M3 - Principles of Connected Devices and Protocols in IOT

III	**Principles of Connected Devices and Protocols in IoT**	RFID and NFC (Near-Field Communication), Bluetooth Low Energy (BLE) roles, LiFi , WPAN std : 802.15 standards: Bluetooth, IEEE 802.15.4, Zigbee, Z-wave, Narrow Band IoT, Internet Protocol and Transmission Control Protocol, 6LoWPAN, WLAN and WAN , IEEE 802.11, Long-range Communication Systems and Protocols: Cellular Connectivity-LTE, LTE-A, LoRa and LoRaWAN.	8	CO3

- Working of protocol
- In which application to use it
- Comparison with other protocols

Book :

- David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry, IoT Fundamentals Networking Technologies, Protocols, and Use Cases for the Internet of Things CISCO , Ch 4 ,5
- Analytics for the Internet of Things (IoT) Intelligent Analytics for Your Intelligent Devices.Andrew Minteer,Packet , ch 2

Blooms level : L1,L2,L3,L4

SENSORS, ACTUATORS, AND SMART OBJECTS

- **A sensor**: It senses
- More specifically, *a sensor measures some physical quantity and converts that measurement reading into a digital representation.*
- *That digital representation is typically passed to another device for transformation into useful data that can be consumed by intelligent devices or humans*
- Sensors are not limited to human-like sensory data.
- They are able to provide an extremely wide spectrum of rich and diverse measurement data with far greater precision than human senses

Active

Passive sensors

We have three types of active transducers, which are mentioned below:

- Piezo Electric Transducer.
- Photo Electric Transducer.
- Thermo Electric Transducer.

07 Jun 2022

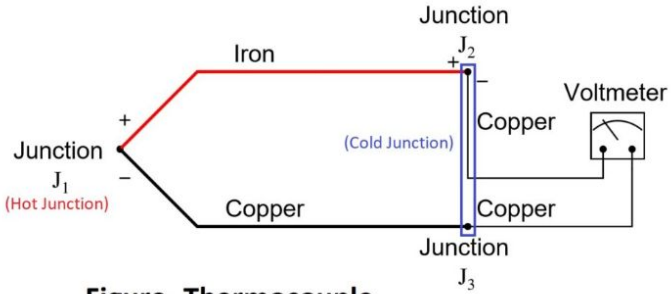
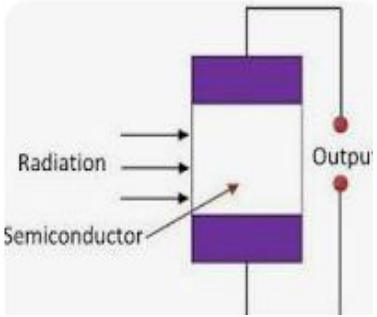
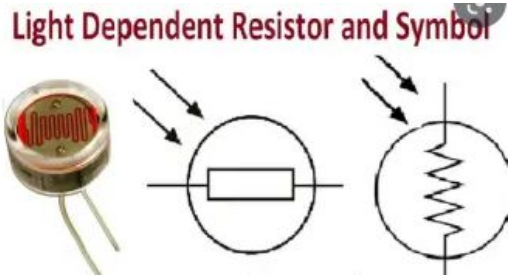
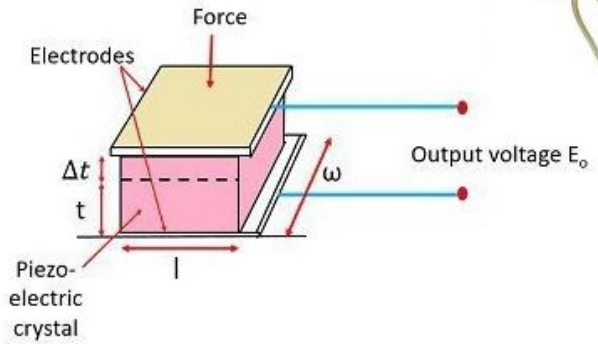


Figure- Thermocouple

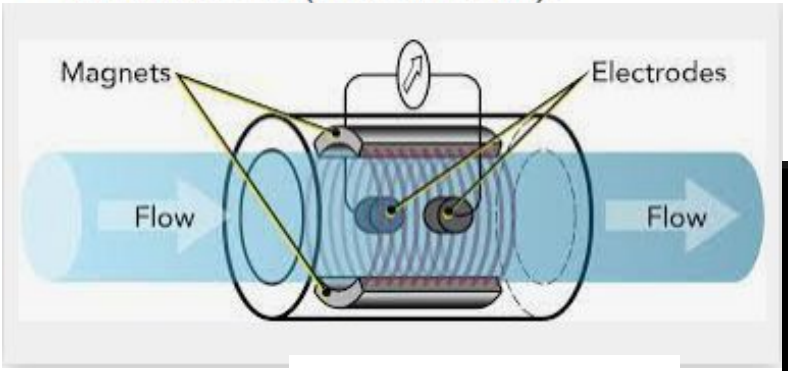


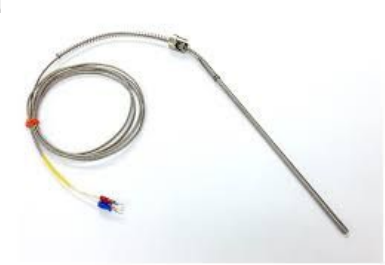


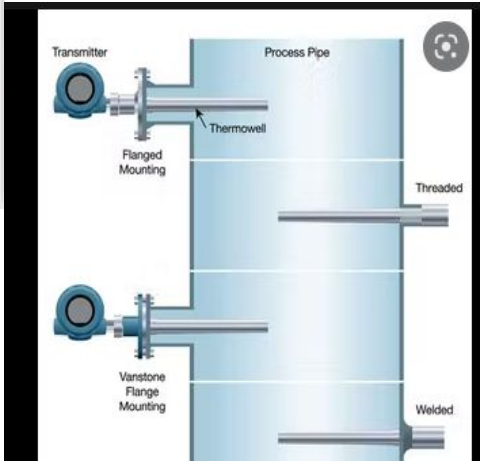


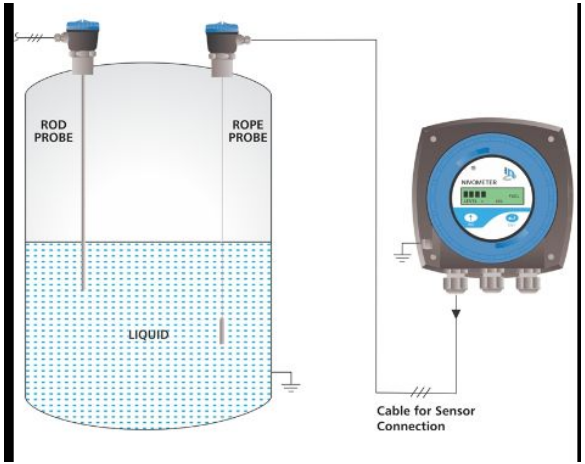
Invasive or non-invasive

- **Invasive or non-invasive:**
- Sensors can be categorized based **on whether a sensor is part of the environment it is measuring (invasive)** or
- **External to it (non-invasive).**

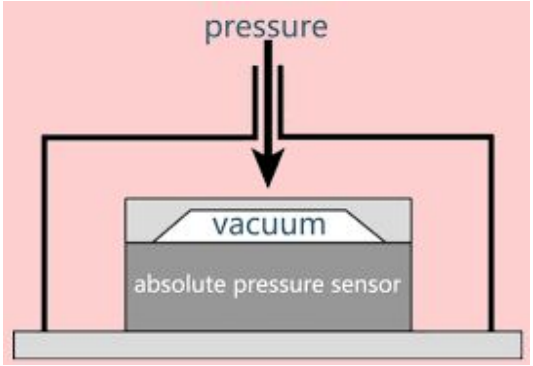




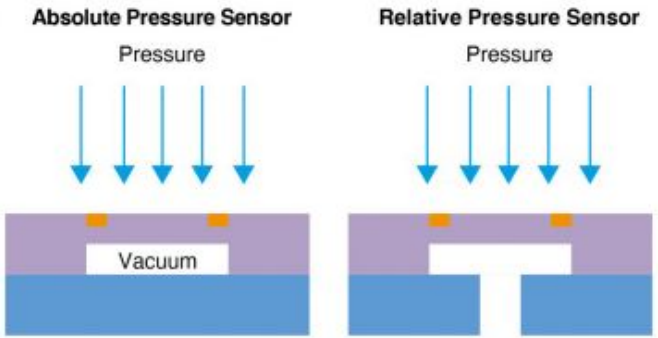




- **Contact or no-contact:**
- Sensors can be categorized based on whether they **require physical contact with what they are measuring (contact)** or **not (no-contact).**



- **Absolute or relative:**
- Sensors can be categorized based on **whether they measure on an absolute scale (absolute)** or based on a difference with **a fixed or variable reference value (relative).**



Categorization based on what physical phenomenon a sensor is measuring

Sensor Types	Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors generate a signal even when a person is stationary, whereas motion sensors do not.	Electric eye, radar

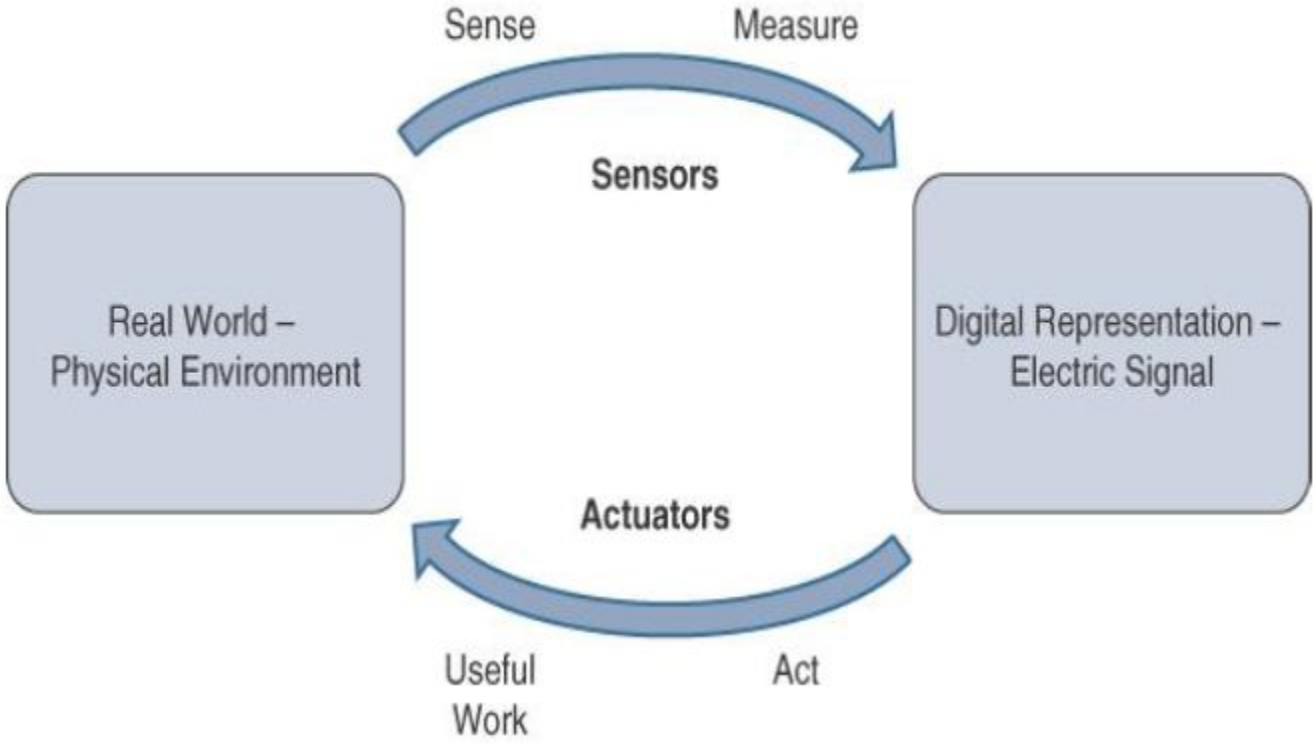
Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors, measuring force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, Bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter

Acoustic	Acoustic sensors measure sound levels and convert that information into digital or analog data signals.	Microphone, geophone, hydrophone
Humidity	Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on.	Hygrometer, humistor, soil moisture sensor
Light	Light sensors detect the presence of light (visible or invisible).	Infrared sensor, photodetector, flame detector
Radiation	Radiation sensors detect radiation in the environment. Radiation can be sensed by scintillating or ionization detection.	Geiger-Müller counter, scintillator, neutron detector

Temperature	Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation.	Thermometer, calorimeter, temperature gauge
Chemical	Chemical sensors measure the concentration of chemicals in a system. When subjected to a mix of chemicals, chemical sensors are typically selective for a target type of chemical (for example, a CO_2 sensor senses only carbon dioxide).	Breathalyzer, olfactometer, smok detector
Biosensors	Biosensors detect various biological elements, such as organisms, tissues, cells, enzymes, antibodies, and nucleic acid.	Blood glucose biosensor, pulse oximetry, electrocardiograph

Actuators

- Actuators are natural complements to sensors
- Sensors are designed to sense and measure practically any measurable variable in the physical world.
- They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human).
- **Actuators, on the others hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.**
- *Sensors provide the information, actuators provide the action*


Sense
Measure
Sensors
Real World –
Physical Environment
Digital Representation –
Electric Signal
Actuators
Useful
Work
Act

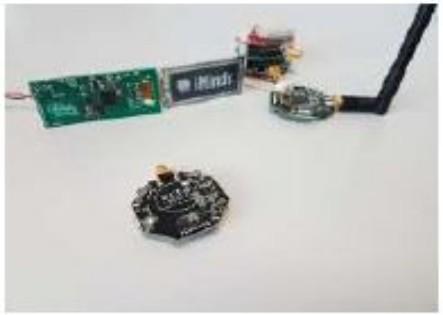
- Actuators also vary greatly in function, size, design, and so on.
- Some common ways that they can be classified include the following:
- **Type of motion:** Actuators can be classified based on the type of motion they produce (for example, linear, rotary, one/two/three-axes).
- **Power:** Actuators can be classified based on their power output (for example, high power, low power, micro power)
- **Binary or continuous:** Actuators can be classified based on the number of stable-state outputs.
- **Area of application:** Actuators can be classified based on the specific industry or vertical where they are used.
- **Type of energy:** Actuators can be classified based on their energy type.

Classification based on energy type

Type	Examples
Mechanical actuators	Lever, screw jack, hand crank
Electrical actuators	Thyristor, biopolar transistor, diode
Electromechanical actuators	AC motor, DC motor, step motor
Electromagnetic actuators	Electromagnet, linear solenoid
Hydraulic and pneumatic actuators	Hydraulic cylinder, pneumatic cylinder, piston, pressure control valves, air motors
Smart material actuators (includes thermal and magnetic actuators)	Shape memory alloy (SMA), ion exchange fluid, magnetorestrictive material, bimetallic strip, piezoelectric bimorph
Micro- and nanoactuators	Electrostatic motor, microvalve, comb drive

Explore few more sensors and actuators …..

Constrained Devices



- "A node where some of the characteristics that are otherwise pretty much taken for granted for Internet nodes **at the time of writing** are not attainable, […] due to **cost, size, and energy constraints**"

- Significant constraints on:
  - maximum code complexity (ROM/Flash)
  - size of state and buffers (RAM)
  - available computational power
  - connectivity

Constrained Networks

- "A network where some of the characteristics pretty much taken for granted with link layers in common use in the Internet **at the time of writing** are not attainable"

- Significant constraints on:
  - low achievable **throughput**
  - high **packet loss**
  - highly **asymmetric links**
  - severe penalties for using **larger packets**
  - limits on **reachability** over time

Classes of Constrained Nodes

Name	Data size (RAM)	Code size (Flash)
Class 0	<< 10 KiB	<< 100 KiB
Class 1	~ 10 KiB	~ 100 KiB
Class 2	~ 50 KiB	~ 250 KiB

Values in 2014

- C0 Devices
  - no direct secure Internet connection
  - use larger devices as gateways/proxies
  - preconfigured and rarely reconfigured
- C1 Devices
  - can use environment specific protocols, e.g., CoAP
  - no access to standard Internet protocols, e.g., HTTP, TLS
  - can be integrated into an IP network
- C2 Devices
  - can use most of protocols

Constrained Devices: Class 0

- Very constrained **sensor-like**
- They need **the help of larger devices** acting as proxies, gateways, or servers to participate in Internet communications
- **They cannot be secured** or managed in a traditional way and are most likely preconfigured

- In other words, **they cannot be used without a gateway**

Constrained Devices: Class 1

- Cannot easily talk to other Internet nodes employing a full stack, e.g., no HTTP, TLS, and XML
- However, they are capable enough to
  - use a protocol stack **specifically designed for constrained nodes** (CoAP over UDP)
  - **participate in conversations** without the help of a gateway node
- Class 1 devices can provide support for the **security functions** required on a large network

- They still **need to be parsimonious** with state memory, code space, and often power expenditure for protocol and application usage

Constrained Devices: Class 2

- Less constrained and **fundamentally capable of supporting most of the same protocol** stacks as used on notebooks or servers
- However, even class 2 devices can **benefit from lightweight and energy-efficient protocols** and from consuming less bandwidth, e.g., using the protocol stacks defined for more constrained devices

Limitations based on energy constrains

- Devices are classified also based on their energy capabilities

Name	Type of limitation	Example power source
E0	Event energy-limited	Event-based harvesting
E1	Period energy-limited	Battery periodically recharged/replaced
E2	Lifetime energy-limited	Non-replaceable primary battery
E9	No energy limitation	Mains-powered

The Evolution of Constrained Devices

- **Phase 1: Smart Tags** to uniquely identify physical things
  - textual identifiers: bar code, QR code
  - digital identifiers: passive/active RFID, i.e., small chips transmitting their unique identification number via wireless at small range

- **Phase 2: Automated Sensing** to transmit sensed data to remote devices
  - periodic or on-demand transmission
  - read-only and battery-powered

- **Phase 3: Smart Devices** allowing to develop modern complex IoT applications
  - sensors and actuators
  - gateways and fog nodes

COMMUNICATIONS CRITERIA

- *The characteristics and attributes you should consider when selecting and dealing with connecting smart objects*
- **Range**
- **Frequency Bands:**
- **Power Consumption:**
- **Topology**
- **Constrained Devices:**
- **Constrained-Node Networks:**

Technologies for connecting smart devices

- **IEEE 802.15.4:** This section highlights IEEE 802.15.4, an older but foundational wireless protocol for connecting smart objects.
- **IEEE 802.15.4g and IEEE 802.15.4e:** This section discusses improvements to 802.15.4 that are targeted to utilities and smart cities deployments.
- **IEEE 1901.2a:** This section discusses IEEE 1901.2a, which is a technology for connecting smart objects over power lines.
- **IEEE 802.11ah:** This section discusses IEEE 802.11ah, a technology built on the well-known 802.11 Wi-Fi standards that is specifically for smart objects.
- **LoRaWAN:** This section discusses LoRaWAN, a scalable technology designed for longer distances with low power requirements in the unlicensed spectrum.
- **NB-IoT and Other LTE Variations:** This section discusses NB-IoT and other LTE variations, which are often the choice of mobile service providers looking to connect smart objects over longer distances in the licensed spectrum.

Connecting smart devices

Smart cities deployment

Connecting objects over power lines

Built on wi-Fi standards

Longer distances with low power - unlicensed spectrum

Narrow-Band - long distances in licensed spectrum -LTE - Long Term Evolution technology

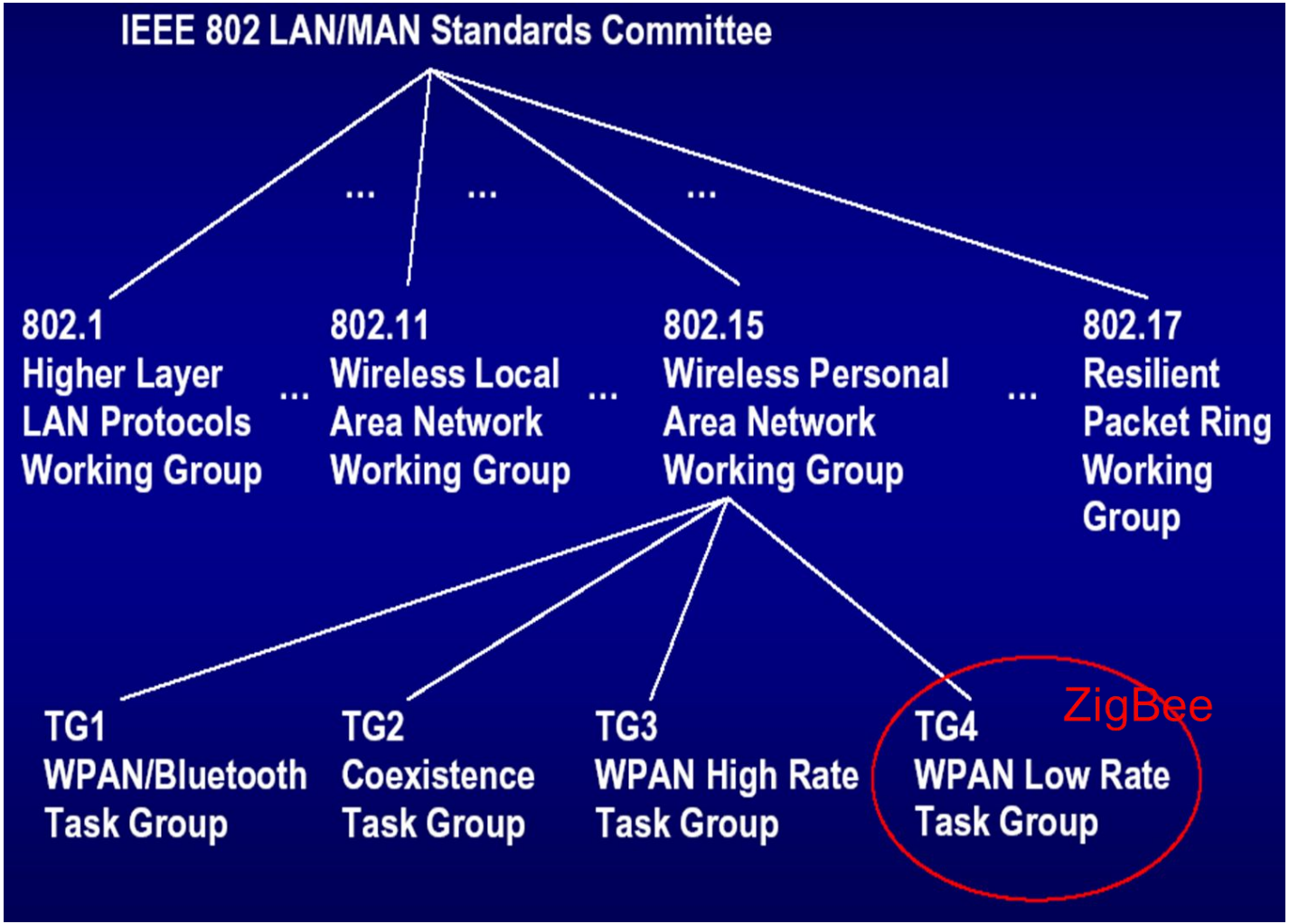
WPAN

- **A personal area network (PAN) is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person**
- **Reach:** *A few meters*
- **Use:** *Intrapersonal communication in devices.*

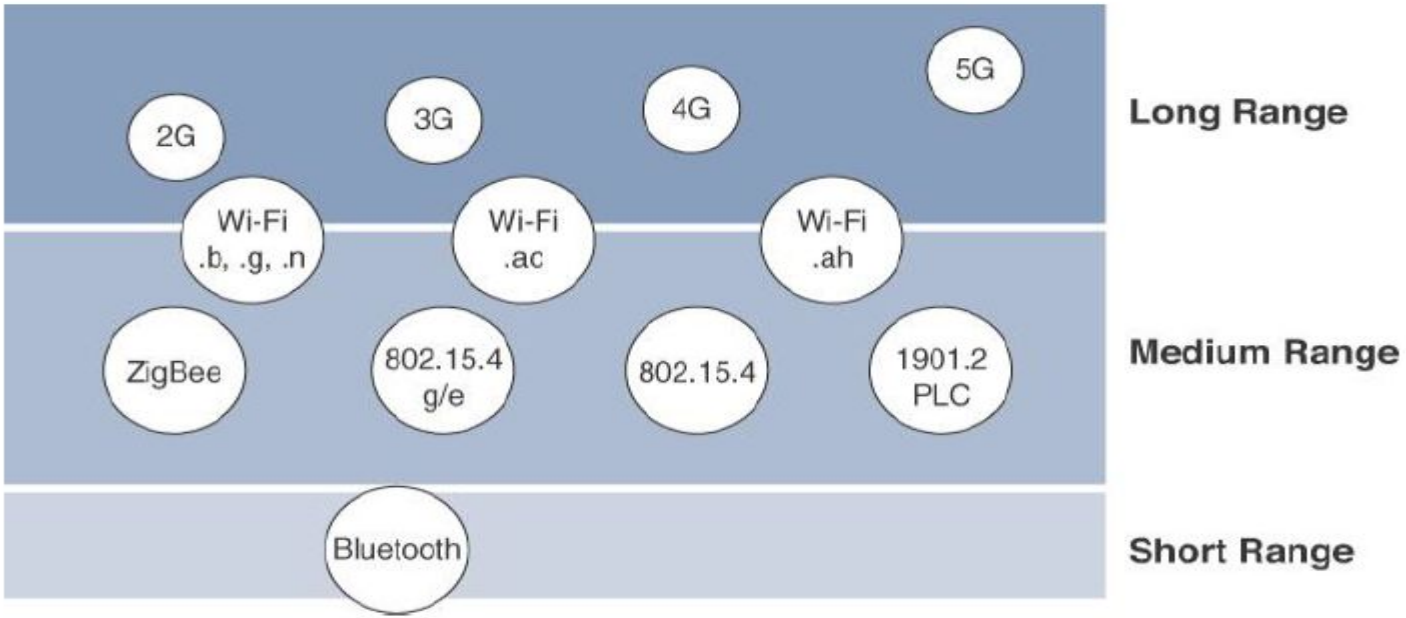
  Connecting to a higher level network and the Internet.
- **A wireless PAN consists of a dynamic group of less than 255 devices that communicate within about a 33-foot range**

802.15

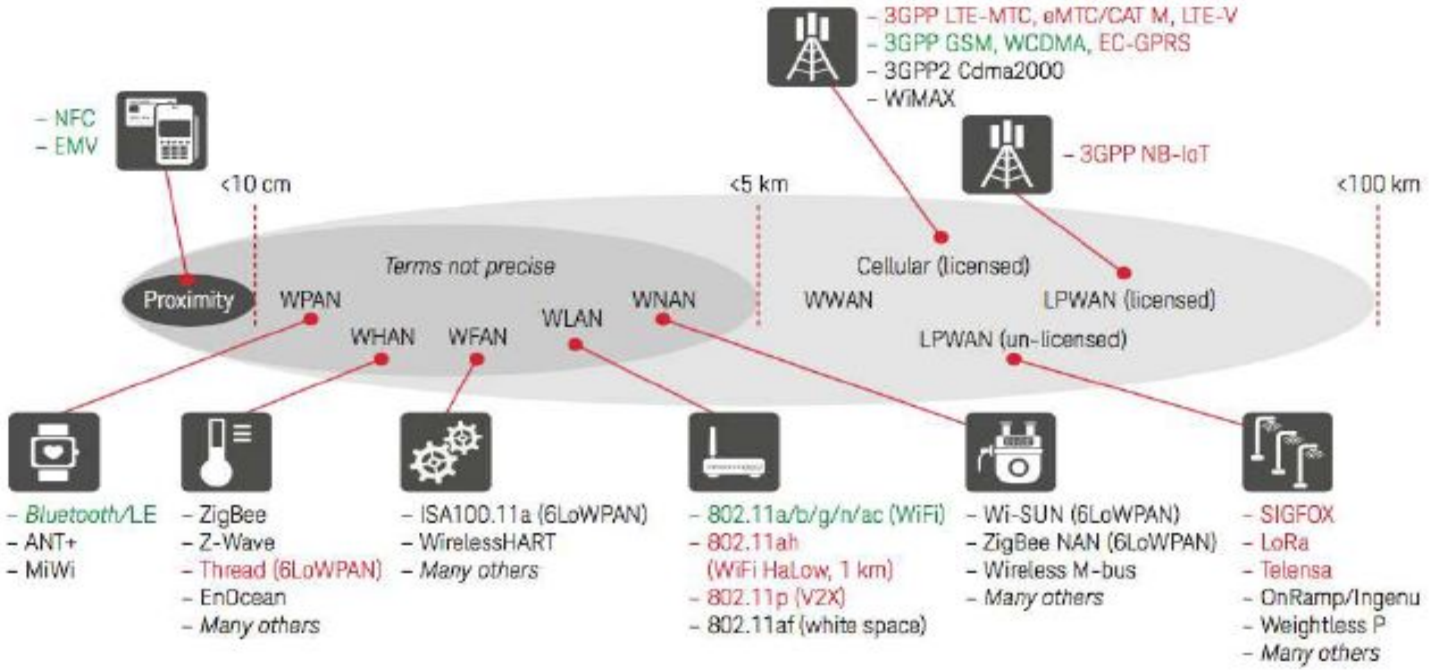
- IEEE 802.15 is the 15th working group of the IEEE 802
- Specializes in Wireless PAN (Personal Area Network)
- It includes four task groups (numbered from 1 to 4)


IEEE 802 LAN/MAN Standards Committee
802.1
Higher Layer
LAN Protocols
Working Group
802.11
Wireless Local
Area Network
Working Group
802.15
Wireless Personal
Area Network
Working Group
802.17
Resilient
Packet Ring
Working
Group
TG1
WPAN/Bluetooth
Task Group
TG2
Coexistence
Task Group
TG3
WPAN High Rate
Task Group
TG4
WPAN Low Rate
Task Group
ZigBee

- **Range**
- How far does the signal need to be propagated?
- That is, what will be the area of coverage for a selected wireless technology?
- Should indoor versus outdoor deployments be differentiated?



Several Wireless Communication Protocols

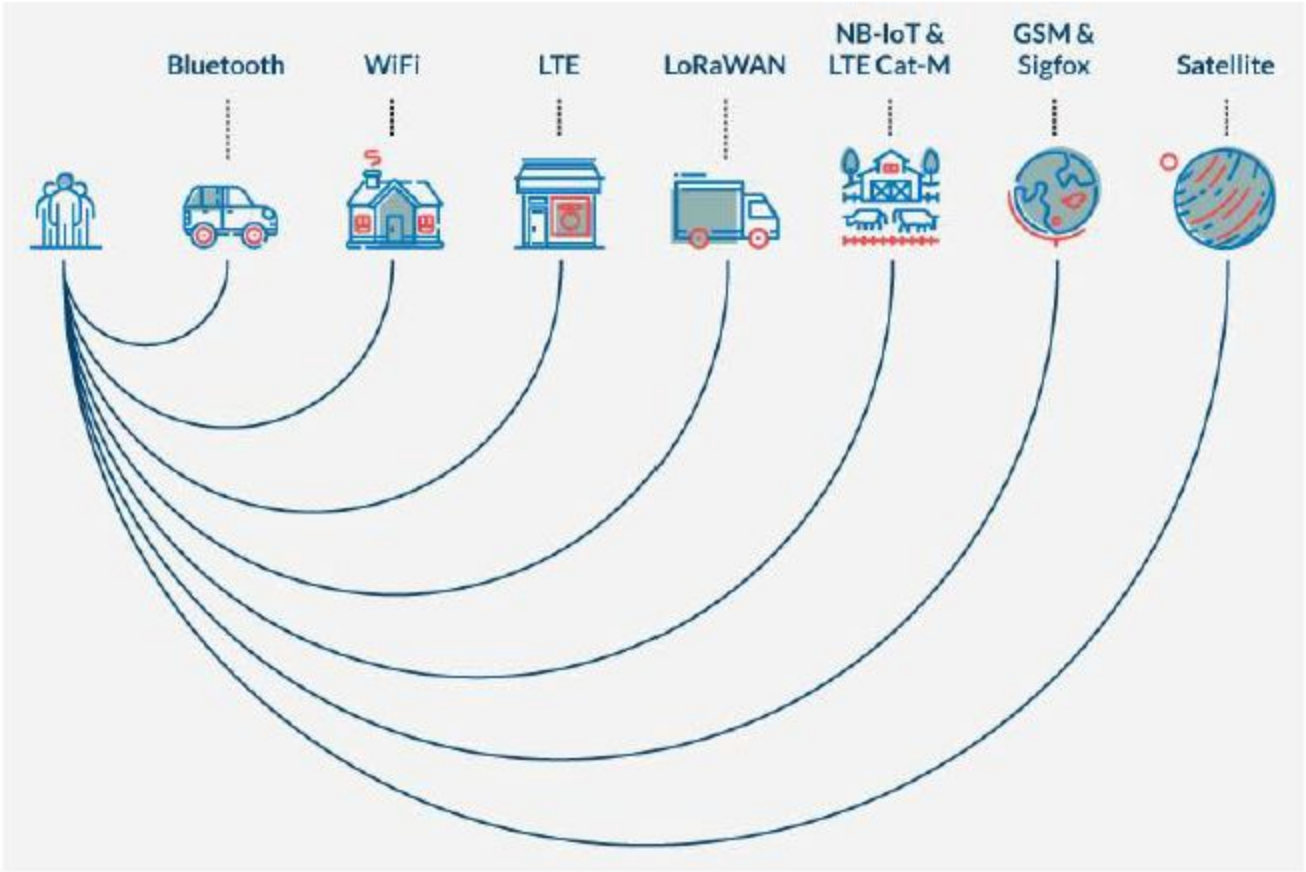


■ : > Billion units/year now
■ : Emerging

WPAN: Wireless Personal Area Network
WHAN: Wireless Home Area Network
WFAN: Wireless Field (or Factory) Area Network
WLAN: Wireless Local Area Network

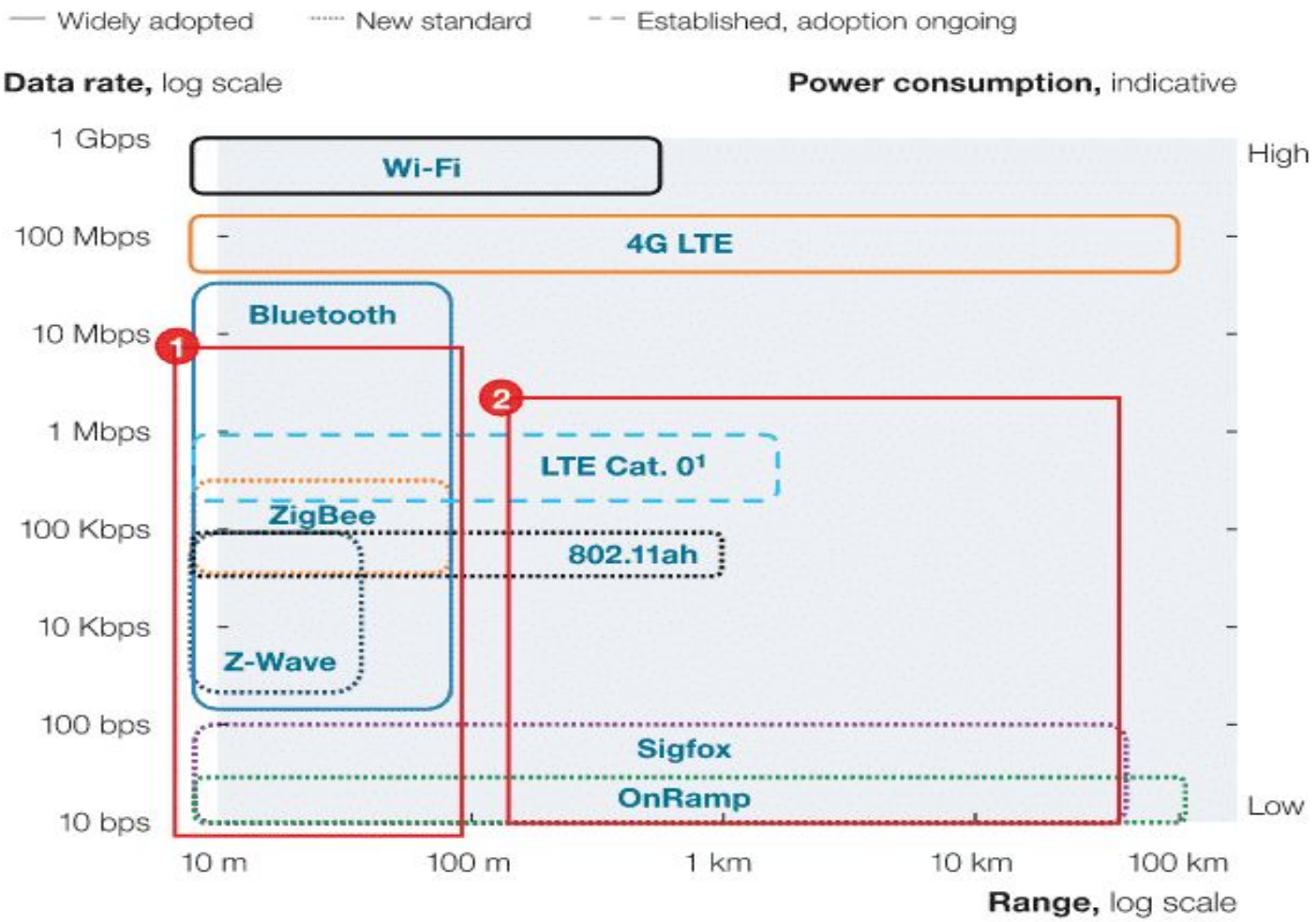
WNAN: Wireless Neighborhood Area Network
WWAN: Wireless Wide Area Network
LPWAN: Low Power Wide Area Network

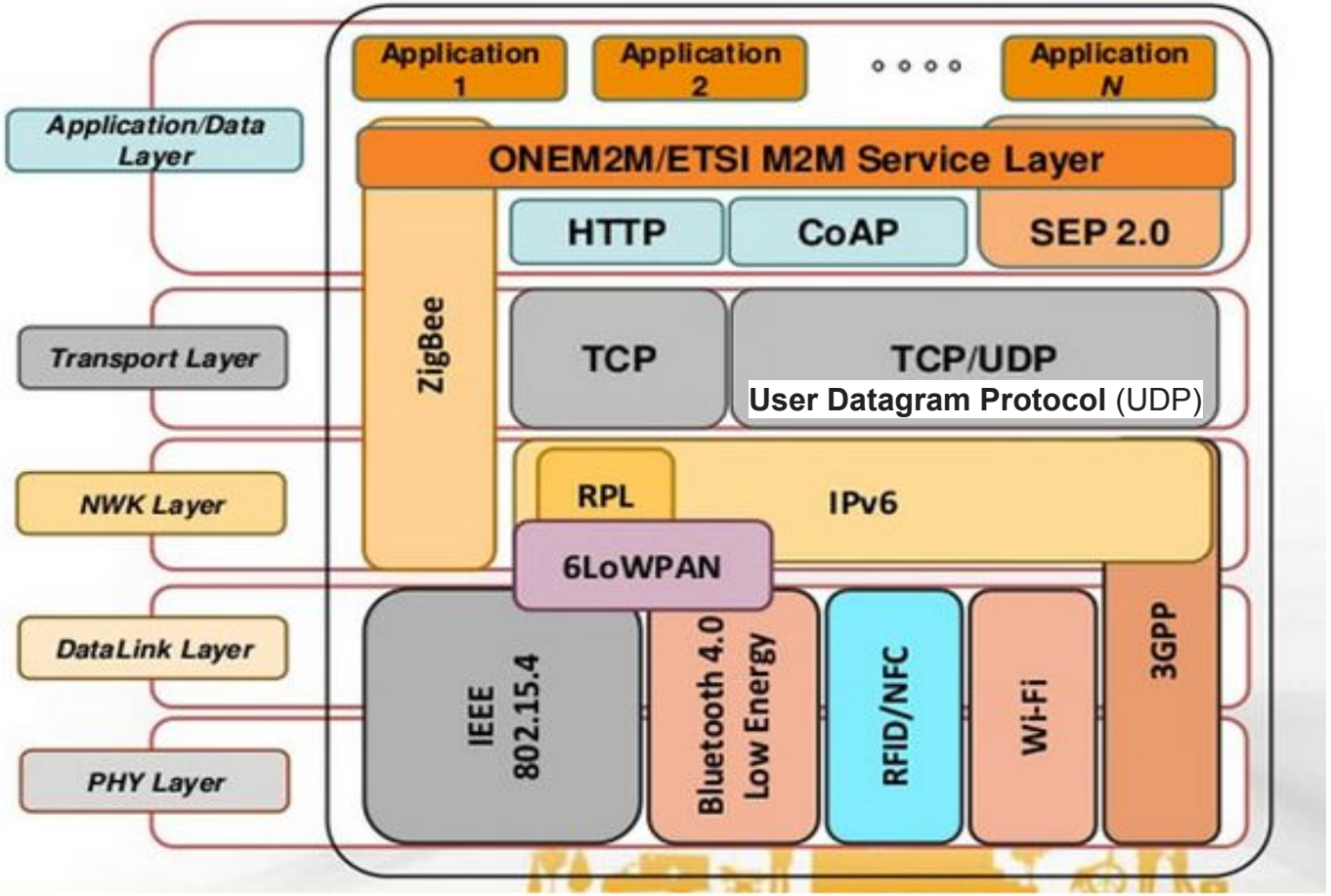
Wireless Protocols per Coverage Range



Communication / Transport layer

Technology	Frequency	Data Rate	Range	Power Usage	Cost
2G/3G	Cellular Bands	10 Mbps	Several Miles	High	High
Bluetooth/BLE	2.4Ghz	1, 2, 3 Mbps	~300 feet	Low	Low
802.15.4	subGhz, 2.4GHz	40, 250 kbps	> 100 square miles	Low	Low
LoRa	subGhz	< 50 kbps	1-3 miles	Low	Medium
LTE Cat 0/1	Cellular Bands	1-10 Mbps	Several Miles	Medium	High
NB-IoT	Cellular Bands	0.1-1 Mbps	Several Miles	Medium	High
SigFox	subGhz	< 1 kbps	Several Miles	Low	Medium
Weightless	subGhz	0.1-24 Mbps	Several Miles	Low	Low
Wi-Fi	subGhz, 2.4Ghz, 5Ghz	0.1-54 Mbps	< 300 feet	Medium	Low
WirelessHART	2.4Ghz	250 kbps	~300 feet	Medium	Medium
ZigBee	2.4Ghz	250 kbps	~300 feet	Low	Medium
Z-Wave	subGhz	40 kbps	~100 feet	Low	Medium


Widely adopted
New standard
Established, adoption ongoing
Data rate, log scale
Power consumption, indicative
1 Gbps
100 Mbps
10 Mbps
1 Mbps
100 Kbps
10 Kbps
100 bps
10 bps
High
Low
Wi-Fi
4G LTE
Bluetooth
1
2
LTE Cat. 0¹
ZigBee
802.11ah
Z-Wave
Sigfox
OnRamp
10 m
100 m
1 km
10 km
100 km
Range, log scale


Application 1
Application 2
Application N
Application/Data Layer
ONEM2M/ETSI M2M Service Layer
HTTP
CoAP
SEP 2.0
ZigBee
Transport Layer
TCP
TCP/UDP
User Datagram Protocol (UDP)
NWK Layer
RPL
IPv6
6LoWPAN
DataLink Layer
IEEE 802.15.4
Bluetooth 4.0 Low Energy
RFID/NFC
Wi-Fi
3GPP
PHY Layer

IoT Access Technologies

- **Standardization and alliances:** The standards bodies that maintain the protocols for a technology
- **Physical layer:** The wired or wireless methods and relevant frequencies
- **MAC layer:** Considerations at the Media Access Control (MAC) layer, which bridges the physical layer with data link control
- **Topology:** The topologies supported by the technology
- **Security:** Security aspects of the technology
- **Competitive technologies:** Other technologies that are similar and may be suitable alternatives to the given technology

IEEE 802.15.4 is a **low-cost, low-data-rate** wireless access technology for devices that are operated or work on batteries. This describes how low-rate wireless personal area networks (LR-WPANs) function.

Properties:

1. Standardization and alliances: It specifies low-data-rate PHY and MAC layer requirements for wireless personal area networks (WPAN).

IEEE 802.15. Protocol Stacks include:

- **ZigBee:**
  a. ZigBee is a Personal Area Network task group with a low rate task group 4.
  b. It is a technology of home networking.
  c. ZigBee is a technological standard created for controlling and sensing the network.
  d. ZigBee is the Personal Area network of task group 4 so it is based on IEEE 802.15.4 and is created by Zigbee Alliance.

- **6LoWPAN: stands for IPv6 over Low-power Wireless Personal Area Networks**
  a. The 6LoWPAN system is used for a variety of applications including wireless sensor networks.
  b. This form of wireless sensor network sends data as packets and uses IPv6 – providing the basis for the name – **IPv6** over Low power Wireless Personal Area Networks.
  c.
- **ZigBee IP:**
  a. Zigbee is a **standards-based wireless technology** that was developed for low-cost and low-power wireless
     i. machine-to-machine (M2M) and
     ii. internet of things (IoT) networks.

- **ISA100.11a:**
  a. It is a mesh network that provides secure wireless communication to process control.
  b.
- **Wireless HART:**
  a. It is also a wireless sensor network technology, that makes use of time-synchronized and self-organizing architecture.
- **Thread: An Open Standard Protocol for Home Automation**
  a. Thread is an IPv6-based networking protocol for low-power Internet of Things devices in IEEE 802.15. 4-2006 wireless mesh network. Thread is independent.
  b. Thread is an IP based wireless networking protocol designed for low-power connected products in home automation space.

2. Physical Layer:
https://www.electronics-notes.com/articles/connectivity/ieee-802-15-4-wireless/6lowpan.php

- This standard enables a wide range of PHY options in ISM bands, ranging from 2.4 GHz to sub-GHz frequencies.
- IEEE 802.15.4 enables data transmission speeds of
  - 20 kilobits per second,
  - 40 kilobits per second,
  - 100 kilobits per second, and
  - 250 kilobits per second.
- The fundamental structure assumes a 10-meter range and a data rate of 250 kilobits per second.
- To further reduce power usage, even lower data rates are possible.
- IEEE 802.15.4 regulates the RF transceiver and channel selection, and even some energy and signal management features, at the physical layer.
- Based on the frequency range and data performance needed, there are now six PHYs specified.
- Four of them employ frequency hopping techniques known as
  - **Direct Sequence Spread Spectrum (DSSS).**
- Both PHY data service and management service share a single packet structure so that they can maintain a common simple interface with MAC.

3. MAC layer:

The MAC layer provides links to the PHY channel by determining that devices in the same region will share the assigned frequencies.

The scheduling and routing of data packets are also managed at this layer.

The 802.15.4 MAC layer is responsible for a number of functions like:

- Beaconing for devices that operate as controllers in a network.
- used to associate and dissociate PANs with the help of devices.
- The safety of the device.
- Consistent communication between two MAC devices that are in a peer-to-peer relationship.

Several established frame types are used by the MAC layer to accomplish these functions. In 802.15.4, there are four different types of MAC frames:

- frame of data
- Frame for a beacon
- Frame of acknowledgement
- Frame for MAC commands

4. Topology: Networks based on IEEE 802.15.4 can be developed in a

- star, peer-to-peer, or mesh topology.
- Mesh networks connect a large number of nodes.
- This enables nodes that would otherwise be out of range to interact with each other to use intermediate nodes to relay data.

5. Security: For data security, the IEEE 802.15.4 standard employs the Advanced Encryption Standard (AES) with a 128-bit key length as the basic encryption technique.

- Activating such security measures for 802.15.4 significantly alters the frame format and uses a few of the payloads.
- The very first phase in activating AES encryption is to use the Security Enabled field in the Frame Control part of the 802.15.4 header.
- For safety, this field is a single bit which is assigned to 1.
- When this bit is set, by taking certain bytes from its Payload field, a field known as the Auxiliary Security Header is formed following the Source Address field.

6. Competitive Technologies: The IEEE 802.15.4 PHY and MAC layers serve as a basis for a variety of networking profiles that operate in different IoT access scenarios. DASH7 is a competing radio technology with distinct PHY and MAC layers.

https://www.topicsforseminar.com/2014/03/near-field-communication-nfc.html?m=1#gsc.tab=0

IEEE 802.15.4

Advantages of IEEE 802.15.4:

IEEE 802.15.4 has the following advantages:

- cheap cost
- long battery life,
- Quick installation
- simple
- extensible protocol stack

Disadvantages of IEEE 802.15.4:

IEEE 802.15.4's drawbacks include:

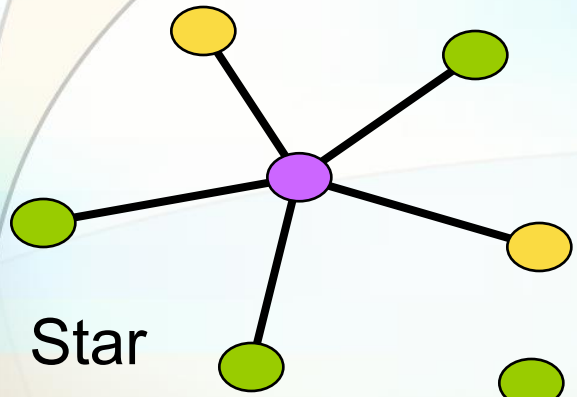
- IEEE 802.15.4 causes interference and multipath fading.
- doesn't employ a frequency-hopping approach.
- unbounded latency
- interference susceptibility

Applications of IEEE 802.15.4:

IEEE 802.15.4 Applications:

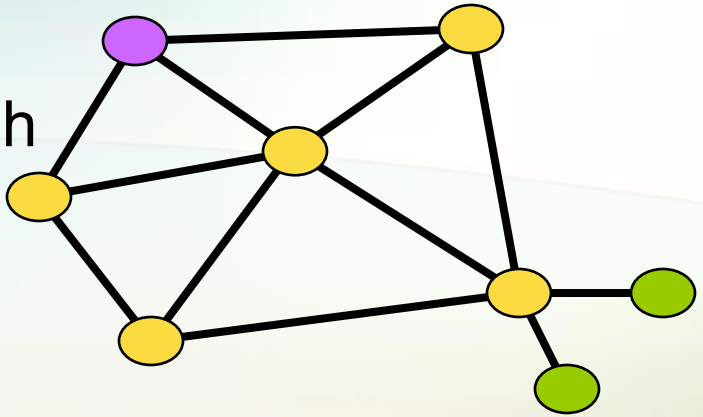
- Wireless sensor networks in the industry
- Building and home automation
- Remote controllers and interacting toys
- Automotive networks

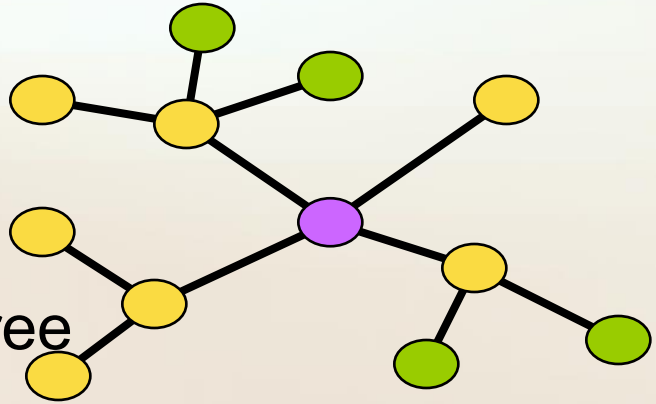
Network Topology Models



Star

Mesh





Cluster Tree

PAN coordinator (PANC)

Full Function Device (FFD,Router)

Reduced Function Device (RFD)

Wireless networking Basics

Network Scan

Device scans the 16 channels to determine the best channel to occupy.

Creating/Joining a PAN

Device can create a network (coordinator) on a free channel or join an existing network

Device Discovery

Device queries the network to discover the identity of devices on active channels

Service Discovery

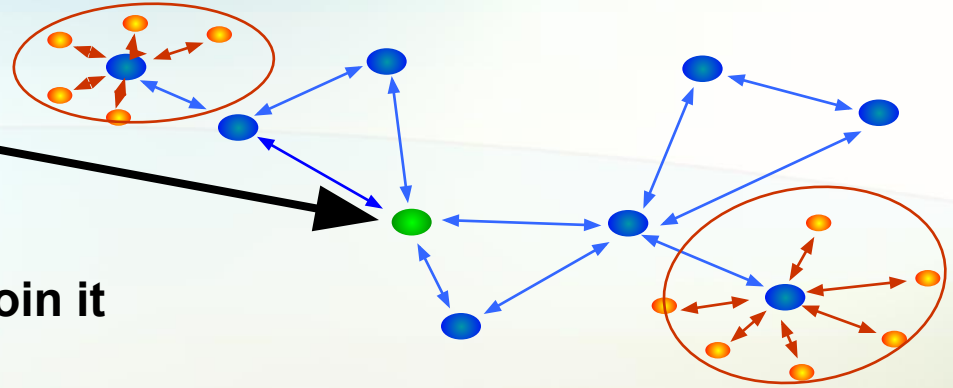
Device scans for supported services on devices within the network

Binding

Devices communicate via command/control messaging

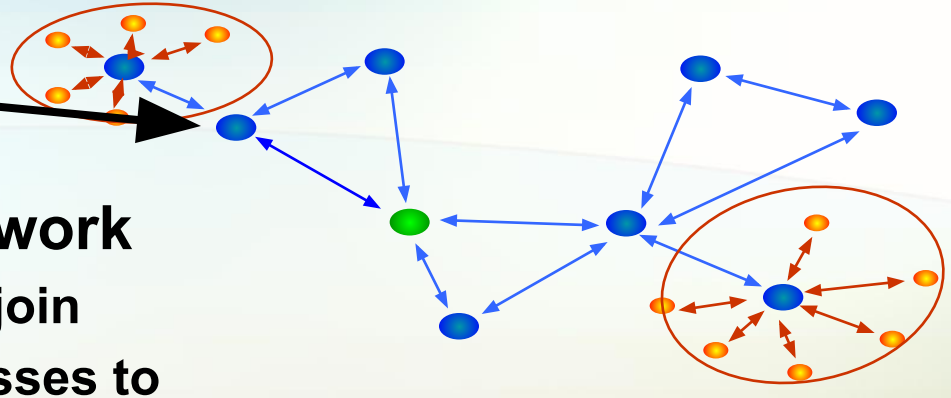
Network Pieces –PAN Coordinator

- PAN Coordinator
  - "owns" the network
    - Starts it
    - Allows other devices to join it
    - Provides binding and address-table services
    - Saves messages until they can be delivered
    - And more… could also have i/o capability
  - A "full-function device" – FFD
  - Mains powered



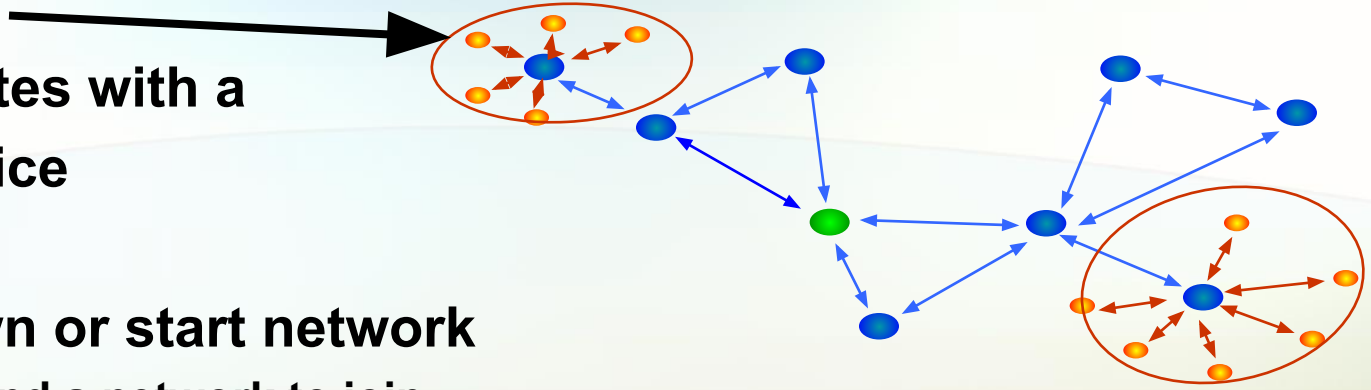
Network Pieces - Router

- Routers
  - Routes messages
  - Does not own or start network
    - Scans to find a network to join
      - Given a block of addresses to assign
  - A “full-function device” – FFD
  - Mains powered depending on topology
  - Could also have i/o capability

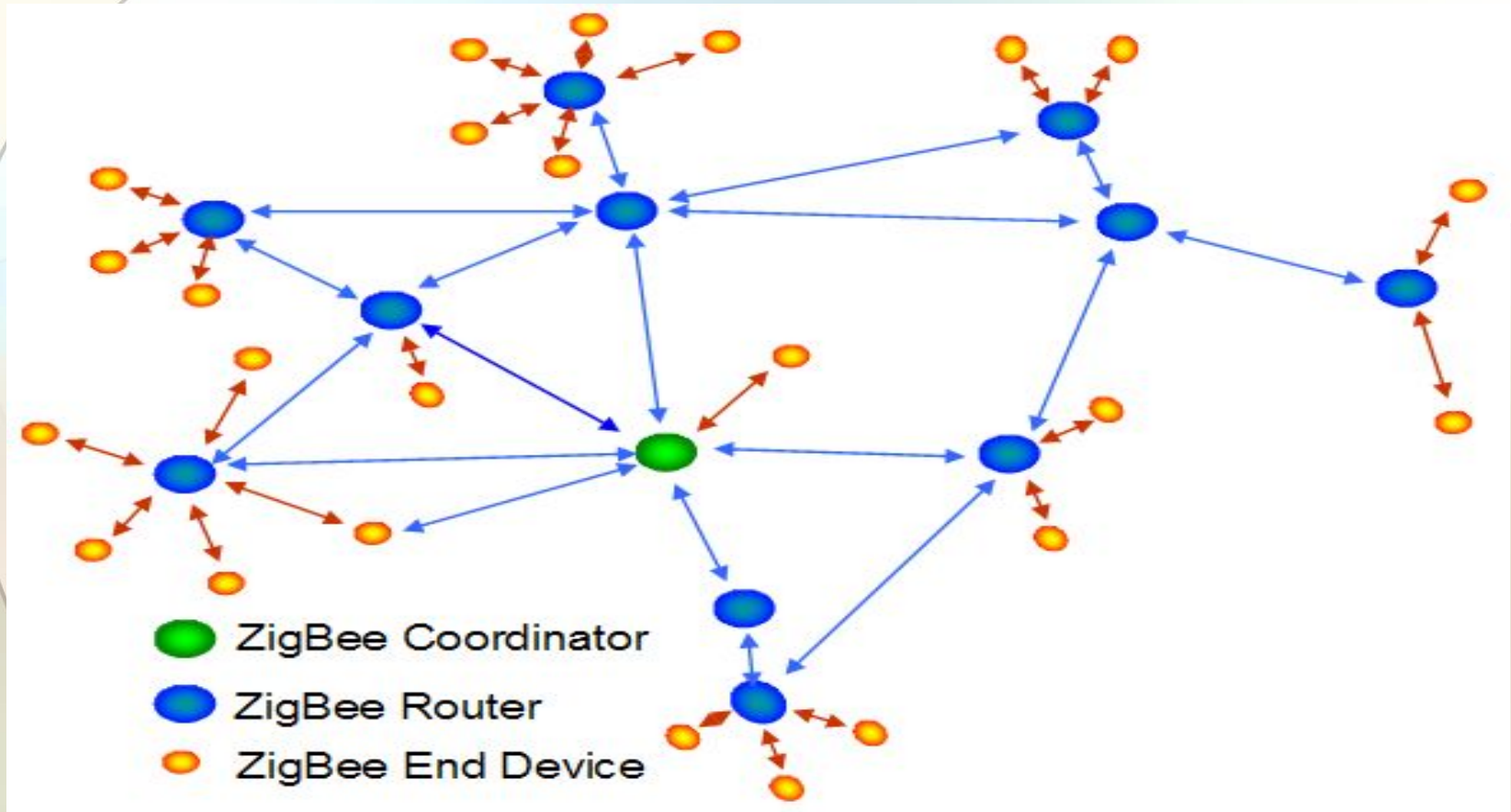


Network Pieces – End Device

- End Device
  - Communicates with a single device
  - Does not own or start network
    - Scans to find a network to join
  - Can be an FFD or RFD (reduced function device)
  - Usually battery powered



ZigBee is Mesh Networking

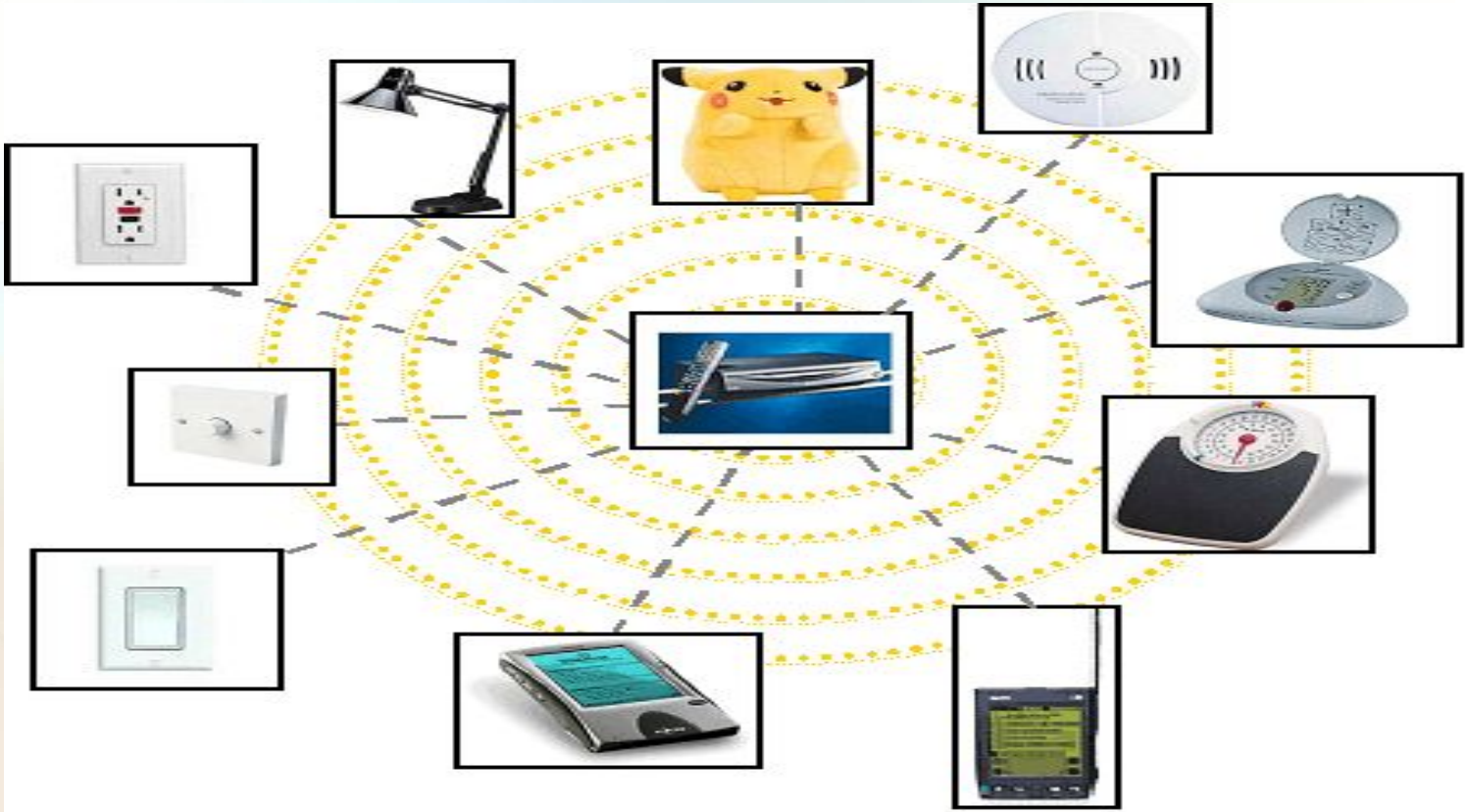


Traffic types

- Periodic data
  - Application defined rate (e.g. sensing temperature)
- Intermittent data
  - Application/external stimulus defined rate (e.g. light switch)
- Repetitive low latency data
  - Allocation of time slots (e.g. mouse)

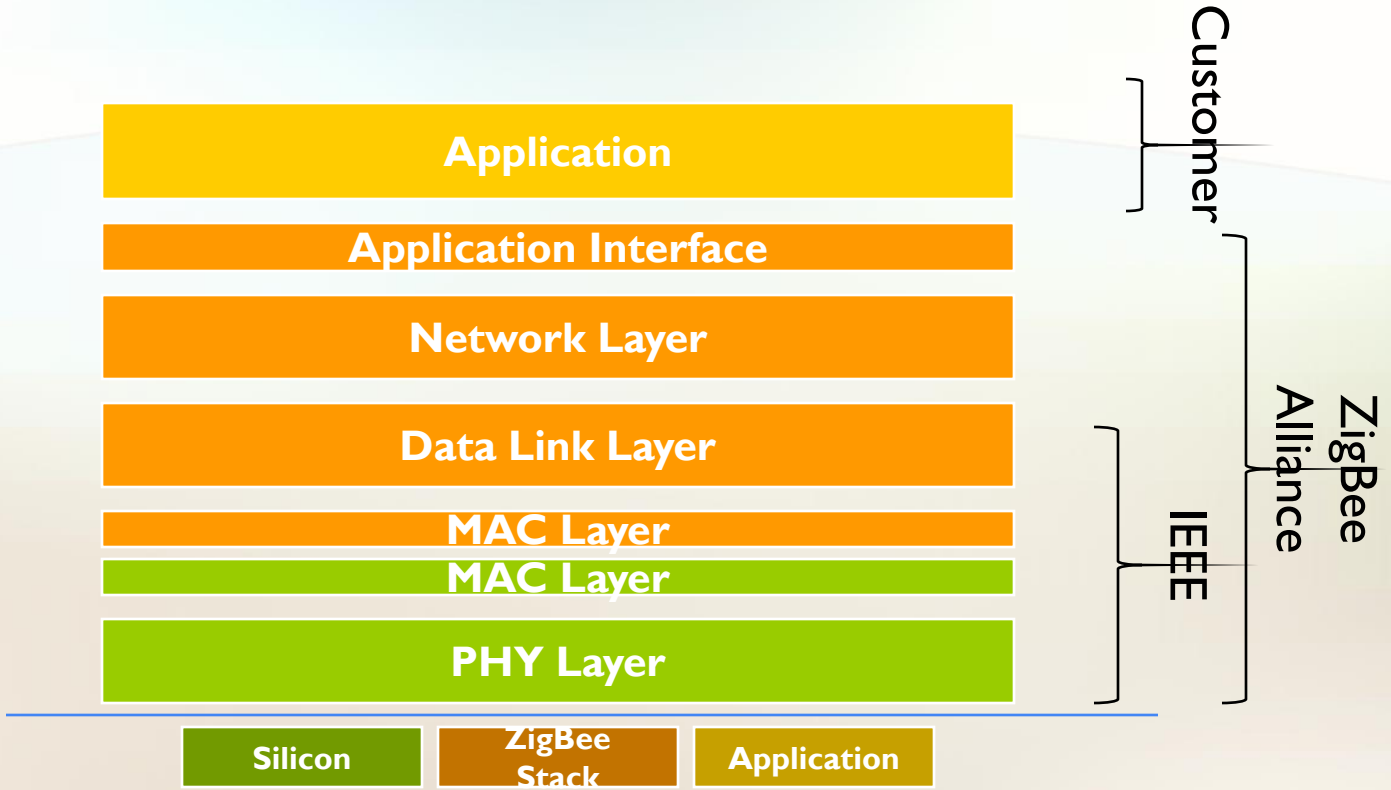
IEEE 802.15.4

ZigBee™ Alliance

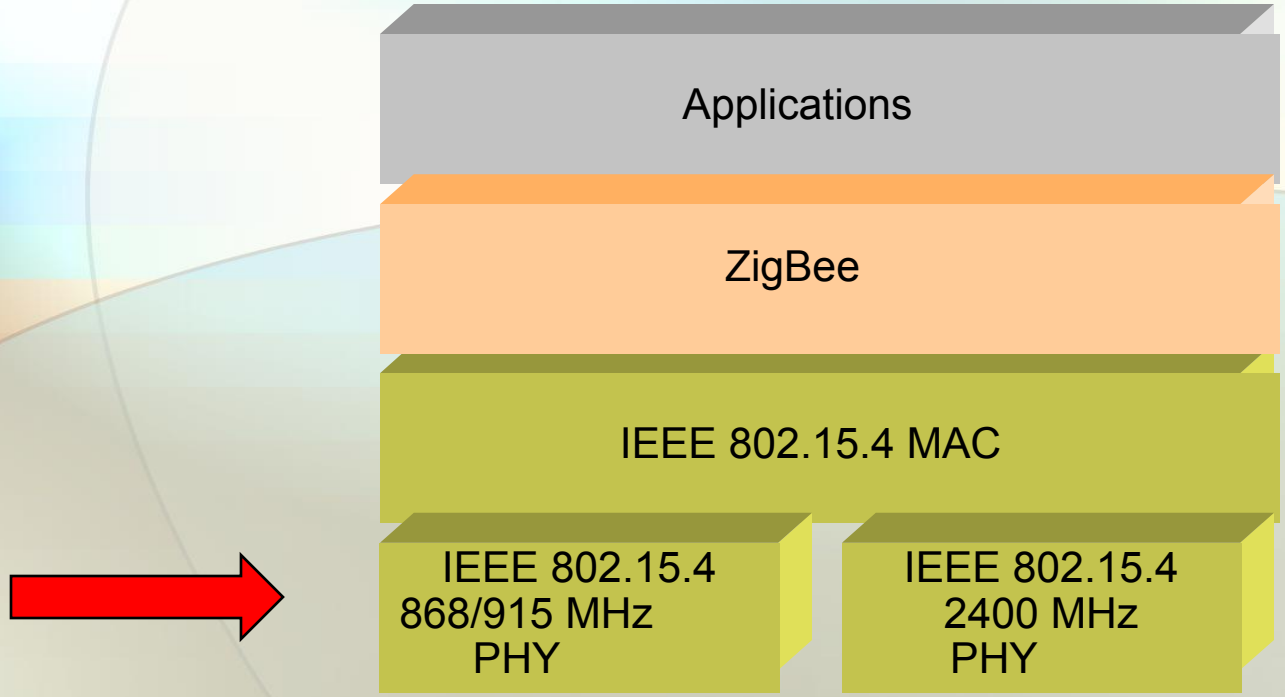


ZigBee Alliance - IEEE - Customer

Relationship



802.15.4 Architecture: Physical Layer



Physical Layer functionalities:

- Activation and deactivation of the radio transceiver
- Energy detection within the current channel
- Link quality indication for received packets
- Clear channel assessment for CSMA-CA
- Channel frequency selection
- Data transmission and reception

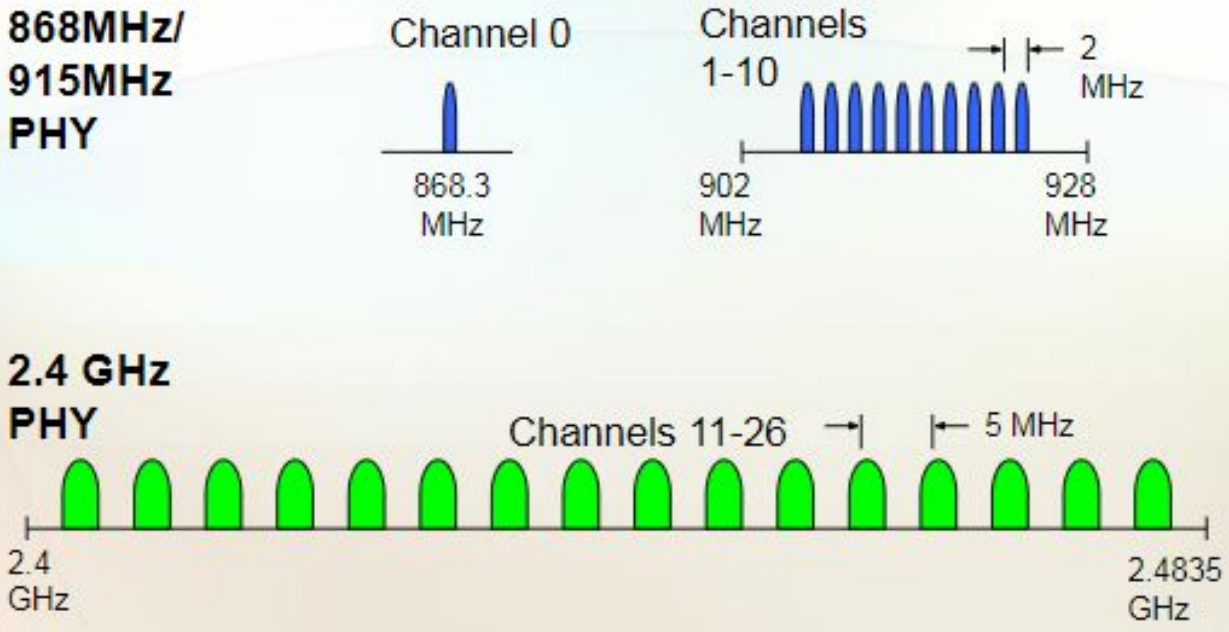
ZigBee specifies two Physical media:

- 868 MHz/915 MHz direct sequence spread spectrum (DSSS) PHY (11 channels)
  - 1 channel (20Kb/s) in European 868MHz band
  - 10 channels (40Kb/s) in 915 (902-928)MHz ISM band
- 2450 MHz direct sequence spread spectrum (DSSS) PHY (16 channels)
  - 16 channels (250Kb/s) in 2.4GHz band

IEEE 802.15.4 Physical Layer

The industrial, scientific, and medical radio band (ISM band) refers to a group of radio bands or parts of the radio spectrum that are internationally reserved for the use of radio frequency (RF) energy intended for scientific, medical and industrial requirements rather than for communications.

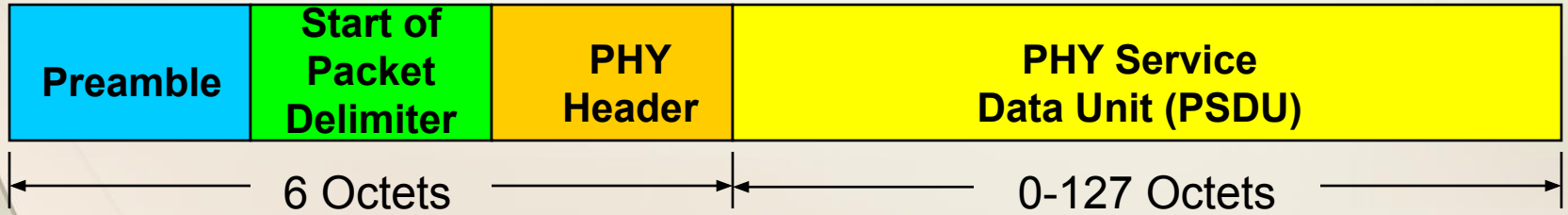
- **Operates in unlicensed ISM bands:**



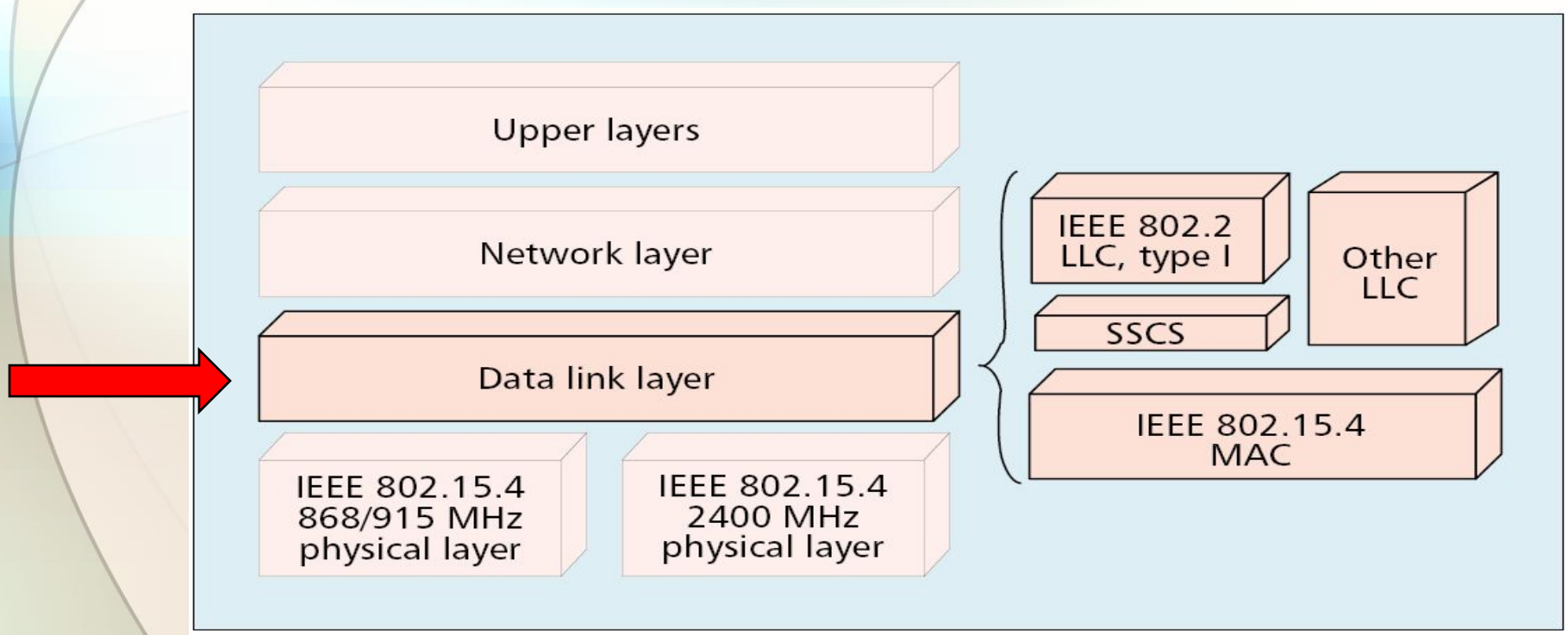
IEEE 802.15.4 PHY Overview Packet Structure

PHY Packet Fields

- Preamble (32 bits) – synchronization
- Start of Packet Delimiter (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – Data field



802.15.4 Architecture: MAC layer



IEEE 802.15.4 MAC Overview

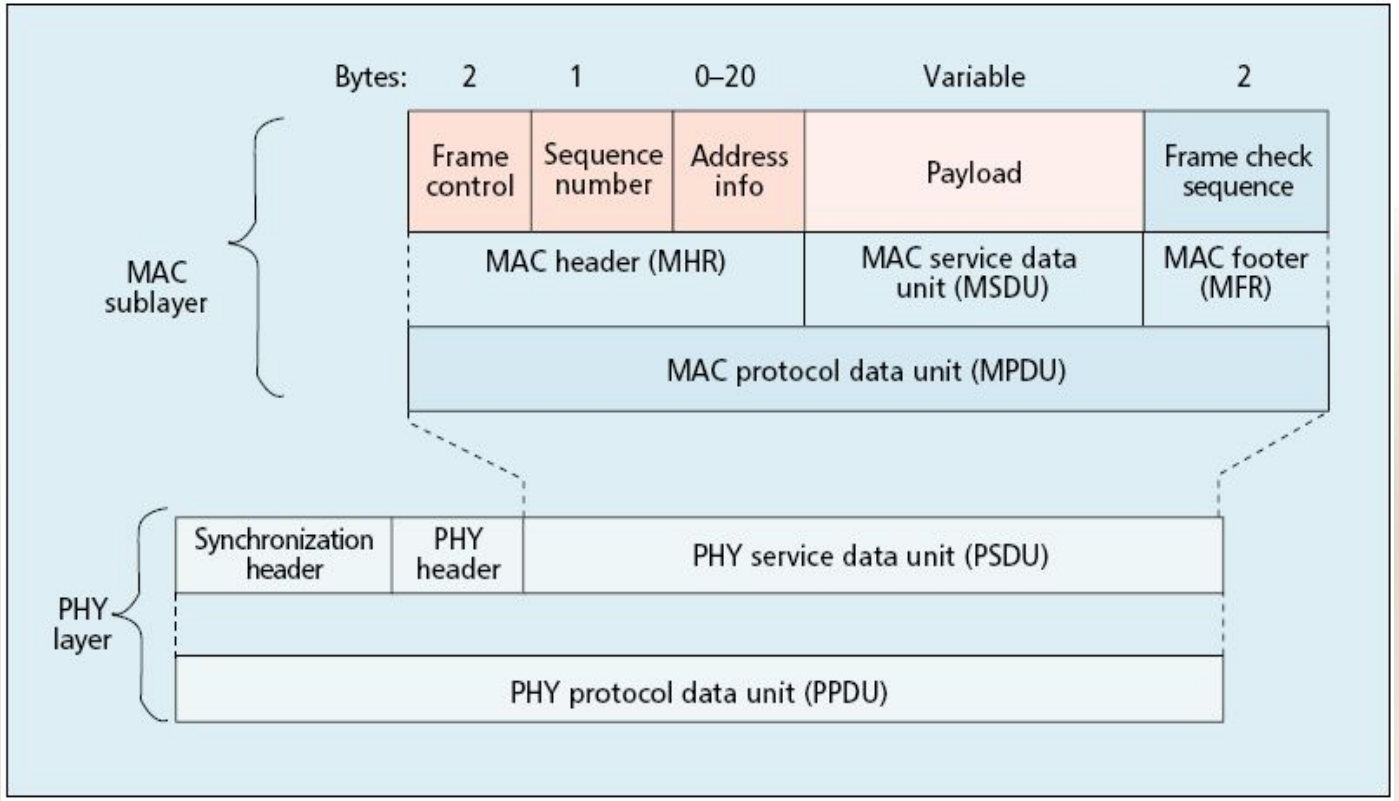
Design Drivers

- Extremely low cost
- Ease of implementation
- Reliable data transfer
- Short range operation
- Very low power consumption

Simple but flexible protocol !

IEEE 802.15.4 MAC Overview: General Frame Structure

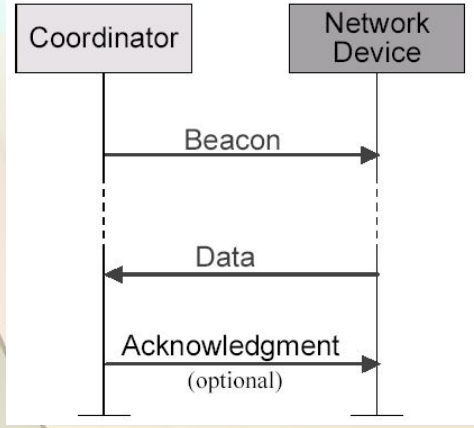
4 Types of MAC Frames:
- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame



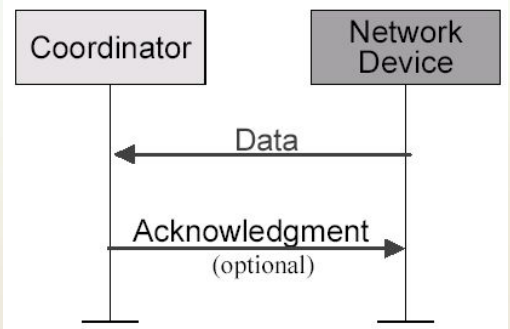
Data Transfer Model

Data transferred from device to coordinator

- **In a beacon-enable network, device finds the beacon to synchronize to the super-frame structure. Then using slotted CSMA/CA to transmit its data.**
- **In a non beacon-enable network, device simply transmits its data using un-slotted CSMA/CA**



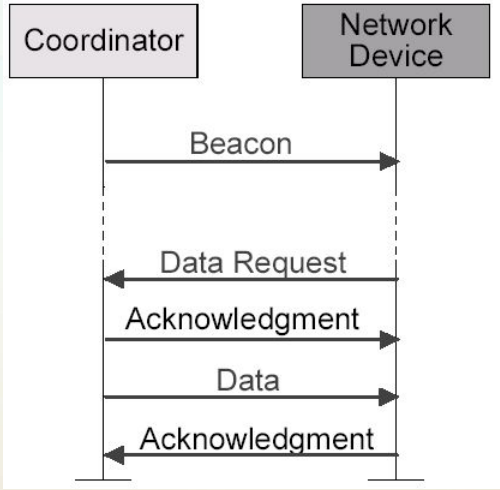
Communication to a coordinator
In a beacon-enabled network



Communication to a coordinator
In a non beacon-enabled network

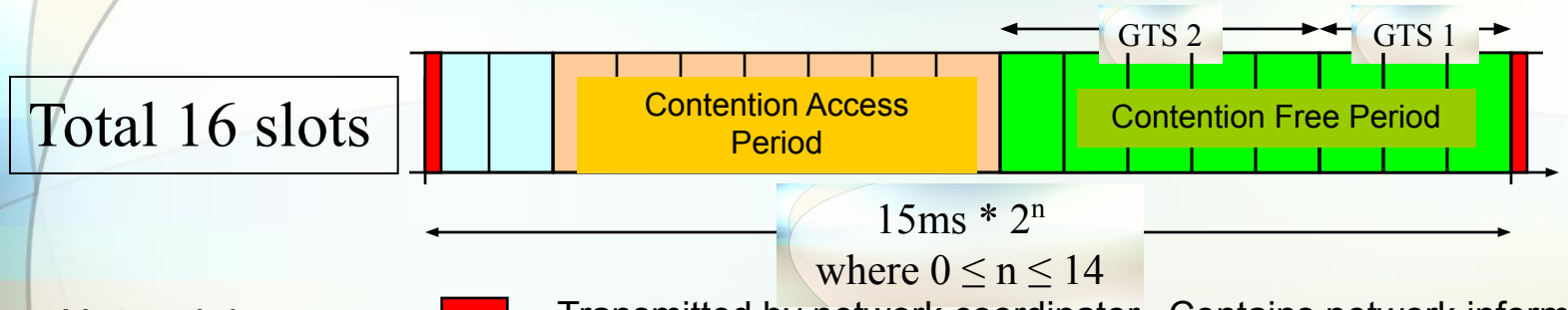
Data Transfer Model

- **Data transferred from coordinator to device**
  - **In a beacon-enable network, the coordinator indicates in the beacon that "data is pending."**
  - **Device periodically listens to the beacon and transmits a MAC command request using slotted CSMA/CA if necessary.**



Communication from a coordinator
In a beacon-enabled network

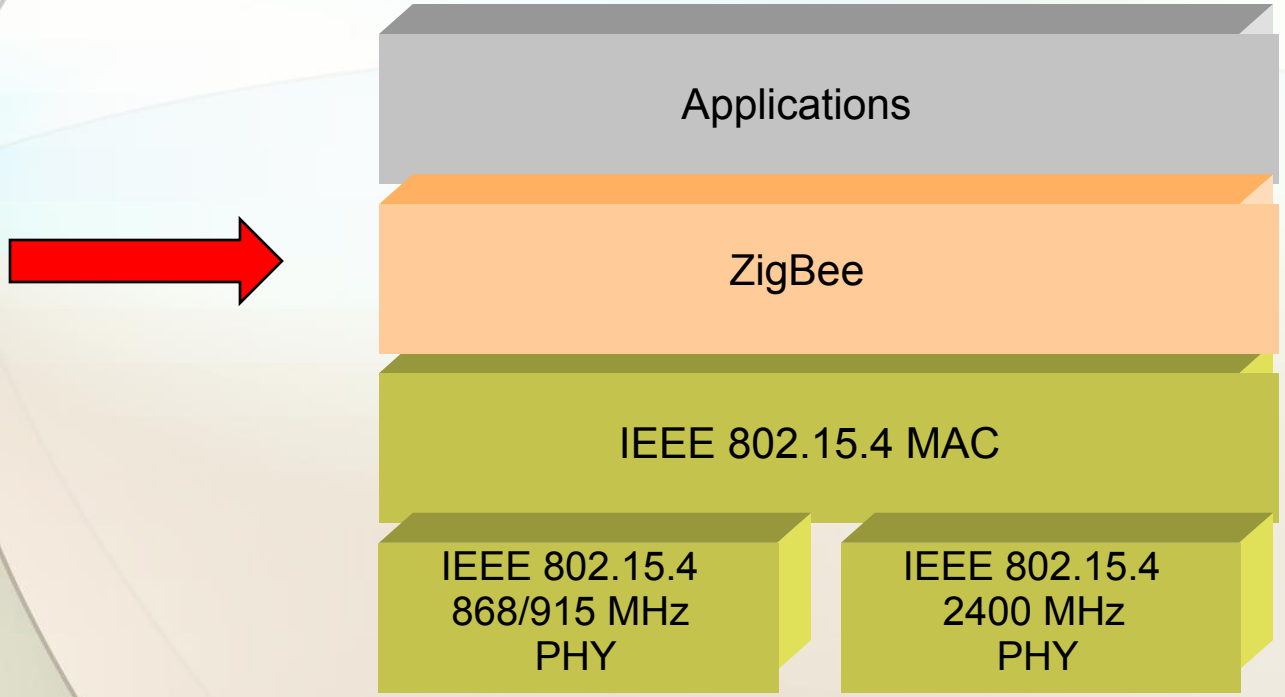
Superframe: CSMA-CA + TDMA



Network beacon		Transmitted by network coordinator. Contains network information, frame structure and notification of pending node messages.
Beacon extension period		Space reserved for beacon growth due to pending node messages
Contention period		Access by any node using CSMA-CA
Guaranteed Time Slot		Reserved for nodes requiring guaranteed bandwidth [n = 0].

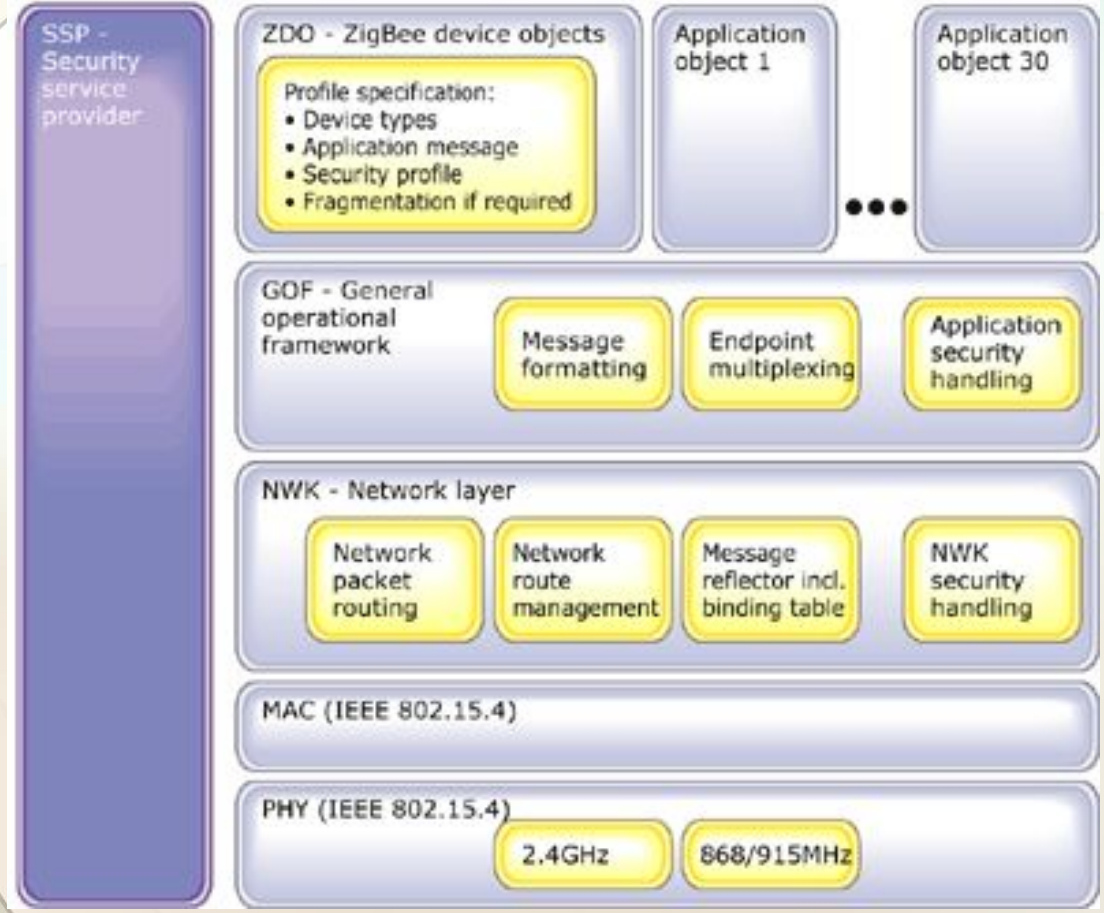
up to 7 GTSes

802.15.4 Architecture



- **Network Routing**
- **Address translation**
- **Packet Segmentation**
- **Profiles**

ZigBee Stack Architecture :



Comparison with peer technologies!

Feature(s)	IEEE 802.11b	Bluetooth	ZigBee
Power Profile	Hours	Days	Years
Complexity	Very Complex	Complex	Simple
Nodes/Master	32	7	64000
Latency	Enumeration upto 3 seconds	Enumeration upto 10 seconds	Enumeration 30ms
Range	100 m	10m	70m-300m
Extendability	Roaming possible	No	YES
Data Rate	11Mbps	1Mbps	250Kbps
Security	Authentication Service Set ID (SSID)	64 bit, 128 bit	128 bit AES and Application Layer user defined

ZigBee vs Bluetooth

Competition or Complementary?

Bluetooth is Best

For :

- Ad-hoc networks between capable devices
- Handsfree audio
- Screen graphics, pictures…
- File transfer

But ZigBee is Better

If :

- The Network is static
- Lots of devices
- Infrequently used
- Small Data Packets

Timing Considerations

ZigBee:

- New slave enumeration = 30ms typically
- Sleeping slave changing to active = 15ms typically
- Active slave channel access time = 15ms typically

Bluetooth:

- New slave enumeration = >3s
- Sleeping slave changing to active = 3s typically
- Active slave channel access time = 2ms typically

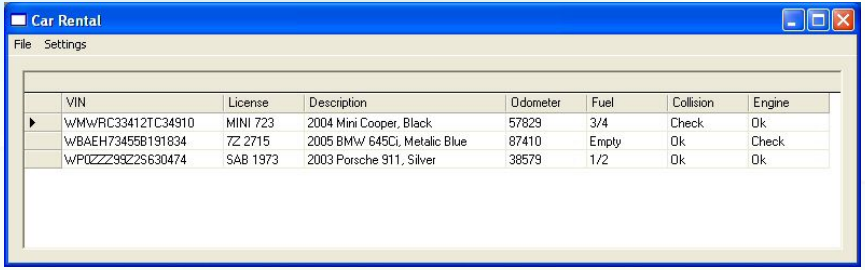
ZigBee protocol is optimized for timing critical applications

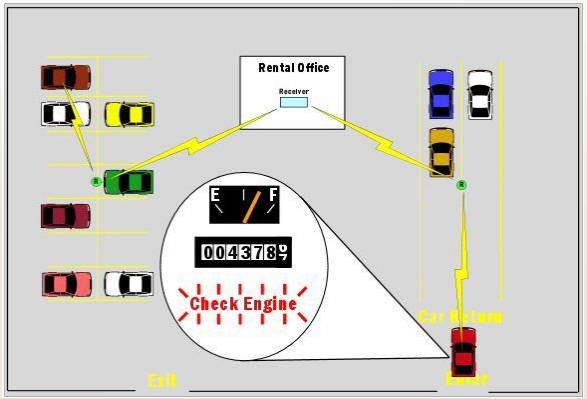
Some Interesting Applications of ZigBee

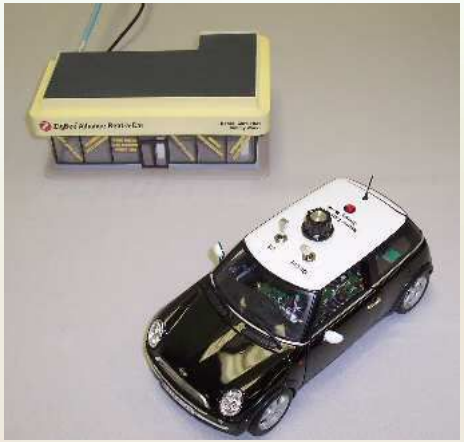
- Using the power of the mesh to automate a manual process
  - *Rental Car Return Automation**
- Long life battery powered sensing
  - *Wireless Termite Detection**

**From Software Technologies Group*

Automated Rental Car Return*

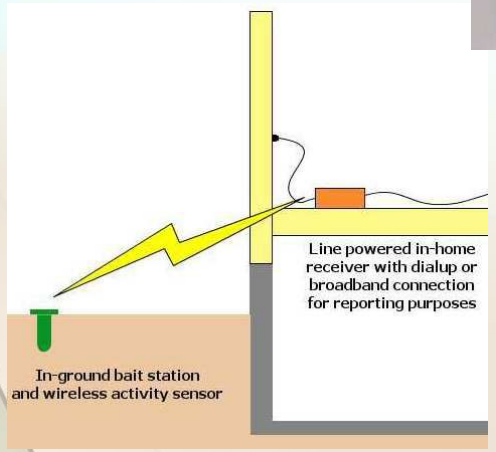


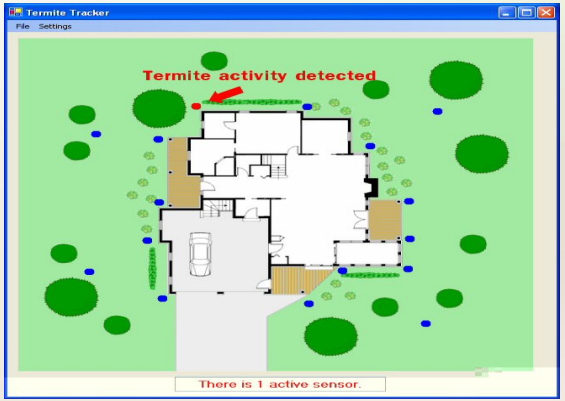




*From Software Technologies Group

Termite Detection*





*From Software Technologies Group

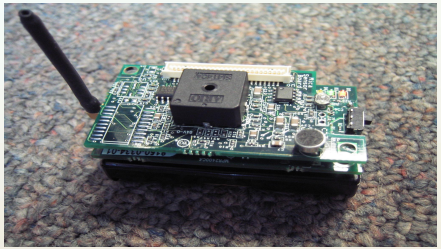
802.15.4/ZigBee Products

Control4 Home Automation System
http://www.control4.com/products/components/complete.htm

Eaton Home HeartBeat monitoring system
www.homeheartbeat.com

Chip Sets
- Ember, http://www.ember.com/index.html
- ChipCon, http://www.chipcon.com
- Freescale, http://www.freescale.com

Software, Development Kits
- AirBee, http://www.airbeewireless.com/products.php
- Software Technologies Group, http://www.stg.com/wireless/



Crossbow Technology - Wireless Sensor Networks
www.xbow.com

SUMMARY:

- IEEE 802.15.4 and ZigBee
  - Allows Designer to concentrate on end application
    - Silicon vendors and ZigBee Alliance take care of transceiver, RF channel and protocol, ZigBee “look and feel”
  - Reliable and robust communications
    - PHY and MAC outperform all known non-standards-based products currently available
  - Flexible network architectures
  - Very long primary battery life (months to years to decades)
  - Low system complexity. (Due to its architecture)

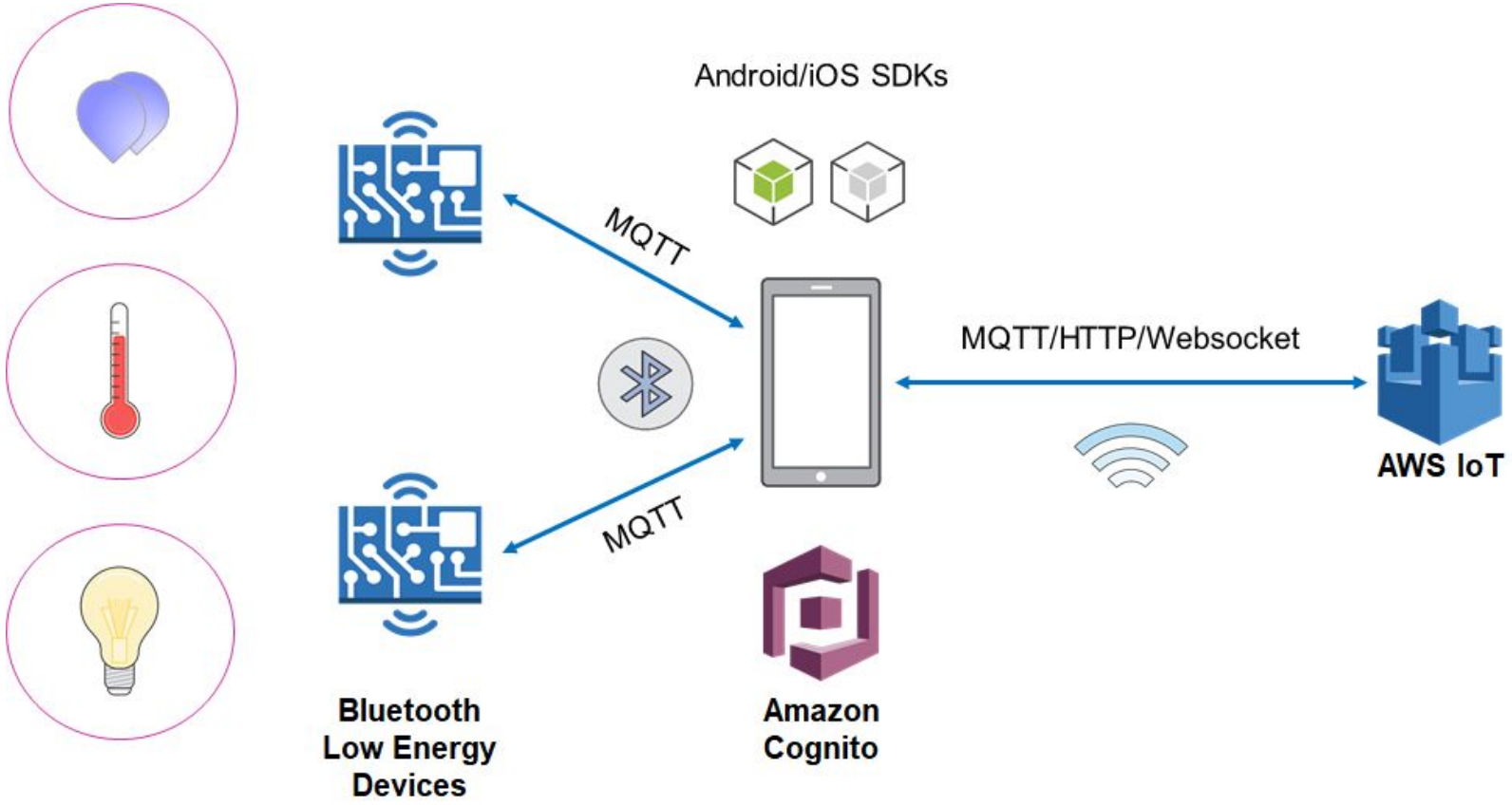
Bluetooth

- Bluetooth and BLE are radio protocols for **Personal Area Networks (PAN)**
- Mostly these are on a person's body or in close proximity to them

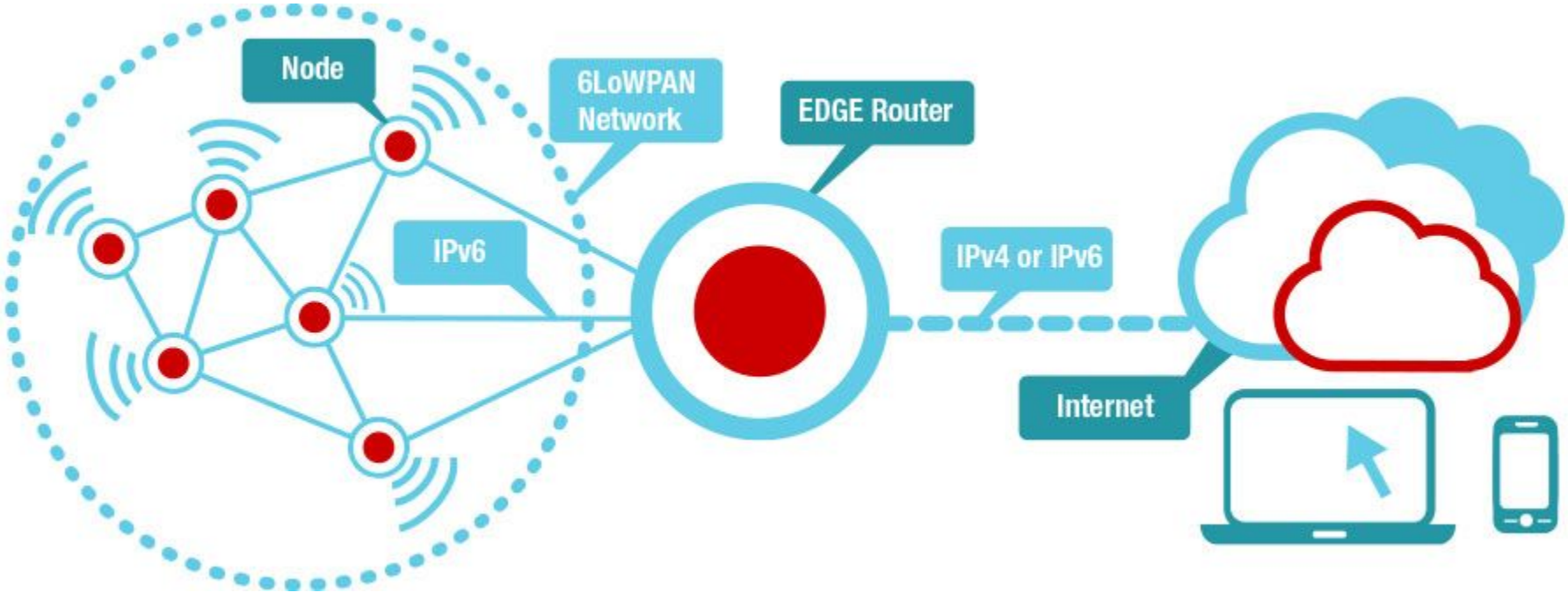
- Typical range: very short, 20m (or less)
- Max output power: very limited, 0.003 W
- Bandwidth: limited, 0.7–2.1 Mbit/s
- Security: pairing task to exchange encryption keys
- Cost: cheap equipment, no transmission costs

- Good for: devices that stay **in close proximity of each other**, like between a smartphone and a headset, heart rate monitor, bicycle speedometer

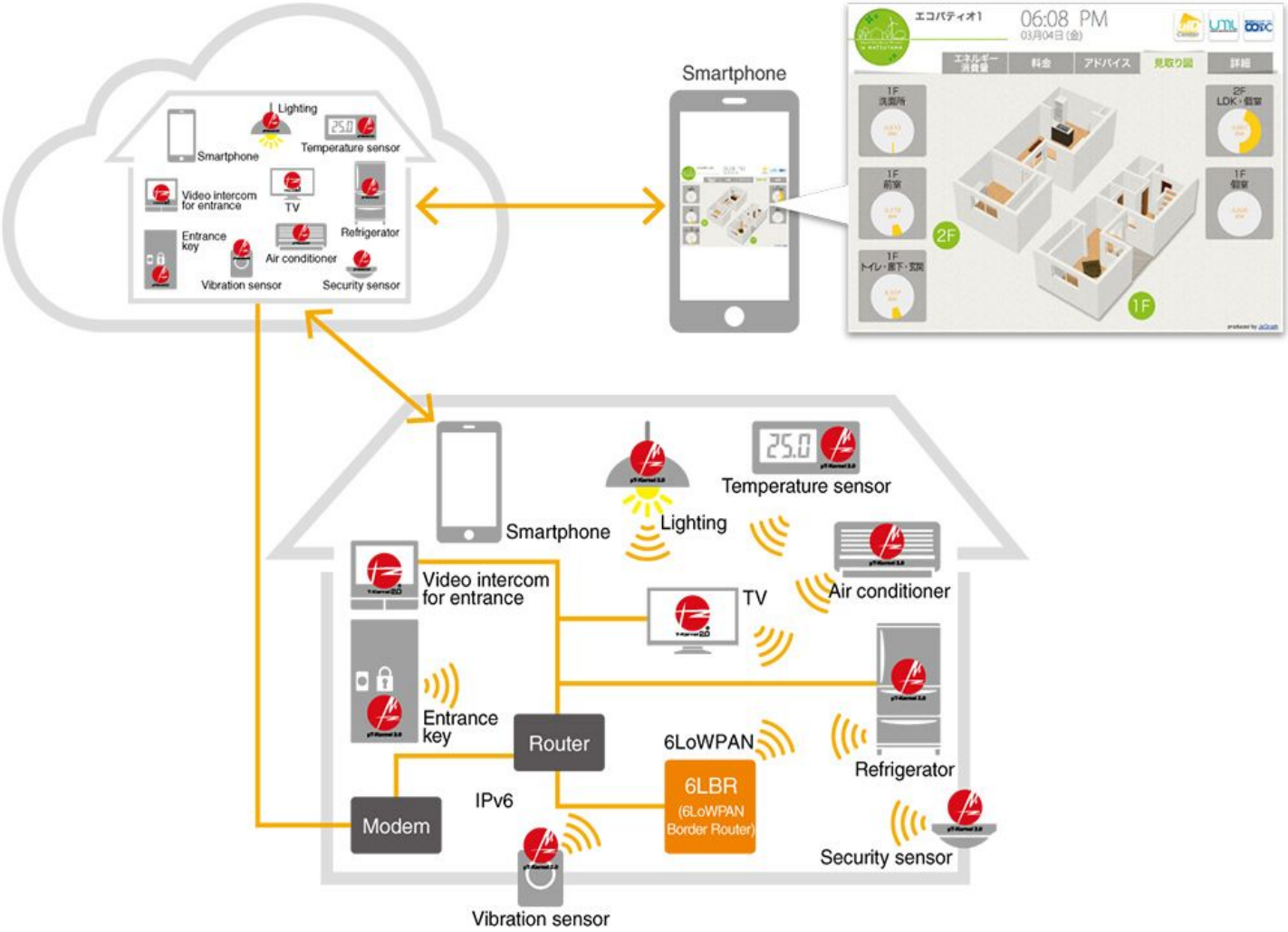
Bluetooth


Android/iOS SDKs
MQTT
MQTT
MQTT/HTTP/Websocket
AWS IoT
Bluetooth
Low Energy
Devices
Amazon
Cognito

6LoWPAN - stands for IPv6 over Low-power Wireless Personal Area Networks.

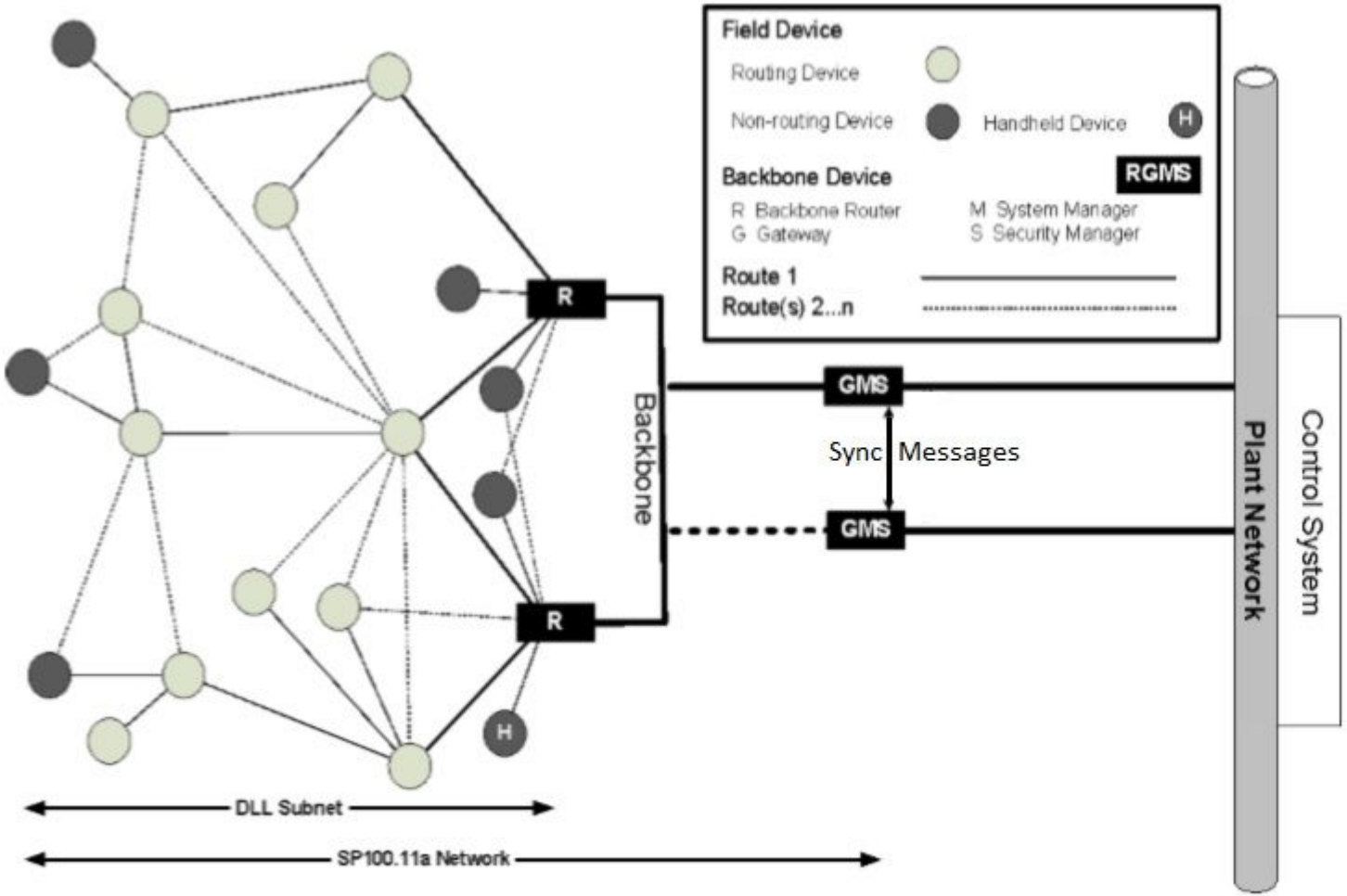


6LoWPAN - stands for IPv6 over Low-power Wireless Personal Area Networks.

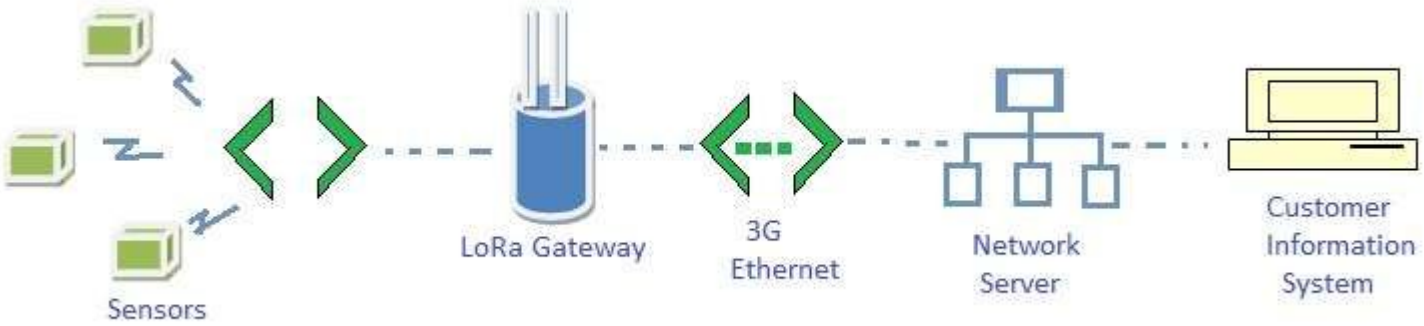


ISA100. 11a - is a IoT protocol used by many IoT devices and is most likely to be found in industrial settings, like petroleum refineries and manufacturing plants.

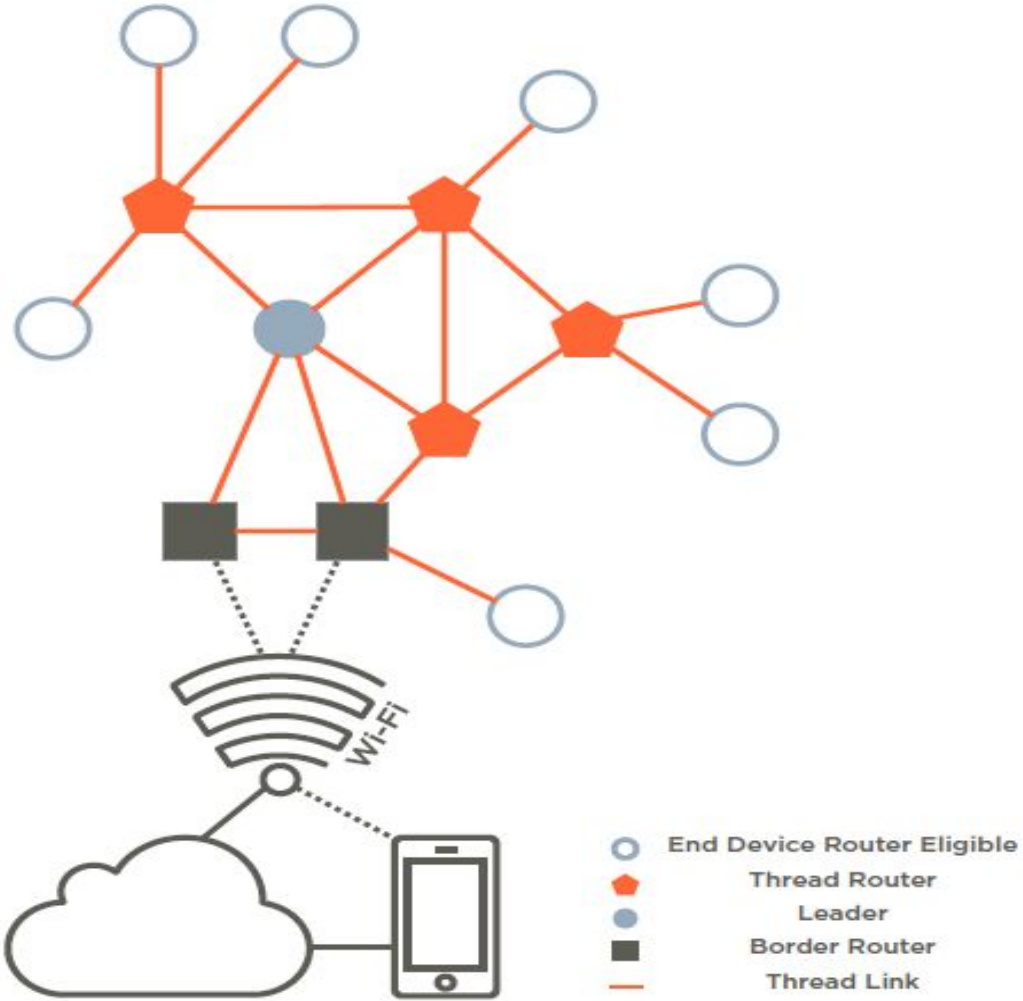
https://www.rfwireless-world.com/Tutorials/ISA100-wireless-tutorial.html



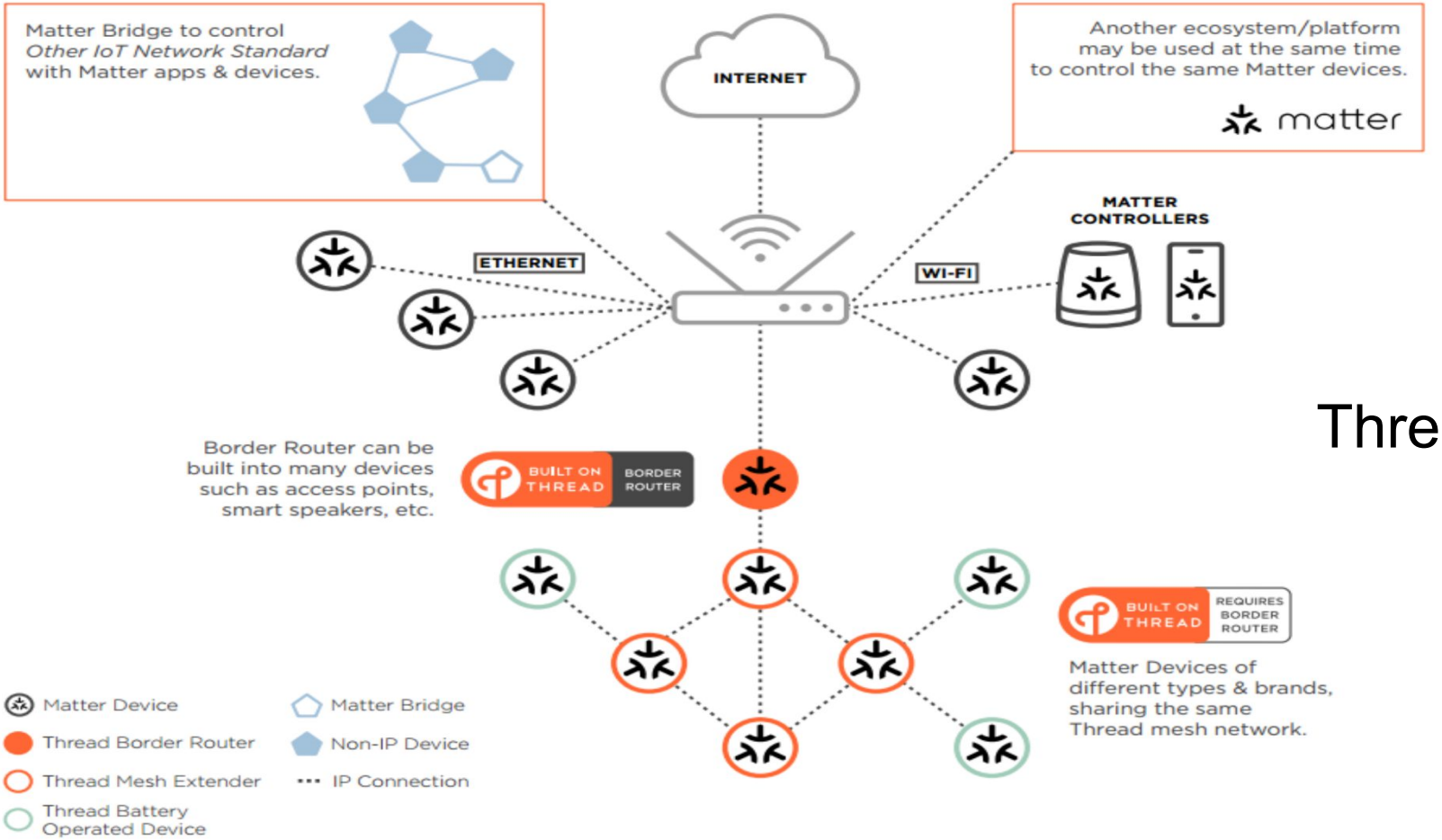
LoRa stands for Long Range Radio.
It is the wireless technology mainly targeted for M2M and IoT networks.



Thread


Wi-Fi
End Device Router Eligible
Thread Router
Leader
Border Router
Thread Link

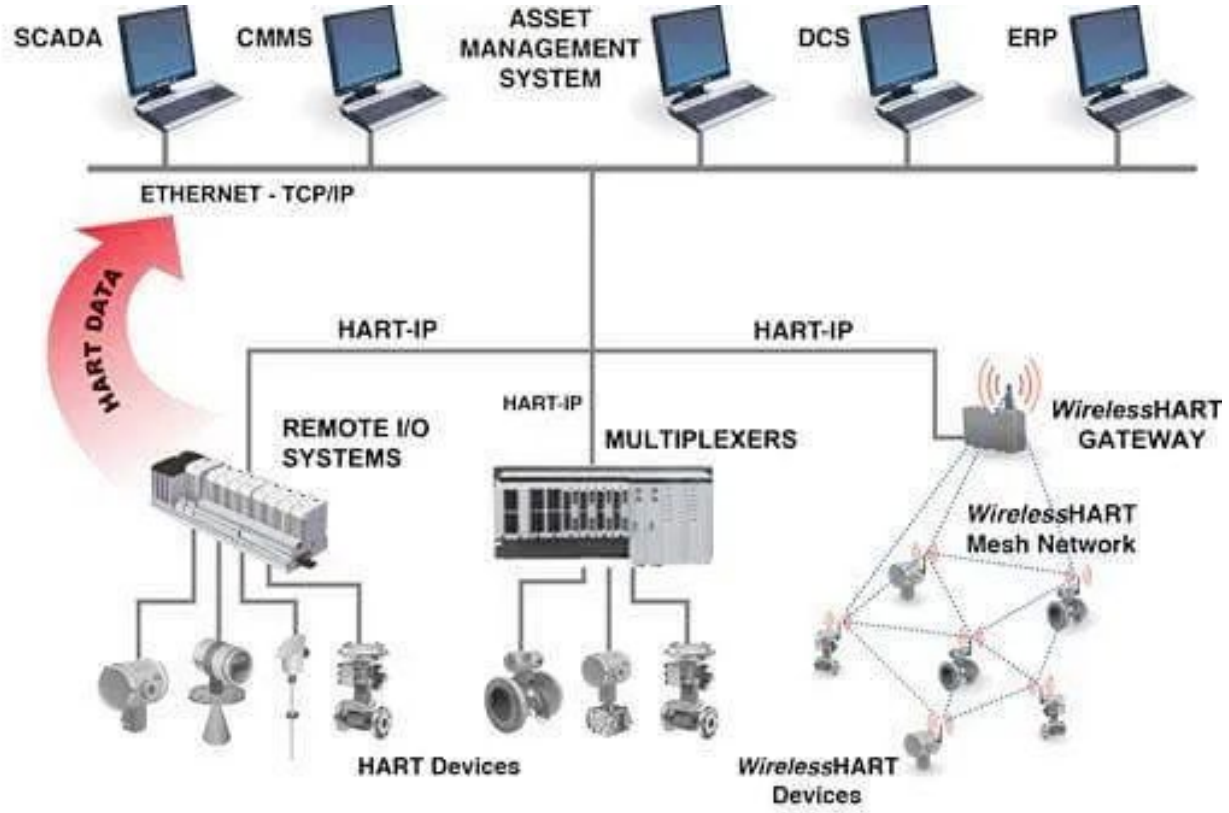
Thread


Matter Bridge to control
Other IoT Network Standard
with Matter apps & devices.
INTERNET
Another ecosystem/platform
may be used at the same time
to control the same Matter devices.
matter
MATTER
CONTROLLERS
ETHERNET
WI-FI
Border Router can be
built into many devices
such as access points,
smart speakers, etc.
BUILT ON THREAD
BORDER ROUTER
BUILT ON THREAD
REQUIRES BORDER ROUTER
Matter Devices of
different types & brands,
sharing the same
Thread mesh network.
Matter Device
Thread Border Router
Thread Mesh Extender
Thread Battery
Operated Device
Matter Bridge
Non-IP Device
IP Connection

Z-Wave


Internet
WiFi
z-wave controller
WiFi
GATES
ALARM
BLINDS
IRRIGATION
SCENES
INTERCOM
CAMERA
EQUIPMENT
MULTIMEDIA
SENSORS
LIGHTING
CLIMATE

Wireless HART - Wireless Highway Addressable Remote Transducer (WirelessHART, WH) Protocol



*The Time Synchronized Mesh Protocol (TSMP)

- TSMP enables
  - reliable,
  - low power,
  - secure communication
  - in a managed wireless mesh network.
- Is a medium access and networking protocol designed for the recently ratified Wireless HART standard in industrial automation.
- Benefits from synchronization of nodes in a multi-hop network to within a few hundred microseconds, allowing scheduling of
  - collision-free pair-wise and
  - broadcast communication to meet the traffic needs of all nodes
  - while cycling through all available channels.

*TSMP

- Provides redundancy and fail-over in
  - time,
  - frequency and
  - space to ensure very high reliability even in the most challenging radio environments.

- Also provides the intelligence
  - required for self-organizing,
  - self-healing mesh routing.

- The result is
  - a network that installs easily with no specialized wireless expertise,
  - automatically adapts to unforeseen challenges, and
  - can be extended as needed without sophisticated planning.

*Five key components of TSMP

- That contribute to end-to-end network reliability, simple installation and power efficiency.

- *Time synchronized communication*
- *Frequency hopping*
- *Automatic node joining and network formation*
- *Fully-redundant mesh routing*
- *Secure message transfer*

*Features of TSMP

TSMP has been targeted to:

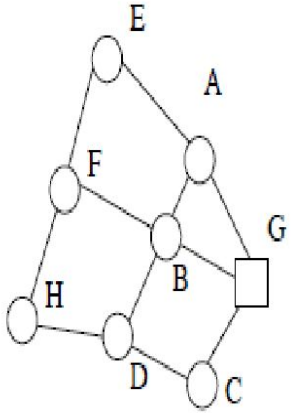
1. Reliability at low-power: >99.9% packet delivery with years of battery life for all nodes
2. Scalability: hundreds of meshed nodes per manager, thousands in the same RF environment
3. Flexibility: support different time-varying traffic patterns from different nodes
4. Security: guarantee confidentiality, integrity, and authenticity of all packets
5. Environment: nodes operate between -40°C and 85°C and in radically changing RF noise levels

*TSMP

- A traditional approach to facilitate synchronization is - beaconing,
  - where longer frame lengths decrease the refresh rate at which synchronization is performed and
  - hence power consumption and
  - shorter frame lengths conversely invoke the opposite.
- TSMP does refrain from doing so because it requires long listening windows which consume power.
- Instead, TSMP nodes maintain a precise sense of time and exchange only offset information with neighbors to ensure alignment.
- These offset values are exchanged during active periods together with the usual data and acknowledgement packets hence invoking negligible overhead.
- TSMP nodes are active in three states:
  - 1) sending a packet to a neighbor;
  - 2) listening for a neighbor to talk; and
  - 3) interfacing with an embedded hardware component.
- The duration of active periods, i.e. the duty cycling, is very flexible in TDMA; typical applications require duty cycles of less than 1%.

*TSMP

- When applied, the sink typically retrieves
  - the list of nodes,
  - their neighbors and
  - their requirements in terms of traffic generation.
- From this information, it constructs a scheduling table in both time and frequency.



	t1	t2	t3	t4	t5	t6	t7	t8	t9	t10
ch.15									E->A	
ch.14	A->G			G->C						
ch.13						D->H				
ch.12		F->E					B->A			
ch.11					C->D					F->B
ch.10			G->B							
ch.9										
ch.8	E->F					G->A		B->G		
ch.7				D->B						A->E
ch.6					H->F					
ch.5		D->C					C->G			
ch.4									B->D	
ch.3										
ch.2	H->D					B->F				
ch.1			F->H							
ch.0					A->B					

Possible schedule for given connectivity graph.

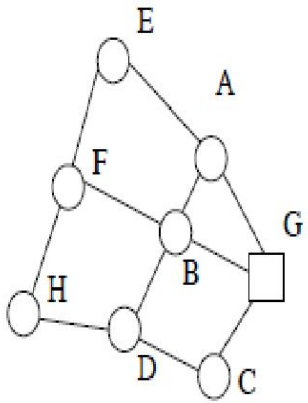
*TSMP

- When implementing TSMP on IEEE 802.15.4 compatible hardware, 16 frequency channels are available.

- Exemplified by means of the scheduling table of Fig. 5, the TSMP link establishment and maintenance rules are simple:
  - never put two transmissions in the same time/frequency slot;
  - at a given time, a given node should not receive from two neighbors nor have to send to two neighbors.

*

- Assuming that slots are 10ms long and node *H* sends a packet following route *H* → *F* → *B* → *G*, then *H* sends to *F* in slot [t5, ch.6], thereafter *F* → *B* in [t10, ch.11], then *B* → *G* at [t8, ch.8].
-
- Latency is hence in this particular case 13 slots (130ms) and in general always guaranteed to be bound by a finite value which depends of the particular design of the time-frequency pattern.



	t1	t2	t3	t4	t5	t6	t7	t8	t9	t10
ch.15									E->A	
ch.14	A->G			G->C						
ch.13						D->H				
ch.12		F->E					B->A			
ch.11					C->D					F->B
ch.10			G->B							
ch.9										
ch.8	E->F					G->A		B->G		
ch.7				D->B						A->E
ch.6					H->F					
ch.5		D->C					C->G			
ch.4									B->D	
ch.3										
ch.2	H->D					B->F				
ch.1			F->H							
ch.0					A->B					

Possible schedule for given connectivity graph.