TAMPEREEN AMMATTIKORKEKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Tutkintotyö

Jarno Toro

BLUETOOTH-TEKNIKKA JA TIETOTURVA

Insinöörityö, joka on jätetty opinnäytteenä tarkastettavaksi insinööritutkintoa varten Tampereella huhtikuussa 2006.

Tekijä: Jarno Toro

Työn nimi: Bluetooth-tekniikka ja tietoturva.

Päivämäärä: 6.4.2006
Sivumäärä: 53 sivua + 1 liitesivu
Hakusanat: Bluetooth, lyhyen kantaman langaton tiedonsiirto.
Koulutusohjelma: Tietotekniikka
Suuntautumisvaihtoehto: Tietoliikennetekniikka

Työn valvoja: Lehtori Ari Rantala

Bluetooth-tekniikka on lisääntynyt merkittävästi viimeisien vuosien aikana. Nykyään sitä käytetään matkapuhelimissa, tietokoneissa kuin kaikenlaisissa muissakin lyhyen kantaman tiedonsiirtoa tarvitsevissa laitteissa. Käyttäjämäärien lisääntyessä on myös väärinkäyttäjien määrät kasvaneet ja siitä syystä tietoturvallisuusasiat nousevat aina puheenaiheeksi. Nykyään on nähtävissä, miten Internetin suuren käyttäjämäärän ansiosta ovat myös haittavaikutukset lisääntyneet suuressa määrin. Nykyään Internet onkin suurin viruksien levittäjä ja sen kautta tehdään suurin osa tietomurroista. Samantapainen trendi on myös näkyvissä muissakin tiedonsiirtojärjestelmissä. Puhuttaessa langattomista tiedonsiirtojärjestelmistä pitää muistaa, että tietomurtojen mahdollisuus kasvaa huomattavasti verrattuna langallisiin järjestelmiin.

Työssä tutkitaan, miten bluetooth-tekniikka on toteutettu alkuajoista lähtien tähän päivään asti ja pohditaan hieman, mitä tulevaisuudessa on suunniteltu bluetoothin varalle. Työssä on myös keskitytty tutkimaan, miten bluetoothin tietoturva on suunniteltu niin teknisesti kuin ihan käytännönkin tasolla. Teknisellä puolella tietoturvan osalta on käsitelty erilaisten salausavainten käyttöä kuin toimintojakin, ja lisäksi on esitelty teoriassa, miten on mahdollista muuttaa muiden bluetooth-laitteiden suojauksia tai miten on mahdollista suojautua muiden bluetooth-laitteiden hyökkäyksiltä.

Author: Jarno Toro

Name of the thesis: Bluetooth tecnich and information security.

Date: 6.4.2006

Number of pages: 53 pages + 1 appendice

Keywords: Bluetooth, short range wireless cmmunications.

Degree programme: Computer System Engineer

Specialisation: Telecommunications Engineer

Supervicor: Lecturer Ari Rantala

Bluetooth-tecnology has grown in last fiew years. Nowadays it is used in mobile phones, computers and many others short range communications needed devices. At the same time while the number of users is growing the abuse is growing and things about information security are becoming main subject of conversation. Nowadays we can notice how the great numbers of Internet users had an effect on the way how advertise effects have grown a lot. Today Internet is the biggest spreader of virus and the most size of information scurity break-in is done through Internet. The same trend is noticed in the others data-transmission systems and now as we are talking about wireless systems, information security break-in possibility is much bigger than in wireline systems.

In my work I am researching how the bluetooth-technic has carried out from that`s beggining untill today, and I am considering how does it`s future looks like. In my work I am allso concentrated in researching how bluetooths information security is designed technicly and in practise. On the technical side of my work information security has handeld how to use different encryption keys and what are their principles, and there is written in the tekst, how is it possible to go through the protection of other bluetooth devices and how can you protect yourself of attack.

ALKUSANAT

Tämä työ on tehty Tampereen ammattikorkeakoulun tietoliikenne tekniikan insinöörityönä.

Työssä käsitellään bluetooth-tekniikan keskeisimpiä asioita, kuten verkkotopologiaa, tiedonsiirron toimintaa tai protokollien toimintaa jne. Työssä on tutkittu myös bluetoothin tietoturvallisuuteen liittyviä asioita. Tietoturvan tutkimisessa on käsitelty mm. salausavaimien toimivuutta sekä tutkittu bluetooth-laitteiden nykyajan kokemia yleisimpiä uhkia.

Tampereella 6. huhtikuuta 2006

Jarno Toro

SISÄLLYSLUETTELO:

KÄYTETYT LYHENTEET

AC	Access Code, perussanoman ensimmäinen lohko.
ACL	Asynchronous Connectionless link, asynkroninen yhteys.
AD – HOC	Rakenteeton verkko, joka muodostuu siirrettävistä päätelaitteista.
ARQ	Automatic Repeat reQuest, menetelmä, jossa suojataan siirrettävä tieto.
ARQN	Kenttä, jolla lähettäjä kuittaa siirron onnistuneeksi.
AT	Puhelinprotokolla, puhelunkontrollisignaalien välittämiseksi.
CAC	Channel Access Code, kanavan tunnistuskoodi.
CRC	Cyclic Redundance Check, virheen korjauksessa käytettävä jakojäännöslaskentaan perustuva periaate.
DAC	Decice Access Code, yhteyksien luomisen ja kuittaamisen koodi.
DH1...5	Data High rate segment, sanomia datatietoja varten.
DM1...5	Data Medium segment, sanomia datatietoja varten.
EDR	Enhanced Data Rate, versiossa 2.0 käytettävä tekniikka.
ETSI	European Telecommunications Standard Institute, telealan standardisoimisjärjestö.
FCS	Frame Check Sequency, virheenkorjauksen tarkiste.
FEC 1/3, 2/3	Virheen koodausmekanismeja, joilla korjataan siirtotien virheitä.
FHS	Sanoma roolin vaihtoihin pikoverkossa.
FHSS	Frequency Hopping Spread Spectrum, hajaspektritekniikka.
FSK	Frequency Shift Keying, modulaatio, jossa käytetään kahta eri kantoaallon taajuutta.
GAP	Generic Access Profile, bluetoothin linkin hallintaprofiili.
HC	Host Controller, isäntäkontrolleri.
HCI	Host Controller Interface, rajapinta.
HEC	8-bitin mittainen CRC tarkiste.
IAC	Inqyiry Access Code, yleiskoodi.

ID	Sanoma, jolla tunnistetaan AC kenttä.
IETF	Interne Engineering Task Force, Internet-protokollien standardoinnista vastaava organisaatio.
IMS	Indrustial Scientific Medical, Euroopassa käytetty vapaa taajuusalue.
LM	Link Manager, ohjelmistopohjainen linkkiohjain.
LMP	Link Manager Protocol, linkkiohjainprotokolla.
L2CAP	Logical Link Control and Adaption Protocol, protokollapohjainen kanavoija.
MAC	Verkkosovittimen verkossa yksilöivä osoite.
NULL	Pakettityyppi liikenteen kuittaukseen.
OBEX	Object Exchange, objektinvaihtoprotokolla.
OSI	Open Systems Interconnection reference model, tiedonsiirtoprotokollien malli.
POLL	Kyselysanoma isännältä rengille.
PPP	Poin to Poin Protocol, protokolla viimeistelemään pisteestä pisteeseen yhteydet.
PSK	Phase Shift Keying, modulaatio menetelmä.
SCO	Synchronous Connection Oriental link, synkroninen yhteys
SDP	Palvelun hallintaprotokolla.
SEQN	Tieto, jolla numeroidaan sanomat siirtotiellä.
SIG	Bluetooth Special Interest Group, bluetoothin kehitystyöstä vastaava järjestö.
TCS	Binäärinen puhelinprotokolla.
TDD	Time Division Duplex, kanavointitekniikka.
TETRA	Terrestial Trunked Radio, digitaalinen matkapuhelinjärjestelmä.
TU – T	Internal Telecommunication Union, YK:n alainen televiestintäverkkojen palveluja koordinoiva järjestö.
VCARD, VCAL	Objektinvaihtoprotokollan objekteja.

1 JOHDANTO

Ericsson aloitti bluetoothin kehitystyön vuonna 1994, ja 1998 sen kehitystyöhön liittyi useita isoja yrityksiä. Näin sai alkunsa SIG (*Bluetooth Special Interes*). SIG hoitaa bluetoothin kehitystyön ja kaikki muut siihen liittyvät asiat. Nykyään bluetoothia käyttävät tuhannet yritykset.

Bluetooth haluttiin tehdä mahdollisimman yksinkertaiseksi langattomaksi standardiksi ja siihen pyrittiin löytämään soveltuva tekniikka. Samalla pyrkimyksenä oli saada laitteet pienikokoisiksi, vähän virtaa kuluttaviksi ja hinnaltaan halvoiksi. Halpa hinta tarkoittaa lähinnä sitä, että laitteet soveltuvat hyvin massatuotantoon. Ensimmäiset spesifikaatiot julkaistiin vuonna 1999 ja tämän jälkeen kehitystyötä on jatkettu.

Nykyään bluetoothia-laitteita käytetään luultavasti eniten matkapuhelimissa, kämmenmikroissa ja näiden oheislaitteissa, mikä tarkoittaa lähinnä langattomia korvakuulokkeita.
Jonkin verran näkee myös bluetoothia viihde-elektroniikassa. Varsinkin korvakuulokkeissa bluetoothin käyttö on viime aikoina lisääntynyt huimalla vauhdilla.

2 BLUETOOTH YLEISESTI

2.1 Historia

Bluetooth on nimetty tanskalaisen viikinkikuninkaan Harald Blåtandin (*sinihammas*) mukaan. Harald hallitsi rautaisella otteella vuosina 940 – 980 jKr. Hän yhdisti Tanskan ja Norjan sekä toi kristinuskon skandinaavisiin maihin. Kyseisten maiden yhdistäminen onkin haluttu liittää symbolisesti bluetooth-nimeen ja käyttötarkoitukseen. / 5, s. 9/

Ericsson (*nykyinen SonyEricsson*) ajatteli, että markkinoilla olisi kysyntää lyhyen kantaman langattomille laitteille. Vuonna 1994 Ericsson aloitti projektin, jossa pyrittiin edullisilla ja suhteellisen halvoilla eli massatuotantoon soveltuvilla osilla korvaamaan johdotukset matkapuhelimien ja oheislaitteiden väliltä. Tavallisesti keskityttiin korvakuulokkeen ja matkapuhelimen langattomaan yhteyteen. / 5, s. 5/

Ericsson halusi laajentaa tutkimustaan ottamalla kehitystyöhön mukaan muita alan suuria yrityksiä, kuten Nokian, IBM:n, Toshiban ja Intelin. Nämä yritykset perustivat Ericssonin kanssa vuonna 1998 Bluetooth Special Interest Groupin (*SIG*). / 5, s. 6/

Ericsson ymmärsi jo alkuaikoina, että ainoastaan sen käyttämänä ja kehittämänä bluetooth-tekniikka jäisi kovin rajoittuneeksi, joten se halusi liittää kehitystyöhön muitakin yrityksiä, mikä takaisi sen, että tekniikasta tulisi laajasti käytetty. Tästä seuraisi myös se, että suurimmasta osasta bluetooth-laitteita tulisi yhteensopivia.
/ 5, s. 6/

SIG on avoin järjestö. Siihen voivat liittyä kaikki asiasta kiinnostuneet yritykset. Kiinnostusta lisää avoin ja maksuton bluetooth-spesifikaatio. Nykyisin järjestöön on liittynyt tuhansia eri yrityksiä.

Ensimmäinen bluetooth-spesifikaatio julkaistiin vuonna 1999 ja hiukan myöhemmin julkaistiin päivitetty versio 1.0b. Vuonna 2001 tuotiin markkinoille

versio 1.1, jossa oli tehty parannuksia eri valmistajien laitteiden yhteistoimintaan. Marraskuussa 2003 julkaistiin versio 1.2.
Vuonna 2004 julkaistiin versio 2.0, johon on liitetty EDR-tekniikka (*Enhanced Data Rate-tekniikka*). EDR:n pitäisi kasvattaa datan siirtonopeuden kolminkertaiseksi ja alentaa sen myötä tehonkulutusta. Samalla vaihdettiin gfsk-modulaatio gpsk-modulaatioon. Siitä seuraa, että jokaisella symbolilla voidaan siirtää entistä enemmän bittejä ja näin ollen symbolinopeus pysyy samana.

2.2 Esitietoa bluetoothista

Bluetooth on langaton tiedonsiirtotekniikka, jolla erilaiset laitteet pystyvät kommunikoimaan keskenään radioaaltoja pitkin. Bluetoothin tiedonsiirto tapahtuu taajuushyppelyyn perustuvalla hajaspektritekniikalla (*FHSS, Frequency Hopping Spread Spectrum*). Pääasiassa bluetooth-laitteet on kehitetty lyhyen kantaman tiedonsiirtoon ja sen kantosäde on 10m:stä 100m:iin, sen mukaan minkä teholuokan laitetta käytetään. Yleisin käytetty kantama on 10 metrin sisällä.

Bluetooth käyttää 2,45 gigahertsin (GHz) ISM-taajuutta (*Indrustrial – Scientific – Medical*) ja se vaihtelee hieman eri maiden ja maanosien välillä. Tämä taajuus on valittu sen takia, että se on kansainvälisesti yleisesti vapaasti käytettävissä eikä ole luvanvarainen. Tällä samalla taajuudella toimivat mm. wlan-yhteydet. / 8, s.2/

Bluetooth on suunniteltu tekniikaksi, joka soveltuisi hyvin massatuotantoon ja olisi valmistuskustannuksiltaan mahdollisimman halpa. On pyritty siihen, että yhden bluetooth-sirun hinnaksi tulisi noin 5 dollaria., joten bluetooth voitaisiin lisätä kaikkiin laitteisiin, joissa on mikroprosessori kokonaishinnan juuri kohoamatta.

Nykyään bluetooth-laitteita käytetään mm. matkapuhelimien ja kuulokemikrofonien toisiinsa kytkemisessä sekä korvaamassa tietokoneiden johdotuksia. Toisena sovellusalueena on pidetty kotiautomaatiota missä näköyhteydet ovat rajalliset. Bluetooth-laitteet ovatkin juuri parhaimmillaan laitteissa, jotka kestävät vähän virran kulutusta ja ovat kooltansa pieniä.

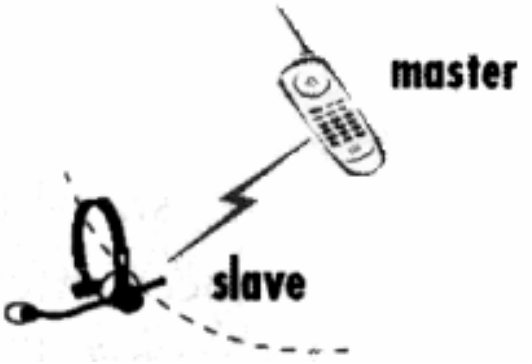
3 VERKKOTOPOLOGIA

Bluetoothin verkkotopologia perustuu täysin niin sanottuun isäntä–renki-periaatteeseen. Pikoverkossa yksi laite on aina isännän roolissa ja muut laitteet saavat sitten osaksensa rengin roolin. Itse asiassa isännän roolissa oleva laite ei eroa mitenkään muista laitteista, ainoastaan on kysymyksessä laitteiden toisilleen asettamat roolit. / 1, s.289 /

Bluetooth tukee kolmea erilaista yhteyttä: *suoraa yhteyttä, pisteestä pisteeseen –yhteyttä* (*Point to Point*) ja *yhdestä pisteestä moneen pisteeseen* -yhteyttä (*Poin –to Multipoint*). / 2, s.18 /

3.1 Suora yhteys

Tämä yhteystyyppi sopii ainoastaan silloin, kun tiedetään, että halutaan luoda yhteys tiettyjen laitteiden välille. Yksi parhaimmista käyttötarkoituksista tämänlaiselle yhteydelle on esimerkiksi matkapuhelimen ja kuulokemikrofonin välinen yhteys. Suoraa yhteystyyppiä käytetään ehkä harvemmin. Aika useasti tämäntyyliset yhteydet tehdään pisteestä pisteeseen -yhteydellä.



Kuva 1. Suora yhteys. / 2 /

3.2 Pisteestä pisteeseen -yhteys (*Poin to Point*)

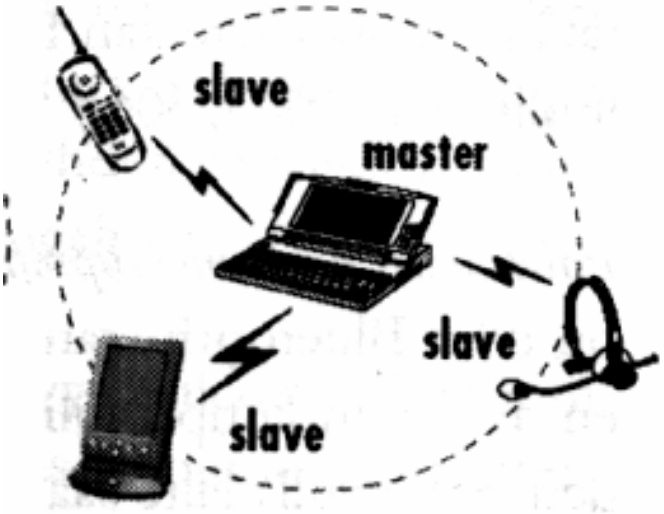
Pisteestä pisteeseen -yhteyttä käytetään kahden laitteen liittämisessä toisiinsa, ja nyt liitettävät laitteet voivat olla ihan satunnaisia. Pisteestä pisteeseen -yhteys ei ole läheskään niin rajoitettu kuin suora yhteys. Tämä yhteystyyppi on ehkä käytetyin. Tätä yhteystapaa kutsutaan ad-hoc -yhteydeksi, koska yhteys muodostetaan ilman kiinteätä verkkoinfrastruktuuria. / 2, s.18 /

Kuva 2. Pisteestä pisteeseen –yhteys *(ad hoc*) / 2 /

Kappaleessa 3.4 keskitytään hiukan tarkemmin ad–hoc verkon toiminnan pääkohtiin.

3.3 Yhdestä pisteestä moneen pisteeseen -yhteys (*Point to Multipoint*)

Yhdestä pisteestä moneen pisteeseen -yhteydessä voidaan liittää nimensä mukaisesti useita laitteita toisiinsa. Näitä verkkoja voidaan kutsua henkilökohtaisiksi verkoiksi (pan, *personal area networks*) tai pikoverkoiksi (*piconet*). Käytän tässä työssäni mieluummin pikoverkko-nimikettä.



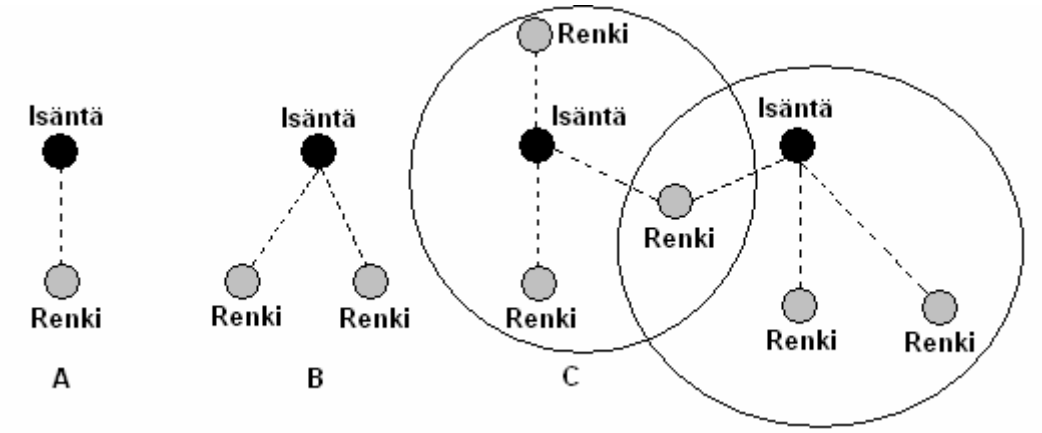
Kuva 3. Yhdestä pisteestä moneen pisteeseen –yhteys. / 2 /

Pikoverkko on hyvin pieni verkko, jonka käyttäjämäärä on rajattu 2 – 8 aktiiviseen käyttäjään ja 256 passiiviseen käyttäjään. Tilanne on sellainen, että pikoverkossa on yksi isäntälaite ja enintään 7 aktiivista renkilaitetta. Lisäksi verkossa ovat passiiviset renkilaitteet, jotka eivät saa käyttää kanavaa, mutta ovat synkronoituneita isäntälaitteen mukaan. Laite, joka ensimmäisenä liittyy verkkoon, saa isäntälaitteen aseman (*master*). Kaikki muut laitteet, jotka tämän jälkeen liittyvät verkkoon, saavat renkilaitteen aseman (*slave*). Kaikki renkilaitteet ovat samassa asemassa toisiinsa nähden. / 3, s.80 ; 1, s.290 /

Bluetooth-laitteilla on oma 48-bittinen osoitteensa. Kyseisen osoitteen on laitteen valmistaja yksilöinyt kaikille bluetooth-laitteille. Tämän avulla bluetooth-laitteet löytävät toisensa. Aina on tietysti poikkeuksia, jos esim. on kyseessä laite, jota ei ole standardoitu tai muuten tehty yhteensopivaksi muiden bluetooth-laitteiden kanssa. / 2, s.19 /

Pikoverkossa kaikilla laitteilla on sama tiedonsiirtokanava, jonka toiminta perustuu siihen, että yksi lähettää ja kaksi tai useampi vastaanottaa. Isäntälaite hallitsee koko verkkoa ja siitä syystä sen kelloa ja taajuushyppelyä käytetään muiden laitteiden synkronointiin. Silloin kun synkronoidaan, passiiviset ja aktiiviset renkilaitteet omaksuvat isäntälaitteen taajuus- ja aikaparametrit. Yksi isäntälaitteen tehtävistä on

myös ohjata tiedonsiirtoa, joten renkilaitteet joutuvat kysymään lupaa tiedonsiirtoon. Isäntälaite pystyy muuttamaan passiivisen renkilaitteen aktiiviseksi ja toisinpäin. Lisäksi isäntälaitteen ja renkilaitteen roolit on aina mahdollista vaihtaa. (*master slave switch*). / 3, s.80 /



Kuva 4. Kolme erilaista pikoverkon toimintamuotoa. / 9 /

Pikoverkolla on kolme erilaista toimintamuotoa (kuva 4). Ensimmäisessä tapauksessa (kohta A) verkon alueella on vain kaksi erillistä laitetta (*single slave operation*). Toisessa tapauksessa (kohta B) on kyseessä verkko, jossa on enemmän kuin yksi renkilaite (*multi slave operation*). Viimeisessä tapauksessa (kohta C) on kaksi pikoverkkoa, jotka yhdistyvät yhdeksi verkoksi yhden renkilaitteen kautta. Tätä kutsutaan hajaverkoksi (*scatternet operation*).

Silloin kun muutamasta pikoverkosta on yhdistetty hajaverkko, jokaisella pikoverkolla on oma isäntälaitteensa. Ainoastaan yksi laite kulkee näiden verkkojen välissä yhdyskäytävänä. Verkkojen välissä oleva laite voi olla renkilaitteena molemmissa verkoissa tai isäntälaitteena toisessa ja renkilaitteena toisessa verkossa. Tämä yhdyskäytävä ei ole jatkuvatoimisesti kaksisuuntainen, vaan tämä laite keskustelee kerrallaan vain toiselle osapuolelle.

3.4 Ad-hoc -verkko

Bluetooth tekniikassa pisteestä pisteeseen yhteys käyttää ad–hoc verkko tekniikkaa, mutta sitä käytetään ainoastaan kahden erillisen laitteen muodostaessa yhteyttä. Siitä syystä laitan tähän päättötyöhöni vain muutaman pääkohdan kyseisestä tekniikasta.

Ad-hoc -verkko on rakenteeton verkko, joka muodostuu siirrettävistä päätelaitteista, jotka keskustelevat keskenään. Tällaisella verkolla viitataan siihen, että laitteita syntyy sekä katoaa jatkuvasti. Ad-hoc verkko ei perustu kiinteisiin rakennelmiin, eikä verkoissa ole tukiasemia tai tiedonsiirtopalveluita. Kaikki laitteet tekevät samat toiminnot eli toimivat päätelaitteena ja reitittäjinä.
Reititystoiminto on silloin käytössä, kun kaksi laitetta on keskenään yhteydessä, mutta kumpikaan laite ei ole toistensa toiminta-alueella. Silloin välissä olevat laitteet joutuvat reitittämään liikennettä. / 9 /

Bluetooth tukee tätä verkkotekniikkaa baseband tasolla ja tämän vuoksi osaavat tyhmemmätkin bluetooth-laitteet suoraan etsiä toisia laitteita ja avata uusia yhteyksiä.
Bluetoothin palveluista inquiry on hyödyllinen ad hoc -verkotukselle, koska sen palvelun avulla pystytään etsimään tai kartoittamaan kuulolla olevia laitteita.

Tämäntapaisissa tekniikoissa yleensä tietoturva perustuu avaimien levittämiseen ja autentikoimiseen. Toisaalta pakettikokojen kasvaminen hidastuttaa protokollien toimintaa. / 9 /

4 TIEDONSIIRRON TEKNIIKKA

4.1 Bluetoothin taajuuskaista

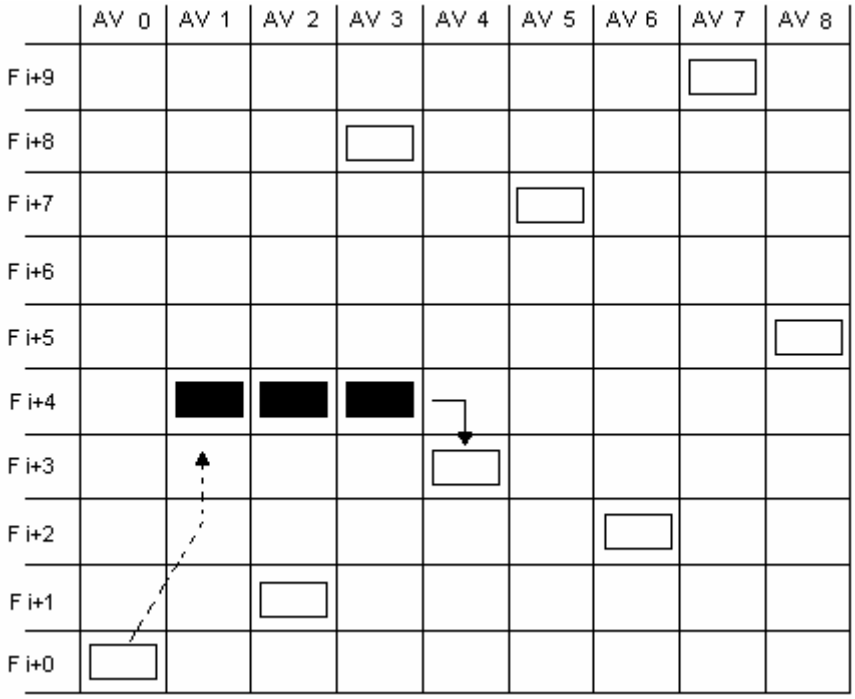
Bluetooth verkko toimii 2,4 gigahertsin (GHz) taajuudella. Tämä taajuusalue vaihtelee hieman eri maanosien ja maiden välillä. Poikkeuksena ovat muutamat maat, kuten Ranska ja Espanja. Tämä taajuusalue kuuluu maailmanlaajuisesti vapaasti käytettävään ja ilmaiseen kaupan, teollisuuden sekä tieteen käyttöön varattuun IMS-taajuuksiin (*Indrustial Medical and Scienfic*). Kun käytämme tätä taajuusaluetta, olemme varmoja siitä, että se on vapaa ympäri maailmaa ja parantaa yhteensopivuutta bluetoothin käytössä. Ilman yhdenmukaista taajuusaluetta bluetooth olisikin jo ollut alkuvaiheissaan vaillinainen. Täysin ongelmaton ei ole tämänkään taajuusalueen käyttö. Pitää muistaa, että taajuusalueella on monia muitakin käyttäjiä. Ehkä merkittävin taajuusalueen käyttäjistä on wlan, mutta myös mikroaaltouunit, murto- ja palohälyttimet, sisäpuhelimet sekä monet muut samantapaiset laitteet on syytä muistaa. Näiden laitteiden yhtäaikainen käyttö luo siirtotielle häiriöitä. Tiedonsiirron suunnitteluvaiheesta alkaen on pyritty jo estämään tämäntyyppiset häiriöt, ja esim. tiedonsiirto on suunniteltu taajuushyppelytekniikalla jne. / 3, s.3 ; 1, s.292 /

ISM-alue alkaa 2400 megahertsistä (MHz) ja loppuu 2483,5 megahertsiin (MHz). Näin ollen ISM-alueen laajuudeksi jää 83,5 megahertsiä (MHz). Poikkeuksellinen alue on Ranskassa 2446,5 – 2483,5 megahertsiä (MHz) ja Espanjassa 2445 – 2475 megahertsiä (MHz). Alue on jaettu 79 kanavaan (23 kanavaan Ranskassa ja Espanjassa) ja jokaisen kanavan väli on 1 megahertsi (MHz). Lähettäminen tapahtuu 2402 – 2480 megahertsin (MHz) välillä.

4.2 Taajuushyppelytekniikka (FHSS, *frequency-hopping, spread-spectrum*).

Taajuushyppelyyn perustuvat tekniikat on alkujaan suunniteltu 1970-luvun sotilaskäyttöön. Ne olivat siihen omiaan, koska niiden avulla saatiin salakuuntelutoiminta ja taajuuksien häiritseminen vaikeaksi. IMS–alueen laitteissa tämä tekniikka on laajalti käytössä, koska useat laitteet toimivat samalla taajuusalueella ja keskinäisiä häiriöitä on paljon ilmassa. Taajuushyppelytekniikka sietääkin kohtuullisen hyvin kaikenlaista häiriötä. / 11 /

Useimmissa maissa käytetään 79 taajuuskaistaa (Ranska ja Espanja käyttävät 23 kaistaa). Yhden aikavälin pituus on $625\,\mu s$ ja näin saamme hyppelytaajuudeksi 1600 hyppyä sekunnissa. Taajuushyppelyn yhtä aikaväliä ei voida käyttää kokonaan lähettämiseen, koska radiolaite käyttää tietyn ajan, ennen kuin se asettuu oikealle taajuudelle. Radiolaitteiden asettumiseen aikaa kuluu noin 220 μs ja tätä kutsunaan niin sanotuksi suoja-ajaksi. Tästä huomaamme, että suoja-aika on noin yhden kolmanneksen niin sanotusta kokonaisajasta. / 1, s.294 /



Kuva 5. Aikavälien muutokset taajuushyppelyssä. / 1 /

Kuvasta 5. huomaamme, että kun lähetettävä paketti on yhtä aikaväliä suurempi, niin tämä paketti lähetetään useammassa aikavälissä samalla taajuudella. Taajuushyppely jatkuu tämän jälkeen samalle taajuudelle, johon se olisikin mennyt, jos paketti olisi ollut vain yhden aikavälin. Muut laitteet, jotka eivät lähetä tai vastaanota mitään taajuushyppelevät tämän aikaa annetun kaavan mukaisesti. Voimme pitää tätä jonkinlaisena bluetooth-verkon erikoisuutena.

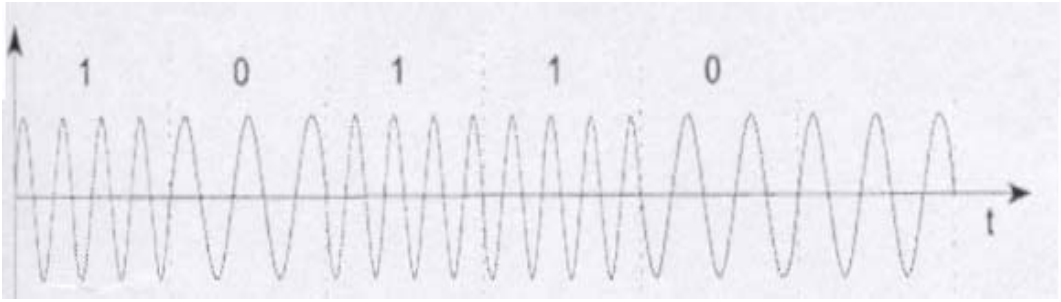
Jos lähetettäessä ilmenisi siirtotiellä häiriötä tietyillä kanavilla tai muuten ei saataisi signaalia menemään perille virheettömästi, silloin suoritetaan uudelleen lähetys, mutta kuitenkin eri kanavilla, eli siis eri taajuuksilla. Jos lähetämme paketteja taajuushyppelytekniikkaa hyväksikäyttäen, jokainen paketti menee eri taajuudella, joten on erittäin epätodennäköistä, että häiriöisessä siirtotiessä menettäisimme kaikki lähettämämme paketit. Todennäköisesti häviäisi paketteja ainoastaan satunnaisesti, ja nämäkin saisimme uudelleenlähetyksen kautta paikattua. Tähän juuri perustuu taajuushyppelytekniikan häiriöiden sietokyky. Bluetoothissa käytettävä pakettien koko on paljon pienempi ja hyppelyssä käytettävä nopeus paljon suurempi kuin yleensä käytetyissä muissa taajuushyppelyyn perustuvissa järjestelmissä. / 3, s.75 /

4.3 Modulaatio

Moduloinnissa lähetettä muokataan lähetyksen ja siirron kannalta entistä parempaan muotoon. Modulaatiossa muutetaan tarkoituksella tunnetun aaltomuodon eli kantoaallon, jotakin tiettyä ominaisuutta.
Esimerkiksi lähetyksen tapahtuessa antennin kautta, antennin pitää vähintäänkin olla 1/10 siirrettävän signaalin aallonpituudesta. Tästä seuraisi, että pienillä taajuuksilla antenni olisi tavattoman isokokoinen. Vältymme tältä, kun siirrämme kantataajuisen signaalin entistä korkeampaan taajuuteen, moduloimalle sen kantoaallon kanssa ja lähettämällä sitten eteenpäin. Jos moduloimme signaalin eri kantoaaltoihin, niin voimme lähettää useita lähetteitä samanaikaisesti ja samassa siirtovälineessä.

4.3.1 FSK-modulaatio

FSK (*Frequency Shift Keying*) on modulaatio, jossa käytetään kahta eri kantoaallon taajuutta, eli tässä modulaatiossa taajuus muuttuu sen mukaan, onko kysessä 1- vai 0-bitti. Kuvasta 6. huomaamme, kun kyseessä on 1-bitti, taajuus pysyy korkeampana, kuin muuttuessaan 0-bitiksi. / 7, s.1 /

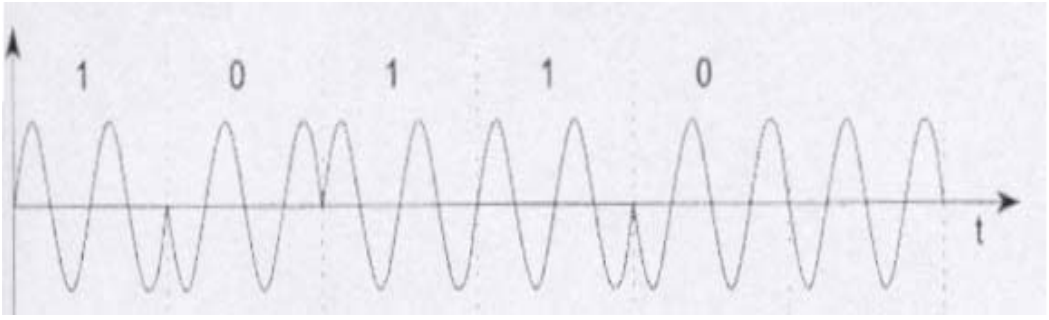


Kuva 6. FSK-modulaatio. / 7 /

Bluetoothissa 1-bitti ilmaistaan taajuudella, joka on 140 – 175 kilohertsiä (KHz) kanavan keskitaajuuden yläpuolella, ja 0-bitin taajuus on saman verran keskitaajuuden alapuolella. / 1, s.292 /

4.3.2 PSK-modulaatio

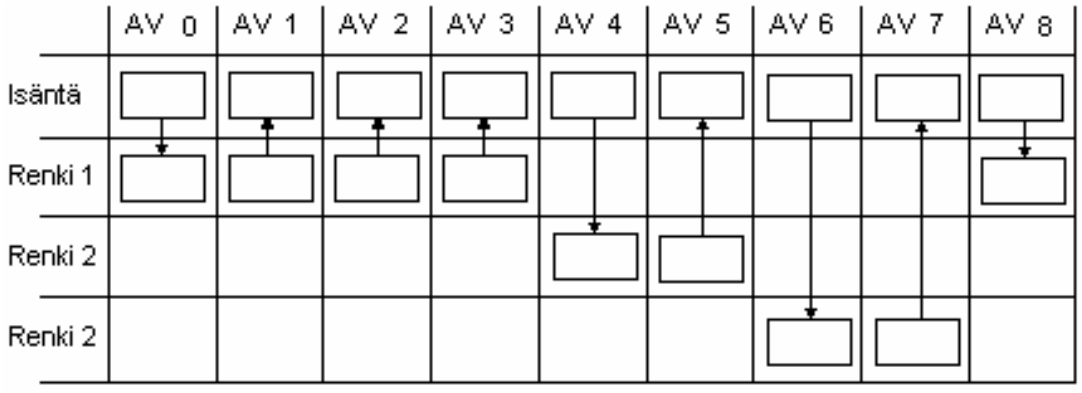
PSK-modulaatiossa (*Phase Shift Keying*) käytetään muuttuvana tekijänä vaihekulman muutosta. Vaihekulma muuttuu +180 astetta silloin, kun muuttuu bitti. Tämän huomaamme kuvasta 7. / 7, s.1 /



Kuva 7. PSK-modulaatio. / 7 /

4.4 Kanavanvaraus

Radiotiellä paketteja siirretään aikaväleissä 1600 kertaa sekunnissa ja näiden aikavälien keston pituus on $625\,\mu s$, johon sisältyy $220\,\mu s$:n suoja-aika. Yhtä aikaväliä kutsutaan kanavaksi. Aikaväleissä paketteja siirretään kumpaankin suuntaan (*half duplex*). Tarkoittaen sitä, että kanavalla vaihdetaan siirtosuuntaa sen mukaan kun vuoro siirtyy osapuolelta toiselle. Tämän toiminnan nimitys on TDD (*Time Dividion Duplex*). Kaikki purskeet lähetetään omissa aikaväleissään. Jos lähetettävä purske on liian iso yhteen aikaväliin, niin sitä jatketaan seuraavalle aikavälille taajuuden pysyessä samana. Yhden purskeen suurin mahdollinen kesto on viisi aikaväliä. Tämän voit todeta kuvasta 8. Pikoverkoissa isäntälaitteen ja renkilaitteen välissä toimii vuorottelumekanismi. Tämän tarkoituksena on säädellä lähetystä siten, että isäntälaite lähettää parillisilla aikaväleillä ja renkilaite vastaa tähän parittomilla aikaväleillä. Siitä syystä lähetteiden pituudet voivat olla ainoastaan 1,3 tai 5 aikaväliä. Jos käyttäisimme esimerkiksi neljän aikavälin lähetystä, jäisi väliin yksi aikaväli käyttämättä, koska vastaanottaja joutuisi odottamaan seuraavaan parilliseen tai parittomaan aikaväliin, jotta pääsisi vastaamaan. Tästä asiasta saa parhaiten mielikuvan katsomalla kuvaa 8.



Kuva 8. Kanavanvarauksen aikavälien käyttäminen. / 1 /

4.5 Kanavat

Kanavointi bluetoothissa perustuu kahteen erilaiseen kanavaan. Voidaankin sanoa, että puheliikenteelle on tarkoitettu synkroninen lähetys (SCO) ja dataliikenteelle vastaavasti paremmin soveltuu asynkroninen lähetys (ACL).

4.5.1 Synkroninen yhteys (SCO)

Synkroninen yhteys on tarkoitettu jatkuvan ja tasaisen bittivirran lähetykseen. Voidaankin sanoa, että synkroninen lähetys on yhteydellinen eli piirikytkentäinen. Yleisin tämän tyypin käyttötarkoitus on puheen siirto, koska puhe on aina sidottu aikaan.

käytettäessä synkronista yhteyttä, osapuolille annetaan siirtoaikaa aina säännöllisin väliajoin. Se miten siirtoaikaa annetaan, sovitaan aina, kun yhteyttä ruvetaan muodostamaan. Renkilaite joutuu vielä odottamaan isäntälaitteelta tulevaa kyselyä ennen kuin se voi alkaa lähettämään mitään isäntälaitteelle. Synkroninen yhteys on aina kaksisuuntainen. Aina kun isäntälaite lähettää renkilaitteelle päin, se samalla pyytää renkilaitteen lähettämään isäntälaitteelle päin ja toisinpäin. Synkronisessa yhteydessä renkilaite tietää aina, koska sen pitäisi lähettää. Joskus sattuu tietysti niitäkin tapauksia, että isäntälaitteelta tuleva kysely jää matkalle. Silloin renkilaitteella on oikeus lähettää sille määrätylle aikavälille.

Isäntälaite voi maksimissaan tukea kolmea synkronista yhteyttä, joko samalle laitteelle tai eri laitteille. Vastaavasti taas renkilaite voi maksimissaan tukea kolmea synkronista yhteyttä yhdelle isäntälaitteelle tai kahta eri synkronista yhteyttä kahdelle eri isäntälaitteelle.

Synkronisen äänikanavan nopeus on likimain sama kuin digitaalisessa puhelinverkossa eli 64 kb/s. Yhteyksien nopeudet voi nähdä myös taulukosta 1.

/ 1, s.295 ; 9 ; 3, s76 /

4.5.2 Asynkroninen yhteys (ACL)

Asynkroninen yhteys on tarkoitettu purskeisen bittivirran lähetykseen. Voidaankin sanoa, että asynkroninen lähetys on yhteydetön eli pakettikytkentäinen. Siitä syystä tämä yhteys sopii parhaiten datansiirtoon, koska sitä ei ole sidottu mitenkään aikaan.

Asynkronista kanavaa käytetään silloin, kun ei tarvitse käyttää samaan aikaan synkronista kanavaa. Asynkronisessa yhteydessä käytetään kiertokyselymenetelmää (*polling*). Tämä toteutetaan siten, että isäntälaite lähettää renkilaitteille data- tai kyselysanomia ja renkilaitteet vastailevat näihin. Silloin kun isäntälaitteelta lähtevä kyselysanoma ei tule renkilaitteelle asti tai renkilaite ei jostain syystä pysty tulkitsemaan sitä, niin se ei saa lähettää mitään tietoa verkossa.
Koska verkossa voi olla muitakin laitteita, jokin toinen laite voi löytää osoitteensa tästä sanomasta. Tämä siis toimii juuri vastakkaisella tavalla, kuin synkronisessa yhteydessä, koska synkronisessa yhteydessä on aina tiedossa aikaväli, jolla lähetetään. Taas asynkronisessa yhteydessä ei ole entuudestaan tiedossa, millä aikavälillä lähetetään. Asynkronisessa yhteydessä isäntälaite voi lähettää myös levitysviestin kaikille verkossa oleville laitteille, silloin käytetään lähetettäessä isäntälaitteen osoitetta 0.
Asynkroninen yhteys on maksimissaan 723 kb/s datansiirtoa yhteen suuntaan ja sen lisäksi jää vielä 57 kb/s dataväylä paluusuuntaan. Symmetrisenä siirtona saamme liikkumaan dataa 434 kb/s molempiin suuntiin. Nämä nopeudet näkyvät myös taulukosta 1. / 1, s.295 ; 9 ; 3, s.76 /

Kanava tyyppi	Konfiguraatio	Maksimisiirtonopeus ylävirtaan	Maksimisiirtonopeus alavirtaan
Synkroninen yhteys	3 samanaikaista puhekanavaa	64 kb/s * 3 kanavaa	64 kb/s *3 kanavaa
Asynkroninen yhteys	Symmetrinen data	434 kb/s	434 kb/s
	Asymmetrinen data	723 kb/s tai 57 kb/s	57 kb/s tai 723 kb/s

Taulukko 1. Kanavien siirtonopeudet.

Taulukosta 1. näemme, etteivät siirtonopeudet ole kovin lähellä teoreettista yhden megabitin siirtonopeutta. Lähimpänä tätä nopeutta on asymmetrinen datansiirto, kun ylempien kerrosten protokollat otetaan huomioon, niin nopeus laskee alle 700kb/s.

4.6 Teholuokat

Yleisin versio bluetoothista toimii 10 metrin toimintasäteellä, mutta toimintasädettä on mahdollista kasvattaa aina 100 metriin asti. Toimintasäteen pituus on suoraan verrattavissa siihen, kuinka suuri on laitteen lähetysteho. Mitä suuremmilla lähetystehoilla lähetetään, sitä pidemmäksi toimintasäde kasvaa. Käytettäessä isoa lähetystehoa, on myös otettava huomioon suuret häiriösäteilyt muualle ympäristöön. Lisäksi lähetystehojen kasvaessa laitteiden vaatimukset kasvavat, esimerkiksi sirun koko kasvaa, ja mitä todennäköisimmin myös hinta nousee sen mukana. Lähetysteho vaikuttaa myös virrankulutukseen. Bluetoothin lähetystehot näkyvät taulukosta 2.

Käytettäessä pieniä akullisia laitteita siitä seuraa, että suositaan pienikulutuksellisia tekniikoita. Vielä kun ajatellaan, että bluetoothia pyritään tekemään mahdollisimman halvalla sekä massatuotannossa mahdollisimman yksinkertaisesti, ei tule yllätyksenä toimintasäteen ja teholuokan pysyminen pienenä. Olihan bluetooth tarkoitus istuttaa kaikkiin laitteisiin, joissa on mikroprosessori ilman, että kokonaishinta nousee. / 3, s.72 /

Teholuokka	Kantama	Suurin teho	Pienin teho	Tehonsäätö
1	100m	100mW	1mW	pakollinen
2	10m	2,5mW	1mW	ei pakollinen
3	10m	1mW	1mW	ei pakollinen

Taulukko 2. Bluetoothin lähetysteholuokat. / 1, s.293 /

4.7 virheenkorjaus

Tiedonsiirto on aina silloin turhaa, jos sanomat eivät tule perille tai ovat vääristyneet matkalla. Bluetoothissa on kolme erilaista virheiden korjausmenetelmää, joilla varmistetaan tiedonsiirto. Virheenkorjausmenetelmiä ovat kolminkertainen toistokoodi (*1/3 – FEC*), (*15,10*) lyhennetty Hamming-koodi ja ARQ-kaava. Näistä kahdella ensimmäisellä menetelmällä virhe korjataan etukäteen ja kolmas perustuu automaattiseen uudelleenlähetysmekanismiin.

4.7.1 1/3 FEC-korjaus

Kolminkertainen toistokoodi perustuu siihen, että se korjaa yhden virheellisen bitin kolmesta. Jos ajattelemme tiedon sisältävän bitit $b_0 b_1 b_2 .....b_n$, tällöin ne muodostuvat linjalle näin $b_0 b_0 b_0 b_1 b_1 b_1 b_2 b_2 b_2 .....b_n b_n b_n$. Kuten huomaamme, tämä on erittäin yksinkertainen tapa suojautua siirtovirheiltä ja se suojaakin ainoastaan pieniltä siirtovirheiltä. Yleisesti virheet tulevat purskeissa ja suurin virhemäärä, joka tämäntyyppisellä korjausmenetelmällä voidaan korjata, on kahden bitin mittainen. Tämäkin on mahdollista vain silloin, jos virheet sattuvat osumaan kahden databitin väliin, muuten menetetään kyseinen lähetetty data. / 1, s. 303 /

4.7.2 2/3 FEC-korjaus

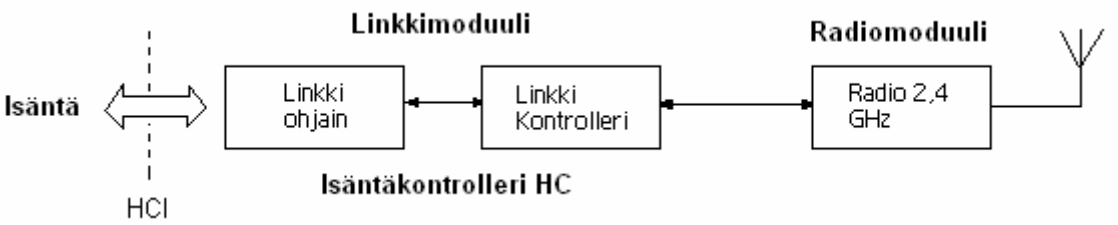
2/3 FEC-korjaus on menetelmä, joka perustuu Hamming-koodaukseen (*15,10*). Hamming-koodauksessa 10 bitistä tuotetaan 15 bittiä ja se tehdään LFRS-rekisterissä. LFRS-rekisterissä nämä 15 bittiä tuotetaan polynomin $G(x) = x5 + x4 + x + 1$ mukaisesti. Kyseisellä virheenkorjausmenetelmällä pystytään korjaamaan yhden bitin virheet ja havaitsemaan kahden bitin virheet. Silloin kun kaksi bittiä on vääristynyt, mutta emme pysty korjaamaan niitä,

suosituksen mukaan poistetaan korjausbitit ja databitit käytetään sellaisenaan. Tässäkin virheenkorjauksessa on ongelmana virheiden purskeisuus ja näin ollen purskeisissa virheissä todennäköisesti menetetään lähetetty data. / 1, s. 303 /

4.7.3 ARQ-korjaus

ARQ tulee sanoista *Automatic Repeat Reguest* ja nimensä mukaisesti kyseessä on virheenkorjaus, jossa tarkisteella suojataan siirrettävä sanoma. Bluetooth käyttää CRC-periaatetta (*Cyclic Redundance Check*). CRC-periaatteessa käytetään jakojäännöslaskentaa ja siirrettävä sanoma jaetaan tietyillä polynomeilla. Jakojäännös liitetään tarkisteeksi sanoman perään. Kyseistä tarkistetta kutsutaan myös FCS:ksi (*Frame Check Sequency*). Jos ARQ korjauksessa havaittu virhe korjataan, niin virheellinen sanoma pyydetään uudestaan palauttamalla negatiivinen kuittaus sanoman lähettäjälle. Bluetoothissa on vain yksi bitti sanomien numerointia varten. Siten tämän johdosta negatiivinen kuittaus on lähetettävä välittömästi lähettäjälle. Bluetoothin suojauskenttä on 8-bittinen ja tämä lasketaan polynomilla $G(x) = x^8 + x^7 + x^5 + x^2 + x + 1$. Jos hyötykuorma jaetaan CRC-tarkisteella, niin jakajapolynomi on $G(x) = x^{16} + x^{12} + x^5 + 1$. / 1, s. 304 /

5 FYYSISET OSAT



Kuva 9. Bluetooth-järjestelmän radio- ja linkkimoduuli. / 9 /

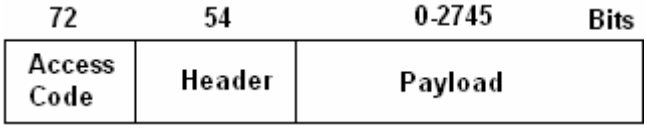
Ei ole aivan sanomatta selvää, mitkä osat bluetooth-laitteissa on muodostettu ohjelmistotasolla ja mikä on laitteistoina. SIG-järjestö ei määrittele mitenkään kyseistä asiaa, vaan jokaisen yrityksen on annettu luoda omat toimintakenttänsä tämän asian suhteen. Kuitenkin bluetooth-järjestelmä voidaan jakaa karkeasti kahteen eri toiminnalliseen osaan, radiomoduuliin ja linkkikontrolleriin. Asiaa on paremmin selvittämässä kuva 9. Linkkikotrollerin kanssa hyvin läheisissä tekemisissä on ohjelmistopohjainen linkkiohjain LM (*Link Manager*). Linkkikontrolleri ja linkkiohjain ovat eri sovelluksissa liitettyinä toisiinsa, mitä erinäisin tavoin, jonka johdosta näitä kutsutaan yhteisellä nimellä isäntäkontrolleriksi HC (*Host Controller*)./ 9 /

Radiomoduuli vastaa lähettämisestä, vastaanottamisesta ja kaikesta muusta radiotiellä tapahtuvasta tiedonsiirtämisestä. Radio toimii 2,4 GHz IMS-alueella, tarkemmat tiedot löytyvät kappaleessa 4.1.
Linkkikontrolleri prosessoi kantataajuussignaalia ja kontrolloi fyysisen tason koodausta. Linkkikontrolleri käyttää hyväkseen linkkiohjainprotokollaa LMP (*Link Manager Protocol*).
Linkkiohjaimen tehtävä on vastata erilaisista protokollista. Kyseisessä tapauksessa vastuualueena ovat kantataajuus protokollat ja muut alhaisen linkkitason toiminnot. Toimintoihin kuuluvat datan lähetys, vastaanotto, yhteyksien luominen, virheiden havaitseminen ja korjaaminen, datan valkaisu (*Data Whitening*), tehon säätely ja autentikointi. Linkkiohjain on LMP:n kautta yhteydessä muihin verkon linkkiohjaimiin.

6 BLUETOOTHIN SANOMAT

6.1 Bluetoothin perussanoman rakenne

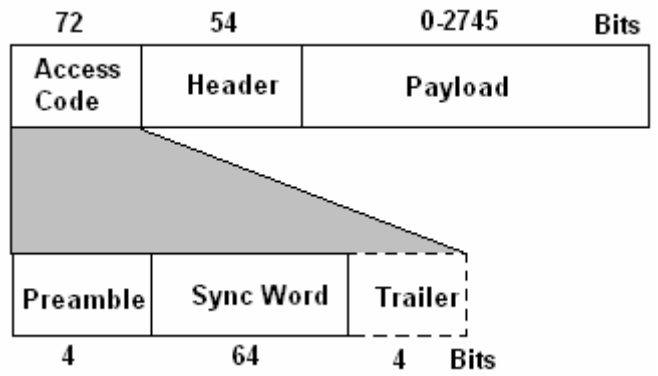
Bluetoothin-spesifikaatiossa on määritetty käytettäväksi kahta erilaista pakettityyppiä SCO (Synkroninen yhteys) ja ACL (Asynkroninen yhteys). SCO paketit käyttävät synkronoitua yhteyttä ääntä varten ja reitittävät synkronoitua I/O ääni porttia. Virheen tarkistamista ja uudelleen lähettämistä ei voida tehdä, koska viiveen lisääntyminen huonontaisi puheen laatua.
ACL paketeissa käytetään asynkronoitua linkkiä. Sanomien välityksessä pystytään käyttämään käyttäjien datatietoja tai hallintalaitteiden datatietoja. Asynkronisessa yhteydessä ei lähetyksissä tapahtuvilla viiveillä ole merkitystä. / 6, s.77 /



Kuva 10. Bluetooth sanoman perusrakenne. / 6, s.78 /

Kuvassa 10. on esitetty bluetoothin perussanoma. Bluetooth perussanomassa on 72-bittinen AC (*Access Code*), 54-bittinen otsikko (*Header*) ja hyötykuorma (*Payload*), joka vaihtelee 0 – 2745 bitin välissä. Liitteestä 1 voi nähdä kokonaiskuvan, kuinka bluetoothin perussanomat jakautuvat eriasteisiin alaluokkiinsa.

6.1.1 72-bittinen AC-koodi (*Access Code*)



Kuva 11. Access code:n alaluokat. / 6, s.78 /

Kuvassa 11. on esitetty 72-bittinen access code ja sen käyttämät kolme eri alaluokkaa. Ensimmäinen alaluokka muodostuu neljän bitin mittaisesta alkutahdistuksesta (*Preamble*), 64-bitin mittaisesta synkronointikentästä (*Sync Word*) ja neljästä häntäbitistä (*Trailer*).

Alkutahdistuksen tehtävänä on esittää vastaanottajalle, että paketit ovat saapuneet perille. Alkutahdistuksessa käytetään kahta eri neljän bitin sarjaa. Bitit ovat 1010 tai 0101, sen mukaan alkaako synkronointikenttä 1-bitillä vai 0-bitillä. Kyseisellä toiminnolla pyritään poistamaan tasavirtakomponentti vastaanotosta. Samasta syystä neljä häntäbittiä muodostetaan samalla tavalla. Häntäbittien sarjoja muodostaessa ratkaisevana tekijänä käytetään synkronointikentän viimeistä bittiä. Synkronointikenttää käytetään vastaanottajan ajoituksen kohdalleen synkronointiin. Vastaanottaja käyttää synkronointiin koko 64-bitin mittaisen jaksonsa ja tämän tuloksena syntyy hyvin toimiva signalointi mekanismi. Perässä olevilla neljällä häntäbitillä pystytään erottamaan otsikkokenttä ja AC-kenttä toisistaan. / 6, s.78 /

On kolme toiminnaltaan erilaista AC:a. Koodien ominaisuudet eroavat toisistaan sen mukaan, missä tilassa bluetooth-laitetta käytetään.

Channel Access Code (CAC)

CAC tunnistaa pikoverkon ja tämän kautta kaikki pikoverkon sisällä tapahtuvat kanavan vaihdot. Kaikki paketit lähetetään samassa pikoverkossa aloittaen samalla CAC:llä.

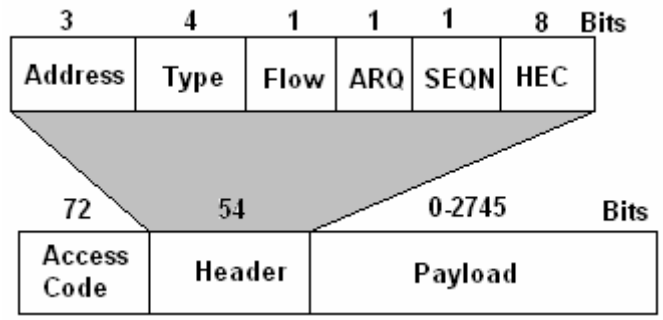
Decice Access Code (DAC)

DAC käyttää erikoista kyselymenettelyä yhteyksien luomisessa ja kuittaamisessa. Kyselyt sekoitetaan lähetettäessä sarja viesteiksi, joilla saadaan eri aktiivisten yksiköiden välille asetettua siirtotietä varten vaadittavat asetukset. Muiden yksiköiden vastatessa näihin kutsuihin, saadaan radiotien asetukset asetettua kohdalleen.

Inqyiry Access Code (IAC)

IAC:a on kahdenlaisia, yleisiä ja omistautuneita. Yleinen IAC on käytössä kaikissa laitteissa ja sitä käytetään mm. muiden laitteiden havaitsemiseen toiminta-alueella. Omistautuneessa IAC:ssa ennalta määrätyn ryhmän kesken jaetaan tietty ominaisuus. Ryhmän pitää tietenkin löytyä toiminta-alueen sisältä. / 6, s.78 /

6.1.2 54-bittinen otsikkokenttä (*Header*)



Kuva 12. Otsikkokentän alaluokat. / 6, s.79 /

Kuvassa 12. on esitelty 54-bittinen otsikkokenttä (*Header*), joka on jaettu kuuteen eri alaluokkaan. Otsikkokenttää käytetään sanoman vastaanotossa ja kaikenlaisessa muussa tunnistamisessa. Otsikkokenttää käytetään vuonohjauksessa, kuittauksissa ja kun halutaan erilaisia järjestysnumerollisia tietoja. / 6, s.79 /

Adress

Adress-kentän pituus on kolme bittiä ja kentän tarkoituksena on yksilöidä vastaanottaja. Pikoverkkoa käytettäessä adress-kenttää käytetään tilapäisenä osoitteena, jokaiselle aktiiviselle laitteelle. Pikoverkossa ollessa osoitteella

tunnistetaan laiteet verkossa. Laitteen kytkeytyessä irti, täytyy sen luovuttaa osoitteensa isäntälaitteelle, joka jakaa sitä taas seuraavalle kytkeytyvälle laitteelle. / 6, s.79 /

Type

Type on neljän bitin mittainen tyyppitietokenttä. Kentän tehtävänä on kertoa, minkälaisesta sanomasta on kysymys. Type-kentän avulla erotamme ACL-kanavat SCO-kanavien sanomista ja pystymme erottamaan erityyppiset kanavakohtaiset sanomat toisistaan. Type-kentän yksi tärkeimmistä ominaisuuksista on, että se pystyy tyyppitiedon perusteella päättelemään, kuinka monta aikaväliä vastaanottajan sanoma kestää. / 1, s.297 /

Flow

Flow on yhden bitin mittainen vuonohjauskenttä. Käytettäessä ACL-kanavaa, vuonohjauskentällä viestitetään vastaanottajalle, koska sen puskurit ovat täyttyneet. Puskurien täyttyessä flow-kenttä asetetaan nollaksi ja puskurien ollessa tyhjänä flow arvo on yksi. / 1, s.297 /

ARQN

ARQN on yhden bitin mittainen kenttä, jolla seurataan siirron onnistumisia. Viestitettäessä lähettäjälle siirron onnistumisesta saa ARQN arvon 1 ja se tulkitaan positiiviseksi kuittaukseksi. Viestitettäessä siirron epäonnistumisesta saa ARQN arvon nolla ja se tulkitaan negatiiviseksi kuittaukseksi. Sanoman puuttuminen tulkitaan aina negatiiviseksi kuittaukseksi ja kaksi suuntaisessa liikenteessä sanomat kulkevat datasanomien mukana vastakkaiseen suuntaan kuitattavaan tietoon nähden. / 1, s.297 /

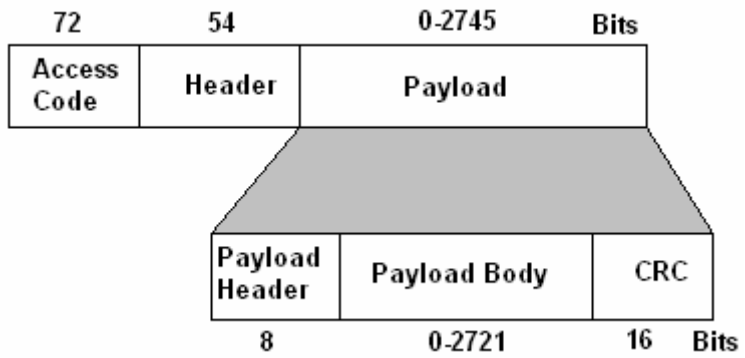
SEQN

SEQN on yhden bitin mittainen kenttä, jonka tehtävänä on numeroida sanomat siirtotielle. Sanomien numeroinnissa ei käytetä, kuin yhden bitin mittaista kenttää, koska jo sillä pystytään havaitsemaan kahdennetut sanomat. Tosin tämä edellyttää käytettäväksi protokollaa, jossa jokaista sanomaa seuraa kuittaus. / 1, s.297 /

HEC

HEC on kahdeksan bitin mittainen CRC-tarkiste, minkä tarkoituksena on tarkistaa pelkkä otsikkokenttä. Pyrkimyksenä on suojata otsikko kentän tietoja, ettei otsikkokenttää tulkittaisi väärin siirtovirheiden takia. Tarkistetta lasketaan jakajapolynomilla $x^8 + x^7 + x^5 + x^2 + x + 1$. / 1, s.297 /

6.1.3 2745-bittinen hyötykuorma kenttä (*Payload*)



Kuva 13. Hyötykuormakentän alaluokat. / 6, s.81 /

Kuvassa 13. on esitelty hyötykuormakenttä (*Payload*), joka on jaettu kolmeen eri alaluokkaan. Hyötykuorman koko on 0 – 2745 bittiä sen mukaan, mitä on lähetettävänä. Hyötykuormakenttiä on kahta erilaista. On (SCO) äänikanavia käyttäviä kenttiä ja (ACL) datakanavia käyttäviä kenttiä. / 6, s.81 /

Payload Header

Ainoastaan data kentässä on Payload Header. Kenttä on kahdeksan bittinen, josta on käytössä yksi tai kaksi tavua. Yksi tavu on aina neljän bitin mittainen. Se toimii kontrolloiden loogisia kanavia ja sitä käytetään hyötykuorman pituuden ilmaisimena. Pituuden ilmaisimena se ilmaisee tavujen määrää. / 6, s.81 /

Payload Body

Payload body-kentän koko on 0 – 2721 sen mukaan mitä on lähetettävänä. Huomaa, että 2721+8+16 = 2745 bittiä. Payload body-kenttä sisältää pelkästään lähetettävän informaation. / 6, s.81 /

CRC

CRC-kentän koko on 16-bittiä. CRC-tarkisteena käytetään 16-bittistä jakojäännöstä. Jakojäännös on aina lähetettävän informaation perässä, jolloin sisään tulevan datan saadessaan, vastaanottaja aloittaa heti sen jakamisen. Vastaanottajan jakojäännöksen ollessa nolla, tiedetään datan tulleen perille oikein. Taas vastaanottajan jakojäännöksen ollessa jotain muuta kuin nolla, nähdään, että siirrossa on tapahtunut virheitä. / 6, s.81 /

6.2 Hallintasanomat

Hallintasanomien mukana ei koskaan siirry käyttäjien dataa ja hallintasanomia on neljää erilaista. Nämä neljä ovat ID, NULL, POLL ja FHS-sanoma.

ID

ID sanoman voi ainoastaan tunnistaa AC-kentän perusteella. ID-sanoma käyttää sekä DAC:a (*Device Access Code*), että IAC:a (*Inqyiry Access Code*). DAC-koodilla toimivaa sanomaa käytetään yhteyden luomisessa ja sen kuittaamisessa. IAC-koodilla toimivaa sanomaa käytetään kaikille laitteille menevänä kyselynä. Tästä on olemassa erilaisia versioita, kuten GIAC (*General IAC*) tai DIAC (*Dedicated IAC*). / 1, s.298 /

NULL

NULL on paremminkin pakettityyppi, kuin sanoma. Sitä käytetään silloin, kun dataa ei ole, mutta jotenkin tulevaa liikennettä on kuitattava. / 1, s.298 /

POLL

POLL on kyselysanoma. Verkoissa, joissa on isäntälaitteita ja renkilaitteita, tarvitaan POLL sanomia. POLL sanomat toimivat siten, että isäntälaite lähettää kyseistä sanomaa renkilaitteille. Renkilaitteiden vastaanottaessa sanoman, siihen on vastattava riippumatta siitä onko lähetettävää vai ei. / 1, s.298 /

FHS

FHS-sanoma on kaikista suurin hallintasanomista. FHS-sanoma on 160-bittinen, joka sisältää 11 kenttää. Sanomaa käytetään tilanteissa, joissa isäntälaite ja renkilaite ovat keskenään vaihtamassa rooleja pikoverkon sisällä tai kun jokin laite haluaa muodostaa kanavan pikoverkossa. / 1, s.299 /

6.3 ACL-kanavan sanomat

ACL-kanavat on tarkoitettu datan siirrolle ja ohjaustietojen käytölle. ACL-liikenne perustuu suurimmaksi osaksi isäntälaitteen tekemistä lähetyksistä ja renkilaitteiden POLL- tai SELECT-sanomiin lähettämistä vastauksista. ACL-kanavalla on seitsemän erilaista sanomaa, jotka ovat: DM1, DH1, DM3, DH3, DM5, DH5 ja AUX. Taulukosta 4. näemme ACL-kanavien perustiedot ja nopeudet.

				Symmetrinen	Asymmetrinen nopeus	
Tyyppi	Data	FEC	CRC	Nopeus	Alavirtaan	Ylävirtaan
DM1	0 - 17	2/3	kyllä	108,8	108,8	108,8
DH1	0 - 27	ei	kyllä	172,8	172,8	172,8
DM3	0 - 121	2/3	kyllä	258,1	387,2	54,4
DH3	0 - 183	ei	kyllä	390,4	585,6	86,4
DM5	0 - 224	2/3	kyllä	286,7	477,8	36,3
DH5	0 - 339	ei	kyllä	433,9	723,2	57,6
AUX	0 - 29	ei	ei	185,6	185,6	185,6

Taulukko 4. ACL-kanavan sanomien tiedot. / 1, s.301 /

DM1

DM1-sanoma (*Data Medium segment 1*) kuljettaa datatietoa 18 tavun hyötykuormassa. Hyötykuorman perässä on 16-bittinen CRC-tarkiste ja kyseistä sanomaa korjataan 2/3 lohkokoodauksella. Koodauksessa on 5 suojabittiä jokaista 10 bitin lohkoa kohti.

DH1

DH1-sanoma (*Data High rate segment 1*) kuljettaa dataa 28-tavun hyötykuormassa ja perässä on suojattu 16-bittinen CRC-tarkiste. DH1 ei ole suojattu FEC-koodauksella, koska sen kustannuksella on saatu pidempi hyötykuorma.

DH3

DH3-sanoma on verrattavissa DM1:n. Ainoana erona on 123 tavun hyötykuorma. Hyötykuorman perässä 16-bittinen CRC-tarkiste, jossa käytetään 2/3 FEC koodausta. Pidempi hyötykuorma mahdollistetaan, kun sanomia lähetettäessä varataan siirtotieltä aina kolme aikaväliä. Sanomat jatkuvat yli aikavälien ilman suoja-aikoja. Tämä mahdollistaa 1655ms:n siirtoajan. Sanomia lähetettäessä ei tapahdu taajuushyppelyä, vaan koko sanoma lähetetään samalla taajuudella.

DM3

DM3-sanoma on muuten samanlainen kuin DH3-sanoma, mutta FEC-koodaus on jätetty pois. Sen seurauksen on saatu pidempi hyötykuorma, joka on mahdollistanut vähän nopeammat yhteydet.

DM5

DM5-sanoma varaa viisi aikaväliä aina kerrallaan, muuten toiminnaltaan samanlainen, kuin DM3:n. Viiden aikavälin varauksella pystytään siirtämään aina 266 tavua kerrallaan ja näin saadaan hieman nopeuksia kasvatettua.

DH5

DH5-sanoma on muuten samanlainen kuin DM5-sanoma, mutta erottavana tekijänä on FEC-koodauksen puuttuminen. FEC-koodauksen puuttumisella saadaan isompi hyötykuorma. Hyötykuorman pituus on 341 tavua ja näin saadaan hieman nopeuksia kasvatettua.

AUX

AUX-sanoma on samantyyppinen kuin DH1-sanoma, mutta pieniä kevennyksiä on tehty. Hyötykuorman pituus on 30 tavua, joka on kaksi tavua suurempi kuin DH1:ssa. Kahden tavun lisääntyminen on saatu aikaiseksi poistamalla CRC-tarkiste. / 1, s.300 /

6.4 SCO-kanavan sanomat

Yleensä SCO-kanavassa siirretään puhetta kaksisuuntaisesti, mutta voidaan myös siirtää ihan mitä vain tietoa kaksisuuntaisesti. Puheenkoodaus tapahtuu aina ylemmillä kerroksilla. / 1, s.301 /

Synkronisessa siirrossa käytetään kolmea erilaista sanoma tyyppiä, jotka ovat HV1:n, HV2:n ja HV3:n. Yhteinen tekijä kolmelle eri sanomalle on, että jokaisen hyötykuorma on 240 bittiä bruttona ja ainoana erottavana tekijänä on, miten databitit suojataan.

HV1-sanoma käyttää 1/3 FEC-koodausta (*kappale 4.6.1*). Koodauksessa siirrettävä bittimäärä kolminkertaistuu ja sen seurauksena sanoma kuljettaa vain 10 tavua, joka on 80 bittiä.

HV2-sanoma käyttää 2/3 FEC-koodausta (*kappale 4.6.2*). Koodauksessa siirrettävä bittimäärä kasvaa 1,5-kertaiseksi ja sen seurauksena sanoma pystyy kuljettamaan 20 tavua, joka tarkoittaa 160 bittiä. HV3-sanoma on samanlainen, kuin HV2-sanomakin, mutta erottavana tekijänä HV3:ssa on että, dataa siirretään suojaamattomana. Sen seurauksena siirrettävä data kasvaa 30 tavuun, joka tarkoittaa täyteen 240 bittiin.

Yksi SCO-kanavan mahdollisuuksista on siirtää puhetta ja dataa yhtä aikaa, jolloin puhutaan DV-sanomista (*Data&Voice*). Dataa suojataan 2/3 FEC-koodauksella ja puhetta siirretään suojaamattomana. SCO-kanavan sanomien tietoja voi tutkia myös taulukosta 5. / 1, s.301 /

Typpi	Data	FEC	CRC	Symmetrinen nopeus
HV1	10	1/3	ei	64 kbps
HV2	20	2/3	ei	64 kbps
HV3	30	ei	ei	64 kbps
DV	10+(0-9)	2/3,D	k,D	64 kbps + 57,6 kbps

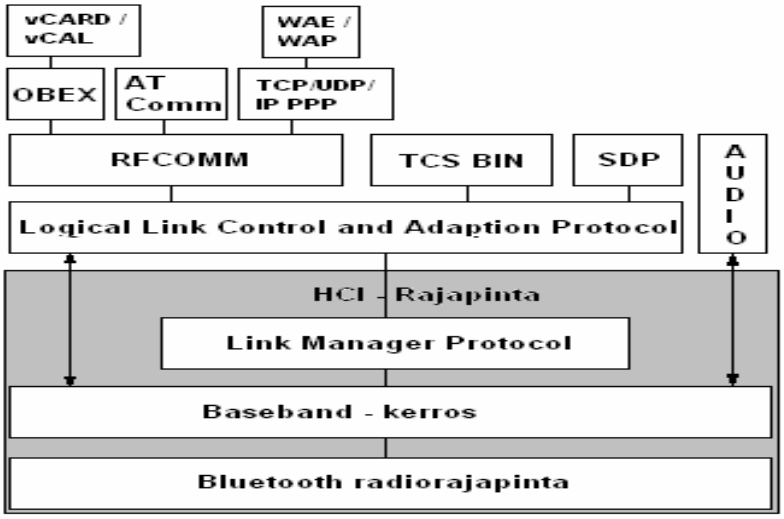
Taulukko 5. SCO-kanavan sanomien tiedot. / 1, s.301 /

Neljän eri sanoman lisäksi SCO-kanavassa voidaan siirtää myös POLL- ja DM1-sanomia, jotka ovat ACL-kanavan sanomia. Sanomia siirretään puhekanavassa siten, että aina yksi kanavaväli käytetään niiden siirtoon. Jos SCO–kanavassa siirretään DM1-sanomia, niin yleensä sen päällä kuljetetaan merkinantoa osapuolelta toiselle. / 1, s.302 /

7 BLUETOOTHIN PROTOKOLLAT

Lähtökohtana bluetooth-protokollia suunniteltaessa on ollut sulauttaa siihen mahdollisimman paljon jo olemassa olevia protokollia. Pyrkimyksenä on ollut välttämään suunnittelemasta uudelleen jo keksittyjä asioita. Toisena asiana on mietitty sitä, että jo käytössä olevilla sovelluksilla voisi olla helpompi muodostaa yhteistoimintaa bluetooth-laitteiden kanssa. Uusina protokollina on vain kehitetty L2CAP, SDP, TCS, BINARY, AT sekä RFCOMM. Bluetoothin-protokollat jaetaan neljään eri kerrokseen tehtäviensä ja toimintansa mukaan. Kerrokset ovat jaoteltu seuraavalla tavalla: ydin-, kaapelinkorvaavat-, puhelin-, adoptoidut protokollat.

Bluetooth-protokollat eivät puhdasoppisesti noudata OSI-mallia. Voidaankin sanoa esimerkiksi Baseband-kerroksen jakautuvan OSI-kerrokselle 1 ja 2. Bluetooth-arkkitehtuurisssa ei noudateta kerrosarkkitehtuurin perusperiaatetta. Perusperiaatteessahan pitäisi aina yhden kerroksen keskustella naapurikerroksen kanssa, mutta näin ei tapahdu bluetooth-laitteissa, vaan bluetooth sallii joidenkin toimintojen osalta kerrosarkkitehtuurin palvelujen ohittamisen. Tyypillinen tällainen toiminto on puheensiirto. / 1,s.292 ; 9 ; 10 /



Kuva 14. Bluetoothin-protokollapino. / 6, s.101 /

7.1 Ydinprotokollat

Ydinprotokolliin lasketaan kuusi eri protokollaa, jotka ovat Baseband, LMP (*Link Manager Protocol*), HCI (*Host Controller Interface*), Audio, L2CAP ja SDP.

BASEBAND

Baseband-protokollan tehtävänä on hoitaa fyysisen radioyhteyden luomista piconetin muodostavien laitteiden välille ja määritellä link controller kerroksen. Yhtenä tärkeimmistä tehtävistä baseband protokollalla on kontrolloida laitteiden synkronointia sekä käytettävää taajuushyppelyä. Käytettävät yhteystyypit ovat SCO ja ACL. / 10 /

LMP

LMP-protokolla ottaa vastuun yhteyden muodostamisesta. LMP protokollaa käytetään, kun neuvotellaan pakettien koosta tai piconetissa olevien laitteiden tiloista. LMP:n tasolla käsitellään myös linkkitason autentikaatiota, hallitaan salausavaimien luontia ja kontrollointia. LMP myös hoitaa nimipalvelut. / 9 /

HCI

HCI-rajapinnalla luodaan yhtenäinen pohja kaikkien bluetooth-laitteiden käsittelyyn. HCI-rajapinnan sisällä on baseband-kerros ja LMP:n kontrollirajapinta. Siitä syystä rajapinta tarjoaa pääsyn laitteiden tila- ja kontrollirekistereihin. HCI-rajapinta lisää tuleviin datapaketteihin otsikkona 4 tavua (ACL-paketit) tai 3 tavua (SCO-paketit) . / 10 /

AUDIO

Äänilähetykset ohjataan suoraan kantataajuustasolle audio-protokollan kautta bluetooth-yhteyden muodostamisen jälkeen. / 9 /

L2CAP

L2CAP:n tehtävänä on olla kantataajuuden ja ylempien kerrosten protokollien välissä. L2CAP sovittelee näiden protokollien tehtäviä. Usein L2CAP ajatellaan olevan LMP:n kanssa rinnakkain, mutta nämä kaksi erottaa siitä, että L2CAP:n varustaa palveluja ylemmille protokollille. Eikä LMP:n kautta koskaan kulje hyötydataa. Toisena tehtävänä L2CAP:llä on hankkia yhteydellisiä ja yhteydettömiä palveluja ylemmille protokollille kanavointi mahdollisuudella, segmentaatiolla ja uudelleenkoonti operaatiolla sekä ryhmän abstraktioinilla. / 10 /

SDP

SDP on palvelunlöytö protokolla, joka nimensä mukaan löytää palveluita. SDP on kriittinen osa runkoa, koska palvelut luovat perustan kaikille käyttötavoille. SDP:tä käytetään kun halutaan kysellä laitteiden tietoja, palveluita ja palveluiden luonteita. Näiden jälkeen voidaan muodostaa yhteys. Täytyy muistaa, että bluetooth-laiteita voidaan käyttää yhtä aikaa sekä SDP-palvelimena, että asiakkaana. Palvelimien joukko muuttuu dynaamisesti, kun laitteita saapuu ja poistuu kuuluvuusalueelta. / 10 /

7.2 Kaapelinkorvaavat protokollat

Kaapelinkorvaaviin protokolliin kuulu ainoastaan RFCOMM, joka on sarjalinjan emulointi protokolla. RFCOMM protokolla perustuu ETSI TS 07.10 standardiin. RFCOMM protokollan tehtävänä on emuloida RS-232 kontrolli- ja data signaaleja bluetooth kantataajuudelle ja luoda siirtomahdollisuus ylemmille palveluille, jotka käyttävät sarjaporttia yhteysvälineenä. RFCOMM tukee kahdentyyppisiä laitteita, niitä jotka ovat tiedonsiirron päätepisteenä, kuten tietokoneet. Ja niitä, jotka ovat tiedonsiirron välineenä, esimerkiksi modeemit. RFCOMM:lla voi olla yhtäaikainen yhteys kahden laitteen välillä sekä myös yhteyksiä useampiin muihin laitteisiin yhtä aikaa. / 10 /

7.3 Puhelinprotokollat

Puhelinprotokolliin kuuluu kaksi erilaista protokollaa, nämä ovat TCS binäärinen puhelunhallinta protokolla ja AT – komennot.
Binäärinen puhelunhallinta protokolla on bittipohjainen protokolla, jonka tehtävänä on määritellä puhelunhallintasignaalit puhe- ja datasoittojen muodostamiseksi. Toisena asiana puhelunhallinta protokolla määrittelee liikkuvuudenhallintaprosessit TCS laitteiden käsittelyyn. Binäärinen puhelunhallinta protokolla perustuu ITU-T:n.
AT-komentoja käytetään silloin, kun esimerkiksi modeemia tarvitsee hallita usean käyttäjän tilassa. AT-komennotkin perustuvat ITU-T:n suositukseen. AT-komentoja tuetaan puhelukontrollisignaalien välittämiseen. Välittämisessä käytetään RFCOMM-protokollaa. / 10 /

7.4 Adoptoidut protokollat

Adoptoidut protokollat toimivat RFCOMM:n päällä ja niihin lasketaan seuraavat kahdeksan erilaista protokolla tyyppiä: PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC ja WAE. / 10 /

PPP

Bluetoothissa PPP protokolla on suunniteltu toimimaan RFCOMM:ssa viimeistelläkseen point to point -yhteydet. PPP on IETF:n Point to point Protocol. / 10 /

OBEX, vCARD ja vCAL

OBEX on objektinvaihtoprotokolla, joka perustuu aiemmin kehitettyyn infrapunayhteyksien IrOBEX:iin. Protokolla on kehitetty alkujaan arvattavia tilanteita varten, esimerkkinä käyntikorttien vaihtaminen tai viestien vaihtaminen. OBEX protokolla määrittelee saman toiminnallisuudellaan kuin http, mutta OBEX protokolla on tehty kevyemmäksi versioksi. OBEX protokollalla pystytään

vaihtamaan neljää erilaista objektia, jotka ovat vCARD (*käyntikortti*), vCAL (*sähköiset kalenterit ja aikataulut*), vNOTE (*lyhyt viesti*) ja vMESSAGE (*edellistä pidempi viesti*). / 9 /

UDP/TCP/IP

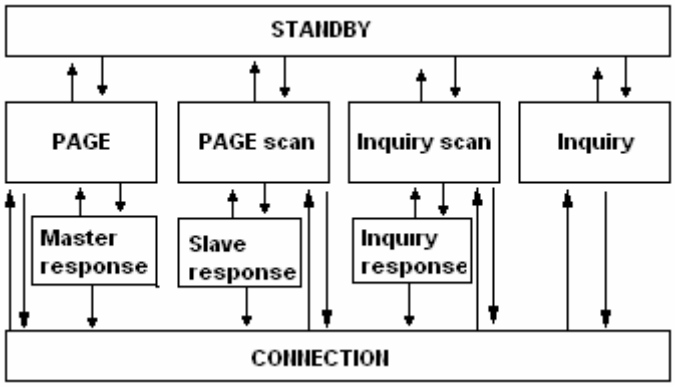
UDP, TCP ja IP protokollat on standardoitu IETF:ään. Nämä protokollat on suunniteltu Internetyhteyksiä varten. Näiden protokollien käyttäminen on systeemiriippuvaista, koska niiden avulla bluetooth-laitteet voivat olla yhteydessä toisiin laitteisiin, jotka ovat taas yhteydessä Internetiin. Toisin sanoen bluetooth-laiteita voidaan käyttää siltana Internetiin. / 10 /

WAP

WAP:lla pystytään käyttämään piilotettuja tietokonemalleja. WAP suunniteltiin alkujaan tuomaan Internetin sisältö ja puhelinpalvelut langattomiin päätelaitteisiin. Näin alettiin kehittämään siihen tarvittavia ohjelmistoja. Yleensä WAP:a käytetään palvelimen ja PC:n välillä, joten näin olisi mahdollista toteuttaa erilaisia piilotettuja tietokoneominaisuuksia. Bluetoothin WAP ominaisuudet tukevat muotoja WML, WMLScript, WTA event, WBMP ja vCARD/vCAL, jotka kaikki ovat osa WAE:ta. / 9 /

8 BLUETOOTHIN YHTEYDEN LUOMINEN

8.1 Bluetoothin-tilat



Kuva 15. Bluetoothin-tilakone. / 1, s.304 /

Kuvasta 15. on esitetty, miten bluetooth-laitteiden tilat muodostuvat. Bluetoothin tärkeimmät lopputilat sen toimiessaan ovatkin standby eli odotus-tila ja connection eli yhteys-tila. Kaikki muut tilat ovatkin väliaikaisia tiloja.

Standby – tila

Bluetooth-laitteiden käynnistämisen jälkeen ne asettuvat standby tilaan, joka toimii myös virran säästötilana. Standby-tilassa ainoastaan laitteiden sisäiset kellot käyvät ja luonnollisesti minkäänlaista liikennöintiä eri laitteiden välillä ei tapahdu. Stanby-tilassa olevat laiteet kuuntelevat liikennöintiä aina 1,28 sekunnin välein 32 eri hyppelytaajuudella mahdollisten kutsujen takia. / 1, s.304 ; 9 /

Page / Inquiry

Yhteyksien luomiset tapahtuvat tiedustelu- ja hakukutsuja käyttämällä (*Inquiry / page*). Inquiry-tilassa oleva laite yrittää paikallistaa muut verkossa olevat laitteet ja taas page-tilassa oleva laite yrittää ottaa isäntälaitteen roolia. Jos bluetooth-laite haluaa isäntälaitteen roolin, niin se lähettää page-kutsuja potentiaalisille renkilaitteille, kun joku renkilaiteista vastaa näihin, niin siirrytään master response -tilaan. / 1, s.304 /

Page scan / Inquiry scan

Bluetooth-laitteen mennessä inquiry scan -tilaan, se haluaa julkaista omat ominaisuutensa verkon muille laitteille ja vastaavasti ollessaan inquiry scan -tilassa se reagoi muihin tuleviin inquiry -sanomiin.

Bluetooth-laite käy säännöllisesti page scan -tilassa ja vastaanottaa page sanomia. Vastaanottaessa page-sanomia se siirtyy automaattisesti slave response -tilaan, jossa se saa isäntälaitteen FHS-sanoman. FHS-sanoma sisältää tiedot isäntälaitteen toiminnasta ja ajoituksesta. / 1, s.305 /

Connection

Bluetooth-laitteen ollessa yhteys tilassa, se vastaanottaa isäntälaitteen kellon ja hyppelyjärjestyksen. Isäntälaite tekee yhteyden tarkistukset käyttämällä POLL-sanomia renkilaitteille. Renkilaitteiden tehtävänä on kuitata POLL-sanomat NULL-sanomilla. Yhteydessä ollessaan, renkilaitteiden tehtävänä on ylläpitää synkronointia verkon isäntälaitteeseen ja tähän ei saa vaikuttaa onko isäntälaitteella liikennettä vai ei. Liikenteetön renkilaite yrittää synkronoida itseään muihin renkilaitteisiin. / 1, s.305 /

8.2 Bluetoothin virransäästötilat

Bluetooth-laitteet ovat yleensä kooltaan pieniä ja näin ollen sisältävät myös kooltaan pienet akut, joista ei muodostu tehoa paljoakaan. Siitä syystä olisi aina etu jos virrankulutus olisi mahdollisimman pieni. Minimoitaessa virrankulutusta, on siihen tehokas keino asettaa logiikat eritasoisiin virransäästötiloihin. Bluetooth-laitteisiin on kehitetty kolme erilaista virransäästö tilaa, jotka ovat pitotila (*hold*), pysäköitytila (*park*) ja nuhkimistila (*sniff*). / 1, s.307 /

Pitotila (connection hold)

Pitotilassa laite ei vastaanota tai lähetä minkäänlaista liikennettä. Pitotilassa ei ole mikään muu toiminnassa, kuin sisäinen ajastin. Pitotila on säädetty siten, että tietyn ajan päästä laite herää ja lähetys toiminta alkaa taas uudelleen. Pitotilassa varataan yksi AM-osoite. / 13 /

Pysäköitytila (connection park)

Pysäköidyssä tilassa kulutetaan kaikista vähiten virtaa ja pysäköidyt laitteet hylkäävät AM-osoitteensa, mutta pysyvät synkronoituna pikoverkkoon. Liikennettä pysäköidyssä tilassa ei ole mahdollista pitää yllä mihinkään suuntaan. Ainoa mitä pysäköidyssä tilassa oleva laite pystyy tekemään, on oman kellonsa tarkistus ja tämäkin ainoastaan sen takia, että broadcast lähetyksien vastaanottaminen olisi mahdollista. Isäntälaite herättää park-tilassa olevan laitteen. / 1, s.308 /

Nuuhkimistila (connection sniff)

Nuuhkimistilassa bluetooth-laite säilyttää oman AM-osoitteensa ja pitää yllä synkronointia verkkoon. Nuuhkimistilan tehonkulutuksen pieneneminen perustuu siihen, että liikennettä kuunnellaan harventuneella tahdilla. Se kauanko laite on nuuhkimistilassa, on ihan ohjelmallisesti muutettavissa ja eri valmistajilla on omat aikansa. / 9 /

8.3 Yhteyden muodostus

Muodostaessamme bluetooth-laitteelle yhteyttä oletamme, että jossain ympärillämme on myös muita aktiivisia bluetooth-laitteita. Mikäli toimintasäteen sisällä on muita laitteita, ne vastaavat kyselyihin. Oletamme tietenkin, että ne ovat asettuneet havaittaviksi ja tällä havaittavuudella ei ole mitään tekemistä näköyhteyden kanssa, vaan puhumme ohjelmallisesta muodostamisesta. Mikäli laitteet ovat ohjelmallisesti asetettu piilotetuiksi, ne eivät vastaa kyselyihin. Se ovatko laitteet piilotettuja vai havaittavissa olevia, on tietoturvalle iso merkitys, mutta siitä tulee vasta hiukan edempänä.

Kyselyihin vastaava laite lähettää vastauksena FHS-paketin, josta ilmenee laiteosoite, kellonajat jne. Kyselyiden aloittamisen alkanut laite leimataan isäntälaitteeksi ja muut niihin vastanneet laitteet ovat renkilaitteita. Jos jostain syystä käy niin huono tuuri, että kyselyiden vastaukset eivät tule perille asti, niin alkuperäinen aloitteen tekijä lähettää uudelleen kyselyt.

Varsinaisen yhteyden muodostamisessa käytetään page-hakuja. Hakuja tehdään silloin, kun tunnetaan jo jollakin tavalla muiden laitteiden laiteosoitteet ja on jo jonkin verran tietoa niiden kelloista. Haussa isäntälaite etsii renkilaitetta ja renkilaite vastailee hakuvastauspaketeilla. / 9 /

9 TIETOTURVA

Aina kun on kysymyksessä langaton tiedonsiirtojärjestelmä, niin siihen käsiksi pääseminen on aina huomattavasti helpompaa, kuin langallisissa järjestelmissä. Bluetoothissa käytettävä tekniikka ja käyttöolosuhteet edistävät kuitenkin tietoturvallisuutta. Bluetoothin taajuushyppely vaikeuttaa huomattavasti salakuuntelua sekä yhteyksien häiritsemistä. Kantosäteen ollessa pieni on yleensä liikennöinti rajoittunut suppeaksi.

Yksinkertaisesti sanottuna bluetooth-laitteiden tietoturva perustuu kahteen osaan; uusien laitteiden autentikointiin ja siirrettävän tiedon salaukseen. Näiden hallinnassa käytetään laitteiden MAC-osoiteita, kahta salaista avainta ja autentikoinnissa käytettävää tiedon salausta.

Kuitenkin pitää aina muistaa että, erilaiset laitteet ja ohjelmat tarvitsevat eri tietoturvasovelluksia. Joissakin tapauksissa tietoturva saa olla heikko ja joissakin tapauksissa sen pitää olla erittäin luotettava. Siitä syystä bluetoothille on kehitetty joustava määrittely tietoturvalle, joka pitää sisällään kolme eri tietoturvatasoa. Tietoturvataso 1 on suojaamaton tiedonsiirto, tietoturvataso 2 on joustava palvelutason suojaus ja kiinteä linkkitason suoja sekä tietoturvataso 3 on autentikointi sekä salaus. / 3, s.77 /

9.1 Turva-arkkitehtuuri

9.1.1 Profiilien luoma tietoturva

Bluetoothin profiilit määrittelevät, miten erilaiset operaatiot tulisi toteuttaa. Profiileita on määritelty bluetooth-laitteille 13 erilaista.

GAP (*Generic Access Profile*) määrittelee yleiset toimintatavat laitteiden hakemiseen ja linkkien hallintaan. Kaikki muut profiilit tukeutuvat tähän profiiliin. Nimenomaan tietoturvan kannalta GAP profiili on kaikista tärkein ja sen takia käsittelemmekin vain tätä profiilia. / 9 /

Joustavan tietoturvan määrittelyt luodaan GAP:ssä. Joustavaan tietoturvaan on määritetty kolme eriasteista tietoturvatasoa. Tietoturvataso 1 on suojaamaton tiedonsiirto, tieturvataso 2 on joustava palvelutason suojaus ja kiinteä linkkitasonsuoja sekä tietoturvataso 3 on autentikointi ja salaus.

Tieturvataso 1 on nimensä mukaan täysin suojaamaton ja ensimmäisessä tasossa ei tehdä minkäänlaista suojausta pitäen sisällään tiedonsiirron ja muut toiminnot. Tietoturvatasojen 2 ja 3 erot ovat siinä, että tietoturvatasolla 2 suojaus tehdään vasta yhteyden muodostuksen jälkeen ja tietoturvatasolla 3 se tehdään jo ennen yhteyden muodostusta. Voidaankin päätellä, että toisen tietoturvatason suojaukset tehdään protokollan ylemmissä kerroksissa ja taas vastaavasti kolmannen tietoturvatason suojaukset tehdään protokollan alemmissa kerroksissa. Kuitenkin kaikki turvatoiminnot tapahtuvat aina linkkitasolla. / 9 /

9.1.2 Palvelutasojen tietoturva

Palvelutason tietoturvasta vastaavat ylemmän tason protokollat. Kaikki bluetooth-laitteet jaetaan luotettuihin ja ei-luotettuihin laitteisiin. Jaon tarkoituksena on säädellä eri laitteiden pääsyä eri palveluihin. Aina yksi laite voi toimia yhdessä luokassa kerrallaan. Yleensä luotettavilla laitteilla on pääsy kaikkiin tarjottuihin palveluihin ja taas vastaavasti epäluotettavat laitteet ryhmitellään sen mukaan kuinka korkeatasoista tunnistusta niiltä vaaditaan.

Palvelut jaetaan aina kolmeen eri luokkaan. Luokka 1 on turvaton, luokka 2 on joustava ja luokka 3 on kiinteä. Luokkien määrittely toimii samalla tavalla, kuin tasojenkin määrittelyt. Luokka 1 on kevyin versio ja luokka kolme on kaikista suojatuin luokka. Luokassa 1 on kaikille laiteille avoimet palvelut. Luokassa 2 taas vaaditaan autentikaatiota ja auktorisointia. Käytettäessä toista luokkaa on automaattinen pääsy vain luotetuilla laitteilla. Kolmas luokka toimii muuten samalla tavalla, kuin toinenkin luokka, mutta auktorisointi joudutaan tekemään käsin. Luokassa 3 lisäksi vaaditaan autentikointia ja luottamuksellisuutta. / 9 /

9.1.3 Linkkitason tietoturva

Linkkitasolla käytetään tietoturvan ylläpitämiseen neljää eri parametria. Jokaisella bluetooth-laitteella on uniikki 48-bittinen laiteosoite, joka on ensimmäinen parametri. Toisena parametrina käytetään 128-bittistä linkkiavainta (*Link key*). Yleisin käyttö tilanne on, kun kaksi bluetooth-laitetta autentikoi toisilleen. Linkki avaimesta on mahdollista johtaa 8 – 128 bittinen salausavain (*encryption key*). Tällä salauksella salataan pakettien sisältö. Täytyy muistaa, että salausavain on aina erotettu linkki avaimesta. Neljäntenä parametrina käytetään generoitua satunnaislukua. Käyttäjä saa vielä halutessaan asettaa PIN-koodin, jolla pystytään entisestään nostamaan turvallisuuden tasoa. / 9 /

9.2 Autentikointi ja salaus

Autentikointi

Perus lähtökohtana bluetooth-laitteiden autentikoinnissa on haaste vastaus -menetelmä. Menetelmän perus ideana on, että toinen laite lähettää jonkun satunnaisluvun ja vastaanottaja soveltaa jo ennalta sovittua autentikoimismenetelmää omalla avaimellaan. Vastaanottaja lähettää jo tässä vaiheessa salatun vastauksen ja jos avaimet täsmäävät, niin lähettäjä pystyy lukemaan viestin sekä hyväksymään autentikoinnin. Jos lähettäjä ei saa vastausta perille tai ei pysty avaamaan salausta, lähettäjä odottaa satunnaisen ajan ja lähettää viestit uudelleen. Bluetooth-laitteet autentikoivat samalla tavalla kuin TETRA-laitteet. Eli autentikointi voidaan tehdä molempiin suuntiin ja tämän hyötynä on, että verkossa naamioinnin mahdollisuus pienenee. / 3, s.308 /

Salaus

Salausavain on 8 – 128 bitin pituinen, joten bluetooth-laitteiden tarvitsee, jo ennalta sopia minkälaista salausavainta käytetään. Salauksessa käytetään salausjono

menetelmää, mikä aikaan saadaan neljällä rinnakkaisella LFSR-salaajalla. Salausjonon tulos yhdistetään summalogiikan avulla yhdeksi bittijonoksi. Jonka jälkeen bittijonoon lisätään yhteenlaskulla XOR salaajan tuottama ”satunnainen” bittijono. Vastaanottaessa sanomaa, sen purkaminen tehdään samalla tavalla kuin muodostaminenkin, mutta käänteisessä järjestyksessä. / 3, s.309 /

9.3 Tietoturvaongelmat

Bluetoothin tietoturvasta on lähes yhtä monta eriävää mielipidettä, kuin on käyttäjääkin. Yleisesti bluetooth-laitteita ei pidetä mitenkään erityisen turvattomana. Bluetooth-laitteiden yleistyessä kovaa vauhtia niiden tietoturvallisuuteenkin on panostettava entistä enemmän, jonka huomaamme myös vanhojen bluetooth-laitteiden eri ohjelmien päivityksissä.
Bluetooth-laitteissa suurimmat tietoturvauhat muodostuvat käyttäjien huolimattomuudesta tai epätietoisuudesta.

Bluetooth-laiteita käytettäessä pitää ajatella liikenteen laatua ja käytettäviä kantomatkoja. WLAN yhteyksiä murrettaessa tietomurtoa tekevän ei tarvitse olla kauhean lähellä kyseistä verkkoa, koska WLAN yhteyksien toimintasäde on kohtuullisen pitkä ja suuntaavilla antenneilla, siihen pääsee käsiksi vaikka vähän kauempaakin. Bluetooth-laitteiden kantama on taas vastaavasti aika pieni, yleisesti noin 10 metrin luokkaa. Tarkoittaen sitä, että tietomurtoa tekevän tarvitsee istua samassa huoneessa. Toisena asiana on, että bluetooth verkkoa on huomattavasti vaikeampi löytää, koska bluetooth-laitteiden tarvitsee olla lähellä toisiansa, että ne löytävät toisensa.

Bluetooth-laitteiden tietoturva protokollaan suunniteltaessa yritettiin saada protokolla, joka olisi mahdollisimman joustava ja antaisi mahdollisimman suuren läpinäkyvyyden sekä käytettävyyden. Tämän seurauksena on protokollasta tullut hiukan monimutkainen. Tietoturva-arkkitehtuuri on myös pyritty pitämään infrastruktuuriltaan käyttäjille näkymättömänä, joka on luonut myös siitä hiukan monimutkaisen. Yhtenä nyrkkisääntönä pidetäänkin, että mitä monimutkaisempi

laite, niin sitä hankalampi hallita. Hankalasti hallittavissa oleva laite taas puolestaan johtaa siihen että tietomurtoja on helpompi tehdä. / 11 /

9.4 Bluetooth-laitteiden turvaongelmat

Bluetooth-laitteet käyttävät taajuushyppely tekniikkaa, mutta se ei tuo paljoakaan lisää turvallisuutta, koska sitäkin voidaan seurata. Nykyään neljä vakavinta turvaongelmaa bluetooth-laitteissa on avaimen hallintaa liittyvät ongelmat, PIN – koodihyökkäykset, laiteosoitteisiin perustuvat hyökkäykset ja käyttäjien tunnistaminen. / 11 /

9.4.1 Tukkeutuminen

Sotateknologiassa, kun käytetään taajuushyppelyyn perustuvaa tekniikkaa, niin laitteiden liikennöinnin tukkiminen on hyvin yleinen ja perus häirintämuoto. Siviilimaailmassa se on jo monissa maissa laitonta, mutta ei ihan joka maassa. Tukkimisessa laitteet yleensä ylikuormitetaan, mutta bluetooth-laitteissa tukkiminen on hiukan harvinaisempaa, johtuen siitä, kun tukkivan laitteen tarvitsisi olla lähellä tukittavaa laitetta. . / 11 /

9.4.2 PIN-koodin murtaminen

PIN-koodin murtaminen tehdään joko passiivisesti käymällä kaikki vaihtoehdot läpi tai aktiivisesti välimieshyökkäysten avulla.

Kun oletetaan hyökkääjän salakuuntelevan liikennettä, niin hyökkääjä yrittää murtaa PIN-koodin raakaa voimaa käyttäen. Käytettäessä raakaa voimaa yritetään

arvata kaikki PIN-koodin mahdollisuudet alustusavaimen luonnin todentamisvaiheessa. Salakuuntelua käyttäessä hyökkääjällä on mahdollisuus saada haltuunsa haasteen ja salatun vastauksen. Sattuessa saamaan oikean PIN-koodin on tie auki laitteelle asti. Tämän tyylisessä hyökkäyksessä ainoastaan kuunnellaan liikennettä. Ainoa asia miten tämäntapainen hyökkäys voidaan estää, on käyttää pitkiä PIN-koodeja. / 11 /

Hyökkääjän pystyessä osallistumaan hyökkäykseen hän yrittää ensin tehdä yhden PIN-arvauksen ja ottaa ensimmäisen siirron alustusavaimen luonti protokollasta. Toisella siirrollaan hän yrittää olla haaste vastausprotokollan aloittava osapuoli. On hyvin todennäköistä, että uhrin vastaus on sama kuin hyökkääjän laskema arvo. Hyökkääjän arvatessa oikein PIN-koodin hän saa uhrin kaikki muut tiedot vastauksen mukana. / 11 /

9.4.3 Paikantamishyökkäys

Bluetooth-laitteen ollessa havaittavassa tilassa, se vastaa kaikkiin kyselyihin. Bluetooth-laiteen vastatessa isäntälaitteen kyselyyn, se lähettää samalla laiteosoitteensa. Laiteosoitteen avulla hyökkääjä pystyy seuraamaan laitteen liikkeitä.

Ensimmäinen tapa tehdä paikantamishyökkäys on yrittää luoda yhteyttä kaikkiin uhrin vaikutuspiirissä oleviin laitteisiin. Muitten laitteiden vastatessa, se lähettää laiteosoitteensa, jonka perusteella se myös tunnistetaan.

Toinen tapa tehdä paikantamishyökkäys on riippuvainen siitä vastaako uhrilaite hyökkääjän kyselyihin. Laitteet, jotka ovat toisiinsa yhteydessä lähettävät toistensa osoitteita kommunikoidessaan. Laitteiden liikennettä on mahdollista seurata ja hyökkäys perustuukin siihen. Laitteiden kommunikoidessa keskenään valitsemillaan kanavilla, ne tunnistetaan kanavantunnistuskoodista. Näin ollen hyökkääjä voi muuttaa kanavan tunnistus koodia ja saada selville isäntälaitteen laiteosoitteen. / 11 /

9.4.4 Hyökkäys salausta vastaan

Kun tehdään hyökkäys suoraan salausta vastaan, niin se on matemaattinen operaatio. E0-salauksessa käytetään kolmen pienimmän LFSR-rekisterin ja summausrekisterien tiloja. Se miten tämä salaus muodostetaan voi katsoa osasta 9.2. Salaus arvataan oikein todennäköisyydellä 2 potenssiin -93, koska rekisterien pituudet ovat 25,31 ja 33 sekä 25+31+33+4= 93. Hyökkäävällä osapuolella on käytössään 128 tavua selvää tekstiä ja on mahdollista että 2 potenssiin 7 bittioperaatiolla tarkastetaan, mikä arvauksista on oikein. Hyökkäys menetelmä on teoriassa mahdollinen, mutta käytännössä aivan mahdoton. Tämän tyylinen hyökkäys ei toimi bluetooth-laitteissa, koska salaus tahdistetaan jokaiselle paketille erikseen. / 11 /

9.5 Hyökkäysten estämiset.

9.5.1 Hyökkäysten estäminen suunniteltaessa bluetooth-laitteita

Bluetoothin heikoin kohta on PIN-koodi, joten olisi ensisijaisen tärkeää käyttää riittävän pitkiä koodeja, minimissään 64 bitin mittaisia
On lopetettava yksikköavaimien käyttö salauksessa ja tarvittaessa ne on korvattava, vaikka satunnaisavaimilla.
Sovellusten salausta pyritään käyttämään avaimien vaihdossa, joka tarkoittaa mekanismeja, joissa on julkinen salakirjoitus.
Kanavantunnistus koodeissa on pyrittävä käyttämään laskentamekanismeja, koska laitteet eivät jokaisella yhteydellä näyttäisi identiteettiään.
Bluetooth-laitteet ei tunnista laitteiden käyttäjiä vaan laitteita. Varastettu laite toimii samalla tavalla, vaikka siinä olisi kuka käyttämässä. Joten tähän olisi tehtävä sovellustason turvamekanismi.
Suurin osa bluetooth-laitteista on akkukäyttöisiä, niiden akut voidaan tyhjentää palvelunestohyökkäyksillä, mutta tähän ei pystytä puuttumaan. / 11 /

9.5.2 Miten perus käyttäjä voi estää hyökkäykset

- Ostaessasi tai ottaessasi käyttöön uuden bluetooth-laitteen, vaihda kaikki oletussalasanat.
- Pidä bluetooth-yhteyttä päällä ainoastaan tarvittaessa.
- Pistä bluetooth-laitteen asetuksista laite piilotetuksi, jotta se ei näkyisi kaikille muille laitteille.
- Älä hyväksy yhteyden ottoja tuntemattomilta laitteilta.
- Älä pidä linux-, mac- tai windows – kannettavien bluetooth verkkojen kansiossa mitään salassa pidettäviä tietoja.
  / 4, s.1 /

9.6 Tietoturvan termistöä

Bloover on käyttöön tarkoitettu demo työkalu, joka on suunniteltu tietoturvan testaamiseen.

Blueprint on linuxille saatava ohjelma, jonka tarkoituksena on etsiä bluetooth-laitteiden laiteosoitteita ja käytössä olevia palveluita. Näiden perusteella löytää laitteen mallin ja valmistajan.

Car whisperer on tutkimuskäyttöön kehitelty linux-ohjelma, joka on luotu testaamaan bt- ja hf-laitteiden kautta puhelinkeskusteluiden salakuuntelua. Kehitelty autolaitteita varten.

Bluebug on löydetty laajasti eri valmistajien puhelimista ja on at – komentojen sekä radiorajapinnan haavoittuvaisuus. Blubugin kautta esimerkiksi puhelimista saadaan tietoja sekä pystyttään lähettämään osoitekirjaan uusia nimiä sekä numeroita.

Bluejacking on vaaraton, mutta kiusallinen ominaisuus, jonka avulla puhelimeen voidaan vastaanottaa ja lähettää käyntikortteja anonyymisti.

Bluesmack on bluetooth-laitteisiin kohdistettu puhelinesto hyökkäys. Hyökkäyksellä pystytään kaatamaan päätelaite kokonaan tai hetkellisesti pois käytöstä.
Bluesnarfing on samantyylinen kuin bluebug hyökkäys, mutta bluesnarfingilla voidaan varastaa laitteista tietoja esimerkiksi kalenteri, osoitekira, sms-viestit ja laitteen imei-koodit.
Bluesniper on erikoisvalmistettu bluetooth-laite, jossa on tehokas suuntaava antenni. / 4, s.2 /

9.6 Esimerkki bluejacking toiminnasta

Nykyään bluetooth on yleistynyt kovalla tahdilla ja melkein jokaisesta kännykästä löytyykin jonkinasteinen bluetooth-laite. Bluejacking toiminnolla pystytään tekemään pieni muotoisia piloja muille bluetoothin omaaville kännyköille, mutta muuten sillä ei saa puhelinta kontrolloitua. Bluejacking eli suoraa suomennettuna sinikaappaus. Nimi ei sinänsä pidä paikkaansa, koska tällä toiminnalla ei pysty mitään kaappaamaan, mutta tällä pystytään lähettämään ja vastaanottamaan käyntikortteja anonyymisti. Eli joku tuntematon voi lähettää puhelimeen pienenä pilana käyntikortteja sinun koskaan tietämättä, mistä ne tulevat.
Blujacking toimii siten, että joku tuntematon henkilö kirjoittaa omaan laitteeseensa uuden osoitekirja merkinnän. Hän kirjoittaa nimitietoihinsa haluamansa viestin, jonka jälkeen etsii laitteellaan läheisyydessä olevia bluetooth-laitteita. Laitteen löytyessä, hän tutkii uhrin profiilit, valitsee käyntikortti profiilin ja lähettää kirjoittamansa viestin. Sen jälkeen toisen puhelimeen pamahtaa viesti perille, eikä uhri saa koskaan selville mistä se on tullut. / 2, s.51 /

9.7 Bluetooth puhelimien tietoturvan kokeileminen

Vuonna 2005 Tietokone-lehti kokeili bluetooth puhelimien tietoturvan kestävyyttä. Varusteina oli Ubuntu Linuxilla varustettu kannettava tietokone, johon oli asennettu car whisperer -ohjelma, bluetooth-sovitin ja siihen kytketty Daimlerin 13 desibelin kohdentava antenni. Tarkoituksena oli kokeilla voidaanko hf-antennien kautta kuunnella ihmisten keskusteluita. Kyseisellä yhdistelmällä oli mahdollista jatkaa bluetooth-signaalia ulkotiloissa 30 tai 50 metriin asti. Ohjelmassa käytettiin Linuxin Bluez-protokollapinoa ja useita Internetistä saatuja työkaluja. Bluez-ohjelmalla voidaan esimerkiksi salata käytettävän tietokoneen nimi.. / 4 /

Ensimmäisessä yrityksessä yritettiin päästä kuuntelemaan bluetooth-kuulokkeen ja puhelimen välistä yhteyttä. Tämä olisi mahdollistanut muiden ihmisten puheluiden kuuntelemisen. Yhteyden muodostus onnistui vain, kun kuulokkeessa ei ollut jo aktiivista yhteyttä auki ja se oli päällä paritustilassa. Eli jo avoimeen yhteyteen ei ollut mahdollista päästä kaappaamaan yhteyttä. / 4 /

Useissa vanhoissa puhelimissa on ollut bluebug-nimellä tunnettu ohjelma virhe, joka mahdollistaa puhelimen kalenterin ja osoitekirjan ryöstämisen käyttäjän huomaamatta. Hyökkäys simuloitiin Internetistä saavalla Bloover-ohjelmalla, joka toimii java-puhelimissa. Kohdelaite oli Nokian 6310i-puhelin ja hyökkäyslaitteena uudempi 6630.
Kohdelaitteessa oli bluetooth päällä ja kaikille näkyvänä. Osoitekirjan ryövääminen puhelimesta osoittautui lapsellisen helpoksi. Kohdelaitteessa vilahti ainoastaan nopeasti viesti, että bluetooth-yhteys on muodostettu, mutta muuten se ei paljastanut olevansa hyökkäyksen kohteena. Haavoittuvuus ei koskenut vain osoitekirjaa, vaan myös puhelimen kalenterin sisältöä ja sms-viestejä, jotka oli mahdollista ladata käyttäjältä lupaa kysymättä. / 4 /

Haavoittuvuus koskee lähinnä vain vanhoja puhelimia ja se on korjattu uusista puhelimista, mutta on hyvä muistutus siitä miksi bluetooth käyttöön kannattaa suhtautua varovaisesti. / 4 /

10 BLUETOOTHIN TULEVISUUS JA KILPAILEVAT TEKNIIKAT

Bluetooth ei ole ensimmäinen, eikä varmastikaan viimeinen tekniikka, joka on suunniteltu korvaamaan johtoja ja luomaan lyhyen kantaman verkkoja. Useat muut tekniikat menevät bluetoothin kanssa päällekkäin, joten luonnollisesti markkinoille on tullut kilpailua näiden tekniikoiden kesken. Käsittelen hieman työssäni yleisempiä kilpailevia tekniikoita, joihin kuuluvat Irda, IEEE 802.11b eli wlan sekä uusia tekniikoita ZigBee ja WUSB eli langaton USB Kerron vielä lopussa bluetooth-tekniikan tulevaisuudesta ja mihin sen kehitystyö on suuntaamassa..

10.1 IrDA

Irda eli Data Associationin spesifioima infrapunayhteys. Irda tekniikka on laajasti levinnyt maailmalle, mutta alkaa olla nykyään hieman vanhentunutta tekniikkaa. Infrapunalinkkiä käytetään mm. tietokoneissa, matkapuhelimissa ja kämmenmikroissa. Irda tekniikka on tarkoitettu lyhyen kantaman siirtoon, kuten bluetoothkin, mutta varsinaisesti tämä tekniikka ei kilpaile bluetoothin kanssa. Irda on kuitenkin toiminnaltaan hyvin samantapainen kuin bluetoothkin. Irda on täsmällinen pisteestä pisteeseen linkki. Lähettimen ja vastanottimen väliin ei saa muodostua suuria esteitä, eikä lähettimen ja vastaanottimen välimatka saa olla kovinkaan suuri, muuten yhteys katkeaa. Infrapunatekniikka on halvempaa kuin bluetooth-tekniikka. Infrapunatekniikka ei häiritse muita laitteita, on tehonkulutukseltaan pienempää ja on tietoturvallisempi kuin bluetooth-laitteet. Tietoturvallisuus johtuu lähinnä siitä, kun etäisyydet ovat todella pienet.

Infrapunatekniikkaa käyttävät lukuisat kauko-ohjaimet, kulunvalvontalaitteet, television ja stereoiden kauko-ohjaimet sekä autojen keskuslukitukset ja varashälyttimet. / 9 /

10.2 IEEE 802.11b eli wlan

WLAN eli Wireless Local Area Network on standardin 802.11b mukainen langaton yhteys. WLAN tekniikan suosio on kasvanut räjähdysmäisesti viime aikoina ja nykyään se onkin yleisin tietokoneissa käytettävä langaton tiedonsiirto tekniikka. Wlan tekniikka toimii samalla taajuusalueella kuin bluetoothkin ja tämän seurauksena nämä tekniikat eivät toimi kunnolla yhtä aikaa. Kummatkin tekniikat ovat alkujaan suunniteltu korvaamaan johtoja, mutta aikojen saatossa wlan:n käyttökohde on muuttunut, johtuen sen pitkästä toimintasäteestä ja paljon suuremmasta tiedonsiirto nopeudesta. On sanottu, että wlan ja bluetooth olisivat kilpailevia tekniikoita, mutta uskon niiden erilaisuudesta johtuen siihen, että nämä tekniikat täydentävät toisiansa.

Yleisin käyttökohde wlan:lle on Internet yhteyksien luominen, mutta nykyään wlan:t alkavat yleistymään myös matkapuhelimissa. Tulevaisuudessa en usko, että wlan menettää suosiotaan ennen, kuin markkinoille tulee tekniikka, joka täysin korvaa nykyisen. Koko ajan myös WLAN tekniikkaan panostetaan lisää tutkimustyötä, joten onkin luultavaa, että tämä tekniikka muuntautuu vuosien edetessä.

10.3 ZigBee

ZigBee on pienitehoinen, lyhyen kantaman radioliikenteen standardi IEEE 802.15.4 ja ZigBee tekniikka on valmistunut syyskuussa 2003. Ensisijaiseksi tarkoitukseksi ZigBee tekniikka on kehitelty pienten ja yksinkertaisten laitteiden langattomaan verkottamiseen. On ajateltu, että tekniikkaa käytettäisiin erityisesti kotien valaistuksen, ilmastoinnin, lämmityksen. automatisointiin ja teollisuudella olisi paljon käyttötarpeita tämäntyyliselle tekniikalle. Kuitenkin kyseinen tekniikka on vielä sen verran uusi, ettei sitä ole otettu käyttöön laajasti. ZigBee tekniikka ei ole suoranaisesti kilpaileva tekniikka bluetoothille, mutta varmasti tulevaisuudessa voi vaikuttaa

sen kehitykseen. ZigBee on jo alusta alkaen tehty yhteen sopivaksi monien valmistajien kanssa ja sen seurauksena ennustetaankin tekniikan leviämistä lähi tulevaisuudessa. On kuitenkin vielä tehtävä suunnittelutyötä ennen, kuin tekniikka alkaa yleistymään laajalti maailmalla. / 12 /

10.3 WUSB eli langaton USB

WUSB eli Wireless Universal Serial Bus on langaton USB. WUSB tekniikka perustuu täysin vanhaan USB arkkitehtuuriin. Perinteinen USB on erittäin suosittu kaikissa nykyisissä tietokoneissa. Tulevaisuuden suurena markkinavaltti on langattomuus, joten USB:stä haluttiin myös kehittää langaton versio. WUSB tekniikka onkin bluetooth:lle suoranainen kilpailija ja tulevaisuudessa nähdään, kuinka paljon WUSB tekniikka horjuttaa bluetoothin markkina arvoa.

WUSB käyttää (UWB) ultralaajakaista modulointi tekniikkaa, missä signaali lähetetään laajalle taajuusalueelle. WUSB käyttämä taajuusalue on 3.1GHz - 10.6GHz. WUSB maksimi tiedonsiirtonopeudeksi on luvattu 480 Mbps, mutta laitteiden etäisyys saa olla maksimissaan 10 metriä. Pitemmillä matkoilla tiedonsiirtonopeudeksi on luvattu 110 Mbps.
WUSB on saatu määriteltyä vuonna 2005 ja laitteet tulivat markkinoille jo vuoden 2005 lopussa. Kuitenkaan WUSB ei ole vielä levinnyt markkinoille läheskään niin kovalla tahdilla kuin perinteinen USB, mutta todennäköisesti se vielä valtaa markkinoita jo lähi tulevaisuudessa.
Tulevaisuudessa yritetään WUSB:n tiedonsiirtonopeutta kasvattaa 1 Gbps:n nopeuteen ja sen virrankulutusta yritetään parantaa. Odotetaankin, että vuonna 2008 WUSB sirujen pitäisi olla jo matkapuhelimissa. Koko ajan tehdään kovasti lisää kehitystyötä tämän tekniikan eteen. / 13 /

10.4 Bluetoothin tulevaisuus

Nykyään bluetooth-tekniikan käyttäminen on lisääntynyt paljon ja bluetooth-tekniikka onkin vakiinnuttanut asemansa langattomana tiedonsiirto tekniikkana. Suurimpana syynä tähän on ollut hands free -laitteiden yleistyminen, joten bluetooth-laitteita löytyy melkein jokaisesta matkapuhelimesta ja nykyään jo uusiin tietokoneisiin liitetään integroidut bluetooth-lähettimet. SIG järjestön tarvitseekin kehitellä koko ajan bluetooth-tekniikkaa eteenpäin tai muuten se jää uudistuvien tekniikoiden jalkoihin.

Nykyään SIG järjestö lupaa edr-tekniikan kehityttyä bluetoothin maksimi tiedonsiirtonopeudeksi 2.1 megabittiä sekunnissa. Pitää kuitenkin muistaa että, langattomien järjestelmien jatkuvassa kehityksessä myös niiden vaatimukset kasvavat, joten tulevaisuudessa bluetoothia yritetään kehittää toimivaksi UWB moduloinnilla. UWB modulointi takaisi paljon nopeammat yhteydet ja SIG järjestö onkin luvannut, että bluetooth-laitteet toimisivat jo vuonna 2007 480 Mbps nopeudella. Ensimmäinen kehitetty standardi sai nimekseen Lissabon ja Lissabonia on laajennettu toisen asteen standardiksi, jonka nimeksi on annettu Seatle. Ensimmäisessä standardissa kehitettiin standardin ydin ja edr-laajennukset. Toisen asteen standardissa kehitellään UWB yhteen sopivuus MAC-määritysten kanssa. Nopean bluetoothin kanssa on vielä kuitenkin monenlaisia ongelmia ja suurin näistä varmasti on radiotaajuuksien sopiminen. Siihen kuitenkin pitäisi tulla sopimus vuoden 2006 aikana.

Jos bluetooth-tekniikka saadaan toimimaan yhtä nopealla yhteydellä, kuin langaton USB, niin sen tulevaisuuden näkymät parantuvat huomattavasti. Jos taas SIG järjestö ei saa nopeuksia nousemaan huomattavasti, niin bluetooth jää varmasti muiden tekniikoiden jalkoihin. Tosin bluetooth on vakiinnuttanut asemansa aika hyvin pienten ja yksinkertaisten laitteiden tiedonsiirto järjestelmänä. Tarkoitan tässä juuri nimenomaan Hands free laitteita ja muita matkapuhelimen oheislaitteita. Yleistyminen matkapuhelin tekniikkaan vaikuttaa suuresti, kun bluetooth-tekniikka on yhteen sopiva monien valmistajan kesken ja bluetoothin standardit ovat avoimia kaikille. Kuitenkin on vielä paljon jossittelua, mutta tulevaisuus sen näyttää mihin bluetooth tekniikan elämänkaari kääntyy. / 14 /

LÄHTEET

Painetut lähteet

1 Granlund, Kaj , 2001 : *Langaton tiedonsiirto*, Porvoo : WS Bookwell

2 Haapala, Juha , 2004 : *Bluetooth – teoriaa ja käytäntöä*, Turun ammattikorkeakoulun raportteja 24

3 Kontio – Tervo – Jääskeläinen – Arokoski – Vierimaa – Raatikainen – Köykkä, 2002 : *Mobiiliteknologiat*, Helsinki : Edita Prima Oy

4 Lehto, Tero : *Bluetooth*
Tietokone 10/2005, s.36 - 38

5 Miller, Brent.A & Bisdikian, Chatschik, 2002 : *Bluetooth revealed*, Prentice Hall, USA

6 Muller, Nathan. J, 2001 : *Bluetooth demystifield*, McGraw Hill, USA

7 Ranta-Ojala, Juha, Tietokone tekniikan kurssi monisteet

Sähköiset lähteet

8 Jyrki Oraskari [www-sivu] saatavissa:
http://users.tkk.fi/~joraskur/bluetooth.html

9 Huttunen Jari ; Ylijoki, Mikael, Tietoverkkotekniikan seminaari 2002 [www-sivu] saatavissa:
http://www.netlab.hut.fi/opetus/s38119/k02/raportti.pdf

10 Pekka Laitinen, Tietoliikennetekniikan raportti [www-sivu] saatavissa :
http://batman.jypoly.fi/~19346/harjoitustyot/bluetooth/boikea.htm

11 Bluetoothin tietoturvasta [www-sivu] saatavissa:
http://www.tol.oulu.fi/~avesanen/Langaton_TT/luennot/wlan/Bluetooth.html

12 Zigbee – Wikipedia [www-sivu].[viitattu 9.1.-05] saatavissa:
http://fi.wikipedia.org/wiki/Zigbee

13 WUSB – Wikipedia [www-sivu].[viitattu 9.1.-05] saatavissa:
http://fi.wikipedia.org/wiki/WUSB

14 Tietokonelehti [www.sivu].[viitattu 9.1.-05] saatavissa:
http://www.tietokone.fi/uutta/uutinen.asp?news_id=25386&tyyppi=1

LIITTEET

/ 1 / Bluetooth-sanomien rakenteen kokonaiskuva.

LIITE 1 Bluetooth-sanomien rakenteen kokonaiskuva.