IEEE 802.15.4 and Zigbee

CS 687
University of Kentucky
Fall 2015

Acknowledgment: Some slides are adapted from presentations by Bob Heile from ZigBee Alliance, Joe Dvorak from Motorola, Geir E. Oien from NTNU, and Marco Naevve from Eaton Corporation.

Outline

- Introduction
- PHY Layer
- MAC Layer
- Network Layer
- Applications
IEEE 802.15.4 Application Space

- Home Networking
- Automotive Networks
- Industrial Networks
- Interactive Toys
- Remote Metering
- Active RFID/asset tracking

Sensor/Control Network Requirements

- Networks form by themselves, scale to large sizes and operate for years without manual intervention
- Extremely long battery life (years on AA cell),
  - low infrastructure cost (low device & setup costs)
  - low complexity and small size
- Low device data rate and QoS
- Standardized protocols allow multiple vendors to interoperate
The IEEE 802 Wireless Space

ZigBee standard uniquely fills a gap for low data rate applications.

802.15.4 / ZigBee Architecture
802.15.4 General Characteristics

Data rates of 250 kb/s, 40 kb/s and 20 kb/s.
Star or Peer-to-Peer operation.
Support for low latency devices.
Fully handshaked protocol for transfer reliability.
Low power consumption.

Frequency Bands of Operation
- 16 channels in the 2.4GHz ISM* band
- 10 channels in the 915MHz ISM band
- 1 channel in the European 868MHz band.

* ISM: Industrial, Scientific, Medical

<table>
<thead>
<tr>
<th>Standard</th>
<th>Bandwidth</th>
<th>Power Consumption</th>
<th>Protocol Stack Size</th>
<th>Stronghold</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi</td>
<td>Up to 54Mbps</td>
<td>400mA TX, standby 20mA</td>
<td>100+KB</td>
<td>High data rate</td>
<td>Internet browsing, PC networking, file transfers</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>1Mbps</td>
<td>40mA TX, standby 0.2mA</td>
<td>~100KB</td>
<td>Interoperability, cable replacement</td>
<td>Wireless USB, handset, headset</td>
</tr>
<tr>
<td>ZigBee</td>
<td>250kbps</td>
<td>30mA TX, standby 356 µA</td>
<td>34KB /14KB</td>
<td>Long battery life, low cost</td>
<td>Remote control, battery-operated products, sensors</td>
</tr>
</tbody>
</table>
ZigBee Alliance

- Organized as an independent, neutral, nonprofit corporation in 2002
- Open and global
  - Anyone can join and participate
  - Membership is global
- Activity includes
  - Specification creation
  - Certification and compliance programs
  - Branding, market development, and user education

The ZigBee Promoters
ZigBee Member Geographic Distribution

<table>
<thead>
<tr>
<th>Region</th>
<th>November 2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia / Pacific</td>
<td>60 (29%)</td>
</tr>
<tr>
<td>Europe / Middle East/Africa</td>
<td>58 (28%)</td>
</tr>
<tr>
<td>North/South America</td>
<td>86 (43%)</td>
</tr>
<tr>
<td>Total Member Companies</td>
<td>204</td>
</tr>
</tbody>
</table>

ZigBee Applications

- **Building Automation**
  - security
  - HVAC
  - AMR
  - lighting control
  - access control

- **Consumer Electronics**
  - TV
  - VCR
  - DVD/CD remote

- **Personal Health Care**
  - patient monitoring
  - fitness monitoring

- **Industrial Control**
  - asset mgmt
  - process control
  - environmental energy mgmt

- **Telecom Services**
  - m-commerce
  - info services
  - object interaction (Internet of Things)

- **Home Control**
  - security
  - HVAC
  - lighting control
  - access control
  - irrigation

- **PC & Peripherals**
  - mouse
  - keyboard
  - joystick

- **Operational Services**
  - patient
  - monitoring
  - fitness
  - monitoring

**ZigBee Wireless Control that Simply Works**
Outline

• Introduction
• PHY Layer
• MAC Layer
• Network Layer
• Applications
### Basic Radio Characteristics

ZigBee technology relies upon IEEE 802.15.4, which has excellent performance in low SNR environments.

<table>
<thead>
<tr>
<th>Frequency Band</th>
<th>License Required?</th>
<th>Geographic Region</th>
<th>Data Rate</th>
<th>Channel Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>868.3 MHz</td>
<td>No</td>
<td>Europe</td>
<td>20 kbps</td>
<td>0</td>
</tr>
<tr>
<td>868-928 MHz</td>
<td>No</td>
<td>Americas</td>
<td>40 kbps</td>
<td>1-10</td>
</tr>
<tr>
<td>2405-2480 MHz</td>
<td>No</td>
<td>Worldwide</td>
<td>250 kbps</td>
<td>11-26</td>
</tr>
</tbody>
</table>

### Operating Frequency Bands

#### 868MHz / 915MHz PHY
- Channel 0
- Channels 1-10

#### 2.4 GHz PHY
- Channels 11-26

- 868.3 MHz
- 902 MHz
- 928 MHz
- 2.4 GHz
- 2.4835 GHz
IEEE 802.15.4 PHY layer tasks

- activate/deactivate transceivers (low duty cycle saves energy)
- estimate signal strengths (energy detection) as part of CSMA mechanism
- compute link quality indicators (LQI, or SINR)
- listen to channels and declare availability or not (clear channel assessment -CCA)
- tuning of transceivers to supported channels
- transmit and receive data (16-symbol "quasi-orthogonal" modulation using O-QPSK and DSSS)
- conform to out-of-band power level regulations

Packet Structure

PHY Packet Fields
- Preamble (32 bits) – synchronization
- Start of Packet Delimiter (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – Data field

6 Octets 0-127 Octets
Outline

- Introduction
- PHY Layer
- MAC Layer
- Network Layer
- Applications

802.15.4 Architecture

- Channel acquisition
- Contention mgt
- NIC address
- Error Correction

IEEE 802.15.4
868/915 MHz PHY

IEEE 802.15.4
2400 MHz PHY

ZigBee

Applications
Design Drivers

- Extremely low cost
- Ease of implementation
- Reliable data transfer
- Short range operation
- Very low power consumption

Simple but flexible protocol

IEEE 802.15.4 Device Classes

- Full function device (FFD)
  - Any topology
  - PAN coordinator capable
  - Talks to any other device
  - Implements complete protocol set
- Reduced function device (RFD)
  - Limited to star topology or end-device in a peer-to-peer network.
  - Cannot become a PAN coordinator
  - Very simple implementation
  - Reduced protocol set
IEEE 802.15.4 Definitions

• **Network Device**: An RFD or FFD implementation containing an IEEE 802.15.4 medium access control and physical interface to the wireless medium.

• **Coordinator**: An FFD with network device functionality that provides coordination and other services to the network.

• **PAN Coordinator**: A coordinator that is the principal controller of the PAN. A network has exactly one PAN coordinator.

IEEE 802.15.4 MAC layer tasks

• for PAN coordinators: generate *beacons* (if operating in beacon-enabled mode)
  – A beacon is a special frame sent out by the PAN coordinator for the purpose of synchronization with other units. Beacon-enabled mode offers power savings since units can "sleep" between being "woken up" by beacons.

• for all nodes: synchronize against received beacons

• maintain and break up PAN connections

• give channel access to nodes according to CSMA-CA (based on PHY layer info)

• maintain *guaranteed time slot* mechanism in beacon-enabled mode

• frame acknowledgement, ARQ, CRC
802.15.4 Channel Access Options

- Non-beacon network
  - A simple, traditional multiple access system used in simple peer and near-peer networks
  - Standard CSMA-CA communications
  - Positive acknowledgement for successfully received packets

- Beacon-enabled network:
  - Network coordinator transmits beacons (start and end of time-slotted superframe) at predetermined intervals
  - Superframe may be split between contention access period, contention free period (containing guaranteed time slots), and inactive period
  - Beacon Mode powerful for controlling power consumption in extended networks like cluster tree or mesh
  - Allows all clients in a local piece of the network the ability to know when to communicate with each other
  - PAN coordinator manages the channel and arranges the calls
Low-Power Operation

• Duty-cycle control using superframe structure
  – Beacon order and superframe order
  – Coordinator battery life extension
• Indirect data transmission
• Devices may sleep for extended period over multiple beacons
• Allows control of receiver state by higher layers

Optional Frame Structure

<table>
<thead>
<tr>
<th>Slot</th>
<th>GTS 1</th>
<th>GTS 2</th>
<th>GTS 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

15ms * 2^n where 0 ≥ n ≥ 14

- **Network beacon**: Transmitted by PAN coordinator. Contains network information, frame structure and notification of pending node messages.
- **Beacon extension period**: Space reserved for beacon growth due to pending node messages.
- **Contention period**: Access by any node using CSMA-CA.
- **Guaranteed Time Slot**: Reserved for nodes requiring guaranteed bandwidth [n = 0].
Optional Frame Structure

- Superframe may have inactive period

\[ 15 \text{ms} \times 2^{SO} \]
where \( 0 \leq SO \leq 14 \)

\[ 15 \text{ms} \times 2^{BO} \]
where \( SO \leq BO \leq 14 \)

SO = Superframe order
BO = Beacon order

General Frame Structure

4 Types of MAC Frames:
- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame
### General MAC Frame Format

<table>
<thead>
<tr>
<th>Octets: 2</th>
<th>1</th>
<th>0/2</th>
<th>0/2</th>
<th>0/2</th>
<th>0/2</th>
<th>variable</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame control</td>
<td>Sequence number</td>
<td>Destination PAN identifier</td>
<td>Destination address</td>
<td>Source PAN identifier</td>
<td>Source address</td>
<td>Frame payload</td>
<td>Frame check sequence</td>
</tr>
</tbody>
</table>

#### MAC header
- **Addressing fields**
- Destination address
- Source address

#### MAC payload
- **Frame check sequence**

#### Frame control field

### Beacon Frame Format

<table>
<thead>
<tr>
<th>Octets: 2</th>
<th>1</th>
<th>4 or 10</th>
<th>2</th>
<th>variable</th>
<th>variable</th>
<th>variable</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame control</td>
<td>Beacon sequence number</td>
<td>Source address information</td>
<td>Superframe specification</td>
<td>GTS fields</td>
<td>Pending address fields</td>
<td>Beacon payload</td>
<td>Frame check sequence</td>
</tr>
</tbody>
</table>

#### MAC header

#### MAC payload

#### Frame control field

<table>
<thead>
<tr>
<th>Bits: 0-2</th>
<th>3</th>
<th>4-7</th>
<th>8-11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beacon order</td>
<td>Superframe order</td>
<td>Final CAP slot</td>
<td>Battery life extension</td>
<td>Reserved</td>
<td>PAN coordinator</td>
<td>Association permit</td>
<td></td>
</tr>
</tbody>
</table>
MAC Command Frame

- Command Frame Types
  - Association request
  - Association response
  - Disassociation notification
  - Data request
  - PAN ID conflict notification
  - Orphan Notification
  - Beacon request
  - Coordinator realignment
  - GTS request

Data Frame Format

Acknowledgement Frame Format
Data Service

- Data transfer to neighboring devices
  - Acknowledged or unacknowledged
  - Direct or indirect
  - Using GTS service
- Maximum data length (MSDU) $aMaxMACFrameSize$ (102 bytes)

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)
Slotted CSMA Procedure

Used in beacon enabled networks.

Un-slotted CSMA Procedure

Used in non-beacon networks.
Outline

- Introduction
- PHY Layer
- MAC Layer
- Network Layer
- Applications

802.15.4 Architecture

- Network Routing
- Address translation
- Packet Segmentation
- Profiles

- IEEE 802.15.4
  - 868/915 MHz PHY
  - 2400 MHz PHY

- ZigBee

- Applications
Basic Network Characteristics

- 65,536 network (client) nodes
- 27 channels over 2 bands
- 250Kbps data rate
- Optimized for timing-critical applications and power management
- Full Mesh Networking Support

Star Topology

- PAN Coordinator
- Master/slave
- Full function device
- Reduced function device
- Communications flow
Peer-Peer Topology

- Point to point
- Cluster tree

Communications flow

- Full function device

Combined Topology

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

Communications flow

- Full function device
- Reduced function device
ZigBee Mesh Networking

ZigBee Mesh Networking

Slide Courtesy of Control4

Slide Courtesy of Control4
ZigBee Mesh Networking

ZigBee Routing

- Ad hoc On Demand Distance Vector (AODV)
  - Path discovery on demand
  - Path maintenance (inform upstream nodes of broken links for active source nodes)

- Cluster-Tree Algorithm
  - Single cluster network
    - Cluster head selection
  - Multi-cluster network
    - Designated device for assigning a unique cluster ID to each cluster head
Outline

- Introduction
- PHY Layer
- MAC Layer
- Network Layer
- Applications

Application Profiles

- Application profiles define what messages are sent over the air for a given application
- Devices with the same application profiles interoperate end to end
- ZigBee publishes a set of public profiles, but vendors may create manufacturer specific ones as well
Manufacturer Specific Profiles

- Allows a vendor to build specialized products with a ZigBee Compliant Platform
- Certification testing ensures their product does not harm other ZigBee networks
- Manufacturer specific applications are not intended to interoperate at the application layer
- Allows product vendor to use ZigBee language and logos on their product

ZigBee Public Profiles

- Guarantees interoperability between products all running the same public application profile
- Product vendors may add additional features to the public profiles
- Allows product vendor to use ZigBee language and logos on their product
Interoperability Summary

- Devices built on ZigBee interoperate on different levels
- Wide spectrum of interoperability choices
- It’s a designer choice on level of vendor interoperability to support

Some Application Profiles

- **Home Automation [HA]**
  - Defines set of devices used in home automation
    - Light switches
    - Thermostats
    - Window shade
    - Heating unit
    - etc.

- **Industrial Plant Monitoring**
  - Consists of device definitions for sensors used in industrial control
    - Temperature
    - Pressure sensors
    - Infrared
    - etc.
More Application Profiles

- Multiple profiles at various stages of completion
  - Commercial Building Automation
    - Building control, management, and monitoring
  - Telecom Services/M-commerce
  - Automated Meter Reading
    - Addresses utility meter reading
  - Wireless Sensor Networks
    - Very low power unattended networks
- Vendors may form new profile groups within ZigBee and/or propose private profiles for consideration
- 400+ private profile IDs issued

Multi-Profile Devices

- Vendor devices may implement multiple profiles
- Additional application profiles live on different endpoints within the device
- Allows creation of vendor specific extensions
ZigBee – Highly Reliable

- Mesh networking protocol provides redundant paths
- Automatic retries and acknowledgements
- Parents keep track of messages for sleeping children
- High intrinsic interference tolerance
  - Multiple channels
  - Supports Frequency agility
  - Robust modulation

ZigBee – Highly Secure

- Utilizes AES 128-bit encryption
- Concept of a “trust center”
- Link and network keys
- Authentication and encryption
- Security can be customized for the application
- Keys can be “hard-wired” into application
Home Awareness

Home Heartbeat

Home Entertainment & Control
In-Home Patient Monitoring

- Patients receive better care at reduced cost with more freedom and comfort---
  - Patients can remain in their own home
    - Monitors vital statistics and sends via internet
    - Doctors can adjust medication levels
  - Allows monitoring of elderly family member
    - Sense movement or usage patterns in a home
    - Turns lights on when they get out of bed
    - Notify via mobile phone when anomalies occur
    - Wireless panic buttons for falls or other problems
  - Can also be used in hospital care
    - Patients are allowed greater movement
    - Reduced staff to patient ratio

Commercial Lighting Control

- Wireless lighting control
  - Dimmable intelligent ballasts
  - Light switches/sensors anywhere
  - Customizable lighting schemes
  - Quantifiable energy savings
  - Opportunities in residential, light commercial and commercial

- Extendable networks
  - Lighting network can be integrated with and/or be used by other building control solutions
HVAC Energy Management

• Hotel energy management
  – Centralized HVAC management allow hotel operator to ensure empty rooms are not cooled
  – Easy to retrofit
  – Battery operated thermostats, occupancy detectors, humidistats can be placed for convenience
  – Personalized room settings at check-in

AMR network example
Advanced Metering Platform with ZigBee

- Rapid method to help manage global electric generation shortage and meet existing and pending legislation for energy control
- Can network with other ZigBee devices in the home for load control – e.g. Heating/AC, Security, Lighting, White Goods
- Worldwide standard ZigBee allows communications between various meter types from different manufacturers.

Why ZigBee?

- Standards based
- Low cost
- Can be used globally
- Reliable and self healing
- Supports large number of nodes
- Easy to deploy
- Very long battery life
- Secure

- Open Standards Enable Markets