Marko Ilmari

Lyhyen kantaman langattomat tiedonsiirtotekniikat

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietoliikennetekniikka
Insinöörityö
1.5.2012

Metropolia

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Marko Ilmari Lyhyen kantaman langattomat tiedonsiirtotekniikat 55 sivua + 1 liite 5.6.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoliikennetekniikka
Ohjaaja(t)	Yliopettaja Antti Koivumäki

Tässä insinöörityössä perehdytään langattomiin lyhyen kantaman tiedonsiirtotekniikoihin ja niiden ominaisuuksiin. Työ tehtiin kurssimateriaaliksi Metropolia Ammattikorkeakoululle, koska sillä ei aiemmin ollut hallussaan kompaktia kurssimateriaaliksi soveltuvaa esittelyä nykyaikaisista tiedonsiirtotekniikoista.

Työn tavoitteena on esitellä 12 tiedonsiirtotekniikkaa. Tarkoitus on auttaa opiskelijaa ymmärtämään, miten tiedonsiirtotekniikat eroavat toisistaan käyttösovelluksen, verkon rakenteen, kantaman, taajuuden ja tiedonsiirtonopeuden suhteen.

Työn valmistelu aloitettiin kysymällä ihmisiltä, missä järjestyksessä he mieluiten lukisivat tietoa uudesta tiedonsiirtotekniikasta. Tämän pohjalta luotiin järjestys, jonka mukaan tiedonsiirtotekniikoiden tiedot kerättiin muistiin. Näiden tietojen pohjalta kirjoitettiin tekniikoiden esittelyt.

Esittelyiden kirjoittamisen jälkeen tarkistettiin, mitä perustietoja niiden lukeminen edellyttää. Sen mukaan kirjoitettiin työn alkuun luku langattoman tiedonsiirron perusteista. Tiedonhakuun käytettiin pääasiassa internetiä. Työn lopuksi koottiin kaikkien esiteltyjen tekniikoiden ominaisuuksista taulukko, joka helpottaa tekniikoiden vertailua keskenään.

Työn tuloksena syntyi oppikirjan kaltainen teos, joka esittelee tiedonsiirtotekniikoita ja auttaa lukijaa vertailemaan niitä keskenään. Metropolia Ammattikorkeakoulu saa tästä kurssimateriaalin, jota voidaan hyödyntää tietoliikennetekniikan kursseilla. Työ soveltuu myös itseopiskelumateriaaliksi. Työssä mainittuja tietoja voidaan hyödyntää myös tulevien kurssimateriaalien ja muiden esittelyjen teossa.

Avainsanat	Bluetooth, WLAN, RFID, WUSB, Dash7, EnOcean

Metropolia

Abstract

Author(s) Title Number of Pages Date	Marko Ilmari Short-range Wireless Data Transfer Methods 55 pages + 1 appendices 5 June 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Telecommunication
Instructor(s)	Supervisor & Instructor: Antti Koivumäki, Principal Lecturer

In this study different short-range wireless data transfer methods and their qualities are demonstrated. The study was done for Metropolia University of Applied Sciences to serve as course material, because there was no such material available prior to the present study.

The target was to demonstrate 12 data transfer methods. The aim is to help the student to understand, how different data transfer methods diverge from each other as to application, network topology, range, frequency and bit rate.

The preparation for the study was begun by asking people in which order they would prefer reading information about a new wireless data transfer method. Based on the answers a demonstrating order was created and it was followed through the study while writing the demonstrations of the methods.

After demonstrating the methods the readability and simplicity of the written information was checked. Based on this, the basics of wireless data transfer were introduced at the beginning of the study.

In the study the Internet was mostly used as a source for information. In the end of the study there is a collective table of the properties of data transfer methods, where the aim is to ease the comparison of the methods.

As the result of the study a textbook-like production was created. The study demonstrates short-range wireless data transfer methods and helps the student to compare them against each other. Metropolia University of Applied Sciences has this as a course material that can be used in telecommunication courses. It is also usable as a self-study material.

Keywords	Bluetooth, WLAN, RFID, WUSB, Dash7, EnOcean

Sisällys

Liitteet

Lyhenteet

8DPSK	8-Differential Phase-shift keying, vaiheen muuntamiseen perustuva modulaatiotekniikka, käytössä esimerkiksi Bluetoothissa.
ASK	Amplitude-Shift keying, Amplitudin muuttamiseen perustuva modulaatiotekniikka.
b	bitti, pienin mahdollinen informaation yksikkö. Bitillä on kaksi mahdollista arvoa, joita kuvaavat yleensä ykkönen ja nolla.
B	tavu, kahdeksan bitin muodostama informaation yksikkö.
BLE	Bluetooth Low Energy technology, vähävirtainen versio Bluetoothista.
DCM	Dual Carrier Modulation, kahteen kantoaaltoon perustuva tiedon modulaatiomenetelmä.
ETSI	European Telecommunications Standards Institute, eurooppalainen telealan standardoimisjärjestö.
FSK	Frequency Shift Keying, kantoaallon taajuuden muuttamiseen perustuva modulaatiotekniikka.
GFSK	Gaussian Frequency Shift Keying, kantoaallon taajuuden muuttamiseen perustuva modulaatiotekniikka, jossa signaali menee gausaalisen suotimen läpi.
HID	Human Interface Device, ihmisen ja koneen väliseen rajapintaan suunniteltu laite.
ISM	Industrial, Scientific and Medical, teolliseen, tieteelliseen ja lääketieteelliseen käyttöön tarkoitettu radiotaajuusalue, joka on yleisesti käytettävissä.

kbps	kilobittiä sekunnissa, tiedonsiirtonopeuden mittayksikkö. Tämän synonyymejä ovat myös kbit/s ja kb/s.
Mbit/s	megabittiä sekunnissa, tiedonsiirtonopeuden mittayksikkö. Tämän synonyymejä ovat myös Mbps ja Mt/s.
OOK	On-Off keying, yksinkertaisin tapa toteuttaa amplitudin muuntamiseen perustuva modulaatio.
PSK	Phase-Shift keying, signaalin vaiheen muuttamiseen perustuva modulaatiotekniikka.
π/4-DQPSK	π/4-Differential Quadrature Phase-shift keying, vaiheen muuntamiseen perustuva modulaatiotekniikka, käytössä esimerkiksi Bluetoothissa
QoS	Quality of Service, prioriteettijärjestelmä verkkoliikenteelle, jossa tärkeäksi luokiteltu tieto voi kulkea ruuhkaisessakin tietoverkossa ongelmitta.
UWB	Ultra Wide Band, erittäin laajan taajuusalueen omaava tiedonsiirtotekniikka, jota käytetään muun muassa Wireless USB-standardissa.
WUSB	Wireless USB, eli Wireless Universal Serial Bus; langaton kehitteillä oleva tiedonsiirtotekniikka tietokoneen ja sen oheislaitteiden väliseen kommunikaatioon.
XTEA	Extended Tiny Encryption Algorithm, yksinkertainen algoritmi tiedon salaukseen.

1 Johdanto

Tässä insinöörityössä esitellään nykyaikaisia langattomia lyhyen kantaman tiedonsiirtotekniikoita. Työ on tehty kurssimateriaaliksi Metropolia Ammattikorkeakoulun tietoliikennetekniikan opiskelijoille. Työ katsottiin tarpeelliseksi tehdä, sillä Metropolialla ei aiemmin ollut tämän kaltaista esittelyä eri tiedonsiirtotekniikoista.

Työn tavoite on antaa opiskelijalle selkeä kuva 12 nykyaikaisesta langattomasta tekniikasta sekä helpottaa niiden vertailemista keskenään. Työhön on valikoitu yleisiä käytössä olevia tekniikoita, kuten WLAN, Bluetooth ja RFID. Niiden lisäksi mukana on myös vähemmän tunnettuja tekniikoita, joilla kuitenkin on joitakin edistyksellisiä ominaisuuksia käytössään. Sellaisia ovat Dect, Dash7, EnOcean, One-Net ja Z-Wave. Osa esitellyistä tekniikoista, kuten ZigBee, WUSB, MyriaNed ja NFC, tekevät vasta tuloaan.

Ennen työn aloittamista ihmisiltä kysyttiin, missä järjestyksessä he mieluiten opiskelisivat tietoja uudesta langattomasta tiedonsiirtomenetelmästä. Tekniikoita esiteltäessä noudatettiin sitä järjestystä, joka oli saanut kyselyssä eniten ihmisten kannatusta.

Tekniikoiden esittelyissä keskitytään siihen, missä niitä käytetään, millaista tietoa niillä siirretään ja minkä mallisen verkon laitteet voivat muodostaa keskenään. Tekniikoissa perehdytään myös niiden teknisiin ominaisuuksiin, kuten taajuuksiin, kantamiin, tiedonsiirtonopeuksiin ja salauksiin.

Lisäksi kunkin tekniikan kohdalla kerrotaan lyhyesti sen historiasta sekä sitä hallitsevasta organisaatiosta. Joihinkin esittelyihin on sisällytetty myös muuta oleelliseksi katsottua tietoa esimerkiksi tekniikan tavasta toteuttaa tiedonkulku. Esittelyihin on sisällytetty tekniikoiden muistamista ja ymmärtämistä helpottavia kuvia ja taulukoita.

Työn lopuksi tekniikoista on koottu niiden ominaisuuksia vertaileva taulukko. Tekniikat on mahdollista opiskella satunnaisessa järjestyksessä, joskin kaikissa esitelmissä edellytetään tietoliikennetekniikan perusteiden ymmärtämistä. Seuraavassa luvussa perusteet on käyty lyhyesti läpi.

2 Langattoman tiedonsiirron perusteet

2.1 Kantama

Kantamalla eli kuuluvuusalueella tarkoitetaan laitteiden välisen langattoman tiedonsiirron maksimietäisyyttä. Kantamaan vaikuttaa tiedonsiirrossa käytettävä lähetysteho, vastaanottimen herkkyys sekä antennin tyyppi. Käytetty taajuus puolestaan vaikuttaa yhteyden kykyyn läpäistä esteitä.

Monissa laitteissa antennit ovat ympärisäteileviä, mikä tarkoittaa sitä, että antennit lähettävät tietoa samalla voimakkuudella kaikkiin suuntiin. Tämä mahdollistaa laitteiden vapaan sijoittelun sekä useassa tapauksessa laitteiden liikuttelun tiedonsiirron aikana, mutta haittapuolena tässä on lähetystehon nopea heikkeneminen kauemmaksi mentäessä.

Tätä sovellusta voisi verrata hehkulamppuun, mikä säteilee valoa kaikkiin suuntiin. Läheltä katsottaessa valo on kirkas, mutta sen teho heikkenee eksponentiaalisesti pois päin mentäessä. Vaihtoehtona ympärisäteilevälle antennille on suunta-antenni, mikä on järkevä vaihtoehto kiinteästi asennettuihin laitteisiin. Tällöin valtaosa säteilystä kulkee tiettyyn suuntaan, mikä nostaa kantamaa huomattavasti pienentäen sitä muualta. Ratkaisua voisi verrata tavalliseen spottivalaisimeen.

Mitä kauempaa tieto tulee, sitä heikompaa se on, ja sitä herkemmän vastaanottimen se myös tarvitsee. Myös vastaanotin on mahdollista suunnata keräämään tietoa tietystä suunnasta, jolloin heikommastakin lähetyksestä voidaan saada selvää. Esimerkiksi lautasantennit toimivat näin kooten saapuvan radiosäteilyn tiettyyn kohtaan antennissa.

2.2 Taajuudet

Radioaallot jakautuvat useisiin taajuusalueisiin. Lähes kaikki tässä materiaalissa esiteltävät tekniikat käyttävät korkealla, UHF-radiotaajuusalueella värähteleviä 300 - 3000 MHz:n taajuuksia. UHF tulee sanoista Ultra High Frequency.

300 - 3000 MHz:n radiotaajuuksia kutsutaan myös mikroaalloiksi, mutta tässä työssä käytetään kuitenkin selkeyden vuoksi aina radio-etuliitettä. Taulukkoon 1 on listattu korkeat radiotaajuusalueet.

Taulukko 1. Korkeat radiotaajuusalueet

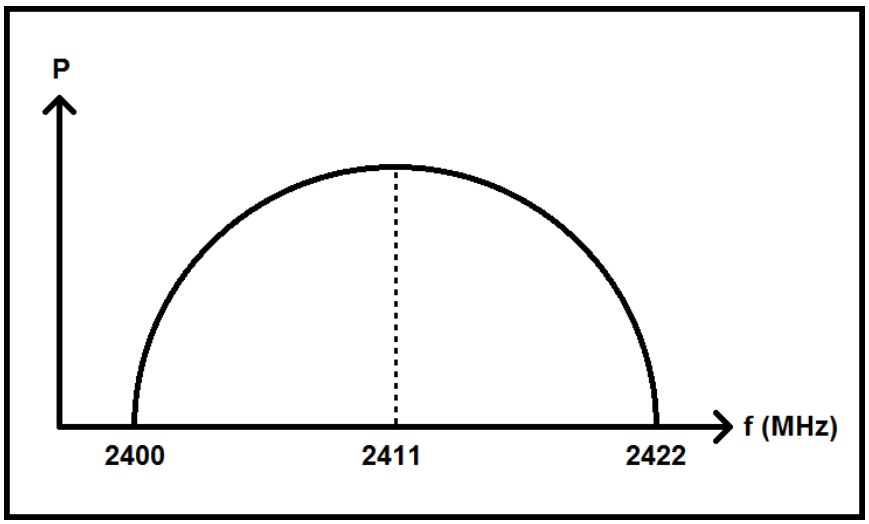
Lyhenne	Taajuusalueen nimi	ITU-numero	Taajuusalue ja aallonpituus	Käyttö-sovellus
HF	High frequency	7	3 – 30 MHz 100 m – 10 m	
VHF	Very high frequency	8	30 – 300 MHz 10 m – 1 m	FM-radiokanavat
UHF	UHF high frequency	9	300 – 3000 MHz 1 m – 100 mm	Langattomat lyhyen kantaman tiedonsiirto-tekniikat
SHF	Super high frequency	10	3 – 30 GHz 100 mm – 10 mm	
EHF	Extremely high frequency	11	30 – 300 GHz 10 mm – 1 mm	
THz tai THF	Terahertz tai Tremendously high frequency	12	300 – 3000 GHz 1 mm – 100 µm	

Taajuuden valinnalla on merkitystä yhteyden ominaisuuksiin. Jos käytettäväksi valitaan korkeampi taajuus (esimerkiksi yli 2 GHz), tällöin voidaan saavuttaa suuri tiedonsiirto-nopeus, ja myös antennit ovat pienempiä. Toisaalta korkeat taajuudet läpäisevät esteitä heikommin. Matalien taajuuksien etuna on vastaavasti parempi esteenläpäisykyky,

mikä antaa lisämahdollisuuksia käyttösovelluksiin, mutta tiedonsiirto on lähtökohtaisesti hitaampaa ja antennit isompia.

Mikäli kaksi eri tietoliikenneyhteyttä käyttää samassa fyysisessä tilassa samaa taajuutta, ne interferoituvat, eli sekoittuvat keskenään. Tämä ei kuitenkaan tarkoita, että kaikki tietylle, esimerkiksi 2,4 GHz:n alueelle kuuluvat taajuudet interferoisivat keskenään: 2,4 GHz:n alueella kunkin taajuuden teho jakautuu yhteensä 22 MHz:n alueelle siten, että teho on suurimmillaan kanavan ominaistaajuuden kohdalla.

Kanavasta poispäin mentäessä sen teho heikkenee eksponentiaalisesti ja saavuttaa nollakohdan 11 MHz:n päässä kanavasta. Tällöin esimerkiksi 2411 MHz:n taajuus häiritsee aluetta 2400 - 2422 MHz kuvan 1 mukaisesti.



Kuva 1. 2,4 GHz taajuuden tehon jakautuminen vierekkäisille taajuuksille

2.3 Modulointi

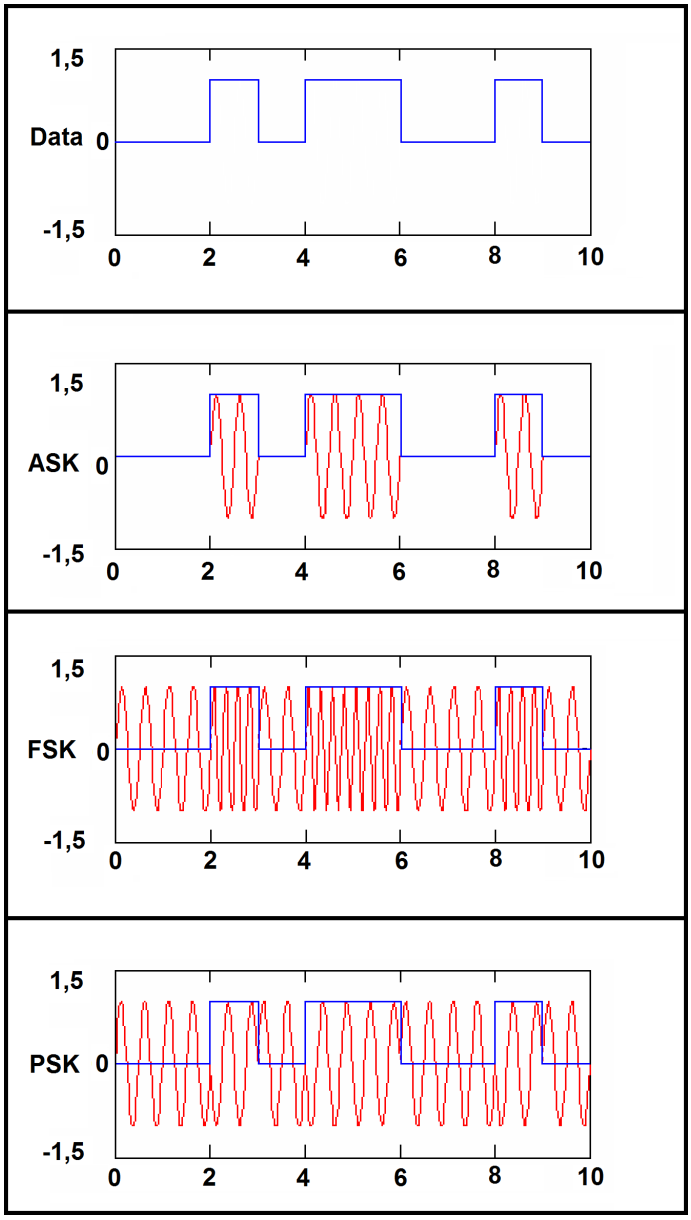
Radioliikenteessä lähetettävää tietoa voidaan myös muuntaa eli moduloida ja sitä hyödynnetäänkin lähes kaikissa tekniikoissa. Tämä tarkoittaa sitä, että signaaliin, joka normaalisti näyttäisi yksinkertaiselta siniaallolta, sisällytetään lisäinformaatiota muuntamalla sen muotoa. Moduloinnilla voidaan kasvattaa bittinopeutta tietoliikenteessä, kun signaaliin saadaan muitakin vaihtoehtoja kuin 1 ja 0 (lähetys ja ei lähetystä).

Seuraavaksi käydään läpi muutamia yksinkertaisia modulaatiotekniikoita. Niiden toimintaperiaatetta havainnollistetaan kuvassa 2. Nykyisissä tiedonsiirtotekniikoissa käytetään usein näitä hienostuneempia ja monipuolisempia modulaatiotekniikoita, jotka yhdistelevät eri tapoja sisällyttää signaaliin lisäinformaatiota.

Yksi tapa moduloida signaalia on muuttaa sen amplitudia, joka normaalisti olisi vakio. Tällöin siniaallon taajuus ja vaihe pysyvät ennallaan, mutta sen voimakkuuden vaihtelut välittävät tarvittavan tiedon. Tästä esimerkkinä on ASK-modulaatio (Amplitude-Shift keying).

Lähetettävästä signaalista voidaan muuttaa myös taajuutta. Tämä on tehtävä siten, että taajuuden muutos ei ole merkittävän suuri itse lähetettävään taajuuteen (kantoaaltoon) nähden. Tätä käytetään muun muassa FSK-modulaatiossa (Frequency-Shift keying).

Signaalista voidaan muuttaa myös vaihetta. Vaihemodulaatiossa siniaalto ja sen vaiheen muutoskohdat välittävät lähetetyn informaation. Esimerkiksi PSK-modulaatio (Phase-Shift keying) käyttää tätä hyödykseen.



Kuva 2. Siirrettävän datan lähetys ASK:ta, FSK:ta ja PSK:ta käyttäen [1]

Erilaisia modulaatiotekniikoita on olemassa runsaasti. Niissä voidaan käyttää muitakin menetelmiä, joilla tiedonsiirtonopeus saadaan kasvamaan. Toisaalta mitä hienostuneemmin signaalia moduloidaan, sitä alttiimpi se on häiriöille. Hyvissä olosuhteissa signaalia voidaan moduloida reilustikin, ja häiriöisissä ympäristöissä tarvitaan puolestaan yksinkertaisempaa modulaatiota, jotta lähetyksestä saataisiin selvää.

2.4 Bitit ja tavut

Tiedonsiirtonopeudet ilmoitetaan tässä työssä bittinopeuksina eli bitteinä sekunnissa. Tässä on kuitenkin pieni mahdollisuus sekoittaa kaksi asiaa toisiinsa: Arkikielessä esimerkiksi 3 Mbit/s tiedonsiirtonopeuden omaavaa yhteyttä sanotaan usein "kolmemegaiseksi". Myös tiedostojen koista puhuttaessa käytetään usein nimitystä "mega", mikä puolestaan tarkoittaa megatavua.

Tavu kuitenkin koostuu aina kahdeksasta bitistä. Taulukkoon 2 on merkitty keskeisimmät tiedot biteistä ja tavuista.

Taulukko 2. Bitit ja tavut

Nimitys	Yksikkö	Tiedonsiirtonopeuden yksikkö	Lukumäärien vastaavuus	Nopeuksien vastaavuus (esimerkki)
bitti	b, bit	b/s, bit/s, bps	8 kpl	24 Mb/s
tavu	B, t	B/s, t/s, Bps	1 kpl	3 MB/s

2.5 Protokollat

Tietoliikennetekniikat määritellään niiden käyttämien protokollien eli yhteyskäytäntöjen avulla. Protokollat ovat standardeja, jotka määrittelevät laitteiden ja ohjelmien väliset yhteydet. Määritelmät sisältävät tiedot siitä, miten yksi osapuoli lähettää viestin toiselle, kuinka tämä reagoi siihen ja niin edelleen.

2.6 Radiosäteilyn vaikutukset elävään kudokseen

Radiotaajuuksien vaikutuksista ympäristöön ja ihmiskeholle on tehty tutkimuksia. Monet tässä työssä esitellyt tekniikat, kuten Bluetooth ja WLAN toimivat lisensöimättömällä 2,4 GHz:n taajuusalueella, josta käytetään myös nimitystä ISM Band (Industry, Science and Medical Band).

USA:n liittovaltion viestintäkomissio (FCC) määritteli nämä taajuudet toisarvoisiksi taajuuksiksi vuonna 1985 [4]. Samoja radiotaajuuksia käyttävät muiden muassa mikroaaltouunit, joskin huomattavasti suuremmilla tehoilla.

Havaintoja radiolaitteista saatujen säteilymäärien vaikutuksista on tehty. Esimerkiksi alankomaalaisen Wageningenin yliopiston tekemän tutkimuksen mukaan WLAN-laitteet vahingoittavat puita: saarnipuita altistettiin kolmen kuukauden ajan WLAN-yhteydelle, jonka johdosta puiden lehdistä hävisi osa uloimmasta solukerroksesta ja lehdet alkoivat kuihtua. [2, s. 13.]

Myös Maailman terveysjärjestö WHO:n syöpävirasto IARC (International Agency for Research on Cancer) on ilmoittanut lehdistötiedotteessaan, että langattomien laitteiden säteily on mahdollisesti syöpää aiheuttavaa. Viraston mukaan säteily asettuu IARC-asteikolla luokkaan 2B - mahdollisesti karsinogeeniset. Tiedotteessa ei kuitenkaan kerrottu, mistä taajuuksista tarkalleen ottaen on kyse. [3.]

Tavanomaisia GSM-taajuuksia ovat 900 MHz:n, 1800 MHz:n ja 1900 MHz:n taajuudet. 3G-taajuuksia puolestaan ovat useat taajuudet välillä 700 MHz - 2600 MHz. Radiosäteilylle altistumisen määrä riippuu altistumisajasta ja säteilijän etäisyydestä sekä sen lähetystehosta. Radiosäteilyä on kaikkialla, joten täydellinen suojautuminen siltä on lähes mahdotonta: muiden muassa antenni-TV- ja radiolähettimet, GPS-satelliitit ja GSM-tukiasemat säteilevät radiosäteilyä jatkuvasti.

Säteilyn määrää voi minimoida myös henkilökohtaisessa elämässään: WLAN-yhteyden sijasta voi harkita langallisen yhteyden käyttöä, älypuhelimesta voi sulkea joutilaana päällä olevat yhteydet ja kännykkäpuhelut voi halutessaan hoitaa myös langallisella kuulokemikrofonilla.

3 Bluetooth

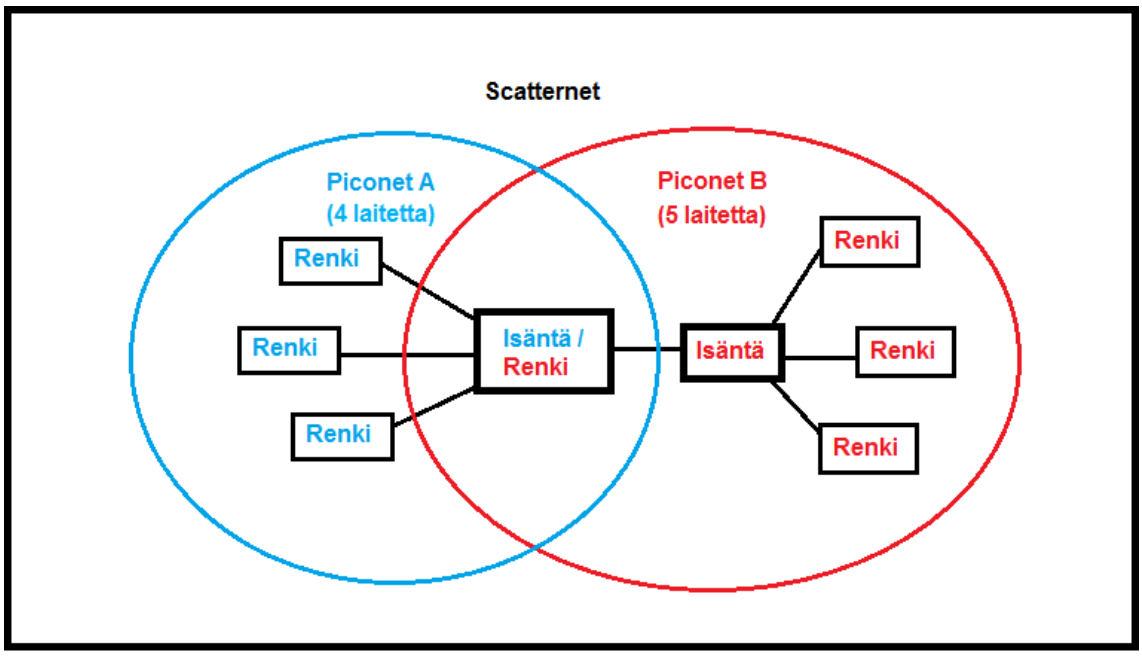
Tässä luvussa perehdytään Bluetoothiin, joka on radioteitse toimiva, lyhyille välimatkoille suunniteltu tiedonsiirtostandardi. Sen tarkoituksena on korvata kaapelit esimerkiksi kännykän ja tietokoneen välillä. Bluetooth on käytössä nykyään monissa laitteissa ja sen avulla voidaan siirtää tietoa useassa eri muodossa. Bluetooth-valmius löytyy

myös monista tietokoneen oheislaitteista, sykemittareista, tulostimista, tableteista sekä GPS-vastaanottimista. Bluetoothin logo on kuvassa 3.

Kuva 3. Bluetooth-logo

Bluetooth perustuu Personal Area Network -malliin, jossa on yksi isäntä (master) ja 1-7 renkiä (slave). Tällainen verkko on nimeltään piconet. Piconet-verkossa isäntä hallinnoi tiedon lähetystä. Esimerkiksi valokuvien jako matkapuhelimesta toiseen muodostaa kahden osapuolen välisen piconetin, jossa on isännän lisäksi vain yksi renki.

Bluetooth-standardi mahdollistaa laitteiden olemisen samaan aikaan useassa eri piconetissä, jolloin kyseessä on scatternet-verkko. Tällöin sama laite voi toimia sekä isäntänä että renkinä samanaikaisesti eri piconet-verkoissa. [5] Scatternet-verkon rakenne on esitetty kuvassa 4.



Kuva 4. Kahdesta piconetistä koostuva scatternet-verkko, jossa yksi laite toimii kaksoisroolissa

3.1 Historia

Ericsson (nykyisin Sony Ericsson) kehitti Bluetoothin vuonna 1994. Sen oli tarkoitus tulla RS-232-kaapelin langattomaksi vaihtoehdoksi. Kehiteltyään Bluetoothia hetken Ericsson perusti Bluetooth SIG -ryhmän (Special Interest Group) mm. Nokian, IBM:n ja Intelin kanssa. Tavoitteena oli luoda de facto -standardi, jossa korostuvat standardin itsenäisyys ja tunnettuus.

Sigin tehtävänä on alusta lähtien ollut hallinnoida Bluetooth-standardia ja valvoa sen määrittelyä. Sigillä oli vuonna 2011 jäsenenä yli 15 000 yritystä tietotekniikan eri aloilta. Kaikkien Bluetooth-laitteiden tulee läpäistä Sigin laatustandardit ennen markkinoille tulemistaan.

Bluetooth on nimetty 900-luvulla eläneen viikinkikuninkaan, Harald Bluetoothin mukaan. Logo puolestaan on luotu yhdistämällä skandinaaviset riimut Hagall ja Berkanan.

3.2 Tekniset tiedot

Bluetooth-tiedonsiirron ominaisuudet riippuvat paljolti siitä, mikä versio on käytössä ja missä luokassa tietoa siirretään. Bluetoothista on julkaistu tähän mennessä neljä versiota, joiden myötä etenkin tekniikan tiedonsiirtonopeus ja virransäästöominaisuudet ovat kehittyneet. Käytettävä luokka puolestaan määrää tiedonsiirrolle lähetystehon ja siten myös maksimietäisyyden.

Käyttäjälle nämä asiat ovat usein läpinäkyviä, joten hänen ei yleensä tarvitse välittää niistä. Taulukko 3 kertoo eri Bluetooth-versioiden nopeuksista ja yhteensopivuuksista. Kolmannessa ja neljännessä versiossa suurin osa tiedonsiirrosta voi tapahtua WLAN-yhteyttä pitkin, mikäli sellainen on saatavilla.

Taulukko 3. Versiot

Versio	Tiedonsiirtonopeus (teoreettinen)	Taaksepäin yhteensopivuus
v1.1	1 Mbit/s	N/A
v1.2	1 Mbit/s	v1.1

v2.0 + EDR	3 Mbit/s	v1.2
v2.1 + EDR	3 Mbit/s	v2.0, v1.2
v3.0 + HS	24 Mbit/s (WLAN)	v2.1 + EDR
v4.0	24 Mbit/s (WLAN)	Kaikki aikaisemmat

Bluetooth-luokat on eritelty taulukossa 4. Tästä nähdään, että kantaman kasvaessa aritmeettisesti tarvittava lähetysteho kasvaa eksponentiaalisesti.

Taulukko 4. Bluetooth-luokat, niiden lähetystehot ja kantamat

Luokka	Maksimiteho (mW)	Maksimiteho (dBm)	Kantama (m)
Class 1	100	20	100
Class 2	2,5	4	10
Class 3	1	0	5

3.3 Virransäästö

Bluetoothin aikaisemmilla versioilla on joitakin virransäästöominaisuuksia, mutta eniten virransäästöön on panostettu Bluetoothin neljännessä versiossa. Siinä on pienennetty virrankulutusta niin tiedonsiirron kuin valmiustilankin aikana. Sulautetuissa järjestelmissä voidaan saavuttaa parhaimmillaan muutaman vuoden toiminta-aika yhdellä nappiparistolla.

Tämä uusi virransäästötekniikka sai alkunsa Nokian Wibree-tekniikasta, ja kulkee nykyään Bluetooth 4.0:aa täydentävänä ominaisuutena nimikkeellä Bluetooth Low Energy Technology, eli BLE. Perinteistä Bluetoothia ja BLE:tä on vertailtu taulukossa 5.

Taulukko 5. Bluetoothin ja BLE:n vertailua

Ominaisuus	Perinteinen Bluetooth-tekniikka	Bluetooth low energy technology (BLE)
Kantama	100 m	50 m
Tiedonsiirtonopeus (kokonaisnopeus)	1 – 24 Mbit/s	1 Mbit/s
Tiedonsiirtonopeus (sovelluksessa)	0.7 – 2.1 Mbit/s	0,26 Mbit/s
Renkejä	1 - 7	Riippuu toteutuksesta
Salaus	56/128-bittinen salaus	128-bittinen AES-salaus
Kanavia (kpl)	79	40
Kanavien vaihto-väli (MHz)	1	2
Latenssiaika yh-teydettömästä tilasta	100 ms	6 ms
Äänen siirtomah-dollisuus	Kyllä	Ei
Verkkotopologia	Scatternet	Tähtimäinen
Virrankulutus	(Bluetoothin määritel-mä ei määrää virran-kulutusta)	1-5 % perinteisen Blue-toothin virrankulutuksesta
Virrankulutuksen huippuarvo	<30 mA	<20 mA (maks. 15 mA nappiparistolla)
Ensisijaiset käyttö-sovellukset	Matkapuhelimet, peli-konsolit, kuulokemikro-fonit, äänensiirto, au-tosovellukset, PC:t, turvallisuus, lähitunnis-tus, terveydenhuolto, urheilu	Matkapuhelimet, pelikon-solit, autosovellukset, PC:t, turvallisuus, lähi-tunnistus, kellot, tervey-denhuolto, urheilu, kodin elektroniikka, automaa-tio, teollisuus

3.4 Tietoturvallisuus

Bluetooth on lähtökohtaisesti tietoturvallinen standardi sen käyttämän taajuushyppelyn ansiosta. Tiheästi vaihtuvat kanavat asettavat omat haasteensa salakuuntelulle, ja myös käytettävät salausavaimet tuovat lisäsuojaa tiedonsiirrolle.

Bluetooth tukee AES-kryptausta. Myös osapuolten mahdollinen liikkuminen vaikeuttaa salakuuntelun onnistumista, koska tällöin signaalien tehot vaihtelevat helposti. Omat haasteensa salakuuntelulle tuo myös tiedonsiirron satunnaisuus ajan ja paikan suhteen.

Vaikka Bluetooth on lähtökohtaisesti tietoturvallinen standardi, on sen kautta kuitenkin mahdollista joutua hyökkäyksen kohteeksi. Näin voi käydä, jos esimerkiksi hyväksyy julkisissa tiloissa ollessaan tuntemattoman, harmittoman kuuloisen lähetyksen, joka sisältääkin haittaohjelman. On perusteltua ottaa Bluetooth-lähetyksiä vastaan vain silloin, kun lähettäjän identiteetti on tiedossa.

3.5 Kanavat ja modulaatio

Bluetooth toimii lisensöimättömällä 2,4 GHz:n ISM-taajuusalueella samoin kuin esimerkiksi WLAN. Bluetooth käyttää tiedonsiirtoon 79:ää kanavaa, jotka sijaitsevat sen taajuusalueella 1 MHz:n välein. Varsinaista taajuushyppelyaluetta reunustavat suojakanavat (guardian channels). Taulukkoon 6 on merkitty tarkemmat tiedot taajuuksista ja kanavista.

Taulukko 6. Bluetooth-taajuudet ja kanavat

Taajuusalue (suojakanavien kanssa)	2400 - 2483,5 MHz
Taajuushyppelyalue	2402 - 2480 MHz
Kanavia	79 kpl
Kanavien väli toisiinsa nähden	1 MHz
Taajuuden vaihtoväli, jakson pituus	1 s / 1600 = 0,625 ms

Paketin pituus	1, 3 tai 5 jaksoa

Alun perin Bluetooth käytti GFSK-modulaatiota, jossa tietoa välitetään muuttamalla lähetyksen taajuutta. Kanavavälin ollessa 1 MHz taajuuden muutokset voivat olla 500 kHz molempiin suuntiin. Myöhemmät Bluetooth-versiot tukevat vaiheen muuntamiseen perustuvia modulaatiomenetelmiä, kuten π/4-DQPSK:ta ja 8DPSK:ta.

3.6 Protokollat

Bluetooth määritellään sen protokollien, eli yhteyskäytäntöjen avulla. Kukin Bluetooth-laite käyttää vain tarvitsemaansa osaa kaikista olemassa olevista protokollista. Bluetooth-protokollat jakautuvat ydinprotokolliin, kaapelit korvaaviin protokolliin, puhelinprotokolliin sekä muualta adoptoituihin protokolliin.

Ydinprotokollista kantataajuusprotokolla hallinnoi Bluetoothissa yhteyden synkronointia ja taajuushyppelyä. Se tarkistaa lähtevän datan ja palauttaa yhteyden virheistä. LMP, eli Link Management Protocol puolestaan muodostaa radioyhteyden ja pitää sitä yllä.

HCI (Host Controller Interface) taas sisältää rajapinnan näiden protokollien hallinnointiin ja Bluetooth-laitteiden käsittelyyn. Yhdistämällä nämä protokollat yhteen fyysiseen moduuliin ja lisäämällä siihen antenni ja virtalähde, saadaan yksinkertaisin mahdollinen Bluetooth-laite ilman palveluita.

Adoptoituja protokollia ovat mm. PPP (Point-to-Point) -protokolla, joka nimensä mukaan muodostaa PPP-yhteydet sekä TCP/IP/UDP, joka mahdollistaa kommunikoinnin internetiin kytkettyjen laitteiden kanssa esimerkiksi Bluetooth-modeemeissa.

4 WLAN

WLAN (Wireless Local Area Network) on yksi yleisimmistä langattomista lyhyen kantaman tiedonsiirtostandardeista. Se on tarkoitettu lähinnä internetin käyttöä varten, ja se löytyy nykyään lähes kaikista kannettavista tietokoneista ja älypuhelimista.

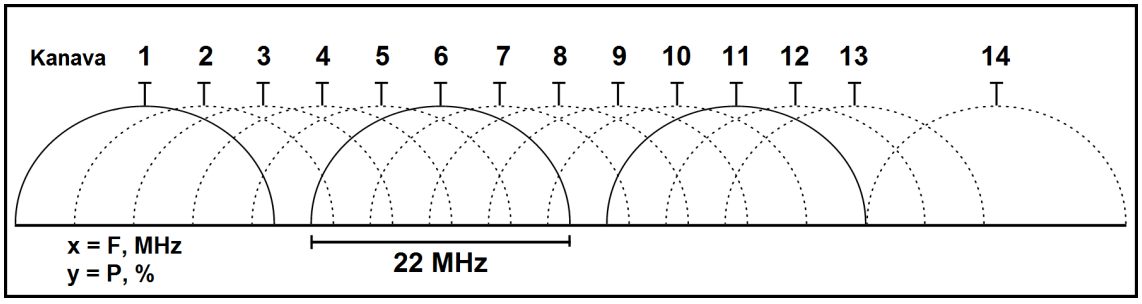
WLAN-standardista käytetään myös nimitystä IEEE 802.11. Sitä käytetään erityisesti silloin, kun halutaan keskittyä johonkin tiettyyn standardiin, jotka voidaan ymmärtää myös WLAN:in eri versioina.

Eri 802.11-standardeja merkitään päätekirjaimilla, ja jokaisella niistä on omat ominaisuutensa. Niistä kerrotaan lisää tuonnempana. WLAN:ia kutsutaan myös nimellä WiFi, joka on tekniikan kaupallinen nimitys. WiFi:n logo on kuvan 5 mukainen.

Kuva 5. WiFi-logo

WLAN käyttää tiedonsiirtoon 2,4 GHz:n taajuusaluetta. Amerikassa kanavia on käytössä 11, Euroopassa 13 ja Japanissa 14. Kanavia on huomattavasti vähemmän kuin esimerkiksi Bluetoothissa, joka käyttää hyödykseen lähes samaa taajuusaluetta.

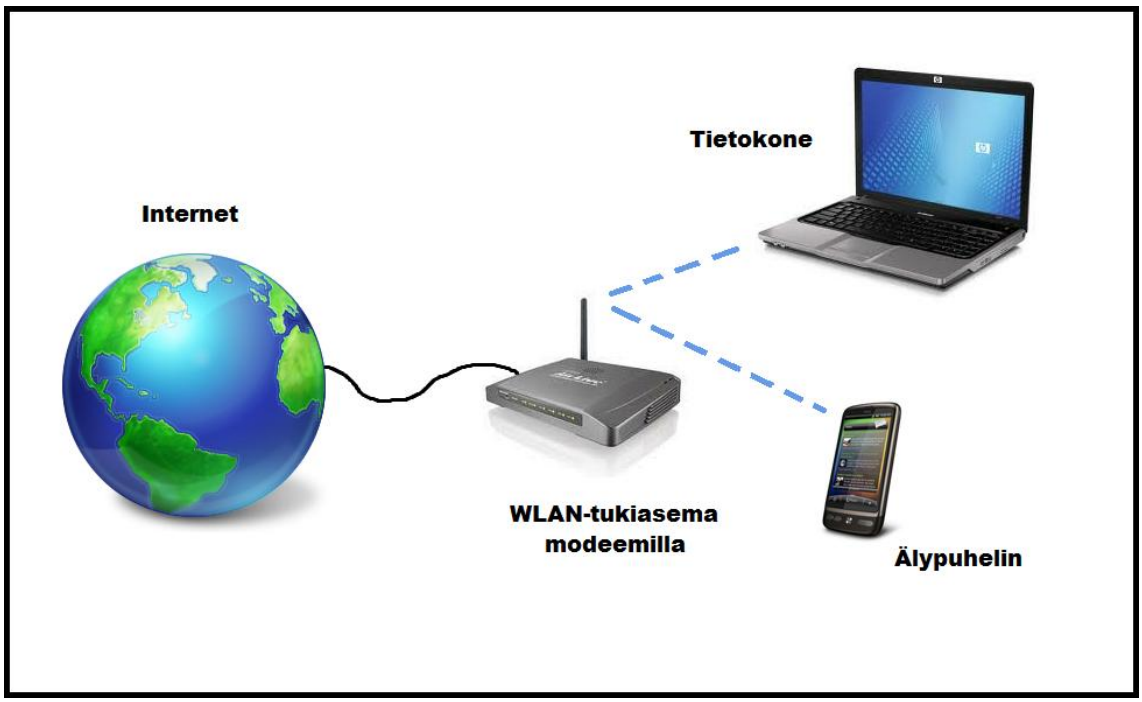
WLAN:in taajuusalue on 2412 - 2484 MHz, ja kanavien väli 5,0 MHz. Toisin kuin ehkä voitaisiin olettaa, WLAN:issa vierekkäiset kanavat häiritsevät toisiaan, sillä kanavien tehot jakautuvat kyseisellä alueella 22 MHz:n alueelle. Tästä johtuu, että mikäli samassa tilassa on useita WLAN-yhteyksiä päällä, laitteiden pitää käyttää toisistaan riittävän etäällä olevia kanavia. Kuvassa 6 on havainnollistettu eri kanavien sekoittumista keskenään.



Kuva 6. Käyrät kuvaavat eri kanavien lähetystehojen sekoittumista keskenään. Toisiaan häiritsemättömät kanavat on vahvistettu mustalla viivalla. [6]

4.1 Verkon rakenne

WLAN:in verkkotopologia koostuu tukiasemista (access points), jotka muodostavat WLAN-verkkoja ja päätelaitteista (clients) kuten tietokoneista ja älypuhelimista. Koti-käyttöisissä tukiasemissa yhdistyy usein reititin ja kytkin, sekä monissa tapauksissa myös modeemi. Yksinkertainen WLAN-verkko voi olla rakenteeltaan esimerkiksi kuvan 7 mukainen.



Kuva 7. WLAN-verkkomalli, jossa tukiasema on langallisesti yhteydessä internetiin ja tarjoaa päätelaitteille langattoman internetyhteyden

WLAN-tukiasemiin voi yhdistyä tyypillisesti enintään 255 päätelaitetta. Näin suurilla käyttäjämäärillä verkko tosin voi ruuhkautua helposti. Käyttäjämäärää voidaan myös rajoittaa sovelluksesta riippuen. Esimerkiksi 3G-Android-älypuhelimet sallivat WLAN-tukiasemana toimiessaan yhteyden enintään kahdeksalle päätelaitteelle.

Päätelaite voi olla kerrallaan yhdistettynä vain yhteen WLAN-tukiasemaan, joskin se voi olla samanaikaisesti tietoinen lukuisista eri verkoista. Tietokoneiden ja älypuhelinten lisäksi myös IP-puhelimista, kämmentietokoneista ja tableteista löytyy usein WLAN-yhteys. WLAN:illa on vahva asema internetliikenteen siirrossa, mutta sillä voidaan käyttää internetliikenteen lisäksi muissakin sovelluksissa, kuten esimerkiksi äänen siirtämisessä tietokoneelta kotistereoihin.

4.2 Historia

802.11-standardin juuret ulottuvat vuoteen 1985, kun U.S. Federal Communications Commission (FCC) päätti avata useita radioaaltokanavia hallituksen ulkopuoliseen käyttöön. Nämä niin kutsutut roskakanavat (garbage bands) oli jo kohdennettu muun muassa mikroaaltouuneille.

Toimiakseen näillä kanavilla laitteiden täytyi käyttää hajaspektritekniikkaa. Tämä tekniikka hajauttaa radiosignaalin useille taajuuksille minimoidakseen interferenssin mahdollisuuden sekä vaikeuttaakseen yhteyden kaappaamista. Vuonna 1990 perustettiin uusi IEEE-valiokunta, jota kutsuttiin nimellä 802.11. Sen tehtävänä oli selvittää uuden langattoman standardin luomismahdollisuudet.

Vuonna 1997 julkaistiin ensimmäinen 802.11-standardi. Sitä selvennettiin vuonna 1999, ja 2,4 GHz:n taajuudella toimiva 802.11a sai alkunsa. Sitä seurasi 802.11b, joka puolestaan toimii 5,3 GHz:n taajuudella. Näiden jälkeen uusia WLAN-versioita on tullut muutamia. WLAN-tekniikan suosio kasvoi laajakaistayhteyksien yleistyessä kotitalouksissa. [4]

WLAN-tekniikkaa kehitetään edelleen, ja nykyään 802.11n on kannettavissa tietokoneissa uusin käytössä oleva standardi. Taulukossa 7 on kuvattu standardit ja niiden keskeisimmät ominaisuudet.

Taulukko 7. WLAN-standardit ominaisuuksineen [7]

802.11-protokolla	Julkaistu	Freq. (GHz)	Kaistanleveys (MHz)	Tiedon-siirtonopeus (Mbit/s)	Modu-laatio	Kantama (m)
802.11-1997	6/1997	2,4	20	1 - 2	DSSS, FHSS	100
a	9/1999	5	20	6 - 54	OFDM	120
b	9/1999	2,4	20	5,5 – 11	DSSS	140
g	6/2003	2,4	20	6 – 54	OFDM, DSSS	140

a (laajennos)	9/2008	3,7	20	6 – 54	OFDM	5000
n	10/2009	2,4	20	7,2 – 72,2	OFDM	250
n	10/2009	5	40	15 – 150	OFDM	250
ac (DRAFT)	Nov. 2011	2,4	80	433 – 867	OFDM	

4.3 IEEE (Institute of Electrical and Electronics Engineers)

IEEE (Institute of Electrical and Electronics Engineers) on kansainvälinen järjestö, joka hallinnoi monien muiden tekniikoiden ohella myös WLAN-tekniikkaa. Siihen kuuluu yli 370 000 jäsentä yli 160 maassa. IEEE harjoittaa laajaa julkaisutoimintaa, alan tilaisuuksien järjestämistä, teknisen koulutuksen edistämistä ja standardien määrittelyä.

4.4 Virransäästö

WLAN:issa on käytössä virtaa säästävä WMM Power Save -tekniikka. WMM:n tarkoituksena on virransäästön lisäksi parantaa tiedonsiirron tehokkuutta ja joustavuutta.

Esimerkiksi asiakkaan työasema voi mennä aina lepotilaan pakettien välillä, kun tukiasema puskuroi ladattavia paketteja. Asiakkaan laite herää uudelleen pikaisesti määrätyllä hetkellä. Tällöin tiedonsiirron energiatehokkuus paranee ilman, että QoS:n tarvitsee heikentyä.

4.5 Tietoturvallisuus

WLAN voi toimia joko salauksella tai ilman. Jos tiedonsiirto salataan WEP-kryptauksella, se on murrettavissa nykytekniikalla muutamassa minuutissa. Jos tieto salataan WPA- tai WPA2-kryptauksella, sen murtaminen vaikeutuu ja onnistuu enää hyvillä työkaluilla. Vahva ja usein päivitettävä salasana voi antaa tähän merkittävää lisäsuojaa.

Jos WLAN-yhteyttä käytetään pääsääntöisesti vain tietyillä päätelaitteilla, voidaan salasanaksi valita pisin mahdollinen, esimerkiksi satunnaisgeneraattorilla luotu salasana. Kirjautuminen tukiaseman asetuksiin tulee myös suojata salasanalla.

WLAN-yhteyden suojaamiseen on olemassa useita neuvoja, mutta tärkein niistä on edellä kuvattu, oikealla tavalla salattu yhteys. Yleisimpiä muita tietoturvaneuvoja ovat laitekohtaisiin Mac-osoitteisiin perustuva yhteyden salliminen, käyttäjien lukumäärän rajaaminen, lähetystehon pienennys, SSID-nimen vaihto ja piilotus, ohjauspaneelin suojaaminen salasanalla sekä tietokoneen kytkeminen verkkoon langalla.

Viimeistä neuvoa lukuunottamatta kaikki konstit ovat ohitettavissa: esimerkiksi Mac-osoitteiden perusteella tapahtuva yhteyden salliminen kuulostaa hyvältä idealta, mutta se on ohitettavissa muuttamalla lähtevien pakettien Mac-osoitetta.

Käyttäjien lukumäärän rajaaminen on melko työläs ja kankea tapa estää asiaton verkkoon kirjautuminen. Toimiakseen optimaalisesti sitä täytyisi säätää jatkuvasti sen mukaan, montako luvallisesti kirjautunutta käyttäjää yhteydellä kulloinkin on.

Tukiaseman lähetystehoa voi pienentää fyysisillä esteillä, tai joissakin malleissa poistamalla laitteesta ulkoisen antennin. On kuitenkin syytä muistaa, että vaikka tietokone ei havaitsisikaan verkkoa tällaisen operaation jälkeen, herkemmät vastaanottimet voivat edelleen saada siihen yhteyden.

Tilastollisesti tämä lienee kuitenkin asiatonta käyttöä vähentävä konsti, koska se rajaa yhteyden käyttöalueen millä tahansa päätelaitteella murto-osaan alkuperäisestä. Tämä tosin voi heikentyneen signaalin takia pudottaa yhteyden nopeutta myös normaalissa käytössä.

SSID:n, eli ympäristöön lähetettävän WLAN-yhteyden nimen voi myös vaihtaa ja piilottaa, mutta tällöin täytyy ottaa huomioon, että piilotus koskee vain yleisintä tapaa nähdä SSID. WLAN-yhteys lähettää SSID:tä muillakin tavoilla 2,4 GHz:n ja 5 GHz:n verkoissa, ja nämä tavat todennäköisesti ovat murtoa yrittävän osapuolen tiedossa. [8.]

Viimeinen ja varmin konsti on käyttää internetyhteyttä kaapelilla. Tämä myös pudottaa tietokonelaitteiston virrankulutusta hieman, ja nopeuttaa yhteyttä laskemalla sen viivet-

tä (ping). Tällöin myöskään ylimääräistä säteilyä ei synny ympäristöön, ja muulle 2,4 GHz:n taajuudella toimivalle tietoliikenteelle jää enemmän tilaa. Vaikka päätelaitteen liikuteltavuus pienenee kaapelia käytettäessä merkittävästi, kaapeliyhteys on tiettävästi kaikilta teknisiltä ominaisuuksiltaan parempi kuin langaton yhteys.

5 ZigBee

ZigBee on vähävirtainen tekniikka pienten tietomäärien siirtoon. Sillä on sovelluksia muun muassa kodin automaatiossa. Sen avulla voidaan toteuttaa esimerkiksi TV:n automaattinen vaimentaminen matkapuhelimen soidessa. ZigBee noudattaa IEEE:n kehittämää 802.15.4-standardia, ja on avoin vain ei-kaupallisiin tarkoituksiin. ZigBeen logo on kuvan 8 mukainen.

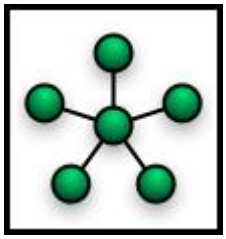
Kuva 8. ZigBeen logo

ZigBeessä on kolme erilaista laitetta: ZigBee coordinator (ZC), ZigBee Router (ZR) ja ZigBee End Device (Zed). ZC on vastuussa verkon muodostamisesta sekä verkon tietojen säilyttämisestä. Siinä on kaikki standardin vaatimat ominaisuudet. ZC-laitteita on yksi jokaista ZigBee-verkkoa kohden.

ZR-laite toimii nimensä mukaan reitittimenä. Se huolehtii laitteiden välisestä tiedonsiirrosta. Zed-laite puolestaan on ominaisuuksiltaan karsittu ja toimintaperiaatteeltaan hyvin yksinkertainen. Se vaatii myös vähemmän muistia kuin ZC tai ZR. [9.]

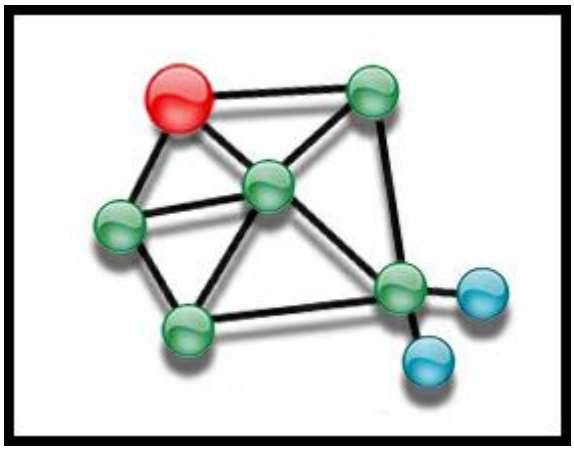
5.1 Verkon rakenne

ZigBeellä on kaksi mahdollista verkkotopologiaa: tähtimäinen ja peer-to-peer -topologia. Tähtimäisessä verkossa yksi ZC-laite toimii PAN (Personal Area Network) -koordinaattorina, joka mahdollistaa muiden laitteiden kommunikaation itsensä kautta. Topologiaa selventää kuva 9.



Kuva 9. Tähtimäinen verkkotopologia

Peer-to-peer-verkossa taas tarvitaan yksi PAN-koordinaattori kuuluttamaan verkon olemassaolosta muille laitteille. Nämä laitteet voivat kuitenkin kommunikoida myös keskenään. Verkko voi olla rakenteeltaan paljon tähtimäistä verkkoa monimuotoisempi ja sisältää kahdenkeskisiä kytkentöjä laitteiden välillä. Verkkotopologia on kuvan 10 mukainen.



Kuva 10. ZigBee P2P -verkko, joka muistuttaa rakenteeltaan multi-hop-verkkoa [10]

802.15.4-standardi määrittelee ZigBeelle myös tietoliikennetyypit. Niitä ovat jaksollinen, epäsäännöllinen ja säännöllinen tieto. Jaksollisessa tiedossa ohjelma määrittää tiedon siirtymisen, vastaanotin aktivoituu virransäästösyistä vain tiedon vastaanoton ja tarkastelun ajaksi.

Epäsäännöllisessä tiedonsiirrossa ohjelma tai jokin herätesignaali (esimerkiksi palohälyttimessä savu) määrää tiedonsiirron alkamishetken. Myös tässä laite kytkeytyy verkkoon vain tiedonsiirron ajaksi. Säännöllisessä tiedonsiirrossa tiedon siirtymiselle on määrätty tahti. Tällöin laitteet toimivat tietyillä aikaväleillä.

5.2 Historia

ZigBee-tyylisiä verkkoja alettiin suunnitella vuonna 1998. Idea sai alkunsa, kun useat insinöörit arvioivat sekä WiFin että Bluetoothin olevan sopimattomia tiettyihin käyttötarkoituksiin, kuten esimerkiksi itsestään järjestäytyviin digitaalisiin radioverkkoihin.

Termi ZigBee liittyy mehiläisiin: Niiden ZigBeeksi nimetty kommunikointitekniikkana on äänetön ja tehokas, ja ne voivat viestiä sillä tietoa keskenään ruokapaikan etäisyydestä, olinpaikasta ja suunnasta. Mehiläisten tapaan ZigBee-laitteet toimivat ikään kuin yhdyskunnassa, jossa jäsenten välinen kommunikointi on elintärkeää yhdyskunnan säilymiselle.

5.3 ZigBee Alliance

ZigBee-alliance on ZigBee-laitevalmistajien välinen liitto, johon kuuluu yli 175 yritystä, mukaan lukien Intel, HP ja Philips. Liitto vastaa ZigBee-standardin kehittämisestä. Sen jäsenmaksu on 3500 USD, jonka jälkeen ZigBeetä voi käyttää kaupallisiin tarkoituksiin.

5.4 Tekniset tiedot

ZigBee toimii maailmanlaajuisesti 2,4 GHz:n taajuusalueella, jolloin sen nopeus on 250 kb/s. ZigBeetä voidaan käyttää myös eri taajuuksilla riippuen maantieteellisestä sijainnista. Sen tiedonsiirtonopeus vaihtelee käytettävän taajuuden mukaan. ZigBeen kantama on parhaimmillaan 500 m. Taulukko 8 kertoo tarkemmin ZigBeen taajuusalueista.

Taulukko 8. Kanavat, taajuudet ja nopeudet alueittain

Taajuus, MHz	Kanavia	Nopeus (kb/s)	Käytettävä alue
868,0 – 868,8 [11]	1 kpl	20	Eurooppa
902 – 928 [11]	10 kpl, 2 Mhz välein	40	Amerikka
2400,0 – 2483,5 [11]	16 kpl, 5 Mhz välein	250	Maailmanlaajuinen

5.5 Tietoturvallisuus

ZigBeen tietoturvallisuudessa on kolme tasoa: Ensimmäisellä tasolla ei ole tietoturvaa lainkaan. Toinen taso perustuu pääsylistoihin, jossa yksinkertaisella tunnistusmenetelmällä tunnistetaan verkkoon kuuluvat laitteet. Kolmannella tasolla on AES-kryptaus, jolla tiedonsiirto salataan.

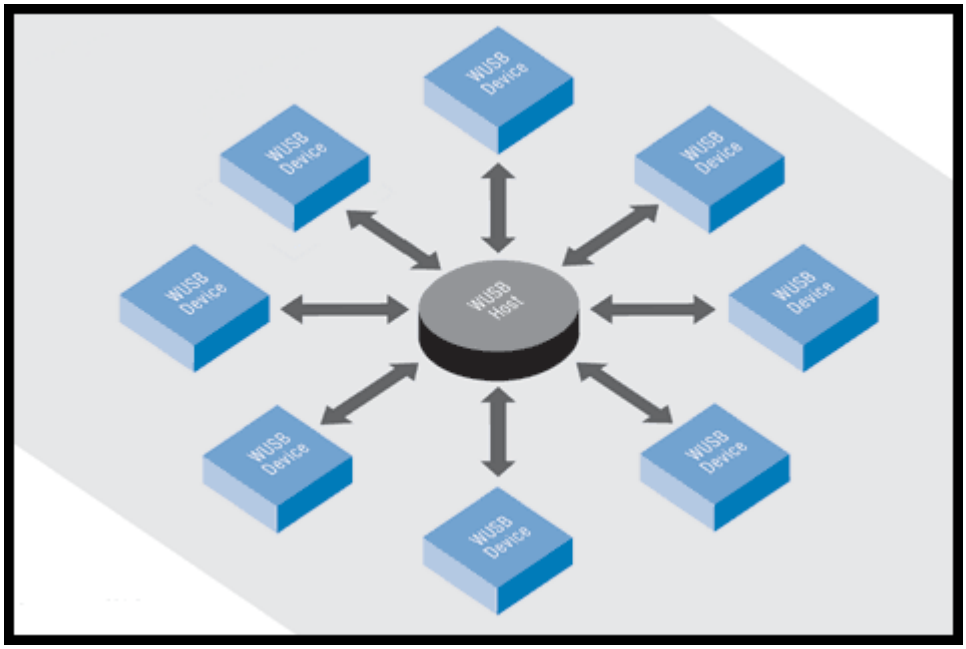
5.6 Yhteenveto

Tähän mennessä ZigBeen toimitus ja myyntivolyymi on ollut pientä. ZigBeen etuna on se, että se on standardoitu ajoissa ja se on yhteensopiva eri laitevalmistajien kanssa. Se on myös lepotila- ja tiedusteluominaisuuksiensa ansiosta vähävirtainen tekniikka. Matalammat taajuudet läpäisevät myös esteitä hyvin.

6 Wireless USB

Wireless USB, eli WUSB on langaton tiedonsiirtotekniikka tietokoneen ja sen oheislaitteiden liittämiseksi toisiinsa. WUSB perustuu nimensä mukaisesti USB:n arkkitehtuuriin. WUSB:n logo on kuvassa 11. Sen verkkotopologia perustuu kuvan 12 mukaiseen malliin, jossa on yksi keskitin, johon muut laitteet ovat liitettyinä.

Kuva 11. Wireless USB-tekniikan logo



Kuva 12. WUSB:n verkkotopologia [12]

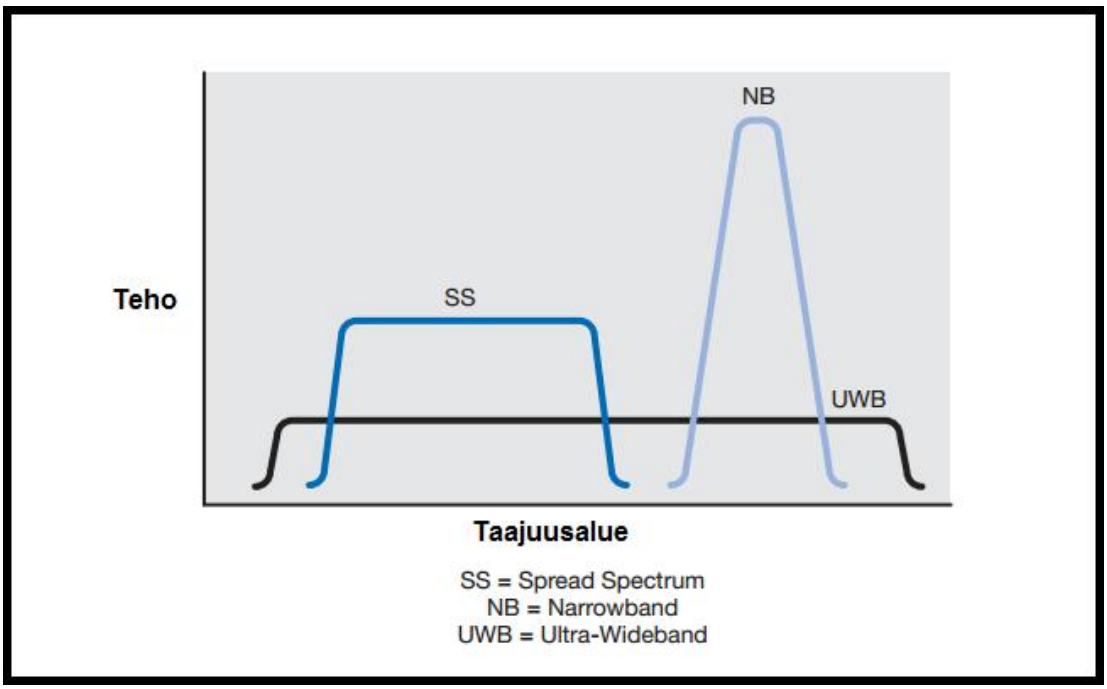
Yhteen WUSB-keskittimeen voi kytkeytyä maksimissaan 127 laitetta. WUSB-verkossa laite voi toimia myös isännän tavoin. Tätä kutsutaan nimellä kaksoisroolimalli (dual-role model). WUSB:n tehonkulutus on 300 mW:n luokkaa. Tekniikkaa voidaan käyttää USB:n tavoin lähes kaikissa laitteissa, kuten tulostimissa, digikameroissa, älypuhelimissa, ulkoisissa muisteissa, modeemeissa ja viivakoodinlukijoissa.

Yhdistyminen WUSB-verkkoon tapahtuu siten, että laite lähettää isännälle viestin määrätyllä hetkellä. Tämän jälkeen isäntä ja laite autentikoivat, eli todentavat toisensa käyttäen omia ID-tunnuksiaan ja salausavaimiaan. Kun autentikointi on suoritettu, isäntä antaa laitteelle oman USB-osoitteen ja ilmoittaa omalle ohjelmistolleen, että laite on kytketty järjestelmään.

6.1 UWB WUSB:n perustana

WUSB käyttää tiedonsiirtoon UWB-tekniikkaa (Ultra Wide Band), jossa tietoa lähetetään hyvin leveällä, esimerkiksi 1-2 GHz:n taajuuskaistalla. UWB-tekniikka toimii muutamien metrien etäisyydellä mahdollistaen muihin tekniikoihin nähden suuret tiedonsiirtonopeudet, ja sitä voidaan hyödyntää monissa sovelluksissa. UWB:n kehittely jatkuu par-

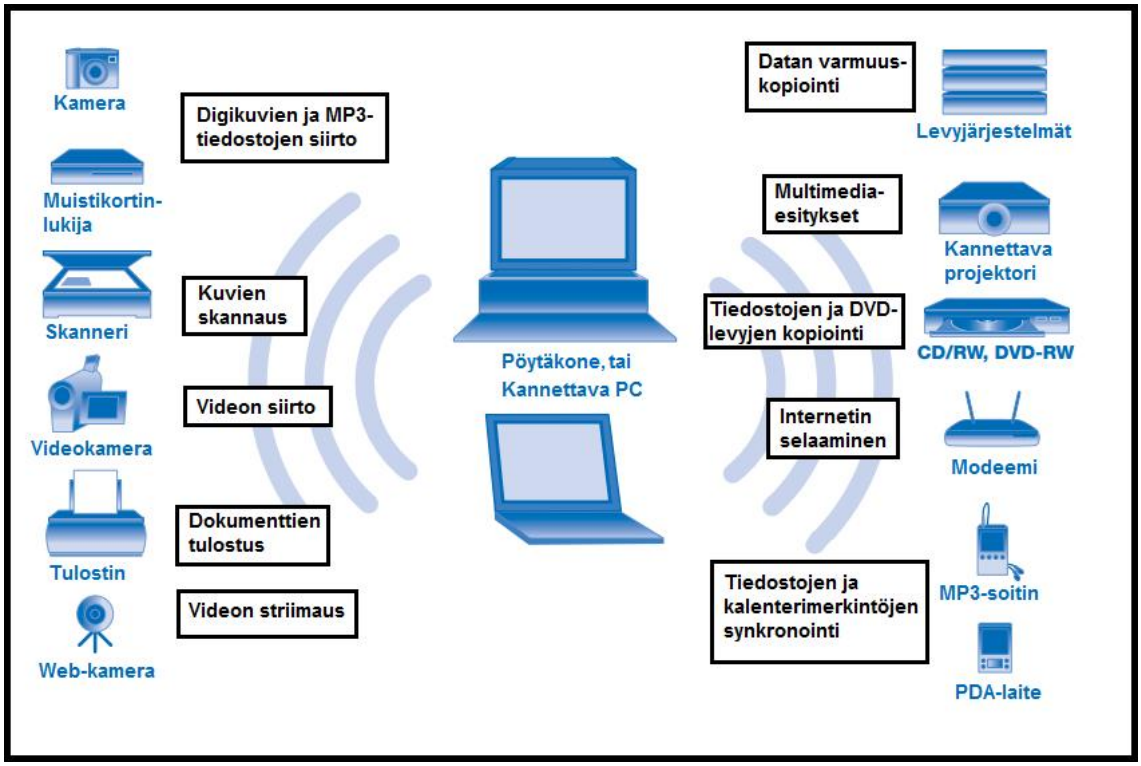
haillaan. Kuvassa 13 on vertailtu UWB:tä hajaspektriin (SS) ja kapeakaistaiseen tiedonsiirtoon (NB).



Kuva 13. UWB:n, SS:n ja NB:n vertailua tehon ja taajuusalueen suhteen

UWB:ssä pulssit ovat hyvin lyhyitä ja pienitehoisia. Ne lähetetään pseudosatunnaisin, eli määrätyin, satunnaisuutta muistuttavin väliajoin. Tällöin ne eivät resonoi voimakkaasti ympäristön rakenteiden kanssa. Haasteena UWB-tekniikassa on laitteiden synkronointi, kun vastaanottajan tulee löytää nanosekuntien tarkkuudella lähettäjän lähettämät pulssit.

UWB:lla voidaan luoda kotitalouksiin WPAN-verkkoja (Wireless Personal Area Network), joihin on mahdollista liittää tulevaisuudessa paljon erilaisia laitteita, kuten kännyköitä, tietokoneita, mp3-soittimia ja muuta elektroniikkaa. Tämä avaa uudenlaisia mahdollisuuksia, kuten esimerkiksi digikameran kuvien katselun suoraan tietokoneen näytöltä ilman johtoja. Kuvassa 14 on havainnollistettu näitä mahdollisuuksia.



Kuva 14. Esimerkkejä UWB:n käyttösovelluksista

6.2 Historia

WUSB:ta määrittelemään perustettiin ryhmä Wireless USB Promoter Group vuonna 2004. Ryhmän jäseninä ovat mm. HP, Intel, Microsoft, Samsung ja Texas Instruments. WUSB:n määrittely valmistui toukokuussa 2005.

Laitteita odotettiin markkinoille vuoden 2005 lopussa, mutta niiden suosio ei lähtenyt leviämään odotusten mukaisesti. Vuoden 2005 lopussa WUSB saatiin alustavissa testeissä toimimaan 880 Mbps nopeudella 8 metrin kantamalla. Kantaman ollessa 20 metriä yhteys toimi testeissä vielä 220 Mbps nopeudella.

6.3 Tekniset tiedot

Tämänhetkisen WUSB-version tiedonsiirtonopeus on 480 Mbps. Laitteiden välinen etäisyys toisistaan voi olla enintään 10 metriä, jolloin tiedonsiirtonopeus putoaa 110 Mbps nopeuteen. Taulukossa 9 vertaillaan WUSB-tekniikan ominaisuuksia Bluetoothiin ja WLAN:iin.

Taulukko 9. WUSB:n, Bluetoothin sekä WLAN:in vertailua [13]

Ominaisuus	WUSB 1.1	Bluetooth 4.0	WLAN (802.11n)	WLAN (802.11ac)
Taajuusalue	3,1 GHz–10,6 GHz	2,4 GHz	2,4 GHz / 5 GHz	5 GHz
Tiedonsiirto-nopeus	53 – 480 Mbit/s	3 – 24 Mbit/s	Maks. 450 Mbit/s	Maks. 6,93 Gbit/s
Kantama	3 – 10 m	1 – 100 m	100 m	N/A
Modulaatio	MB-OFDM	MB-OFDM	DSSS, DBPSK, DQPSK, CCK, OFDM	OFDM

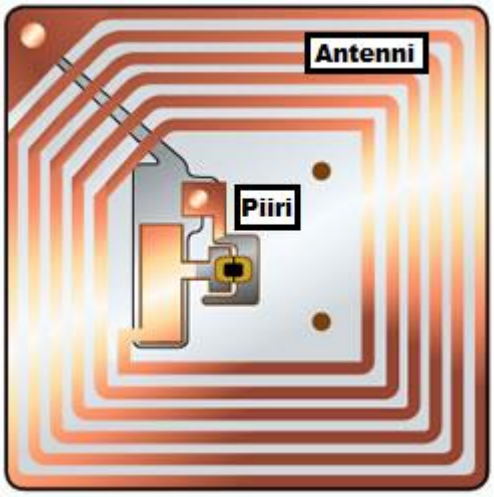
6.4 Tulevaisuudennäkymiä

Wireless USB Promoter Group on asettanut tavoitteeksi tulevaisuudessa yli 1 Gbps siirtonopeuden. Lisäksi tehonkulutus on tarkoitus pudottaa kolmannekseen nykyisestä, eli 100 mW:iin. WUSB:n on myös ennustettu tulevan kännyköihin lähitulevaisuudessa.

7 RFID

RFID on radiotaajuuksiin perustuva etätunnistusmenetelmä, jonka kantama on sovelluksesta riippuen 10 cm - 200 m. RFID-tekniikka toteutetaan siten, että RFID-lukija lähettää signaalin tunnisteeseen, eli tagiin, joka signaalin saatuaan vastaa lukijalle omalla koodillaan ja kertoo täten läsnäolostaan.

Tagit ovat pienikokoisia, piirillä ja antennilla varustettuja laitteita, jotka ovat halpoja valmistaa. RFID:tä sovelletaan muun muassa logistiikkakeskuksissa tuotteiden lajitteluun sekä vähittäiskaupoissa tuotehävikin hallintaan. Kuvassa 15 on passiivinen RFID-tagi.



Kuva 15. Piirros passiivisesta RFID-tagista, jossa piiri on antennin ympäröimänä

RFID:n yksi tavoite on korvata tavalliset viivakoodit. Sillä on muutamia etuja verrattuna viivakoodeihin. Se pystyy muun muassa lukemaan tageja esteiden läpi. Toisekseen se voi lukea niitä kerrallaan jopa satoja, sillä tuotteet voivat olla lukuhetkellä vapaasti eri asennoissa. Myös sen kantama on suhteellisen pitkä verrattuna perinteisen viivakoodin lukuetäisyyteen.

7.1 Käyttösovellukset

RFID:tä voidaan logistiikka- ja myymäläsovellusten lisäksi käyttää myös eläinten tunnistamisessa, ja tehtailla tuotteiden valmistuksen valvonnassa. Tällöin kunkin tuotteen valmistusprosessin kaikki vaiheet saadaan dokumentoitua yksitellen.

Tuotteiden lähtiessä valmistajilta kohti vähittäiskauppoja jokainen tuote voidaan yksilöidä. Näin tuotteiden seurantaa varten avautuu paljon uusia mahdollisuuksia, ja häviköä voidaan täten kontrolloida entistä tehokkaammin.

7.2 RFID-laitteet

Piiristä ja antennista koostuvat tagit ovat yksinkertaisimpia RFID-laitteita. Lukijat koostuvat näiden lisäksi myös muista komponenteista. Tagit voivat olla passiivisia, puolipassiivisia tai aktiivisia.

Passiivitagit toimivat kokonaisuudessaan lukijalta saamansa radioimpulssin virralla, ja puolipassiiviset tagit saavat lukijan virrasta herätteen, mutta käyttävät lähettämiseen omaa virtalähdettään. Aktiivitagit puolestaan käyttävät virtaa toistuvaan lähettämiseen riippumatta lukijan läsnäolosta.

Passiivitagit ovat täten yleisimpiä, pienimpiä ja halvimpia RFID-laitteita. RFID-laitteet voivat käyttää tiedonsiirrossa monia erilaisia modulaatiotekniikoita. Niitä ovat muun muassa ASK, OOK, FSK ja PSK [14].

7.3 Historia

Leo Theremin keksi vuonna 1945 Neuvostoliiton hallitukselle vakoilulaitteen. Tätä pidetään monissa yhteyksissä RFID-tekniikan alkuna. Toisaalta RFID:tä vastaavaa tekniikkaa on ollut käytössä jo 1920-luvulta lähtien.

Esimerkiksi toisessa maailmansodassa Britanniassa käytettiin RFID-laitteita erottamaan saapuvat britannialaiset koneet saksalaisista. Tästä oli briteille huomattavasti etua, sillä vastaavasti perinteisellä tutkalla voitiin havaita vain koneen saapuminen, ei sen tyyppiä.

7.4 RFID-standardointi

RFID-teknologiaan on liitoksissa olennaisesti EPC-koodi (Electronic Product Code), joka on maailmanlaajuinen standardi, joka varmistaa että jokainen RFID-tagi on yksilöllinen. RFID-standardointi sisältää EPC-tagien eri valmistajien välisen yhteensopivuuden.

ISO on kehittänyt RFID-standardointia määrittelemällä ISO 18000 –ilmarajapintastandardisarjan. Se on myö määritellyt kaikille käytettäville RFID-taajuuksille oman ilmarajapintaprotokollan.

7.5 Tietoturvallisuus

RFID-järjestelmässä on neljä suojattavaa kohtaa: tagilla säilytettävä tieto, lukijan muistissa oleva tieto, itse tiedonsiirto sekä tietoa käsittelevä järjestelmä, kuten esimerkiksi palvelin.

Tagilla olevaan tietoon pääsee käsiksi vain lukijalla, joskin lukijoita on myös mahdollista väärentää. Tagilla olevan tiedon muuttamisen ja poistamisen voi estää esimerkiksi käyttämällä vain lukutyyppisiä tageja. Myös tagien tiedon salaamiseen on kehitetty ratkaisuja, mutta ne lisäävät tageihin toiminnallisuutta ja täten kasvattavat niiden hintaa.

Tagilta lukijalle radioaaltojen avulla siirrettävä tieto on myös vaarassa hyväksikäytölle, sillä tietoa voidaan siepata ilmasta väärennetyllä lukijalla. Lukijoille voidaan syöttää väärää tai vahingollista tietoa. Tai tiedonsiirtoa voidaan häiritä esimerkiksi palvelunestohyökkäyksillä sähkömagnetiikkaa käyttäen.

Lukijoita voidaan häiritä myös esimerkiksi foliolla, ilmankosteudella, nesteillä, lämpösäteilyllä sekä tietyn taajuuden omaavilla puhelimilla, tietokoneilla ja jopa moottoreilla. Koska lukija käsittelee tietoa ennen sen lähettämistä eteenpäin, esimerkiksi tietoverkkoon, sen katsotaan olevan tietokone, jonka sisältö pitää myös suojata.

7.6 Ihonalaiset sirut

Monien sovellusten ohella RFID-siruista on alettu markkinoida myös ihmisiin asennettavia versioita. Niitä markkinoidaan käytännön asioita helpottavana ratkaisuna, jolloin esimerkiksi sirutetun dementiapotilaan ei tarvitse muistaa omia potilastietojaan, tai mitään muutakaan, mitä sirun tietokantaan on tallennettu.

Teoriassa siruun voitaisiin helposti tallettaa käyttäjän pankkitilin saldo ja mahdolliset velat päivitettävinä muuttujina sekä henkilötiedot koulutus- ja ammattihistorioineen. Mahdollisuudet tiedon tallettamiseen ovat lähes rajattomat, ja näin monet hukattavissa olevat tavarat, kuten pankkikortti ja kännykän SIM-kortti, voitaisiin korvata yhdellä ihonalaisella sirulla. Näin kukaan ei voisi enää varastaa toisen rahoja tai henkilötietoja varastamatta häneen implantoitua sirua.

Kätevyydestään huolimatta ihonalaiset sirut ovat herättäneet suurta vastarintaa eri syistä etenkin sosiaalisessa mediassa. Pääsyy sirujen vastustamiselle on luottamuksen puute niitä markkinoiviin organisaatioihin. Tietojen myös epäillään joutuvan helposti vääriin käsiin.

8 NFC

NFC, eli Near Field Communication on RFID:stä alkunsa saanut tunnisteteknologia, joka mahdollistaa tiedonsiirron lyhyillä, alle kymmenen senttimetrin etäisyydellä. NFC:llä voidaan suorittaa esimerkiksi mobiilimaksuja, tai fyysisestä läsnäolosta kertovia tunnistautumisia. Kuvassa 16 on havainnollistettu NFC:n käyttösovelluksia.

Kuva 16. NFC:n sovelluksia

NFC:ssä käytetään kahden laitteen välistä point-to-point-verkkotopologiaa. Tällaisen rakenteen omaavassa verkossa toinen osapuolista on aloitteentekijä (initiator) ja toinen kohde (target). Aloitteentekijä nimensä mukaisesti aloittaa tiedonsiirron ja hallinnoi sitä koko tiedonsiirron ajan. Kohde taas toimii passiivisena osapuolena vastaten aloitteen-

tekijältä saamiinsa komentoihin. Toisin kuin esimerkiksi RFID-tekniikassa, NFC:ssä sama laite voi toimia sekä lukijalaitteena että tunnisteena.

8.1 Historia

NFC:n kantaisästä RFID:stä tuli ensimmäinen patentti vuonna 1983, joskin itse tekniikalla on juuret 1900-luvun alkupuoliskolla. Vuonna 2004 Nokia, Philips ja Sony perustivat NFC-foorumin, ja vuonna 2006 saatiin alustavat määritelmät NFC-tageille, eli tunnisteille.

Ensimmäinen NFC-ominaisuudella varustettu kännykkä oli Nokian vuonna 2006 julkaisema malli 6131. 2009 NFC-foorumi julkaisi Peer-to-Peer-standardit yhteystietojen, verkko-osoitteen ja bluetooth-yhteyden avauskäskyn lähettämiselle.

Vuonna 2011 NFC-kännyköiden yleistyessä hiljalleen Google alkoi opettaa käyttäjilleen NFC-tekniikan mahdollisuuksia. Samana vuonna RIM otti ensimmäisenä yrityksenä maailmassa käyttöön MasterCard Worldwide -sertifioidun tekniikan, joka tähtää perinteisten korttimaksutapahtumien nopeuttamiseen.

Vuoden 2012 maaliskuussa brittiravintola Eat sekä Orange-matkapuhelinoperaattori (Everything Everywhere) ottivat käyttöön ensimmäisenä maailmassa Samat Poster -tekniikan. Tämän avulla matkapuhelin voi kommunikoida ns. älypaperin kanssa ja saada siitä tietoja vaivattomasti näytölleen jatkotoimenpiteitä varten.

8.2 NFC Forum

NFC Forum on voittoa tavoittelematon laitevalmistajien välinen liitto, jonka tavoitteena on edistää NFC:n standardointia, kehittymistä ja käyttöönottoa. Liitolla on yli 130 jäsentä.

Joukossa on myös paljon tunnettuja jäseniä, kuten esimerkiksi MasterCard, Visa, Microsoft, Motorola ja Samsung. Mukana on myös suomalaisia organisaatioita, kuten VTT ja Nokia. NFC-Foorumin Jäsenet muodostavat kahdeksan työryhmää, joiden toimialoja ovat muun muassa markkinointi, tekniikan kehitys ja yhteensovittaminen sekä testaus.

8.3 Tekniset tiedot

NFC käyttää 13,56 MHz:n taajuutta, ja sen tiedonsiirtonopeus voi olla 106 - 424 kbit/s, mikä soveltuu pienten tietomäärien siirtoon. Suurempia määriä varten NFC-laitteisto voi muodostaa Bluetooth-yhteyden varsinaisen tiedon siirtämiseen.

Toisin kuin esimerkiksi Bluetooth, NFC ei tarvitse paritusta; sen ansiosta yhteys voidaan muodostaa 0,1 sekunnissa. Taulukossa 10 on vertailtu NFC:n ominaisuuksia kahteen Bluetooth-versioon.

Taulukko 10. NFC- ja Bluetooth-tekniikoiden vertailua [15]

	NFC	Bluetooth 3.0	Bluetooth Low Energy
Sandardoija	ISO/IEC	Bluetooth SIG	Bluetooth SIG
Standardi	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1
Verkkotopologia	Point-to-point	WPAN	WPAN
Kantama	< 0,2 m	5 – 100 m	~50 m
Taajuuus	13,56 MHz	2,4 – 2,5 GHz	2,4 – 2,5 GHz
Bittinopeus	424 kbit/s	2.1 Mbit/s	~1,0 Mbit/s
Verkon pystytysaika	< 0,1 s	< 6 s	< 0,006 s
Virrankulutus	< 15mA	1 - 100 mW	< 20 mA

8.4 Yhteenveto

NFC:n vahvuuksia ovat sen vähäinen virrankulutus sekä nopea yhteydenmuodostus. Nykyään (5/2012) NFC on vielä yleistymässä oleva tekniikka, mutta sitä on suunniteltu käytettäväksi erityisesti matkapuhelimissa eri sovelluksia varten. NFC:n saa puhelimeen myös jälkiasennettuna erityisen SIM- tai microSD-kortin mukana. Sen ei uskota leviävän kovin laajaan käyttöön ennen vuotta 2015.

Juniper Research-niminen yritys ennusti vuonna 2011, että vuonna 2014 maailman markkinoilla olisi noin 300 miljoonaa NFC-yhteensopivaa kännykkää, mikä tarkoittaisi maailman kännykkäkannasta noin 20 prosenttia.

9 Dect

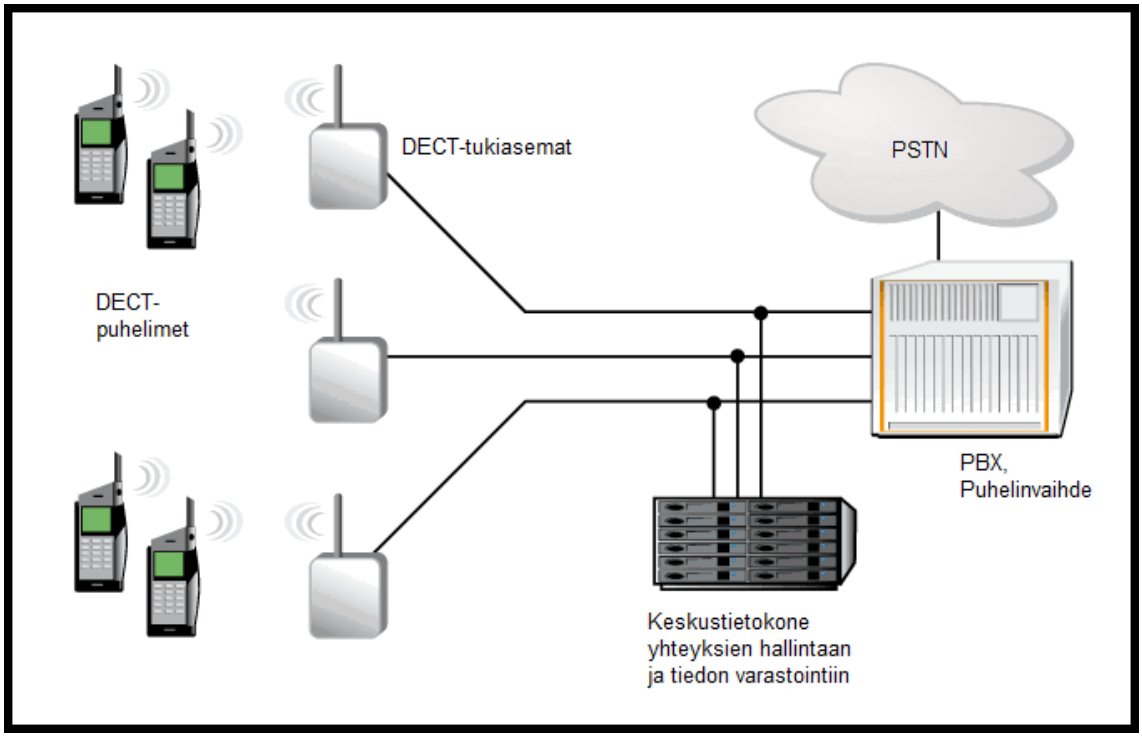
Dect on etsi Etsi:n (European Telecommunications Standards Institute) kehittämä teollisuusstandardi digitaalisille, yleensä koti- tai yrityskäyttöön suunnatuille langattomille puhelimille. Dect toimii lisensöimättömällä, suojatulla 1900 MHz taajuusalueella. Äänen lisäksi sen avulla voi lähettää ja vastaanottaa viestejä. Dectiä hallinnoi Dect Forum, joka on Dect-laitteita valmistavien yritysten välinen liitto. Sen logo on kuvassa 17.

Kuva 17. Dect Forumin logo

Vuonna 2007 Dect:iä täydentämään suunniteltiin CAT-IQ (Cordless Advanced Technology - Internet & Quality) -standardi IP- ja VOIP -tuilla. Sen logo on kuvan 18 mukainen.

Kuva 18. Cat-IQ-standardin logo

Dect-verkossa monet puhelimet voivat yhdistyä samaan tukiasemaan. Puhelimilla on yleensä lataustelakat, jotka kuitenkaan eivät ole yhdistettyinä puhelinverkkoon. Puhelimet pystyvät joissakin sovelluksissa kommunikoimaan myös suoraan toisilleen ilman tukiaseman läsnäoloa. Kuvassa 19 on esimerkki Dect-verkon toteutuksesta.



Kuva 19. Esimerkki Dect-verkosta

9.1 Historia

1980-luvun alussa analogisten langattomien puhelinten tullessa Euroopan markkinoille Kauko-Idästä digitaalinen tiedonsiirto alkoi tulla tunnetuksi. Digitaalisen langattoman tiedonsiirron eduiksi katsottiin sen häiriönsietokyky sekä useamman laitteen sopiminen samaan tilaan. Myös digitaalisen tiedonsiirron mahdollisuudet tietoturvan luomiseen sekä tukiaseman vaihtoon yhteyden katkeamatta kiinnostivat monia yrityksiä.

Vuoden 1987 lopussa kaksi aikaisempaa tekniikkaa, UK CT2 ja CT3, olivat kehittyneet pitkälle näiden asioiden kannalta. ETSI yhdisteli näiden tekniikoiden parhaat ominaisuudet uudeksi standardiksi, ja kehitteli sitä edelleen. Näin vuoden 1988 alussa syntyi Dect. [16]

9.2 Tekniset tiedot

Dect-tekniikalle luvataan 100 metrin kantama esteettömässä ympäristössä. 1,9 gigahertsin taajuuden kohtalaisen esteenläpäisykyvyn takia kantama kuitenkin putoaa mentäessä sisätiloihin. Dect-tekniikan etuna on sen selviäminen ruuhkaisessa radioympäris-

tössä. Taajuutensa ansiosta se on immuuni muiden muassa WiFille ja Bluetoothille, ja se myös selviää rinnakkain toisten Dect-järjestelmien kanssa.

Puhelinten toiminta-ajat vastaavat jokseenkin kännyköiden toiminta-aikoja: valmiusajat ovat tyypillisesti joitain päiviä ja puheajat joitain tunteja. Jotkut järjestelmät tarjoavat tavallista pidemmän kantaman puhelimen ja tukiaseman välillä, ja jotkut tarjoavat pidennetyn puheajan, joka voi olla yhdellä latauksella esimerkiksi 24 tuntia.

Dectin lähetystehoille ja käytettäville aikaväleille on eri määräykset Euroopassa ja Amerikassa. Taulukkoon 11 on koottu niiden lisäksi Dectin tärkeimpiä tietoja.

Taulukko 11. Dectin ominaisuuksia [17]

Ominaisuus	Tieto	Lisätiedot
Bittinopeus (kpbs)	32	
Taajuusalue (MHz)	1880 – 1930	Vaihtelee maanosittain
Kanavien etäisyys toisistaan (MHz)	1,728	Kanavien lukumäärä 5 – 10, vaihtelee maanosittain
Aikavälit tiedonsiirrossa (kpl)	lähetys: 12 vastaanotto: 12	
Kanavien jakoperuste	Dynaaminen	
Keskimääräinen lähetysteho	Eurooppa: 10 mW per aikaväli, enintään 250 mW	Amerikka: 4 mW per aikaväli, enintään 100 mW

9.3 Dect ULE

Dect-standardista on kehitetty myös vähävirtainen versio, Dect ULE (Dect Ultra Low Energy). Dectin tavoin Dect ULE käyttää 1,9 GHz taajuusaluetta.

Standardi on luotu puhumisen sijasta kodin automaatio- ja monitorointisovellusten kehittämiseen, sillä Dect-modeemit ovat yhteydessä internetiin ja tarkkailevat Dect-signaaleja jatkuvasti. Dect ULE:a voidaan käyttää esimerkiksi turvallisuus-, terveyden-

huolto- sekä sähkönkulutuksen mittaussovelluksissa. Nämä tiedot voidaan nähdä mistä päin maailmaa hyvänsä internetin välityksellä.

9.4 Tietoturvallisuus

Dectin kulunvalvontakerros tarjoaa suhteellisen yksinkertaisen, 35-bittisen Dect Standard Cipher -salauksen. Ääniyhteys puolestaan kryptataan 64-bittisellä salauksella.

Kryptausalgoritmi on murrettu, ja myös tukiasemia on onnistuttu teeskentelemään. Tämä mahdollistaa puheluiden kuuntelemisen, äänittämisen sekä siirtämisen ympäri internetiä tai muita tietoverkkoja.

9.5 Tulevaisuudennäkymät

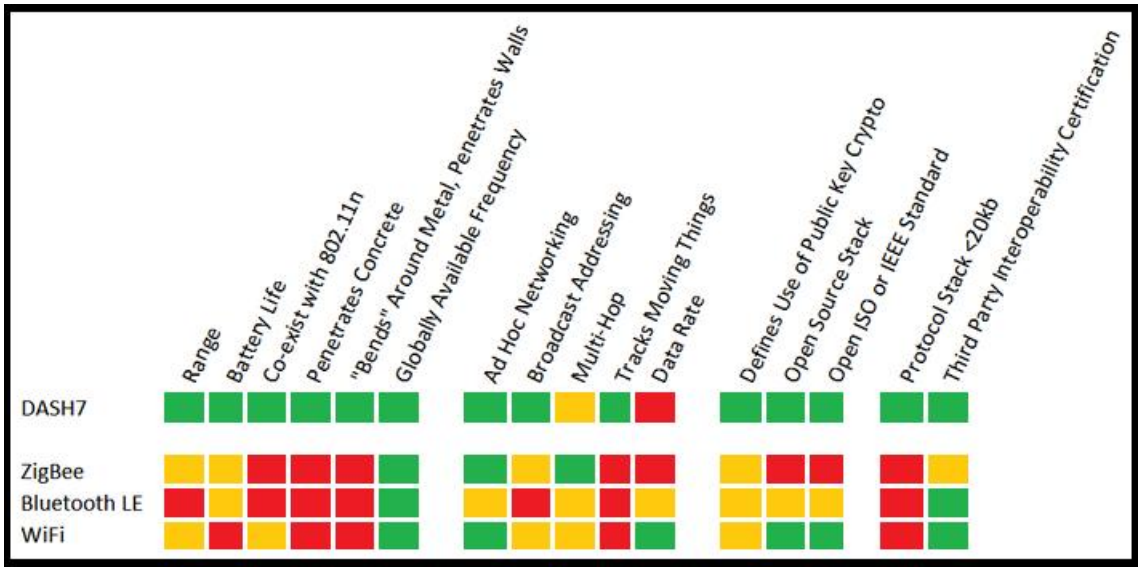
Dect:iä tullaan kehittämään tulevaisuudessa. Sillä on vahva asema langattomien äänipuheluiden tekniikkana. Esimerkiksi 802.11b- tai g-standardit eivät sisällä mekanismia, mikä kertoisi verkolle, että äänipakettien pitää päästä muun datan edelle.

10 Dash7

Dash7 on avoin standardi langattomalle sensoriverkolle. Dash7-verkolla voidaan viestittää tietoverkkoihin tietoa ympäristön ominaisuuksista, kuten lämpötilasta, ilmanpaineesta ja saastepitoisuuksista sekä olotilan muutoksista, kuten liikkeestä, äänestä ja maanpinnan värähtelyistä. Dash7:n logo on kuvassa 20.

Kuva 20. Dash7:n logo

Kuvassa 21 on vertailtu Dash7:n ominaisuuksia muiden tekniikoiden ominaisuuksiin. Vihreällä värillä merkityt kentät kuvaavat korkeaa, keltaiset keskinkertaista ja punaiset alhaista suorituskykyä.



Kuva 21. Dash7:n vertailua muiden tekniikoiden kanssa [18]

10.1 Historia

Savi Technology alkoi kehittää Dash7-tekniikkaa 1990-luvun alussa. Dash7 oli alun perin tarkoitettu kotitalouksiin aikuisille lasten seurantaa varten, mutta hanke ei saanut kunnolla kannatusta. Savi Technologyn neuvonantajat olivat sitä mieltä, että hankkeelle pitäisi löytää kunnon bisnesidea.

Myöhemmin Savi muutti suuntaa ja päätti keskittyä sotateollisuuteen. Siitä lähtien Savi alkoi kehittää USA:n puolustusministeriölle (USDOD:lle) järjestelmiä, joilla armeijat pystyvät jäljittämään esimerkiksi hyökkäyksiin tarvittavia materiaaleja ja kuljetuksia.

Sotateollisuuteen osallistuminen on ollut Saville rahallinen siunaus, mutta toisaalta USA:n puolustusministeriö painosti yhtiötä luovuttamaan patenttinsa myös muutamille muille yhtiöille, koska se ei halunnut olla riippuvainen yhden yhtiön tuotteista.

Savi myös liittyi muutaman muun yhtiön kanssa Dash7 Allianceen vuonna 2009. Se on myös vapauttanut lisenssisopimuksensa ja alentanut Dash7:n käyttöönottomaksuja, mikä on tehnyt tekniikasta houkuttelevan vaihtoehdon monille yrityksille.

10.2 Tekniset tiedot

Dash7 Alliancen mukaan Dash7 on maailman vähävirtaisin ja pisimmän kantaman omaava tekniikka. Tekniikan kantamaksi on ilmoitettu 10 m - 10 km, ja tehonkulutus on tietojen mukaan alimmillaan alle milliwatin luokkaa. Ainoa selkeä miinuspuoli Dash7:ssa on sen alhainen tiedonsiirtonopeus, joka vaihtelee 28 - 200 kbps välillä, joskaan sovelluksille tämä ei välttämättä ole ongelma. [25.]

Dash7 käyttää 433,92 MHz lisenssivapaata ISM-taajuutta, joka on sopivasti 13,56 MHz:n monikerta. Täten Dash7 voi hyödyntää samoja antenneja kuin esimerkiksi NFC, FeLiCa, MiFare ja muut RFID-lähitunnistustekniikat.

Yksi ja sama taajuus kaikkialla myös helpottaa verkon suunnittelua ja toteutusta. 433,92 MHz on verrattain matala radiotaajuus, jonka yksi tärkeimmistä ominaisuuksista on sen kyky läpäistä esteitä, kuten betonia, metalleja ja vettä. Taulukossa 12 on vertailtu Dash7- ja ZigBee-tekniikoita keskenään.

Taulukko 12. Dash7- ja ZigBee -tekniikoiden vertailua [19]

Nimi	Taajuus (MHz)	Globaali	Kantama (m)	Virran-kulutus	Latens-siaika	Laitteen hinta	Bitti-nopeus
DASH7	433	Kyllä	10 000	Alhainen etäherätteen ansiosta	maks. 2 s	> $10	200 kbit/s
ZigBee	2400 915 868	2.4 GHz – kyllä 915 MHz – ei 868 MHz – ei	30 – 500	Korkeampi synkronoiden kuuntelun takia	maks. Joitain minuut-teja	> $10	250 kbit/s

Toisin kuin monet aktiiviset RFID-tekniikat, Dash7 tukee tunnisteiden välistä kommunikaatiota, mikä yhdistettynä alhaiseen virrankulutukseen ja pitkään kantamaan tarjoaa hyvät edellytykset sensoriverkon rakentamiselle. Tagit voidaan paikantaa noin 4 metrin tarkkuudella, ja latenssiajaksi on ilmoitettu enintään vajaat 2 sekuntia. Dash7 tukee myös suoraan IPv6:ta, mikä mahdollistaa verkon kytkemisen internetiin.

Dash7 tukee myös 128-bittistä julkisen avaimen AES-kryptausta. Tekniikassa voidaan käyttää FSK- tai GFSK-modulaatioita, jotka määräävät tiedonsiirron nopeuden. Dash7:lla on pieni avoin protokollapino, mikä kertoo sen yksinkertaisesta toteutuksesta.

Dash7 ei käytä tavanomaisia sessioita tiedonsiirrossa, vaan siinä on käytössä ratkaisu nimeltä BLAST (Bursty, Light, Asynchronous, Transitive). Tiedonsiirto on purskemaista, eikä sisällä raskaita elementtejä, kuten kuvaa tai videota. Keveys näkyy myös paketin koossa, joka on rajoitettu 256 tavuun. Paketteja voidaan lähettää myös peräkkäin ilman taukoja, mutta sitä pyritään välttämään, mikäli mahdollista.

Synkronoimattomuus poistaa tiedonsiirrosta tiettyjä vaatimuksia, kuten esimerkiksi kättelyn (handshake). Tällöin tiedonsiirto tapahtuu yksinkertaisesti siten, että laite lähettää komennon toiselle laitteelle ja saa tältä siihen kuittauksen. Pääpaino Dash7-laitteiden tiedonsiirrossa on tiedon lähettämisessä. Täten tukiasemien ei tarvitse laajamittaisesti hallinnoida laitteita. Lisäksi laitteet ovat pienikokoisia ja helposti liikuteltavia.

10.3 Yleistietoa

Dash7-tekniikan haasteena on pienikokoisten tehokkaiden antennien suunnittelu 70 cm aallonpituuksille [20]. Tekniikkaa kehitetään parhaillaan, ja sillä katsotaan olevan monia käyttösovelluksia, kuten esimerkiksi autonrenkaiden paineen tunnistus, kuljetuskonttien paikannus ja RFID-paikantimien apuna toimiminen.

11 EnOcean

EnOcean on saksalainen, ympäristön uusiutuvia energiamuotoja hyödyntävä suljettu standardi, jota käytetään ensisijaisesti erilaisissa automaatiojärjestelmissä. Teknologialla voidaan automatisoida vaikkapa kodin valaistukseen ja lämmitykseen tarkoitetut kytkimet langattomasti. Kuvassa 22. on EnOceanin logo.

Green. Smart. Wireless.
enocean®

Kuva 22. EnOcean-logo

Tekniikan keskeinen idea on muuntaa ympäristöstä saatu energia laitteessa herätteeksi tiedonsiirron aloittamiselle. EnOcean-laitteet voivat hyödyntää radiosignaalien lähettämiseen aurinkokennoja, lämpöpareja, sähkömagnetismia ja muita vastaavia menetelmiä. Akkuja tai kytkentöjä sähköverkkoon ei siis tarvita. EnOcean-verkon rakenne koostuu lähettimistä, vastaanottimista sekä näiden yhdistelmistä.

11.1 Käyttösovellukset

Esimerkkinä EnOcean-pohjaisesta kodin automaatiojärjestelmästä on kuvan 23 mukainen sensori- ja kontrollointijärjestelmä. Sen avulla voidaan automatisoida ja kaukoohjata kodin valaistusta, kaihtimia, lämmitystä ja muita etähallinnan piiriin asennettuja laitteita. Taulukkoon 21 on merkitty kuvassa 23 numeroitujen laitteiden käyttötarkoitukset.

Kuva 23. EnOcean-laitteita huoneistossa [21]

Taulukko 13. Kuvan 23 laitteiden kuvaukset [21]

Numero	Kuvaus
1	Valaistuksen ja kaihdinten säädin

2	Ulkoilman valoisuuden mittari
3	Tunnistin, joka huolehtii huoneen lämpötilasta ja valaistuksesta
4	Lämpötila-anturi
5	Ilmankosteuden ja hiilidioksidipitoisuuden mittari
6 - 7	Ikkunan asennon tunnistimet, jotka pitävät ilmastoinnin suljettuna ikkunan aukiolon ajan
8 - 9	Hallintajärjestelmä tietokoneelle ja älypuhelimelle

EnOceania voidaan käyttää myös esimerkiksi langattomassa yleisöäänestyksessä, jossa jokaisen äänestäjän ääni saadaan poimittua yleisön joukosta. Tällä menetelmällä äänestäjät voidaan tarvittaessa myös yksilöidä. EnOcean valmistaa automaatiojärjestelmiä myös tehdastarkoitukseen sekä uusissa autoissa sovellettavaan automaatioon.

11.2 Historia

EnOceanin ideaa lähdettiin kehittämään sen pohjalta, että haluttiin mahdollistaa paristottomien sensorien ja kytkinten käyttö langattomassa automaatiotekniikassa. EnOcean GmbH -yritys sai alkunsa Siemens AG -osakeyhtiöstä, josta se eriytyi vuonna 2001. Yrityksessä työskentelee joitain kymmeniä työntekijöitä, ja sen tarkoitus on valmistaa lähettimiä, vastaanottimia sekä lähetinvastaanottimia muille yrityksille.

EnOcean GmbH on voittanut palkintoja saavutuksistaan langattomassa teknologiassa, kuten vuonna 2002 pidetyssä Bavarian Innovation Prize -tilaisuudessa EnOcean sai maailmanlaajuisesti ainutlaatuisen tekniikan palkinnon. Yritys palkittiin myös vuonna

2006 pidetyssä Technology Pioneer -tilaisuudessa sekä Top-10 Product for 2007 -tilaisuudessa vihreän arvomaailman mukaisesta toiminnasta.

Vuonna 2007 EnOcean GmbH julkaisi kahden celsiuksen lämpötilaerolla toimivan, 1,5 cm^2 kokoisen Peltier-paneelin, mikä riittää radiolähetyksen suorittamiseen. Vuonna 2007 MK Electric, Brirannian suurin kulutuselektroniikkavalmistaja, adoptoi EnOcean-tekniikan käytettäväksi langattomissa kytkimissään.

11.3 EnOcean Alliance

EnOcean Alliance on EnOcean-laitevalmistajien välinen liitto. Standardi ei ole avoin, joskin sitä hallinnoiva yritys, EnOcean GmbH tarjoaa standardia ja lisenssejä EnOcean Alliancelle. Liitolla on monentasoisia osanottajia, joihin kuuluvat mm. Texas Instruments, Siemens ja Yamaha.

11.4 Tekniset tiedot

EnOcean toimii lisensöimättömällä 868,3 MHz:n taajuusalueella, ja käyttää virransäästösyistä tiedonsiirtoon pelkkiä ykkösbittejä. Tekniikan ominaisuudet on koottu taulukkoon 14.

Taulukko 14. EnOcean-tekniikan ominaisuudet [22]

Taajuus	868,3 MHz
Bittinopeus	120 kbit/s
Paketin pituus	14 tavua = 112 bittiä
Modulaatio	ASK
Kantama	300 m

EnOcean-sensoriverkossa lähetetään kolme pakettia kerrallaan satunnaista järjestystä muistuttavilla ajanhetkillä, jotta ruuhkaisissa verkoissa paketit interferoisivat vähemmän keskenään. Kytkinlaitteissa lähetys tapahtuu kytkimen painallus- tai säätöhetkellä,

mikä mahdollistaa esimerkiksi olohuoneessa valaistuksen interaktiivisen himmentämisen.

11.5 Yleistietoa

EnOcean-tekniikan vahvuutena on sen kyky kerätä energiaa ympäristöstään. Lisäksi 868,3 MHz:n taajuus läpäisee esteitä kohtuullisen hyvin. Nämä asiat antavat tiettyjä vapauksia verkon rakentamiseen. Myös interferenssi kyseisellä taajuusalueella on harvinaista.

EnOceanin pienen lähetystehon ansiosta myös sen tuottamat säteilyannokset ovat pieniä. Se ei ole yhtä läpitunkevaa kuin esimerkiksi Dash7:n 433 MHz säteily, mutta toisaalta antennien suunnittelu on helpompaa.

EnOceanin virallisilla sivuilla tekniikalla nähdään olevan paljon kehitysmahdollisuuksia. Tekniikkaa voidaan EnOcean GmbH:n visioiden mukaan hyödyntää tulevaisuudessa myös dementiapotilaiden muistuttamiseen, huolettoman elämän rakentamiseen sekä elämänlaadun parantamiseen.

12 MyriaNed

MyriaNed on alankomaisen DevLab-tutkimusliiton kehittämä langaton sensoriverkkoteknologia. Sen avulla voidaan mitata esimerkiksi ilman lämpötilaa ja kosteutta. Luottamusta tekniikan kehittäjältä ei tekniikkaa kohtaan puutu, sillä tekniikkaa sovelletaan myös polkupyörän langattomissa käsijarruissa. MyriaNedin logo on kuvassa 24.

Kuva 24. MyriaNedin logo

Verkon rakenne perustuu ideaan, jossa yksi lähetin lähettää tiedon radioteitse usealle vastaanottajalle, ja kaikki nämä lähettävät saamansa tiedon eteenpäin. Tiedon leviämistä voisi verrata kulkutautiin: jos yksilöllä ei vielä ole kyseistä kulkutautia, hän saa sen taudinkantajalta ja toimii tästä lähtien sellaisena myös itse. Taudin saaneet eivät

enää reagoi sen tartuttajiin. Tästä tulee MyriaNedin yhteydessä käytetty termi "epidemic communication", eli epideeminen tiedonkulku.

Viestien lähetys MyriaNed-verkossa tapahtuu jaksollisesti, ja kaikki lähistöllä olevat laitteet vastaanottavat sen. Verkon vahvuudeksi katsotaan sen luotettavuus sekä selviytyminen liikkuvissa sovelluksissa, koska viestillä on lukuisia mahdollisia reittejä kulkea lähettäjältä vastaanottajalle. Viestiä välittäviä laitteita kutsutaan tässä yhteydessä yhdyslaitteiksi (nodes).

Verkon tehokkuutta ja luotettavuutta on omiaan tukemaan sekin, että yhdyslaitteiden ei tarvitse tietää mitään viestin lähettäjästä eikä naapureistaan: riittää, että ne lähettävät saamansa viestin eteenpäin välittömästi. Yhdyslaitteita voidaan lisätä ja poistaa vapaasti verkosta ilman, että verkkoa tarvitsee konfiguroida uudelleen.

MyriaNed käyttää tiedon välityksessä itseorganisoituvaa Gossip-protokollaa [23]. Suomeksi tämä tarkoittaa juoruamista. Verkko voi olla heterogeeninen, jossa useat eri yhdyslaitetyypit kommunikoivat erilaisia tietoja välittäen samanaikaisesti. Tämä on mahdollista, koska yhdyslaitteet eivät tulkitse saamaansa viestiä, vaan välittävät sen suoraan eteenpäin. MyriaNed tukee myös "over the air" -tyyppistä, eli radioteitse tapahtuvaa yhdyslaitteiden päivittämistä pystytettyyn verkkoon.

Inspiraatio MyriaNedin kehittämiseen lähti siitä, kun sen suunnittelijat vertasivat perinteistä isännän ja rengin välistä tiedonsiirtotapaa luonnon tapaan siirtää tietoa. Esimerkiksi kehossa oleva adrenaliini käyttäytyy täysin tästä poiketen: Viesti adrenaliinin vapauttamisesta kulkee kehossa samanaikaisesti erityyppisille soluille, ja jokainen solu tietää, miten tämän viestin kanssa tulee toimia. Toimenpiteitä ovat elimistön osasta riippuen esimerkiksi pulssin nostaminen, verisuonten supistaminen ja keuhkojen laajentaminen. Yksikään solu ei myöskään lähetä tästä varmennusta viestin lähettäjälle, mutta reaktiot toimivat kehossa silti varmasti.

Toinen inspiraatiota antanut ajatus MyriaNedin kehittämiselle oli radiolähetyksen periaate: tyypillinen radiolaite on tehty lähettämään tietoa kaikkiin suuntiin ja myös vastaanottamaan sitä kaikkialta. Se ei selvästikään ole optimoitu point-to-point-tyyppiselle kommunikaatiolle, jossa viesti kulkee vain kahden laitteen välillä: Johdot ovat tähän tarkoitukseen ideaalisia, kun ne yhdistävät kaksi laitetta toisiinsa, eivätkä säteile infor-

maatiota toistensa ohi. Tästä näkökulmasta katsottuna MyriaNed käyttää ympäristöön leviävää radiosäteilyä paremmin hyödyksi.

Myös ihmisten tapa levittää tietoa juoruamalla on antanut MyriaNedille inspiraatiota. Tässä yhteydessä ei tarkoiteta kuitenkaan tiedon vääristelyä, vaan sen leviämisperiaatetta, jossa monienkaan linkkien toiminnan estyminen ei välttämättä haittaa tiedon siirtymistä eteenpäin.

MyriaNedissä myös se on huomionarvoista, että viesti välitetään heti, kun se on saatu. Tämän jälkeen yhdyslaitteelle tulee todennäköisesti samoja viestejä toistamiseen muilta yhdyslaitteilta, mutta se jättää ne huomiotta, koska tarvittava työ on jo tehty. Verkko on yksinkertaisen ideansa ansiosta myös varsin hyvin skaalautuva tavanomaisiin verkkoihin nähden.

12.1 Sovellukset

Yksinkertaisuutensa ja skaalautuvuutensa ansiosta MyriaNedillä ei ole tarvetta erilaisille profiileille markkinoilla. Sitä käytetään edellä mainittujen sovellusten lisäksi muun muassa rakennusteollisuudessa koneiden kauko-ohjaukseen sekä lämmönsäätelyyn, kotitalouksissa lastenhoitoon ja maataloudessa puutarhanhoitoon. Yksi MyriaNedin eduista on, että rinnakkaiset verkot lisäävät toistensa toimintavarmuutta sen sijaan, että häiritsisivät toisiaan.

Tutkimusliitto DevLabin jäsenistä kaikki ovat vapaita käyttämään MyriaNedia mihin tahansa haluamaansa tarkoitukseen. Tästä on seurannut se, että monet laitteet täysin eri käyttötarkoituksista ovat viestien välitystasolla kuitenkin yhteensopivia.

12.2 Tekniset tiedot

MyriaNed käyttää monien muiden tekniikoiden tapaan 2,4 GHz:n taajuusaluetta, mikä vähentää signaalien läpäisykykyä sekä saattaa aiheuttaa interferenssiä muiden tekniikoiden samanaikaisen käytön yhteydessä. Toisaalta se mahdollistaa matalampia taajuuksia nopeamman tiedonsiirron ja pienemmät antennit. 2,4 GHz on yksi monista taajuusalueista, jolla tekniikkaa voidaan jatkossa toteuttaa.

Virransäästö MyriaNedissä on toteutettu siten, että yhdyslaitteet kommunikoivat jaksollisesti, ja ovat täten lepotilassa suurimman osan ajasta. Yhdyslaitteissa on sisäänrakennettu synkronointimekanismi, mikä herättää kaikki verkossa olevat laitteet samanaikaisesti, jolloin laitteet joko lähettävät tai vastaanottavat tietoa.

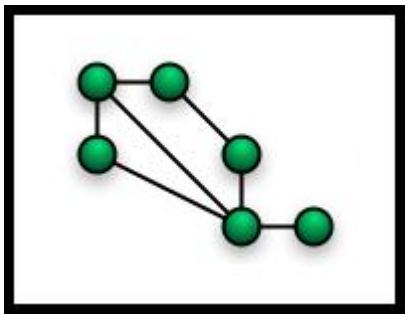
13 One-Net

One-Net on avoin tietoliikennestandardi langattomalle tietoliikenteelle hallintaverkoissa, kuten esimerkiksi kodin laitteita ja turvallisuutta kontrolloivissa järjestelmissä. Sillä voidaan toteuttaa näiden lisäksi myös esimerkiksi langaton sääominaisuuksia havainnoiva sensoriverkko. One-Netin logo on kuvassa 25.

Kuva 25. One-Netin logo

One-Net ei ole sidonnainen mihinkään tiettyyn laitteisto- tai ohjelmistotyyppiin, joten valmistajat voivat käyttää sitä monissa edullisissakin radiolähetinvastaanottimissa ja muissa laitteissa. Tekniikka on tarkoitettu hallintakäskyjen ja tilannetiedon siirtämiseen.

Monista muista tekniikoista poiketen One-Net tukee multi-hop-verkkomallia, missä lähes minkä tahansa tyyppinen verkon rakenne on mahdollinen. Yhdyslaitteiden suhteet toisiinsa määräytyvät aina tilanteen mukaan, ja jokainen laite voi olla yhteydessä niin moneen muuhun laitteeseen kuin on tarpeellista. Multi-hop-verkkomalli on esitetty kuvassa 26.



Kuva 26. Multi-hop-verkkomalli

Täten One-Net-verkko voi muotoutua myös tähtimäiseen ja peer-to-peer-verkkomalliin. Tähtimäisessä verkossa kaikki laitteet yhdistyvät vain keskellä olevaan laitteeseen, eivät toisiinsa. Tämä helpottaa verkon hahmottamisen lisäksi salausavainten hallintaa. Kahden laitteen välisessä peer-to-peer-verkossa toisen tarvitsee olla isäntä ja toisen renki. Tämä tosin ei hyödynnä lähellekään koko One-Net-tekniikan potentiaalia, ja tällöin vain keskeisimmät tiedonsiirtotoiminnot ovat käytössä.

13.1 Avoin lisenssi

One-Net -lisenssi perustuu avoimeen lähdekoodiin ja on täten vapaasti hyödynnettävissä. One-Netin verkkosivut tarjoavat runsaasti tietoa liittyen tekniikan soveltamisen suunnitteluun, antennisuunnitteluun sekä tekniikan käyttöönottoon. Sivuilla on myös valmiita antenni- ja piirilevymalleja, lähdekoodit, dokumentaatioita sekä käyttäjäfoorumit. One-Net -lisenssiä käyttävät Texas Instrumentsin ohella monet muut laitevalmistajat.

13.2 Tekniset tiedot

One-Net käyttää 868 – 915 MHz:n radiotaajuusalueella toimivia UHF-lähetinvastaanottimia (transcievers). One-Netin saa toimimaan myös 433 MHz:n ja 2,4 GHz:n taajuuksilla. Tiedonsiirrossa hyödynnetään taajuuden muuttamiseen perustuvaa FSK-modulaatiota (Frequency Shift Keying).

One-Netin tiedonsiirtonopeus on 38,4 kbit/s, joskin sen protokollat mahdollistavat nopeuden 230 kbit/s asti. Peer-to-peer-tilassa tiedonsiirto onnistuu esteettömässä ympäristössä vielä 500 metrin etäisyydeltä. Sisätiloissa etäisyys voi käytännössä olla 60 metristä 100 metriin. Multi hop -tilassa tiedonsiirto voi onnistua vielä kilometrienkin päästä. [23.]

13.3 Virransäästö

One-Net on optimoitu kuluttamaan vähän virtaa ja toimimaan paristokäyttöisissä ratkaisuissa. Alhaisen näytteenottotaajuuden laitteissa, kuten kosteusmittareissa tai ikku-

natunnistimissa yksi AAA- tai AA-paristo voi riittää 3-5 vuodeksi. Signaalien dynaaminen tehonsäätö vähentää energiantarvetta, ja myös lyhyet paketit ja verrattain suuret tiedonsiirtonopeudet lyhentävät lähetyksen kestoa, mikä on omiaan parantamaan energiatehokkuutta.

13.4 Tietoturvallisuus

Tiedon salaus on integroitu One-Net -tekniikkaan, joten tiedon lähetys ilman sitä ei ole mahdollista. One-Net käyttää aina vähintään XTEA-algoritmia tiedon kryptaukseen (Extended Tiny Encryption Algorithm). Myös vahvempien salausten käyttö on mahdollista.

One-Net -tiedonsiirtoa voidaan yrittää häiritä esimerkiksi spoofing-hyökkäyksillä, tai tekaistuilla vastaushyökkäyksillä. Näiden ehkäisemiseksi tiedonsiirrossa käytetään tilannekohtaisia tunnisteita (cryptographic nonces), jotka tekevät jokaisesta lähetyksestä uniikin.

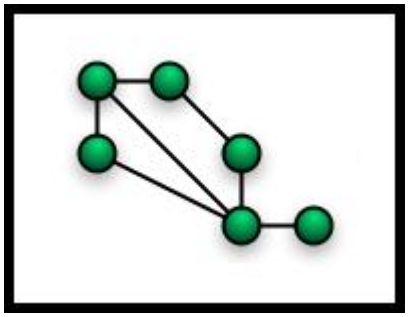
14 Z-Wave

Z-Wave on yksityisessä omistuksessa oleva langaton tiedonsiirtostandardi, joka on tarkoitettu laitteiden etähallintaan. Z-Wave soveltuu akkukäyttöisiin ratkaisuihin, ja sitä voidaan käyttää esimerkiksi valaistuksen, lukkojen, viihde-elektroniikan ja kodinkoneiden etähallintaan. Se soveltuu myös käytettäväksi kodin turvalaitteissa, kuten palovaroittimissa. Kuvassa 27 on Z-Wave -tekniikan logo.

Kuva 27. Z-Wave-tekniikan logo

Z-Wave kuluttaa niukasti virtaa ja reagoi nopeasti annettuihin käskyihin. Se toimii 900 MHz:n radiotaajuudella, mikä auttaa sitä läpäisemään esteitä paremmin kuin esimerkiksi 2,4 GHz:lla toimivat tekniikat.

Z-Wave -verkon rakenne perustuu multi-hop -malliseen silmukkaverkotukseen (mesh networking), jossa mikä tahansa yhdyslaite voi toimia viestinvälittäjänä. Tällöin laitteiden asettelu helpottuu. Ideana on, että esimerkiksi kahden toisiinsa yhteydessä olevan laitteen ei tarvitse olla toistensa kuuluvuusalueella, jos niiden välissä on yksikin laite, joka tavoittaa niistä molemmat. Kuva 28 selventää silmukkaverkotuksen ideaa.



Kuva 28. Mesh-silmukkaverkko on rakenteeltaan multi-hop-mallinen.

Monet yhdyslaitteen asemassa toimivat Z-Wave-laitteet eivät voi mennä lepotilaan, mikä vaatii niiltä enemmän virtaa. Tämän vuoksi useimmat akkukäyttöiset Z-Wave-laitteet eivät toimi yhdyslaitteina, eli ne eivät toista saamiaan viestejä. Z-Wave-verkko voi koostua enintään 232 laitteesta. Jos jossakin sovelluksessa tarvitaan enemmän laitteita, verkkoja voidaan linkittää toisiinsa.

Z-Wave-laitteita voidaan kontrolloida myös kodin ulkopuolelta internetin välityksellä. Siten voidaan hallinnoida myös kodin energiankulutusta. Z-Wave tarjoaa myös edistyksellisiä automaatioratkaisuja: esimerkiksi kun kodin ulko-ovi on avattu kotiavaimella, kodin turvajärjestelmät ja hälytyslaitteet voivat mennä automaattisesti pois päältä, ja eteisen valaistus syttyä päälle. Jos lapsi tulee koulusta kotiin ennen vanhempia, järjestelmä voi myös lähettää vanhempien kännyköihin tekstiviestin kotioven avautumisesta.

Z-Wave tarjoaa möys liikkeen tunnistavia valoja ja web-kameroita kotipihoille, mikä mahdollistaa energiatehokkaan ympäristönvalvonnan. Z-Wave -kaukosäätimiin on myös mahdollista rakentaa omavalintaisia käskyketjuja eri laitteiden välille.

Jos käyttäjä painaa esimerkiksi "Soita DVD" -painiketta, moottoroidut kaihtimet voivat himmentää huoneen ja valot mennä pois päältä. Kuvassa 29 on havainnollistettu Z-Waven käyttömahdollisuuksia.

Kuva 29. Z-Waven käyttömahdollisuuksia [26]

14.1 Z-Wave Alliance

Z-Wave Alliance on yli 160 yrityksen välinen liitto, jonka jäsenet ovat sitoutuneet valmistamaan Z-Wave-tekniikalla varustettuja laitteita. Tuotteita on nykyään saatavilla Euroopan ja Amerikan markkinoilla. Suljettu Z-Wave-standardi on saatavilla vain Zensys-yrityksen asiakkaille salassapitosopimuksen nojalla.

14.2 Tekniset tiedot

Z-Wave tukee 128-bittistä AES-kryptausta. Sen toimintataajuus on Euroopassa 868 MHz ja sillä on lupa olla aktiivisena 1 % ajasta, mikä myös rajoittaa myös tiedonsiirtokapasiteetin 1 %:iin siitä, mitä se voisi olla. Amerikassa tekniikkaa käytetään eri tavalla. Taulukko 15 kertoo Z-Waven alueellisista taajuuksista ja sen käytön rajoituksista.

Taulukko 15. Z-Waven ominaisuuksia [24]

Ominaisuus	Tieto	Lisätiedot

kaistanleveys	9600 bit/s	
modulaatio	GFSK	
taajuus	868,42 MHz (Eurooppa)	908,42 MHz (Amerikka), 919,82 (Hong Kong), 921,42 MHz (Australia/New Zealand)
rajoitus ajan suhteen	1 % ajasta (Eurooppa)	ei rajoitusta (Amerikka)
lähetysteho maks.	25 mW (Eurooppa)	1 mW (Amerikka)
kantama	30 metriä	

15 Yhteenveto

Tässä työssä esiteltiin 12 lyhyen kantaman langatonta tiedonsiirtotekniikkaa. Täten työssä päästiin sille asetettuun tavoitteeseen. Metropolia Ammattikorkeakoulu voi nyt käyttää työtä kurssimateriaalina tietoliikennetekniikan kursseilla.

Työn tekemisessä ei varsinaisesti tullut vastaan ongelmia. Joistakin tekniikoista tosin oli haastavampaa saada tietoa kuin toisista, mutta loppujen lopuksi tietoja saatiin kuitenkin riittävästi kerättyä. Työssä onnistuttiin kertomaan tekniikoiden käyttösovelluksista, verkkotopologioista sekä siirrettävän tiedon salaamisesta. Esittelyissä keskityttiin myös tekniikoiden teknisiin ominaisuuksiin, kuten taajuuksiin, kantamiin ja tiedonsiirtonopeuksiin. Niissä tehtiin myös lyhyet katsaukset tekniikoiden historioihin ja tekniikoita hallitseviin organisaatioihin.

Esittelyissä tekniikoita myös vertailtiin toisiinsa jonkin verran. Tämän katsottiin kuitenkin olevan riittämätöntä kokonaiskuvan saamisen kannalta. Tämän seurauksena työn päätteeksi koottiin taulukko liitteeseen 1, jossa on mukana kaikki esitellyt tekniikat. Sen avulla tekniikoita voidaan vertailla laajemmin keskenään.

Taulukkoon on merkitty kunkin tekniikan verkkotopologia, käyttösovellukset, kantama, tiedonsiirtonopeus ja käytettävä taajuusalue. Tekniikoiden ominaisuudet on kerätty muista tämän työn taulukoista.

Taulukko myös auttaa hahmottamaan, millaiset verkkotopologiat soveltuvat mihinkin käyttötarkoitukseen sekä millaisia nopeuksia ja taajuuksia niissä yleensä käytetään. Esimerkiksi sensoriverkkotekniikat, kuten EnOcean ja Dash7, käyttävät alhaisia tiedonsiirtonopeuksia, mutta monimuotoista verkkotopologiaa. Niiden käyttämät matalat taajuudet myös läpäisevät esteitä hyvin.

Tietotekniikkalaitteissa käytettävät Bluetooth, WLAN ja WUSB puolestaan käyttävät suurempia tiedonsiirtonopeuksia, ja niiden verkkotopologiat ovat yksinkertaisempia. Ne myös käyttävät korkeampia taajuuksia, mikä heikentää niiden kykyä läpäistä esteitä. Tosin tällöin antennien koko pienenee, mikä helpottaa niiden sijoittelua.

RFID:hen pohjautuvat lähitunnistustekniikat taas toimivat lyhyillä aikajaksoilla, ja kommunikaatio on vain kahden laitteen välistä. Tekniikat sopivat muiden muassa tuotteiden tunnistamiseen ja yksilöintiin. Tekniikoiden kantamat ja tiedonsiirtonopeudet vaihtelevat käyttötarkoituksen mukaan.

Erilaisia langattomia tiedonsiirtotekniikoita on olemassa runsaasti. Tähän työhön koottiin tunnetuimpia tai muulla tavalla huomionarvoisia tekniikoita. Langattomat tekniikat luovat monia mahdollisuuksia elämän helpottamiseen. Kun tekniikoita käytettäessä huolehditaan vielä tietoturvasta ja radiosäteilyn ympäristövaikutuksista asianmukaisesti, tekniikoista saadaan suurin hyöty irti.

Lähteet

1 All About Modulation – Part I. 2005. Verkkodokumentti. Charan Langton. <www.complextoreal.com/chapters/mod1.pdf> Luettu 24.5.2012.

2 Tieteen Kuvalehti 7/2011, s. 13. Bonnier Publications

3 IARC Press Release Nº208, s.1–5. 2011. Verkkodokumentti. WHO. <http://www.iarc.fr/en/media-centre/pr/2011/pdfs/pr208_E.pdf> Luettu 26.5.2012.

4 Intel and 802.11, Helping Define 802.11n and other Wireless LAN Standards, IEEE 802.11 wireless local area networks. Verkkodokumentti. Intel Corporation. < http://www.intel.com/standards/case/case_802_11.htm>

5 A Look at the Basics of Bluetooth Wireless Technology. 2012. Verkkodokumentti. Bluetooth SIG. <http://www.bluetooth.com/Pages/Basics.aspx>

6 IEEE 802.11, Channels and international compatibility. Verkkodokumentti. <http://en.wikipedia.org/wiki/IEEE_802.11> Luettu 24.5.2012.

7 IEEE 802.11, Protocols. Verkkodokumentti. <http://en.wikipedia.org/wiki/IEEE_802.11> Luettu 25.5.2012.

8 The six dumbest ways to secure a wireless LAN. 2005. Verkkodokumentti. George Ou. <http://www.zdnet.com/blog/ou/the-six-dumbest-ways-to-secure-a-wireless-lan/43>

9 ZigBee, Verkon osat ja verkkotopologiat. Verkkodokumentti. <http://fi.wikipedia.org/wiki/ZigBee> Luettu 25.5.2012.

10 What is ZigBee? Verkkodokumentti. ICP DAS Co., Ltd. <http://www.icpdas.com/products/GSM_GPRS/zigbee/zigbee_introduction.htm>

11 EVM measurements on ZigBee signals. 2005. Verkkodokumentti. News from Rohde & Schwarz. <http://www2.rohde-schwarz.com/file_4830/n185_fsq2.pdf>

12 Wireless USB - An Overview, 3. WUSB Topology. 2008. Verkkodokumentti. Innovative Logic, Inc. <http://www.inno-logic.com/resourcesWUSB.html>

13 WUSB, Comparison of digital RF systems. Verkkodokumentti. <http://en.wikipedia.org/wiki/Wireless_USB> Luettu 26.5.2012.

14 RFID Modulation, Encoding, and Data Rates. 2009. Verkkodokumentti. Dale R. Thompson. <http://rfidsecurity.uark.edu/course/mod4/lessons/pdf/mod04_lesson04_plan.pdf>

15 Near field communication, Comparison with Bluetooth. Verkkodokumentti. <http://en.wikipedia.org/wiki/Near_field_communication> Luettu 27.5.2012.

16 What is DECT? Some answers, Origins of DECT. Verkkodokumentti. <http://www.dectweb.com/Introduction/answers.htm> Luettu 27.5.2012.

17 DECT 6.0 vs. 900 MHz vs. 2.4GHz vs. 5.8 GHz, What is DECT? Verkkodokumentti. <http://www.telecomuserguides.com/manuals/filesupload/Panasonic/wireless-phones/What_is_DECT.pdf> Luettu 28.5.2012.

18 Feature Comparison. 2009. Verkkodokumentti. Dash7 Alliance. <http://www.dash7.org/index.php?option=com_content&view=article&id=148&Itemid=203> Luettu 28.5.2012.

19 Dash7, Technical summary. Verkkodokumentti. <http://en.wikipedia.org/wiki/DASH7> Luettu 27.5.2012.

20 Dash7 Wireless Networking Gains Momentum. 2010. Verkkodokumentti. David Schneider. <http://spectrum.ieee.org/telecom/wireless/dash7-wireless-networking-gains-momentum> Luettu 28.5.2012.

21 Office Buildings, EnOcean - the Energy Harvesting Wireless Standard for Building Automation. Verkkodokumentti. <http://www.enocean-alliance.org/en/office/> Luettu 28.5.2012.

22 EnOcean, EnOcean Technology. Verkkodokumentti. <http://en.wikipedia.org/wiki/EnOcean> Luettu 29.5.2012.

23 MyriaNed, a self organizing, gossiping Wireless Sensor Network. Verkkodokumentti. Devlab. <http://www.devlab.nl/myrianed> Luettu 29.5.2012.

24 One-Net, Wireless Transmission. Verkkodokumentti. <http://en.wikipedia.org/wiki/ONE-NET> Luettu 29.5.2012.

25 What is DASH7 Technology? 2009. Verkkodokumentti. Dash7 Alliance. <http://www.dash7.org/index.php?option=com_content&view=article&id=9&Itemid=10> Luettu 29.5.2012.

26 Z-Wave: The New Standard in Wireless Remote Control. Verkkodokumentti. Z-Wave Alliance. <http://www.z-wave.com/modules/AboutZ-Wave/> Luettu 29.5.2012.

Lyhyen kantaman langattomien tiedonsiirtotekniikoiden vertailua

Tekniikka	Verkon rakenne	Käyttö-sovelluksia	Kantama (m)	Tiedon-siirtonopeus maks.	Taajuus
Bluetooth 3.0	Piconet / Scat-ternet	Matka-puhelimet, kuuloke-mikrofonit	100	3 – 24 Mbit/s	2,4 GHz
Bluetooth Low Energy	Star-bus	Matka-puhelimet, kodin elektro-niikka	50	1 Mbit/s	2,4 GHz
WLAN 802.11g	Tukiasema + päätelaitteet	Langaton internet tieto-koneissa ja älypuhelimissa	140	54 Mbit/s	2,4 GHz
WLAN 802.11n	Tukiasema + päätelaitteet	Langaton internet tieto-koneissa ja älypuhelimissa	250	72 – 150 Mbit/s	2,4 GHz ja 5 GHz
ZigBee	Tähtimäinen / Peer-to-Peer	Kodin auto-maatio	500	250 kbps	868 MHz, 915 MHz, 2,4 GHz
WUSB	Tähtimäinen	PC:n oheislait-teet	10	480 Mbit/s	3,1 – 10,6 GHz
RFID	Lähitunnistus	Tuotteiden ja lemmikkien lähitunnistus			
NFC	Lähitunnistus	Lähitunnistus maksamisessa ja mainoksis-sa	0,1	424 kbps	13,56 MHz
Dect	Tukiasema + puhelimet	Yritysten sisä-tila-puhelimet	100	32 kbps	1880 – 1930 MHz
Dash7	Sensoriverkko	Säänmittaus, liikkeen tun-	10 000	200 kbps	433 MHz

		nistus			
EnOcean	Sensoriverkko	Energia-omavaraiset automaatio-sovellukset		120 kbps	868,3 MHz
MyriaNed	Sensoriverkko	Säänmittaus, langattomat käsijarrut			2,4 GHz
One-Net	Multi-hop - sensoriverkko	Kodin tuvalli-suus, sään-mittaus	500	230 kbps	433 MHz; 868 – 915 MHz; 2,4 GHz
Z-Wave	Multi-hop - sensoriverkko	Tunnistimet, mittarit, yms.	30	9600 bps	868,42 MHz