Aalto University

The IEEE 802.15.4 Standard and the ZigBee Specifications

Course T-110.5111 (Computer Networks II – Advanced Topics)

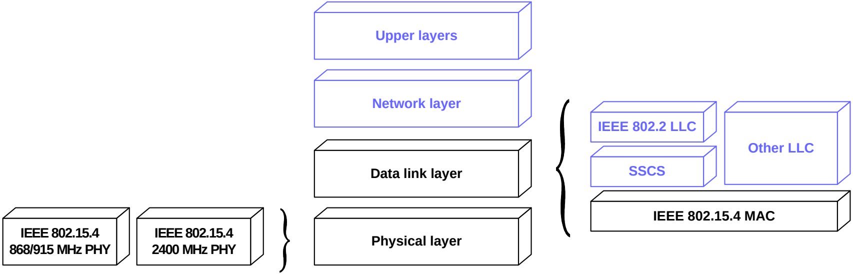
Mario Di Francesco

Department of Computer Science and Engineering, Aalto University

October 13, 2014

The IEEE 802.15.4 Standard

Architecture and objectives



Architecture

- two physical (PHY) layer
- MAC layer
- **ZigBee** for the upper layers

Objectives

- low-rate
- low-power
- low-complexity

Components

Full Function Device (FFD)

Implements the entire standard

- **Coordinator**
  manages (part of) the network
- **PAN coordinator**
  manages the whole PAN (unique in the network)
- **(Regular) Device**
  communicates with FFDs and/or RFDs

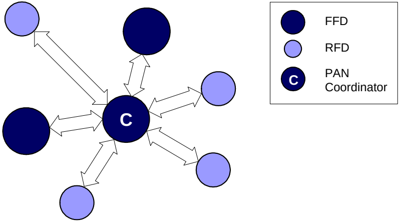
Reduced Function Device (RFD)

Implements a reduced portion of the standard

- **cannot** be a (PAN) coordinator
- **only** communicates with FFDs

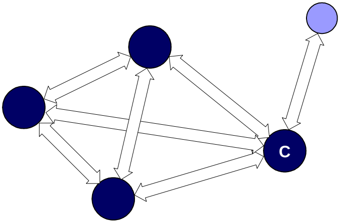
Topology

Star



- all messages flow through the center (hub) of the star

Peer-to-peer



- neighboring nodes can communicate directly
- only available to FFDs

Radio and modulation (1 of 2)

Two distinct physical layers

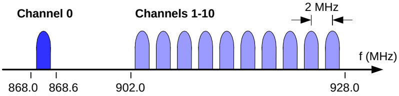
- PHY 868/915 MHz
- PHY 2400 MHz

Shared features

- direct sequence spread spectrum (DSSS)
- ISM (**Industrial, Scientific and Medical**) bands

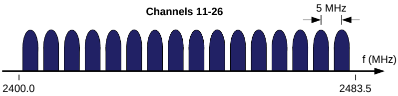
Radio and modulation (2 of 2)

PHY 868/915 MHz



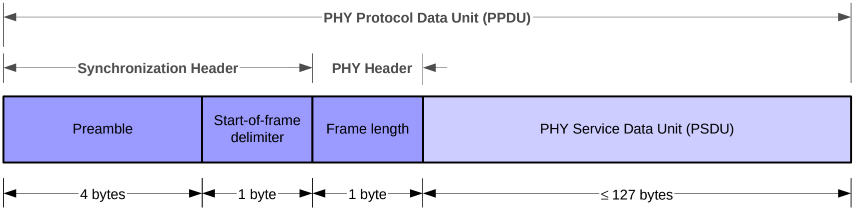
- 868 MHz (Europe)
  1 channel (20 kbps)
- 915 MHz (USA)
  8 channel (40 kbps)
- differential encoding
  (1 sym = 1 bit)
- BPSK encoding

PHY 2400 MHz



- 16 channels
- 250 kbps bandwidth
- orthogonal encoding
  (1 sym = 4 bits)
- O-QPSK modulation

Format of the PHY frame



Header

- synchronization preamble
- delimiter of the PHY frame
- frame length

Payload

- is the same as the MSDU
- maximum size of 127 bytes

Available primitives

Transceiver modes

- RX_ON active
  in **receive** mode
- TX_ON active
  in **transmit** mode
- TRX_OFF inactive
  (**idle** mode)

Channel Selection

Energy Detection (ED)

Link Quality Indication (LQI)

- "quality" of received frames
- SNR, ED, or both

Clear Channel Assessment (CCA)

Different modes

1. energy above threshold
2. carrier sense only
3. combination of 1 and 2

Addressing modes

PAN address

- PANs can be co-located
- 16 bits chosen by the PAN coordinator

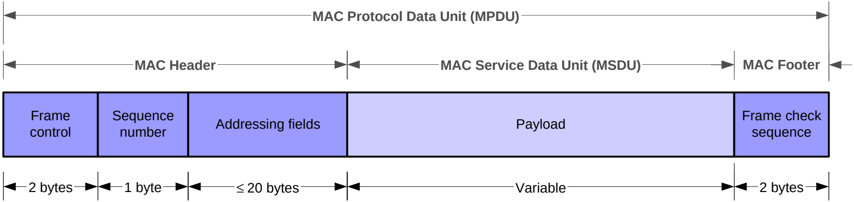
Device address

- 64-bit IEEE Extended Unique Identifier (EUI-64)
  - 24-bit Organizationally Unique Identifier (OUI)
  - 40 bits assigned by the manufacturer
- 16-bit short address
  - assigned by the PAN coordinator during association

Overhead reduction

- flag in the **frame control** field

Format of the MAC frame



Header

- frame control
- sequence number
- addressing fields

Frame payload

Footer

- frame check sequence (FCS) ITU-T CRC-16

Frame types

Beacon frame

- synchronization and management of the PAN
  - list of devices with pending messages
  - superframe parameters

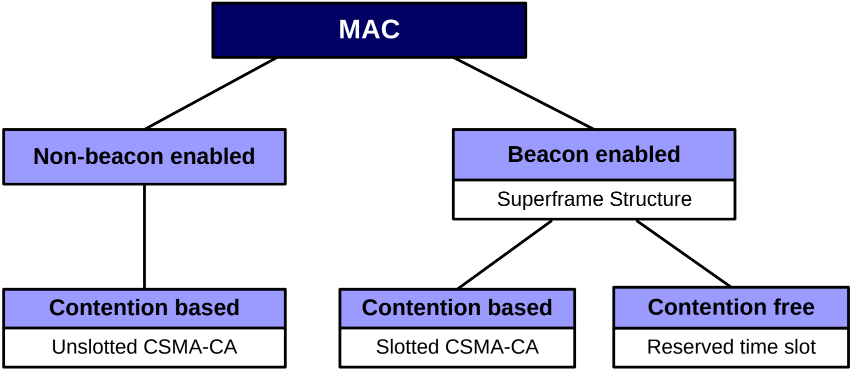
Acknowledgment frame

MAC payload

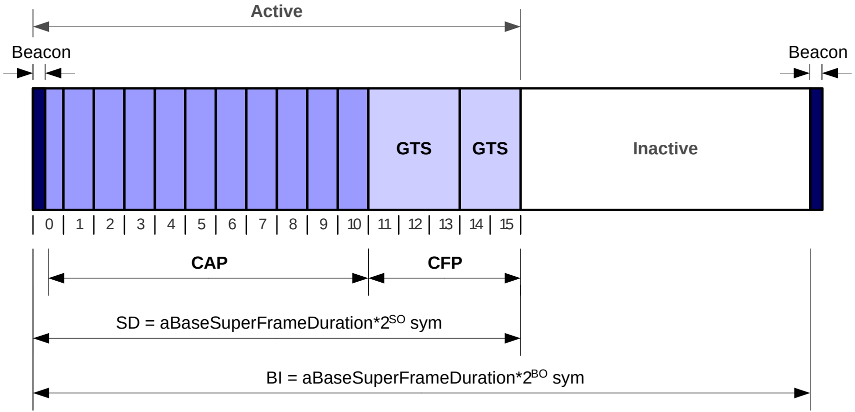
MAC command

- command identifier (1 byte)
- command payload

Channel access methods



Superframe structure



Active period

Contention Access Period (CAP)

- always present in the superframe
- immediately follows the beacon
- slotted CSMA-CA protocol

Contention Free Period (CFP)

- optional
- contiguous slots at the end of the superframe
- without CSMA-CA

All transactions end within the CAP (CFP)

Superframe parameters

Beacon interval

$BI = aBaseSuperFrameDuration \cdot 2^{BO}$ sym

- interval between subsequent beacons
- $0 \leq BO \leq 14$, if $BO = 15$ no beacons

Superframe duration

$SD = aBaseSuperFrameDuration \cdot 2^{SO}$ sym

- duration of the active part
- $0 \leq SO \leq BO \leq 14$, if $SO = 15$ only active period (no duty-cycle)

$aBaseSuperFrameDuration = 960$ sym $\approx 32\ \mu$s (2.4 GHz PHY)

Synchronization

Tracking mode

- the device gets the first beacon
- then activates the transceiver before the subsequent one

Non tracking mode

- the device only gets a single beacon
- it has to reactivate the transceiver for at most *aBaseSuperframeDuration*$\cdot\,(2^{BO}+1)$ sym

Orphaned device

- does not detect beacons for *aMaxLostBeacons* (4) superframes

GTS management

Features of GTSs

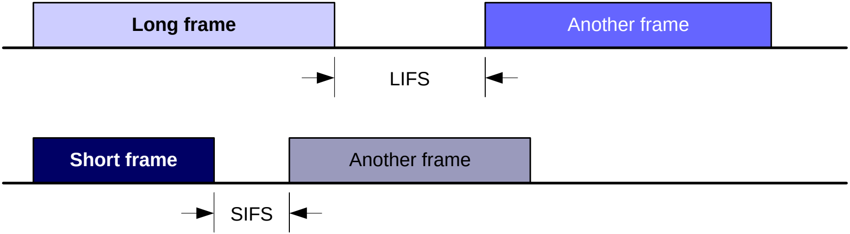
- unidirectional
- at most 7, all in the CFP
- each spanning one or more contiguous slots

GTS allocation

- managed by the PAN coordinator
  - the device requests a GTS to the PAN coordinator
  - the PAN coordinator decides whether to assign it or not
- advertised in the GTS parameters of the superframe
- not always possible
  - no GTS available
  - cannot reduce the size of the CAP further

Frame spacing

Frames need to be separated by an **Inter Frame Space (IFS)**



- if $p_{frame} \leq$ *aMaxSIFSFrameSize* (18) bytes
  then SIFS (**Short IFS**) $\geq$ *aMinSIFSPeriod* (12) sym
- if $p_{frame} >$ *aMaxSIFSFrameSize* bytes
  then LIFS (**Long IFS**) $\geq$ *aMinLIFSPeriod* (40) sym

The CSMA-CA algorithm

Common features

- wait **before** transmitting
- **without** RTS/CTS

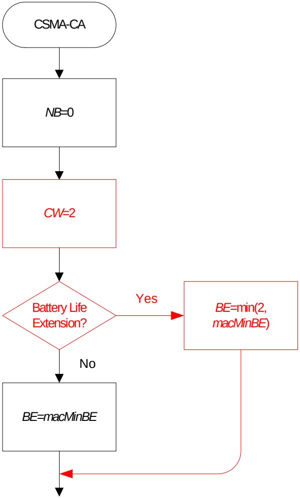
Two variants

- **slotted** (beacon enabled mode CAP)
- **unslotted** (non-beacon enabled mode)

Features

- **backoff period slot** of 20 sym ($\neq$ **superframe slot**)
- slotted variant aligns rx/tx to backoff periods

Initialization



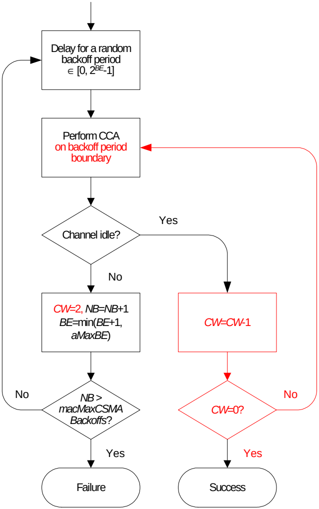
Parameters

- *NB* number of **backoffs** (i.e., *backoff attempts*)
- *CW* **contention window**
- *BE* backoff exponent
- *macMinBE* = 3 (default)

Battery Life Extension

- power saving mode

Main loop



Slotted mode

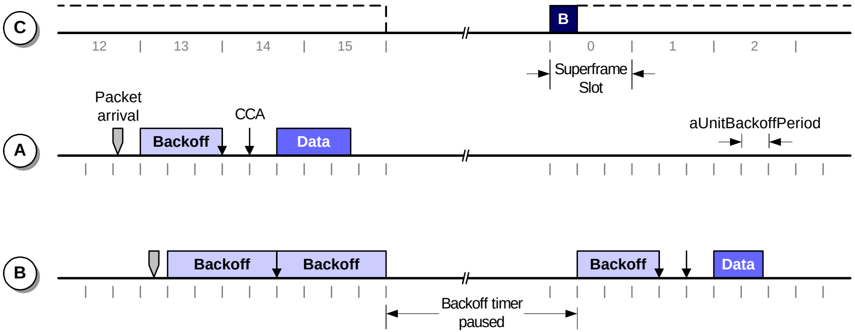
- waiting and CCAs are aligned to backoff periods
- **two CCAs** before tx
- backoff timer stopped at the end of the CAP and reactivated at the beginning of the subsequent one

In both cases

- default max backoffs is 4

Channel access example

Slotted CSMA-CA



Communication reliability

CRC (FCS) check

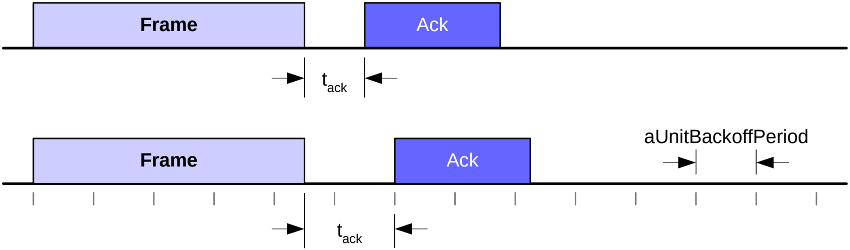
- CRC-16 computed over header and payload
- checked against the FCS

Acks and retransmissions

- at most $aMaxFrameRetries = 3$
- ack waiting time is $macAckWaitDuration$ (54 sym)

Acks and retransmissions

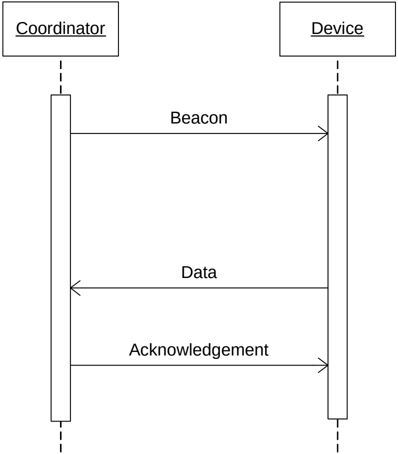
Ack timing



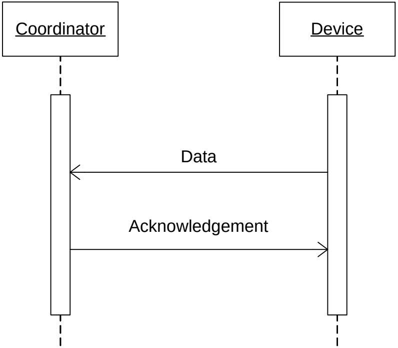
- $t_{ack} = aTurnAroundTime$ (**unslotted**)
- $aTurnAroundTime \leq t_{ack} \leq$ $aTurnAroundTime + aUnitBackoffPeriod$ (**slotted**)
- $t_{ack} < SIFS < LIFS$, at most $aMaxFrameRetries = 3$

Sending data

Beacon enabled (CAP)

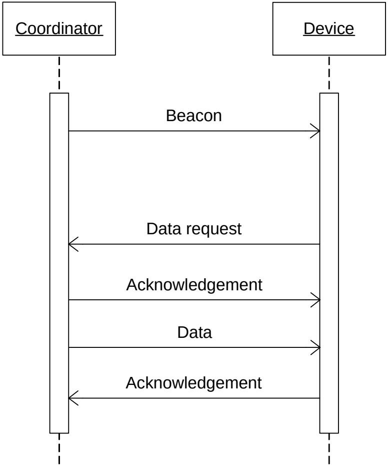


Non-beacon enabled

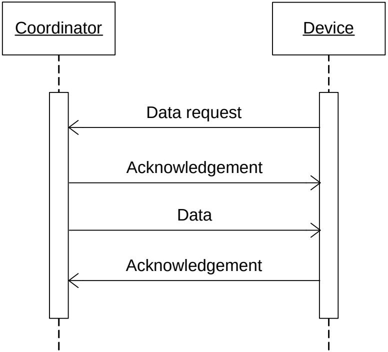


Receiving data (indirect transfer)

Beacon enabled (CAP)



Non-beacon enabled



Peer-to-peer communications

We have previously considered

- star topology
- FFD or RFD devices

Peer-to-peer topology

- only between FFDs
- according to the tx case already seen
  in the non-beacon enabled mode
- synchronization not defined by the standard

Security

Unsecured mode

- no security
- delegated to the upper layers

ACL mode

- based on **Access Control Lists**

Secured mode

- access control
- anti-replay protection
- confidentiality and integrity of messages

Scanning modes

ED channel scan (only FFDs)

- ED of the PHY layer

Active channel scan (only FFDs)

- sends a **beacon request** command
- waits for a reply

Passive channel scan

- waits for a beacon

Orphan channel scan

- resynchronization of orphaned nodes

PAN creation

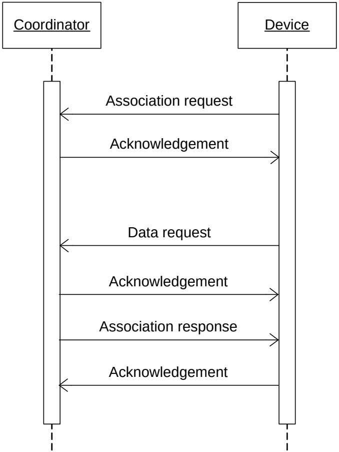
FFD intending to be a PAN coordinator

- starts an **active channel scan**
- selects a (possibly **unused**) channel
- selects a PAN identifier
- starts transmitting beacons (in the beacon-enabled mode)

PAN identifier conflict

- detection and resolution are supported by the MAC layer

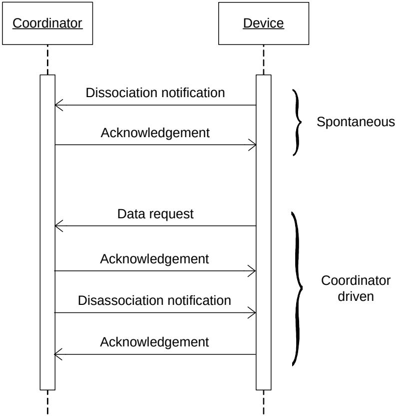
Association



Message exchange

- the first ack does not imply that the request has been accepted
- it depends on available resources
- replies obtained as an indirect transmission
- maximum waiting time *aResponseWaitTime* (30720 sym)

Dissociation



Spontaneous

- decided by the device
- ack not really needed

Forced

- decided by the coordinator
- indirect transfer
- ack not really needed

References

- E. Callaway et al., *Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks*, IEEE Communications Magazine, August 2002
- IEEE 802.15.4, *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, May 2003
- Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta, Y. Fun Hu, *Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards*, Computer Communications, Volume 30, Issue 7, 26 May 2007, Pages 1655–1695

The ZigBee specifications

The ZigBee consortium

ZigBee™ Alliance
Wireless Control That Simply Works

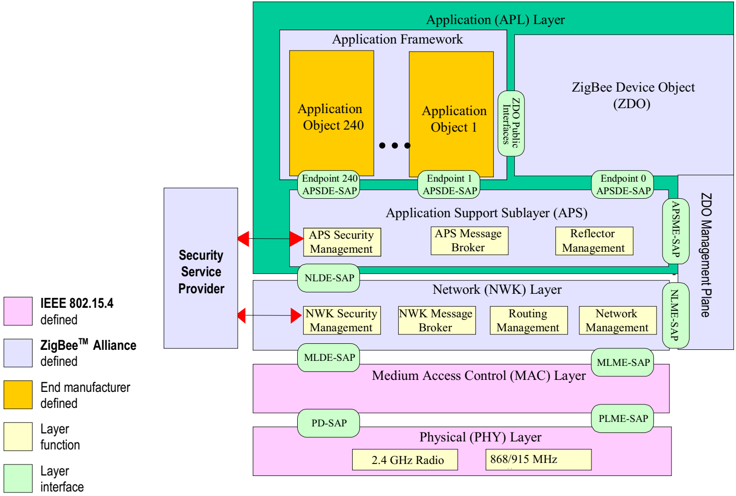
Objectives

- interoperability between platforms of different vendors
- *low-energy*
- *low-cost*
- high node density

Reference scenarios

- industrial and commercial
- consumer electronics and PC peripherals
- personal healthcare and home automation

The protocol stack (1 of 2)



The protocol stack (2 of 2)

The layers

- **Application layer** (APL)
  - service discovery
  - binding between devices and services
  - communication modes
- **Network layer** (NWK)
  - network topology
  - addressing and routing
- physical and MAC layers defined by the IEEE 802.15.4 standard

Other elements

- ZDO Management Plane
- Security Service Provider

ZigBee device model

Type	Description	Elements
Application Device Type	Type of device from the user perspective	Motion detection sensor, light switch, etc.
ZigBee Logical Device Type	Type of device from the network perspective	Network coordinator, router, end device
IEEE 802.15.4 Device Type	Type of ZigBee hardware (radio) platform	Full Function Device, Reduced Function Device

- ZigBee products are a combination of Application, Logical e Physical Device Types
- how to combine the different Device Types is defined by the vendor or by a profile

The application layer (APL)

Sublayers

- **Application Framework** (AF)
  - contains the higher layer application components (**application objects**) defined by the vendor
- **Application Support Layer** (APS)
  - links the application layer to the network layer
- **ZigBee Device Object** (ZDO)
  - is a special application object with management purposes

General concepts (1 of 2)

Profile

- an agreement over messages, formats and actions adopted by the applications running on different devices to create a given distributed application

Component

- a physical object and the corresponding application profile

ZigBee device

- a (set of) component(s) sharing a ZigBee transceiver
- each device has a unique 64-bit IEEE address and a 16-bit network address

General concepts (2 of 2)

Attribute

- an entity representing a physical quantity or state

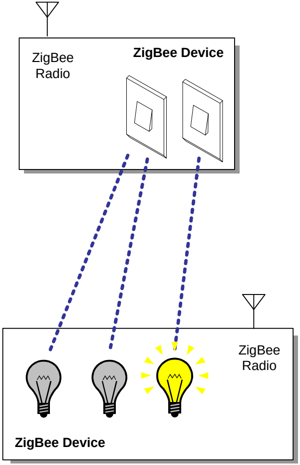
Endpoint

- a specific (sub)component within a ZigBee device
- each device supports up to 240 endpoints
  with distinct addresses

Cluster

- container of attributes or a message
- has a unique 8-bit address within a certain profile

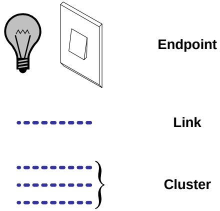
Sample addressing at the application layer



Home Control Profile

- light control (on/off)
- dimmer
- motion detection

Legend



Application Framework (1 of 2)

Features

- contains application objects
- provides two data services
  - key value pair service (KVP)
  - messsage service (MSG)

Observations

- exploits services made available by the APS
- control and management of application objects are handled by the ZigBee Device Object (ZDO)

Application Framework (2 of 2)

Key Value Pair (KVP) service

- allows to manipulate attributes defined within the application objects
- takes an approach based on state variables with transitions
  - `get`, `get response` commands
  - `set`, `event` (and eventual `response`) commands
- uses data structures in compressed XML format

Message (MSG) service

- allows the application profile to use its own frame format
- has more flexibility than the KVP apprach

The application support layer (APS)

Objective

- interfacing the application layer (AP) with the network layer

Features

- generation of messages at the application layer (APDUs)
- binding between devices and services
- transport of APDUs between different devices

Message transmission

Message format

Octets: 1	0/1	0/1	0/2	0/1	Variable
Frame control	Destination end-point	Cluster Identifier	Profile Identifier	Source endpoint	Frame payload
	Addressing fields				
APS header					APS payload

Transmission modes

- direct or indirect transmissions
- unicast or broadcast transmissions
- acknowlegments and (optional) retransmissions

Binding

Definition

- creation of a unidirectional link between devices and endpoints
- every devices keeps a **binding table** with entries in the format

$$(a_s, e_s, c_s) = \{(a_{d1}, e_{d1}), (a_{d2}, e_{d2}), \ldots, (a_{dn}, e_{dn})\}$$

where

a_s address of the source device in the link

e_s endpoint of the source device in the link

c_s cluster identifier used in the link

a_{di} the *i*-th destination device address in the link

e_{di} the *i*-th destination endpoint address in the link

Features of the NWK layer

Objectives

- ensures the proper functioning of the MAC layer
- provides an interface to the application level

Major features

- services for creating a PAN (*ZigBee Coordinator*)
- services for device association (*ZigBee Router* and *End Devices*)
- logical address assignment and routing (*ZigBee Router*)

Network management

Network creation, device association and dissociation

- high-level primitives of the IEEE 802.15.4 standard

Additional functions

- message filtering
- broadcast transmissions

Message format

Octets: 2	2	2	1	1	Variable
Frame Control	Destination Address	Source Address	Radius[a]	Sequence Number[b]	Frame Payload
	Routing Fields				
NWK Header					NWK Payload

ZigBee devices

ZigBee Coordinator

- manages the entire network
- PAN coordinator in IEEE 802.15.4 (*FFD*)

ZigBee Router

- manages device association
- routes the messages to devices
- coordinator in IEEE 802.15.4 (*FFD*)

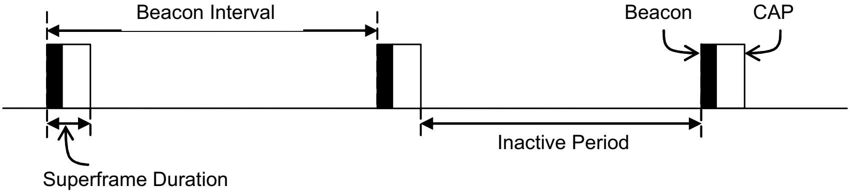
ZigBee End Device

- regular device in the network
- RFD or FFD in IEEE 802.15.4

Network topologies

Tree network

- non beacon-enabled mode of IEEE 802.15.4
- beacon-enabled mode of IEEE 802.15.4
  - active periods of different superframes should not interfere



Mesh network

- corresponds to the peer-to-peer network of IEEE 802.15.4
- devices cannot use IEEE 802.15.4 beacons

Distributed address assignment (1 of 2)

Used in tree networks (**nwkUseTreeAddrAlloc** `= TRUE`)

Parameters

C_m max number of children (per parent) **nwkMaxChildren**

L_m maximum depth of the tree **nwkMaxDepth**

R_m max number of routers (per parent) **nwkMaxRouters**

The address block assigned by each parent at level d to their own (child) routers is

$$C_{skip}(d) = \begin{cases} 1 + C_m \cdot (L_m - d - 1) & \text{if } R_m = 1 \\ \dfrac{1 + C_m - R_m - C_m \cdot R_m^{L_m - d - 1}}{1 - R_m} & \text{otherwise} \end{cases}$$

Distributed address assignment (2 of 2)

Parent node

- accepts children if $C_{skip}(d) > 0$
- uses $C_{skip}(d)$ as offset for router childrens
- the n-th address A_n is given by

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

with $1 \leq n \leq (C_m - R_m)$ and A_{parent} the parent address

Observations

- addresses are sequentially assigned
- a block of addresses cannot be shared between multiple devices
  - one parent can run out of addresses
    while another parent has unused addresses

Address assigned by upper layers

Used in the general case (**nwkUseTreeAddrAlloc** `= FALSE`)

Layer above the network

- picks the block of addresses to assign
- next address to assign **nwkNextAddress**
- number of available addresses **nwkAvailableAddresses**
- step used when assigning addresses **nwkAddressIncrement**

Algorithm

- a router accepts associations if **nwkAvailableAddresses** > 0
- the device is assigned the address **nwkNextAddress**
- the router decrements **nwkAvailableAddresses**
  and adds **nwkAddressIncrement** to **nwkNextAddress**

Hierarchical routing

Finding the descendants

- D is a descendant of A (at level d) if

$$A < D < A + C_{skip}(d-1)$$

Forwarding towards descendants

- if D is an **End Device**[1] the next hop is $N = D$
- if D is a **Router** the next hop is

$$N = A + 1 + \left\lfloor \frac{D-(A+1)}{C_{skip}(d)} \right\rfloor \cdot C_{skip}(d)$$

[1] I.e., $D > A + R_m \cdot C_{skip}(d)$

Table-driven routing

Features

- uses a simplified version of the
  Ad Hoc On Demand Distance Vector Routing (AODV) protocol
- every device with enough memory resources
  keeps a routing table

Hybrid solution

- hierarchical and table-driven routing can be used together
  - if the destination is in the routing table
    then the corresponding entry is used
  - if the destination is not known and the routing table has room
    for a new entry then the device starts route discovery
  - otherwise messages are routed along the tree

Routing metric (1 of 2)

Definitions

P path of length L, i.e., $(D_1, D_2, \ldots, D_L)$

(D_i, D_{i+1}) link (sub-path of length 2)

$C(D_i, D_{i+1})$ cost of the link (D_i, D_{i+1})

Cost of a link

- cost of a link l

$$[0, 1, \ldots, 7] \ni C\{l\} = \begin{cases} 7 \\ \min\left(7, \text{round}\left(\frac{1}{p_l^4}\right)\right) \end{cases}$$

where p_l is the probability of delivering a message over link l

Routing metric (2 of 2)

Path cost

- path cost

$$C\{P\} = \sum_{i=1}^{L-1} C\{(D_i, D_{i+1})\}$$

Observations

- p_l can be estimated through the LQI of IEEE 802.15.4
- use of the metric
  - route discovery
  - route maintenance

References

- ZigBee Alliance, *ZigBee Specification, Version 1.0*, December 2004
- Don Sturek, *ZigBee V1.0 Architecture Overview*, ZigBee Open House Presentations, Oslo, June 2005
- Ian Marsden, *Network Layer Technical Overview*, ZigBee Open House Presentations, Oslo, June 2005
- Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta, Y. Fun Hu, *Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards*, Computer Communications, Volume 30, Issue 7, 26 May 2007, Pages 1655–1695