ZigBee/IEEE 802.15.4 Overview
New trend of wireless technology

- Most wireless industry focus on increasing high data throughput
- A set of applications requiring simple wireless connectivity, relaxed throughput, very low power, short distance and inexpensive
  - Industrial
  - Agricultural
  - Vehicular
  - Residential
  - Medical
ZigBee/802.15.4 Architecture

- IEEE 802.15.4
  - Defines lower layers of protocol stack: MAC and PHY
- ZigBee Specification
  - Defines upper layers of protocol stack: from network to application, including application profiles
IEEE 802.15 Working Group
## Comparison Between WPANs

**Wireless Personal Area Networks**

<table>
<thead>
<tr>
<th>Project</th>
<th>Data Rate</th>
<th>Range</th>
<th>Configuration</th>
<th>Other Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.15.1 (Bluetooth)</td>
<td>1 Mbps</td>
<td>10M (class 3)</td>
<td>8 active device Piconet/Scatternet</td>
<td>Authentication, Encryption, Voice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100M (class 1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.15.3 High Rate</td>
<td>22, 33, 44, 55 Mbps</td>
<td>10M</td>
<td>256 active device Piconet/Scatternet</td>
<td>FCC part 15.249 QoS, Fast Join Multi-Media</td>
</tr>
<tr>
<td>802.15.4 Low Rate</td>
<td>up to 250Kbps</td>
<td>10M nominal 1M-100M based on settings</td>
<td>Master/Slave (256 Devices or more) Peer to Peer</td>
<td>Battery Life: multi-month to infinite</td>
</tr>
<tr>
<td>802.15.2 Coexistence</td>
<td>Develop a Coexistence Model and Mechanisms Document as a Recommended Practice</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


What is ZigBee Alliance?

- An organization with a mission to define reliable, cost effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- Alliance provides interoperability, certification testing, and branding

ZigBee™ Alliance
Wireless Control That Simply Works
How is ZigBee related to IEEE 802.15.4?

- ZigBee takes full advantage of a powerful physical radio specified by IEEE 802.15.4
- ZigBee adds logical network, security and application software
- ZigBee continues to work closely with the IEEE to ensure an integrated and complete solution for the market
ZigBee/IEEE 802.15.4 market feature

- Low power consumption
- Low cost
- Low offered message throughput
- Supports large network orders (≤ 65k nodes)
- Low to no QoS guarantees
- Flexible protocol design suitable for many applications
ZigBee Network Applications

**ZigBee**
LOW DATA-RATE RADIO DEVICES

- **PERSONAL HEALTH CARE**
  - monitors
  - diagnostics
  - sensors

- **INDUSTRIAL & COMMERCIAL**
  - automation
  - control

- **TOYS & GAMES**
  - consoles
  - portables
  - educational

- **HOME AUTOMATION**
  - security
  - HVAC
  - lighting
  - closures

- **PC & PERIPHERALS**
  - mouse
  - keyboard
  - joystick

- **CONSUMER ELECTRONICS**
  - TV
  - VCR
  - DVD/CD
  - Remote control
Wireless Technologies

- **GSM**
- **GPRS**
- **EDGE**
- **3G**
- **802.11b**
- **ZigBee**
- **802.11a/g**
- **Hiper LAN/2**
- **Bluetooth 1.5**
- **Bluetooth 2.0**
- **WiMedia**

**Bandwidth (kbps)**: 10, 100, 1,000, 10,000, 100,000

**Range (Meters)**: 10, 100, 1,000, 10,000

Years:
- 2000
- 2003-4
- 2005
IEEE 802.15.4 Overview
General Characteristics

- Data rates of 250 kbps, 20 kbps and 40 kbps.
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- CSMA/CA channel access.
- Dynamic device addressing.
- Fully handshaked protocol for transfer reliability.
- Low power consumption.
- 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz ISM band and one channel in the European 868MHz band.
- Extremely low duty-cycle (<0.1%)
IEEE 802.15.4 Basics

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
  - Channel Access is via CSMA/CA and optional time slotting
  - Message acknowledgement and an optional beacon structure
  - Multi-level security
  - Works well for
    - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics
    - Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries
IEEE 802.15.4 Physical Layer
IEEE 802.15.4 PHY Overview

- PHY 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
IEEE 802.15.4 PHY Overview

- Operating frequency bands

**868MHz/915MHz PHY**

Channel 0

- 868.3 MHz

Channels 1-10

- 902 MHz to 928 MHz
- 2 MHz

**2.4 GHz PHY**

Channels 11-26

- 2.4 GHz to 2.4835 GHz
- 5 MHz
The standard specifies two PHYs:

- **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
PHY Frame Structure

- **PHY packet fields**
  - **Preamble** (32 bits) – synchronization
  - **Start of packet delimiter** (8 bits) – shall be formatted as “11100101”
  - **PHY header** (8 bits) – PSDU length
  - **PSDU** (0 to 127 bytes) – data field

<table>
<thead>
<tr>
<th>Sync Header</th>
<th>PHY Header</th>
<th>PHY Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
<td>Start of Packet Delimiter</td>
<td>Frame Length (7 bit)</td>
</tr>
<tr>
<td>4 Octets</td>
<td>1 Octets</td>
<td>1 Octets</td>
</tr>
</tbody>
</table>

- **PHY Service Data Unit (PSDU)**

0-127 Octets
IEEE 802.15.4 MAC
IEEE 802.15.4 Device Types

- Two different device types:
  - A full function device (FFD)
  - A reduced function device (RFD)
- FFDs can operate in three modes serving
  - End device
  - Coordinator
  - PAN coordinator
- RFDs can only operate in a mode serving END device
FFD vs. RFD

- Full function device (FFD)
  - Any topology
  - Network coordinator capable
  - Talks to any other device

- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Talks only to a network coordinator
  - Very simple implementation
Device Addressing

- Two or more devices communicating on the same physical channel constitute a WPAN which includes at least one FFD (PAN coordinator).
- Each independent PAN will select a unique PAN identifier.
- All devices operating on a network shall have unique 64-bit extended address. This address can be used for direct communication in the PAN.
- An associated device can use a 16-bit short address, which is allocated by the PAN coordinator when the device associates.
Star Topology

Master/slave

Network coordinator

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

Communications Flow
Mesh and Tree Topology

Mesh

Tree

Full Function Device (FFD)

Communications Flow
Combined Topology

Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

- Full function device
- Reduced function device can only be terminal nodes

Communications flow
IEEE 802.15.4 MAC Overview

General Frame Structure

4 Types of MAC Frames:

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame
IEEE 802.15.4 MAC Overview
Traffic Types

- Periodic data
  - Application defined rate (e.g. sensors)

- Intermittent data
  - Application/external stimulus defined rate (e.g. light switch)

- Repetitive low latency data
  - Allocation of time slots (e.g. mouse)
A superframe is divided into two parts

- **Inactive**: all devices sleep
- **Active**: Consists of 16 slots; can be further divided into two parts
  - Contention access period (CAP)
  - Contention free period (CFP)
Beacons are used for
- starting superframes
- synchronizing with associated devices
- announcing the existence of a PAN
- informing pending data in coordinators

In a beacon-enabled network,
- Devices use slotted CAMA/CA to contend for the usage of channels
- FFDs which require fixed rates of transmissions can ask for guarantee time slots (GTS) from the coordinator
Beacon Order and Superframe Order

The structure of superframes is controlled by two parameters: beacon order (BO) and superframe order (SO)

- BO decides the length of a superframe
- SO decides the length of the active portion in a superframe

\[
SD = a_{\text{BaseSuperFrameDuration}} \times 2^{SO}
\]

For channels 11 to 26, \(a_{\text{BaseSuperFrameDuration}}=5.36\) ms

\[
BI = a_{\text{BaseSuperFrameDuration}} \times 2^{BO}
\]
Duty Cycle

- For a beacon-enabled network, the setting of BO and SO should satisfy the relationship $0 \leq SO \leq BO \leq 14$

- **Duty cycle** = the ratio of active period to the whole superframe duration $= 2^{-(BO-SO)}$

- Each device will be active for $2^{-(BO-SO)}$ portion of the time, and sleep for $1-2^{-(BO-SO)}$ portion of the time

<table>
<thead>
<tr>
<th>BO-SO</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>≥10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duty cycle (%)</td>
<td>100</td>
<td>50</td>
<td>25</td>
<td>12</td>
<td>6.25</td>
<td>3.125</td>
<td>1.56</td>
<td>0.78</td>
<td>0.39</td>
<td>0.195</td>
<td>&lt; 0.1</td>
</tr>
</tbody>
</table>
Channel access mechanism

- Two types:
  - In non beacon-enabled networks
    - unslotted CSMA/CA channel access mechanism
  - In beacon-enabled networks
    - slotted CSMA/CA channel access mechanism

- Based on a basic time unit called **Backoff Period** (BP)
  - $= aUnitBackoffPeriod = 80$ bits (0.32 ms)
Unslotted/Slotted CSMA/CA Algorithm

- Each device shall maintain two variables for each transmission attempt
  - **BE**: the backoff exponent which is related to how many BPs a device shall wait before attempting to assess a channel
  - **NB**: number of time the CSMA/CA algorithm was required to backoff while attempting the current transmission

- Additional one variable for slotted CSMA/CA
  - **CW**: contention window length, the number of BPs that needs to be clear of channel activity before transmission can commence (initial to 2 and reset to 2 if sensed channel to be busy)
Unslotted CSMA/CA

CSMA-CA

Slotted?

No

NB = 0,
BE = max-MinBE

Delay for random(2^{BE} - 1) unit backoff periods

Perform CCA

Channel idle?

Y

N

NB = NB + 1,
BE = min(BE + 1, aMaxBE)

N

Y

Failure

Success
The backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries of the PAN coordinator.

- i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission.
- The MAC sublayer shall ensure that the PHY layer commences all of its transmissions on the boundary of a backoff period.
Illustrating Slotted CSMA/CA

Slot boundary

\[ \text{random}(2^{\text{BE}} - 1) \times \text{BP} \]

\[ \text{CW} \times \text{BP} \]

\[ \text{CW} = 0 \]

One CAP slot

Slot boundary
Slotted CSMA/CA

CSMA-CA

Slotted? Yes

NB = 0, CW = 2

Yes

Battery life extension? Yes

BE = min(2, macMinBE)

No

BE = macMinBE

locate backoff period boundary

(2) Delay for random(2BE - 1) unit backoff periods

(3) Perform CCA or backoff period boundary

Channel idle? Y

(4) CW = 2, NB = NB + 1, BE = min(BE + 1, aMaxBE)

N

NB > macMaxCSMAbackoff?

Y Failure

No CW = 0?

Y Success

N
GTS concepts

- A guaranteed time slot (GTS) allows a device to operate on the channel within a portion of the superframe.
- A GTS shall only be allocated by the PAN coordinator.
- The PAN coordinator can allocate up to seven GTSs at the same time.
- The PAN coordinator decides whether to allocate GTS based on:
  - Requirements of the GTS request
  - The current available capacity in the superframe.
A GTS can be deallocated
- At any time at the discretion of the PAN coordinator or
- By the device that originally requested the GTS

A device that has been allocated a GTS may also operate in the CAP

A data frame transmitted in an allocated GTS shall use only short addressing

The PAN coordinator shall be able to store the info of devices that necessary for GTS, including starting slot, length, direction and associated device address
Before GTS starts, the GTS direction shall be specified as either transmit or receive.

Each device may request one transmit GTS and/or one receive GTS.

A device shall only attempt to allocate and use a GTS if it is currently tracking the beacon.

If a device loses synchronization with the PAN coordinator, all its GTS allocations shall be lost.

The use of GTSs by an RFD is optional.
Association procedures

- A device becomes a member of a PAN by associating with its coordinator
- Procedures

Diagram:

- Coordinator
- Device
- Association req.
- ACK
- Make decision
- Beacon (pending address)
- Data req.
- ACK
- Association resp.
- Ack
- Scan channel
- Wait for response
Association Procedures

- In IEEE 802.15.4, association results are announced in an indirect fashion.
- A coordinator responds to association requests by appending devices’ long addresses in beacon frames.
- Devices need to send a data request to the coordinator to acquire the association result.
- After associating to a coordinator, a device will be assigned a 16-bit short address.
In a beacon-enabled network, device finds the beacon to synchronize to the superframe structure. Then using slotted CSMA/CA to transmit its data.

Communication to a coordinator
In a beacon-enabled network
Data transfer model (device to coordinator)

- In a non beacon-enabled network, device simply transmits its data using unslotted CSMA/CA
In a **beacon-enabled network**

- the coordinator indicates in the beacon that the data is pending.
- Device periodically listens to the beacon and transmits a MAC command request using slotted CSMA/CA if necessary.
Data transfer model (coordinator to device)

- In a non beacon-enabled network
  - a device transmits a MAC command request using unslotted CSMA/CA.
  - If the coordinator has its pending data, the coordinator transmits data frame using unslotted CSMA/CA.
  - Otherwise, coordinator transmits a data frame with zero length payload.
ZigBee Network Layer Protocols
ZigBee network layer overview

- ZigBee network layer provides reliable and secure transmissions among devices
- Three kinds of networks are supported: **star**, **tree**, and **mesh** networks
ZigBee network layer overview

- Three kinds of devices in the network layer
  - ZigBee coordinator (ZC): response for initializing, maintaining, and controlling the network
  - ZigBee router (ZR): form the network backbone
  - ZigBee end device (ZED)

- In a tree network, the coordinator and routers can announce beacons.
- In a mesh network, regular beacons are not allowed.
  - Devices in a mesh network can only communicate with each other by peer-to-peer transmissions
Topological Parameter (Lm, Cm, Rm) for a ZigBee Tree

- ZigBee coordinator determines three network parameters:
  - \(Lm\): the maximum depth value of the tree.
  - \(Cm\): the maximum number of children of a ZC/ZR.
  - \(Rm\): the maximum number of children of a ZC/ZR that can be ZRs.

Example: \(Lm = 3\)

devices at depth \(Lm\) can only be ZEDs

depth = 0
Distributed Address Assignment Mechanism (DAAM)

- A parent device utilizes $C_m$, $R_m$, and $L_m$ to compute a parameter called $C_{skip}$
  - which is used to compute the size of its children’s address pools

$$C_{skip}(d) = \begin{cases} 
1 + C_m \cdot (L_m - d - 1), & \text{if } R_m = 1 \quad \cdots \cdots (a) \\
1 + C_m - R_m - C_m \cdot R_m^{L_m - d - 1}, & \text{Otherwise } \quad \cdots \cdots (b) \\
\frac{1 - R_m}{1 - R_m} & 
\end{cases}$$

The depth value of the parent
If a parent node at depth $d$ has an address $A_{\text{parent}}$,

- the $n$th child router is assigned to address $A_{\text{parent}} + (n-1) \times \text{Cskip}(d) + 1$
- $n$th child end device is assigned to address $A_{\text{parent}} + R_m \times \text{Cskip}(d) + n$
Properties of DAAM

- Hierarchical addressing
  - reserve an address for each possible location in the tree
  - locations in the same subtree are allocated a continuous address block
  - Each device’s address can be assigned by its parent
  - routing can be performed without consulting any routing table (routing table eliminated)

Lm = 3, Cm = 4, Rm = 3

addresses 1 - 17
addresses 2 - 6
Weakness of DAAM

- Lack of flexibility
  - The highest usable address is $C_{skip}(0) \times R_m + C_m - R_m$. Addresses higher than this are not used.
  - A device may reach some ZR but this ZR cannot allocate an address to this device because all of its addresses have already been allocated.
    - H cannot associate with the ZC because the ZC has no more address for H
    - G has to associate with C for the same reason
    - F is configured as a ZED rather than a ZR

Assume $C_m = 4$, $R_m = 3$, $L_m = 3$. 

- FFD configured as a ZR/ZC
- FFD configured as a ZED
- Unconfigured FFD
- Configured RFD
Stochastic Address Assignment Mechanism (SAAM)

- Proposed in ZigBee 2007
- Addressing is no longer hierarchical
- Devices randomly and independently select their addresses
- Address conflicts occur when two or more devices select an identical network address
- Extra efforts are made to detect and resolve address conflicts
- A conflicting device may need to rejoin the network to obtain a new address
- Tree-based routing is no longer feasible with SAAM
- An independent routing protocol is needed
ZigBee routing protocols

- In a tree network
  - Utilize the address assignment to obtain the routing paths

- In a mesh network
  - Two options
    - Reactive routing: if having routing capacity
    - Use tree routing: if do not have routing capacity

- Note:
  - ZigBee coordinators and routers are said to have *routing capacity* if they have *routing table capacities and route discovery table capacities*
ZigBee routing in a tree network

- **Routing procedures**
  - When a device receives a packet, it first checks if it is the destination or one of its child end devices is the destination
  - If so,
    - this device will accept the packet or forward this packet to the designated child
  - Otherwise,
    - this device will relay packet along the tree

- The relationships between ancestors and descendants can be easily inferred by network addresses
Routing Determination

- Needs no routing table
- When a ZC/ZR at depth $d$ with address $A$ receives a packet destined for address $D$
  - If $A < D < A + C_{skip}(d - 1)$, the packet is for some node in the subtree rooted at $A$
    $$\text{Next-hop} = A + 1 + \left\lfloor \frac{(D - A - 1)}{C_{skip}(d)} \right\rfloor \times C_{skip}(d)$$
  - Otherwise, the packet should be passed to $A$’s parent
ZigBee routing in a mesh network

The route discovery in a ZigBee network is similar to the AODV routing protocol
- Links with lower cost will be chosen into the routing path.
- The cost of a link is defined based on the packet delivery probability on that link

Route discovery procedure
- The source broadcasts a route request packet
- Intermediate nodes will rebroadcast route request if
  - They have routing discovery table capacities
  - The cost is lower
- Otherwise, nodes will relay the request along the tree
- The destination will choose the routing path with the lowest cost and then send a route reply
## Summary of ZigBee network layer

### Pros and cons of different kinds of ZigBee network topologies

<table>
<thead>
<tr>
<th></th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| **Star** | 1. Easy to synchronize  
2. Support low power operation  
3. Low latency | 1. Small scale |
| **Tree** | 1. Low routing cost  
2. Can form superframes to support sleep mode  
3. Allow multihop communication | 1. Route reconstruction is costly  
2. Latency may be quite long |
| **Mesh** | 1. Robust multihop communication  
2. Network is more flexible  
3. Lower latency | 1. Cannot form superframes (and thus cannot support sleep mode)  
2. Route discovery is costly  
3. Needs storage for routing table |