ZigBee tutorial

Emad Ebeid  
Ph.D. student @ CS depart  
University of Verona, Italy  
EmadSamuelMalki.Ebeid@univr.it

Davide Quaglia  
Assistant Professor @ CS depart  
University of Verona, Italy  
Davide.Quaglia@univr.it
Outline

- Introduction
- ZigBee frequencies
- ZigBee concepts
  - protocol Stack, Profiles, Clusters
- ZigBee application
  - Addressing
- ZigBee Architecture
  - ZC, ZR, ZED
- Practical part and ZigBee tools
Introduction

- **ZigBee** stands for “Zonal Intercommunication Global-standard, where Battery life was long, which was Economical to deploy, and which exhibited Efficient use of resources.”

- ZigBee stands over IEEE 802.15.4 PHY & MAC

- ZigBee aims:
  - Low data rate
  - Low power consumption
  - Small packet devices
802.15.4/ZigBee Frequencies

- Operates in ISM radio bands:
  - 868 MHz European Band at 20kbps
  - 915 MHz North American Band at 40kbps
  - 2.4 GHz Global Band at 250kbps
# ZigBee and Other Wireless Technologies

<table>
<thead>
<tr>
<th>Market Name</th>
<th>ZigBee™</th>
<th>---</th>
<th>Wi-Fi™</th>
<th>Bluetooth™</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>802.15.4</td>
<td>GSM/GPRS CDMA/1×RTT</td>
<td>802.11b</td>
<td>802.15.1</td>
</tr>
<tr>
<td>Application Focus</td>
<td>Monitoring &amp; Control</td>
<td>Wide Area Voice &amp; Data</td>
<td>Web, Email, Video</td>
<td>Cable Replacement</td>
</tr>
<tr>
<td>System Resources</td>
<td>4KB - 32KB</td>
<td>16MB+</td>
<td>1MB+</td>
<td>250KB+</td>
</tr>
<tr>
<td>Battery Life (days)</td>
<td>100 - 1,000+</td>
<td>1 - 7</td>
<td>.5 - 5</td>
<td>1 - 7</td>
</tr>
<tr>
<td>Network Size</td>
<td>Unlimited (2G)</td>
<td>1</td>
<td>32</td>
<td>7</td>
</tr>
<tr>
<td>Bandwidth (KB/s)</td>
<td>20 - 250</td>
<td>64 - 128+</td>
<td>11,000+</td>
<td>720</td>
</tr>
<tr>
<td>Transmission Range (meters)</td>
<td>1 - 100+</td>
<td>1,000+</td>
<td>1 - 100</td>
<td>1 - 10+</td>
</tr>
<tr>
<td>Success Metrics</td>
<td>Reliability, Power, Cost</td>
<td>Reach, Quality</td>
<td>Speed, Flexibility</td>
<td>Cost, Convenience</td>
</tr>
</tbody>
</table>
ZigBee protocol stack

- ZigBee builds upon the physical layer and medium access control defined in IEEE standard 802.15.4 (2003 version) for low-rate WPANs.
ZigBee products are a combination of Application, Logical, and Physical device types
Profiles may define specific requirements for this combination, but can also leave this up to manufacturers
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 Application profiles

• Determines application-level features, protocol
• Defines device types with different capabilities (clusters)
  – 2 bytes "device ID" enumerates device type within the profile
• Inherits network-level features from stack feature set
• Identified by 2 bytes application profile IDs
  – assigned by ZigBee Alliance
  – can request private profile IDs for custom applications or use one of ZigBee's published application profiles

• Examples:
  – Home Automation (HA) — based on ZigBee or Zigbee Pro
  – Commercial Building Automation (CBA) — based on ZigBee Pro
  – Smart Energy (SE) — based on ZigBee or ZigBee Pro
  – Manufacturer-Specific Profile (MSP) — anything proprietary
A "cluster" is a set of message types related to a certain device function.

Enumerated by **2 bytes** Cluster ID.

Defines clusters for use in public profiles:
- Same cluster (and ID) can be used in multiple profiles.

Defines "attributes" and "commands" for a given cluster.

Groups clusters into "functional domains", e.g. Lighting, HVAC.

Uses "client" and "server" model of communication:
- Client sends messages to server: server maintains attributes.
ZigBee clusters

ZigBee Cluster Library
- Others...
- Closures
- Safety & Security
- Measurement & Sensing
- Lighting
- HVAC
- General

Application Profiles
- Others...
- Commercial Building Auto.
- AMI
- Home Automation
ZigBee addressing

- Addressing is the way in which a message gets from one place to another in a network.
ZigBee addressing

• For 2.4 GHz

<table>
<thead>
<tr>
<th>Name</th>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>11–26</td>
<td>A physical portion of the RF spectrum</td>
</tr>
<tr>
<td>PAN ID</td>
<td>0x0000–0xffff</td>
<td>The address of a network within a channel</td>
</tr>
<tr>
<td>NwkAddr</td>
<td>0x0000–0xfffff</td>
<td>The address of a node within a network</td>
</tr>
<tr>
<td>Endpoint</td>
<td>1–240</td>
<td>The address of an application within a node</td>
</tr>
<tr>
<td>Cluster</td>
<td>0x0000–0xfffff</td>
<td>The object within the application</td>
</tr>
<tr>
<td>Command</td>
<td>0x00–0xff</td>
<td>An action to take within the cluster</td>
</tr>
<tr>
<td>Attribute</td>
<td>0x0000–0xfffff</td>
<td>A data item within the cluster</td>
</tr>
</tbody>
</table>
ZigBee addressing

- The MAC address, also called IEEE address, long address, or extended address, is a 64-bit number that uniquely identifies this board from all other ZigBee boards in the world.
ZigBee architecture

- There are three different types of ZigBee devices:
  - ZigBee coordinator (ZC)
  - ZigBee Router (ZR)
  - ZigBee End Device (ZED)
ZigBee Coordinator (ZC)

- only one in a network
- initiates network
- stores information about the network
- all devices communicate with the ZBC
- routing functionality
- bridge to other networks
ZigBee Router (ZR)

- optional component
- routes between nodes
- extends network coverage
- manages local address allocation/de-allocation
ZigBee End Device (ZED)

- optimized for low power consumption
- cheapest device type
- communicates only with the coordinator via routers
- sensor would be deployed here
## Summary for ZigBee device types

<table>
<thead>
<tr>
<th>ZigBee Type</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZigBee Coordinator (ZC)</td>
<td>Special router that forms the network; only 1 per PAN</td>
</tr>
<tr>
<td>ZigBee Router (ZR)</td>
<td>No duty cycling available</td>
</tr>
<tr>
<td>ZigBee End Device (ZED)</td>
<td>Does not participate in routing; may be sleepy; requires ZC/ZR “parent” for network participation</td>
</tr>
</tbody>
</table>
ZigBee tools

- **Z-Stack™**: is TI's ZigBee compliant protocol stack for a growing portfolio of IEEE 802.15.4 products and platforms
- **IAR**: is a development tools for testing and compiling Z-Stack based applications.
  - It incorporates IAR C/C++ Compiler for ARM Cortex-M3, assembler, linker, librarian, text editor, project manager, and debugger
- **SmartRF™ Studio**: is a Windows application that can be used to evaluate and configure Low Power RF-ICs from Texas Instruments.
Practical part

- Zigbee boards:
  - Chipcon SmartRF04EB Evaluation Board with CC2430EM
Practical part
Practical part

• Zigbee boards:
  – Chipcon CC2430DB Development Board
Open example

- Open GenericApp example (Zstack & IRA tools) from example folder as shown below:
  
  - C:\texasInstrument\Zstack-1.4.2.1.1.0\project\Zstack\samples\GenericApp\CC2430DB\GenericApp
Practical part

– Choose Coordinator or End device based on your board type (ED, DB) and ZigBee role (ZC, ZR, ZED)
Practical part

– then
  • Project-> buildall
  • Project->Debug
    ( for configuration)

Reset zigBee kit from its switch.
– S300 for EB
– S2 for DB

• Repeat these steps to configure other devices
Practical part

- SmartRF tool
  - IEEE address 8 bytes (static)

1. Read
2. Change IEEE
3. Write
RF sniffing

Connected Device
  SoC/Transceiver
  Data Buffer
  USB controller
  Data Buffer

PC
  Abstraction layer
  8 kB buffer
  Temporary Disk file
  Cache buffer
  In RAM
  Screen/GUI
RF sniffing
RF sniffing
RF sniffing

Figure 12: Packet sniffer screenshot from the IEEE802.15.4/ZigBee protocols
Any questions?