairing
- ARM Cryptocell™-310 cryptographic accelerator
  – several high-level cryptographic functions that are key to strong wireless security, such as true random number generation, hashing functions, and public key cryptography.

https://www.lairdconnect.com/resources/case-studies/mightons-avia-smartlock-provides-unparalleled-security-laird-connectivitys-family-bluetooth-5

BLE Use Case: Smart Hospital Wayfinding

- Digital wayfinding at an NYC hospital complex
  - https://www.pointr.tech/blog/smart-hospital-wayfinding-cisco-dna-spaces
- Use of blue-dots for accurate position (<1m) in a big complex of multi-floor building

Good References

[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

[Bluetooth5Pt1] Bluetooth Core Specification ver5.1, Bluetooth SIG, Jan. 2019

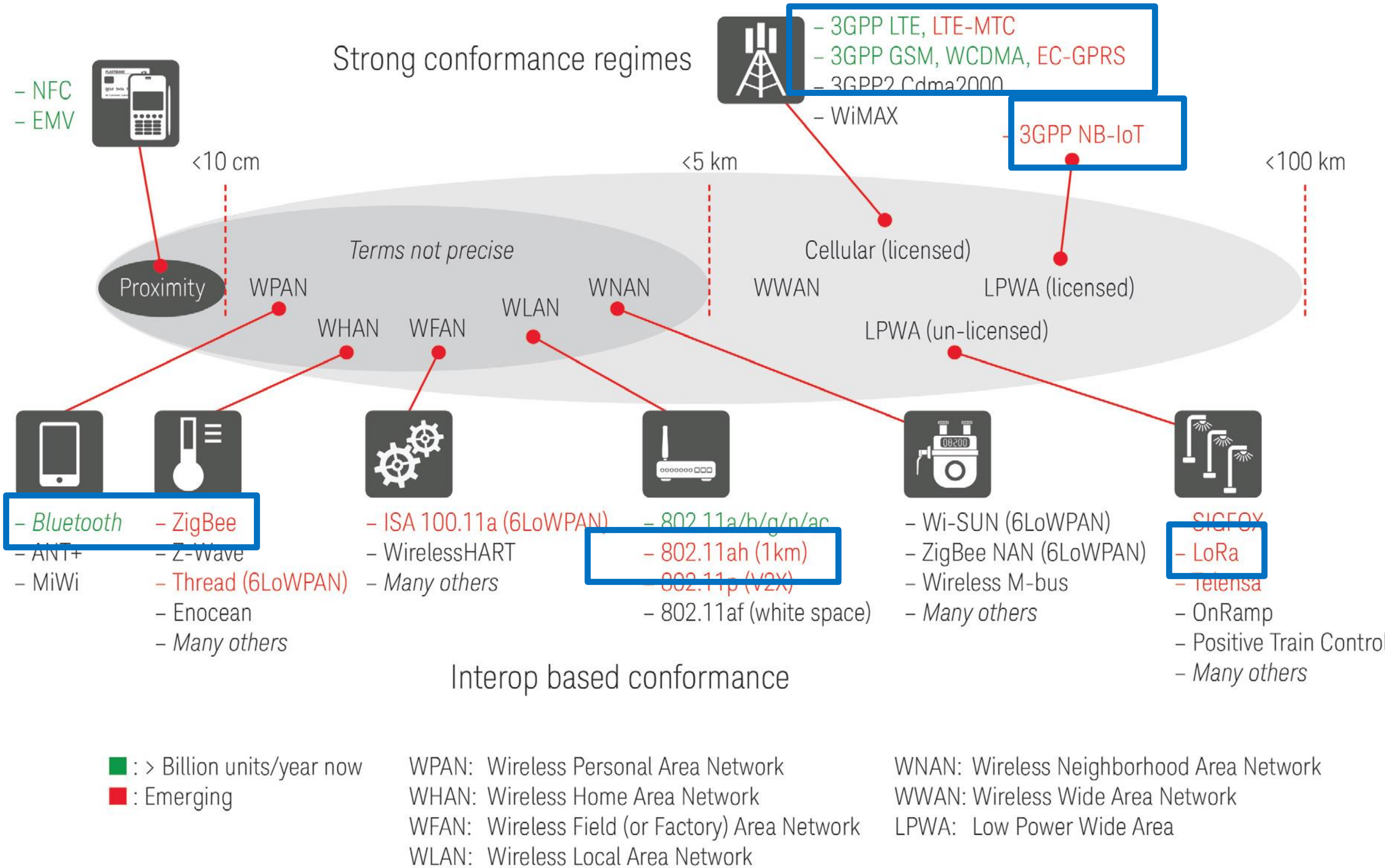
[Bluetooth5] M. Wooley, “Bluetooth Core Specification Version 5.0 Feature Enhancements”, *Bluetooth Resources*, Sept. 2021

[Signils] Online, https://www.signils.com/whats-the-difference-between-classic-bluetooth-and-bluetooth-low-energy/ Accessed: 30 Dec 2021

Questions?

Comparison of Different 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

Issues in IoT from Communication Perspective

[Not an exhaustive list!]

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

Key IoT Features (802.11ah)

- Highest data rates
  - Can handle diverse range of applications including camera
- Longer range (1 Km)
- Scalable to thousands of nodes
- WiFi family widely used

Issues

- Most of the world is using 2.4 GHz
- Very few 802.11ah products available
  - Mostly using 802.11b/g/n
- Security *(Popularity)*
- High power consumption
- Roaming

Key IoT Features (Cellular)

Advantages

- **Quality of service**
  - Licensed band, Low latency
- **Ubiquitous**
- **Present on Phone, Convergence**
- **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

Key IoT Features (LoRaWAN)

- Designed for majority of IoT applications
- **Low powered sensors (Battery life of 2-5 years)**
  - Class A and B
- **Wide coverage area up to 15 Kms**
- **Low Costs**
  - free(unlicensed) frequencies
- One gateway can support thousands of end devices
- **Simple Architecture**
- Security: a layer of security for the network and one for the application with AES encryption.
- **Localization without GPS**
- **Roaming**
- LoRa Alliance: 500+ members companies including IBM and Cisco

IoT Features: *Disadvantages (LoRaWAN)*

- **Payload limited to 100 bytes**
- High latency (actuators are not possible)
- Low data rates
  - Does not support voice or video
- **Low duty cycles (1% in EU)**
- Interference issues
  - Unlicensed frequency for other technology users
  - Crowding of LoRaWAN gateways increase interference
  - High packet error rate
- Cost in terms of cloud-based servers for network and applications
  - Things Network, LoRIoT
- Needs fair amount of development work
  - DIY; Not a complete protocol stack
- Not for continuous or real-time monitoring and actuations (most of industry cases)
  - High latency (actuators are not possible), High packet error rate, Low data rates, Low duty cycles

Key IoT Features (BLE)

Advantages

- **Low power: years on button battery**
- **Small size and low cost (License free)**
- **Ubiquitous**
- **Connectivity to mobile phones**
- Decent Security (AES 128 bit)

Issues

- Low range
- Low data rates: No voice or video capability
  - Now possible on low quality: https://www.youtube.com/watch?v=eqAFVi16l5E
- Roaming
- Security
  - Wearables, Smart locks: https://www.tomsguide.com/us/bluetooth-lock-hacks-defcon2016,news-23129.html

Key IoT Features (IEEE 802.15.4)

Advantages

- **Low power**
- Large coverage of 1 Km 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)
- Decent Security (AES 128 bit)

Issues

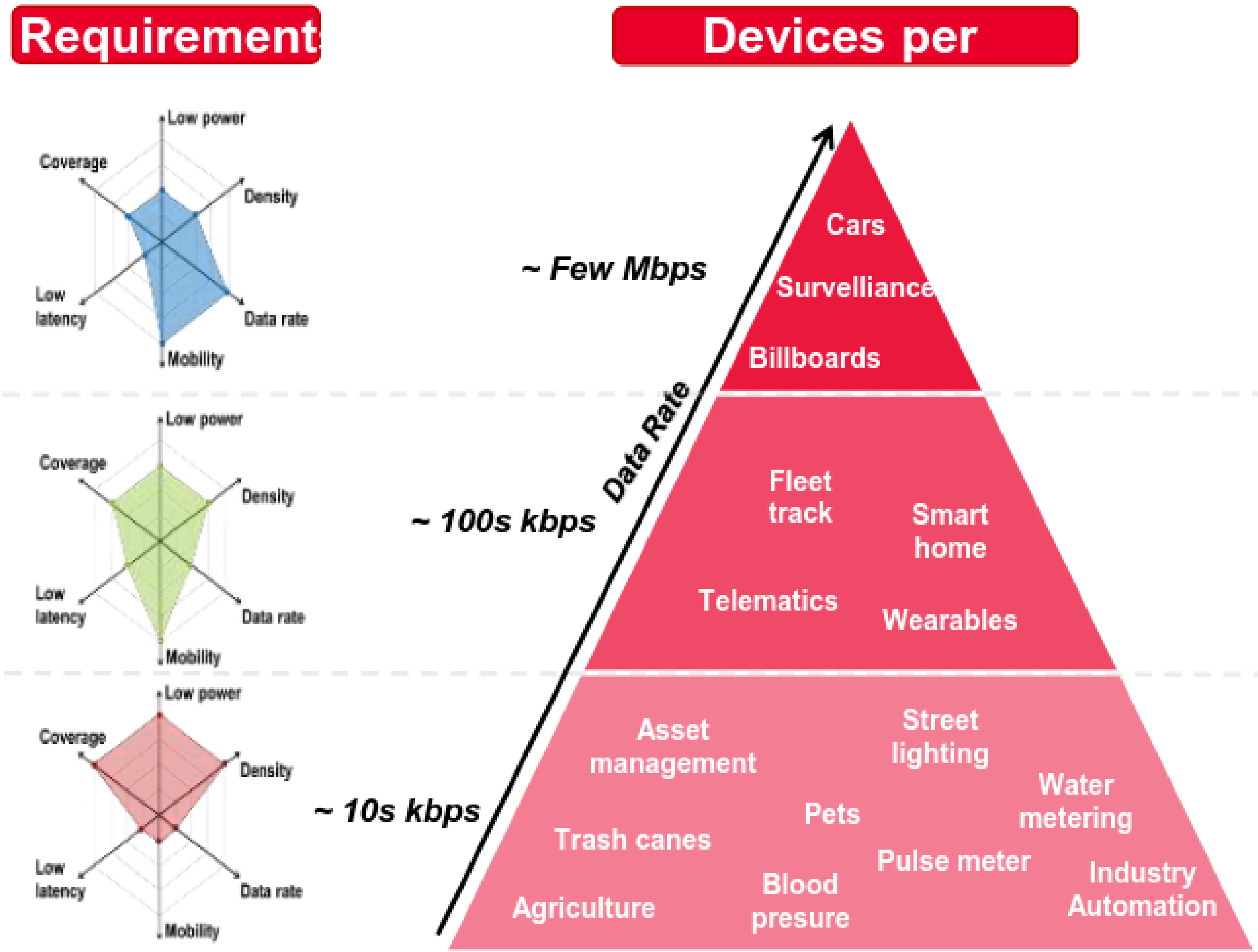
- No mobility support, Scalability
- Less coverage area in 2.4 GHz band
- Not part of mobile phones

WiSUN Features

- Both star and mesh topologies are possible
  - Powerful use of mesh topology
    - One cluster of 5000 sensor nodes in 1 Km range
- Unlicensed band operation
- Leverages IPv6
- Can be designed for frequent communications
  - Every 10 secs
- Low latency of about 0.02-1 secs
- Data rates of upto 300 Kbps
- Coverage of 4 Km point-to-point using 1W non-directional antenna
- Security at multiple levels
  - Native public-key infrastructure (PKI) integration providing security certification capabilities for each device
- Networks designed for long lifecycle
  - Low power design (15-20 year battery target)
  - Backward and forward compatibility with different generations

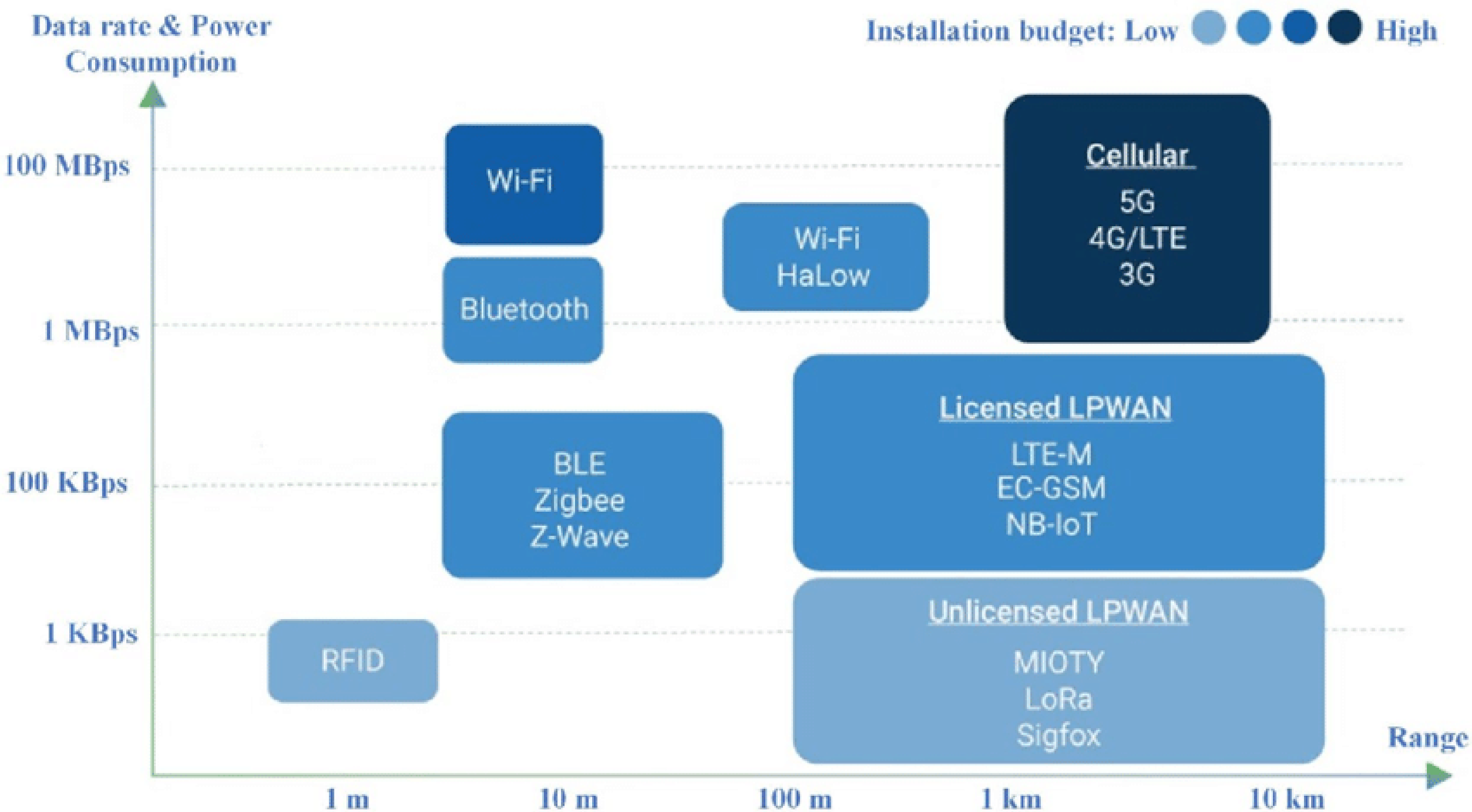
	IEEE 802.15.4	IEEE 802.11ah	BLE	NB-IoT	LoRaWAN
Bands	868, 915 MHz 2.4 GHz (ISM)	900 MHz (ISM)	2.4 GHz (ISM)	Between 400-2200 MHz (Licensed Frequency)	868/915/433 MHz (ISM)
Topology	Star, Mesh, Cluster Tree	Star, Mesh, Cluster-Tree	Piconet, Scatternet, Mesh	Star	Star of Stars
Max. Range	1 Km	1 Km	100 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. No. 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

One size does not fit all!



- IoT is a very broad field with too diverse requirements!
- Different applications have different requirements !

Competing and Complementing



https://industrytoday.com/best-uses-of-wireless-iot-communication-technology/

IoT market is diverse and big to accommodate several technologies!

Comparison

- Current trends
  - Indoor: WiFi, BLE, IEEE 802.15.4
  - Outdoor: Cellular, LoRaWAN, WiSUN, WiFi (Halow)
- On-mobile advantage
  - Cellular, WiFi, and BLE
- Lead advantage
  - WiFi, BLE, and LoRaWAN
- Ecosystem advantage
  - Cellular
    - Convergence of applications

Use Cases (Personal Assessment)

- Smart Metering
  - All Technologies
- Agriculture
  - LoRaWAN and then Cellular
- Mining
  - LoRaWAN and then Cellular
- Asset Tracking
  - Indoors or Jobsites
    - Since long time, RFID and Barcode
    - Bluetooth tags for construction tools
  - Outdoors (Vehicles, machinery, containers, tools):
    - Mostly cellular: https://www.hologram.io/blog/10-best-iot-asset-tracking-systems
    - LoRaWan based GPS tracker (Tata), https://iot.tatacommunications.com/product/gps-tracker
- Wearables
  - All Technologies
  - Bluetooth dominant and cellular

Few More Use Cases

- Smart Home
  - Metering: All technologies
  - Lighting: BLE, WiFi, Cellular, WiSUN
    - Signify has smart bulbs based on BLE, WiFi, and Zigbee
- Smart City
  - Street lighting: WiSUN (London example), LoRaWAN (Bordeaux), Cellular IoT (Australia)
  - Parking
  - Waste Management
- Forest: LoRaWAN

Smart Metering

- WiFi:
  - Acrel
  - AmiciSmart3
  - Kigg
- LoRaWAN:
  - Acrel
- Cellular: NB-IoT, LTE-M
  - Digikey Link
  - Acrel (4G)
  - Sierra Wireless (NB-IoT and LTE-M)
  - Kigg
- BLE:
  - Kigg
- IEEE 802.15.4
  - Kigg
- PLC
  - Kigg

Mines

Semtech's LoRa Technology Enabling Smarter Mining Solutions from Transco Industries Inc.

Small and durable LoRa-enabled sensors monitor data in real-time to prevent costly conveyor damage and fires

https://www.semtech.com/company/press/semtechs-lora-technology-enabling-smarter-mining-solutions-from-transco-industries-inc

5G for healthcare

- 5G (not NB-IoT and LTE-M) is going to make these applications wide-spread
  - Telemedicine
  - Large file transfer
  - Improving augmented / virtual reality
  - Real time monitoring

https://www.business.att.com/learn/updates/how-5g-will-transform-the-healthcare-industry.html

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

[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

That’s all for today!
Thank You!