Sensor Network Application Development

ZIGBEE INTRODUCTION

Cruise Summerschool
Johannes Kepler University
November 5 - 7, 2007, Linz / Austria
Dipl.-Ing. Andreas Riener
riener@pervasive.jku.at
Overview

Structure of this lesson

- Bluetooth and Zigbee: comparison
- What is ZigBee & the ZigBee-Alliance?
- IEEE 802.15.4: MAC, PHY layers
  - Frequency bands, channels, data rates
- ZigBee Wireless Networking
  - Basics
  - Device types/classes
  - Network topologies
  - How are ZigBee networks formed?
  - Packet fragmentation
  - Routing capabilities
Wireless technologies: data rates and ranges

DATA RATE (Mbps)

RANGE

WWAN

WMAN

WLAN

WPAN

IEEE 802.22

IEEE 802.20

WiMax

IEEE 802.16

ZigBee

IEEE 802.15.4

Bluetooth

IEEE 802.15.1

WiFi

IEEE 802.11

802.15.3

802.15.3a

802.15.3c

Courtesy, ZigBee Alliance
ZigBee and Bluetooth – development timeline

IBM, Nokia, Intel, Toshiba joins Bluetooth

Ericsson

IEEE 802.15.1 std

Motorola and others

Bluetooth SIG

Microsoft, Lucent, 3Com, Motorola joins Bluetooth

ZigBee Alliance

802.15.4 std

ZigBee spec.
Bluetooth objectives

What is Bluetooth?

- ...a short range wireless specification for connecting mobile devices
- ...wireless connectivity with fixed, portable and moving devices within or entering a personal operating space (POS; a POS is the space about a person or object that typically extends up to 10m in all directions and envelops the person whether stationary or in motion)

Bluetooth protocol stack

- Designed and implemented by the Bluetooth SIG
- Definition of “device-profiles” - Bluetooth devices that wish to communicate must support the same profile as each other
- New profiles continue to be developed

Possible applications

- PC and office equipment, automotive, medical, mobile phone, headset, handheld, leisure, at home, etc.
ZigBee objectives

What is ZigBee?

- Open global standard to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products
- Specification for low data-rate wireless connectivity with fixed, portable and moving devices with no battery or very limited battery consumption requirements typically operating in the POS of 10m
- A longer range at a lower data rate may be an acceptable trade-off?

ZigBee protocol stack

- ZigBee has added to 802.15.4 by defining the network layer of the ZigBee stack to support star, mesh and hybrid networking
- Network management that allows certain node types to sleep most of the time to conserve power

Possible applications

- A wide range of products and applications across consumer, commercial, industrial and government markets worldwide
- Focus on remote monitoring and control
ZigBee and Bluetooth – comparative analysis

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>ZigBee</th>
<th>Bluetooth</th>
</tr>
</thead>
<tbody>
<tr>
<td>RANGE</td>
<td>10-100 metres up to 400 metres</td>
<td>10 metres 100+ metres</td>
</tr>
<tr>
<td>DATA RATE</td>
<td>20 – 250 kpbs</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>NETWORK LATENCY (typ.)</td>
<td>30 ms</td>
<td>20 s</td>
</tr>
<tr>
<td>SECURITY</td>
<td>128 bit AES and appl. layer user definable</td>
<td>64 bit, 128 bit</td>
</tr>
<tr>
<td>OPERATING FREQUENCY</td>
<td>868, 915 MHz, 2.4 GHz</td>
<td>2,4 GHz ISM</td>
</tr>
<tr>
<td>COMPLEXITY</td>
<td>Simple</td>
<td>Complex</td>
</tr>
<tr>
<td>NETWORK TOPOLOGY</td>
<td>Ad hoc, star, mesh, hybrid</td>
<td>Ad hoc piconets</td>
</tr>
<tr>
<td>NR. OF DEVICES/NETWORK</td>
<td>2 to 65.000</td>
<td>8</td>
</tr>
<tr>
<td>SCALABLE / EXTENDABLE</td>
<td>Very High / Yes</td>
<td>Low / No</td>
</tr>
<tr>
<td>FLEXIBILITY</td>
<td>Very High</td>
<td>Medium, profile dep.</td>
</tr>
</tbody>
</table>
ZigBee vs. Bluetooth: **Summary**

Both are different by design and are optimized for different applications

- They are complementary in the industrial context
- ZigBee can address a wider range of real industrial requirements
- The underlying reasons for ZigBee is the industries importance to:
  - long-term battery operation
  - greater range and network deployment flexibility
  - mesh network resilience and reliability

**ZigBee**

- Smaller packets over larger network
- Mostly static networks with many, infrequently addressed devices
- “Unattended” battery life

**Bluetooth**

- Larger packets over smaller networks
- Ad-hoc networks with few “always-on”-devices
- Regular recharging or mains power
The 802.15 alphabet soup

802.15 Wireless Personal Area Networks (WPAN)
- 802.15.1 WPAN’s based on Bluetooth
- 802.15.2 Coexistence of WPAN’s and WLAN’s
- 802.15.3 High data rates 20Mbps+ on WPAN
  - 802.15.3a High speed PHY enhancements
  - 802.15.3b High speed MAC enhancements
- 802.15.4 Low rate WPAN
  (low data rate, simple, multi year battery life)
  ...defines only
  a) the PHY (physical layer)
  b) the MAC (media access control)
- 802.15.5 Mesh Networking
What is ZigBee? (Short definition)

ZigBee

- Is a technology that addresses the market needs for cost-effective wireless networking solutions based on IEEE 802.15.4 standard
- IEEE 802.15.4:
  - Wireless MAC (media access control; sublayer of the data link level of OSI model) and PHY (physical layer of OSI model) specifications for low-rate wireless personal area networks (LR-WPANs)
    - Ultra-low complexity, ultra-low cost, ultra-low power consumption, and low data rate (20-250 kb/s) wireless connectivity among inexpensive devices
    - Lower power consumption and lower cost (per node) than other W-PANs (e.g. Bluetooth)
- Designed by Motorola, Philips and other companies to supply the radio and protocol, allowing the designer to concentrate on the application and their customers’ needs
What is the ZigBee Alliance? (Short definition)

ZigBee Alliance

- Non-profit industry consortium defining a global specification for reliable, cost-effective, low power wireless applications based on the IEEE 802.15.4 standard
- Six promoters (Honeywell, Invensys, Mitsubishi, Motorola, Philips and Samsung) and more than 150 participants

Challenges of the alliance

- Defining the network, security and application software layers
- Providing interoperability and conformance software layers
- Promoting the ZigBee-brand to build market awareness (global)
- Managing the evolution of the standards…
ZigBee: Advantages and Applications

Advantages

- Most complex ZigBee node requires only 10% of the code a typical bluetooth node would require
- Simplest ZigBee node require only 2% of the code a typical bluetooth node would require
- ZigBee nodes currently come in at 25% of the cost of bluetooth nodes

Field of applications

- Wireless monitoring
- Building automation
  - Control of lights
  - Security alarms
- Motion sensing, thermostats, pressure sensors, smoke detectors, etc.
- A wireless mouse that works for years (not weeks) without needing new batteries…
ZigBee - Target Markets (1)

- Security
- Climate Control (HVAC*)
- Lighting Control
- Access Control

ZigBee
Wireless Control that Simply Works

- TV
- VCR
- DVD/CD player
- RF remote controls

- Patient monitoring
- Fitness monitoring

- Asset mgt.
- Process control
- Environment energy mgt.

*H-V-AC…heating, ventilation, air-conditioning

- Security
- HVAC*
- Lighting Control
- Access Control
- Lawn&Garden
- Irrigation

Chart Copyright ZigBee Alliance 2004
ZigBee – Target Markets (2)

Estimated Market Size

- Strong growth in areas such as wireless sensors will help the growth of 802.15.4 / ZigBee
  - *In-Stat* 2004 report has an aggressive forecast of over 150 million annual units of 802.15.4 and ZigBee chipsets by 2008
  - *ABI Research* forecasts shipments of ZigBee devices in 2005 at about 1 million, growing to 80 million units by the end of 2006
  - *Harbor Research* reports that by 2008, 100 million wireless sensors will be in use
  - *On World* reports that by 2010 more than 500 million nodes will ship for wireless sensor applications

![Graph showing estimated market size of ZigBee devices from 2005 to 2010.](image-url)
What is a ZigBee-node/mote? (Definition)

Small, autonomous computers, containing:
- Real sensor (GPS, light, temperature, magnetometer, humidity, etc.) that allows data acquisition
- Computing power that allows data processing
- Radio that allows data communication

Characteristics
- **Battery operated**
- Ability to self-organize into ad hoc networks
- Programmable (e.g. running TinyOS, http://www.tinyos.net)
- Various sensor board detachable, multiple sensors per board, sensor boards cascadeable?
- Applications including the civil and military field
ZigBee in three tiers

- **Application/Profiles**: User Defined
  - [APPLICATION]

- **Application Framework**: ZigBee Alliance
  - [ZIGBEE PLATFORM STACK]

- **Network/Security**: Defined by IEEE 802.15.4
  - [SILICON ON CHIP]

- **MAC Layer**

- **PHY Layer**
IEEE 802.15.4: Basics

Simple packet oriented data protocol for lightweight wireless networks
- Released in May 2003
- Channel access via CSMA (carrier sense multiple access) with collision avoidance and optional time slotting mechanism
- Message acknowledgement and an optional beacon structure
- Multi-level security (ZigBee security box)
  - Secure distribution of keys in the network
  - Secure remote control/administration of networks/nw-components
- 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
IEEE 802.15.4: MAC (media access control)

Employs 64 bit IEEE & 16 bit short addresses
- Ultimate network size can be more than we'll probably need… (64 bit adr.)
- Using local (16 bit) addressing, simple networks of 65,536 (= $2^{16}$) nodes are possible (with reduced address overhead)

Three devices types specified
- Network/PAN coordinator (PANC)
- Full function device (FFD)
- Reduced function device (RFD)
- (Bluetooth: only master = coordinator and slave)

More about MAC
- Simple frame structure
- Reliable delivery of data
- Association/disassociation
- AES (advanced encryption standard)-128 security
- CSMA-CA channel access (CA = collision avoidance)
- Optional superframe structure with beacons
- Optional GTS (guaranteed time slots) mechanism
Excurse: the ISM band

- The ISM (industrial, scientific and medical) radio bands were orig. internationally reserved for (non-commercial) RF- (radio frequency) applications for industrial, scientific and medical purposes
- Recently also used for license-free error-tolerant communication applications like WLAN, Bluetooth, ZigBee
  - Possible frequencies: 900 Mhz, 2.4 Ghz band and 5.8 Ghz band

ZigBee transmission rates:

- The **2400 Mhz** (2.4 Ghz) frequency band is recognized as global standard in almost any country (2400 to 2483.50 Mhz @ 250kbps)
  - The **868 Mhz** band has been designed to use as fallback-band (with lower data rate) in europe (868 to 870 Mhz @ 20kbps)
  - The **915 Mhz** band is used as fallback-band in (North-)America, Australia, etc. (902 to 928 Mhz @ 40kbps)
IEEE 802.15.4: PHY (physical layer)

BPSK (binary phase shift keying)
- 868 Mhz PHY in Europe (@ 20kbps), licence free
- 915 Mhz PHY in America (@ 40kbps), licence free

QPSK (quadrature phase shift keying)
- 2400 MHz PHY Worldwide (@ 250kbps), licence free
### IEEE 802.15.4: Summary of frequency bands and data rates (PHY)

<table>
<thead>
<tr>
<th>PHY (Mhz)</th>
<th>Frequ. Band (Mhz)</th>
<th>Channel Numbers</th>
<th>Chip Rate</th>
<th>Mode</th>
<th>Bit Rate</th>
<th>Symbol Rate</th>
<th>Modulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>868</td>
<td>868 – 870</td>
<td>0</td>
<td>300 kchip/s</td>
<td>1)BPSK</td>
<td>20 kb/s</td>
<td>20 ksymbol/s</td>
<td>BPSK</td>
</tr>
<tr>
<td>915</td>
<td>902 – 928</td>
<td>1 – 10</td>
<td>600 kchip/s</td>
<td>BPSK</td>
<td>40 kb/s</td>
<td>40 ksymbol/s</td>
<td>BPSK</td>
</tr>
<tr>
<td>2400</td>
<td>2400 - 2483,5</td>
<td>11 – 26</td>
<td>2 Mchip/s</td>
<td>2)O-QPSK</td>
<td>250 kb/s</td>
<td>62.5 ksymbol/s</td>
<td>16-ary Orthogonal</td>
</tr>
</tbody>
</table>

1) BPSK…Binary phase shift keying  2) O-QPSK…Offset quadrature PSK
ZigBee: Device types/classes (1)

ZigBee coordinator (ZC)

- Acts as 802.15.4 PANC (personal area network coordinator)
- The most capable device
- Is the root of the network tree, initiates network formation
- Capability of bridging to other networks
- Exactly one ZC in a network
- Enabled to store information about the network, including acting as the repository for security keys
ZigBee: Device types/classes (2)

ZigBee routers (ZR)
- Acts as 802.15.4 FFD (full function device)
- Available in any topology
- Capable of becoming a network coordinator, talking to any other device
- Typically continuously active looking for stimuli
- Optional network component
- Participates as an intermediary in multihop routing of messages
- ZR may associates with the ZC or with previously associated ZR

ZigBee end device (ZED)
- Also known as RFD (reduced function device)
- Limited to only star topologies (with a ZC or ZR in the center)
- Cannot become a network coordinator
- Communicates only to a network coordinator (ZC, ZR)
- Simple implementation, therefore efficient, low power consumption
ZigBee: Device types/classes (3)

Tree Structures Address Assignment

Routers at depth \( d+1 \) separated by:

\[
C_{skip}(d) = \frac{1 + C_m - R_m - C_m \cdot R_m^{L_m-d-1}}{1 - R_m}
\]

Address of \( n \)th end device at depth \( d+1 \):

\[
A_n = A_{parent} + C_{skip}(d) \cdot R_m + n
\]

In v1.0 address assignment from NHLE will also be allowed.
ZigBee: **Network topology (1)**

ZigBee supports various network topologies

- **Star (direct) connection**
  - Wire replacement
  - Point to point

- **Star**
  - Central routing and control point
  - Single-hop, point to multi-point
  - All data flows through central point

- **Mesh**
  - Multiple data paths
  - Multi-hop
  - Self configuring, self healing

- **Ad-hoc**

- **Hybrid**
ZigBee: Network topology (2)

Star topology
- single ZC with one or more ZED (or ZR as end devices)
- theoretic maximum of 65,536 (=2^16) nodes (=local addresses)
ZigBee: Network topology (3)

Mesh topology
- Dynamic reconfiguration, “hopping”
- Self-healing
- Very reliable
ZigBee: Network topology (4)

- **ZC** (zigbee coordinator, PANC)
- **ZR** (zigbee router, FFD)
- **ZED** (zigbee end device, RFD)

**Communication** (star link)

**Communication** (mesh link)

Mesh-networking

ZED...only in a star topology!
ZigBee: Network topology (5)

Applications for topology models

- Star Networks (PAN - personal area network)
  - Home automation
  - PC peripherals
    - keyboard, mouse, printer, etc. + “server” as central control
  - Personal health care
    - ECG, respiration, skin conductance, etc. + central analysis

Peer-to-Peer, Mesh (ad hoc network, self organizing & healing)

- Industrial control and monitoring
- Wireless Sensor Networks
- Intelligent Agriculture
ZigBee: **Network topology (6)**

Cluster tree

- ZC (zigbee coordinator, PANC)
- ZR (zigbee router, FFD)
- ZED (zigbee end device, RFD)

Communication (star link)
Communication (mesh link)
ZigBee: **Network topology (7)**

Applications for topology models
- Cluster tree networks
  - Employ multi-hop routing
  - Can be very large
    - 255 clusters of 254 nodes each = 64,770 nodes
- May span physically large areas
- Suitable for latency-tolerant applications
ZigBee: Feature set

Ad hoc, self forming networks
  ▪ Mesh, cluster tree and star

Logical Device Types
  ▪ ZC (coordinator), ZR (router) and ZED (end device)

Applications
  ▪ Device and Service Discovery
  ▪ Messaging with optional responses
  ▪ Home Controls Lighting Profile
  ▪ General mechanism to define private Profiles

Security
  ▪ Symmetric Key with AES-128
  ▪ Authentication & Encryption at MAC, NWK and Application levels
  ▪ Master Keys, Network Keys and Link Keys

Qualification
  ▪ Conformance Certification (Platform and Profile)
  ▪ Interoperability Events
ZigBee: How a network forms (1)

Devices are pre-programmed for their network function

- Coordinator (ZC) scans to find an unused channel to start a network
- Router (ZR, which is a mesh device within a network) scans to find an active channel to join, then permits other devices to join
- ZigBee end device (ZED) will always try to join an existing network

Devices search and discover other devices in the network providing complementary services

- Service Discovery can be initiated from any device within the network

Devices can be bound to other devices offering complementary services

- Binding provides a command and control feature for specially identified sets of devices
ZigBee: How a network forms (2)

Stack architecture basics – addressing
- Every device has a unique 64 bit MAC address
- Upon association, every device receives a unique 16 bit network address
- Only the 16 bit network address is used to route packets in the network
- Devices retain their 16 bit address if they disconnect from the network, however, if they leave the network, the 16 bit address is reassigned
- Network broadcast implemented above the MAC
  - Network address 0xFFFF is the broadcast address
  - Special algorithm in NWK to propagate the message
  - “Best effort” or “guaranteed delivery” options
  - Radius limited broadcast feature
ZigBee: How a network forms (3)

Network Scan
- Device scans the 16 channels to determine the best channel to occupy

Creating/Joining a PAN
- Device (coordinator) can create a network on a free channel or join an existing network

Device Discovery
- Device queries the network to discover the identity of devices on active channels

Service Discovery
- Device scans for supported services on devices within the network

Binding
- Devices communicate via command/control messaging
ZigBee: How a network forms (4)

- Star networks support a single ZigBee coordinator (ZC, ZR) with one or more end devices (up to 65,536 in theory)
- Mesh networks routing permits path formation from any source device to any destination device
ZigBee: How a network forms (5)

- ZigBee coordinator
- “owns” the network
  - Starts it
  - Allows other devices to join
  - Provides binding and address-table services
  - Saves messages until delivering is possible
  - Could also have I/O capabilities
- Is a FFD (full function device)
- Mains powered (e.g. serial-, USB- or network-interface)
ZigBee: How a network forms (6)

**ROUTER**

- Routes messages
- Does not own or start the network
  - Scans to find a network to join
    - Given a block of addresses to assign
- Is a FFD (full function device)
- Mains powered or battery powered (depending on topology)
- Could also have I/O capabilities
ZigBee: How a network forms (7)

- Communications with a single device
- Does not own or start the network
  - But: scans to find a network to join
- Can be an FFD or RFD (reduced function device)
- Normally battery powered
ZigBee: How a network forms (8)

extending a network
- ZED (ZigBee Extension Device)
  - A ZigBee router with a wire interface
- Joins two or more radio disjoint PAN’s
- Provides a “wormhole” within a single PAN
  - A low cost, high reliability link within the radio network
- “Extends” the ZigBee network layer
- Specification is nearly complete with reference ZEDs available soon
ZigBee: How a network forms (9)

gateways to a network
- Joins two different network protocols
  - Network layers are terminated
- Provides a way for non-ZigBee devices to communicate with ZigBee devices without knowing the ZigBee protocol
- Standard specification is still in progress
  - But: already some proprietary and focused solutions available
ZigBee: Traffic types

Traffic types

- **Periodic** data
  - Data rate defined/"dictated" by the application
  - Sensor activates, checks for data/sends, deactivates
  - Example: “regular” sensors

- **Intermittent** data
  - Data rate determined by the application (or external stimulus)
  - Device needs to connect to the network only when communication is necessitated
  - Enables optimum saving on energy
  - Example: light switch, smoke detector

- **Repetitive** (low latency) data
  - Allocation of a-priori fixed time slots, called GTS (guaranteed time slot)
  - Example: input devices (mouse, keyboard)
ZigBee: Data packets (1)

Packet Fields

- Preamble (4 byte) - for synchronization
- Start of packet delimiter (1 byte) - specifies one of 3 packet types
- PHY header (1 byte) - Sync burst flag, PSDU length
- PSDU (0 to 127 bytes) - data
ZigBee: Data packets (2)

Preamble sequence (synchronization)
Start of packet delimiter
Length for decoding simplicity
Frame control specifies the type of MAC frame & the addressing mode

Addressing according to spec. mode
Data sequence number
CRC-16

Max. 127 bytes

MAC header
MAC service data (payload)
MAC footer

PRE SPD LEN FC ADDRESSING DSN Link Layer (PDU) CRC
4 1 1
ZigBee: Routing – Overview

ZigBee routing properties

- AODV is used (= Ad-hoc On-Demand Distance Vector)

- Capable of both,
  - uni-cast routing
  - multi-cast routing

- Reactive protocol, establishes route to destination on demand not proactively like IP routing on the usage of a particular paths

- Network is silent until a connection is needed

- When a link fails, a routing error is passed back to a transmitting node, and the process repeats
### ZigBee: Routing – Frame format

<table>
<thead>
<tr>
<th>Octets: 2</th>
<th>2</th>
<th>2</th>
<th>1</th>
<th>1</th>
<th>Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Frame Control</strong></td>
<td>Destination Address</td>
<td>Source Address</td>
<td>Broadcast Radius</td>
<td>Broadcast Sequence Number</td>
<td>Frame Payload</td>
</tr>
<tr>
<td><strong>Routing Fields</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NWK Header</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NWK Payload</td>
</tr>
</tbody>
</table>

**Frame Control**

<table>
<thead>
<tr>
<th>Bits: 0-1</th>
<th>2-5</th>
<th>6-7</th>
<th>8</th>
<th>9</th>
<th>10-15</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Frame type</strong></td>
<td>Protocol version</td>
<td>Discover route</td>
<td>Reserved</td>
<td>Security</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

Courtesy ZigBee Alliance
ZigBee: Routing – Tree routing

If the following expression is true then a destination device (D) is a descendent of router A

\[ A < D < A + C_{skip}(d - 1) \]

The address of the next hop is

\[ A + 1 + \left\lfloor \frac{D - (A + 1)}{C_{skip}(d)} \right\rfloor \times C_{skip}(d) \]

if the device is a router or (trivially) D if the device is an end device. Otherwise the destination is not a descendant and the message should be routed through A’s parent.
ZigBee: Routing – Table routing

Usage
- In the case where a routing table entry for the destination exists
- Simply consists of extracting the next-hop address from that entry and routing the message through (or to) that address

Routing table fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination address</td>
<td>2 bytes</td>
<td>The 16-bit network address of this route's destination.</td>
</tr>
<tr>
<td>Status</td>
<td>3 bits</td>
<td>The status of the route.</td>
</tr>
<tr>
<td>Next-hop address</td>
<td>2 bytes</td>
<td>The 16-bit network address of the next hop on the way to the destination.</td>
</tr>
</tbody>
</table>

Courtesy ZigBee Alliance
ZigBee: Routing – Route discovery

Usage

- A device wishing to discover (or repair) a route issues a route request command frame which is broadcast throughout the network.

- When the intended destination receives the route request command frame it responds with at least one route reply command frame.

- Potential routes are evaluated with respect to a routing cost metric at both source and destination.
ZigBee: Routing – Route request/reply

Route request command frame:

<table>
<thead>
<tr>
<th>Octets: 1</th>
<th>1</th>
<th>1</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command frame identifier</td>
<td>Command options</td>
<td>Route request identifier</td>
<td>Destination address</td>
<td>Path cost</td>
</tr>
</tbody>
</table>

NWK payload

Route reply command frame:

<table>
<thead>
<tr>
<th>Octets: 1</th>
<th>1</th>
<th>1</th>
<th>2</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command frame identifier</td>
<td>Command options</td>
<td>Route request identifier</td>
<td>Originator Address</td>
<td>Responder address</td>
<td>Path cost</td>
</tr>
</tbody>
</table>

For both: only 1 command option – RouteRepair
### ZigBee: Routing – Route discovery table

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route request ID</td>
<td>1 byte</td>
<td>A sequence number for a route request command frame that is incremented each time a device initiates a route request.</td>
</tr>
<tr>
<td>Source address</td>
<td>2 bytes</td>
<td>The 16-bit network address of the route request's initiator.</td>
</tr>
<tr>
<td>Sender address</td>
<td>2 bytes</td>
<td>The 16-bit network address of the device that has sent the most recent lowest cost route request command frame corresponding to this entry. Route request identifier and Source address. This field is used to determine the path that an eventual route reply command frame should follow.</td>
</tr>
<tr>
<td>Forward Cost</td>
<td>1 byte</td>
<td>The accumulated path cost from source of the route request to the current device.</td>
</tr>
<tr>
<td>Residual cost</td>
<td>1 byte</td>
<td>The accumulated path cost from the current device to the destination device.</td>
</tr>
<tr>
<td>Expiration time</td>
<td>2 bytes</td>
<td>A countdown timer indicating the number of milliseconds until route discovery expires. The initial value is <code>nwkcRouteDiscoveryTime</code>.</td>
</tr>
</tbody>
</table>

Route discovery table fields
ZigBee: Routing – Routing costs

For a link \( l \), the cost to send a message across that link is:

\[
C\{l\} = \begin{cases} 7, \\ \min\left(7, \frac{1}{p_1^4}\right) \end{cases}
\]

where \( p_1 \) is the estimated probability of delivery.

- The pathcost for a multihop route is just the sum of the link costs along the path. This is the metric used to evaluate routes during route discovery and maintenance.
ZigBee: Routing – Route error

Route error command frame:

<table>
<thead>
<tr>
<th>Octets: 1</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command frame identifier</td>
<td>Error code</td>
<td>Destination address</td>
</tr>
</tbody>
</table>
Sensor Network Application Development
ZIGBEE INTRODUCTION

Cruise Summerschool
Johannes Kepler University
November 5 - 7, 2007, Linz / Austria
Dipl.-Ing. Andreas Riener

Univ. Prof. Alois Ferscha
Institute for Pervasive Computing
Altenberger Straße 69, A-4040 Linz/Austria
www.pervasive.jku.at