Chapter 7

ZigBee (IEEE 802.15.4)
Outline

7.1 Introduction and Overview of IEEE 802.15.4 / ZigBee

7.2 IEEE 802.15.4: Physical Layer Protocols

7.3 IEEE 802.15.4: MAC Layer Protocols

7.4 ZigBee
IEEE 802.15.4: Motivation

- Simpler and more power saving than Bluetooth
- Cheaper than WLAN
- Robust against interference

- End 1998: HomeRF-lite Working group
- Results were given to IEEE 802.15.4. in 2001
- Foundation of ZigBee Alliance in 2002
- IEEE 802.15.4: Physical and Data Link Layer
- ZigBee: higher layers
## Comparison of Wireless Standards

<table>
<thead>
<tr>
<th>Market Name Standard</th>
<th>GPRS/GSM 1xRTT/CDMA</th>
<th>Wi-Fi™ 802.11b</th>
<th>Bluetooth™ 802.15.1</th>
<th>ZigBee 802.15.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Focus</td>
<td>Wide Area Voice &amp; Data</td>
<td>Web, Email, Video</td>
<td>Cable Replacement</td>
<td>Monitoring &amp; Control</td>
</tr>
<tr>
<td>System Resources</td>
<td>16MB+</td>
<td>1MB+</td>
<td>250KB+</td>
<td>4KB - 32KB</td>
</tr>
<tr>
<td>Battery Life (days)</td>
<td>1-7</td>
<td>0.5 - 5</td>
<td>1 - 7</td>
<td>100 - 1,000+</td>
</tr>
<tr>
<td>Network Size</td>
<td>1</td>
<td>32</td>
<td>7</td>
<td>Unlimited (2⁶⁴)</td>
</tr>
<tr>
<td>Bandwidth (KB/s)</td>
<td>64 - 128+</td>
<td>11,000+</td>
<td>720</td>
<td>20 - 250</td>
</tr>
<tr>
<td>Transmission Range (meters)</td>
<td>1,000+</td>
<td>1 - 100</td>
<td>1 - 10+</td>
<td>1 - 100+</td>
</tr>
<tr>
<td>Success Metrics</td>
<td>Reach, Quality</td>
<td>Speed, Flexibility</td>
<td>Cost, Convenience</td>
<td>Reliability, Power, Cost</td>
</tr>
</tbody>
</table>

Andreas Könsgen
TZI – FB 1 – Communication Networks
Summer Term 2013
802.15.4: General remarks (1)

- 300 pages standardisation
- 26 primitives against 131 with 802.15.1 (Bluetooth)
- Depending on functionality 4 to 30 kbyte code for ZigBee code
- Direct access to MAC without LLC implementation is simpler, but not compatible to other 802.x
- 802.15.4a: additional PHY layers
802.15.4: General remarks (2)

Simple packet data protocol for lightweight wireless networks:
- Channel Access: Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and optional time slotting
- Message Acknowledgement (ACK) and an optional beacon structure
- Multi-level security (32-, 64-, 128-bit encryption)
- Full and reduced function devices
- Works well for long battery life, selectable latency for controllers and sensors, remote monitoring and portable electronics
- Configured for maximum battery life
  - Lasts as long as the shelf life of most batteries
802.15.4 Supported Topologies

Star Topology

Peer-to-Peer Topology

http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf
Outline

7.1 Introduction and Overview of IEEE 802.15.4 / ZigBee

7.2 IEEE 802.15.4: Physical Layer Protocols

7.3 IEEE 802.15.4: MAC Layer Protocols

7.4 ZigBee
IEEE 802.15.4: PHY Layer

- Overview
- Operating frequency bands and data rates
- Direct Sequence Spread Spectrum (DSSS)
- Modulation and spreading
- Data frames
- PHY services
Operating frequency bands and data rates

- **868–868.6 MHz: channel 0**
  - Available in most European countries
  - Bit rate: 20 kbit/s

- **902–928 MHz: channel 1–10**
  - North America, Australia, New Zealand
  - Bit rate: 40 kbit/s

- **2.4000–2.4835 MHz: channel 11–26**
  - Most countries worldwide
  - Bit rate: 250 kbit/s
Modulation and Spreading: 868/915 MHz

- Digital data communication only; half-duplex operation only
- DSSS employing BPSK
  - No complex signal processing required
  - Spreading with 15-chip pseudo-random sequence

<table>
<thead>
<tr>
<th>Band</th>
<th>868MHz</th>
<th>915 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_b$</td>
<td>Bit period</td>
<td>50µs</td>
</tr>
<tr>
<td>$R_b$</td>
<td>Bit rate</td>
<td>20kb/s</td>
</tr>
<tr>
<td>$T_c$</td>
<td>Chip period</td>
<td>3.33µs</td>
</tr>
<tr>
<td>$R_c$</td>
<td>Chip rate</td>
<td>300kc/s</td>
</tr>
<tr>
<td>$N_c$</td>
<td>Chips per symbol</td>
<td>15</td>
</tr>
</tbody>
</table>
Modulation and spreading: 2.4 GHz

- 4 data bits → 1 symbol → 1 of 16 DSSS chip sequences
- Modulation with offset QPSK (OQPSK)
- Specification symbol rate: 62.5 ksymbols/s → 250kbit/s data rate, $T_c = 0.5$µs; chip rate: 1 Mchip/s
- Creating the offset for O-QPSK: half-chip delay in Q channel

<table>
<thead>
<tr>
<th>I Phase</th>
<th>C0</th>
<th>C2</th>
<th>C4</th>
<th>C6</th>
<th>..........</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q Phase</td>
<td>C1</td>
<td>C3</td>
<td>C5</td>
<td>C7</td>
<td>..........</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C24</th>
<th>C26</th>
<th>C28</th>
<th>C30</th>
</tr>
</thead>
<tbody>
<tr>
<td>C25</td>
<td>C27</td>
<td>C29</td>
<td>C31</td>
</tr>
</tbody>
</table>
Radio Characteristics

- Power output limitation
  - At least: –3 dBm, equiv. to 0.5 mW
  - Maximum: US 1 Watt; EU 100 mW

- Sensitivity
  - 2.4 GHz: –85 dBm
  - Lower bands: –92 dBm

- Range
  - 2.4 GHz: maximum ≈220 m
  - Lower bands: maximum ≈1 km
PHY frame structure

- **PHY Packet Fields**
  - Preamble (32 bits binary zeros) – for synchronization
  - Start of Packet Delimiter (8 bits 0xE6 = ‘11100101’)
  - PHY Header (8 bits) – Packets length in bytes
  - PSDU (0 to 1016 bits) – Data field
More Considerations for Saving Power

- RF stage / antenna efficiency: \( \approx 10\% \)
  - Less efficient in 2.4 GHz band than in lower bands

- Achieve low duty cycle
  - Sleep is better than idle

- Start up consumption
  - Process multiple packets in one wakeup period

- Computation vs. transmission
  - \( \approx 1000 \) instructions: 1 bit

  *Example:*
  - Active power: 10mW; standby power: 10\( \mu \)W
  - Duty cycle: 0.1\%: time-average power 19.9\( \mu \)W
  - 750 mAh AAA battery with 1V: 37,000 hours (more than 4 years)
Outline

7.1 Introduction and Overview of IEEE 802.15.4 / ZigBee

7.2 IEEE 802.15.4: Physical Layer Protocols

7.3 IEEE 802.15.4: MAC Layer Protocols

7.4 ZigBee
MAC Layer Functionality

- Transmission to neighbour, not end-to-end
  - Addressing

- Medium Access

- Reliable delivery of data (optional)
  - ACK frames

- Association/disassociation

- Encryption
  - Advanced Encryption Standard (AES-128) security with symmetric key
MAC Layer Protocol

• Requirements
  ‣ General requirements of Wireless MAC layer Protocols
  ‣ Specific requirements and design considerations for MAC layer protocols in Wireless Sensor Networks

• IEEE 802.15.4 MAC Protocol
  ‣ Device Classes
  ‣ Addressing
  ‣ Beaconed and unbeaconed modes
  ‣ MAC services
Addressing

- **64-bit IEEE addresses**: unique to each node
  - Network size up to $2^{64}$ nodes

- **16-bit short addresses**: assigned by PAN coordinator
  - Using local addressing, $2^{16}$ nodes (assigned by coordinator)
    - lower latency
    - lower overhead
  - Addressing modes:
    - network + device identifier (star)
    - source/destination identifier (peer-peer)
Device classes

- **Full Function Device (FFD)**
  - Can communicate with other FFDs as well as RFDs
  - PAN Coordinator
  - Coordinator
  - “Normal” device

- **Reduced Function Device (RFD)**
  - Can only communicate with FFD

- **Coordinator**
  - Must be full function device (FFD)
  - Exactly one coordinator per network
  - Provides synchronisation (transmits beacons)
  - One or more alternate PAN coordinators, which take over coordinator role, if coordinator leaves network
Data transfers and beacons

- Data Transfers
  - Between a coordinator and a device
  - Between two devices

- Beacons
  - Support for devices to associate to the network
  - Reservation of time slots for individual devices
Superframe structure

- Superframe is initiated by beacon
- CAP: contention access period, uses CSMA/CA access
- CFP: Contention-free period
- Contention period in CAP and GTS duration are multiples of base slot length
- GTS: guaranteed time slot: allocated airtime for a station
- Inactive period: stations are sleeping
Interframe spacing

- **LIFS**: long interframe spacing – after transfer of long frame
- **SIFS**: short interframe spacing – after transfer of short frame
- Time periods for „long“ and „short“ defined by standard
- \( t_{\text{ack}} \): acknowledgement period
- Transmission of consecutive frames inside same CAP possible without back off for each frame

**acknowledged mode**

\[
\begin{array}{c}
\text{long frame} & \xrightarrow{t_{\text{ack}}} & \text{ACK} & \xrightarrow{\text{LIFS}} & \text{short frm.} & \xrightarrow{t_{\text{ack}}} & \text{ACK} & \xrightarrow{\text{SIFS}} \\
\end{array}
\]

**unacknowledged mode**

\[
\begin{array}{c}
\text{long frame} & \xrightarrow{\text{LIFS}} & \text{short frm.} & \xrightarrow{\text{SIFS}} \\
\end{array}
\]
## MAC frame structure

<table>
<thead>
<tr>
<th>Header</th>
<th>Payload</th>
<th>Footer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Beacon</strong></td>
<td></td>
<td><strong>FCS</strong></td>
</tr>
<tr>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Addressing Fields</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Superframe Specification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add.list Fields</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pending Addr. Field</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Beacon Payload</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>FCS</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td></td>
<td><strong>FCS</strong></td>
</tr>
<tr>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Addressing Fields</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Payload</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>FCS</strong></td>
</tr>
<tr>
<td><strong>MAC command</strong></td>
<td></td>
<td><strong>FCS</strong></td>
</tr>
<tr>
<td>Frame Control</td>
<td>Sequence Number</td>
<td>Addressing Fields</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAC Command Payload</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>FCS</strong></td>
</tr>
<tr>
<td><strong>ACK</strong></td>
<td></td>
<td><strong>FCS</strong></td>
</tr>
<tr>
<td>Frame Control</td>
<td>Seq Number</td>
<td><strong>FCS</strong></td>
</tr>
</tbody>
</table>
Security

- Difference to other wireless networks?
  - No – vulnerable against: eavesdropping, tampering
  - May be – sensor node are more limited (processing, storage, battery, costs...)

- Therefore 802.15.4 supports the following security services
  - Data confidentiality
  - Data authenticity
  - Replay protection

- Security mechanisms in 802.15.4
  - 128 bit Advanced Encryption Standards (key management not included)
Outline

- Introduction and Overview of IEEE 802.15.4 / ZigBee
- IEEE 802.15.4: Physical Layer Protocols
- IEEE 802.15.4: MAC Layer Protocols
- ZigBee
6.4 ZigBee

- ZigBee stack
- ZigBee devices
- Routing
- Application
What is ZigBee™?

- **ZigBee™** - a new global standard for wireless connectivity
  - focusing on standardizing and enabling interoperability of products within home control, building automation and industrial control and monitoring

- **ZigBee™ Alliance**
  - association of companies
  - enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard

- **Members:** Texas Instruments, Motorola, PHILIPS, Samsung, ATMEL, Analog Devices, etc. (over 230)

- Gateway products to link ZigBee™ with existing home, building automation, and industrial WLAN/WPAN networks.
IEEE 802.15.4 / ZigBee Protocol Stack

User applications based on application Profiles

Generic interface to applications based on generalised profiles

Topology management, Binding, Discovery

Topology management, MAC mngmnt, routing

PAN management, Channel access, Reliable hop-to-hop transport, Bitwise transmission

From: Elektronik Wireless – März 2004, p.18
ZigBee Topology

- Peer-to-Peer topology
  - Can cover a large physical area
  - High message latency
  - Wireless sensor network, industrial control and monitoring

- Type of Peer-to-Peer networks
  - Flat ‘Mesh’ network
    - a network composed of a number of identical network devices
    - protocols for mesh networks are not part of the standard 802.15.4
  - Cluster network
    - concept of a ‘parent-child’ relationship between network devices
  - Cluster tree network
    - ‘parent-child’ relationship
    - large cluster is broken up into several, smaller clusters, connected in a hierarchical tree
ZigBee Architecture (1)

- Network Layer
- APS – Application Support Layer
  - Connection to Network Layer (NLDE)
  - Management Entity (NLME):
    - maintains APS Information Base – AIB
    - device Discovery
    - binding of devices into network
- ZigBee Device Object (ZDO)
  - Generic functions
    - RFD or FFD functionality
    - initialization of ZigBee Network Layer (NWK) or APS
    - initiate device discovery, binding, security functions
ZigBee Architecture (2)

- Application Framework
  - Up to 30 Application Objects
    - some predefined by ZigBee Alliance
- Security
  - Generation of keys
  - Dynamic distribution of keys in networks
  - Concept with Trust Center
ZigBee Devices

- Physical devices
  - RFD
    - star and talks only to FFD
    - simple implementation—8 bit Microcontroller, min RAM and ROM
    - generally battery powered
  - FFD
    - any topology and talks to any other devices
    - capable of being a coordinator
    - generally line powered

- Logical devices
  - Coordinator
  - Router
  - End Devices
ZigBee – Network Layer (1)

- Transport of data between two stations (devices) (MAC Layer only between two neighbouring devices)
- Network Management
  - Configuring of new devices
  - Configure and administrate network topology
  - Associate and disassociate stations
  - Addressing
  - Discovery of devices
  - Routing using “pairing tables”
ZigBee – Network Layer (2)

- Supports three network topologies
  - Star: common, provides very long battery life operation
  - Peer-to-peer (mesh): high levels of reliability and scalability by providing more than one path through the network
  - Cluster-tree: high levels of reliability and support for battery-powered nodes

Ed Callaway et. al., Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks, IEEE Communication Magazine August 2002
Network Topology

- Star
- Cluster Tree
- Mesh

Zigbee: "Wireless Control That Simply Works"
William C. Craig
Table-based routing

Data to be sent from E to I
Established route: E-B-A-D-I

Station with Routing capability
Station without Routing capability

RREQ unicast
RREQ broadcast
RREP unicast
Cluster Tree Routing

Address determines the path

Number of steps $L_m = 3$
Children per node $C_m = 4$
ZigBee Applications

- For the transmission of
  - Periodic data
    - wireless sensor or meter
    - using a beacon system
    - providing for very low duty-cycle (<1%) and enables multi-year battery life
  - Intermittent data
    - wireless light switch
    - unbeaconed system
  - Repetitive low latency data
    - security system
    - beacons
    - providing QoS using GTS (Guaranteed Time Slice support)
### ZigBee Applications

<table>
<thead>
<tr>
<th>PERSONAL HEALTH CARE</th>
<th>INDUSTRIAL CONTROL</th>
<th>BUILDING AUTOMATION</th>
<th>PC &amp; PERIPHERIALS</th>
<th>CONSUMER ELECTRONICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Monitoring</td>
<td>Asset Mgmt</td>
<td>Security</td>
<td>Keyboard</td>
<td>TV</td>
</tr>
<tr>
<td>Fitness Monitoring</td>
<td>Process Control</td>
<td>HVAC</td>
<td>Mouse</td>
<td>VCR</td>
</tr>
<tr>
<td></td>
<td>Environmental</td>
<td>AMR</td>
<td>etc.</td>
<td>CD/DVD</td>
</tr>
<tr>
<td></td>
<td>Energy Mgmt</td>
<td>Light Control</td>
<td></td>
<td>Remote</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Control</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Acknowledgement & References

- Some pictures and slides in this presentation are referenced from:
  - Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirc, A Survey on Sensor Networks, IEEE Communications Magazine August 2002
  - Ed Callaway et. al., Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks, IEEE Communication Magazine August 2002
  - http://www.moteiv.com
  - A. Sikora, ZigBee: Grundlagen und Applikation, Der IEEE-Standard 802.15.4 als Basis, Elektronik Wireless – March 2004
  - Tutorial at CRUISE Summer School 2006 „802.15.4 PHY and MAC Layer“ by Liang Zhao, Hongyu Wang, Andreas Timm-Giel
  - http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf