ZigBee /
IEEE 802.15.4

ZigBee Alliance:
http://www.ZigBee.org

IEEE 802.15.4:
http://www.ieee802.org/15/pub/TG4.html
The Wireless Market

<table>
<thead>
<tr>
<th>TEXT</th>
<th>INTERNET/AUDIO</th>
<th>COMPRESSED VIDEO</th>
<th>MULTI-CHANNEL DIGITAL VIDEO</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHORT RANGE</td>
<td></td>
<td>802.11b</td>
<td>802.15.3/WIMEDIA</td>
</tr>
<tr>
<td>SHORT RANGE</td>
<td></td>
<td>802.11a/HL2 &amp; 802.11g</td>
<td></td>
</tr>
<tr>
<td>SHORT RANGE</td>
<td></td>
<td>Bluetooth 2</td>
<td></td>
</tr>
<tr>
<td>SHORT RANGE</td>
<td></td>
<td>Bluetooth1</td>
<td></td>
</tr>
<tr>
<td>LONG RANGE</td>
<td></td>
<td>802.11b</td>
<td></td>
</tr>
<tr>
<td>LOW</td>
<td>&lt; ACTUAL THROUGHPUT &gt; HIGH</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Wireless Market (2)

- Text
- Graphics
- Internet
- Hi-Fi audio
- Streaming video
- Digital video
- Multi-channel video

GSM/CDMA
GPRS/3G
LMDS

- Low Data Rate
- High Data Rate

- ZigBee
- Bluetooth 1
- Bluetooth 2
- 802.11b
- 802.11a/HL2

WAN
LAN
PAN
What Is the 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
  - Upper layer stack and application profiles
  - Compliance and certification testing
  - Branding

- Result is a set of interoperable solutions recognizable in the market

- Eight promoter companies
  - Ember, Freescale, Honeywell, Invensys, Mitsubishi, Motorola, Philips and Samsung

- A rapidly growing list (Over 120 participants) of industry leaders worldwide committed to providing ZigBee-compliant products and solutions
  - Companies include semiconductor manufacturers, wireless IP providers, OEMs, and end-users
Why Do We Need ZigBee Technology?

- No standard approach today that addresses the unique needs of most remote monitoring and control applications
  - Enables the broad-based deployment of reliable wireless networks with low-complexity, low-cost solutions
  - Provides the ability to run for years on inexpensive primary batteries for a typical monitoring application
  - Capable of inexpensively supporting robust mesh networking technologies
How Is ZigBee Related to IEEE 802.15.4?

- ZigBee takes full advantage of a physical radio and MAC layers specified by IEEE 802.15.4 (lower layers)
- ZigBee adds logical network, security and application software (higher layers)
- ZigBee continues to work closely with the IEEE to ensure an integrated and complete solution for the market
Zigbee target markets

- Industrial & Commercial
  - Monitors
  - Sensors
  - Automation
  - Control

- Consumer Electronics
  - TV
  - VCR
  - DVD
  - CD
  - Remote

- PC Peripherals
  - Mouse
  - Keyboard
  - Joystick
  - Gamepad

- Personal Healthcare
  - Monitors
  - Diagnostics
  - Sensors

- Toys & Games
  - PETs
  - Gameboys
  - Educational

- Home Automation
  - Security
  - HVAC
  - Lighting
  - Closures

Low Data Rate Radio Devices
Applications

**ZigBee**

*Wireless Control that Simply Works*

- **BUILDING AUTOMATION**
  - security
  - HVAC
  - AMR
  - lighting control
  - access control

- **CONSUMER ELECTRONICS**
  - TV
  - VCR
  - DVD/CD
  - remote

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

- **PERSONAL HEALTH CARE**
  - patient monitoring
  - fitness monitoring

- **INDUSTRIAL CONTROL**
  - asset mgt
  - process control
  - environmental energy mgt

- **RESIDENTIAL/ LIGHT COMMERCIAL CONTROL**
  - security
  - HVAC
  - lighting control
  - access control
  - lawn & garden irrigation
HVAC Energy Management

- Hotel energy management
  - Major operating expense for hotel
    - Centralized HVAC management allow hotel operator to make sure empty rooms are not cooled
  - Retrofit capabilities
  - Battery operated t-stats can be placed for convenience
  - Personalized room settings at check-in
Industrial/Commercial Spaces

- Warehouses, Fleet management, Factory, Supermarkets, Office complexes
- Gas/Water/Electric meter, HVAC
- Smoke, CO, H₂O detector
- Refrigeration case or appliance
- Equipment management services & Preventative maintenance
- Security services
- Lighting control
- Assembly line and work flow, Inventory
- Materials processing systems (heat, gas flow, cooling, chemical)

Energy, diagnostics, e-Business services
- **Gateway or Field Service links to sensors & equipment**
  - Monitored to suggest PM, product updates, status changes
- **Nodes link to PC for database storage**
  - PC Modem calls retailer, Service Provider, or Corp headquarters
  - Corp headquarters remotely monitors assets, billing, energy management

![Diagram of industrial/commercial spaces with various sensors, gateways, and services connected to back end server and system components like Tel/Co line, Mfg Flow (Materials handling), HVAC, Database Gateway, and Security Gateway with connections to Field Service or mobile worker, Security Sensor, and Temp. Sensor.]
Asset Management

- Within each container, sensors form a mesh network
- Multiple containers in a ship form a mesh to report sensor data
- Increased security through on-truck and on-ship tamper detection
- Faster container processing. Manifest data and sensor data are known before ship docks at port
IEEE 802.15.4

- "the hardware"
- Physical & Media Access Control layers

ZigBee Alliance

- "the software"
- Network, Security & Application layers
- Brand management

### PHY
868MHz / 915MHz / 2.4GHz

### MAC

### Network
Star / Mesh / Cluster-Tree

### Security
32- / 64- / 128-bit encryption

### API

### Application

<table>
<thead>
<tr>
<th>Silicon</th>
<th>Stack</th>
<th>App</th>
</tr>
</thead>
</table>

IEEE 802.15.4 & ZigBee In Context
### Frequencies and Data Rates (2006)

<table>
<thead>
<tr>
<th>Band</th>
<th>Coverage</th>
<th>Data Rate</th>
<th># of Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz</td>
<td>ISM Worldwide</td>
<td>250kbps</td>
<td>16</td>
</tr>
<tr>
<td>868 MHz</td>
<td>Europe</td>
<td>20kbps, 100kbps, 250kbps</td>
<td>1</td>
</tr>
<tr>
<td>915MHz</td>
<td>ISM Americas</td>
<td>250kbps, 40kbps</td>
<td>10</td>
</tr>
</tbody>
</table>
Basic Network Characteristics

- 65,536 network (client) nodes

- Optimized for timing-critical applications
  - Network join time: 30 ms (typ)
  - Sleeping slave changing to active: 15 ms (typ)
  - Active slave channel access time: 15 ms (typ)
## Comparison of Key Features of Complementary Protocols

<table>
<thead>
<tr>
<th>Feature(s)</th>
<th>IEEE 802.11b</th>
<th>Bluetooth</th>
<th>ZigBee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Profile</td>
<td>Hours</td>
<td>Days</td>
<td>Years</td>
</tr>
<tr>
<td>Complexity</td>
<td>Very Complex</td>
<td>Complex</td>
<td>Simple</td>
</tr>
<tr>
<td>Nodes/Master</td>
<td>32</td>
<td>7</td>
<td>64000</td>
</tr>
<tr>
<td>Latency</td>
<td>Enumeration up to 3 Seconds</td>
<td>Enumeration up to 10 seconds</td>
<td>Enumeration 30ms</td>
</tr>
<tr>
<td>Range</td>
<td>100 m</td>
<td>10 m</td>
<td>70m-300m</td>
</tr>
<tr>
<td>Extendibility</td>
<td>Roaming Possible</td>
<td>No</td>
<td>YES</td>
</tr>
<tr>
<td>Data Rate</td>
<td>11Mbps</td>
<td>1 Mbps</td>
<td>250Kbps</td>
</tr>
<tr>
<td>Security</td>
<td>Authentication Service Set ID (SSID), WEP</td>
<td>64 bit, 128 bit</td>
<td>128 bit AES and Application Layer user defined</td>
</tr>
</tbody>
</table>
Why ZigBee?

- Reliable and self healing
- Supports large number of nodes
- Easy to deploy
- Very long battery life
- Secure
- Low cost
- Can be used globally
IEEE 802.15.4 Tutorial
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 and an optional beacon structure
  - Multi-level security
  - Three bands, 27 channels specified
    - 2.4 GHz: 16 channels, 250 kbps
    - 868.3 MHz: 1 channel, 20 kbps (BPSK) / 100 kbps (O-QPSK), 250 kbps (ASK)
    - 902-928 MHz: 10 channels, 40 kbps (BPSK) / 250kbps (ASK or O-QPSK)
  - 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
802.15.4 General Characteristics

Data rates of 250 kb/s, 100 kb/s, 40 kb/s and 20 kb/s.
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.

Frequency Bands of Operation, either:

- 16 channels in the 2.4GHz ISM band;
- Or 10 channels in the 915MHz ISM band
  and 1 channel in the European 868MHz band.
802.15.4 Architecture
IEEE 802.15.4 PHY Overview

Operating Frequency Bands

868MHz / 915MHz PHY

Channel 0
868.3 MHz

Channels 1-10
902 MHz - 928 MHz

2.4 GHz PHY

Channels 11-26
2.4 GHz - 2.4835 GHz
IEEE 802.15.4 PHY Overview
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
IEEE 802.15.4 PHY Overview
Modulation/Spreading

2.4 GHz PHY
- 250 kb/s (4 bits/symbol, 62.5 kBaud)
- Data modulation is 16-ary orthogonal modulation
- 16 symbols are orthogonal set of 32-chip PN codes
- Chip modulation is O-QPSK at 2.0 Mchips/s

868MHz/915MHz PHY
- Symbol Rate
  - 868 MHz Band: 250 kb/s (10 bit/symbol, 12.5 kBaud), 100 kb/s (4 bit/symbol, 25 Kbaud), 20 kb/s (1 bit/symbol, 20 kBaud)
  - 915 MHz Band: 250 kb/s (5 bit/symbol, 50 Kbaud or 4 bit/symbol, 62.5 Kbaud), 40 kb/s (1 bit/symbol, 40 kBaud)
- Data modulation is BPSK with differential encoding
- Spreading code is a 15-chip m-sequence
- Chip modulation is BPSK, ASK or O-QPSK at
  - 868 MHz Band: 300 or 400 kchips/s
  - 915 MHz Band: 600, 1600 or 1000 kchips/s
IEEE 802.15.4 PHY Overview

Common Parameters

Transmit Power
• Capable of at least .5 mW

Transmit Center Frequency Tolerance
• ± 40 ppm

Receiver Sensitivity (Packet Error Ratio <1%)
• ≤-85 dBm @ 2.4 GHz band
• ≤-92 dBm @ 868/915 MHz band

RSSI Measurements
• Packet strength indication
• Clear channel assessment
• Dynamic channel selection
IEEE 802.15.4 PHY Overview

PHY Primitives

PHY Data Service
• PD-DATA – exchange data packets between MAC and PHY

PHY Management Service
• PLME-CCA – clear channel assessment
• PLME-ED - energy detection
• PLME-GET / -SET– retrieve/set PHY PIB parameters
• PLME-TRX-ENABLE – enable/disable transceiver
PHY Performance

802.15.4 has excellent performance in low SNR environments

802.11b, 802.15.x BER Comparison

Working zone BER
IEEE 802.15.4 MAC Overview

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 MAC Overview

- Employs 64-bit IEEE & 16-bit short addresses
  - Ultimate network size can reach $2^{64}$ nodes (more than we’ll probably need…)
  - Using local addressing, simple networks of more than 65,000 ($2^{16}$) nodes can be configured, with reduced address overhead

- Three devices specified
  - Network Coordinator
  - Full Function Device (FFD)
  - Reduced Function Device (RFD)

- Simple frame structure
- Reliable delivery of data
- Association/disassociation
- AES-128 security
- CSMA-CA channel access
- Optional superframe structure with beacons
- Optional GTS mechanism
IEEE 802.15.4 MAC Overview
Device Classes

- 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
Topology Models

- Star
- Cluster Tree
- Mesh

- PAN coordinator
- Full Function Device
- Reduced Function Device
IEEE 802.15.4 MAC Overview

Star Topology

PAN Coordinator

Master/slave

Full function device

Reduced function device

Communications flow
IEEE 802.15.4 MAC Overview

Peer-Peer (Mesh) Topology

- Point to point
- Cluster tree

- Full function device
- Communications flow
Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.
Cluster Tree
Star Network Key Attributes

- Simplicity
- Low Cost
- Long Battery Life
- Single Point of Failure
Mesh Network Key Attributes

- Reliability
- Extended Range
- No Battery Life
- Routing Complexity

Diagram labels:
- Router Node
- Controller
Hybrid Network Key Attributes

- Flexibility
- Reliability/Range of Mesh
- Battery Life of Star
- Design Complexity
IEEE 802.15.4 MAC Overview

Addressing

- All devices have 64 bit IEEE addresses
- Short addresses can be allocated
- Addressing modes:
  - Network + device identifier (star)
  - Source/destination identifier (peer-peer)
IEEE 802.15.4 MAC Overview

General Frame Structure

4 Types of MAC Frames:

- Data Frame
- Acknowledgment Frame
- MAC Command Frame
- Beacon Frame
### Data Frame format

**MAC sublayer**

<table>
<thead>
<tr>
<th>Octets:</th>
<th>2</th>
<th>1</th>
<th>4 to 20</th>
<th>n</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Control</td>
<td>Data Sequence Number</td>
<td>Address Information</td>
<td>Data Payload</td>
<td>FCS</td>
<td></td>
</tr>
<tr>
<td>MHR</td>
<td>MSDU</td>
<td>MFR</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PHY layer**

<table>
<thead>
<tr>
<th>Octets:</th>
<th>4</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble Sequence</td>
<td>Start of Frame Delimiter</td>
<td>Frame Length</td>
<td></td>
</tr>
</tbody>
</table>

| SHR | PHR |

| 11 + (4 to 20) + n |

| PPDU |

- One of two most basic and important structures in 802.15.4
- Provides up to 104 byte data payload capacity
- Data sequence numbering to ensure that packets are tracked
- Robust structure improves reception in difficult conditions
- Frame Check Sequence (FCS) validates error-free data
The other most important structure for 15.4

Provides active feedback from receiver to sender that packet was received without error

Short packet that takes advantage of standards-specified “quiet time” immediately after data packet transmission
MAC Command Frame format

- Mechanism for remote control/configuration of client nodes
- Allows a centralized network manager to configure individual clients no matter how large the network
Beacon Frame format

- Beacons add a new level of functionality to a network.
- Client devices can wake up only when a beacon is to be broadcast, listen for their address, and if not heard, return to sleep.
- Beacons are important for mesh and cluster tree networks to keep all of the nodes synchronized without requiring nodes to consume precious battery energy listening for long periods of time.
# Frame Control field

<table>
<thead>
<tr>
<th>Bits: 0–2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7–9</th>
<th>10–11</th>
<th>12–13</th>
<th>14–15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Type</td>
<td>Security Enabled</td>
<td>Frame Pending</td>
<td>Ack. Request</td>
<td>PAN ID Compression</td>
<td>Reserved</td>
<td>Dest. Addressing Mode</td>
<td>Frame Version</td>
<td>Source Addressing Mode</td>
</tr>
</tbody>
</table>


IEEE 802.15.4 MAC Overview

Optional Superframe Structure

Network beacon
- Transmitted by network coordinator. Contains network information, frame structure and notification of pending node messages.

Contention period
- Access by any node using CSMA-CA

Guaranteed Time Slot
- Reserved for nodes requiring guaranteed bandwidth

15ms \( \times 2^n \)
where \( 0 \leq n \leq 14 \)
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)
IEEE 802.15.4 MAC Overview
MAC Data Service

Originator MAC

Recipient MAC

MCPS-DATA.request

Data frame

Acknowledgement
(if requested)

Channel access

MCPS-DATA.confirm

MCPS-DATA.indication
IEEE 802.15.4 PHY Overview
MAC Primitives

MAC Data Service
- MCPS-DATA – exchange data packets between MAC and PHY
- MCPS-PURGE – purge an MSDU from the transaction queue

MAC Management Service
- MLME-ASSOCIATE/DISASSOCIATE – network association
- MLME-SYNC / SYNC-LOSS - device synchronization
- MLME-SCAN - scan radio channels
- MLME- COMM-STATUS – communication status
- MLME-GET / -SET– retrieve/set MAC PIB parameters
- MLME-START / BEACON-NOTIFY – beacon management
- MLME-POLL - beaconless synchronization
- MLME-GTS - GTS management
- MLME-RESET – request for MLME to perform reset
- MLME-ORPHAN - orphan device management
- MLME-RX-ENABLE - enabling/disabling of radio system
802.15.4 MAC Layer Specs

- CSMA-CA (like 802.11) channel access scheme
- Unlike 802.11 no RTS/CTS mechanism (due to relatively low data rate collisions are much less likely)

- Different Modes of Operation Depending on Nature of Traffic
  - Periodic Transmissions
    - Beacon Mode
  - Intermittent Transmissions
    - Disconnection Mode, node not attached to network when it doesn't need to communicate (energy savings!)
  - Low Latency Transmissions
    - Guaranteed Time Slot (GTS), allows for device to get an assigned time slot in super frame (a TDMA scheme)

- 16 bit short addressing scheme or 64bit long addressing scheme

- Four MAC frame types:
  - Beacon Frame
  - Data Frame
  - ACK Frame
  - MAC Command Frame
Non-Beacon Mode (Unslotted CSMA-CA)

Coordinator always active, Node with low duty cycle

Data to Coordinator

Data from Coordinator
**Beacon Mode (Slotted CSMA-CA)**

Nodes *synchronized* with Coordinator

- **Data to Coordinator**
  - Coordinator
  - Beacon
  - Data frame
  - Acknowledgement *(opcional)*
  - Node

- **Data from Coordinator**
  - Coordinator
  - Beacon
  - Data Request
  - Acknowledgement
  - Data frame
  - Acknowledgement
Peer-Peer Transfer

Nodes synchronized with each other

Node 1

Node 2

Data frame

Acknowledgement
Network Layer Functions

- **Starting a network** – able to establish a new network
- **Joining and Leaving Network** – nodes are able to become members of the network as well as quit being members
- **Configuration** – Ability of the node to configure its stack to operate in accordance with the network type
- **Addressing** – The ability of a ZigBee coordinator to assign addresses to devices joining the network
- **Synchronization** – ability of a node to synchronize with another node by listening for beacons or polling for data
- **Security** – ability to ensure end-to-end integrity of frames
- **Routing** – nodes can properly route frames to their destination (AODV, etc.)
Application Support Layer Functions

- Zigbee Device Object (ZDO) maintains what the device is capable of doing and makes binding requests based on these capabilities.

- Discovery – Ability to determine which other devices are operating in the operating space of this device.

- Binding – Ability to match two or more devices together based on their services and their needs and allow them to communicate.
Binding

EP – Endpoint (subunit of a node)
MicaZ, TinyOS, and Zigbee
Micaz Crossbow

- MicaZ motes use the 802.15.4 standard defined in 2003
- MicaZ motes do not use the network and application layers defined by the Zigbee Alliance’s network and application layers
- Zigbee upper layers had not been finalized in time
- MicaZ motes are using TinyOS 1.1.7 and Crossbow’s mesh networking stack
MicaZ Network & Application layers

Network Layer:
- Any Network Layer/ Routing Algorithm can be implemented in TinyOS
  - Many available already

Application Layer
- open-source TinyOS supported
  - Applications can be developed for use with TinyOS
More 802.15.4 Specs

- **MicaZ Power Consumption**
  - 30 μW during sleep
  - 33 mW while active

- **MicaZ Lifetime**
  - ~1 year (Zigbee specifies up to 2 years) *(ATTN!)*

- **MicaZ Range**
  - 75 – 100 m (outdoors)
  - 20 – 30 m (indoors)
MICAz MOTE

- IEEE 802.15.4
- 250 kbps radio
- 4KB SRAM
- 4KB Configuration EEPROM
- 128KB program flash memory
- 512KB measurement log flash memory (xbow estimates > 100000 samples)
- 10 bit Analog to Digital Converter
- Red, Green, & Yellow LEDs
- 51-pin expansion connector
TinyOS

- Open Source Operating System designed for MOTEs
- Programs written in an extension of C called nesC
  - TinyOS is event driven
  - nesC - wire together components that handle events/fire commands through interfaces to build an application (highly modular)
- Preinstalled (8 motes) Surge ad-hoc multi-hop (Destination-Sequenced Distance Vector routing) software (xbow) written in nesC
Simulation Tools

- TOSSIM - TinyOS simulator
  - simulates application code more so than a network simulation like ns2, Opnet

- TinyViz - graphical interface for TOSSIM
  - can be extended with plug-ins
Most important characteristics of WSN

Survey conducted mid-2002 on the characteristics of a wireless sensor network most important to its users:

- Data Reliability
- Battery Life
- Cost
- Transmission Range
- Data Rate
- Data Latency
- Physical Size
- Data Security
Designing with 802.15.4 and ZigBee

IEEE 802.15.4 vs Bluetooth
Motorola 802.15.4 / ZigBee™ features

- 2.4 GHz Band, -92 dBm RX sensitivity at 1% PER
  - IEEE requirement is at least –85 dBm
- Power supply 2.0-3.6 V w/ on-chip regulator, logic interface 1.7 to 3.3
  - Runs off a single Li or 2 alkaline cells
- Complete RF transceiver data modem – antenna in, fully packetized data out
- Data and control interface via standard SPI at 4 MHz minimum
- 802.15.4 MAC supplied
- Four new Motorola HCS08 MCUs will interoperate with the data modem chip
  - Often 802.15.4 functionality can be added to existing systems simply by including the modem chip and reprogramming an existing MCU that may already be in the application
- HC08 RAM/FLASH configurations from 384B/4kB to 2kB/60kB depending upon application SW needs
System Simplicity and Flexibility

ZigBee Example Block Diagram for a Sensor Application

RF Data Modem
- RX Analog/RF
- RX Baseband
- Freq Gen
- SPI/Control
- TX Analog/RF
- TX Baseband
- Power Management

8-bit Microcontroller
- Sensor App
- Sensor Driver
- ZigBee NWK
- 154 MAC

Motorola RF Packet Radio  Motorola 8-Bit MCU
Motorola’s 802.15.4 Platform Advantages

■ One-Stop-Shop Solution
  • Single source for platform solution
    o Integrated Circuits, Reference Designs, Modules, Stack Software, Development Systems

■ Key technology enhancements provide for a superior solution
  • Excellent adjacent channel rejection
    o No external filtering required under most conditions
  • High Sensitivity Radio Solution
    o 7 dBm better than spec – longer range
  • Extended Temperature Operating Range
    o -40°C to +85°C for industrial and automotive applications
  • Operating voltage range optimized for alkaline or lithium primary cells
    o 2.0 Vdc to 3.6 Vdc, disposable
      o Nearly 100% of available battery life whether Alkaline or Lithium
      o Normal 2.7v EOL silicon systems can only get perhaps 30% of available alkaline battery energy
  • Adjustable TX Output power
    o Improved coexistence for short range applications

■ IEEE Participation and ZigBee™ Alliance leadership
  • Technology and standards driver
  • Early access to new technology
IEEE 802.15.4/ZigBee and Bluetooth

- Instantaneous Power Consumption
  - 15.4 Transceivers are “similar” to Bluetooth Transceivers
    - 802.15.4
      - O-QPSK with shaping
      - Max data rate 250kbps over the air
      - 2Mchips/s over the air Direct Sequence Spread Spectrum (62.5ksps*32 spread)
      - -92 dBm sensitivity nominal
      - 40ppm xtal
    - Bluetooth
      - FSK
      - Max data rate 720kbps over the air
      - 1Mmps over the air Frequency Hop Spread Spectrum (79 channels @ 1600 hps)
      - -83 to -84 dBm sensitivity nominal
      - 20ppm xtal

- Instantaneous power consumption will be similar for the raw transceivers without protocol

- Bluetooth’s FHSS makes it impractical to create extended networks without large synchronization cost
IEEE 802.15.4 Protocol Built for the Mission

- 15.4 Protocol was developed for very different reasons than Bluetooth
  - 802.15.4
    - Very low duty cycle, very long primary battery life applications as well as mains-powered
    - Static and dynamic mesh, cluster tree and star network structures with potentially a very large number (>>65534) of client units, low latency available as required
    - Ability to remain quiescent for long periods of time without communicating to the network
  - Bluetooth
    - Moderate duty cycle, secondary battery operation where battery lasts about the same as master unit
    - Wire replacement for consumer devices that need moderate data rates with very high QoS and very low, guaranteed latency
    - Quasi-static star network structure with up to 7 clients (and ability to participate in more than one network simultaneously)
    - Generally used in applications where either power is cycled (headsets, cellphones) or mains-powered (printers, car kits)

- Protocol differences can lead to tremendous optimizations in power consumption
Security Sensors

- **Battery Operation**
  - 2 AA Alkaline or 1 Li-AA cell
- **802.15.4/ZigBee Mode**
  - Non-beacon network environment
- **Sensor process**
  - RC Oscillator waking up MCU and doing network check-in at some interval
    - Many security systems have between ~10 second and ~15 minute requirement
  - On a sensor event, device immediately awakens and reports in to network
Security Sensor Timing

Battery-Powered Sensor

- Interval timer expires: Wake Up

- 256µs CCAx2

- 192µs RX>TX

- ~650µs TX

- 192µs TX>RX

- ~350µs ACK RX

- ~650µs RX Data

- Set Interval timer

- Sleep

Mains-Powered Router

- RX

- RX>TX

- ACK TX OPT: Pending ON

- TX Data

Check-in only ~1640µs

Event and Get Data ~2300µs

RX>TX ~650µs

TX>RX 192µs

RX Data ~650µs
802.15.4 Security Sensor

Any check-in interval exceeding ~14 sec allows sensor to surpass alkaline battery shelf life.

Only at 15-min interval does BT reach battery shelf life.
Body-Worn Medical Sensors

- Heartbeat Sensor
  - Battery-operated using CR2032 Li-Coin cell

- 802.15.4/ZigBee Mode
  - Network environment using Guaranteed Time Slot (GTS)
  - Network beacons occurring either every
    - 960ms or 61.44s (closest values to 1 and 60 s)

- Sensor has two ongoing processes
  - Heartbeat time logging
  - Transmit heart rate and other information (8 bytes total)
    - Instantaneous and average heart rate
    - Body temperature and battery voltage
IEEE 802.15.4/ZigBee vs Bluetooth

Li-Coin Cell Battery Life
(Beacon Interval vs Heartbeat vs Days)

- 802.15.4/ZigBee more battery-effective at all beacon intervals greater than 0.246s
- At beacon interval ~60s, 15.4/ZigBee battery life approx 416 days
- At beacon interval ~1s, 15.4/ZigBee battery life 85 days

Bluetooth 30 days (park mode @ 1.28s)
Summary

- IEEE 802.15.4 and ZigBee
  - Designer concentrates on end application
    - Silicon vendors and ZigBee Alliance take care of transceiver, RF channel and protocol
  - Reliable and robust communications
  - Flexible network architectures
  - Very long primary battery life (months to years to decades)
  - Very inexpensive Bill Of Materials
  - Low system complexity for the OEM

- More Information
  - Motorola: www.motorola.com/zigbee
  - ZigBee: www.zigbee.org
Low Data Rate Wireless Evolution

First Stage
........... 2002 2003
- Proprietary Dominates
- IEEE 802.15.4 Emerges
- System Integrator Focus
- Leading Edge OEMs
- $.1 - $1B Industry
- $1,000 - $100 Unit Cost

Second Stage
2004 2005 2006
- Proprietary Fades
- ZigBee Emerges
- Semiconductor Focus
- Early Adopter OEMs
- $1 - $10B Industry
- $100 - $10 Unit Cost

Third Stage
2007 2008 2009+
- Standards Dominate
- IEEE 1451.5 Emerges
- OEM Focus
- Wireless Ubiquitous
- $10 - $100B+ Industry
- $10 - $1 Unit Cost
## Wireless Networking 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>.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>255 / 65,000</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>
IEEE 802.15.4 Key Features

- **High Data Reliability**
  - DSSS, bi-directional, message acknowledgement, low latency
  - Beacon mode enables Guaranteed Time Slots (priority comm.)

- **Advanced Power Management**
  - Typical monitoring applications good for shelf life of battery

- **Inherent Data Security**
  - Data encryption, message authentication, packet freshness

- **Protocol Simplicity**
  - Designed for minimal cost & complexity
ZigBee Overview

- **Specifications Managed by the ZigBee Alliance**
  - Global consortium of OEMs, IC vendors & tech companies
  - Specify device, network and service discovery / pairing

- **Defining Star, Mesh & Cluster-Tree Networks**
  - Allows users to balance system cost, reliability & battery life

- **Defining Security Management**
  - Extends 32-, 64- & 128-bit AES encryption of 802.15.4

- **Defining Application Profiles & Brand Compliance**
  - Ensures product & application interoperability (e.g., AMR & DSM)
Transmission of IPv6 Packets over IEEE 802.15.4 Networks

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document describes the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly autoconfigured addresses on IEEE 802.15.4 networks. Additional specifications include a simple header compression scheme using shared context and provisions for packet delivery in IEEE 802.15.4 meshes.
6LoWPAN …
what it means for sensors

- Low-Power Wireless Embedded devices can now be connected using familiar networking technology,
  - like ethernet (but even where wiring is not viable)
  - and like WiFi (but even where power is not plentiful)
- all of these can interoperate in real applications
- Interoperate with traditional computing infrastructure
- Utilize modern security techniques

- Application Requirements and Capacity Plan dictate how the network is organized,
  - not artifacts of the underlying technology
Making sensor nets make sense

LoWPAN – 802.15.4
- 1% of 802.11 power, easier to embed, as easy to use.
- 8-16 bit MCUs with KBs, not MBs.
- Off 99% of the time

Web Services
XML / RPC / REST / SOAP / OSGI
HTTP / FTP / SNMP
TCP / UDP
IP
Ethernet  Sonet  802.11
802.15.4, …

IETF 6lowpan
Many Advantages of IP

- **Extensive interoperability**
  - Other wireless embedded 802.15.4 network devices
  - Devices on any other IP network link (WiFi, Ethernet, GPRS, Serial lines, …)

- **Established security**
  - Authentication, access control, and firewall mechanisms
  - Network design and policy determines access, not the technology

- **Established naming, addressing, translation, lookup, discovery**

- **Established proxy architectures for higher-level services**
  - NAT, load balancing, caching, mobility

- **Established application level data model and services**
  - HTTP/HTML/XML/SOAP/REST, Application profiles

- **Established network management tools**
  - Ping, Traceroute, SNMP, … OpenView, NetManager, Ganglia, …

- **Transport protocols**
  - End-to-end reliability in addition to link reliability

- **Most “industrial” (wired and wireless) standards support an IP option**
Key Factors for IP over 802.15.4

■ Header
  › Standard IPv6 header is 40 bytes [RFC 2460]
  › Entire 802.15.4 MTU is 127 bytes [IEEE]
  › Often data payload is small

■ Fragmentation
  › Interoperability means that applications need not know the constraints of physical
    links that might carry their packets
  › IP packets may be large, compared to 802.15.4 max frame size
  › IPv6 requires all links support 1280 byte packets [RFC 2460]

■ Allow link-layer mesh routing under IP topology
  › 802.15.4 subnets may utilize multiple radio hops per IP hop
  › Similar to LAN switching within IP routing domain in Ethernet

■ Allow IP routing over a mesh of 802.15.4 nodes
  › Options and capabilities already well-defines
  › Various protocols to establish routing tables
6LoWPAN – IP Header Optimization

Network IPv6 packet

802.15.4 frame

- Eliminate all fields in the IPv6 header that can be derived from the 802.15.4 header in the common case
  - Source address: derived from link address
  - Destination address: derived from link address
  - Length: derived from link frame length
  - Traffic Class & Flow Label: zero
  - Next header: UDP, TCP, or ICMP

- Additional IPv6 options follow as options
6LoWPAN Fragmentation

- IP interoperability over many links => users not limited by frame size
- IP datagrams that are too large to fit in a 802.15.4 frame are fragmented into multiple frames
  - Self describing for reassembly

Network IPv6 packet

![IP header](net payload (e.g. 1500 bytes))

Multiple 802.15.4 frames

- ![15.4 header](F1 IP chk)
- ![15.4 header](F2 IP chk)
- ![15.4 header](Fn IP chk)
Conclusion

- 6LoWPAN turns IEEE 802.15.4 into the next IP-enabled link
- Provides open-systems based interoperability among low-power devices over IEEE 802.15.4
- Provides interoperability between low-power devices and existing IP devices, using standard routing techniques
- Paves the way for further standardization of communication functions among low-power IEEE 802.15.4 devices
- Offers watershed leverage of a huge body of IP-based operations, management and communication services and tools
- Great ability to work within the resource constraints of low-power, low-memory, low-bandwidth devices like WSN
Future convergence Zigbee/ 6LoWPAN for Internet of Thinks

http://zachshelby.org/2009/02/20/zigbee-vs-ipv6/