

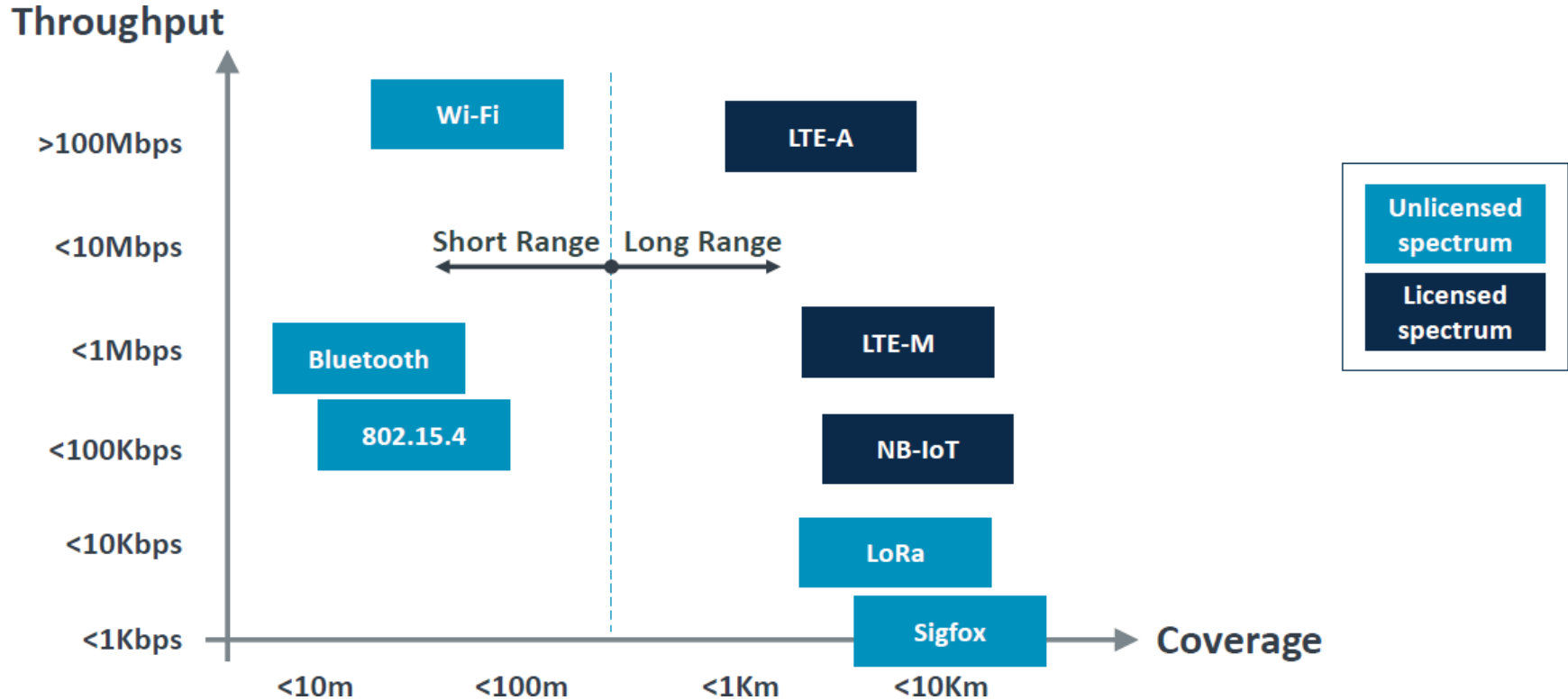
PROIECTAREA CU MICROPROCESOARE

Cursul 9

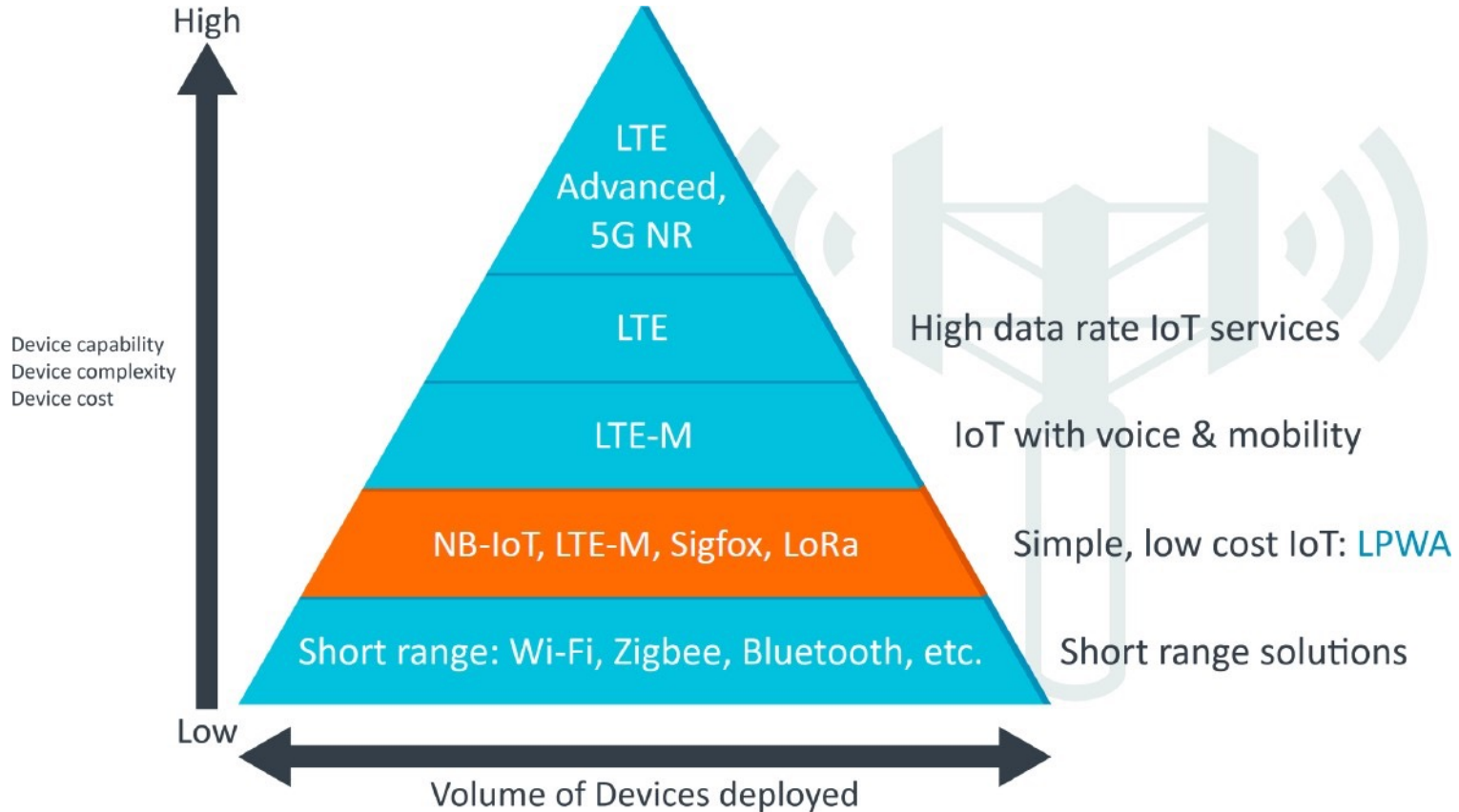
WiFi, Bluetooth, Zigbee, LTE, LoRA

Facultatea de Automatică și Calculatoare
Politehnica București

Wireless connectivity technologies



The wireless connectivity pyramid



Bluetooth

- Started with Ericsson's Bluetooth Project in 1994 for radio-communication between cell phones over short distances
 - Named after Danish king Harald Blatand (AD 940-981)
 - Intel, IBM, Nokia, Toshiba, and Ericsson formed Bluetooth Special Interest Group (SIG) in May 1998
 - Version 1.0A of the specification came out in late 1999
 - IEEE 802.15.1 approved in early 2002 is based on Bluetooth. Later versions handled by Bluetooth SIG directly
 - Key Features:
 - Lower Power: 10 mA in standby, 50 mA while transmitting
 - Cheap: \$5 per device
 - Small: 9 mm² single chips
-

Bluetooth

- Radio band: 2.4-2.48 GHz
- Average 1Mbps - up to 3Mbps
- Supports point-to-point and point-to-multipoint
 - Creates personal area networks (PANs/Piconets)
 - Connects up to 8 devices simultaneously
- Minimal interference between devices
 - **Devices alter frequencies arbitrarily after packet exchanges - up to 1600 times/second - frequency hopping**
- 3 classes of Bluetooth transmit power

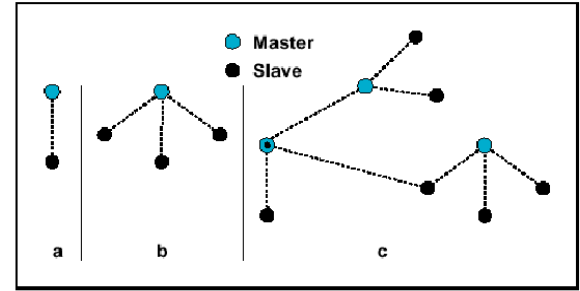


Figure 1.2: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c).

Class	Maximum Power	Operating Range
Class 1	100mW (20dBm)	100 meters
Class 2	2.5mW (4dBm)	10 meters
Class 3	1mW (0dBm)	1 meter

Frequency hopping communication was invented by actress Hedy Lamar

UNITED STATES PATENT OFFICE

2,292,387

SECRET COMMUNICATION SYSTEM

Hedy Kiesler Markey, Los Angeles, and George
Antheil, Manhattan Beach, Calif.

Application June 10, 1941, Serial No. 397,412

6 Claims. (Cl. 250—2)

This invention relates broadly to secret communication systems involving the use of carrier waves of different frequencies, and is especially useful in the remote control of dirigible craft.

Fig. 2 is a schematic diagram of the apparatus at a receiving station;

Fig. 3 is a schematic diagram illustrating a starting circuit for starting the motors at the



Bluetooth Versions

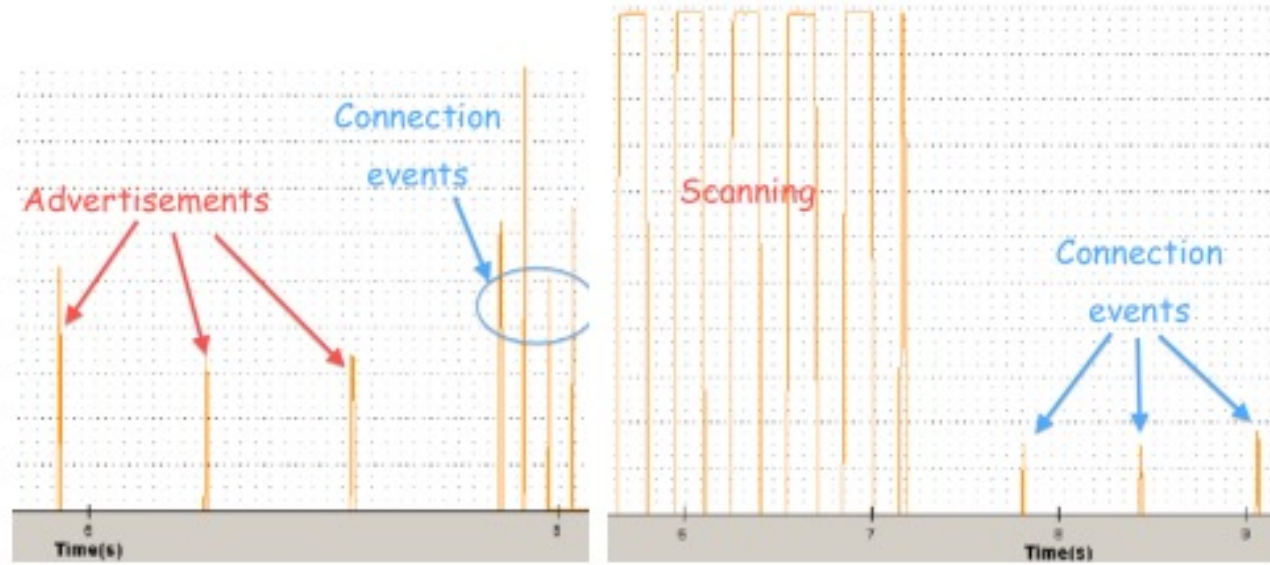
- **Bluetooth 1.1:** IEEE 802.15.1-2002
 - **Bluetooth 1.2:** IEEE 802.15.1-2005. Completed Nov 2003. Extended SCO, Higher variable rate retransmission for SCO + Adaptive frequency hopping (avoid frequencies with interference)
 - **Bluetooth 2.0 + Enhanced Data Rate (EDR)** (Nov 2004): 3 Mbps using DPSK. For video applications. Reduced power due to reduced duty cycle
 - **Bluetooth 2.1 + EDR** (July 2007): Secure Simple Pairing to speed up pairing
 - **Bluetooth 3.0+ High Speed (HS)** (April 2009): 24 Mbps using WiFi PHY + Bluetooth PHY for lower rates
 - **Bluetooth 4.0** (June 2010): Low energy. Smaller devices requiring longer battery life (several years). New incompatible PHY. Bluetooth Smart or BLE
 - **Bluetooth 4.1:** 4.0 + Core Specification Amendments (CSA) 1, 2, 3, 4
 - **Bluetooth 4.2** (Dec 2014): Larger packets, security/privacy, IPv6 profile
 - **Bluetooth 5** (2016): Improved energy consumption, increased range (200m)
-

Bluetooth low energy

- From 2001 – 2006 Nokia asked:
 - How do we design a radio that can transmit short bursts of data for months or years *only being powered by a coin cell battery?*
 - **The answer is: Keep the radio asleep mode most of the time!**
 1. Advertise on only one of three channels
 2. Transmit quickly at 1 Mbit/s
 3. Make the minimum time to send data only 3 msec
 4. Make a very predictable time when the device accepts connections
 5. Limit the max transmit power to 10 mW
 6. However, don't sacrifice security: AES 128-bit
-

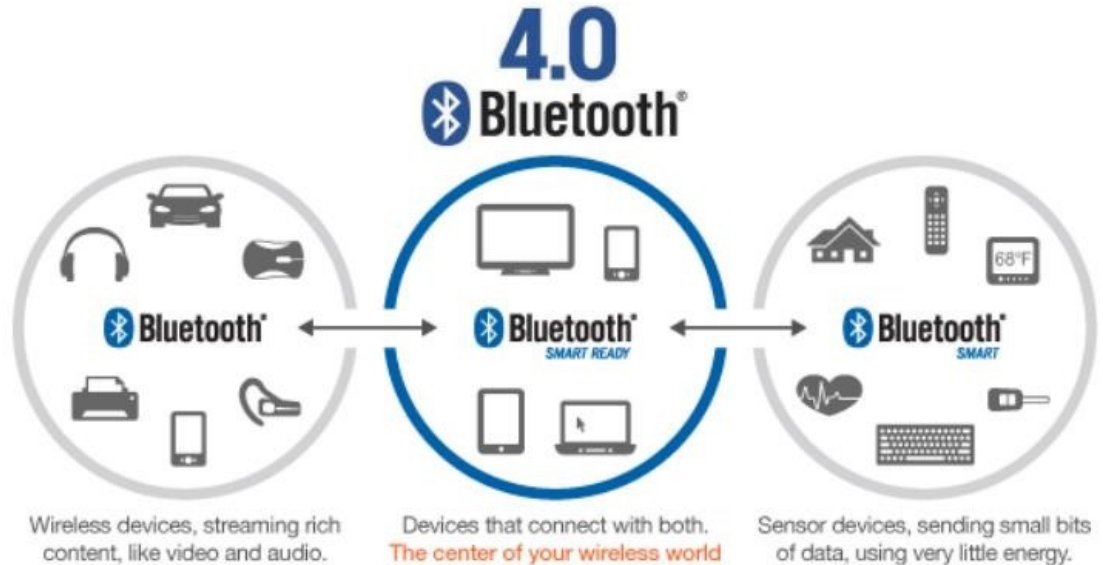
What tradeoffs were made?

- The protocol is designed for transmitting tiny data
- 4 operations: Read, Write, Notify, Indicate
- Maximum of 20 bytes of data per packet



Naming for Bluetooth 4.x

- Bluetooth 4.0
- Bluetooth Low Energy
 - BLE, BTLE, LE
- SIG Preferred
 - Bluetooth Smart
 - Bluetooth Smart Ready



Bluetooth Low Energy (BLE)

- **Low Energy:** 1% to 50% of Bluetooth classic
 - **For short broadcast:** Your body temperature, Heart rate, Wearables, sensors, automotive, industrial
Not for voice/video, file transfers, ...
 - **Small messages:** 1Mbps data rate but throughput not critical
 - **Battery life:** In years from coin cells
 - **Simple:** Star topology. No scatter nets, mesh, ...
 - **Lower cost** than Bluetooth classic
 - New protocol design based on Nokia's **WiBree** technology
 - Shares the same 2.4GHz radio as Bluetooth - Dual mode chips
 - All smartphones (iPhone, Android, ...) have dual-mode chips
-

BLE Roles

Master

Client

*Can read/write data to
Slave/Server*



Central



Peripheral

Slave

Server

Has read/write data

Can receive broadcast data



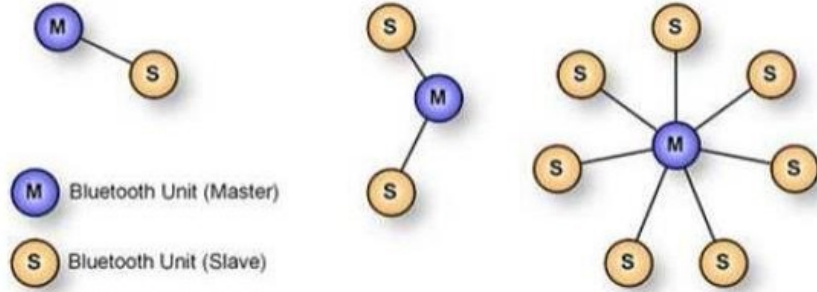
Observer



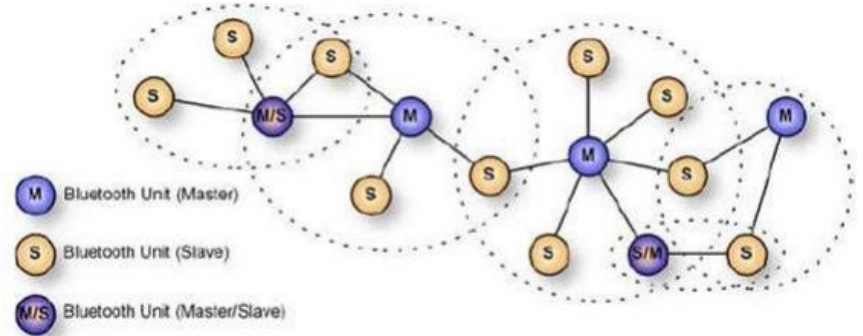
Broadcaster

Has read-only broadcast data

Network Topology

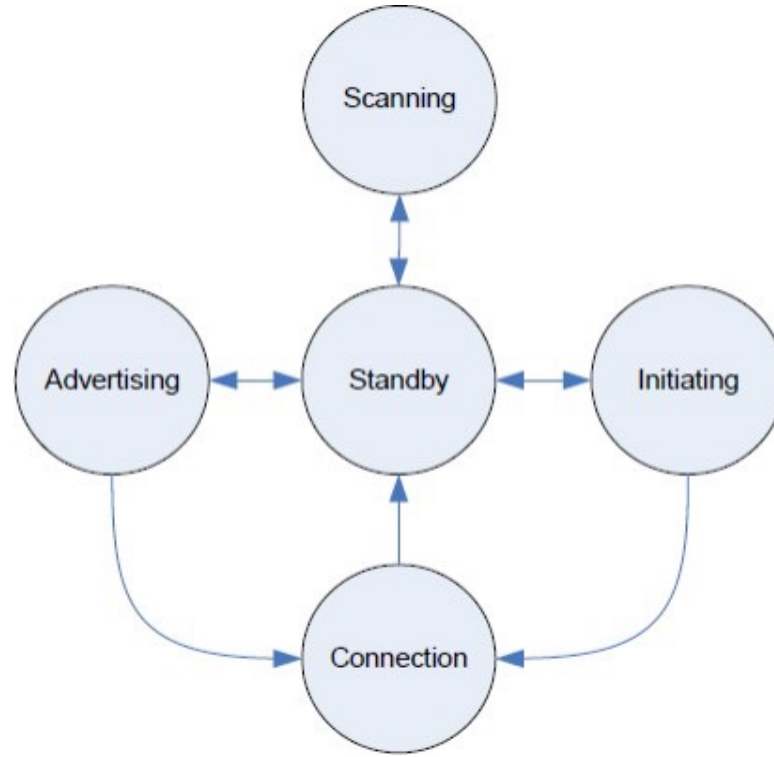


Piconet v4.0



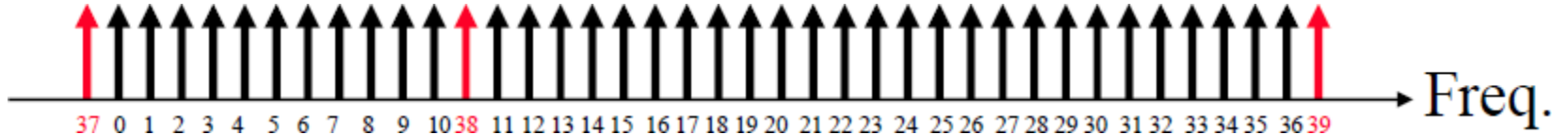
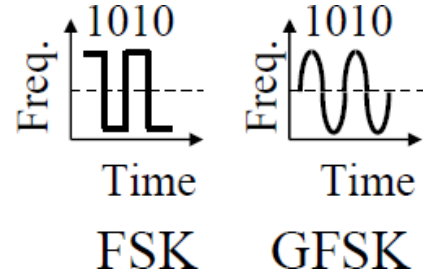
Scatter net v4.1

BLE Power Status



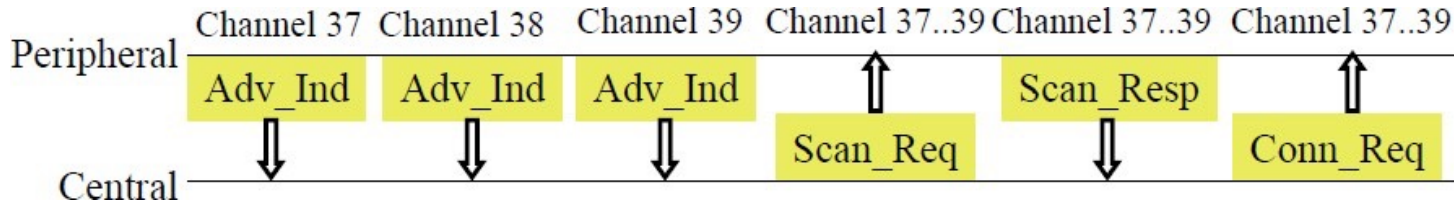
Bluetooth Smart PHY

- 2.4 GHz. 150 m open field
- Star topology
- 1 Mbps Gaussian Frequency Shift Keying.
- Better range than Bluetooth classic
- Adaptive Frequency hopping. 40 Channels with 2 MHz spacing
- 3 channels reserved for advertizing and 37 channels for data
- Advertising channels specially selected to avoid interference with WiFi channels

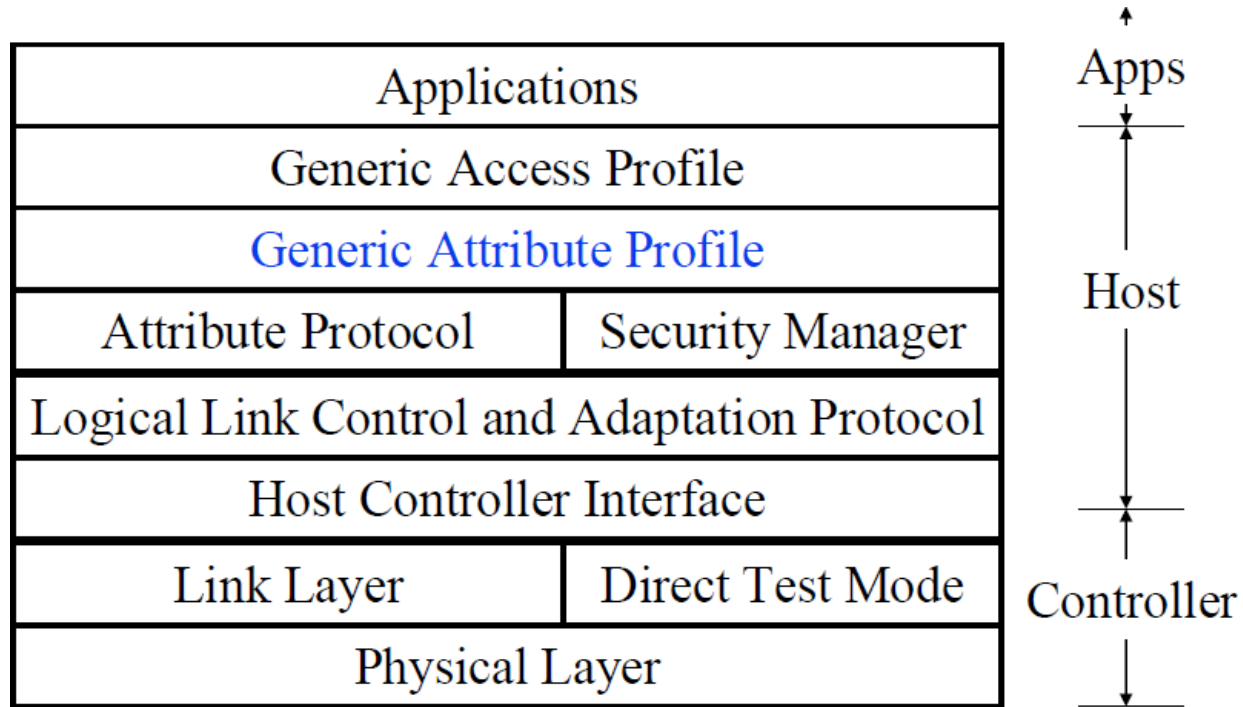


Bluetooth Low Energy MAC

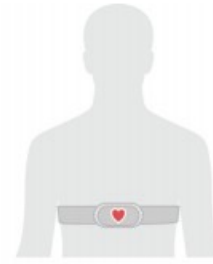
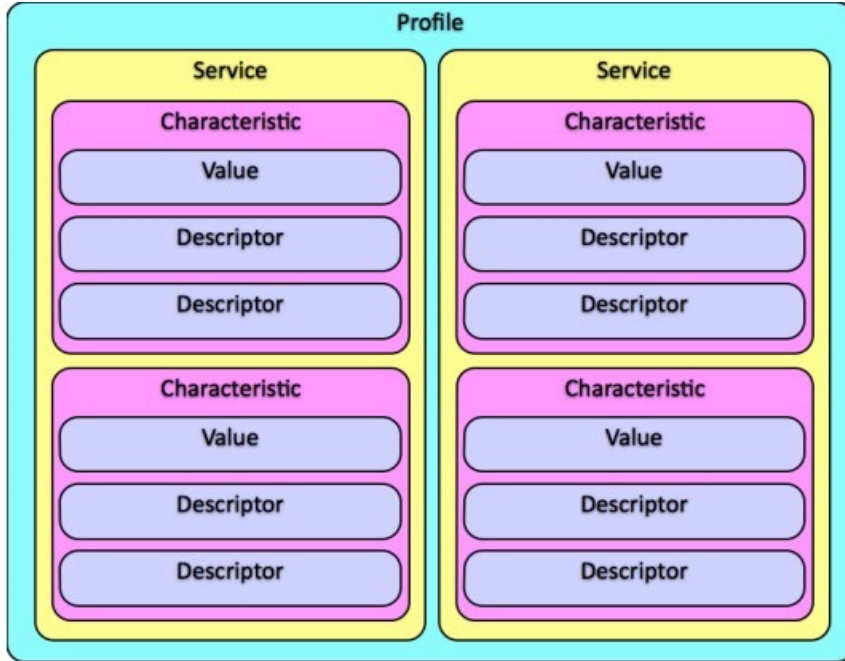
- Two Device Types: “**Peripherals**” simpler than “**central**”
- Two PDU Types: Advertising, Data
- **Non-Connectable Advertising**: Broadcast data in clear
- **Discoverable Advertising**: Central may request more information. Peripheral can send data without connection
- **General Advertising**: Broadcast presence wanting to connect. Central may request a short connection.
- **Directed Advertising**: Transmit signed data to a previously connected master



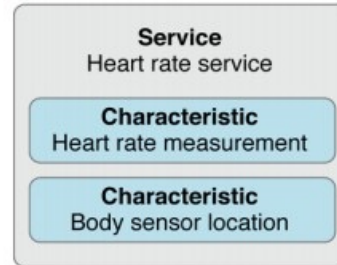
Bluetooth Low Energy Protocol Stack



Generic Attribute Profile - GATT



Peripheral



Services, characteristics, and descriptors are collectively referred to as *attributes*, and identified by [UUIDs](#). 16 bits (e.g. "180A") or 128 bits (e.g. "6BCF0ED3-68E3-4804-96D5-5AB8765FB9BC ")

GATT Operations

- Central can
 - Discover UUIDs for all primary services
 - Find a service with a given UUID
 - Find secondary services for a given primary service
 - Discover all characteristics for a given service
 - Find characteristics matching a given UUID
 - Read all descriptors for a particular characteristic
 - Can do read, write, long read, long write values etc.
 - Peripheral
 - Notify or indicate central of changes
-

Security

- Encryption (128 bit AES)
 - Pairing (without key, with a shared key, out of band pairing)
 - Passive eavesdropping during key exchange (but fixed in Bluetooth 4.2)
 - Many products are building their own security on top of BLE
-

Bluetooth Low Energy Applications

- Proximity: in car, in room 404, in the mall
 - Locator: keys, watches, animals
 - Health devices: Heart rate monitors, physical activities monitors, thermometers
 - Sensors: Temperature, Battery Status, tire pressure
 - Remote control: Open/close locks, turn on lights
-

Use Cases – Physical Security



INTERIOR TRIM

Use Cases – Home Automation



Use Cases – Geo-fencing/ Positioning



Use Cases - Fun

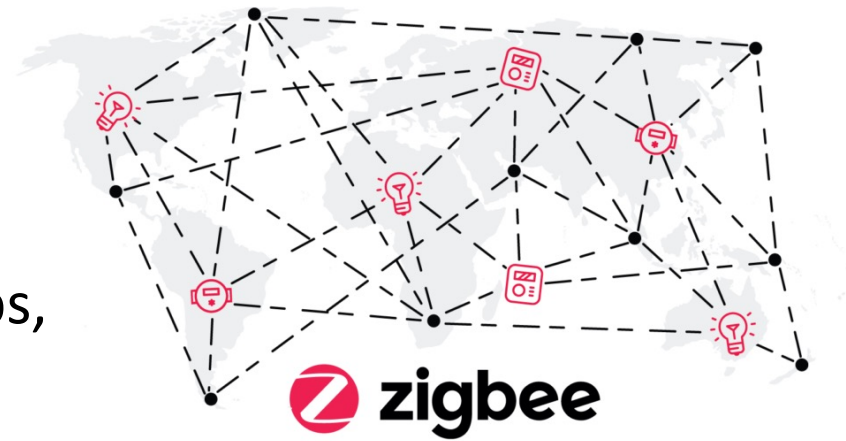


Development Kits/Boards



ZigBee

- Technological standard created for the control and sensor networks
- Suited for low-cost, low-power wireless IoT networks
- Based on IEEE 802.15.4 standard
- Created by ZigBee Alliance – Philips, Motorola, HP, Intel etc.
- Conceived in 1998, standardized in 2003, and revised in 2006

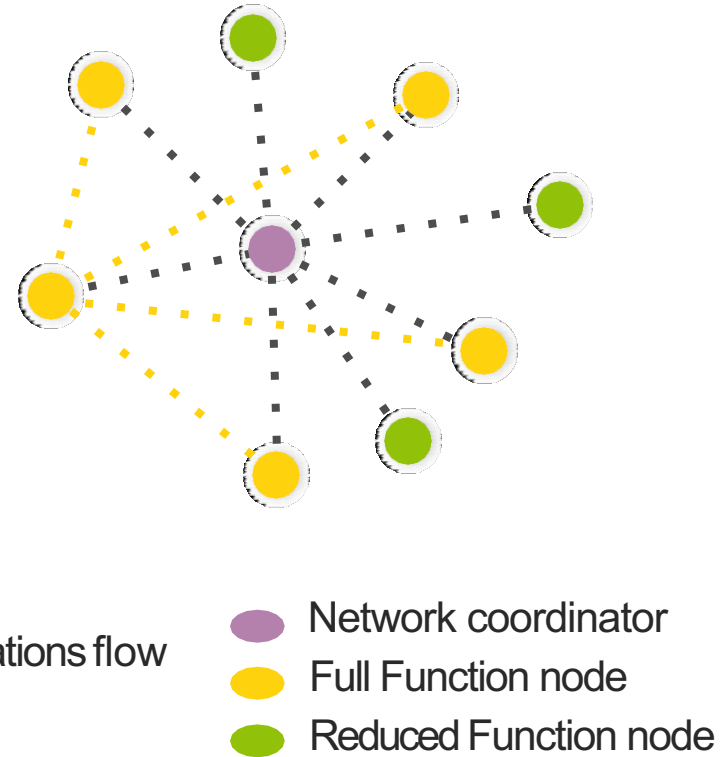


ZigBee Technology-Performance

- Proven excellent in-building coverage
 - Inherently robust radio link
 - Mesh networking
 - Acknowledge oriented protocol
 - Proven tolerance to interference
 - Trade shows like CES-works when WiFi and Bluetooth fail
 - Montage Hotels and MGM City Center deployments
 - Products which implement multiple radio technologies
 - Proven coexistence
 - Many multi-radio products and multi-radio deployments
 - Proven scalability
 - City Center at 70,000 plus radios
 - Montage Hotels at 4000 plus radios per property
-

Basic Network Characteristics

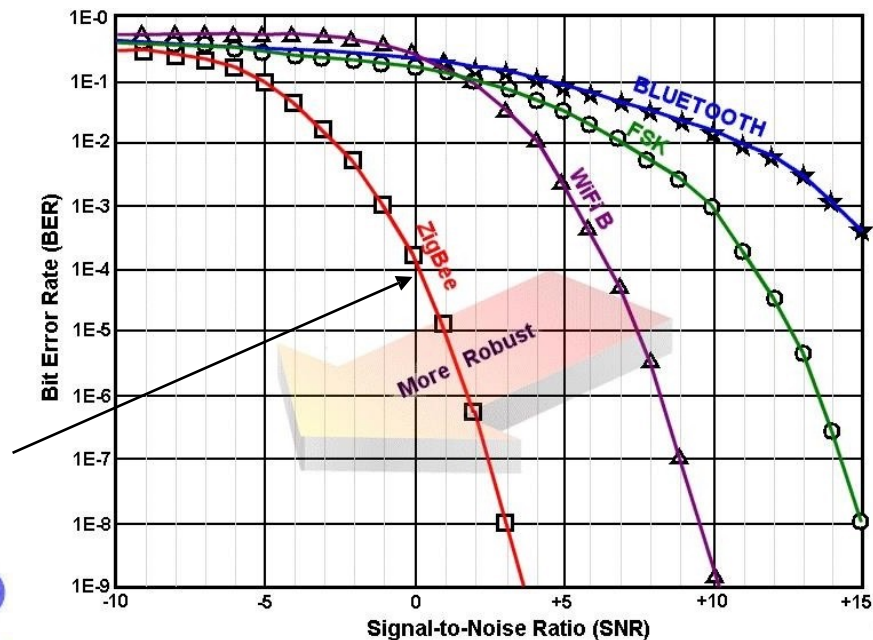
- 65,536 network (client) nodes
- 27 channels over 2 bands
- 250Kbps data rate
- Optimized for timing-critical applications and power management
- Full Mesh Networking Support



Basic Radio Characteristics

ZigBee technology relies upon IEEE 802.15.4, which has excellent performance in low SNR environments

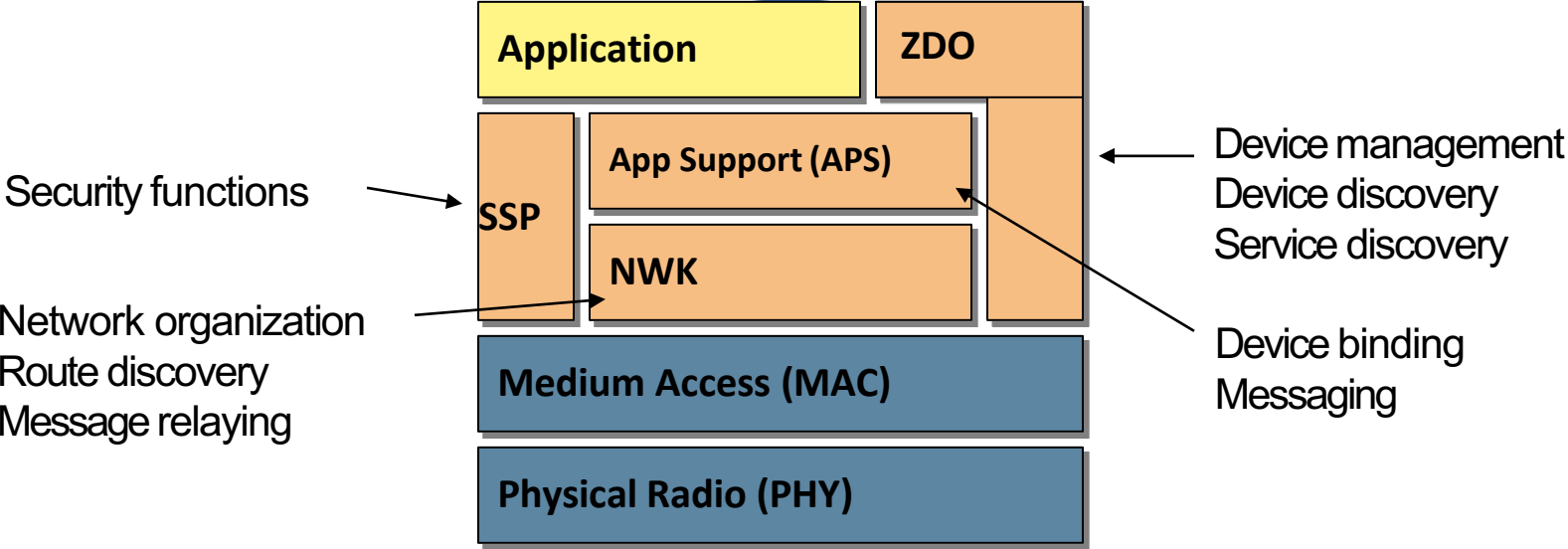
Frequency Band	License Required?	Geographic Region	Data Rate	Channel Number(s)
868.3 MHz	No	Europe	20kbps	0
902-928 MHz	No	Americas	40kbps	1-10
2405-2480 MHz	No	Worldwide	250kbps	11-26



ZigBee Stack Architecture

Application

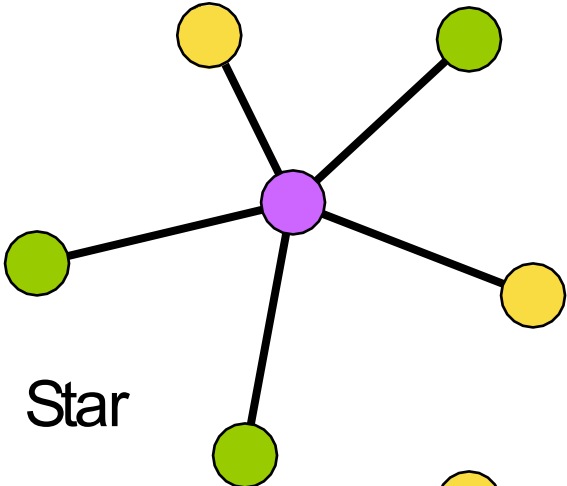
- Initiate and join network
- Manage network
- Determine device relationships
- Send and receive messages



ZigBee Device Types

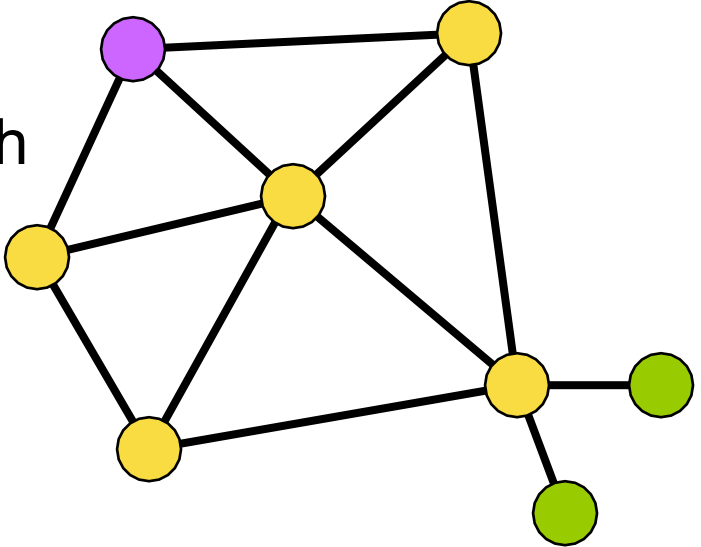
- ZigBee Coordinator (ZC)
 - One required for each ZB network.
 - Initiates network formation.
 - ZigBee Router (ZR)
 - Participates in multihop routing of messages.
 - ZigBee End Device (ZED)
 - Does not allow association or routing.
 - Enables very low cost solutions
-

ZigBee Network Topologies

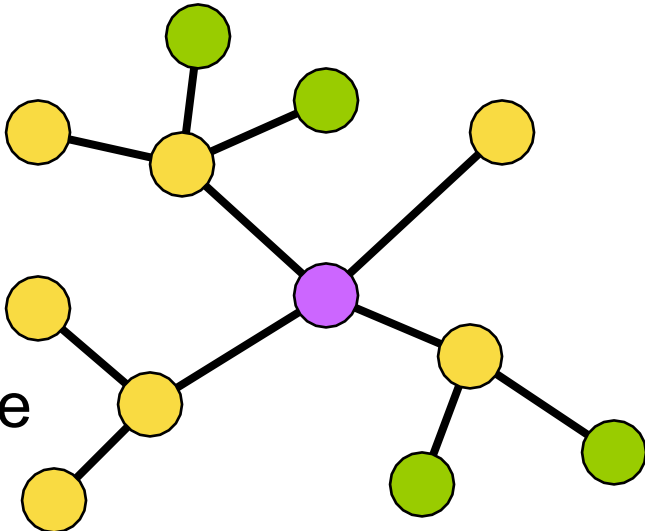





Star

Mesh



Cluster Tree



-  ZigBee Coordinator
-  ZigBee Router
-  ZigBee End Device

ZigBee Public Profiles

- Home Automation (HA)
- Smart Energy (SE)
- Commercial Building Automation (CBA)
- ZigBee Health Care (ZHC)
- Telecom Applications (TA)



- ZigBee RF4CE Remote Control



- +Future profiles proposed by member companies...
-



ZigBee Home Automation: for Home Control



ZigBee Home Area Network (HAN)

Smart Energy & Home Automation



Urgent demand for Smart Energy + compatibility with mainstream Home Automation systems enables customer choice



Wi-Fi Alliance

- Wi-Fi technology builds on IEEE 802.11 standards. The IEEE develops and publishes these standards, but does not test equipment for compliance with them. The non-profit Wi-Fi Alliance formed in 1999 to fill this void.
 - The Wi-Fi Alliance, a global association of companies.
 - As of 2009 the Wi-Fi Alliance consisted of more than 300 companies from around the world.
 - Manufacturers with membership in the Wi-Fi Alliance, whose products pass the certification process, gain the right to mark those products with the Wi-Fi logo.
-

IEEE 802.11b

- Appeared in late 1999
 - Operates at 2.4GHz radio spectrum
 - 11 Mbps (theoretical speed) - within 30 m Range
 - 4-6 Mbps (actual speed)
 - 20—30 meters range
 - Most popular, Least Expensive
 - Interference from mobile phones and Bluetooth devices which can reduce the transmission speed.
-

IEEE 802.11a

- Introduced in 2001
 - Operates at 5 GHz (less popular)
 - 54 Mbps (theoretical speed)
 - 15-20 Mbps (Actual speed)
 - 25 – 30 meters range
 - More expensive
 - Not compatible with 802.11b
-

IEEE 802.11g

- Introduced in 2003
 - Combine the feature of both standards (a,b)
 - 100-150 feet range
 - 54 Mbps Speed
 - 2.4 GHz radio frequencies
 - Compatible with 'b'
-

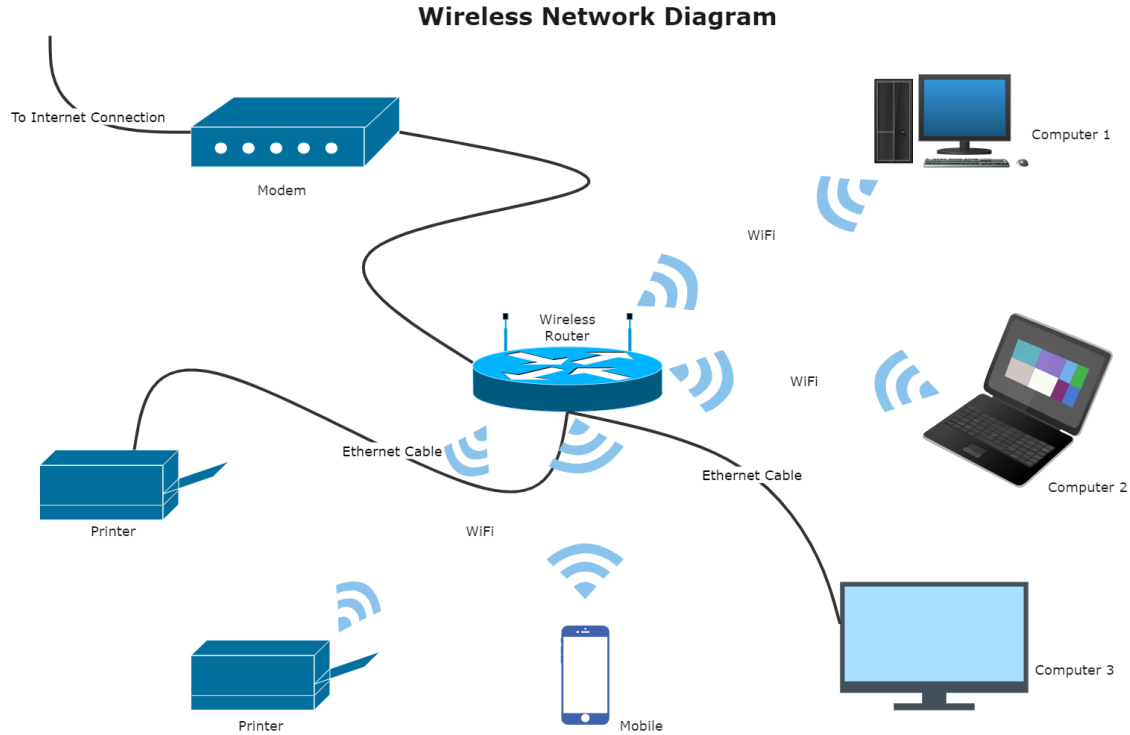
Standards

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard
 - IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
 - IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
 - IEEE 802.11d - International (country-to-country) roaming extensions
 - IEEE 802.11e - Enhancements: QoS, including packet bursting
 - IEEE 802.11f - Inter-Access Point Protocol (IAPP)
 - IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
 - IEEE 802.11h - 5 GHz spectrum
 - IEEE 802.11n - Higher throughput improvements
 - IEEE 802.11p - Wireless Access for the Vehicular Environment
 - IEEE 802.11r - Fast roaming
 - IEEE 802.11s - Wireless mesh networking
 - IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
 - IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
 - IEEE 802.11v - Wireless network management
 - IEEE 802.11w - Protected Management Frames
-

Elements of a WI-FI Network

- **Access Point (AP)** - The AP is a wireless LAN transceiver or “base station” that can connect one or many wireless devices simultaneously to the Internet.
- **Wi-Fi cards** - They accept the wireless signal and relay information. They can be internal and external.(e.g PCMCIA Card for Laptop and PCI Card for Desktop PC)
- **Safeguards** - Firewalls and anti-virus software protect networks from uninvited users and keep information secure.

How a Wi-Fi Network Works



Wi-Fi Security

- Service Set Identifier (SSID)
 - Wired Equivalent Privacy (WEP)
 - Wireless Protected Access (WPA)
 - IEEE 802.11i
-
- WEP and WPA are encryption protocols that you can choose from in your router's firmware.
 - Wi-Fi Protected Access (WPA), a subset of the upcoming 802.11i security standard, will replace the flawed Wired Equivalent Privacy (WEP).
 - Without your SSID, people will not be able to join your Wi-Fi hotspot.

Advantages

- Mobility
- Ease of Installation
- Flexibility
- Cost
- Reliability
- Security
- Use unlicensed part of the radio spectrum
- Roaming
- Speed

Limitations

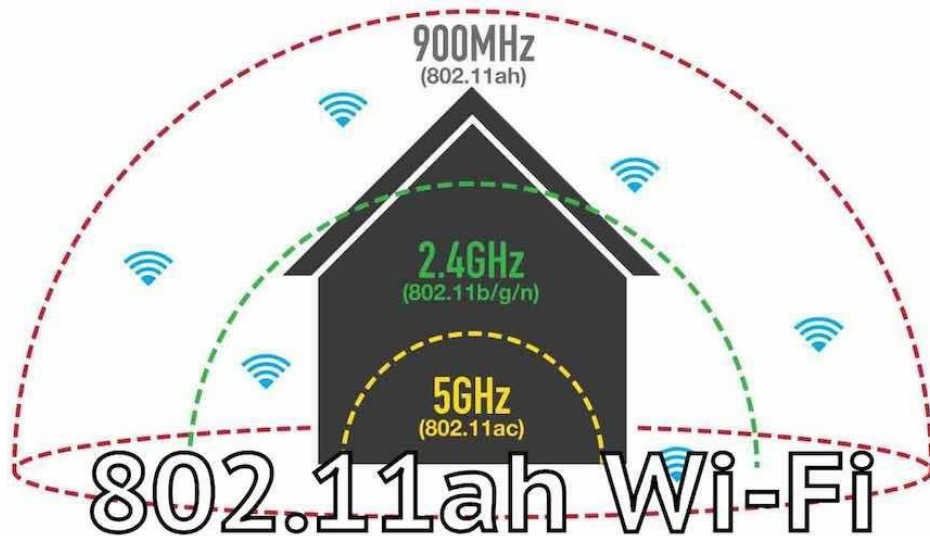
- Interference
- Degradation in performance
- High power consumption
- Limited range

IEEE 802.11ah

- Defines operation of license-exempt (ISM) IEEE 802.11 wireless networks in frequency bands below 1 GHz
 - Excluding the TV White Space bands (802.11af)
- IEEE 802.11 WLAN user experience for fixed, outdoor, point to multi point applications

Sub-1GHz WLAN for IoT

What lies beneath Wi-Fi HaLow

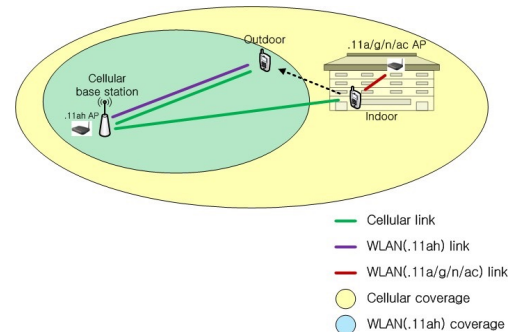
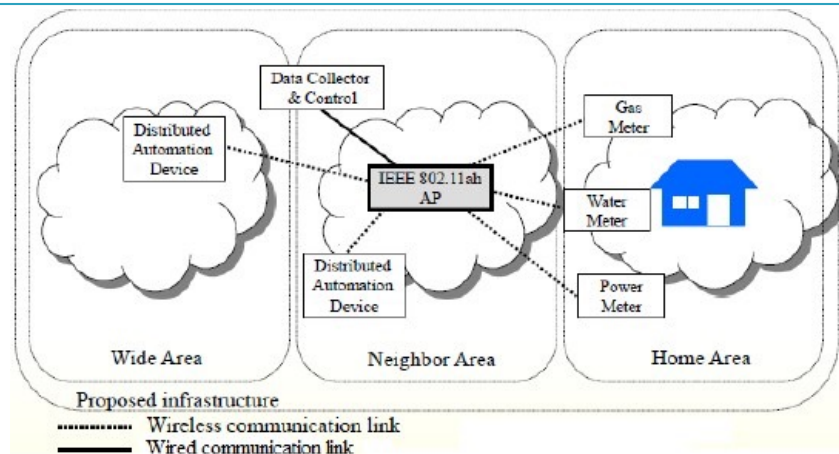


IEEE 802.11ah: scope

- Defines an **OFDM PHY** operating in the license-exempt bands below 1 GHz
 - Enhancements to the IEEE 802.11 MAC to support this PHY, and to provide mechanisms that enable coexistence with other systems in the bands (e.g. IEEE 802.15.4 P802.15.4g)
 - The PHY is meant to optimize the ***rate vs. range*** performance of the specific channelization in a given band
 - Transmission range up to 1 km
 - Data rates > 100 kbit/s
 - The MAC is designed to support **thousands of connected devices**
-

IEEE 802.11ah: use cases

- Use Case 1 : Sensors and meters
 - Smart Grid -meter to pole
 - Environmental monitoring
 - Industrial process sensors
 - Healthcare
 - Home/Building automation
 - Smart city
- Use Case 2 : Backhaul sensor and meter data
 - Backhaul aggregation of sensor networks
 - Long point-to-point wireless links
- Use Case 3 : Extended range Wi-Fi
 - Outdoor extended range hotspot
 - Outdoor Wi-Fi for cellular traffic offloading



IEEE 802.11ah: PHY (1)

- Advantages of transmitting in sub 1 GHz:
 - Spectrum characteristics
 - good propagation and penetration
 - large coverage area and one-hop reach
 - license-exempt, light licensing
 - Reliability:
 - less congested frequency band
 - high sensitivity and link margin
 - available diversity –(frequency, time, space)
 - Battery operation
 - long battery life
 - short data transmissions
-

IEEE 802.11ah: PHY (2)

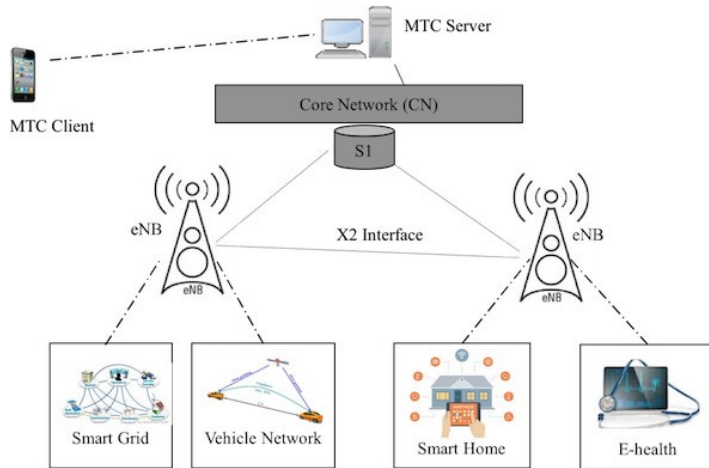
- Channelization:
 - Configurable bandwidth (*channel bonding*) of: 1, 2, 4, 8 and 16MHz
 - Inherited from IEEE 802.11ac (adapted to S1G)
 - OFDM
 - MIMO + MU-MIMO
 - PHY rates ranging from 150kbps to 347Mbps
-

IEEE 802.11ah: MAC

- Need to **reduce overhead**: low data rates + short frames (typical in some use cases)
 - Short MAC headers and Beacons
 - Implicit acknowledgement (no ACK needed)
 - Need to **support thousands of associated devices** (increases coverage - increases reachable STAs)
 - Thousands of STAs -> huge collision probability!
 - Restricted Access Window (RAW): regular RAW
 - Divide STAs into groups (AID)
 - Split channel access into time slots
 - Assign slots to groups (AP indicates RAW allocation and slot assignments in its Beacons)
 - Different *backoff* rules apply during RAW (due to different contention conditions)
-

LTE-A

- Long-Term Evolution Advanced (LTE-A) is a set of standards designed to fit M2M communication and IoT applications in **cellular networks**



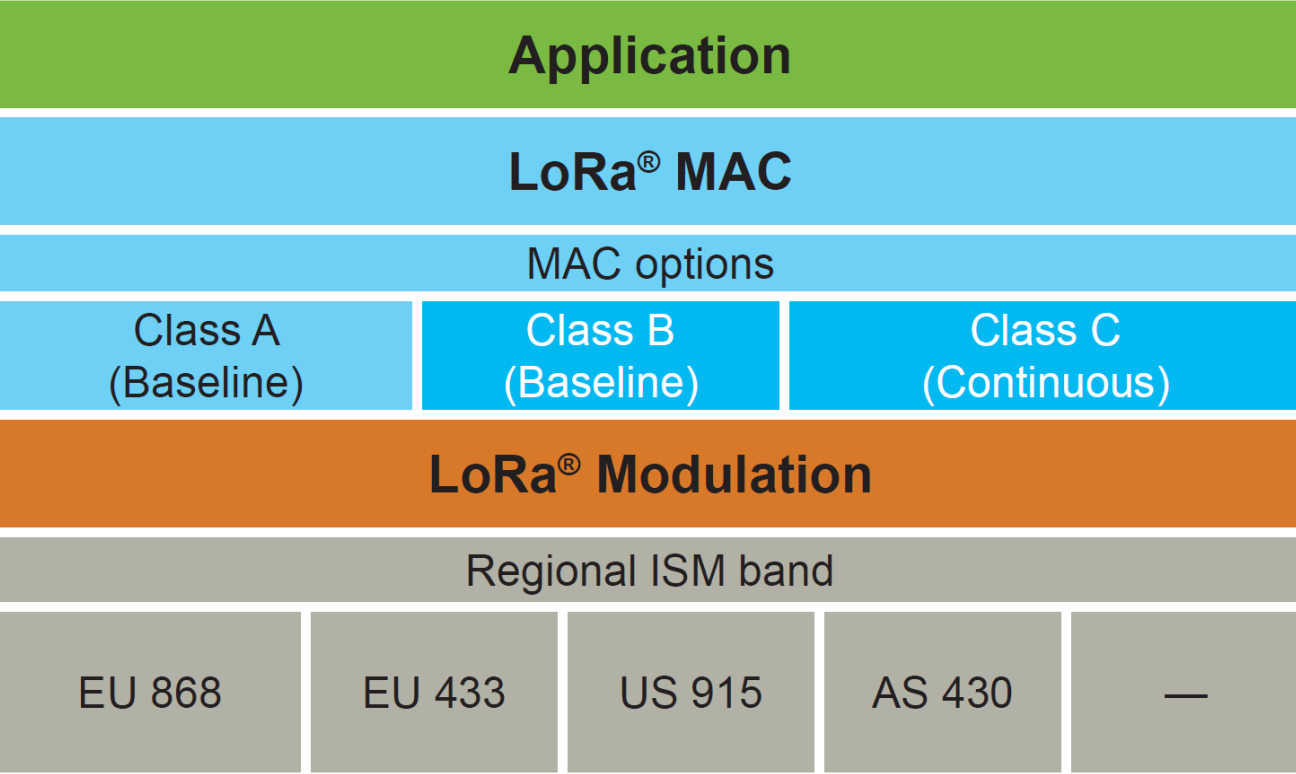
- LTE-A is a **scalable, lower-cost** protocol compared to other cellular protocols
- LTE-A uses OFDMA (Orthogonal Frequency Division Multiple Access) as a MAC layer access technology, which divides the frequency into multiple bands and each one can be used separately
- The architecture of LTE-A consists of a core network (CN), a radio access network (RAN), and the mobile nodes
 - The CN is responsible for controlling mobile devices and to keep track of their IPs
 - RAN is responsible for establishing the control and data planes and handling the wireless connectivity and radio-access control

LoRaWAN

- LoRaWAN is a wireless technology designed for low-power WAN networks with low cost, mobility, security, and bidirectional communication for IoT applications
 - It is a low-power consumption optimized protocol designed for scalable wireless networks with millions of devices
 - It supports redundant operation, location free, low cost, low power and energy harvesting technologies to support the future needs of IoT while enabling mobility and ease of use features
-

WHAT IS LoRaWAN™?

LoRaWAN™ defines the communication protocol and system architecture for the network while the LoRa physical layer enables the long-range communication link.



LoRa

What is it?

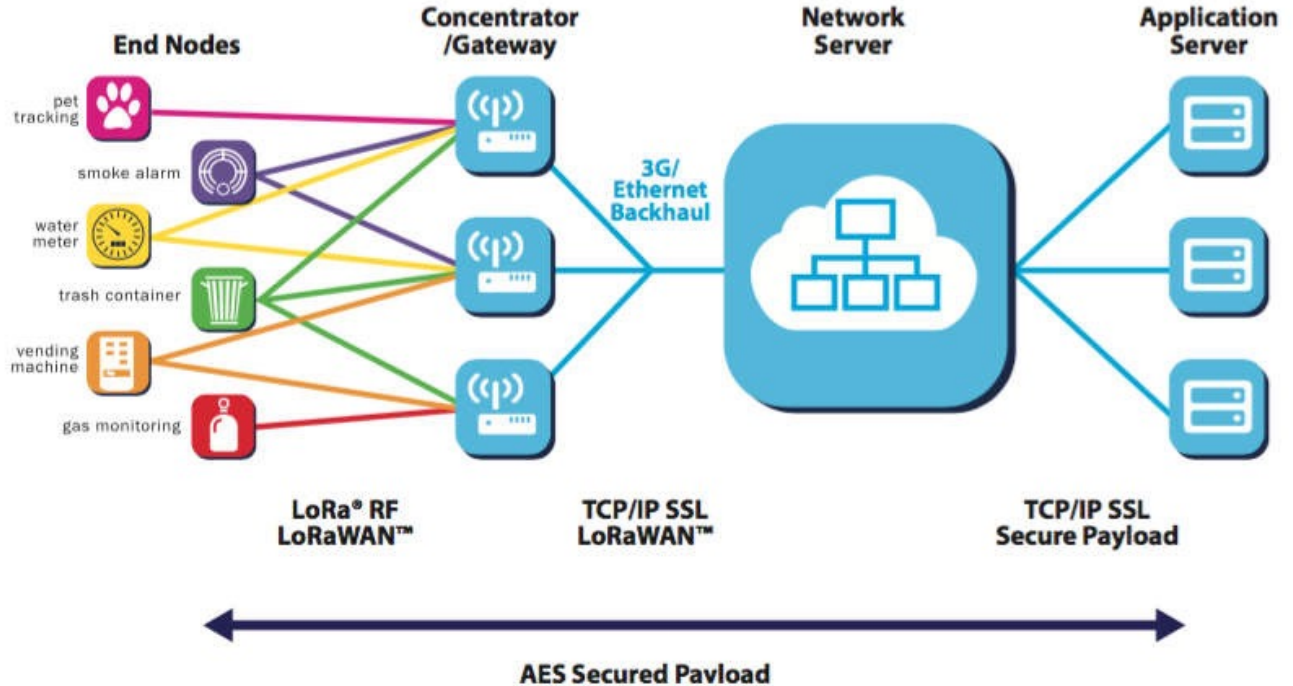
- LoRa technology was originally developed by a French company, Cycleo (founded in 2009 as an IP and design solution provider), a patented spread spectrum wireless modulation technology that was acquired by SemTech in 2012 for \$5 million
 - In April 2013, SemTech released the SX1272 chip, which was equipped with LoRa technology
 - At that time, FSK modulated European smart meter transceivers were used, with a maximum transmission distance of 1 to 2 kilometers
 - LoRa operated under the same conditions, and the transmission distance could be more
-

LoRa Technology

Two major components

End device: ED

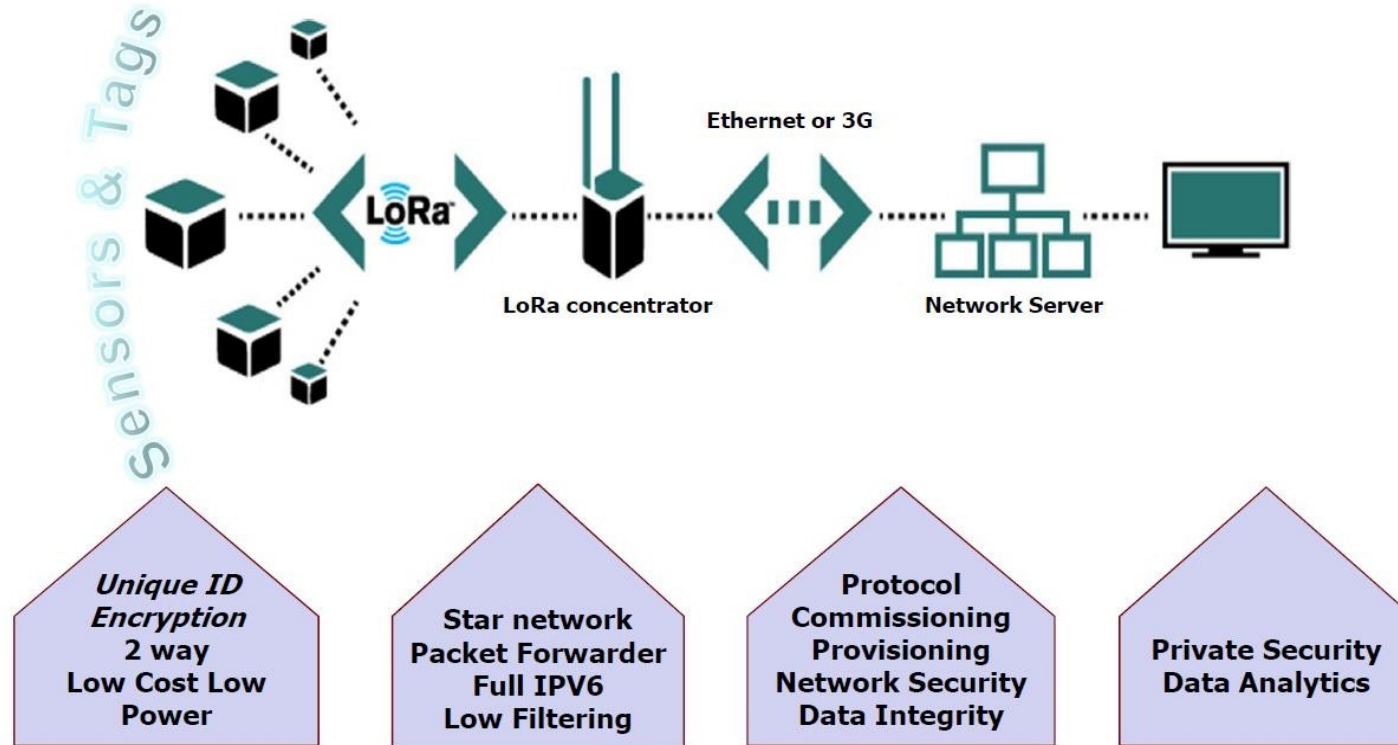
Base Station: BS



LoRaWAN network protocol

- LoRaWAN network protocol is optimized specifically for energy limited EDs
 - LPWAN typically has star topology and consists of BSs relaying data messages between the EDs and an application server
 - The BSs can be connected to the central server via backbone internet protocol (IP) based link, and the wireless communication based on LoRa or GFSK modulation is used to move the data between EDs and the BSs
-

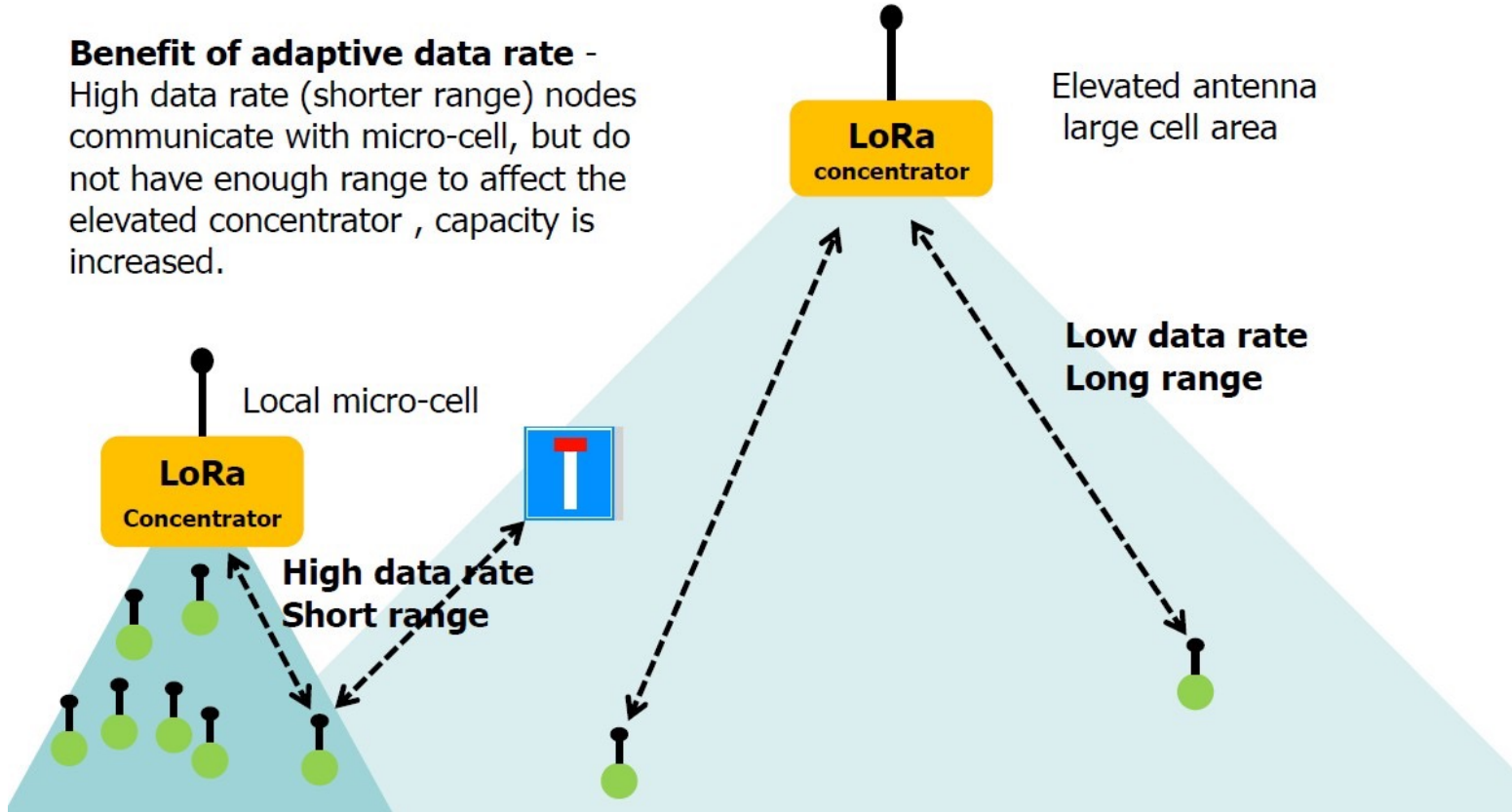
Network Architecture



Network Capacity: Adaptive Data Rate

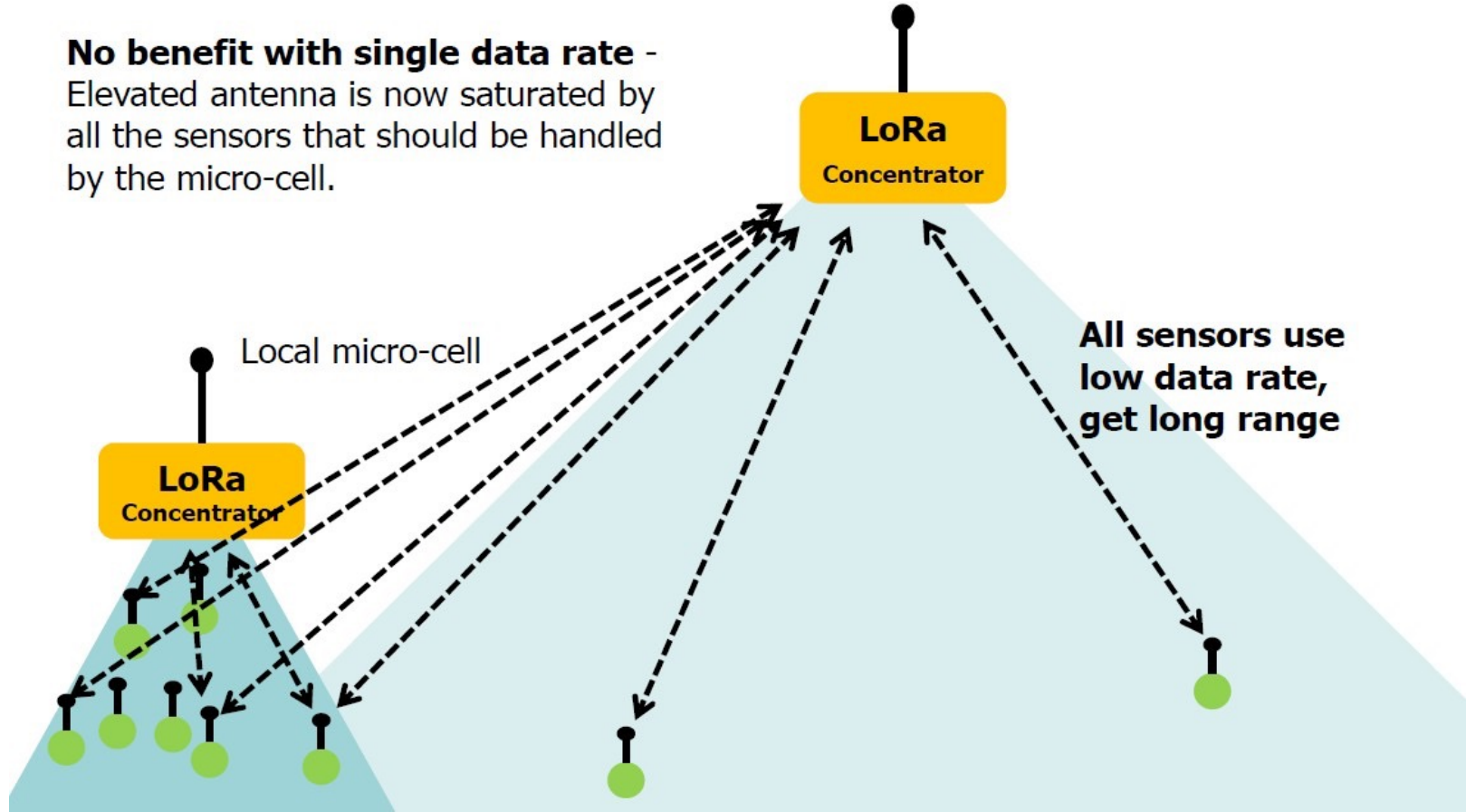
Benefit of adaptive data rate -

High data rate (shorter range) nodes communicate with micro-cell, but do not have enough range to affect the elevated concentrator, capacity is increased.



Network Capacity: Single Data Rate

No benefit with single data rate -
Elevated antenna is now saturated by all the sensors that should be handled by the micro-cell.



Three classes of EDs

