ZigBee Protocol

Prof SRN Reddy, IGDTUW

Abbreviations

PABC: Personal Area Network Coordinator

MHR: MAC Header

MFR: MAC Footer

PLCP: Physical Layer Convergence Procedure

MPDU:MAC Protocol Data Unit

PSDU: PLCP Service Data Unit

FFD: Full Function Device

RFD: Reduced Function Device

Outline

- ZigBee Introduction
- Architecture
- Topologies
- Protocols
- Versions
- Applications

ZigBee

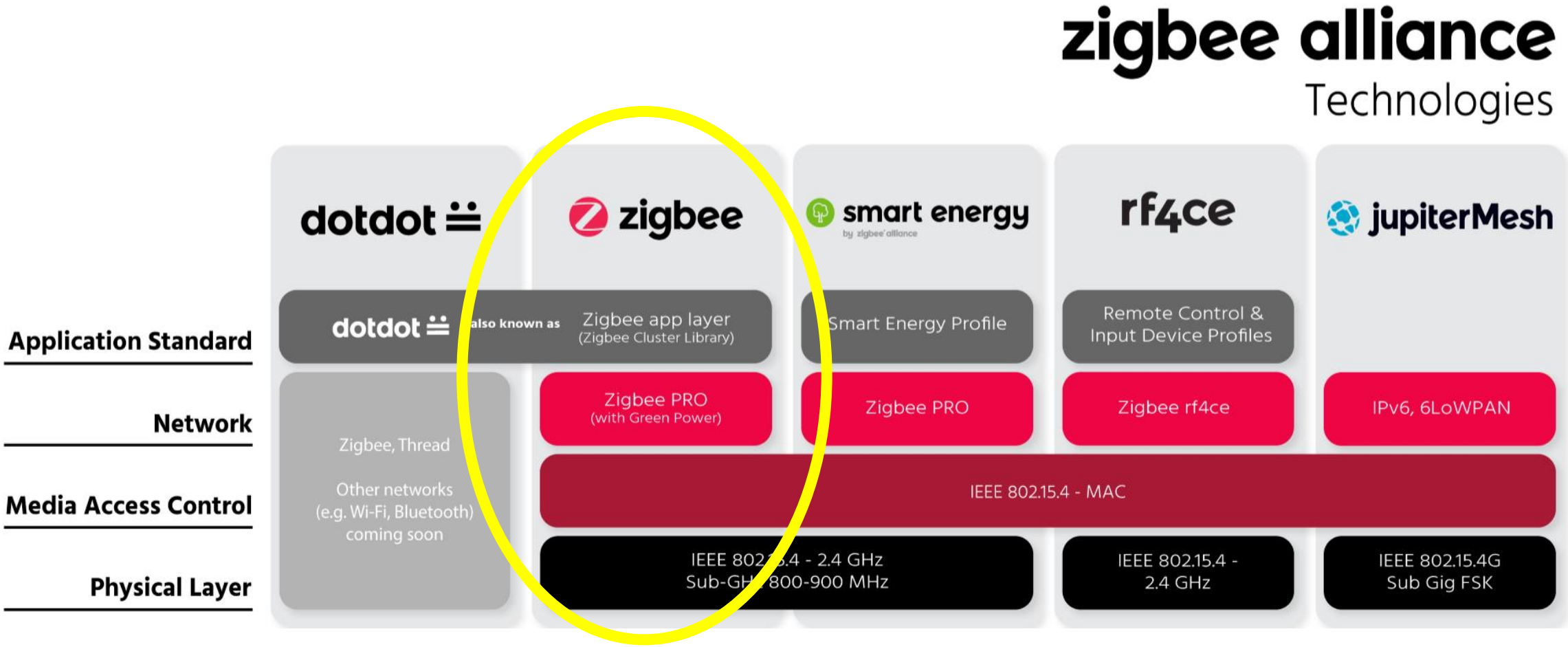
- Created by the ZigBee Alliance: NxP, NEC, Samsung, Atmel, TI,LG etc.
- Ad-hoc networking technology for LRWPAN.
- Ultra-low power, low-data rate, multi-year battery life
- Power management to ensure low power consumption.
- Based On IEEE 802.15.4 standard that defines the PHY and Mac Layers for ZigBee.
- Low in cost ,complexity & power consumption as compared to competing technologies.
- Data rates touch 250Kbps for 2.45Ghz ,40 Kbps 915Mhz and 20Kbps for 868Mhz band
- ZigBee is targeted at radio-frequency (RF) applications which require a low data rate, long battery life, and secure networking.

Solution	Description
Network Protocol	Zigbee PRO 2015 (or newer)
Network Topology	Self-Forming, Self-Healing MESH
Network Device Types	Coordinator , Router, End Device, Zigbee Green Power Device
Network Size (theoretical)	Up to 65,000
Radio Technology	IEEE 802.15.4-2011
Frequency Band / Channels	2.4 GHz (ISM band), 16-channels (2 MHz wide) [Total: 27]
Data Rate	250 Kbits/sec
Security Models	Centralized (with Install Codes support) Distributed
Encryption Support	AES-128 at Network Layer, AES-128 available at App. Layer
Comm. Range(Average)	Up to 300+ meters (line of sight), Up to 75-100 meter indoor
Low Power Support	Sleeping End Devices, Zigbee Green Power Devices
Legacy Profile Support	Zigbee 3 devices can join legacy Zigbee profile networks.

Major initiative: Zigbee

20+ Compliant Platforms (silicon); Half a billion chipsets sold worldwide

Over 2,500 Certified Products on the market.



Zigbee Growth and Applications

Zigbee Certifications growing exponentially

- Includes lighting, sensors, reference designs, with more in the pipeline.
- 75+ device types and growing

Zigbee products are backwards-compatible with existing Zigbee products built to previous specifications

- They can connect *and* communicate using the same IoT language with each other
- Millions of Zigbee products already deployed in smart homes and buildings.

IEEE 802.15.4

- IEEE 802.15.4 is a technical standard which defines the operation of low-rate wireless personal area networks (LR-WPAN).
- It specifies the physical layer and media access control for LR-WPANs, and is maintained by the IEEE 802.15
- Total channels: 27

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

IEEE 802.15.4 Data Frame Format

- Provides up to 102 Byte data payload capacity
- Data sequence numbering to ensure that packets are tracked
- Frame Check Sequence (FCS) validates error-free data
- min. 16 Bytes = 128 bits = 0.512 ms @ 250 kbps
- max. 133 Bytes = 1064 bits = 4.256 ms @ 250 kbps

MHR: MAC Header

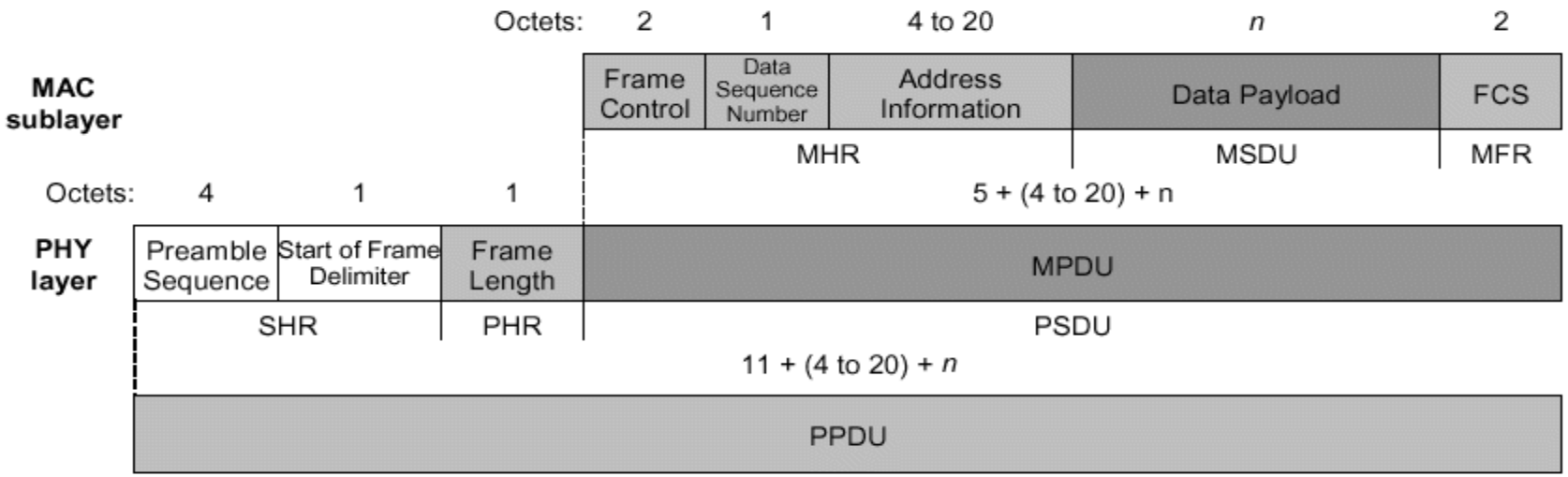
MFR: MAC Footer

PLCP: Physical Layer Convergence Procedure

MPDU:MAC Protocol Data Unit

PSDU: PLCP Service Data Unit

PPDU:PLCP Service Data Unit



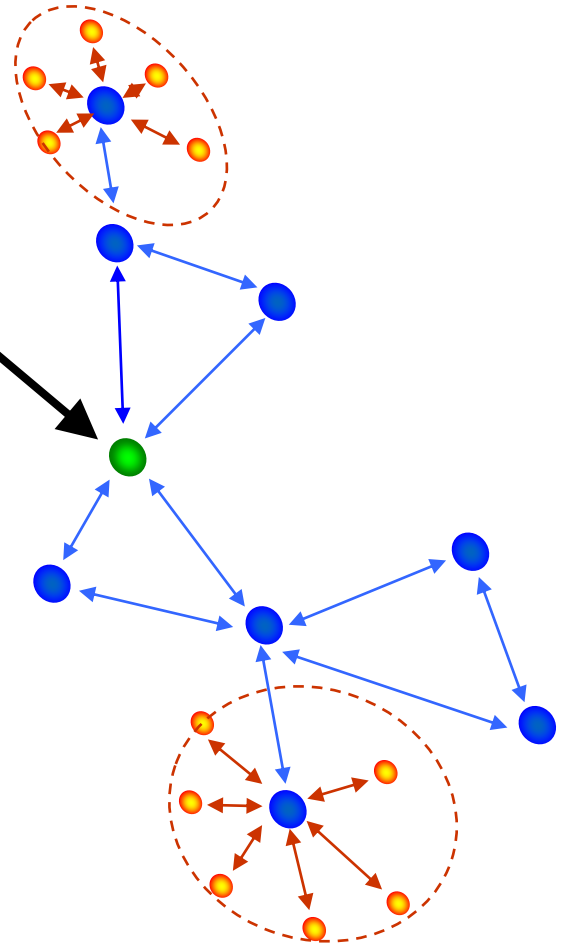
IEEE 802.15.4 Device Types

- Full Function Device (FFD)
  - Talks to several devices
  - Normally Always ON
  - Can Route Messages
- Reduced Function Device (RFD)
  - Limited functionality to control cost
  - Talks to parent
  - Requires less memory
  - Can be a sleeping device
  - Used as network edge devices

Zigbee – PAN Coordinator

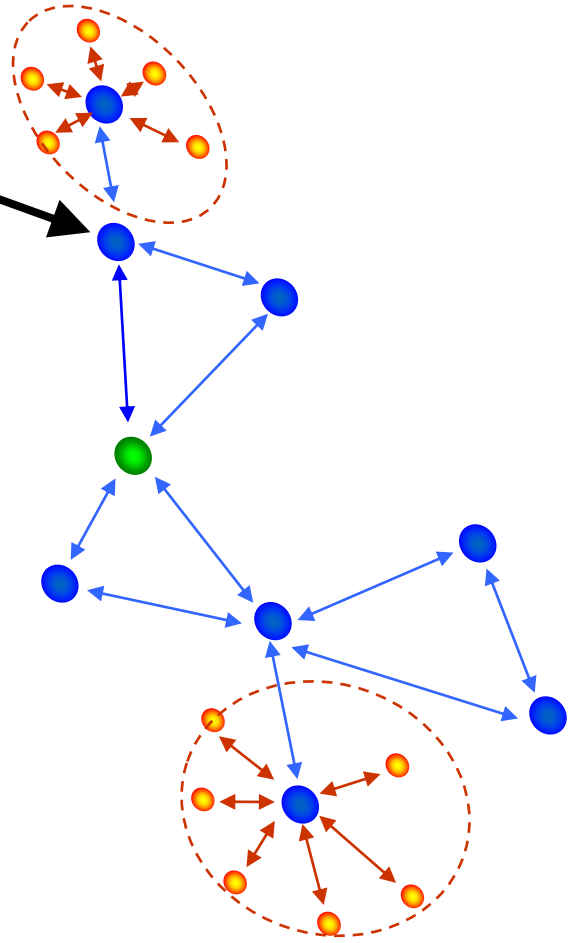
- Only One for a N/W and mandatory
- “Owns” the network
  - Starts the network
  - Opens the network for joining
  - Allocates address
  - Saves messages until they can be delivered
  - Can function as Trust Center
- A “full-function device” – FFD
- Mains-powered
- Can have other functionality
  - Sensor
  - Monitor

  Only One for a N/W



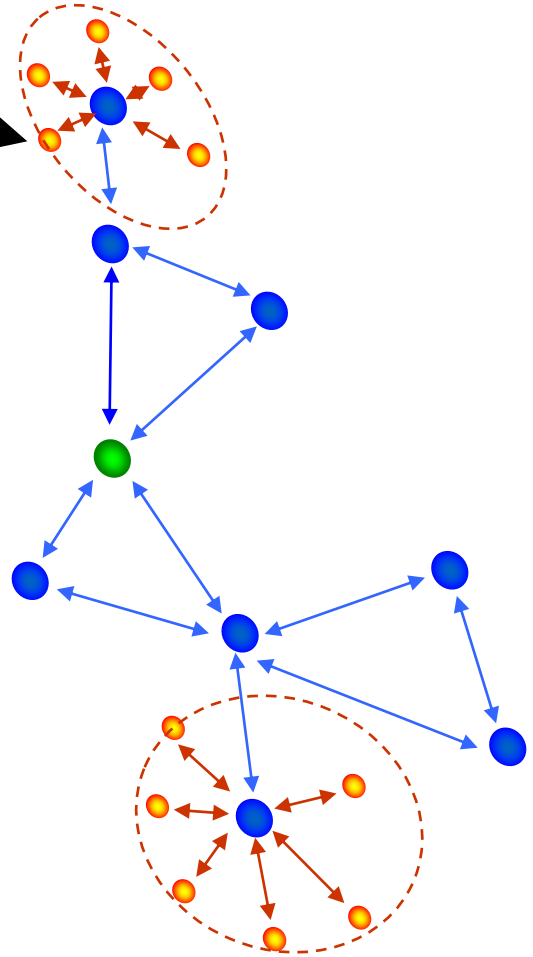
Zigbee - Router

- Optional and many for a N/W
- 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
- Can have other functionality
  - Sensor
  - Monitor

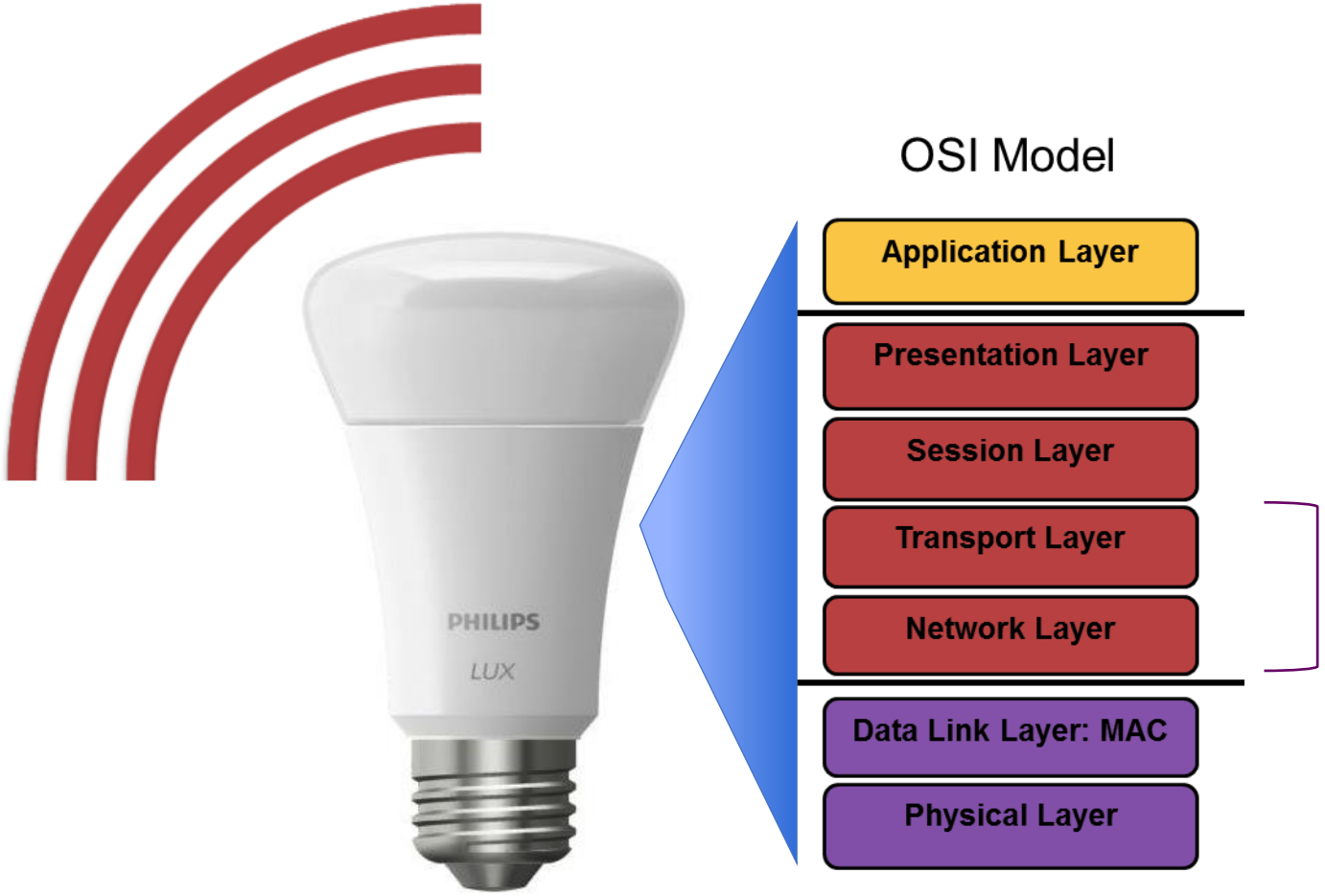


Zigbee – End Device

- Specific Device function
  - Sensor
  - Monitor
- Communicates with a single device (parent)
- Does not own or start network
  - Scans to find a network to join
- Can be an FFD or RFD
- Does NOT route packets
- Often battery-powered



Standardized at all Layers



Zigbee PRO

Zigbee Wireless Networking Basics

- Network Scan
  - Device scans the available 16 2.4 GHz 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
- Service Discovery
  - Device scans for supported services on devices within the network
- Binding
  - Devices communicate via command/control messaging

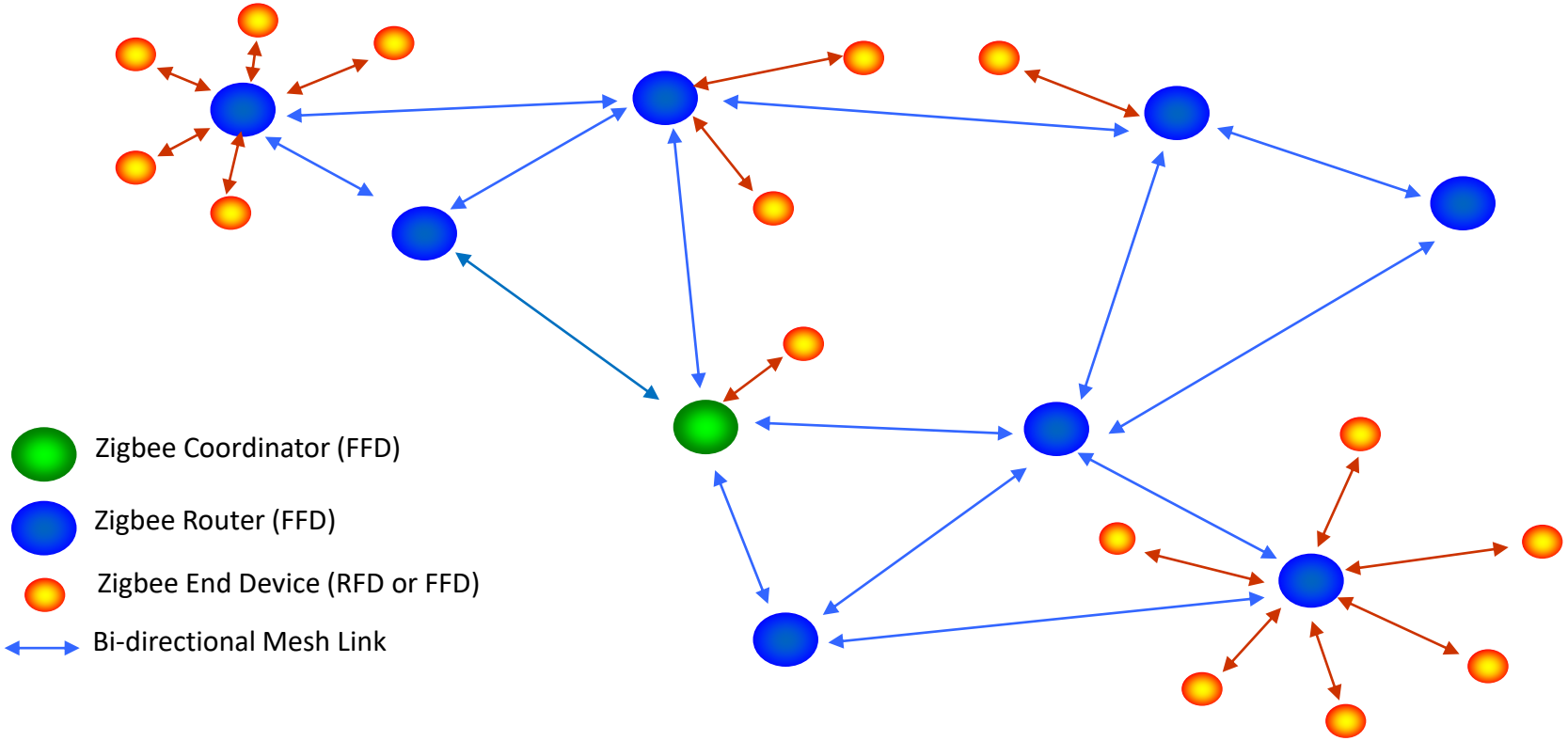
Zigbee Stack Architecture Basics

- Addressing
  - Every device has a unique 64 bit MAC address
  - Upon association, every device receives a unique 16 bit network address
  - Only the 16 bit network address is used to route packets within the network
  - Devices retain their 16 bit address if they disconnect from the network.
  - NWK/ Network broadcast implemented above the MAC

Zigbee Stack Architecture Basics

- Devices
  - Pre-programmed for their network function
    - Coordinator
      - Scans to find an unused channel to start a network
    - Router (mesh device within a network)
      - Scans to find an active network to join, then permits other devices to join
    - End Device
      - Always tries to join an existing network
  - Discover other devices in the network providing complementary services
    - Service Discovery can be initiated from any device within the network
  - Can be bound to other devices offering complementary services
    - Binding provides a command and control feature for specially identified sets of devices

Zigbee PRO Network Communication

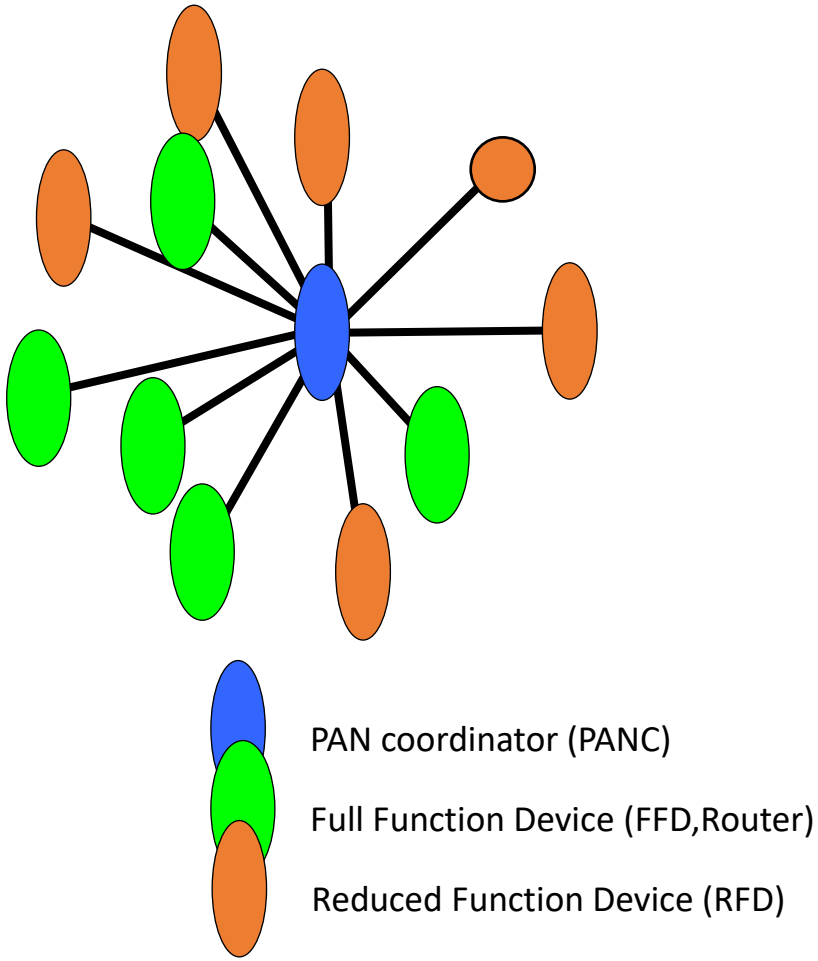


- Mesh, self-organizing, self-healing topology scalable to thousands of nodes
- Point to Point communication gives range > 100 m,
- Full mesh deployment can have several kilometer range

Network Topology Models

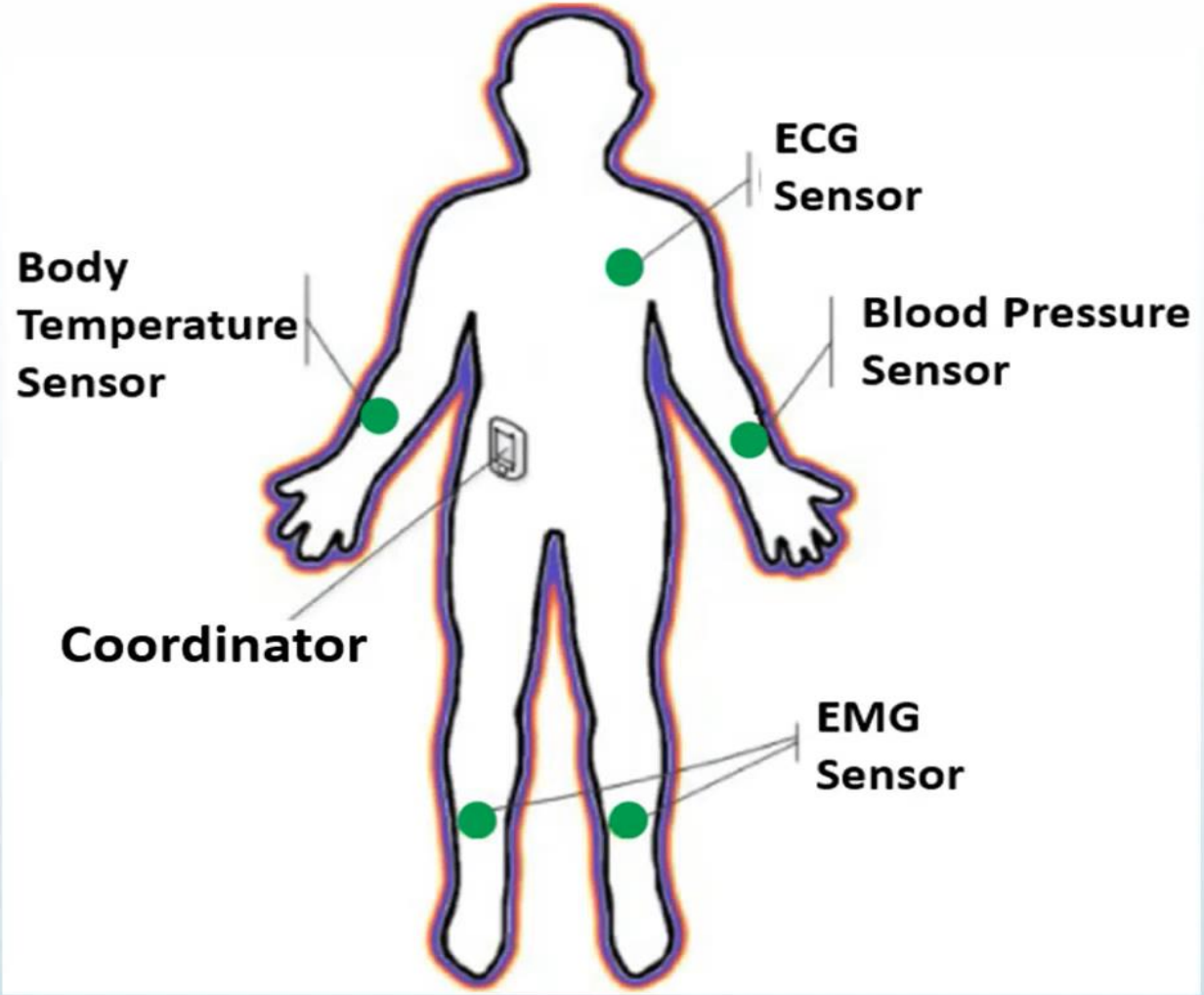
1. Star Network

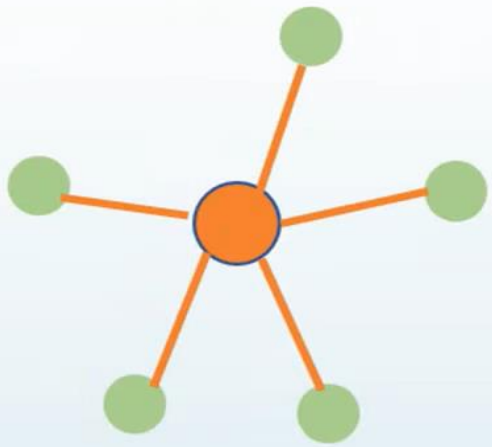
- Lowest complexity
- Limited Range
- Coordinator can become bottleneck



ZIGBEE Network Architecture

STAR Topology



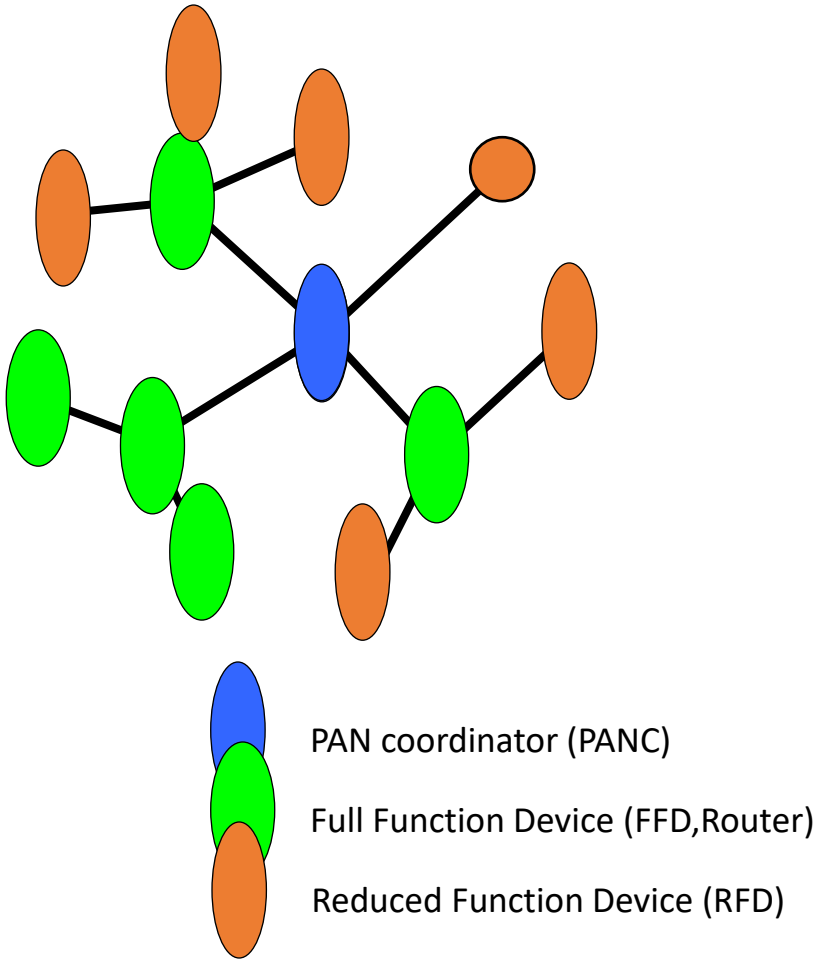


Health monitoring system

Network Topology Models

2. Tree Network

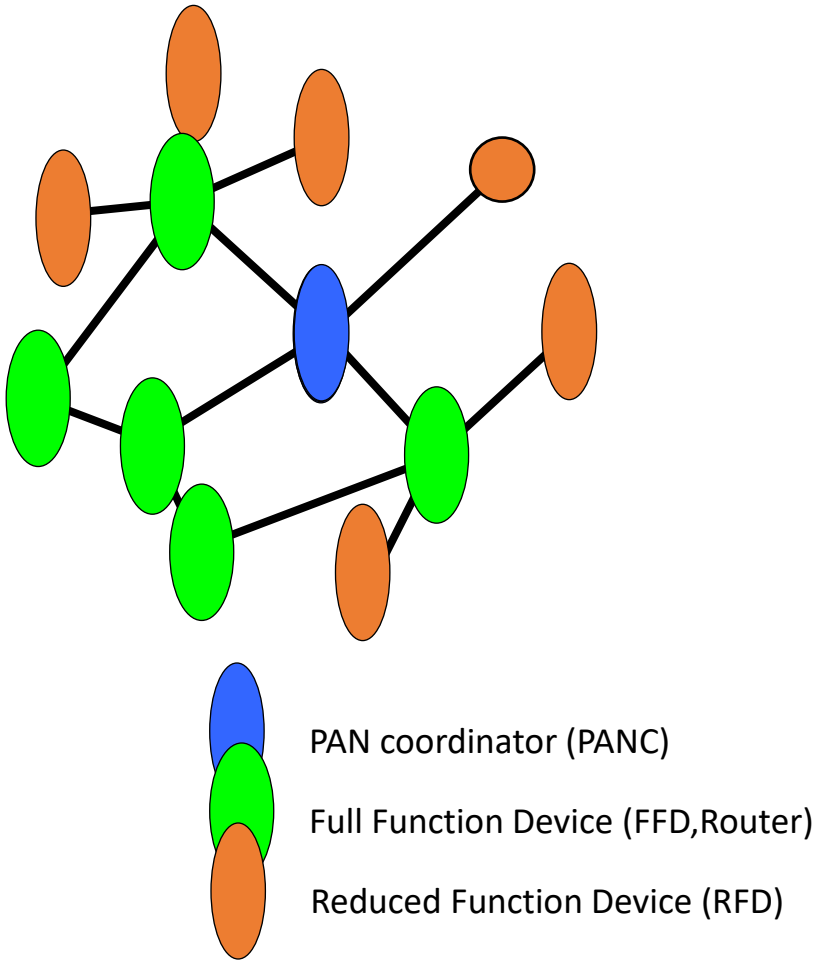
- Extends range of network
- More predictive
- Bottlenecks still exist



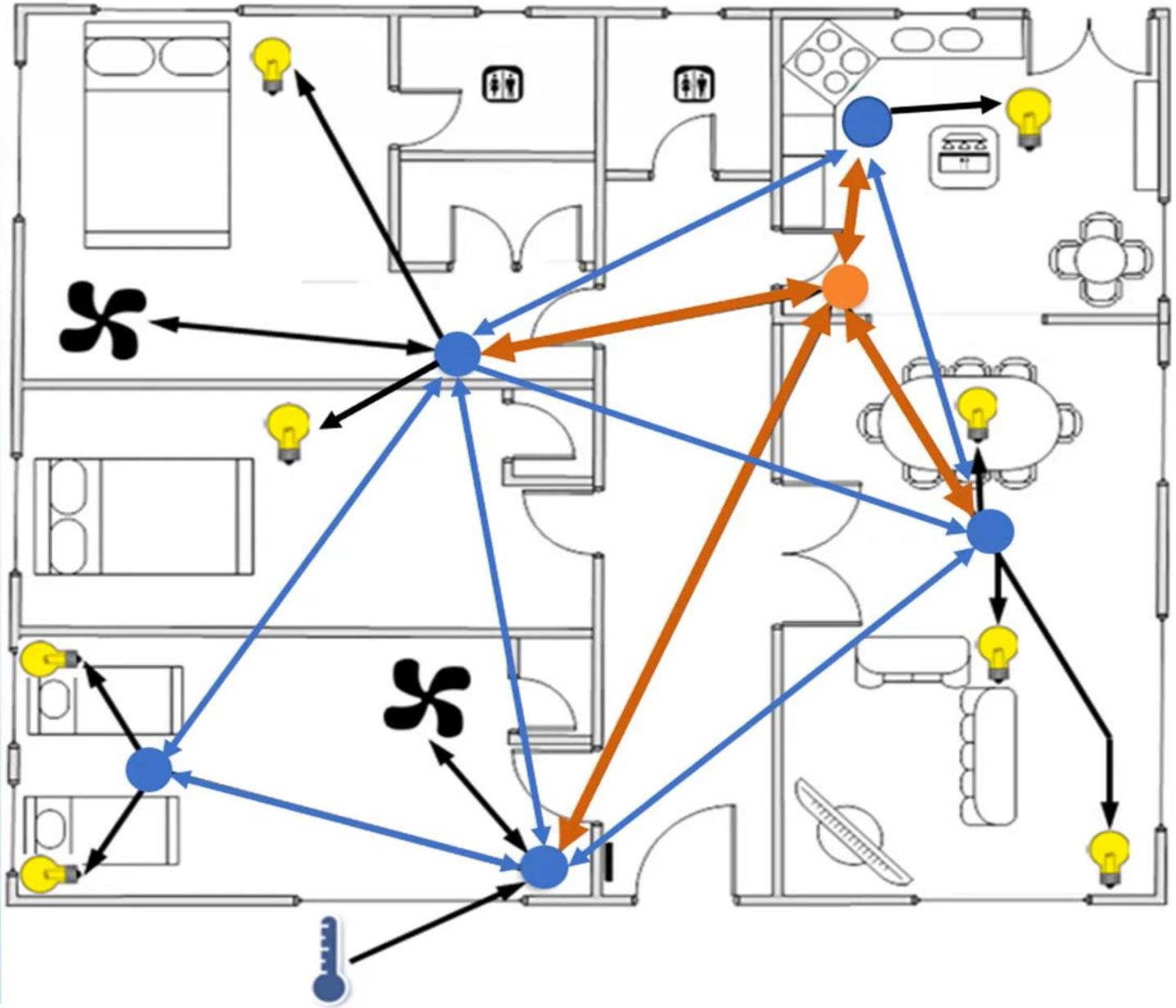
Network Topology Models

3. Mesh Network

- Most complex
- Highest reliability
- Reduces bottlenecks



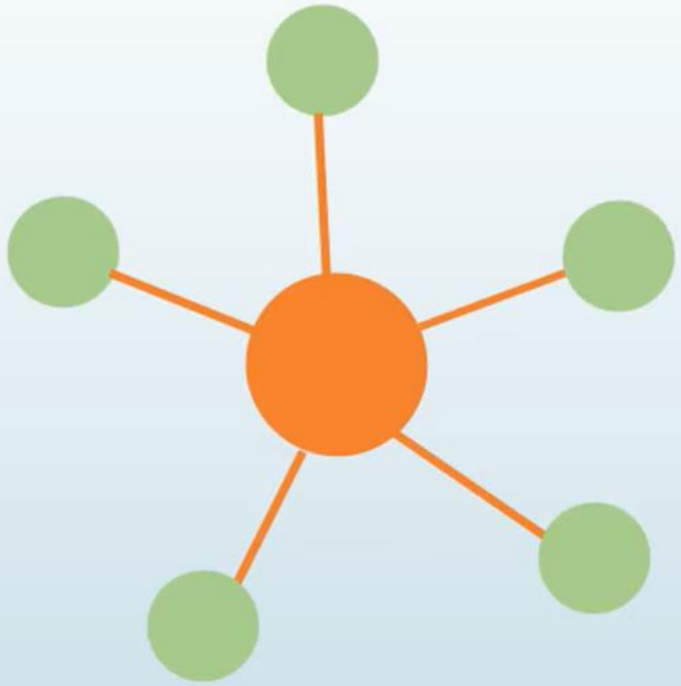
Mesh Topology

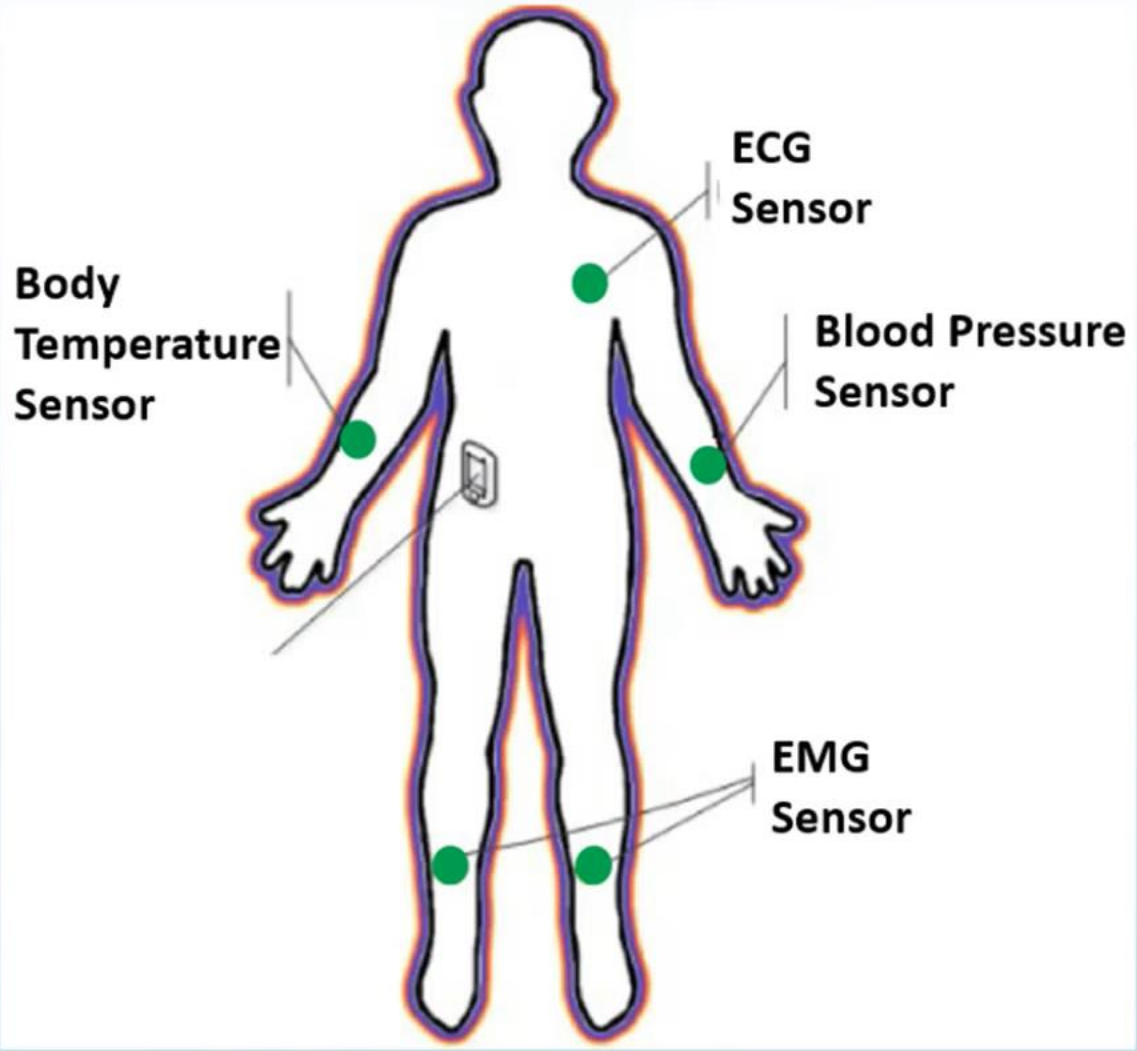


Channel Access

Contention-free method

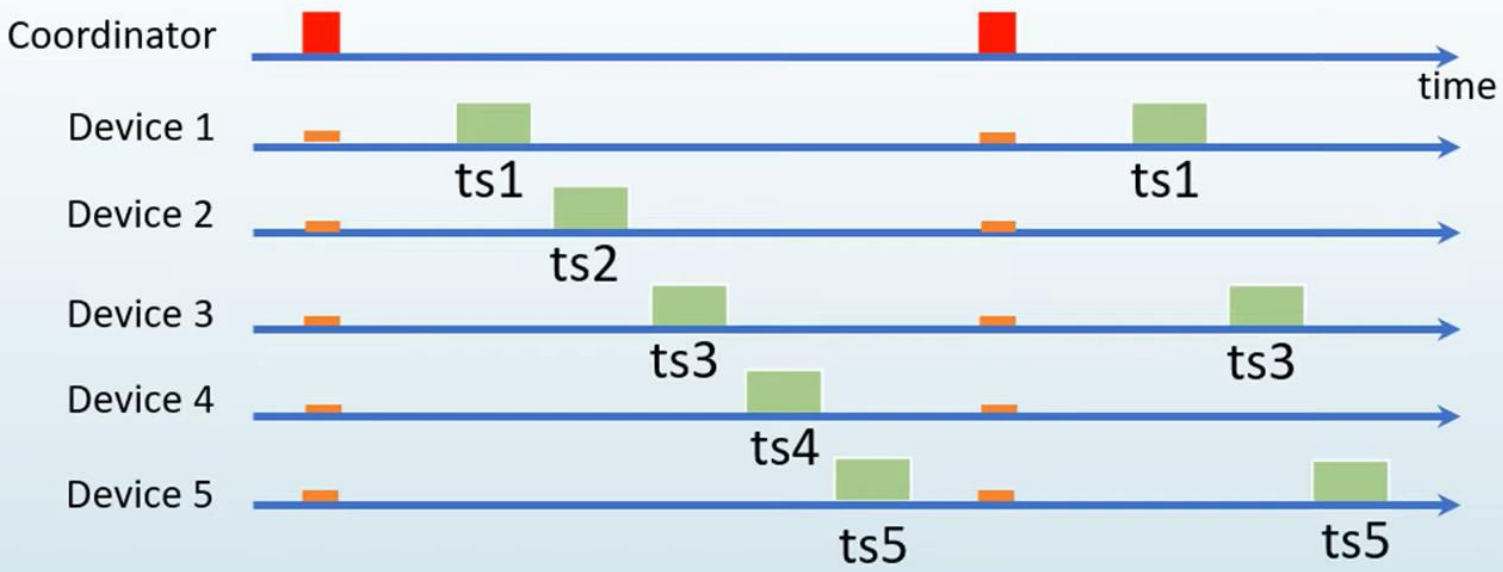
- The coordinator dedicates a specific time slot to each device. This is called a guaranteed time slot (GTS).





Channel Access

Contention-free method



Channel Access

Contention based method

- Devices do not need to be synchronized
- Carrier Sense Multiple Access – Collision Avoidance mechanism
- Anytime a device wants to transmit:

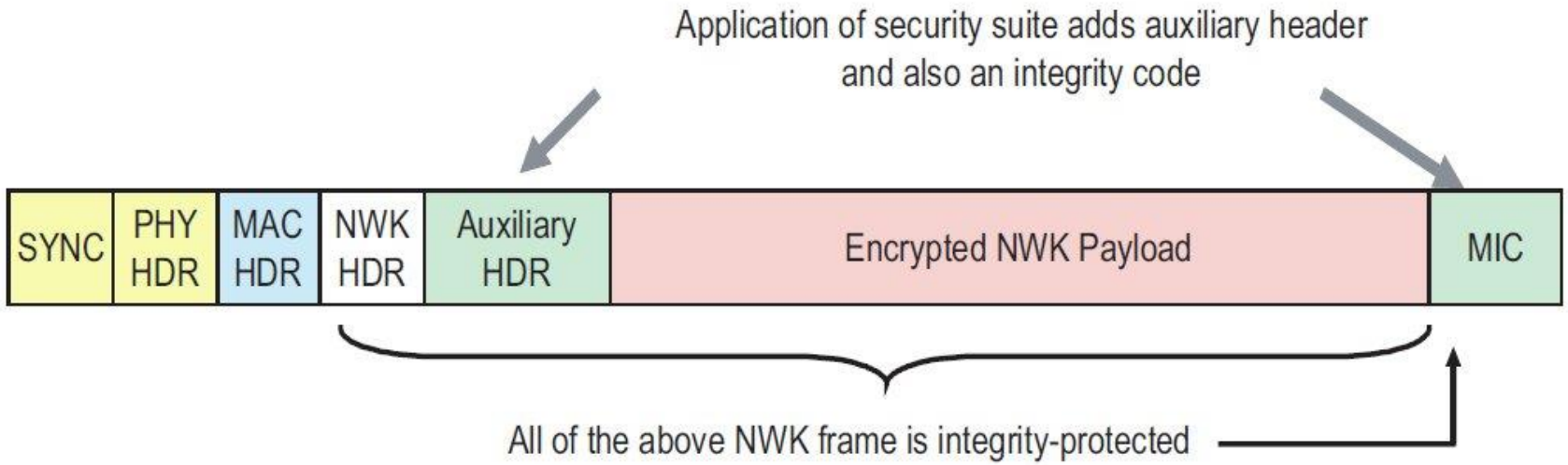
  1- It first goes into receive mode

  2- Detect if there is any signal in the channel.

  3- Device will only transmit the data if the channel is clear.

  - If the channel is not clear, the device backs off for a random period of time and tries again.

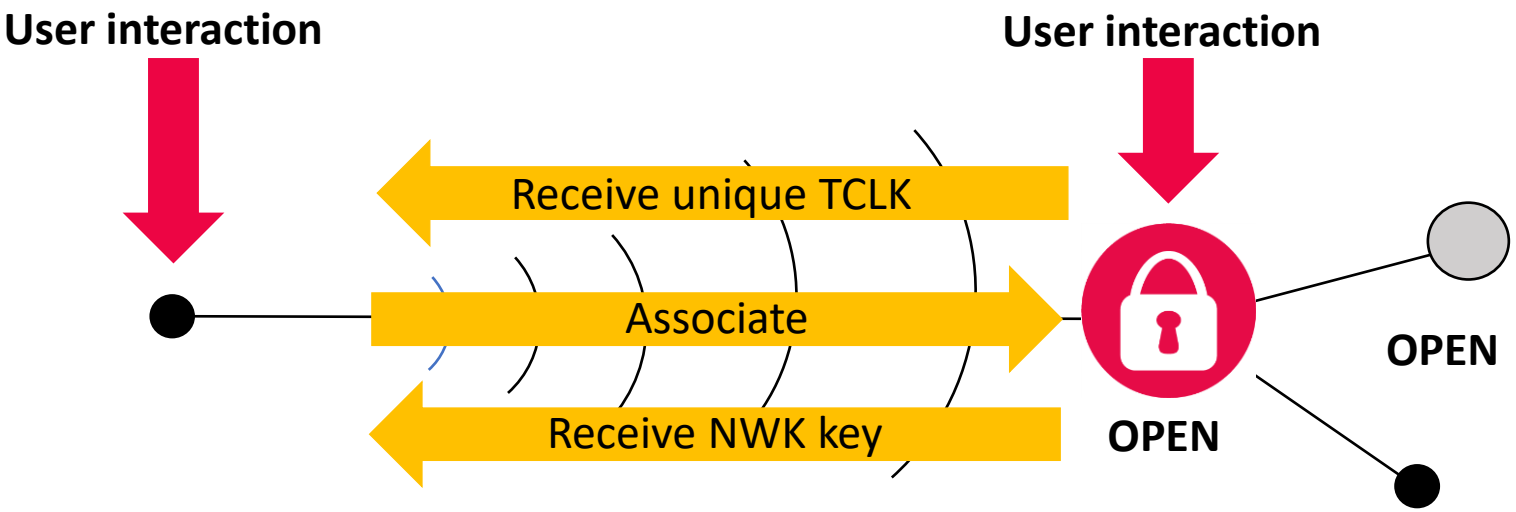
Zigbee PRO Communications Model



- Standard Frame Format builds on the 802.15.4 format to add network and application specific commands/responses as part of the 802.15.4 payload

- Secure (AES-128 encryption) at network level for all nodes
- Additional application layer security available with a single key for every node pair

Zigbee Base Device Behavior: Joining a Zigbee network



Joining device

- Perform a channel scan
- Select an open network & associate
- Authenticate
- Receive the network key
- If joining a centralized security network, exchange TCLK

Node on a network

- Open the network for 180s
- Participate in the association as parent
- Participate in the key exchange as parent and/or coordinator
- Close the network

Green Power

What is Green Power?

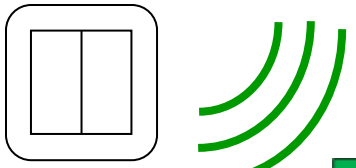
- Green Power is a feature of Zigbee PRO networks
- Integrating battery-less (energy harvesting-based) or life-long battery operated devices into the Zigbee network
  - **Key benefit**: adds nodes/devices to the network that are virtually completely maintenance free
- Green Power adds green capability to Zigbee by eliminating battery usage and waste

Green Power applications

- (Light) switch: flipping the switch generates the energy for data-communication

Sensors, open/close detectors, emergency buttons, industrial switches, …

Green Power Device (GPD)

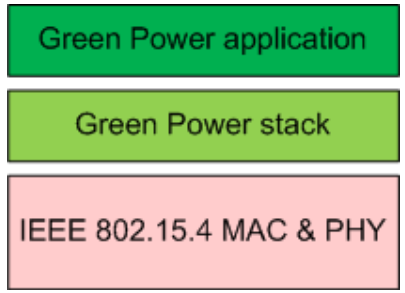


GPD

Green Power Device Frame

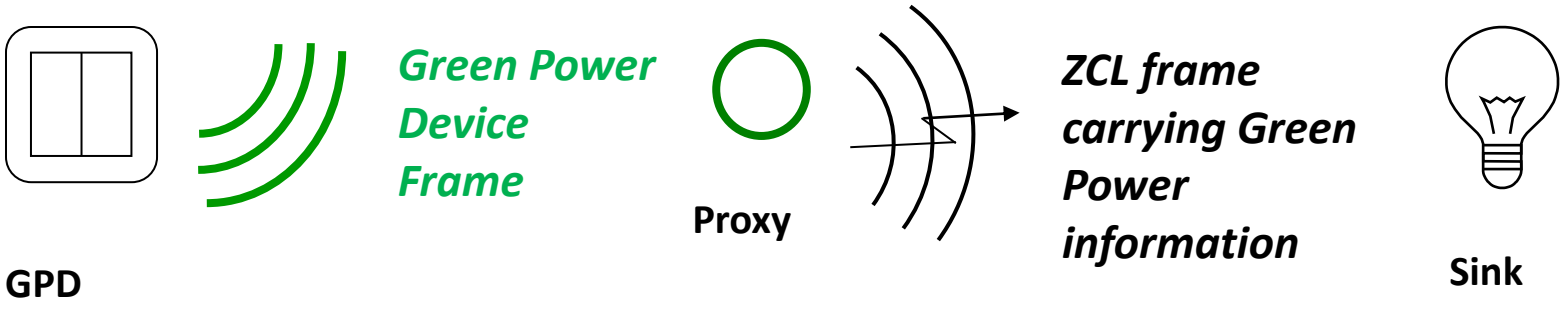
<u>Compact frame with:</u>

- unique identification of the Green Power Device (GPD)
- Scalable security
- Future-proof application framework

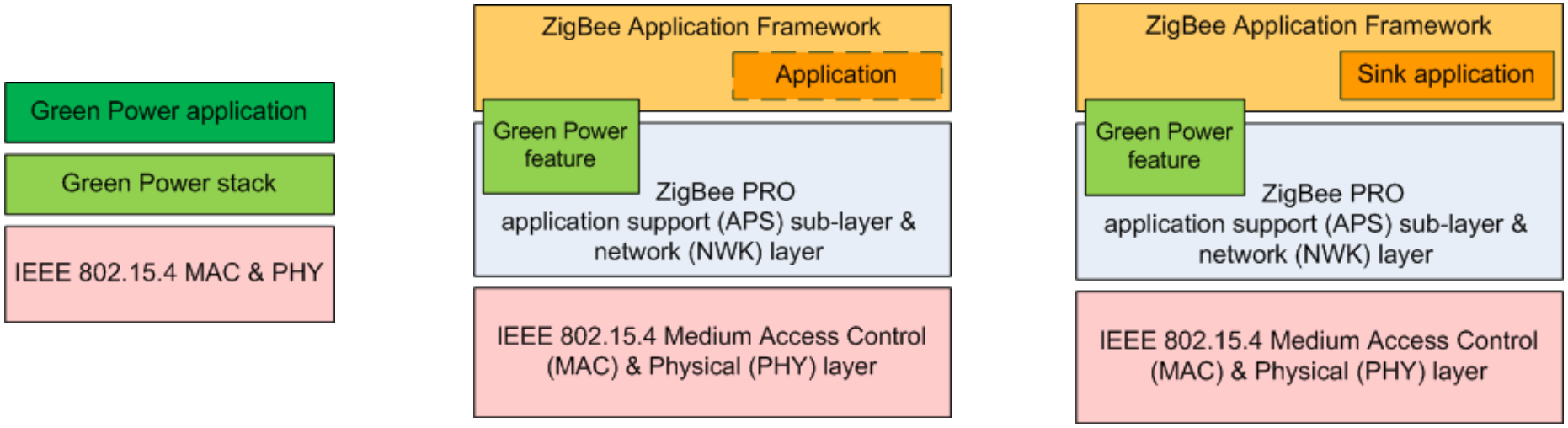


*<u>GPD is *NOT* a ZED! It's less.</u>*

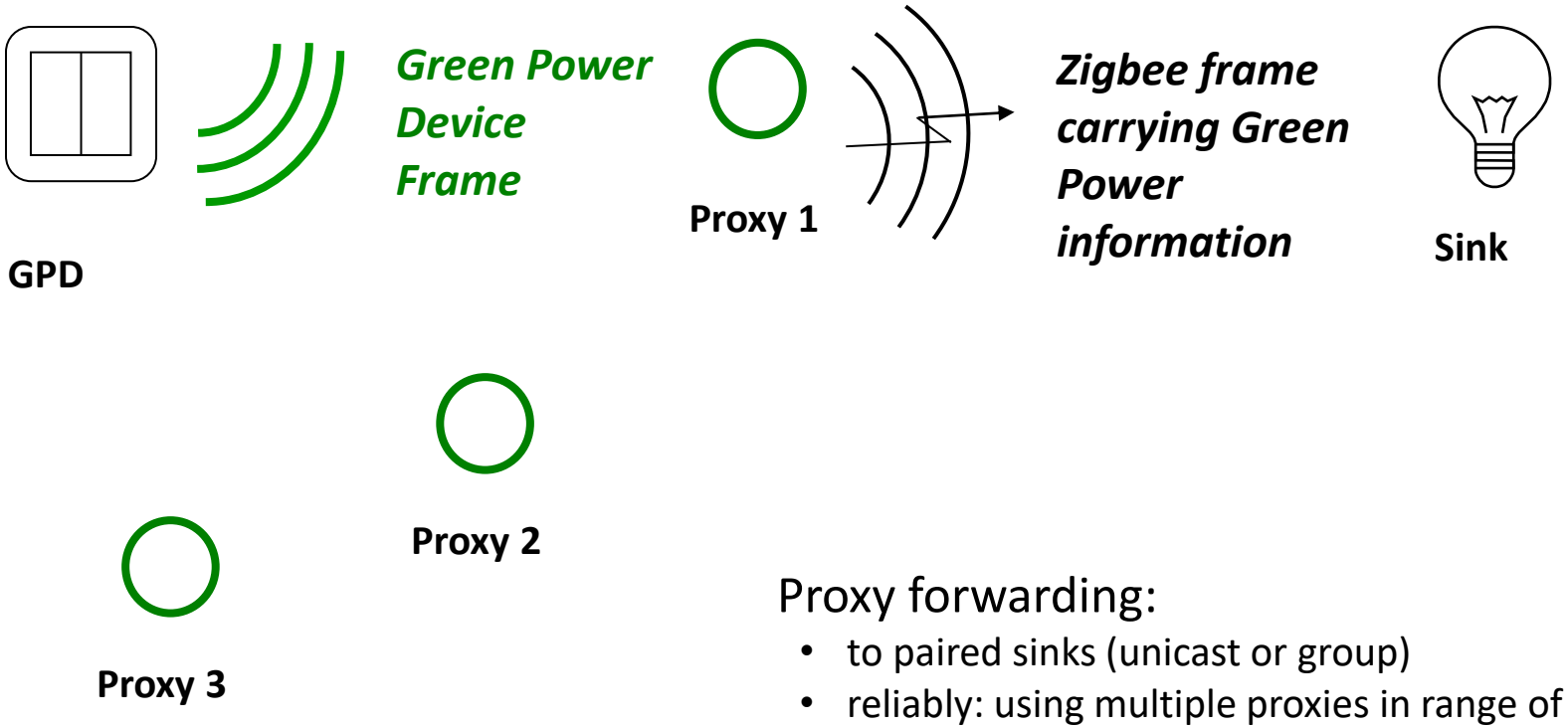
Green Power & Zigbee PRO: Proxy & Sink



Application-agnostic



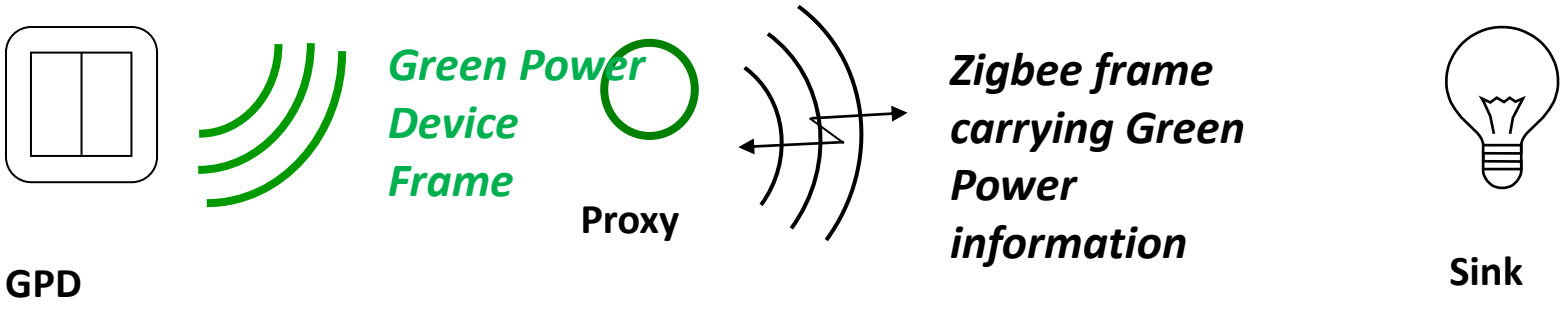
Green Power: Proxy functionality



Proxy forwarding:

- to paired sinks (unicast or group)
- reliably: using multiple proxies in range of the GPD (no single parent problem)
- efficiently (bandwidth usage)

Green Power: Commissioning

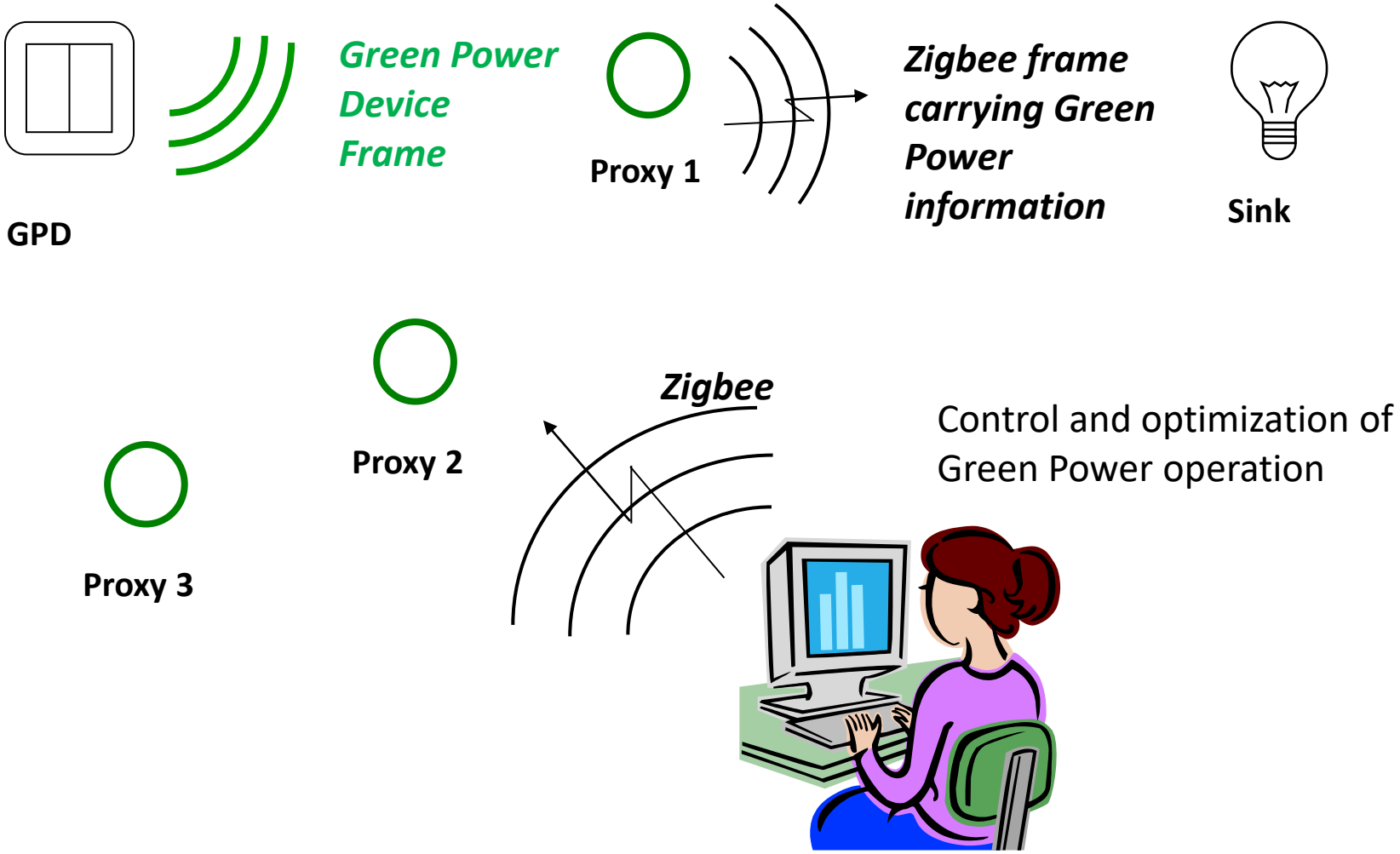


Commissioning:

- brings the Green Power Device on the operational channel;
- bootstraps GPD security;
- creates a control relationship between the Green Power Device and the sink – at the sink;

Without tools; in the same simple user interaction

Green Power: Management



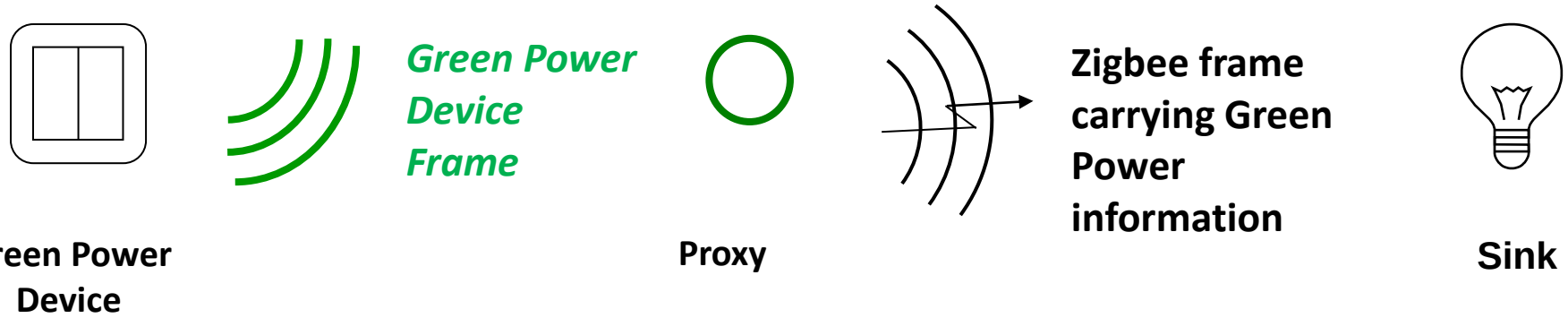
Zigbee Green Power

where mains and battery are impractical or for lifelong battery life

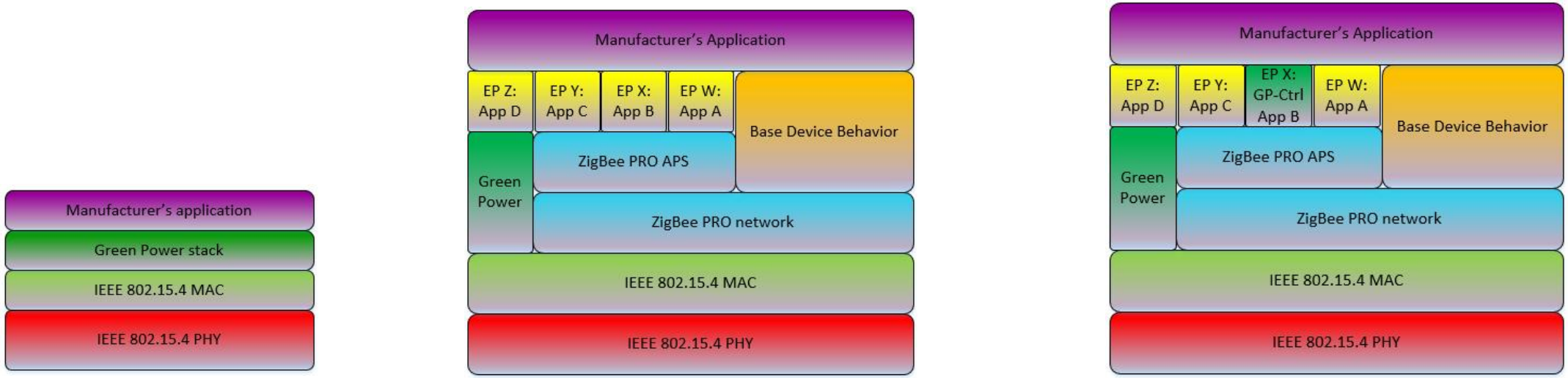
Energy & complexity

- Zigbee Coordinator & Trust Center
  - A router dedicated to managing security credentials and performing other network management tasks in a centralized manner
- Zigbee Router
  - Mains powered, always on
- Zigbee End Device
  - Battery powered, fully bi-directional
- Zigbee Green Power Device
  - Energy-harvesting (battery-less) or life-long battery; may be transmit-only;
  - E.g. switches, setpoint controllers, sensors

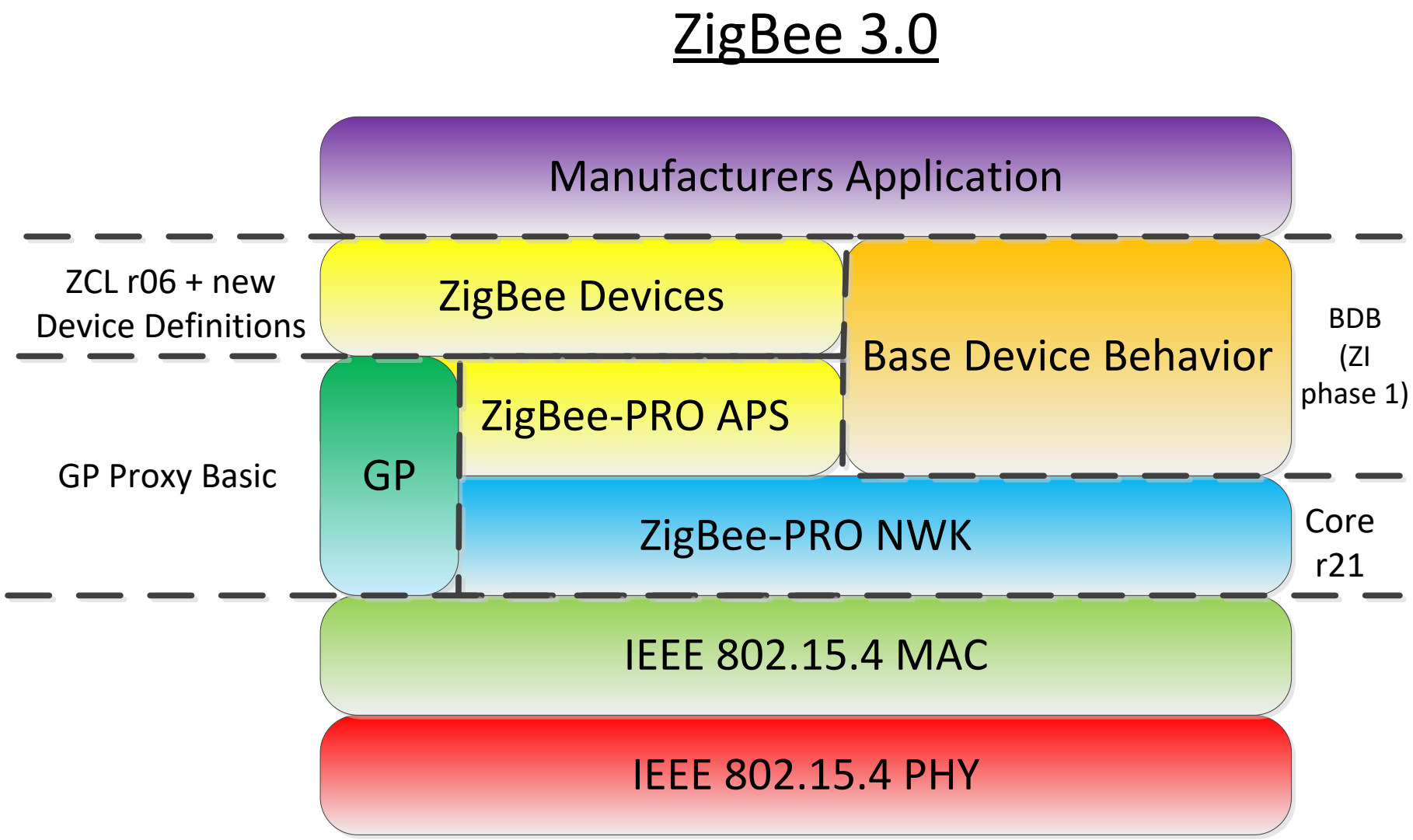
Zigbee Green Power explained



Application-agnostic

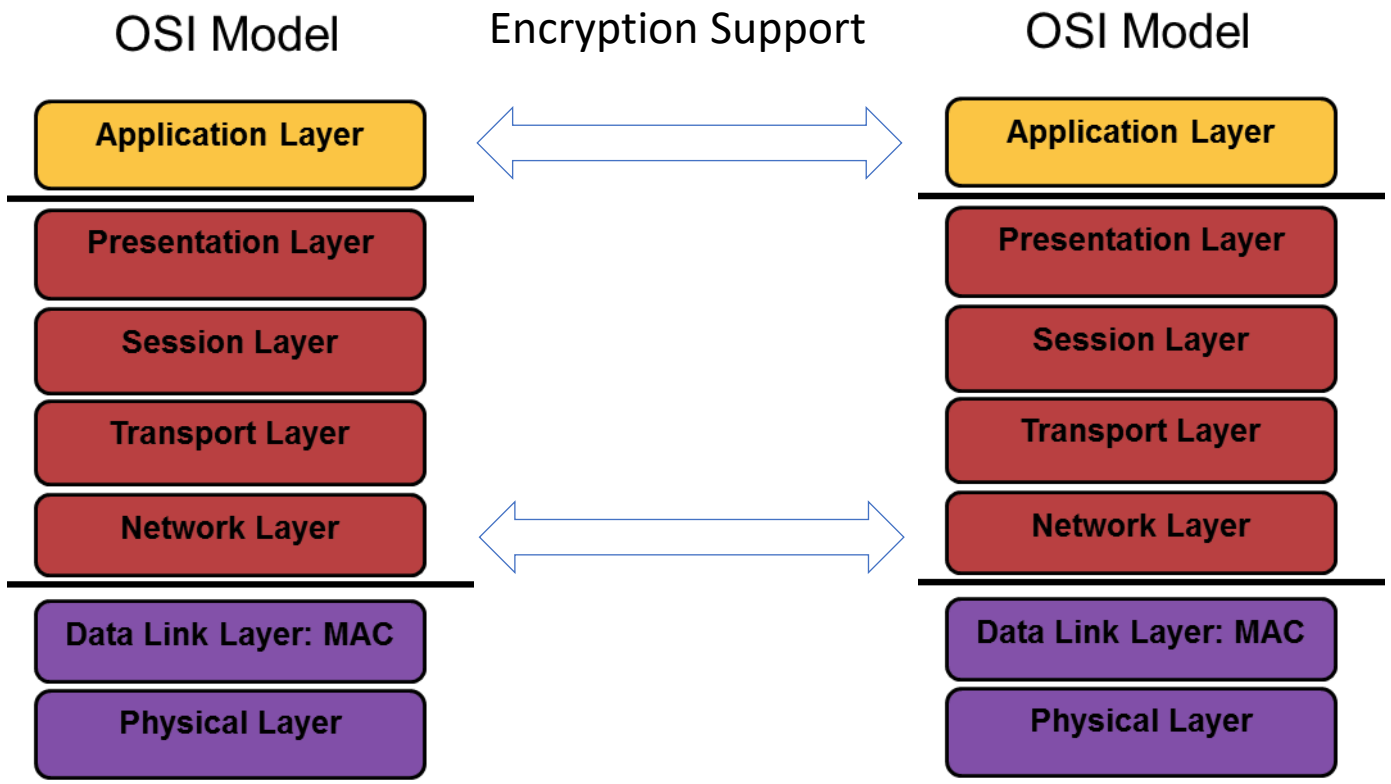


Green Power in Zigbee 3.0



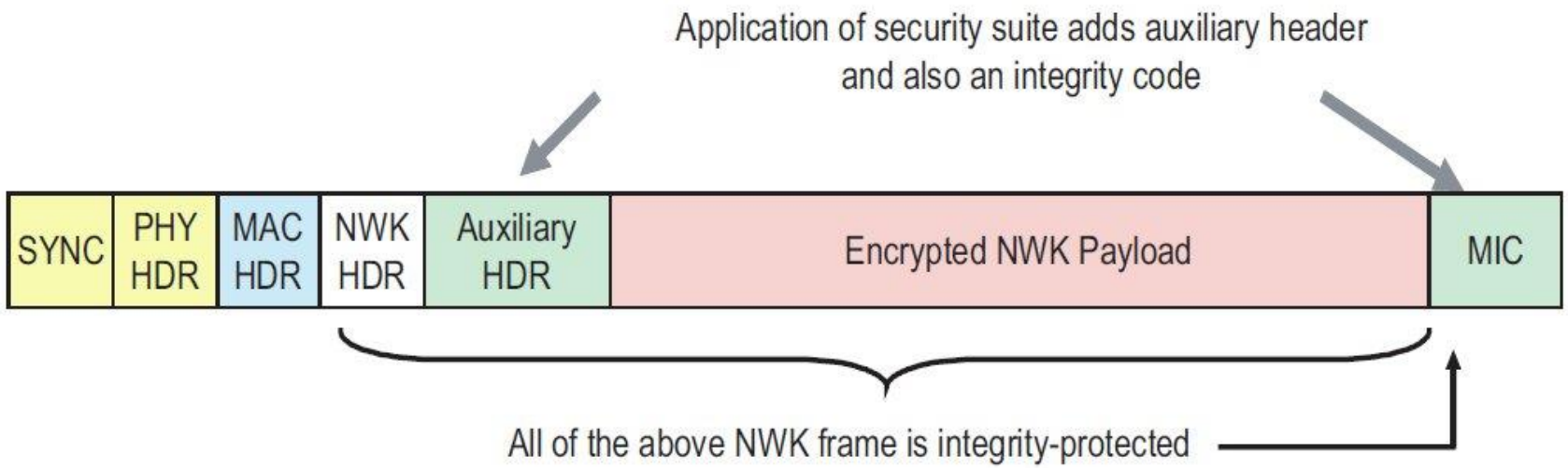
Security Considerations

Standardized at all Layers



AES 128 Security with varying keys

Zigbee PRO Communications Model



- Standard Frame Format builds on the 802.15.4 format to add network and application specific commands/responses as part of the 802.15.4 payload

- Secure (AES-128 encryption) at network level for all nodes
- Additional application layer security available with a single key for every node pair

Location Awareness

Wireless Coexistence

The Challenge

- Co-existence in a crowded spectrum is a major concern for any wireless network

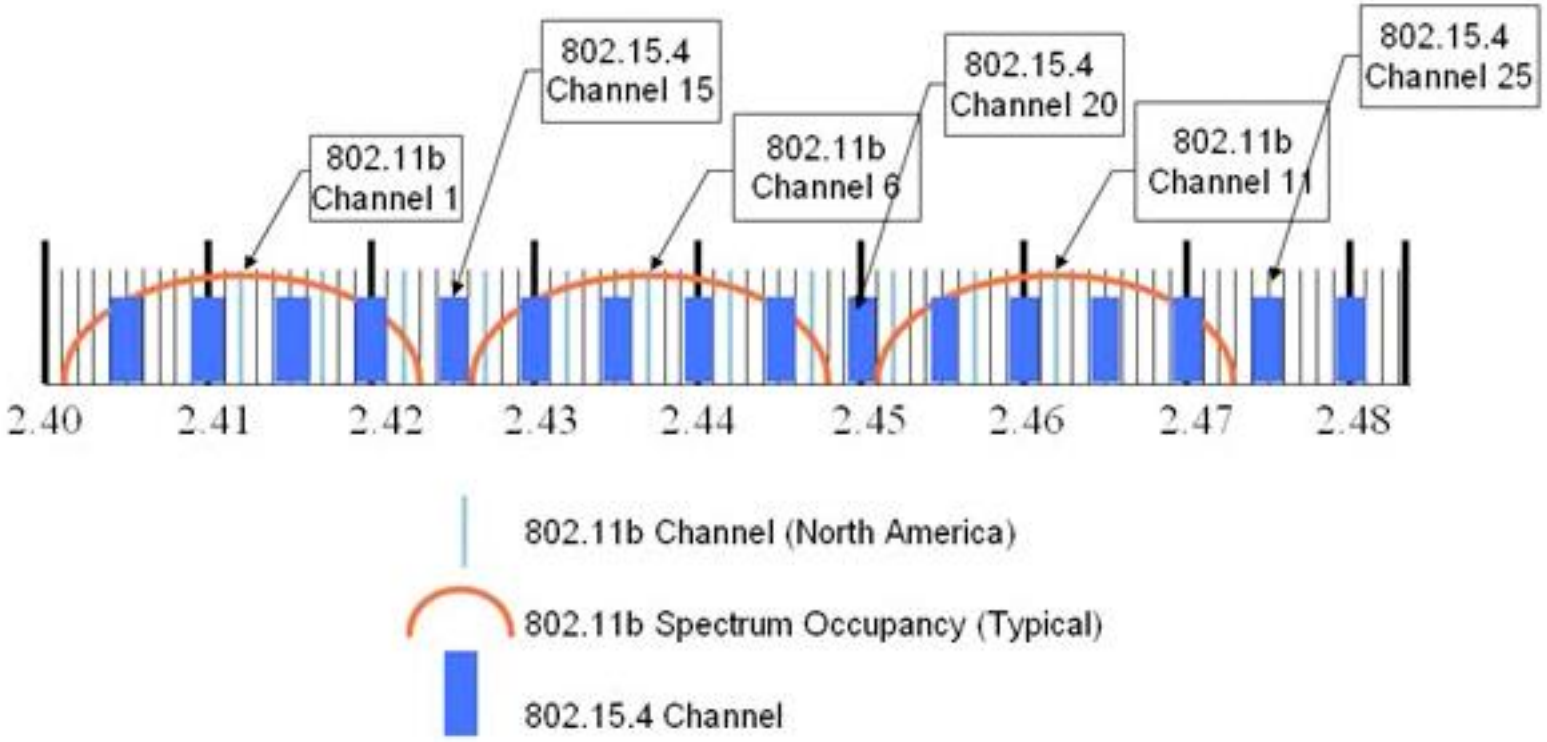
- There is a multitude of products in use today that operate in the 2.4 GHz ISM band
  - **Bluetooth**
  - **Wi-Fi**
  - **Microwave ovens**
  - **Etc.**

- IEEE 802.15.4 standard (and protocols based on it) is equipped with system attributes that are key to surviving the interference rich 2.4 GHz environment

IEEE 802.15.4 Pedigree

- Global standard
- Variety of sources
- Technology in mass production since 2003
- Optimized for low duty cycle application
  - **Longer battery life (months to years)**
  - **Small packets (short Tx times)**
- Interference avoidance
  - **DSSS**
  - **CSMA-CA**
  - **Short burst transmission**
  - **Retries**

IEEE 802.15.4 Spectrum Usage



IEEE 802.15.4 CSMA-CA

Wi-Fi Speaks at less than 100% duty cycle

802.15.4 uses CSMA-CA to speak in the quiet periods

CSMA-CA Algorithm (Carrier Sense Multiple Access – Collision Avoidance) listens before transmitting and "backs off" in the presence of interference

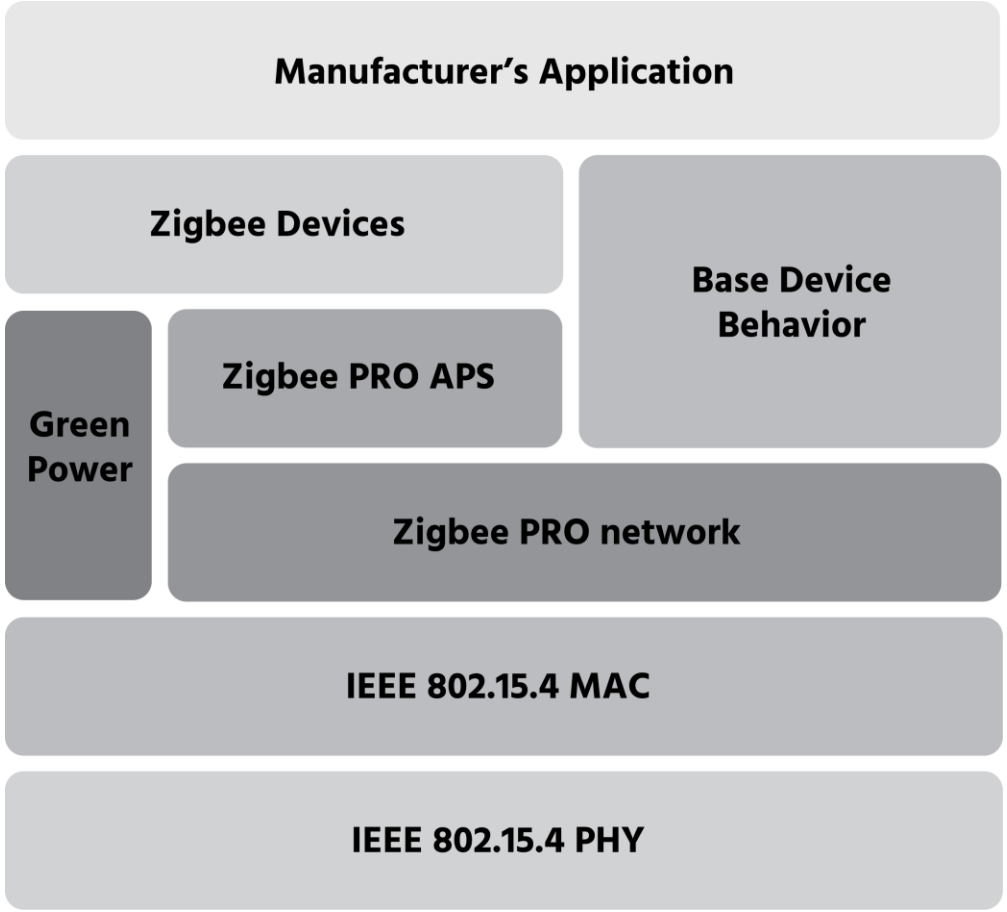
Symbol rate is 62.5 kHz so a symbol only last 16 μs

Network Level Enhancements

- Networking Protocols can extend the interference avoidance capabilities of IEEE 802.15.4 by providing advanced protocol features to deal with interference sources
  - Zigbee PRO
    - Network level acknowledgements
    - Network Level re-tries
    - Frequency Agility
      - Network Moves to “cleaner” spectrum
  - Zigbee RF4CE
    - Multi-channel operation
      - IEEE 802.15.4 channels 15, 20, and 25

Zigbee 3.0: flexibility of Zigbee PRO

A toolbox for many needs



Routing:
Table routing?
Many to one routing?
Source routing?

Security:
Centralized?
Distributed?

Addressing:
Unicast?
Groupcast?
Broadcast?

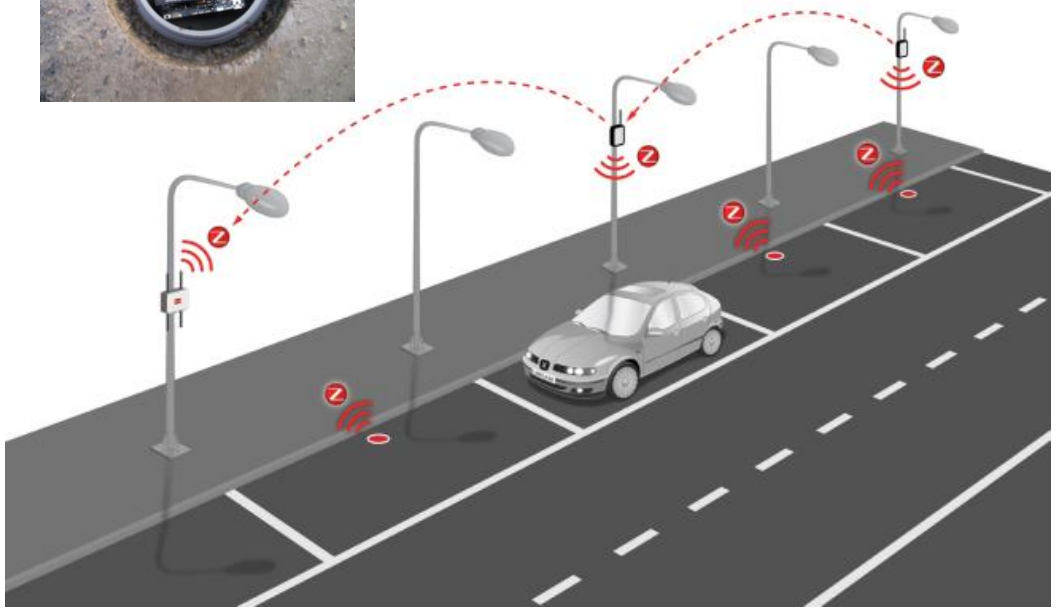
Applications

Applications

GM Spring Hill Plant:
28,773 connected lights,
20 million square feet

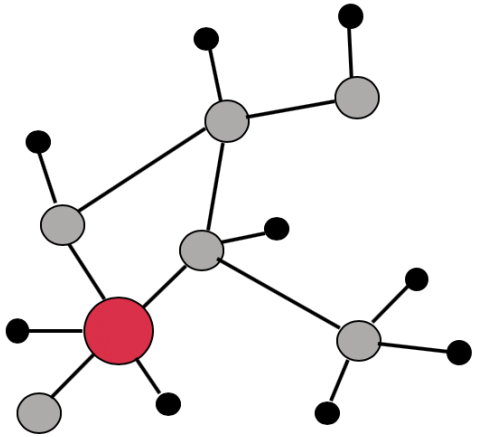
Aria Hotel City Center, Las Vegas:
+ 100,000 Zigbee devices

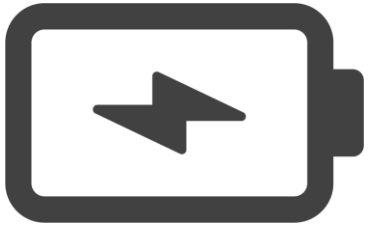
Hampshire City Council, Hampshire UK:
90,000 connected street lights



zigbee

Security & Safety
HVAC
Lighting
Retail
Sensing
Commissioning
Energy metering
Appliances
Telecommunication





Flexible self-organizing mesh + **Ultra low-power** + **Library of applications**

References

- https://www.cse.wustl.edu/~jain/cse574-14/j_13zgb.htm
- https://zigbeealliance.org/solution/zigbee/
- https://www3.nd.edu/~mhaenggi/ee67011/zigbee.pdf[ZigBee Specifications]

Thank you.