ZigBee/IEEE 802.15.4
Overview

Y.-C. Tseng
CS/NCTU
New trend of wireless technology

- Most Wireless industry focuses on increasing high data throughput

- A set of applications require simple wireless connectivity, relaxed throughput, very low power, short distance and inexpensive hardware.
  - Industrial
  - Agricultural
  - Vehicular
  - Residential
  - Medical
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
IEEE 802.15 working group
## Comparison between WPAN

<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>100M (class 1)</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>
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

- **PERSONAL HEALTH CARE**: monitors, sensors, automation, control
- **INDUSTRIAL & COMMERCIAL**: industrial devices
- **CONSUMER ELECTRONICS**: televisions, VCRs, DVD/CD, remote control
- **PC & PERIPHERALS**: computers, keyboards, joysticks
- **TOYS & GAMES**: educational devices
- **HOME AUTOMATION**: security, HVAC, lighting, closures
Wireless technologies

- GSM
- GPRS
- EDGE
- 3G
- 802.11b
- ZigBee
- Bluetooth
- Bluetooth 1.5
- Bluetooth 2.0
- 802.11a/g
- HiperLAN/2
- WiMedia
- Bandwidth: kbps
ZigBee/802.15.4 architecture

- **ZigBee Alliance**
  - 45+ companies: semiconductor mfrs, IP providers, OEMs, etc.
  - Defining upper layers of protocol stack: from network to application, including application profiles
  - First profiles published mid 2003

- **IEEE 802.15.4 Working Group**
  - Defining lower layers of protocol stack: MAC and PHY

<table>
<thead>
<tr>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Framework</td>
</tr>
<tr>
<td>Network &amp; Security</td>
</tr>
<tr>
<td>MAC Layer</td>
</tr>
<tr>
<td>PHY Layer</td>
</tr>
</tbody>
</table>

- ZigBee Specification
- 802.15.4
- Application
- ZigBee stack
- Hardware
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
IEEE 802.15.4 overview
General characteristics

- Data rates of 250 kbps, 20 kbps and 40kbps.
- 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.

Channels:
- 16 channels in the 2.4GHz ISM band,
- 10 channels in the 915MHz ISM band
- 1 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 Carrier Sense Multiple Access with collision avoidance and optional time slotting
  - Message acknowledgement
  - Optional beacon structure
  - Target applications
    - 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 Device Types

- There are two different device types:
  - A full function device (FFD)
  - A reduced function device (RFD)

- The FFD can operate in three modes by serving as:
  - Device
  - Coordinator
  - PAN coordinator

- The RFD can only serve as:
  - 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
Star topology

- Full Function Device (FFD)
- Reduced Function Device (RFD)
- Communications Flow
Peer to peer topology

- Point to point
- Tree

Full Function Device (FFD)

Communications Flow
Device addressing

- Two or more devices communicating on the same physical channel constitute a WPAN.
  - A WPAN includes at least one FFD (PAN coordinator).
  - Each independent PAN will select a unique PAN identifier.

- Each device operating on a network has a unique **64-bit extended address**. This address can be used for direct communication in the PAN.

- A device also has a **16-bit short address**, which is allocated by the PAN coordinator when the device associates with its coordinator.
IEEE 802.15.4 physical layer
IEEE 802.15.4 PHY overview

- **PHY functionalitites:**
  - 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 bandwidth

2.4 GHz PHY

- Channels 11-26
  - 928 MHz to 2.4835 GHz
  - 5 MHz bandwidth
Frequency Bands and Data Rates

- 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>Reserve (1 bit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PHY Service Data Unit (PSDU)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0-127 Bytes</td>
</tr>
</tbody>
</table>
IEEE 802.15.4 MAC
A superframe is divided into two parts
- Inactive: all station sleep
- Active:
  - Active period will be divided into 16 slots
  - 16 slots can further divided into two parts
    - Contention access period
    - Contention free period

\[ SD = a_{BaseSuperframeDuration} \times 2^{SO} \text{ symbols (Active)} \]

\[ BI = a_{BaseSuperframeDuration} \times 2^{SO} \text{ symbols} \]
Superframe

- Beacons are used for
  - starting superframes
  - synchronizing with other devices
  - announcing the existence of a PAN
  - informing pending data in coordinators

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

- The structure of superframes is controlled by two parameters:
  - *beacon order (BO)*: decides the length of a superframe
  - *superframe order (SO)*: decides the length of the active portion in a superframe

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

- For channels 11 to 26, the length of a superframe can range from $15.36\, msec$ to $215.7\, sec$ ($= 3.5\, min$).
Superframe

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

- Duty Cycle:

<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>
Data Transfer Model (I)

- Data transferred from device to coordinator
  - In a beacon-enable network, a device finds the beacon to synchronize to the superframe structure. Then it uses slotted CSMA/CA to transmit its data.
  - In a non-beacon-enable network, device simply transmits its data using unslotted CSMA/CA
Data Transfer Model (II-1)

- Data transferred from coordinator to device in a beacon-enabled network:
  - The coordinator indicates in the beacon that some data is pending.
  - A device periodically listens to the beacon and transmits a Data Request command using slotted CSMA/CA.
  - Then ACK, Data, and ACK follow …

Communication from a coordinator in a beacon-enabled network
Data transfer model (II-2)

- Data transferred from coordinator to device in a non-beacon-enable network:
  - The device transmits a Data Request using unslotted CSMA/CA.
  - If the coordinator has its pending data, an ACK is replied.
  - Then the coordinator transmits Data using unslotted CSMA/CA.
  - If there is no pending data, a data frame with zero length payload is transmitted.

Communication from a coordinator in a non beacon-enabled network
Channel Access Mechanism

- Two type channel access mechanism:
  - beacon-enabled networks → slotted CSMA/CA channel access mechanism
  - non-beacon-enabled networks → unslotted CSMA/CA channel access mechanism
**Slotted CSMA/CA algorithm**

- In slotted CSMA/CA
  - 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
Slotted CSMA/CA algorithm (cont.)

- Each device maintains 3 variables for each transmission attempt
  - **NB**: number of times that backoff has been taken in this attempt (if exceeding `macMaxCSMABackoff`, the attempt fails)
  - **BE**: the backoff exponent which is determined by NB
  - **CW**: contention window length, the number of clear slots that must be seen after each backoff
    - always set to 2 and count down to 0 if the channel is sensed to be clear
    - The design is for some PHY parameters, which require 2 CCA for efficient channel usage.

- **Battery Life Extension**:
  - designed for very low-power operation, where a node only contends in the first 6 slots
Slotted CSMA/CA (cont.)

1. Slotted?
   - Y: \( NB = 0, CW = 2 \)
   - N: \( BE = \text{maxMinBE} \)

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

3. Perform CCA on backoff period boundary

4. If channel is idle:
   - Y: \( CW = 2, NB = NB + 1, BE = \min(BE + 1, e\text{MaxBE}) \)
   - N: \( NB > \text{macMaxCSMABackoffs} \)
   - If \( NB > 0 \):
     - Y: Failure
     - N: Success
   - If \( NB = 0 \):
     - Y: \( CW = CW - 1 \)

5. \( N \): Need 2 CCA to ensure no collision
Why 2 CCAs to Ensure Collision-Free

- Each CCA occurs at the boundary of a backoff slot (= 20 symbols), and each CCA time = 8 symbols.

- The standard species that a transmitter node performs the CCA twice in order to protect acknowledgment (ACK).
  - When an ACK packet is expected, the receiver shall send it after a $t_{ACK}$ time on the backoff boundary
    - $t_{ACK}$ varies from 12 to 31 symbols
  - One-time CCA of a transmitter may potentially cause a collision between a newly-transmitted packet and an ACK packet.
  - (See examples below)
Why 2 CCAs (case 1)

Existing session

New transmitter

New transmitter

Backoff boundary

Detect an ACK

Backoff end here

Detect an ACK

Backoff end here

CCA

CCA

DATA

ACK

20 sym
Why 2 CCAs (Case 2)

- Backoff boundary
- New transmitter
- Existing session
- New transmitter

Diagram:
- DATA
- ACK
- CCA
- 12sym
- Backoff end here
- Detect an ACK
- Detect an DATA
- Backoff end here
Why 2 CCAs (Case 3)

Existing session

New transmitter

New transmitter

Backoff boundary

Backoff end here

Detect a DATA

Detect an ACK

Data: $12 \text{sym} < t_{\text{ACK}} < 32 \text{sym}$
Unslotted CSMA/CA

1. Slotted?
   - Y: Slotted
   - N: CSMA-CA

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

3. Perform CCA

4. Channel idle?
   - Y: channel idle
   - N: $NB = NB + 1$, $BE = \min(\text{BE} + 1, a\text{MaxBE})$

5. $NB > \text{max}\text{MaxCSMABackoff}$?
   - Y: Failure
   - N: Success

Note: only one CCA
GTS Concepts (I)

- 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 **7 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
GTS Concepts (II)

- 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
GTS Concepts (III)

- 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 be an RFD is optional
Association Procedures (1/2)

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

![Diagram showing the association procedures between a coordinator and a device.]

1. The device starts scanning the channel.
2. The coordinator sends a Beacon (pending address) frame.
3. The device responds with an ACK.
4. The coordinator sends the Data request frame.
5. The device responds with an ACK.
6. The coordinator sends the Association response frame.
7. The device responds with an ACK.
8. The device makes a decision and becomes a member of the PAN.
Association Procedures (2/2)

- 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.
ZigBee Network Layer Protocols
ZigBee Network Layer Overview

- 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**: responsible for initializing, maintaining, and controlling the network
  - **ZigBee router**: form the network backbone
  - **ZigBee end device**: must be connected to router/coordinator

- In a tree network, the coordinator and routers can announce beacons.
- In a mesh network, there is no regular beacon.
  - Devices in a mesh network can only communicate with each other in a **peer-to-peer** manner.
Address Assignment

- In ZigBee, network addresses are assigned to devices by a distributed address assignment scheme.

- ZigBee coordinator determines three network parameters:
  - the maximum number of children \( (C_m) \) of a ZigBee router
  - the maximum number of child routers \( (R_m) \) of a parent node
  - the depth of the network \( (L_m) \)

- 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

\[
C_{skip}(d) = \begin{cases} 
1 + C_m \cdot (L_m - d - 1), & \text{if } R_m = 1 \quad \cdots \cdots (a) \\
1 + C_m - R_m - C_m \cdot R_m^{L_m - d - 1}, & \text{Otherwise} \quad \cdots \cdots (b)
\end{cases}
\]
If a parent node at depth $d$ has an address $A_{parent}$,

- the $n$th child router is assigned to address $A_{parent} + (n-1) \times C_{skip}(d) + 1$

- $n$th child end device is assigned to address $A_{parent} + R_m \times C_{skip}(d) + n$
ZigBee Routing Protocols

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

- In a mesh network:
  - **Routing Capability**: ZigBee coordinators and routers are said to have *routing capacity* if they have *routing table capacities* and *route discovery table capacities*
  - There are 2 options:
    - **Reactive routing**: if having “routing capacity”
    - **Tree routing**: if having no routing capacity
ZigBee Tree Routing

- 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, accept the packet or forward it to a child
  - Otherwise, relay it along the tree

- Example:
  - 38 ➔ 45
  - 38 ➔ 92
ZigBee Mesh Routing

- Route discovery by AODV-like routing protocol
  - 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
Routing in a Mesh network: Example
## Summary of ZigBee network layer

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