

# ZigBee and IEEE 802.15.4

By: Vishal Parmar  
CS558L

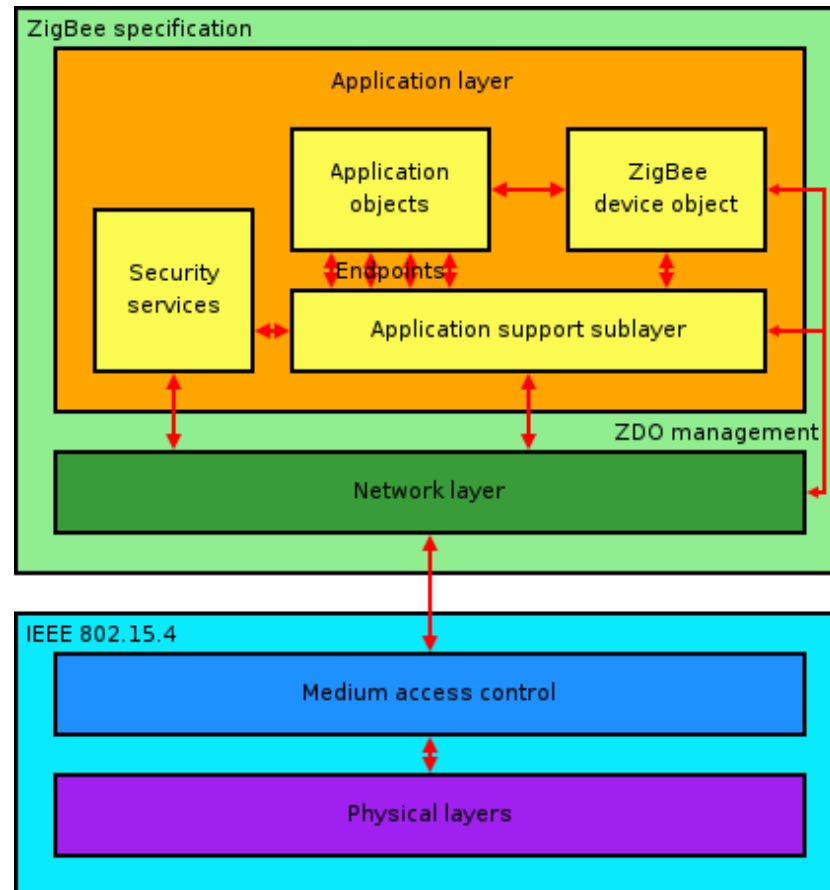
# Introduction

- **ZigBee**
- **IEEE 802.15.4:-** Low-Rate WPAN(Wireless Personal Area Network).

# ZigBee Specification

- Low cost
- Low-power wireless communication solution
- Maintained by ZigBee Alliance
- Builds on PHY(Physical Layer) and MAC Sublayer( defined in IEEE 802.15.4)

# ZigBee Protocol Stack



# ZigBee Specification Cont.

- Four main components
  - Network Layer
  - Application Layer
  - ZigBee device objects ( ZDO's)
  - Manufacture-defined application objects
- Significant addition of ZDO: Includes keeping Device roles, request to join network, device discovery and Security.

# Network Layer

- Main function
  - Correct use of MAC Sublayer
  - Provide suitable interface for upper layer
- Includes Capability and structure of typical network layer including routing.
- Data Control: Creates and manages network layer data units from upper layer payloads
- Layer Control: Handles Configuration of new device and establish new networks.

# Application Layer

- Highest Layer
- Provide service to End User
- Comprises of major components added to Zigbee Specification
- Includes Zigbee device object and Application Objects, security services and Application Support Sublayer

# Application Layer Cont.

- Main Components
  - ZigBee Device Objects (ZDO)
    - Responsible for defining the role of device.
    - Discovery of new devices and identification of offered services
  - Application support sublayer(APS)
    - Well defined interface and control services
    - Manages Binding tables of device and services

# Security Services

- ZigBee facilitates:
  - Secure communication
  - Protecting establishment
  - Transport of cryptographic keys
  - Ciphering frames
  - Controlling devices
- Builds on the security framework of IEEE 802.15.4
- It relies on the correct management of symmetric keys and the correct implementation of methods and security policies.

# Security Services Cont.

- Basic Security Model
  - Adequate protection of keying material.
  - Different transcribers are supposed to be trustworthy.
  - Different network layers are not cryptographically separated so, Access policies needed b/w different network layers.

# ZigBee Security Architecture

- Uses 128 Bit Keys
- Keys associated to
  - Network
  - Link
    - Acquired through pre installation agreement.
- Key Distribution: By Trust center

# Distributed Security Architecture

Security architecture is distributed as follows

- MAC Sublayer
  - Single hop reliable communication
  - The security level is specified by the upper layers.
- Network Layer
  - Link or network key is used.
- Application Layer
  - Offers Key establishment and transport services to both ZDO and applications.

# IEEE 802.15.4 (LR-WPAN)

## IEEE 802.15.4 (LR-PAN)

- LR-WPAN: Low Rate Wireless Personal Area Network.
- Simple, Low-Cost Communication network.
- Applicable with limited power and relaxed throughput requirement.

## IEEE 802.15.4: Characteristics

- Data Rates: 250kb/s, 100kb/s, 40kb/s & 20kb/s.
- Star or Peer-to-peer Operations
- Allocated 16-bit short or 64-bit extended addresses.
- Optional allocation of Guaranteed Time Slots(GTS)
- CSMA-CA Channel Access

## IEEE 802.15.4: Characteristics Cont.

- Fully acknowledged protocol for transfer reliability.
- Low power consumption
- Energy Detection(ED)
- Link Quality indication

# Frequency Band & Channels

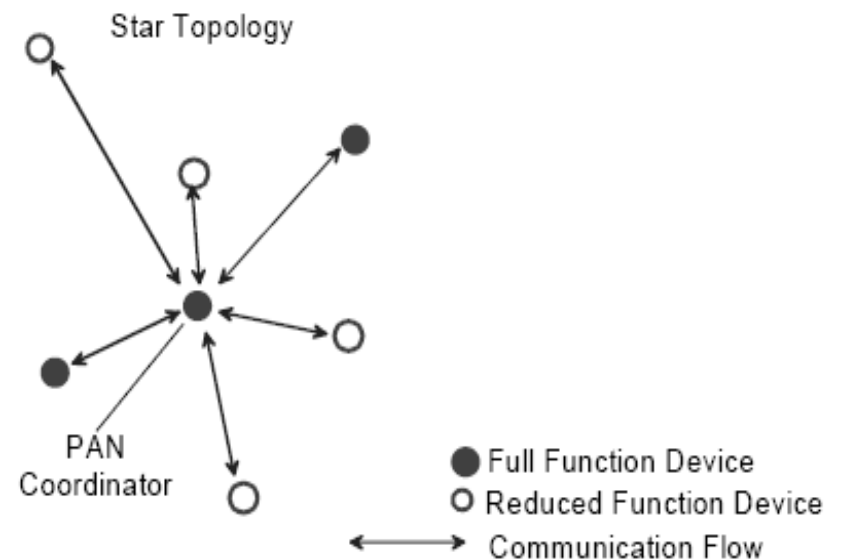
- 16 channels in 2450 MHz band.
- 30 channels in 915 MHz Band.
- 3 channels in 868 MHz Band

# Components of IEEE 802.15.4

- FFD: Full Function Device
  - 3 modes of serving
    - PAN Coordinator
    - Coordinator
    - A device
- RFD: Reduced Function Device
  - A device

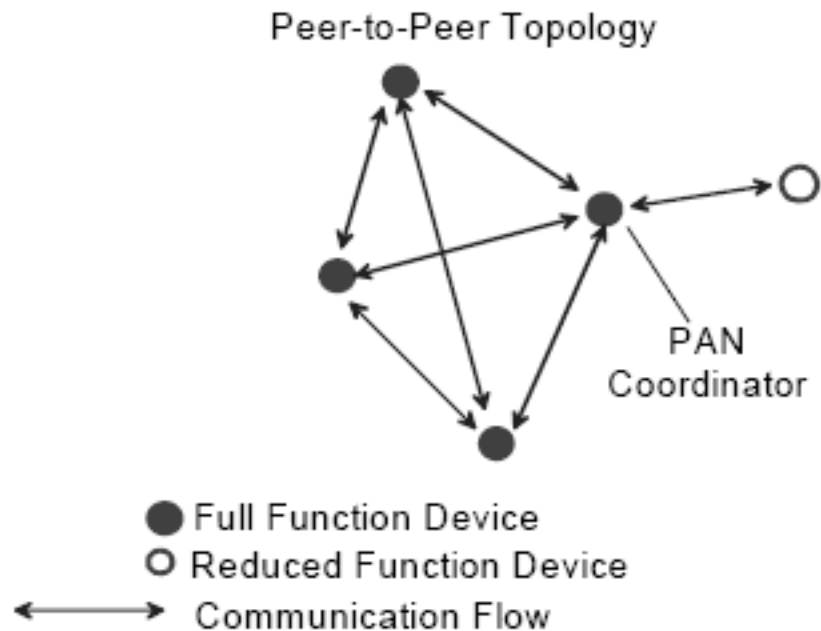
# Network Topologies

- Star Topology
  - Devices connected to single central controller known as PAN coordinator.
  - Pan coordinator: used to initiate, terminate or route communication around network.
  - Device is either initiation Point or Termination Point.

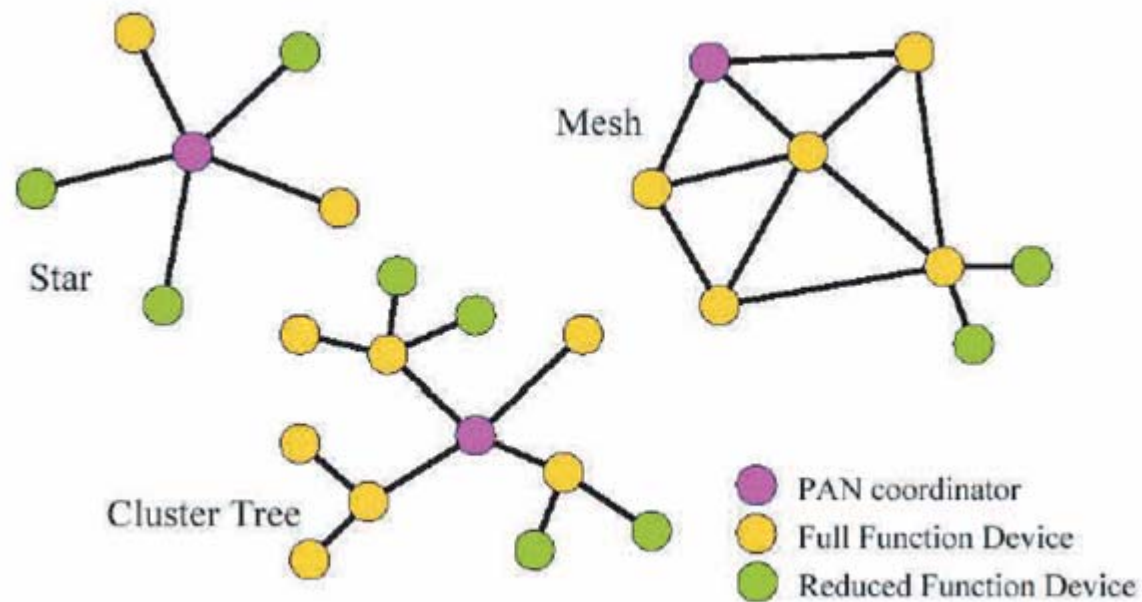


# Network Topologies Cont.

- Peer-To-Peer Network
  - Allows complex network formation.
  - Any device can communicate to any other device.
  - One device nominated as PAN Coordinator.
  - Example: Cluster tree.



# Cluster Tree



# Architecture

- Defined in terms of layers
- Each layer is responsible for one part of standard
- Each layer provide the service to the upper layer

## Architecture Cont.

- It comprises of 2 Layer
- PHY: RF transceiver with low-level control mechanism
- MAC: Provides the access to Physical channel for transfers

# PHY: Physical Layer

- Provides 2 services.
  - PHY data service
  - PHY management service
- Features:
  - Radio Transceiver: Activation and Deactivation
  - Energy Detection
  - Link Quality Indication

# MAC Sublayer

- Provides 2 Services
  - MAC Data Service
  - MAC Management Service
- Features:
  - Beacon management
  - Channel access
  - GTS Management
  - Frame validation

# Functional Overview

- Superframe Structure
  - Optional
  - Format definition: by Coordinator
  - Bounded by network beacons with 16 equally sized slots.
  - Optional: active portion or inactive portion
  - Devices use CSMA-CA to communicate during the Contention Access Period (CAP).

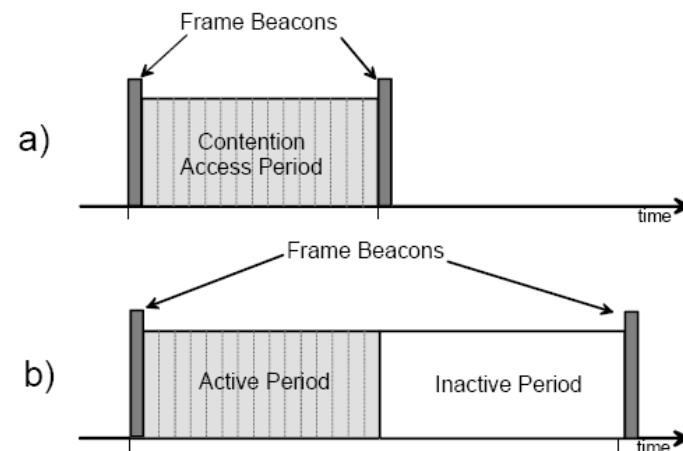


Figure 4—Superframe structure without GTSSs

# Functional Overview Cont.

- Superframe Structure
  - With GTS:
    - For low-latency applications.
    - Includes Contention Free Period (CFP).
    - CFP has Guaranteed time slots

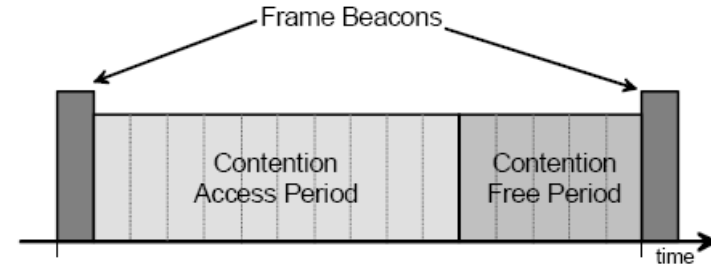


Figure 5—Superframe structure with GTSs

# Functional Overview Cont.

- Data Transfer Model
  - Data transfer to coordinator.
  - Data transfer from a coordinator
  - Peer-To-Peer data transfer

# Data Transfer to Coordinator

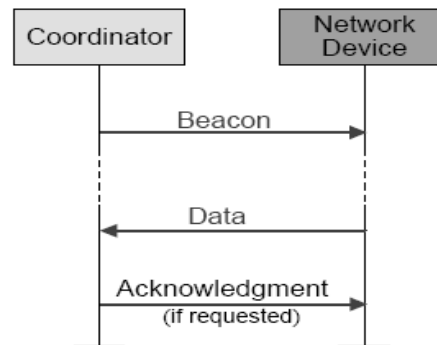


Figure 6—Communication to a coordinator in a beacon-enabled PAN

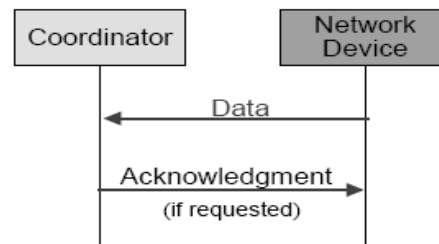


Figure 7—Communication to a coordinator in a nonbeacon-enabled PAN

# Data Transfer from Coordinator

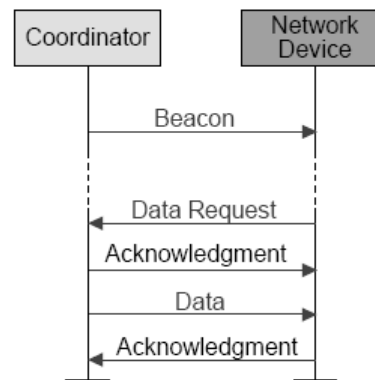


Figure 8—Communication from a coordinator a beacon-enabled PAN

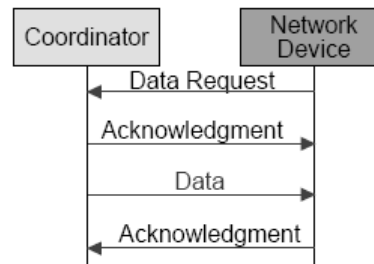


Figure 9—Communication from a coordinator in a nonbeacon-enabled PAN

# Peer to Peer Data Transfer

- Device may communicate with every other device in its radio sphere.
- Two types of communication style
  - Asynchronours: Receive Constantly using unslotted CSMA-CA.
  - Synchronise: Duty cycle to save power, still use CSMA-CA with each other.

# Improving Reliability

- Mechanisms to improve data transmission
  - CSMA-CA
  - Frame Acknowledgement
  - Data Verification: 16 bit ITU-T Cyclic Redundancy Check.

# Security

- Cryptographic mechanisms:
  - Symmetric-key cryptography
  - Keys: Provided by higher layers.
    - Link key
    - Network key
  - Services:
    - Data Confidentiality
    - Data Authenticity
    - Replay Protection

# Summary

- Zigbee Routing Layer
  - Routing layer on top of PHY and MAC, enabling support for the “star and peer-to-peer” network topologies

## IEEE 802.15.4 WPAN

- Defines standard for low power, low data rate networks
- Defines network topologies that should be supported
- IEEE 802.15.4 PHY
  - Physical layer specification of standard
- IEEE 802.15.4 MAC
  - MAC specification of standard

# References

- Wikipedia article, [ZigBee Specification](#).
- IEEE LAN/MAN Standards Committee, IEEE 802.15.4 Standard.

**Thank You**

**QUESTIONS?**