The ZigBee® RF4CE standard
New application scenarios

Ingolf Leidert, Application Engineer

Atmel Corporation
Table of Contents

- Remote control technology now and tomorrow
- The ZigBee RF4CE standard
- ZigBee RF4CE terms and concept
- Device roles & topologies
- Protocol mechanisms
- ZigBee RF4CE stack internals
- Atmels certified RF4CE stack: RF4Control
- Frame types, service primitives
- Network operation concepts
- New application scenarios
Remote Controls: Past/Present/Future

- Wireless remote controls exist for many decades
- Infrared technology is standard for consumer electronic devices since the 80’s
  - ... Nothing really new for more than 20 years?
- RF technology available since a few years
- No real standard so far ...
Remote Controls: Infrared

Infrared technology

- is established and cheap

But:

- has short range
- needs line-of-sight
- allows only one-way communication
- needs more energy
- is not secure
RF4CE technology

- is a bit more complex and not low cost yet

But:

- has long range and wall penetration
- needs no line-of-sight
- uses two-way communication
- has ultra-low power consumption
- offers 128-bit AES security

And:

- is a certified standard supported by multiple vendors
The ZigBee RF4CE Standard

- RF4CE stands for „Radio frequency for consumer electronics“
- Based on initial specification from the RF4CE consortium:
  - Panasonic, Philips, Samsung and Sony
- Since early 2009 maintained by the ZigBee alliance
- Version 1.00 released in March 2009, downloadable from ZigBee alliance
- Certified end products will carry this logo:
ZigBee RF4CE – device roles & topologies

- Consumer electronics primarily consist of a device that controls and one or more devices that are controlled.

- ZigBee RF4CE defines two primary roles:

  I. Target node
    - PAN coordinator, defines network parameters, starts network
    - Decides about pairing with other nodes
    - Controls frequency agility

  II. Controller node
    - Initiates pairing and discovery process to Target Nodes
    - Implements frequency agility
    - On-demand communication
ZigBee RF4CE Mechanisms

- Channel agile solution operating over three channels
- Incorporates power management mechanism
- Discovery mechanism
- Pairing mechanism
- Multiple star topology with inter-PAN communication
- Various transmission options including unicast, broadcast, acknowledged, unacknowledged, secured and un-secured
- Security mechanism
ZigBee RF4CE Frequency Agility

- ZigBee RF4CE Networks operate on IEEE 802.15.4 channels 15, 20 & 25
  - Channel 15 – 2.425 GHz
  - Channel 20 – 2.450 GHz
  - Channel 25 – 2.475 GHz

- All node types support frequency agility

- Target specifies PAN base frequency

- Target can switch frequency on adverse channel conditions

- Other nodes know where the target was and attempt to transmit

- If target not found, nodes re-acquire by trying each frequency
  - Once found, new channel information is stored for future communications
  - Due to reduced number of channels in use this procedure is very fast
ZigBee RF4CE Frequency Agility

- 802.11b/g Channel 1
- 802.11b/g Channel 6
- 802.11b/g Channel 11

Channel Agility

- 802.11b/g Channel (North America)
- 802.11b/g Spectrum Occupancy (Typical)
- ZigBee RF4CE Channel

2.400 GHz

2.485 GHz

Copyright 2009 ATMEL
RF4CE relies on IEEE 802.15.4 devices with very low power consumption

- Example: Atmel AT86RF231
- TX current
  - with +3dBm TX power: 14 mA
  - with minimum TX power: 7.5 mA
- RX current:
  - at highest sensitivity of -101dBm: 12.3 mA
  - at reduced sensitivity < -101dBm: 11.7 mA
- Sleep current: 20 nA
Two states for Power Save: Active (until event or defined duration) & Standby

Controllers simply turn off when no buttons are being pressed

Targets must also use power save when in standby
  - But must ensure a (human) reasonable reaction time

Power saving utilizes
  - Active period during which the device wakes
  - Duty cycle at which device repeats active period

\[
\text{nwkDutyCycle (no more than 1 sec)}
\]

\[
\text{nwkActivePeriod (min. of 16.8 msec)}
\]

Rx on

Rx off
Security is established during pairing process

Utilizes AES-128

- Security mode: CCM* (ENC-MIC-32)
  - Data confidentiality (via payload encryption)
  - Data authentication (via Message Integrity Code)
  - Replay protection (via frame counter)

Nodes use 128-bit link keys

- Keys are generated automatically, if security is supported
- Keys are stored in the pairing table
ZigBee RF4CE stack architecture

User application

Profile 0x01: ZRC
- Cmd 0x00
- Cmd 0x01
- ... Cmd 0xff
- Vendor specific command set

Profile 0x02:
- Cmd 0x00
- Cmd 0x01
- ... Cmd 0xff
- Vendor specific command set

Profile 0xc0:
- Vendor specific command set

ZigBee RF4CE network layer

IEEE 802.15.4

IEEE 802.15.4 defined
ZigBee RF4CE defined
Vendor specific
Application specific
Atmels RF4Control stack specifics

End-user Application

ZRC

RF4CE NWK

STB

MAC (MCL)

TAL

TFA

TPS

Resource Management (BMM, QMM)

Abstraction of other Peripherals

PAL (TRX Access, Timers, GPIO, IRQ, Stream I/O)

Hardware Platform (i.e. Microcontroller, Board, Configuration)
Atmels RF4Control stack specifics

- **Small footprint:**

<table>
<thead>
<tr>
<th>Build Configuration*</th>
<th>Stack</th>
<th>Basic Demo</th>
<th>Serial Interface</th>
<th>Key Remote Controller</th>
<th>Terminal Target</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Controller</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>w/o security</td>
<td>17.8 kB</td>
<td>+ 0.9 kB</td>
<td>+ 1.2 kB</td>
<td>+ 1.4 kB</td>
<td>-</td>
</tr>
<tr>
<td>w/ security</td>
<td>20.8 kB</td>
<td>+ 0.9 kB</td>
<td>+ 1.3 kB</td>
<td>+ 1.5 kB</td>
<td>-</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>w/o security</td>
<td>25.2 kB</td>
<td>+ 0.7 kB</td>
<td>+ 1.6 kB</td>
<td>-</td>
<td>+ 9.7 kB</td>
</tr>
<tr>
<td>w/ security</td>
<td>29.2 kB</td>
<td>+ 0.8 kB</td>
<td>+ 1.6 kB</td>
<td>-</td>
<td>+ 9.8 kB</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>w/ security</td>
<td>29.6 kB</td>
<td>-</td>
<td>+ 1.6 kB</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

*) Implementations leave room for further footprint optimization.

- **Stack packet also supports Atmels IEEE 802.15.4 transceiver AT86RF212**
  - Allows development of RF remote controls with longer range and better wall penetration by using 780/868/915 MHz frequency bands
ZigBee RF4CE - primitives

- Concept of primitives

Originator (e.g. RF4CE Application) → Request → Service Provider (e.g. NWK) → Indication → Designator (e.g. RF4CE Application) → Response → Confirm
Example for primitive use

Pairing with a target

- A device wants to pair with a target and asks the target for permission.
- The target verifies that this particular controller is allowed to pair. If yes it will sends a positive confirmation.

```
<table>
<thead>
<tr>
<th>Controller RF4CE layer</th>
<th>Target RF4CE layer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify</td>
</tr>
<tr>
<td>Pair request</td>
<td>Pair confirm</td>
</tr>
<tr>
<td></td>
<td>Pair response</td>
</tr>
<tr>
<td></td>
<td>Pair indication</td>
</tr>
<tr>
<td>Controller MAC &amp; PHY</td>
<td>Target MAC &amp; PHY</td>
</tr>
</tbody>
</table>
```

1. Pair request
2. Pair indication
3. Pair response
4. Pair confirm
primitives for network management:

<table>
<thead>
<tr>
<th>Name</th>
<th>Request</th>
<th>Indication</th>
<th>Response</th>
<th>Confirm</th>
</tr>
</thead>
<tbody>
<tr>
<td>NLME-AUTO-DISCOVERY</td>
<td>3.1.2.1</td>
<td></td>
<td></td>
<td>3.1.2.2</td>
</tr>
<tr>
<td>NLME-COMM-STATUS</td>
<td></td>
<td>3.1.2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLME-DISCOVERY</td>
<td>3.1.2.4</td>
<td>3.1.2.5</td>
<td>3.1.2.6</td>
<td>3.1.2.7</td>
</tr>
<tr>
<td>NLME-GET</td>
<td>3.1.2.8</td>
<td></td>
<td></td>
<td>3.1.2.9</td>
</tr>
<tr>
<td>NLME-PAIR</td>
<td>3.1.2.10</td>
<td>3.1.2.11</td>
<td>3.1.2.12</td>
<td>3.1.2.13</td>
</tr>
<tr>
<td>NLME-RESET</td>
<td>3.1.2.14</td>
<td></td>
<td></td>
<td>3.1.2.15</td>
</tr>
<tr>
<td>NLME-RX-ENABLE</td>
<td>3.1.2.16</td>
<td></td>
<td></td>
<td>3.1.2.17</td>
</tr>
<tr>
<td>NLME-SET</td>
<td>3.1.2.18</td>
<td></td>
<td></td>
<td>3.1.2.19</td>
</tr>
<tr>
<td>NLME-START</td>
<td>3.1.2.20</td>
<td></td>
<td></td>
<td>3.1.2.21</td>
</tr>
<tr>
<td>NLME-UNPAIR</td>
<td>3.1.2.22</td>
<td>3.1.2.23</td>
<td>3.1.2.24</td>
<td>3.1.2.25</td>
</tr>
<tr>
<td>NLME-UPDATE-KEY</td>
<td>3.1.2.26</td>
<td></td>
<td></td>
<td>3.1.2.27</td>
</tr>
</tbody>
</table>
- primitives for data transfer:

<table>
<thead>
<tr>
<th>Name</th>
<th>Request</th>
<th>Indication</th>
<th>Confirm</th>
</tr>
</thead>
<tbody>
<tr>
<td>NLDE-DATA</td>
<td>3.1.1.1</td>
<td>3.1.1.2</td>
<td>3.1.1.3</td>
</tr>
</tbody>
</table>
ZigBee RF4CE - basic operation steps

- Network start
- Discovery
- Pairing
- Data transfer
Node initiates & configures stack

Target performs active scan to identify potentially occupied channels
based on network parameters like PAN ID, base channel etc.
  • parameters are stored in network information base (NIB)
  • access to NIB with NLME-SET.request & NLME-GET.request

Primitives:
  • NLME-RESET.request
    • resets RF4CE network layer
  • NLME-START.request
    • if device is configured as target (NIB) it initiates a active scan
    • defines PAN ID and operating channel
RF4CE devices use discovery procedure to find devices that they can be paired to.

Discovery requests sent by originating device (e.g. RC)
- Use broadcast, multi-channel service so multiple devices can respond
  - This allows a list of devices in the “RF vicinity” to be built
- performed on all channels until discovery response is received
  - “Discovery trial“
- Discovery request contains originator informations like:
  - Node capabilities
  - Vendor information (Vendor ID)
  - Application information ("User String", supported & requested device types)

Recipient devices normally inform application of discovery information
- Application decides whether to respond
- Discovery response only sent if application approves
Discovery response sent by recipient device (e.g. TV)
  - Uses unicast service directly back to the originator (e.g. RC)
  - Discovery response contains recipient information
  - Targets can switch into automatic discovery response mode
    - only active for a certain timeframe
    - target automatically responds to discovery requests during that timeframe

Originator devices inform application of all discovery information
  - Application decides whether to pair with a particular device

Primitives:
  - NLME-AUTO-DISCOVERY.request
    - requests automatic discovery response mode
  - NLME-DISCOVERY.request
    - sends discovery requests on all channels
    - switches to next channel after certain duration & can repeat whole procedure
• After successful discovery of a potential node to pair with the device initiates a pairing sequence

• During that the target and the controller establish a secured link

• after successful pairing target and controller create an entry in their pairing table
  ▪ Contains addressing information
  ▪ Application uses this entry via a reference

• Pairing information is stored in non-volatile memory

• Primitives:
  • NLME-PAIR.request
    ▪ initiates the pairing sequence
ZigBee RF4CE – data transmission

- Data transmission only between paired devices
  - can be acknowledged, unacknowledged, unicast, broadcast, single channel, multiple channel

- Data can be encrypted or unencrypted

- Primitives:
  - NLDE-DATA.request
    - sends data to other node
New application scenarios
Paradigm change

- ZigBee RF4CE will change the way we see and use remote controls
- Technology that offers every device capable of handling user input to be used as control entity for consumer electronics
- Due to the standards interoperability new application scenarios for controlling TV’s, DVD players, home audio systems possible
- Really „smart“ remote controls:
  - „RF4CE Apps“ for Smartphones equipped with IEEE 802.15.4 radios can be provided and updated by the Vendor of the CE device
- Security allows transmission of sensitive data (e.g. direct TV home shopping)

> A few RF4CE application scenarios that already exist or will become reality very soon:
1. Start RF4CE TV Control App
   - Use App to switch TV to channel 1

2. Start RF4CE DVD Player Control App
   - Use App to play DVD
Proximity based applications

1. TV Control App started
2. Air Condition Control App started
Control devices from other rooms
Vendors will come up with completely new application scenarios supported by ZigBee RF4CE

You decide what's possible, RF4CE enables it
Thank you!
どうもありがとうございます