

Sensor Networks

Part 2: ZigBee and IEEE 802.15.4

CATT Short Course, March 11, 2005

Mark Coates

Mike Rabbat

1

IEEE 802.15.4



- Low data-rate solution
- Long (multi-month, multi-year) battery life
- Very low complexity (cheap)
- Wireless Personal Area Networks (WPANs) – short distances
- Unlicensed, international frequency band
- Sensor, smart badges, remote controls, home automation → sensor networks

Part 2: 2

IEEE 802.15.4



- CSMA-CA (Carrier sense multiple access with collision avoidance)
- Supports star and peer-to-peer topologies
- Media-access generally contention based
- PAN coordinator
 - Provides connectivity to higher performance networks
 - Can allocate time slots to devices with time-critical data

Part 2: 3

IEEE 802.15.4 Standard



- Defines physical layer (PHY)
- Provides specifications for media access control (MAC) sublayer
- Fixed, portable and moving devices with no battery or very limited battery consumption requirements
- Devices typically operating in the personal operating space (POS) of 10m
- Longer range at lower data rate may be possible
- Raw data rate - scalable from 20 kb/s or below (sensor and automation) to 250 kb/s

Part 2: 4

LR-WPAN



- Low-rate wireless personal area network
- Objectives
 - easy installation
 - reliable data transfer
 - extremely low cost
 - reasonable battery life
 - simple and flexible protocol

Part 2: 5

LR-WPAN Characteristics



- Data rates of 250, 40 and 20 kb/s
- Star or peer-to-peer operation
- 16 bit or 64 bit addresses
- Allocation of guaranteed time slots
- CSMA-CA
- Fully acknowledged protocol for reliable data transfer
- Low power consumption
- Energy detection
- Link quality indication
- 16 channels in 2450 MHz band, 10 in 915 MHz band, 1 in 868 MHz band

Part 2: 6

LR-WPAN Devices



- Two types of device
 - Full-function (FFD) and reduced-function (RFD)
- FFD
 - Can serve as a PAN coordinator, a coordinator or a device.
 - FFD can talk to RFDs or other FFDs;
- RFD
 - can only talk to FFDs
 - Intended for extremely simple applications (sensors relaying small amounts of data)
 - Can be implemented using minimal resources & memory

Part 2: 7

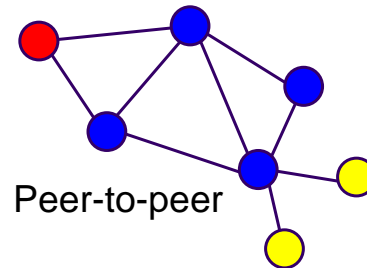
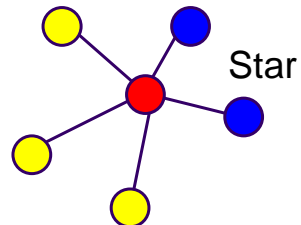
PAN Coordinator






- Most basic component is device (FFD or RFD)
- Network includes at least one FFD that operates as the PAN coordinator
- PAN coordinator
 - Can initiate, terminate or route communication
 - Can allocate short addresses (16 bit) to devices
 - In star topology, devices communicate solely with the PAN coordinator

Part 2: 8

Network Topologies



-  PAN Coordinator
-  Full Function Device (FFD)
-  Reduced Function Device (RFD)

Part 2: 9

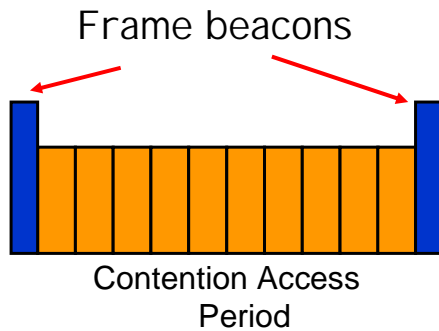
WPAN Architecture



- PHY:
 - Radio frequency (RF) Transceiver
 - Low-level control mechanism
- MAC sublayer:
 - Access to physical channel for all types of transfer

Part 2: 10

Superframe structure



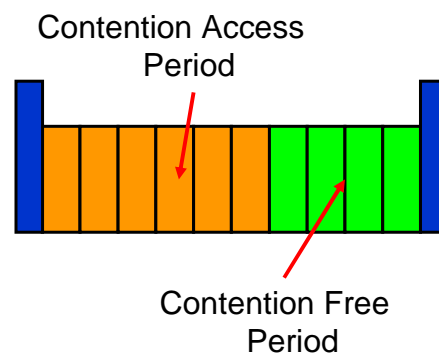
- Superframe bounded by network beacons
- Beacons used to:
 - Synchronize devices
 - Describe superframe structure
 - Identify PAN
- Devices compete using CSMA-CA during contention access period

Part 2: 11

Superframe structure



- PAN coordinator can provide guaranteed time slots (GTSS) to devices
- GTSS form a contention free period - always at end of superframe
- Up to 7 GTSS - each may occupy more than one slot



Part 2: 12

Data transfer model



- Three types of data transfer
 - Device transmits to coordinator
 - Coordinator transmits to device
 - Peer-to-peer transfer
- Device to coordinator
 - In a beacon-enabled PAN
 - Device listens for network beacon
 - Synchronizes to superframe structure
 - Transmits data frame using **slotted** CSMA-CA
 - Nonbeacon-enabled PAN
 - Transmits data frame using **unslotted** CSMA-CA
 - Coordinator acknowledges using optional acknowledgement frame

Part 2: 13

Data transfer model



- Coordinator to device (beacon-enabled)
 - Coordinator indicates in beacon that data message is pending
 - Device listens to network beacon and, if message is pending, transmits a MAC command requesting data using slotted CSMA-CA
 - Coordinator acknowledges reception of data request using optional acknowledgement frame
 - Coordinator sends data frame using slotted CSMA-CA
 - Device acknowledges with acknowledgement frame
 - Message removed from list of pending messages on beacon

Part 2: 14

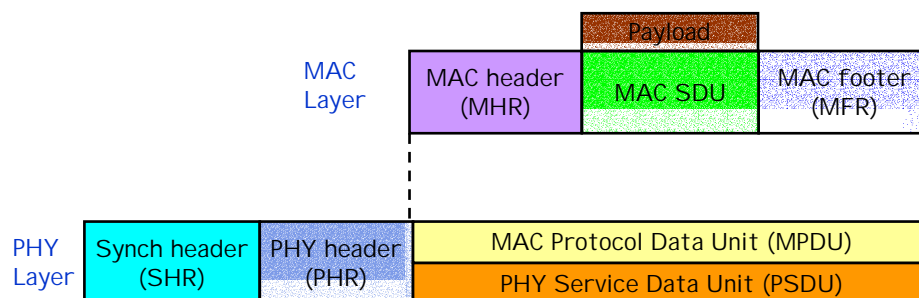
Data transfer model



- Coordinator to device (no beacon)
 - Coordinator stores data and waits for device to make contact and request data
 - Device makes contact by transmitting a MAC command requesting the data, using unslotted CSMA-CA at an application-defined rate
 - Coordinator acknowledges request
 - If data pending, coordinator transmits data using unslotted CSMA-CA.
 - If no data pending, coordinator transmits zero-length payload
 - Device acknowledges receipt of data

Part 2: 15

Frame structure



- Four types of frame
 - Beacon frames
 - Data frame
 - Acknowledgement Frame
 - MAC Command Frame

Part 2: 16

PHY Layer



PHY	Frequency band	Data parameters			Spreading parameters	
		Bit rate (kb/s)	Symbol rate (kbaud)	Modulation	Chip rate (Mchips/s)	Modulation
868/915	868.0–868.6 MHz	20	20	BPSK	0.3	BPSK
MHz PHY	902.0–928.0 MHz	40	40	BPSK	0.6	BPSK
2.4 GHz PHY	2.4–2.4835 GHz	250	62.5	16-ary orthogonal	2.0	O-QPSK

- Frequency bands and data rates

Part 2: 17

2450 MHz



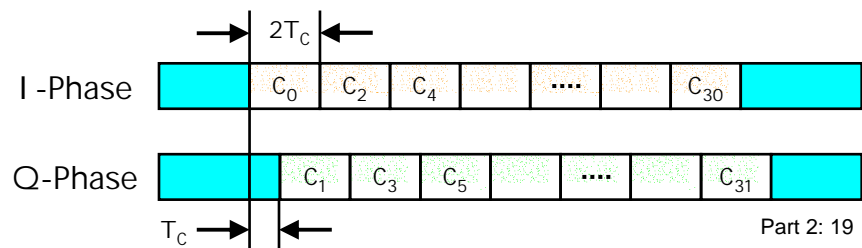
- Data rate = 250 kb/s
- 16-ary quasi-orthogonal modulation
 - During each data symbol period, four information bits select one of 16 nearly orthogonal pseudo-random noise (PN) sequences
 - PN sequences are concatenated
 - Aggregate chip sequence modulated onto carrier using offset quadrature phase-shift keying (O-QPSK)

Part 2: 18

O-QPSK



- Half-sine pulse shaping
- Even indexed chips modulated onto in-phase (I) carrier
- Odd-indexed chips modulated onto quadrature-phase (Q) carrier
- Q-phase chips are offset by T_c



868/915 MHz



- 20 kb/s in 868 MHz band
- 40 kb/s in 915 MHz band
- Direct sequence spread spectrum (DSSS)
- Binary phase-shift keying (BPSK) for chip modulation
- Differential encoding for data symbols

Part 2: 20

Robustness



- CSMA-CA for channel access
- Frame acknowledgement
- Security

Part 2: 21

Frame Acknowledgement



- Optional acknowledgements
 - Confirm successful reception and validation
- If originator does not receive and acknowledgement
 - assumes transmission was unsuccessful
 - If no acknowledgement after several retries, originator can choose to terminate transaction
- 16-bit ITU Cyclic Redundancy Check (CRC) for each frame

Part 2: 22

CSMA-CA



- **Nonbeacon-enabled (Unslotted)**
 - Device that wishes to transmit waits for a random period
 - If channel is idle, it transmits. Otherwise, it waits for another random period.
 - Acknowledgement frames do not use CSMA-CA
- **Beacon-enabled (Slotted CSMA-CA)**
 - Backoff slots aligned with start of beacon transmission
 - Device locates boundary of next backoff slot, then waits for a random number of slots
 - Channel busy: wait for another random number of slots
 - Channel idle: transmit on next available slot boundary
 - Acknowledgment and beacon frames do not use CSMA-CA

Part 2: 23

Security



- Symmetric-keys
 - keys provided by higher layer processes
- Access control
 - device maintains list of devices in its **Access Control List (ACL)** from which it expects to receive frames.
- Data encryption
 - Encryption of beacon, data and command payloads
 - Key may be shared by group of devices or two peers
- Frame integrity
 - Message integrity code (MIC) protects data from being modified by third parties
 - Integrity on beacon, data and command frames

Part 2: 24

Security



- Sequential freshness
 - Ordered sequence of inputs to reject replayed frames
 - Frame received -> compare freshness value with last known value
 - Must be a more recent value for check to pass
- Security modes
 - Unsecured
 - ACL : access control, but limited security
 - Secured : access control, data encryption, frame integrity, sequential freshness

Part 2: 25

Zigbee



- Wireless networking standard addressing the needs of sensors and control devices
- Low latency, very low energy consumption
- Large number of devices

Part 2: 26

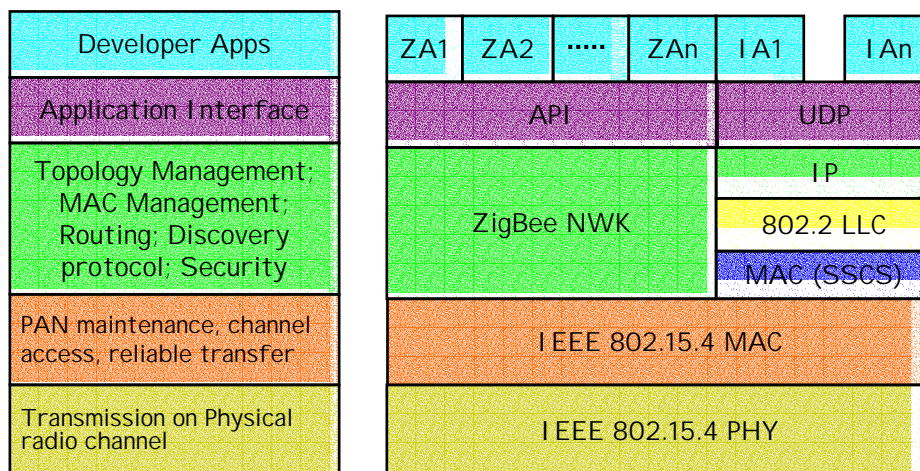
Zigbee Features



- Low power consumption
- Two power modes: **active** (transmit/receive) and **sleep**
- Low device cost, low installation cost, minimal maintenance
- Relatively small protocol stack
- Optimized for low duty-cycle applications (< 1 percent)
- Address space allows high density of nodes
 - 64 bit IEEE addresses
 - 16 bit network addresses
- Range: typically 50 m, (5-500m)

Part 2: 27

Zigbee Stack



Part 2: 28

Zigbee



- Physical layer: IEEE 802.15.4
 - Low-cost, but permits high degree of integration
 - Direct sequence spread spectrum allows simple analog circuitry and inexpensive implementations
- MAC layer (enhanced 802.15.4)
 - Allows multiple topologies
 - Reduced functionality devices (RFDs) for the low-power sensor devices
 - Handle networks with large numbers of devices
- Network Layer
 - Allow spatial growth without high-power transmission
 - Permit many nodes with relatively low latency

Part 2: 29

Traffic types



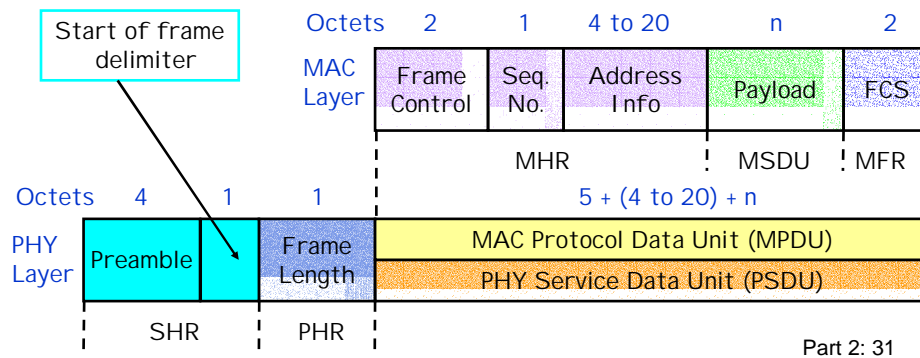
- Periodic data
 - Use beaconing system; devices wake up to check for messages
- Intermittent data
 - Response to external stimulus
 - Beaconless or disconnected system
 - Disconnected operation: device only attaches to network when it needs to communicate
- Low latency data
 - Guaranteed time-slot option
 - No contention, less variable latency

Part 2: 30

Data Frame



- Overhead of 15-31 octets (min. 120 bits)
 - Depends on use of short or long addressing



Zigbee Security – MAC layer



- MAC layer security for single-hop MAC command, beacon and acknowledgement frames
- AES (Advanced Encryption Standard) as core cryptographic system
- When MAC layer transmits a frame with security enabled, it
 - Retrieves key associated with destination
 - Processes frame using this key according to security suite associated with that key
- Upper layer selects and manages keys and security level
- MAC frame header has bit indicating whether security is enabled

Part 2: 32

Zigbee Security – MAC Layer



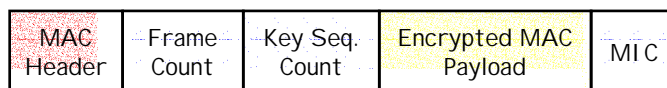
- Integrity
 - MAC header and payload used to create a Message Integrity Code (MIC) consisting of 4, 8 or 16 octets
 - MIC is right-appended to MAC payload
- If confidentiality required
 - Frame and sequence counts (nonce) left-appended
 - Nonce prevents replay attacks
- Upon receipt,
 - MIC verified and payload decrypted
 - Sending devices increment frame count
 - Receiving devices keep track of last frame received

Part 2: 33

Zigbee Security – MAC Layer



- Security Suites
 - Three modes of operation
 - 1) Encryption at MAC layer
 - AES in Counter (CTR) mode
 - 2) Authentication (Integrity)
 - AES in Cipher Block Chaining (CBC-MAC) mode
 - 3) Combination of Encryption and Integrity
 - AES in Counter with CBC-MAC (CCM) mode



4 bytes 1 byte

Part 2: 34

Zigbee Security – Network Layer



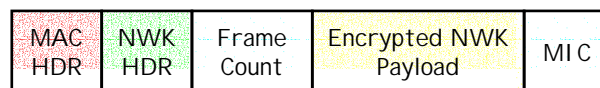
- Network Layer also makes use of AES
- All security suites based on CCM* mode of operation
 - CCM* offers both encryption-only and integrity-only capabilities
 - Allows single key to be used for multiple suites
 - Application can specify the security suite to apply to each NWK frame

Part 2: 35

Zigbee Security – Network Layer



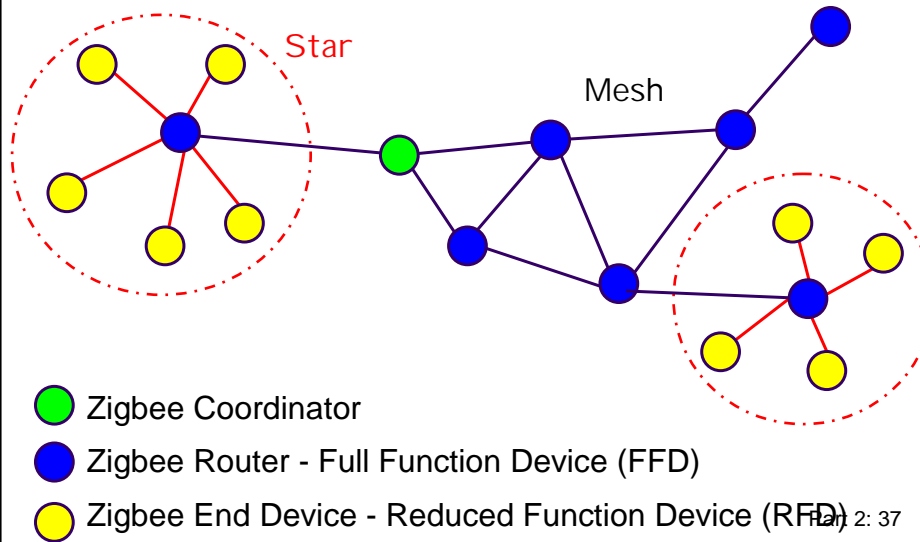
- When NWK layer transmits a frame
 - Uses the Security Services Provider (SSP) to process frame
 - SSP retrieves key associated with destination
 - Applies security suite to the frame
- SSP primitives for applying/removing security
- NWK layer responsible for security processing
- Upper layers set up keys and determine the CCM* suite to apply



4 bytes

Part 2: 36

Zigbee Network Model



ZigBee Coordinator



- Sets up network
- Transmits network beacons
- Manages network nodes
- Stores network node information
- Routes messages between pairs of nodes
- Typically operates in the receive state

Part 2: 38

ZigBee Network Node



- Designed for low energy usage
- Searches for available networks
- Transfers data from its application when necessary
- Determines whether data is pending
- Requests data from network coordinator
- Can sleep for extended periods

Part 2: 39

ZigBee Stack



- 8-bit microcode
- Full protocol stack < 32K
- RFD stack ~ 6K
- Coordinators require extra RAM
 - Node device database, transaction table, pairing table

Part 2: 40

ZigBee Network Layer



- Responsibilities
 - Starting network
 - Joining and leaving network
 - Configuring a new device
 - Addressing - assign addresses to devices joining the network
 - Synchronization - tracking beacons or polling
 - Security
 - Routing

Part 2: 41

ZigBee Routing



- Default routing is tree-based
 - Routers don't have to maintain extensive tables or perform route discovery
 - Paths can be longer than necessary - extra traffic, more likely to fail
- Routers have capability to discover shortcuts
 - Maintain table of form (D,N) - (destination, next device)
 - Request/response protocol for shortcut discovery based on Ad-hoc On Demand Distance Vector (AODV) protocol
- Combination of AODV, Motorola's Cluster-Tree algorithm and Ember Corporations GRAd.

Part 2: 42

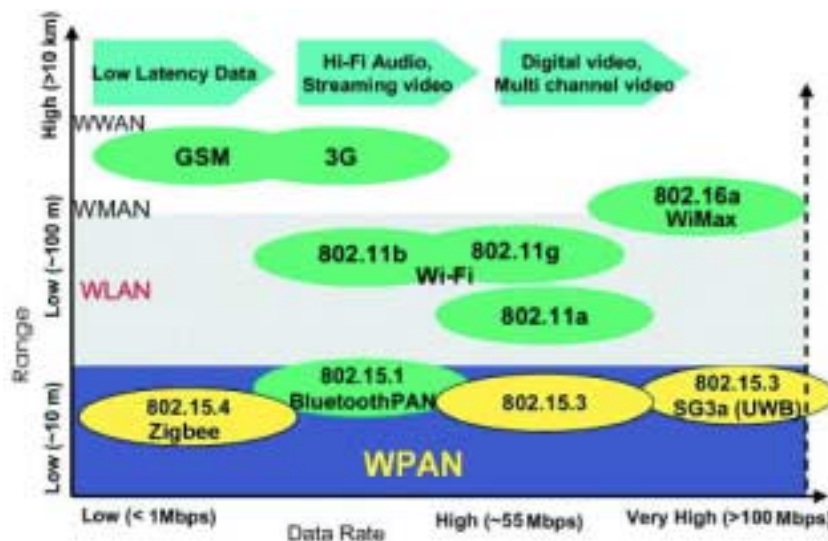
ZigBee Application Layer



- Application-specific code incorporating hardware devices
- Written into ZigBee device object (ZDO)
- In ZDO, specify:
 - function of device within Zigbee framework
 - how to respond to events & system messages
 - whether FFD or RFD, type of network layer security
- Application support sublayer
 - Handles binding and discovery
 - Binding: match devices based on form of interaction
 - Relays messages between devices that cannot talk directly

Part 2: 43

ZigBee position in wireless standard spectrum



ZigBee vs Bluetooth



- ZigBee
 - Smaller packets over large network
 - Primarily static
 - Many, infrequently used devices
 - Home automation, sensors, remote controls...
 - Device batteries rarely replaced or charged
 - Small fraction of host power
- Bluetooth
 - Larger packets over small network
 - Ad-hoc networks
 - File transfer
 - Screen graphics, pictures, mobile phones, PDAs, etc...
 - Expects regular charging of devices
 - Devices <10 % of host power

Part 2: 45

ZigBee vs Bluetooth



- ZigBee
 - DSSS - 11 chips/symbol
 - 62.5 K symbol/s
 - 4 bits/symbol
 - Peak information rate ~ 128 Kbit/s
- Bluetooth
 - FHSS
 - 1 M symbol/s
 - Peak information rate ~ 720 Kbit/s

Part 2: 46

ZigBee vs Bluetooth



- ZigBee
 - DSSS
 - 62.5 K symbol/s
 - 4 bits/symbol
 - Peak information rate ~ 250 Kbit/s
 - Network join time = 30 ms
 - Sleeping slave changing to active = 15 ms
 - Active slave channel access time = 15 ms
- Bluetooth
 - FHSS
 - 1 M symbol/s
 - Peak information rate ~ 720 Kbit/s
 - Network join time = 3 s
 - Sleeping slave changing to active = 2 s
 - Active slave channel access time = 2 ms

Part 2: 47