# zigbee

By

Emirkan Sali

Yashodhan Deshpande

Lochana Abhayawardana

Motivation

- Wireless communication widespread and widely used
- Wireless sensor networks (WSN) in many modern application areas
- The diverse areas of application call for different standards
- Low-rate WPAN for low cost, adequate battery life, and easy installation
- ZigBee communication protocol as a prevalent low-rate WPAN

IEEE 802.15.4 Standard - Architecture

- Network specification used by ZigBee

- One physical and one MAC layer

- Physical layer for radio frequency transceivers

- MAC layer for transfer access
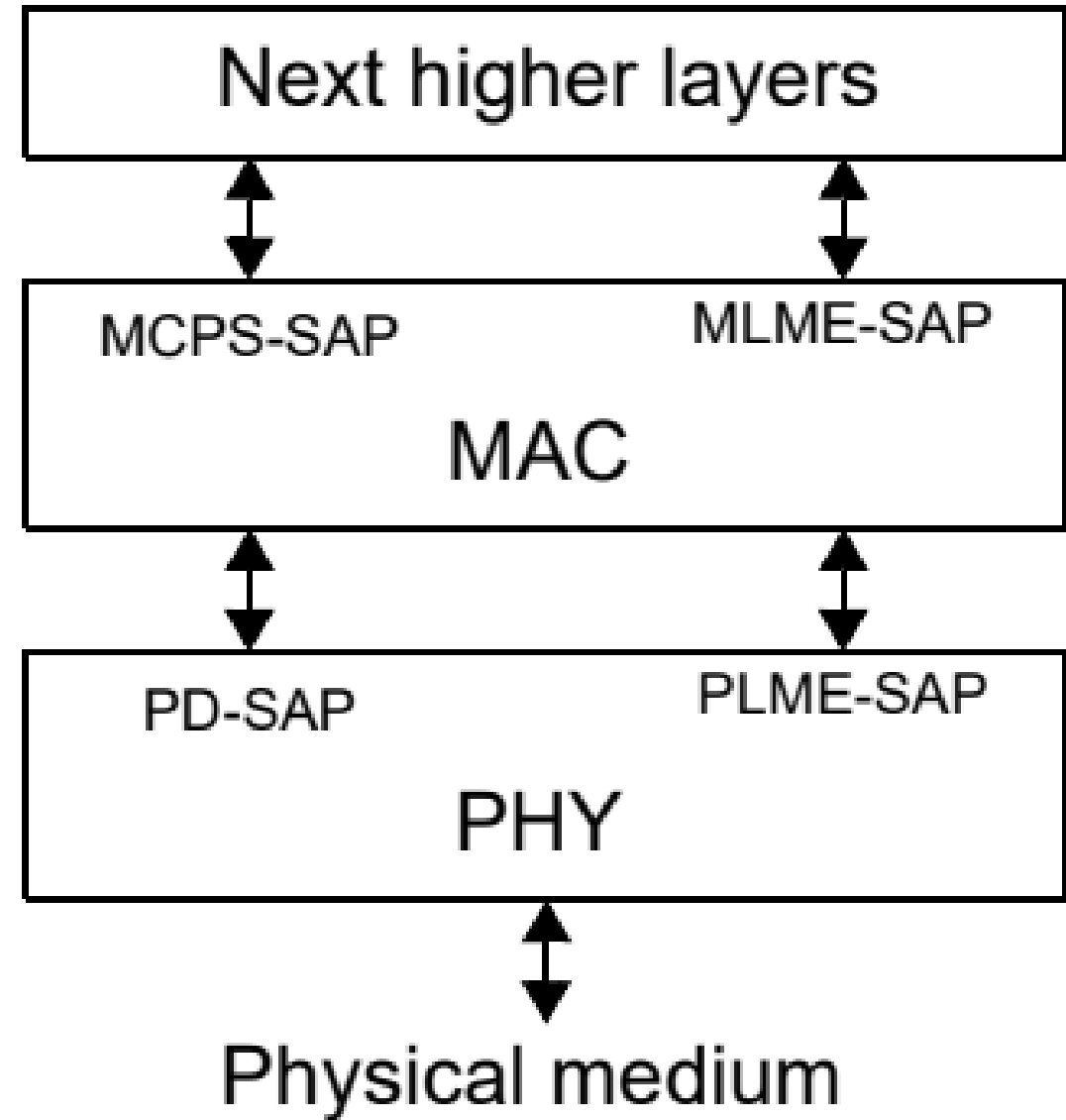
IEEE 802.15.4 Standard – Network

Two different type of devices:

Full-function device (FFD)

Reduced function device (RFD)
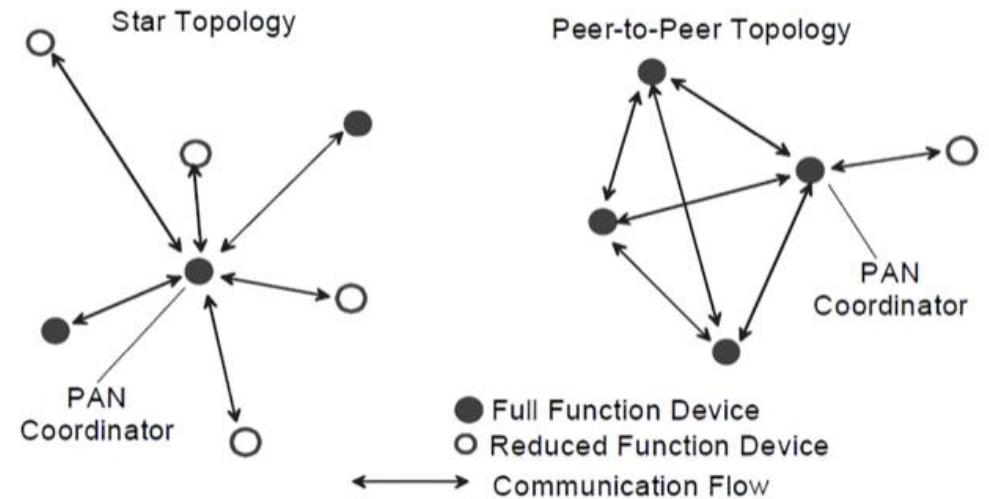
FFD as the central node of a network – PAN coordinator

RFD as a sensor or actuator for low-cost
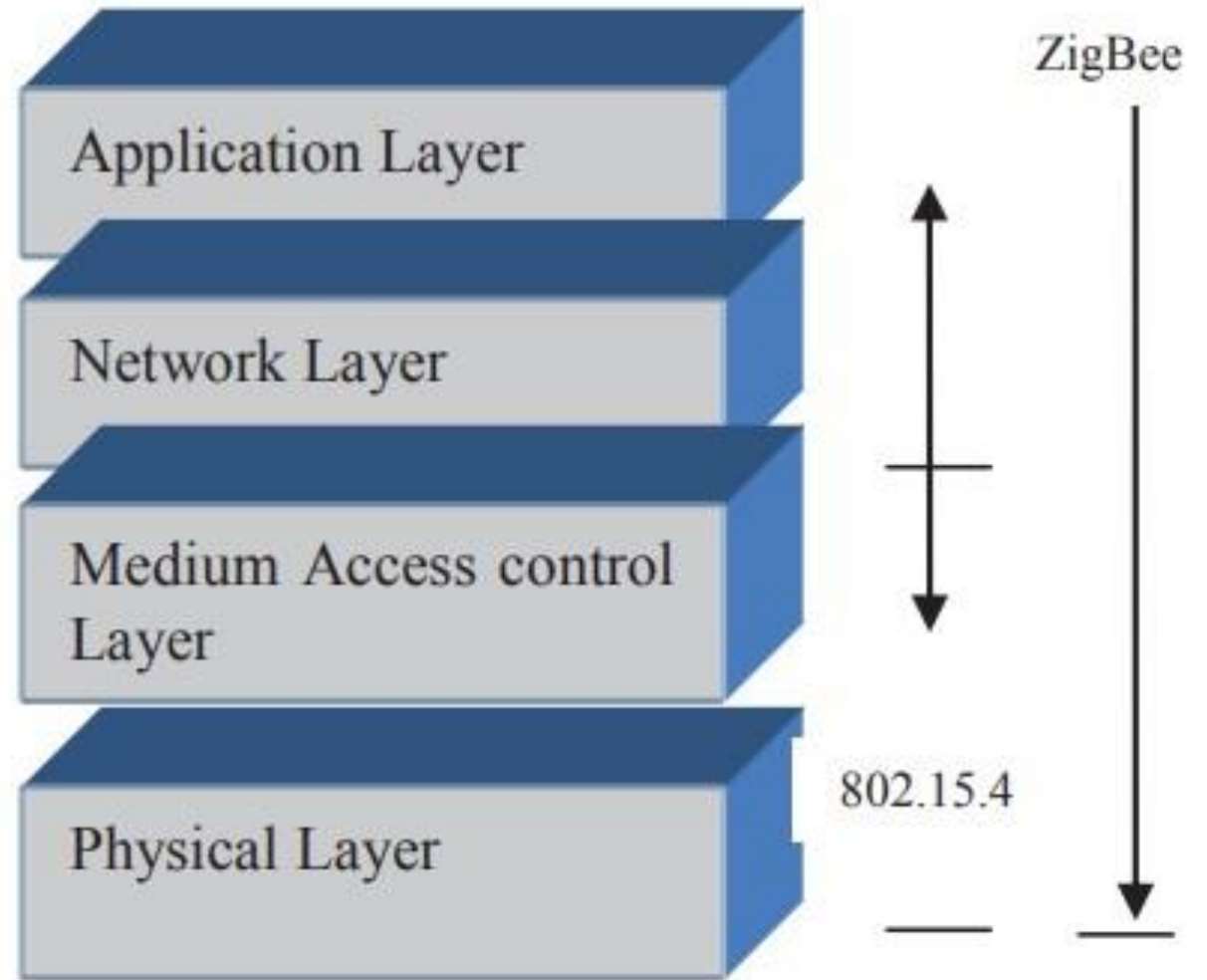
IEEE 802.15.4 - Topology

- 4 possible topologies using this standard:

1. Star topology

2. Peer-to-Peer topology

3. Tree topology

4. Mesh topology

ZigBee Specifications

- Expands on the layers of IEEE 802.15.4 standard

- Network and application layer added ontop

- Each layer has entity for data and management

ZigBee Specifications

- 2.4 GHz Worldwide with 16 channels and 250 kbps

- 915 MHz in USA with 10 channels and 40 kbps

- 868 MHz in Europe with 1 channel and 20 kbps

- Uses Star, Mesh or Tree topology

- FFD devices for routing in the network – ZigBee routers

- RFD devices for communicating with parent device – ZigBee End-devices

Technical components of a Zigbee network
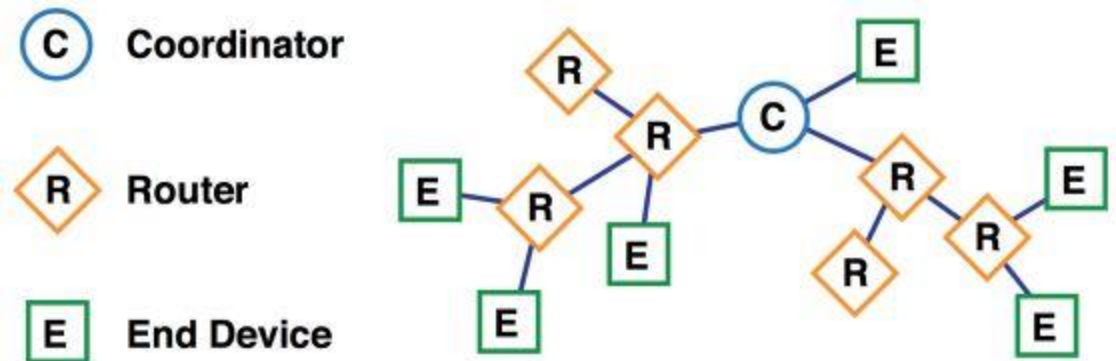
- **Coordinator**:
1. Functions as a **trust center** that provides security control of the network.
2. Stores and distributes the **network keys**.
3. Configures devices, **gives permission** to other devices to **join or leave the network** and keeps track of the devices.

- **Router**:
1. Intermediate **nodes** between the coordinator and the end devices.
2. Can **route traffic** between end devices and the coordinator, as well as **transmit** and **receive data**.
3. Can allow other routers and end devices to join the network.

- **End device**:
1. It is often low-power or battery-powered device.
2. Examples are motion sensors, contact sensors, and **smart light bulbs**.
3. The end devices **do not route any traffic** and **cannot allow other devices to join the network**.
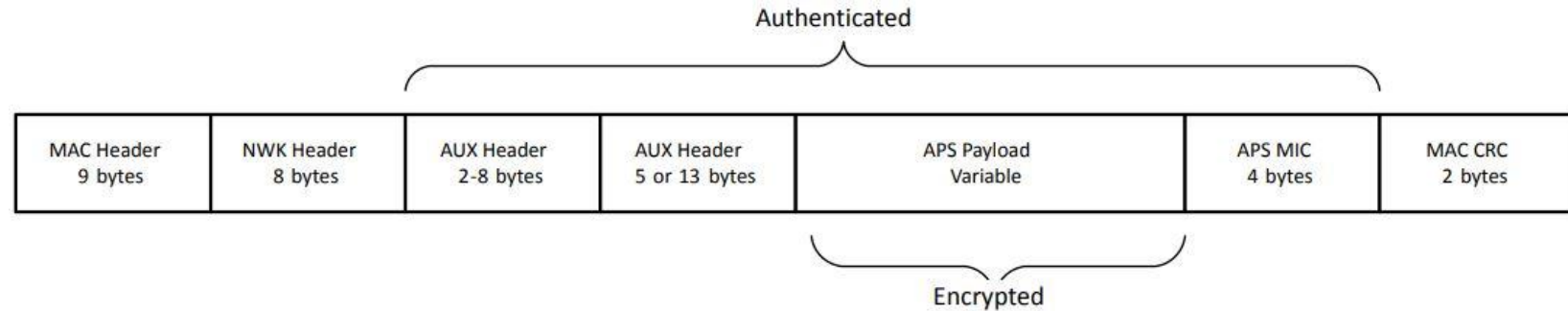
Device Configuration and establishing secured connection
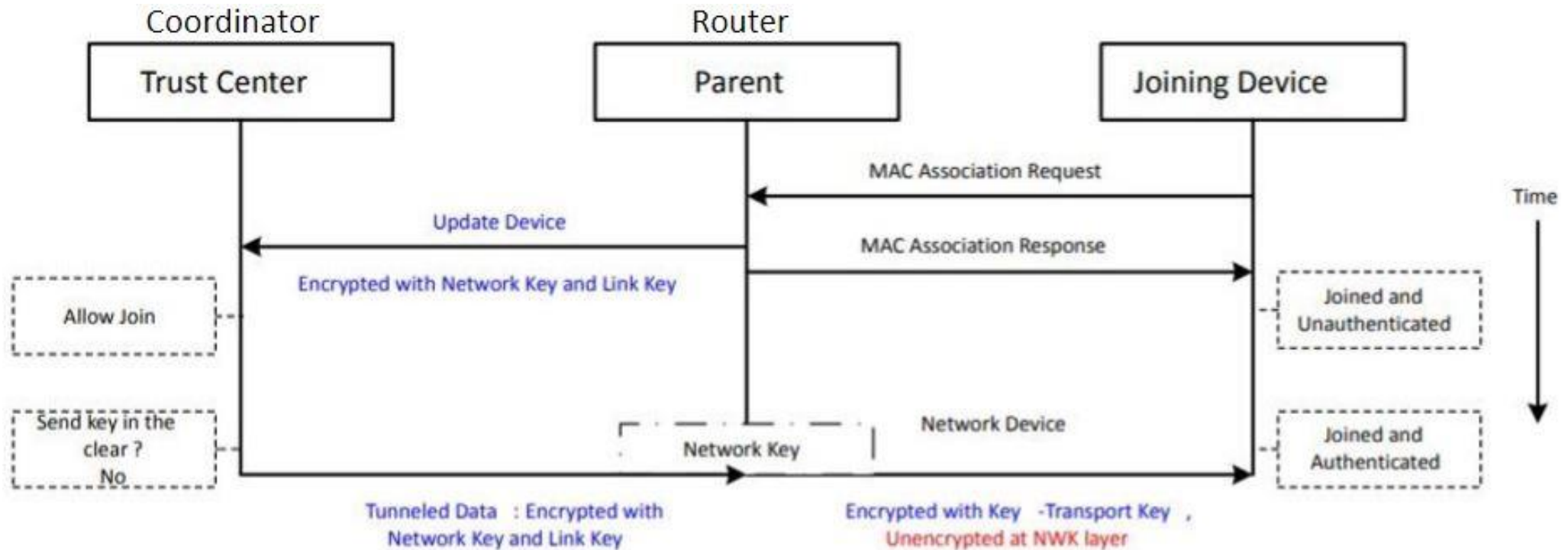
- **Link key**: Encrypting the initial transfer of the network key to a joining node

- **Pre-configured global link key**:
The Zigbee-defined key, 5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39 (ZigbeeAlliance09)

- **Pre-configured unique link key:** This link key is usually **pre-configured** or pre-programmed into the relevant nodes either in the **factory or during commissioning**.
Zigbee 3.0 - **installation code**

Zigbee data packet and related security

Authenticated				

MAC Header 9 bytes	NWK Header 8 bytes	AUX Header 2-8 bytes	AUX Header 5 or 13 bytes	APS Payload Variable	APS MIC 4 bytes	MAC CRC 2 bytes

Encrypted

- **MAC Header:** The **upper layer sets the MAC layer default key** to coincide with the **active network key** and the MAC layer link keys to coincide with any link keys from the upper layer.

- **NWK Header:** Uses a **network-wide key** for encryption and decryption.

- **AUX Header** (Auxiliary Header):
1. Data about the security of the packet that a receiving node uses to correctly **authenticate and decrypt the packet**.
2. A **frame counter** is included in the auxiliary headers.

- **APS payload** (Application Support (APS) layer):   Data to be transmitted.

- **APS MIC (Message Integrity Code (MIC)):**
1. Used to authenticate the message by insuring it has **not been modified**.
2. A **receiving device verifies the message** by calculating MIC against the value written at the end of the message.

- **MAC CRC (MAC cyclic redundancy check): Detect errors** in the data and information transmitted over the network.

Applications of ZigBee

Home Automation:

- Connect multiple devices to a hub in a **mesh network**.
- The **hub** is the master **coordinator of the system** that gives instructions to every other device.

- Home Automation **clusters** are **group of smart home systems** or sensor.
1. **General clusters** are common to all ZigBee Alliance products.
2. **Measuring and sensing clusters**
3. **HVAC clusters (Heating, Ventilation and air conditioning)**

- **Commissioning** is a method to setup a device in ZigBee network.
1. **Automatic mode** : Plug and play. In this mode the device configures itself.
2. **Easy mode** : The devices contains some switches that the user configures to setup the device.
3. **System mode** : A laptop or PDA(Personal Digital Assistant) device is used to install the device.

- Amazon Echo (Fourth Generation) functions as a **Zigbee Hub**.

Advantages of ZigBee

- **Low power consumption:** designed to function on low-power and battery-efficient devices

- **Mesh capability :** all the nodes are signal repeaters

- **High Compatibility:** based on a single standard, uses common language and protocols, over 6000 devices

- **Security and Privacy:** 128-bit encryption algorithms and frame counter,

  does not require Internet connections

Disadvantages or Challenges to ZigBee

- **Implementation Cost -** infrastructure

- **Channel noise:** Bluetooth, cordless phones, microwaves and other wire-less devices share the common band of 2.4 GHz, overlap/ interference

- **Low transmission rate:** designed for low-rate data transmission, Lower than Wi-Fi and Bluetooth

- **Security and compatibility:** If in a centralised ZigBee system – centralised device fails then all nodes are failed,

    Not built-in with smartphone and computers

Comparison with other protocols
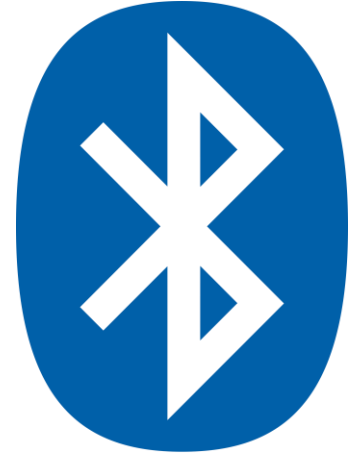
1. Bluetooth:

- Bluetooth Special Interest Group (SIG)

- Bluetooth Classic, Bluetooth Low Energy (BLE) and Bluetooth mesh

- BLE same motivation, Tiney devices required longer battery life

- BLE is more power efficient

- ZigBee Mesh capability: large scale home automation

    House with multi-floors, several rooms

    Self-configuring and self-healing

2. **ISA100**:

- developed by International Society of Automation
- Focuses on Wireless systems for manufacturing and control applications
- mesh network, operate in 2.4 GHz or 900MHz, Higher data rate
- ISA100 is industry focused, ZigBee mostly home automation

3. **Z-wave:**
- Danish Cooperation Zensys
- Wireless communication protocol, Home automation
- Half Duplex

- Differences between Zigbee and Z-wave
1. Data rate: ZigBee 250kbps but Z wave is limited to 40kbps
2. Frequency: 2.4GHz and 900MHz, but z-wave 99Mhz
3. Range : 10-75m , Z wave 30m
4. Cost: ZigBee cheaper than Z-wave

Conclusion

- IEEE 802.15.4 Standard - **Architecture**

- IEEE 802.15.4 -**Topologie**

- **Zigbee data Packet transmission**

- **Applications of Zigbee**

- Selecting the **communication protocol** will depend on the **requirements**.

1. **Bluetooth**
2. **Z wave**