

TAMPEREEN AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

Tietoliikennetekniikka

Tutkintotyö

Joni Jokipii

ZigBee-lähetin

Tutkintotyö, joka on jätetty opinnäytteenä tarkastettavaksi insinöörin tutkintoa varten
Tampereella 2.6.2009.

Työn ohjaaja: Ari Rantala

Tampere 2009

Tietotekniikan koulutusohjelma, Tietoliikennetekniikka

Joni Jokipii

Tekijä: Joni Jokipii
Työn nimi: ZigBee-lähetin
Päivämäärä: 2.6.2009
Sivumäärä: 46 sivua + 1 liite
Hakusanat: ZigBee, AES, 802.15.4, lähetin, kehys
Koulutusohjelma: Tietotekniikka
Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työ ohjaaja: Ari Rantala, Tampereen ammattikorkeakoulu

TIIVISTELMÄ

Työssäni oli tarkoitus tutkia Jennicin ZigBee-laitteistoa. Ideana oli katsoa, mitä ZigBee-lähetin pitää sisällään ja samalla selvittää, mistä eri komponenteista laite on rakennettu sekä mahdollisesti toteuttaa laite itse. Se ei kuitenkaan ollut mahdollista, koska melkein kaikki lähettimen osat oli integroitu yhdelle ohjelmoitavalle piirille.

Jouduin siis vaihtamaan hieman työ tavoitteita. Tavoitteeksi valitsin ZigBee-lähettimen toiminnan ja standardin perusteiden selvittämisen. Tutkimuskohteena oli Jennicin piiri JN5139.

Aloitin mittaamalla, kuinka pitkiä yhteysvälejä keraamisella antennilla saa. Tästä siirryin mittaamaan, kuinka hyvin laitteet kuuluvat sisätiloissa kerrosten läpi. Lopuksi mittasin isommilla antenneilla, kuinka pitkän yhteysvälin niillä saa.

Ulkona sain yhteysväliksi keraamisella antennilla 92 metriä. Sisällä Signaali kantoi kolmen kerroksen läpi. Isommilla antenneilla yhteysväliksi muodostui 460 metriä.

Tulokset ovat hyviä, koska uusin mittaukset useasti ja käytin virtalähteenä mittauksissa aina ladattuja akkuja.

Author: Joni Jokipii
Title: ZigBee transmitter
Date: 2.6.2009
Number of pages: 46 pages + 1 attachment
Keywords: ZigBee, AES, 802.15.4, transmitter, frame
Degree programme: Computer System Engineering
Specialisation: Telecommunications Engineering and Data Network Systems

Thesis supervisor: Ari Rantala, TAMK University of Applied Sciences

ABSTRACT

My job was to explore Jennic ZigBee device. The idea was to examine what ZigBee transmitter includes and how it is built. Second task was to make own ZigBee chip. That was impossible because all the components of the transmitter was integrated to one programmable chip.

So I had to exchange my work goals. I chose a ZigBee transmitter and its basic operations for my goals. The research target was Jennic's JN5139 chip.

I started by measuring how long was the connection between two Jennic's devices. The result was 92 meters with ceramic antenna. Then i moved to measure how well the devices penetrate through the floors. Signal went through 3 floors. Finally, I measured with larger antennae how long the connection between them was. The result was 460 meters.

The results are good because I renewed them several times and I used charged batteries for the power source.

Alkusanat

Tämä työ on tehty Tampereen ammattikorkeakoulun tietoliikennetekniikan insinöörityönä.

Työssä käsitellään IEEE:n 802.15.4- ja ZigBee 2006-standarien yleisimpiä asioita, kuten lähetin, verkkotopologiat, verkon laitteet ja tiedonsiirtokehykset. Lisäksi ZigBee standardista on esitelty verkon avaimien hallinta ja tietoturva.

Tampereella 2. kesäkuuta 2009

Joni Jokipii

Sisällys

TIIVISTELMÄ.....	i
ABSTRACT	ii
Alkusanat	iii
Sisällys.....	iv
Lyhenteiden ja merkkien selitykset	vi
1 Johdanto.....	1
2 ZigBee	2
2.1 Mitä Zigbee tarkoittaa	2
2.2 Zigbee-standardin historia	2
2.3 ZigBee Allianssi	3
3 ZigBee- ja 802.15.4-standardi	4
3.1 Verkkotopologia	4
3.1.1 Peer-to-peer -verkko	4
3.1.2 Tähtiverkko.....	5
3.1.3 Rypäsverkko	5
3.1.4 Mesh-verkko.....	6
3.2 ZigBee-verkon osat.....	7
3.2.1 Full function device (FFD)	7
3.2.2 PAN-koordinaattori	7
3.2.3 Reduced function device (RFD)	8
3.3 ZigBeen lähetysteho 2,4 GHz:n taajuusalueella.....	9
3.4 ZigBee-verkon osoitteet ja käyttäjämäärät	9
3.5 Tietoliikennetyypit ja liikennöintitilat	10
3.6 Taajuudet ja siirtonopeudet	11
4 ZigBee-lähetin: Jennic JN5139	13
4.1 Radiolähetin.....	13
4.2 Antennin diversiteetti	14
4.3 Modeemi	15
4.4 Kantataajuusprosessori	16
4.5 Lähetys.....	17
5 ZigBee mittaukset.....	19
5.1 Mittaukset	19
5.2 Tulokset	20
6 Tietoturva	22
6.1 AES -salaukset.....	22
6.2 Avainten hallinta ja avaimet	22

Tietotekniikka, tietoliikennetekniikka

Joni Jokipii

7 Liikennöinnit ja kehykset	24
7.1 Liikennöinnit	24
7.1.1 Tiedonsiirto päätelaitteelta koordinaattorille.....	24
7.1.2 Tiedonsiirto koordinaattorilta päätelaitteelle.....	26
7.1.3 Peer-to-peer tiedonsiirto	27
7.2 Kehykset	27
7.2.1 Superkehys	28
7.2.2 Beacon-kehys	30
7.2.3 Datakehys	31
7.2.4 Kuittauskehys	32
7.2.5 MAC-käskykehys	33
8 MAC-alikerros.....	35
9 Datan saapumisen varmistus	36
9.1 CSMA/CA	36
9.2 Kuittaukset.....	37
9.3 Datan virheettömyys.....	37
10 Modulaatiot ZigBee-verkossa ja DSSS	38
10.1 Binäärinen vaihevainnus (BPSK)	38
10.2 O-QPSK (Offset quadrature phase-shift keying)	39
10.3 DSSS (Direct Sequence Spread Spectrum)	40
11 Käyttötarkoitus, käyttökohteet ja tulevaisuus.....	41
11.1 Käyttötarkoitus ja käyttökohteet.....	41
11.2 Tulevaisuus	41
12 Yhteenvedo.....	43
Lähteet	44
Liitteet.....	46

Lyhenteiden ja merkkien selitykset

AES	Edistyksellinen salaus standardi (Advanced encryption standard)
BPSK	Binääri vaiheavainnus (Binary phase-shift keying)
CAP	Kilpailuaikaväli (Contention Access Period)
CFP	Aikaväli, jossa ei kilpailua (Contention Free Period)
CSMA/CA	Kaistanvaraustekniikka (Carrier Sense Multiple Access with Collision Avoidance)
DAC	Digitaal-Analogi-muunnin (Digital-to-analog converter)
DSSS	Suorasekventointi (Direct Sequence Spread Spectrum)
EIRP	Säteilyteho (Effective isotropically radiated power)
FFD	Päätelaite, joka toteuttaa standardin kokonaan (Full Function Device)
GTS	Taattu aikaväli (Guaranteed Time Slot)
IEEE	Tekniikan alan järjestö (Institute of Electrical and Electronics Engineers)
ISM	(Industrial, Scientific and Medical)
MAC	OSI-mallin yksi kerros (Medium Access Control)
O-QPSK	Orthogonaalinen vaiheavainnus (Offset Quadrature Phase-Shift Keying)
OSI	Protokolla malli (Open System Interconnection)
PHY	Fyysinen kerros (Physical layer)
PLL	Vaihelukitusilmukka (Phase locked loop)
RFD	Päätelaite, joka toteuttaa standardin osittain (Reduced Function Device)
VCO	Jänniteohjattu oskillaattori (Voltage controlled oscillator)
WPAN	Langaton henkilökohtainen lähiverkko (Wireless Personal Area Network)

1 Johdanto

IEEE 802.15.4-standardi määrittelee tekniikan lyhyen kantaman langattomaan kommunikointiin. ZigBee-standardi on tästä hieman kehitetty versio, jossa perusajatus on käytännössä sama kuin IEEE:n määrittelemässä standardissa. Lähtökohdat kummassakin standardissa ovat olleet mahdollisimman alhainen virrankulutus, toteutusten yksinkertaisuus ja edullisuus.

Zigbee Alliance, joka on kehittänyt ZigBee 2006 -standardin, on taloudellista voittoa tavoittelematon kansainvälinen yritysten yhteenliittymä. ZigBee Alliancen tehtävänä on ollut suunnitella 802.15.4-standardiin perustuvaa ZigBee-standardia ja siinä se on onnistunutkin. Tämä raportti tutkii juuri ZigBee-standardia ja siihen liittyviä tärkeitä asioita.

ZigBee-laitteiden ideana on ollut se, että ne olisivat täysin yhteensopivia laitevalmistajista riippumatta. Tämän on mahdollistanut standardoimisen jo hyvissä ajoin. ZigBee-tekniikka saattaa mahdollistaa tulevaisuudessa jokaisen elektronisen laitteen ja jopa ihmisten liittämisen verkkoon?

2 ZigBee

Työn tarkoituksena oli selvittää millainen on ZigBee-standardi. Työssä oli myös tarkoitus luoda hyvä peruskuva ZigBee-verkosta ja -laitteistosta. Seuraavissa alaluvuissa esitellään mitä ZigBee tarkoittaa, standardin historia ja ZigBee Allianssi.

2.1 Mitä Zigbee tarkoittaa

Termi ZigBee tulee alun perin mehiläisistä. Tekniikoita, joita mehiläiset käyttävät tiedottaessaan uusista ruokapaikoista yhdyskunnan jäsenille, kutsutaan nimellä Zigbee. (ZigBee 2009, 1.)

Tässä yhteydessä Zigbee tarkoittaa Institute of Electrical and Electronics Engineers 802.15.4 -standardin mukaista lyhyen kantaman langatonta tietoliikenneverkkoa. Tämä 802.15.4 -standardi määrittelee vähävirtaisen henkilökohtaisen verkon eli Wireless Personal Area Network:n tai lyhyesti WPAN:n. Kyseinen 802.15.4 standardi määrittelee verkon OSI- mallin fyysisen ja siirtoyhteyskerroksen. ZigBee -standardin tarkoituksena on määritellä lisäksi OSI-mallin verkkoyhteys- ja kuljetuskerroksen. OSI-mallin sovelluskerros on sen sijaan jätetty muiden toteutettaviksi. (ZigBee 2009, 1.)

2.2 Zigbee-standardin historia

Ensimmäiset ZigBeeen kaltaiset standardit julkaistiin vuonna 1998, kun useat insinöörit huomasivat, että langaton lähiverkko ja Bluetooth eivät ole sopivia muutamiin tiettyihin käyttötarkoituksiin, kuten esimerkiksi sensoriverkkoihin, joissa tarvitaan pieni virrankulutus ja kohtuullisen pitkä yhteysväli. Institute of Electrical and Electronics Engineers kehittikin tätä käyttötarkoitusta varten standardin 802.15.4, joka valmistui vuonna 2003. (ZigBee 2009, 1.)

Standardin valmistumisen jälkeen suuri rahoittaja Philips Semiconductors kuitenkin vetäytyi projektista. Sen jälkeen Philips Lighting on jatkanut projektissa mukana ja on edelleen tutkijajäsenenä Allianssin lautakunnassa. (ZigBee Alliance verkkosivut, 2.)

Vuonna 2004 ZigBee Allianssi ilmoitti jäsenmääränsä olevan yli 100. ZigBee-standardi hyväksyttiin maailmanlaajuisesti joulukuussa 2004. Vuonna 2005 Allianssi julkisti ZigBeen version 1.0 olevan vapaasti käytössä ei-kaupalliseen käyttöön. Syyskuussa 2006 Allianssi julkaisi päivitetyn ZigBee-standardin nimeltään ZigBee 2006. Nykyään Allianssissa on ilmoitettu olevan yli 175 jäsentä. (ZigBee Alliance verkkosivut, 2.)

2.3 ZigBee Allianssi

ZigBee Allianssi on yritysten ja yksityishenkilöiden ryhmittymä, joiden tehtävänä on luoda, testata ja kehittää luotettavaa sekä vähätehoista ja edullista langatonta verkkoratkaisua, joka perustuu avoimeen maailmanlaajuisen standardiin. Allianssiin kuuluu monia suuria yrityksiä kuten HP, Intel ja Philips. Allianssin perustajajäseninä toimivat Honeywell, Invensys, Motorola, Mitsubishi, Philips ja Samsung. Allianssiin liittyminen edellyttää jäsenmaksun maksamista, mutta samalla se oikeuttaa standardin käyttämiseen kaupalliseen tarkoitukseen. Allianssi on perustettu vuonna 2002. Sen perusjäsenmaksu on 3500 dollaria vuodessa. (ZigBee Alliance verkkosivut, 2)

3 ZigBee- ja 802.15.4-standardi

Standardit 802.15.4 ja ZigBee eroavat vain hieman toisistaan. Käytännössä ZigBee on vain kehitetty 802.15.4-standardi, johon on lisätty muutama käytännöllinen yksityiskohta. Nämä kehitetyt kohdat koskevat esimerkiksi tietoturvaa ja verkon tietoturva-avaimien hallintaa.

3.1 Verkkotopologia

Verkkotopologiat ZigBee-verkossa ovat hyvin samanlaisia kuin esimerkiksi Ethernet-verkossa. Laitteilla on mahdollista muodostaa niin sanottuja Peer-to-peer-verkkoja, rypäsverkkoja, mesh-verkkoja sekä tähtiverkkoja. Eri verkkotopologiat ovat esitetty Kuvissa 1, 2 ja 3. Kuvissa harmaat pallot ovat ”tyhmiä” päätelaitteita eli Reduce Function Device (RFD), keltaiset pallot kuvaavat Full Function Device (FFD) ja siniset pallot kuvaavat koordinaattoreita. (Software Technologies Group 2009, 3.)

3.1.1 Peer-to-peer -verkko

Peer-to-peer-ratkaisu, silloin kun käytetään vain kahta laitetta, on kaikkein yksinkertaisin verkkoratkaisu mitä ZigBeellä voidaan toteuttaa. Tähän verkkoon kuuluu vain yksi koordinaattori ja yksi RFD. Verkko on esitetty Kuvassa 1 vasemmalla. Kuvassa sininen pallo kuvaa koordinaattoria, harmaa RFD:tä eli ”tyhmää” päätelaitetta ja keltainen FFD:tä eli ZigBee-reititintä. Peer-to-peer-verkko voi olla Ad hoc, itse järjestäytyvä ja itse korjautuva. Verkko voi myös sallia monta hyppyä (hops), jotta viesti saadaan toiselta laitteelta toiselle. Tämä mahdollistetaan vain OSI-mallin korkeammilla kerroksilla, joita ei IEEE:n 802.15.4 standardissa määritellä. (Software Technologies Group 2009, 3.)

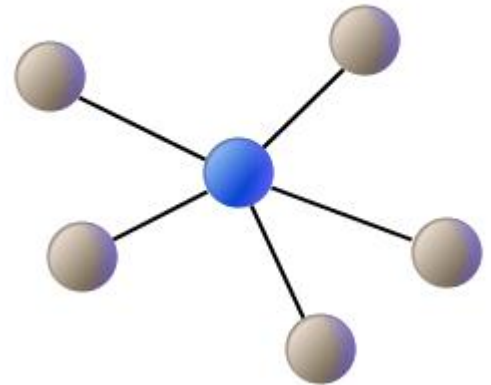
3.1.2 Tähtiverkko

Tähtiverkko ei juuri eroa Peer-to-peer-verkosta, mutta nyt yhden RFD:n tilalla monta RFD:tä. Verkko on esitetty Kuvassa 1 oikealla.

Peer to peer -verkko



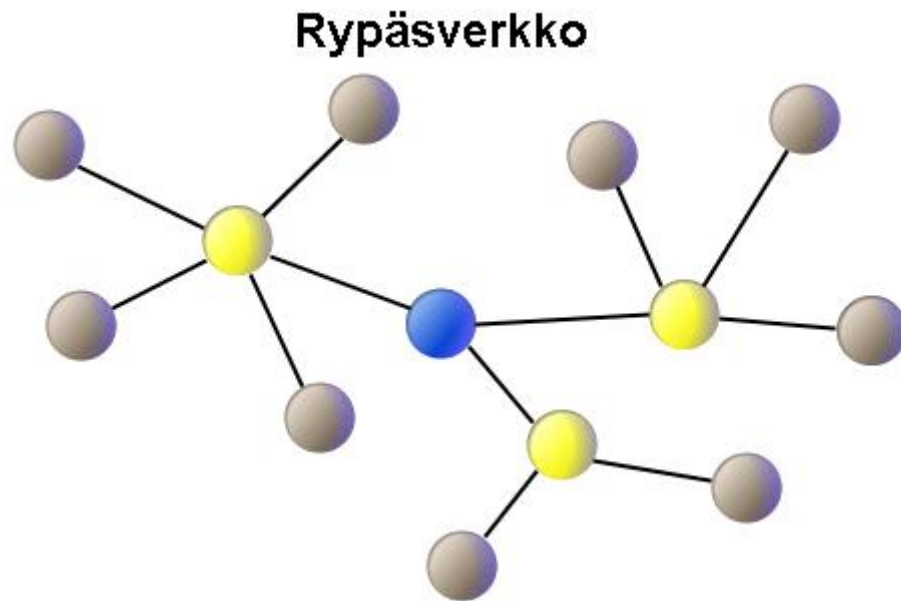
Tähtiverkko



Kuva 1: Peer-to-peer-verkon ja tähtiverkon topologiat (Software Technologies Group 2009, 3.)

3.1.3 Rypäsverkko

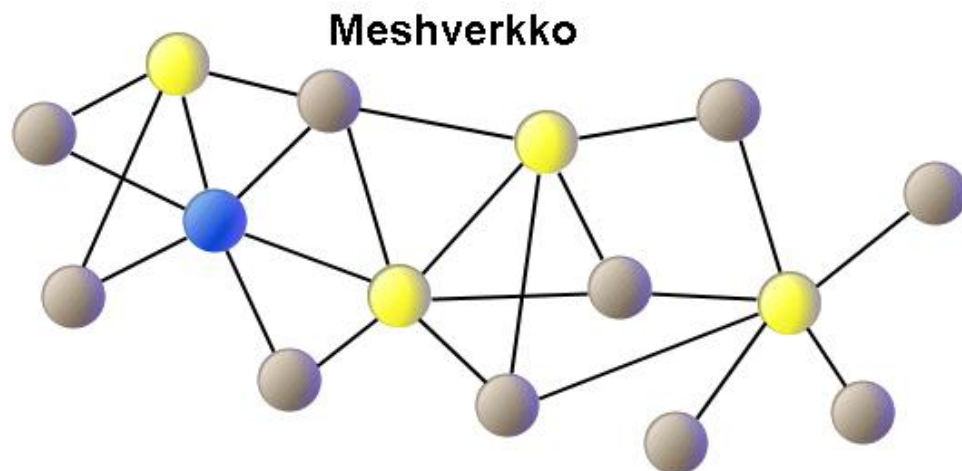
Rypäsverkko on paljon monimutkaisempi ratkaisu kuin esimerkiksi tähtiverkko. Tässä verkkoratkaisussa verkossa on monta koordinaattoria, FFD:tä ja RFD:tä. FFD:t reitittävät tietoa koordinaattoreille ja takaisin päätelaitteille. Verkon ongelma on se että jos yksi reitittävä FFD menee rikki tai sen patteri loppuu, niin yhteys katkeaa tämän reitittimen takana oleviin päätelaitteisiin. Verkko on esitetty Kuvassa 2. (Software Technologies Group 2009, 3.)



Kuva 2: Rypäsverkon topologia (Software Technologies Group 2009, 3.)

3.1.4 Mesh-verkko

Mesh-verkko on ZigBee:n monimutkaisin verkkoratkaisu. Se on lähes samankaltainen rypäsverkon kanssa, mutta nyt päätelaitteille voi olla monta yhteyttä, joka tuo verkkoon samalla viansietokykyä lisää. Verkko on esitetty Kuvassa 3. (Software Technologies Group 2009, 3.)



Kuva 3: Mesh-verkon topologia (Software Technologies Group 2009, 3.)

3.2 ZigBee-verkon osat

ZigBee verkossa on käytännössä kolmea erilaista laitetta. Laitteet ovat verkon koordinaattori, FFD ja RFD. Seuraavissa kappaleissa on esitelty tarkemmin verkon eri osat. (Software Technologies Group 2009, 3.)

3.2.1 Full function device (FFD)

FFD on laite, joka toteuttaa standardin kaikilta osin ja voi täten myös toimia personal area network -koordinaattorina (PAN-coordinator). FFD voi myös reitittää dataa eri verkkoihin ja näin ollen mahdollistaa erittäin monimutkaisten verkkojen toteutuksen. ZigBeessä tällaista laitetta kutsutaan myös nimellä ZigBee router (ZR). (Software Technologies Group 2009, 3.)

3.2.2 PAN-koordinaattori

PAN-koordinaattori on itse asiassa FFD, jolla on hiukan erilainen rooli normaaleihin FFD-laitteisiin verrattuna. Verkossa koordinaattori hoitaa laitteiden yhdistämisen ja verkon tietojen säilyttämisen, joten se tarvitsee muistia enemmän kuin esimerkiksi RFD. Tämän takia koordinaattori saattaa olla kytkettynä suoraan verkkovirtaan. (Software Technologies Group 2009, 3.)

Jokaisessa ZigBee-verkossa on aina oltava yksi koordinaattori. ZigBeessä tällaista laitetta kutsutaan myös nimellä ZigBee coordinator (ZC). ZigBee-verkossa koordinaattorin osoite on aina 0. Jennic koordinaattori on esitetty Kuvassa 4. (Software Technologies Group 2009, 3.)



Kuva 4: Jennic koordinaattori, missä on kiinni M02 moduuli

(<http://electronicdesign.com/Files/29/16485/Zigbee%20%20Jennic%20Fig%201.jpg>)

3.2.3 Reduced function device (RFD)

RFD on laite, josta on karsittu ominaisuuksia, eikä se kaikilta osin toteuta standardin vaatimia kriteerejä. Käytännössä RFD kerää tietoa ympäristöstä, ja lähettää sen koordinaattorille mitenkään tietoa varastoimatta. Tästä syystä laite on saatu pieneksi, edulliseksi ja vähän virtaa vieväksi. Tämän takia RFD käyttää yleensä vain pattereista tai akuista saatavaa virtaa. Jennic RFD on esitetty Kuvassa 5. (Software Technologies Group 2009, 3.)



Kuva 5: Jennic RFD, missä kiinni M01 moduuli (http://www.ed-china.com/ARTICLES/2006FEB/1/2006FEB01_ES_RFD_OT_275F1.JPG)

3.3 ZigBeen lähetysteho 2,4 GHz:n taajuusalueella

ZigBeen lähetysteho määräytyy sen käyttämän taajuuden mukaan. Suomessa lähetystehoja määrää Viestintävirasto. 2,4 GHz:n alueella ZigBee-lähetin saa lähettää dataa korkeintaan 10 mW:n (EIRP) teholla. (Viestintävirasto 2009, 4.)

3.4 ZigBee-verkon osoitteet ja käyttäjämäärät

ZigBee käyttää laitteiden tunnistukseen kahta erilaista osoitetta. Toinen on niin sanottu pitkä osoite, jota kutsutaan myös nimellä IEEE- tai MAC-osoite. Pitkä osoite on 64-bittiä pitkä. Pitkän osoitteen määrittää aina laitteen valmistaja. Osoite yksilöi kaikki ZigBee-verkkoa käyttävät laitteet maailmassa. Osoiteavaruutta ylläpitää IEEE, josta ZigBee-laitteiden valmistaja voi ostaa itselleen oman osoiteavaruuden palan. (ZigBee Wireless Networking 2009 sivut 297 - 299, 5.)

IEEE-osoite rakentuu kahdesta osasta. Toinen on organisaation yksilöllinen tunniste (OUI, organisation unique identifier), joka on 24 bittiä pitkä. Jäljelle jäävä osuus on laitteen valmistajan yksilöllinen laitetunniste (OEM, original equipment manufacturer), joka on 40 bittiä pitkä. IEEE-osoite on esitetty Kuvassa 6. (ZigBee Wireless Networking 2009 sivut 297 - 299, 5.)

OUI (24 bittiä eli 3 tavua)	OEM (40 bittiä eli 5 tavua)
-----------------------------	-----------------------------

Kuva 6: IEEE-osoite

Toinen osoitteista on lyhyt osoite, jota kutsutaan myös nimellä verkko-osoite. Verkko-osoite on 16-bittiä pitkä. Laite saa aina verkko-osoitteen, kun se liittyy ZigBee-verkkoon. Lyhyitä osoitteita käytetään sen takia, että hyötykuormalle jäisi enemmän tilaa kehyksessä. ZigBee-kehyksessä osoitteita on yhteensä 4 kappaletta ja niihin käytetään yhteensä 64 bittiä. Jos taas käytettäisiin pitkiä osoitteita, osoitekenttiin hukattaisiin yhteensä 256 bittiä. (ZigBee Wireless Networking 2009 sivut 297 - 299, 5.)

ZigBee-verkon osoitteet mahdollistavat jopa 18,45 triljoonaan laitteen osoitteen. Tämä tarkoittaa sitä, että maapallon jokaisella neliömetrillä voisi olla 123 853 laitetta. (ZigBee Wireless Networking 2009 sivut 297 - 299, 5.)

3.5 Tietoliikennetyypit ja liikennöintitilat

ZigBee standardi käsittää kolme eri tietoliikennetyyppiä. Nämä tietoliikennetyypit ovat jaksoittainen, epäsäännöllinen ja toistuva.

Jaksoittainen tarkoittaa sitä, että sensori mittaa jotakin suuretta ja lähettää siitä tietoa silloin tällöin. Tällöin ohjelma päättää, koska tietoa lähetetään ja käynnistää lähettimen. Kun tieto on lähetetty, lahetin kytketään pois päältä. (ZigBee 2009, 1.)

Epäsäännöllisen tiedon kanssa ohjelman keskeytys tai jokin heräte käynnistävät lähettimen ja lähetyksen jälkeen se sammuu automaattisesti. Heräte voi olla esimerkiksi lämpötilan äkillinen nousu tai palohälyttimeen tullut savu. Tämä tietoliikenne tyyppi säästää virtaa eniten, koska laite on verkossa vain tiedonsiirron ajan. (ZigBee 2009, 1.)

Toistuva tiedonsiirto hoidetaan siten, että tiedolle sovitaan tahti. Tieto jaetaan tiettyihin aikaväleihin eli taattuihin aikaväleihin (GTSs, Guaranteed Time Slots). (ZigBee 2009, 1.)

Lisäksi ZigBee-verkolla on kaksi eri liikennöintitilaa. Nämä tilat ovat beacon- ja non-beacon-tila. Beacon-tilassa laite odottaa verkon koordinaattorilta herätepakettia, joka laukaisee datan lähetyksen. Herätepaketissa määritellään myös seuraavan paketin saapuminen ja laite voi mennä sleep-tilaan odotusajaksi. Non-beacon -tilassa laite saa ulkopuolisen herätteen, esimerkiksi savu palohälyttimissä laukaisee datan lähetyksen koordinaattorille. Koordinaattori ei voi olla sleep-tilassa. (ZigBee 2009, 1.)

3.6 Taajuudet ja siirtonopeudet

ZigBee käyttää kolmea eri taajuusaluetta. Pelkästään Eurooppaan kaavailtu 868 MHz:n alueelta löytyy vain yksi kapea kanava. Tämän takia tiedonsiirtonopeus jää hitaaksi ja on vain 20 kb/s. Yhdysvalloissa tiedonsiirtokaista löytyy 915 MHz:n alueelta. Alueella on yhteensä kymmenen eri kanavaa ja kanavavälinä käytetään 2 MHz:ä. Yhdellä kanavalla päästään jo 40 kb/s nopeuteen. (ZigBee 2009, 1.)

Maailmanlaajuisesti ZigBee käyttää ISM-taajuusaluetta. Tällä taajuusalueella on 16 kanavaa ja kanavavälinä käytetään 5 MHz:ä. ISM-taajuusalueen yhdellä kanavalla päästään 250 kb/s nopeuteen optimaalisissa olosuhteissa. Taulukossa 1 on esitetty levitys- ja dataparametrit tarkemmin. (ZigBee 2009, 1.)

Tietotekniikka, tietoliikennetekniikka

Joni Jokipii

Taulukko 1: Levitys- ja dataparametrit

<https://oa.doria.fi/bitstream/handle/10024/5169/TMP.objres.533.pdf?sequence=1>

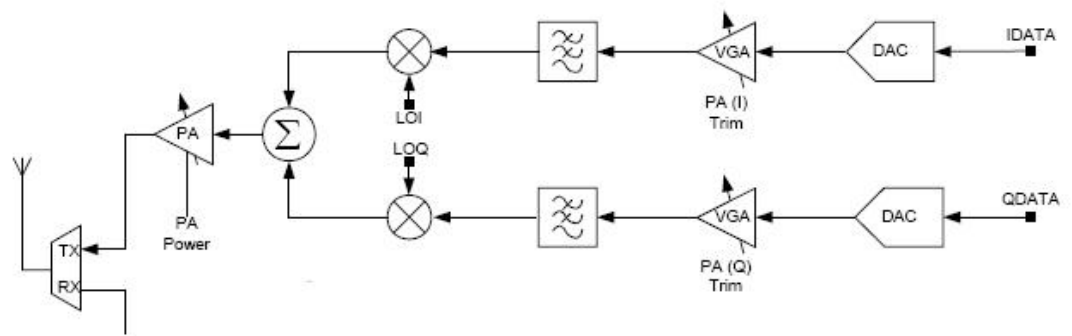
Taajuusalue	Levitysparametrit		Dataparametrit		
	Chip rate	Modulaatio	Bittinopeus	Symbolinopeus	Modulaatio
868-870 MHz	300 kchip/s	BPSK	20 kbit/s	20 baud	BPSK
902-928 MHz	600 kchip/s	BPSK	40 kbit/s	40 baud	BPSK
2,4-2,4835 GHz	2 Mchip/s	O-QPSK	250 kbit/s	62.5 baud	16-ary orthogonal

4 ZigBee-lähetin: Jennic JN5139

ZigBee lähetin käsittää 2.45 GHz:n radion, O-QPSK modeemin, kantataajuuskaista prosessorin, salaus lisäprosessorin ja fyysisen kerroksen ohjaimen (PHY controller). Näiden lohkojen ja IEEE 802.15.4 protokollaa tukevan ohjelmiston kanssa ZigBee-lähetin on mahdollista lähettää dataa langattomasti lisensoimattomalla 2,4 GHz:n kaistalla. (Jennic Wireless Microcontrollers 2009 sivu 23, 6.)

4.1 Radiolähetin

Radio käsittää Low-IF-tulolinjan ja Direct up-conversion-lähetyslinjan, joka yhtyy lähetys- ja vastaanotto kytkimellä. Kyttimeen kuuluu kaikki tarvittavat komponentit 200 ohmin differentiaali antennin kytkemiseksi suoraan lähtöliitäntään ilman erillisiä komponentteja. Antenniporttiin on mahdollista kytkeä myös yksi piiska antenni, jos käytetään sovitinta. Lähettimen lohkokaaavio näkyy kuvassa 7. (Jennic Wireless Microcontrollers 2009 sivu 23, 6.)



Kuva 7: Lähettimen lohkokaaavio (Jennic Wireless Microcontrollers 2009 sivu 23, 6.)

16 MHz:n oskillaattori antaa pulssia jakajalle joka mahdollistaa taajuus synteesoinnin referenssi taajuuteen. Taajuussyntesoiija käsittää ohjelmoitavat jakajat, vaiheen tunnituksen, jännitepumpun ja sisäisen jänniteohjatun oskillaattorin.

Jänniteohjatussa oskillaattorissa ei ole mitään ulkoisia komponentteja. Lisäksi oskillaattorissa on mukana kalibrointi piiri, joka poistaa virheet, jotka syntyvät sisäisten komponenttien lämpötilavaihteluista. Jänniteohjattua oskillaattoria (VCO) ohjaa vaihelukittu silmukka eli PLL. Vaihelukittua silmukkaa varten tarvitaan vain kolme lisäkomponenttia. Ohjelmoitavaa jännitepumppua käytetään myös parantamaan laitteiston toimintaa. (Jennic Wireless Microcontrollers 2009 sivu 23, 6.)

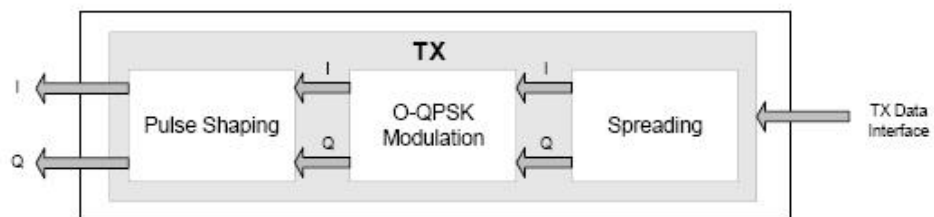
Lohkokaaviossa I- ja Q-datat tulevat modeemilta. Tämän jälkeen ne muutetaan analogiseksi DAC-lohkossa (Digital to analog converter). Siitä signaalit etenevät esivahvistimeen (VGA), jonka jälkeen signaali alipäästösuodatetaan. Alipäästösuodatuksen jälkeen signaalit nostetaan 2,4 GHz:n kaistalle mikserissä. Tämän jälkeen signaalit summataan ja lähetetään tehovahvistimelle. Tehovahvistin varmistaa, että signaalin teho riittää vastaanottolaitteelle asti ja säätää tehoa mikäli sitä on liikaa tai liian vähän. Tehovahvistimella on kuusi eri tehoporrasta. Vahvistimelta signaali syötetään TX/RX-kytkimelle, josta se etenee antennia pitkin siirtotielle. (Jennic Wireless Microcontrollers 2009 sivu 23, 6.)

4.2 Antennin diversiteetti

Antennin diversiteetti tarkoittaa sellaista tekniikkaa millä saadaan antennista/antenneista täysi hyöty irti. Se mahdollistaa laitteen radion vaihtaa toiseen antenniin, jos yhteyttä ei pystytä muodostamaan. Nämä antennit korreloivat vähän keskenään eli eivät ole riippuvaisia toisistaan. Tyypillisesti tämä saavutetaan sillä, että kaksi antennia sijoitetaan 0,25 aallonpituuden päähän toisistaan tai käytetään kahta ortogonaalista polarisaatiota eli antennit ovat kohtisuoraan toisiaan vastaan. Joten, jos paketti on lähetetty eikä vastausta ole kuulunut, radio voi vaihtaa antennia ja yrittää uudelleen. JN5139:ssa on kaksi antennia. (Jennic Wireless Microcontrollers 2009 sivu 24, 6.)

4.3 Modeemi

Modeemi hoitaa kaikki tarpeelliset modulaatio ja levitystehtävät mitä vaaditaan digitaaliseen lähetykseen ja vastaanottoon 250 kbps nopeudella ja 2450 MHz:n taajuusalueella. Samalla se on yhteensopiva IEEE 802.15.4-standardin kanssa. Modeemin lohkokaavio on esitetty kuvassa 8.



Kuva 8: Modeemin lohkokaavio (Jennic Wireless Microcontrollers 2009 sivu 25, 6.)

Lähetin vastaanottaa symboleita kantataajuuskaista prosessorilta ja käyttää DSSS menetelmää levittämään jokaisen 4-bittisen symbolin 32-chippiseksi pseudo-satunnaiseksi kohinasarjaksi (PN). Kohinasarjat on esitetty taulukossa 2. Tämän jälkeen O-QPSK:n ja puolikkaan sinipulssi-muokkauksen avulla saadaan aikaan yksilölliset I- ja Q-signaalit. Sen jälkeen ne syötetään DAC-lohkoon, mistä olikin jo aikaisemmin puhetta. (Jennic Wireless Microcontrollers 2009 sivu 25, 6.)

Puolikas sinipulssi-muokkain on käytännössä suodatin, joka auttaa modeemia luomaan yksilölliset I- ja Q-signaalit.

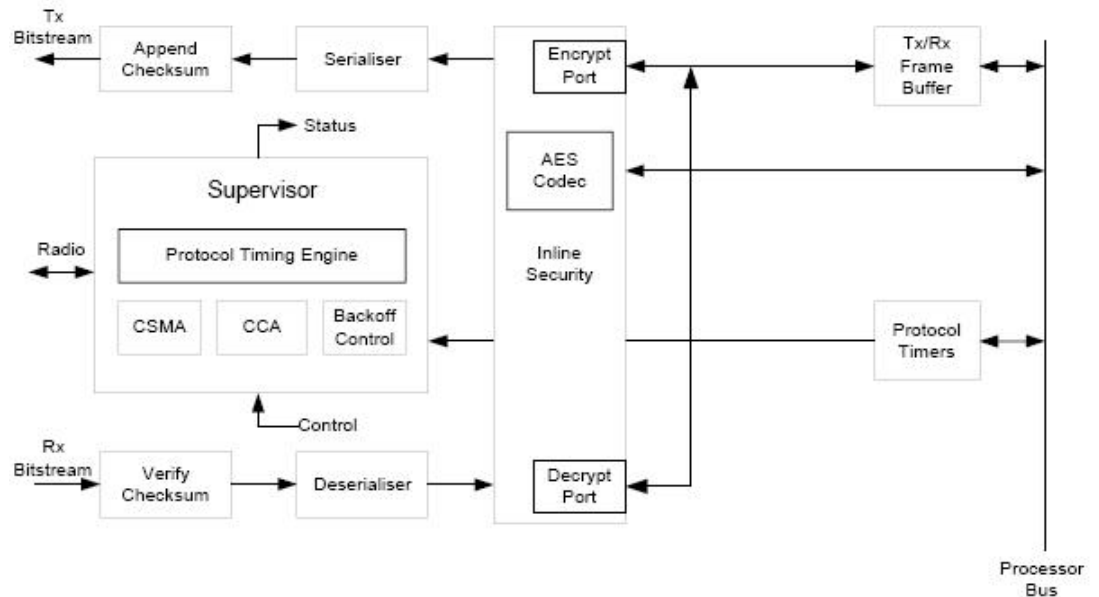
Taulukko 2: Kohinasarjat eli pseudo-satunnaiset koodit (IEEE 802.15.4 2009 sivu 48, 10.)

Data symbol (decimal)	Data symbol (binary) ($b_0 b_1 b_2 b_3$)	Chip values ($c_0 c_1 \dots c_{30} c_{31}$)
0	0000	11011001110000110101001000101110
1	1000	11101101100111000011010100100010
2	0100	00101110110110011100001101010010
3	1100	00100010111011011001110000110101
4	0010	01010010001011101101100111000011
5	1010	00110101001000101110110110011100
6	0110	11000011010100100010111011011001
7	1110	10011100001101010010001011101101
8	0001	10001100100101100000011101111011
9	1001	10111000110010010110000001110111
10	0101	01111011100011001001011000000111
11	1101	01110111101110001100100101100000
12	0011	00000111011110111000110010010110
13	1011	01100000011101111011100011001001
14	0111	10010110000001110111101110001100
15	1111	11001001011000000111011110111000

4.4 Kantataajuusprosessori

Kantataajuusprosessori tarjoaa kaikki IEEE 802.15.4 MAC-kerroksen aika kriittiset toiminnot. Prosessori huolehtii ohjelmiston avulla siitä että ilmarajapinnan ajastus on kohdallaan. MAC kerroksen rauta ja ohjelmisto jakavat tiedot sellaisiin paketteihin että kehyksien lähetys on mahdollista protokollan vaatimalla tavalla oikeaan aikaan. Tämä vaatii millisekunnin tarkkuutta ilmarajapinnan ajastuksessa ja mikrosekuntien tarkkuutta tiedon jakamisen kanssa. Protokollan ohjelmistokerros huolehtii huolto- ja data-viestien lähetyksen loppupisteen ja

koordinaattorin välillä. Kantataajuusprosessorin lohkokaavio on esitetty kuvassa 9. (Jennic Wireless Microcontrollers 2009 sivu 26, 6.)



Kuva 9: Kantataajuusprosessorin lohkokaavio (Jennic Wireless Microcontrollers 2009 sivu 26, 6.)

4.5 Lähetys

Lähetys tapahtuu siten, että ohjelma kirjoittaa datan ensin TX/RX-puskuriin, yhdessä parametrien (kohdeosoitteen ja uusintayritysten määrän) kanssa. Samalla ohjelma aktivoi yhden protokollan ajastimen, mikä osoittaa, koska viesti tulisi lähettää. Lähetysten aika määräytyy protokollan korkeampien kerrosten, kuten esimerkiksi superkehysten ja kehysten reunojen mukaan. Kun paketti on valmis lähetettäväksi ja protokolla-ajastin asetettu, päälohko aloittaa lähetysten hallinnan. Ennen kuin lähettäminen alkaa, päälohko odottaa oikeaa aikaväliä. Kun aikaväli tulee, päälohko ohjaa radiota ja modeemia siten, että ne tekevät oikeanlaisen lähetteen. Päälohko (Supervisor block) pystyy hoitamaan kaikki IEEE 802.15.4:n vaatimat tehtävät. (Jennic Wireless Microcontrollers 2009 sivut 26-27, 6.)

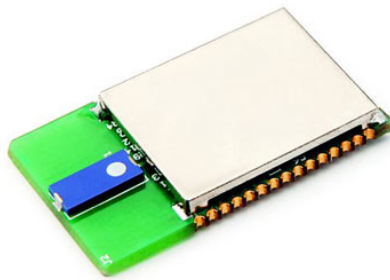
Kun datan lähettäminen alkaa, ohjelma rakentaa kehyksen otsikkokentän. Kenttä rakennetaan parametreista, jotka lähetettiin TX/RX-puskuriin. Tämän jälkeen data lähetetään modeemille. Samaan aikaan, radio valmistautuu lähetykseen. Kun bittivirta läpäisee modeemin, siitä lasketaan CRC-tarkistussumma. Tämän summan laskeminen suoritetaan ”lennosta”. Tämän jälkeen summa lisätään kehyksen perään. (Jennic Wireless Microcontrollers 2009 sivut 26-27, 6.)

5 ZigBee mittaukset

Mittausten tarkoituksena oli selvittää kuinka pitkiä välimatkoja ZigBee-laitteilla on mahdollista muodostaa.

5.1 Mittaukset

Aloitimme tutkimisen Jennicin JN5139-Z01-M01 moduulista Björnisen Kallen kanssa. Moduuli on esitetty kuvassa 10. Tarkoituksenamme oli selvittää, miten moduuli oli rakennettu ja mistä osista sen lähetys- ja vastaanottopuolet koostuivat.



Kuva 10: Jennic JN5139-Z01-M01 moduuli

(http://www.jennic.com/files/media/Jennic_3_module_2.jpg)

Kolvasimme kuvassa 10 näkyvän metallisuojan irti ja huomasimme, että melkein kaikki lähettimen ja vastaanottimen osat on integroitu samalle ohjelmoitavalle piirille. Tämän piirin tutkiminen olisi ollut erittäin vaikeata ja sen luovuimme siitä.

Seuraavana vuorossa olivat mittaukset. Mittauksien tarkoituksena oli selvittää kuinka kauas signaali kantaisi. Muutaman mittauksen jälkeen huomasimme, että signaali hukkui kohinaan, kun yhteysväli kasvoi yli 10 metriin ja täten sitä oli mahdoton mitata.

Lopulta päätimme mitata yhteysvälin yhdellä koordinaattorilla ja yhdellä RFD:llä. RFD:ssä lähettävänä elimenä toimi moduuli M01 ja koordinaattorissa M02. Moduuli M02 on esitetty kuvassa 11. Moduuli M01 sisältää kaksi keraamista

antennia integroituna yhteen komponenttiin. Kuvassa 10 antennit näkyvät turkoosina komponenttina. Viimeisessä mittauksessa RFD:ssä oli myös moduuli M02.



Kuva 11: Jennic JN5139-Z01-M02 moduuli

(http://www.jennic.com/files/media/Jennic_3_module_2.jpg)

5.2 Tulokset

Ensimmäinen mittaus tapahtui koulun pihalla, mikä oli tarpeeksi laaja-alue, jotta voitiin selvittää, kuinka pitkä kantama keraamisella antennilla olisi mahdollista saada. Saimme tulokseksi muutamien uusintayritysten jälkeen 92 metriä.

Mittaaminen tapahtui 50 metrin rullamitalla ja virtalähteenä käytimme juuri ladattuja akkuja. ZigBee lupaa vapaassa tilassa kantamaksi 100 metriä, joten olimme tyytyväisiä tulokseen.

Tämän jälkeen mittasimme, kuinka pitkä kantama on silloin, kun käytetään vaimentavaa laatikkoa. Tämäkin mittaus tapahtui koulun pihalla. Laatikko, mitä käytimme, vaimensi 24 dB. Yhteysväliksi saimme laatikkoa käyttäen vain 27 metriä. Tulokset mittasimme 50 metrin rullamitalla. Laitteissa käytimme juuri ladattuja akkuja. Mittauksen aikana koordinaattori oli laatikossa, ja sen antenni näytti ylöspäin. RFD oli kädessä.

Seuraavan mittauksen tarkoituksena oli selvittää kuinka monta kerrosväliä signaali kantaa. Mittaus tapahtui A-3 kerroksen ja A-kellari kerroksen välillä. Saimme signaalin kuulumaan aina kellariin asti eli välissä oli 3 kerrosta. Lattiat on

Tietotekniikka, tietoliikennetekniikka

Joni Jokipii

mahdollisesti tehty teräsbetonista. Mittauksessa käytimme laitteissa juuri ladattuja akkuja. Mittauksen aikana pidimme laitteita käsissämme ja koordinaattorin antenni näytti ylöspäin.

Neljännän ja viimeisen mittauksen tarkoituksena oli selvittää, kuinka pitkä signaalin kantama saataisiin M02 moduuleilla eli paremmilla antennilla. Mittaus tapahtui Pirkkahallin parkkipaikalla eli vanhalla lentokentän kiitoradalla. Mittauksesta saimme tulokseksi 460 metriä. Tulos on mitattu auton matkamittarilla. Laitteita pidimme käsissämme ja niiden antennit näyttivät ylöspäin. Mittauksessa käytimme juuri ladattuja akkuja.

5.3 Tulosten tarkastelu ja arviointi

Yhteysväliksi keraamisella antennilla saimme 92 metriä. Uskon, että tulos pitää paikkansa 1 metrin tarkkuudella.

Kerrosvälimittaus ei ollut kovin tarkka koska emme mitanneet kerroksia lattiasta kattoon ja kerroksien välien paksuutta. Eri materiaaleista valmistetussa talossa saa varmasti paljon erilaisia tuloksia.

Yhteysväliksi paremmilla antennilla saimme 460 metriä. Uskon että tulos pitää paikkansa 50 metrin tarkkuudella. Tarkkuuteen on huomioitu esteet ja auton matkamittarin heitto.

6 Tietoturva

Niin kuin kaikki muukin tietoliikenne myös ZigBeen tietoliikenne on suojattava hyökkäyksiä vastaan. Hyökkääjä voi esimerkiksi haluta, että koordinaattori saa väärän tiedon ja aloittaa palohälyttimen hälytyksen. Tämän takia ZigBee verkkoon tuleva laite on aina hyväksyttävä koordinaattorin tai reitittimen toimesta. Lisäksi laitteille on mahdollista asettaa verkon salasana ja eri linkkien salasanat. ZigBee -verkossa tieto salataan 128 bittisellä AES-salausalgorithmilla. (Movable Type Scripts 2009, 7.)

6.1 AES -saltaus

AES tulee sanoista Advanced Encryption Standard. Sen on kehittänyt USA:n standardoimisvirasto (NIST). AES tuli markkinoille vuonna 2001 ja korvasi samalla vanhan DES:n eli Data Encryption Standardin. AES –salausta käytetään laajalti tietoliikenteen eri sovelluksissa. (CSRC 2009, 8.)

AES –saltaus on niin sanottua lohkosalausta. AES luotiin NIST:n järjestämän kilpailun voittajaehdokkaan pohjalta. Voittajaksi selviytyi kahden belgialaisen tutkijan, Joan Daemenin ja Vincent Rijmenin, luoma Rijndael-salaus. Nimityksiä AES ja Rijndael käytetäänkin usein synonyymeinä, vaikka AES:ään kuuluu vain osa Rijndaelin ominaisuuksista. (CSRC 2009, 8.)

6.2 Avainten hallinta ja avaimet

ZigBee-verkossa avainten hallinnan hoitaa yleensä koordinaattori. Se jakaa verkossa oleville laitteille uudet avaimet, jos ne päivitetään sekä huolehtii siitä, että mikään tuntematon laite ei pysty liittymään verkkoon. Tällaista laitetta kutsutaan myös Trust manageriksi. Network manager hallitsee verkkoavaimia ja jakaa niitä tarvittaessa. Tämä laite on yleensä myös koordinaattori. Lisäksi verkossa on vielä

yksi tai useampi laite, joka ottaa Configuration managerin roolin. Nämä laitteet asettavat linkkiavaimet tarvittaessa. (ZigBee Alliance esitys 2009, 9.)

Kun ZigBee-verkko halutaan suojata, siihen käytetään kolmea erilaista avainta.

Ensimmäinen ja ehkä tärkein avain on verkkoavain (Network key). Se on sama kaikilla laitteilla, ja se varmistaa, että ulkopuoliset laitteet eivät pääse kytkeytymään verkkoon. Verkkoavain myös mahdollistaa datan salauksen, joten ulkopuolisten on myös mahdotonta saada salatusta tiedosta mitään selvää ilman oikeaa avainta. Verkkoavain voidaan uusina tasaisin väliajoin ja näin parantaa tietoturva. (ZigBee Alliance esitys 2009, 9.)

Toinen avaimista on pääavain (Master key). Se mahdollistaa perus tietoturvan kahden laitteen välillä.

Kolmas avain on linkkiavain (Link key). Linkkiavain ehkäisee verkon sisältä tulevia hyökkäyksiä, koska vain yhdellä koordinaattorilla tai reitittimellä on yksi avain jokaista linkkiä kohden. Linkkiavain voidaan uusina tasaisin väliajoin ja näin parantaa tietoturva. (ZigBee Alliance esitys 2009, 9.)

7 Liikennöinnit ja kehykset

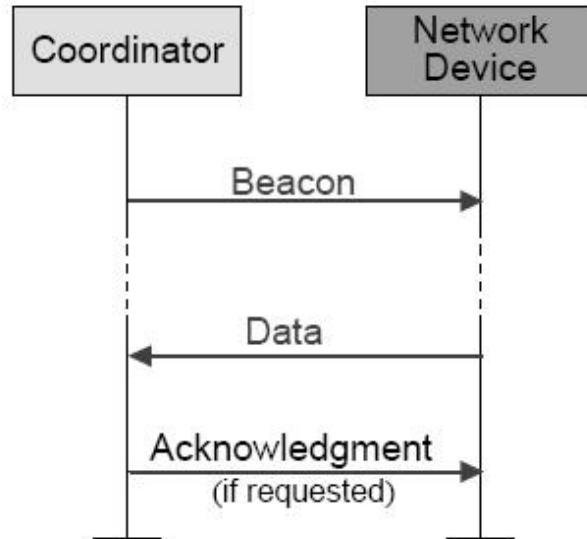
Seuraavissa kappaleissa on esitelty ZigBee-verkon liikennöinti mahdollisuudet ja ZigBeen käyttämät kehysrakenteet.

7.1 Liikennöinnit

ZigBee verkossa laitteilla on kolme eri liikennöintimahdollisuutta. Ensimmäinen niistä on tiedonsiirto verkon joltain laitteelta koordinaattorille. Toinen tapa on tiedonsiirto koordinaattorilta jollekin laitteelle. Kolmas tapa on tiedonsiirto kahden peer-laitteen välillä. Tähtiverkossa käytetään ainoastaan kahta näistä tiedonsiirtotyyleistä koska tieto siirtyy verkon päätelaitteelta suoraan koordinaattorille. Peer-to-peer-topologia käyttää kaikkia mainittuja tiedonsiirtotyylejä, koska tieto voi siirtyä päätelaitteelta mille tahansa verkon toiselle laitteelle. Mitä näistä tiedonsiirtotyyleistä käytetään, riippuu siitä, onko verkko asetettu niin sanottuun Beacon-tilaan. Verkossa, jossa Beacon-tila on päällä, laiteilta vaaditaan synkronointia tai pientä viiveaikaa. Jos verkossa ei tarvita synkronointia tai pientä viiveaikaa voidaan Beacon kytkeä pois päältä. Tämä vaikuttaa vain normaaliin tiedonsiirtotapahtumaan, koska Beacon-tilaa tarvitaan kuitenkin, kun yritetään etsiä uusia laitteita verkkoon. (IEEE 802.15.4 2009 sivu 17-21, 10.)

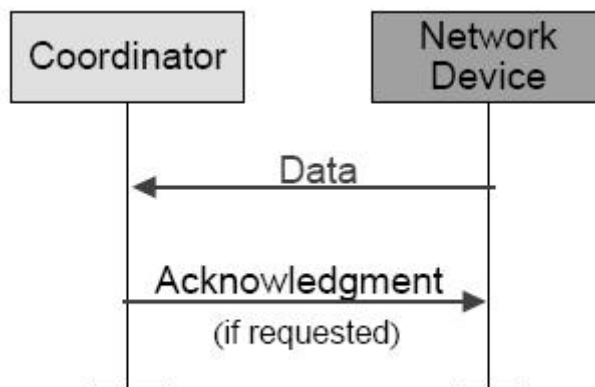
7.1.1 Tiedonsiirto päätelaitteelta koordinaattorille

Kun päätelaite haluaa siirtää tietoa koordinaattorille verkossa, jossa Beacon-tila on päällä, niin päätelaite kuuntelee ensin verkon Beaconia. Beaconin löydettyään se synkronoituu superkehysrakenteeseen. Sopivana ajankohtana laite lähettää oman kehyksensä koordinaattorille käyttäen ajakaollista CSMA/CA. Kun tieto saapuu koordinaattorille, se on mahdollista kuitata. Tämä tiedonsiirtotyylä on esitetty kuvassa 12. (IEEE 802.15.4 2009 sivut 17-21, 10.)



Kuva 12: Tiedonsiirto päätelaitteelta koordinaattorille Beacon-tilassa (IEEE 802.15.4 2009 sivu 19, 10.)

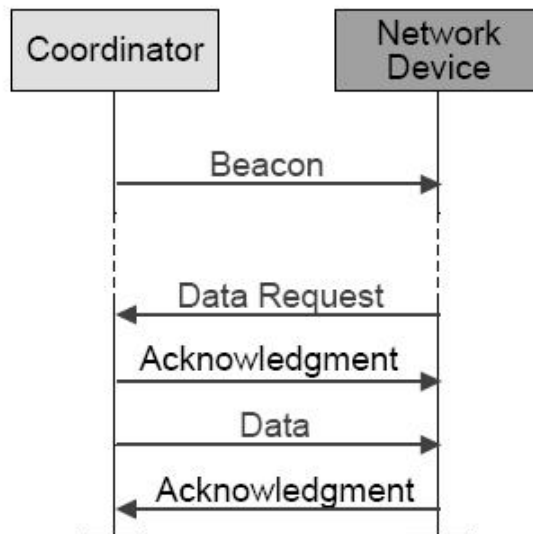
Kun päätelaite haluaa siirtää tietoa ja verkko on non-Beacon-tilassa, päätelaite käyttää aikajaotonta CSMA/CA:ta siirtäessään dataa koordinaattorille. Kun tieto saapuu koordinaattorille, se on mahdollista kuitata. Tämä tiedonsiirtotapahtuma on esitetty kuvassa 13. (IEEE 802.15.4 2009 sivut 17-21, 10.)



Kuva 13: Tiedonsiirto päätelaitteelta koordinaattorille non-Beacon-tilassa. (IEEE 802.15.4 2009 sivu 19, 10.)

7.1.2 Tiedonsiirto koordinaattorilta päätelaitteelle

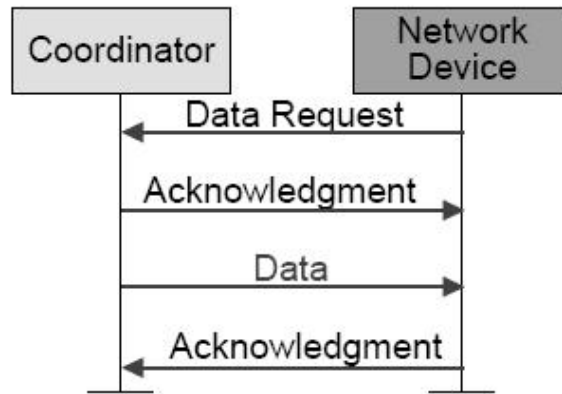
Koordinaattorin halutessa lähettää dataa verkon jollekin päätelaitteelle, verkon ollessa Beacon-tilassa, koordinaattori ilmoittaa Beacon-signaalisella, että data odottaa lähetystä. Vastaanottava laite huomaa tämän, koska se kuuntelee Beacon-signaalia ajoittain ja lähettää koordinaattorille MAC-lähetyspyynnön. Koordinaattori kiittää lähetyspyynnön, ja tämän jälkeen lähettää odottavan datan jos kanava on vapaa käyttäen ajakaajallista CSMA/CA:ta. Kun päätelaite on vastaanottanut datan, se lähettää kiittauksen datan saapumisesta. Kun viesti on toimitettu, koordinaattori vaihtaa Beacon-signaalin sellaiseksi, että päätelaitteet ymmärtävät, että dataa ei ole tulossa. Lähetysjärjestys on vielä esitetty kuvassa 14. (IEEE 802.15.4 2009 sivut 17-21, 10.)



Kuva 14: Tiedonsiirto koordinaattorilta päätelaitteelle Beacon-tilassa. (IEEE 802.15.4 2009 sivu 20, 10.)

Koordinaattorin halutessa lähettää dataa verkon jollekin päätelaitteelle, verkon ollessa non-Beacon-tilassa, koordinaattori tallentaa datan muistiinsa odottamaan sopivaa yhteydenottoa. Kun yhteydenotto tulee halutulta päätelaitteelta, se lähettää MAC-lähetyspyynnön käyttäen ajakaajotonta CSMA/CA:ta. Koordinaattorin saatua tämän se kiittää viestin ja lähettää datan heti, kun se on mahdollista käyttäen

aikajaotonta CSMA/CA:ta. Tiedonsiirto on esitetty kuvassa 15. (IEEE 802.15.4 2009 sivut 17-21, 10.)



Kuva 15: Tiedonsiirto koordinaattorilta päätelaitteelle non-Beacon-tilassa. (IEEE 802.15.4 2009 sivu 20, 10.)

7.1.3 Peer-to-peer tiedonsiirto

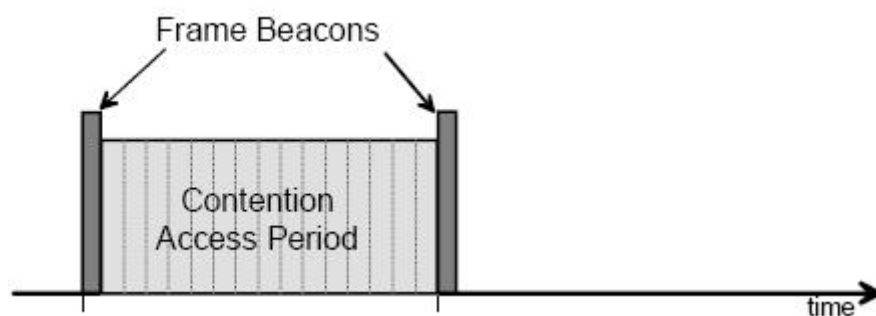
Peer-to-peer-verkossa kaikkien laitteiden on mahdollista keskustella toisen laitteen kanssa, mikäli se on kuuluvuusalueella. Jotta tiedonsiirto onnistuisi, täytyy laitteiden lähettää/vastanottaa koko ajan tai synkronoitua jotenkin. Periaatteessa tämä on mahdollista käyttäen apuna aikajaotonta CSMA/CA tekniikkaa. (IEEE 802.15.4 2009 sivut 17-21, 10.)

7.2 Kehykset

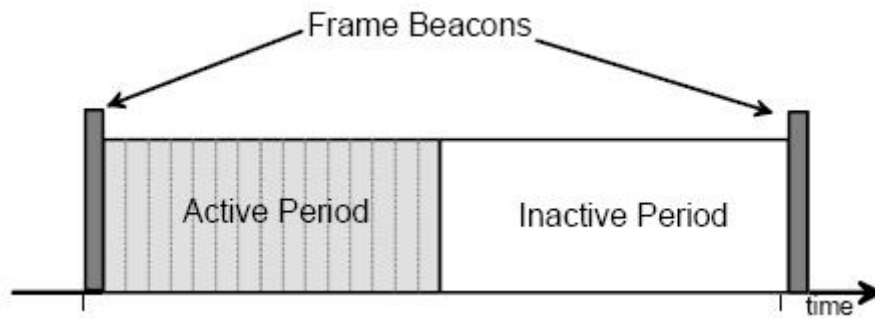
Kuten tiedonsiirrossa yleensä myös ZigBee-tekniikka käyttää erilaisia kehyksiä siirtäessään tietoa laitteelta toiselle. Kehyksiä on viisi erilaista. Ensimmäinen, nimeltään superkehys, ei oikeastaan ole kehys vaan kehyksien rykelmä. Superkehysten tunteminen on kuitenkin tärkeää ymmärtääksemme laitteiston toiminnan perustan. Seuraavissa luvuissa on esitelty ZigBee-verkon kehykset.

7.2.1 Superkehys

Superkehys on sellainen, jonka sisään muut tiedonsiirrossa tarvittavat kehykset tulevat. Standardi 802.15.4 mahdollistaa superkehysten käytön. Superkehysten mallin määrittelee koordinaattori. Kehys muodostuu Beacon-kehuksesta ja Beacon-kehysten väliin jäävistä kilpailuajaväleistä. Kilpailuajava on jaettu 16 yhtä suureen osaan. Superkehysten rakenne on nähtävissä kuvassa 16. Vaihtoehtoisesti kehyksessä voi olla aktiivinen ja ei-aktiivinen osa. Ei-aktiivisen tilan aikana koordinaattori voi mennä tilaan, jossa se käyttää erittäin vähän virtaa. Tämä vaihtoehto on nähtävissä kuvassa 17. Beacon-kehys lähetetään aina jokaisen superkehysten alussa. Jos koordinaattori ei halua, että superkehysmallia käytetään, se kytkee Beacon-kehysten pois käytöstä. Beacon-kehystä käytetään synkronoimaan verkon laitteet, tunnistamaan verkko, kertomaan käytetäänkö superkehysmallia sekä millainen superkehysmalli on käytössä. Jokainen laite, joka haluaa lähettää dataa, kilpailee kilpailuajaväleistä Beacon-kehysten välillä. Kenelle kilpailuajaväli kuuluu, ratkaistaan ajakaollisen CSMA/CA:n avulla. (IEEE 802.15.4 2009 sivut 17-18, 10.)

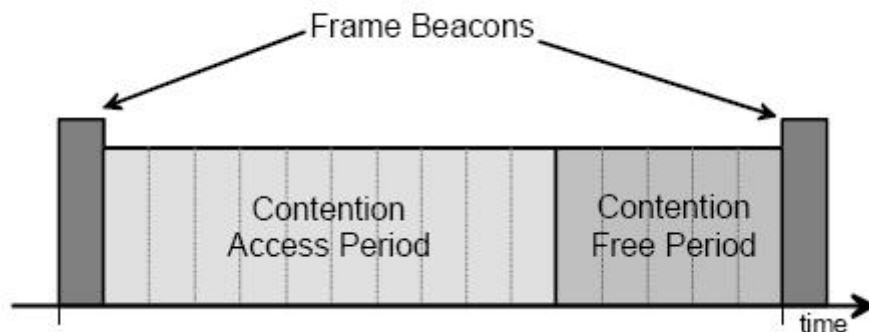


Kuva 16: Superkehysten perusrakenne (IEEE 802.15.4 2009 sivu 18, 10.)



Kuva 17: Superkehysten rakenne, kun käytetään ei-aktiivista tilaa (IEEE 802.15.4 2009 sivu 18, 10.)

Verkon koordinaattori voi määrittää superkehystä tietyn aikavälin ohjelmille, jotka vaativat pienen tiedonsiirtoviiveen tai jatkuvaa tiedonsiirtoa. Näitä aikavälejä sanotaan taatuiksi aikaväleiksi (GTSs, guaranteed time slots). GTS:t muodostavat aina superkehysten loppuun kehyksiä, mistä muut laitteet, eivät voi kilpailla. Koordinaattori voi määrätä 7 taattua aikaväliä, ja yksi taattu aikaväli voi sisältää yhden tai useamman aikavälin. Koordinaattori kuitenkin säästää kilpailuaikavälejä tarvittavan määrän, jotta muiden laitteiden datan lähetys ja uusien laitteiden verkkoon liittyminen olisi mahdollista. Kuvassa 18 on esitetty superkehys taattujen aikavälien kanssa. (IEEE 802.15.4 2009 sivu 17-18, 10.)



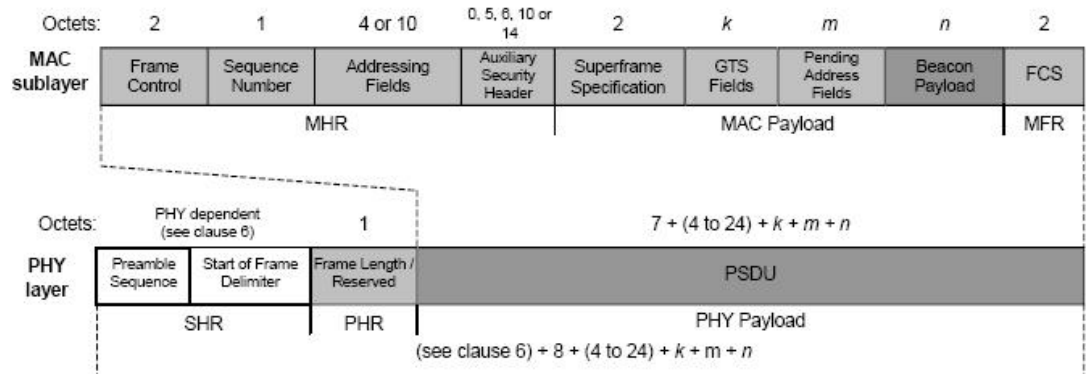
Kuva 18: Superkehys taattujen aikavälien kanssa (GTSs) (IEEE 802.15.4 2009 sivu 18, 10.)

7.2.2 Beacon-kehys

Beacon-kehysten rakenne on esitetty kuvassa 19. Sellaisessa ZigBee-verkossa jossa Beacon-kehysten lähetyksellä on päällä, koordinaattori voi lähettää Beacon-kehystään. (IEEE 802.15.4 2009 sivu 21, 10.)

MAC-hyötydata (MAC payload) käsittää superkehysten määrittelyn (superframe specification), taatut aikavälit (GTS fields), avoimen osoitekentän (pending address field) ja Beacon-hyötydatan (beacon payload). MAC-hyötydata on liitetty MAC-otsikkoon (MHR, MAC header) ja siihen on vielä perään lisätty MAC-alatunniste (MFR, MAC footer). MAC-otsikko sisältää kehysten hallintakentän, Beacon-järjestynumeron (BSN, beacon sequence number), osoitekentät ja vaihtoehtoisen lisäturvallisuusotsikon. MAC-alatunniste sisältää 16:sta bittisen kehysten tarkistusluvun (FCS, frame check sequence). MAC-hyötydata, MAC-otsikko ja MAC-alatunniste yhdessä muodostavat Beacon-kehysten. (IEEE 802.15.4 2009 sivu 21, 10.)

Tämän jälkeen Beacon-kehys siirretään fyysiselle kerrokselle ja siitä tulee fyysisen kerroksen hyötydataa (PHY payload). Ennen lähetystä fyysinen kerros liittyy kehysten vielä synkronointiosikon (SHR), joka käsittää Preamble sequence kentän, Start-of-frame delimiter (SFD) kentän ja Fyysisenkerroksen otsikon (PHR, PHY header). Otsikko sisältää luvun, joka kertoo montako oktetia hyötydataa kehysten on. Yhdessä nämä kentät muodostavat fyysisenkerroksenkehysten (PPDU), mikä lähetetään siirtotielle. (IEEE 802.15.4 2009 sivu 21, 10.)

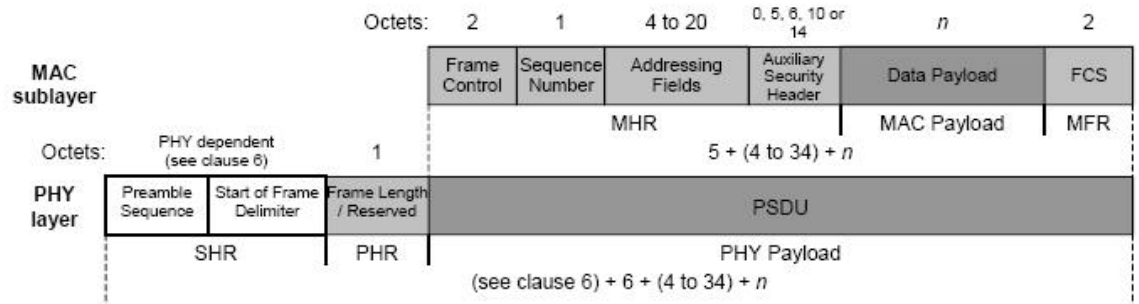


Kuva 19: Beacon-kehiksen rakenne (IEEE 802.15.4 2009 sivu 21, 10.)

7.2.3 Datakehys

Kun datakehystä luodaan, sen hyötydata siirretään MAC-alikerrokselle. Tämän jälkeen kehystä kutsutaan MAC-palvelun datayksiköksi (MSDU, MAC service data unit). MAC-alikerroksella hyötydataan yhdistetään MAC-otsikko (MHR). Lisäksi kehikseen laitetaan perään vielä MAC-alatunniste (MFR). MAC-otsikko sisältää kehiksen hallintakentän, datajärjestynumeron (DSN, data sequence number), osoitekentät ja vaihtoehtoisen lisäturvallisuusotsikon. MAC-alatunniste sisältää 16:sta bittisen kehiksen tarkistus luvun (FCS, frame check sequence). Nämä kentät yhdessä muodostavat datakehiksen (MPDU). (IEEE 802.15.4 2009 sivu 22, 10.)

Tämän jälkeen datakehys siirretään fyysiselle kerrokselle ja siitä tulee fyysisen kerroksen hyötydataa (PHY payload). Ennen lähetystä fyysinen kerros liittää kehikseen vielä synkronointiotsikon (SHR), joka käsittää Preamble sequence ja Start-of-frame delimiter (SFD) kentät ja Fyysisenkerroksen otsikon. Otsikko sisältää luvun, joka kertoo montako oktettia hyötydataa kehiksessä on. Yhdessä nämä kentät muodostavat fyysisen kerroksen kehiksen (PPDU), mikä lähetetään siirtotielle. Kehys on esitetty Kuvassa 20. (IEEE 802.15.4 2009 sivu 22, 10.)

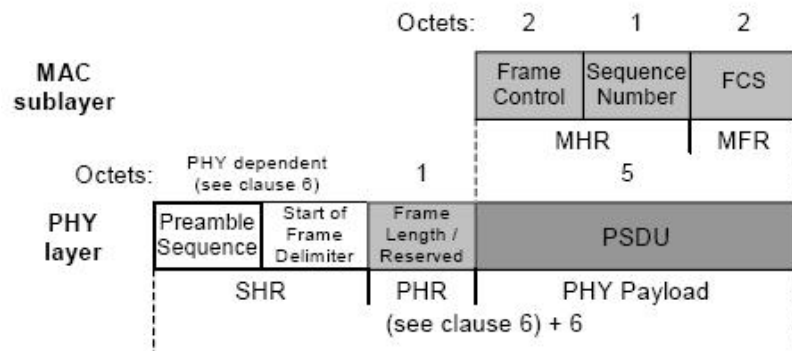


Kuva 20: Data-kehysten rakenne (IEEE 802.15.4 2009 sivu 22, 10.)

7.2.4 Kuittauskehys

Kuittauskehys muodostetaan MAC-alikerroksella. Kuittauskehys muodostuu ainoastaan MAC-otsikosta ja MAC-alatunnisteesta, koska sillä ei ole lainkaan hyötydataa. MAC-otsikko sisältää kehysten hallintakentän ja datajärjestysnumeron (DSN, data sequence number). MAC-alatunniste sisältää 16:sta bittisen kehysten tarkistusluvun (FCS, frame check sequence). MAC-otsikko ja MAC-alatunniste -kentät yhdessä muodostavat kuittauskehysten (MPDU). (IEEE 802.15.4 2009 sivu 22, 10.)

Kuittauskehysten muodostuksen jälkeen kehys siirretään fyysiselle kerrokselle. Sen jälkeen kehyksestä tulee fyysisen kerroksen hyötydataa. Fyysinen kerros lisää vielä kehykseen synkronointiotsikon (SHR), joka käsittää Preamble sequence ja Start-of-frame delimiter (SFD) kentät ja fyysisen kerroksen otsikon. Otsikko sisältää luvun, joka kertoo montako oktetia hyötydataa kehyksessä on. Yhdessä nämä kentät muodostavat fyysisen kerroksen kehysten (PPDU), mikä lähetetään siirtotielle. Kehys on esitetty kuvassa 21. (IEEE 802.15.4 2009 sivu 22, 10.)



Kuva 21: Kuittauskehysten rakenne (IEEE 802.15.4 2009 sivu 22, 10.)

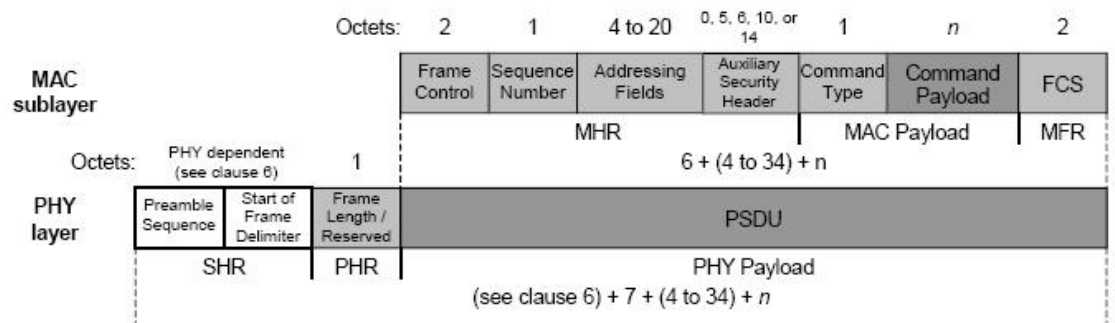
7.2.5 MAC-käskykehys

MAC-käskykehys muodostetaan MAC-alikerroksella. MAC-käskykehys sisältää käskyntyyppi- ja hyötydatakentän. Hyötydata sisältää itse käskyn. MAC-alikerroksella hyötydataan yhdistetään MAC-otsikko (MHR) ja perään lisätään MAC-alatunniste (MFR). MAC-otsikko sisältää kehyksen hallintakentän, datajärjestynumeron (DSN, data sequence number), osoitekentät ja vaihtoehtoisen lisäturvallisuusotsikon. MAC-alatunniste sisältää 16:sta bittisen kehyksen tarkistusluvun (FCS, frame check sequence). Nämä osat yhdessä muodostava MAC-käskykehysten (MPDU). (IEEE 802.15.4 2009 sivu 23, 10.)

Sen jälkeen kehykset siirretään fyysisellekerrokselle. Fyysiselläkerroksella kehyksestä tulee fyysisen kerroksen hyötydataa. Hyötydatan eteen lisätään vielä synkronointiotsikko (SHR), joka käsittää Preamble sequence ja Start-of-frame delimiter (SFD) kentät ja fyysisenkerroksen otsikon. Otsikko sisältää luvun, joka kertoo montako oktetia hyötydataa kehyksessä on. Preamble sequence mahdollistaa datan synkronoimisen vastaanottopäässä. Yhdessä nämä kentät muodostavat fyysisenkerroksen kehyksen (PPDU), mikä lähetetään siirtotielle. Kehys on esitetty kuvassa 22. (IEEE 802.15.4 2009 sivu 23, 10.)

Tietotekniikka, tietoliikennetekniikka

Joni Jokipii



Kuva 22: MAC-käskykehksen rakenne (IEEE 802.15.4 2009 sivu 23, 10.)

8 MAC-alikerros

MAC-alikerros tarjoaa kaksi palvelua. Ensimmäinen palveluista on MAC-datapalvelu (MAC data service), joka mahdollistaa datansiirron fyysisen kerroksen palveluita hyväksi käyttäen. Toinen palveluista on MAC-hallintapalvelu (MAC management service). Nämä kaksi palvelua liittyvät MAC-alikerroksen hallinta kokonaisuuteen (MLME, MAC sublayer management entity). Lisäksi MAC-alikerros huolehtii verkon Beacon-signaalin generoimisesta (mikäli laite on koordinaattori), synkronoinnista, verkon muodostuksesta, tietoturvasta, CSMA/CA tekniikan käyttämisestä, GTS:sien hyödyntämisestä sekä linkkien luonnista laitteiden välille. (IEEE 802.15.4 2009 sivu 17, 10)

9 Datan saapumisen varmistus

ZigBee käyttää monia tapoja varmistaakseen, että lähetetty data on mennyt perille ja se on pysynyt muuttumattomana matkan varrella. Nämä tavat ovat CSMA-CA:n käyttö, kuittaukset ja datan oikeellisuuden tarkistus esimerkiksi FCS:n (frame check sequence) avulla. Ensimmäisenä esittelyssä on CSMA/CA mekanismi. (IEEE 802.15.4 2009 sivu 23-24, 10.)

9.1 CSMA/CA

CSMA/CA on lyhenne sanoista Carrier Sense Multiple Access With Collision Avoidance. CSMA/CA on tapa jolla tietoliikenteessä varataan siirtotie. Tällä tavalla se on mahdollista jakaa monen eri käyttäjän kesken. ZigBee-verkko käyttää hyväkseen kahta CSMA/CA:n vaihtoehtoa riippuen verkon konfiguraatiosta. (IEEE 802.15.4 2009 sivu 23, 10.)

Ensimmäinen on aikajaoton (unsoltted) CSMA/CA. Se on käytössä niissä verkoissa, joissa Beacon-signaalin lähetys on pois käytöstä. Kun verkon laite haluaa lähettää dataa tai MAC-komentoja, sen täytyy odottaa satunnainen aika. Jos siirtotie on vapaa ja laite on odottanut satunnaisen vara-ajan, se lähettää datan siirtotielle. Jos siirtotie on käytössä vara-ajan jälkeen, niin laite odottaa toisen satunnaisen ajan ennen kuin yrittää ottaa siirtotietä uudelleen käyttöön. Näissä verkoissa kuittaukset lähetetään ilman CSMA/CA tekniikkaa. (IEEE 802.15.4 2009 sivu 23, 10.)

Verkoissa, joissa Beacon-signaalin lähetys on päällä, käytetään aikajaoteltua (slotted) CSMA/CA:ta. Se tarkoittaa sitä, että Beacon-signaalien välinen aika on jaettu aikaväleihin. Jokaisella aikavälillä on oma numeronsa. Verkon koordinaattori määrittelee aikavälit. Verkon laitteen halutessa lähettää kilpailuajavälien (CAP, contestion access period) aikana, se paikallistaa seuraavan aikavälin alkavan reunan. Kun reuna on löytynyt, laite odottaa satunnaisen aikavälien määrän. Jos

aikaväli on varattu, laite odottaa toisen satunnaisen aikavälien määrän ennen kuin yrittää ottaa siirtotietä uudelleen käyttöön. Jos siirtotie on vapaa, laite aloittaa lähetyksen seuraavan alkavan aikavälin alusta lähtien. Kuittaukset ja Beacon-signaalit lähetään ilman CSMA/CA tekniikkaa. (IEEE 802.15.4 2009 sivu 23, 10.)

9.2 Kuittaukset

Onnistunut vastaanotto ja datan oikeellisuuden vahvistus tai MAC-käskykehys voidaan todeta onnistuneeksi kuittauksella. Jos vastaanottava laite ei jostain syystä pysty käsittelemään tai ymmärtämään saapunutta kehystä, kuittausta ei lähetetä. Lähettänyt laite kuuntelee tuleeko siirtotieltä kuittausta, jos ei tule se olettaa että tiedonsiirto on epäonnistunut ja yrittää uudelleen. Jos kuittausta ei vielääkään kuulu, on lähettäjällä kaksi vaihtoehtoa, se voi yrittää tiedonsiirtoa uudelleen tai päättää että yritykset lopetetaan. Kun kuittausta ei vaadita, lähettäjä olettaa että jokainen viesti on saatu perille. (IEEE 802.15.4 2009 sivu 24, 10.)

9.3 Datan virheettömyys

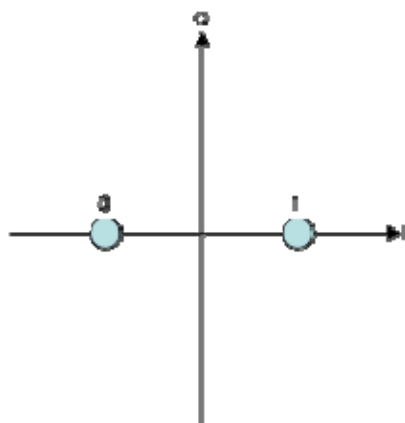
Jotta voitaisiin erottaa virheellinen tai puutteellinen data oikeasta, täytyy käyttää jotakin tarkistus algoritmia. ZigBee käyttää tiedonsiirrossa FCS (frame check sequence) mekanismia löytääkseen virheet saapuneesta kehyksestä. Kehyksien FCS-kenttä on kahden oktetin pituinen eli 16 bittiä. Tämä FCS kentän arvo lasketaan ITU-T:n CRC:n mukaan ja se lasketaan alkaen MHR-kentästä lähtien. (IEEE 802.15.4 2009 sivu 24, 10.)

10 Modulaatiot ZigBee-verkossa ja DSSS

ZigBee käyttää eri taajuusalueilla erilaisia modulaatio tapoja. Alemmat taajuudet, 868 MHz ja 915 MHz, käyttävät binääristä vaiheavainnusta (BPSK, binary phase-shift keying). 2,4 GHz:n alueella toimiva verkko käyttää modulaationa nelivaiheista vaiheavainnusta (O-QPSK, Offset quadrature phase-shift keying). O-QPSK:ssa kantoaalto voi olla neljässä eri vaiheessa. Täten yhdellä muutoksella voidaan siirtää kaksi bittiä.

10.1 Binäärinen vaiheavainnus (BPSK)

Binäärinen vaiheavainnus on vaiheavainnusten yksinkertaisin malli. Se käyttää kahta vaihetta, jotka ovat 180-asteen kulmassa toisiinsa nähden. Binaarinen vaiheavainnusta kutsutaan myös joskus nimellä 2-PSK. Binaarinen vaiheavainnus ei määrittele, missä kohtaa reaali- ja imaginaariakseleita vaiheet ovat. Kuvassa 23, nähdään BPSK:n konstellaatio Kuva, jossa vaiheet ovat 0 ja 180 asteen kohdalla. (Wikipedia: PSK 2009, 13.)



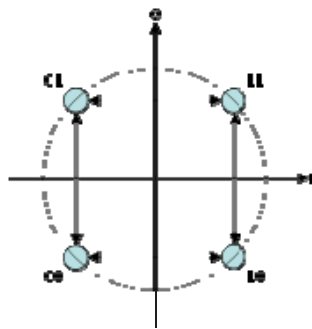
Kuva 23: BPSK:n konstellaatio Kuva (Wikipedia: PSK 2009, 13.)

Koska BPSK-modulaatio on näinkin yksiselitteinen, se on samalla myös erittäin robustinen. Robustinen tarkoittaa sitä, että tarvitaan suuri virhe, jotta demoduloinnista saatava tulkinta on väärä. Tämä kuitenkin aiheuttaa sen, että tällä

moduloinnilla voidaan koodata vain yksi bitti kerrallaan eli symbolinopeus on 1. Tästä syystä BPSK:ta ei voida käyttää nopeutta vaativaan tiedonsiirtoon varsinkin kun tiedonsiirtokaistaa on rajoitetusti. (Wikipedia: PSK 2009, 13.)

10.2 O-QPSK (Offset quadrature phase-shift keying)

O-QPSK on paranneltu versio QPSK:sta. Toisin kuin QPSK, O-QPSK:n signaali ei koskaan ylitä origoa. Tämä siksi, että vain yksi bitti muuttuu yhdessä muutoksessa. Kuvassa 24 on esitelty O-QPSK:n konstellaatioKuva, josta selviää myös mistä tilasta pääsee mihinkin tilaan. (Wikipedia: PSK 2009, 13.)



Kuva 24: O-QPSK:n konstellaatioKuva (Wikipedia: PSK 2009, 13.)

QPSK:ssa vaihe voi vaihdella maksimissaan 180 astetta. Kun signaali alipäästösuodatetaan, tämän vaiheen muutos aiheuttaa suuren amplitudi-muutoksen ja täten vaikeuttaa pääteasteen suunnittelua. O-QPSK:ssa ongelma on ratkaistu siten että toista, tässä tapauksessa Q-signaalia, viivästetään puolen symbolin verran. Tällä menettelyllä saadaan aikaan se, että amplitudi ei muutu niin nopeasti ja vaihe ei ikinä mene origon läpi. O-QPSK:ssa vaihe voi muuttua kerralla vain 90 astetta. Tämä helpottaa pääteasteen suunnittelua. (Wikipedia: PSK 2009, 13.)

Kuitenkin tällä modulaatiolla on samat ominaisuudet kuin QPSK:lla. Se pystyy yhdellä kokonaisella muutoksella siirtämään kaksi bittiä eli symbolinopeus on 2. (Wikipedia: PSK 2009, 13.)

10.3 DSSS (Direct Sequence Spread Spectrum)

Suorasekventointi eli DSSS on CDMA:ta hyödyntävissä järjestelmissä yleinen spektrin levitystekniikka. Suorasekvennoinnissa lähetettävä sanoma jaetaan pieniin osiin. Osien bittien perusteella katsotaan taulukosta 2, mikä pseudo-satunnainen koodi vastaa osan bittijonoa. Kun vastaavuus on löytynyt, se lähetetään siirtotielle. (Webopedia: DSSS 2009, 11.)

Siirtotiellä ongelmaksi muodostuu bittien koodaaminen niin, että viesti näyttää kohinalta. Vastaanottaja kuitenkin ymmärtää viestin, koska vastaanottaja tietää etsiä juuri tämän kaltaista bittijonoa kohinasta. Viesti voidaan vielä ymmärtää, vaikka se olisi 10 dB kohinan alapuolella. ZigBee käyttää 16 erilaista Speudo-satunnaista bittijonoa, jotka kaikki ovat 32 bitin pituisia. Jokainen 4 bitin sarja, mikä halutaan lähettää siirtotielle, koodataan tällaiseksi Speudo-satunnaiseksi bittijonoksi. (Wikipedia: DSSS 2009, 12.)

DSSS:n hyvänä puolena on se, että jos joku näistä Speudo-satunnaisista bittijonoista vahingoittuu ollessaan siirtotiellä, se on mahdollista korjata. Korjauksen ansiosta viesti saattaa olla vielä ymmärrettävissä ja täten viestiä ei tarvitse uusida. (Wikipedia: DSSS 2009, 12.)

11 Käyttötarkoitus, käyttökohteet ja tulevaisuus

Seuraavissa kappaleissa on esitetty ZigBeen käyttötarkoitus ja mahdolliset käyttökohteet sekä kerrottu hiukan tulevaisuuden näkymistä.

11.1 Käyttötarkoitus ja käyttökohteet

ZigBee-tekniikan etuina on sen erittäin pieni virrankulutus, yksinkertaisuus ja edullisuus. Näistä syistä johtuen käyttötarkoituksia ja kohteita on monia. ZigBee-tekniikkaa voitaisiin hyödyntää sekä teollisuudessa että kotona.

Kotiautomaatiossa ZigBeellä voitaisiin ohjata esimerkiksi lämmitystä, ilmastointia sekä valaistusta. Hyötyinä olisi suuri energiansäästö. Kotona ZigBeellä on mahdollista toteuttaa erilaiset laitteet, jotka toimivat kaukosäätimen avulla, korvaamalla kaukosäätimen lähetin ZigBee-tekniikalla.

Teollisuusautomaatio voisi hyödyntää ZigBee-tekniikkaa erilaisissa kohteissa, josta on vaikea tai mahdoton vetää kiinteitä kaapelointeja. Tällainen kohde voisi olla esimerkiksi siirrettävä kivenmurskain.

Yksi käyttökohde voisi olla sairaanhoito, jossa olisi mahdollista käyttää ihonalaisia tai ihonpäällisiä implantteja. Implantit kertoisivat hoitohenkilökunnalle jos potilaan tilassa tapahtuisi jotakin vakavaa, äkillistä tai muuta vastaavaa.

ZigBeen huonona puolena on sen tiedonsiirron hitaus, mutta jos ei tarvita suurta tiedonsiirtokapasiteettia, niin ZigBee käy melkein tarkoitukseen kuin tarkoitukseen.

11.2 Tulevaisuus

Tähän asti ZigBee laitteiden toimitusmäärät ovat olleet pieniä, mutta kasvu on ollut kuitenkin räjähdysmäistä. ZigBeen etuna on se, että se on standardoitu ja hyvissä

Tietotekniikka, tietoliikennetekniikka

Joni Jokipii

ajoin. Tämän takia ZigBee on hyvin yhteensopiva monien eri laitevalmistajien kesken. Oman haasteensa kuitenkin luo erilaisista verkkotopologioista aiheutuvat viive- ja virrankulutuserot sekä avoin sovelluskerros. Lisähaastetta tuo tietoturva, joka on sovelluskerrokselle jätetty sovelluksen tekijän harteille.

12 Yhteenveto

Tarkoituksena oli tutkia, Jennicin 5139-Z01-M01, lähetin/vastaanotin moduulia ja katsoa, mitä moduuli on sisälleen kätkenyt. Ideana oli kehitellä oma ZigBee-piiri ja mahdollisuuksien rajoissa myös toteuttaa se. Tämä ei kuitenkaan onnistunut.

Aloin tutkimaan ZigBeen standardia ja lähinnä sen lähetyspuolta. Itse lähetyspuolesta tiedon löytäminen oli vaikeaa, mutta kaikki mitä löysin on laitettu tähän raporttiin jossain muodossa. Onneksi ZigBee-standardista löytyi hyvin tietoa ja sain tehtyä tämän raportin. Tässä vaiheessa muutin hieman tavoitteitani siihen suuntaan, että lähetin osa jäi hieman vähemmälle huomiolle.

Mielestäni onnistuin tavoitteissani luoda aika kattavan tietopaketin ZigBeestä ja sen toiminnasta. Raporttia tehdessäni minulle valkeni aika monta termiä mitkä olivat aikaisemmin olleet hieman hämärän peitossa. Opin mielestäni paljon ZigBeestä ja muistakin termeistä mitkä eivät ainoastaan liity ZigBeehen.

Uskon että keräämästäni ZigBee tietopaketista on jollekin tulevaisuudessa hyötyä.

Lähteet

Sähköiset lähteet

1. Zigbee [viitattu 4.5.2009] Saatavissa:
<http://fi.wikipedia.org/wiki/ZigBee>
2. ZigBee Alliance [viitattu 5.5.2009] Saatavissa:
<http://www.zigbee.org/About/OurMission/tabid/217/Default.aspx>
- 3.. Software Technologies Group [viitattu 5.5.2009] Saatavissa:
http://www.stg.com/wireless/ZigBee_netw.html
4. Viestintävirasto [viitattu 20.5.2009] Saatavissa:
http://www.ficora.fi/attachments/suomiry/5DfGDjsyy/TJT_suomi.pdf
5. ZigBee Wireless Networkin [viitattu 15.5.2009] Saatavissa:
http://books.google.fi/books?id=up8Oa7456I8C&pg=PA297&lpg=PA297&dq=zigbee+address&source=bl&ots=ICFq7XwNBw&sig=ES6qpGk11YIr0JEvGY9vM6bBWw&hl=fi&ei=l3QSSqfcKdWD-AbP1LWmDw&sa=X&oi=book_result&ct=result&resnum=3#PPA297,M1
6. Jennic Wireless Microcontrollers [viitattu 9.5.2009] Saatavissa:
http://www.jennic.com/download_file.php?supportFile=JN-DS-JN5139-1v6.pdf
7. Movable Type Scripts [viitattu 15.5.2009] Saatavissa:
<http://www.movable-type.co.uk/scripts/aes.html>
8. CSRC [viitattu 13.5.2009] Saatavissa:
<http://csrc.nist.gov/archive/aes/index.html>

9. ZigBee Alliance esitys [viitattu 16.5.2009] Saatavissa:
http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=9436
10. IEEE 802.15.4 [viitattu 17.5.2009] Saatavissa:
<http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf>
11. Webopedia: DSSS [viitattu 21.5.2009] Saatavissa:
<http://www.webopedia.com/TERM/D/DSSS.html>
12. Wikipedia: DSSS [viitattu 21.5.2009] Saatavissa:
<http://fi.wikipedia.org/wiki/DSSS>
13. Wikipedia: PSK [viitattu 20.5.2009] Saatavissa:
http://en.wikipedia.org/wiki/Phase-shift_keying

Liitteet

Liite 1: ZigBee-radion lohkokaavio

Liite 1: ZigBee-radion lohkaavio

