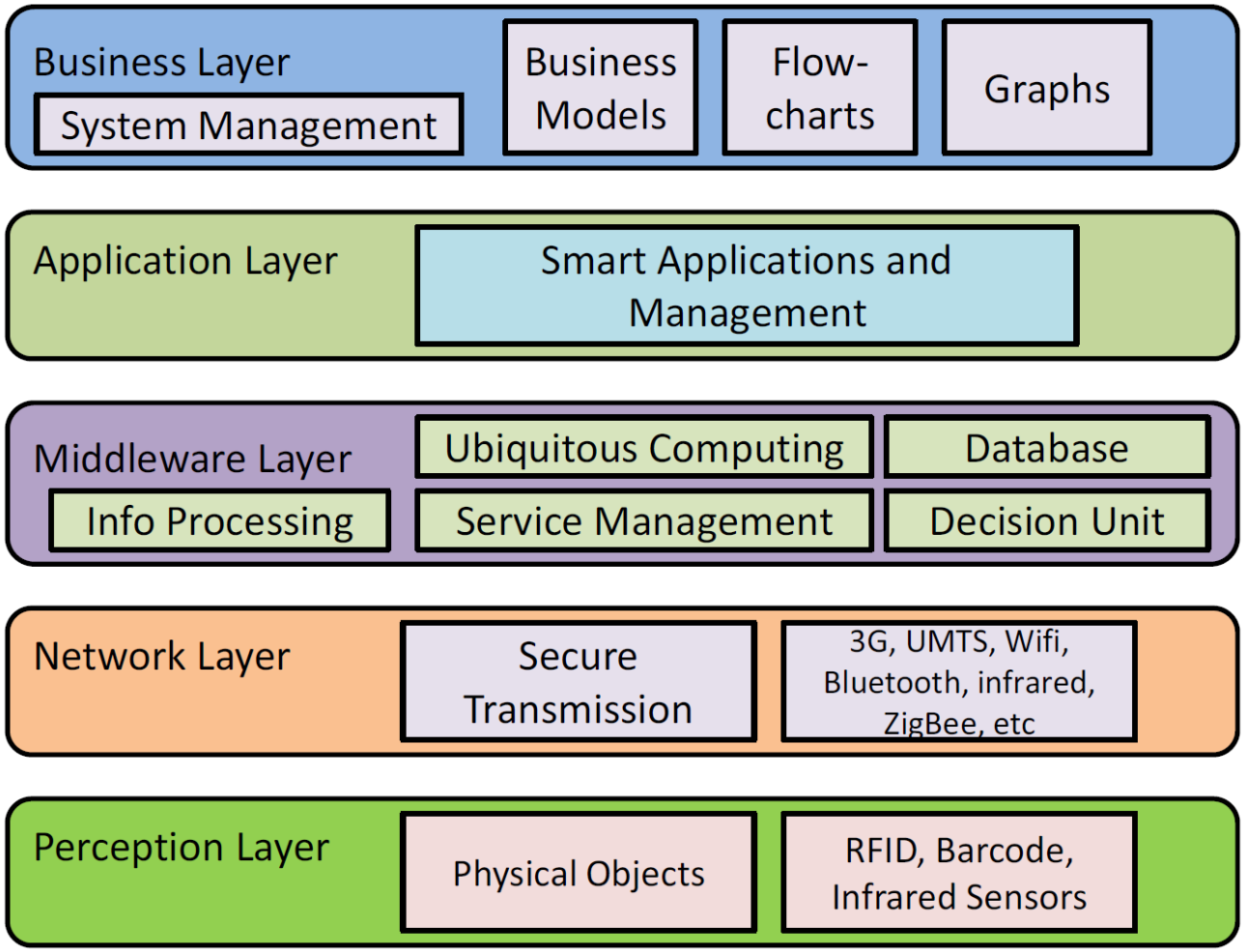
Communication/Networking Protocols – Part 1

Instructor: Deepak Gangadharan

IoT Architecture



Source- Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, 2012

Perception Layer

- Also known as the Device Layer
- Consists of physical objects and sensor devices (i.e., RFID, 2-D barcode, or any sensor depending on the functionality)
- Collection of object specific information by the sensor devices
- Collected information is passed to Network layer for secure transmission to the information processing system in the middleware layer

Network Layer

- Also called Transmission Layer
- Securely transfers the information from sensor devices to the information processing system
- Transmission medium can be wired or wireless and technology can be 3G/4G/5G, WiFi, Bluetooth, ZigBee, infrared, etc depending upon the sensor devices
- Supports the communication requirements of latency, bandwidth and security

Middleware Layer

- Each device connects and communicates with only those devices that implement similar type of service
- Main responsibility of service management
- Receives information from network layer and stores in the database
- Performs information processing and ubiquitous computation and takes automatic decision based on results

Application Layer

- Provides global management of the application based on the information processed in the Middleware Layer

- Different applications implemented can be smart health, smart farming, smart home, intelligent transportation, etc.

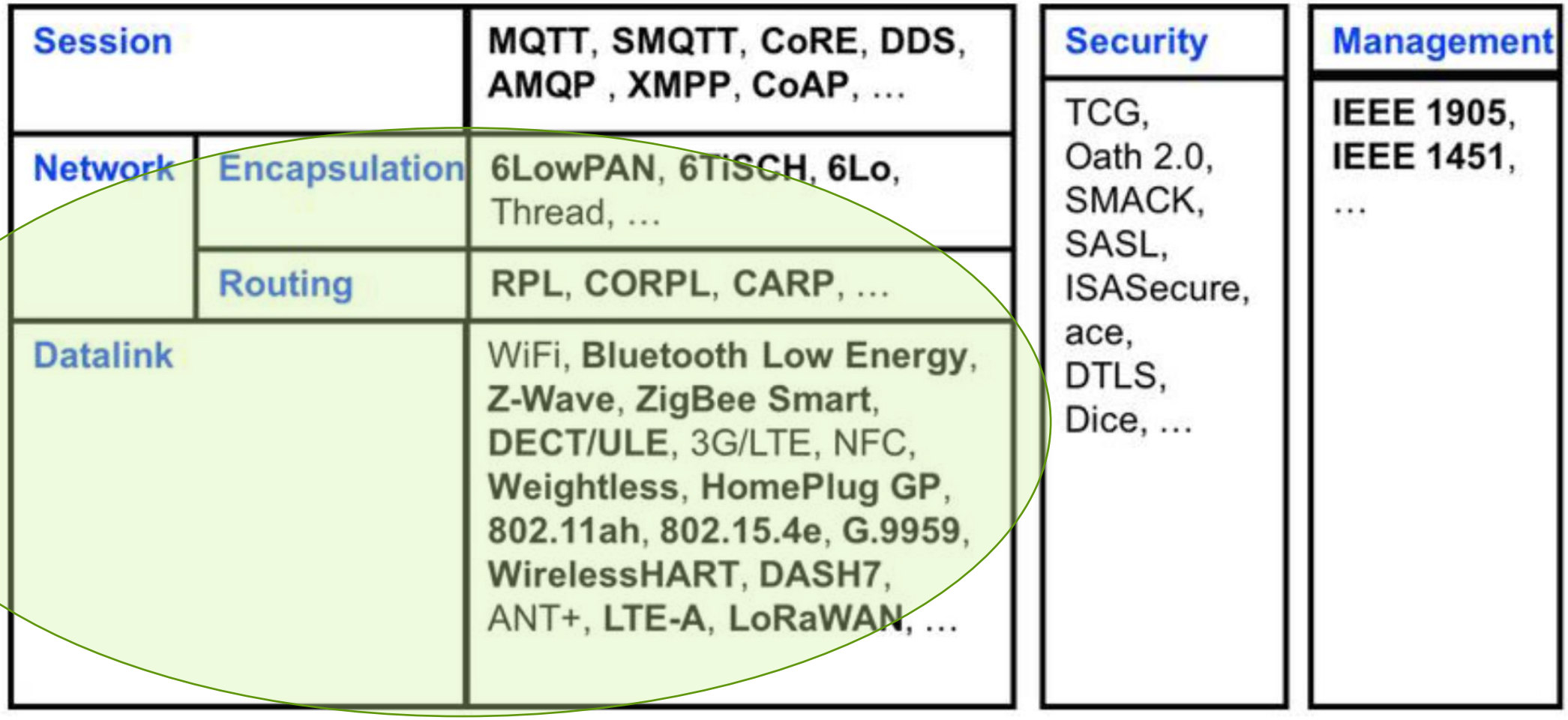
Business Layer

- Responsible for management of the overall IoT system including the applications and services
- Builds business models, graphs, flow charts, etc. based on data received from Application Layer
- Analyzing and monitoring of model results, which help to determine the future actions and business strategies

Communication Protocols

- Sensors and things need a way to communicate information
- In IoT, communication to a sensor or actuator can be via a copper wire or wireless medium
- Wireless Personal Area Networks (WPANs) are prevalent method for industrial, commercial and consumer connections to things
- Wires are used in legacy industries and areas that are not radio frequency friendly
- Wide variety of communication possibilities – some built on traditional IP stack and some use non-IP based communication (such as BLE)
- Non-IP based communications are optimized for cost and energy usage, while IP-based techniques do not have many constraints

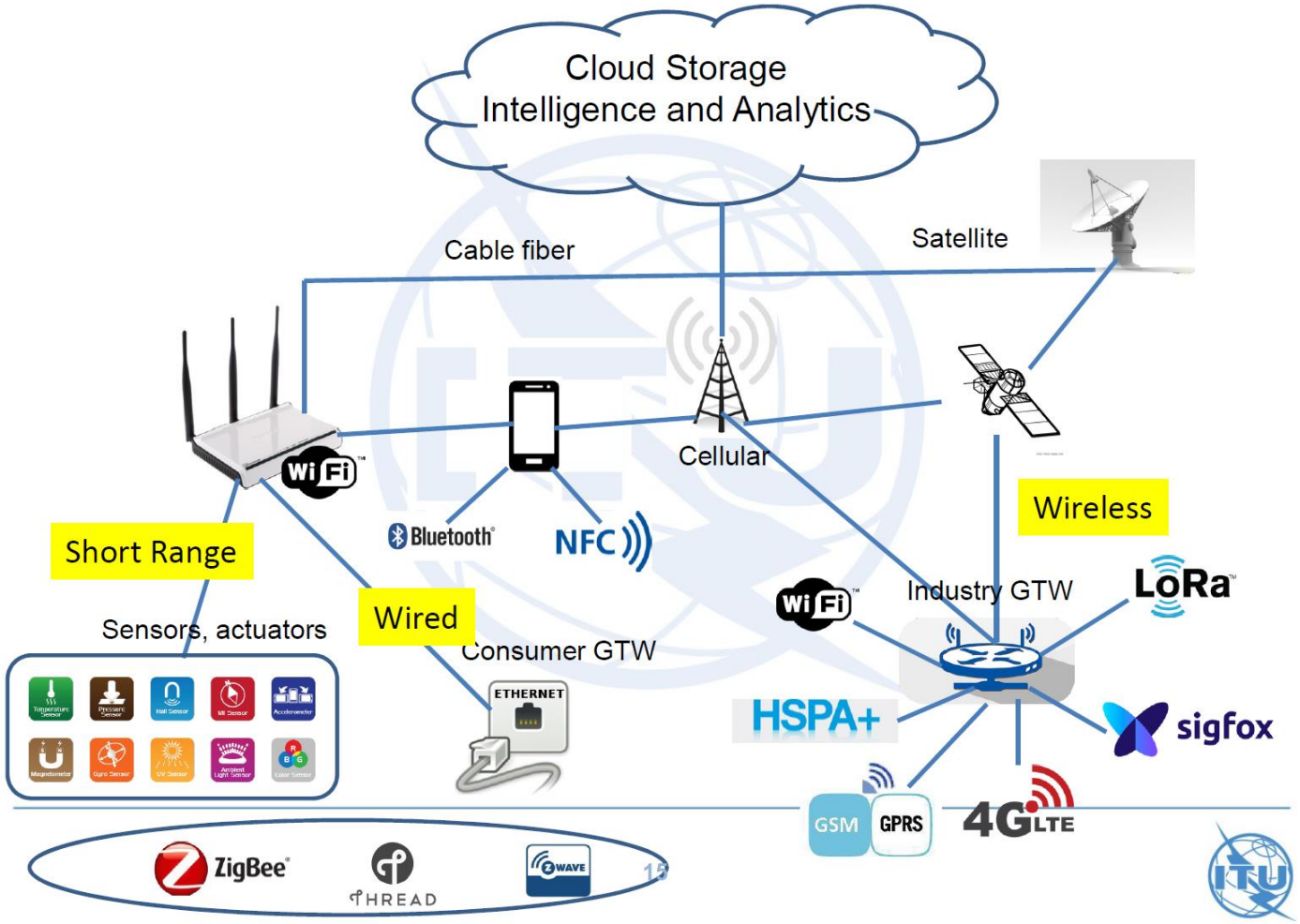
Protocols for IoT



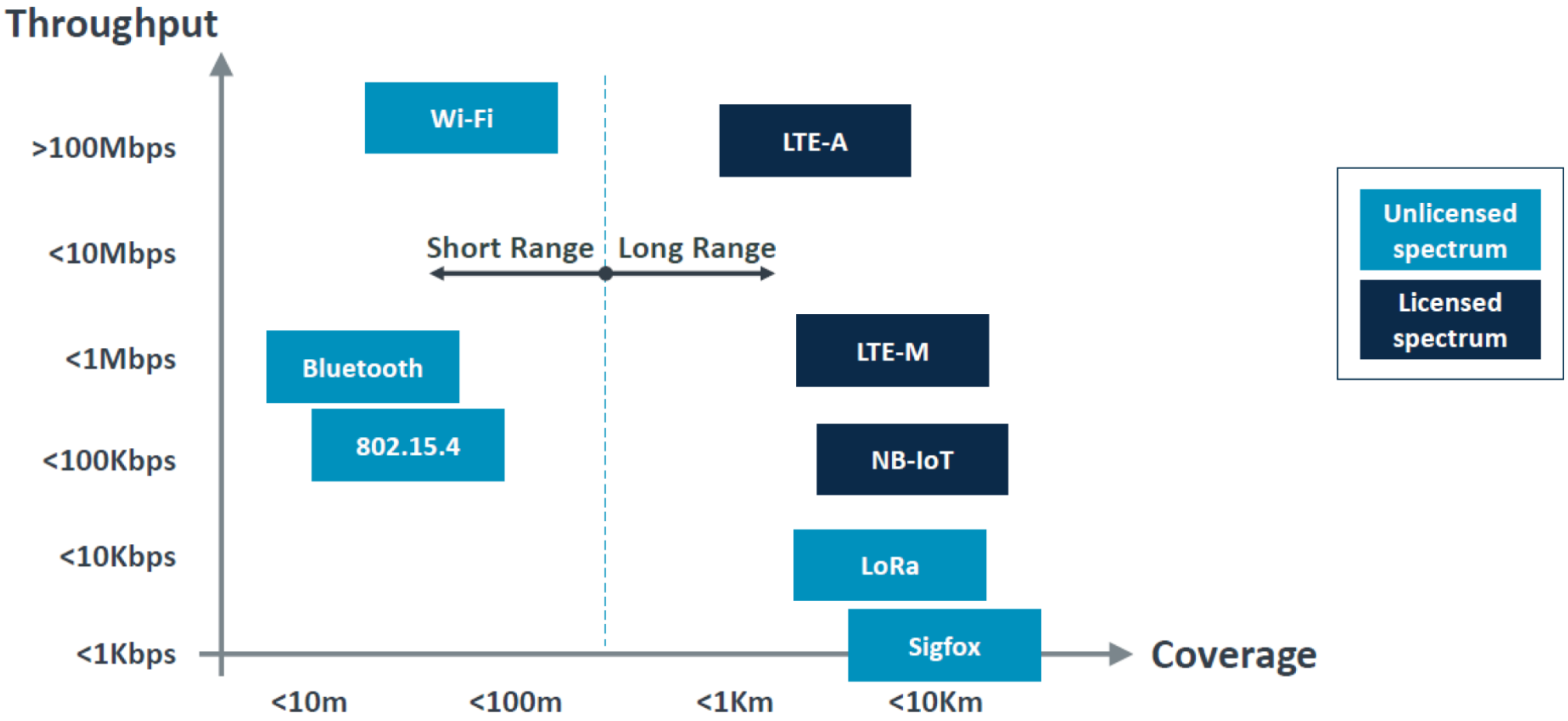
Desired characteristics of IoT communications

- Low cost
- Low power
- Long battery duration
- High number of connections
- Low bitrate (not broadband)
- Long or short range
- Low processing capacity
- Low storage capacity
- Small size devices
- Simple network architecture and protocols

IoT network general architecture



IoT Connectivity Technologies



- Short Range
  - RFID
  - Bluetooth
  - Zigbee
  - WiFi

RFID

What is RFID ?

- RFID stands for Radio Frequency identification.
- Wireless non-contact use of radio-frequency electromagnetic fields to transfer data
- For the purpose of automatic identification & tracking of tags attached to assets

RFID Tags

- RFID tags may or may not have a battery in them.
- Those that do not have a battery are called **passive tags**
- Those that use a battery are called **active tags**. The battery mostly assists in boosting the read range of the RFID tag (greater range but higher cost and finite life)
- Passive tags are powered by the RF signal from the interrogator/reader (smaller, lighter and less expensive, and almost unlimited life)

RFID

Frequencies

- LF – Low frequency @ 125 khz
- HF: High frequency @ 13.56 Mhz
- UHF: Ultra high frequency @ 860 – 960 Mhz

Why 3 different frequencies ?

- Different applications demand different frequencies to be effective & operational
- **LF tags** are ideal for reading metal objects or objects with high water content such as fruit & veg/Animals. But the read range is limited to inches or cms.
- **HF tags** work fairly well on metal objects and objects with medium to high water content. Max read range is 3 feet to 1 meter
- **UHF** offers better read ranges(inches to 50ft +, depending on the strength of the RFID reader/interrogator), can transfer data much faster, however since they have a shorter wave length compared to LF or HF tags, the signal does not pass through metal or objects with water content

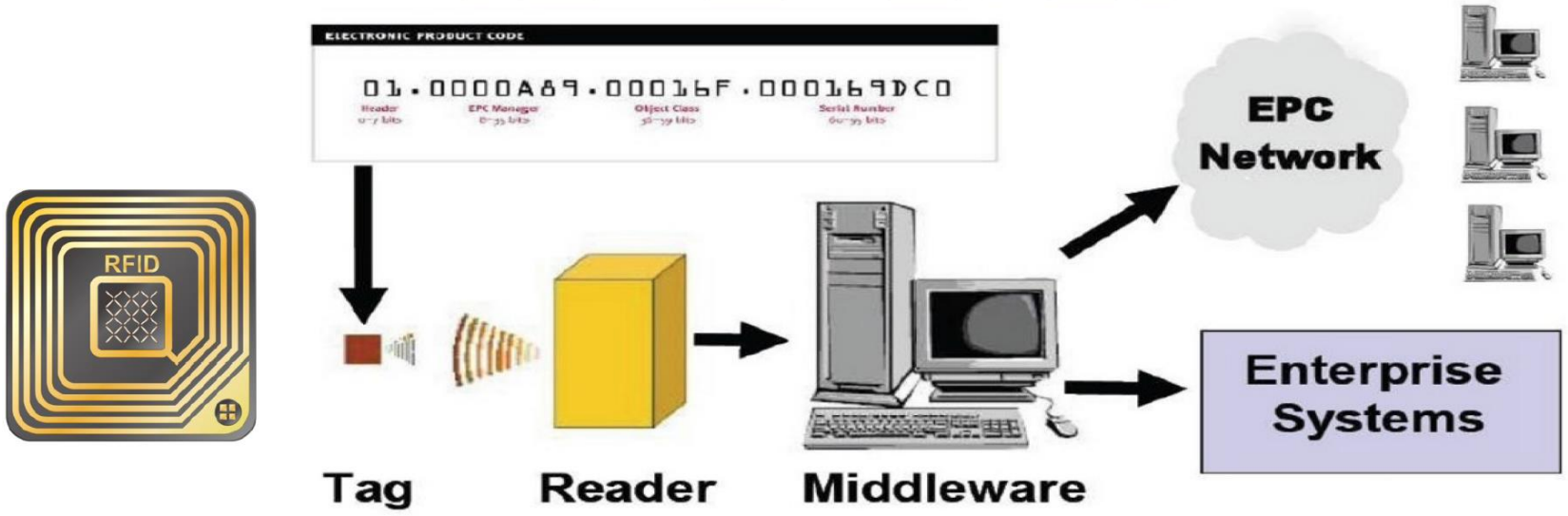
RFID – How does it work?

Tag

- Microchip connected to an antenna
- Can be attached to an object as his identifier

Reader

- RFID reader communicating with the **RFID tag** through radio waves



RFID – How does it work?

- Host manages Reader(s) and issues commands

- Reader and tag communicate via RF signal
- Carrier signal generated by the reader
- Carrier signal sent out through the antennas
- Carrier signal hits tag(s)
- Tag receives and modifies carrier signal
- Antennas receive the modulated signal and send them to the Reader

- Reader decodes the data
- Results returned to the host application

What has changed for RFIDs?

- Cost has decreased due to improvements in micro-chips
- Smaller micro-chip width size lowers power needs and size of the chip
- Better antennas allow smaller tags that can be embedded in labels and products
- Higher frequency means more data can be transmitted
- Multiple tags can be read by a reader

Bluetooth

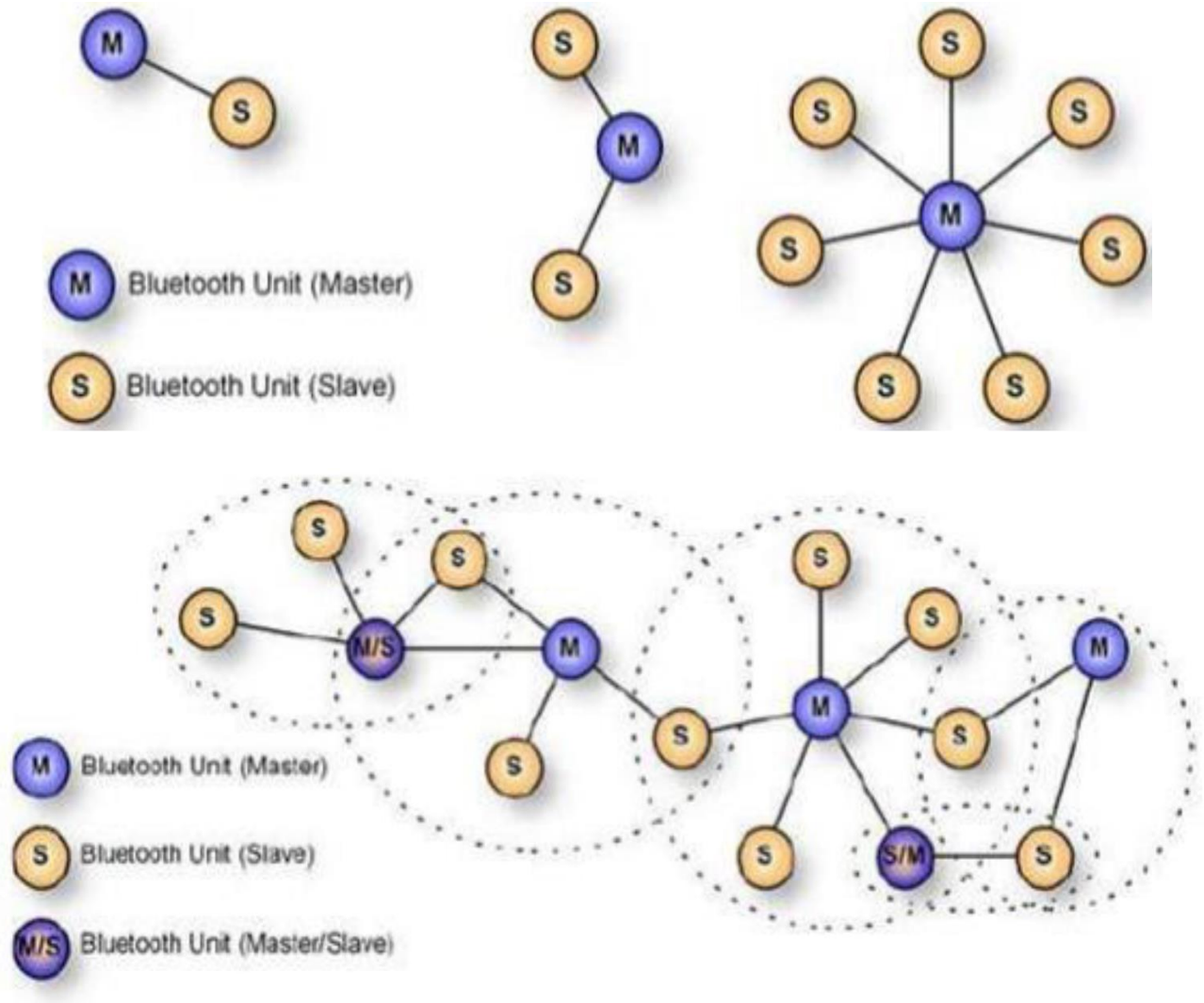
- Low power wireless technology
- First conceived at Ericsson in 1994 with an intent to replace wires with wireless alternative
- Short range radio frequency at 2.4 GHz ISM Band
- Creating Personal Area Networks
- Supports data rate of 1 Mbps
- Uses frequency hopping spread spectrum technique

Class	Maximum Power	Range
1	100 mW (20 dBm)	~100 m
2	2,5 mW (4 dBm)	~10 m
3	1 mW (0 dBm)	~1 m

Piconet

- Devices can form a quick ad-hoc network called "**piconet**" and start communication
- Connections in the piconet can happen even when mobile
- A piconet starts with two connected devices and may grow to eight connected devices
- All Bluetooth devices are peer units and have identical implementations. However, when establishing a piconet, one unit will act as a ***Master*** and the other(s) as ***Slave***(s) for the duration of the piconet connection

Piconet vs Scatternet

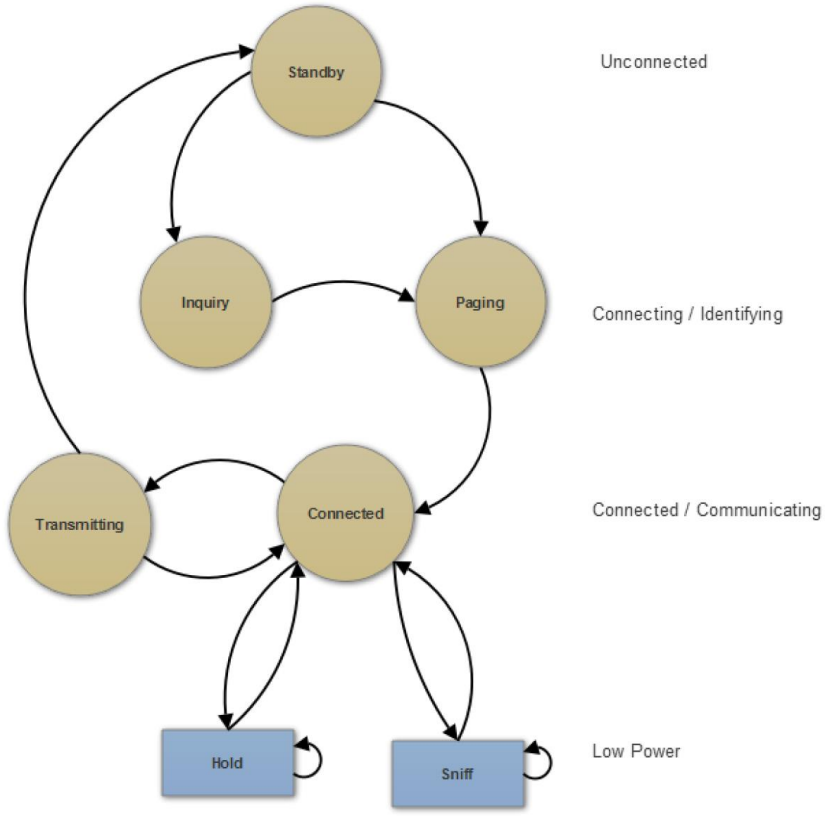


Modes of Operation

- Low Energy (LE) mode
  - Uses 2.4 GHz ISM band
  - Uses Frequency Hopping Spread Spectrum (FHSS) for interference protection
  - Bit rate of 1 Mbps
- Basic Rate/Enhanced Data Rate mode (BR/EDR)
  - Operates in 2.4 GHz ISM band but radio is different than LE and AMP
  - Basic radio operation supports a bit rate of 1 Mbps
  - EDR supports a data rate of 2 or 3 Mbps
  - Uses FHSS for interference protection
- Alternative MAC/PHY (AMP)
  - Optional feature that uses 802.11 for high speed transport up to 24 Mbps
  - Requires both master and slave device to support AMP

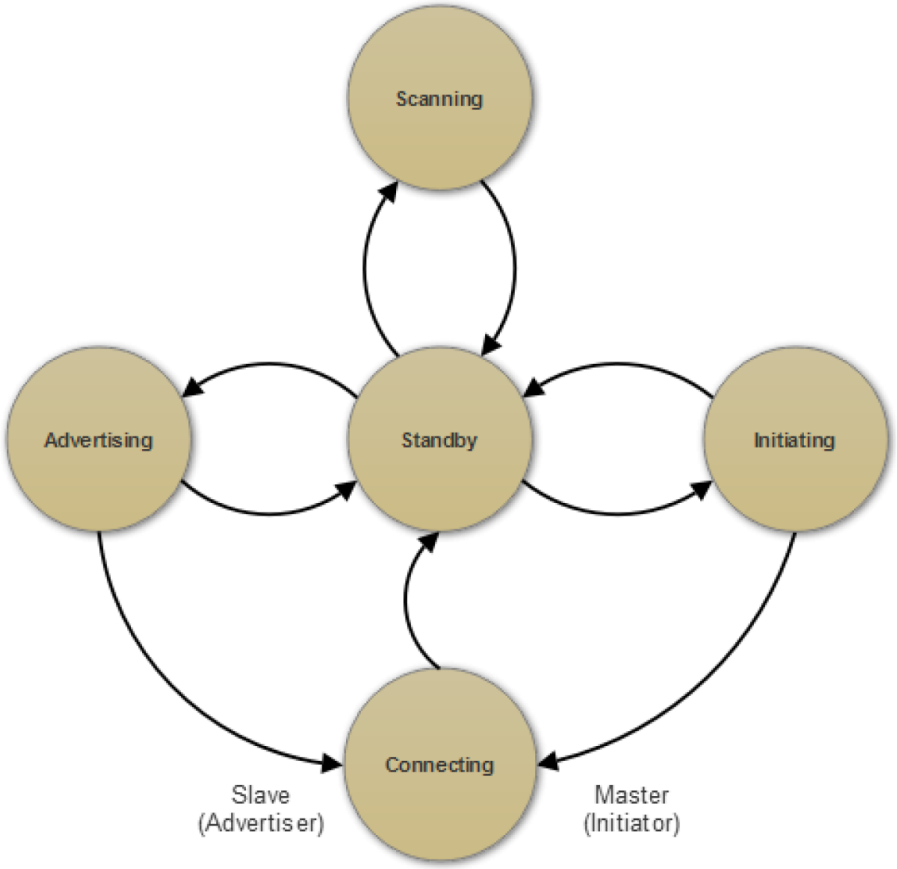
BR/EDR Operation

- Classic Bluetooth (BR/EDR) mode is connection-oriented
- A device must be discoverable to respond to physical channel scans with address and other parameters
- Three steps in connection process:
  - Inquiry: Devices discover each other through an inquiry request → if the other device is listening, it may respond with its address
  - Paging: Forms a connection between two devices and each knows the address of the other
  - Connected: Four sub-modes of the connection state
    - Active mode: Normal mode of operation for transmission and receiving data
    - Sniff mode: Power saving mode → Asleep but will listen for transmissions in specific slots
    - Hold mode: Temporary low power mode initiated by the master or slave → no sniffing
    - Park mode: Not there is Bluetooth 5

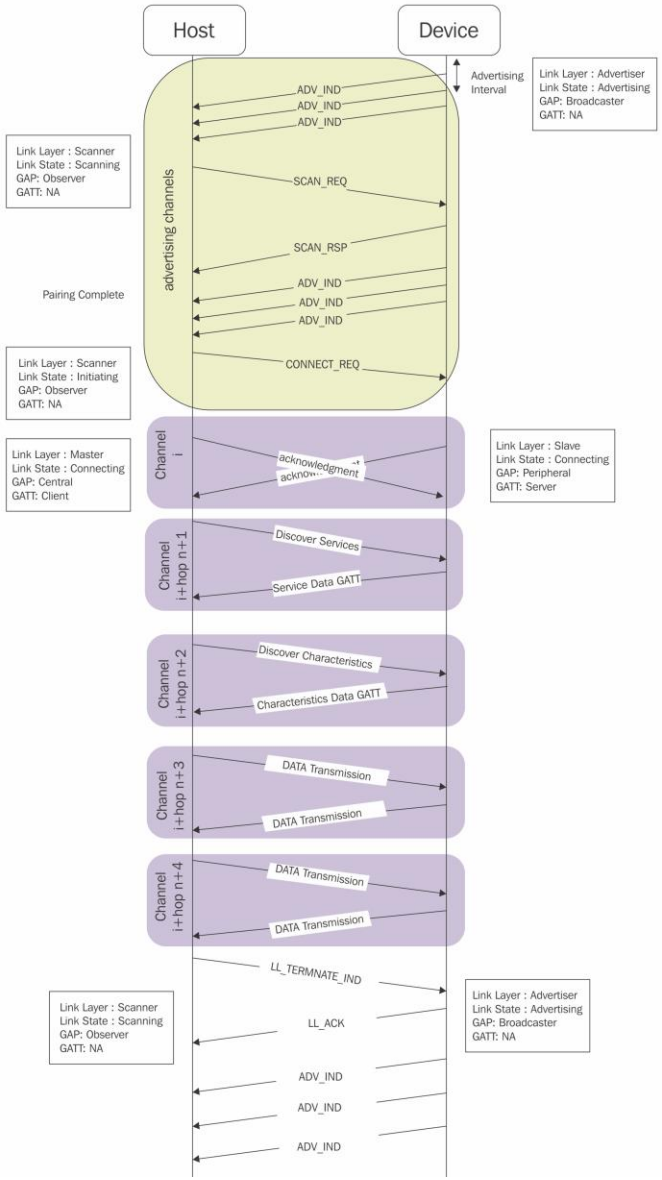


BLE operation

- Five link states negotiated by the host and device
  - ➢ Advertising: Devices transmit advertising packets on the advertising channels
  - ➢ Scanning: Receive advertising on the advertising channels without intention to connect
    - Active scanning
    - Passive scanning
  - ➢ Initiating: Devices intending to form connection listen for connectable advertising packets and initiate by sending connect packet
  - ➢ Connected: Master is the initiator and slave is the advertiser
  - ➢ Standby: Device in unconnected state



Phases of BLE operation



Bluetooth Low Energy (BLE)

- **Low Energy**: Upto 50% of Bluetooth classic
- **For short broadcast**: Your body temperature, Heart rate, Wearables, sensors, automotive, industrial
  Not for voice/video, file transfers
- **Small messages**: Data rate is 1 Mbps - sending just small data packets
- **Battery Life**: In years from coin cells
- **Simple**: Star topology, no scatter nets, mesh
- Lowest cost and easy to implement
- Discovery and connection improvements
- Low latency, fast transaction (3 ms from start to finish)

Bluetooth Smart Applications

- Proximity: In car, In the room
- Locator: Keys, watches, animals
- Health devices: Heart rate monitor, physical activities monitor, thermometer
- Sensors: Temperature, Battery Status, tire pressure
- Remote control: Open/close locks, turn on lights

Use Cases – Physical Security

Use Cases – Home Automation

What is ZigBee

- An open, global, packet-based protocol designed to provide an easy to use architecture for secure, reliable, low power wireless networks
- Technological Standard created for control and sensor networks
- Based on IEEE 802.15.4 standard
- Created by ZigBee Alliance
- Enables a Wireless Personal Area Network (WPAN)
- IEEE 802.15.4 protocol operates in the unlicensed spectrum in three different radio frequency bands: 868 MHz, 915 MHz and 2400 MHz
- Lower frequencies pose fewer issues with RF interference, but 2.4 GHz band is the most often used band worldwide

802.15.4 bands

- Range: 200 meters in open air line of sight test. Indoors – 30 meters
- Higher power transceivers or mesh networking can extend range

Frequency range (MHz)	Channel numbers	Modulation	Data rate (Kbps)	Region
868.3	1 channel: 0	BPSK O-QPSK ASK	20 100 250	Europe
902-928	10 channels: 1-10	BPSK O-QPSK ASK	40 250 250	North America, Australia
2405-2480	16 channels: 11-26	O-QPSK	250	Worldwide

ZigBee

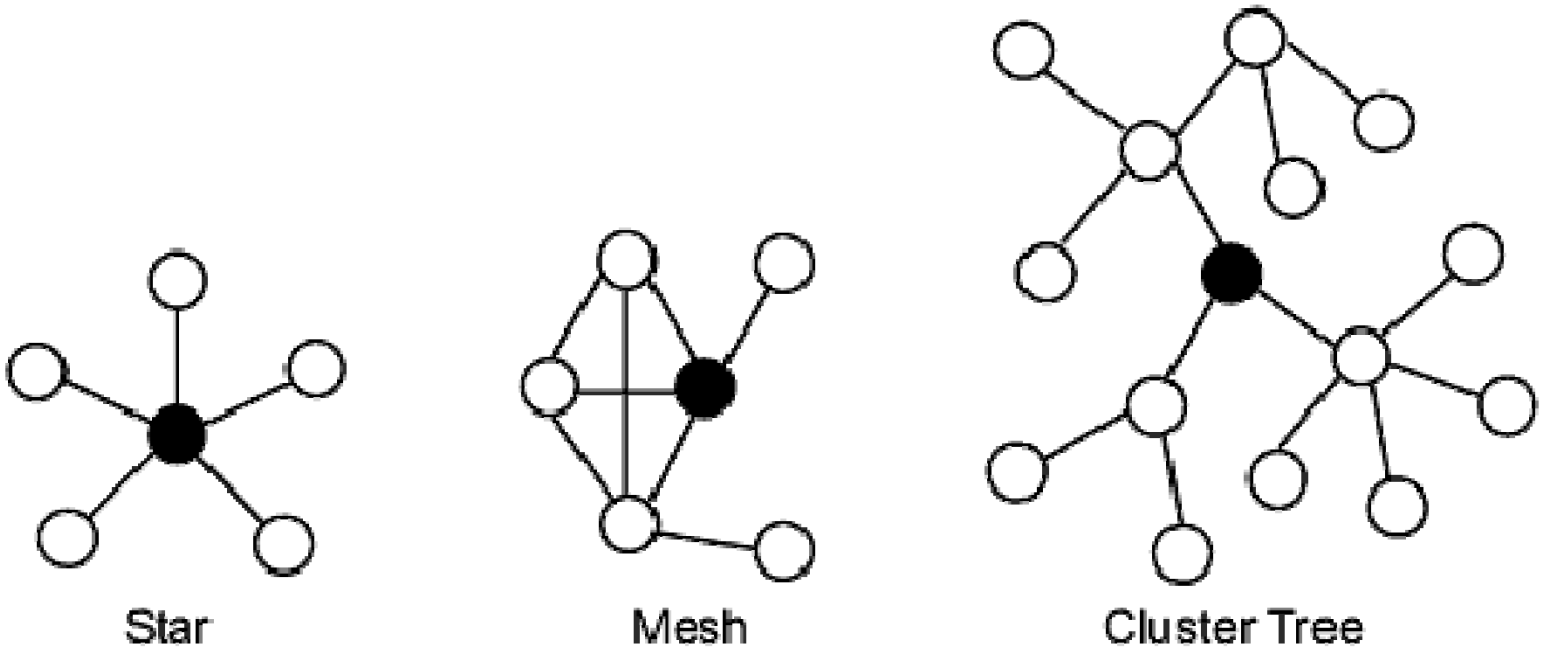
- Designed for low power consumption allowing batteries to last for a long time
- Provides network, security and application support services operating on top of the IEEE 802.15.4 standard

Advantages of ZigBee

- Low power consumption
- Low cost (device, installation and maintenance)
- High density of nodes per network
- Simple protocol – ZigBee protocol stack around 1/4th of Bluetooth's or WiFi

Network Topologies Supported

- Topology of a network describes how the nodes are connected



ZigBee Network Devices

- Three different ZigBee device types
  - ZigBee coordinator node
    - Root of the network tree and a bridge to other network
    - Stores information about the network
    - Only one coordinator node for a network
  - Full Function Device (FFD)
    - An intermediate router transmitting data from other devices
    - Needs lesser memory than coordinator node
    - Can also act as coordinator
    - Supports any network topology
  - Reduced Function Device (RF)
    - Capable of talking in the network
    - Cannot relay data from other device
    - Talks only to the network coordinator
    - Limited to only Star topology

IEEE 802.15.4 Start-up Sequence

- Process of startup, network configuration and joining of existing networks
  - Device initializes its stack (PHY and MAC layers)
  - PAN coordinator is created (each network has only one)
  - PAN coordinator will listen to other networks and derives a PAN ID that is unique
  - PAN coordinator will choose a specific radio frequency for the network
  - Network started by configuring PAN coordinator and starting the device in coordinator mode → PAN coordinator can accept requests
  - Nodes can join the network by finding the PAN coordinator using an active channel scan. Passive channel scan used in beacon-based network
  - PAN coordinator decides whether the device can join based on access control rules or resource availability of the PAN coordinator

Comparison of Wireless Standards

Wireless Parameter	Bluetooth	Wi-Fi	ZigBee
Frequency band	2.4 GHz	2.4 GHz	2.4 GHz
Physical/MAC layers	IEEE 802.15.1	IEEE 802.11b	IEEE 802.15.4
Range	9 m	75 to 90 m	Indoors: up to 30 m Outdoors (line of sight): up to 100 m
Current consumption	60 mA (Tx mode)	400 mA (Tx mode) 20 mA (Standby mode)	25-35 mA (Tx mode) 3 µA (Standby mode)
Raw data rate	1 Mbps	11 Mbps	250 Kbps
Protocol stack size	250 KB	1 MB	32 KB 4 KB (for limited function end devices)
Typical network join time	>3 sec	variable, 1 sec typically	30 ms typically
Interference avoidance method	FHSS (frequency-hopping spread spectrum)	DSSS (direct-sequence spread spectrum)	DSSS (direct-sequence spread spectrum)
Minimum quiet bandwidth required	15 MHz (dynamic)	22 MHz (static)	3 MHz (static)
Maximum number of nodes per network	7	32 per access point	64 K
Number of channels	19	13	16

Thank You